riverbed

SteelHead™ SaaS User Guide (for Legacy Cloud Accelerator)

RiOS® Version 9.8

June 2018

riverbed®

Riverbed Technology
680 Folsom Street
San Francisco, CA 94107
www.riverbed.com

Part Number
712-00112-08

Contents

Welcome

Welcome to the *SteelHead SaaS User Guide*. Read this preface for an overview of the information provided in this guide, the documentation conventions used throughout, and contact information.

This preface includes these sections:

About this guide

The *SteelHead SaaS User Guide* describes the Riverbed SteelHead Software as a Service (SaaS) optimization platform based the Akamai internet optimization technology.

Note: The name for this feature has changed from SteelHead Cloud Accelerator to Legacy Cloud Accelerator. The SaaS Accelerator through SteelConnect replaces the Legacy Cloud Accelerator and provides a Riverbed end-to-end solution with simplified deployment and certificate management.

Reading this guide will provide you with an overview of the Legacy Cloud Accelerator, a checklist for setup and configuration, instructions for using the Riverbed Cloud Portal, and troubleshooting information to solve common issues.

This guide includes information relevant to these products:

- Riverbed SteelHead SaaS (SteelHead SaaS)
- Riverbed SteelHead CX appliance (SteelHead CX)
- Riverbed Cloud Portal

Audience

This guide is written for storage and network administrators familiar with Software as a Service (SaaS) technology and administering and managing WANs using common network protocols such as TCP/IP, CIFS, HTTP, FTP, and NFS.

You must also be familiar with:

- using the SteelHead Management Console. For details, see the *SteelHead User Guide*.
- connecting to the RiOS CLI. For details, see the *Riverbed Command-Line Interface Reference Manual*.

- configuring SSL on a SteelHead appliance.

Document conventions

This guide uses this standard set of typographical conventions.

Convention	Meaning
italics	Within text, new terms and emphasized words appear in *italic* typeface.
boldface	Within text, CLI commands, CLI parameters, and REST API properties appear in **bold** typeface.

Courier	Code examples appear in Courier font:
	`amnesiac > enable`
	`amnesiac # configure terminal`

< >	Values that you specify appear in angle brackets: **interface <ip-address>**
[ ]	Optional keywords or variables appear in brackets: **ntp peer <ip-address> [version <number>]**
{ }	Elements that are part of a required choice appear in braces: **{<interface-name> | ascii <string> | hex <string>}**
|	The pipe symbol separates alternative, mutually exclusive elements of a choice. The pipe symbol is used in conjunction with braces or brackets; the braces or brackets group the choices and identify them as required or optional: **{delete <filename> | upload <filename>}**

Documentation and release notes

To obtain the most current version of all Riverbed documentation, go to the Riverbed Support site at https://support.riverbed.com.

If you need more information, see the Riverbed Knowledge Base for any known issues, how-to documents, system requirements, and common error messages. You can browse titles or search for keywords and strings. To access the Riverbed Knowledge Base, log in to the Riverbed Support site at https://support.riverbed.com.

Each software release includes release notes. The release notes identify new features in the software as well as known and fixed problems. To obtain the most current version of the release notes, go to the Software and Documentation section of the Riverbed Support site at https://support.riverbed.com.

Examine the release notes before you begin the installation and configuration process.

Contacting Riverbed

This section describes how to contact departments within Riverbed.

- **Technical support** - If you have problems installing, using, or replacing Riverbed products, contact Riverbed Support or your channel partner who provides support. To contact Riverbed Support, open a trouble ticket by calling 1-888-RVBD-TAC (1-888-782-3822) in the United States and Canada or +1 415-247-7381 outside the United States. You can also go to https://support.riverbed.com.

- **Professional services** - Riverbed has a staff of professionals who can help you with installation, provisioning, network redesign, project management, custom designs, consolidation project design, and custom coded solutions. To contact Riverbed Professional Services, email proserve@riverbed.com or go to http://www.riverbed.com/services/index.html.
- **Documentation** - The Riverbed Technical Publications team continually strives to improve the quality and usability of Riverbed documentation. Riverbed appreciates any suggestions you might have about its online documentation or printed materials. Send documentation comments to techpubs@riverbed.com.

1

Overview of SteelHead SaaS

This chapter provides an overview of SteelHead SaaS software. It includes these sections:

Note: RiOS 9.8 adds SteelHead support for SaaS optimization through SteelConnect and the existing SaaS accelerator (using Akamai and described in this guide) has been renamed from SteelHead Cloud Accelerator to Legacy Cloud Accelerator. The SaaS Accelerator through SteelConnect replaces the Legacy Cloud Accelerator and provides a Riverbed end-to-end solution with simplified deployment and certificate management, however, the full functionality depends on a future release of SteelConnect Manager. See this Knowledge Base article for the compatibility information:
https://supportkb.riverbed.com/support/index?page=content&id=S32337

About SteelHead SaaS

SteelHead SaaS combines the Riverbed WAN optimization technology (RiOS) with the Akamai internet optimization technology (SureRoute) for accelerating SaaS application performance. SteelHead SaaS uses Akamai SureRoute to provide a reliable transport across the fastest path through thousands of servers in many countries while dynamically adding RiOS instances at points nearest to the SaaS application provider.

Note: Version 9.7 and later support Microsoft Azure Front Door for SharePoint and SharePoint Anycast with the default configuration.

To deploy SteelHead SaaS, you do not need to change your existing network infrastructure. You simply purchase the service and then register your existing branch SteelHead appliances with the Riverbed Cloud Portal. After they are registered, the appliances can accelerate your SaaS applications.

You can use the Riverbed Cloud Portal to register or unregister SteelHead SaaS appliances, obtain the service status, manage SSL certificates, manage licenses, and enable optimization for available SaaS applications.

System components

The SteelHead SaaS system consists of these components:

- **SaaS Application** - The application delivered as Software as a Service.
- **Akamai Intelligent Platform** - The Akamai distributed network of more than 100,000 servers deployed in more than 1000 locations world-wide across the public internet. The platform hosts Riverbed SteelHead technology and provides internet-based optimization for Enterprise SaaS traffic.
- **Akamai SureRoute Optimization** - Akamai SureRoute Optimization uses a suite of technologies to provide fast and reliable delivery between the Akamai Edge Servers. Route optimization examines multiple paths across the internet to find the fastest path and route past any failures; the Enhanced Akamai Protocol overcomes the inefficiencies of TCP to provide the highest throughput and fastest recovery; and Packet Redundancy enables you to re-create any lost data without having the client or server retransmit.
- **Akamai Edge Server** - The Akamai Edge Server in the Akamai Intelligent Platform closest to the end user is dynamically and intelligently selected (regardless of whether the end-user location has direct internet access or the data is back-hauled to the internet gateway at the data center). The Akamai Edge Server closest to the SaaS application runs a RiOS instance, referred to in this system as the Akamai Cloud SteelHead, which acts as a peer to the registered appliance.
- **Data Center SteelHead** - The SteelHead appliance located in the customer data center close to the customer's internet egress point. It contains the Akamai Cloud Proxy (ACP) feature.

  ACP is a software component that grants the SteelHead appliance access to the Akamai Intelligent Platform. The data center SteelHead appliance connects to the Akamai Intelligent Platform using a configurable UDP port over a wide range of IP addresses.
- **Branch SteelHead** - The SteelHead appliance located in the customer branch office that intercepts any connections destined for the SaaS platform to be accelerated. The Enterprise Branch SteelHead can host the Akamai Cloud Proxy (ACP) feature, but does not require it.
- **Akamai Cloud SteelHead (ACSH)** - A SteelHead unique to each customer dynamically created and managed in the Akamai network based on SaaS traffic from the customer's branch office locations.
- **Riverbed Cloud Portal** - An always-on, always-available web portal that enables you to manage your SteelHead SaaS services and your branch appliances.

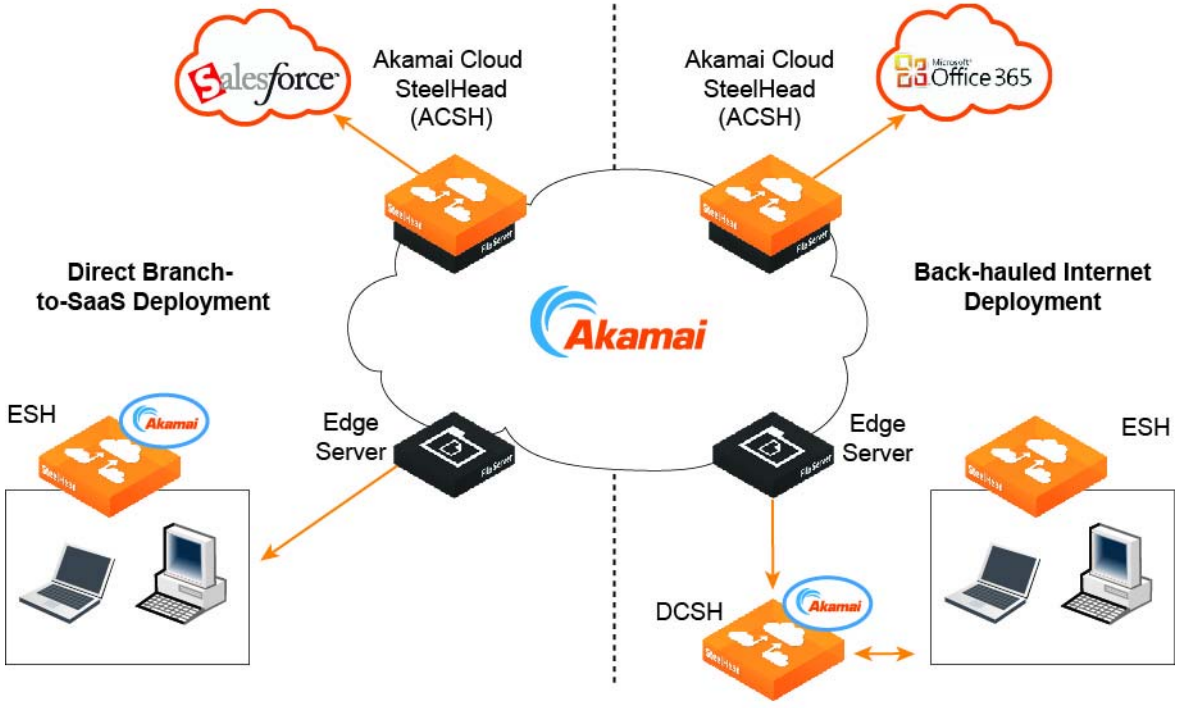
Note: The Riverbed Cloud Portal uses elastic scaling technology. As a result, the portal is not always served from a static IP address. Ensure that all appliances that you want to communicate with the Riverbed Cloud Portal are configured to use DNS and hostnames for the portal.

Deployment configurations

There are two types of deployment configurations defined by how the branch offices access the internet. In *direct branch internet deployment* mode, branch offices access the internet directly without passing through a data center. In *back-hauled internet deployment* configurations, branch offices connect to the internet over an internal WAN or VPN connection to a centralized data center that controls all internet access.

Note: SteelHead SaaS does not support SteelHead Mobile.

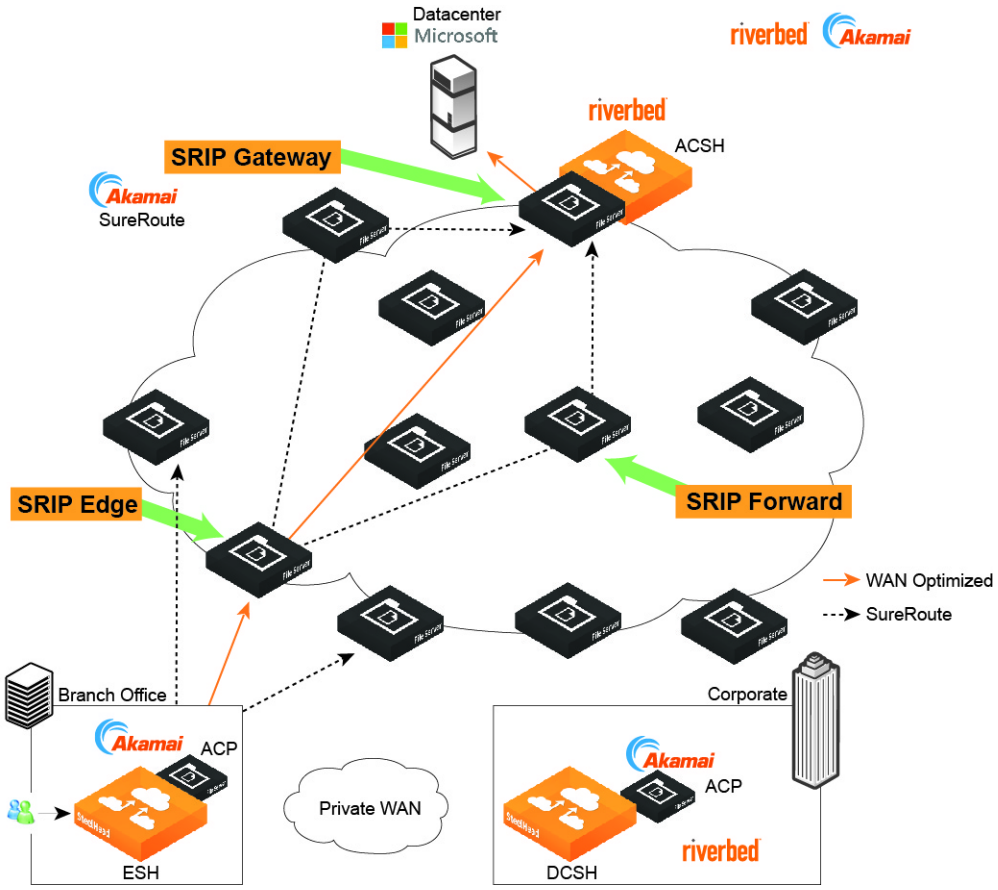
Figure 1-1. SteelHead SaaS configurations



Direct branch internet deployment

In direct mode, the branch SteelHead appliance encapsulates the traffic and sends it directly to a server in the Akamai network. Akamai SureRoute optimization technology ensures that the traffic is forwarded through the Akamai network along the fastest path toward its destination at the data center hosting the SaaS application.

Figure 1-2. Direct branch internet deployment



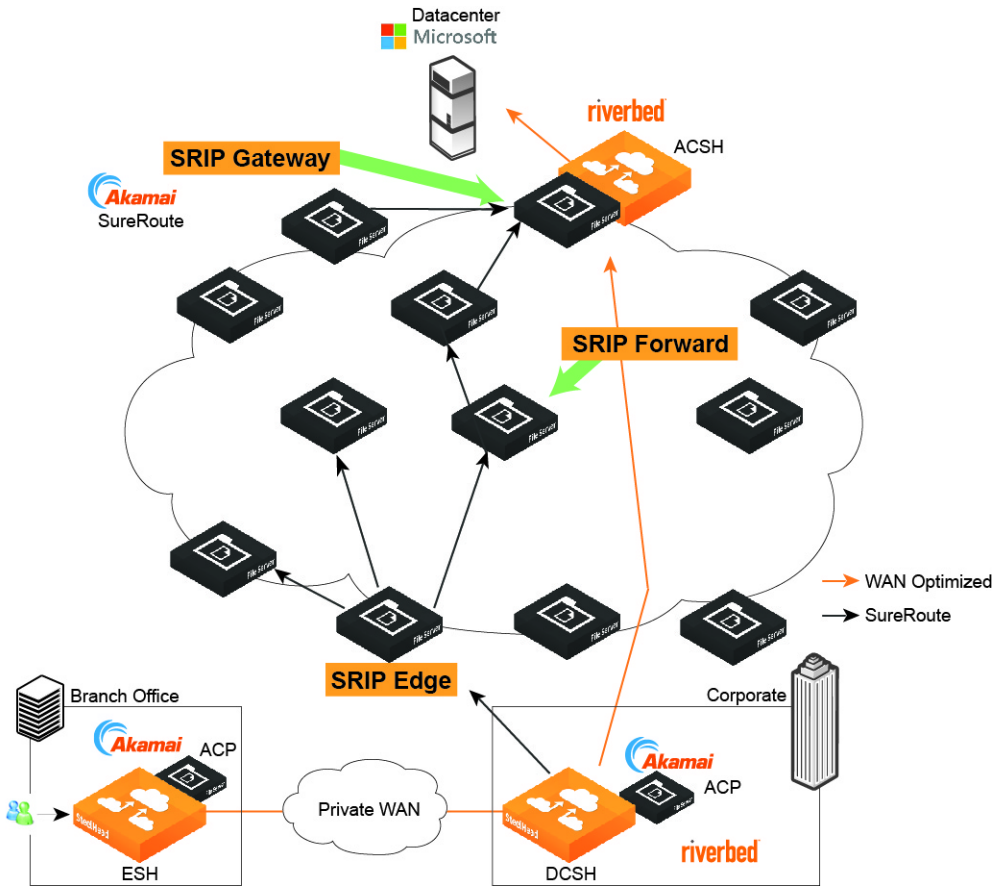
After the branch SteelHead appliance is licensed and registered on the Riverbed Cloud Portal, it downloads a set of rules from the portal and obtains the IP addresses for all of the servers for the SaaS applications to which you are subscribed.

This topology does not involve an intermediary SteelHead appliance. All SSL optimization and peering trusts are established directly between the branch SteelHead appliance and the ACSH.

Back-hauled internet deployment

In this topology, the branch does not have its own connection to the internet. All traffic directed to the internet is back-hauled over a private WAN or VPN to the organization's data center.

Figure 1-3. Back-hauled internet deployment



In this mode, the branch SteelHead appliance adds special information to the inner channel packets to indicate that this is traffic directed to the SaaS provider. When the data center SteelHead appliance receives the traffic with this special information, it redirects the traffic into a UDP tunnel and sends it to the Akamai network to be SureRoute routed to the SaaS application provider. For traffic coming back from Akamai, the data center SteelHead appliance unwraps the inner channel traffic from the tunnel before sending it across the WAN to the branch SteelHead appliance.

Although the data center SteelHead appliance encapsulates the traffic, it plays no role in the SSL optimization process. SSL optimization still takes place between the branch SteelHead appliance and the ACSH. Ensure that you establish the SSL peering trust between them.

In the back-hauled mode, you can configure the branch SteelHead appliance with full transparency and maintain existing QoS policies on the WAN.

If there is another branch with a SteelHead appliance that is not running a version of RiOS that supports SteelHead SaaS, then traffic from that branch appliance directed to the SaaS provider is passed through.

Note: If there is a firewall in the data center, you must configure it to allow the UDP traffic between the data center SteelHead appliance and the Simple Routing Information Protocol (SRIP) network.

Note: Ensure that you register both the branch SteelHead appliance and the data center SteelHead appliance with the Riverbed Cloud Portal and that they are granted access to the SRIP network. Also, ensure that the RiOS software running on both the branch appliance and the data center SteelHead appliance support SteelHead SaaS.

Deciding on a deployment configuration

The key deciding factor to choosing a deployment configuration is whether or not your network requires QoS or NetFlow reporting on the WAN between the data center and the branch. This is because in a back-hauled configuration traffic directed to the SaaS provider is encapsulated within a UDP tunnel and is no longer visible on the WAN.

If your network does not need QoS or NetFlow reporting on the link between the data center and the branch, then use a direct mode deployment. Otherwise, use a back-hauled deployment. In a back-hauled deployment, the data center SteelHead appliance redirects the traffic to the Akamai network, but the branch SteelHead appliance performs the optimization. Traffic from the branch SteelHead appliance to the ACSH uses TCP on ports 7800 through 7899 as visible on the network. When traffic arrives at the data center SteelHead appliance, the appliance redirects the traffic using UDP on port 9545.

Note: If the data center has a firewall, ensure that it allows UDP access from the in-path IP address of the branch SteelHead appliance.

Supported SaaS providers

Riverbed periodically adds support for SaaS providers. Supported SaaS providers are listed on the Riverbed Cloud Portal. Before a SaaS provider is fully supported, it is available to customers for engineering-supported beta testing through the Riverbed Advanced Access Program (RAAP). Contact your Riverbed sales representative if you are interested in beta testing new offerings.

SteelHead SaaS licensing

A SteelHead SaaS license is based on the number of users that are subscribed to the SaaS provider. In the case of All-SaaS licenses where there may be more than one SaaS provider being optimized by the SteelHead appliances, the licensed user count is based on the service with the highest number of subscribed users.

Unlike other add-on SteelHead licenses – for example, SCPS – the SteelHead SaaS license is organization wide, not per SteelHead appliance. You can register any number of SteelHead appliances in your organization with the SteelHead SaaS platform.

After you purchase a SteelHead SaaS license, you are provided with an account to the Riverbed Cloud Portal where you obtain a unique registration key that enables SteelHead appliances to register with the Riverbed Cloud Portal to activate the appliances' SteelHead SaaS service and to start optimizing SaaS traffic. For details, see "Registering and unregistering appliances on the portal" on page 31.

The SteelHead SaaS license does not increase the optimization capacity of SteelHead appliances registered with the platform. In other words, connections optimized by the SteelHead SaaS service running on a SteelHead appliance count towards the optimized connection limit for that SteelHead appliance. These connections will also count towards the appliance's outbound optimized throughput limit if there is one.

Before you activate SteelHead SaaS optimization on a SteelHead appliance, ensure that you account for the added connection and throughput usage in the same way you would when introducing any other additional application for optimization on the SteelHead appliance.

Note: Registering a SteelHead appliance with the SaaS optimization platform does not change the optimized session limit for that appliance. Ensure that you account for the appliance's optimized session limit when you consider it as a candidate for use with the SteelHead SaaS optimization platform.

SteelHead SaaS connection and bandwidth limits

This table provides some guidance for the purpose of sizing a SteelHead for use with SteelHead SaaS. While metrics like connections per user and bandwidth consumed per user vary from one deployment to another and among individual users, in general, these metrics average out within a group of users.

SaaS Service group	Per user	Per 10-user pack
Office 365 Multi-Tenant	10 connections/80 kbps per user	100 connections/800 kbps
Salesforce.com	5 connections/40 kbps per user	50 connections/400 kbps
All-SaaS	20 connections/160 kbps per user	200 connections/1600 kbps

Compatibility with SteelHead models

SteelHead model families xx50, xx55, xx70, SteelHead EX, SteelFusion Edge, and GX10000 support SteelHead SaaS. All SteelHead (virtual edition) models also support SteelHead SaaS.

Note: Legacy SteelHead models – xx50, xx55 (excluding CX255), SteelHead EX, and VCXxx55 – do not support the latest versions of RiOS software. Consult the Riverbed support site for RiOS versions applicable to your SteelHead models.

2

SteelHead SaaS Quick Start Checklist

To help you get up and running quickly, here is a checklist that will guide you in setting up SteelHead SaaS. All the activities mentioned here are explained in later chapters. Refer to later chapters for more details.

Ensure these network requirements are in place

- ❑ The SteelHead appliance can connect to the internet from its primary and in-path interfaces.
- ❑ These SteelHead connections are allowed on the firewall facing the internet:
  - ❑ Outbound stateful (reverse traffic inbound needs to reach the SteelHead) TCP port 443 from the SteelHead appliance's primary interface.
  - ❑ Outbound stateful UDP port 9545 from the SteelHead appliance's in-path interfaces.
  - ❑ NTP (UDP/123) from the SteelHead primary interface, if the SteelHead appliance is configured with an internet NTP.
  - ❑ DNS (TCP/UDP/53) from the SteelHead primary interface, if the SteelHead appliance is configured with an internet DNS server.
- ❑ Enable access from the Akamai Cloud SteelHeads (ACSHs) if access to the SaaS application is restricted to specific source IP addresses. For details, visit the Riverbed Knowledge Base and search for S16182 for a list of ACSH IP addresses.

Configure the Riverbed Cloud Portal

- ❑ Choose a secure socket layer (SSL) certificate authority (CA) to use for SaaS proxy certificates. You can do this in the Cloud Accelerator tab > SaaS Platforms page. For more information about which certificates to sign, read this article on the Riverbed Knowledge Base:

  https://supportkb.riverbed.com/support/index?page=content&id=S16076

To configure a customer-hosted CA

Note: Certificates signed by an internal CA may already be trusted by the internal clients.

1. Log in to the Riverbed Cloud Portal and choose customer-hosted.
2. Ensure that the Proxy Certificate Settings found under Settings > Certificate Settings are filled out.
3. Generate Certificate Signing Requests (CSRs) that correspond with the SaaS you want to optimize, and download those CSRs.

4. Sign the CSRs in PEM format with the internal CA certificate that each of your clients trust.
5. Upload the new proxy certificate, signed in PEM format, back on to the Portal.

To configure a cloud-hosted CA

1. Log in to the Riverbed Cloud Portal and choose Cloud-hosted certificates if you want the service to create and manage a dedicated SSL CA for you.
2. Go to the Riverbed Cloud Portal and choose cloud-hosted.
3. Download the CA certificate and install it on every client that will use the SaaS service.
4. Request new proxy certificates for each platform hostname.

- ❑ If the internal SteelHead appliance peering certificates are signed by a CA, upload the CA public certificate to the Riverbed Cloud Portal. You can do this in the Cloud Accelerator tab > Secure Peering page.
- ❑ If the internal SteelHead appliance peering certificates are self-signed, verify that the Trust Enterprise SteelHead Peering Certificates check box is selected.

Configure the SteelHead

- ❑ Upgrade the SteelHead to RiOS 9.1 or later. All-SaaS/Universal SaaS license requires RiOS 9.1 or later.
- ❑ Ensure that the SteelHead has enough capacity to optimize the extra SaaS connections.
- ❑ Enable information-level logging to troubleshoot in the event a problem arises.
- ❑ Enable and configure NTP to point to at least two NTP servers that are synced within one minute of exact time.
- ❑ Enable and configure DNS settings to point to at least two DNS servers that can resolve internet names.
- ❑ Enable Simplified Routing All if the in-path gateway is on the WAN side, or use the LAN-side gateway.
- ❑ Enable HTTP optimization. For Microsoft Office 365 SharePoint refer to the general recommendation in Knowledge Base article S16785.

Configure SSL:

- ❑ Ensure the SteelHead appliance has an SSL license. If not, apply for one at http://sslcert.riverbed.com.
- ❑ Ensure the SteelHead appliance has a valid SSL peering certificate (self-signed or CA-signed).

- ❑ Enable SSL optimization.

  For RiOS 9.0 and later:

  - ❑ If you have clients that do not have the proxy CA certificate installed, enter this command:

    ```
    protocol ssl no-data conn-bypass enable
    ```

  For RiOS 9.2 and earlier:

  - ❑ Add pass-through in-path rules for internal SSL servers that you do not want to optimize.
  - ❑ Add pass-through peering rules in the case of SteelHead deployment with backhauled internet links through other branches or data centers with SteelHeads.
  - ❑ Remove port 443 from the secure port label list (the default pass-through in-path rule for secure ports will no longer apply to 443).

  For RiOS 9.2.1 and later:

  - ❑ Configure an in-path autodiscover rule using the `_cloud-accel-saas_` host label, with latency optimization policy set to Exchange Autodetect and cloud acceleration set to Auto.

  For RiOS 9.6 and later:

  - ❑ There is a new bypass option you can enable that allows you to bypass connections regardless of the server IP. This addresses a problem where Outlook, for example, tries new IPs which you also want to bypass.

    ```
    protocol ssl no-data conn-bypass by-client enable
    ```

  For Microsoft Office 365, enable MAPI optimization.

  - ❑ Enable MAPI auto-detect outlook anywhere.
  - ❑ Enable encrypted optimization transparent mode.

- ❑ If testing with only a few clients, we recommend to configure an in-path rule to perform auto-discovery and cloud acceleration on port 443. The rule should be placed above the pass-through rule that is associated with the secure port label.
- ❑ For RiOS 8.6 through 9.0, enable GeoDNS through the CLI by entering this command. GeoDNS is enabled by default in RiOS 9.1 and later:

  ```
  service cloud-accel geodns enable
  ```

- ❑ Register the SteelHead for SteelHead SaaS optimization. You can obtain a registration key from the Riverbed Cloud Portal.
- ❑ Enable Cloud Acceleration.

Grant service to the SteelHead

- ❑ Go to the Riverbed Cloud Portal and grant service to the newly configured SteelHead appliance.

Turn on service for SaaS applications

- ❑ Go to the Riverbed Cloud Portal > SaaS Platforms page and enable Acceleration Service for the SaaS application you want to optimized.
- ❑ In the SteelHead SaaS appliance's management console, go to Optimization > Cloud Accelerator and enable Acceleration Service for the SaaS application you want to optimize.

3

Using the Riverbed Cloud Portal

The Riverbed Cloud Portal enables you to manage your SteelHead SaaS subscriptions through a web interface. This chapter describes how to navigate the Riverbed Cloud Portal. It includes these sections:

Obtaining a Riverbed Cloud Portal Account

Contact Riverbed Sales to purchase SteelHead SaaS or request an evaluation. After your purchase or request is processed, a portal account is created for you and you will receive an email with the URL to the portal, your username (usually your email address), and a temporary password.

Logging in to and out of the Riverbed Cloud Portal

You will need a portal account and login credentials. See "Obtaining a Riverbed Cloud Portal Account" on page 23.

To log in to the Riverbed Cloud Portal

1. Point a browser to this URL: http://cloudportal.riverbed.com.
2. Enter your login credentials.
3. Click **Log In**.

To log out of the portal

- Click **Logout** in the upper-right corner of the portal.

Managing your portal account

The user account menu and the Support menu located on the right side of the portal toolbar enable you to access portal pages where you can perform these account management activities:

Change your password

If you forgot your password, you can reset it. You can also change your password under account settings.

To reset your password

1. At the log in page, click **Forgot your password?** to display the Reset Password page.
2. Type your email address and click **Reset Password**. The system emails a link to you. Click the link to change your password.

To change your password

1. Log in to the portal.
2. Select your username located in the upper-right corner of the portal.
3. Select Account Settings from the drop-down menu.
4. Click **Change Password**.
5. Enter your old password.
6. Enter a new password.
7. Confirm your new password.
8. Click **Change Password**.

View event history

The event history page displays a list of recent events. Each entry includes the date, user, and description of the event. The list can be sorted.

To view the event history

1. Log in to the portal.
2. Select your username located in the upper-right corner of the portal.
3. Select Event History.
4. (Optional) Sort the list by clicking a column heading.

Configure OAuth

OAuth is an open standard for authorizing client access to server resources without the need for sharing credentials. OAuth is designed to work with HTTP and uses access tokens to allow client systems access to their server resources.

Note: OAuth is not applicable to SteelHead SaaS.

To generate an OAuth code

1. Log in to the portal.
2. Select your username located in the upper-right corner of the portal.
3. Select OAuth Setup.
4. Click **Generate New OAuth Code**.
5. Enter a descriptive name for the new code.
6. Click **Generate**.

View portal news

The News page displays news stories published to the Riverbed Cloud Portal.

To view portal news

1. Log in to the portal.
2. Select Support in the upper-right corner of the portal.
3. Select News.

Download software

You can download SteelHead (in the cloud) software, Discovery Agent software, and other Riverbed product software from the Riverbed support site.

Note: Downloading software is not applicable to SteelHead SaaS.

To download software

1. Log in to the portal.
2. Select Support in the upper-right corner of the portal.
3. Select Downloads. The Riverbed support site SteelHead (in the cloud) software download page is displayed.

Access Riverbed Support

You file support cases from the Riverbed support site.

To access Riverbed Support

1. Log in to the portal.
2. Select Support in the upper-right corner of the portal.
3. Select Cloud Support. The Riverbed support log in page is displayed.

View Riverbed Cloud Portal online help

The portal online help is context sensitive. Launching the help will display information pertaining to the portal page you are viewing.

To view portal online help

1. Log in to the portal.
2. Do one of these actions:
   - Select the **?** icon in the upper-right corner of the portal.
   - Select Support > Help.

View account information

The Account Info page displays information about the current authenticated user's account. You can also change your password on this page (see "Change your password" on page 24).

To view account settings

1. Log in to the portal.
2. Select your username in the upper-right corner of the portal.
3. Select Account Settings.

Viewing your service summary

After you log in to the Riverbed Cloud Portal, select the Cloud Accelerator tab. When you log in to the Riverbed Cloud Portal for the first time the portal remembers this selection; the next time you log in, the Riverbed Cloud Portal automatically displays the tab you selected during your previous login.

The Cloud Accelerator Service Summary page provides a dashboard view of the system. It displays:

- **Service Summary** - Displays the SaaS platforms that are using SteelHead SaaS, the application provider, and the status of the acceleration service (on or off). It also displays the ESHs that are pending service or that have been granted or denied service.
- **Portal News** - Displays the last three news stories published by Riverbed employees to the portal.
- **Recent Events** - Describes recent events and activity in your company. For example, it might report that a particular user has logged in.

You can view the details page for a SaaS application by selecting the application's name. This page is divided into two sections: SaaS Details and SaaS Platform Proxy Certificates. This information is displayed:

- SaaS provider
- Application ID
- Service Group
- Acceleration Service (enabled status)
- Details
- Proxy certificates for specific SaaS hostnames

You can select a hostname to view the proxy certificate associated with it. You can also request a new certificate for a specific hostname by selecting the Request New Proxy Certificate for that hostname.

For information about configuring proxy certificates, see "Configuring SaaS proxy certificates" on page 43.

Viewing the appliance registration key

The appliance registration key is used to enable SaaS optimization services on your SteelHead appliances. The registration key must be entered into the SteelHead appliances that you want to use for SaaS optimization.

Note: Generating a new registration key does not affect previously registered appliances.

For information about how to register SteelHead appliances, see "Registering and unregistering appliances on the portal" on page 31.

To view the appliance registration key

1. Log in to the portal.
2. Select Appliance Registration Key.

To generate a new appliance key

- Click **Generate new key**.

Viewing SteelHead service status

You can view the service status of your SteelHead appliances on the Enterprise SteelHeads page.

For information about granting, denying, or suspending service, see "Enabling and disabling optimization services on registered appliances" on page 32.

To view SteelHead service status

1. Log in to the portal.
2. Select Enterprise SteelHeads.

   The Enterprise SteelHeads portal page displays three sections: SteelHeads Pending Service, SteelHeads Granted Service, SteelHeads Denied Service.

Viewing secure peering certificates

You can view the peering relationship between your Enterprise SteelHeads and the Cloud Accelerator in the Secure Peering Management page. You can also view, copy, and download the certificates from this page.

For information about configuring certificates, see Chapter 6, "Managing Certificates."

To view a list of Enterprise SteelHead peering certificates

1. Log in to the portal.
2. Select Secure Peering.

   The Secure Peering Management page is divided into three tabs: Enterprise SteelHead Peering Certificates, Cloud-Hosted Peering CA, and Event Log.

Viewing licenses, available SaaS Platforms, and proxy certificates

You can view your SaaS licenses; view, enable and disable SaaS applications for all SteelHead appliances; and view, download and request new proxy certificates on the SaaS Platforms page.

For information about configuring proxy certificates, see "Configuring SaaS proxy certificates" on page 43.

To view the SaaS Platforms page

1. Log in to the portal.
2. Select SaaS Platforms.

   The SaaS Platforms page is divided into three sections: SaaS Licenses, Manage SaaS Platforms, and Proxy Certificate Authority management.
3. (Optional) Select the name of a SaaS application to view the details page for it. See "Viewing your service summary" on page 27 for a description of the SaaS application details page.

To enable or disable SaaS platforms for all SteelHead appliances

- In the Manage SaaS Platforms section of the SaaS Platforms page, place a check mark next to the SaaS applications that you want to enable. Remove the check mark to disable.

Viewing Cloud Accelerator statistics

The Accelerator Statistics report summarizes the data sent to the cloud and retrieved from the cloud within the time period specified. It includes these statistics.

Field	Description
WAN Throughput To Cloud	Total data sent to the cloud by all ESHs registered for SteelHead SaaS.
WAN Throughput From Cloud	Total data received from the cloud by all ESHs registered for SteelHead SaaS.
Maximum Concurrent Connections	Maximum number of concurrent connections at the time you specify.

The Accelerator Statistics report answers these questions:

- What was the total data sent to the cloud by all ESHs registered for SteelHead SaaS?
- How much data was received from the cloud by all ESHs registered for SteelHead SaaS?
- What are the maximum concurrent connections?

To view cloud accelerator statistics

1. Select Accelerator Statistics to display the Accelerator Statistics page.
2. Use the controls to customize the report as described in this table.

Control	Description
Period	Select the time period from the drop-down list. For **Custom**, enter the Start Time and End Time and click **Update**. Use this format: yyyy/mm/dd hh:mm:ss.
Service Group	Select a SaaS Service Group from the drop-down list and click **Update**.
Update	Displays the report.

4

Managing SteelHead SaaS

This chapter describes how to use the Riverbed Cloud Portal to manage SteelHead SaaS. It includes these sections:

Controlling SaaS optimization

You can configure SaaS optimization on a per-application basis. You can control SaaS optimizations either through the Riverbed Cloud Portal user interface or through the user interface of the individual appliances. Changes made through the Riverbed Cloud Portal affect all registered appliances; however, changes made to a specific appliance affect only that appliance.

Settings on the appliance take precedence over settings specified in the Riverbed Cloud Portal. If you disable the service for a particular SaaS platform on an appliance, the appliance stops optimizing connections to that SaaS platform regardless of the settings downloaded from the Riverbed Cloud Portal.

Registering and unregistering appliances on the portal

After you purchase a SteelHead SaaS license and receive your Riverbed Cloud Portal account information, register the SteelHead appliances that you want to use for SaaS optimization with the Riverbed Cloud Portal. After an appliance is registered with the portal, you can enable SaaS optimization services on the appliance.

To register the appliance

1. Log in to the Riverbed Cloud Portal.
2. Select Cloud Accelerator.

3. Select Appliance Registration Key.
4. Copy the Appliance Registration Key.
5. Log in to the appliance.
6. Choose Optimization > SaaS: Legacy Cloud Accelerator.
7. Paste the registration key into the Appliance Registration Key text field under Registration Control and click **Register**.

   Under Registration Control, this message appears:

   ```
   This appliance is currently registered with the Cloud Portal.
   ```

To unregister an appliance

1. Log in to the Riverbed Cloud Portal.
2. Select Cloud Accelerator.
3. Select Enterprise SteelHeads.
4. Select the serial number of the appliance you want to unregister.
5. Select the Details tab.
6. Click **Deregister**.

   The appliance stops optimizing traffic and is no longer registered with the portal. To use this appliance with the portal again, you must reregister it.

Enabling and disabling optimization services on registered appliances

After you register a SteelHead appliance with the Riverbed Cloud Portal, it is listed under SteelHeads Pending Service on the Enterprise SteelHead Appliances page of the Riverbed Cloud Portal. You must explicitly grant the appliance SaaS optimization services to use it to optimize a SaaS application.

You can move an appliance into Pending status at any time. You might find this useful to pause optimization services on the appliance in this way prior to performing maintenance on the appliance.

If you have lost direct access to an appliance and want to prevent it from optimizing SaaS traffic, you can deny SaaS optimization for that appliance.

Note: If you deny an appliance access to SaaS optimization services, the appliance will delete all SteelHead SaaS settings the next time it connects to the Riverbed Cloud Portal. You must reregister the appliance if you want it to participate in the cloud acceleration service again.

To grant SaaS optimization services on an appliance

1. Log in to the Riverbed Cloud Portal.
2. Select Cloud Accelerator.
3. Select Enterprise SteelHead Appliances.
4. Under SteelHeads Pending Service, select the appliances you want.
5. Click **Grant Service**.

To deny SaaS optimization services on an appliance

1. Log in to the Riverbed Cloud Portal.
2. Select Cloud Accelerator.
3. Select Enterprise SteelHead Appliances.
4. Under SteelHeads Granted Service or SteelHeads Pending Service, select the appliances you want.
5. Click **Deny Service**.

To change an appliance's access status to pending

1. Log in to the Riverbed Cloud Portal.
2. Select Cloud Accelerator.
3. Select Enterprise SteelHead Appliances.
4. Under SteelHeads Granted Service, select the appliances you want.
5. Click **Move to Pending Service**.

Managing SaaS platforms

You manage settings for SaaS applications or platforms using the Manage SaaS Platforms page of the Riverbed Cloud Portal.

To manage SaaS platforms

- Select SaaS Platforms on the Cloud Accelerator page.

The SaaS Platforms page displays a list of available SaaS platforms and whether the Acceleration Service is on or off.

The SaaS Platforms page also displays the proxy settings. For details, see Chapter 7, "Deploying SteelHead SaaS with Enterprise Proxy."

Obtaining SaaS optimization details

You obtain details about a specific SaaS application in the SaaS Service Details page.

To obtain SaaS optimization details

1. Select SaaS Platforms.
2. In the table under the Manage SaaS Platforms section, select the name of the platform to display the SaaS Service Details page.

The SaaS Services page displays these details about the selected SaaS application:

Parameter	Description
SaaS Provider	Name of the SaaS provider such as Salesforce.com.
Application ID	The ID assigned to the SaaS platform by the Riverbed Cloud Portal.
Service Group	Identifies the type of license (AllSaaS or al-la-carte) under which the service is operating.
Acceleration Service	Global status of all appliances, it displays ON if the cloud acceleration service is turned on; OFF if it is turned off.

3. Click **Disable Acceleration** to stop the cloud acceleration service on all registered appliances. It can take a few minutes for all registered appliances to detect this configuration.

For services under the al-la-carte license, the SaaS Services page also displays this information under Purchased Services:

Parameter	Description
Service serial number	Number assigned to SteelHead SaaS by Riverbed.
Connections	Maximum number of connections optimized for the service that you have purchased.
Bandwidth	Maximum cloud bandwidth allowed for the SaaS platform.
Start Time	Date and time at which the application acceleration starts.
End Time	Date and time at which the application acceleration stops.

The SaaS Platform Proxy Certificate section is used to manage trust between your client machines and SteelHead SaaS. For details, see Chapter 7, “Deploying SteelHead SaaS with Enterprise Proxy.”

Specifying general settings

You specify the concurrently registered SteelHead (maximum number of SteelHeads that can be registered at a time) limit in the Settings > General Settings page.

To specify general settings

1. Log in to the Riverbed Cloud Portal.
2. Select Cloud Accelerator.
3. Choose Settings > General Settings to display the General Settings page.
4. Under Enterprise SteelHead Settings, click **Modify** to change the concurrently registered SteelHead appliance (maximum number of SteelHead appliances that can be registered at a time) limit.
5. Specify the new limit and click **Update**.

Specifying certificate settings

You specify the proxy certificate settings in the Certificate Settings page.

To specify certificate settings

1. Log in to the Riverbed Cloud Portal.
2. Select Cloud Accelerator.
3. Choose Settings > Certificate Settings to display the Certificate Settings page.
4. Select Edit Proxy Certificate Details to display the Proxy Certificate Details dialog box. Updating the settings in this dialog box does not change existing proxy certificates. You must upload or request generation of new proxy certificates for your changes to be applied.
5. In the Proxy Certificate Details dialog box, enter your email, organization (company), organization unit (department), locality, state, and country.
6. Specify the new limit and click **Save Details**.

5

Configuring SteelHead SaaS

You configure SteelHead SaaS in the Optimization > SaaS: Legacy Cloud Accelerator page of the appliance console.

This section includes these topics:

SteelHead SaaS configuration prerequisites

Before you configure SteelHead SaaS on the appliance, ensure that you configure these items:

- DNS (Domain Name System) - Configure and enable DNS. Ensure that the appliance can access the configured name server(s).
- NTP (Network Time Protocol) - Configure and enable NTP and ensure that the NTP server(s) is accessible.
- SSL Configuration - Obtain an SSL license for the SteelHead appliance, and then enable SSL optimization on the Optimization > SSL: SSL Main Settings page of the appliance.

For details about DNS and NTP, see the *SteelHead User Guide*.

To configure SteelHead SaaS

1. Log in to the appliance.
2. Choose Optimization > SaaS: Legacy Cloud Accelerator to display the Legacy Cloud Accelerator page.

Note: The name for this feature has changed from SteelHead Cloud Accelerator to Legacy Cloud Accelerator.

3. Under Cloud Accelerator Control, select the Enable Cloud Acceleration check box to activate the cloud acceleration feature on the appliance.

4. Select the Enable Cloud Acceleration Redirection check box to activate traffic redirection from the appliance to the Akamai network (direct mode). This feature is enabled by default. There are two options for redirection:
   - Direct mode - The appliance redirects traffic to the Akamai network. Leave the Enable Cloud Acceleration Redirection check box selected to use the direct mode.
   - Back-hauled mode - The Data Center SteelHead (DCSH) appliance redirects traffic to the Akamai network for all the branch appliances. So, you must disable cloud acceleration redirection in the branch SteelHead appliances and leave it enabled on the DCSH appliance.
5. In the Redirection Tunnel Port text field, leave the default value (9545) of the port number for the configurable outbound port for UDP connections to the Akamai network as it is. The appliance connected to the Akamai network uses this configurable UDP port over a wide range of IP addresses.

   It is necessary to configure the UDP port 9545 only for outbound connectivity from the in-path IP address of the appliance. If there are multiple in-paths, then the firewall must allow access for each in-path IP address.
6. Under Cloud Accelerator Service Status, click **Refresh Service** to force the appliance to fetch the latest service details from the Riverbed Cloud Portal.
7. Click **Apply** to apply your configuration.

Managing ports through a firewall

When you connect to the network to accelerate SaaS platforms, if you have configured a firewall that blocks outbound traffic, ensure these ports are open:

- Port 443 and port 80 for outbound connections to the Riverbed Cloud Portal. The appliances connect to the Riverbed Cloud Portal through these ports.

Note: Configure the firewall so that it allows connections from the appliance.

- Outbound stateful UDP port 9545 from the SteelHead in-path interface. The appliance connected to the Akamai Intelligent Platform uses this UDP port over a wide range of IP addresses.

In a back-hauled deployment, the data center SteelHead appliance redirects the traffic to the Akamai network, but the Branch SteelHead appliance performs the optimization. Traffic from the Branch SteelHead appliance uses TCP on ports 7800 through 7899. Traffic from the data center SteelHead appliance uses UDP on port 9545.

Modifying ports in a port label

You can add or delete ports associated with a port label in the Port Label: <port label name> page in the SteelHead appliance Management Console.

To modify ports in a port label

1. Choose Networking > App Definitions: Port Labels to display the Port Labels page.
2. Select the port label name in the Port Labels list to display the selected group.

3. Under Editing Port Label <port label name>, add or delete ports in the Ports text box.
4. Click **Apply** to save your settings to the running configuration.
5. Click **Save** to save your settings permanently.

Next steps

After you connect to the Riverbed Cloud Portal, register your appliances, and manage SaaS platforms, you can use the appliance for WAN optimization. Refer to these documents for details on the SteelHead appliance:

- *SteelHead User Guide*
- *SteelHead Deployment Guide*
- *Riverbed Command-Line Interface Reference Manual*

6

Managing Certificates

This chapter describes how to manage certificates in the SteelHead SaaS system. It includes these sections:

SSL certificates overview

You configure certificates on the Riverbed Cloud Portal.

Secure Socket Layer (SSL) is a cryptographic protocol that provides secure communications between two parties over the internet.

An SSL certificate is an electronic document that binds a public key with a specific entity. An SSL certificate is digitally signed. You can send information to the entity securely (the information cannot be read by others during transmission) if you know the public key.

Certificates can be either self-signed or signed by a third-party known as a Certificate Authority (CA).

In a web-based application, it is the client that authenticates the server. To identify itself, an SSL certificate is installed on a web server and the client checks the credentials of the certificate to make sure it is valid and signed.

Each appliance is manufactured with its own self-signed certificate and private key that uniquely identifies it. Peer appliances authenticate each other by exchanging certificates and negotiating a separate encryption key for each intercepted connection. These certificates are called *peering certificates.*

You can use one or both of these types of peering certificates in the Riverbed Cloud Portal on the client side:

- **ESH self-signed peering certificate** - The self-signed peering certificate that uniquely identifies the appliance.
- **ESH CA-signed peering certificate** - Certificate signed by a trusted CA and installed on the appliance.

Prerequisites for configuring SSL certificates

Before you configure SSL certificates on the appliance, ensure that your system meets these prerequisites:

- The SteelHead SaaS appliance has a valid (not expired) SSL certificate.
- The SteelHead SaaS appliance has a valid SSL license installed.
- You have enabled SSL optimization on the appliance.
- You have removed port 443 from the secure ports label list (choose Networking > App Definitions: Port Labels, select the Secure Label, remove port 443, and click **Apply**).
- The primary interface of the appliance is connected and configured with valid DNS server entries.
- The SteelHead SaaS appliance has NTP configured and at least one NTP server is accessible.
- The firewall allows outbound access for ports 80 and 443 from the primary interface.

For details about SSL configuration, see the *SteelHead Deployment Guide*.

Configure the Riverbed Cloud Portal to trust SteelHead peering certificates

To use a SteelHead appliance with the SteelHead SaaS platform, the appliance must be registered with the Riverbed Cloud Portal and the appliance's peering certificate must be uploaded to the Riverbed Cloud Portal. You can configure the portal to automatically trust and upload SteelHead appliance peering certificates.

To configure the Riverbed Cloud Portal to trust SteelHead appliance peering certificates

1. Select Secure Peering to display the Secure Peering page.
2. Select the Enterprise SteelHead Peering Certificates tab.
3. Select the Trust Enterprise SteelHead Appliance Peering Certificates check box:
   - Each registered appliance uploads its peering certificates to the Riverbed Cloud Portal.
   - The Riverbed Cloud Portal forwards all of the uploaded Enterprise SteelHead appliance peering certificates to the Akamai network.

   After the appliance uploads the peering certificate, the certificate record appears in the Trusted Enterprise SteelHead Appliance Peering Certificates table in the Riverbed Cloud Portal.

To stop the automatic trusting and uploading of SteelHead appliance peering certificates

- Clear the Trust Enterprise SteelHead Appliance Peering Certificates check box. If you clear the check box, the Riverbed Cloud Portal deletes its records of the peering certificates; however, the peering certificates remain on the appliance itself.

To upload a new peering certificate

- Click **Upload**.

To delete a peering certificate

1. Find the certificate in the Trusted Enterprise SteelHead Appliance Peering Certificates table.
2. Click **Delete**.
3. Click **Confirm**.

   Appliances using the certificate will no longer be trusted by other appliances on the SteelHead SaaS platform.

Viewing cloud-hosted peering CA certificates

During normal operation, the appliance automatically downloads the latest certificate, used to sign all cloud-hosted SteelHead peering certificates, from the Riverbed Cloud Portal. You do not need to download the cloud-hosted peering CA certificates.

There is only one CA that signs all cloud-hosted SteelHead appliance peering certificates.

To view the cloud-hosted peering CA certificate

1. Select Secure Peering to display the Secure Peering page.
2. Select the Cloud-Hosted Peering CA tab to display the Cloud-Hosted Peering CA Certificate page.
3. Click **View Cloud Accelerator Peering CA Certificate**.

Viewing event log

You view the event log for the appliance in the Secure Peering page.

1. Select Secure Peering to display the Secure Peering page.
2. Select the Event Log tab to display the Event Log page.

Configuring SaaS proxy certificates

Proxy certificates are certificates specific to a particular SaaS domain that are signed by a CA trusted by the client applications inside your network. SaaS proxy certificates allow the cloud-hosted SteelHead to intercept and accelerate secure sessions between the SSL-based client and server applications.

Note: SteelHead SaaS does not support self-signed SaaS proxy certificates; it only supports CA-signed SaaS proxy certificates.

Proxy certificates can come from either of these sources: a third-party, cloud-hosted CA, or a CA within your enterprise.

To change the type of Certificate Authority

1. Log in to the Riverbed Cloud Portal.
2. Select Cloud Accelerator to display the Cloud Accelerator page.
3. Select SaaS Platforms to display the SaaS Platforms page.
4. Under Proxy Certificate Authority, the CA used to sign the SaaS server proxy certificates appears. Click **change mode** to select one of these options:
   - Cloud-Hosted CA - In this mode a third-party, cloud-hosted CA signs the proxy certificates.
   - Customer CA - In this mode your company's CA signs the proxy certificates.

In the SaaS Platforms page, under Manage SaaS Platforms, select the name of a SaaS platform listed in the table to display the SaaS Service Details page. The section under SaaS Platform Proxy Certificates changes depending on the CA mode that you select on this SaaS Platforms page.

To use proxy certificates issued by a third-party, cloud-hosted CA

1. Select Cloud Accelerator to display the Cloud Accelerator page.
2. Select SaaS Platforms to display the SaaS Platforms page.
3. Under Proxy Certificate Authority, click **change mode** and select the Cloud-Hosted CA mode.
4. Click **View/Download CA Certificate** to download the CA certificate from the Riverbed Cloud Portal.
5. Install the certificate on all clients that access the SaaS application by either:
   - adding it directly to the client's browser.

     or
   - adding it to the certificate store of the client's Windows operating system.
6. Optionally, click **Request New Proxy Certificate Authority** to regenerate the proxy CA and confirm your request.

Note: Regenerating the proxy CA might disrupt existing SSL connections.

7. In the SaaS Platforms page, under Platform, click the name of the platform to display the SaaS Service Details page.
8. Under SaaS Platform Proxy Certificate, select the Proxy Certificates tab to display the list of SaaS hostnames and their proxy certificate status.
9. Select Request New Proxy Certificate (in the last column) to regenerate the proxy certificate for the SaaS platform and sign it using the trusted CA.
10. Import the certificate into your preferred browser on the client system. Consult your browser vendor's documentation for details about how to import proxy certificates.

To use proxy certificates issued by your enterprise CA

1. Select Cloud Accelerator to display the Cloud Accelerator page.
2. Select SaaS Platforms to display the SaaS Platforms page.
3. Under Proxy Certificate Authority, click **change mode**.
4. Select the Customer CA mode and then click **Update**.
5. In the SaaS Platforms page, under Platform, select the name of the platform.
6. Under SaaS Platform Proxy Certificate, select the Proxy Certificates tab to display the list of SaaS hostnames and their Certificate Signing Request (CSR) status.
7. Select Generate New CSR (in the last column of the table) to generate a new CSR for that SaaS hostname.
8. Select Download CSR in the table to download the CSR that you generated for your computer.
9. Use the CSR to obtain your CA's signature on your proxy certificate.
10. Select Upload Certificate in the table (next to the specific SaaS hostname).
11. Select the signed proxy certificate from your local file system or copy and paste the certificate details and click **Upload** to upload the proxy certificate for the specific SaaS hostname.

Viewing proxy certificate logs

The Log page displays this information.

Control	Description
Level	Severity level of the log. The log contains all messages with the selected level or higher. You can change the depth of the log information by selecting a severity level from the drop-down menu: ▪ **Critical** - Conditions that affect the optimization service. ▪ **Error** - Conditions that probably affect the functionality of the appliance. ▪ **Warning** - Conditions that affect the functionality of the appliance. ▪ **Notice** - Normal but significant conditions, such as a configuration change. ▪ **Informational** - Messages that provide general information about system operations. ▪ **Debug** - Messages that help you debug a failure.
Records	Maximum number of records to display. The default value is 20.
Timestamp	Date and time at which the event occurred. Select the arrow to sort this column in descending order.
ID	System-generated identification number for the log.
IP Address	IP address of the client machine that initiated the action.
User	Name of the user who performed the action.

Control	Description
Log Level	Severity level of the log message.
Message	Log message that describes the action that occurred.

7

Deploying SteelHead SaaS with Enterprise Proxy

This chapter describes how to configure chained interception for accelerating SaaS platform traffic when explicit proxy is set up in the enterprise network.

After you complete the tasks in this chapter, user connections to SaaS providers through the enterprise proxy server are optimized by two pairs of SteelHead appliances to achieve best performance.

This chapter includes these sections:

Overview

Most enterprises today require that internet traffic go through a web proxy server for performance and security. The proxy server is typically deployed as an out-of-path server in the enterprise network.

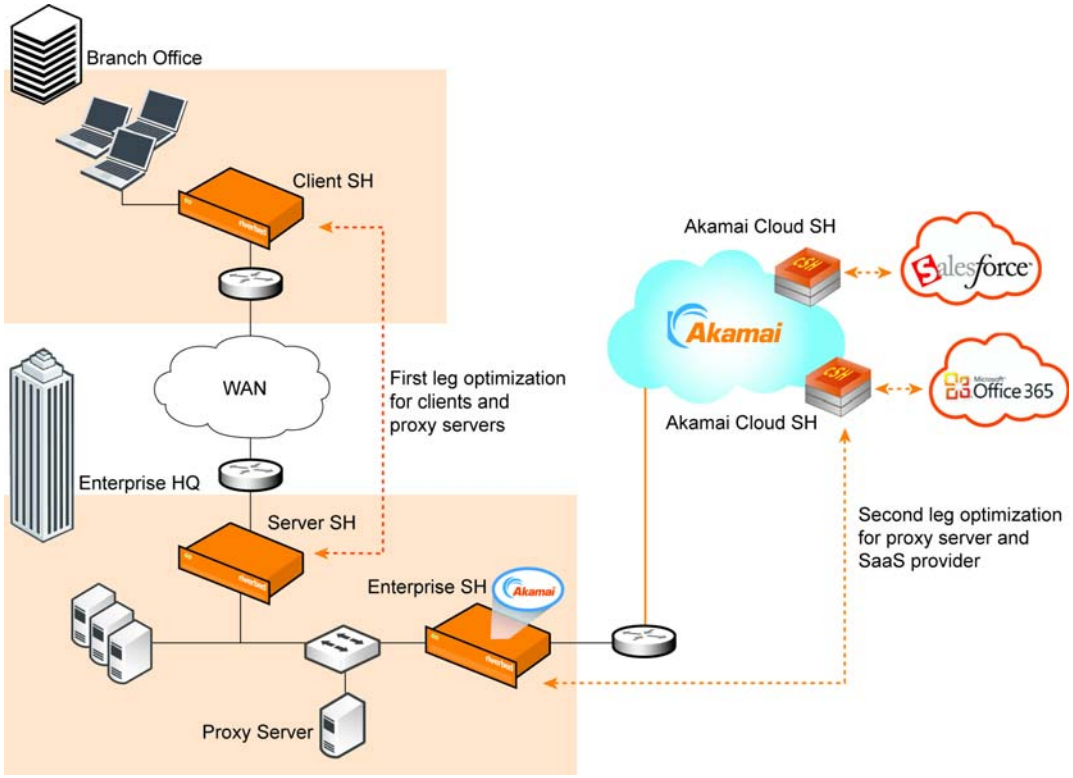
You can configure the proxy server to intercept the traffic in these deployments:

- **Transparent proxy deployment** - This method uses packet redirection mechanisms, such as Layer-4 switch, WCCP, or policy-based routing (PBR) for packet redirection.
- **Explicit proxy deployment** - In this method, you configure browsers to communicate with the proxy server for internet traffic using an automatic script or hard-coded configuration. When you access a secure web server through an HTTPS connection, the browser tunnels HTTPS requests to the proxy server by sending HTTP CONNECT requests. If you are deploying an explicit proxy server, it might not terminate the SSL connections. Use the configuration described in the section "Configuring the first optimization phase" on page 50.

To deploy SteelHead SaaS in a network with a proxy server, you must set up chained optimization to obtain maximum performance. In chained optimization, a single request is optimized by two separate pairs of SteelHead appliances. The first SteelHead appliance pair optimizes the front-end proxy requests. The second pair intercepts the proxy server requests from the ESH to the Akamai Cloud SteelHead appliance.

To deploy the chained optimization, set up the first pair of SteelHead appliances to optimize SSL proxy requests from the client to the proxy server and then set up the second pair of SteelHead appliances to optimize the HTTPS request from the proxy server to the SaaS server.

Figure 7-1. Network topology with a proxy server



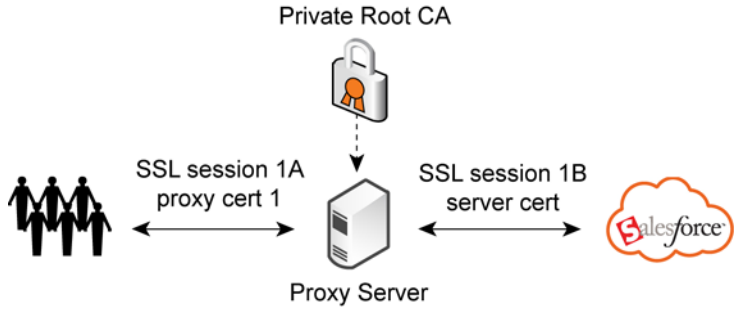
Test and verify one pair of SteelHead appliances to optimize the traffic before you set up the second pair.

Understanding chained interception

In an explicit proxy setup, the client connects to the proxy server for outbound internet HTTPS requests, and then the proxy server establishes a separate TCP session to perform an SSL handshake with the SaaS platform server.

To intercept SSL connections, the proxy server replaces the certificate from the original server with a new certificate signed by an internal private-hosted root CA. Your browser must trust the internal private-hosted root CA to validate the certificate returned by the proxy server.

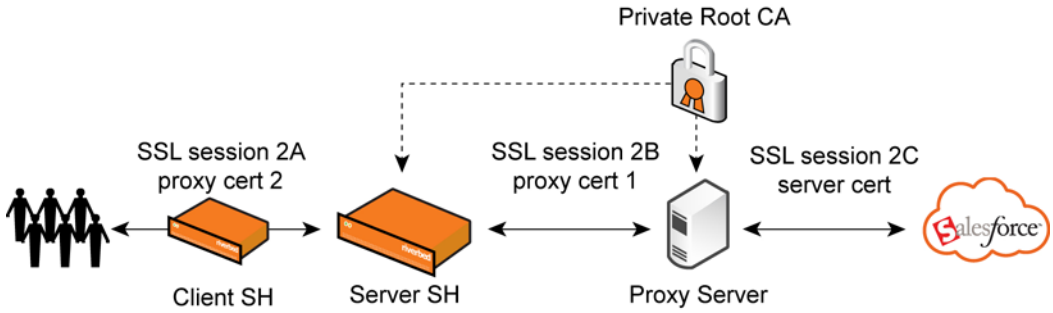
Figure 7-2. Proxy certificate generation



Install the HTTPS server certificate and the private key on the server-side SteelHead appliance for the first pair of SteelHead appliances to optimize SSL proxy connections. You cannot import the server certificate and the private key to the server-side SteelHead appliance because the proxy server dynamically issues the proxy certificate with the root CA.

You must generate a new set of the certificate and the private key (for proxy cert2) for each SaaS platform server to optimize the proxy connections. The certificate is signed by an internal private root CA; you must import the private root CA to the server-side SteelHead appliance.

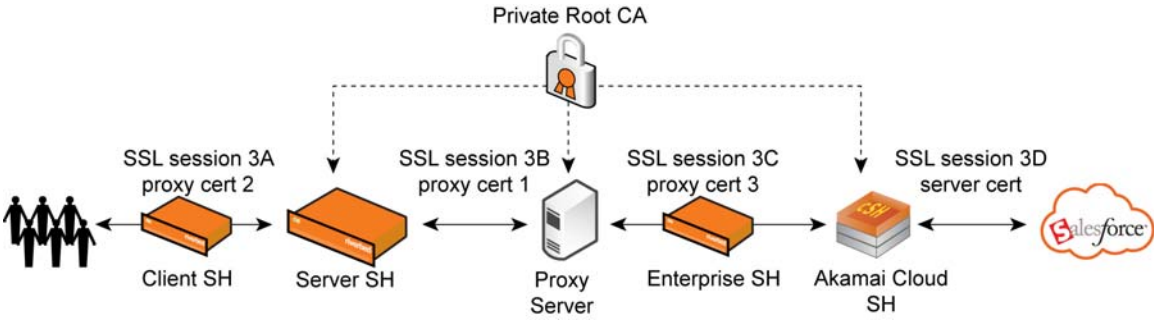
Figure 7-3. Proxy certificate installation



For the second pair of SteelHead appliances optimizing using SteelHead SaaS, the Riverbed Cloud Portal manages the proxy certificates for SteelHead SaaS. You can use a customer-hosted CA as the proxy server root CA to sign the CSR that is generated from the Riverbed Cloud Portal for SaaS platform servers. Because the Riverbed Cloud Portal generates the SaaS platform server proxy CSR and private key, you cannot download the private key; therefore, you must ensure that the new set of proxy certificates are signed.

In Figure 7-4, the Akamai Cloud SteelHead appliance returns the proxy cert3 for the second optimization phase to the proxy server (client).

Figure 7-4. Riverbed Cloud Portal managing proxy certificate



The deployment described here assumes that the same internal private root CA installed on the proxy server is the root CA that signs proxy certificates for these appliances:

- Server-side SteelHead appliance.
- Akamai Cloud SteelHead appliance.
- All of the peering certificates on the client SteelHead appliance, server-side SteelHead appliance, and the Enterprise SteelHead appliance (ESH).

Configuring the first optimization phase

This section describes how to configure the first optimization phase.

Prerequisites

Before you configure the first optimization phase, ensure that:

- non-SSL traffic is optimized between the client SteelHead appliances and server-side SteelHead appliance.
- users access SaaS platform service through an enterprise proxy server.
- an in-path rule is configured to pass through the proxy SSL request on the client SteelHead appliance.
- both the client SteelHead appliance and server-side SteelHead appliance are running RiOS v.7.0 or later.
- the SteelHead appliance has a valid SSL license installed. If you are configuring an explicit proxy, it might terminate the SSL connections.
- the SteelHead appliance has a valid (not expired) SSL peering certificate.
- the server-side SteelHead appliance has a valid SSL server certificate and private key for each SaaS platform server.
- you generate a separate CSR and private key outside of the Riverbed Cloud Portal for the server-side SteelHead appliance because you cannot share and install the private key (generated by the Riverbed Cloud Portal) on the server-side SteelHead appliance.

- client browsers have the internal CA certificate installed to validate the proxy certificate returned by the server-side SteelHead appliance and the proxy server.
- you obtain a copy of the internal root CA certificate from the proxy server for the server-side SteelHead appliance.
- you determine the secure port for SSL proxy requests by reviewing the proxy automatic file (.pac), automatic configuration script, or the browser proxy setting. The deployment described in this document uses port 8080 for SSL proxy on the proxy server.

Configuring peer SSL certificates

This section describes how to install a peer certificate that is presigned by the internal root CA for the SSL connection between the client SteelHead appliance and the server SteelHead appliance.

By default, the SteelHead appliance has a self-signed certificate out of the box. If you do not require a signed certificate, you can configure a self-signed peering certificate.

To configure peer SSL certificates

1. Choose Optimization > SSL: Secure Peering (SSL) on the SteelHead appliance to display the Secure Peering (SSL) page.
2. Under Certificate, select Replace, choose Import Existing Private Key and CA-Signed Public Certificate and click **Import Key and Certificate**.
3. Access the same page from the SteelHead appliance management console, import the internal root certificate that signs the peering certificates, and click **Add**.
4. Repeat steps 1 through 3 on the peer SteelHead appliance.

Importing the internal root certificate

This section describes how to import the internal root certificate to the server SteelHead appliance.

1. Choose Optimization > SSL: Certificate Authorities on the server SteelHead appliance to display the Certificate Authorities page.
2. Under Certificate Authorities, complete the configuration as described in this table.

Control	Description
Add a New Certificate Authority	**Optional Local Name (ignored if importing multiple certificates)** - Specify the local name.
	Local File - Browse to the local file.
	Cert Text - Paste the into the text box and click **Add**.
Add	Adds the certificate authority.
Remove Selected	Select the check box next to the name and click **Remove Selected**.

Enabling SSL proxy support

You must enable SSL proxy support on both the client and server SteelHead appliance.

1. On the client SteelHead appliance, choose Optimization > SSL: Advanced Settings to display the Advanced Settings page.
2. Under Proxies, select the Enable SSL Proxy Support check box.
3. Repeat steps 1 and 2 on the server SteelHead appliance.

Enabling SSL optimization

You must enable SSL optimization on both the client and server SteelHead appliance.

1. On the client SteelHead appliance, choose Optimization > SSL: SSL Main Settings to display the SSL Main Settings page.
2. Under General SSL Settings, select the Enable SSL Optimization check box.
3. Repeat steps 1 and 2 on the server SteelHead appliance.

Intercepting SSL proxy requests

This section describes how to configure intercepting the SSL proxy requests between the client SteelHead appliance and server SteelHead appliance.

By default, the client and server traffic is optimized by the two endpoint SteelHead appliances. To allow chained optimization, you can either disable enhanced auto-discovery on the server side SteelHead appliance or set up a peering rule to accept the SSL proxy requests at the server side SteelHead appliance.

If you use port 443 as the default proxy port for SSL proxy service from the client to the proxy server, remove port 443 from the secure ports lists.

Modifying ports in a port label

You can add or delete ports associated with a port label in the Port Label: <port label name> page.

To modify ports in a port label

1. Choose Networking > App Definitions: Port Labels on the client SteelHead appliance to display the Port Labels page.
2. Select the port label name in the Port Labels list to display the Editing Port Labels Interactive group.

3. Enter your changes in the Ports text box.
4. Click **Apply** to save your settings to the running configuration.
5. Click **Save** to save your settings permanently.
6. Repeat steps 1 through 5 on the server SteelHead appliance.

Configuring peering rules

For the initial set up, configure a source subnet with a small test group.

To add a peering rule on the server SteelHead appliance

1. Choose Optimization > Network Services: Peering Rules to display the Peering Rules page.
2. Select the rule type Accept. The SteelHead appliance accepts peering requests that match the source-destination-port pattern. The receiving SteelHead appliance responds to the probing SteelHead appliance and becomes the remote-side SteelHead appliance (that is, the peer SteelHead appliance) for the optimized connection.
3. Specify 2 for Insert Rule At. The system evaluates rules in numerical order starting with rule 1. If the conditions set in the rule do not match, then the system moves on to the next rule until a rule matches. If it matches, then the rule is applied and no further rules are consulted. For example, if the conditions of rule 1 do not match, rule 2 is consulted. If rule 2 matches the conditions, it is applied, and no further rules are consulted.
4. Specify the proxy server IP and proxy port for proxy requests for the destination subnet. For example, 10.35.80.225/32:8080.
5. Select Capable for SSL Capability. The peering rule determines that the connection is SSL-capable if the destination port is 443 (irrespective of the destination port value on the rule), and the destination IP and port do not appear on the bypassed servers list. The SteelHead appliance accepts the condition and, assuming all other proper configurations and that the peering rule is the best match for the incoming connection, optimizes SSL.
6. Click **Add**.

Configuring the SteelHead appliances for SaaS providers

This section describes the configurations specific to SaaS applications.

Configuring the SteelHead appliances for Microsoft Office 365 (O365) with Outlook

Ensure that you set up this items to configure the first pair of SteelHead appliances for O365 with Outlook:

- Enable encrypted optimization.
- Disable MAPI acceleration module for chained optimization.

- Enable Outlook Anywhere optimization.
- Enable Auto-Detect Outlook Anywhere Connections.
- Enable MAPI encryption for Office 365 on the server-side SteelHead appliance.

To configure O365 with Outlook

1. Establish a Secure Shell (SSH) session to the client SteelHead appliance and enter these commands:

```
enable
configure terminal
protocol mapi encrypted enable
protocol mapi encrypted only
protocol mapi outlook-anywhr auto-detect
protocol mapi outlook-anywhr enable
service restart
```

2. Establish an SSH session to the server-side SteelHead appliance and enter these commands:

```
enable
configure terminal
protocol mapi encrypted only
protocol mapi outlook-anywhr auto-detect
protocol mapi outlook-anywhr enable
service restart
```

HTTP configuration for browser-based applications

Perform these steps for browser-based applications:

1. Log in to the client SteelHead appliance.
2. Choose Optimization > Protocols: HTTP to display the HTTP page.
3. Under Server Subnet and Host Settings:
   - Specify the server subnet.
   - Select the Object Prefetch Table check box.
4. Click **Add** to add the server subnet.

Verifying the first optimization phase

This section describes how to verify the first optimization phase with a limited subnet and for the whole branch. You verify optimization by creating an in-path rule and inserting it before the pass-through rule and then removing the pass-through rule that you added as a prerequisite (for details, see “Prerequisites” on page 50).

To verify the first optimization phase with a limited subnet

1. Choose Optimization > Network Services: In-Path Rules to display the In-Path Rules page.
2. Create a new in-path rule and place it before the pass-through rule with a specific IP range as the source subnet.
3. Specify the proxy server IP address in the destination subnet and the proxy port as the destination subnet port.
4. Click **Add** to add the in-path rule.
5. Sign in to the SaaS provider account from the client.
6. From the client or server SteelHead appliance, choose Reports > Networking: Current Connections to display the current connections report.
7. Check that the Destination:Port column contains the Proxy Server IP address and port number.

To verify optimization for the whole branch

1. Remove the pass-through rule that you added as a prerequisite (“Prerequisites” on page 50).
2. Choose Optimization > Network Services: In-Path Rules to display the In-Path Rules page.
3. Specify all-IPV4 as the source IP address.
4. Click **Add** to add the in-path rule.

Configuring the second optimization phase

This section describes how to configure the second optimization phase.

Prerequisites

Before you configure the second optimization phase, ensure that your system meets these prerequisites:

- The SteelHead is running the latest RiOS version with the SteelHead SaaS feature enabled.
- The SteelHead appliance has a valid SSL license installed.
- The SteelHead appliance has a valid (not expired) SSL certificate for peering.
- SSL optimization is enabled on the SteelHead appliance.
- Port 443 is removed from the Secure ports label list.
- The primary interface of the SteelHead appliance is connected and configured with valid DNS server entries.
- The SteelHead appliance has NTP configured and that at least one NTP server is reachable.
- You have an account on the Riverbed Cloud Portal.

- The firewall allows outbound access for ports 80 and 443 from the primary interface. Also, if you use external DNS and or NTP server(s), ensure that you allow outbound port 53 and 123 respectively. Ensure that the stateful feature is enabled for UDP packets.
- The firewall allows outbound UDP port 9545 from the in-path interface of the SteelHead appliance. If there are multiple in-path interfaces, then the firewall must allow outbound access to UDP port 9545 from the IP address of each in-path interface. Also, ensure that the stateful feature is enabled on the firewall to allow for returning UDP packets.
- You have an account with your SaaS provider.
- If another administrator or group is signing the SaaS proxy certificates, you must generate the CSR from the Riverbed Cloud Portal.

Managing peer certificates and customer-signed proxy certificates

1. Log in to the Riverbed Cloud Portal.
2. Select Cloud Accelerator to display the SteelHead SaaS page.
3. Select Secure Peering to display the Secure Peering page.
4. Choose Settings > Certificate Settings on the left panel to display the Certificate Settings page and view the proxy certificates.
5. To generate the CSR for each platform server, select SaaS Platforms to display the Manage SaaS Platforms page.
6. Select a SaaS platform in the Platform column.
7. Under SaaS Platform Proxy Certificates, click **Generate New CSR** for the corresponding SaaS hostname.
8. Under SaaS Platform Proxy Certificates, click **Download CSR** for the corresponding SaaS hostname.
9. Take the CSR to your internal root CA and have it signed.
10. After the certificates are signed, return to the Salesforce.com Details page.
11. Under SaaS Platform Proxy Certificates, click **Upload Certificate** for the corresponding SaaS hostname.

Note: It might take up to 15 minutes for the certificates to be processed.

Registering appliances with the Riverbed Cloud Portal

1. Log in to the appliance's management console.
2. Choose Optimization > Network Services: In-Path Rules to display the In-Path Rules page.
3. Select the Pass Through option from the drop-down menu for both Type and Cloud Acceleration to pass through the proxy server request until the SteelHead appliance is set up.
4. Log in to the Riverbed Cloud Portal.
5. Select Cloud Accelerator to display the SteelHead SaaS page.
6. On the left panel, click **Appliance Registration Key** to display the Appliance Registration Key page.
7. Copy the Appliance Registration Key from this page into a text editor such as Notepad.
8. Return to the management console and choose Optimization > SaaS: Legacy Cloud Accelerator to display the Legacy Cloud Accelerator page.
9. Paste the Appliance Registration Key into the text box and click **Register**.
10. Choose Optimization > SaaS: Legacy Cloud Accelerator again to display the Legacy Cloud Accelerator page.
11. Under Cloud Accelerator Control, select the Enable Cloud Acceleration check box and also the Enable Cloud Acceleration Redirection check box. Specify 9545 as the Redirection Tunnel Port.
12. Click **Apply** to apply your changes to the running configuration.
13. Log in to the Riverbed Cloud Portal.
14. Select Enterprise SteelHead Appliance on the left panel to display the ESH page.
15. Under SteelHead Appliances Pending Service, select the ESH and click **Grant Service** to grant the ESH access to the Riverbed Cloud Portal.

    The system moves the ESH to the SteelHead Appliances Granted Service table.
16. Go back to the SteelHead management console and choose Optimization > SaaS: Legacy Cloud Accelerator to display the Legacy Cloud Accelerator page.
17. Click **Refresh Service** to display the SaaS platform service that you subscribe to (at the bottom of the page).
18. Check that you completed the SaaS platform-specific configurations on the SteelHead appliance. For details, see "Configuring the SteelHead appliances for SaaS providers" on page 53.
19. Log in to the SteelHead management console and choose Optimization > Network Services: In-Path Rules to display the In-Path Rules page.

20. Modify the pass-through rule that you created when you registered the ESH with the Riverbed Cloud Portal to Auto Discover. For details, see “Registering appliances with the Riverbed Cloud Portal” on page 57.

21. If you want to use SMTP-over-SSL (port 587) or IMAP-over-SSL (port 993), then create two more rules and specify the correct port number.

Verifying the second optimization phase

After you set up and configure the second optimization phase, you can verify this phase.

To verify the second optimization phase

1. Sign in to the SaaS provider account from the client.

2. Log in to the SteelHead management console and choose Reports > Networking: Current Connections to display the Current Connections report.

3. Verify that the Destination:Port column contains the SaaS server IP address and port.

A

Troubleshooting

This section describes how to enable logging on an ESH and how to troubleshoot issues:

Enabling info logging level

Before you do any troubleshooting, ensure that information-level logging is enabled on the SteelHead. Enter this command on the SteelHead command line:

```
amnesiac # enable
amnesiac # configure terminal
amnesiac(config)# logging local info
```

Troubleshooting issues

This section describes solutions for common issues.

Cannot invoke and run SteelHead SaaS

If you cannot run SteelHead SaaS, try one of these solutions.

Solution #1

Verify that your SteelHead SaaS subscription is valid and acceleration service is turned on using these steps:

1. In the Riverbed Cloud Portal, select the Cloud Accelerator tab.
2. Select SaaS Platforms.
3. Select a SaaS platform to view its Details page.
4. Check that the Start Time and the End Time are valid.

- The Active columns should display **true** and the Terminated column should display **false**.
- The Acceleration Service should be ON.

If you are trying multiple SaaS Providers, verify this for each provider.

Figure 7-5. SaaS details page

Solution #2

Check that the SteelHead is communicating with the Riverbed Cloud Portal using these steps:

1. In the Riverbed Cloud Portal, select the Cloud Accelerator tab.
2. Select Enterprise SteelHead Appliances. Verify that the serial number of the ESH is listed in either the Pending, Granted, or Denied sections.
3. Check the output of the **show service cloud-accel** command. The Reason field indicates the current status of the ESH.
4. Perform one of these actions:
   - If the reason is Disabled by administrative action and Enabled is Yes, the ESH might have been denied service by the Riverbed Cloud Portal or unregistered from the ESH. You must register the ESH again.

     ```
     ESH # show service cloud-accel
       Enabled:              Yes
       Status:               Unregistered
       Reason:               Disabled by administrative action (Tue Aug 21
       Portal:               cloudportal.riverbed.com:443 (HTTPS)
       Redirection:          Enabled
         Port:               9545
         State:              Active
         Spill-over Policy: Disabled
     ESH #
     ```

   - If the reason is Disabled by administrative action and Enabled is No, the ESH might have been denied service by the Riverbed Cloud Portal or unregistered from the ESH. Also, the SteelHead SaaS service was disabled on the ESH.

     ```
     ESH # show service cloud-accel
       Enabled:              No
       Status:               Unregistered
       Reason:               Disabled by administrative action (Tue Aug 21
       Portal:               cloudportal.riverbed.com:443 (HTTPS)
       Redirection:          Enabled
         Port:               9545
       State:              Inactive
       Spill-over Policy: Disabled
     ESH #
     ```

   - If the reason is **Appliance is Pending Service**, you must grant access to the ESH on the Riverbed Cloud Portal. For details, see “Enabling and disabling optimization services on registered appliances” on page 32.

- If the reason is **Couldn't resolve host name**, check DNS settings on the ESH. SteelHead SaaS uses the SteelHead appliance DNS settings. When you change DNS settings, remember to disable and reenable the cloud acceleration service on the ESH.

5. Enter the **service cloud-accel enable** command to enable SteelHead SaaS service on the ESH.

6. Enter the **service cloud-accel register <key> command** to reregister the ESH.

The connections are passed through because there is no SteelHead appliance on the path to the server

If this problem occurs, try one of these solutions.

Solution #1

Verify that your default gateway is correct for the in-path interface. Verify that the SteelHead appliance has IP connectivity and that the Akamai Cloud Proxy feature uses the in-path interface to reach the Akamai network.

Solution #2

If the server IPs belong to a SaaS application that you believe should be optimized through cloud accelerator, there might be an issue with the IP list maintained for SteelHead SaaS optimization. Please contact Riverbed Support to assist with this issue.

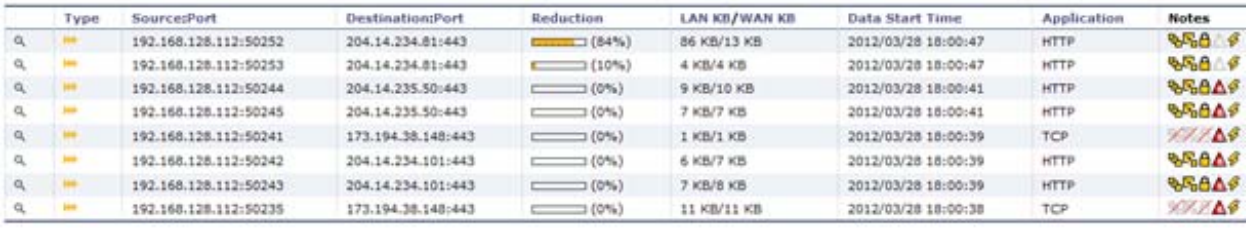
Some connections result in protocol errors

If this problem occurs, try this solution.

Solution

Protocol errors from some connections is expected behavior because the system does not optimize every single SSL connection. For example, in this figure (Figure 7-6), connections to www.salesfore.com (204.14.235.50) and login.salesforce.com (204.14.234.101) are not optimized (not SSL decrypted). However, connections to na2.salesforce.com (204.14.234.81) are optimized.

Figure 7-6. Optimized and unoptimized connections



	Type	Source:Port	Destination:Port	Reduction	LAN KB/WAN KB	Data Start Time	Application	Notes
		192.168.128.112:50252	204.14.234.81:443	(84%)	86 KB/13 KB	2012/03/28 18:00:47	HTTP	
		192.168.128.112:50253	204.14.234.81:443	(10%)	4 KB/4 KB	2012/03/28 18:00:47	HTTP	
		192.168.128.112:50244	204.14.235.50:443	(0%)	9 KB/10 KB	2012/03/28 18:00:41	HTTP	
		192.168.128.112:50245	204.14.235.50:443	(0%)	7 KB/7 KB	2012/03/28 18:00:41	HTTP	
		192.168.128.112:50241	173.194.38.148:443	(0%)	1 KB/1 KB	2012/03/28 18:00:39	TCP	
		192.168.128.112:50242	204.14.234.101:443	(0%)	6 KB/7 KB	2012/03/28 18:00:39	HTTP	
		192.168.128.112:50243	204.14.234.101:443	(0%)	7 KB/8 KB	2012/03/28 18:00:39	HTTP	
		192.168.128.112:50235	173.194.38.148:443	(0%)	11 KB/11 KB	2012/03/28 18:00:38	TCP	

How do I know my traffic is redirected to the SRIP network?

If this problem occurs, try this solution.

Solution

From a Windows PC, do a traceroute (tracert) to a SaaS provider server and observe the IP address of the first hop. If the first hop is not the IP address of your default gateway, then the packets are redirected into the SRIP network.

```
Default gateway is 192.168.128.1

C:\>tracert ch1prd0410.outlook.com

Tracing route to ch1prd0410.outlook.com [157.56.244.182]
over a maximum of 30 hops:

  1    23 ms    38 ms    19 ms  58.27.86.183   <--- SRIP-Edge
  2   305 ms   236 ms   234 ms  198.63.231.204 <--- SRIP-Gateway
  3   235 ms   235 ms   237 ms  be-5.r05.chcgil09.us.bb.gin.ntt.net [131.103.136.1]
  4   235 ms   265 ms   237 ms  0.xe-10-2-0.BR3.CHI13.ALTER.NET [204.255.168.69]
  5   234 ms   239 ms   236 ms  0.ae3.XL4.CHI13.ALTER.NET [152.63.66.77]
  6   237 ms   235 ms   236 ms  TenGigE0-5-2-0.GW2.CHI13.ALTER.NET [152.63.67.106]
  7   268 ms   415 ms   417 ms  microsoft-gw.customer.alter.net [63.84.96.94]
  8   240 ms   238 ms   239 ms  xe-3-0-1-0.ch1-16c-1a.ntwk.msn.net [207.46.46.153]
  9   236 ms   235 ms   238 ms  xe-5-0-0-0.ch1-96c-1b.ntwk.msn.net [207.46.46.125]
.
.
.
```

The error message “Inner channel is not secure” appears

If this problem occurs, try this solution.

Figure 7-7. Connection details

Solution

If the connection details display the error message “Inner channel is not secure,” then there is an issue with peering between the SteelHead appliance and the cloud. Check the validity of the peering certificate and ensure that the Peering Trust list contains the appropriate CA.

When I access the SaaS provider’s website, my browser displays an error message about the SSL security certificate

The browser displays the error message “There is a problem with this website’s security certificate.”

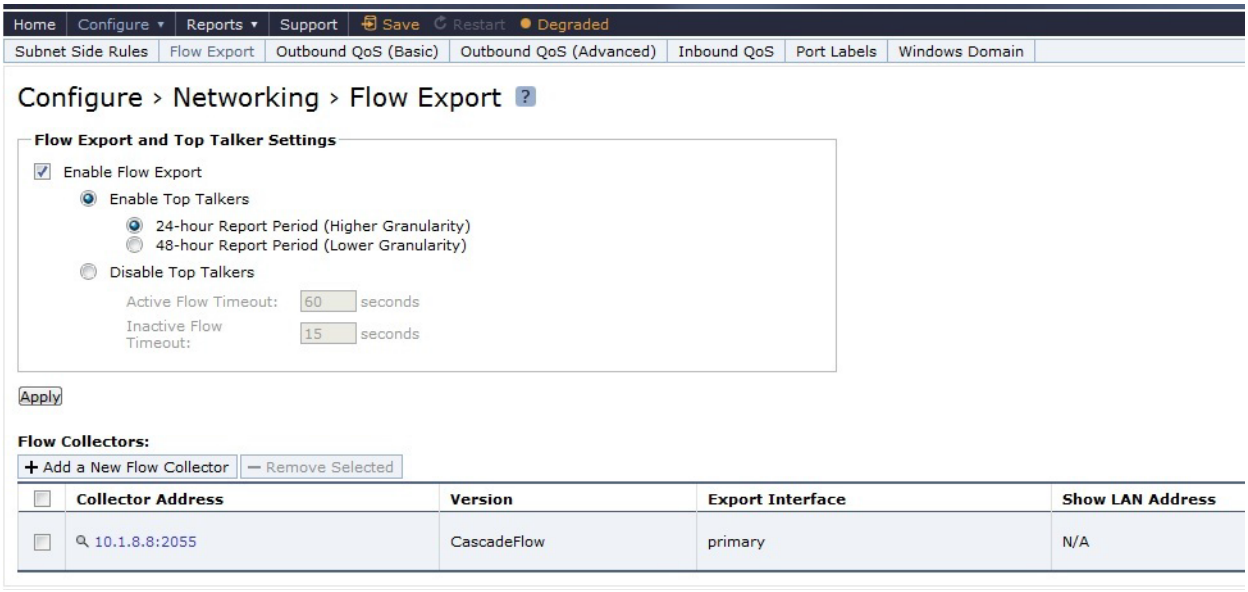
Solution

Ensure that the CA (CA that signed the Proxy Certificate) root certificate is installed correctly on your computer.

A flow collector is configured to capture flow from the WAN port of my SaaS-enabled SteelHead but the SaaS traffic is not being classified correctly, and the corresponding rbtpipeX_X is not displayed in the Capture Interfaces list

If this problem occurs, try this solution.

Figure 7-8. The flow export page displays the capture interfaces list



Solution

This issue can happen if SaaS/Cloud Accelerator is enabled on the SteelHead after the flow collector was configured. In this scenario all SaaS traffic is reported only as a single UDP flow on the WAN.

For normal TCP flow reporting of SaaS traffic, reenable the flow collector.

The rbtpipeX_X associated with a flow collector that is configured to capture SaaS flow continues to be displayed in the Capture Interfaces list even though SaaS is disabled on the SteelHead

If this problem occurs, try this solution.

Solution

1. Disable the flow collector.
2. Disable SaaS on the SteelHead.
3. Reenable the flow collector.
4. Confirm that the rbtpipeX_X associated with the flow collector is no longer displayed in the Capture Interfaces list.

Note: This is a display-only issue, which does not impact functionality of SaaS or flow-collection in any way.