silver peak™

Silver Peak
Global Management System

Operator's Guide

GMS 7.1

February 2015

PN 200095-001 Rev M

Silver Peak Global Management System Operator’s Guide

Document PN 200095-001 Rev M

Date: February 2015

Trademark Notification

Silver Peak Systems^{TM}, the Silver Peak logo, Network Memory^{TM}, and Silver Peak NX-Series^{TM} are trademarks of Silver Peak Systems, Inc. All trademark rights reserved. All other brand or product names are trademarks or registered trademarks of their respective companies or organizations.

Warranties and Disclaimers

THIS DOCUMENTATION IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. SILVER PEAK SYSTEMS, INC. ASSUMES NO RESPONSIBILITY FOR ERRORS OR OMISSIONS IN THIS DOCUMENTATION OR OTHER DOCUMENTS WHICH ARE REFERENCED BY OR LINKED TO THIS DOCUMENTATION. REFERENCES TO CORPORATIONS, THEIR SERVICES AND PRODUCTS, ARE PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED. IN NO EVENT SHALL SILVER PEAK SYSTEMS, INC. BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT OR CONSEQUENTIAL DAMAGES OF ANY KIND, OR ANY DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, THOSE RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER OR NOT ADVISED OF THE POSSIBILITY OF DAMAGE, AND ON ANY THEORY OF LIABILITY, ARISING OUT OF OR IN CONNECTION WITH THE USE OF THIS DOCUMENTATION. THIS DOCUMENTATION MAY INCLUDE TECHNICAL OR OTHER INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN; THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THE DOCUMENTATION. SILVER PEAK SYSTEMS, INC. MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED IN THIS DOCUMENTATION AT ANY TIME.

Silver Peak Systems, Inc.
2860 De La Cruz Boulevard, Suite 100
Santa Clara, CA 95050

1.877.210.7325 (toll-free in USA)
+1.408.935.1850

http://www.silver-peak.com/support

Contents

Preface

The Silver Peak Global Management System (GMS) provides simplified appliance configuration for rapid, large-scale deployment of Silver Peak appliances in your network.

Who Should Read This Manual?

Anyone who wants to centrally manage Silver Peak appliances should read this manual. Users should have some background in Windows® terminology, Web browser operation, and a knowledge of where to find the TCP/IP and subnet mask information for your system.

Manual Organization

This section outlines the chapters and summarizes their content.

Chapter 1, "Getting Started," provides an overview of the Silver Peak Global Management System's functions and features and a summary of the tasks for getting started.

Chapter 2, "Configuration Templates," describes how to use the **Configuration** templates to manage appliances and appliance objects.

Chapter 3, "Network & Policy Configuration Tabs," describes the read-only reports that display appliance configuration parameters.

Chapter 4, "Appliance Administration," describes the read-only reports that display appliance administration parameters.

Chapter 5, "Alarms & Threshold Crossing Alerts," describes alarm categories and definitions. It also describes how to configure, view, and handle alarm notifications. Additionally, it describes threshold crossing alerts, which are pre-emptive, user-configurable thresholds that declare a Major alarm when crossed.

Chapter 6, "Monitoring Status and Performance," focuses on traffic- and performance-related reports.

Chapter 7, "GMS Administration," describes the administrative tasks that directly relate to managing **GMS-related events and tasks only**. These activities do not relate to managing appliances.

Chapter 8, "Maintenance and Support," describes the activities related to maintaining the appliances. This includes database and software image management, as well as reboot operations.

Appendix A, "TCP/IP Ports Used by the GMS and Silver Peak Appliances,"uses tables and diagrams to list the ports that the GMS and use for TCP/IP.

Support

For product and technical support, contact Silver Peak Systems at either of the following:

- **1.877.210.7325 (toll-free in USA)**
- **+1.408.935.1850**
- **www.silver-peak.com/support**

We're dedicated to continually improving the usability of our products and documentation.

- If you have suggestions or feedback for our documentation, please send an e-mail to **techpubs@silver-peak.com**.
- If you have comments or feedback about the GUI's ease of use, please send an e-mail to **usability@silver-peak.com**.

CHAPTER 1

Getting Started

This chapter outlines the typical tasks involved in setting up the Global Management System (GMS) and using it to monitor and manage your Silver Peak appliances.

In This Chapter

Overview

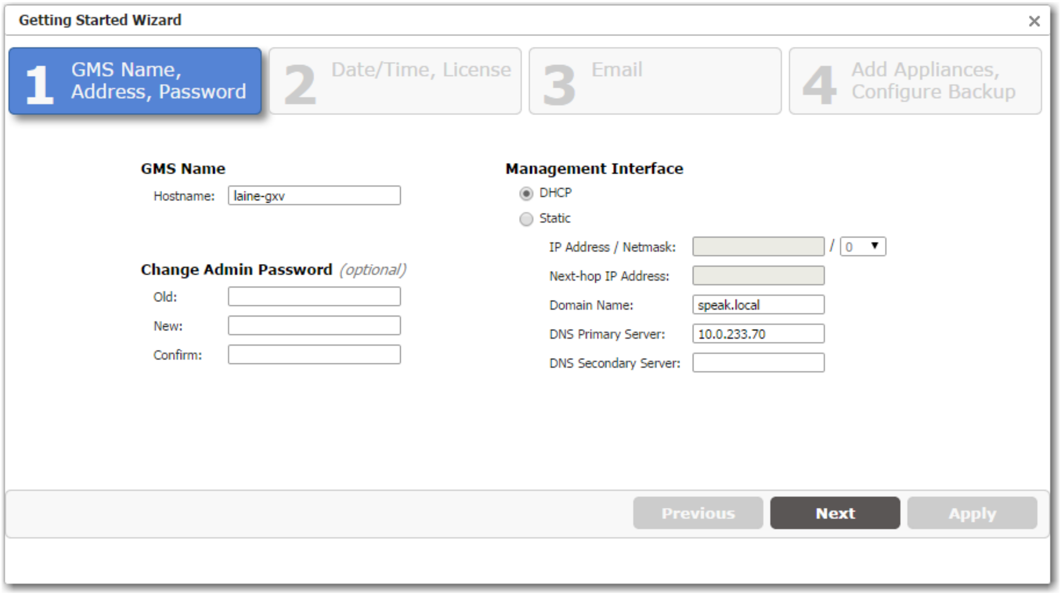
Use the GMS to globally monitor performance and manage Silver Peak appliances.

This section discusses the following:

- **Completing the Getting Started Wizard** See page 2.
- **Assumptions** See page 3.
- **What to Configure Next** See page 4.
- **Understanding Topology and Layout** See page 6.

Completing the Getting Started Wizard

After you first install the GMS and use a web browser to go to the IP address you've assigned it, the **Getting Started Wizard** appears.



Getting Started Wizard

GMS Name

Hostname: laine-gxv

Change Admin Password *(optional)*

Old:

New:

Confirm:

Management Interface

● DHCP

○ Static

IP Address / Netmask: / 0

Next-hop IP Address:

Domain Name: speak.local

DNS Primary Server: 10.0.233.70

DNS Secondary Server:

×
1 GMS Name, Address, Password
2 Date/Time, License
3 Email
4 Add Appliances, Configure Backup
Previous
Next
Apply

It takes you through the basics of configuring the following:

- **GMS Name**, management IP **address**, and **password**
  - The default for username and password is **admin**.
- **Date/Time**, **License**
  - Silver Peak strongly recommends using an NTP server so that data across the GMS and appliances is synchronized.
  - When upgrading an existing physical GMS, no **License** field displays.
- **Email**
  - Default settings are provided. You can change and test values. [*Optional*]
  - GMS reports are sent to all specified recipients. The entered email addresses populate the **Email Recipients** field on the **Monitoring > Schedule & Run Reports** tab.
- **Add Appliances, Configure Backup**
  - [*Optional*] You can add appliances that are up and running, assign them a **Network Role** (Mesh, Hub, or Spoke) for use in creating tunnels, change their GMS **Admin** password, and specify which protocol(s) to use when communicating with the GMS.

- [*Optional*] When using the GMS web interface, you can only configure the GMS backup in the wizard. Once specified, the backup runs once every 7 days and is kept indefinitely. In this release, you can only review and/or restore GMS backups by using the Command Line Interface (CLI).

If you don't **Apply** the configuration after you complete the last screen, the wizard reappears at the next login.

To access the wizard after initial configuration, go to **GMS Administration > Getting Started Wizard**.

Assumptions

The assumptions here are as follows:

- Any appliance that you add has already been deployed with Appliance Manager, either ***in-line*** (Bridge mode) or ***out-of-path*** (Router or Server[1] modes).
- Any necessary flow redirection is already configured on the appliance and, if necessary, the appropriate router.

For detailed appliance configuration information, refer to the *Appliance Manager Operator's Guide*. Also see the *Network Deployment Guide* for specific scenarios.

[1] **Server mode** is a subset of Router mode. It uses one interface for both management and datapath traffic.

What to Configure Next

Initially, you'll configure the more generic items. For example:

1 You'll **add users** to the GMS server database. By default, the GMS uses this local database for authentication. However, you can also to point to a RADIUS or TACACS+ server for that function.

Related Menus

GMS Administration > User Management
GMS Administration > Authentication

For more information, see "Managing GMS User Accounts and Authentication" on page 9.

2 In the Navigation Pane, use contextual menus to **create a group** or groups to which you'll assign each appliance. For example, you may choose to create a group for Engineering or Finance.

3 If you didn't **add the appliances** while completing the **Getting Started Wizard**, it's time to add them now. Use the GMS wizard or add them to your ready-made group with contextual menus.

As soon as you add an appliance, the GMS establishes communication. All of the appliance's existing configuration, alarm, and statistical data is available immediately.

If you're adding appliances that were deployed with an earlier release that didn't have the subnet sharing feature, then go to Maintenance > Migrate GMS Route Maps to simplify routing management.

4 **Create and apply configuration templates**. Create templates for non-unique variables and apply across one or more appliances. They include templates for SNMP, DNS, date and time, tunnel characteristics, SSL certificates, web-related parameters, user-defined applications, policies, logging, etc.

For more information, see Chapter 2, "Configuration Templates."

IMPORTANT: Templates will **REPLACE** all settings on the appliance with the template settings unless the template has a **MERGE** option and that option is selected.

However, in the case of templates for policies (Route, Optimization, QoS) and ACLs:

- You can create template rules with priority from **1000 – 9999**, inclusive. When you apply the template to an appliance, the GMS deletes all appliance entries in that range before applying its policies.
- If you access an appliance directly (via the WebUI or the command line interface), you can create rules that have higher priority (**1 – 999**) than GMS rules and rules that have lower priority (**10000 – 65534**).

Related Menus

Configuration > Templates

5 **Subnet sharing** is a method for automatically routing a flow into the appropriate tunnel for optimization based on destination IP alone. The appliance builds a subnet table from entries added automatically by the system or manually by a user. When two appliances are connected by a tunnel, they exchange this information ("learn" it) and use it to route traffic to each other.

Locally connected networks are automatically added to the subnet table. You will need to add any additional local subnets manually.

For more information, see "Adding to the Subnet Table" on page 10.

Related Menus

Configuration > Subnets

6 If **tunnels** don't already exist, then:

- You can enable each appliance's **auto tunnel** feature. This feature automatically creates tunnels between Silver Peak appliances that have network connectivity and active flows.

  Related Menus

  Configuration > Templates > System

- If you prefer to retain more control and configure the tunnels yourself, you can disable the **auto tunnel** feature in the appliance's system configuration and create the configurations manually.

  Related Menus

  Configuration > Templates > System
  Configuration > Templates > Tunnels
  Configuration > Tunnels
  Configuration > Tunnel Builder

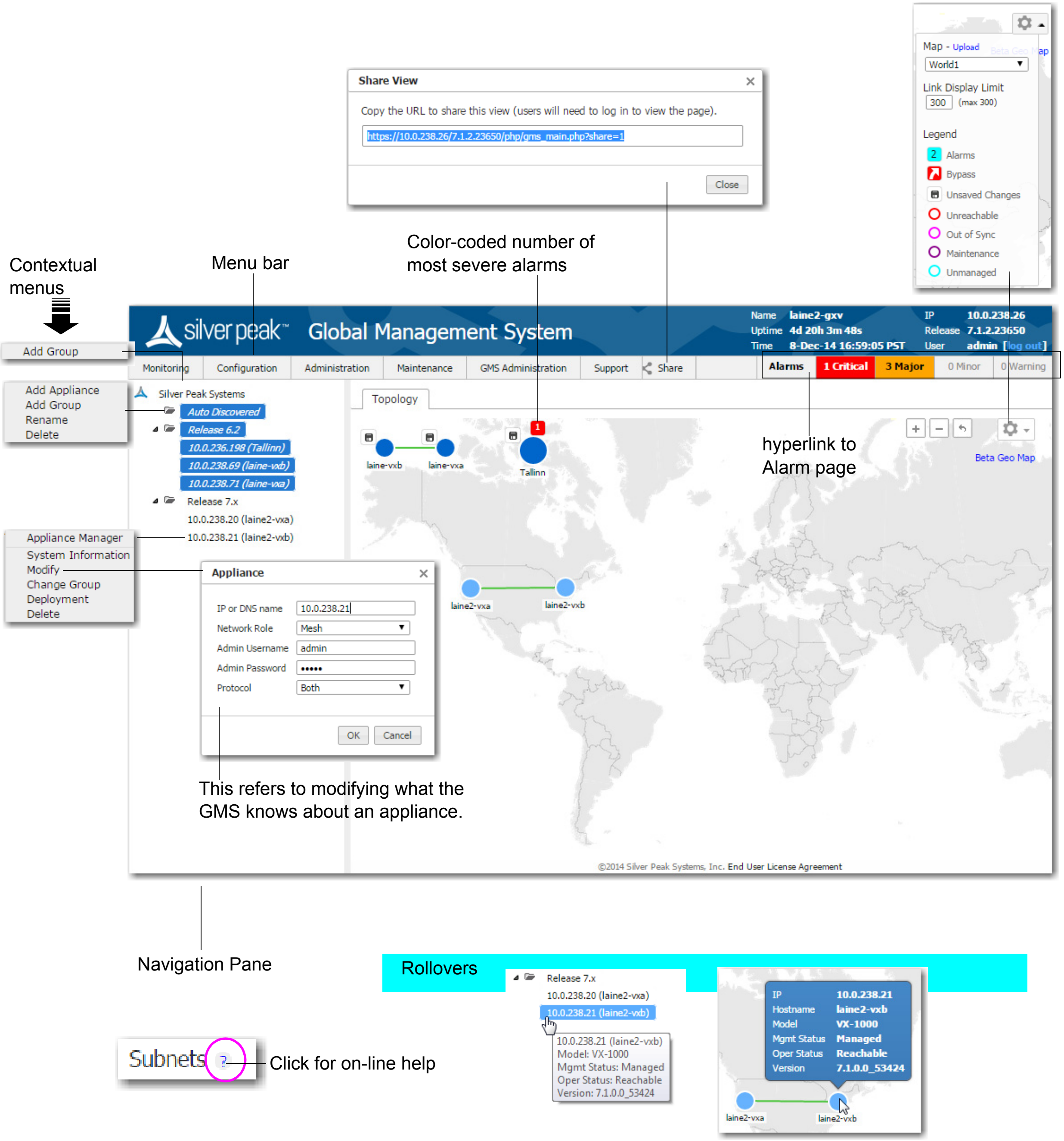
7 Generate your first reports.

For more information, see "Configuring and Distributing Custom Reports" on page 110.

Related Menus

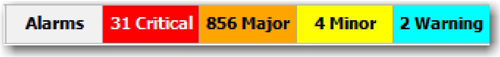
Monitoring > Schedule & Run Reports

Understanding Topology and Layout



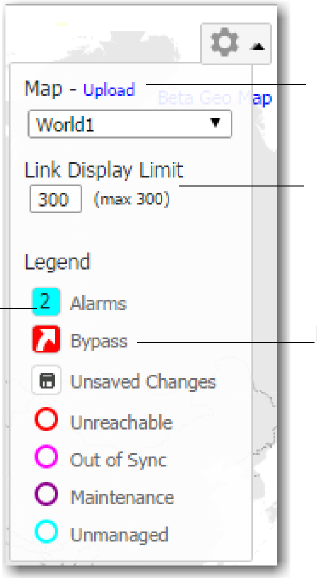
Alarms

- The **Alarms Summary** shows the total number of GMS and appliance alarms, and color-codes them.
- Click the summary bar to hyperlink to the **Alarms** page.


Alarms 31 Critical 856 Major 4 Minor 2 Warning

Topology Settings & Legend

- The **Legend** details the appliances' management and operational states.



Map - Upload

World1 ▼

Link Display Limit

300 (max 300)

Legend

Upload a topology map of your own, or select from the drop-down list

Maximum number of tunnels to draw on the map

Number of most severe alarms on appliance. This one shows two **Warnings**.

Refers to *hardware bypass*

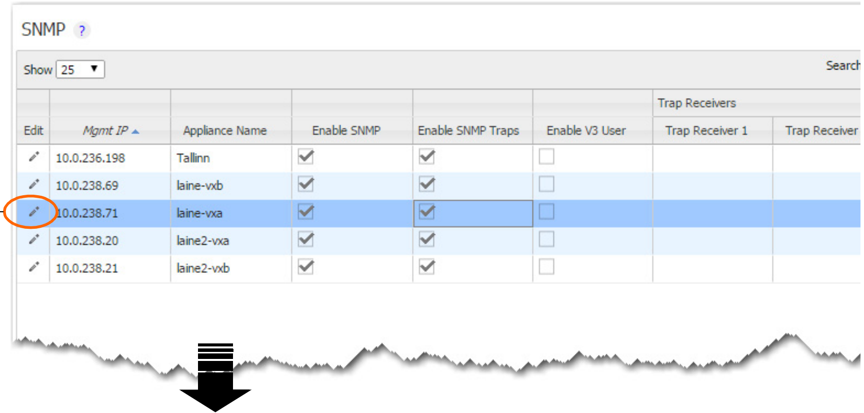
- **Bypass** refers to ***hardware bypass***. If there is a major problem with the appliance hardware, software, or power, all traffic goes through the appliance without any processing. Additionally, you can manually put the appliance into **Bypass** mode as an aid to troubleshooting or during maintenance events.
- If an appliance displays **Unsaved Changes**, you must log into the appliance directly to save the changes.
- An **Unreachable** appliance is one that the GMS can't contact.
- The GMS acts as configurations cache for the appliances.When the GMS doesn't have a configuration cache from an appliance, it is **Out Of Sync**.
- When an appliance is **Out Of Sync**, it first cycles through the **Maintenance** state before being managed again. Typically, this is a short cycle.
- An appliance is **Unmanaged** when the GMS software version doesn't support the appliance's software version.

Other

- Tunnel states are color-coded, and rollover with the mouse displays the state. For example, **Up**.
- Tables are sortable by column.

- Clicking the **Edit** icon provides direct access to editing a specific appliance by opening the corresponding Appliance Manager page in a separate browser tab.

[GMS]



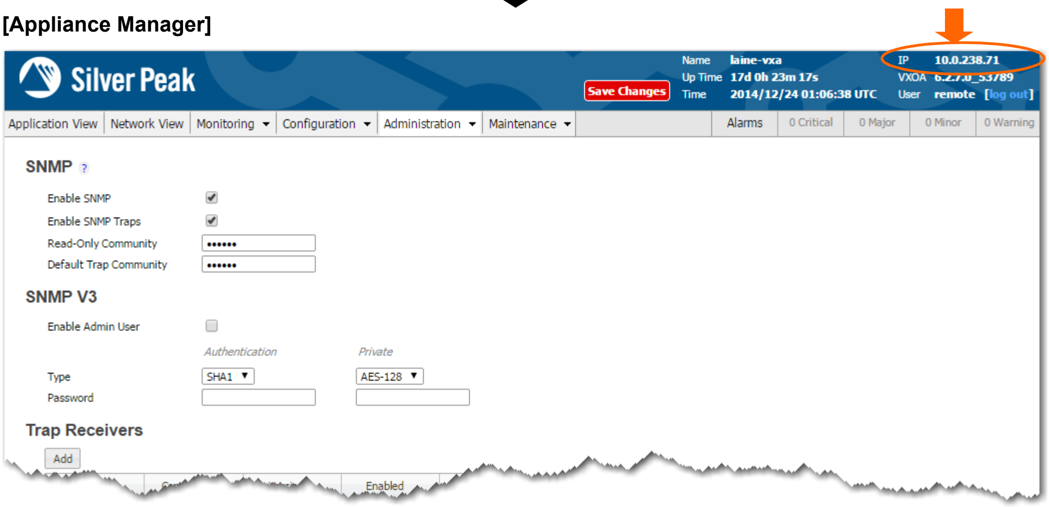
SNMP ?

Show 25 ▼ Search

Edit	Mgmt IP ▲	Appliance Name	Enable SNMP	Enable SNMP Traps	Enable V3 User	Trap Receivers	
						Trap Receiver 1	Trap Receiver
✎	10.0.236.198	Tallinn	☑	☑	□		
✎	10.0.238.69	laine-vxb	☑	☑	□		
✎	10.0.238.71	laine-vxa	☑	☑	□		
✎	10.0.238.20	laine2-vxa	☑	☑	□		
✎	10.0.238.21	laine2-vxb	☑	☑	□		

Click to open Appliance Manager for this **mgmt0** IP address

[Appliance Manager]



Name laine-vxa
Up Time 17d 0h 23m 17s
Time 2014/12/24 01:06:38 UTC
IP 10.0.238.71
VXOA 6.2.7.0_53789
User remote [log out]

SNMP ?

Enable SNMP ☑
Enable SNMP Traps ☑
Read-Only Community ••••••
Default Trap Community ••••••

SNMP V3

Enable Admin User □

	Authentication	*Private*
Type	SHA1 ▼	AES-128 ▼
Password		

Trap Receivers

Add

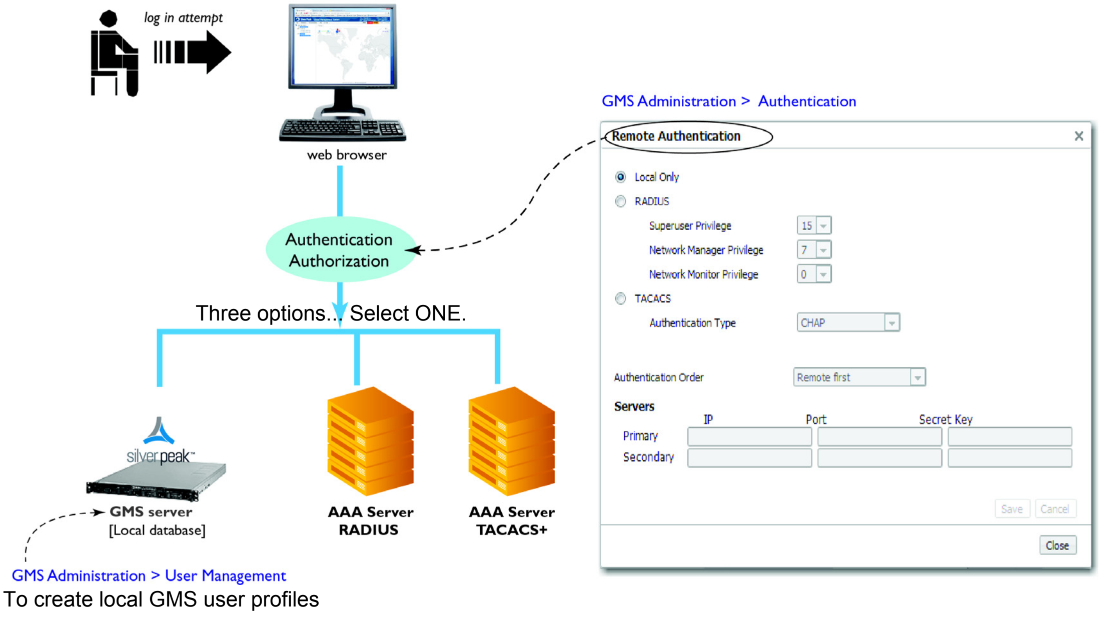
Enabled

Managing GMS User Accounts and Authentication

For a user to successfully log into the GMS client, the GMS server must authenticate and authorize the user. Only then does the user have access to the GMS server and, by extension, the appliances.

Based on its configuration, the GMS authenticates the user via its own built-in local database or via a network server used for access control.

- The AAA server (Authentication Authorization Accounting server) can be either a **RADIUS** server or a **TACACS+** server.
- Add users to the GMS server's local database via the GMS client's **GMS Administration > User Management** menu. The user profile includes the user role, which maps to a particular level of authorization and determines what the user can do.



● Local Only

○ RADIUS

Superuser Privilege: 15

Network Manager Privilege: 7

Network Monitor Privilege: 0

○ TACACS

Authentication Type: CHAP

Authentication Order: Remote first

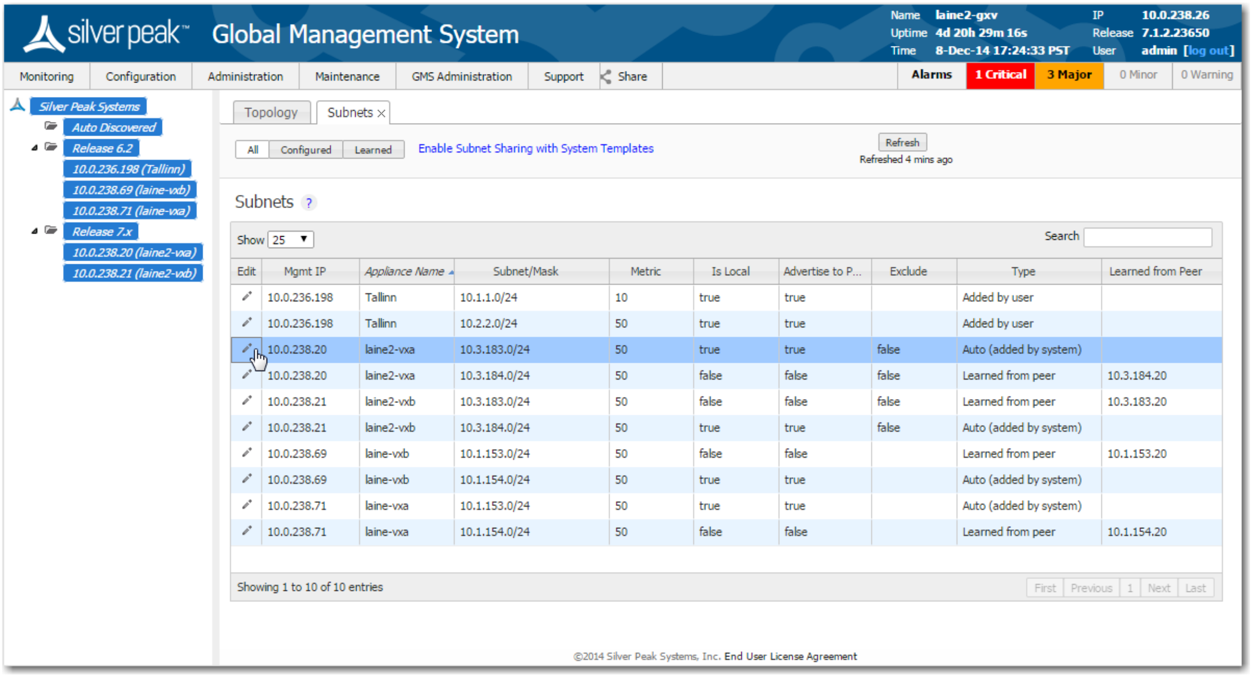
Servers

	IP	Port	Secret Key
Primary			
Secondary			

- GMS has three user roles: ***Admin Manager (Superuser)***, ***Network Manager***, and ***Network Monitor***. Authorization always maps to one of these three levels:
  - ***Admin Manager*** has all privileges. It's the equivalent of ***Superuser.***
  - ***Network Manager*** has read/write privileges. In practice, these are the same privileges that Admin Manager has.
  - ***Network Monitor*** has view-only privileges.
- Although there are three authentication options to choose from, you can only configure one.
  - If **Local Only** is selected, then authentication defaults to the GMS server's local database.
  - If **Local Only is not** selected, then either a (remote) **RADIUS** or **TACACS+** server is also involved.
    - If **Remote first** is selected and fails, then the GMS tries the **Local** database.
    - If **Local first** is selected and fails, then the GMS tries the **Remote** database.
- The **Secret Key** enables the GMS to talk to the access control server. The GMS has hard-coded keys for TACACS+, so no user entry is required.
- You can also use GMS templates to create remote authentication profiles for direct access to individual appliances via Appliance Manager or the CLI. Be aware, though, that that is different than creating a remote authentication profile for the GMS.

Adding to the Subnet Table

To add, edit, or delete a subnet, you must select an individual subnet from the navigation panel and click in **Edit**. That opens a new browser tab on the specific appliance’s **Subnets** page.



Name laine2-gxv
Uptime 4d 20h 29m 16s
Time 8-Dec-14 17:24:33 PST
IP 10.0.238.26
Release 7.1.2.23650
User admin [log out]

Refreshed 4 mins ago

Subnets ?

Show 25

Edit	Mgmt IP	Appliance Name	Subnet/Mask	Metric	Is Local	Advertise to P...	Exclude	Type	Learned from Peer
✎	10.0.236.198	Tallinn	10.1.1.0/24	10	true	true		Added by user	
✎	10.0.236.198	Tallinn	10.2.2.0/24	50	true	true		Added by user	
✎	10.0.238.20	laine2-vxa	10.3.183.0/24	50	true	true	false	Auto (added by system)	
✎	10.0.238.20	laine2-vxa	10.3.184.0/24	50	false	false	false	Learned from peer	10.3.184.20
✎	10.0.238.21	laine2-vxb	10.3.183.0/24	50	false	false	false	Learned from peer	10.3.183.20
✎	10.0.238.21	laine2-vxb	10.3.184.0/24	50	true	true	false	Auto (added by system)	
✎	10.0.238.69	laine-vxb	10.1.153.0/24	50	false	false		Learned from peer	10.1.153.20
✎	10.0.238.69	laine-vxb	10.1.154.0/24	50	true	true		Auto (added by system)	
✎	10.0.238.71	laine-vxa	10.1.153.0/24	50	true	true		Auto (added by system)	
✎	10.0.238.71	laine-vxa	10.1.154.0/24	50	false	false		Learned from peer	10.1.154.20

Showing 1 to 10 of 10 entries

©2014 Silver Peak Systems, Inc. End User License Agreement

What is subnet sharing ?

Subnet sharing is one of the three strategies that Silver Peak uses to auto-optimize all IP traffic, automatically directing flows to the appropriate tunnel. Auto-optimization strategies reduce the need to create explict route map entries to optimize traffic. The other two strategies are **TCP-based** auto-opt and **IP-based** auto-opt.

Note Enabled by default, the global settings for all three reside on the **Templates** tab, under **System**.

How is subnet sharing implemented?

Each appliance builds a subnet table from entries added automatically by the system and manually by a user. When two appliances are connected by a tunnel, they exchange this information ("learn" it) and use it to route traffic to each other.

When would you need to use a Route Policy template?

Subnet sharing takes care of optimizing IP traffic.

Use and apply a Route Policy template for flows that are to be:

- sent pass-through (shaped or unshaped)
- dropped
- configured for a specific high-availability deployment
- routed based on application, ports, VLAN, DSCP, or ACL (Access Control List)

Subnet table columns

- **Subnet/Mask:** Actual subnet to be shared or learned
- **Metric:** Metric of the subnet. Value must be between 0 and 100. When a peer has more than one tunnel with a matching subnet (for example, in a high availability deployment), it chooses the tunnel with the greater numerical value.
- **Is Local:** Specifies if the subnet is local to this site.

  The appliance sets this parameter for **automatically** for locally connected subnets of the appliance.

  Also, you can select the parameter when manually adding a subnet:

  - Select this option for a **manually** added subnet if all the IP addresses in the subnet are known to be local.
  - Deselect this option if the subnet is so large (for example, 0.0.0.0/0) that it may include IP addresses that are not local to this appliance. If a subnet is too wide, and it's marked **local**, then the stats will count any pass-through packets with an IP address within that range as WAN-to-LAN.
- **Exclude:** Use this option to prevent optimization of more specific subnets from a wider advertised subnet range.
- **Advertise to Peers:** Selected by default, it shares the subnet information with peers. Peers then learn it. To add a subnet to the table without divulging it to peers, yet, deselect this option.
- **Type** of subnet:
  - **Auto (added by system)** = automatically added subnets of interfaces on this appliance
  - **Added by user** = manually added/configured subnets for this appliance
  - **Learned from peer** = subnets added as a result of exchanging information with peer appliances
- **Learned from Peer:** Which peer appliance advertised (and shared) this subnet information

CHAPTER 2

Configuration Templates

This chapter describes how to use the **Configuration** templates to manage appliances and appliance objects.

It acts as a reference and follows the order of the items in the **Configuration** menu.

In This Chapter

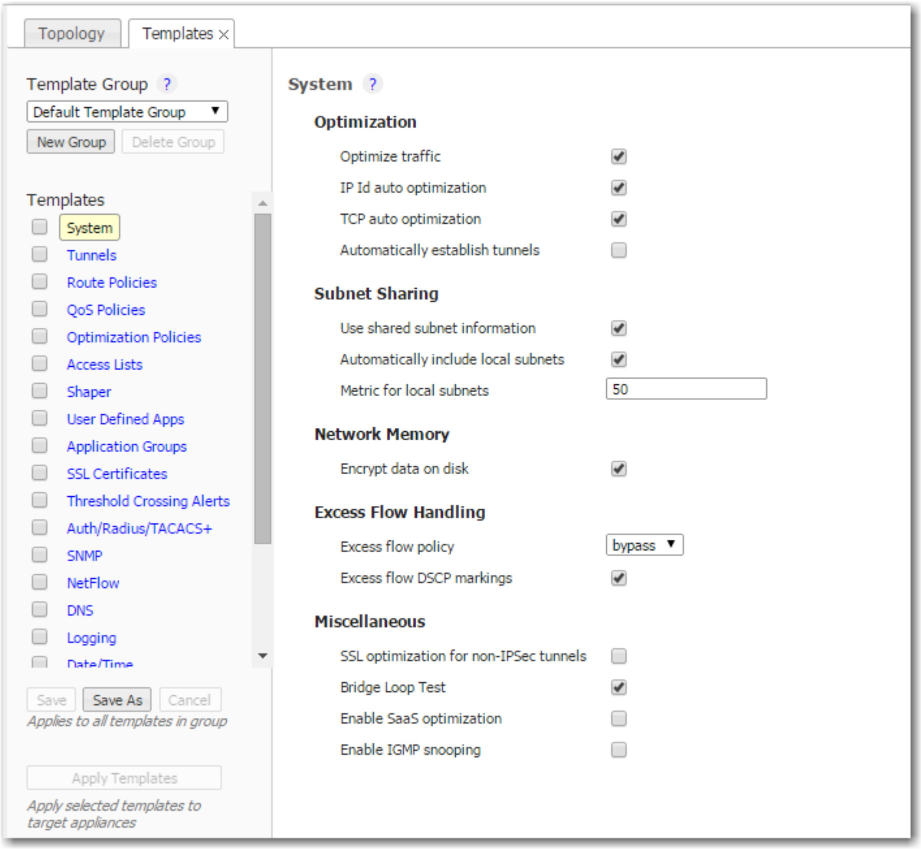
Using Configuration Templates

A ***Template Group*** is a collection of templates used to configure settings across multiple appliances.

- **IMPORTANT:** Templates will **REPLACE** all settings on the appliance with the template settings unless the template has a **MERGE** option and that option is selected.
- To edit a template, click the template label next to its checkbox.
- You cannot save changes to the **Default Template Group**. To save the edits as a new template group, click **Save As**.
- To apply templates to appliances selected in the tree, select the desired template checkbox(es) and click **Apply Templates**. A dialog appears, asking you to confirm your choices.
- There is no permanent association between a template and an appliance - it's a one-time, one-way action.
- When returning to the **Templates** page, the **Template Group** field defaults to showing the last template group viewed.
- Unsaved changes display as an icon to the right of the template label.

System Template

Use this page to configure system-level features.



Templates

- □ System
- □ Tunnels
- □ Route Policies
- □ QoS Policies
- □ Optimization Policies
- □ Access Lists
- □ Shaper
- □ User Defined Apps
- □ Application Groups
- □ SSL Certificates
- □ Threshold Crossing Alerts
- □ Auth/Radius/TACACS+
- □ SNMP
- □ NetFlow
- □ DNS
- □ Logging
- □ Date/Time

Applies to all templates in group

Apply selected templates to target appliances

System ?

Optimization

Optimize traffic	☑
IP Id auto optimization	☑
TCP auto optimization	☑
Automatically establish tunnels	□

Subnet Sharing

Use shared subnet information	☑
Automatically include local subnets	☑
Metric for local subnets	50

Network Memory

Encrypt data on disk	☑

Excess Flow Handling

Excess flow policy	bypass ▼
Excess flow DSCP markings	☑

Miscellaneous

SSL optimization for non-IPSec tunnels	□
Bridge Loop Test	☑
Enable SaaS optimization	□
Enable IGMP snooping	□

Optimization

- **Optimize traffic** is a global setting for turning optimization on or off. Useful for comparing statistics before and after.
- **IP Id auto optimization** enables any IP flow to automatically identify the outbound tunnel and gain optimization benefits. Enabling this option reduces the number of required static routing rules (route map policies).
- **TCP auto optimization** enables any TCP flow to automatically identify the outbound tunnel and gain optimization benefits. Enabling this option reduces the number of required static routing rules (route map policies).
- **Automatically establish tunnels** reduces configuration overhead by removing the need to manually create tunnels.

Subnet Sharing

- **Use shared subnet information** enables Silver Peak appliances to use the shared subnet information to route traffic to the appropriate tunnel. Subnet sharing eliminates the need to set up route maps in order to optimize traffic.
- **Automatically include local subnets** adds the local subnet(s) to the appliance subnet information.
- **Metric for local subnets** is a weight that is used for subnets of local interfaces. When a peer has more than one tunnel with a matching subnet, it chooses the tunnel with the greater numerical value.

Network Memory

- **Encrypt data on disk** enables encryption of all the cached data on the disks. Disabling this option is not recommended.

Excess Flow Handling

- **Excess flow policy** specifies what happens to flows when the appliance reaches its maximum capacity for optimizing flows. The default is to bypass flows. Or, you can choose to drop the packets.
- **Excess flow DSCP markings** specifies whether the appliance should continue to set DSCP markings for flows that are beyond appliance's capacity to optimize.

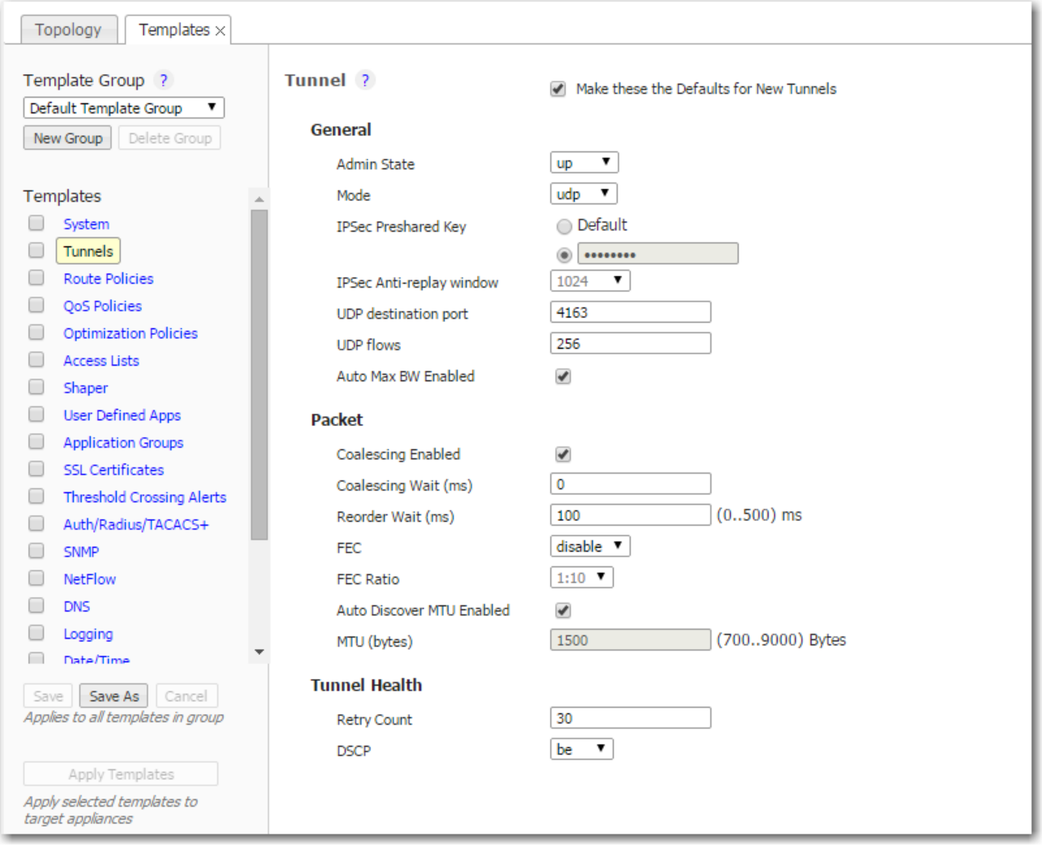
Miscellaneous

- **SSL optimization for non-IPSec tunnels** specifies if the appliance should perform SSL optimization when the outbound tunnel for SSL packets is not encrypted (for example, a GRE or UDP tunnel). To enable Network Memory for encrypted SSL-based applications, you must provision server certificates via the Silver Peak GMS. This activity can apply to the entire distributed network of Silver Peak appliances, or just to a specified group of appliances.
- **Bridge Loop Test** is only valid for virtual appliances. When enabled, the appliance can detect bridge loops. If it does detect a loop, the appliance stops forwarding traffic and raises an alarm. Appliance alarms include recommended actions.
- **Enable SaaS optimization** enables the appliance to determine what SaaS applications/services it can optimize. It does this by contacting Silver Peak's portal and downloading SaaS IP address and subnet information.
- **Enable IGMP Snooping**. IGMP snooping is a common layer-2 LAN optimization that filters the transmit of multicast frames only to ports where multicast streams have been detected. Disabling this feature floods multicast packets to all ports. IGMP snooping is recommended and enabled by default.

Tunnels Template

Use this template to assign and manage **tunnel properties**.

- Tunnel templates can be applied to any appliances (with or without tunnels). However, only existing tunnels can accept the template settings. To enable an appliance to apply these same settings to future tunnels, select **Make these the Defaults for New Tunnels**.
- Applying tunnel templates does not create new tunnels. To create tunnels, use the **Tunnel Builder** tab.
- To **view**, **edit**, and **delete** tunnels, use the **Tunnels** tab.



☑ Make these the Defaults for New Tunnels

General

Admin State: up
Mode: udp
IPSec Preshared Key: ○ Default ● ••••••••
IPSec Anti-replay window: 1024
UDP destination port: 4163
UDP flows: 256
Auto Max BW Enabled: ☑

Packet

Coalescing Enabled: ☑
Coalescing Wait (ms): 0
Reorder Wait (ms): 100 (0..500) ms
FEC: disable
FEC Ratio: 1:10
Auto Discover MTU Enabled: ☑
MTU (bytes): 1500 (700..9000) Bytes

Tunnel Health

Retry Count: 30
DSCP: be

Definitions (alphabetically)

- **Admin State** brings the tunnel **Up** or **Down**.
- **Auto Discover MTU Enabled** allows an appliance to determine the best MTU to use.
- **Auto Max BW Enabled** allows the appliances to auto-negotiate the maximum tunnel bandwidth.
- **Coalescing Enabled** allows the appliance to coalesce smaller packets into larger packets.
- **Coalescing Wait (ms)** is the number of milliseconds that the appliance should hold packets while attempting to coalesce smaller packets into larger ones.
- **DSCP** determines which DSCP marking the keep-alive messages should use.
- **FEC** (Forward Error Correction) can be set to enable, disable, and auto.
- **FEC Ratio** is an option when FEC is set to auto, that specifies the maximum ratio. The options are 1:2, 1:5, 1:10, or 1:20.

- **IPSec Anti-replay window** provides protection against an attacker duplicating encrypted packets by assigning a unique sequence number to each encrypted packet. The decryptor keeps track of which packets it has seen on the basis of these numbers. The default window size is 64 packets.
- **IPSec Preshared Key** is a shared, secret string of Unicode characters that is used for authentication of an IPSec connection between two parties.
- **Mode** determines whether the tunnel is **udp**, **gre**, or **ipsec**. Tunnel modes must match at both ends of the tunnel.
- **MTU (bytes)** (Maximum Transmission Unit) is the largest possible unit of data that can be sent on a given physical medium. For example, the default MTU of Ethernet is 1500 bytes. Silver Peak provides support for MTUs up to 9000 bytes.
- **Reorder Wait (ms)** is the number of milliseconds to allow for out-of-order packets to reorder. The default value is 100 ms.
- **Retry Count** is the number of failed keep-alive messages that are allowed before the appliance brings the tunnel down.
- **UDP destination port** is used in UDP mode. Accept the default value unless the port is blocked by a firewall.
- **UDP flows** is the number of flows over which to distribute tunnel data. Accept the default.

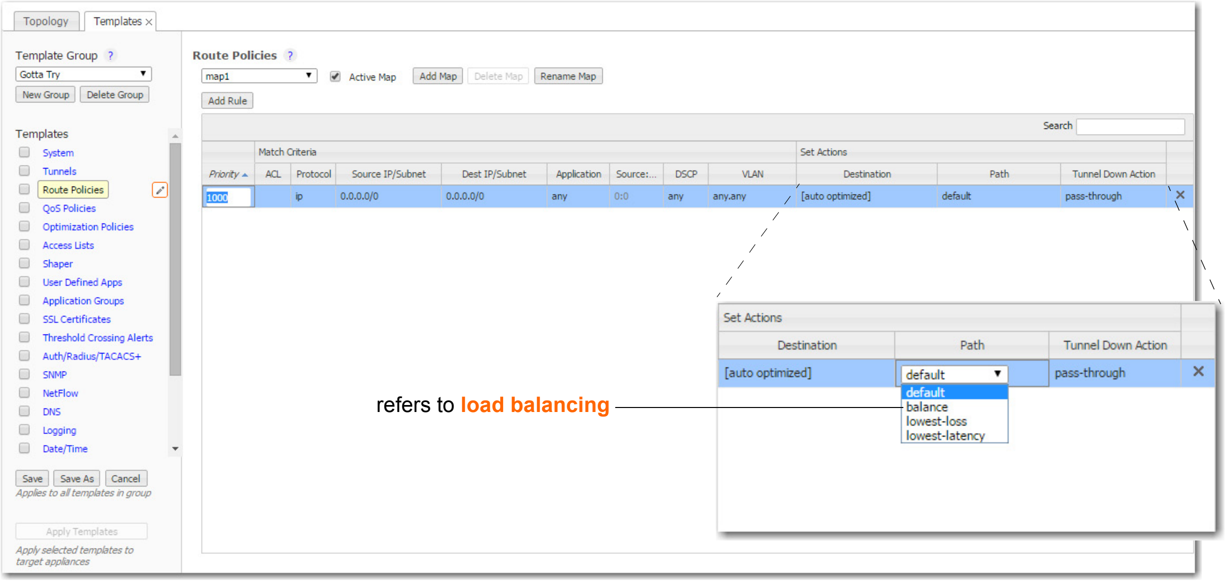
Route Policies Template

Only use the Route Policy template to create (and apply) rules for flows that are to be:

- sent pass-through (shaped or unshaped)
- dropped
- configured for a specific high-availability deployment
- routed based on application, ports, VLAN, DSCP, or ACL (Access Control List)

Beginning with VXOA Release 7.1 for the appliances, the Dynamic Path Control (DPC) feature is available in the template’s **Set Actions**. When you choose **auto-optimized** in the **Destination** field, you can tell the appliance to dynamically select the best path based on one of these criteria:

- load balancing
- lowest loss
- lowest latency



	Match Criteria								Set Actions		
Priority	ACL	Protocol	Source IP/Subnet	Dest IP/Subnet	Application	Source:...	DSCP	VLAN	Destination	Path	Tunnel Down Action
1000		ip	0.0.0.0/0	0.0.0.0/0	any	0:0	any	any.any	[auto optimized]	default	pass-through

Set Actions		
Destination	Path	Tunnel Down Action
[auto optimized]	default	pass-through

refers to load balancing

Why?

Each appliance's default routing behavior is to auto-optimize all IP traffic, automatically directing flows to the appropriate tunnel. **Auto-optimization** strategies reduce the need to create explicit route map entries for optimization. The three strategies that Silver Peak uses are **TCP-based** auto-opt, **IP-based** auto-opt, and **subnet sharing**. By default, all three are enabled on the **System** template.

Tip If you're upgrading from a software version that precedes VXOA 6.2.x, you can migrate subnets from legacy GMS route maps to the appliance's subnet table for subnet sharing. In the menus, go to **Maintenance > Tools > Migrate GMS Route Maps**.

Priority

- With this template, you can create rules with priority from **1000 – 9999**, inclusive.When you apply the template to an appliance, the GMS deletes all appliance Route Policy entries in that range before applying its policies.

- If you access an appliance directly (via the WebUI or the command line interface), you can create rules with higher priority than GMS rules (**1 – 999**) and rules with lower priority (**10000 – 65534**).
- Adding a rule increments the last Priority by 10. This leaves room for you to insert a rule in between rules without having to renumber subsequent priorities. Likewise, you can just edit the number.

Source or Destination

- An IP address can specify a subnet - for example: 10.10.10.0/24.
- To allow **any IP address**, use 0.0.0.0/0.
- Ports are available only for the protocols **tcp**, **udp**, and **tcp/udp**.
- To allow **any port**, use **0**.

Set Actions Definitions

The Route Policy template’s SET actions determine:

- where the appliance directs traffic
  - In the **Destination** column, you specify how to characterize the flow. The options are **auto-optimized**, **pass-through** [shaped], **pass-through-unshaped**, or **drop**ped.
  - When **auto-optimized**, a flow is directed to the appropriate tunnel. If you choose, you can specify that the appliance use metrics to dynamically select the best path based on one of these criteria:
    - load balancing
    - lowest loss
    - lowest latency

Note When configuring the Route Policy for an **individual** appliance when multiple tunnels exist to the remote ***peer***, you can also select the path based on a preferred interface or a specific tunnel. For further information, see the *Appliance Manager Operator’s Guide*.

- how traffic is managed if a tunnel is down
  - A **Tunnel Down Action** can be **pass-through** [shaped], **pass-through-unshaped**, or **drop**ped.

Note When configuring the Route Policy for an **individual** appliance, the **continue** option is available if a specific tunnel is named in the **Tunnel** column. That option enables the appliance to read subsequent entries in the individual Route Policy in the event that the tunnel used in a previous entry goes down. For further information, see the *Appliance Manager Operator’s Guide*.

QoS Policies Template

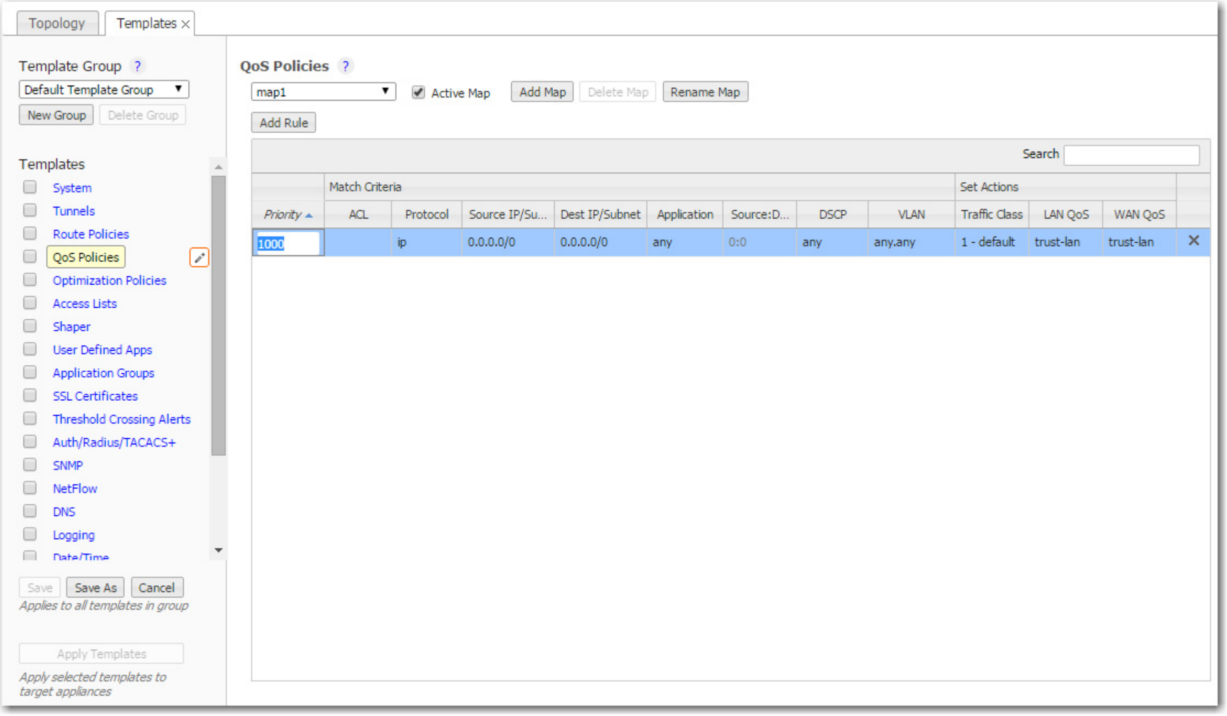
The **QoS Policy** determines how flows are queued and marked.

The QoS Policy's SET actions determine two things:

- what traffic class a shaped flow -- whether optimized or pass-through -- is assigned
- whether to trust incoming DSCP markings for LAN QoS and WAN QoS, or to remark them as they leave for the WAN

Use the **Shaper** to define, prioritize, and name traffic classes.

Think of it as the Shaper **defines** and the QoS Policy **assigns**.



Template Group: Default Template Group

map1 ☑ Active Map

	Match Criteria								Set Actions			
Priority ▲	ACL	Protocol	Source IP/Su...	Dest IP/Subnet	Application	Source:D...	DSCP	VLAN	Traffic Class	LAN QoS	WAN QoS	
1000		ip	0.0.0.0/0	0.0.0.0/0	any	0:0	any	any.any	1 - default	trust-lan	trust-lan	✕

Priority

- You can create rules with any priority between 1 and 65534.
  - If you are using GMS templates to add route map entries, GMS will delete all entries from **1000 – 9999**, inclusive, before applying its policies.
  - You can create rules from **1 – 999**, which have higher priority than GMS rules.
  - Similarly, you can create rules from **10000 – 65534** which have lower priority than GMS rules.
- Adding a rule increments the last Priority by 10. This leaves room for you to insert a rule in between rules without having to renumber subsequent priorities. Likewise, you can just edit the number..

Source or Destination

- An IP address can specify a subnet - for example: 10.10.10.0/24.
- To allow **any IP address**, use 0.0.0.0/0.
- Ports are available only for the protocols **tcp**, **udp**, and **tcp/udp**.
- To allow **any port**, use **0**.

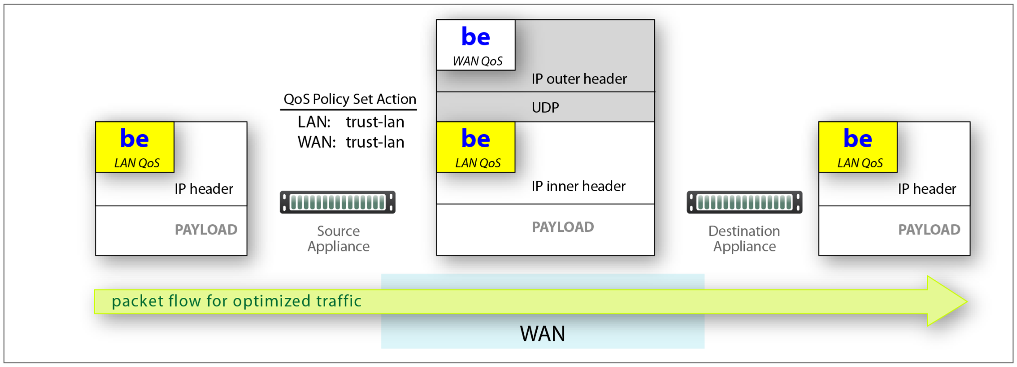
Handling and Marking DSCP Packets

- DSCP markings specify end-to-end QoS policies throughout a network.
- The default values for **LAN QoS** and **WAN QoS** are **trust-lan**.

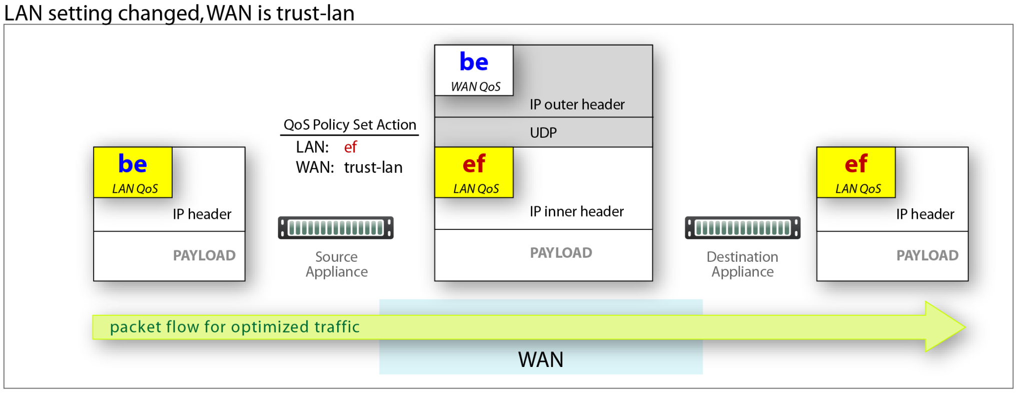
Applying DSCP Markings to Optimized (Tunnelized) Traffic

- The appliance encapsulates optimized traffic. This adds an IP outer header to packets for travel across the WAN. This outer header contains the **WAN QoS** DSCP marking.
- **LAN QoS** – the DSCP marking applied to the IP header before encapsulation
- **WAN QoS** – the DSCP marking in the encapsulating outer IP header. The remote appliance removes the outer IP header.

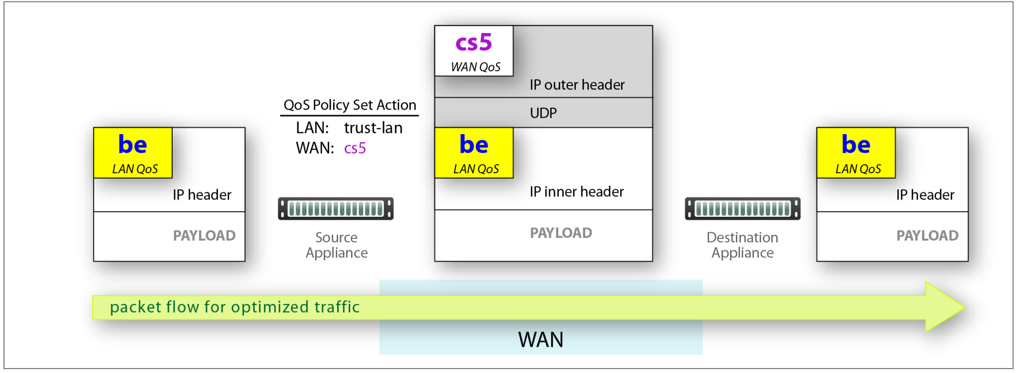
LAN and WAN set to trust-lan



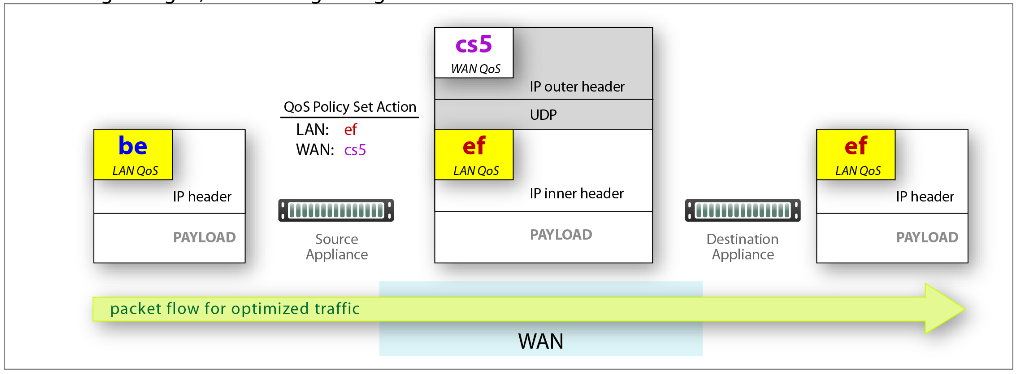
LAN setting changed,WAN is trust-lan



LAN is trust-lan,WAN setting changed



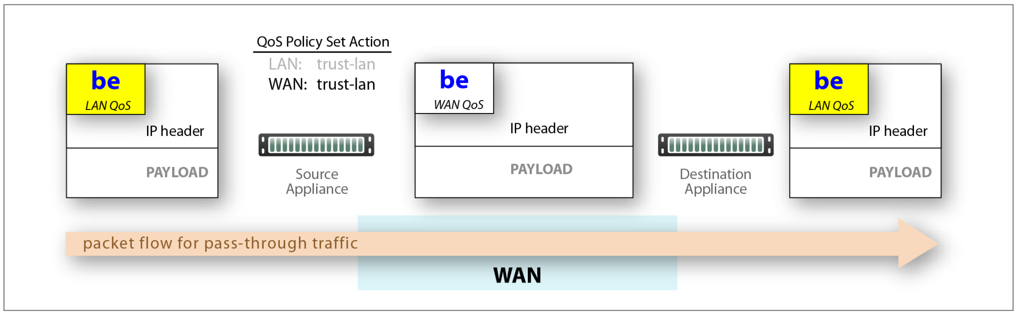
LAN setting changed,WAN setting changed



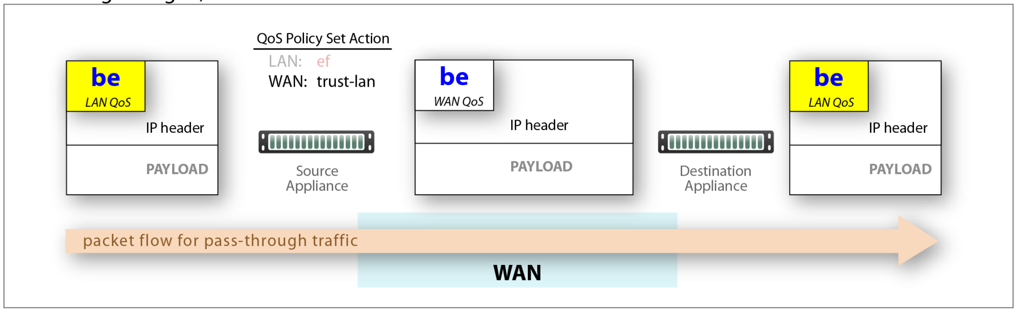
Applying DSCP Markings to Pass-through Traffic

- The appliance applies the QoS Policy's DSCP markings to all pass-through flows -- shaped and unshaped.
- Pass-through traffic doesn't receive an additional header, so it's handled differently:
  - The Optimization Policy's LAN QoS Set Action is ignored.
  - The specified WAN QoS marking replaces the packet's existing LAN QoS DSCP marking.
  - When the packet reaches the remote appliance, it retains the modified QoS setting as it travels to its destination.

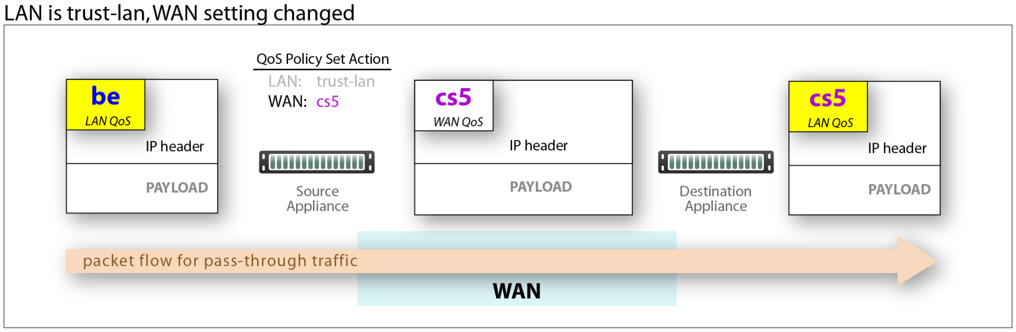
LAN and WAN set to trust-lan



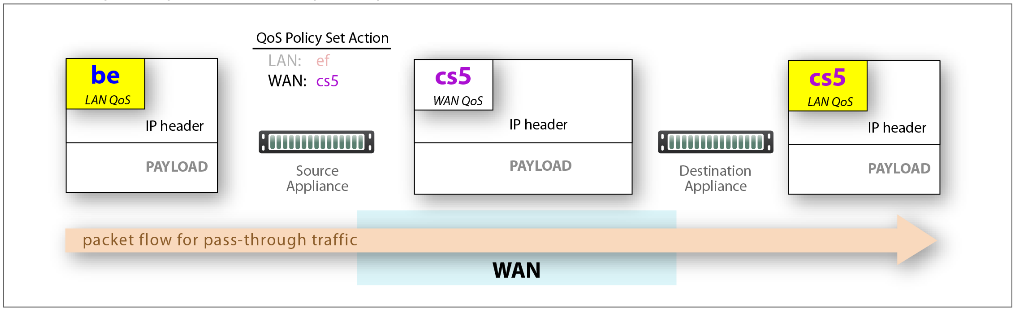
LAN setting changed,WAN is trust-lan



LAN is trust-lan, WAN setting changed

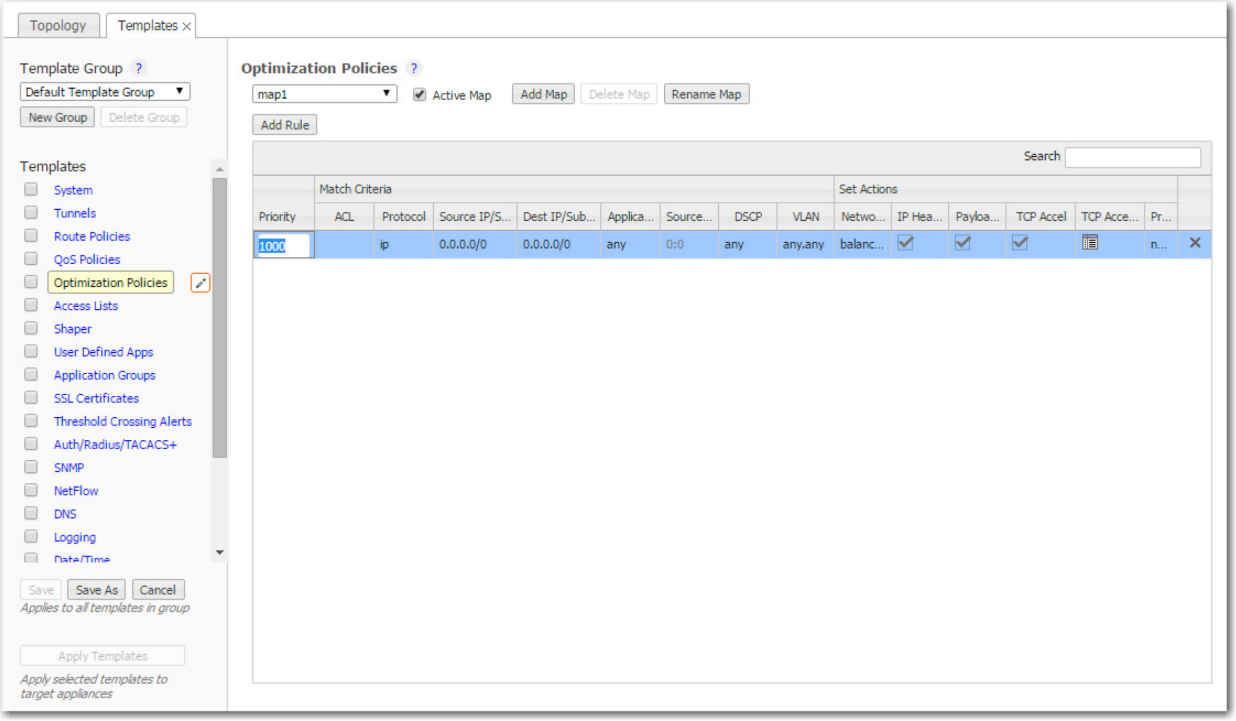


LAN setting changed, WAN setting changed



Optimization Policies Template

Optimization templates apply Optimization policies to appliances.



Template Group: Default Template Group

map1 ☑ Active Map

	Match Criteria									Set Actions						
Priority	ACL	Protocol	Source IP/S...	Dest IP/Sub...	Applica...	Source...	DSCP	VLAN	Netwo...	IP Hea...	Payloa...	TCP Accel	TCP Acce...	Pr...	
1000		ip	0.0.0.0/0	0.0.0.0/0	any	0:0	any	any.any	balanc...	☑	☑	☑	▤	n...	✕

Priority

- With this template, you can create rules with priority from **1000 – 9999**, inclusive. When you apply the template to an appliance, the GMS deletes all appliance entries in that range before applying its policies.
- If you access an appliance directly (via the WebUI or the command line interface), you can create rules with higher priority than GMS rules (**1 – 999**) and rules with lower priority (**10000 – 65534**).
- Adding a rule increments the last Priority by 10. This leaves room for you to insert a rule in between rules without having to renumber subsequent priorities. Likewise, you can just edit the number.

Source or Destination

- An IP address can specify a subnet - for example: 10.10.10.0/24.
- To allow **any IP address**, use 0.0.0.0/0.
- Ports are available only for the protocols **tcp**, **udp**, and **tcp/udp**.
- To allow **any port**, use **0**.

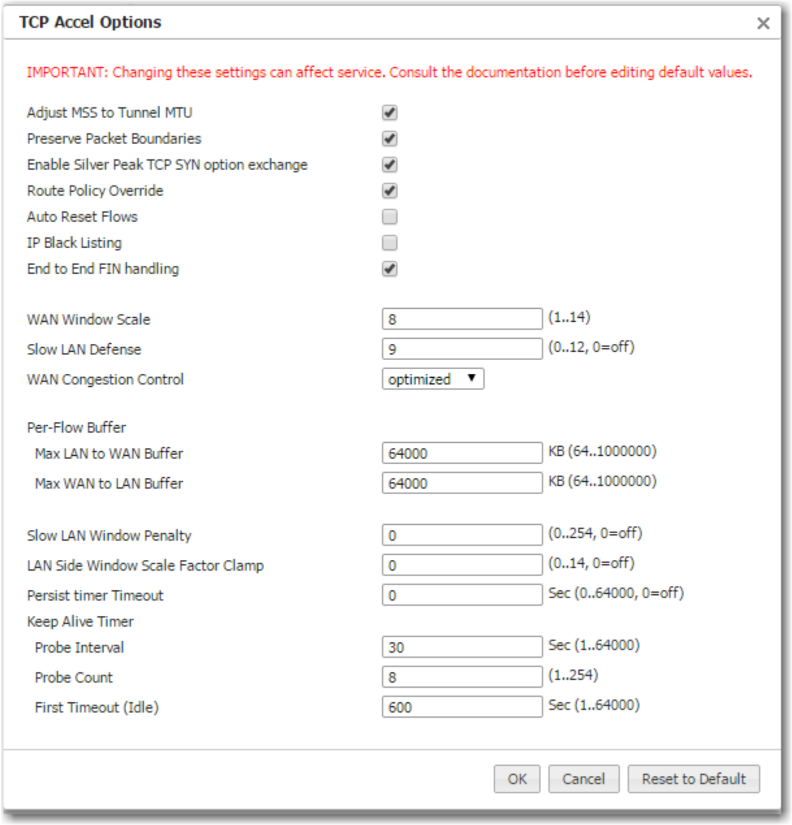
Set Actions Definitions

- **Network Memory** addresses limited bandwidth. This technology uses advanced fingerprinting algorithms to examine all incoming and outgoing WAN traffic. Network Memory localizes information and transmits only modifications between locations.
    - **Maximize Reduction** optimizes for maximum data reduction at the potential cost of slightly lower throughput and/or some increase in latency. It is appropriate for bulk data transfers such as file transfers and FTP, where bandwidth savings are the primary concern.
    - **Minimize Latency** ensures that Network Memory processing adds no latency. This may come at the cost of lower data reduction. It is appropriate for extremely latency-sensitive interactive or transactional traffic. It's also appropriate when the primary objective is to to fully utilize the WAN pipe to increase the LAN-side throughput, as opposed to conserving WAN bandwidth.
    - **Balanced** is the default setting. It dynamically balances latency and data reduction objectives and is the best choice for most traffic types.
    - **Disabled** turns off Network Memory.
- **IP Header Compression** is the process of compressing excess protocol headers before transmitting them on a link and uncompressing them to their original state at the other end. It's possible to compress the protocol headers due to the redundancy in header fields of the same packet, as well as in consecutive packets of a packet stream.
- **Payload Compression** uses algorithms to identify relatively short byte sequences that are repeated frequently. These are then replaced with shorter segments of code to reduce the size of transmitted data. Simple algorithms can find repeated bytes within a single packet; more sophisticated algorithms can find duplication across packets and even across flows.
- **TCP Acceleration** uses techniques such as selective acknowledgements, window scaling, and maximum segment size adjustment to mitigate poor performance on high-latency links.
- **Protocol Acceleration** provides explicit configuration for optimizing CIFS, SSL, SRDF, Citrix, and iSCSI protocols. In a network environment, it's possible that not every appliance has the same optimization configurations enabled. Therefore, the site that initiates the flow (the *client*) determines the state of the protocol-specific optimization.

TCP Acceleration Options

TCP acceleration uses techniques such as selective acknowledgement, window scaling, and message segment size adjustment ot compensate for poor performance on high latency links.

This feature has a set of advanced options with default values.



TCP Accel Options

IMPORTANT: Changing these settings can affect service. Consult the documentation before editing default values.

Adjust MSS to Tunnel MTU	☑	
Preserve Packet Boundaries	☑	
Enable Silver Peak TCP SYN option exchange	☑	
Route Policy Override	☑	
Auto Reset Flows	☐	
IP Black Listing	☐	
End to End FIN handling	☑	
WAN Window Scale	8	(1..14)
Slow LAN Defense	9	(0..12, 0=off)
WAN Congestion Control	optimized ▼	
Per-Flow Buffer		
Max LAN to WAN Buffer	64000	KB (64..1000000)
Max WAN to LAN Buffer	64000	KB (64..1000000)
Slow LAN Window Penalty	0	(0..254, 0=off)
LAN Side Window Scale Factor Clamp	0	(0..14, 0=off)
Persist timer Timeout	0	Sec (0..64000, 0=off)
Keep Alive Timer		
Probe Interval	30	Sec (1..64000)
Probe Count	8	(1..254)
First Timeout (Idle)	600	Sec (1..64000)

CAUTION Because changing these settings can affect service, Silver Peak recommends that you **do not modify** these without direction from Customer Support.

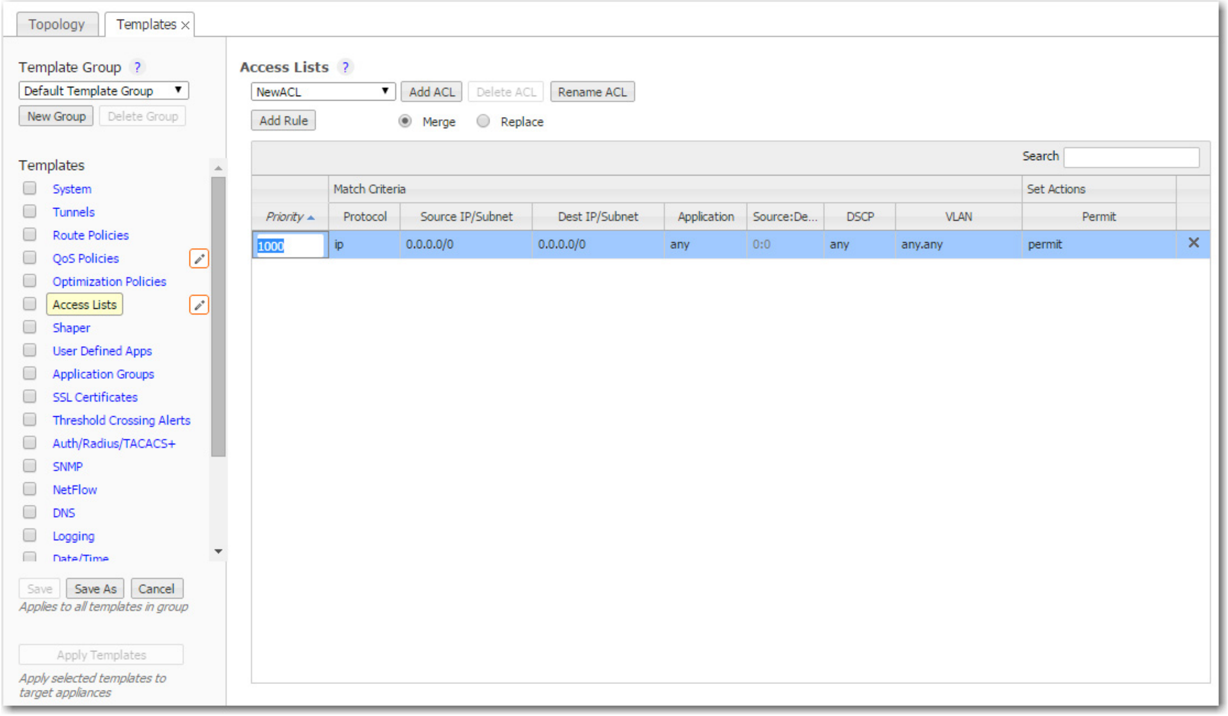
Option	Explanation
Adjust MSS to Tunnel MTU	Limits the TCP MSS (Maximum Segment Size) advertised by the end hosts in the SYN segment to a value derived from the Tunnel MTU (Maximum Transmission Unit). This is TCP MSS = Tunnel MTU – Tunnel Packet Overhead. This feature is enabled by default so that the **maximum value** of the end host MSS is always coupled to the Tunnel MSS. If the end host MSS is smaller than the tunnel MSS, then the end host MSS is used instead. A use case for disabling this feature is when the end host uses Jumbo frames.
Preserve Packet Boundaries	Preserves the packet boundaries end to end. If this feature is disabled, then the appliances in the path can coalesce consecutive packets of a flow to use bandwidth more efficiently. It's enabled by default so that applications that require packet boundaries to match don't fail.

Option	Explanation (Continued)
Enable Silver Peak TCP SYN option exchange	Controls whether or not Silver Peak forwards its proprietary TCP SYN option on the LAN side. Enabled by default, this feature detects if there are more than two Silver Peak appliances in the flow's data path, and optimizes accordingly. Disable this feature if there's a LAN-side firewall or a third-party appliance that would drop a SYN packet when it encounters an unfamiliar TCP option.
Route Policy Override	Tries to override asymmetric route policy settings. It emulates auto-opt behavior by using the same tunnel for the returning SYN+ACK as it did for the original SYN packet. Disable this feature if the asymmetric route policy setting is necessary to correctly route packets. In that case, you may need to configure flow redirection to ensure optimization of TCP flows.
Auto Reset Flows	**NOTE:** Whether this feature is enabled or not, the default behavior when a tunnel goes Down is to automatically reset the flows. If enabled, it resets all TCP flows that aren't accelerated but should be (based on policy and on internal criteria like a Tunnel Up event). The internal criteria can also include: • Resetting all TCP accelerated flows on a Tunnel Down event. • Resetting all unaccelerated TCP flows that are associated with a normally operating Tunnel, where: - TCP acceleration is enabled - SYN packet was not seen (so this flow was either part of WCCP redirection, or it already existed when the appliance was inserted in the data path).
IP Black Listing	If selected and if the appliance doesn't receive a TCP SYN-ACK from the remote end within 5 seconds, the flow proceeds without acceleration and the destination IP address is blacklisted for one minute.
End to End FIN Handling	This feature helps to fine tune TCP behavior during a connection's graceful shutdown event. When this feature is ON (Default), TCP on the local appliance synchronizes this graceful shutdown of the local LAN side with the remote Silver Peak's LAN side. When this feature is OFF (Default TCP), no such synchronization happens and the two LAN segments at the ends gracefully shutdown independently.
WAN Window Scale	This is the WAN-side TCP Window scale factor that Silver Peak uses internally for its WAN-side traffic. This is independent of the WAN-side factor advertised by the end hosts.
Slow LAN Defense	Resets all flows that consume a disproportionate amount of buffer and have a very slow throughput on the LAN side. Owing to a few slower end hosts or a lossy LAN, these flows affect the performance of all other flows such that no flows see the customary throughput improvement gained through TCP acceleration. This feature is enabled by default. The number relates indirectly to the amount of time the system waits before resetting such slow flows.
WAN Congestion Control	Selects the internal Congestion Control parameter: • **Optimized** - This is the default setting. This mode offers optimized performance in almost all scenarios. • **Standard** - In some unique cases it may be necessary to downgrade to Standard performance to better interoperate with other flows on the WAN link. • **Aggressive** - Provides aggressive performance and should be used with caution. Recommended mostly for Data Replication scenarios.
Per-Flow Buffer	(**Max LAN to WAN Buffer** and **Max WAN to LAN Buffer**) This setting clamps the maximum buffer space that can be allocated to a flow, in each direction.

Option	Explanation (Continued)
Slow LAN Window Penalty	This setting (OFF by default) penalizes flows that are slow to send data on the LAN side by artificially reducing their TCP receive window. This causes less data to be received and helps to reach a balance with the data sending rate on the LAN side.
LAN Side Window Scale Factor Clamp	This setting allows the appliance to present an artificially lowered WSF to the end host. This reduces the need for memory in scenarios where there are a lot of out-of-order packets being received from the LAN side. These out-of-order packets cause a lot of buffer utilization and maintenance.
Persist timer Timeout	Allows the TCP to terminate connections that are in Persist timeout stage after the configured number of seconds.
Keep Alive Timer	Allows us to change the Keep Alive timer for the TCP connections. • **Probe Interval** - Time interval in seconds between two consecutive Keep Alive Probes • **Probe Count** - Maximum number of Keep Alive probes to send • **First Timeout (Idle)** - Time interval until the first Keep Alive timeout

Access Lists Template

Use this page to create, modify, delete, and rename **Access Control Lists** (ACL).



Template Group: Default Template Group

Access Lists: NewACL

● Merge ○ Replace

	Match Criteria							Set Actions
Priority	Protocol	Source IP/Subnet	Dest IP/Subnet	Application	Source:De...	DSCP	VLAN	Permit
1000	ip	0.0.0.0/0	0.0.0.0/0	any	0:0	any	any.any	permit

An **ACL** is a reusable MATCH criteria for filtering flows, and is associated with an action, **permit** or **deny**: You can use the same ACL as the MATCH condition in more than one policy --- Route, QoS, or Optimization.

- An Access Control List (ACL) consists of one or more ordered access control rules.
- An ACL only becomes active when it's used in a policy.
- **Deny** prevents further procesing of the flow by ***that ACL, specifically***. The appliance continues to the next entry in the policy.
- **Permit** allows the matching traffic flow to proceed on to the policy entry's associated SET action(s). The default is **permit**.
- When creating ACL rules, list **deny** statements first, and prioritize less restrictive rules ahead of more restrictive rules.

Priority

- With this template, you can create rules with priority from **1000 – 9999**, inclusive. When you apply the template to an appliance, the GMS deletes all appliance entries in that range before applying its policies.
- If you access an appliance directly (via the WebUI or the command line interface), you can create rules with higher priority than GMS rules (**1 – 999**) and rules with lower priority (**10000 – 65534**).
- Adding a rule increments the last Priority by 10. This leaves room for you to insert a rule in between rules without having to renumber subsequent priorities. Likewise, you can just edit the number.

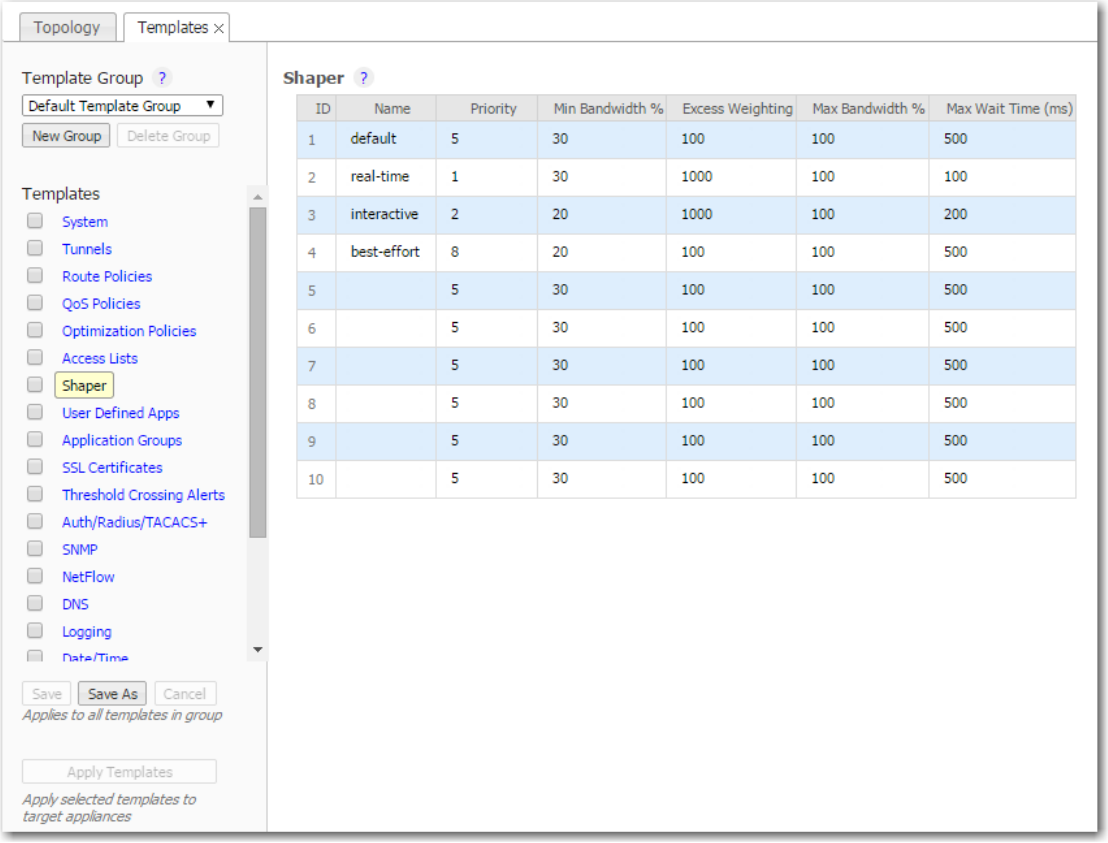
Source or Destination

- An IP address can specify a subnet - for example: 10.10.10.0/24.
- To allow **any IP address**, use 0.0.0.0/0.
- Ports are available only for the protocols **tcp**, **udp**, and **tcp/udp**.
- To allow **any port**, use **0**.

Shaper Template

The **Shaper** template is a simplified way of globally configuring QoS (Quality of Service) on the appliances:

- The Shaper shapes outbound traffic by allocating bandwidth as a percentage of the **system bandwidth**.
- The Shaper's parameters are organized into ten traffic classes. Four traffic classes are preconfigured and named --- **real-time**, **interactive**, **default**, and **best effort**.
- The system applies these QoS settings globally after compressing (deduplicating) all the outbound tunnelized and pass-through-shaped traffic --- shaping it as it exits to the WAN.
- Applying the template to an appliance updates its system-level **wan** Shaper. If the appliance has any added, interface-specific Shapers, they are preserved.
- You can rename or edit any traffic class.
- To view any applied configurations, access the **Configuration > Shaper** page.



ID	Name	Priority	Min Bandwidth %	Excess Weighting	Max Bandwidth %	Max Wait Time (ms)
1	default	5	30	100	100	500
2	real-time	1	30	1000	100	100
3	interactive	2	20	1000	100	200
4	best-effort	8	20	100	100	500
5		5	30	100	100	500
6		5	30	100	100	500
7		5	30	100	100	500
8		5	30	100	100	500
9		5	30	100	100	500
10		5	30	100	100	500

Definitions

- **Priority:** Determines the order in which to allocate each class's minimum bandwidth - 1 is first, 10 is last.
- **Min Bandwidth:** Refers to the percentage of bandwidth guaranteed to each traffic class, allocated by priority. However, if the sum of the percentages is greater than 100%, then lower-priority traffic classes might not receive their guaranteed bandwidth if it's all consumed by higher-priority traffic.

  If you set **Min Bandwidth** to a value greater than **Max Bandwidth**, then **Max** overrides **Min**.

- **Excess Weighting:** If there is bandwidth left over after satisfying the minimum bandwidth percentages, then the excess is distributed among the traffic classes, in proportion to the weightings specified in the **Excess Weighting** column. Values range from 1 to 10,000.
- **Max Bandwidth:** You can limit the maximum bandwidth that a traffic class uses by specifying a percentage in the **Max Bandwidth** column. The bandwidth usage for the traffic class will never exceed this value.
- **Max Wait Time:** Any packets waiting longer than the specified **Max Wait Time** are dropped.

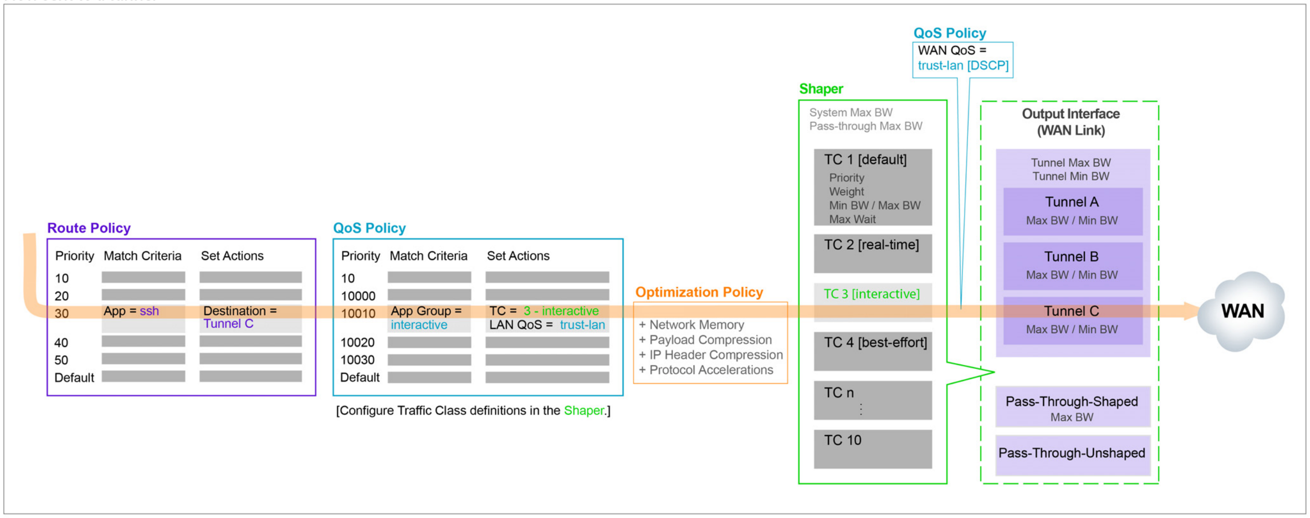
The Paths Through Policies and Shaping

The following diagram illustrates a flow's progress through the policies and the Shaper when the Route Policy Set Action, **Destination**, is:

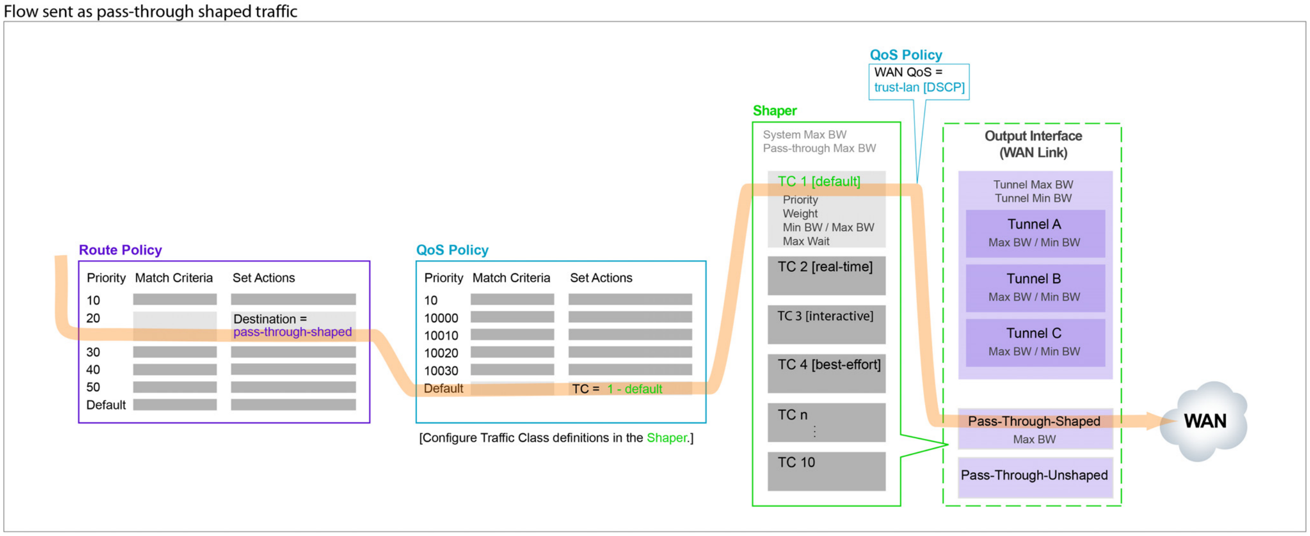
- a specific tunnel
- pass-through shaped
- pass-through unshaped

Note If the Route Policy's Set Action is ***auto-optimized*** and the local appliance initiates either TCP-based or IP-based handshaking, then the remote appliance determines which tunnel to use, based on information it receives in the first packets from the local appliance. (For more information about auto-optimization, see the *Appliance Manager Operator's Guide*.)

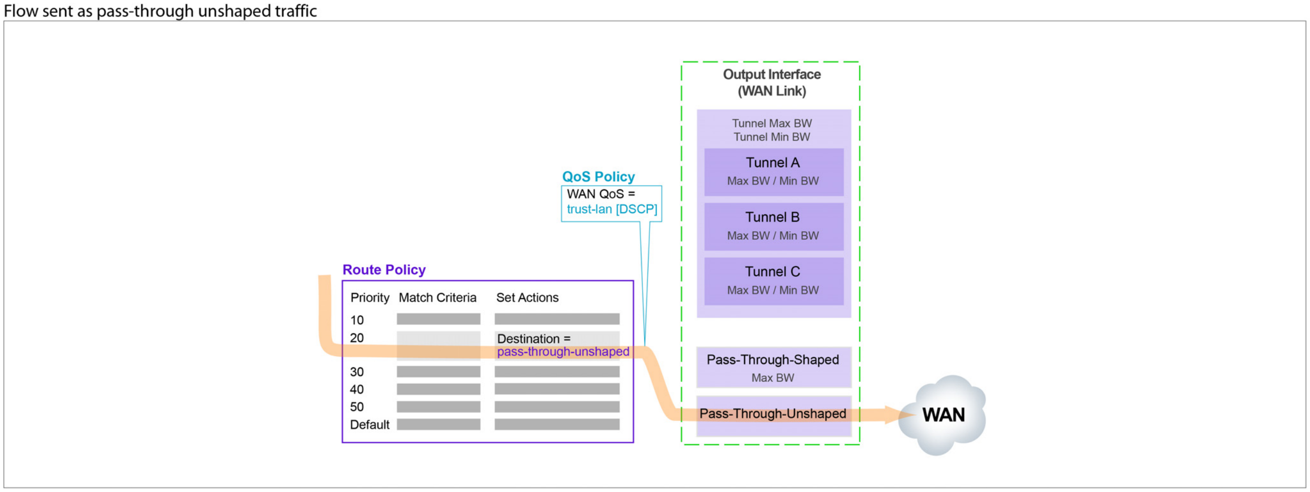
Flow sent to a tunnel



Flow sent as pass-through shaped traffic

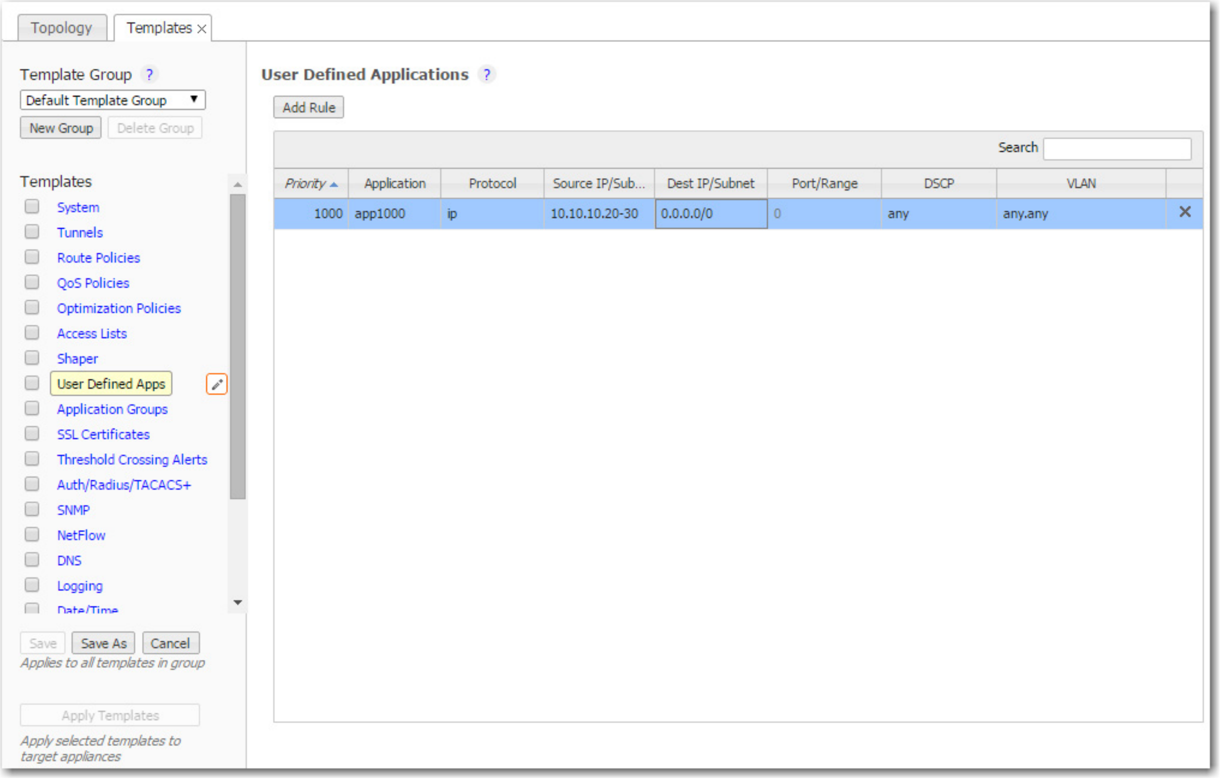


Flow sent as pass-through unshaped traffic



User Defined Apps Template

Use this template to create user-defined applications (UDA).



Priority ▲	Application	Protocol	Source IP/Sub...	Dest IP/Subnet	Port/Range	DSCP	VLAN	
1000	app1000	ip	10.10.10.20-30	0.0.0.0/0	0	any	any.any	✕

Where can you use them?

- Route Policy
- QoS Policy
- Optimization Policy
- Access Lists (ACL)
- Application Groups

Behavior

- For reporting symmetry, you must define the same application(s) on peer appliances. Otherwise, the application may be a UDA on one appliance, and yet be categorized as an **unassigned application** on another, paired appliance.
- Each application consists of at least one rule.
- A warning displays if you reach the maximum number of rules, ports, or addresses allowed.
- If a UDA is in use, deleting it deletes **all** the dependent entries. A warning message appears before deletion.
- Multiple UDAs can have the same name. Whenever that name is referenced, the software sequentially matches against each UDA definition having that name. So, dependent entries are only deleted when you delete the **last** definition of that UDA.

Note When it comes to flow and application statistics reports, user-defined applications are always checked before built-in applications.

Ports are unique. If a port or a range includes a built-in port, then the custom application is the one that lays claim to it.

If two distinctly named user-defined applications have a port number in common, then report results will be skewed, depending on the priority assigned to the custom applications. A port is only counted once.

Priority

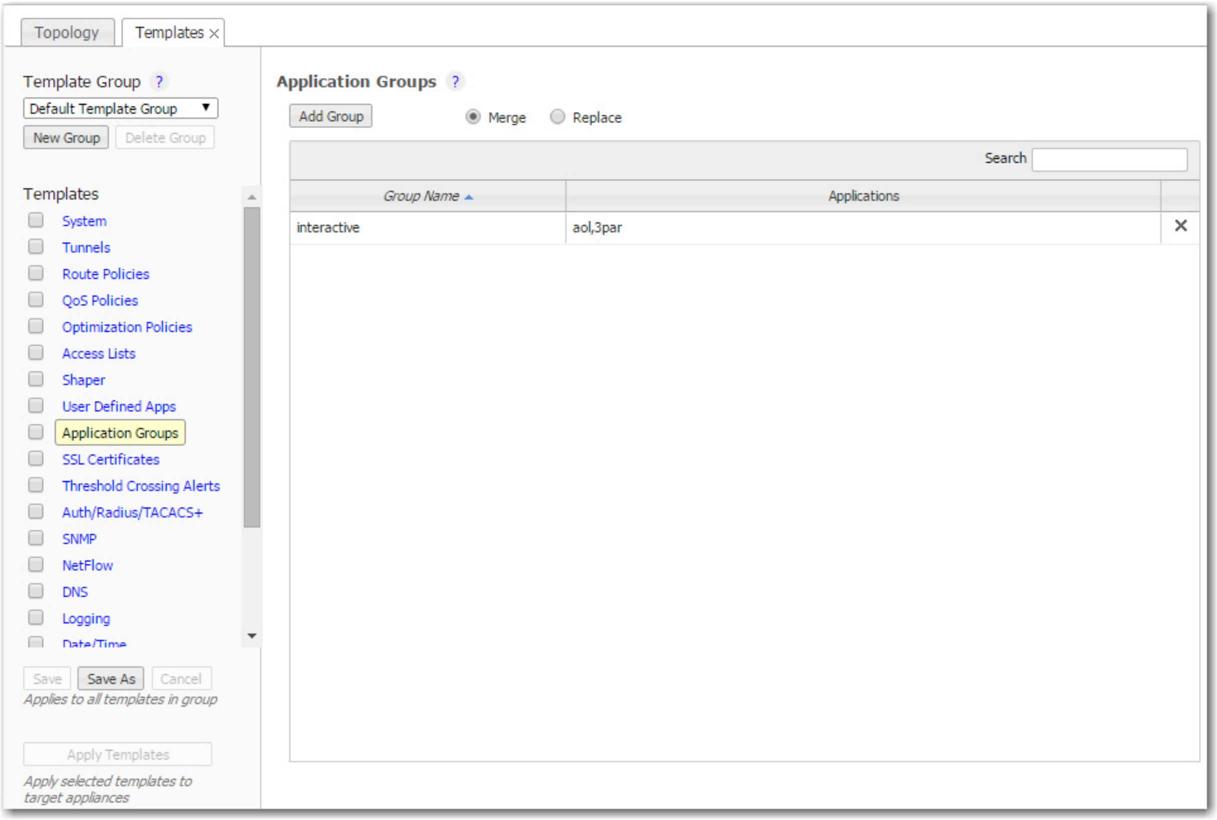
- Range = 1000 – 50000
- Templates won't overwrite or delete applications on the appliances that have priorities in the range, 1 – 999.
- By default, adding a rule/application increments the last Priority by 10.

Source or Destination

- An IP address can specify a subnet - for example: 10.10.10.0/24.
- An IP address can specify a range - for example: 10.10.10.20-30.
- To allow **any IP address**, use 0.0.0.0/0.
- Ports are available only for the protocols **tcp**, **udp**, and **tcp/udp**.
- Specify either a single port or a range of ports - for example: 1234-1250.
- To allow **any port**, use **0**.
- Separate multiple items with any of the following: a line break, a comma, or a single space.

Application Groups Template

Application groups associate applications into a common group that you can use as a MATCH criteria. The applications can be built-in, user-defined, or a combination of both.



Template Group: Default Template Group

● Merge ○ Replace

Group Name ▲	Applications	
interactive	aol,3par	×

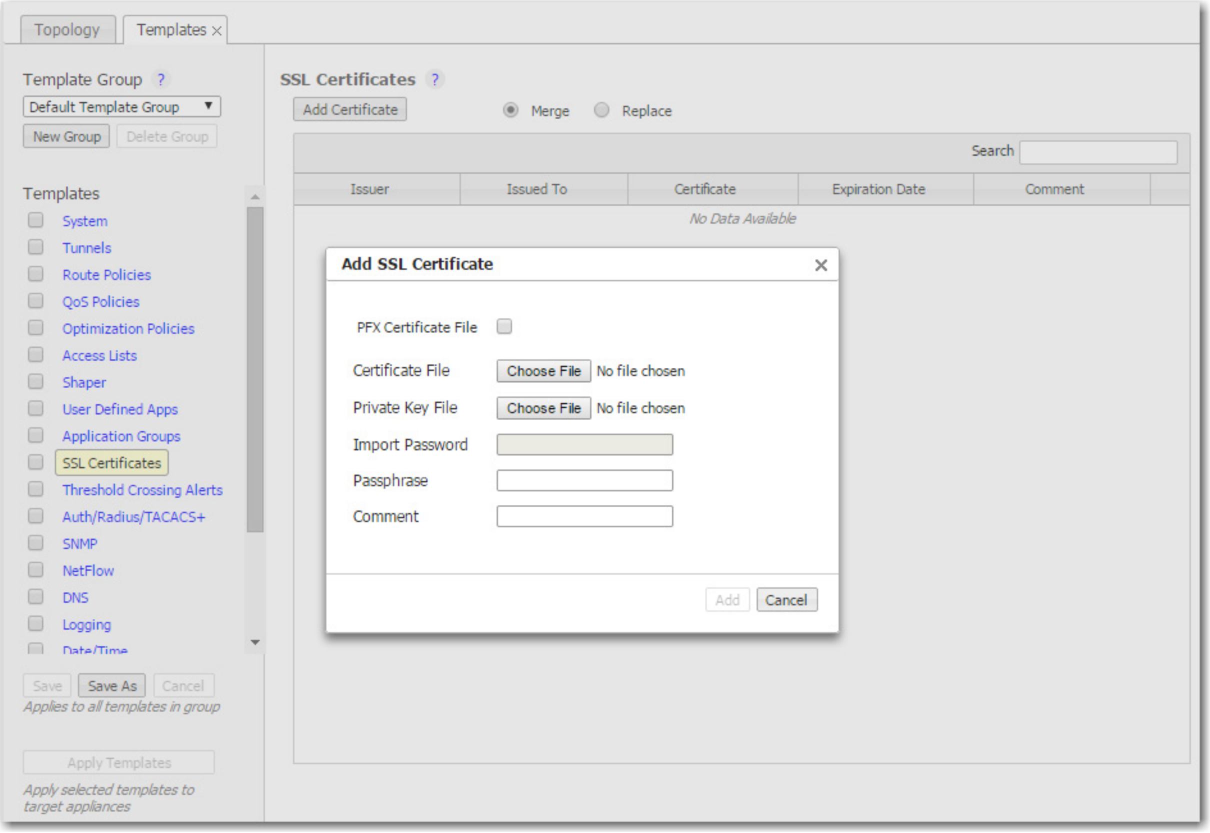
- The **Group Name** cannot be empty or have more than 64 characters.
- Group names are not case-sensitive.
- A group can be empty or contain up to 128 applications.
- An application group cannot contain an application group.
- For reporting symmetry, you must define the same application groups on peer appliances. Otherwise, the application group may be named on one appliance, and yet be categorized as an **unassigned application** on another, paired appliance.

By default, applying the template to an appliance completely deletes and replaces the appliance's application groups.

If you would rather append the template's groups to the appliance's application groups, then select **Merge** before applying the template. If both have a group with the same name, the content will be combined on the appliance.

SSL Certificates Template

By supporting the use of SSL certificates and keys, Silver Peak provides deduplication for Secure Socket Layer (SSL) encrypted WAN traffic

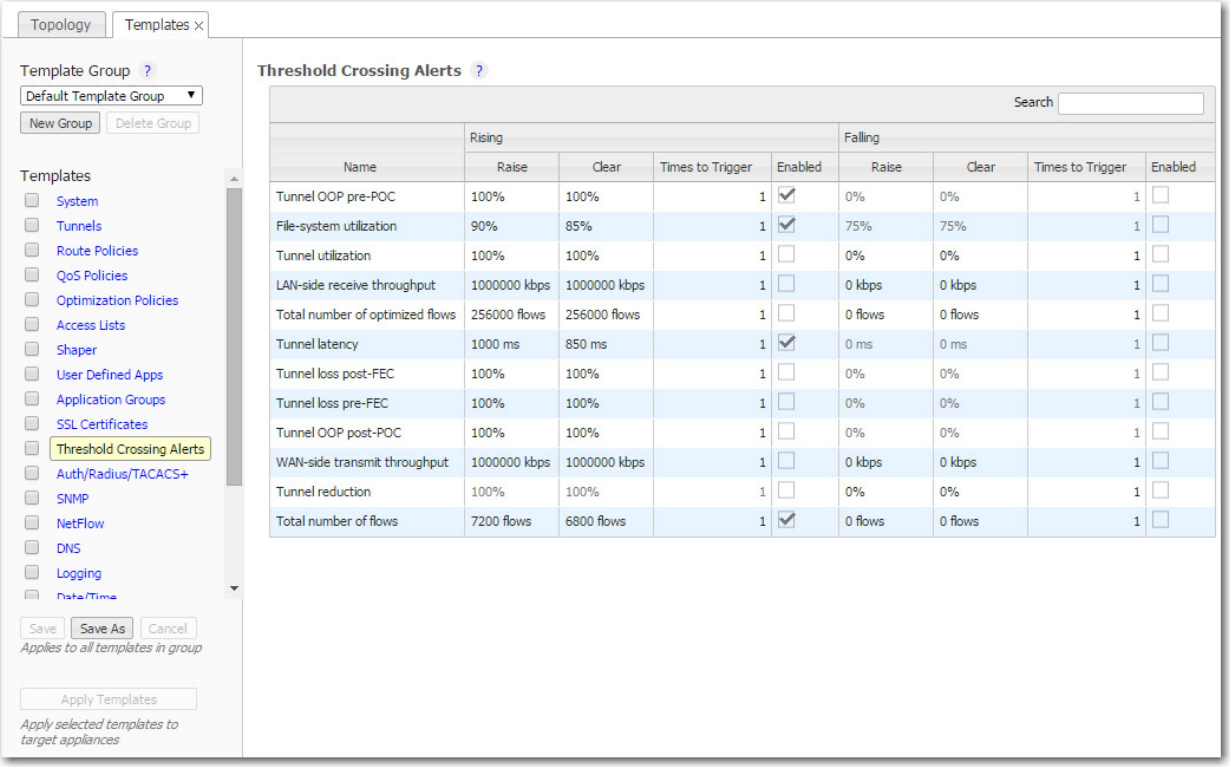


- Silver Peak decrypts SSL data using the configured certificates and keys, optimizes the data, and transmits data over an IPSec tunnel. The peer Silver Peak appliance uses configured SSL certificates to re-encrypt data before transmitting.
- Peers that exchange and optimize SSL traffic must use the same certificate and key.
- Use this template to provision a certificate and its associated key across multiple appliances.
  - You can add either a PFX certificate (generally, for Microsoft servers) or a PEM certificate.
  - The default is PEM when PFX Certificate File is deselected.
  - If the key file has an encrypted key, enter the passphrase needed to decrypt it.
- Silver Peak supports
  - X509 Privacy Enhanced Mail (PEM), Personal Information Exchange (PFX), and RSA key 1024-bit and 2048-bit certificate formats.
  - SAN (Subject Alternative Name) certificates. SAN certificates enable sharing of a single certificate across multiple servers and services.
- Silver Peak appliances support:
  - **Protocol versions:** SSLv3, SSLv3.3, TLS1.0, TLS1.1, TLS1.2
  - **Cipher algorithms:** AES128, AES256, RC4, 3DES
  - **Digests:** MD5, SHA1

- Before installing the certificates, you must do the following:
  - Configure the tunnels bilaterally for **IPSec** mode.
    To do so, access the **Tunnels** template and for **Mode**, select **ipsec**.
  - Verify that **TCP acceleration** and **SSL acceleration** are enabled.
    To do so, access the **Configuration > Optimization Policies** page, and review the **Set Actions**.
- If you choose to be able to decrypt the flow, optimize it, and send it in the clear between appliances, then access the **System** template and select **SSL optimization for non-IPsec tunnels**.

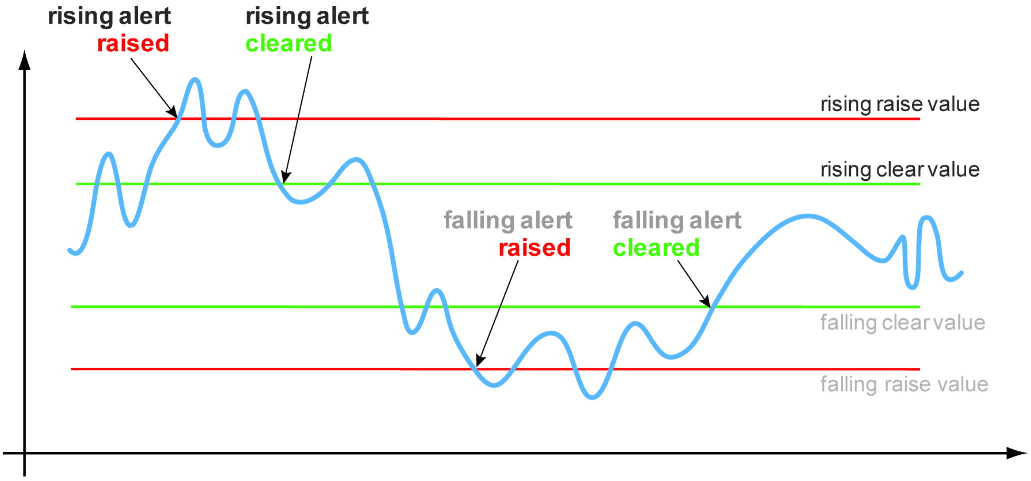
Threshold Crossing Alert Template

Threshold Crossing Alerts are preemptive, user-configurable alarms triggered when the specific thresholds are crossed.



	Rising				Falling			
Name	Raise	Clear	Times to Trigger	Enabled	Raise	Clear	Times to Trigger	Enabled
Tunnel OOP pre-POC	100%	100%	1	☑	0%	0%	1	□
File-system utilization	90%	85%	1	☑	75%	75%	1	□
Tunnel utilization	100%	100%	1	□	0%	0%	1	□
LAN-side receive throughput	1000000 kbps	1000000 kbps	1	□	0 kbps	0 kbps	1	□
Total number of optimized flows	256000 flows	256000 flows	1	□	0 flows	0 flows	1	□
Tunnel latency	1000 ms	850 ms	1	☑	0 ms	0 ms	1	□
Tunnel loss post-FEC	100%	100%	1	□	0%	0%	1	□
Tunnel loss pre-FEC	100%	100%	1	□	0%	0%	1	□
Tunnel OOP post-POC	100%	100%	1	□	0%	0%	1	□
WAN-side transmit throughput	1000000 kbps	1000000 kbps	1	□	0 kbps	0 kbps	1	□
Tunnel reduction	100%	100%	1	□	0%	0%	1	□
Total number of flows	7200 flows	6800 flows	1	☑	0 flows	0 flows	1	□

They alarm on both rising and falling threshold crossing events (i.e., floor and ceiling levels). For both levels, one value raises the alarm, while another value clears it.



Rules:

- High raise threshold is greater than high clear threshold
- Low raise threshold is less than low clear threshold

Metrics and Defaults

Times to Trigger – A value of 1 triggers an alarm on the first threshold crossing instance. The default sampling granularity (or *rate* or *interval*) is one minute.

This table lists the **metrics** of each type of threshold crossing alert:

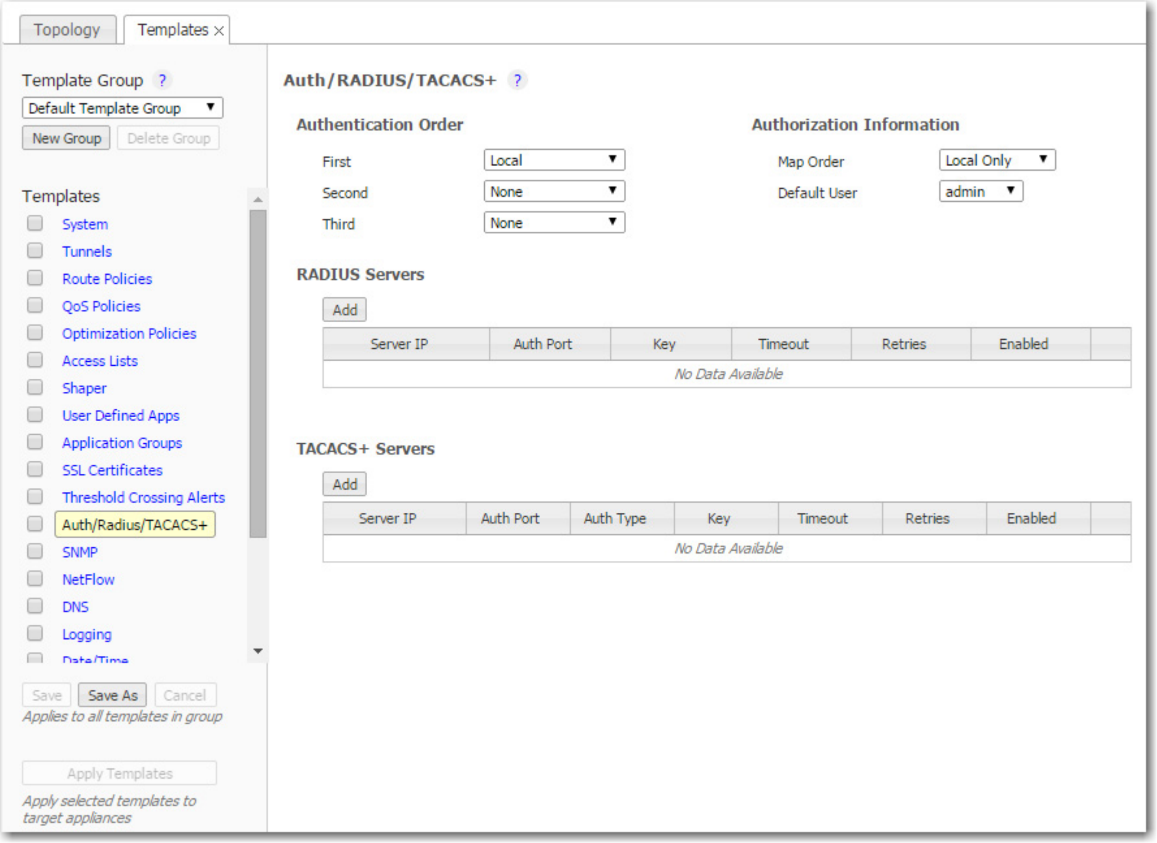
Table 2-1 Metrics for Threshold Crossing Alerts

	TCA Name	Unit	Metric
Appliance Level	**WAN-side transmit throughput**	kbps	Minute average WAN-side transmit TOTAL for all interfaces
	LAN-side receive throughput	kbps	Minute average LAN-side receive TOTAL for all interfaces
	Total number of optimized flows	flows	End of minute count
	Total number of flows	flows	End of minute count
	File-system-utilization	% (non-Network Memory)	End of minute count
Tunnel Level	**Tunnel latency**	msec	Second-sampled maximum latency during the minute
	Tunnel loss pre-FEC	1/10th %	Minute average
	Tunnel loss post-FEC	1/10th %	Minute average
	Tunnel OOP pre-POC	1/10th %	Minute average
	Tunnel OOP post-POC	1/10th %	Minute average
	Tunnel utilization	% of configured bandwidth	Minute average
	Tunnel reduction	%	Minute average

Note Enabled by default, there is also an **Appliance Capacity** TCA that triggers when an appliance reaches 95% of its total flow capacity. It doesn't automatically clear, but can be cleared by an operator. It is also not configurable.

Auth/Radius/TACACS+ Template

Silver Peak appliances support user **authentication** and **authorization** as a condition of providing access rights.



Authentication Order

First: Local

Second: None

Third: None

Authorization Information

Map Order: Local Only

Default User: admin

RADIUS Servers

Server IP	Auth Port	Key	Timeout	Retries	Enabled
No Data Available					

TACACS+ Servers

Server IP	Auth Port	Auth Type	Key	Timeout	Retries	Enabled
No Data Available						

- **Authentication** is the process of validating that the end user, or a device, is who they claim to be.
- **Authorization** is the action of determining what a user is allowed to do. Generally, authentication precedes authorization.
- **Map order** refers to the order in which the authentication databases are queried.
- The configuration specified for authentication and authorization **applies globally** to all users accessing that appliance.
- If a logged-in user is inactive for an interval that exceeds the inactivity time-out, the appliance logs them out and returns them to the login page. You can change that value, as well as the maximum number of sessions, in the **Session Management template**.

Authentication and Authorization

To provide authentication and authorization services, Silver Peak appliances:

- support a built-in, **local database**
- can be linked to a **RADIUS** (Remote Address Dial-In User Service) server
- can be linked to a **TACACS+** (Terminal Access Controller Access Control System) server.

Both RADIUS and TACACS+ are client-server protocols.

Appliance-based User Database

- The local, built-in user database supports user names, groups, and passwords.
- The two user groups are **admin** and **monitor**. You must associate each user name with one or the other. Neither group can be modified or deleted.
- The **monitor** group supports reading and monitoring of all data, in addition to performing all actions. This is equivalent to the Command Line Interface's (CLI) ***enable*** mode privileges.
- The **admin** group supports full privileges, along with permission to add, modify, and delete. This is equivalent to the Command Line Interface's (CLI) ***configuration*** mode privileges.

RADIUS

- RADIUS uses UDP as its transport.
- With RADIUS, the authentication and authorization functions are coupled together.
- RADIUS authentication requests must be accompanied by a shared secret. The shared secret must be the same as defined in the RADIUS setup. Please see your RADIUS documentation for details.
- **Important:** Configure your RADIUS server's ***priv levels*** within the following ranges:
  - **admin** = 7 - 15
  - **monitor** = 1 - 6

TACACS+

- TACACS+ uses TCP as its transport.
- TACACS+ provides separated authentication, authorization, and accounting services.
- Transactions between the TACACS+ client and TACACS+ servers are also authenticated through the use of a shared secret. Please see your TACACS+ documentation for details.
- **Important:** Configure your TACACS+ server's roles to be **admin** and **monitor**.

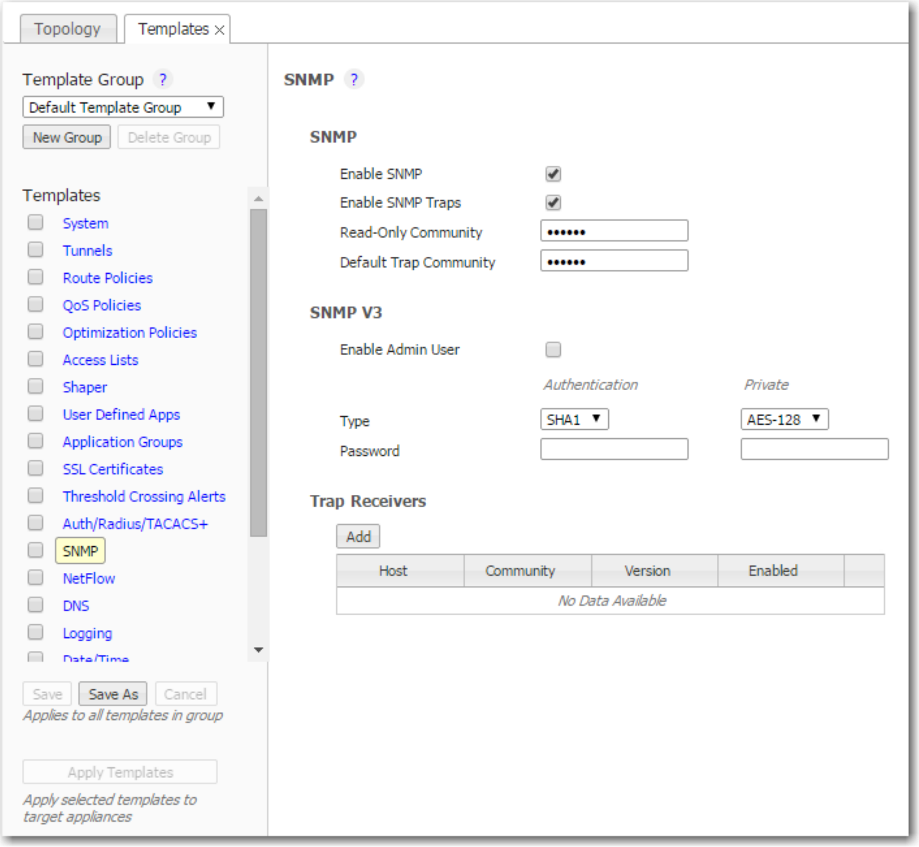
What Silver Peak recommends

- Use either RADIUS or TACACS+, but not both.
- For **Authetication Order**, configure the following:
  - **First** = Local
  - **Second** = either RADIUS or TACACS+. If not using either, then None.
  - **Third** = None
- When using RADIUS or TACACS+ to authenticate users, configure **Authorization Information** as follows:
  - **Map Order** = Remote First
  - **Default User** = admin

SNMP Template

Use this page to configure the appliance's **SNMP** agent, the trap receiver(s), and how to forward appliance alarms as SNMP traps to the receivers.

- The Silver Peak appliance supports the Management Information Base (MIB) II, as described in RFC 1213, for cold start traps and warm start traps, as well as Silver Peak proprietary MIBs.
- The appliance issues an SNMP trap during reset—that is, when loading a new image, recovering from a crash, or rebooting.
- The appliance sends a trap every time an alarm is raised or cleared. Traps contain additional information about the alarm, including severity, sequence number, a text-based description of the alarm, and the time the alarm was created. For additional information, see SILVERPEAK-MGMT-MIB.TXT in the MIBS directory.



SNMP

Enable SNMP ☑
Enable SNMP Traps ☑
Read-Only Community ••••••
Default Trap Community ••••••

SNMP V3

Enable Admin User ☐

	Authentication	Private
Type	SHA1	AES-128
Password		

Trap Receivers

Host	Community	Version	Enabled
No Data Available			

For **SNMP v1** and **SNMP v2c**, you only need configure the following:

- **Enable SNMP** = Allows the SNMP applicaton to poll this Silver Peak appliance.
- **Enable SNMP Traps** = Allows the SNMP agent (in the appliance) to send traps to the receiver(s).
- **Read-Only Community** = The SNMP application needs to present this text string (secret) in order to poll this appliance's SNMP agent. The default value is **public**, but you can change it.
- **Default Trap Community** = The trap receiver needs to receive this string in order to accept the traps being sent to it. The default value is **public**, but you can change it.

For additional security ***when the SNMP application polls the appliance***, you can select **Enable Admin User** for **SNMP v3**, instead of using **v1** or **v2c**. This provides a way to authenticate without using clear text:

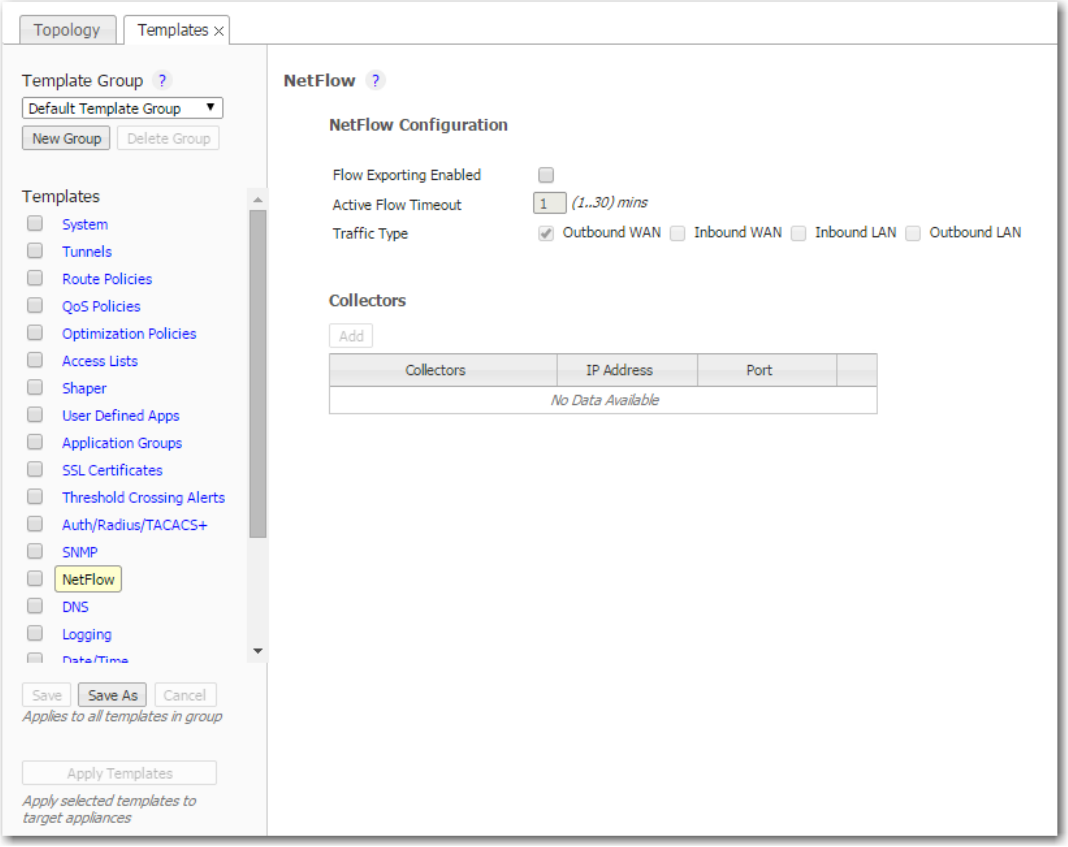
- To configure SNMP v3 **admin** privileges, you must be logged in as **admin** in Appliance Manager.
- For SNMP v3, **authentication** between the user and the server acting as the SNMP agent is bilateral and **required**. You can use either the MD5 or SHA-1 hash algorithm.
- Using DES or AES-128 to encrypt for **privacy** is optional. If you don't specify a password, the appliance uses the default privacy algorithm (AES-128) and the same password you specified for authentication.

You can configure up to 3 **trap receivers**:

- **Host** = IP address where you want the traps sent
- **Community** = The trap receiver needs to receive a specific string in order to accept the traps being sent to it. By default, this field is blank because it uses the Default Trap Community string, which has the value, **public**. If the trap receiver you're adding has a different Community string, enter the community string that's configured on the trap receiver.
- **Version** = Select either **v1** (RFC 1157) or **v2c** (RFC 1901) standards. For both, authentication is based on a community string that represents an unencrypted password.
- **Enabled** = When selected, enables this specific trap receiver.

NetFlow Template

You can configure your appliance to export statistical data to NetFlow collectors.



NetFlow Configuration

Flow Exporting Enabled □

Active Flow Timeout 1 (1..30) mins

Traffic Type ☑ Outbound WAN □ Inbound WAN □ Inbound LAN □ Outbound LAN

Collectors

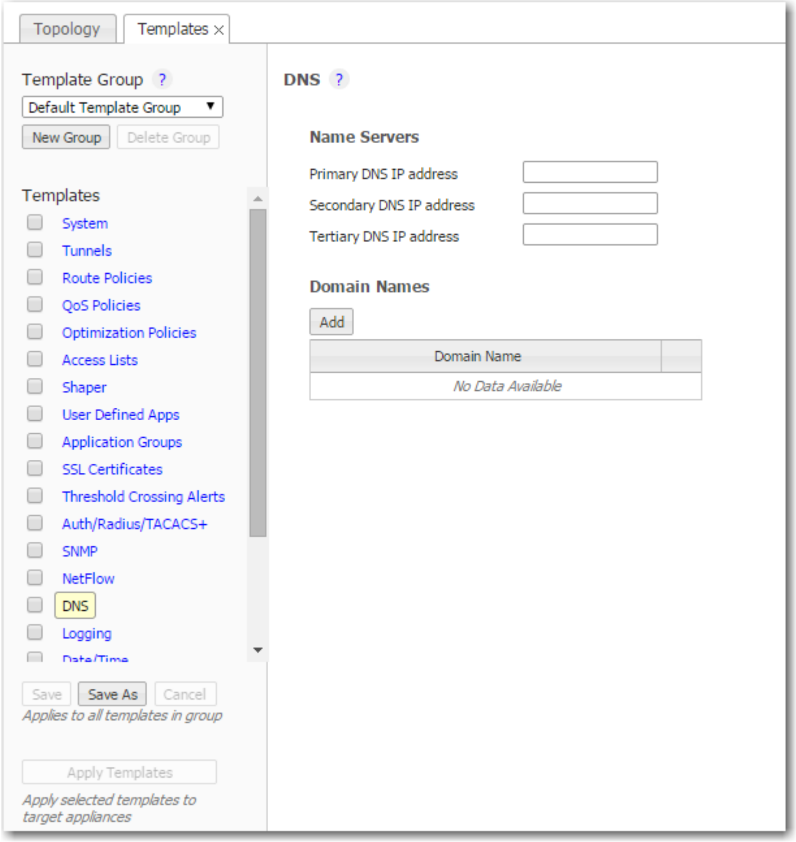
Collectors	IP Address	Port
No Data Available		

- The appliance exports flows against two virtual interfaces -- **sp_lan** and **sp_wan** -- that accumulate the total of LAN-side and WAN-side traffic, regardless of physical interface.
- These interfaces appear in SNMP and are therefore "discoverable" by NetFlow collectors.
- **Flow Exporting Enabled** allows the appliance to export the data to collectors (and makes the configuration fields accessible).
- The Collector's **IP Address** is the IP address of the device to which you're exporting the NetFlow statistics. The default Collector Port is 2055.
- In **Traffic Type**, you can select as many of the traffic types as you wish. The default is **Outbound WAN**.

DNS Template

A Domain Name Server (DNS) keeps a table of the IP addresses associated with domain names. It allows you to reference locations by domain name, such as mycompany.com, instead of using the routable IP address.

- You can configure up to three name servers.
- Under Domain Names, add the network domains to which your appliances belong.

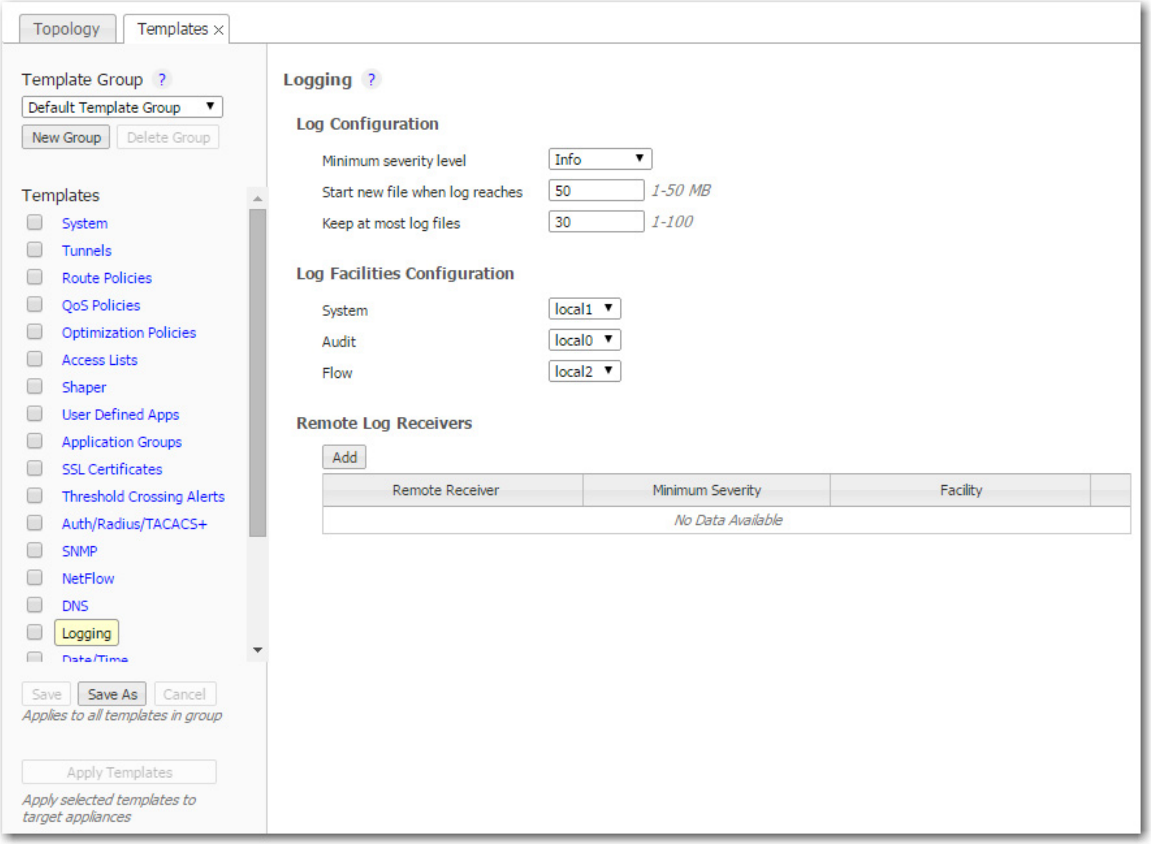


Logging Template

Use this template to configure local and remote logging parameters.

Each requires that you specify the minimum severity level of event to log.

- Set up local logging in the **Log Configuration** section.
- Set up remote logging by using the **Log Facilities Configuration** and **Remote Log Receivers** sections.



Logging

Log Configuration

Minimum severity level: Info

Start new file when log reaches: 50 (1-50 MB)

Keep at most log files: 30 (1-100)

Log Facilities Configuration

System: local1

Audit: local0

Flow: local2

Remote Log Receivers

Remote Receiver	Minimum Severity	Facility
No Data Available		

Minimum Severity Levels

In decreasing order of severity, the levels are as follows.

EMERGENCY The system is unusable.

ALERT Includes all alarms the appliance generates: **CRITICAL**, **MAJOR**, **MINOR**, and **WARNING**

CRITICAL A critical event

ERROR An error. This is a non-urgent failure.

WARNING A warning condition. Indicates an error will occur if action is not taken.

NOTICE A normal, but significant, condition. No immediate action required.

INFORMATIONAL Informational. Used by Silver Peak for debugging.

DEBUG Used by Silver Peak for debugging

NONE If you select **NONE**, then no events are logged.

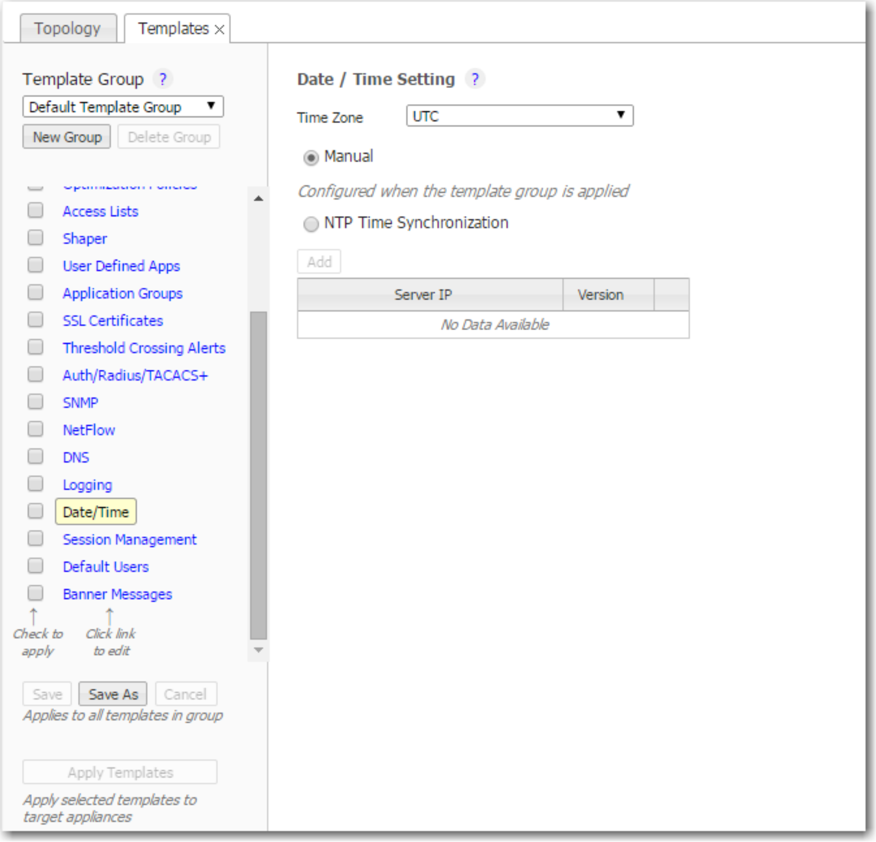
- The bolded part of the name is what displays in Silver Peak's logs.
- If you select **NOTICE** (the default), then the log records any event with a severity of NOTICE, WARNING, ERROR, CRITICAL, ALERT, and EMERGENCY.
- These are purely related to event logging levels, **not** alarm severities, even though some naming conventions overlap. Events and alarms have different sources. Alarms, once they clear, list as the ALERT level in the **Event Log**.

Configuring Remote Logging

- You can configure the appliance to forward all events, at and above a specified severity, to a remote syslog server.
- A syslog server is independently configured for the minimum severity level that it will accept. Without reconfiguring, it may not accept as low a severity level as you are forwarding to it.
- In the **Log Facilities Configuration** section, assign each message/event type (System / Audit / Flow) to a syslog facility level (**local0** to **local7**).
- For each remote syslog server that you add to receive the events, specify the receiver's IP address, along with the messages' minimum severity level and facility level.

Date/Time Template

Configure an appliance's **date and time** manually, or configure it to use an NTP (Network Time Protocol) server.



- From the **Time Zone** list, select the appliance's geographical location.
- Selecting **Manual** will match the appliance time to your web client system time when the template is applied. This is done to eliminate the delay between configuring time manually and applying the template.
- To use an NTP server, select **NTP Time Synchronization**.
  - Click **Add**.
  - Enter the IP address of the server, and select the version of NTP protocol to use.

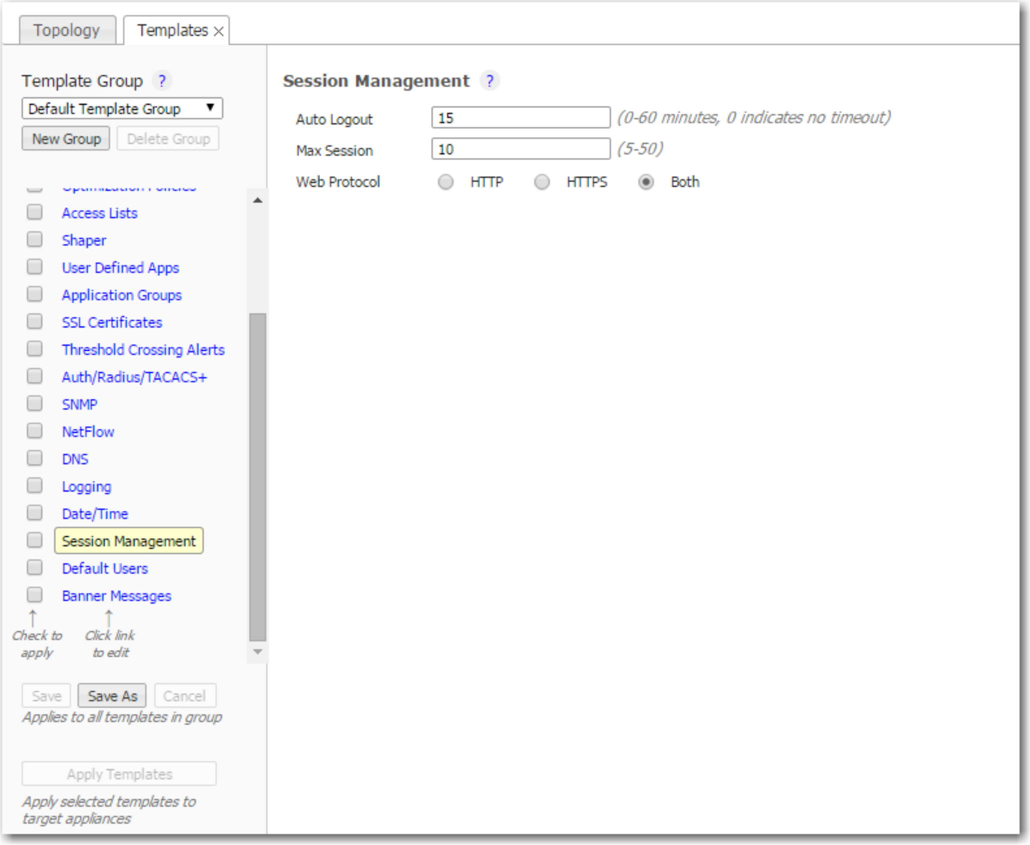
When you list more than one NTP server, the Appliance Manager selects the servers in the order listed, always defaulting to the available server uppermost on the list.

Data Collection

- Silver Peak's GMS (Global Management System) collects and puts all stats in its own database in Coordinated Universal Time (UTC).
- When a user views stats, the appliance (or GMS server) returning the stats always presents the information relative to its own time zone.

Session Management Template

Use this page to configure access to the web server.



Session Management ?

Auto Logout 15 (0-60 minutes, 0 indicates no timeout)

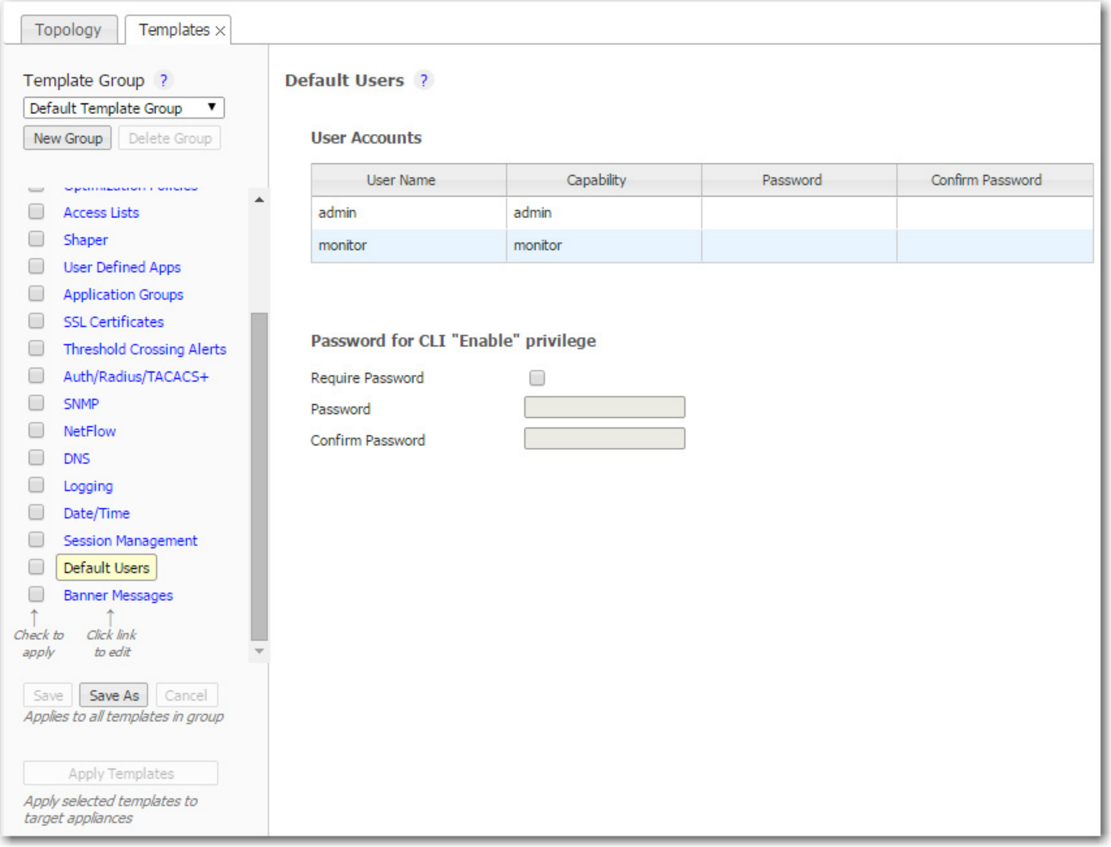
Max Session 10 (5-50)

Web Protocol ○ HTTP ○ HTTPS ● Both

- **Auto Logout** ends your web session after the specified minutes of inactivity.
- If the number of **Max Sessions** is exceeded, there are two possible consequences:
  - You'll get a message that the browser can't access the appliance.
  - Since the GMS must create a session to communicate with the appliance, it won't be able to access the appliance.
- Although **Web Protocol** defaults to **Both** for legacy reasons, Silver Peak recommends that you select **HTTPS** for maximum security.

Default Users Template

Use this page to manage the default users and, if desired, require a password with the highest user privilege level when using the Command Line Interface.



User Accounts

User Name	Capability	Password	Confirm Password
admin	admin		
monitor	monitor		

Password for CLI "Enable" privilege

Require Password □

Password

Confirm Password

Default User Accounts

- Each appliance has two default users, **admin** and **monitor**, who cannot be deleted.
- You can, however, assign a new password for either one, and apply it to any appliances you wish.

Command Line Interface privileges

- The Command Line Interface (CLI) for Silver Peak physical (NX) appliances has three command modes. In order of increasing permissions, they are User EXEC Mode, Privileged EXEC Mode, and Global Configuration Mode.
- When you first log into a Silver Peak appliance via a console port, you are in User EXEC Mode. This provides access to commands for many non-configuration tasks, such as checking the appliance status.
- To access the next level, Privileged EXEC Mode, you would enter the ***enable*** command. With this template, you can choose to associate and enforce a password with the ***enable*** command.

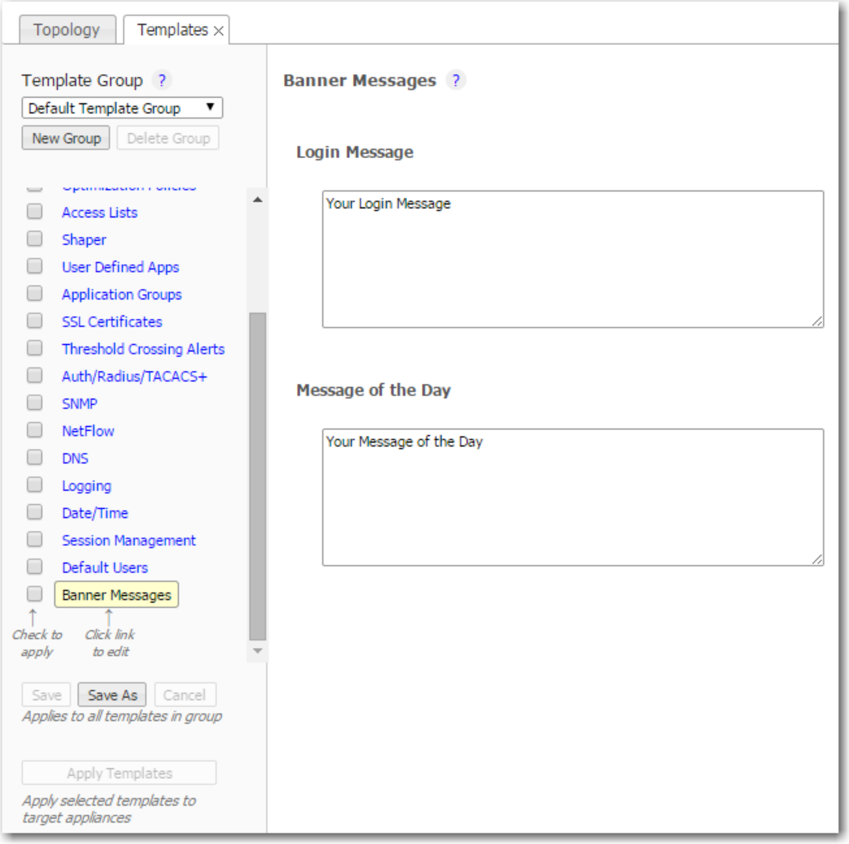
Guidelines for Creating Passwords

- Passwords should be a minimum of 8 characters.
- There should be at least one lower case letter and one upper case letter.

- There should be at least one digit.
- There should be at least one special character.
- Consecutive letters in the password should not form words found in the dictionary.

Banner Messages Template

- The **Login Message** appears before the login prompt.
- The **Message of the Day** appears after a successful login.



Template Group: Default Template Group

Login Message: Your Login Message

Message of the Day: Your Message of the Day

CHAPTER 3

Network & Policy Configuration Tabs

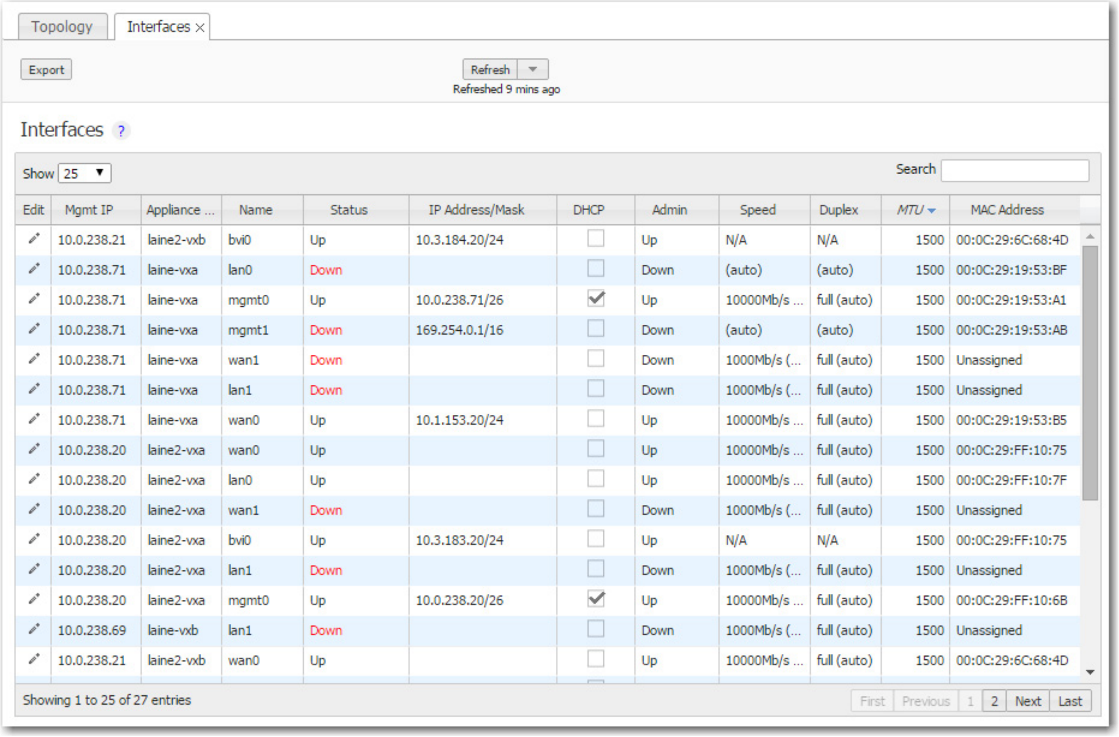
This chapter describes the tabs for configuring network and appliance parameters.

In This Chapter

Interfaces Tab

Configuration > Interfaces

The **Interfaces** tab lists the appliance interfaces.



Interfaces ?

Show 25 ▼ Search

Edit	Mgmt IP	Appliance ...	Name	Status	IP Address/Mask	DHCP	Admin	Speed	Duplex	MTU	MAC Address
✎	10.0.238.21	laine2-vxb	bvi0	Up	10.3.184.20/24	□	Up	N/A	N/A	1500	00:0C:29:6C:68:4D
✎	10.0.238.71	laine-vxa	lan0	Down		□	Down	(auto)	(auto)	1500	00:0C:29:19:53:BF
✎	10.0.238.71	laine-vxa	mgmt0	Up	10.0.238.71/26	☑	Up	10000Mb/s ...	full (auto)	1500	00:0C:29:19:53:A1
✎	10.0.238.71	laine-vxa	mgmt1	Down	169.254.0.1/16	□	Down	(auto)	(auto)	1500	00:0C:29:19:53:AB
✎	10.0.238.71	laine-vxa	wan1	Down		□	Down	1000Mb/s (...	full (auto)	1500	Unassigned
✎	10.0.238.71	laine-vxa	lan1	Down		□	Down	1000Mb/s (...	full (auto)	1500	Unassigned
✎	10.0.238.71	laine-vxa	wan0	Up	10.1.153.20/24	□	Up	10000Mb/s ...	full (auto)	1500	00:0C:29:19:53:B5
✎	10.0.238.20	laine2-vxa	wan0	Up		□	Up	10000Mb/s ...	full (auto)	1500	00:0C:29:FF:10:75
✎	10.0.238.20	laine2-vxa	lan0	Up		□	Up	10000Mb/s ...	full (auto)	1500	00:0C:29:FF:10:7F
✎	10.0.238.20	laine2-vxa	wan1	Down		□	Down	1000Mb/s (...	full (auto)	1500	Unassigned
✎	10.0.238.20	laine2-vxa	bvi0	Up	10.3.183.20/24	□	Up	N/A	N/A	1500	00:0C:29:FF:10:75
✎	10.0.238.20	laine2-vxa	lan1	Down		□	Down	1000Mb/s (...	full (auto)	1500	Unassigned
✎	10.0.238.20	laine2-vxa	mgmt0	Up	10.0.238.20/26	☑	Up	10000Mb/s ...	full (auto)	1500	00:0C:29:FF:10:6B
✎	10.0.238.69	laine-vxb	lan1	Down		□	Down	1000Mb/s (...	full (auto)	1500	Unassigned
✎	10.0.238.21	laine2-vxb	wan0	Up		□	Up	10000Mb/s ...	full (auto)	1500	00:0C:29:6C:68:4D

Showing 1 to 25 of 27 entries

- As a best practice, assign static IP addresses to management interfaces to preserve their reachability.
- **Speed/Duplex** should never display as half duplex after auto-negotiation. If it does, the appliance will experience performance issues and dropped connections. To resolve, check the cabling on the appliance and the ports on the adjacent switch/router.
- To directly change interface parameters for a particular appliance, click **Edit**. It takes you to the Appliance Manager's **Configuration > Interfaces** page.
- To change the IP address for a **lan** or **wan** interface, either use the Appliance Manager's **Configuration > Deployment** page or the CLI (Command Line Interface).
- To change the IP address for **mgmt0**, either use the Appliance Manager's **Administration > Management IP/Hostname** page or the CLI.

Terminology

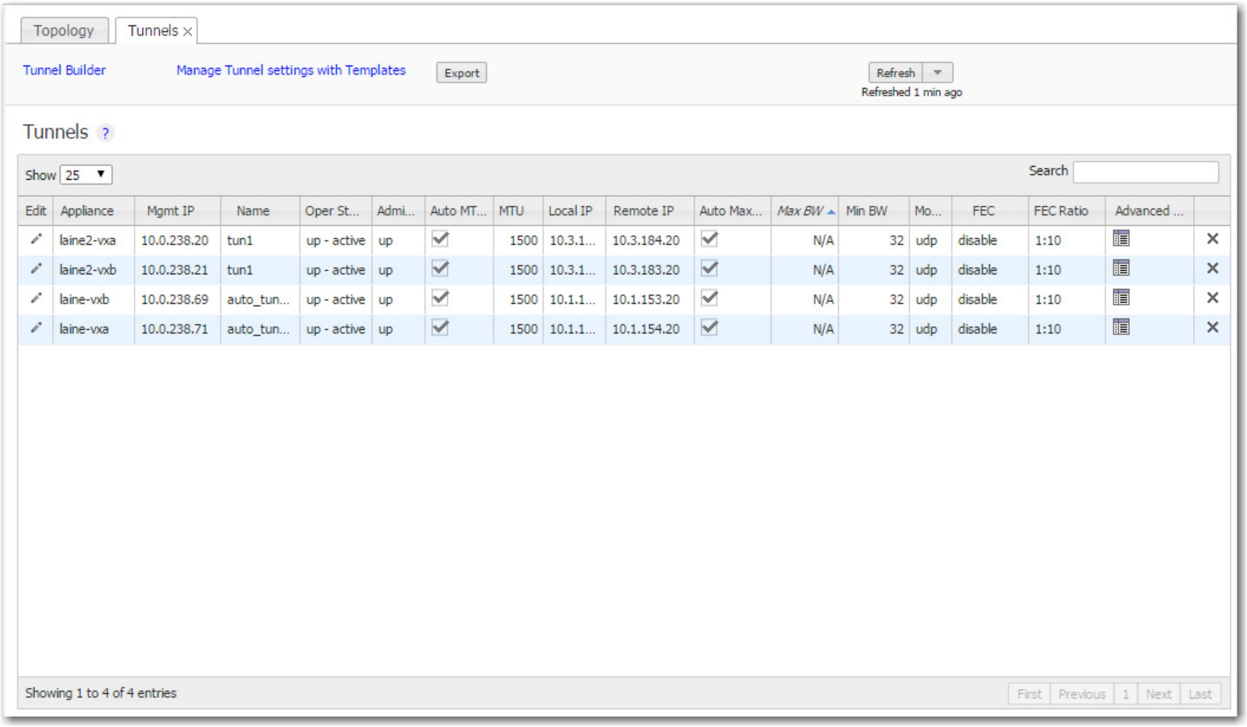
- **blan**: Bonded lan interfaces (as in **lan0** + **lan1**).
- **bvi0**: Bridge Virtual Interface. When the appliance is deployed in-line (Bridge mode), it's the routed interface that represents the bridging of **wan0** and **lan0**.
- **bwan**: Bonded **wan** interfaces (as in **wan0** + **wan1**).
- **tlan**: 10-Gbps fiber **lan** interface.
- **twan**: 10-Gbps fiber **wan** interface.

Tunnels Tab

Configuration > Tunnels

Use this page to **view**, **edit**, and **delete** tunnels.

- To manage tunnels and assign their properties, use the **Tunnels** section of the **Templates** tab.
- To create tunnels, use the **Tunnel Builder** tab.



Edit	Appliance	Mgmt IP	Name	Oper St...	Admi...	Auto MT...	MTU	Local IP	Remote IP	Auto Max...	*Max BW* ▲	Min BW	Mo...	FEC	FEC Ratio	Advanced ...	
✎	laine2-vxa	10.0.238.20	tun1	up - active	up	☑	1500	10.3.1...	10.3.184.20	☑	N/A	32	udp	disable	1:10	▤	✕
✎	laine2-vxb	10.0.238.21	tun1	up - active	up	☑	1500	10.3.1...	10.3.183.20	☑	N/A	32	udp	disable	1:10	▤	✕
✎	laine-vxb	10.0.238.69	auto_tun...	up - active	up	☑	1500	10.1.1...	10.1.153.20	☑	N/A	32	udp	disable	1:10	▤	✕
✎	laine-vxa	10.0.238.71	auto_tun...	up - active	up	☑	1500	10.1.1...	10.1.154.20	☑	N/A	32	udp	disable	1:10	▤	✕

Showing 1 to 4 of 4 entries

Definitions (alphabetically)

- **Admin Status** indicates whether the tunnel has been set to admin **Up** or **Down**.
- **Local IP** is the IP address for the local appliance.
- **Max BW** is the maximum bandwidth for this tunnel, in kilobits per second. This must be **less than or equal to** the upstream bandwidth of your WAN connection.
- **Mode** indicates whether the tunnel protocol is **udp**, **gre**, or **ipsec**.
- **MTU (bytes)** (Maximum Transmission Unit) is the largest possible unit of data that can be sent on a given physical medium. For example, the MTU of Ethernet is 1500 bytes. Silver Peak provides support for MTUs up to 9000 bytes.
- **Oper Status** indications are as follows:
  - **Down** = The tunnel is down. This can be because the tunnel administrative setting is down, or the tunnel can't communicate with the appliance at the other end. Possible causes are:
    - Lack of end-to-end connectivity / routability (test with *iperf*)
    - Intermediate firewall is dropping the packets (open the firewall)
    - Intermediate QoS policy (**be** packets are being starved. Change control packet DSCP marking)

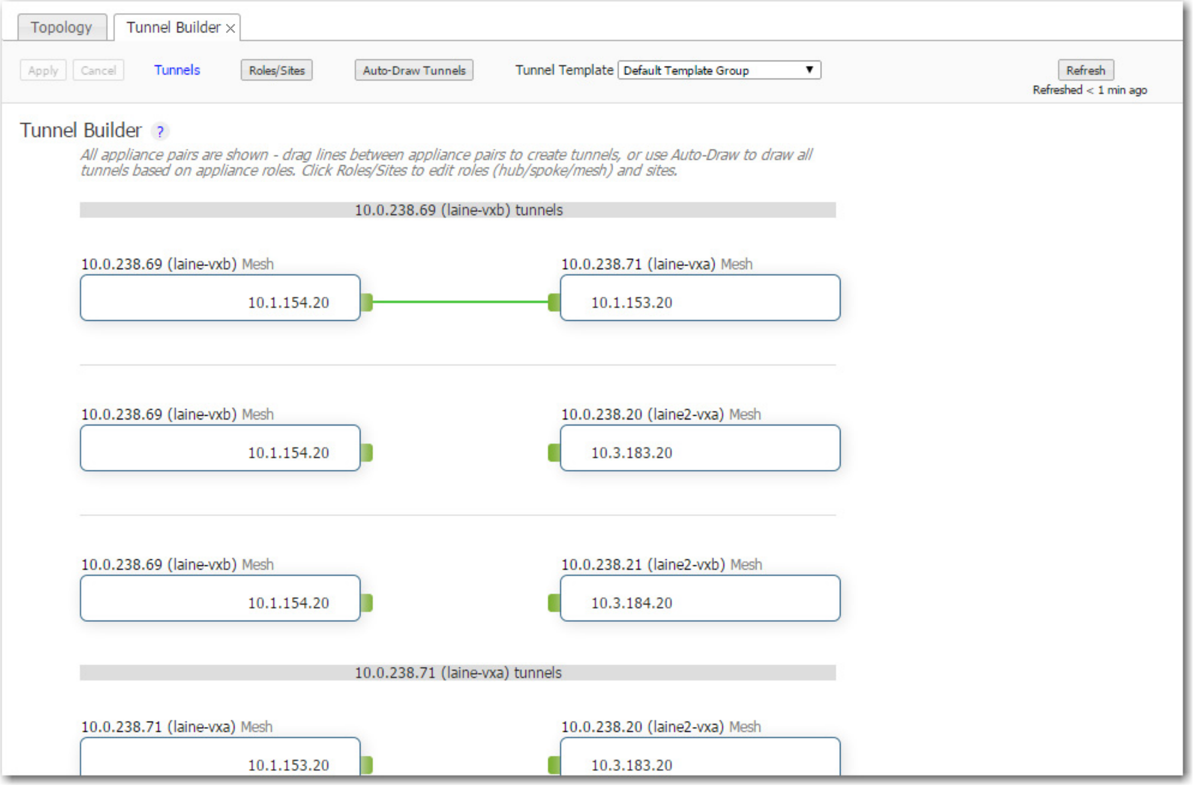
        - Mismatched tunnel mode (**udp** / **gre** / **ipsec**)
        - IPsec is misconfigured: (1) enabled on one side (see *show int tunnel configured*), or (2) mismatched pre-shared key
    - **Down - In progress** = The tunnel is down. Meanwhile, the appliance is exchanging control information with the appliance at the other end, trying to bring up the tunnel.
    - **Down - Misconfigured** = The two appliances are configured with the same System ID. (see show system)
    - **Up - Active** = The tunnel is up and active. Traffic destined for this tunnel will be forwarded to the remote appliance.
    - **Up - Active - Idle** = The tunnel is up and active but hasn't had recent activity in the past five minutes, and has slowed the rate of issuing keep-alive packets.
    - **Up - Reduced Functionality** = The tunnel is up and active, but the two endpoint appliances are running mismatched software releases that give no performance benefit.
    - **UNKNOWN** = The tunnel status is unknown. This can be because the appliance is unable to retrieve the current tunnel status. Try again later.
- **Remote IP** is the IP address for the remote appliance.
- **Uptime** is how long since the tunnel came up.

Tunnel Builder

Configuration > Tunnel Builder

Use this page to **create** tunnels.

- To manage tunnels and assign their properties, use the **Tunnels** section of the **Templates** tab.
- To view, edit, and delete tunnels, use the **Tunnels** tab.
- Tunnels are **color-coded**: Green = Up, Red = Down, Blue = Pending (before final **Apply**)
- To delete a tunnel (pending or not), click on it. Confirm in the dialog box that appears.



All appliance pairs are shown - drag lines between appliance pairs to create tunnels, or use Auto-Draw to draw all tunnels based on appliance roles. Click Roles/Sites to edit roles (hub/spoke/mesh) and sites.

10.0.238.69 (laine-vxb) tunnels

10.0.238.69 (laine-vxb) Mesh 10.1.154.20 — 10.0.238.71 (laine-vxa) Mesh 10.1.153.20

10.0.238.69 (laine-vxb) Mesh 10.1.154.20 — 10.0.238.20 (laine2-vxa) Mesh 10.3.183.20

10.0.238.69 (laine-vxb) Mesh 10.1.154.20 — 10.0.238.21 (laine2-vxb) Mesh 10.3.184.20

10.0.238.71 (laine-vxa) tunnels

10.0.238.71 (laine-vxa) Mesh 10.1.153.20 — 10.0.238.20 (laine2-vxa) Mesh 10.3.183.20

To create tunnels, follow this sequence:

1. In the **Navigation** window, select the appliances.
   For 4 and fewer appliances, all appliances and interfaces display. For more, a scaled view appears.
2. To verify or change a Network Role (mesh / hub / spoke), click **Roles/Sites**.
   To exclude peers from having connecting tunnels, assign them the same Site name, and assign the primary appliance the lower **Priority** value.
3. Assign tunnel properties by selecting a **Tunnel Template**.
4. Use ***either*** of these two methods to create tunnels:
   - Click and drag a line from one interface to another.
   - Click **Auto-Draw Tunnels**. When an appliance has more than 2 interfaces and its peer has more than 1 interface, then auto-build will not create tunnels.

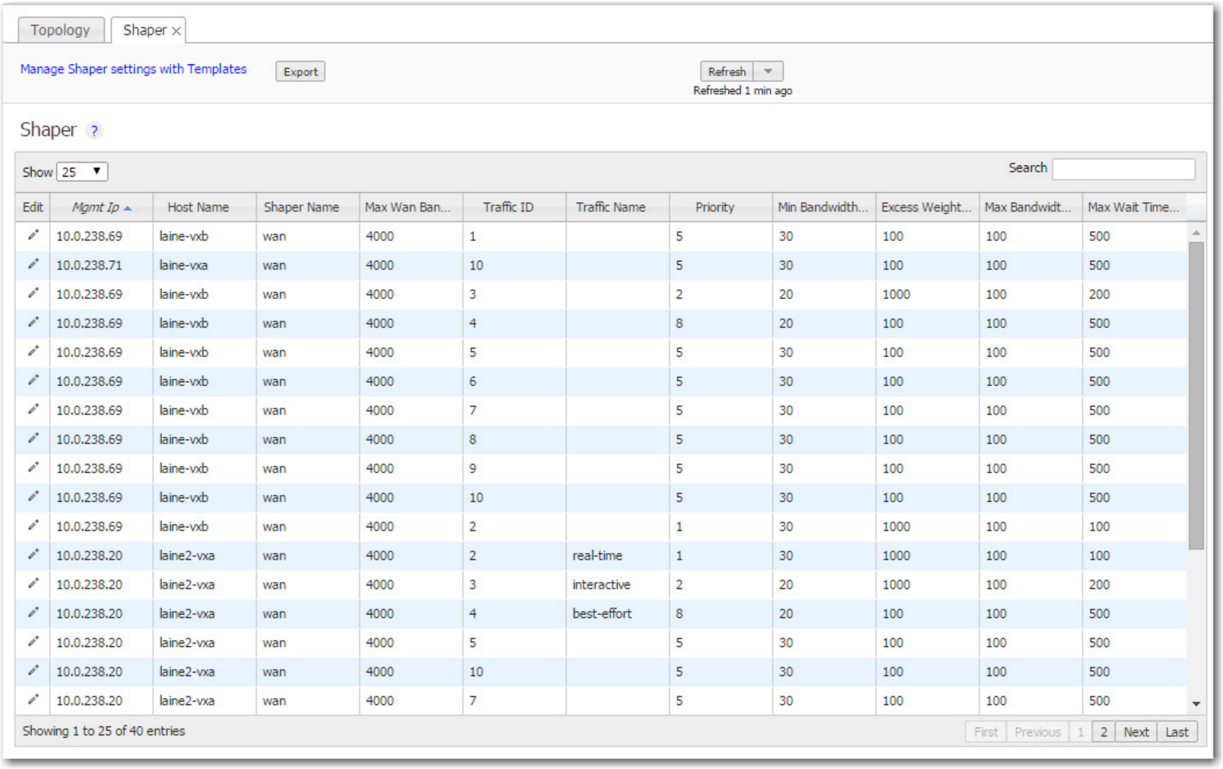
   If you deselect an appliance (in the Navigation pane) that has pending tunnels, its pending tunnels are discarded.
5. Click **Apply**. A table summarizing the proposed changes appears. To implement them, click **Apply**.

Shaper Tab

Configuration > Shaper

This report provides a view of the Shaper settings.

The **Shaper** provides a simplified way to globally configure QoS (Quality of Service) on the appliances.



Edit	Mgmt Ip ▲	Host Name	Shaper Name	Max Wan Ban...	Traffic ID	Traffic Name	Priority	Min Bandwidth...	Excess Weight...	Max Bandwidt...	Max Wait Time...
✎	10.0.238.69	laine-vxb	wan	4000	1		5	30	100	100	500
✎	10.0.238.71	laine-vxa	wan	4000	10		5	30	100	100	500
✎	10.0.238.69	laine-vxb	wan	4000	3		2	20	1000	100	200
✎	10.0.238.69	laine-vxb	wan	4000	4		8	20	100	100	500
✎	10.0.238.69	laine-vxb	wan	4000	5		5	30	100	100	500
✎	10.0.238.69	laine-vxb	wan	4000	6		5	30	100	100	500
✎	10.0.238.69	laine-vxb	wan	4000	7		5	30	100	100	500
✎	10.0.238.69	laine-vxb	wan	4000	8		5	30	100	100	500
✎	10.0.238.69	laine-vxb	wan	4000	9		5	30	100	100	500
✎	10.0.238.69	laine-vxb	wan	4000	10		5	30	100	100	500
✎	10.0.238.69	laine-vxb	wan	4000	2		1	30	1000	100	100
✎	10.0.238.20	laine2-vxa	wan	4000	2	real-time	1	30	1000	100	100
✎	10.0.238.20	laine2-vxa	wan	4000	3	interactive	2	20	1000	100	200
✎	10.0.238.20	laine2-vxa	wan	4000	4	best-effort	8	20	100	100	500
✎	10.0.238.20	laine2-vxa	wan	4000	5		5	30	100	100	500
✎	10.0.238.20	laine2-vxa	wan	4000	10		5	30	100	100	500
✎	10.0.238.20	laine2-vxa	wan	4000	7		5	30	100	100	500

Showing 1 to 25 of 40 entries

- It shapes outbound traffic by allocating bandwidth as a percentage of the system bandwidth.
- The Shaper's parameters are organized into ten traffic classes. Four traffic classes are preconfigured and named --- **real-time**, **interactive**, **default**, and **best effort**.
- The system applies these QoS settings globally after compressing (deduplicating) all the outbound tunnelized and pass-through-shaped traffic --- shaping it as it exits to the WAN.
- To manage Shaper settings for an appliance's system-level **wan** Shaper, access the Shaper template.

Definitions

- **Traffic Name**: Name assigned to a traffic class, either prescriptively or by the user.
- **Priority**: Determines the order in which to allocate each class's minimum bandwidth - 1 is first, 10 is last.
- **Min Bandwidth**: Refers to the percentage of bandwidth guaranteed to each traffic class, allocated by priority. However, if the sum of the percentages is greater than 100%, then lower-priority traffic classes might not receive their guaranteed bandwidth if it's all consumed by higher-priority traffic.

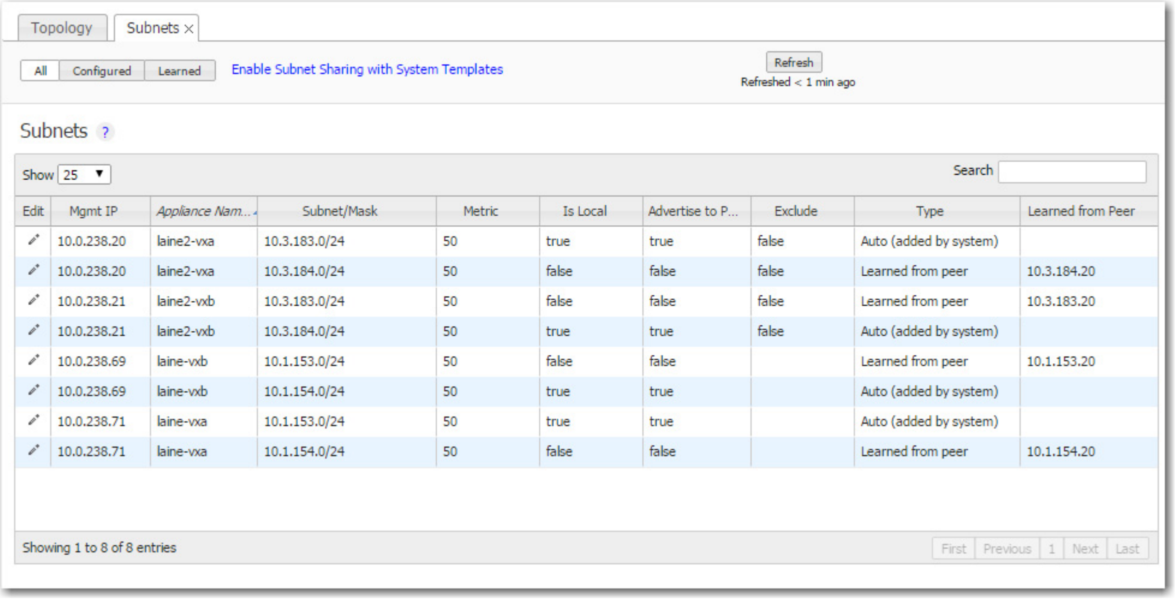
  If you set **Min Bandwidth** to a value greater than **Max Bandwidth**, then **Max** overrides **Min**.
- **Excess Weighting**: If there is bandwidth left over after satisfying the minimum bandwidth percentages, then the excess is distributed among the traffic classes, in proportion to the weightings specified in the **Excess Weighting** column. Values range from 1 to 10,000.

- **Max Bandwidth**: You can limit the maximum bandwidth that a traffic class uses by specifying a percentage in the **Max Bandwidth** column. The bandwidth usage for the traffic class will never exceed this value.
- **Max Wait Time**: Any packets waiting longer than the specified **Max Wait Time** are dropped.

Subnets Tab

Configuration > Shaper

To add, edit, or delete a subnet, you must ***select an individual appliance*** from the navigation panel.



Edit	Mgmt IP	Appliance Nam...	Subnet/Mask	Metric	Is Local	Advertise to P...	Exclude	Type	Learned from Peer
✎	10.0.238.20	laine2-vxa	10.3.183.0/24	50	true	true	false	Auto (added by system)	
✎	10.0.238.20	laine2-vxa	10.3.184.0/24	50	false	false	false	Learned from peer	10.3.184.20
✎	10.0.238.21	laine2-vxb	10.3.183.0/24	50	false	false	false	Learned from peer	10.3.183.20
✎	10.0.238.21	laine2-vxb	10.3.184.0/24	50	true	true	false	Auto (added by system)	
✎	10.0.238.69	laine-vxb	10.1.153.0/24	50	false	false		Learned from peer	10.1.153.20
✎	10.0.238.69	laine-vxb	10.1.154.0/24	50	true	true		Auto (added by system)	
✎	10.0.238.71	laine-vxa	10.1.153.0/24	50	true	true		Auto (added by system)	
✎	10.0.238.71	laine-vxa	10.1.154.0/24	50	false	false		Learned from peer	10.1.154.20

Showing 1 to 8 of 8 entries

What is subnet sharing?

Subnet sharing is one of the three strategies that Silver Peak uses to auto-optimize all IP traffic, automatically directing flows to the appropriate tunnel. Auto-optimization strategies reduce the need to create explict route map entries to optimize traffic. The other two strategies are **TCP-based** auto-opt and **IP-based** auto-opt.

Note Enabled by default, the global settings for all three reside on the **Templates** tab, under **System**.

How is subnet sharing implemented?

Each appliance builds a subnet table from entries added automatically by the system or manually by a user. When two appliances are connected by a tunnel, they exchange this information ("learn" it) and use it to route traffic to each other.

When would you need to use a Route Policy template?

Subnet sharing takes care of optimizing IP traffic.

Use and apply a Route Policy template for flows that are to be:

- sent pass-through (shaped or unshaped)
- dropped
- configured for a specific high-availability deployment
- routed based on application, ports, VLAN, DSCP, or ACL (Access Control List)

Subnet table columns

- **Subnet/Mask**: Actual subnet to be shared or learned
- **Metric**: Metric of the subnet. Value must be between 0 and 100. When a peer has more than one tunnel with a matching subnet (for example, in a high availability deployment), it chooses the tunnel with the greater numerical value.
- **Is Local**: Specifies if the subnet is local to this site.

  The appliance sets this parameter for **automatically** added subnets because those subnets are directly attached to an appliance interface, and therefore are most likely local to the appliance.

  Also, you can select the parameter when **manually** adding a subnet:

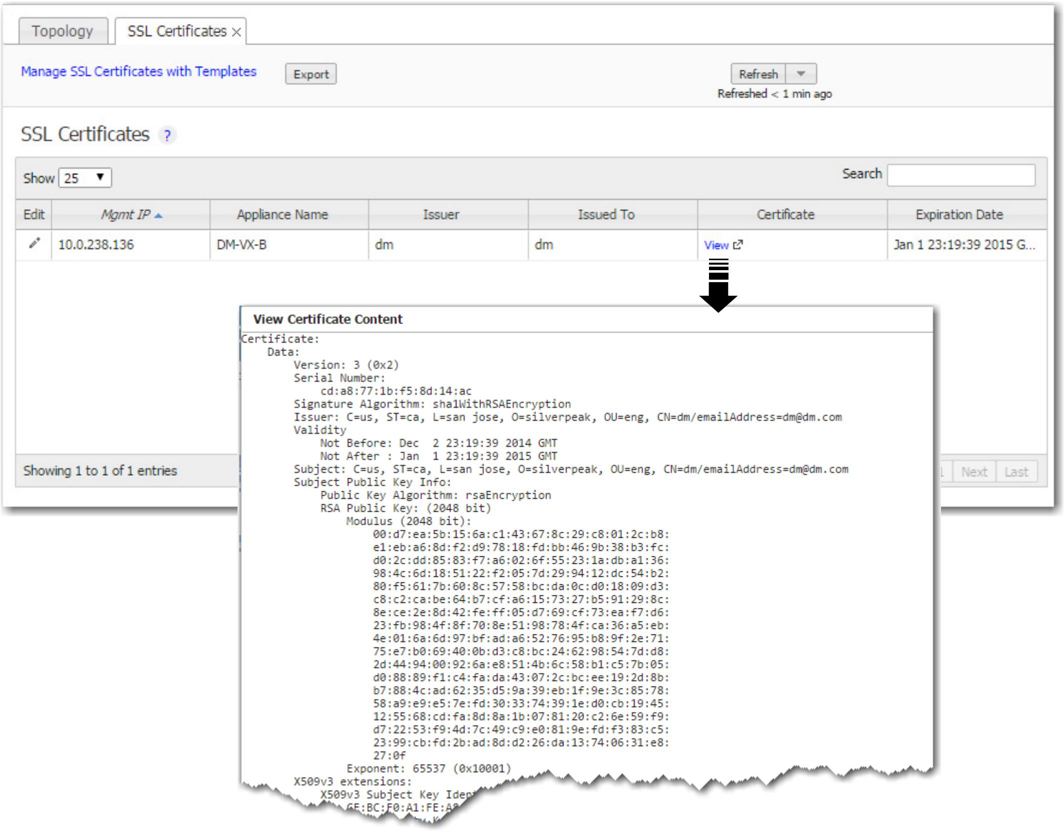
  - Select this option for a manually added subnet if all the IP addresses in the subnet are known to be local.
  - Deselect this option if the subnet is so large (for example, 0.0.0.0/0) that it may include IP addresses that are not local to this appliance. If a subnet is too wide, and it's marked **local**, then the stats will count any pass-through packets with an IP address within that range as WAN-to-LAN.
- **Exclude**: Use this option to prevent optimization of more specific subnets from a wider advertised subnet range.
- **Advertise to Peers**: Selected by default, it shares the subnet information with peers. Peers then learn it.

  To add a subnet to the table without divulging it to peers, yet, deselect this option.
- **Type** of subnet:
  - **Auto (added by system)** = automatically added subnets of interfaces on this appliance
  - **Auto (added by saas optimization)** = automatically added subnets from SaaS services
  - **Added by user** = manually added/configured subnets for this appliance
  - **Learned from peer** = subnets added as a result of exchanging information with peer appliances
- **Learned from Peer**: Which peer appliance advertised (and shared) this subnet information

SSL Certificates Tab

Configuration > SSL Certificates

Silver Peak provides deduplication for Secure Socket Layer (SSL) encrypted WAN traffic by supporting the use of SSL certificates and keys.



Edit	*Mgmt IP* ▲	Appliance Name	Issuer	Issued To	Certificate	Expiration Date
✎	10.0.238.136	DM-VX-B	dm	dm	View	Jan 1 23:19:39 2015 G...

Showing 1 to 1 of 1 entries

View Certificate Content

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            cd:a8:77:1b:f5:8d:14:ac
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=us, ST=ca, L=san jose, O=silverpeak, OU=eng, CN=dm/emailAddress=dm@dm.com
        Validity
            Not Before: Dec  2 23:19:39 2014 GMT
            Not After : Jan  1 23:19:39 2015 GMT
        Subject: C=us, ST=ca, L=san jose, O=silverpeak, OU=eng, CN=dm/emailAddress=dm@dm.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:d7:ea:5b:15:6a:c1:43:67:8c:29:c8:01:2c:b8:
                    e1:eb:a6:8d:f2:d9:78:18:fd:bb:46:9b:38:b3:fc:
                    d0:2c:dd:85:83:f7:a6:02:6f:55:23:1a:db:a1:36:
                    98:4c:6d:18:51:22:f2:05:7d:29:94:12:dc:54:b2:
                    80:f5:61:7b:60:8c:57:58:bc:da:0c:d0:18:09:d3:
                    c8:c2:ca:be:64:b7:cf:a6:15:73:27:b5:91:29:8c:
                    8e:ce:2e:8d:42:fe:ff:05:d7:69:cf:73:ea:f7:d6:
                    23:fb:98:4f:8f:70:8e:51:98:78:4f:ca:36:a5:eb:
                    4e:01:6a:6d:97:bf:ad:a6:52:76:95:b8:9f:2e:71:
                    75:e7:b0:69:40:0b:d3:c8:bc:24:62:98:54:7d:d8:
                    2d:44:94:00:92:6a:e8:51:4b:6c:58:b1:c5:7b:05:
                    d0:88:89:f1:c4:fa:da:43:07:2c:bc:ee:19:2d:8b:
                    b7:88:4c:ad:62:35:d5:9a:39:eb:1f:9e:3c:85:78:
                    58:a9:e9:e5:7e:fd:30:33:74:39:1e:d0:cb:19:45:
                    12:55:68:cd:fa:8d:8a:1b:07:81:20:c2:6e:59:f9:
                    d7:22:53:f9:4d:7c:49:c9:e0:81:9e:fd:f3:83:c5:
                    23:99:cb:fd:2b:ad:8d:d2:26:da:13:74:06:31:e8:
                    27:0f
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Iden
                6E:BC:F0:A1:FE:A
```

This report summarizes the SSL certificates installed on appliances.

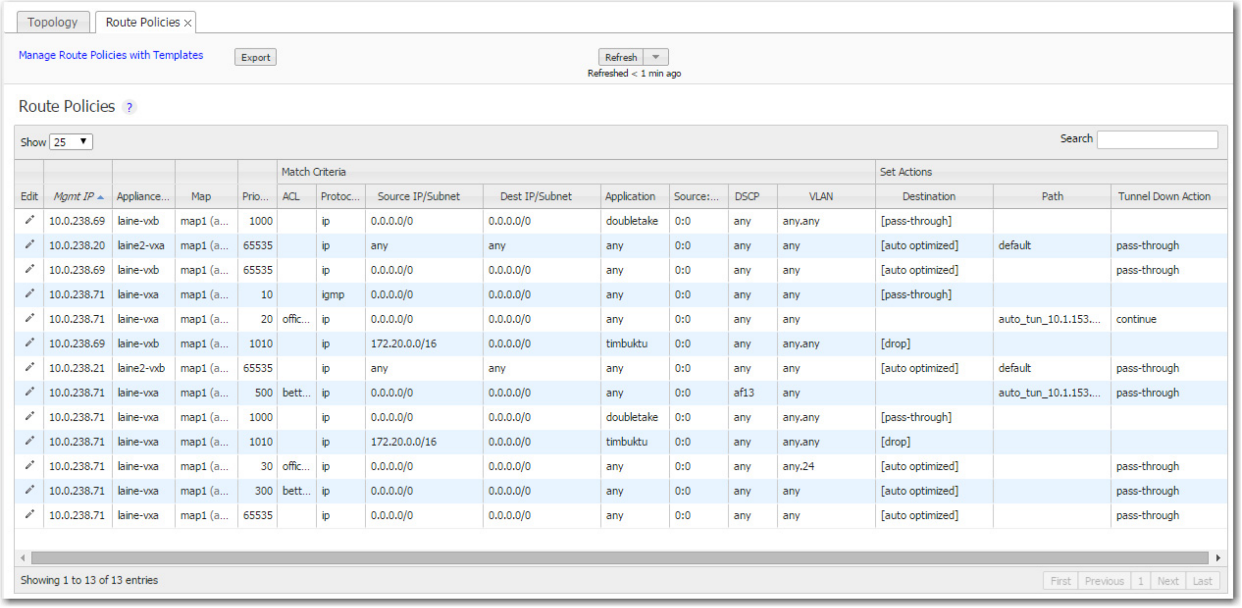
- Silver Peak decrypts SSL data using the configured certificates and keys, optimizes the data, and transmits data over an IPSec tunnel. The peer Silver Peak appliance uses configured SSL certificates to re-encrypt data before transmitting.
- Peers that exchange and optimize SSL traffic must use the same certificate and key.
- Silver Peak supports X509 Privacy Enhanced Mail (PEM), Personal Information Exchange (PFX, generally for Microsoft servers), and RSA key 1024-bit and 2048-bit certificate formats.
- Silver Peak appliances support:
  - **Protocol versions**: SSLv3, SSLv3.3, TLS1.0, TLS1.1, TLS1.2
  - **Cipher algorithms**: AES128, AES256, RC4, 3DES
  - **Digests**: MD5, SHA1
- For the SSL certificates to function, the following must also be true:
  - The tunnels are in **IPSec** mode for both directions of traffic.
  - In the *Optimization Policy*, **TCP acceleration** and **SSL acceleration** are enabled.

Route Policies Tab

Configuration > Route Policies

The **Route Policies** report displays the route policy entries that exist on the appliance(s).

This includes the appliance-based defaults, entries applied manually (via the WebUI or CLI), and entries that result from applying a GMS Route Policies template.



Route Policies ?

Show 25 ▼ Search

					Match Criteria								Set Actions		
Edit	Mgmt IP ▲	Appliance...	Map	Prio...	ACL	Protoc...	Source IP/Subnet	Dest IP/Subnet	Application	Source:...	DSCP	VLAN	Destination	Path	Tunnel Down Action
✎	10.0.238.69	laine-vxb	map1 (a...	1000		ip	0.0.0.0/0	0.0.0.0/0	doubletake	0:0	any	any.any	[pass-through]		
✎	10.0.238.20	laine2-vxa	map1 (a...	65535		ip	any	any	any	0:0	any	any	[auto optimized]	default	pass-through
✎	10.0.238.69	laine-vxb	map1 (a...	65535		ip	0.0.0.0/0	0.0.0.0/0	any	0:0	any	any	[auto optimized]		pass-through
✎	10.0.238.71	laine-vxa	map1 (a...	10		igmp	0.0.0.0/0	0.0.0.0/0	any	0:0	any	any	[pass-through]		
✎	10.0.238.71	laine-vxa	map1 (a...	20	offic...	ip	0.0.0.0/0	0.0.0.0/0	any	0:0	any	any		auto_tun_10.1.153....	continue
✎	10.0.238.69	laine-vxb	map1 (a...	1010		ip	172.20.0.0/16	0.0.0.0/0	timbuktu	0:0	any	any.any	[drop]		
✎	10.0.238.21	laine2-vxb	map1 (a...	65535		ip	any	any	any	0:0	any	any	[auto optimized]	default	pass-through
✎	10.0.238.71	laine-vxa	map1 (a...	500	bett...	ip	0.0.0.0/0	0.0.0.0/0	any	0:0	af13	any		auto_tun_10.1.153....	pass-through
✎	10.0.238.71	laine-vxa	map1 (a...	1000		ip	0.0.0.0/0	0.0.0.0/0	doubletake	0:0	any	any.any	[pass-through]		
✎	10.0.238.71	laine-vxa	map1 (a...	1010		ip	172.20.0.0/16	0.0.0.0/0	timbuktu	0:0	any	any.any	[drop]		
✎	10.0.238.71	laine-vxa	map1 (a...	30	offic...	ip	0.0.0.0/0	0.0.0.0/0	any	0:0	any	any.24	[auto optimized]		pass-through
✎	10.0.238.71	laine-vxa	map1 (a...	300	bett...	ip	0.0.0.0/0	0.0.0.0/0	any	0:0	any	any	[auto optimized]		pass-through
✎	10.0.238.71	laine-vxa	map1 (a...	65535		ip	0.0.0.0/0	0.0.0.0/0	any	0:0	any	any	[auto optimized]		pass-through

Showing 1 to 13 of 13 entries

Each appliance's default behavior is to auto-optimize all IP traffic, automatically directing flows to the appropriate tunnel. **Auto-optimization** strategies reduce the need to create explicit route map entries for optimization. The three strategies that Silver Peak uses are **TCP-based** auto-opt, **IP-based** auto-opt, and **subnet sharing**. By default, all three are enabled on the **Templates** tab, under **System**.

The Route Policy, then, only requires entries for flows that are to be:

- sent pass-through (shaped or unshaped)
- dropped
- configured for a specific high-availability deployment
- routed based on application, VLAN, DSCP, or ACL (Access Control List)

You may also want to create a Route Policy entry when multiple tunnels exist to the remote ***peer***, and you want the appliance to dynamically select the best path based on one of these criteria:

- load balancing
- lowest loss
- lowest latency
- specified tunnel

Manage these instances on the **Templates** tab, or click the **Edit** icon to manage Route policies directly for a particular appliance.

Tip If you're upgrading from a software version that precedes VXOA 6.2.x, you can migrate subnets from legacy GMS route maps to the appliance's subnet table for subnet sharing. In the menus, go to **Maintenance > Tools > Migrate GMS Route Maps**.

Priority

- You can create rules with any priority between 1 and 65534.
    - If you are using GMS templates to add route map entries, GMS will delete all entries from **1000 – 9999**, inclusive, before applying its policies.
    - You can create rules from **1 – 999**, which have higher priority than GMS template rules.
    - Similarly, you can create rules from **10000 – 65534** which have lower priority than GMS template rules.
- Adding a rule increments the last Priority by 10. This leaves room for you to insert a rule in between rules without having to renumber subsequent priorities. Likewise, you can just edit the number.

Source or Destination

- An IP address can specify a subnet - for example: 10.10.10.0/24 (IPv4) or fe80::204:23ff:fed8:4ba2/64 (IPv6).
- To allow **any IP address**, use 0.0.0.0/0 (IPv4) or ::/0 (IPv6).
- Ports are available only for the protocols **tcp**, **udp**, and **tcp/udp**.
- To allow **any port**, use **0**.

QoS Policies Tab

Configuration > QoS Policies

The QoS Policy determines how flows are queued and marked.

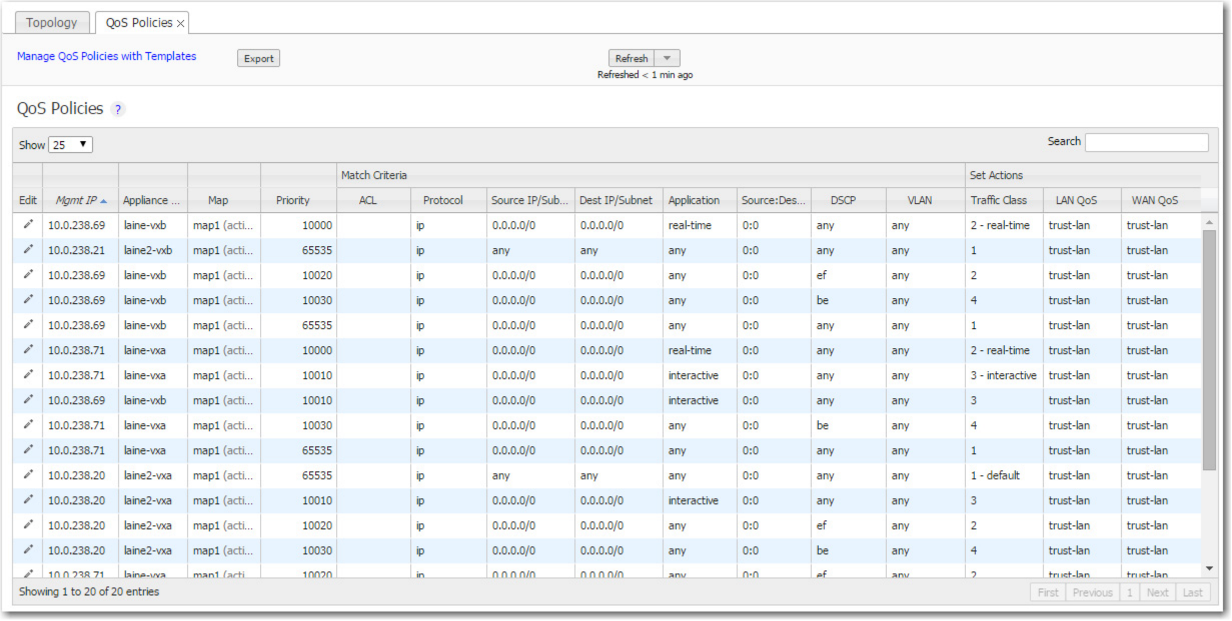
The **QoS Policies** tab displays the QoS policy entries that exist on the appliances.

This includes the appliance-based defaults, entries applied manually (via the WebUI or CLI), and entries that result from applying a GMS QoS Policy template.

Both the Shaper and the QoS Policy deal with traffic classes. How are they related?

>> The Shaper **defines** and the QoS Policy **assigns**. <<

Use the **Templates** tab to create and manage QoS policies for multiple appliances, or click the **Edit** icon to manage QoS Policies directly for a particular appliance.



QoS Policies ?

Show 25 ▼

					Match Criteria								Set Actions		
Edit	Mgmt IP ▲	Appliance ...	Map	Priority	ACL	Protocol	Source IP/Sub...	Dest IP/Subnet	Application	Source:Des...	DSCP	VLAN	Traffic Class	LAN QoS	WAN QoS
✎	10.0.238.69	laine-vxb	map1 (acti...	10000		ip	0.0.0.0/0	0.0.0.0/0	real-time	0:0	any	any	2 - real-time	trust-lan	trust-lan
✎	10.0.238.21	laine2-vxb	map1 (acti...	65535		ip	any	any	any	0:0	any	any	1	trust-lan	trust-lan
✎	10.0.238.69	laine-vxb	map1 (acti...	10020		ip	0.0.0.0/0	0.0.0.0/0	any	0:0	ef	any	2	trust-lan	trust-lan
✎	10.0.238.69	laine-vxb	map1 (acti...	10030		ip	0.0.0.0/0	0.0.0.0/0	any	0:0	be	any	4	trust-lan	trust-lan
✎	10.0.238.69	laine-vxb	map1 (acti...	65535		ip	0.0.0.0/0	0.0.0.0/0	any	0:0	any	any	1	trust-lan	trust-lan
✎	10.0.238.71	laine-vxa	map1 (acti...	10000		ip	0.0.0.0/0	0.0.0.0/0	real-time	0:0	any	any	2 - real-time	trust-lan	trust-lan
✎	10.0.238.71	laine-vxa	map1 (acti...	10010		ip	0.0.0.0/0	0.0.0.0/0	interactive	0:0	any	any	3 - interactive	trust-lan	trust-lan
✎	10.0.238.69	laine-vxb	map1 (acti...	10010		ip	0.0.0.0/0	0.0.0.0/0	interactive	0:0	any	any	3	trust-lan	trust-lan
✎	10.0.238.71	laine-vxa	map1 (acti...	10030		ip	0.0.0.0/0	0.0.0.0/0	any	0:0	be	any	4	trust-lan	trust-lan
✎	10.0.238.71	laine-vxa	map1 (acti...	65535		ip	0.0.0.0/0	0.0.0.0/0	any	0:0	any	any	1	trust-lan	trust-lan
✎	10.0.238.20	laine2-vxa	map1 (acti...	65535		ip	any	any	any	0:0	any	any	1 - default	trust-lan	trust-lan
✎	10.0.238.20	laine2-vxa	map1 (acti...	10010		ip	0.0.0.0/0	0.0.0.0/0	interactive	0:0	any	any	3	trust-lan	trust-lan
✎	10.0.238.20	laine2-vxa	map1 (acti...	10020		ip	0.0.0.0/0	0.0.0.0/0	any	0:0	ef	any	2	trust-lan	trust-lan
✎	10.0.238.20	laine2-vxa	map1 (acti...	10030		ip	0.0.0.0/0	0.0.0.0/0	any	0:0	be	any	4	trust-lan	trust-lan
✎	10.0.238.71	laine-vxa	map1 (acti	10020		ip	0.0.0.0/0	0.0.0.0/0	any	0:0	ef	any	2	trust-lan	trust-lan

Showing 1 to 20 of 20 entries

The QoS Policy's SET actions determine two things:

- to what traffic class a shaped flow -- optimized or pass-through -- is assigned
- whether to trust incoming DSCP markings for LAN QoS and WAN QoS, or to remark them as they leave for the WAN

Priority

- You can create rules with any priority between 1 and 65534.
  - If you are using GMS templates to add route map entries, GMS will delete all entries from **1000 – 9999**, inclusive, before applying its policies.
  - You can create rules from **1 – 999**, which have higher priority than GMS template rules.
  - Similarly, you can create rules from **10000 – 65534** which have lower priority than GMS template rules.

- Adding a rule increments the last Priority by 10. This leaves room for you to insert a rule in between rules without having to renumber subsequent priorities. Likewise, you can just edit the number.

Source or Destination

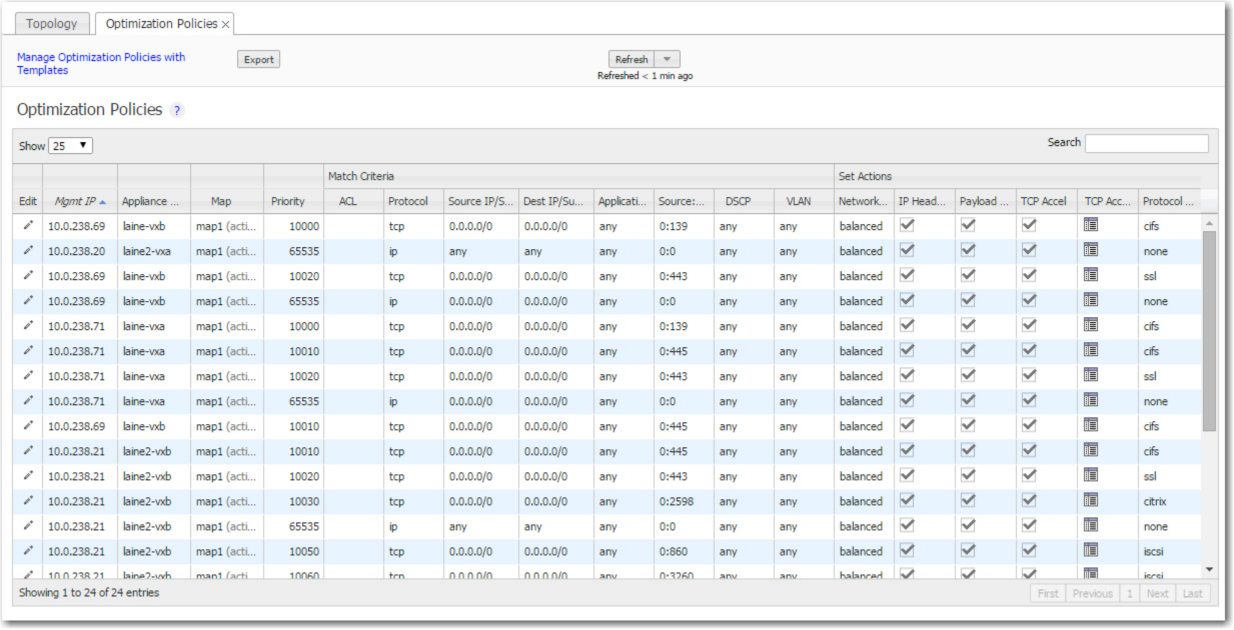
- An IP address can specify a subnet - for example: 10.10.10.0/24 (IPv4) or fe80::204:23ff:fed8:4ba2/64 (IPv6).
- To allow **any IP address**, use 0.0.0.0/0 (IPv4) or ::/0 (IPv6).
- Ports are available only for the protocols **tcp**, **udp**, and **tcp/udp**.
- To allow **any port**, use **0**.

Optimization Policies Tab

Configuration > Optimization Policies

The **Optimization Policies** report displays a polled, read-only view of the Optimization policy entries that exist on the appliance(s). This includes the appliance-based defaults, entries applied manually (via the WebUI or CLI), and entries that result from applying a GMS Optimization Policy template.

Use the **Templates** tab to create and manage Optimization policies.



					Match Criteria									Set Actions					
Edit	Mgmt IP ▲	Appliance ...	Map	Priority	ACL	Protocol	Source IP/S...	Dest IP/Su...	Applicati...	Source:...	DSCP	VLAN	Network...	IP Head...	Payload ...	TCP Accel	TCP Acc...	Protocol ...
✎	10.0.238.69	laine-vxb	map1 (acti...	10000		tcp	0.0.0.0/0	0.0.0.0/0	any	0:139	any	any	balanced	✓	✓	✓	▤	cifs
✎	10.0.238.20	laine2-vxa	map1 (acti...	65535		ip	any	any	any	0:0	any	any	balanced	✓	✓	✓	▤	none
✎	10.0.238.69	laine-vxb	map1 (acti...	10020		tcp	0.0.0.0/0	0.0.0.0/0	any	0:443	any	any	balanced	✓	✓	✓	▤	ssl
✎	10.0.238.69	laine-vxb	map1 (acti...	65535		ip	0.0.0.0/0	0.0.0.0/0	any	0:0	any	any	balanced	✓	✓	✓	▤	none
✎	10.0.238.71	laine-vxa	map1 (acti...	10000		tcp	0.0.0.0/0	0.0.0.0/0	any	0:139	any	any	balanced	✓	✓	✓	▤	cifs
✎	10.0.238.71	laine-vxa	map1 (acti...	10010		tcp	0.0.0.0/0	0.0.0.0/0	any	0:445	any	any	balanced	✓	✓	✓	▤	cifs
✎	10.0.238.71	laine-vxa	map1 (acti...	10020		tcp	0.0.0.0/0	0.0.0.0/0	any	0:443	any	any	balanced	✓	✓	✓	▤	ssl
✎	10.0.238.71	laine-vxa	map1 (acti...	65535		ip	0.0.0.0/0	0.0.0.0/0	any	0:0	any	any	balanced	✓	✓	✓	▤	none
✎	10.0.238.69	laine-vxb	map1 (acti...	10010		tcp	0.0.0.0/0	0.0.0.0/0	any	0:445	any	any	balanced	✓	✓	✓	▤	cifs
✎	10.0.238.21	laine2-vxb	map1 (acti...	10010		tcp	0.0.0.0/0	0.0.0.0/0	any	0:445	any	any	balanced	✓	✓	✓	▤	cifs
✎	10.0.238.21	laine2-vxb	map1 (acti...	10020		tcp	0.0.0.0/0	0.0.0.0/0	any	0:443	any	any	balanced	✓	✓	✓	▤	ssl
✎	10.0.238.21	laine2-vxb	map1 (acti...	10030		tcp	0.0.0.0/0	0.0.0.0/0	any	0:2598	any	any	balanced	✓	✓	✓	▤	citrix
✎	10.0.238.21	laine2-vxb	map1 (acti...	65535		ip	any	any	any	0:0	any	any	balanced	✓	✓	✓	▤	none
✎	10.0.238.21	laine2-vxb	map1 (acti...	10050		tcp	0.0.0.0/0	0.0.0.0/0	any	0:860	any	any	balanced	✓	✓	✓	▤	iscsi
✎	10.0.238.21	laine2-vxb	map1 (acti	10060		tcp	0.0.0.0/0	0.0.0.0/0	any	0:3260	any	any	balanced	✓	✓	✓	▤	iscsi

Showing 1 to 24 of 24 entries

Set Actions Definitions

- **Network Memory** addresses limited bandwidth. This technology uses advanced fingerprinting algorithms to examine all incoming and outgoing WAN traffic. Network Memory localizes information and transmits only modifications between locations.
    - **Maximize Reduction** optimizes for maximum data reduction at the potential cost of slightly lower throughput and/or some increase in latency. It is appropriate for bulk data transfers such as file transfers and FTP, where bandwidth savings are the primary concern.
    - **Minimize Latency** ensures that Network Memory processing adds no latency. This may come at the cost of lower data reduction. It is appropriate for extremely latency-sensitive interactive or transactional traffic. It's also appropriate when the primary objective is to to fully utilize the WAN pipe to increase the LAN-side throughput, as opposed to conserving WAN bandwidth.
    - **Balanced** is the default setting. It dynamically balances latency and data reduction objectives and is the best choice for most traffic types.
    - **Disabled** turns off Network Memory.
- **IP Header Compression** is the process of compressing excess protocol headers before transmitting them on a link and uncompressing them to their original state at the other end. It's possible to compress the protocol headers due to the redundancy in header fields of the same packet, as well as in consecutive packets of a packet stream.
- **Payload Compression** uses algorithms to identify relatively short byte sequences that are repeated frequently. These are then replaced with shorter segments of code to reduce the size of transmitted

data. Simple algorithms can find repeated bytes within a single packet; more sophisticated algorithms can find duplication across packets and even across flows.

- **TCP Acceleration** uses techniques such as selective acknowledgements, window scaling, and message segment size adjustment to mitigate poor performance on high-latency links.
- **Protocol Acceleration** provides explicit configuration for optimizing CIFS, SSL, SRDF, and Citrix protocols. In a network environment, it's possible that not every appliance has the same optimization configurations enabled. Therefore, the site that initiates the flow (the client) determines the state of the protocol-specific optimization.

Priority

- You can create rules with any priority between 1 and 65534.
    - If you are using GMS templates to add route map entries, GMS will delete all entries from **1000 – 9999**, inclusive, before applying its policies.
    - You can create rules from **1 – 999**, which have higher priority than GMS template rules.
    - Similarly, you can create rules from **10000 – 65534** which have lower priority than GMS template rules.
- Adding a rule increments the last Priority by 10. This leaves room for you to insert a rule in between rules without having to renumber subsequent priorities. Likewise, you can just edit the number.

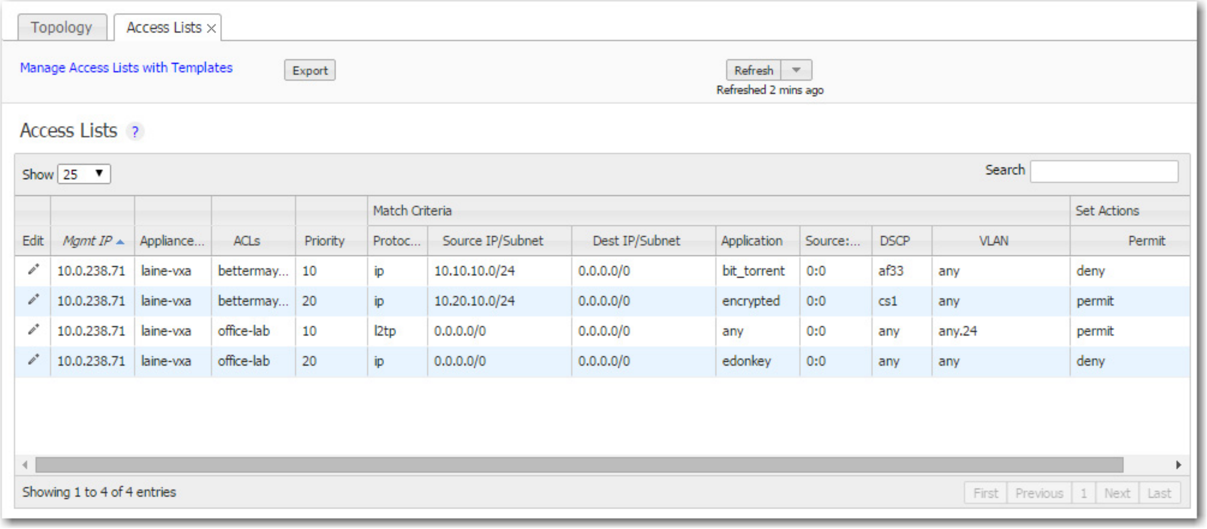
Source or Destination

- An IP address can specify a subnet - for example: 10.10.10.0/24 (IPv4) or fe80::204:23ff:fed8:4ba2/64 (IPv6).
- To allow **any IP address**, use 0.0.0.0/0 (IPv4) or ::/0 (IPv6).
- Ports are available only for the protocols **tcp**, **udp**, and **tcp/udp**.
- To allow **any port**, use **0**.

Access Lists Tab

Configuration > Access Lists

This tab lists the configured **Access Control List** (ACL) rules.



					Match Criteria							Set Actions
Edit	*Mgmt IP* ▲	Appliance...	ACLs	Priority	Protoc...	Source IP/Subnet	Dest IP/Subnet	Application	Source:...	DSCP	VLAN	Permit
✎	10.0.238.71	laine-vxa	bettermay...	10	ip	10.10.10.0/24	0.0.0.0/0	bit_torrent	0:0	af33	any	deny
✎	10.0.238.71	laine-vxa	bettermay...	20	ip	10.20.10.0/24	0.0.0.0/0	encrypted	0:0	cs1	any	permit
✎	10.0.238.71	laine-vxa	office-lab	10	l2tp	0.0.0.0/0	0.0.0.0/0	any	0:0	any	any.24	permit
✎	10.0.238.71	laine-vxa	office-lab	20	ip	0.0.0.0/0	0.0.0.0/0	edonkey	0:0	any	any	deny

Showing 1 to 4 of 4 entries

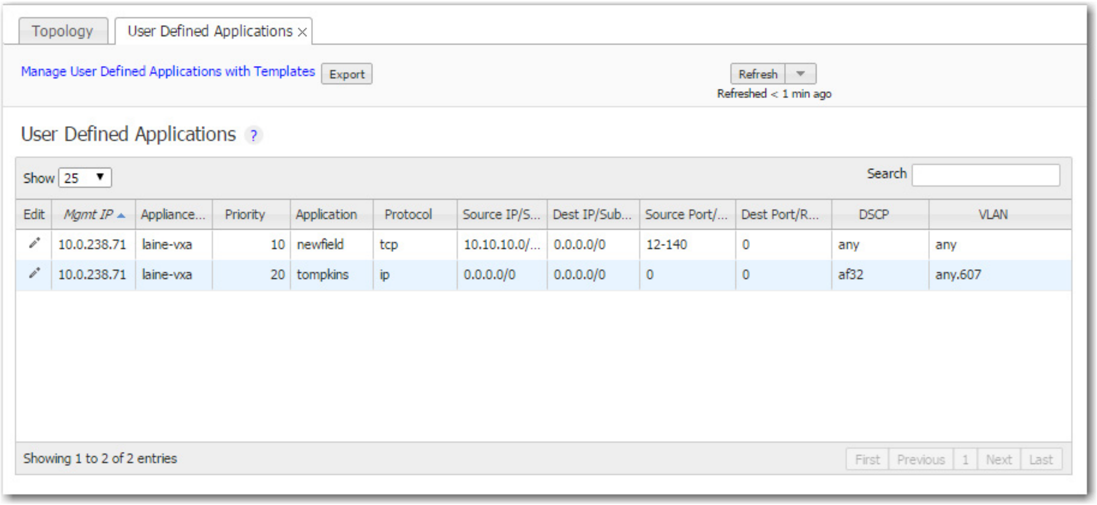
An **ACL** is a reusable MATCH criteria for filtering flows, and is associated with an action, **permit** or **deny**: An ACL can be a MATCH condition in more than one policy --- Route, QoS, or Optimization.

- An Access Control List (ACL) consists of one or more ordered access control rules.
- An ACL only becomes active when it's used in a policy.
- **Deny** prevents further processing of the flow by ***that ACL, specifically***. The appliance continues to the next entry in the policy.
- **Permit** allows the matching traffic flow to proceed on to the policy entry's associated SET action(s).

User Defined Applications Tab

Configuration > User Defined Applications

This tab lists **user-defined applications** (UDA).


Topology
User Defined Applications ×
Manage User Defined Applications with Templates
Export
Refresh
Refreshed < 1 min ago
User Defined Applications ?
Show 25 ▼
Search
First
Previous
1
Next
Last

Edit	Mgmt IP	Appliance...	Priority	Application	Protocol	Source IP/S...	Dest IP/Sub...	Source Port/...	Dest Port/R...	DSCP	VLAN
	10.0.238.71	laine-vxa	10	newfield	tcp	10.10.10.0/...	0.0.0.0/0	12-140	0	any	any
	10.0.238.71	laine-vxa	20	tompkins	ip	0.0.0.0/0	0.0.0.0/0	0	0	af32	any.607

Showing 1 to 2 of 2 entries

UDAs are specific to the appliance on which they're defined.

Where can you use them?

- Route Policy
- QoS Policy
- Optimization Policy
- Access Lists (ACL)
- Application Groups

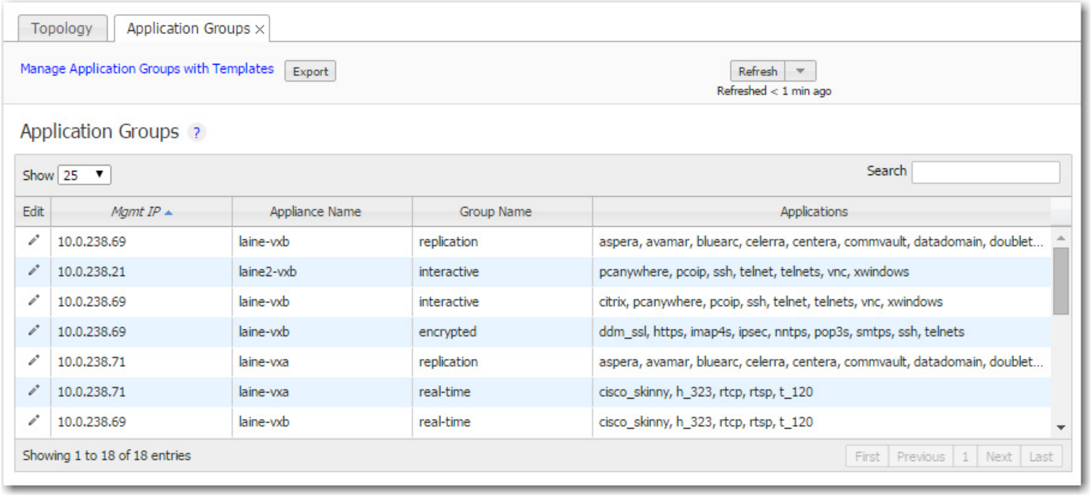
Behavior

- For reporting symmetry, you must define the same application(s) on peer appliances. Otherwise, the application may be a UDA on one appliance, and yet be categorized as an **unassigned application** on another, paired appliance.
- Each application consists of at least one rule.
- A warning displays if you reach the maximum number of rules, ports, or addresses allowed.
- If a UDA is in use, deleting it deletes **all** the dependent entries. A warning message appears before deletion.
- Multiple UDAs can have the same name. Whenever that name is referenced, the software sequentially matches against each UDA definition having that name. So, dependent entries are only deleted when you delete the **last** definition of that UDA.

Application Groups Tab

Configuration > Application Groups

Application groups associate applications into a common group that you can use as a MATCH criteria. The applications can be built-in, user-defined, or a combination of both.



Edit	Mgmt IP ▲	Appliance Name	Group Name	Applications
✎	10.0.238.69	laine-vxb	replication	aspera, avamar, bluearc, celerra, centera, commvault, datadomain, doublet...
✎	10.0.238.21	laine2-vxb	interactive	pcanywhere, pcoip, ssh, telnet, telnets, vnc, xwindows
✎	10.0.238.69	laine-vxb	interactive	citrix, pcanywhere, pcoip, ssh, telnet, telnets, vnc, xwindows
✎	10.0.238.69	laine-vxb	encrypted	ddm_ssl, https, imap4s, ipsec, nntps, pop3s, smtps, ssh, telnets
✎	10.0.238.71	laine-vxa	replication	aspera, avamar, bluearc, celerra, centera, commvault, datadomain, doublet...
✎	10.0.238.71	laine-vxa	real-time	cisco_skinny, h_323, rtcp, rtsp, t_120
✎	10.0.238.69	laine-vxb	real-time	cisco_skinny, h_323, rtcp, rtsp, t_120

Showing 1 to 18 of 18 entries

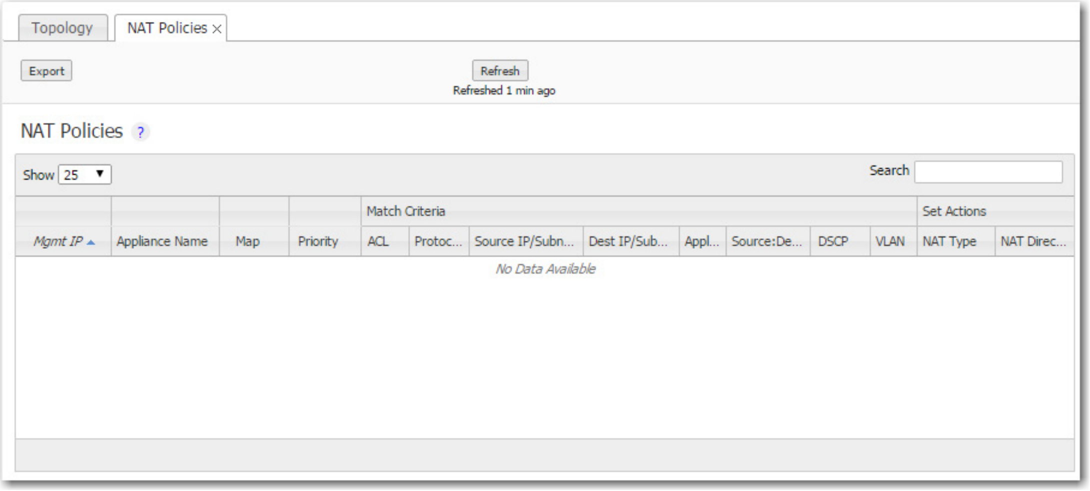
- The **Group Name** cannot be empty or have more than 64 characters.
- Group names are not case-sensitive.
- A group can be empty or contain up to 128 applications.
- An application group cannot contain an application group.
- For reporting symmetry, you must define the same application groups on peer appliances. Otherwise, the application group may be named on one appliance, and yet be categorized as an **unassigned application** on another, paired appliance.

NAT Policies Tab

Configuration > NAT Policies

The appliance automatically creates a source **NAT (Network Address Translation)** map when retrieving subnet information from the Silver Peak Cloud portal.

This ensures that traffic destined to SaaS (Software as a Service) servers has a return path to the appliance from which that traffic originated.



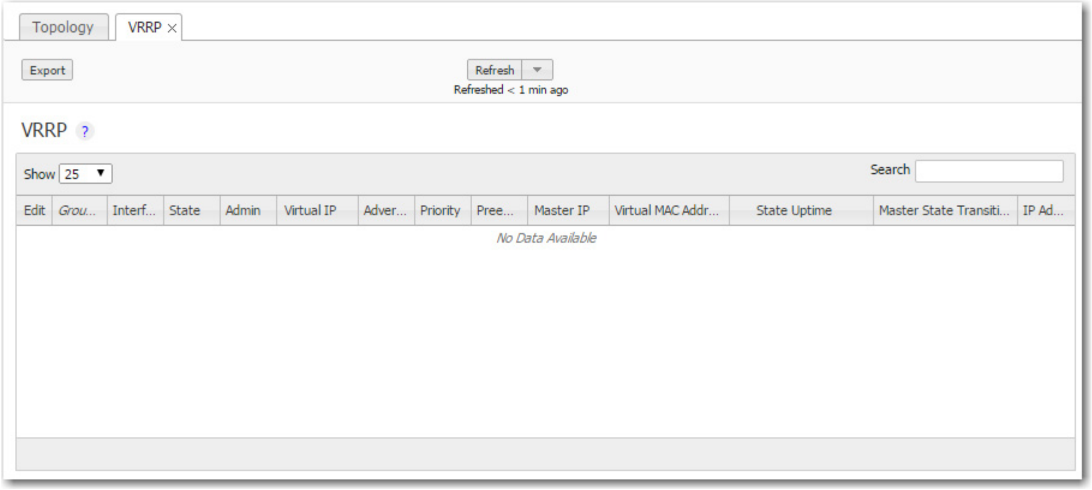
				Match Criteria								Set Actions	
Mgmt IP ▲	Appliance Name	Map	Priority	ACL	Protoc...	Source IP/Subn...	Dest IP/Sub...	Appl...	Source:De...	DSCP	VLAN	NAT Type	NAT Direc...

No Data Available

VRRP Tab

Configuration > VRRP

This tab summarizes the configuration and state for appliances deployed with **Virtual Router Redundancy Protocol (VRRP)**.



Edit	Grou...	Interf...	State	Admin	Virtual IP	Adver...	Priority	Pree...	Master IP	Virtual MAC Addr...	State Uptime	Master State Transiti...	IP Ad...
No Data Available													

In an out-of-path deployment, one method for redirecting traffic to the Silver Peak appliance is to configure VRRP on a common virtual interface. The possible scenarios are:

- When no spare router port is available, a single appliance uses VRRP to peer with a router (or Layer 3 switch). This is appropriate for an out-of-path deployment where no redundancy is needed.
- A pair of active, redundant appliances use VRRP to share a common, virtual IP address at their site. This deployment assigns one appliance a higher priority than the other, thereby making it the Master appliance, and the other, the Backup.

DEFINITIONS (alphabetically)

- **Admin** = The options are up (enable) and **down** (disable).
- **Advertisement Timer** = default is **1 second**.
- **Group ID** is a value assigned to the two peers. Depending on the deployment, the group can consist of an appliance and a router (or L3 switch), or two appliances. The valid range is **1 - 255**.
- **Interface** refers to the interface that VRRP is using for peering.
- **IP Address Owner** = A Silver Peak appliance cannot use one of its own IP addresses as the VRRP IP, so this will always be **No**.
- **Master IP** = Current VRRP Master's Interface or local IP address.
- **Master State Transitions** = Number of times the VRRP instance went from Master to Backup and vice versa. A high number of transitions indicates a problematic VRRP configuration or environment. If this is the case, check the configuration of all local appliances and routers, and review the log files.
- **Preemption**. Leave this selected/enabled so that after a failure, the appliance with the highest priority comes back online and again assumes primary responsibility.
- **Priority**. The greater the number, the higher the priority. The appliance with the higher priority is the VRRP Master.

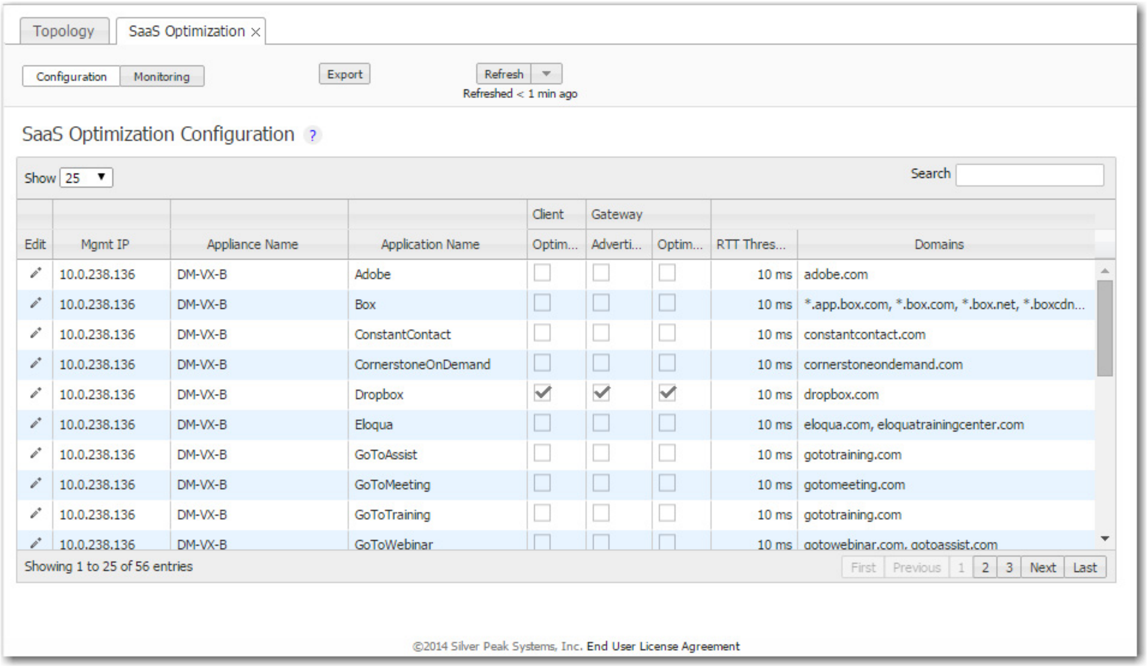
- **State Uptime** = Time elapsed since the VRRP instance entered the state it's in.
- **State** = There are three options for the VRRP instance:
  - **Backup** = Instance is in VRRP backup state.
  - **Init** = Instance is initializing, it's disabled, or the interface is down.
  - **Master** = Instance is the current VRRP master.
- **Virtual IP**. The IP address of the VRRP instance. VRRP instances may run between two or more appliances, or an appliance and a router.
- **Virtual MAC address** = MAC Address that the VRRP instance is using. On an NX Appliance, this is in 00-00-5E-00-01-{VRID} format. On virtual appliances, the VRRP instance uses the interface's assigned MAC Address (for example, the MAC address that the hypervisor assigned to **wan0**).

SaaS Optimization Tab

Configuration > SaaS Optimization

Configuration Tab

Use this tab to select the SaaS (Software as a Service) applications/services you want to optimize.

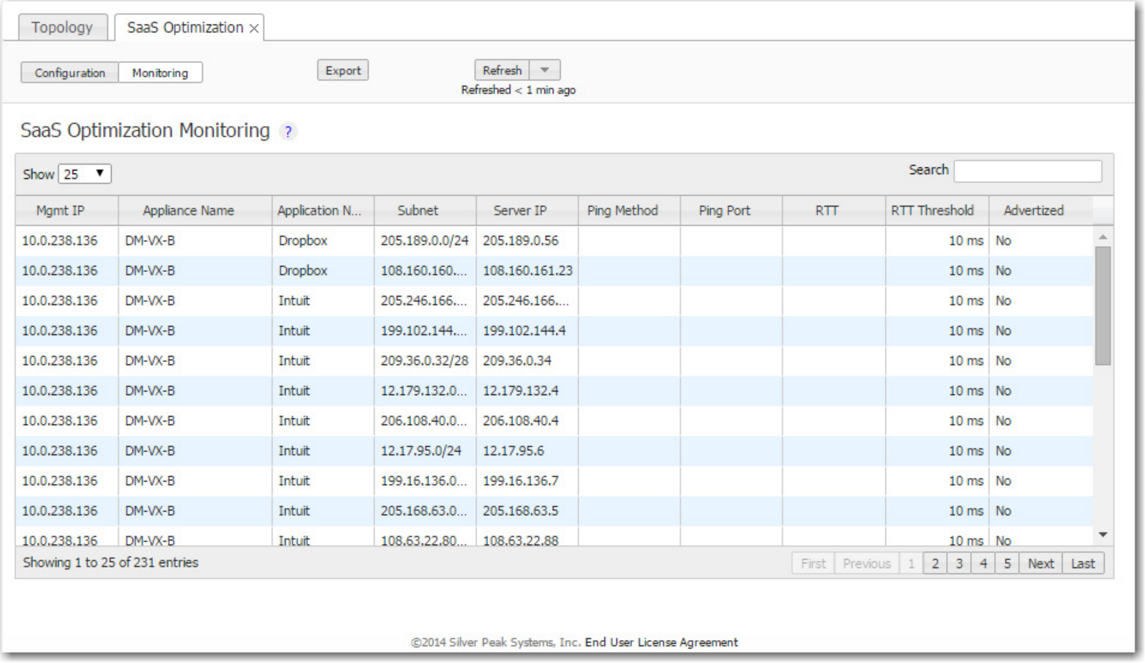


				Client	Gateway			
Edit	Mgmt IP	Appliance Name	Application Name	Optim...	Adverti...	Optim...	RTT Thres...	Domains
	10.0.238.136	DM-VX-B	Adobe	□	□	□	10 ms	adobe.com
	10.0.238.136	DM-VX-B	Box	□	□	□	10 ms	*.app.box.com, *.box.com, *.box.net, *.boxcdn...
	10.0.238.136	DM-VX-B	ConstantContact	□	□	□	10 ms	constantcontact.com
	10.0.238.136	DM-VX-B	CornerstoneOnDemand	□	□	□	10 ms	cornerstoneondemand.com
	10.0.238.136	DM-VX-B	Dropbox	☑	☑	☑	10 ms	dropbox.com
	10.0.238.136	DM-VX-B	Eloqua	□	□	□	10 ms	eloqua.com, eloquatrainingcenter.com
	10.0.238.136	DM-VX-B	GoToAssist	□	□	□	10 ms	gototraining.com
	10.0.238.136	DM-VX-B	GoToMeeting	□	□	□	10 ms	gotomeeting.com
	10.0.238.136	DM-VX-B	GoToTraining	□	□	□	10 ms	gototraining.com
	10.0.238.136	DM-VX-B	GoToWebinar	□	□	□	10 ms	gotowebinar.com, gotoassist.com

Showing 1 to 25 of 56 entries

- **Enable SaaS optimization** enables the appliance to determine what SaaS applications/services it can optimize. It does this by contacting Silver Peak's portal and downloading SaaS IP address and subnet information.
- Initially, you may want to set a higher **RTT Threshold** value so that you can see a broader scope of reachable data centers/servers for any given SaaS application/service.
- If the Monitoring page shows no results at 50 ms, you may want to reposition your SaaS gateway closer to the service.

Monitoring Tab



SaaS Optimization Monitoring ?

Show 25 ▼ Search

Mgmt IP	Appliance Name	Application N...	Subnet	Server IP	Ping Method	Ping Port	RTT	RTT Threshold	Advertized
10.0.238.136	DM-VX-B	Dropbox	205.189.0.0/24	205.189.0.56				10 ms	No
10.0.238.136	DM-VX-B	Dropbox	108.160.160....	108.160.161.23				10 ms	No
10.0.238.136	DM-VX-B	Intuit	205.246.166....	205.246.166....				10 ms	No
10.0.238.136	DM-VX-B	Intuit	199.102.144....	199.102.144.4				10 ms	No
10.0.238.136	DM-VX-B	Intuit	209.36.0.32/28	209.36.0.34				10 ms	No
10.0.238.136	DM-VX-B	Intuit	12.179.132.0...	12.179.132.4				10 ms	No
10.0.238.136	DM-VX-B	Intuit	206.108.40.0...	206.108.40.4				10 ms	No
10.0.238.136	DM-VX-B	Intuit	12.17.95.0/24	12.17.95.6				10 ms	No
10.0.238.136	DM-VX-B	Intuit	199.16.136.0...	199.16.136.7				10 ms	No
10.0.238.136	DM-VX-B	Intuit	205.168.63.0...	205.168.63.5				10 ms	No
10.0.238.136	DM-VX-B	Intuit	108.63.22.80...	108.63.22.88				10 ms	No

Showing 1 to 25 of 231 entries

©2014 Silver Peak Systems, Inc. End User License Agreement

CHAPTER 4

Appliance Administration

This chapter describes the reports that display appliance administration parameters.

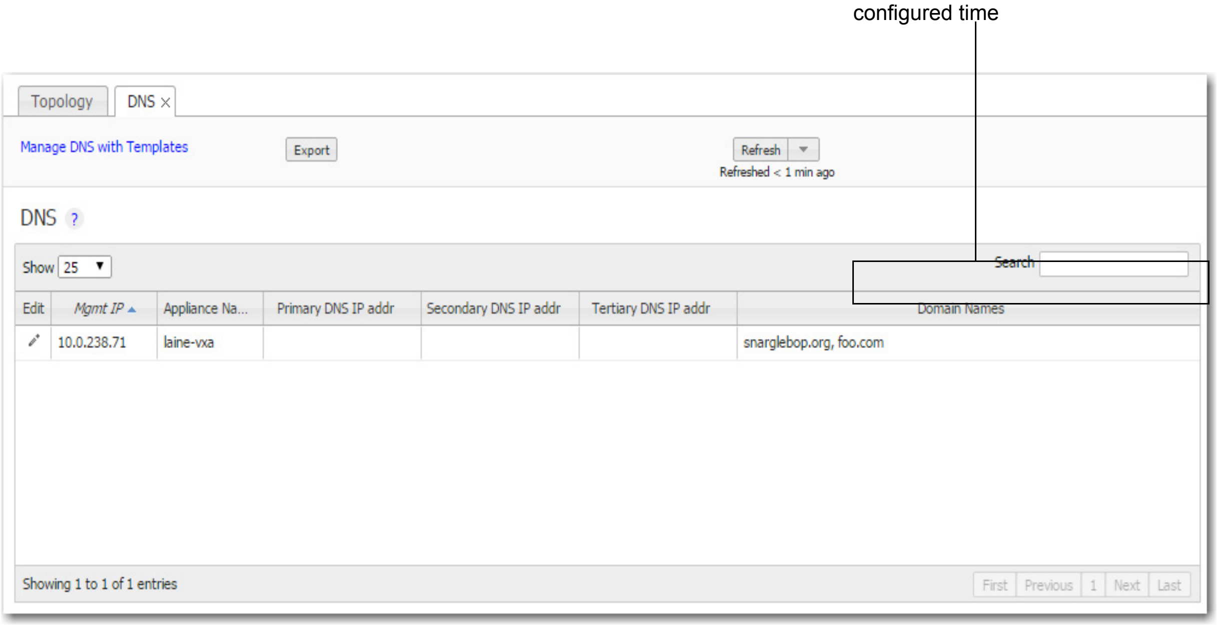
In This Chapter

Date/Time Tab

Administration > Date/Time

This tab highlights significant time discrepancies among the devices recording statistics.

Relative to the appliance's configured time



Edit	Mgmt IP ▲	Appliance Na...	Primary DNS IP addr	Secondary DNS IP addr	Tertiary DNS IP addr	Domain Names
✎	10.0.238.71	laine-vxa				snarglebop.org, foo.com

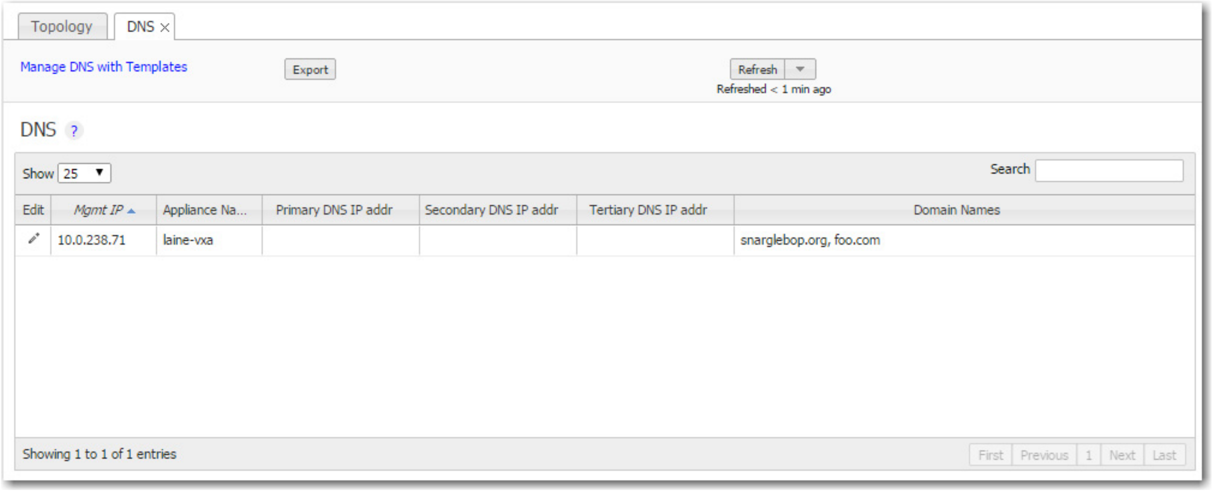
If the **date and time** of an appliance, the GMS server, and your browser aren't all synchronized, then charts (and stats) will inevitably have different timestamps for the same data, depending on which device you use to view the reports.

Recommendation: For consistent results, configure the appliance, the GMS server, and your PC to use an NTP (Network Time Protocol) server.

Domain Name Servers (DNS) Tab

Administration > DNS

This tab lists the Domain Name Servers that the appliances reference.



Edit	Mgmt IP ▲	Appliance Na...	Primary DNS IP addr	Secondary DNS IP addr	Tertiary DNS IP addr	Domain Names
✎	10.0.238.71	laine-vxa				snarglebop.org, foo.com

Showing 1 to 1 of 1 entries

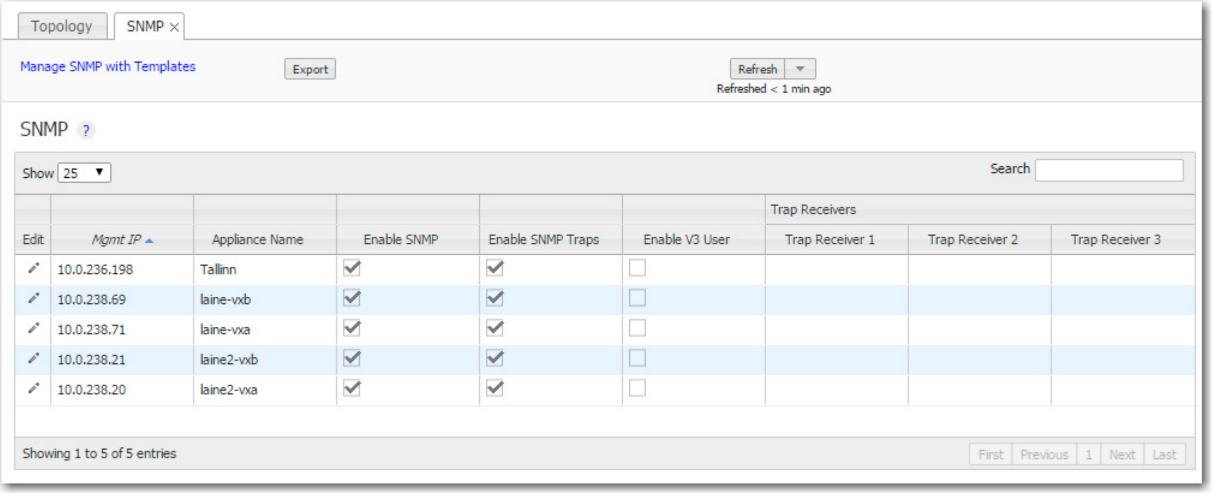
A **Domain Name Server** (DNS) uses a table to map domain names to IP addresses. So, you can reference locations by a domain name, such as ***mycompany.com***, instead of using the IP address.

Each appliance can support up to three name servers.

SNMP Tab

Administration > SNMP

This tab summarizes what SNMP capabilities are enabled and which hosts can receive SNMP traps.



						Trap Receivers		
Edit	Mgmt IP ▲	Appliance Name	Enable SNMP	Enable SNMP Traps	Enable V3 User	Trap Receiver 1	Trap Receiver 2	Trap Receiver 3
✎	10.0.236.198	Tallinn	☑	☑	□			
✎	10.0.238.69	laine-vxb	☑	☑	□			
✎	10.0.238.71	laine-vxa	☑	☑	□			
✎	10.0.238.21	laine2-vxb	☑	☑	□			
✎	10.0.238.20	laine2-vxa	☑	☑	□			

Showing 1 to 5 of 5 entries

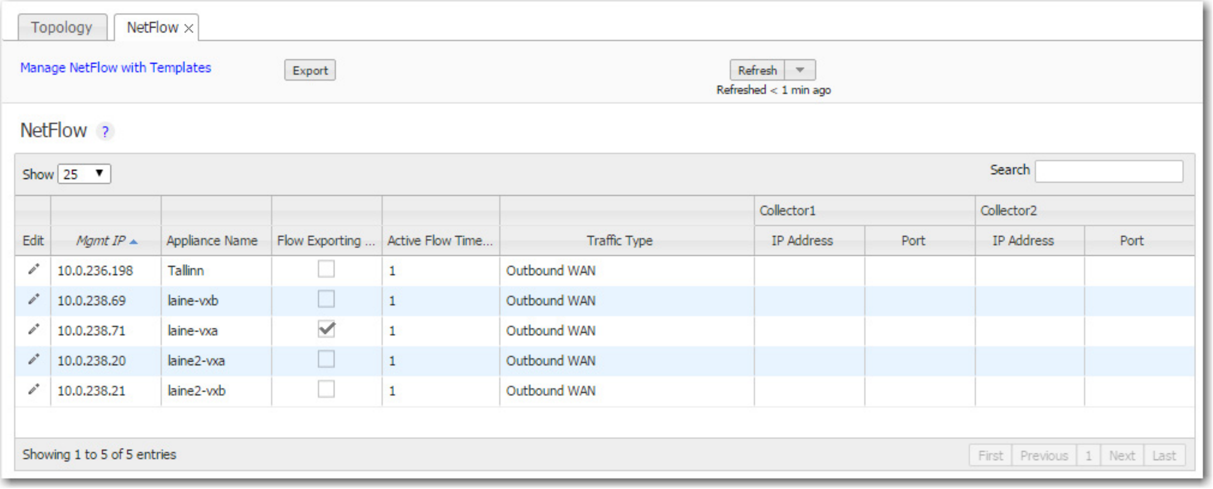
- The Silver Peak appliance supports the Management Information Base (MIB) II, as described in RFC 1213, for cold start traps and warm start traps, as well as Silver Peak proprietary MIBs.
- The appliance issues an SNMP trap during reset--that is, when loading a new image, recovering from a crash, or rebooting.
- The appliance sends a trap every time an alarm is raised or cleared. Traps contain additional information about the alarm, including severity, sequence number, a text-based description of the alarm, and the time the alarm was created.

Term	Definition
Enable SNMP	Allows the SNMP applicaton to poll this Silver Peak appliance. (For SNMP v1 and SNMP v2c)
Enable SNMP Traps	Allows the SNMP agent (in the appliance) to send traps to the receiver(s). (For SNMP v1 and SNMP v2c)
Enable V3 User	For additional security when the SNMP application polls the appliance, you can use SNMP v3, instead of using v1 or v2c. This provides a way to authenticate without using clear text.
Trap Receiver	IP address of a host configured to receive SNMP traps.

NetFlow Tab

Administration > NetFlow

This tab summarizes how the appliances are configured to export statistical data to NetFlow collectors.



						Collector1		Collector2	
Edit	*Mgmt IP* ▲	Appliance Name	Flow Exporting ...	Active Flow Time...	Traffic Type	IP Address	Port	IP Address	Port
✎	10.0.236.198	Tallinn	□	1	Outbound WAN				
✎	10.0.238.69	laine-vxb	□	1	Outbound WAN				
✎	10.0.238.71	laine-vxa	☑	1	Outbound WAN				
✎	10.0.238.20	laine2-vxa	□	1	Outbound WAN				
✎	10.0.238.21	laine2-vxb	□	1	Outbound WAN				

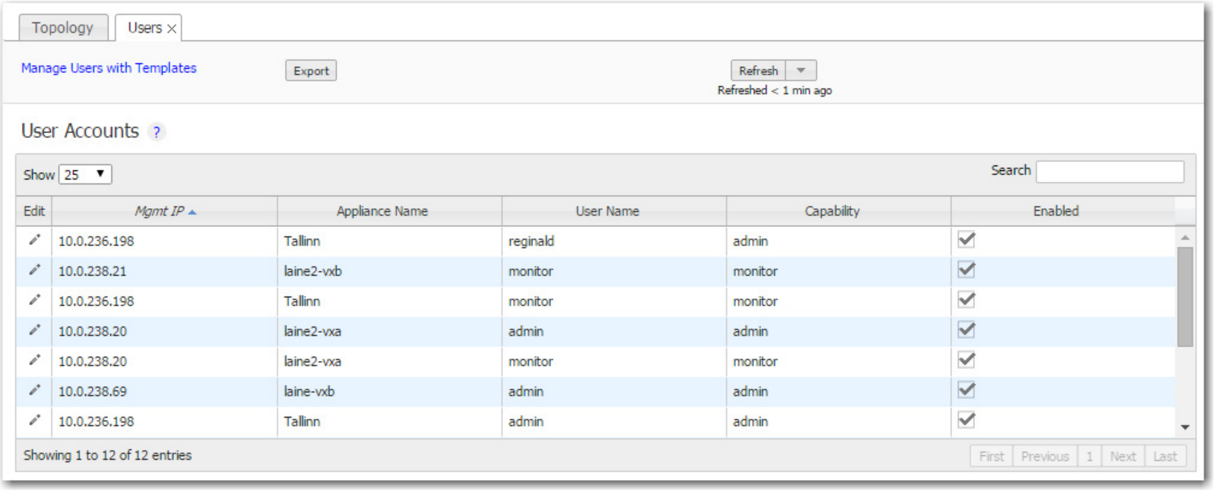
Showing 1 to 5 of 5 entries

- The appliance exports flows against two virtual interfaces -- **sp_lan** and **sp_wan** -- that accumulate the total of LAN-side and WAN-side traffic, regardless of physical interface.
- These interfaces appear in SNMP and are therefore "discoverable" by NetFlow collectors.
- **Flow Exporting Enabled** allows the appliance to export the data to collectors (and makes the configuration fields accessible).
- The **Collector's IP Address** is the IP address of the device to which you're exporting the NetFlow statistics. The default Collector Port is **2055**.
- In **Traffic Type**, you can select as many of the traffic types as you wish. The default is **Outbound WAN**.

Appliance Users Tab

Administration > Users

This tab provides data about the **user accounts** on each appliance.



Edit	Mgmt IP	Appliance Name	User Name	Capability	Enabled
✎	10.0.236.198	Tallinn	reginald	admin	☑
✎	10.0.238.21	laine2-vxb	monitor	monitor	☑
✎	10.0.236.198	Tallinn	monitor	monitor	☑
✎	10.0.238.20	laine2-vxa	admin	admin	☑
✎	10.0.238.20	laine2-vxa	monitor	monitor	☑
✎	10.0.238.69	laine-vxb	admin	admin	☑
✎	10.0.236.198	Tallinn	admin	admin	☑

Showing 1 to 12 of 12 entries

- The Silver Peak appliance's **built-in user database** supports user names, groups, and passwords.
- Each appliance has two default users, **admin** and **monitor**, who cannot be deleted.
- Each **User Name** belongs to one of two user groups -- **admin** or **monitor**.
  - The **monitor** group supports reading and monitoring of all data, in addition to performing all actions. This is equivalent to the Command Line Interface's (CLI) enable mode privileges.
  - The **admin** group supports full privileges, along with permission to add, modify, and delete. This is equivalent to the CLI's ***configuration*** mode privileges.
- Named user accounts can be added via Appliance Manager or the Command Line Interface (CLI).
- The table lists all users known to the appliances, whether or not their accounts are enabled.

Auth/RADIUS/TACACS+ Tab

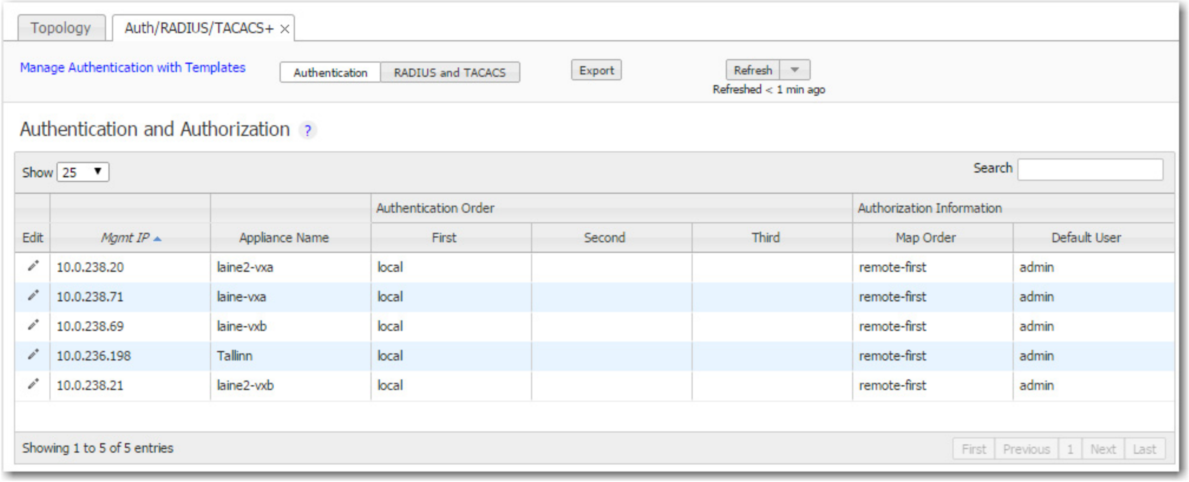
Administration > Auth/RADIUS/TACACS+

This tab displays the configured settings for authentication and authorization.

If the appliance relies on either a RADIUS or TACACS+ server for those services, then those settings are also reported.

All settings are initially applied via the **Auth/RADIUS/TACACS+** configuration **template**.

Authentication and Authorization

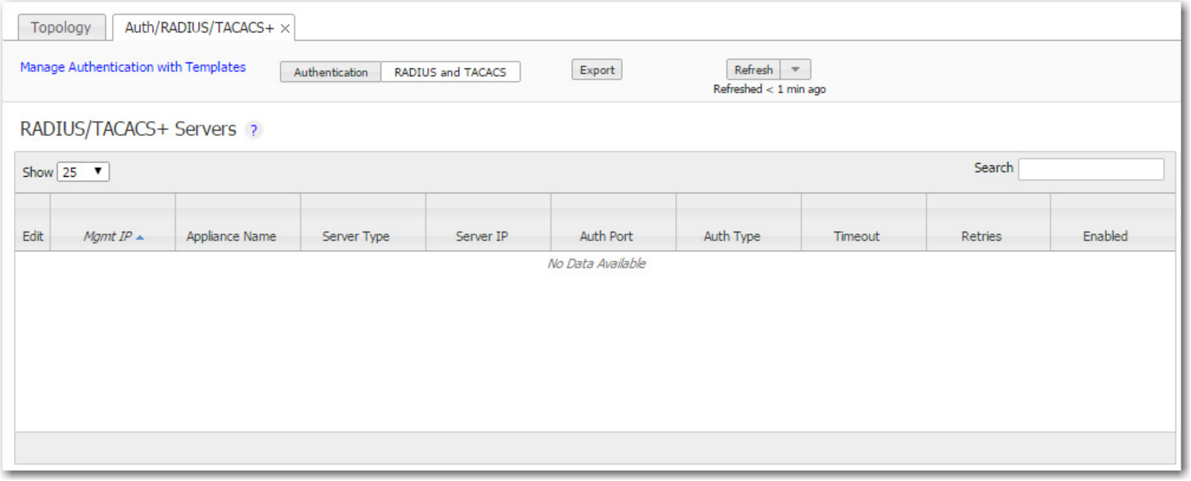


			Authentication Order			Authorization Information	
Edit	*Mgmt IP* ▲	Appliance Name	First	Second	Third	Map Order	Default User
✎	10.0.238.20	laine2-vxa	local			remote-first	admin
✎	10.0.238.71	laine-vxa	local			remote-first	admin
✎	10.0.238.69	laine-vxb	local			remote-first	admin
✎	10.0.236.198	Tallinn	local			remote-first	admin
✎	10.0.238.21	laine2-vxb	local			remote-first	admin

Showing 1 to 5 of 5 entries

- **Authentication** is the process of validating that the end user, or a device, is who they claim to be.
- **Authorization** is the action of determining what a user is allowed to do. Generally, authentication precedes authorization.
- When it's possible to validate against more than one database (local, RADIUS server, TACACS+ server), **Authentication Order** specifies which method to try in what sequence.
- **Map order**. The default—and recommended—value is **remote-first**.
- **Default user**. The default—and recommended—value is **admin**.

RADIUS and TACACS+



RADIUS/TACACS+ Servers ?

Edit	Mgmt IP ▲	Appliance Name	Server Type	Server IP	Auth Port	Auth Type	Timeout	Retries	Enabled

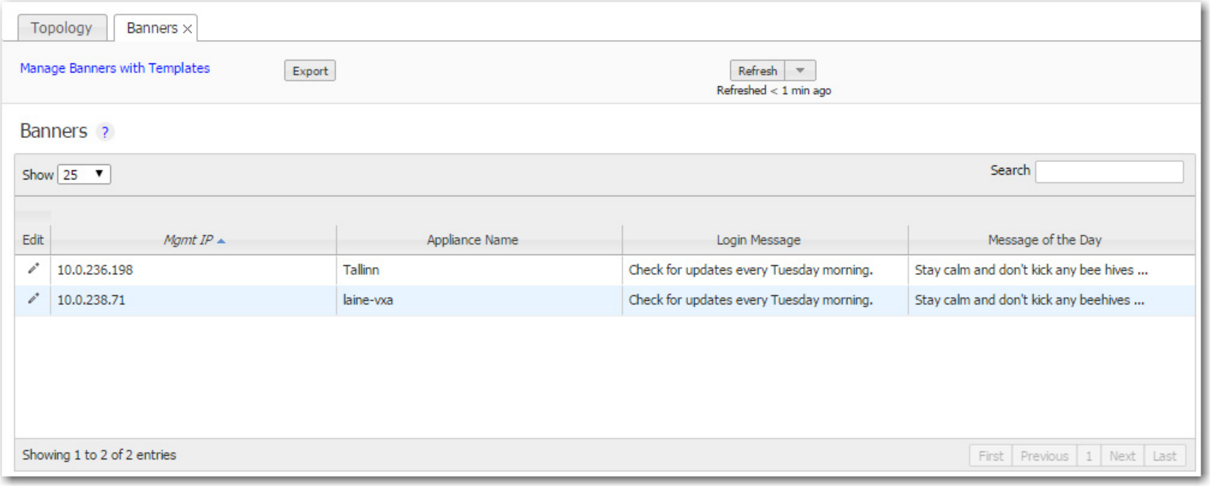
No Data Available

- **Server Type**. RADIUS or TACACS+
- **Auth Port**. For RADIUS, the default value is **1812**. For TACACS+, the default value is **49**.
- **Auth Type**. [TACACS+] The options are **pap** or **ascii**.
- **Timeout**. If a logged-in user is inactive for an interval that exceeds the inactivity time-out, the appliance logs them out and returns them to the login page. You can change that value, as well as the maximum number of sessions, in the **Session Management template**.
- **Retries**. The number of retries allowed before lockout.
- **Enabled**. Whether or not the server is enabled.

Banners Tab

Administration > Banners

This tab lists the banner messages on each appliance.



Edit	Mgmt IP ▲	Appliance Name	Login Message	Message of the Day
✎	10.0.236.198	Tallinn	Check for updates every Tuesday morning.	Stay calm and don't kick any bee hives ...
✎	10.0.238.71	laine-vxa	Check for updates every Tuesday morning.	Stay calm and don't kick any beehives ...

Showing 1 to 2 of 2 entries

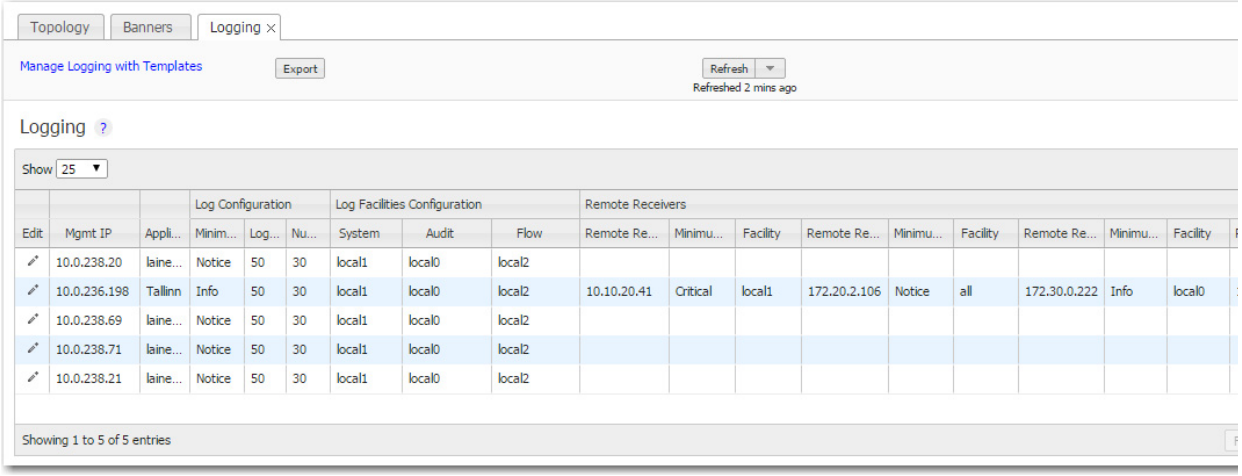
- The **Login Message** appears before the login prompt.
- The **Message of the Day** appears after a successful login.

Logging Tab

Administration > Logging

This tab summarizes the configured logging parameters:

- **Log Configuration** refers to local logging.
- **Log Facilities Configuration** refers to remote logging.



Logging ?

Show 25 ▼

			Log Configuration			Log Facilities Configuration			Remote Receivers								
Edit	Mgmt IP	Appli...	Minim...	Log...	Nu...	System	Audit	Flow	Remote Re...	Minimu...	Facility	Remote Re...	Minimu...	Facility	Remote Re...	Minimu...	Facility
✎	10.0.238.20	laine...	Notice	50	30	local1	local0	local2									
✎	10.0.236.198	Tallinn	Info	50	30	local1	local0	local2	10.10.20.41	Critical	local1	172.20.2.106	Notice	all	172.30.0.222	Info	local0
✎	10.0.238.69	laine...	Notice	50	30	local1	local0	local2									
✎	10.0.238.71	laine...	Notice	50	30	local1	local0	local2									
✎	10.0.238.21	laine...	Notice	50	30	local1	local0	local2									

Showing 1 to 5 of 5 entries

Minimum Severity Levels

In decreasing order of severity, the levels are as follows:

EMERGENCY The system is unusable.

ALERT Includes all alarms the appliance generates: **CRITICAL**, **MAJOR**, **MINOR**, and **WARNING**

CRITICAL A critical event

ERROR An error. This is a non-urgent failure.

WARNING A warning condition. Indicates an error will occur if action is not taken.

NOTICE A normal, but significant, condition. No immediate action required.

INFORMATIONAL Informational. Used by Silver Peak for debugging.

DEBUG Used by Silver Peak for debugging

NONE If you select **NONE**, then no events are logged.

- The **bolded** part of the name is what displays in Silver Peak's logs.
- These are purely related to event logging levels, **not** alarm severities, even though some naming conventions overlap. Events and alarms have different sources. Alarms, once they clear, list as the **ALERT** level in the **Event Log**.

Remote Logging

- You can configure the appliance to forward all events, at and above a specified severity, to a remote syslog server.
- A syslog server is independently configured for the minimum severity level that it will accept. Without reconfiguring, it may not accept as low a severity level as you are forwarding to it.
- Each message/event type (**System** / **Audit** / **Flow**) is assigned to a syslog facility level (**local0** to **local7**).

CHAPTER 5

Alarms & Threshold Crossing Alerts

Monitoring > Alarms
Monitoring > Threshold Crossing Alerts

This chapter describes alarm categories and definitions. It also describes how to view and handle alarm notifications.

Additionally, it describes threshold crossing alerts, which are pre-emptive, user-configurable thresholds that declare a Major alarm when crossed.

In This Chapter

Understanding Alarms

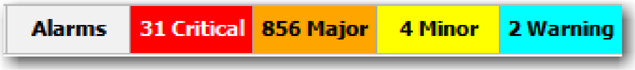
This section defines the four alarm severity categories and lists all Silver Peak appliance alarms.

The **Alarms - Current Alarms** page lists alarm conditions on the appliance. Each entry represents one current condition that may require human intervention. Because alarms are *conditions*, they may come and go without management involvement.

Whereas merely acknowledging most alarms does **not** clear them, some alarm conditions are set up to be self-clearing when you acknowledge them. For example, if you remove a hard disk drive, it generates an alarm; once you’ve replaced it and it has finished rebuilding itself, the alarm clears.

Categories of Alarms

The Appliance Manager categorizes alarms at four preconfigured severity levels: **Critical**, **Major**, **Minor**, and **Warning**.



- **Critical** and **Major** alarms are both service-affecting. **Critical** alarms require immediate attention, and reflect conditions that affect an appliance or the loss of a broad category of service.
- **Major** alarms, while also service-affecting, are less severe than **Critical** alarms. They reflect conditions which should be addressed in the next 24 hours. An example would be an unexpected traffic class error.
- **Minor** alarms are not service-affecting, and you can address them at your convenience. An example of a minor alarm would be a user not having changed their account’s default password, or a degraded disk.
- **Warnings** are also not service-affecting, and warn you of conditions that may become problems over time. For example, a software version mismatch.

Types of Alarms

The appliance can raise alarms based on issues with tunnels, software, equipment, and Threshold Crossing Alerts (TCAs). The latter are visible on the appliance but managed by the GMS (Global Management System).

Although Appliance Manager doesn't display **Alarm Type ID (Hex)** codes, the data is available for applications that can do their own filtering, such as SNMP.

Table 5-1 Silver Peak Appliance Alarms

Subsystem	Alarm Type ID (Hex)	Alarm Severity	Alarm Text
Tunnel	00010003	CRITICAL	Tunnel keepalive version mismatch **RESOLUTION:** Tunnel peers are running incompatible software versions. • Normal during a software upgrade. Run the same or compatible software releases among the tunnel peers.
	00010001	CRITICAL	Tunnel state is Down **RESOLUTION:** Cannot reach tunnel peer. • Check tunnel configuration [Admin state, Source IP/Dest IP, IPsec] • Check network connectivity.
	00010009	CRITICAL	An unexpected GRE packet was detected from tunnel peer. **RESOLUTION:** Check for tunnel encapsulation mismatch.
	00010007	MAJOR	Duplicate license detected in peer (only applies to virtual appliance) **RESOLUTION:** Install unique license on all virtual appliances. To check and/or change license: • In GMS: Initial Configuration page at **Configuration > System (Single Appliance)** • In WebUI: **Configuration - System** page
	00010000	MAJOR	Tunnel remote ID is misconfigured **RESOLUTION:** System ID is not unique. • Virtual Appliance: Was the same license key used? • Physical Appliance: Change System ID in the rare case of a duplicate ID (CLI command: system id < >)
	0001000a	MAJOR	Software version mismatch between peers results in reduced functionality. **RESOLUTION:** Upgrade all connected appliances for full optimization.
	00010005	MINOR	Tunnel software version mismatch **RESOLUTION:** Tunnel are not running the same release of software. They will function, but with reduced functionality. • Normal during an upgrade. • Run the same software version to eliminate the alarm and fully optimize.

Table 5-1 Silver Peak Appliance Alarms (Continued)

Subsystem	Alarm Type ID (Hex)	Alarm Severity	Alarm Text
Software	00040003	CRITICAL	The licensing for this virtual appliance has expired. [For VX series only][a] **RESOLUTION:** Enter a new license.
	00040004	CRITICAL	There is no license installed on this virtual appliance. [For VX series only][a] **RESOLUTION:** Enter a valid license.
	0004000c	CRITICAL	Invalid virtual appliance license. **RESOLUTION:** Enter a new license key on the <System Page> to proceed.
	0004000a	MAJOR	Virtual appliance license expires on mm/dd/yyy. [15-day warning] **RESOLUTION:** Enter a new license key on the <System Page> to avoid loss of optimization or potential traffic disruption.
	00040005	MAJOR	A disk self-test has been run on the appliance. **RESOLUTION:** Reboot the appliance. Traffic will not be optimized until this is performed.
	00040002	MAJOR	Significant change in time of day has occurred, and might compromise statistics. Please contact TAC. **RESOLUTION:** Appliance statistics could be missing for a substantial period of time. Contact Customer Service.
	00040001	MAJOR	System is low on resources **RESOLUTION:** Contact Customer Service.
	0004000d	MAJOR	Dual wan-next-hop topology is no longer supported. **RESOLUTION:** Create an additional bridge and use previous second WAN next-hop as its WAN next-hop. NOTE: Second Silver Peak requires another IP address that is in the same network as the first bridge.
	00040010	MAJOR	Major inconsistency among tunnel traffic class settings found during upgrade. **RESOLUTION:** New QoS traffic class/Queue configuration has changed from a tunnel-based QoS system to one based on the system/WAN interface. Automatic mapping of existing tunnel traffic class configuration to new QoS Shaper traffic has failed. Check QoS Shaper configuration and adjust Traffic Class settings as necessary.
	00040011	MAJOR	Tunnel IP header disable setting was discarded during upgrade. **RESOLUTION:** IP Header configuration has moved from tunnel context to the Optimization Policy. Use Optimization Policy to disable IP Header compression.
	00040019	MAJOR	Application deleted on portal **RESOLUTION:** None. Application is not supported.

Table 5-1 Silver Peak Appliance Alarms (Continued)

Subsystem	**Alarm Type ID (Hex)**	**Alarm Severity**	**Alarm Text**
Software (cont.)	0004000b	WARNING	Virtual appliance license expires on mm/dd/yyy. [45-day warning] **RESOLUTION:** Enter a new license key on the <System Page> to avoid loss of optimization or potential traffic disruption.
	00040007	WARNING	The SSL certificate is not yet valid. **RESOLUTION:** The SSL certificate has a future start date. It will correct itself when the future date becomes current. Otherwise, install a certificate that is current.
	00040008	WARNING	The SSL certificate has expired. **RESOLUTION:** Reinstall a valid SSL certificate that is current.
	00040009	WARNING	The NTP server is unreachable. **RESOLUTION:** Check the appliance's NTP server IP and version configuration: • Can the appliance reach the NTP server? • Is UDP port 123 open between the appliance's mgmt0 IP and the NTP server?
	00040006	WARNING	The SSL private key is invalid. **RESOLUTION:** The key is not an RSA standard key that meets the minimum requirement of 1024 bits. Regenerate a key that meets this minimum requirement.
	0004000e	WARNING	Setting default system next-hop to VLAN next-hop no longer necessary. **RESOLUTION:** No action required. Current system is capable of using multiple WAN next-hops. It routes tunnel traffic to tunnel's source IP interface's WAN next-hop.
	0004000f	WARNING	Minor inconsistency among tunnel traffic class settings found during upgrade. **RESOLUTION:** New QoS traffic class/Queue configuration has changed from a tunnel-based QoS system to one based on the system/WAN interface. Automatic mapping of existing tunnel traffic class configuration to new QoS Shaper traffic has failed. Check QoS Shaper configuration and adjust Traffic Class settings as necessary.
	00040012	WARNING	A very large range has been configured for a local subnet. **RESOLUTION:** Subnet sharing/advertisement module has detected a network mask of less than 8 bits. Verify your configured subnets in the **Configuration > Subnets** page.
	00040017	WARNING	Silver Peak portal is unreachable. **RESOLUTION:** Check your firewall settings.
	00040018	WARNING	Silver Peak portal (web socket) is unreachable. **RESOLUTION:** Check your firewall settings.
Equipment	00030003	CRITICAL	Fan failure detected **RESOLUTION:** Contact Customer Service.

Table 5-1 Silver Peak Appliance Alarms (Continued)

Subsystem	Alarm Type ID (Hex)	Alarm Severity	Alarm Text
Equipment (cont.)	00030007	CRITICAL	Encryption card hardware failure **RESOLUTION:** Contact Customer Service.
	00030024	CRITICAL	Insufficient configured memory size for this virtual appliance **RESOLUTION:** Assign more memory to the virtual machine, and restart the appliance. Traffic will not be optimized until this is resolved.
	00030025	CRITICAL	Insufficient configured processor count for this virtual appliance **RESOLUTION:** Assign more processors to the virtual machine, and restart the appliance. Traffic will not be optimized until this is resolved.
	00030026	CRITICAL	Insufficient configured disk storage for this virtual appliance **RESOLUTION:** Assign more storage to the virtual machine, and restart the appliance. Traffic will not be optimized until this is resolved.
	00030005	CRITICAL	LAN/WAN fail-to-wire card failure **RESOLUTION:** Contact Customer Service.
	00030021	CRITICAL	NIC interface failure **RESOLUTION:** Contact Customer Service.
	00030004	CRITICAL	System is in Bypass mode **RESOLUTION:** Normal with factory default configuration, during reboot, and if user has put the appliance in Bypass mode. Contact Customer Service if the condition persists.
	0003001d	MAJOR	Bonding members have different speed/duplex **RESOLUTION:** Check interface speed/duplex settings and negotiated values on wan0/wan1 and lan0/lan1 etherchannel groups.
	0003001c	MAJOR	[Flow redirection] cluster peer is down **RESOLUTION:** • Check flow redirection configuration on all applicable appliances. • Check L3/L4 connectivity between the peers. • Open TCP and UDP ports 4164 between the cluster peer IPs if they are blocked.
	00030017	MAJOR	Disk removed by operator **RESOLUTION:** Normal during disk replacement. Insert disk using UI/GMS. Contact Customer Service if insertion fails.
	00030001	MAJOR	Disk is failed **RESOLUTION:** Contact Customer Service to replace disk.
	00030015	MAJOR	Disk is not in service **RESOLUTION:** • Check to see if the disk is properly seated. • Contact Customer service for further assistance.

Table 5-1 Silver Peak Appliance Alarms (Continued)

Subsystem	Alarm Type ID (Hex)	Alarm Severity	Alarm Text
Equipment (cont.)	0003000b	MAJOR	Interface is half duplex **RESOLUTION:** Check speed/duplex settings on the router/switch port.
	0003000c	MAJOR	Interface speed is 10 Mbps **RESOLUTION:** • Check speed/duplex settings. • Use a 100/1000 Mbps port on the router/switch.
	00030022	MAJOR	LAN next-hop unreachable[b] **RESOLUTION:** Check appliance configuration: • LAN–side next-hop IP • Appliance IP / Mask • VLAN IP / Mask • VLAN ID
	0003001a	MAJOR	LAN/WAN interface has been shut down due to link propagation of paired interface **RESOLUTION:** Check cables and connectivity. For example, if lan0 is shut down, check why wan0 is down. Applicable only to in-line (bridge) mode.
	00030018	MAJOR	LAN/WAN interfaces have different admin states **RESOLUTION:** Check interface admin configuration for lan0/wan0 (and lan1/wan1). Applicable only to in-line mode.
	00030019	MAJOR	LAN/WAN interfaces have different link carrier states **RESOLUTION:** Check interface configured speed settings and current values (an0/wan0, lan1/wan1). Applicable only to in-line mode.
	0003000a	MAJOR	Management interface link down **RESOLUTION:** • Check cables. • Check interface admin status on the router.
	00030009	MAJOR	Network interface link down **RESOLUTION:** Is the system in Bypass mode? • Check cables. • Check interface admin status on the router.
	00030020	MAJOR	Power supply not connected, not powered, or failed **RESOLUTION:** • Connect to a power outlet. • Check power cable connectivity.
	00030023	MAJOR	Unexpected system restart **RESOLUTION:** Power issues? Was the appliance shutdown ungracefully? Contact Customer Service if the shutdown was not planned.

Table 5-1 Silver Peak Appliance Alarms (Continued)

Subsystem	Alarm Type ID (Hex)	Alarm Severity	Alarm Text
Equipment (cont.)	00030012	MAJOR	VRRP instance is down **RESOLUTION:** Check the interface. Is the link down?
	00030014	MAJOR	WAN next-hop router discovered on a LAN port (box is in backwards) **RESOLUTION:** • Check WAN next-hop IP address. • Check lan0 and wan0 cabling (in-line mode only). • If it cannot be resolved, call Customer Service.
	00030011	MAJOR	WAN next-hop unreachable[b] **RESOLUTION:** • Check cables on Silver Peak appliance and router. • Check IP/mask on Silver Peak appliance and router. Next-hop should be only a single IP hop away. • To troubleshoot, use: show cdp neighbor, show arp, and ping -I <appliance IP> <next-hop IP>.
	0003001e	MAJOR	WCCP adjacency(ies) down **RESOLUTION:** Cannot establish WCCP neighbor: • Check WCCP configuration on appliance and router. • Verify reachability. • Enable debugging on router: debug ip wccp packet
	0003001f	MAJOR	WCCP assignment table mismatch **RESOLUTION:** Check WCCP mask/hash assignment configuration on all Silver Peak appliances and ensure that they match.
	00030002	MINOR	Disk is degraded **RESOLUTION:** Wait for disk to recover. If it does not recover, contact Customer Service.
	00030016	MINOR	Disk is rebuilding **RESOLUTION:** Normal. If rebuilding is unsuccessful, contact Customer Service.
	0003001b	MINOR	Disk SMART threshold exceeded **RESOLUTION:** Contact Customer Service to replace disk.
	0003002d	MINOR	Non-optimal configured memory size for this virtual appliance **RESOLUTION:** Check the specifications.
	0003002e	MINOR	Non-optimal configured processor count for this virtual appliance **RESOLUTION:** Check the specifications.
	0003002f	MINOR	Non-optimal configured disk storage for this virtual appliance **RESOLUTION:** Check the specifications.

Table 5-1 Silver Peak Appliance Alarms (Continued)

Subsystem	Alarm Type ID (Hex)	Alarm Severity	Alarm Text
Equipment (cont.)	00030008	WARNING	Network interface admin down **RESOLUTION:** Check Silver Peak interface configuration.
	00030013	WARNING	VRRP state changed from Master to Backup **RESOLUTION:** VRRP state has changed from Master to Backup. • Check VRRP Master for uptime. • Check VRRP Master for connectivity.
Threshold Crossing Alerts (TCAs)	00050001	WARNING	The average WAN–side transmit throughput of X Mbps over the last minute [exceeded, fell below] the threshold of Y Mbps **RESOLUTION:** User configured. Check bandwidth reports for tunnel bandwidth.
	00050002	WARNING	The average LAN–side receive throughput of X Mbps over the last minute [exceeded, fell below] the threshold of Y Mbps **RESOLUTION:** User configured. Check bandwidth reports.
	00050003	WARNING	The total number of X optimized flows at the end of the last minute [exceeded, fell below] the threshold of Y **RESOLUTION:** User configured. Check flow and real-time connection reports.
	00050004	WARNING	The total number of X flows at the end of the last minute [exceeded, fell below] the threshold of Y **RESOLUTION:** User configured. Check flow and real-time connection reports.
	00050005	WARNING	The file system utilization of X% at the end of the last minute [exceeded, fell below] the threshold of Y **RESOLUTION:** Contact Customer Service.
	00050006	WARNING	The peak latency of X during the last minute [exceeded, fell below] the threshold of Y **RESOLUTION:** User configured. • Check Latency Reports. If latency is too high, check routing between the appliances and QoS policy on upstream routers. • Check tunnel DSCP marking. If latency persists, contact ISP and Silver Peak support.
	00050007	WARNING	The average pre-FEC loss of X% over the last minute [exceeded, fell below] the threshold of Y% **RESOLUTION:** User configured. • Check Loss Reports. • Check for loss between Silver Peak appliances (interface counters on upstream routers). • Use network bandwidth measurement tools such as iperf to measure loss. • Contact ISP (Internet Service Provider).

Table 5-1 Silver Peak Appliance Alarms (Continued)

Subsystem	Alarm Type ID (Hex)	Alarm Severity	Alarm Text
Threshold Crossing Alerts (TCAs) (cont.	00050008	WARNING	The average post-FEC loss of X% over the last minute [exceeded, fell below] the threshold of Y% **RESOLUTION:** User configured. • Check Loss Reports. • Check for loss between Silver Peak appliances (interface counters on upstream routers). • Use network bandwidth measurement tools such as iperf to measure loss. • Enable/Adjust Silver Peak Forward Error Correction (FEC). • Contact ISP (Internet Service Provider).
	00050009	WARNING	The average pre-POC out-of-order packets of X% over the last minute [exceeded, fell below] the threshold of Y% **RESOLUTION:** User configured. • Check Out-of-Order Packets Reports. Normal in a network with multiple paths and different QoS queues. Normal in a dual-homed router or 4-port in-line [bridge] configuration. • Contact Customer Service if out-of-order packets are not 100% corrected.
	0005000a	WARNING	The average post-POC out-of-order packets of X% over the last minute [exceeded, fell below] the threshold of Y% **RESOLUTION:** User configured. • Check Out-of-Order Packets Reports. Normal in a network with multiple paths and different QoS queues. Normal in a dual-homed router or 4-port in-line [bridge] configuration. • Contact Customer Service if out-of-order packets are not 100% corrected.
	0005000b	WARNING	The average tunnel utilization of X% over the last minute [exceeded, fell below] the threshold of Y% **RESOLUTION:** User configured. Check bandwidth reports for tunnel bandwidth utilization.
	0005000c	WARNING	The average tunnel reduction of X% over the last minute [exceeded, fell below] the threshold of Y% **RESOLUTION:** User configured. • Check bandwidth reports for deduplication. • Check if the traffic is pre-compressed or encrypted.
	0005000d	WARNING	The total number of flows <num-of-flows> is approaching the capacity of this appliance. Once the capacity is exceeded, new flows will be <dropped|bypassed>. **RESOLUTION:** If this condition persists, a larger appliance will be necessary to fully optimize all flows.

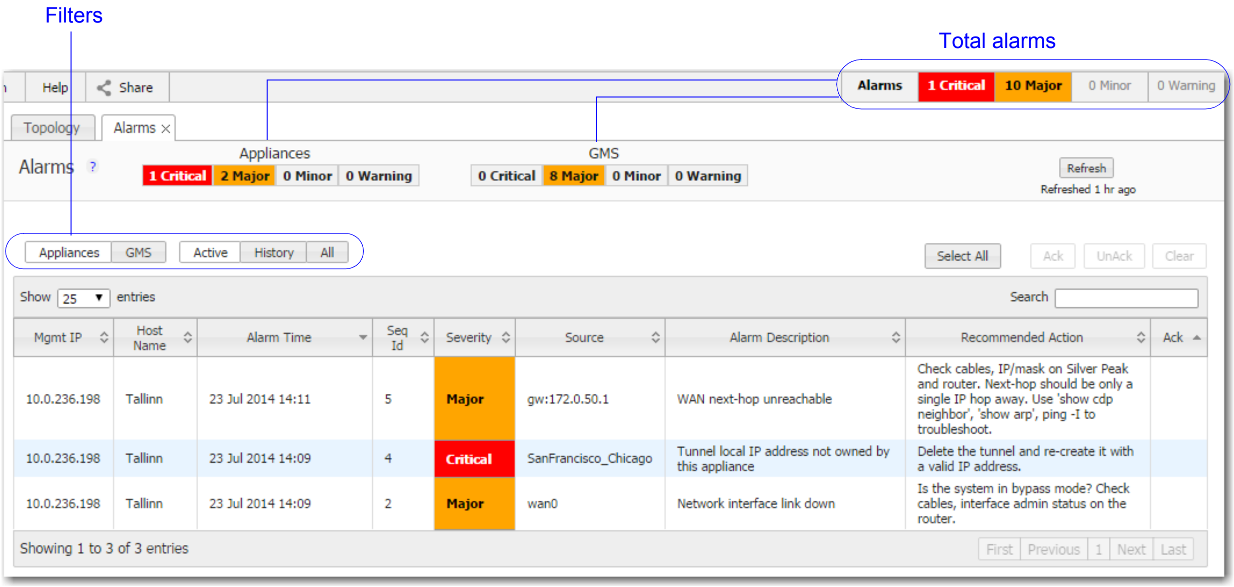
a. The VX appliances are a family of virtual appliances, comprised of the VX-n000 software, an appropriately paired hypervisor and server, and a valid software license.

b. If there is either a **LAN Next-Hop Unreachable** or **WAN Next-Hop Unreachable** alarm, resolve the alarm(s) immediately by configuring the gateway(s) to respond to ICMP pings from the Silver Peak appliance IP Address.

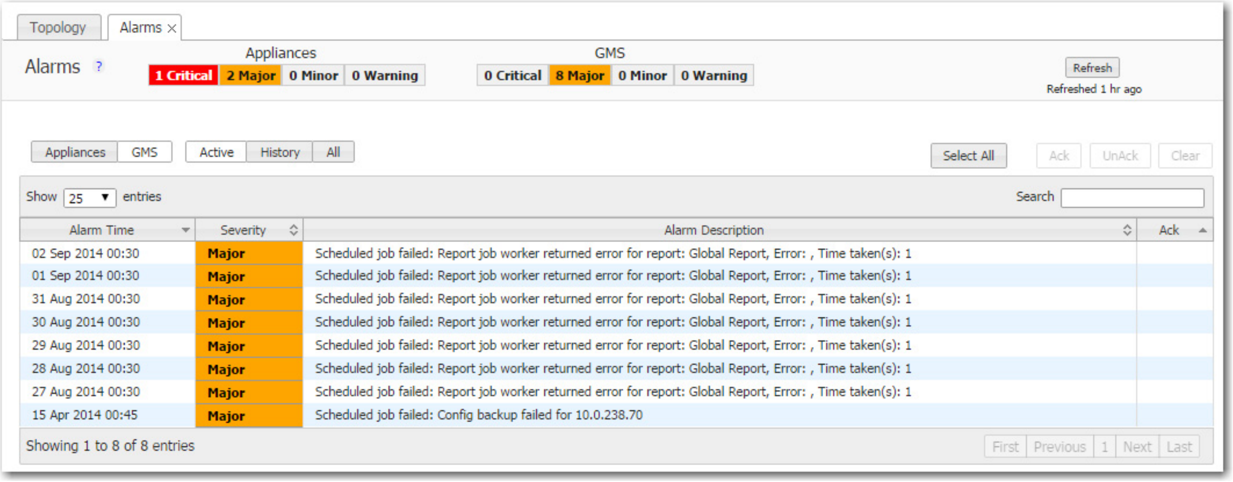
Viewing Alarms

Monitoring > Alarms

- The **Alarms** table displays the alarms for the selected appliances, as well as for the GMS.
- Appliance alarm descriptions list recommended actions for resolving the issue.



Mgmt IP	Host Name	Alarm Time	Seq Id	Severity	Source	Alarm Description	Recommended Action	Ack
10.0.236.198	Tallinn	23 Jul 2014 14:11	5	Major	gw:172.0.50.1	WAN next-hop unreachable	Check cables, IP/mask on Silver Peak and router. Next-hop should be only a single IP hop away. Use 'show cdp neighbor', 'show arp', ping -I to troubleshoot.	
10.0.236.198	Tallinn	23 Jul 2014 14:09	4	Critical	SanFrancisco_Chicago	Tunnel local IP address not owned by this appliance	Delete the tunnel and re-create it with a valid IP address.	
10.0.236.198	Tallinn	23 Jul 2014 14:09	2	Major	wan0	Network interface link down	Is the system in bypass mode? Check cables, interface admin status on the router.	

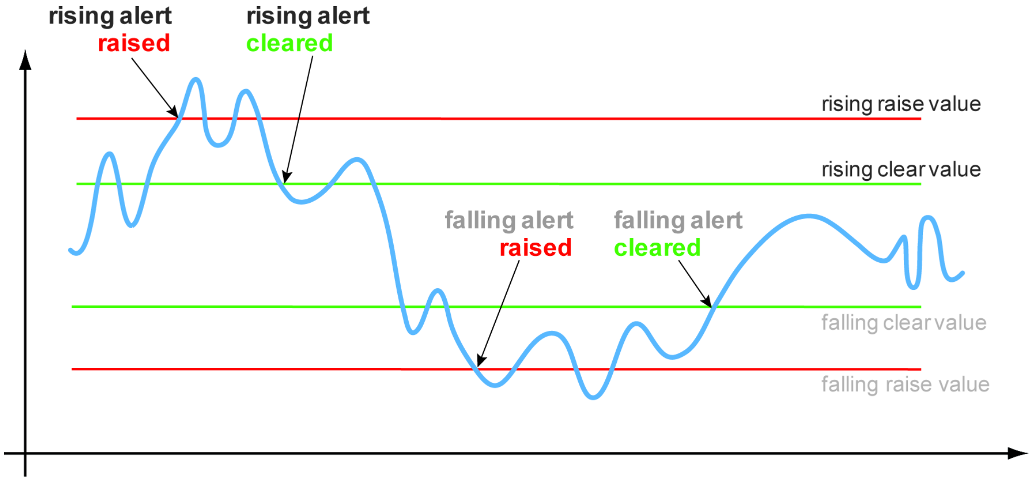


Alarm Time	Severity	Alarm Description	Ack
02 Sep 2014 00:30	Major	Scheduled job failed: Report job worker returned error for report: Global Report, Error: , Time taken(s): 1	
01 Sep 2014 00:30	Major	Scheduled job failed: Report job worker returned error for report: Global Report, Error: , Time taken(s): 1	
31 Aug 2014 00:30	Major	Scheduled job failed: Report job worker returned error for report: Global Report, Error: , Time taken(s): 1	
30 Aug 2014 00:30	Major	Scheduled job failed: Report job worker returned error for report: Global Report, Error: , Time taken(s): 1	
29 Aug 2014 00:30	Major	Scheduled job failed: Report job worker returned error for report: Global Report, Error: , Time taken(s): 1	
28 Aug 2014 00:30	Major	Scheduled job failed: Report job worker returned error for report: Global Report, Error: , Time taken(s): 1	
27 Aug 2014 00:30	Major	Scheduled job failed: Report job worker returned error for report: Global Report, Error: , Time taken(s): 1	
15 Apr 2014 00:45	Major	Scheduled job failed: Config backup failed for 10.0.238.70	

Understanding Threshold Crossing Alerts (TCAs)

Threshold Crossing Alerts are preemptive, user-configurable alarms triggered when the specific thresholds are crossed. They alarm on both rising and falling threshold crossing events (that is, floor and ceiling levels). For both levels, one value raises the alarm, while another value clears it.

Configure TCAs with the **Threshold Crossing Alert** template.



Rules:

- High raise threshold is greater than high clear threshold
- Low raise threshold is less than low clear threshold

Times to Trigger – A value of 1 triggers an alarm on the first threshold crossing instance.

ON by default:

- **Appliance Capacity** – triggers when an appliance reaches 95% of its total flow capacity. It is not configurable and can only be cleared by an operator.
- **File-system utilization** – percent of non-Network Memory disk space filled by the appliance. This TCA cannot be disabled.
- **Tunnel latency** – measured in milliseconds, the maximum latency of a one-second sample within a 60-second span

OFF by default:

- **LAN-side receive throughput** - based on a one-minute average, the LAN-side receive TOTAL for all interfaces
- **WAN-side transmit throughput** - based on a one-minute average, the WAN-side transmit TOTAL for all interfaces
- **TCAs based on an end-of-minute count:**
  - Total number of flows
  - Total number of optimized flows

- **TCAs based on a one-minute average:**
  - Tunnel loss post-FEC
  - Tunnel loss post-FEC
  - Tunnel OOP post-POC
  - Tunnel OOP post-POC
  - Tunnel reduction
  - Tunnel utilization (based on percent of configured maximum [system] bandwidth)

Note Enabled by default, there is also an **Appliance Capacity** TCA that triggers when an appliance reaches 95% of its total flow capacity. It doesn't automatically clear, but can be cleared by an operator. It is also not configurable.

This table lists the **defaults** of each type of threshold crossing alert:

Table 5-2 Defaults values for Threshold Crossing Alerts

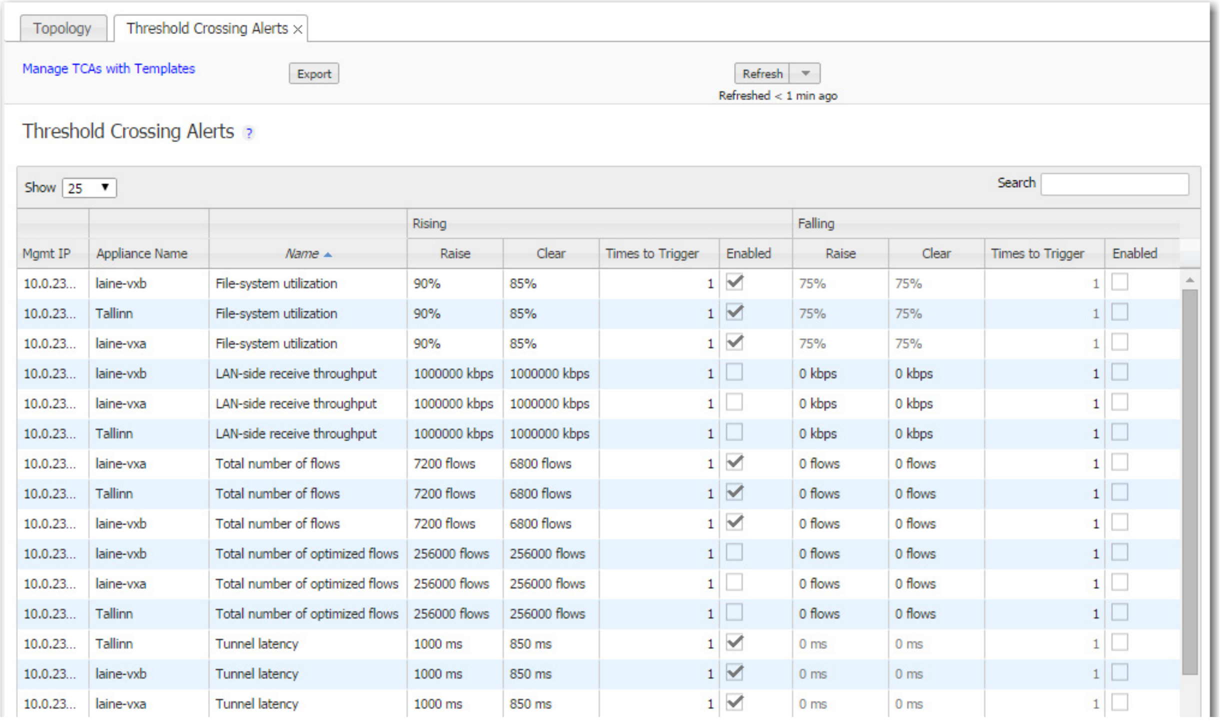
	TCA Name	Default [ON, OFF]	Default Values [Rising Raise, Rising Clear, Falling Raise, Falling Clear]	allow rising	allow falling
Appliance Level	**WAN-side transmit throughput**	OFF	1 Gbps; 1 Gbps; 0; 0	4	4
	LAN-side receive throughput	OFF	1 Gbps; 1 Gbps; 0; 0	4	4
	Total number of optimized flows	OFF	256,000, 256,000; 0; 0	4	4
	Total number of flows	OFF	256,000, 256,000; 0; 0	4	4
	File-system-utilization	**ON**[a]	95%; 85%; 0%; 0%	4	
Tunnel Level	**Tunnel latency**	**ON**	1000; 850; 0; 0	4	
	Tunnel loss pre-FEC	OFF	100%; 100%; 0%; 0%	4	
	Tunnel loss post-FEC	OFF	100%; 100%; 0%; 0%	4	
	Tunnel OOP pre-POC	OFF	100%; 100%; 0%; 0%	4	
	Tunnel OOP post-POC	OFF	100%; 100%; 0%; 0%	4	
	Tunnel utilization	OFF	95%; 90%; 0%; 0%	4	4
	Tunnel reduction	OFF	100%; 100%; 0%; 0%		4

[a] Cannot be disabled.

Threshold Crossing Alerts Tab

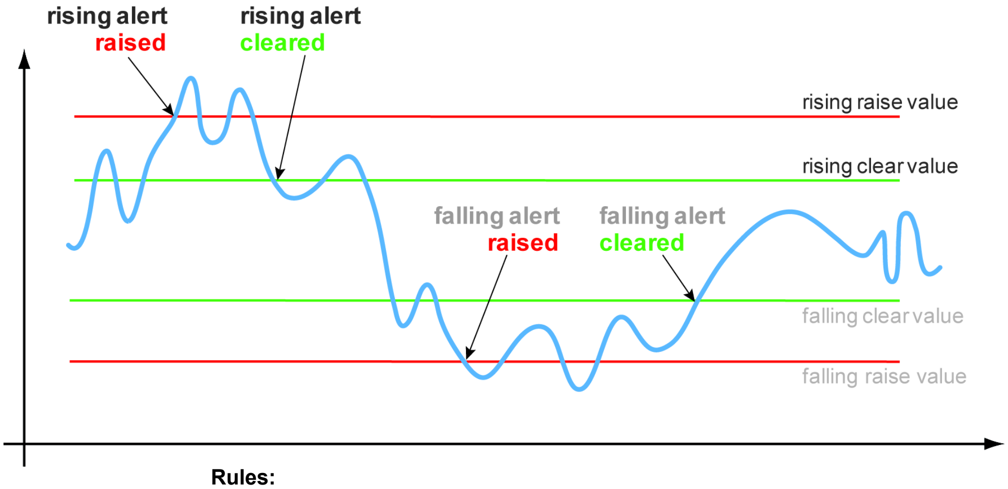
Monitoring > Threshold Crossing Alerts

Threshold Crossing Alerts (TCAs) are pre-emptive, user-configurable alarms triggered when specific thresholds are crossed.


Topology
Threshold Crossing Alerts ×
Manage TCAs with Templates
Export
Refresh
Refreshed < 1 min ago
Threshold Crossing Alerts ?
Show 25
Search

			Rising				Falling			
Mgmt IP	Appliance Name	Name ▲	Raise	Clear	Times to Trigger	Enabled	Raise	Clear	Times to Trigger	Enabled
10.0.23...	laine-vxb	File-system utilization	90%	85%	1	☑	75%	75%	1	□
10.0.23...	Tallinn	File-system utilization	90%	85%	1	☑	75%	75%	1	□
10.0.23...	laine-vxa	File-system utilization	90%	85%	1	☑	75%	75%	1	□
10.0.23...	laine-vxb	LAN-side receive throughput	1000000 kbps	1000000 kbps	1	□	0 kbps	0 kbps	1	□
10.0.23...	laine-vxa	LAN-side receive throughput	1000000 kbps	1000000 kbps	1	□	0 kbps	0 kbps	1	□
10.0.23...	Tallinn	LAN-side receive throughput	1000000 kbps	1000000 kbps	1	□	0 kbps	0 kbps	1	□
10.0.23...	laine-vxa	Total number of flows	7200 flows	6800 flows	1	☑	0 flows	0 flows	1	□
10.0.23...	Tallinn	Total number of flows	7200 flows	6800 flows	1	☑	0 flows	0 flows	1	□
10.0.23...	laine-vxb	Total number of flows	7200 flows	6800 flows	1	☑	0 flows	0 flows	1	□
10.0.23...	laine-vxb	Total number of optimized flows	256000 flows	256000 flows	1	□	0 flows	0 flows	1	□
10.0.23...	laine-vxa	Total number of optimized flows	256000 flows	256000 flows	1	□	0 flows	0 flows	1	□
10.0.23...	Tallinn	Total number of optimized flows	256000 flows	256000 flows	1	□	0 flows	0 flows	1	□
10.0.23...	Tallinn	Tunnel latency	1000 ms	850 ms	1	☑	0 ms	0 ms	1	□
10.0.23...	laine-vxb	Tunnel latency	1000 ms	850 ms	1	☑	0 ms	0 ms	1	□
10.0.23...	laine-vxa	Tunnel latency	1000 ms	850 ms	1	☑	0 ms	0 ms	1	□

They alarm on both rising and falling threshold crossing events (i.e., floor and ceiling levels). For both levels, one value raises the alarm, while another value clears it.



Rules:

- High raise threshold is greater than high clear threshold
- Low raise threshold is less than low clear threshold

ON by default:

- **Appliance Capacity** - triggers when an appliance reaches 95% of its total flow capacity. It is not configurable and can only be cleared by an operator.
- **File-system utilization** - percent of non-Network Memory disk space filled by the appliance. This TCA cannot be disabled.
- **Tunnel latency** - measured in milliseconds, the maximum latency of a one-second sample within a 60-second span

OFF by default:

- **LAN-side receive throughput** - based on a one-minute average, the LAN-side receive **TOTAL** for all interfaces
- **WAN-side transmit throughput** - based on a one-minute average, the WAN-side transmit **TOTAL** for all interfaces
- **TCAs based on an end-of-minute count**:
  - Total number of flows
  - Total number of optimized flows
- **TCAs based on a one-minute average**:
  - Tunnel loss post-FEC
  - Tunnel loss post-FEC
  - Tunnel OOP post-POC
  - Tunnel OOP post-POC
  - Tunnel reduction
  - Tunnel utilization (based on percent of configured maximum [system] bandwidth)

CHAPTER 6

Monitoring Status and Performance

This chapter focuses on reports related to performance, traffic, and appliance status.

Alarms and *Threshold Crossing Alerts* are addressed in a separate chapter.

In This Chapter

About Reports

This section discusses types of reports and understanding traffic direction.

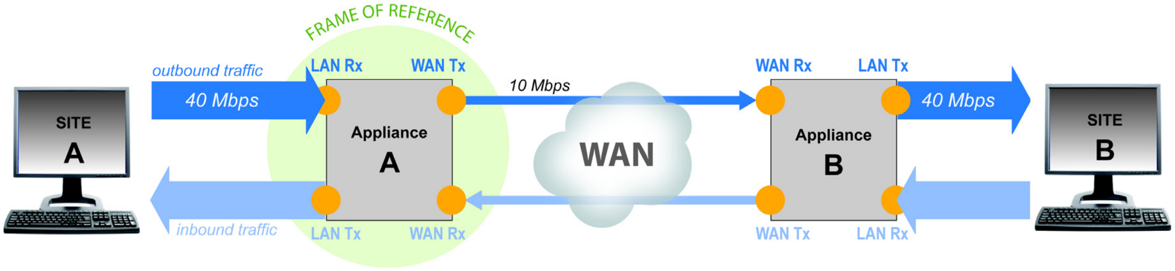
Types of Reports

Reports and statistics help you bracket a problem, question, or analysis. The GMS's collections of reports basically fall into two broad categories:

- Statistics related to **network performance** and **application performance**. These provide visibility into the network, enabling you to investigate problems, and address trends, and evaluate your WAN utilization.
- Reports related to **status** of the network and appliances. For example, alarms, threshold crossing alerts, reachability between the GMS and appliances, scheduled jobs, etc.

Understanding Traffic Direction

Whether you're troubleshooting or just reviewing reports, know what your ***frame of reference*** is.



For any given appliance, statistics and reports reference either of the following:

- the direction of the traffic [LAN to WAN; WAN to LAN]
  - **LAN-to-WAN** refers to traffic exiting the LAN, destined for the WAN. This flow is also referred to as ***outbound traffic***.
  - **WAN-to-LAN** refers to traffic coming from the WAN, destined for the LAN. This flow is also referred to as ***inbound traffic***.

Tip Here's a helpful mnemonic for remembering the difference:

- **Rx** is "Receive fRom", so **LAN Rx** is "receive from LAN"
- **Tx** is "Transmit To", so **LAN Tx** is "transmit to LAN"

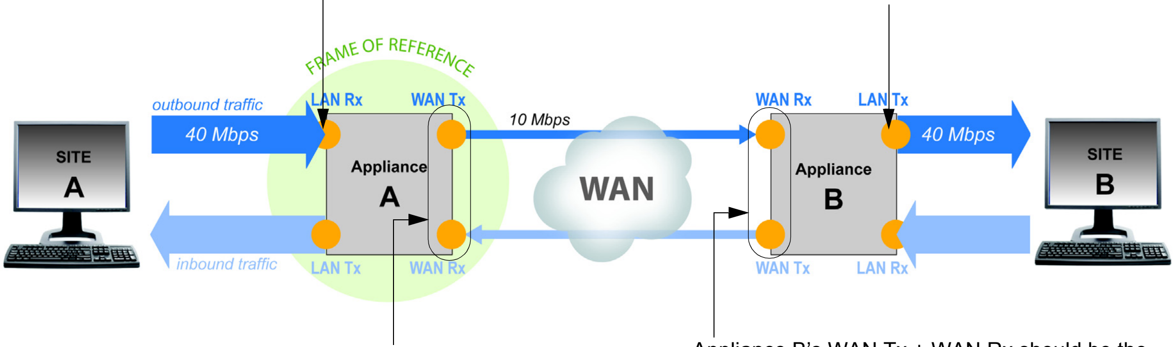
- the points where an appliance collects data about the traffic [**LAN Rx + Tx**, **LAN Rx**, etc.]

For validation and troubleshooting, it always helps to look at both sides of a traffic flow — that is, stats from **Appliance A** alongside stats from **Appliance B**. For example:

From Appliance A's point of view,
if its **LAN Rx** is the "sender" ....

... then Appliance B's **LAN Tx** is the "receiver".

Values should be roughly equal for the pair, so you can view effective throughput by looking in either place.



For Appliance A, the sum of its WAN Tx + WAN Rx equals the total bandwidth being used on the link.

Appliance B's WAN Tx + WAN Rx should be the same for total bandwidth being used on the link.

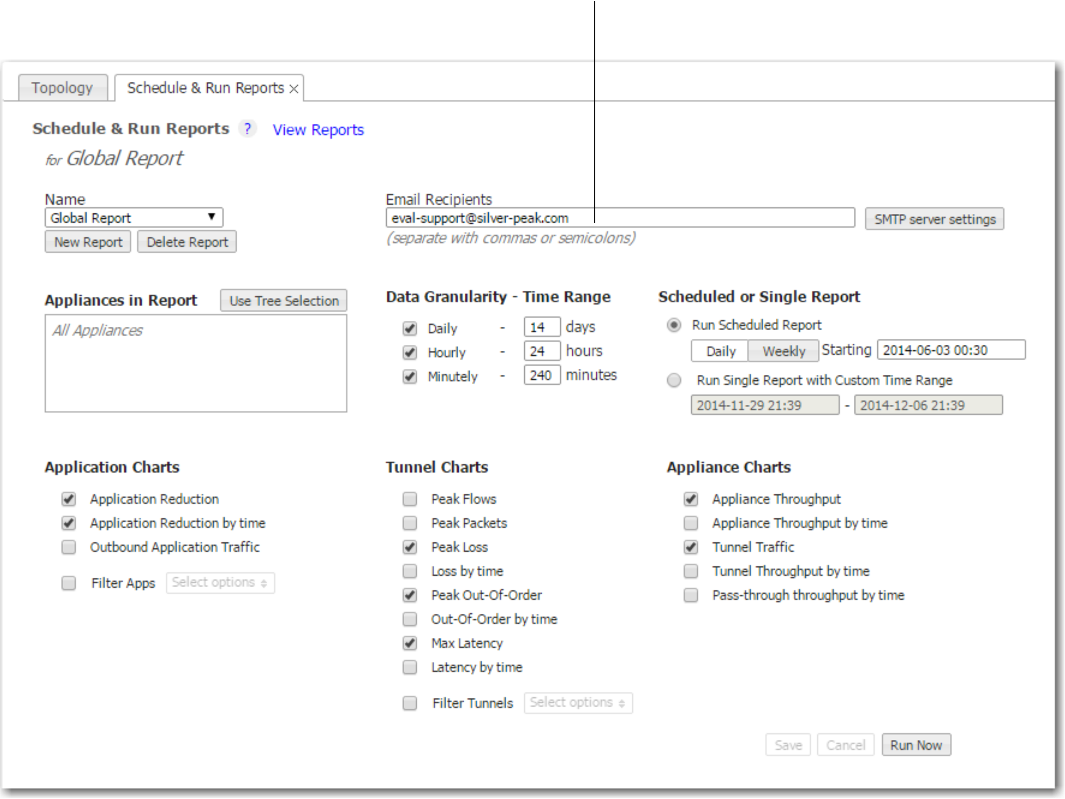
Configuring and Distributing Custom Reports

Monitoring > Schedule & Run Reports

Use the **Schedule & Run Reports** tab to create, configure, run, schedule, and distribute reports.

It is located under **Monitoring > Reports > Schedule & Run Reports**.

Prepopulated from email settings in
GMS Administration > Getting Started Wizard



Schedule & Run Reports ? View Reports

for Global Report

Name: Global Report ▾

Email Recipients: eval-support@silver-peak.com
(separate with commas or semicolons)

Appliances in Report
All Appliances

Data Granularity - Time Range
☑ Daily - 14 days
☑ Hourly - 24 hours
☑ Minutely - 240 minutes

Scheduled or Single Report
● Run Scheduled Report
Daily | Weekly Starting 2014-06-03 00:30
○ Run Single Report with Custom Time Range
2014-11-29 21:39 - 2014-12-06 21:39

Application Charts
☑ Application Reduction
☑ Application Reduction by time
☐ Outbound Application Traffic
☐ Filter Apps Select options

Tunnel Charts
☐ Peak Flows
☐ Peak Packets
☑ Peak Loss
☐ Loss by time
☑ Peak Out-Of-Order
☐ Out-Of-Order by time
☑ Max Latency
☐ Latency by time
☐ Filter Tunnels Select options

Appliance Charts
☑ Appliance Throughput
☐ Appliance Throughput by time
☑ Tunnel Traffic
☐ Tunnel Throughput by time
☐ Pass-through throughput by time

- On schedule or on demand, the GMS can generate Daily, Hourly, and/or Minute Reports containing user-selected charts.
- Each report is a separate PDF file, and takes its filename based on the date, time, granularity, and name of the generated report.
- Along with the PDF report(s), the GMS also generates a corresponding .zip file containing the raw data in .csv files. To open the .zip file, use either Winrar or 7-Zip.
- To access all reports residing on the GMS server, click **View Reports**. The GMS retains reports and zipped .csv files for 30 days.
- The GMS server also sends **reports via email**, using a Silver Peak SMTP server in Amazon Web Services.
  - To send a test email and/or to configure another SMTP server instead, click **SMTP server settings**.
  - If a test email doesn't arrive within minutes, check your firewall.
- **Global Report** - Once you enable it, this preconfigured subset of charts runs at 00:30 each day. This allows time to complete end-of-day processing. You can modify which charts to include and when/whether to run the report, but you cannot delete it.

Data Collection & Management

- The GMS **polls** each of the appliances at **15-minute intervals**, based on the time that the GMS was powered on. So, if the GMS powered on at 14:26, it polls at 14:41, 14:56, 15:11, and 15:26, etc.
- A day begins at 00:00 and ends at 23:59:59.
- A Daily or Hourly report begins at the top of the hour. A Minute report begins at the last poll period.
- Report stats aggregate to 1 minute.
- Reach of reports: **Daily** = 14 days, **Hourly** = 24 hours, **Minute** = 4 hours
- In charts, GMS displays only the maximum peak in each prescribed time interval.
- Reports return the top ten filtered or unfiltered items.

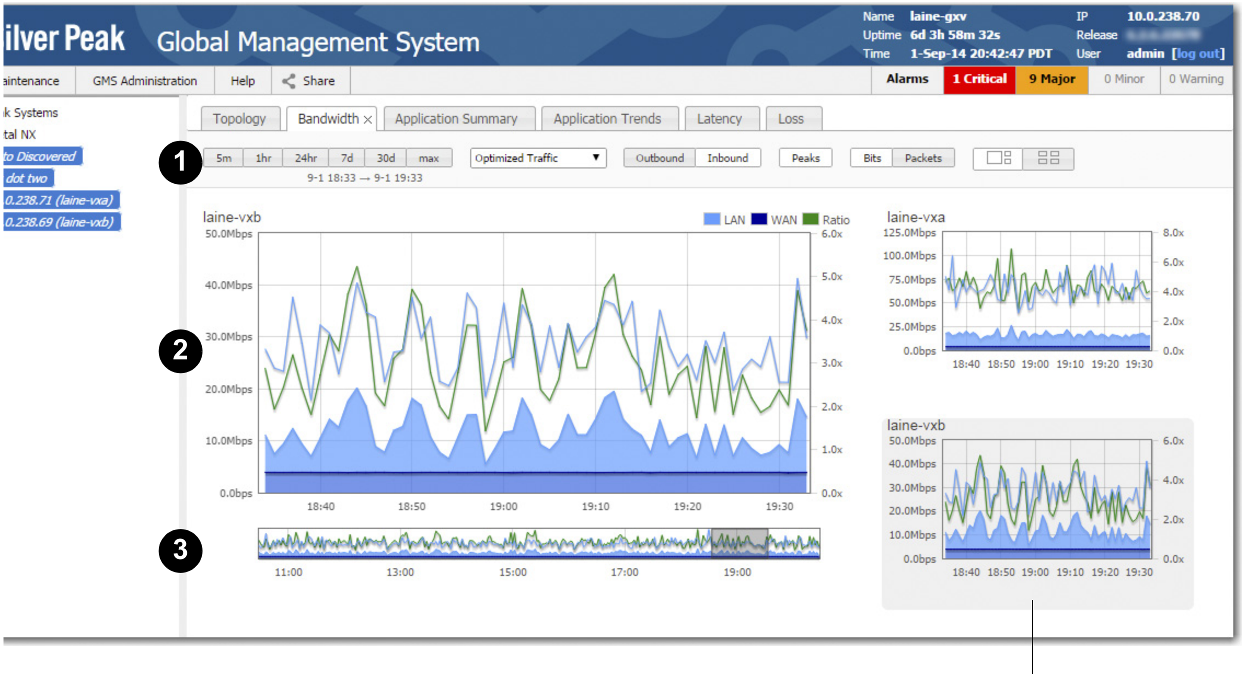
Viewing Performance Charts

Charts feature spark lines, as well as selectable (and modifiable) time ranges for collected data.

Charts exist for the following under **Monitoring**:

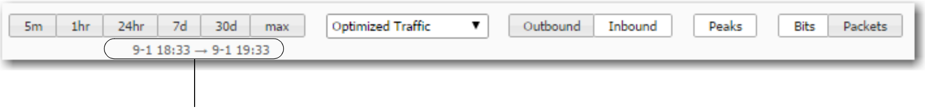
- **Bandwidth** See page 114.
- **Application Summary** See page 115.
- **Application Trends** See page 117.
- **Latency** See page 118.
- **Loss** See page 118.

Charts consist of filters, a main chart display, thumbnails, and a modifiable time range area.



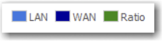
Thumbnails display for each appliance selected in the navigation pane. Select the thumbnail you want to enlarge.

1 FILTER SELECTION

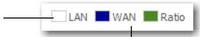


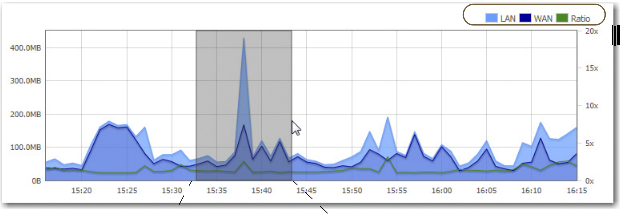
Selected range displays here, whether specified by clicking the interval or by modifying the spark line’s range.

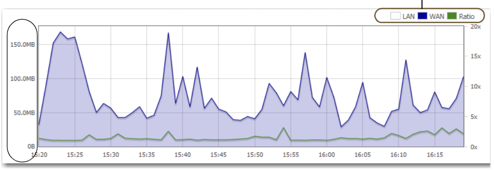
2 CHART DISPLAY — Legend / X-axis / Y-axis



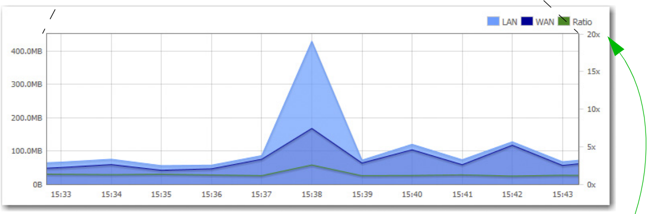
Click color to select/deselect parameter







To zoom in... click, drag, and release. The chart updates to show the new range.



The Y-axis height is calibrated to the maximum Y value in the selected range.

The Y-axis calibration may change if you hide a parameter (LAN, WAN, or Ratio) that has higher values than the remaining parameters.

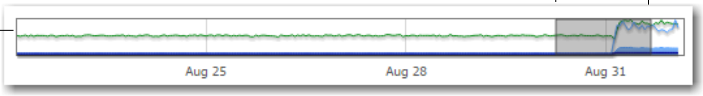
You can not manually zoom to change the Y-axis.

3 MODIFIABLE TIME RANGE

To change the time frame, you can also

- drag the **slider** to change its position
- change the **slider**'s size — click and drag an edge

Spark lines showing the activity

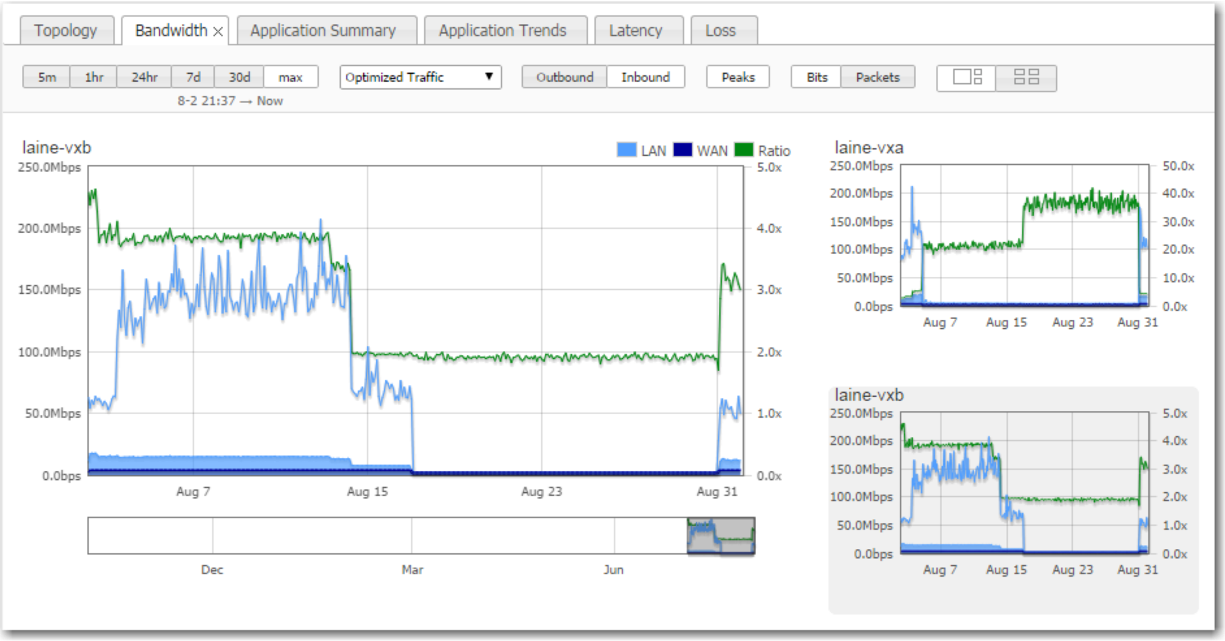


Bandwidth

Monitoring > Bandwidth

The **Bandwidth** chart answers the following questions:

- How much has the bandwidth been optimized?
- At what rate was the data sent and/or received in each time interval?



Application Summary

Monitoring > Application Summary

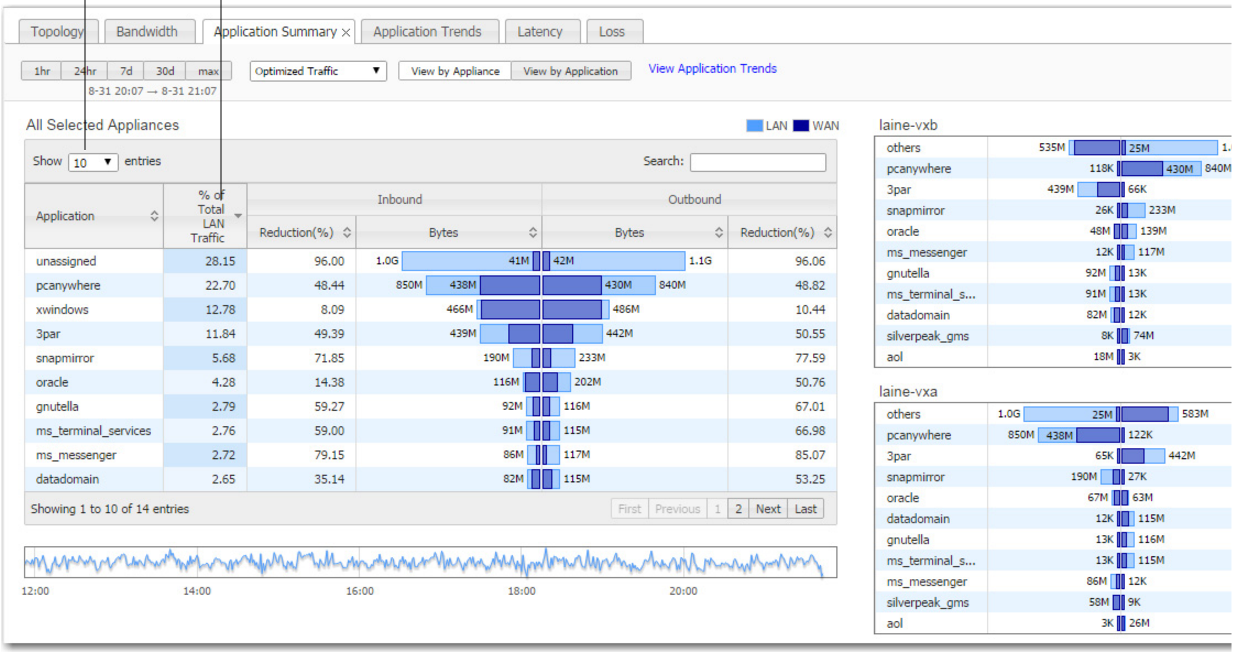
The **Application Summary** chart has two views available — by Appliance and by Application. It answers the following questions:

- What percentage of total LAN traffic does each application comprise?
- What is the data reduction in each direction?
- When comparing outbound and inbound traffic, how are the application distributions different?
- What is the ratio of LAN-to-WAN or WAN-to-LAN traffic for any given application?

View by Appliance

Display up to 1000 applications

Total LAN = Inbound LAN + Outbound LAN



All Selected Appliances

🟦 LAN ■ WAN

Show 10 ▼ entries

Application	% of Total LAN Traffic	Inbound		Outbound	
		Reduction(%)	Bytes	Bytes	Reduction(%)
unassigned	28.15	96.00	1.0G 41M	42M 1.1G	96.06
pcanywhere	22.70	48.44	850M 438M	430M 840M	48.82
xwindows	12.78	8.09	466M	486M	10.44
3par	11.84	49.39	439M	442M	50.55
snapmirror	5.68	71.85	190M	233M	77.59
oracle	4.28	14.38	116M	202M	50.76
gnutella	2.79	59.27	92M	116M	67.01
ms_terminal_services	2.76	59.00	91M	115M	66.98
ms_messenger	2.72	79.15	86M	117M	85.07
datadomain	2.65	35.14	82M	115M	53.25

Showing 1 to 10 of 14 entries

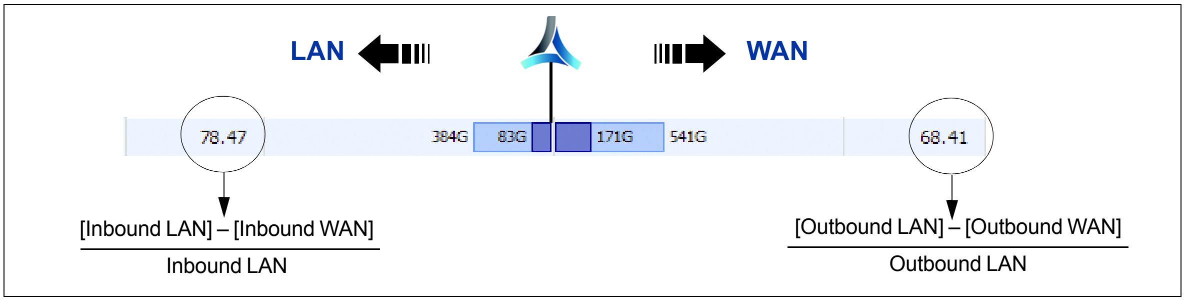
laine-vxb

others	535M	25M 1.
pcanywhere	118K	430M 840M
3par	439M	66K
snapmirror	26K	233M
oracle	48M	139M
ms_messenger	12K	117M
gnutella	92M	13K
ms_terminal_s...	91M	13K
datadomain	82M	12K
silverpeak_gms	8K	74M
aol	18M	3K

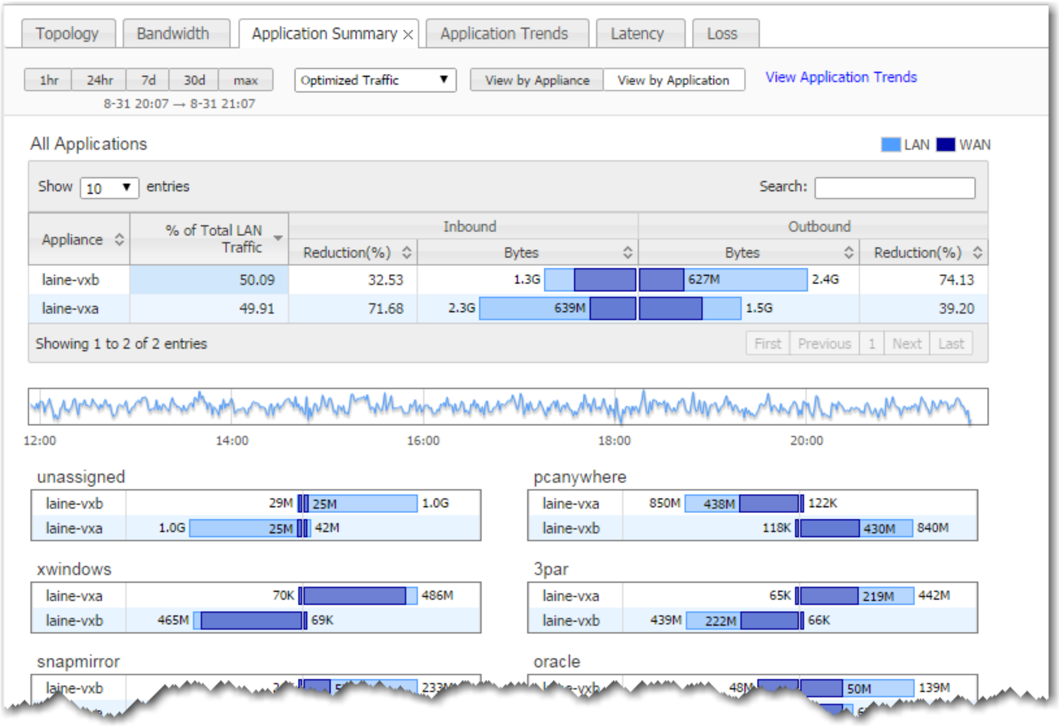
laine-vxa

others	1.0G 25M	583M
pcanywhere	850M 438M	122K
3par	65K	442M
snapmirror	190M	27K
oracle	67M	63M
datadomain	12K	115M
gnutella	13K	116M
ms_terminal_s...	13K	115M
ms_messenger	86M	12K
silverpeak_gms	58M	9K
aol	3K	26M

For each direction of traffic — inbound and outbound — the overlapping bars are paired to show the full volume of traffic and the reduced, optimized size of the same traffic.


LAN
WAN
78.47
384G
83G
171G
541G
68.41
[Inbound LAN] – [Inbound WAN]
Inbound LAN
[Outbound LAN] – [Outbound WAN]
Outbound LAN

View by Application



All Applications

Show 10 ▼ entries

Search:

Appliance	% of Total LAN Traffic	Inbound		Outbound	
		Reduction(%)	Bytes	Bytes	Reduction(%)
laine-vxb	50.09	32.53	1.3G	627M 2.4G	74.13
laine-vxa	49.91	71.68	2.3G 639M	1.5G	39.20

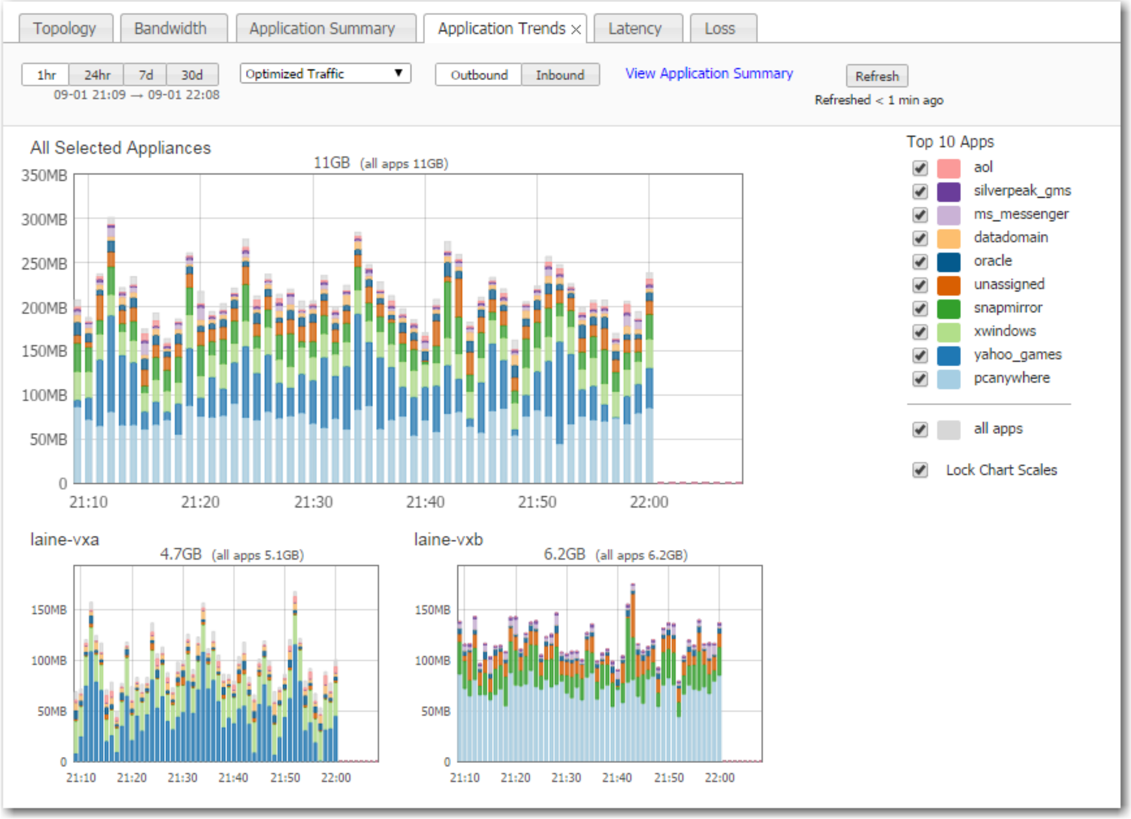
Showing 1 to 2 of 2 entries

Application Trends

Monitoring > Application Trends

The **Application Trends** chart answers the following questions:

- What proportion of traffic does each application account for over time?
- The top 10 applications account for what portion of the total traffic?



Note When it comes to flow and application statistics reports, user-defined applications are always checked before built-in applications.

Ports are unique. If a port or a range includes a built-in port, then the custom application is the one that lays claim to it.

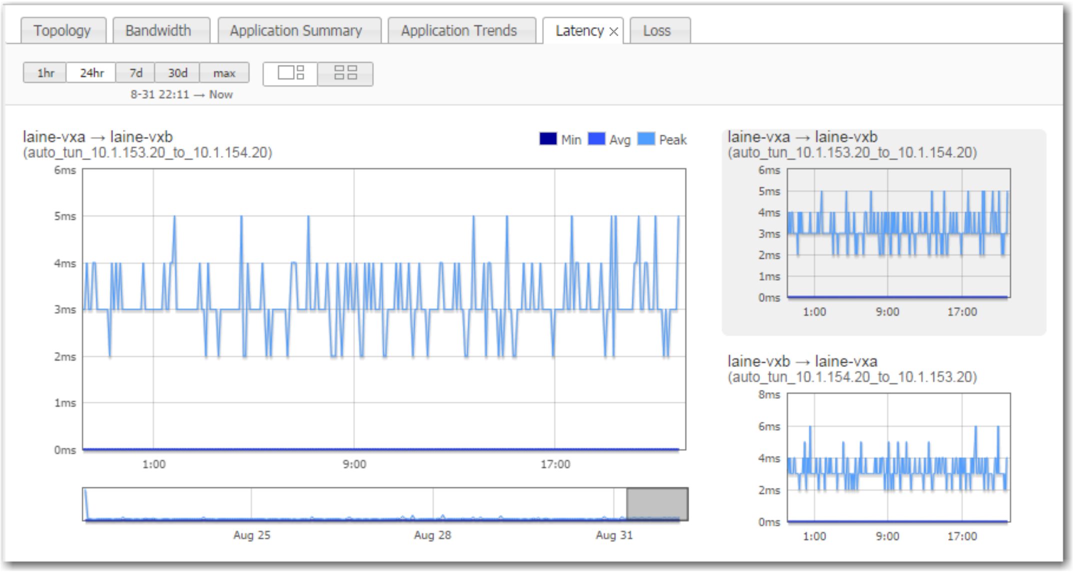
If two distinctly named user-defined applications have a port number in common, then report results will be skewed, depending on the priority assigned to the custom applications. A port is only counted once.

Latency

Monitoring > Latency

The **Latency** chart answers the following questions:

- How long does it take my data to get to the other end of the Silver Peak tunnel?
- What were the peak, average, and minimum time intervals?

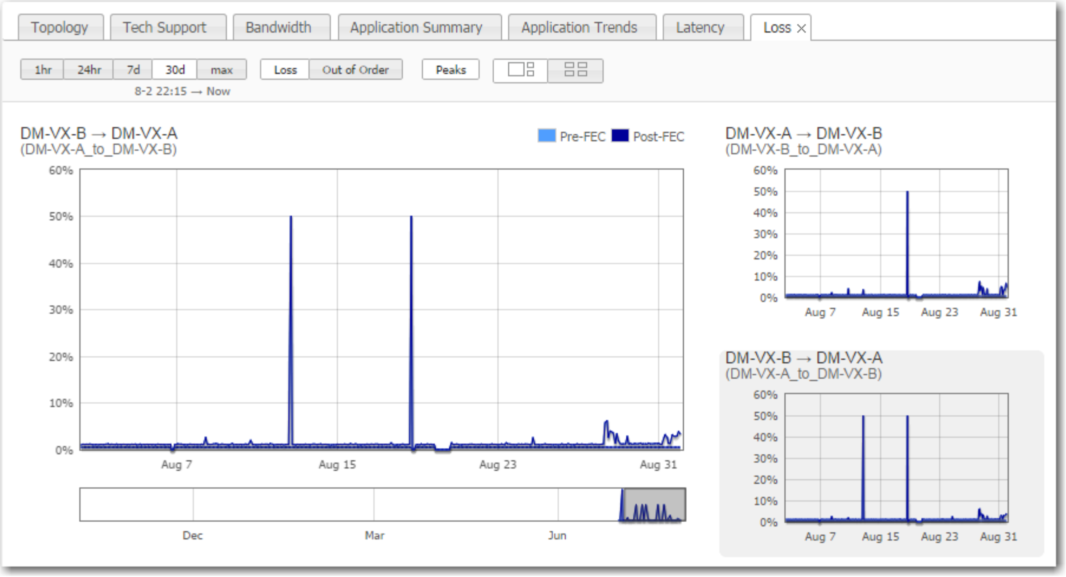


Loss

Monitoring > Loss

The **Loss** dynamic chart summarizes, by tunnel, the number of packets lost before and after enabling **Forward Error Correction (FEC)**. It answers the following questions:

- How many errors were there before and after turning on Forward Error Correction?
- For any given minute, what was the percent loss?



Viewing Current Flows

Monitoring > Flows

Flows are useful for troubleshooting and for detailed visibility into the network.

The **Flows** page retrieves a list of existing connections. The maximum visible number depends on which browser you user.

- The page displays a default set of columns, along with individual links to flow details and to any alerts.
- You can display additional columns from a customization list.

This section discusses the following topics:

- **How Flows Are Counted** See page 119.
- **How Current Flows are Organized** See page 120.
- **Customizing Which Columns Display** See page 122.
- **Current Flow Details** See page 123.
- **Resetting Flows to Improve Performance** See page 134.

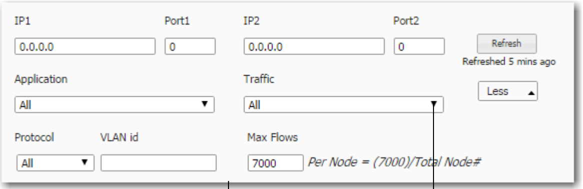
How Flows Are Counted

When it comes to flow and application statistics reports, user-defined applications are always checked before built-in applications.

Ports are unique. If a port or a range includes a built-in port, then the custom application is the one that lays claim to it.

If two distinctly named user-defined applications have a port number in common, then report results will be skewed, depending on the priority assigned to the custom applications. A port is only counted once.

How Current Flows are Organized



IP1 0.0.0.0 Port1 0 IP2 0.0.0.0 Port2 0

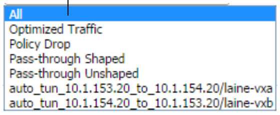
Application All

Traffic All

Protocol All

VLAN id

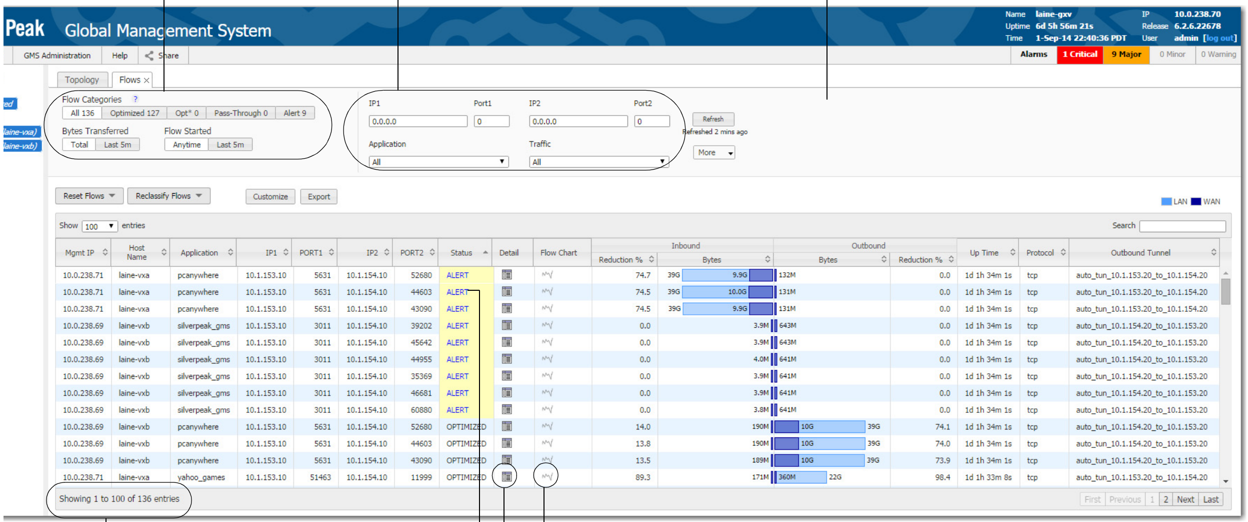
Max Flows 7000 *Per Node = (7000)/Total Node#*



All
Optimized Traffic
Policy Drop
Pass-through Shaped
Pass-through Unshaped
auto_tun_10.1.153.20_to_10.1.154.20/laine-vxa
auto_tun_10.1.154.20_to_10.1.153.20/laine-vxb

Click to select the filter.
Active filters are highlighted.

Enter specific addresses and/or use zeroes (in the octet) as wildcards. The page lists flows that have either endpoint.



Name laine-gxv Uptime 6d 5h 56m 21s Time 1-Sep-14 22:40:36 PDT
IP 10.0.238.70 Release 6.2.6.22678 User admin [log out]

Flow Categories: All 136 | Optimized 127 | Opt* 0 | Pass-Through 0 | Alert 9

Bytes Transferred: Total | Last 5m

Flow Started: Anytime | Last 5m

IP1 0.0.0.0 Port1 0 IP2 0.0.0.0 Port2 0

Application All Traffic All

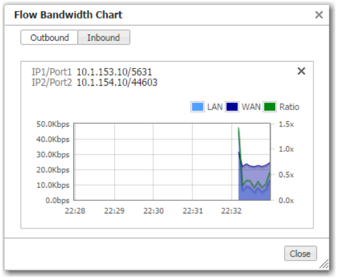
Show 100 entries

Mgmt IP	Host Name	Application	IP1	PORT1	IP2	PORT2	Status	Detail	Flow Chart	Inbound		Outbound		Up Time	Protocol	Outbound Tunnel
										Reduction %	Bytes	Bytes	Reduction %			
10.0.238.71	laine-vxa	pcanywhere	10.1.153.10	5631	10.1.154.10	52680	ALERT			74.7	39G 9.9G	132M	0.0	1d 1h 34m 1s	tcp	auto_tun_10.1.153.20_to_10.1.154.20
10.0.238.71	laine-vxa	pcanywhere	10.1.153.10	5631	10.1.154.10	44603	ALERT			74.5	39G 10.0G	131M	0.0	1d 1h 34m 1s	tcp	auto_tun_10.1.153.20_to_10.1.154.20
10.0.238.71	laine-vxa	pcanywhere	10.1.153.10	5631	10.1.154.10	43090	ALERT			74.5	39G 9.9G	131M	0.0	1d 1h 34m 1s	tcp	auto_tun_10.1.153.20_to_10.1.154.20
10.0.238.69	laine-vxb	silverpeak_gms	10.1.153.10	3011	10.1.154.10	39202	ALERT			0.0	3.9M	643M	0.0	1d 1h 34m 1s	tcp	auto_tun_10.1.154.20_to_10.1.153.20
10.0.238.69	laine-vxb	silverpeak_gms	10.1.153.10	3011	10.1.154.10	45642	ALERT			0.0	3.9M	643M	0.0	1d 1h 34m 1s	tcp	auto_tun_10.1.154.20_to_10.1.153.20
10.0.238.69	laine-vxb	silverpeak_gms	10.1.153.10	3011	10.1.154.10	44955	ALERT			0.0	4.0M	641M	0.0	1d 1h 34m 1s	tcp	auto_tun_10.1.154.20_to_10.1.153.20
10.0.238.69	laine-vxb	silverpeak_gms	10.1.153.10	3011	10.1.154.10	35369	ALERT			0.0	3.9M	641M	0.0	1d 1h 34m 1s	tcp	auto_tun_10.1.154.20_to_10.1.153.20
10.0.238.69	laine-vxb	silverpeak_gms	10.1.153.10	3011	10.1.154.10	46681	ALERT			0.0	3.9M	641M	0.0	1d 1h 34m 1s	tcp	auto_tun_10.1.154.20_to_10.1.153.20
10.0.238.69	laine-vxb	silverpeak_gms	10.1.153.10	3011	10.1.154.10	60880	ALERT			0.0	3.8M	641M	0.0	1d 1h 34m 1s	tcp	auto_tun_10.1.154.20_to_10.1.153.20
10.0.238.69	laine-vxb	pcanywhere	10.1.153.10	5631	10.1.154.10	52680	OPTIMIZED			14.0	190M	10G 39G	74.1	1d 1h 34m 1s	tcp	auto_tun_10.1.154.20_to_10.1.153.20
10.0.238.69	laine-vxb	pcanywhere	10.1.153.10	5631	10.1.154.10	44603	OPTIMIZED			13.8	190M	10G 39G	74.0	1d 1h 34m 1s	tcp	auto_tun_10.1.154.20_to_10.1.153.20
10.0.238.69	laine-vxb	pcanywhere	10.1.153.10	5631	10.1.154.10	43090	OPTIMIZED			13.5	189M	10G 39G	73.9	1d 1h 34m 1s	tcp	auto_tun_10.1.154.20_to_10.1.153.20
10.0.238.71	laine-vxa	yahoo_games	10.1.153.10	51463	10.1.154.10	11999	OPTIMIZED			89.3	171M	360M 22G	98.4	1d 1h 33m 8s	tcp	auto_tun_10.1.153.20_to_10.1.154.20

Showing 1 to 100 of 136 entries

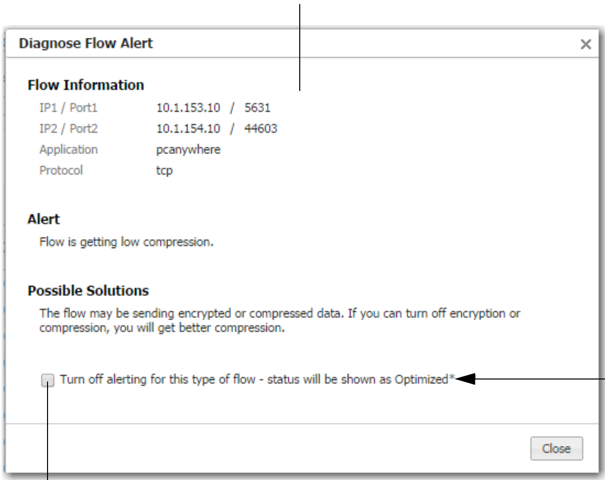
How many entries shown
out of total possible

Details used by Silver Peak
Support for troubleshooting



IP1/Port1 10.1.153.10/5631
IP2/Port2 10.1.154.10/44603

Click **Alert** to
view content



Diagnose Flow Alert

Flow Information

IP1 / Port1 10.1.153.10 / 5631
IP2 / Port2 10.1.154.10 / 44603
Application pcanywhere
Protocol tcp

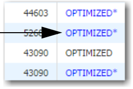
Alert

Flow is getting low compression.

Possible Solutions

The flow may be sending encrypted or compressed data. If you can turn off encryption or compression, you will get better compression.

☐ Turn off alerting for this type of flow - status will be shown as Optimized*



44603	OPTIMIZED*
5268	OPTIMIZED*
43090	OPTIMIZED
43090	OPTIMIZED*

When selected, GMS still registers the alert but changes the status based on user input. OPTIMIZED* also links to the original **Diagnose Flow Alert** dialogue.

The following filters are available:

Parameter or Action	Definition
Flow Categories	The number after each option specifies how many flows fit the criteria • **All** – all flows • **Optimized** – optimized flows • **Optimized*** – these flows originally had a Status of **Alert**, and the user chose to no longer receive Alerts of the same type • Pass-through – includes shaped and unshaped traffic • **Alert** – notifies the user of any issue that might be inhibiting optimization, and offers a possible solution
Bytes Transferred	Choose from **Total** or **Last 5 minutes**.
Flow Started	Choose from **Anytime** or **Last 5 minutes**.
IP1 (2) / **Port1** (2)	The IP address of an endpoint(s) that you want to use as a filter: • Entering a specific endpoint returns flows that have that endpoint. • Entering **0** in any IP address's octet position acts as a wild card for that position. **0** in the **Port** field is also a wild card. • The two IP address (and port) fields are independent of each other. In other words, you can filter on two separate endpoints.
Application	Select which standard or user-defined application (or application group) to use as a filter criteria. The default value is **All**.
Traffic	Select the type of traffic connections you want to retrieve: • **All** – all optimized and pass-through traffic. • **Policy Drop** – traffic with a Set Action of Drop in the Route Policy • **Optimized Traffic** – the sum of all optimized traffic. That is, all tunnelized traffic. • **Pass-through Shaped** – all unoptimized, shaped traffic. • **Pass-through Unshaped** – all unoptimized, unshaped traffic. • **[a named Tunnel]** – that specific tunnel's optimized traffic.
Protocol	Select from the list. The default value is **All**.
VLAN Id	Enter only the integer value for the VLAN Id.
Max Flows	The upper limit depends on what browser you're using.
Reset Flows	Resetting the flow kills it and restarts it. **It is service-affecting.**
Reclassify Flows	Reclassifying the flow is not service-affecting. If a policy change makes a flow stale or inconsistent, then reclassifying makes a best-effort attempt to conform the flow to the change. If the flow can't be successfully "diverted" to this new policy, then an Alert asks if you want to Reset.

Customizing Which Columns Display

Following are some customization guidelines:

- The default set of columns includes the following:

Mgmt IP	Status	Up Time
Host Name	Detail	Protocol
Application	Flow Chart	Outbound Tunnel
IP1	Inbound Reduction %	
PORT1	Inbound Bytes	
IP2	Outbound Bytes	
PORT2	Outbound Reduction %	

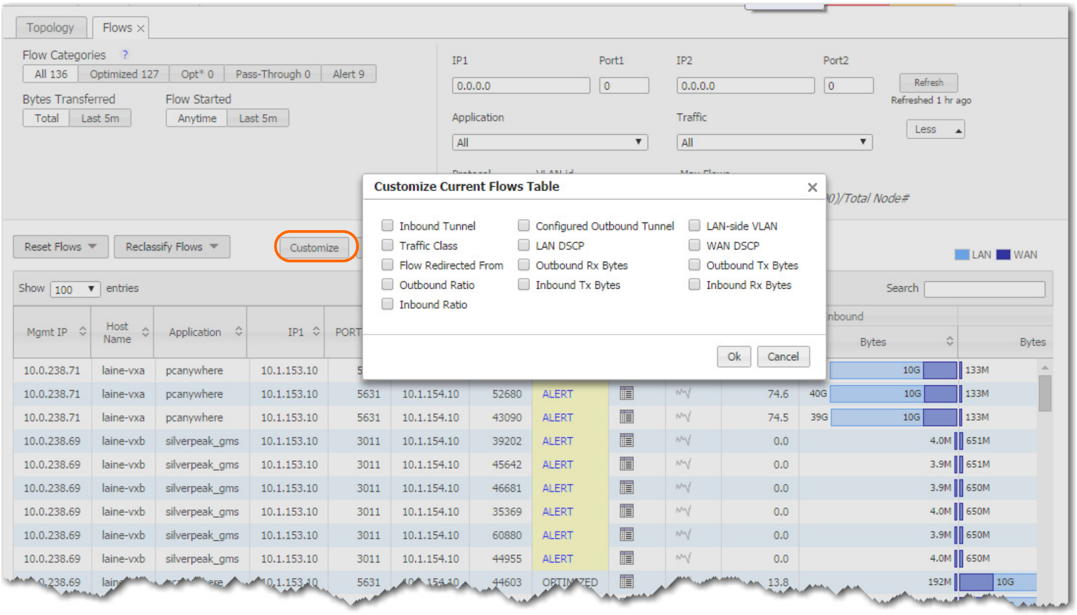
- You can customize by **adding** the following additional columns:

Inbound Tunnel	Configured Outbound Tunnel	LAN-side VLAN
Traffic Class	LAN DSCP	WAN DSCP
Flow Redirected From	Outbound Rx Bytes	Outbound Tx Bytes
Outbound Ratio	Inbound Tx Bytes	Inbound Rx Bytes
Inbound Ratio		

- **Customizations persist** across sessions and across users. For a given appliance, all users see the same columns.
- When you **Export** the data, **all default and possible custom columns are included** in the .csv file.
- **Customize** and **Export** functions are accessible to all users.

To customize the screen display

1 To access the **Customize Current Flows Table**, click **Customize**.



Customize Current Flows Table

□ Inbound Tunnel □ Configured Outbound Tunnel □ LAN-side VLAN
□ Traffic Class □ LAN DSCP □ WAN DSCP
□ Flow Redirected From □ Outbound Rx Bytes □ Outbound Tx Bytes
□ Outbound Ratio □ Inbound Tx Bytes □ Inbound Rx Bytes
□ Inbound Ratio

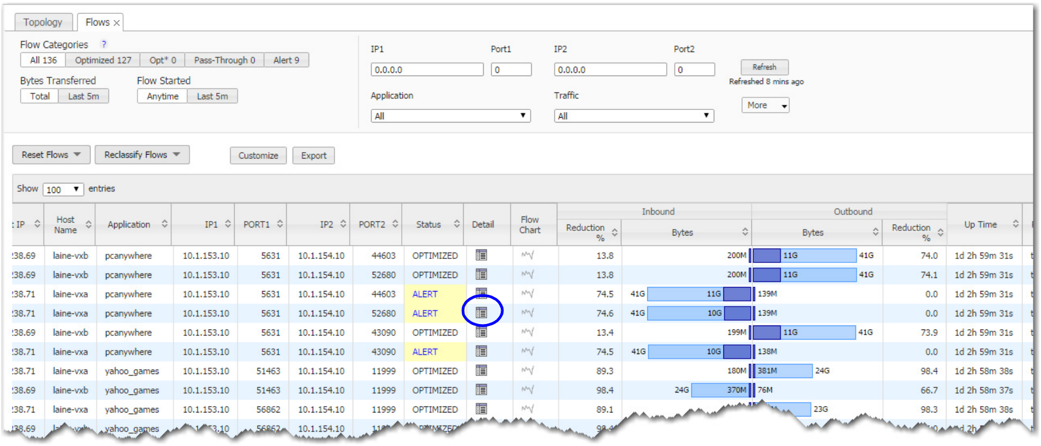
Ok Cancel

Mgmt IP	Host Name	Application	IP1	PORT								Bytes	Bytes
10.0.238.71	laine-vxa	pcanywhere	10.1.153.10	5								10G	133M
10.0.238.71	laine-vxa	pcanywhere	10.1.153.10	5631	10.1.154.10	52680	ALERT			74.6	40G	10G	133M
10.0.238.71	laine-vxa	pcanywhere	10.1.153.10	5631	10.1.154.10	43090	ALERT			74.5	39G	10G	133M
10.0.238.69	laine-vxb	silverpeak_gms	10.1.153.10	3011	10.1.154.10	39202	ALERT			0.0		4.0M	651M
10.0.238.69	laine-vxb	silverpeak_gms	10.1.153.10	3011	10.1.154.10	45642	ALERT			0.0		3.9M	651M
10.0.238.69	laine-vxb	silverpeak_gms	10.1.153.10	3011	10.1.154.10	46681	ALERT			0.0		3.9M	650M
10.0.238.69	laine-vxb	silverpeak_gms	10.1.153.10	3011	10.1.154.10	35369	ALERT			0.0		4.0M	650M
10.0.238.69	laine-vxb	silverpeak_gms	10.1.153.10	3011	10.1.154.10	60880	ALERT			0.0		3.9M	650M
10.0.238.69	laine-vxb	silverpeak_gms	10.1.153.10	3011	10.1.154.10	44955	ALERT			0.0		4.0M	650M
10.0.238.69	lain		10.1.153.10	5631	10.1.154.10	44603	OPTIMIZED			13.8		192M	10G

2 Select additional columns, and click **OK**. The columns append to the right side of the table.

Current Flow Details

Silver Peak Support uses the **Flow Detail** page for troubleshooting.



Topology | Flows ×

Flow Categories ?
All 136 | Optimized 127 | Opt* 0 | Pass-Through 0 | Alert 9

Bytes Transferred: Total | Last 5m
Flow Started: Anytime | Last 5m

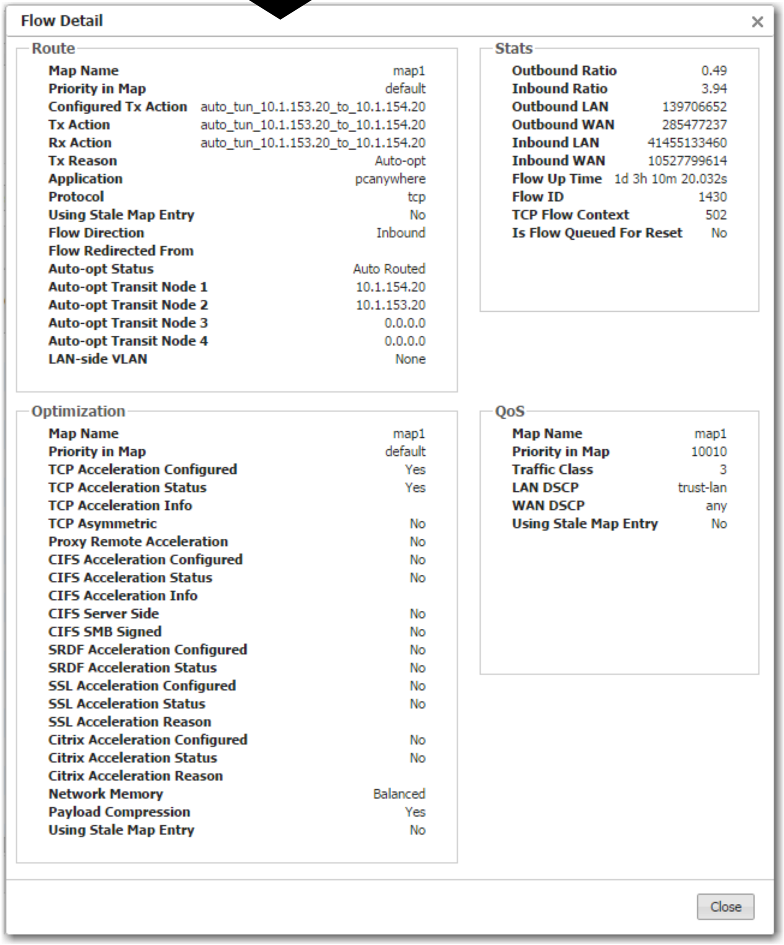
IP1: 0.0.0.0 Port1: 0 IP2: 0.0.0.0 Port2: 0
Application: All Traffic: All
Refresh — Refreshed 8 mins ago
More

Reset Flows | Reclassify Flows | Customize | Export

Show 100 entries

:IP	Host Name	Application	IP1	PORT1	IP2	PORT2	Status	Detail	Flow Chart	Inbound Reduction %	Inbound Bytes	Outbound Bytes	Outbound Reduction %	Up Time
:38.69	laine-vxb	pcanywhere	10.1.153.10	5631	10.1.154.10	44603	OPTIMIZED			13.8	200M	11G 41G	74.0	1d 2h 59m 31s
:38.69	laine-vxb	pcanywhere	10.1.153.10	5631	10.1.154.10	52680	OPTIMIZED			13.8	200M	11G 41G	74.1	1d 2h 59m 31s
:38.71	laine-vxa	pcanywhere	10.1.153.10	5631	10.1.154.10	44603	ALERT			74.5	41G 11G	139M	0.0	1d 2h 59m 31s
:38.71	laine-vxa	pcanywhere	10.1.153.10	5631	10.1.154.10	52680	ALERT			74.6	41G 10G	139M	0.0	1d 2h 59m 31s
:38.69	laine-vxb	pcanywhere	10.1.153.10	5631	10.1.154.10	43090	OPTIMIZED			13.4	199M	11G 41G	73.9	1d 2h 59m 31s
:38.71	laine-vxa	pcanywhere	10.1.153.10	5631	10.1.154.10	43090	ALERT			74.5	41G 10G	138M	0.0	1d 2h 59m 31s
:38.71	laine-vxa	yahoo_games	10.1.153.10	51463	10.1.154.10	11999	OPTIMIZED			89.3	180M	381M 24G	98.4	1d 2h 58m 38s
:38.69	laine-vxb	yahoo_games	10.1.153.10	51463	10.1.154.10	11999	OPTIMIZED			98.4	24G 370M	76M	66.7	1d 2h 58m 37s
:38.71	laine-vxa	yahoo_games	10.1.153.10	56862	10.1.154.10	11999	OPTIMIZED			89.1		23G	98.3	1d 2h 58m 38s

Clicking the icon in the **Details** column displays a detailed flow report.



Flow Detail ×

Route

Map Name	map1
Priority in Map	default
Configured Tx Action	auto_tun_10.1.153.20_to_10.1.154.20
Tx Action	auto_tun_10.1.153.20_to_10.1.154.20
Rx Action	auto_tun_10.1.153.20_to_10.1.154.20
Tx Reason	Auto-opt
Application	pcanywhere
Protocol	tcp
Using Stale Map Entry	No
Flow Direction	Inbound
Flow Redirected From	
Auto-opt Status	Auto Routed
Auto-opt Transit Node 1	10.1.154.20
Auto-opt Transit Node 2	10.1.153.20
Auto-opt Transit Node 3	0.0.0.0
Auto-opt Transit Node 4	0.0.0.0
LAN-side VLAN	None

Stats

Outbound Ratio	0.49
Inbound Ratio	3.94
Outbound LAN	139706652
Outbound WAN	285477237
Inbound LAN	41455133460
Inbound WAN	10527799614
Flow Up Time	1d 3h 10m 20.032s
Flow ID	1430
TCP Flow Context	502
Is Flow Queued For Reset	No

Optimization

Map Name	map1
Priority in Map	default
TCP Acceleration Configured	Yes
TCP Acceleration Status	Yes
TCP Acceleration Info	
TCP Asymmetric	No
Proxy Remote Acceleration	No
CIFS Acceleration Configured	No
CIFS Acceleration Status	No
CIFS Acceleration Info	
CIFS Server Side	No
CIFS SMB Signed	No
SRDF Acceleration Configured	No
SRDF Acceleration Status	No
SSL Acceleration Configured	No
SSL Acceleration Status	No
SSL Acceleration Reason	
Citrix Acceleration Configured	No
Citrix Acceleration Status	No
Citrix Acceleration Reason	
Network Memory	Balanced
Payload Compression	Yes
Using Stale Map Entry	No

QoS

Map Name	map1
Priority in Map	10010
Traffic Class	3
LAN DSCP	trust-lan
WAN DSCP	any
Using Stale Map Entry	No

Close

Most of the information on the **Flow Detail** page exceeds what is included in the **Current Flows** table.

Field	Definition
Route	
Map Name	The name of the Route Policy.
Priority in Map	The number of the entry in the Route Policy that the flow matches.
Configured Tx Action	The SET action configured in the Route Policy's Tunnel field.
Tx Action	How the traffic is actually being transmitted. Usually, this is a tunnel name.
Rx Action	By what path or method the appliance is receiving this flow's traffic.
Tx Reason	Any error associated with packet transmission to the WAN.
Application	Name of the application to which that flow's traffic belongs.
Protocol	The flow's protocol.
Using Stale Map Entry	Whether or not the flow is using a policy entry that has been edited or deleted since the flow began.
Flow Direction	Whether the flow is **Inbound** or **Outbound**.
Flow Redirected From	The IP address of the appliance that's redirecting this flow to this appliance.
Auto-opt Status	Whether it matched a specific Route Policy or was Auto Routed.
Auto-opt Transit Node (1 , 2, 3, 4)	The IP addresses of the hops between this appliance and the other end of the connection.
LAN-side VLAN	Specifies the VLAN tag (1 – 4095) or None.
Optimization	
Map Name	The name of the Optimization Policy.
Priority in Map	The number of the entry in the Optimization Policy that the flow matches.
TCP Acceleration Configured	Whether or not TCP acceleration is configured in the Optimization Policy.
TCP Acceleration Status	Whether TCP is accelerated [Yes] or not [No].
TCP Acceleration Info	The reason that a TCP flow is not accelerated.. For a list of error codes, see *"Error Reasons for TCP Acceleration Failure" on page 127*.
TCP Asymmetric	When the answer is **YES**, the Silver Peak appliance is able to intercept connection establishment in only one direction. As a result, this flow is not accelerated. When this happens, it indicates that there is asymmetric routing in the network.
Proxy Remote Acceleration	Which side is accelerating the flow
CIFS Acceleration Configured	Whether or not CIFS acceleration is configured in the Optimization Policy [Yes/No]
CIFS Acceleration Status	Whether CIFS is accelerated [Yes] or not [No].
CIFS Acceleration Info	The reason that a CIFS flow is not accelerated. For a list of error codes, see *"Error Reasons for CIFS Acceleration Failure" on page 130*
CIFS Server Side	[Yes/No] If **Yes**, then this is the server side and the appliance is not accelerating (only the client side accelerates).

	Field	Definition (Continued)
	CIFS SMB Signed	Specifies whether or not the CIFS traffic is SMB-signed by the server: • **Yes** means it was signed. If that's the case, then the appliance was unable to accelerate any CIFS traffic. • **No** means it wasn't signed. If that's the case, then server requirements did not preclude CIFS acceleration. • **Overridden** means that SMB signing is ON and the appliance overrode it.
	SRDF Acceleration Configured	Whether or not SRDF acceleration is configured in the Optimization Policy [Yes/No]
	SRDF Acceleration Status	Whether SRDF is accelerated [Yes] or not [No].
	SSL Acceleration Configured	Whether or not SSL acceleration is configured in the Optimization Policy [Yes/No]
	SSL Acceleration Status	If a certificate has been appropriately installed via the GMS, then SSL traffic can be deduplicated. Whether SSL is accelerated [Yes] or not [No].
	SSL Acceleration Reason	The reason that an SSL flow is not accelerated. For a list of error codes, see *"Error Reasons for SSL Acceleration Failure" on page 131*
	Citrix Acceleration Configured	Whether or not Citrix cgp (gateway) or ica protocol acceleration is configured in the Optimization Policy [Yes/No]
	Citrix Acceleration Status	Whether Citrix is accelerated [Yes] or not [No].
	Citrix Acceleration Reason	The reason that a Citrix flow is not accelerated.
	Network Memory	There are four Network Memory settings: • **Maximize Reduction** — optimizes for maximum data reduction at the potential cost of slightly lower throughput and/or some increase in latency. It is appropriate for bulk data transfers such as file transfers and FTP where bandwidth savings are the primary concern. • **Minimize Latency** — ensures that no latency is added by Network Memory processing. This may come at the cost of lower data reduction. It is appropriate for extremely latency-sensitive interactive or transactional traffic. It is also appropriate if WAN bandwidth saving is not a primary objective, and instead it is desirable to fully utilize the WAN pipe to increase LAN–side throughput. • **Balanced** — This is the default setting. It dynamically balances latency and data reduction objectives and is the best choice for most traffic types. • **Disabled** — No Network Memory is performed.
	Payload Compression	Whether or not payload compression is turned on.
	Using Stale Map Entry	Whether or not the flow is using a Route Policy entry that has been edited or deleted since the flow began.
Stats Information		
	Outbound Ratio	For the outbound traffic, a ratio of the **Outbound LAN** bytes divided by the **Outbound WAN** bytes. When this ratio is less than 1.0, it's attributable to a fixed overhead (for WAN transmission) being applied to traffic that either is not compressible or consists of few packets.
	Inbound Ratio	For the inbound traffic, a ratio of the **Inbound WAN** bytes divided by the **Inbound LAN** bytes**.**
	Outbound LAN	Total number of bytes received from the LAN [outbound traffic]

Field	Definition (Continued)
Outbound WAN	Total number of bytes sent to the WAN [outbound traffic]
Inbound LAN	Total number of bytes sent to the LAN [inbound traffic]
Inbound WAN	Total number of bytes received from the WAN [inbound traffic]
Flow Up Time	The length of time that there has been a connection between the endpoints.
Flow ID	A unique number that the appliance assigns to the flow.
TCP Flow Context	Silver Peak uses this for debugging purposes.
Is Flow Queued for Reset	Whether the flow is waiting to be reset (after user input) or not.
QoS Information	
Map Name	The name of the QoS Policy.
Priority in Map	The number of the entry in the QoS Policy that the flow matches.
Traffic Class	The number of the traffic class assigned by the QoS to the flow, based on the MATCH conditions satisfied:
LAN DSCP	The LAN DSCP marking that the QoS policy assigned to the flow, based on the MATCH conditions satisfied.
WAN DSCP	The WAN DSCP marking that the QoS policy assigned to the flow, based on the MATCH conditions satisfied.
Using Stale Map Entry	Whether or not the flow is using a policy entry that has been edited or deleted since the flow began.

Error Reasons for TCP Acceleration Failure

Following is a list of possible errors, along with a brief description and possible resolutions.

Error Reason	Description
asymmetric flow	Appliance did not receive a SYN-ACK. **RESOLUTION:** Most likely reason is asymmetric routing.
client advertised zero MSS	Flow is not accelerated because an endpoint did not send the TCP MSS option. **RESOLUTION:** Sometimes older operating systems (like Windows 95) do not send the TCP MSS option. You will have to upgrade the operating system software on the endpoints.
connection reset by peer	During setup, this TCP flow's endpoint(s) reset the connection. **RESOLUTION:** This is a transient condition. If it persists, take a tcpdump for this flow from both the client and server machines and contact Silver Peak Support.
connection to be deleted	Flow is not accelerated due to an internal error. **RESOLUTION:** Contact Silver Peak Support for further help.
disabled in Optimization Map	TCP Acceleration disabled in the Optimization Map. **RESOLUTION:** If you want this flow to be TCP accelerated, enable it in the optimization map.
disabled to allow debug	Flow is not accelerated because it has been disabled by tunbug debug console. **RESOLUTION:** Contact Silver Peak Support for further help.
first packet not a SYN	Appliance did not see the TCP SYN for this flow and therefore could not accelerate it. **RESOLUTION:** This could be due to various reasons: 1. The flow is already established before the appliance sees the first packet for the flow. If so, then resetting the flow will fix the problem. 2. WCCP or PBR is not set up correctly to redirect outbound traffic to the appliance. Check the WCCP or PBR configuration on the router. 3. You have routing issues, so the appliance is not seeing some of the traffic (for example, some packets come to the appliance while others go through another router). If so, you must review and fix your routing. 4. If you are in a cluster of Silver Peak appliances, you may have received a flow redirection timeout. If so, you must investigate why it takes so long for the Silver Peak appliance clusters to communicate with each other.
IP briefly blacklisted	Appliance did not receive a TCP SYN-ACK from remote end within 5 seconds and allowed the flow to proceed unaccelerated. Consequently, the destination IP address has been blacklisted for one minute. **RESOLUTION:** Wait for a minute and then reset the flow. If the problem reappears, the two most likely reasons are: 1) The remote server is slow in responding to TCP connection requests, or 2) a firewall is dropping packets containing Silver Peak TCP options. To check for either of these causes, perform a tcpdump on the server, with the filter set to these IP addresses: • If you don't see a TCP SYN from the client, it is due to firewall or routing issues. • If you notice that SYN-ACK was sent by the server after 5 seconds, it is due to a slow server.

Error Reason	Description (Continued)
keep alive failure	Appliance did not receive a TCP SYN-ACK from the remote end within 5 seconds and allowed the flow to proceed unaccelerated. **RESOLUTION:** Wait for a minute and then reset the flow. If the problem reappears, the two most likely reasons are: 1) The remote server is slow in responding to TCP connection requests, or 2) a firewall is dropping packets containing Silver Peak TCP options. To check for either of these causes, perform a tcpdump on the server, with the filter set to these IP addresses: • If you don't see a TCP SYN from the client, it is due to firewall or routing issues. • If you notice that SYN-ACK was sent by the server after 5 seconds, it is due to a slow server.
no remote appliance detected	Appliance did not receive Silver Peak TCP option in the inbound direction. **RESOLUTION:** This could be due to various reasons: 1. WCCP or PBR is not configured properly on the peer appliance. 2. Silver Peak routing policy not configured properly on the peer appliance. 3. Peer appliance is out of resources. 4. Routing is not configured properly on the router.
out of TCP memory	Appliance is out of resources for accelerating TCP flows. **RESOLUTION:** Contact Silver Peak about upgrading to an appliance with higher flow capacity.
remote appliance dropped out of accel	Flow is not accelerated because Silver Peak flag is not set in TCP header or there was a mismatch in internal settings. **RESOLUTION:** Contact Silver Peak Support for further help.
retransmission timeout	Flow is not accelerated due to TCP protocol timeouts. **RESOLUTION:** This is a transient condition. You can reset the flow and then verify that it gets accelerated. If it does not, then take a tcpdump for this flow from both the client and server machines and contact Silver Peak Support.
Route Map set to drop packets	Flow is not accelerated because the route policy is set to drop packets. **RESOLUTION:** Fix the Set Action in the route policy entry.
Route Map set to pass-through	Flow is not accelerated because the route policy is set to send packets pass-through. **RESOLUTION:** Fix the Set Action in the route policy entry.
software version mismatch	Flow is not accelerated due to software version mismatch between two appliances. **RESOLUTION:** Upgrade software on one or both appliances to the same version of software.
stale flow	Flow is not accelerated due to an internal error. Before the previous flow could terminate cleanly, a new flow began with the same parameters. **RESOLUTION:** Contact Silver Peak Support for further help.
SYN packet fragmented	Flow is not accelerated for unknown reasons. Please contact Silver Peak Support for further help. **RESOLUTION:** Contact Silver Peak Support for further help. You may want to reset the connection to see if the problem resolves.

Error Reason	Description (Continued)
system flow limit reached	Appliance has reached its limit for the total number of flows that can be accelerated. **RESOLUTION:** Contact Silver Peak about upgrading to an appliance with higher flow capacity.
tandem SP appliance involved	Appliance saw Silver Peak TCP option in the outbound direction. This implies that another Silver Peak appliance precedes this one and is responsible for accelerating this flow. **RESOLUTION:** Check the flow acceleration status on an upstream appliance.
TCP auto-optimization failed	Automatic optimization logic failed to accelerate this flow.These are handled for each auto-opt subcode below: • **TCP auto-optimization failed - NOSPS** Auto-optimization failed because the peer appliance is not participating in automatic TCP acceleration. This can be due to various reasons: 1. Peer appliance is configured to not participate in optimization. 2. WCCP or PBR is not configured properly on the peer side. 3. Routing is not configured properly to send traffic to the peer appliance. • **TCP auto-optimization failed - NOTUNNEL** Auto-optimization failed because there is no tunnel between this appliance and its peer, for two possible reasons: 1) Auto-tunnel is disabled. If so, manually create a tunnel. 2) Auto-tunnel is enabled, but needs time to finish creating the tunnel. If so, wait ~30 seconds for tunnel completion, and then reset this flow. • **TCP auto-optimization failed - INVALID_OPT** This is generally due to an internal error. Contact Silver Peak Support for further help. • **TCP auto-optimization failed - MISC** Contact Silver Peak Support for further help. • **TCP auto-optimization failed - TUNNELDOWN** Automatic optimization failed because the tunnel between this appliance and its peer is down.
TCP state mismatch	Flow is not accelerated due to an internal error. This flow will be automatically reset soon. **RESOLUTION:** This is a transient condition. You can wait for this flow to reset, or you can reset it manually now.
terminated by user	Flow has been reset by the user or automatically reset by the system. **RESOLUTION:** This is a transient condition. The flow is in the process of being reset.
tunnel down	Flow is not accelerated because the tunnel is down. **RESOLUTION:** Investigate why the tunnel is down.
unknown cause	Flow is not accelerated for unknown reasons. **RESOLUTION:** Contact Silver Peak Support for further help. You may want to reset the connection to see if the problem resolves.

Error Reasons for CIFS Acceleration Failure

When there is an acceleration failure, the appliance generates an **Alert** link that you can access from the **Current Flows** page. The **Alert** details the reason and the possible resolution.

Following is a list CIFS reason codes. They use the following format:

- **No [reason]** — The connection is not accelerated, and the "reason string" explains why not.
- **Yes [reason]** — The connection is partially accelerated, and the "reason string" explains why the connection is not fully accelerated.
- **Yes** — The connection is fully accelerated.

Yes/ No	Reason Text	Description
No	**CIFS optimization is disabled in the Optimization Policy**	CIFS is disabled in the optmap.
No	**SMB signing is required by the server**	SMB signing is enforced by the server, and this requirement precludes optimization.
No	**SMB version 2 is enforced by the client**	SMB version 2 protocol is enforced by the client, and this requirement precludes optimization.
No	**The flow limit for CIFS optimization has been exceeded**	Maximum flow limit reach for CIFS optimized flows.
Yes	**Sub-optimal read-write optimization - Non standard server**	Sub-optimal read/write optimization due to non-standard server. For example, Windows XP cannot process more than 10 simultaneous outstanding requests.
Yes	**Metadata optimization disabled - NTNOTIFY failure**	Metadata optimization is disabled due to change notification failure.
Yes	**Metadata optimization disabled - OPEN failure**	Metadata optimization is disabled because proxy cannot open the root share. To resolve, check the root share permissions.
Yes	**Metadata optimization disabled - Unsupported Dialect**	Endpoints are using an unsupported CIFS dialect. To resolve, upgrade the CLIFS client/server.
Yes	**Metadata optimization disabled - Unsupported Server**	Unsupported CIFS server, like UNIX/Samba. To resolve, switch to standard servers like Windows/NetApp..
Yes	**Metadata optimization disabled - Unsupported Client**	Unsupported CIFS client, like UNIX/smbclient. To resolve, switch to standard clients like Windows/Mac.

Error Reasons for SSL Acceleration Failure

When there is an acceleration failure, the appliance generates an **Alert** link that you can access from the **Current Flows** page. The **Alert** details the reason and the possible resolution.

Silver Peak appliances support the following:

- **Protocol versions:** SSLv3, SSLv3.3, TLS1.0, TLS1.1
- **Cipher algorithms:** AES128, AES256, RC4, 3DES
- **Digests:** MD5, SHA1

Following is a list of the reasons you may receive a failure message for SSL acceleration.

If the resolution calls for removing or reinstalling the certificate, refer to *"SSL Certificates Template" on page 38*.

Error Reason	Description
error processing certificate	Failure in processing certificate. **RESOLUTION:** Check the certificate. Possible problems include: • There may be an issue with certificate format. • The certificate doesn't match the one that's installed on the server.
error processing client hello1	Failed to create client hello, protocol error, invalid SSL packet, or internal error **RESOLUTION:** Check the SSL protocols on the client and the server. They must be compatible with what Silver Peak supports. If you find that they're incompatible, you must remove it and install the correct certificate.
error processing client hello2	Unsupported client SSL protocol version or options **RESOLUTION:** Check the SSL protocol on the client and the server. They must be compatible with what Silver Peak supports.
error processing client hello3	Invalid random number in SSLv2 client hello, protocol error, invalid SSL packet, or internal error **RESOLUTION:** Check the SSL protocol on the client and the server. They must be compatible with what Silver Peak supports.
error processing SAN certificate	Error while processing SAN certificate. **RESOLUTION:** Check the Subject Alternate Name fields in the SAN certificate. It may be an issue with SAN certificate format or with the certificate not matching the one that's installed on the server. If it's incorrect, you must remove it, and install the correct certificate.
error processing server hello	Error while processing server hello **RESOLUTION:** Contact Silver Peak Support for assistance.
extension parse error	TLS extension parse error, due to unknown TLS extensions **RESOLUTION:** 1. Check the appliance syslog messages (that correspond to the client IP address) for SSL errors to determine which TLS extension is not supported. 2. Disable this (these) extensions in the client-side application's SSL settings. Typically, this application would be your browser.
invalid certificate	SSL certificate is invalid or has expired. **RESOLUTION:** Remove the certificate, and reinstall the correct certificate.

Error Reason	Description (Continued)
invalid client cipher	Client negotiated unsupported cipher algorithm **RESOLUTION:** Check the client-side application's SSL cipher algorithm settings to verify that they're compatible with what Silver Peak supports.
invalid client proto version	Client negotiated unsupported SSL protocol version. **RESOLUTION:** Check the client-side application's SSL protocol settings to verify that they're compatible with what Silver Peak supports.
invalid handshake condition	Received invalid SSL packet or unsupported SSLv2 session resume request during handshake **RESOLUTION:** Contact Silver Peak Support for assistance.
invalid key	SSL private key is invalid **RESOLUTION:** Check that the private key file that was installed is correct and matches the server's private key.
invalid server cipher	Server negotiated unsupported cipher algorithm **RESOLUTION:** Check the SSL server's cipher algorithm settings.
invalid server proto version	Server negotiated unsupported SSL version **RESOLUTION:** Check the server-side application's SSL protocol settings to verify that they're compatible with what Silver Peak supports.
memory flow control	The appliance SSL memory is full and cannot accelerate additional flows. **RESOLUTION:** Contact Silver Peak support for assistance.
miscellaneous error	Generic proxy layer internal error **RESOLUTION:** Contact Silver Peak Support for assistance.
missing active session	Active session not found, cannot accelerate the SSL session. The appliance did not participate in the full handshake phase where the certificate information was exchanged between the client and the server. Or, the certificate was missing or did not match the server's certificate. **RESOLUTION:** If the certificate is missing, install the correct one. Otherwise, restart the client SSL application.
missing certificate	A matching SSL certificate was not found. **RESOLUTION:** Install the certificate on both appliances.
missing key	A matching SSL key was not found. **RESOLUTION:** Install the correct certificate and key.
missing pending session	Pending session not found, possible failure in client hello. **RESOLUTION:** Contact Silver Peak Support for assistance.
missing resume session	Do not have a session to resume in session cache.The session in Silver Peak's cache might have expired. **RESOLUTION:** To get full SSL acceleration, restart the application.
missing SAN certificate	Did not find a matching SAN certificate. **RESOLUTION:** Install the missing SAN certificate.
no ipsec on tunnel	IPsec is not configured on the tunnel. **RESOLUTION:** Configure IPsec on the tunnel.
possibly no certs installed	Possibly no SSL certificate installed. **RESOLUTION:** If the GMS shows no SSL certificate, install an appropriate one.

Error Reason	Description (Continued)
server-side advertised no dedup	Peer appliance SSL did not optimize the flow. **RESOLUTION:** On the other appliance, access the Current Flows report, and look at the reason code.(In some cases, the code is displayed only on one side).
ssl max flows limit	Exceeded maximum SSL optimized flows limit.
unsupported client cipher	Received unsupported cipher suite in SSLv2 client hello message. **RESOLUTION:** Check the client-side application's SSL cipher algorithm settings to verify that they're compatible with what Silver Peak supports. Check the client-side SSL protocol version settings. Silver Peak does not support SSLv2.
unsupported compress method	Unsupported SSL compression method negotiated.The SSL compression method should be disabled on both the client and the server. **RESOLUTION:** On both the client and the server, disable the SSL compression method.
unsupported extension	Unsupported TLS extension negotiated. **RESOLUTION:** 1. Check the appliance syslog messages (that correspond to the client IP address) for SSL errors to determine which TLS extension is not supported. 2. Disable this (these) extensions in the client-side application's SSL settings. Typically, this application would be your browser.
unsupported server cipher	Received unsupported cipher suite in SSLv2 server hello message. **RESOLUTION:** Check the server-side application's SSL cipher algorithm settings to verify that they're compatible with what Silver Peak supports. Check the server-side SSL protocol version settings. Silver Peak does not support SSLv2.
unsupported server protocol	Unsupported SSL protocol: SSLv2 server hello message not supported. **RESOLUTION:** Check the server-side application's SSL protocol settings to verify that they're compatible with what Silver Peak supports.

Resetting Flows to Improve Performance

In the list of **Alerts**, you can look for the flows that aren’t being accelerated, but ***could*** be. Generally, this means flows that use TCP protocol and are not TCP-accelerated:

- This includes tunnelized TCP traffic that is **not** TCP-accelerated. TCP connections are not accelerated if they already exist when the tunnel comes up or when the appliance reboots.
- Pass-through connections are neither tunnelized nor accelerated if they already exist when a new tunnel is added and/or when an ACL is added or edited.

Unaccelerated TCP flows can be reset to allow them to reconnect at a later time. It is assumed that the connection end-points will re-establish the flows. When these flows are reconnected, the appliance recognizes them as new and accelerates them. Note that the time it takes to reset a flow may vary, depending on the traffic activity.

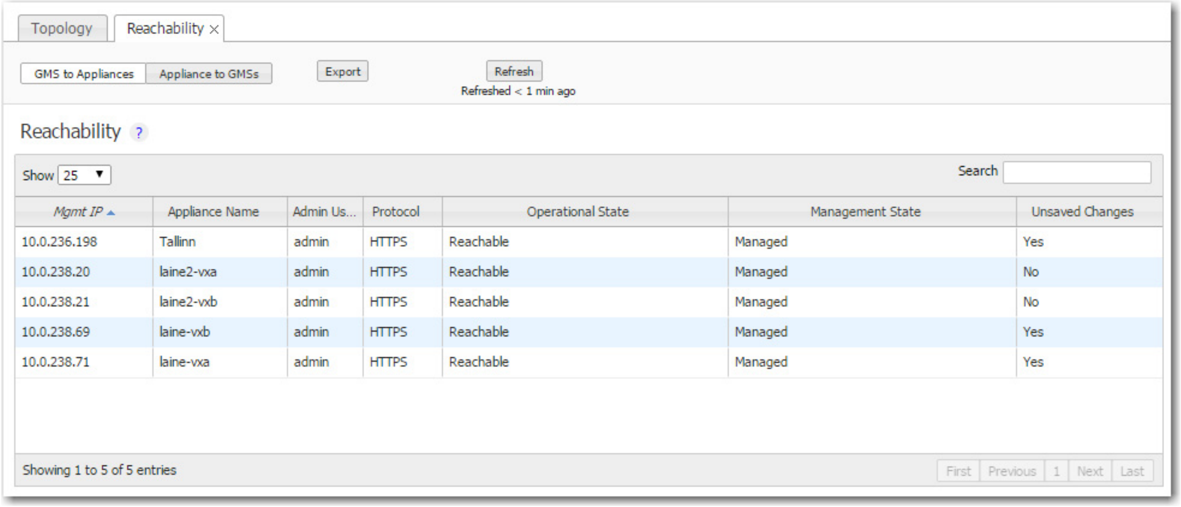
CAUTION **Resetting a flow interrupts service for that flow**. The appliance cannot restore the connection on its own; it relies on the end points to re-establish the flow. Use it only if service interruption can be tolerated for a given flow.

Tip For information about configuring the appliance to automatically reset TCP flows, see the Advanced TCP Options in *“TCP Acceleration Options” on page 27*.

Verifying Reachability

Monitoring > Reachability

This tab summarizes the status of communications in two directions -- ***GMS to Appliance*** and ***Appliance to GMS***.



Mgmt IP ▲	Appliance Name	Admin Us...	Protocol	Operational State	Management State	Unsaved Changes
10.0.236.198	Tallinn	admin	HTTPS	Reachable	Managed	Yes
10.0.238.20	laine2-vxa	admin	HTTPS	Reachable	Managed	No
10.0.238.21	laine2-vxb	admin	HTTPS	Reachable	Managed	No
10.0.238.69	laine-vxb	admin	HTTPS	Reachable	Managed	Yes
10.0.238.71	laine-vxa	admin	HTTPS	Reachable	Managed	Yes

Showing 1 to 5 of 5 entries

GMS to Appliance

- **Admin Username** is the username that a GMS server uses to log into an appliance.
- A GMS can use the web protocols, **HTTP**, **HTTPS**, or **Both** to communicate with an appliance. Although **Both** exists for legacy reasons, Silver Peak recommends using **HTTPS** for maximum security.
- **Operational State** indicates whether an appliance is reachable not.
- An appliance's **Management State** can be Unmanaged, Managed, Maintenance, or Out of Sync. When an appliance is OutOfSync, it first cycles through the Maintenance state before being Managed again. Typically, this is a short cycle.
- **Unreachable** indicates a problem in your network. Check your ports, firewalls, and deployment configuration.

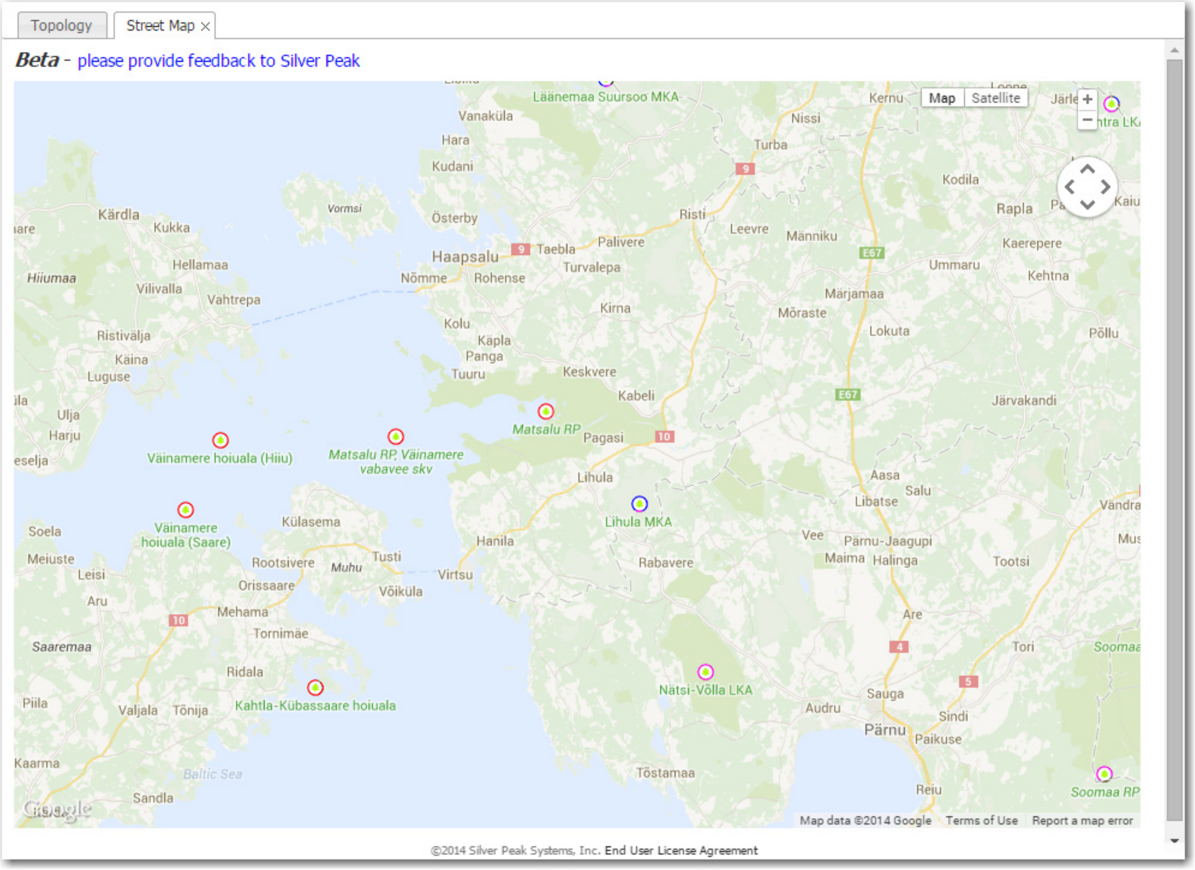
Appliance to GMS

- The table lists the protocols that the appliance uses to communicate with a GMS.
- The possible states are **Reachable**, **In-Progress**, and **Unreachable**.
  - **Unreachable** indicates a problem in your network. Check your ports, firewalls, and deployment configuration.
  - HTTPS and Web Socket share Port 443.

Street Map

Monitoring > Street Map

This **Beta** tab provides the same functionality as the **Topology** tab, albeit with more detailed maps.



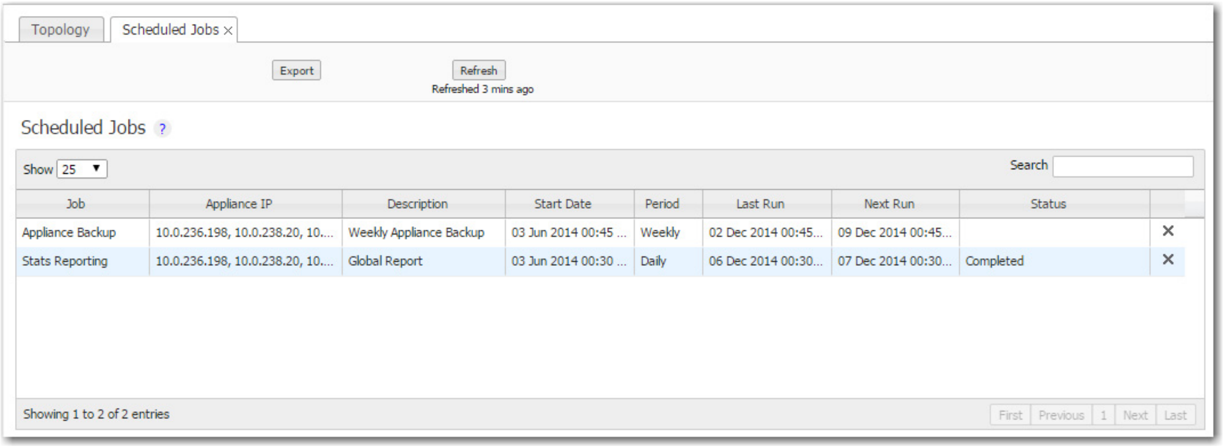
Beta - please provide feedback to Silver Peak

©2014 Silver Peak Systems, Inc. End User License Agreement

Viewing Scheduled Jobs

Monitoring > Scheduled Jobs

This tab provides a central location for viewing and deleting scheduled jobs, such as appliance backup and any custom reports configured for distribution.



Job	Appliance IP	Description	Start Date	Period	Last Run	Next Run	Status	
Appliance Backup	10.0.236.198, 10.0.238.20, 10....	Weekly Appliance Backup	03 Jun 2014 00:45 ...	Weekly	02 Dec 2014 00:45...	09 Dec 2014 00:45...		✕
Stats Reporting	10.0.236.198, 10.0.238.20, 10....	Global Report	03 Jun 2014 00:30 ...	Daily	06 Dec 2014 00:30...	07 Dec 2014 00:30...	Completed	✕

Showing 1 to 2 of 2 entries

CHAPTER 7

GMS Administration

This chapter describes the administrative tasks that directly relate to managing **GMS-related events and tasks only**. These activities do not relate to managing appliances.

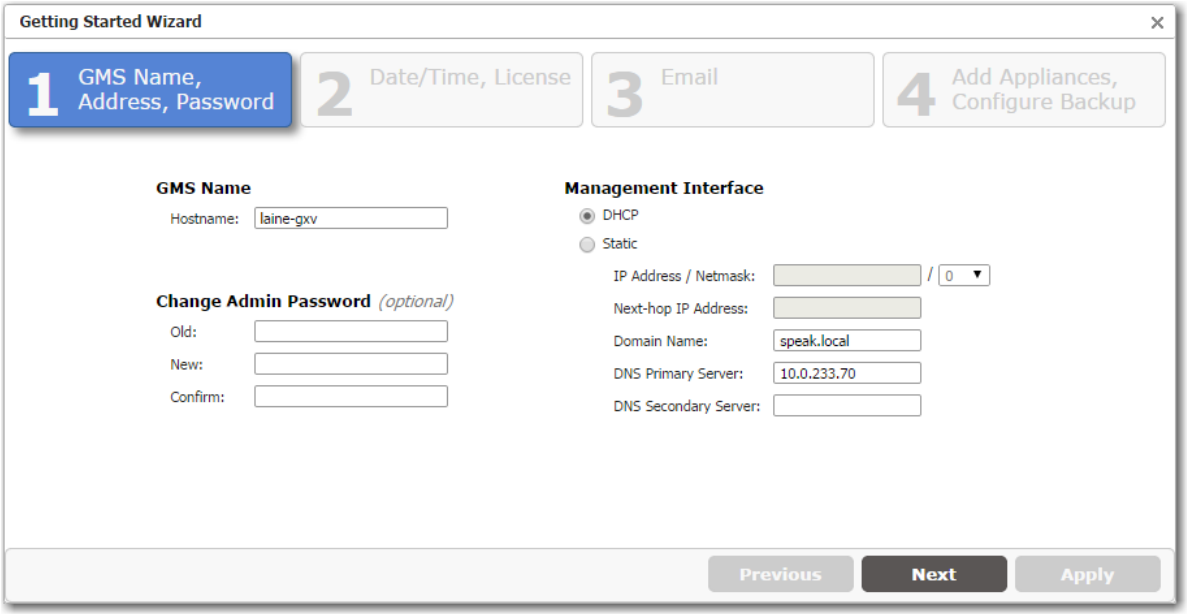
In This Chapter

Getting Started

GMS Administration > Getting Started Wizard

When you first use the web browser to access the GMS server’s IP address, the Getting Started Wizard appears.

After initial configuration, you can always access the Getting Started Wizard from **GMS Administration > Getting Started Wizard**.



GMS Name

Hostname: laine-gxv

Change Admin Password *(optional)*

Old:

New:

Confirm:

Management Interface

● DHCP

○ Static

IP Address / Netmask: / 0 ▼

Next-hop IP Address:

Domain Name: speak.local

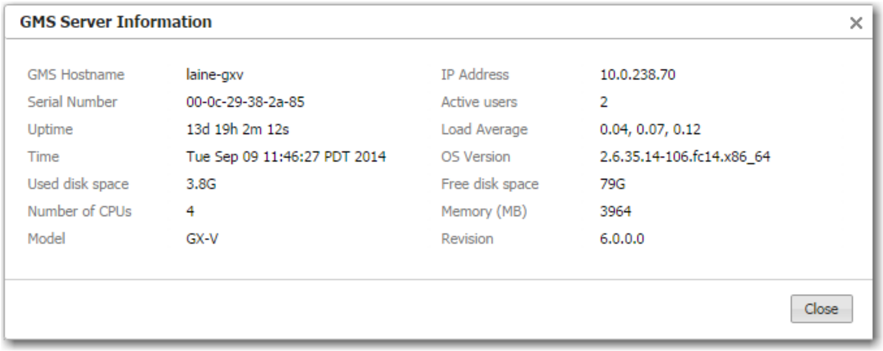
DNS Primary Server: 10.0.233.70

DNS Secondary Server:

Viewing Server Information

GMS Administration > Server Information

This page lists specifications and data specific to this GMS server.



GMS Server Information

GMS Hostname	laine-gxv	IP Address	10.0.238.70
Serial Number	00-0c-29-38-2a-85	Active users	2
Uptime	13d 19h 2m 12s	Load Average	0.04, 0.07, 0.12
Time	Tue Sep 09 11:46:27 PDT 2014	OS Version	2.6.35.14-106.fc14.x86_64
Used disk space	3.8G	Free disk space	79G
Number of CPUs	4	Memory (MB)	3964
Model	GX-V	Revision	6.0.0.0

Restart, Reboot, or Shutdown

GMS Administration > Restart GMS Application

GMS Administration > Reboot Server

GMS Administration > Shutdown Server

The GMS provides these three actions as a convenience, in the **GMS Administration** menu.

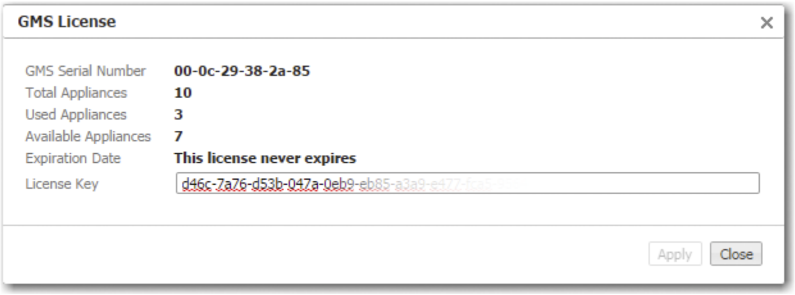
- **Restart Appliance** quickly restarts the GMS software.
- **Reboot GMS Server** is a more thorough restart, accomplished by rebooting the GMS server.
- **Shutdown Server** results in the server being unreachable. You will have to manually power on the server to restart.

Managing the GMS Server License

GMS Administration > License Management

The Silver Peak Global Management System ships with a license to manage 10 appliances.

.



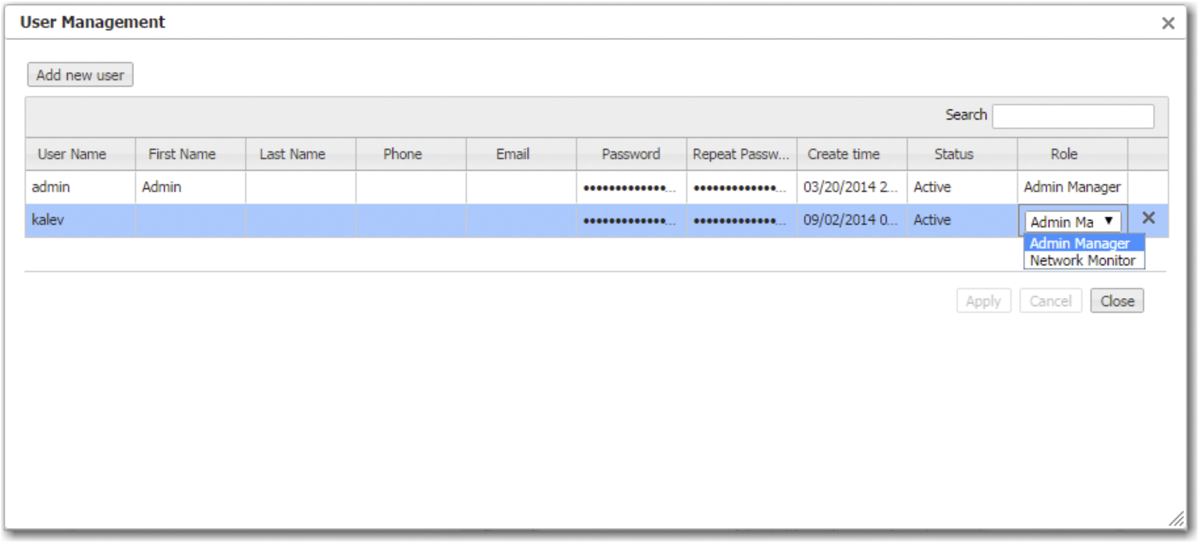
GMS License

GMS Serial Number	**00-0c-29-38-2a-85**
Total Appliances	**10**
Used Appliances	**3**
Available Appliances	**7**
Expiration Date	**This license never expires**
License Key	d46c-7a76-d53b-047a-0eb9-eb85-a3a9-e477-fca5

Managing GMS Users

GMS Administration > User Management

The **User Management** page allows you to manage who has access to the GMS server.



User Name	First Name	Last Name	Phone	Email	Password	Repeat Passw...	Create time	Status	Role
admin	Admin				•••••••••••••...	•••••••••••••...	03/20/2014 2...	Active	Admin Manager
kalev					•••••••••••••...	•••••••••••••...	09/02/2014 0...	Active	Admin Ma

You cannot modify a Username. You must delete it and create a new user.

GMS has two user roles:

- ***Admin Manager*** has all privileges and can see/access all screens. It's the equivalent of ***Superuser.***
- ***Network Monitor*** can view certain configuration, alarm, and report data. They can also troubleshoot network connectivity.

Authorization always maps to one of these.

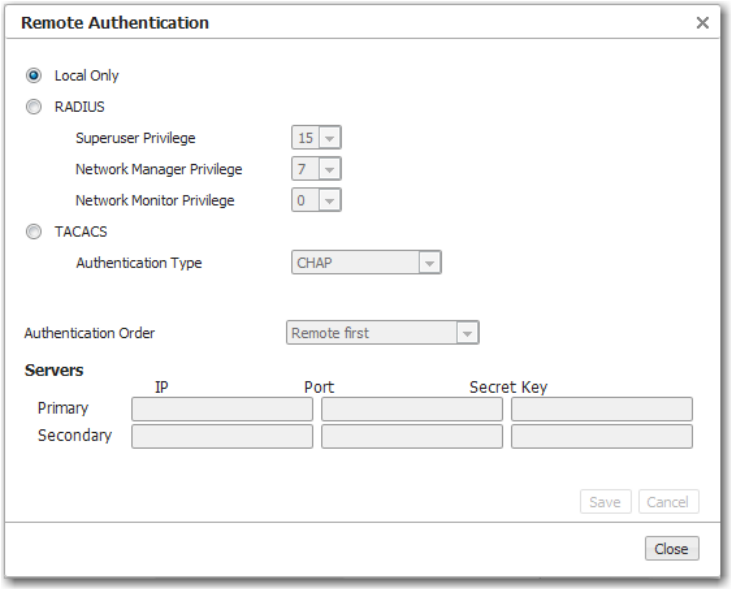
Guidelines for Creating Passwords

- Passwords should be a minimum of 8 characters.
- There should be at least one lower case letter and one upper case letter.
- There should be at least one digit.
- There should be at least one special character.
- Consecutive letters in the password should not be dictionary words.

Remote Authentication

GMS Administration > Authentication

This **Authentication** page specifies how the GMS authenticates GMS users.



Remote Authentication

● Local Only

○ RADIUS

Superuser Privilege 15

Network Manager Privilege 7

Network Monitor Privilege 0

○ TACACS

Authentication Type CHAP

Authentication Order Remote first

Servers

	IP	Port	Secret Key
Primary			
Secondary			

Local Only authenticates based on the users in the GMS database.

To authenticate using RADIUS or TACACS+

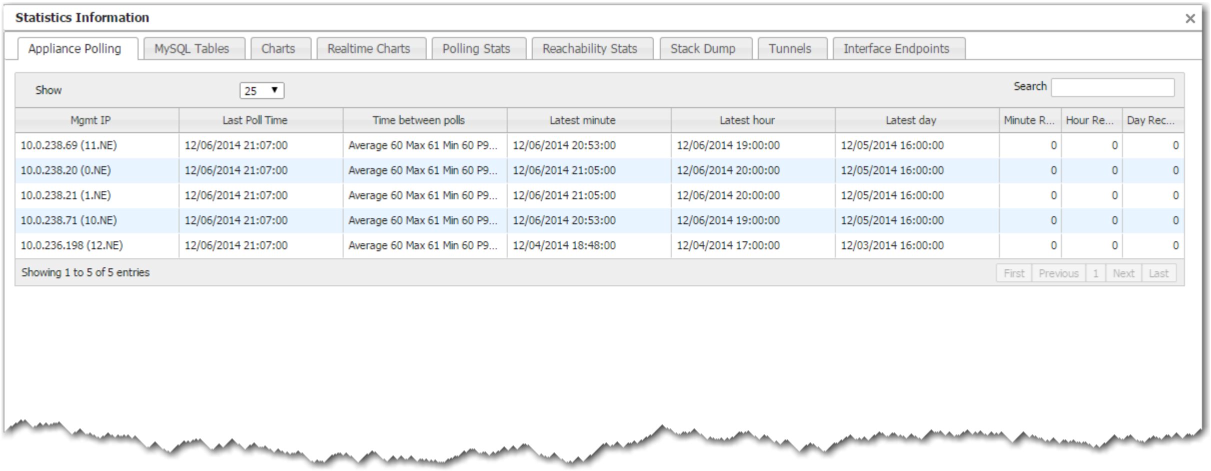
1. Select the access control protocol you want to use.
2. Under **Servers**, enter the information for a Primary server of that type. Entering a Secondary server is optional.

Field	Definition / Purpose
Authentication Order	Whether to use the remote map or the local map first. The default is **Remote first**.
Primary/Secondary Server	The IP address or hostname of the RADIUS or TACACS+ server.
Secret Key	The string defined as the shared secret on the server.
Admin Manager (Superuser) Privilege	These privilege levels must coincide with the values already configured for them at the RADIUS server.
Network Manager Privilege	
Network Monitor Privilege	
Authentication Type	When configuring to use the TACACS+ server, select either **CHAP** or **PAP**, to match what is configured on the TACACS+ server.

Detailed Statistics for Analysis

GMS Administration > Detailed Statistics

As a user, you won’t need to refer to these tabs of statistics. If necessary, Silver Peak’s engineers would be reviewing them in the context of a troubleshooting Webex.



Mgmt IP	Last Poll Time	Time between polls	Latest minute	Latest hour	Latest day	Minute R...	Hour Re...	Day Rec...
10.0.238.69 (11.NE)	12/06/2014 21:07:00	Average 60 Max 61 Min 60 P9...	12/06/2014 20:53:00	12/06/2014 19:00:00	12/05/2014 16:00:00	0	0	0
10.0.238.20 (0.NE)	12/06/2014 21:07:00	Average 60 Max 61 Min 60 P9...	12/06/2014 21:05:00	12/06/2014 20:00:00	12/05/2014 16:00:00	0	0	0
10.0.238.21 (1.NE)	12/06/2014 21:07:00	Average 60 Max 61 Min 60 P9...	12/06/2014 21:05:00	12/06/2014 20:00:00	12/05/2014 16:00:00	0	0	0
10.0.238.71 (10.NE)	12/06/2014 21:07:00	Average 60 Max 61 Min 60 P9...	12/06/2014 20:53:00	12/06/2014 19:00:00	12/05/2014 16:00:00	0	0	0
10.0.236.198 (12.NE)	12/06/2014 21:07:00	Average 60 Max 61 Min 60 P9...	12/04/2014 18:48:00	12/04/2014 17:00:00	12/03/2014 16:00:00	0	0	0

Showing 1 to 5 of 5 entries

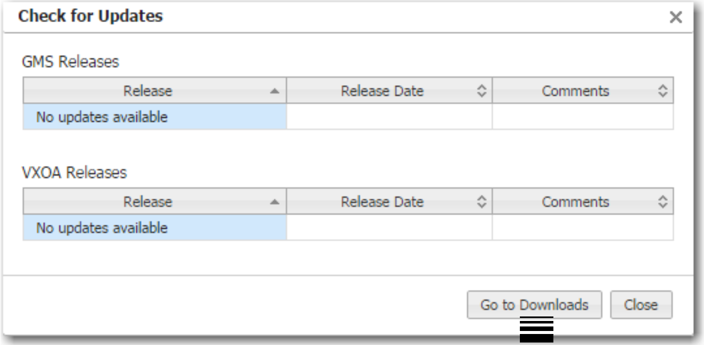
Managing GMS Software

Using these screens, you can check for updated software images, upgrade the GMS server software, and switch to another GMS software partition.

Checking for GMS and Appliance Software Updates

GMS Administration > Check for Updates

Use these screens to see what appliance and GMS server software is available for download.



Check for Updates

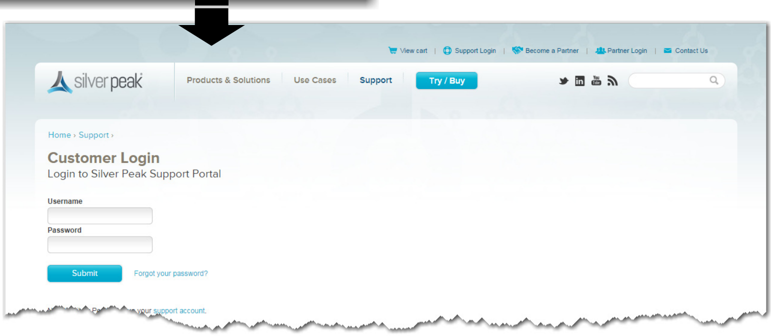
GMS Releases

Release	Release Date	Comments
No updates available		

VXOA Releases

Release	Release Date	Comments
No updates available		

Go to Downloads takes you to the login page of the Support portal.



Customer Login

Login to Silver Peak Support Portal

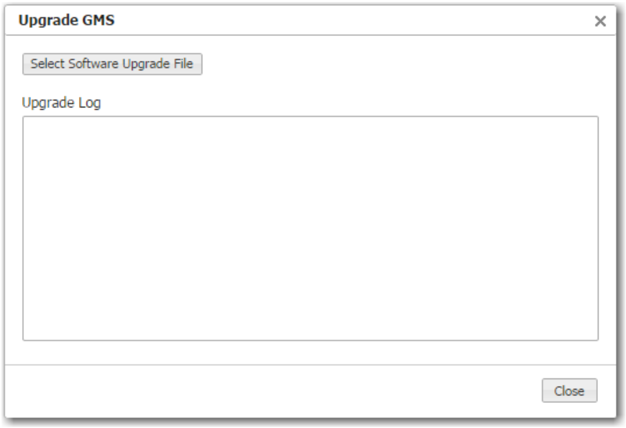
Username

Password

Upgrading GMS Software

GMS Administration > Upgrade GMS Software

Use this screen to navigate to the file and monitor the upgrade progress.

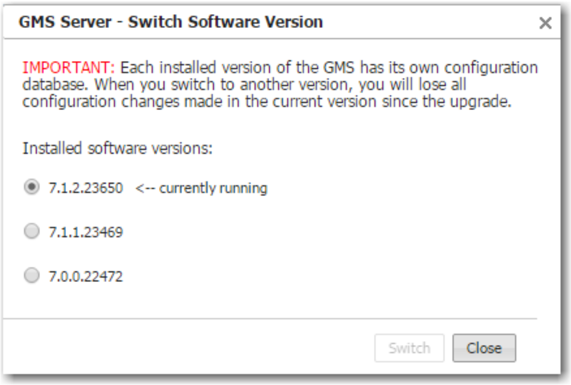


While the GMS software is installing, its management state is **Maintenance**.

Switching Software Versions

GMS Administration > Switch Software Version

Each version of GMS has its own separate database. If you switch to another version, then you only have access to the configuration that existed at the point you upgraded from that version.



GMS Server - Switch Software Version

IMPORTANT: Each installed version of the GMS has its own configuration database. When you switch to another version, you will lose all configuration changes made in the current version since the upgrade.

Installed software versions:

● 7.1.2.23650 <-- currently running

○ 7.1.1.23469

○ 7.0.0.22472

CHAPTER 8

Maintenance and Support

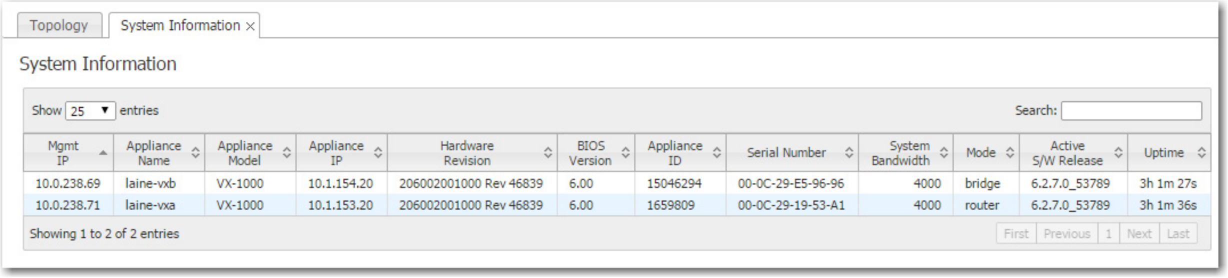
This chapter describes operations related to appliance maintenance and support.

In This Chapter

Viewing System Information

Maintenance > System Information

The **System Information** tab lists the appliances with their relevant information:



System Information

Show 25 entries Search:

Mgmt IP	Appliance Name	Appliance Model	Appliance IP	Hardware Revision	BIOS Version	Appliance ID	Serial Number	System Bandwidth	Mode	Active S/W Release	Uptime
10.0.238.69	laine-vxb	VX-1000	10.1.154.20	206002001000 Rev 46839	6.00	15046294	00-0C-29-E5-96-96	4000	bridge	6.2.7.0_53789	3h 1m 27s
10.0.238.71	laine-vxa	VX-1000	10.1.153.20	206002001000 Rev 46839	6.00	1659809	00-0C-29-19-53-A1	4000	router	6.2.7.0_53789	3h 1m 36s

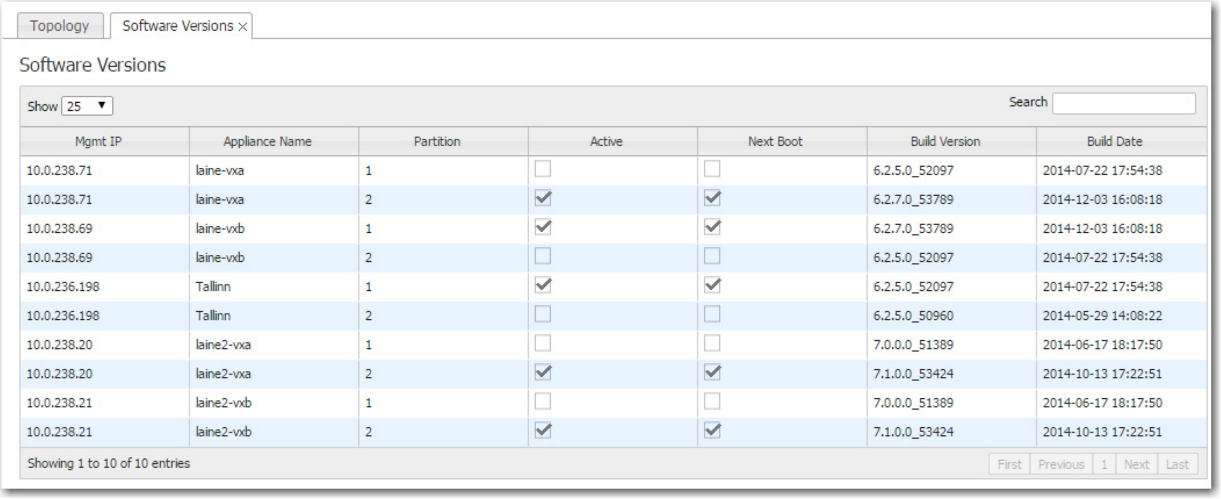
Showing 1 to 2 of 2 entries

- Management IP
- Appliance Name
- Appliance Model
- Appliance IP
- Hardware Revision
- BIOS Version
- Appliance ID
- Serial Number
- System Bandwidth
- Mode
- Active Software Release
- Uptime

Software Versions Tab

Maintenance > Software Versions

The **Software Versions** tab lists the software installed in each appliance’s two partitions.



Software Versions

Show 25 ▼ Search

Mgmt IP	Appliance Name	Partition	Active	Next Boot	Build Version	Build Date
10.0.238.71	laine-vxa	1	□	□	6.2.5.0_52097	2014-07-22 17:54:38
10.0.238.71	laine-vxa	2	☑	☑	6.2.7.0_53789	2014-12-03 16:08:18
10.0.238.69	laine-vxb	1	☑	☑	6.2.7.0_53789	2014-12-03 16:08:18
10.0.238.69	laine-vxb	2	□	□	6.2.5.0_52097	2014-07-22 17:54:38
10.0.236.198	Tallinn	1	☑	☑	6.2.5.0_52097	2014-07-22 17:54:38
10.0.236.198	Tallinn	2	□	□	6.2.5.0_50960	2014-05-29 14:08:22
10.0.238.20	laine2-vxa	1	□	□	7.0.0.0_51389	2014-06-17 18:17:50
10.0.238.20	laine2-vxa	2	☑	☑	7.1.0.0_53424	2014-10-13 17:22:51
10.0.238.21	laine2-vxb	1	□	□	7.0.0.0_51389	2014-06-17 18:17:50
10.0.238.21	laine2-vxb	2	☑	☑	7.1.0.0_53424	2014-10-13 17:22:51

Showing 1 to 10 of 10 entries

Upgrading Appliance Software

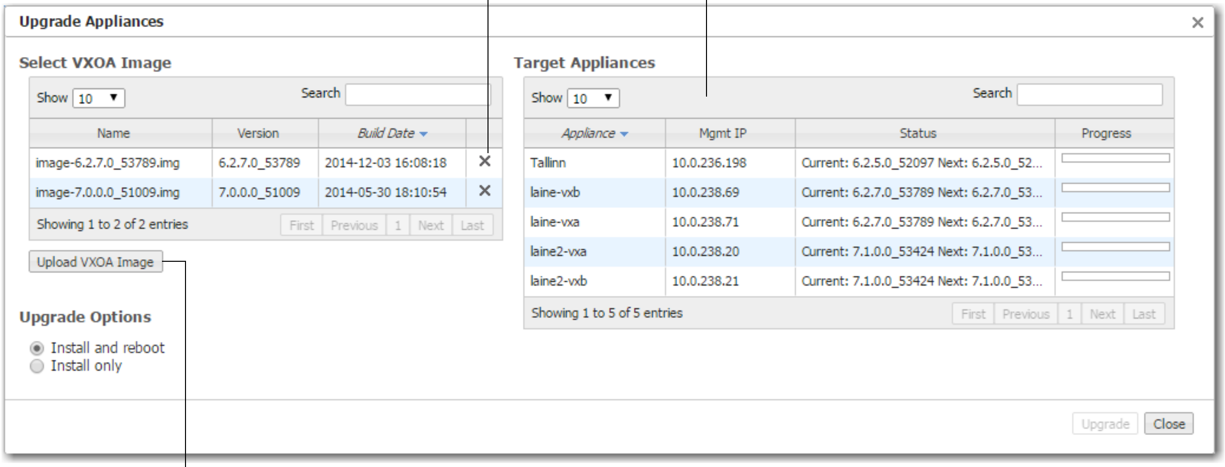
Maintenance > Software Upgrade

You can download and store new appliance software from your network or computer to the GMS server, staging it for installation to the appliance(s).

Use the **Maintenance > Upgrade Appliance Software** page to upload appliance software to the GMS and to install appliance software from the GMS server into the appliance’s inactive partition.

Deletes appliance software from the GMS

Displays the appliances selected before opening this window.



Upgrade Appliances

Select VXOA Image

Show 10 ▼ Search

Name	Version	Build Date	
image-6.2.7.0_53789.img	6.2.7.0_53789	2014-12-03 16:08:18	×
image-7.0.0.0_51009.img	7.0.0.0_51009	2014-05-30 18:10:54	×

Showing 1 to 2 of 2 entries

Upgrade Options

● Install and reboot
○ Install only

Target Appliances

Show 10 ▼ Search

Appliance	Mgmt IP	Status	Progress
Tallinn	10.0.236.198	Current: 6.2.5.0_52097 Next: 6.2.5.0_52...	
laine-vxb	10.0.238.69	Current: 6.2.7.0_53789 Next: 6.2.7.0_53...	
laine-vxa	10.0.238.71	Current: 6.2.7.0_53789 Next: 6.2.7.0_53...	
laine2-vxa	10.0.238.20	Current: 7.1.0.0_53424 Next: 7.1.0.0_53...	
laine2-vxb	10.0.238.21	Current: 7.1.0.0_53424 Next: 7.1.0.0_53...	

Showing 1 to 5 of 5 entries

For adding new appliance software images to the GMS server.

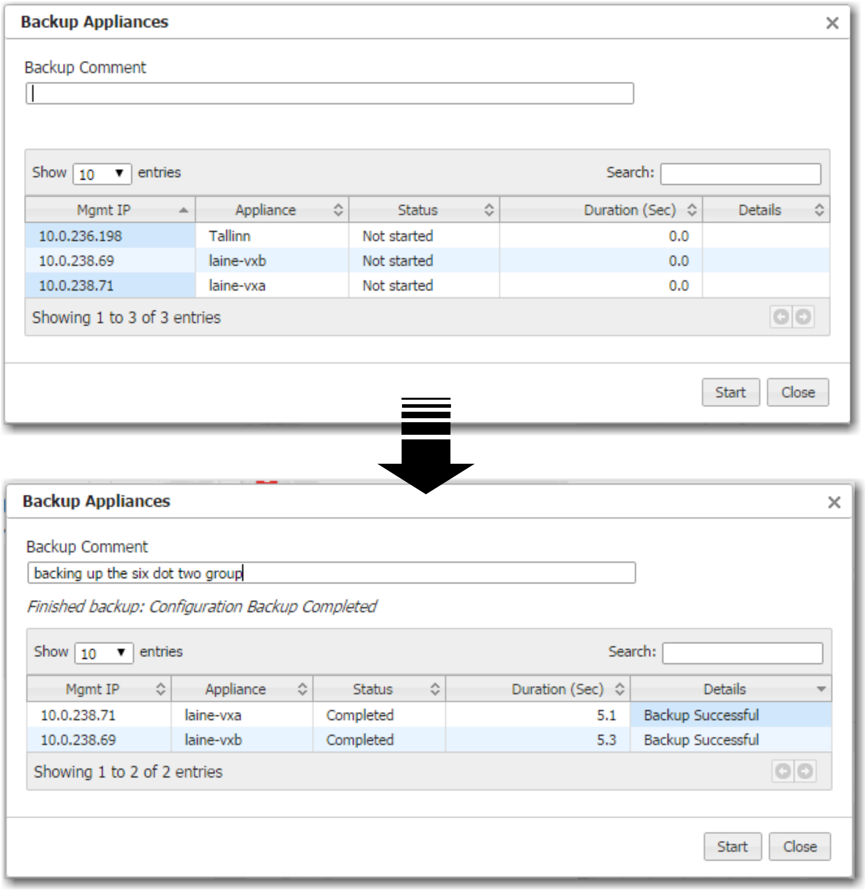
- **Install and reboot** installs the image into the appliance’s inactive partition and then reboots the appliance to begin using the new software.
- **Install only** downloads the image into the inactive partition.

Backing Up Appliance Configuration Files

Maintenance > Backup Now

The Global Management System automatically creates a weekly backup of each appliance's configuration to the GMS server. Additionally, you can create an immediate backup on demand.

After selecting the appliance(s), go to **Maintenance > Backup Now**.



Backup Appliances

Backup Comment:

Show 10 entries   Search:

Mgmt IP	Appliance	Status	Duration (Sec)	Details
10.0.236.198	Tallinn	Not started	0.0	
10.0.238.69	laine-vxb	Not started	0.0	
10.0.238.71	laine-vxa	Not started	0.0	

Showing 1 to 3 of 3 entries

Backup Appliances

Backup Comment: backing up the six dot two group

Finished backup: Configuration Backup Completed

Show 10 entries   Search:

Mgmt IP	Appliance	Status	Duration (Sec)	Details
10.0.238.71	laine-vxa	Completed	5.1	Backup Successful
10.0.238.69	laine-vxb	Completed	5.3	Backup Successful

Showing 1 to 2 of 2 entries

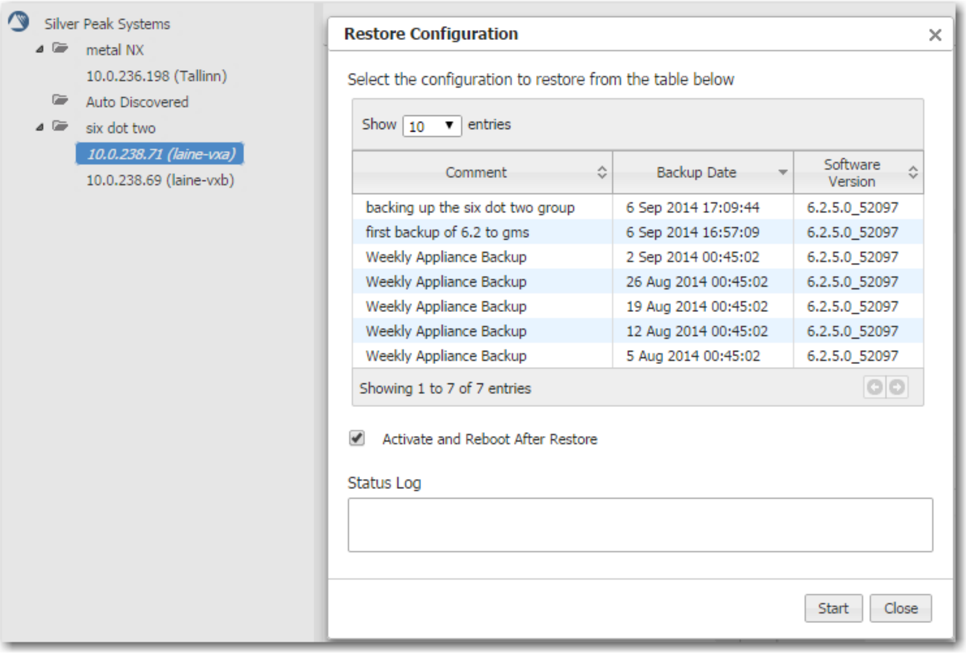
You cannot delete an appliance backup from the GMS.

Restoring a Backup to an Appliance

Maintenance > Restore

- You can restore a configuration backup from the GMS to an individual appliance.
- You **cannot** restore an appliance's backup to a different appliance.

After selecting the appliance, go to **Maintenance > Restore**. Only that appliance's backups display in the table.



Select the configuration to restore from the table below

Show 10 entries

Comment	Backup Date	Software Version
backing up the six dot two group	6 Sep 2014 17:09:44	6.2.5.0_52097
first backup of 6.2 to gms	6 Sep 2014 16:57:09	6.2.5.0_52097
Weekly Appliance Backup	2 Sep 2014 00:45:02	6.2.5.0_52097
Weekly Appliance Backup	26 Aug 2014 00:45:02	6.2.5.0_52097
Weekly Appliance Backup	19 Aug 2014 00:45:02	6.2.5.0_52097
Weekly Appliance Backup	12 Aug 2014 00:45:02	6.2.5.0_52097
Weekly Appliance Backup	5 Aug 2014 00:45:02	6.2.5.0_52097

Showing 1 to 7 of 7 entries

☑ Activate and Reboot After Restore

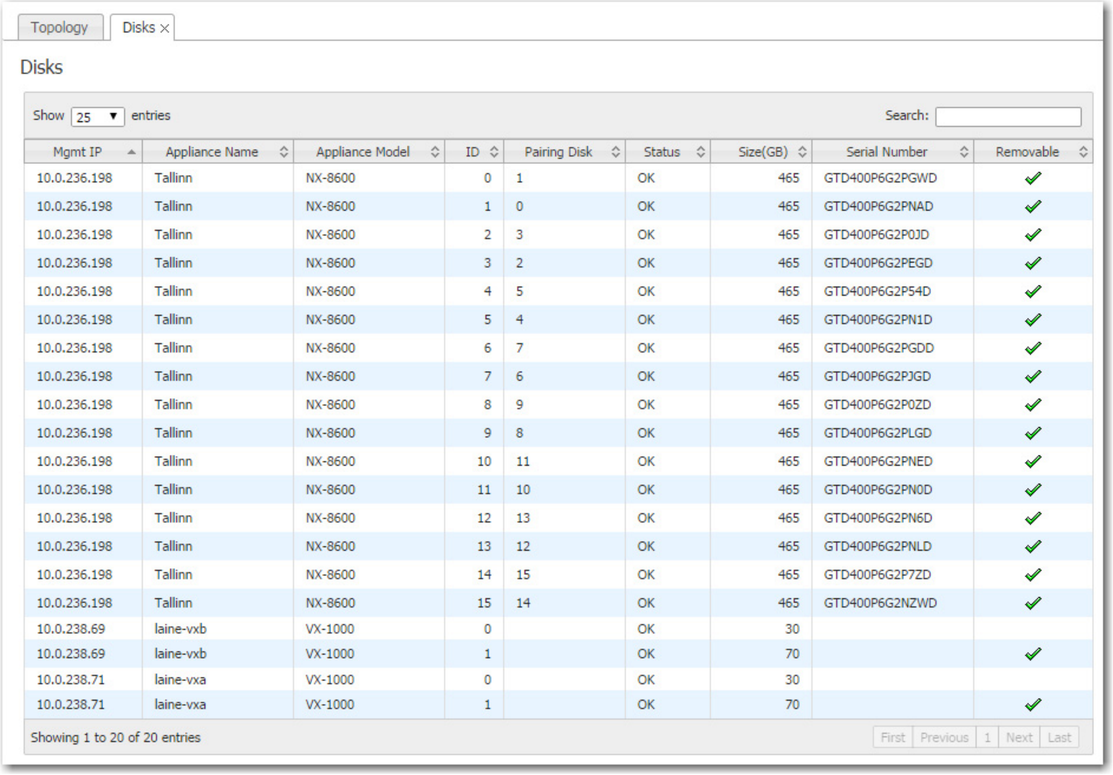
Status Log

Disk Management

Maintenance > Disk Management

The appliances use RAID arrays with encrypted disks.

Disk failure results in a **critical alarm**.



Mgmt IP	Appliance Name	Appliance Model	ID	Pairing Disk	Status	Size(GB)	Serial Number	Removable
10.0.236.198	Tallinn	NX-8600	0	1	OK	465	GTD400P6G2PGWD	✓
10.0.236.198	Tallinn	NX-8600	1	0	OK	465	GTD400P6G2PNAD	✓
10.0.236.198	Tallinn	NX-8600	2	3	OK	465	GTD400P6G2P0JD	✓
10.0.236.198	Tallinn	NX-8600	3	2	OK	465	GTD400P6G2PEGD	✓
10.0.236.198	Tallinn	NX-8600	4	5	OK	465	GTD400P6G2P54D	✓
10.0.236.198	Tallinn	NX-8600	5	4	OK	465	GTD400P6G2PN1D	✓
10.0.236.198	Tallinn	NX-8600	6	7	OK	465	GTD400P6G2PGDD	✓
10.0.236.198	Tallinn	NX-8600	7	6	OK	465	GTD400P6G2PJGD	✓
10.0.236.198	Tallinn	NX-8600	8	9	OK	465	GTD400P6G2P0ZD	✓
10.0.236.198	Tallinn	NX-8600	9	8	OK	465	GTD400P6G2PLGD	✓
10.0.236.198	Tallinn	NX-8600	10	11	OK	465	GTD400P6G2PNED	✓
10.0.236.198	Tallinn	NX-8600	11	10	OK	465	GTD400P6G2PN0D	✓
10.0.236.198	Tallinn	NX-8600	12	13	OK	465	GTD400P6G2PN6D	✓
10.0.236.198	Tallinn	NX-8600	13	12	OK	465	GTD400P6G2PNLD	✓
10.0.236.198	Tallinn	NX-8600	14	15	OK	465	GTD400P6G2P7ZD	✓
10.0.236.198	Tallinn	NX-8600	15	14	OK	465	GTD400P6G2NZWD	✓
10.0.238.69	laine-vxb	VX-1000	0		OK	30		
10.0.238.69	laine-vxb	VX-1000	1		OK	70		✓
10.0.238.71	laine-vxa	VX-1000	0		OK	30		
10.0.238.71	laine-vxa	VX-1000	1		OK	70		✓

Showing 1 to 20 of 20 entries

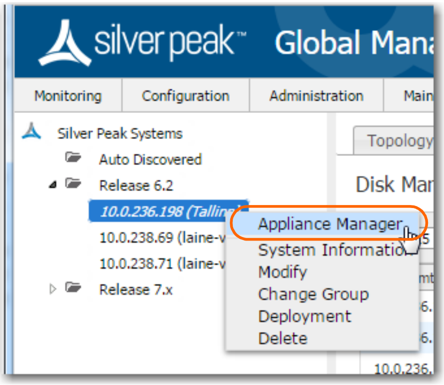
Follow this procedure when replacing a failed disk:

1 Log into your Support portal account, and click Open a Self Service RMA for disk replacement.

2 Complete the wizard, using the serial number of the appliance (not the disk).

3 After you receive the new disk, log into the appliance with Appliance Manager and follow the instructions in the on-line help for disk management in the Maintenance section.

To access Appliance Manager, go to the navigation pane, right-click on the appliance, and select **Appliance Manager**.



Resynching Appliances

Maintenance > Resync

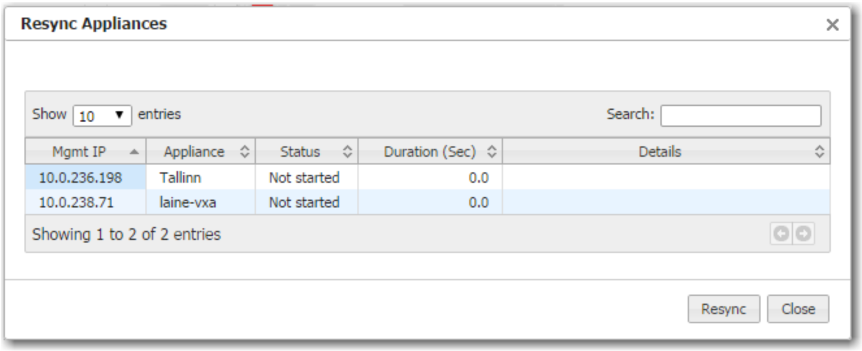
The Global Management System keeps its database synchronized with the appliances' running configurations.

- When you use GMS to make a configuration change to an appliances' running configuration, the appliance responds by sending an **event** back to the GMS server to log, thereby keeping the GMS and appliance in synch.
- Whenever an appliance starts or reboots, the GMS automatically inventories the appliances to resync.
- Whenever the GMS restarts, it automatically resyncs with the appliances.
- When an appliance is in a **Maintenance** or **OutOfSync** management state, the GMS server resyncs with it as it comes back online.

If your overall network experiences problems, then you manually resynch to ensure that the GMS has an appliance's current running configuration.

To manually resync the GMS server with the appliances' configuration database

Select the appliance(s) and choose **Maintenance > Resync**.



Resync Appliances

Show 10 entries Search:

Mgmt IP	Appliance	Status	Duration (Sec)	Details
10.0.236.198	Tallinn	Not started	0.0	
10.0.238.71	laine-vxa	Not started	0.0	

Showing 1 to 2 of 2 entries

Putting the Appliance in System Bypass Mode

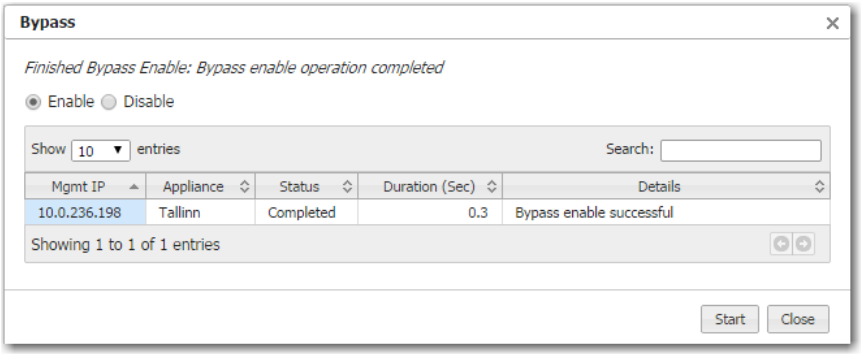
Maintenance > Bypass

This applies only to physical (NX) appliances.

In ***system bypass mode***, the fail-to-wire (or fail-to-glass) card **DOES NOT** receive or process packets:

- In an in-line deployment (Bridge mode), the **lan** interface is physically connected to the **wan** interface.
- In an out-of-path deployment (Router/Server mode), the appliance is in an open-port state.

Fail-to-wire network interfaces mechanically isolate the appliances from the network in the event of a hardware, software, or power failure. This ensures that all traffic bypasses the failed appliance and maximizes up-time.



Bypass

Finished Bypass Enable: Bypass enable operation completed

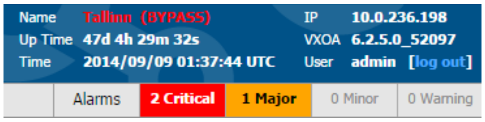
● Enable ○ Disable

Show 10 entries Search:

Mgmt IP	Appliance	Status	Duration (Sec)	Details
10.0.236.198	Tallinn	Completed	0.3	Bypass enable successful

Showing 1 to 1 of 1 entries

When the appliance is in Bypass mode, a message displays in red text at the upper right corner of the user interface.



Name Tallinn (BYPASS) IP 10.0.236.198
Up Time 47d 4h 29m 32s VXOA 6.2.5.0_52097
Time 2014/09/09 01:37:44 UTC User admin [log out]

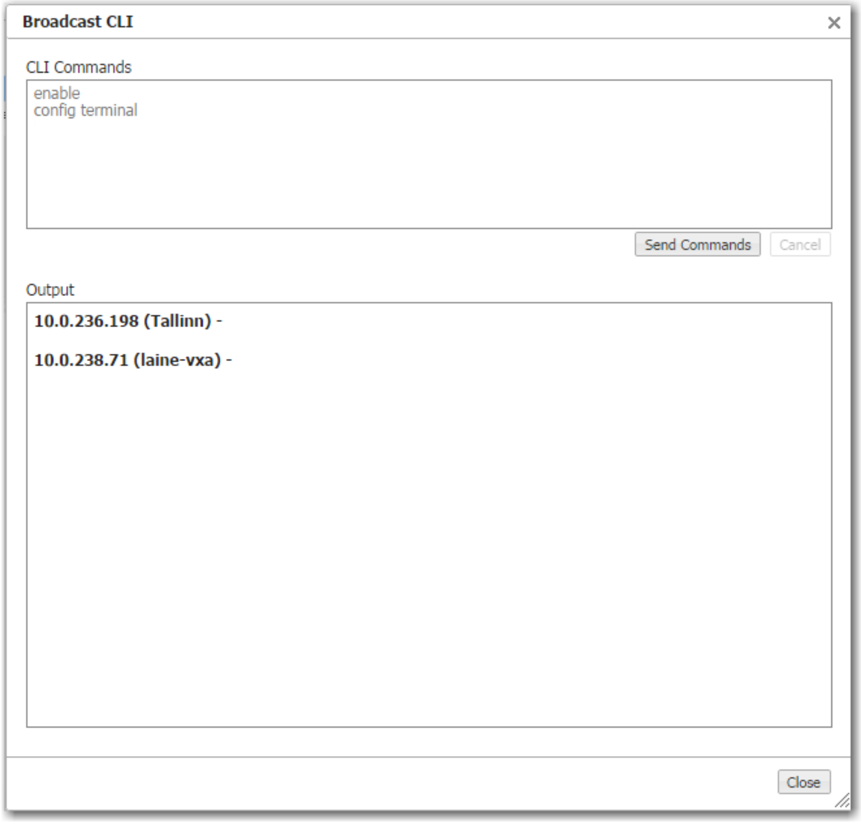
Alarms 2 Critical 1 Major 0 Minor 0 Warning

Broadcasting CLI Commands

Maintenance > Broadcast CLI

You can simultaneously apply CLI (Command Line Interface) commands to multiple, selected appliances.

The window automatically provides you the highest user privilege level.



```
enable
config terminal
```

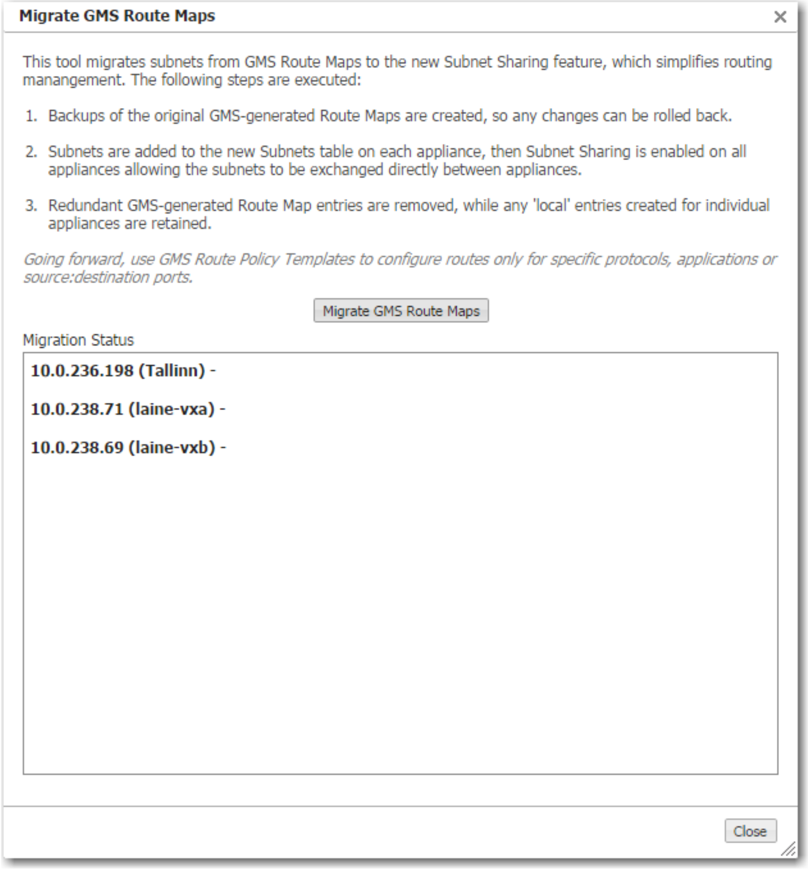
```
10.0.236.198 (Tallinn) -

10.0.238.71 (laine-vxa) -
```

For more information, see the *Silver Peak Command Line Interface Reference Guide*.

Migrating Legacy GMS Route Maps

Maintenance > Migrate GMS Route Maps

For appliances configured with software earlier than VXOA 6.2, this tool migrates subnets from GMS Route Maps to the new subnet sharing feature, which simplifies routing management.



Migrate GMS Route Maps

This tool migrates subnets from GMS Route Maps to the new Subnet Sharing feature, which simplifies routing manangement. The following steps are executed:

1. Backups of the original GMS-generated Route Maps are created, so any changes can be rolled back.
2. Subnets are added to the new Subnets table on each appliance, then Subnet Sharing is enabled on all appliances allowing the subnets to be exchanged directly between appliances.
3. Redundant GMS-generated Route Map entries are removed, while any 'local' entries created for individual appliances are retained.

Going forward, use GMS Route Policy Templates to configure routes only for specific protocols, applications or source:destination ports.

Migration Status

10.0.236.198 (Tallinn) -

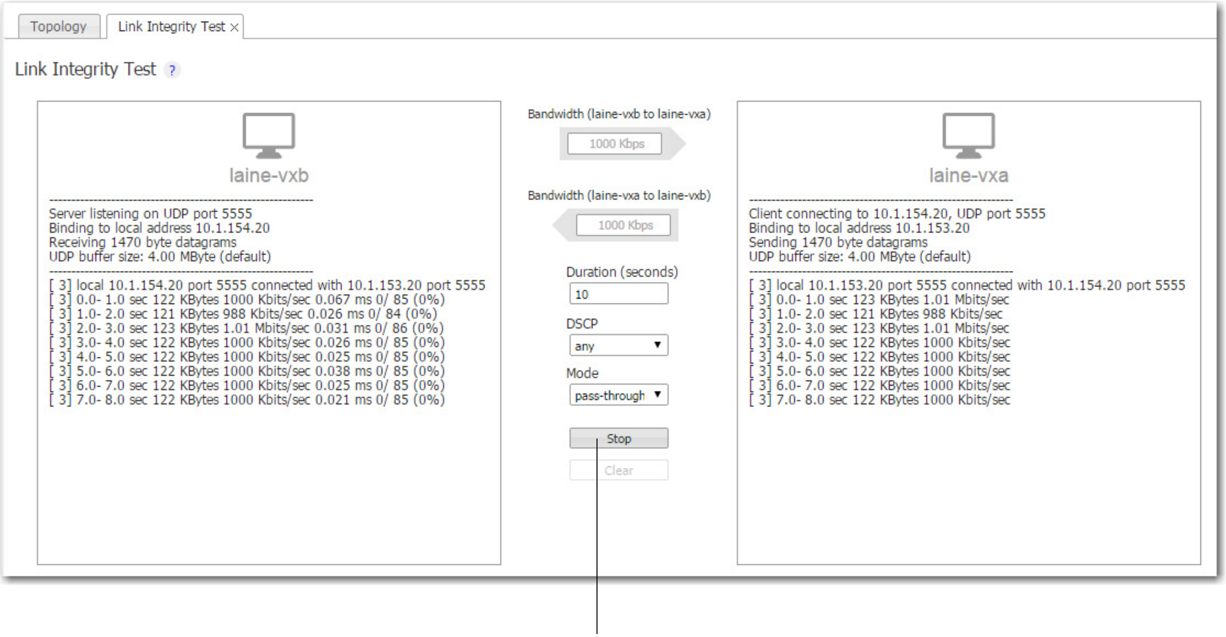
10.0.238.71 (laine-vxa) -

10.0.238.69 (laine-vxb) -

Testing Link Integrity

Maintenance > Link Integrity Test

Used for debugging, the **link integrity** test lets you measure the throughput and integrity (amount of loss) of your WAN link.



laine-vxb

```
------------------------------------------------------------
Server listening on UDP port 5555
Binding to local address 10.1.154.20
Receiving 1470 byte datagrams
UDP buffer size: 4.00 MByte (default)
------------------------------------------------------------
[ 3] local 10.1.154.20 port 5555 connected with 10.1.153.20 port 5555
[ 3] 0.0- 1.0 sec 122 KBytes 1000 Kbits/sec 0.067 ms 0/ 85 (0%)
[ 3] 1.0- 2.0 sec 121 KBytes 988 Kbits/sec 0.026 ms 0/ 84 (0%)
[ 3] 2.0- 3.0 sec 123 KBytes 1.01 Mbits/sec 0.031 ms 0/ 86 (0%)
[ 3] 3.0- 4.0 sec 122 KBytes 1000 Kbits/sec 0.026 ms 0/ 85 (0%)
[ 3] 4.0- 5.0 sec 122 KBytes 1000 Kbits/sec 0.025 ms 0/ 85 (0%)
[ 3] 5.0- 6.0 sec 122 KBytes 1000 Kbits/sec 0.038 ms 0/ 85 (0%)
[ 3] 6.0- 7.0 sec 122 KBytes 1000 Kbits/sec 0.025 ms 0/ 85 (0%)
[ 3] 7.0- 8.0 sec 122 KBytes 1000 Kbits/sec 0.021 ms 0/ 85 (0%)
```

Bandwidth (laine-vxb to laine-vxa): 1000 Kbps

Bandwidth (laine-vxa to laine-vxb): 1000 Kbps

Duration (seconds): 10

DSCP: any

Mode: pass-through

laine-vxa

```
------------------------------------------------------------
Client connecting to 10.1.154.20, UDP port 5555
Binding to local address 10.1.153.20
Sending 1470 byte datagrams
UDP buffer size: 4.00 MByte (default)
------------------------------------------------------------
[ 3] local 10.1.153.20 port 5555 connected with 10.1.154.20 port 5555
[ 3] 0.0- 1.0 sec 123 KBytes 1.01 Mbits/sec
[ 3] 1.0- 2.0 sec 121 KBytes 988 Kbits/sec
[ 3] 2.0- 3.0 sec 123 KBytes 1.01 Mbits/sec
[ 3] 3.0- 4.0 sec 122 KBytes 1000 Kbits/sec
[ 3] 4.0- 5.0 sec 122 KBytes 1000 Kbits/sec
[ 3] 5.0- 6.0 sec 122 KBytes 1000 Kbits/sec
[ 3] 6.0- 7.0 sec 122 KBytes 1000 Kbits/sec
[ 3] 7.0- 8.0 sec 122 KBytes 1000 Kbits/sec
```

The **Start** and **Stop** buttons are colocated.

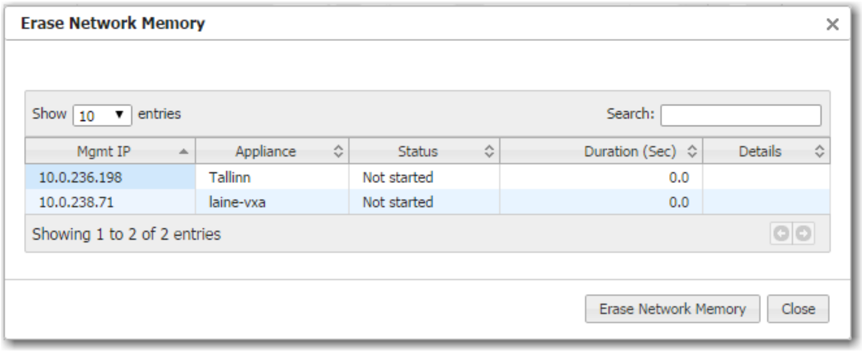
- This test runs **iperf** on the two selected appliances, using user-specified parameters for bandwidth, duration, DSCP marking, and type of traffic (tunnelized / pass-through-shaped / pass-through-unshaped).
- The GMS runs **iperf** twice -- once passing traffic from Appliance A to Appliance B, and the second run passing traffic from Appliance B to Appliance A.

Erasing Network Memory

Maintenance > Erase Network Memory

Erasing Network Memory removes all stored local instances of data.

No reboot required.



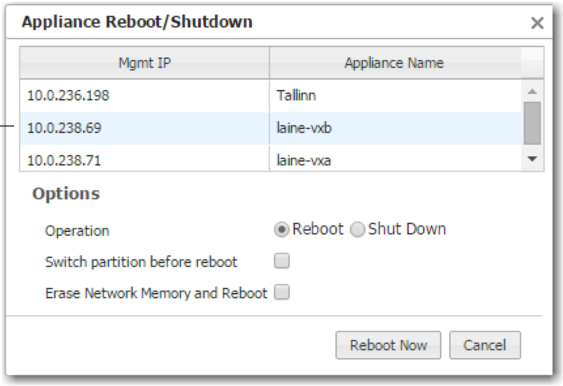
Mgmt IP	Appliance	Status	Duration (Sec)	Details
10.0.236.198	Tallinn	Not started	0.0	
10.0.238.71	laine-vxa	Not started	0.0	

Showing 1 to 2 of 2 entries

Rebooting or Shutting Down an Appliance

Maintenance > Appliance Reboot / Shutdown

The appliance supports three types of reboot:



Displays selected appliances

Appliance Reboot/Shutdown

Mgmt IP	Appliance Name
10.0.236.198	Tallinn
10.0.238.69	laine-vxb
10.0.238.71	laine-vxa

Options

Operation ● Reboot ○ Shut Down

Switch partition before reboot □

Erase Network Memory and Reboot □

- **Reboot**. Reboots the appliance gracefully. This is your typical "vanilla" restart.

  Use case: You're changing the deployment mode or other configuration parameters that require a reboot.

- **Erase Network Memory and Reboot**. Erases the Network Memory cache and reboots the appliance.

  Use case: You need to restart the appliance with an empty Network Memory cache.

- **Shutdown**. Shuts down the appliance and turns the power off. To restart, go to the appliance and physically turn the power on with the Power switch.

  Use case:

  - You're decommissioning the appliance.
  - You need to physically move the appliance to another location.
  - You need to recable the appliance for another type of deployment.

Behavior During Reboot

A ***physical appliance*** enters into one of the following states:

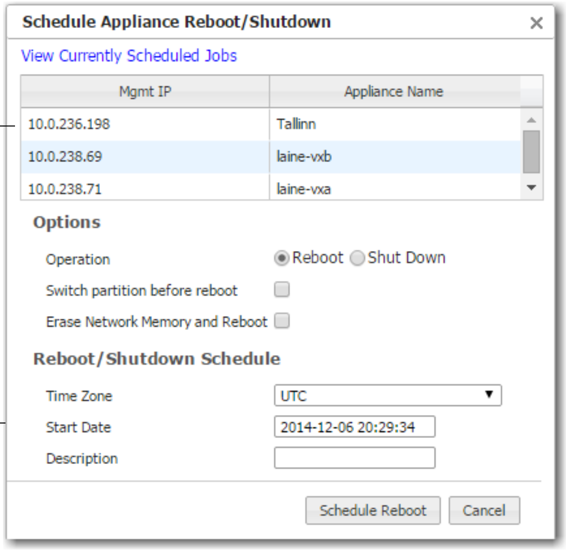
- *hardware bypass*, if deployed in-line (Bridge mode), or
- *an open-port state*, if deployed out-of-path (Router/Server mode).

Unless a ***virtual appliance*** is configured for a high availability deployment, all flows are discontinued during reboot.

Scheduling an Appliance Reboot

Maintenance > Schedule Appliance Reboot

You can schedule an appliance for any of three types of reboot:



Displays selected appliances

Based on GMS's clock

Schedule Appliance Reboot/Shutdown ×

View Currently Scheduled Jobs

Mgmt IP	Appliance Name
10.0.236.198	Tallinn
10.0.238.69	laine-vxb
10.0.238.71	laine-vxa

Options

Operation ● Reboot ○ Shut Down

Switch partition before reboot □

Erase Network Memory and Reboot □

Reboot/Shutdown Schedule

Time Zone UTC ▼

Start Date 2014-12-06 20:29:34

Description

- **Reboot**. Reboots the appliance gracefully. This is your typical "vanilla" restart.

  Use case: You're changing the deployment mode or other configuration parameters that require a reboot.

- **Erase Network Memory and Reboot**. Erases the Network Memory cache and reboots the appliance.

  Use case: You need to restart the appliance with an empty Network Memory cache.

- **Shutdown**. Shuts down the appliance and turns the power off. To restart, go to the appliance and physically turn the power on with the Power switch.

  Use case:

  - You're decommissioning the appliance.
  - You need to physically move the appliance to another location.
  - You need to recable the appliance for another type of deployment.

Behavior During Reboot

A ***physical appliance*** enters into one of the following states:

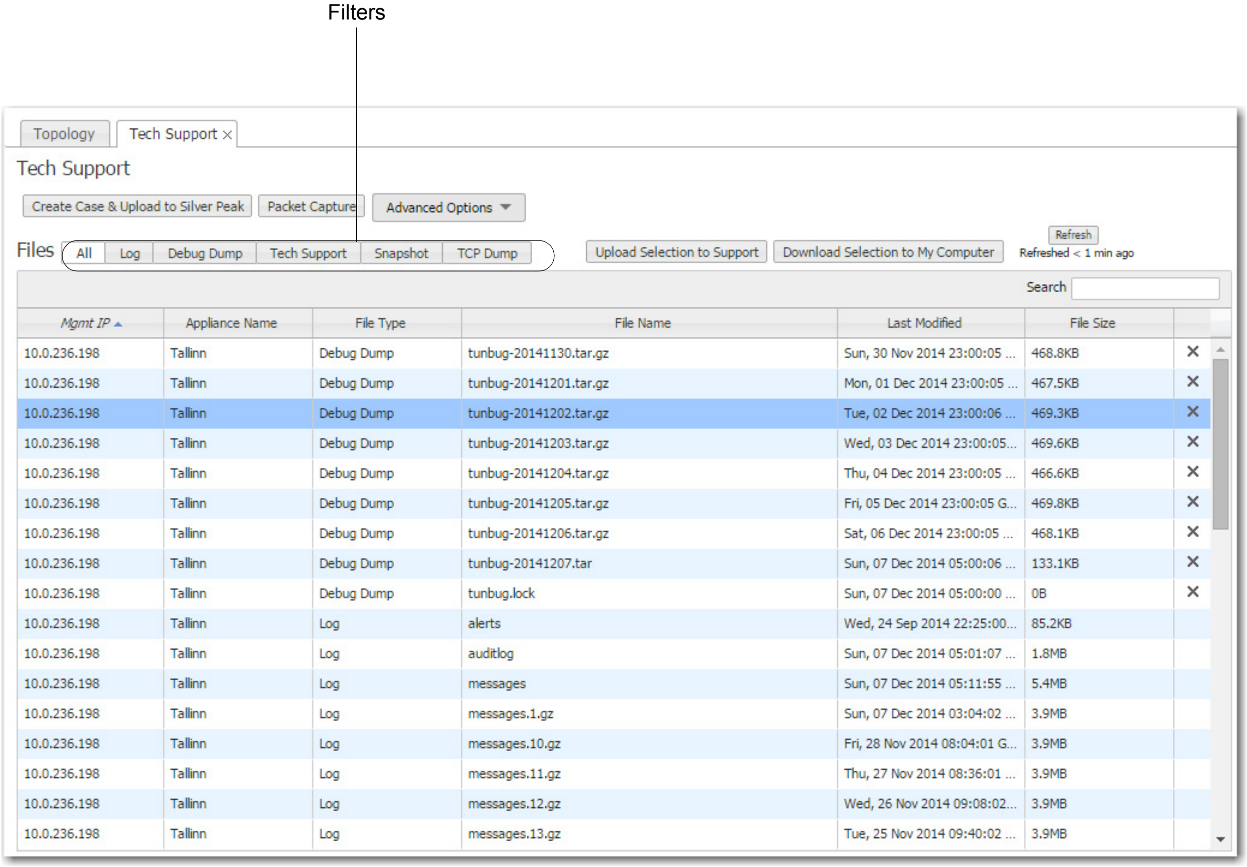
- *hardware bypass*, if deployed in-line (Bridge mode), or
- *an open-port state*, if deployed out-of-path (Router/Server mode).

Unless a ***virtual appliance*** is configured for a high availability deployment, all flows are discontinued during reboot.

Managing Tech Support Files

Support > Tech Support [Create Case, View Logs]

If you have a problem with an appliance, Silver Peak Support may ask you to send them specific debug files for evaluation. Listed under **Help > Tech Support**, these include log files, debug dump files, tech files, snapshots, and tcpdump results.

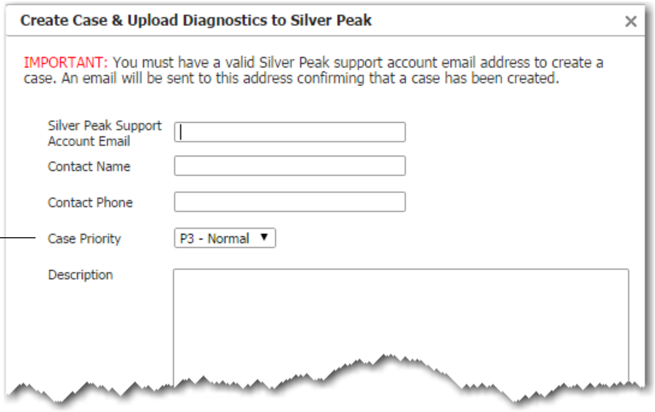


Filters

Mgmt IP ▲	Appliance Name	File Type	File Name	Last Modified	File Size	
10.0.236.198	Tallinn	Debug Dump	tunbug-20141130.tar.gz	Sun, 30 Nov 2014 23:00:05 ...	468.8KB	✕
10.0.236.198	Tallinn	Debug Dump	tunbug-20141201.tar.gz	Mon, 01 Dec 2014 23:00:05 ...	467.5KB	✕
10.0.236.198	Tallinn	Debug Dump	tunbug-20141202.tar.gz	Tue, 02 Dec 2014 23:00:06 ...	469.3KB	✕
10.0.236.198	Tallinn	Debug Dump	tunbug-20141203.tar.gz	Wed, 03 Dec 2014 23:00:05...	469.6KB	✕
10.0.236.198	Tallinn	Debug Dump	tunbug-20141204.tar.gz	Thu, 04 Dec 2014 23:00:05 ...	466.6KB	✕
10.0.236.198	Tallinn	Debug Dump	tunbug-20141205.tar.gz	Fri, 05 Dec 2014 23:00:05 G...	469.8KB	✕
10.0.236.198	Tallinn	Debug Dump	tunbug-20141206.tar.gz	Sat, 06 Dec 2014 23:00:05 ...	468.1KB	✕
10.0.236.198	Tallinn	Debug Dump	tunbug-20141207.tar	Sun, 07 Dec 2014 05:00:06 ...	133.1KB	✕
10.0.236.198	Tallinn	Debug Dump	tunbug.lock	Sun, 07 Dec 2014 05:00:00 ...	0B	✕
10.0.236.198	Tallinn	Log	alerts	Wed, 24 Sep 2014 22:25:00...	85.2KB	
10.0.236.198	Tallinn	Log	auditlog	Sun, 07 Dec 2014 05:01:07 ...	1.8MB	
10.0.236.198	Tallinn	Log	messages	Sun, 07 Dec 2014 05:11:55 ...	5.4MB	
10.0.236.198	Tallinn	Log	messages.1.gz	Sun, 07 Dec 2014 03:04:02 ...	3.9MB	
10.0.236.198	Tallinn	Log	messages.10.gz	Fri, 28 Nov 2014 08:04:01 G...	3.9MB	
10.0.236.198	Tallinn	Log	messages.11.gz	Thu, 27 Nov 2014 08:36:01 ...	3.9MB	
10.0.236.198	Tallinn	Log	messages.12.gz	Wed, 26 Nov 2014 09:08:02...	3.9MB	
10.0.236.198	Tallinn	Log	messages.13.gz	Tue, 25 Nov 2014 09:40:02 ...	3.9MB	

Files you upload to Support must be associated with a Case Number.

- To open a new case, click **Create Case & Upload Diagnostics to Silver Peak**.



Create Case & Upload Diagnostics to Silver Peak

IMPORTANT: You must have a valid Silver Peak support account email address to create a case. An email will be sent to this address confirming that a case has been created.

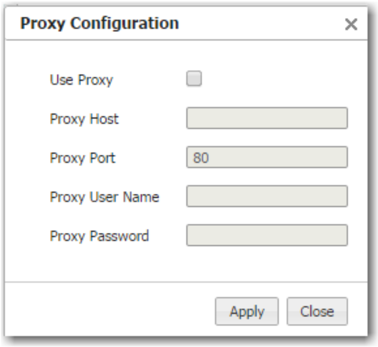
Silver Peak Support Account Email:
Contact Name:
Contact Phone:
Case Priority: P3 - Normal ▾
Description:

The highest priority is **P1**, and the lowest is **P4**.

The default is **P3**.

This requires you to have a valid Silver Peak Support account email address. An email will be sent to this address, confirming that a case has been created and providing you with a Case Number.

- If you already have a Case Number, you'll be asked to enter it when uploading any additionally requested files.
- All debug files are stored on the appliances themselves. From the table, you can download a file to your computer or upload it to Support.
- You can upload a file from your PC to Support, using the **Advanced Options** menu.
- Although GMS logs aren't visible to you in the menus, the **Advanced Options** menu lets you upload GMS logs to Support or download them to your computer.
- If necessary (for example, because of firewall issues), you can configure a proxy for uploading files to Silver Peak Support. Go to **Help > Tech Support > Advanced Options > Proxy Settings.**



Use Proxy □

Proxy Host

Proxy Port 80

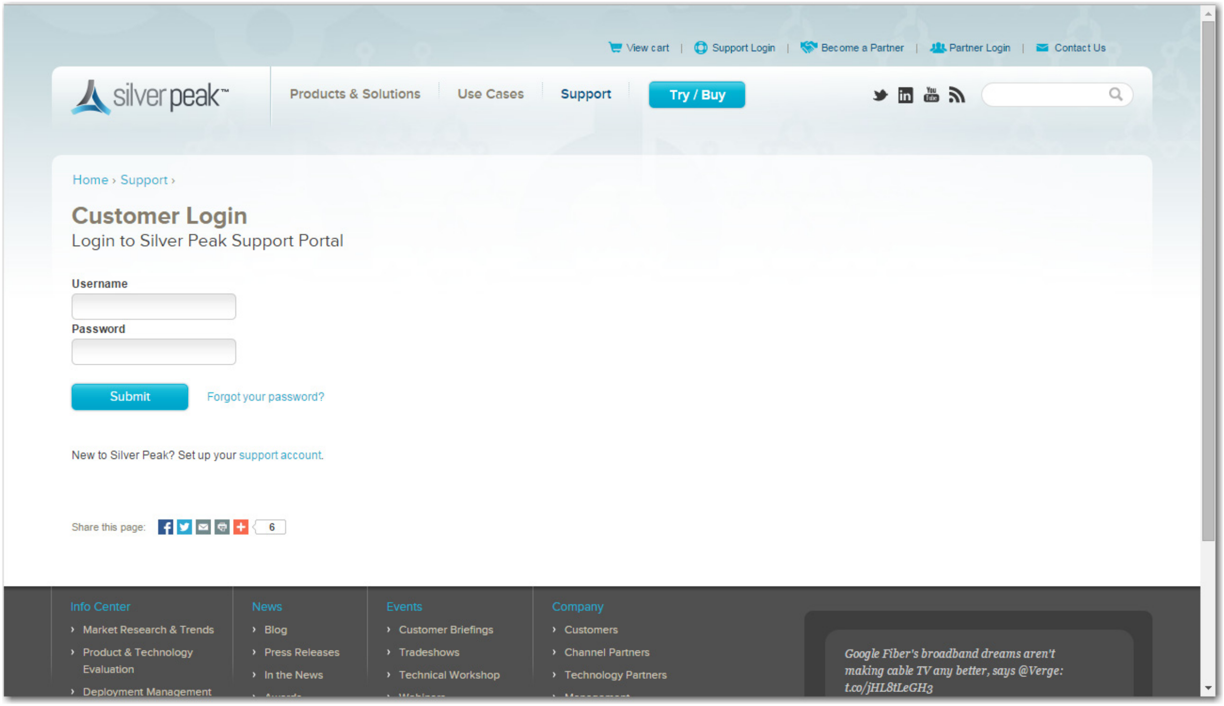
Proxy User Name

Proxy Password

Logging in to the Support Portal

Support > Support Portal Log-in

When you have a Silver Peak account and need technical or customer support, select **Support > Tech Support**. The following page opens in a separate browser tab.



Customer Login

Login to Silver Peak Support Portal

Username

Password

New to Silver Peak? Set up your support account.

Google Fiber's broadband dreams aren't making cable TV any better, says @Verge: t.co/jHL8tLeGH3

You can also access this page directly by going Silver Peak's web page and selecting **Support > Customer Login** from the menu bar.

APPENDIX A

TCP/IP Ports Used by the GMS and Silver Peak Appliances

Following are lists of ports that are used by the appliances and by the Global Management System (GMS). These are the ports used for “listening”.

If you intend to use a port, make sure that it is open in the firewall(s).

List of ports used by the GMS

Following is the list of ports used by the GMS. All are part of the management plane.

It is mandatory for certain ports to be open. Opening other ports is optional (opt.), depending on your network, applications, and chosen deployment.

Must open port?	TCP	UDP	Port	Application	Direction relative to the GMS	Comments
yes	x		22	SSH	bidirectional	CLI (Command Line Interface) access over SSH
yes	x		443	HTTPS	bidirectional	communications between the GMS and a physical or virtual appliance (NX or VX)
opt.	x		21	FTP	outgoing	for GMS backup This is the default port. If you’ve configured a different port, then you also need to configure the firewall with that port number.
opt.	x		22	SCP	outgoing	for GMS backup This is the default port. If you’ve configured a different port, then you also need to configure the firewall with that port number.
opt.	x		49	TACACS+	outgoing	user authentication and authorization
opt.	x	x	53	DNS	outgoing	domain name services
opt.	x		80	HTTP	outgoing	If the appliance’s web configuration is for **HTTP only**, then you must open this port.
opt.		x	123	NTP	outgoing	synchronizes clocks
opt.		x	162	SNMP	outgoing	SNMP trap receivers
opt.		x	1812	RADIUS	outgoing	user authentication and authorization
opt.		x	2055	Netflow	outgoing	Netflow collector

List of ports used by the NX

Data Plane

This is for packets that traverse the optimization path. For creating tunnels, at least one of the first three applications — GRE, IPSec, or UDP — must be open.

Must open port ?	Application	Ports and Protocols	Use
yes	GRE	Protocol 47	If tunnel mode is GRE
yes	IPsec	Protocol ESP 50; UDP port 500 (for IKE key exchange)	If tunnel mode is IPsec
yes	UDP	UDP Port 4163	If tunnel mode is UDP
yes	ICMP	Protocol 1	Checks reachability of next-hop routers
opt.	flow redirection	TCP Port 4164 and UDP Port 4164	If flow direction is enabled and clustered via routers
opt.	iperf	TCP Port 5001 and UDP Port 5001	For testing link integrity outside the tunnel.
opt.	VRRP	Protocol 112	For VRRP protocol messages
opt.	WCCP protocol	UDP Port 2048	For WCCP redirection
opt.	WCCP CRE tunnel	Protocol 47	If L3 WCCP redirection is enabled, then Protocol 47 is used to redirect traffic between WCCP router and VXOA appliance, in both directions.

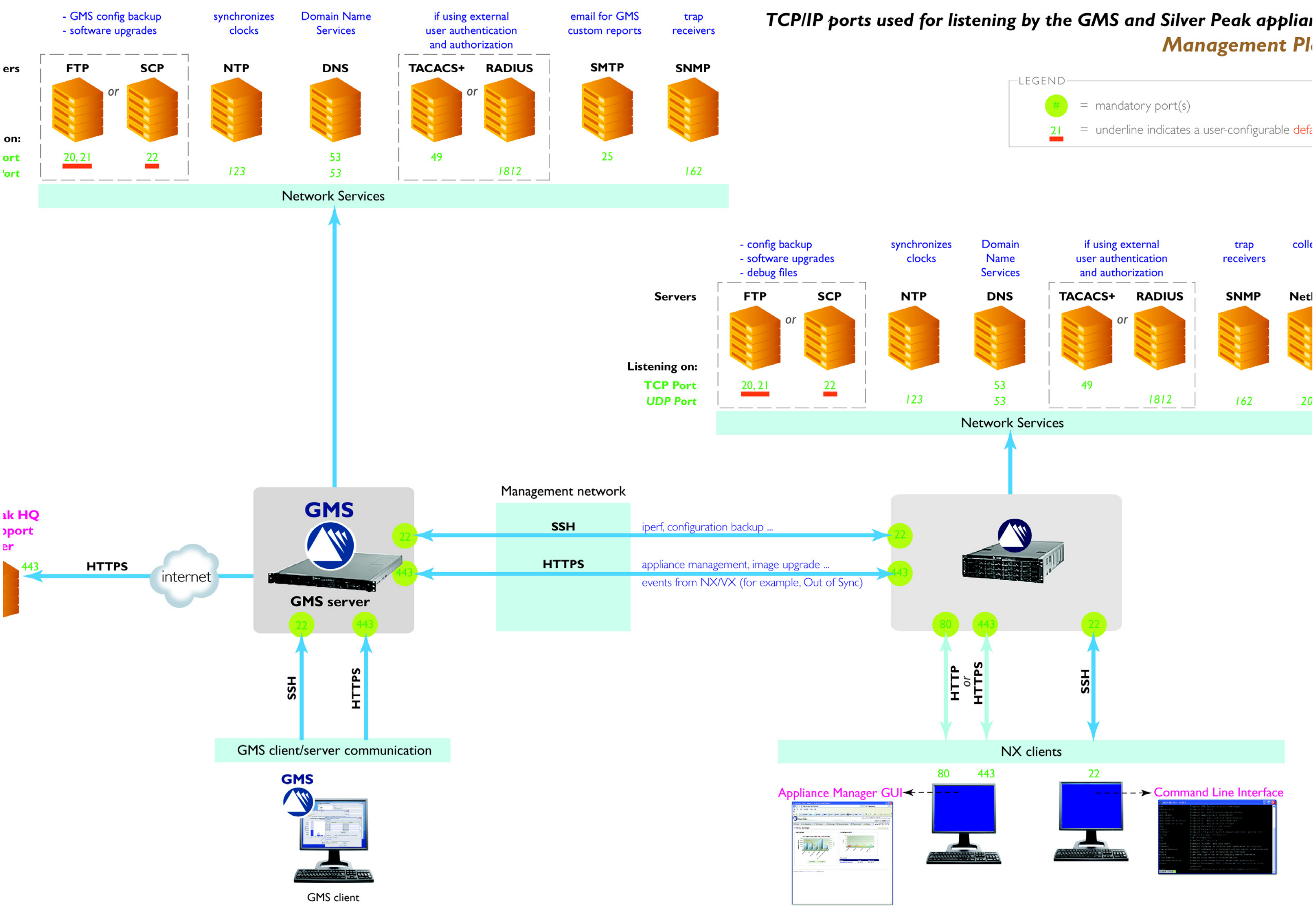
Management Plane

It is mandatory for certain ports to be open. Opening other ports is optional (opt.), depending on your network, applications, and chosen deployment.

Must open port ?	TCP	UDP	Port	Application	Direction relative to the appliance	Used for ...
yes	x		22	SSH and SCP	bidirectional	• configuration backup • software upgrades
yes	x		80	HTTP	bidirectional	communication with VXOA clients and with GMS
yes	x		443	HTTPS	bidirectional	communication with VXOA clients
opt.	x		20 [data channel] 21 [control channel]	FTP	bidirectional	• configuration backup • software upgrades
opt.	x		49	TACACS+	outgoing	user authentication and authorization
opt.	x	x	53	DNS	outgoing	domain name services
opt.		x	123	NTP	outgoing	synchronizes clocks
opt.		x	1812	RADIUS	outgoing	user authentication and authorization
opt.		x	162	SNMP	outgoing	SNMP trap receivers
opt.		x	2055	Netflow	outgoing	Netflow collector

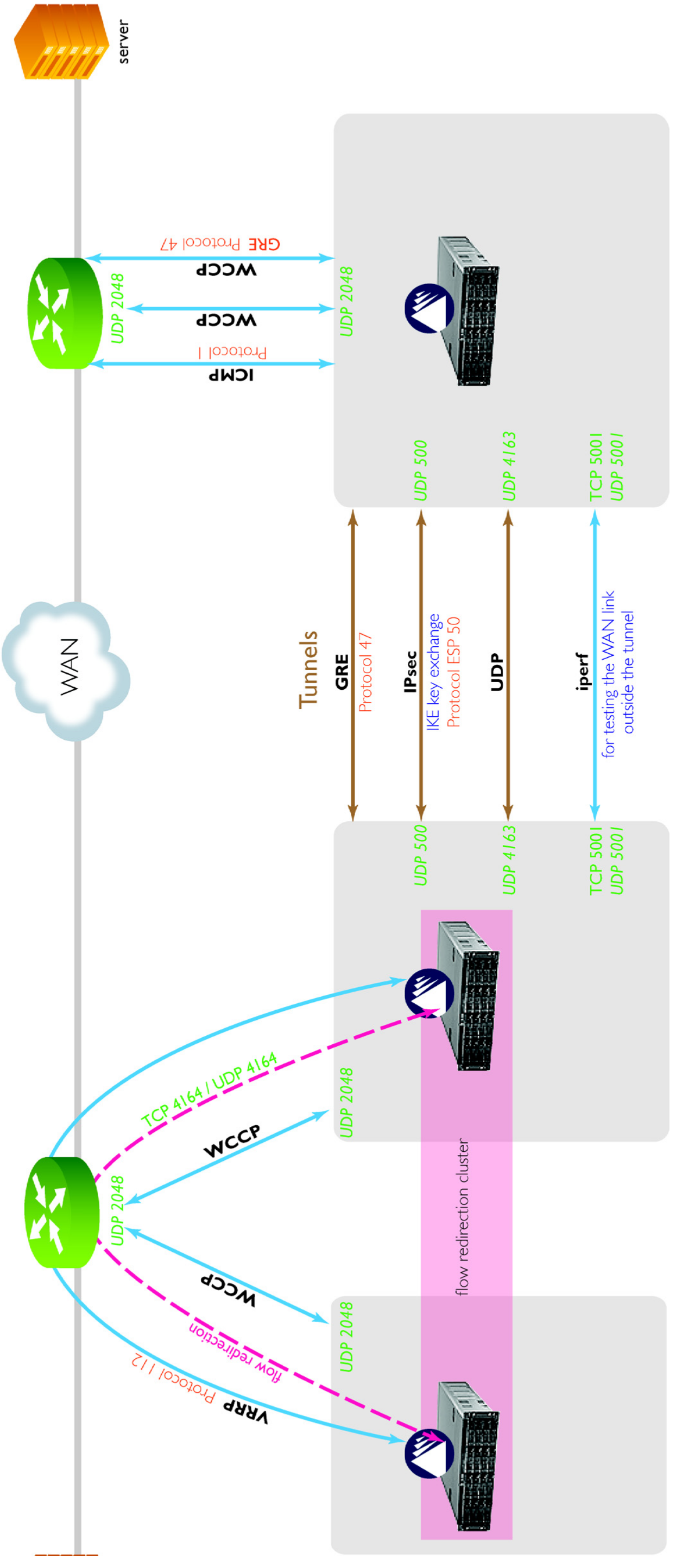
Diagrams of TCP/IP Port Use

See the following two pages.


TCP/IP ports used for listening by the GMS and Silver Peak applia
Management Pl
LEGEND
# = mandatory port(s)
21 = underline indicates a user-configurable defa
- GMS config backup
- software upgrades
synchronizes clocks
Domain Name Services
if using external user authentication and authorization
email for GMS custom reports
trap receivers
ers
FTP
or
SCP
NTP
DNS
TACACS+
or
RADIUS
SMTP
SNMP
on:
ort
'ort
20, 21
22
123
53
53
49
1812
25
162
Network Services
- config backup
- software upgrades
- debug files
synchronizes clocks
Domain Name Services
if using external user authentication and authorization
trap receivers
colle
Servers
FTP
or
SCP
NTP
DNS
TACACS+
or
RADIUS
SNMP
Net
Listening on:
TCP Port
UDP Port
20, 21
22
123
53
53
49
1812
162
20
Network Services
ak HQ
pport
er
443
HTTPS
internet
GMS
GMS server
22
443
Management network
SSH
HTTPS
iperf, configuration backup ...
appliance management, image upgrade ...
events from NX/VX (for example, Out of Sync)
22
443
80
443
22
SSH
HTTPS
GMS client/server communication
GMS
GMS client
HTTP
or
HTTPS
SSH
NX clients
80
443
22
Appliance Manager GUI
Command Line Interface

TCP/IP ports used by the GMS and the Silver Peak appliances

Data Plane



Silver Peak Systems, Inc.
2860 De La Cruz Blvd., Suite 100
Santa Clara, CA 95050

1.877.210.7325
+1.408.935.1850

www.silver-peak.com