riverbed®

SaaS Accelerator User Guide

SteelConnect 2.12 or later

SteelHead 9.8.1 or later

SteelCentral Controller for SteelHead (SCC) 9.9.1 or later

SteelHead Mobile 6.1.0 or later

SteelFusion Edge 6.0.2 or later

December 2019

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

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

Part Number
712-00112-08

Contents

Welcome

Welcome to the *SaaS Accelerator 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" on page 5
- "Documentation and release notes" on page 6
- "Contacting Riverbed" on page 6

About this guide

The *SaaS Accelerator User Guide* describes the Riverbed Software as a Service (SaaS) acceleration service managed by SteelConnect.

Note: 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 SaaS Accelerator, a checklist for setup and configuration, instructions for deployment, and troubleshooting information to solve common issues.

This guide includes information relevant to these products:

- Riverbed SaaS Accelerator
- Riverbed SteelHead CX appliance
- Riverbed SteelHead Mobile
- Riverbed SteelCentral Controller for SteelHead (SCC)
- SteelFusion Edge
- Riverbed SteelConnect

Audience

This guide is written for storage and network administrators familiar with 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. For details, see the *SteelHead User Guide*.
- using SteelConnect Manager (SCM). For details, see the *SteelConnect Manager User Guide*.

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** - 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** - Need help with planning a migration or implementing a custom design solution? Contact Riverbed Professional Services. Email proserve@riverbed.com or go to http://www.riverbed.com/services/index.html.
- **Documentation** - Have suggestions about Riverbed online documentation or printed materials? Send comments to techpubs@riverbed.com.

1

Overview of SaaS Accelerator

This chapter provides an overview of the SaaS Accelerator. It includes these sections:

Note: SaaS Accelerator is a Riverbed managed service controlled through the SteelConnect Manager that works with Riverbed client-side appliances to accelerate SaaS traffic. The SaaS Accelerator is a replacement for SteelHead Cloud Accelerator with Akamai, which has been renamed to Legacy Cloud Accelerator.

About SaaS Accelerator

SteelHeads, SteelFusion Edges, and SteelHead Mobile clients can accelerate SaaS traffic by working with SteelConnect. Through SteelConnect Manager (SCM), you can configure SaaS applications for acceleration, and then register SteelHeads, SteelFusion Edges, or Mobile Controllers with SCM to accelerate their SaaS traffic.

SaaS Accelerator is a service that consists of these components:

- **SaaS Application** - The application delivered as Software as a Service.
- **SteelConnect Manager (SCM)** - SteelConnect Manager provides the management interface for SaaS acceleration and manages the acceleration for registered SteelHeads, SteelFusion Edges, and SteelHead Mobile clients. SCM also configures and manages the SaaS service cluster.
- **Organization** - SCM allows logical separation and segmentation of resources into organizations to support multi-tenant deployments. You can have different organizations to support deployments in different regions. You deploy SaaS Accelerator within an organization.
- **Client-side SteelHead or SteelFusion Edge** - The SteelHead (SteelHead SD and RiOS-based appliances) or SteelFusion Edge located in the customer branch office that intercept any connections destined for the SaaS platform to be accelerated. We strongly recommend that you configure and push SaaS acceleration policies from a SteelCentral Controller for SteelHead (SCC) to the SteelHeads and SteelFusion Edges, particularly in large scale deployments and production networks with multiple SteelHeads and SteelFusion Edges.

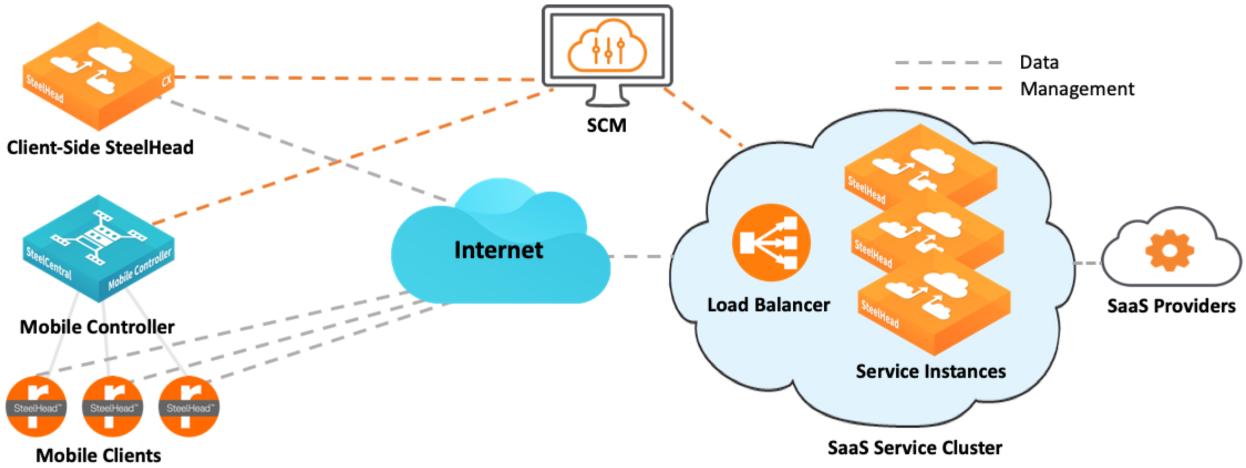
- **SaaS service cluster** - A cluster of service instances behind a service endpoint that peers with client-side appliances. Application acceleration occurs between the client-side appliance and the SaaS service cluster. SCM configures and manages the SaaS service cluster.
- **Service instance** - The application optimization service node deployed in a SaaS service cluster.
- **SteelHead Mobile clients** - SteelHead Mobile clients can accelerate SaaS traffic by connecting directly to the SaaS service cluster. SteelHead Mobile clients get their SaaS acceleration configuration through the policy defined in the SteelCentral Controller for SteelHead Mobile.

When you configure a SaaS application for acceleration, SCM deploys a SaaS service cluster in a public cloud to accelerate SaaS traffic. (You do not need a cloud account, and Riverbed configures and manages the SaaS service cluster.) Each SaaS application is accelerated by a dedicated service cluster. For best performance, you need to deploy the SaaS service cluster in the same region as the SaaS application servers.

The service endpoint is the IP address and port where client-side SteelHeads or SteelFusion Edges connect to the SaaS service cluster, and you need to open port 7810 on the firewall to allow for this communication.

With SaaS acceleration configured in SCM, the end-user traffic meant for the SaaS server goes to the client-side SteelHead or SteelFusion Edge. The client-side SteelHead or SteelFusion Edge has in-path rules configured that direct the traffic to the SaaS service cluster, and the SaaS service cluster forwards the traffic to the SaaS server. The traffic between the client-side SteelHead or SteelFusion Edge and the SaaS service cluster is accelerated.

Figure 1-1. SaaS acceleration overview



As an example of the flow, let's consider a deployment with Microsoft Office 365 traffic. This traffic is sent to the Microsoft Office 365 SaaS server. When you configure SaaS acceleration through SteelConnect, SCM deploys a SaaS service cluster in a cloud and traffic from the user network to the SaaS service cluster is accelerated.

The SaaS Accelerator automatically manages SSL certificates for proxy and peering.

Supported SaaS applications

SCM 2.12.0 or later supports accelerating these applications:

- Box
- Microsoft Office 365 (including Exchange, SharePoint, Office WebApps, and Authentication and Identify Services)
- Salesforce
- ServiceNow
- Veeva

Riverbed periodically adds support for new SaaS providers.

SaaS Accelerator licensing

SaaS Accelerator is a service, and the license defines the parameters of the service. A SaaS Accelerator license applies to an SCM organization for a specific time period and includes these components:

- **AppUnits** - This component defines how many users can accelerate SaaS traffic for an application. You specify the number of users to support when you configure acceleration for an application. The number of users allowed is determined based on the number of available AppUnits, as well as the minimum and maximum size number supported by the application. When configured, SCM allocates the AppUnits to the application.

  AppUnits provide flexibility so you can easily change which applications to accelerate, or resize your configuration based on usage.

  This table provides guidance for AppUnits for each currently supported SaaS application.

SaaS applications	Minimum/maximum number of users	AppUnits per user
Box	400 – 10,000	5
Microsoft Office 365	200 – 5000	10
Salesforce	200 – 5000	10
ServiceNow	200 – 5000	10
Veeva	200 – 5000	20

  As you configure SaaS acceleration in SCM, tooltips provide recommendations specific to each application.

- **AppData** - This component defines the amount of egress data (in GiB) allowed through the SaaS service cluster. You can track the amount of data used on the Optimization > SaaS Data usage page.

  Each AppUnit includes 0.3 GiB of AppData. For example, if you buy 10,000 AppUnits, you can deploy 1000 users for Office 365, and you would get a total of 3000 GiB per month for those users. With a yearly subscription, that provides a pool of 36,000 GiB (12 months x 3000 GiB per month).

  AppData is pooled for all applications and all users. AppData allows monthly carryovers through the end of the subscription, providing flexibility for usage variations.

You can purchase additional AppUnits or AppData through add-on licenses.

The SaaS Accelerator license is specific to your SCM organization, not per SteelHead or SteelFusion Edge. You can register any number of SteelHeads or SteelFusion Edges in your organization with SCM managing the SaaS Accelerator service.

Note: Before you activate SaaS Accelerator on a client-side SteelHead or SteelFusion Edge, 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 or SteelFusion Edge. Registering a SteelHead or SteelFusion Edge with the SaaS Accelerator service does not change the optimized session limit for that appliance.

User and data limits are enforced based on the available license.

Service cluster limits

The SaaS service cluster has the following deployment characteristics:

- A SaaS service cluster for any application can handle a maximum of 50,000 connections.
- The minimum size of the service cluster depends on the license. The minimum license is 2000 AppUnits and the minimum number of users is 200 for Microsoft Office 365, Salesforce, ServiceNow, and Veeva and 400 for Box.
- SaaS service clusters deployed in different SCM organizations are independent of each other.
- Each SCM organization can deploy only one cluster per SaaS application.

SaaS Accelerator connection and user definition

This table provides some guidance to help size a SteelHead for use with SaaS Accelerator.

SaaS applications	Minimum/maximum number of users	Connections per user
Box	400 – 10,000	5 connections
Microsoft Office 365	200 – 5000	10 connections
Salesforce	200 – 5000	10 connections
ServiceNow	200 – 5000	10 connections
Veeva	200 – 5000	10 connections

SaaS Accelerator lets individual users consume more TCP connections per user than those allocated, but does not allow the total number of TCP connections for the SaaS Acceleration cluster to exceed the limit. If you exceed the total number available connections for the cluster, or if the number of active users is significantly higher than the configured value, SaaS Accelerator enters admission control and new connections matching the SaaS application defined in the client-side appliance in-path rule will not be accelerated.

Compatibility with SteelHead models

SaaS Accelerator is supported on SteelHead models CX255, CX570, CX770, CX3070, CX5070, CX7070, CX580, CX780, CX3080, CX5080, CX7080, and GX10000. All SteelHead SD and SteelHead (virtual edition) models also support SaaS Accelerator.

The SteelHead requires RiOS software 9.8.1 or later.

2

SaaS Accelerator Quick Start Checklist

To help you get up and running quickly, here is a checklist to set up the SaaS Accelerator service. All the activities listed here are explained in Chapter 3, “Configuring SaaS Acceleration.”

Add your SaaS Accelerator license

❑ Redeem your token in SCM to activate your license.

Configure SCM

❑ Generate a root CA certificate.

❑ Distribute the root CA certificate from SCM to end-user machines that will accelerate SaaS traffic.

❑ Configure SaaS applications for acceleration.

Configure the SteelHead, SteelFusion Edge, or Mobile Controller

❑ Register clients using the registration token from SCM.

❑ Enable SSL optimization.

❑ Move client-side SteelHead, SteelFusion Edge, or Mobile Controller to the whitelist on SCM.

❑ Enable SaaS acceleration.

❑ Add application-based in-path rule to accelerate the deployed SaaS applications.

Configure the SteelCentral Controller for SteelHead

To configure SaaS acceleration on managed SteelHeads and SteelFusion Edges using SCC, perform these tasks:

❑ Register the SCC with SCM.

❑ Using the SCC, register the managed SteelHeads and SteelFusion Edges with SCM.

❑ Move the SCC, SteelHeads, and SteelFusion Edges to the whitelist on SCM.

❑ Enable SSL optimization in the SCC policy that includes SaaS acceleration.

❑ Enable SaaS Accelerator in the SCC policy that includes SaaS acceleration.

❑ Add an application-based in-path rule, in the SCC policy, to accelerate the deployed SaaS applications.

❑ Push the policy to the managed SteelHeads and SteelFusion Edges.

3

Configuring SaaS Acceleration

You configure SaaS acceleration through the SteelConnect Manager (SCM) as well as the client-side SteelHead, SteelFusion Edge, and/or the Mobile Controller. After you configure the environment, you configure SaaS acceleration on a per-application basis.

This chapter includes these sections:

Before you begin

Before you begin, ensure you have a license for the SaaS Accelerator and your environment meets these requirements:

- SteelHeads require version 9.8.1 software or later.
- SteelFusion Edges require version 6.0.2 or later.
- SCM requires version 2.12 or later.
- SteelCentral Controller for SteelHead Mobile requires version 6.1.0 or later.
- SteelCentral Controller for SteelHead (SCC) requires version 9.9.1 or later.

Licensing SCM for SaaS Accelerator

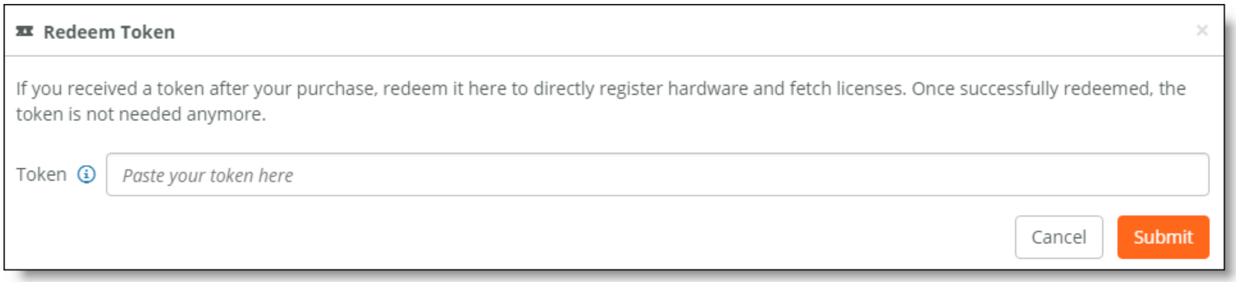
When you purchase SaaS Accelerator, Riverbed emails you a license token that you need to redeem through SCM.

To install your licenses for SaaS acceleration

1. Sign in to the SCM that will manage the SaaS acceleration.
2. Choose Organization > Licenses and click **Redeem Token**.

   The Redeem Token dialog box appears.

Figure 3-1. Redeem Token dialog box



Redeem Token

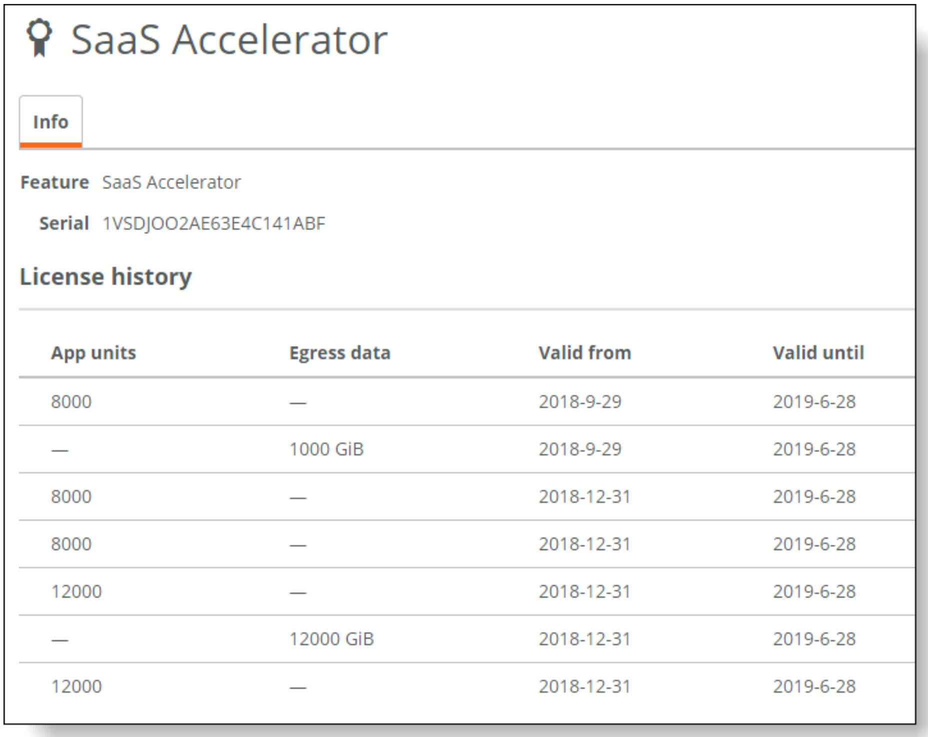
If you received a token after your purchase, redeem it here to directly register hardware and fetch licenses. Once successfully redeemed, the token is not needed anymore.

Token: *Paste your token here*

3. Enter the token and click **Submit**.

The SaaS Accelerator pages are now available, and you can review your license details on the Organization > Licenses page. Click the license serial number to show the details.

Figure 3-2. License details



SaaS Accelerator

Feature SaaS Accelerator

Serial 1VSDJOO2AE63E4C141ABF

License history

App units	Egress data	Valid from	Valid until
8000	—	2018-9-29	2019-6-28
—	1000 GiB	2018-9-29	2019-6-28
8000	—	2018-12-31	2019-6-28
8000	—	2018-12-31	2019-6-28
12000	—	2018-12-31	2019-6-28
—	12000 GiB	2018-12-31	2019-6-28
12000	—	2018-12-31	2019-6-28

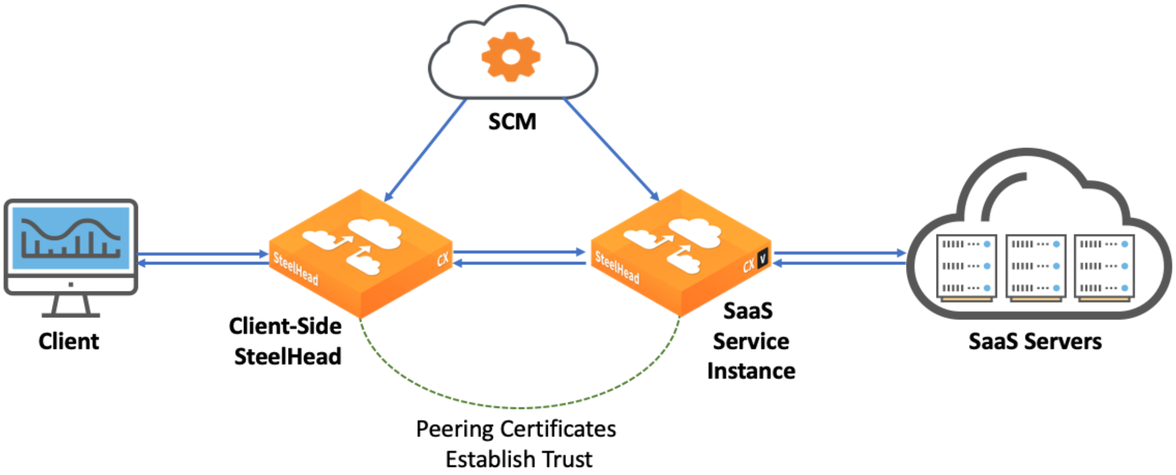
Configuring SSL optimization

SSL optimization is required for SaaS acceleration, and you need to generate a root CA certificate before you can configure SaaS acceleration. A root CA certificate automatically generates trusted certificates to sign optimized TLS/SSL traffic.

SCM uses the root CA certificate to sign peering and proxy certificates, which it pushes to the SaaS service cluster. When a client-side SteelHead or SteelFusion Edge is moved to the SCM whitelist, SCM pushes the peering certificate signed by its root CA to the client-side SteelHead or SteelFusion Edge and the client-side appliance uploads its peering certificate to SCM, which SCM pushes to the service cluster. This establishes the trust relationship between the client-side SteelHead or SteelFusion Edge and the SaaS service cluster.

You also need to install the certificate from SCM on each client system to complete the trust relationship.

Figure 3-3. SSL optimization with peering certificates



If there are any changes to the root CA certificate, SCM automatically updates the client-side SteelHead or SteelFusion Edge and the SaaS service cluster to maintain the trust relationship.

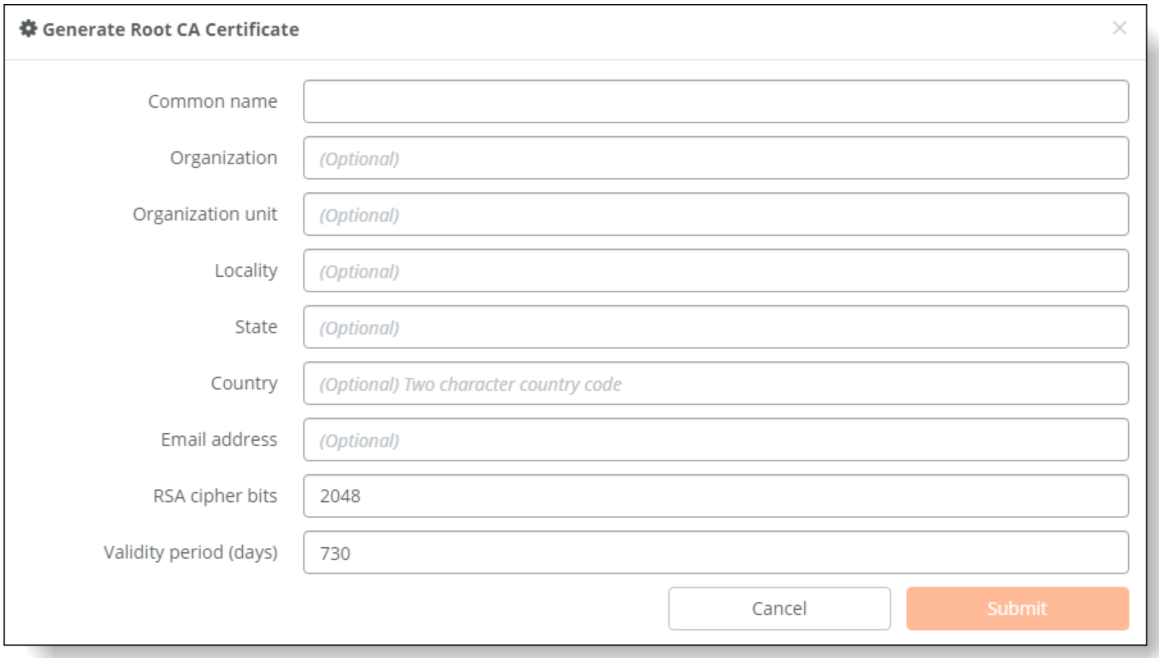
Note: SCM users with read-only permissions are not allowed to generate certificates or configure SaaS acceleration.

To enable automatic signing and generate a root CA certificate

1. In SCM, choose Optimization > SSL Optimization and click **Generate Root CA Certificate**.

The Generate Root CA Certificate dialog box appears.

Figure 3-4. Generate Root CA Certificate dialog box



Generate Root CA Certificate

Common name

Organization (Optional)

Organization unit (Optional)

Locality (Optional)

State (Optional)

Country (Optional) Two character country code

Email address (Optional)

RSA cipher bits 2048

Validity period (days) 730

2. Provide the following information.

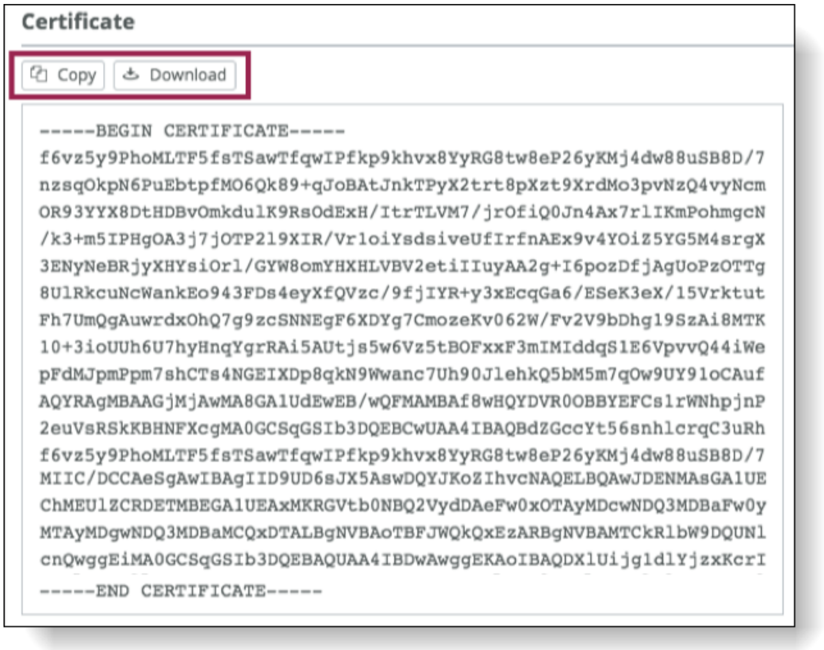
Field	Description
Common name	Specify the common name of the root CA certificate.
Organization	Optionally, specify the organization name (for example, the company).
Organization unit	Optionally, specify the organization unit name (for example, the section or department).
Locality	Optionally, specify the city.
State	Optionally, specify the state.
Country	Optionally, specify the country (2-letter code only).
Email address	Optionally, specify the email address of the contact person.
RSA cipher bits	Select the key length from the drop-down list. The default value is 2048.
Validity period (days)	Specify how many days the root CA certificate is valid. The default value is 730 days (two years).

3. Click **Submit**.

   SCM creates the root CA certificate.

4. Copy or download the root CA certificate from SCM and install it in end-user client systems.

Figure 3-5. Copy or download the root CA certificate



```
-----BEGIN CERTIFICATE-----
f6vz5y9PhoMLTF5fsTSawTfqwIPfkp9khvx8YyRG8tw8eP26yKMj4dw88uSB8D/7
nzsqOkpN6PuEbtpfMO6Qk89+qJoBAtJnkTPyX2trt8pXzt9XrdMo3pvNzQ4vyNcm
OR93YYX8DtHDBvOmkdulK9RsOdExH/ItrTLVM7/jrOfiQ0Jn4Ax7rlIKmPohmgcN
/k3+m5IPHgOA3j7jOTP2l9XIR/Vr1oiYsdsiveUfIrfnAEx9v4YOiZ5YG5M4srgX
3ENyNeBRjyXHYsiOrl/GYW8omYHXHLVBV2etiIIuyAA2g+I6pozDfjAgUoPzOTTg
8UlRkcuNcWankEo943FDs4eyXfQVzc/9fjIYR+y3xEcqGa6/ESeK3eX/15Vrktut
Fh7UmQgAuwrdxOhQ7g9zcSNNEgF6XDYg7CmozeKv062W/Fv2V9bDhg19SzAi8MTK
10+3ioUUh6U7hyHnqYgrRAi5AUtjs5w6Vz5tBOFxxF3mIMIddqS1E6VpvvQ44iWe
pFdMJpmPpm7shCTs4NGEIXDp8qkN9Wwanc7Uh90JlehkQ5bM5m7qOw9UY9loCAuf
AQYRAgMBAAGjMjAwMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFCs1rWNhpjnP
2euVsRSkKBHNFXcgMA0GCSqGSIb3DQEBCwUAA4IBAQBdZGccYt56snhlcrqC3uRh
f6vz5y9PhoMLTF5fsTSawTfqwIPfkp9khvx8YyRG8tw8eP26yKMj4dw88uSB8D/7
MIIC/DCCAeSgAwIBAgIID9UD6sJX5AswDQYJKoZIhvcNAQELBQAwJDENMAsGA1UE
ChMEU1ZCRDETMBEGA1UEAxMKRGVtb0NBQ2VydDAeFw0xOTAyMDcwNDQ3MDBaFw0y
MTAyMDgwNDQ3MDBaMCQxDTALBgNVBAoTBFJWQkQxEzARBgNVBAMTCkRlbW9DQUNl
cnQwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDXlUijg1dlYjzxKcrI
-----END CERTIFICATE-----
```

An active Root Certificate Authority (CA) enables clients to accelerate SaaS traffic when SaaS applications are configured on the SaaS Accelerator page. The root CA certificate needs to be deployed into the Trusted Root Certification Authority certificate store on your clients and then your clients can automatically use certificates issued by this trusted root CA to accelerate encrypted SaaS traffic.

To delete the certificate

1. In SCM, choose Optimization > SSL Optimization.
2. Click **Delete Root CA Certificate**.

   You are prompted to confirm this action.

3. Click **Confirm**.

   The root CA certificate is removed from the system and new SaaS connections will not be accelerated.

Configuring SaaS applications for acceleration

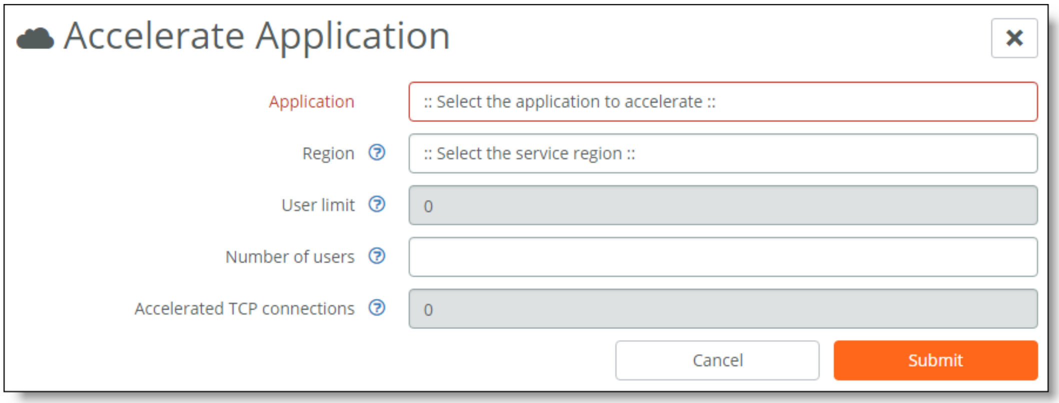
After you have licensed the SaaS Accelerator and configured SSL optimization, you can set up acceleration for SaaS applications.

To configure SaaS applications for acceleration

1. In SCM, choose Optimization > SaaS Accelerator and click **Accelerate Application**.

The Accelerate Application pane appears.

Figure 3-6. Configuring applications for SaaS acceleration



Accelerate Application

Application: :: Select the application to accelerate ::

Region: :: Select the service region ::

User limit: 0

Number of users:

Accelerated TCP connections: 0

2. Select the application from the drop-down list.
3. Select the region from the drop-down list.

   For best performance, select the region closest to the data for the SaaS application. Once you deploy to a specific region, you cannot change it unless you delete the deployed application and set it up again with a different region.

4. Enter the number of Active Users.

   Each application has a minimum and maximum number of users. SCM provides guidelines for the limits as you type numbers in the field.

   SCM uses the number of users to calculate the capacity of service instances in the SaaS service cluster based on the type of application.

   SCM calculates the user limit based on the number of users, the application, and the available AppUnits.

   Note: We recommend that you select number of users carefully for your business needs. Once deployed, you can change the number of users, however, when you change the number of users, the acceleration feature is unavailable for up to 30 minutes while the service cluster updates.

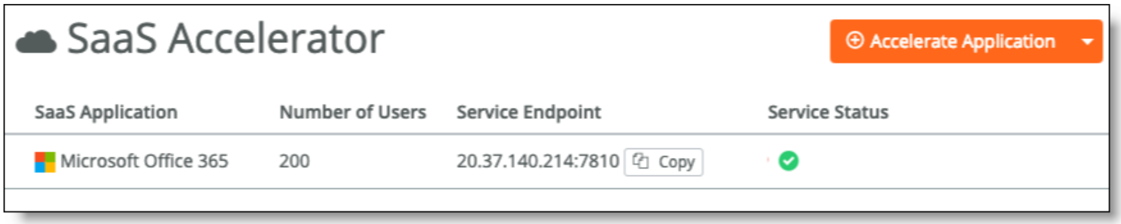
5. Click **Submit**.

   This creates the SaaS service cluster dedicated to accelerating traffic for this application.

   Deployment can take up to 20 minutes, and you cannot edit the configuration while the configuration is in process.

   When deployed, you see the SaaS application, the service endpoint, and service status. The service status appears as a green check mark when deployed and ready for optimization.

Figure 3-7. Status for deployed application



SaaS Accelerator

SaaS Application	Number of Users	Service Endpoint	Service Status
Microsoft Office 365	200	20.37.140.214:7810 Copy	✓

6. As needed, open port 7810 for the service endpoint IP address on your firewall.

   The SaaS service cluster and client-side SteelHeads or SteelFusion Edges need to be able to connect to this location.

To stop SaaS acceleration for an application

1. Choose Optimization > SaaS Accelerator and click the application to stop accelerating.
2. From the Actions drop-down list, select Terminate SaaS acceleration.
3. When prompted, click **Confirm**.

When you terminate SaaS acceleration for an application, you remove the SaaS service cluster that was deployed in the cloud to support the acceleration.

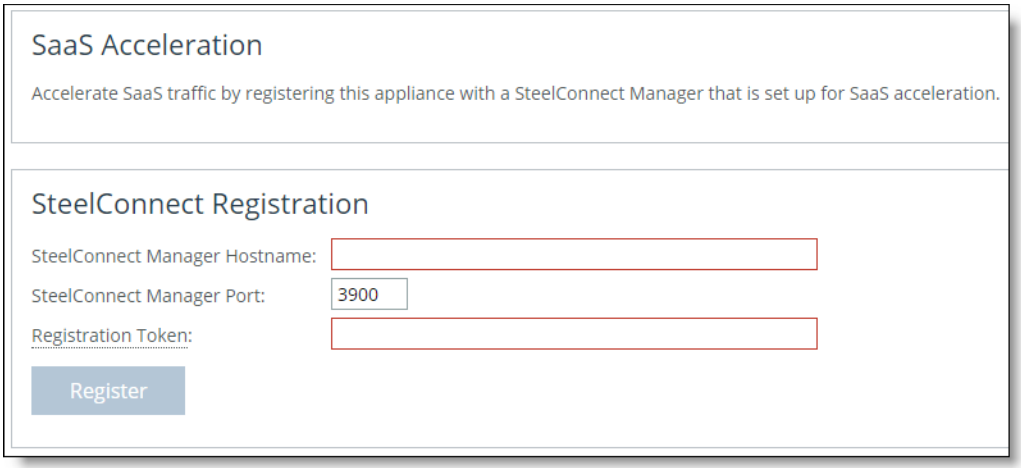
Configuring SaaS acceleration on the client-side SteelHead or SteelFusion Edge

When you have configured SCM for SaaS acceleration, you can configure client-side SteelHead or SteelFusion Edge.

To configure a SteelHead or SteelFusion Edge for SaaS acceleration

1. In SCM, choose Optimization > SaaS Client Appliances and copy the registration token.
2. On the SteelHead or SteelFusion Edge, choose Optimization > SaaS: SaaS Accelerator and add these values:
   - SteelConnect Manager Hostname.
   - SteelConnect Manager Port. The client-side SteelHead or SteelFusion Edge uses port 3900 from the primary interface to communicate with SCM and the port needs to be open on the branch firewall. The field for the port number is editable but we do not recommend changing the value.
   - Registration Token. Paste the registration token you copied in Step 1 into this field.

Figure 3-8. SaaS Acceleration registration page



SaaS Acceleration

Accelerate SaaS traffic by registering this appliance with a SteelConnect Manager that is set up for SaaS acceleration.

SteelConnect Registration

SteelConnect Manager Hostname:

SteelConnect Manager Port: 3900

Registration Token:

3. Click **Register**.

When the registration process completes, the registration details and a helpful list of remaining configuration tasks appear on the page. Completed tasks are prefaced by a check mark.

A new SaaS Acceleration section appears on the page, and you can view the current status and monitor acceleration status.

4. Enable SSL optimization on the SteelHead or SteelFusion Edge.

   Choose Optimization > SSL Main Settings, and in the General SSL Settings area select Enable SSL Optimization and click **Apply**.

5. In SCM, move this appliance to the whitelist.

   Newly added appliances always appear on the graylist in the Access List column. You need to move their status to the whitelist to allow acceleration.

   Choose Optimization > SaaS Client Appliances and select the appliance serial number to display the details pane.

   Under Access List and Notes, select Whitelist from the Access list drop-down list and click **Submit**. For more information, see "Controlling appliance access" on page 34.

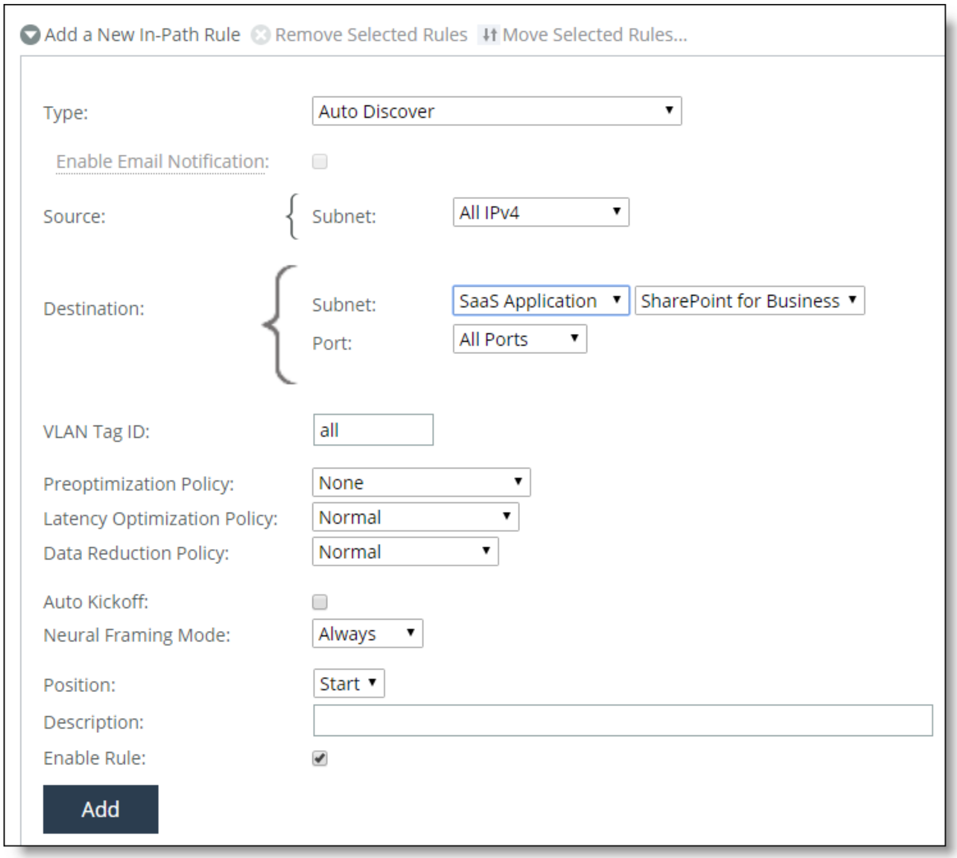
6. Enable SaaS acceleration on this client-side appliance. Choose Optimization > SaaS: SaaS Accelerator, select Enable Acceleration, and click **Apply**.

7. Add an in-path rule to accelerate SaaS applications.

   The in-path rule is application based and lets the client-side SteelHead connect to the service endpoint of the SaaS service cluster deployed for the selected application.

Choose Optimization > Network Services: In-Path Rules and click **Add a New In-Path Rule**. For the Source subnet, choose All IPv4. For the Destination Subnet, choose SaaS Application. A second menu appears to the right. In the second menu, choose a SaaS application for acceleration. (Note: Only applications set up for SaaS acceleration on SCM appear in the list.) Click **Add**.

Figure 3-9. SaaS in-path rule



Type: Auto Discover

Enable Email Notification: □

Source: Subnet: All IPv4

Destination: Subnet: SaaS Application | SharePoint for Business

Port: All Ports

VLAN Tag ID: all

Preoptimization Policy: None

Latency Optimization Policy: Normal

Data Reduction Policy: Normal

Auto Kickoff: □

Neural Framing Mode: Always

Position: Start

Description:

Enable Rule: ☑

For more information about in-path rules, see the *SteelHead User Guide*.

8. Click **Save to Disk** to save your settings permanently.

To verify, generate SaaS traffic. For details about monitoring the first connections, see “Monitoring initial SaaS traffic” on page 37.

Canceling SaaS acceleration

If you want to pause SaaS acceleration, from the Optimization > SaaS: SaaS Accelerator page on the SteelHead clear Enable Acceleration and click **Apply**. When paused, all related in-path rules are ignored.

If you want to permanently cancel SaaS acceleration for this appliance and remove the settings, click **Deregister**. This also removes all related in-path rules.

As another option, you can move the appliance to the blacklist on SCM. When you move an appliance to the blacklist, SCM removes the peering CA that it uploaded from the appliance and stops acceleration. For details, see “Controlling appliance access” on page 34.

Configuring SaaS acceleration on multiple SteelHeads and SteelFusion Edges using SCC

In SCC 9.9.1 and later, you can configure SaaS acceleration on managed SteelHeads and SteelFusion Edges. SaaS Accelerator requires an additional license, but the license is not installed on the SCC, SteelHeads, and SteelFusion Edges; it is installed on SCM.

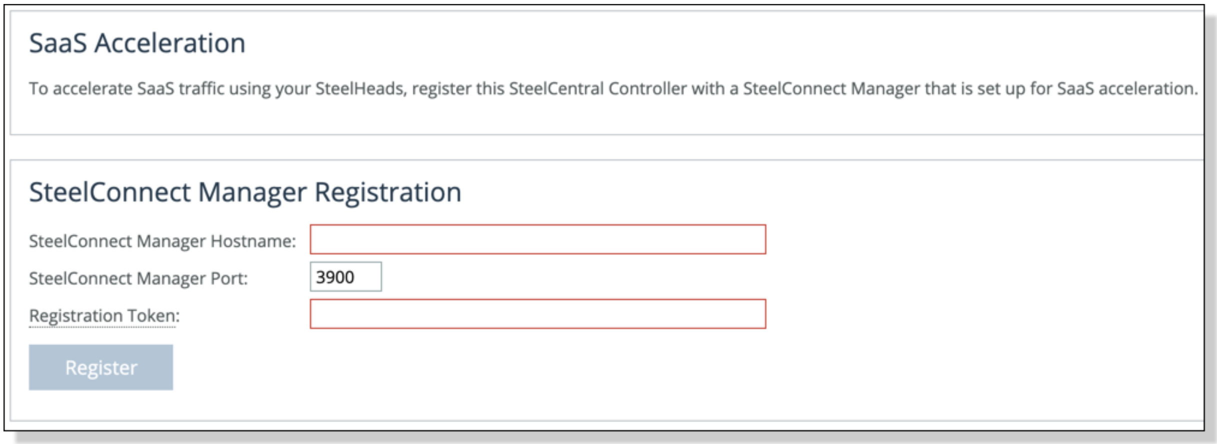
We strongly recommend that you configure and push SaaS acceleration policies from an SCC to the SteelHeads and SteelFusion Edges, particularly in large scale deployments and production networks with multiple appliances.

To accelerate SaaS application traffic using your managed SteelHeads and SteelFusion Edges, register your SCC with an SCM that is set up for SaaS acceleration. After registering the SCC with SCM, register selected SteelHeads and SteelFusion Edges or a group of SteelHeads and SteelFusion Edges with SCM.

To configure SteelHeads and SteelFusion Edges for SaaS acceleration using SCC

1. On SCM, choose Optimization > SaaS Client Appliances and copy the registration token.
2. On the SCC, choose Administration > SaaS: SteelConnect Manager Registration and add these values:
   - SteelConnect Manager Hostname.
   - SteelConnect Manager Port. The SCC uses port 3900 to communicate with SCM, and the port needs to be open on the firewall. The field for the port number is editable but we do not recommend changing the value.
   - Registration Token. Paste the registration token you copied in Step 1 to this field.

Figure 3-10. SteelConnect Manager Registration page



SaaS Acceleration

To accelerate SaaS traffic using your SteelHeads, register this SteelCentral Controller with a SteelConnect Manager that is set up for SaaS acceleration.

SteelConnect Manager Registration

SteelConnect Manager Hostname:

SteelConnect Manager Port: 3900

Registration Token:

3. Click **Register**.

   When the registration process completes, the registration details appear on the page.

   A new SaaS Acceleration Status section also appears on the page where you can view the current access list status and a list of applications set up for SaaS acceleration on SCM.
4. On SCM, move this SCC to the whitelist.

Newly added appliances always appear on the graylist in the Access List column. You need to change their status to the whitelist to allow acceleration.

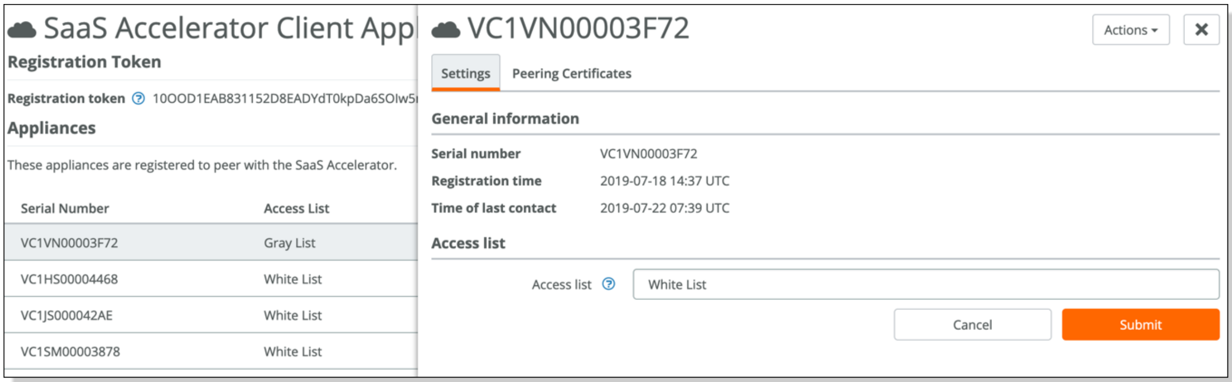
Note: You can safely ignore the No certificates uploaded error message appearing in the Peering Certificates Status column for the SCC appliance. To accelerate SaaS application traffic, only peering certificates for SteelHeads and SteelFusion Edges are uploaded to SCM when the appliances register with SCM. Peering certificates allow a client-side SteelHead or SteelFusion Edge to establish trust relationship and peer with SaaS service cluster to accelerate the SaaS traffic.

To move their status to the whitelist:

- Choose Optimization > SaaS Client Appliances and click the appliance serial number to display the details panel.
- Under Access List, select Whitelist from the Access List drop-down menu and click **Submit**.

Note: Without moving the SCC to the whitelist on SCM, you cannot push a policy with in-path rules for SaaS applications from the SCC to the managed SteelHeads. For more details about the access lists, see the "Controlling appliance access" on page 34.

Figure 3-11. Moving an appliance to the whitelist on SCM



SaaS Accelerator Client Appl

Registration Token

Registration token ⓘ 10OOD1EAB831152D8EADYdT0kpDa6SOlw5

Appliances

These appliances are registered to peer with the SaaS Accelerator.

Serial Number	Access List
VC1VN00003F72	Gray List
VC1HS00004468	White List
VC1JS000042AE	White List
VC1SM00003878	White List

VC1VN00003F72

General information

Serial number VC1VN00003F72

Registration time 2019-07-18 14:37 UTC

Time of last contact 2019-07-22 07:39 UTC

Access list

Access list ⓘ White List

5. On the SCC, choose Administration > SaaS: SteelConnect Manager Registration and click **Refresh Data** under the SaaS Acceleration Status section. Make sure the access list status of the SCC is Whitelist. You can also view a list of applications set up for SaaS acceleration on SCM and their respective service endpoints.

   Note: If you set up new applications for SaaS acceleration on SCM, perform Step 5 on the SCC to view the latest list of SaaS applications set up for acceleration.

6. Register SteelHeads and SteelFusion Edges with SCM.

   If you plan to use SCC policies to accelerate SaaS application traffic, make sure the SCC, the SteelHeads, and SteelFusion Edges are registered with the same SCM. After registering the SCC with SCM, register the selected appliances or a group of appliances with SCM.

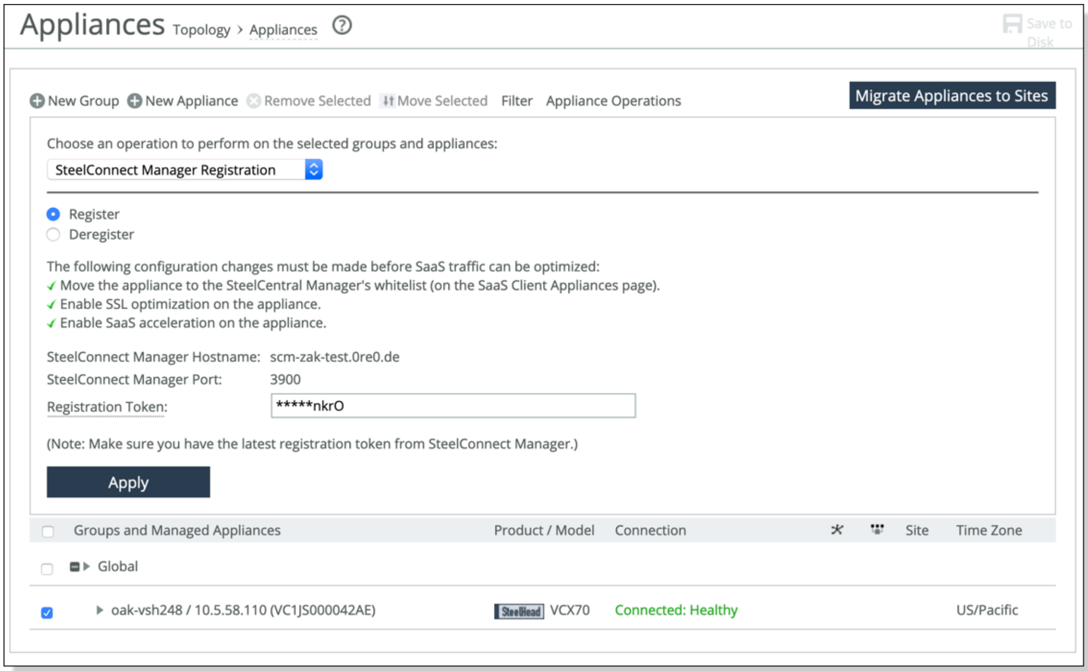
   To register SteelHeads and SteelFusion Edges with SCM:

   - Choose Manage > Topology: Appliances and select SteelHeads and SteelFusion Edges or a group of SteelHeads and SteelFusion Edges you plan to register with SCM.
   - Click **Appliance Operations**, and select SteelConnect Manager Registration from the Choose an operation to perform on the selected groups and appliances drop-down list.

- Select Register, make sure you have the latest registration token from SCM in the Registration Token text field and click **Apply**.

Note: The SteelHeads and SteelFusion Edges use port 3900 to communicate with SCM and the port needs to be open on the branch firewall. The field for the port number is editable but we do not recommend changing the value.

Figure 3-12. Registering appliances with SCM



Choose an operation to perform on the selected groups and appliances:

SteelConnect Manager Registration

● Register
○ Deregister

The following configuration changes must be made before SaaS traffic can be optimized:
✓ Move the appliance to the SteelCentral Manager's whitelist (on the SaaS Client Appliances page).
✓ Enable SSL optimization on the appliance.
✓ Enable SaaS acceleration on the appliance.

SteelConnect Manager Hostname: scm-zak-test.0re0.de
SteelConnect Manager Port: 3900
Registration Token: *****nkrO

(Note: Make sure you have the latest registration token from SteelConnect Manager.)

□	Groups and Managed Appliances	Product / Model	Connection			Site	Time Zone
□	Global						
☑	oak-vsh248 / 10.5.58.110 (VC1JS000042AE)	SteelHead VCX70	Connected: Healthy				US/Pacific

For more details about registering SteelHeads with SCM using SCC, see the *SteelCentral Controller for SteelHead User Guide*.

7. Move the SteelHeads and SteelFusion Edges to the whitelist on SCM.

   Newly added appliances always appear on the graylist in the Access List column. You need to change their status to the whitelist to allow acceleration. For details about moving an appliance to the whitelist, see Step 4. For more information about the access lists, see "Controlling appliance access" on page 34.

8. Enable SSL optimization in the SCC policies that include SaaS acceleration.

   To enable SSL optimization:

   - Choose Manage > Services: Policies, open the policy, and Click **+ Add/Remove Pages**.
   - Under Optimization, select SSL Main Settings and click **Apply**.
   - In the Editing Policy page, click **SSL Main Settings**, click **Include** to include the policy, select Enable SSL optimization, and click **Apply**.

   For more details, see the *SteelCentral Controller for SteelHead User Guide*.

9. Enable SaaS acceleration in the SCC policies to configure SaaS acceleration for groups of SteelHead and SteelFusion Edge clients.

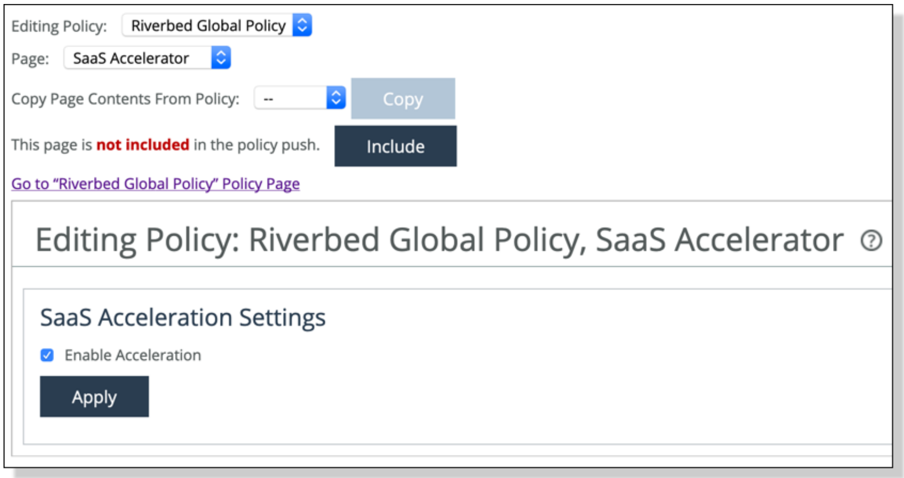
   To enable SaaS acceleration:

   – Choose Manage > Services: Policies, open the policy, and Click **+ Add/Remove Pages**.

   – Under Optimization, select SaaS Accelerator and click **Apply**.

   – In the Editing Policy page, click **SaaS Accelerator**, click **Include** to include the policy, select Enable Acceleration, and click **Apply**.

Figure 3-13. Enabling SaaS acceleration in SCC policy



Editing Policy: Riverbed Global Policy

Page: SaaS Accelerator

Copy Page Contents From Policy: --

This page is **not included** in the policy push.

Go to "Riverbed Global Policy" Policy Page

Editing Policy: Riverbed Global Policy, SaaS Accelerator

SaaS Acceleration Settings

☑ Enable Acceleration

10. Add an in-path rule to each policy for which you want SaaS acceleration enabled.

    The in-path rule associates the IP address of the SaaS service cluster in the cloud (supplied by SCM) with the accelerated application.

    To enable SaaS acceleration:

    – Choose Manage > Services: Policies, open the policy, and Click **+ Add/Remove Pages**.

    – Under Optimization, select In-Path Rules and click **Apply**.

    – In the Editing Policy page, click **In-Path Rules**, click **Include** to include the policy, and click **Add a New In-Path Rule** to expand the page.

    – For the Source Subnet, choose IPv4 or All IPv4.

    – For the Destination Subnet, choose SaaS Application.

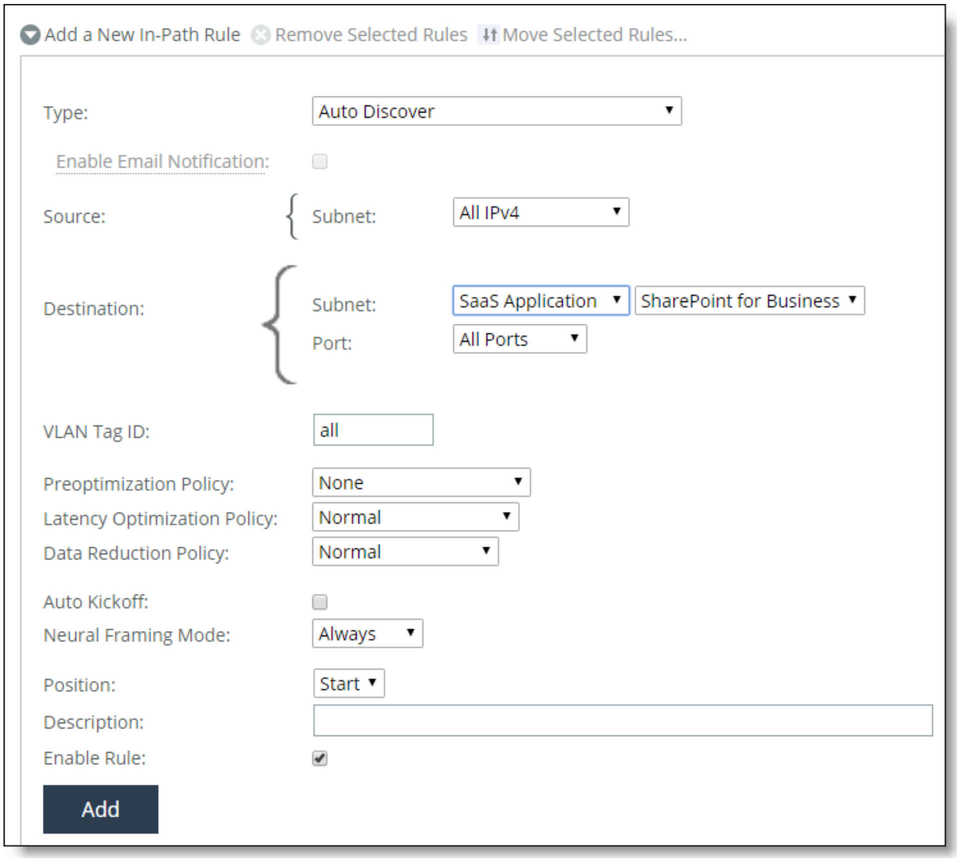
    – A second drop-down list appears to the right. In the second drop-down list, select a SaaS application for acceleration and click **Add**.

      Only applications set up for SaaS acceleration on SCM appear in the list.

    For more details, see the *SteelCentral Controller for SteelHead User Guide*.

Note: At the initial release of SteelHead 9.9.1, you need to configure a unique in-path rule for each Microsoft Office 365 application, such as SharePoint and Exchange Online. An upcoming release of SteelConnect Manager will let you define a single in-path rule for all Office 365 traffic. When available, the Office 365 option will automatically appear as an option for a SaaS application in-path rule.

Figure 3-14. SaaS in-path rule



Type: Auto Discover

Enable Email Notification: □

Source: Subnet: All IPv4

Destination: Subnet: SaaS Application, SharePoint for Business

Port: All Ports

VLAN Tag ID: all

Preoptimization Policy: None

Latency Optimization Policy: Normal

Data Reduction Policy: Normal

Auto Kickoff: □

Neural Framing Mode: Always

Position: Start

Description:

Enable Rule: ☑

11. Click **Save to Disk** to save your settings permanently.

Canceling SaaS acceleration

To pause SaaS acceleration on managed SteelHeads and SteelFusion Edges, on the SCC, choose Manage > Services: Policies and open the policy. In the Editing Policy page, click **SaaS Accelerator**, clear Enable Acceleration, and click **Apply**.

Note: For the configuration to take effect, apply the updated policy to the respective SteelHeads and SteelFusion Edges.

To cancel SaaS acceleration on selected SteelHeads and SteelFusion Edges, deregister the appliances from SCM. For more details about deregistering SteelHeads and SteelFusion Edges, see the *SteelCentral Controller for SteelHead User Guide*.

Configuring SaaS acceleration on SteelHead Mobile

When you have configured SCM for SaaS acceleration, you can configure the Mobile Controller and create a client policy to accelerate SteelHead Mobile client SaaS traffic.

To configure the Mobile Controller for SaaS acceleration

1. In SCM, choose Optimization > SaaS Client Appliances and copy the registration token.

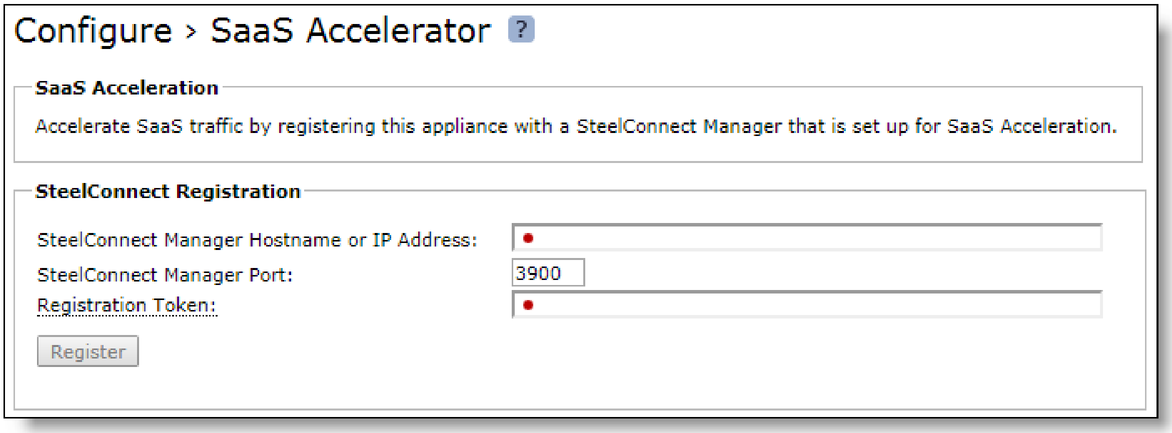
2. On the Mobile Controller, choose Configure > SaaS Accelerator and add these values:

   – SteelConnect Manager Hostname or IP Address.

   – SteelConnect Manager Port. The Mobile Controller uses port 3900 from the primary interface to communicate with SCM, and the port needs to be open on the branch firewall. The field for the port number is editable but we do not recommended changing the value.

   – Registration Token. Paste the registration token you copied in Step 1 into this field.

Figure 3-15. SaaS Accelerator registration page



Configure > SaaS Accelerator ?

SaaS Acceleration

Accelerate SaaS traffic by registering this appliance with a SteelConnect Manager that is set up for SaaS Acceleration.

SteelConnect Registration

SteelConnect Manager Hostname or IP Address: ●

SteelConnect Manager Port: 3900

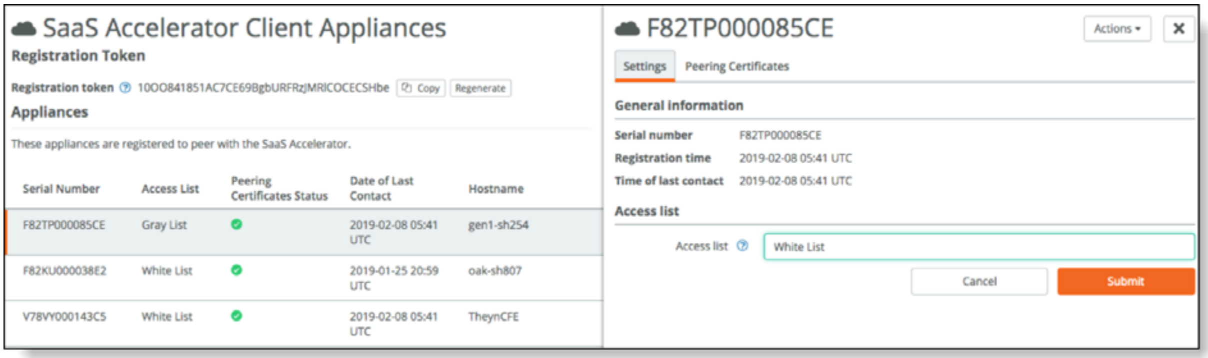
Registration Token: ●

3. Click **Register**.

4. In SCM, move this Mobile Controller to the whitelist.

   Newly added appliances appear on the graylist in the Access List column.

Figure 3-16. Moving an appliance to the whitelist



SaaS Accelerator Client Appliances

Registration Token

Registration token ? 10O0841851AC7CE69BgbURFRzJMRICOCECSHbe

Appliances

These appliances are registered to peer with the SaaS Accelerator.

Serial Number	Access List	Peering Certificates Status	Date of Last Contact	Hostname
F82TP000085CE	Gray List	✓	2019-02-08 05:41 UTC	gen1-sh254
F82KU000038E2	White List	✓	2019-01-25 20:59 UTC	oak-sh807
V78VY000143C5	White List	✓	2019-02-08 05:41 UTC	TheynCFE

F82TP000085CE

General information

Serial number F82TP000085CE

Registration time 2019-02-08 05:41 UTC

Time of last contact 2019-02-08 05:41 UTC

Access list

Access list ? White List

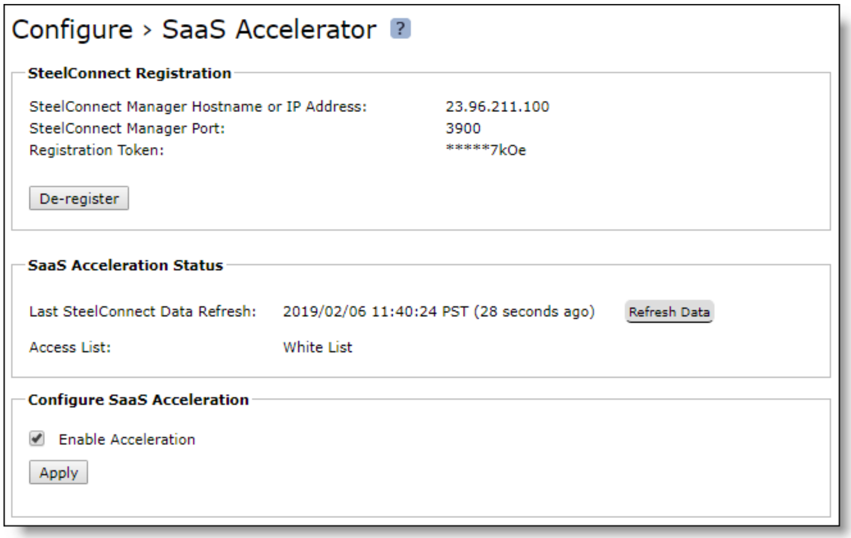
To move their status to the whitelist:

- Choose Optimization > SaaS Client Appliances and click the serial number of the Mobile Controller to display the details pane.
- Under Access List and Notes, select Whitelist from the Access list drop-down list and click **Submit**.

You cannot enable SaaS acceleration without moving the Mobile Controller to the whitelist. In SCM, if a Mobile Controller is moved from the whitelist to the blacklist, SaaS acceleration stops working. For more information about the access lists, see "Controlling appliance access" on page 34.

5. Enable SaaS acceleration on the Mobile Controller. Choose Configure > SaaS Accelerator and in the Configure SaaS Acceleration section, select Enable Acceleration and click **Apply**.

Figure 3-17. Configuring SaaS acceleration



Configure > SaaS Accelerator ?

SteelConnect Registration

SteelConnect Manager Hostname or IP Address: 23.96.211.100
SteelConnect Manager Port: 3900
Registration Token: *****7kOe

SaaS Acceleration Status

Last SteelConnect Data Refresh: 2019/02/06 11:40:24 PST (28 seconds ago)

Access List: White List

Configure SaaS Acceleration

☑ Enable Acceleration

When you click Apply, be patient. It can take several minutes to start acceleration.

6. Enable SSL optimization on the Mobile Controller policies that include SaaS acceleration.

Choose Manage > Policies and open the policy and select the SSL tab. Then select the Enable SSL Optimization check box and the Enable SSL Proxy Support check box.

You cannot enable SaaS acceleration without enabling SSL. If SSL was disabled after SaaS acceleration was enabled, SaaS acceleration will stop working.

For details, see the *SteelCentral Controller for SteelHead Mobile User Guide*.

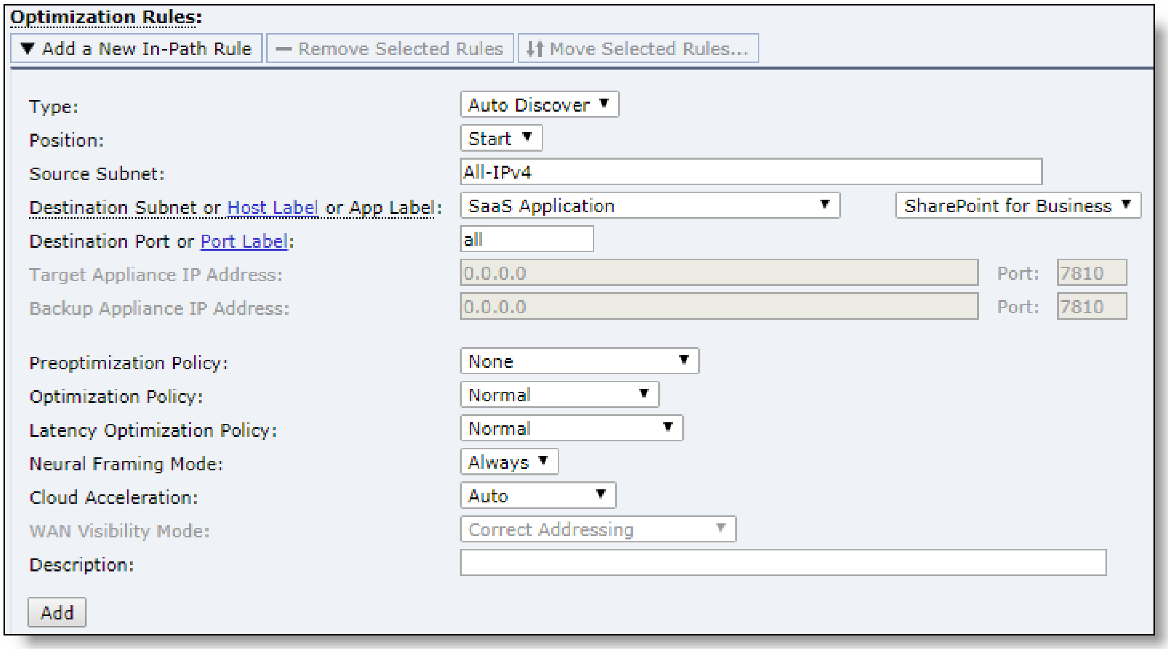
7. On the Mobile Controller, add an in-path rule to each policy for which you want SaaS acceleration enabled.

The in-path rule is application based and lets the Mobile Controller connect to the service endpoint of the SaaS service cluster deployed for the selected application.

- Choose Manage > Policies and select the In-Path Rules tab and click **Add a New In-Path Rule**.
- For the Destination Subnet, choose SaaS Application.
- A second menu appears to the right. In the second menu, select a SaaS application for acceleration. Only applications set up for SaaS acceleration on SCM appear in the list.
- Click **Add**.

See the *SteelCentral Controller for SteelHead Mobile User Guide* for more information.

Figure 3-18. SaaS in-path rule

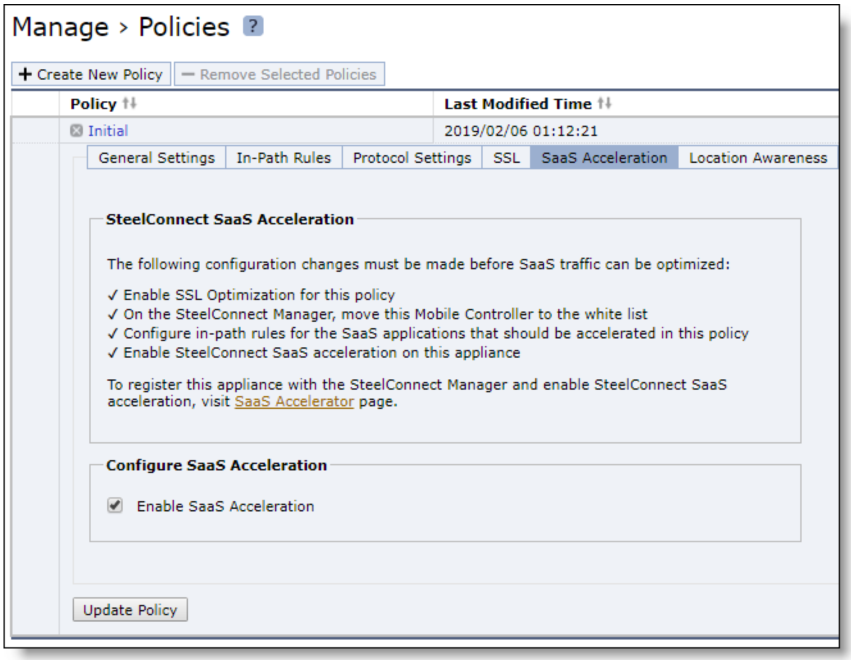


Type:	Auto Discover ▼		
Position:	Start ▼		
Source Subnet:	All-IPv4		
Destination Subnet or Host Label or App Label:	SaaS Application ▼	SharePoint for Business ▼	
Destination Port or Port Label:	all		
Target Appliance IP Address:	0.0.0.0	Port:	7810
Backup Appliance IP Address:	0.0.0.0	Port:	7810
Preoptimization Policy:	None ▼		
Optimization Policy:	Normal ▼		
Latency Optimization Policy:	Normal ▼		
Neural Framing Mode:	Always ▼		
Cloud Acceleration:	Auto ▼		
WAN Visibility Mode:	Correct Addressing ▼		
Description:			

8. Enable SaaS acceleration in a policy to configure SaaS acceleration for groups of SteelHead Mobile clients. Choose Manage > Policies and open a policy to configure and select the SaaS Acceleration tab.

   A helpful list of remaining configuration tasks appears on the page. Completed tasks are prefaced by a check mark.

Figure 3-19. Enabling SaaS acceleration for a policy



Policy ⇅	Last Modified Time ⇅
⊠ Initial	2019/02/06 01:12:21

SteelConnect SaaS Acceleration

The following configuration changes must be made before SaaS traffic can be optimized:

✓ Enable SSL Optimization for this policy
✓ On the SteelConnect Manager, move this Mobile Controller to the white list
✓ Configure in-path rules for the SaaS applications that should be accelerated in this policy
✓ Enable SteelConnect SaaS acceleration on this appliance

To register this appliance with the SteelConnect Manager and enable SteelConnect SaaS acceleration, visit SaaS Accelerator page.

Configure SaaS Acceleration

☑ Enable SaaS Acceleration

Select Enable SaaS Acceleration and click **Update Policy**.

You cannot enable SaaS acceleration in a policy without enabling SaaS acceleration in the Mobile Controller.

9. Click **Save to Disk** to save your settings permanently.

To verify, generate SaaS traffic. For details about monitoring the first connections, see "Monitoring initial SaaS traffic" on page 37.

Canceling SaaS acceleration

If you want to pause SaaS acceleration, from the Configure > SaaS Accelerator page on the Mobile Controller clear Enable Acceleration and click **Apply**. When cleared, all related in-path rules are ignored.

If you want to permanently cancel SaaS acceleration for this appliance and remove the settings, click **Deregister**. This also removes all related in-path rules.

As another option, you can move the Mobile Controller to the blacklist on SCM. When you move an appliance to the blacklist, SCM removes the peering CA that it uploaded from the appliance and stops acceleration. For details, see "Controlling appliance access" on page 34.

Controlling appliance access

When a client-side SteelHead registers with SCM, the SteelHead is added to the access list on the SaaS Client Appliances page. An entry appears in the peering list with the appliance serial number, access list status, peering certificate status, date of last contact, and notes. The access lists are designated by these categories:

- **Graylist** - Indicates a SteelHead of unknown status. This list serves as a temporary holding place for all registered SteelHeads that are attempting to establish SaaS acceleration. You can move these appliances to the whitelist or blacklist, but you cannot move appliances to the graylist.
- **Whitelist** - Indicates a trusted SteelHead or Mobile Controller. When you move an appliance to the whitelist, the appliance's peering certificate is copied to the SaaS service cluster and other peer appliances. Once an appliance has been whitelisted, subsequent peering CA uploads automatically replace the older peering CA and changes are pushed out to the SaaS service cluster and SCM managed SteelHeads.
- **Blacklist** - Indicates untrusted SteelHeads and Mobile Controllers. When you select blacklist for a peer in a whitelist or graylist, SCM removes the peering CA that it uploaded from the appliance and stops acceleration. You can move appliances between the whitelist and the blacklist. (Note: Connections are expected to fail for approximately an hour when moved from the blacklist to the whitelist.)

When you have configured SteelHead appliances and Mobile Controllers to use the SaaS acceleration service, you need to move those systems to the whitelist on SCM to indicate trust and allow acceleration.

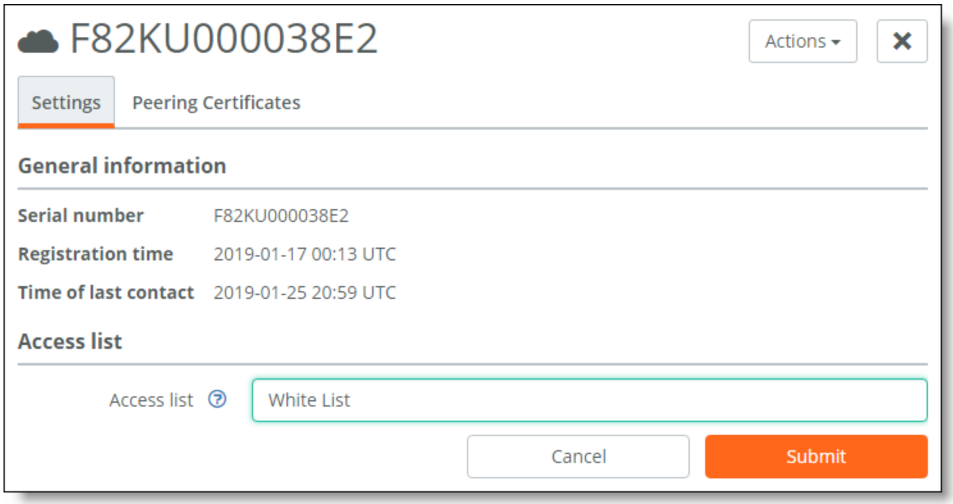
To change the access list status for an appliance

1. In SCM, choose Optimization > SaaS Client Appliances.

2. Select the row for the appliance to change.

The appliance settings pane appears.

Figure 3-20. Changing access list status



F82KU000038E2

General information

Serial number F82KU000038E2

Registration time 2019-01-17 00:13 UTC

Time of last contact 2019-01-25 20:59 UTC

Access list

Access list ⓘ White List

3. From the Access list drop-down list, select the type of list for the appliance.
4. Click **Submit**.

Resizing a SaaS service cluster

You can resize a SaaS service cluster from SCM.

To resize a SaaS service cluster

1. Choose Optimization > SaaS Accelerator and select the application row.

   The application settings pane appears.

2. In the application settings, change the number of users.

   This adjusts the capacity of the cluster without changing the service endpoint. This operation can take up to 30 minutes.

When you resize a service cluster, the cache is cleared (all traffic will be cold) and proxy and peer certificates will be auto-signed again.

Deleting appliances from SCM

If you no longer want an appliance to be part of your SaaS acceleration service, you can permanently remove an appliance from the SCM configuration. This is a permanent alternative to blacklisting.

Tip: The preferred method is to deregister from the client appliance. When you do this, SCM automatically removes the appliance and updates its configuration.

To delete an appliance from SCM SaaS acceleration

1. Choose Optimization > SaaS Client Appliances and select the appliance row.

   The appliance pane appears.

2. From the Actions drop-down list, select Delete this appliance.

3. When prompted, click **Confirm**.

You should also deregister this appliance (using the client's web interface) after deleting the appliance from SCM.

Configuration through the CLI

You can configure SaaS acceleration through the CLI as well as the web interface. These are the primary commands:

- show service saas-accel
- show service saas-accel applications
- service saas-accel register scm <scm-domain-name> token <token-value>
- service saas-accel enable
- in-path rule auto-discover dst-app <app-name> rulenum start
- no service saas-accel register

The Mobile Controller supports these additional commands:

- policy id <id> in-path rule auto-discover dst-app <app-name>
- policy id <id> ssl enable
- policy id <id> saas-accel enable

For more information, see the *Riverbed Command-Line Interface Reference Manual*.

4

Monitoring SaaS Acceleration

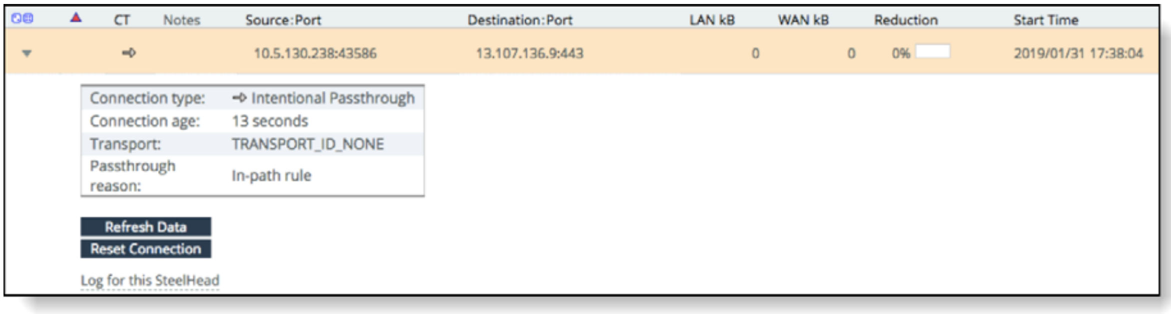
This chapter describes how to monitor SaaS Accelerator components and usage. It includes these sections:

Monitoring initial SaaS traffic

You can review the connection activity and status on the SteelHead on the Reports > Networking: Current Connections page.

For a new cluster, the SaaS application classification for the first connection is not recognized (it does not yet match the in-path rule) and the connection is passed through.

Figure 4-1. First SaaS connection intentionally passed through



		CT	Notes	Source:Port	Destination:Port	LAN kB	WAN kB	Reduction	Start Time
▾		➪		10.5.130.238:43586	13.107.136.9:443	0	0	0%	2019/01/31 17:38:04

Connection type:	➪ Intentional Passthrough
Connection age:	13 seconds
Transport:	TRANSPORT_ID_NONE
Passthrough reason:	In-path rule

The SteelHead uses the first connection to classify the application, and the application classification will be recognized for the second connection.

Subsequent connections are recognized and redirected to the SaaS service cluster. The initial connection to each service instance will generate an SSL error while the SaaS service cluster obtains the proxy certificate for the traffic to accelerate.

For SteelHead Mobile, you can review the connection activity and status of clients from either the Endpoint Report on the SteelCentral Controller for SteelHead Mobile or from the Status tab of an individual SteelHead Mobile client.

SteelHead Mobile begins to accelerate SaaS traffic after receiving the updated policy with the SaaS application in-path rule and SaaS Accelerator is enabled. For SteelHead Mobile communication with a new cluster, the first connection is intentionally passed through to classify the application and acceleration begins with the second connection. SteelHead Mobile might encounter SSL errors and pass through traffic until the proxy certificate for the SaaS application is available on the SaaS service cluster.

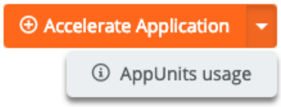
Monitoring AppUnit usage

AppUnits are required for SaaS acceleration, and you need available AppUnits to configure applications for SaaS acceleration.

To view AppUnit usage

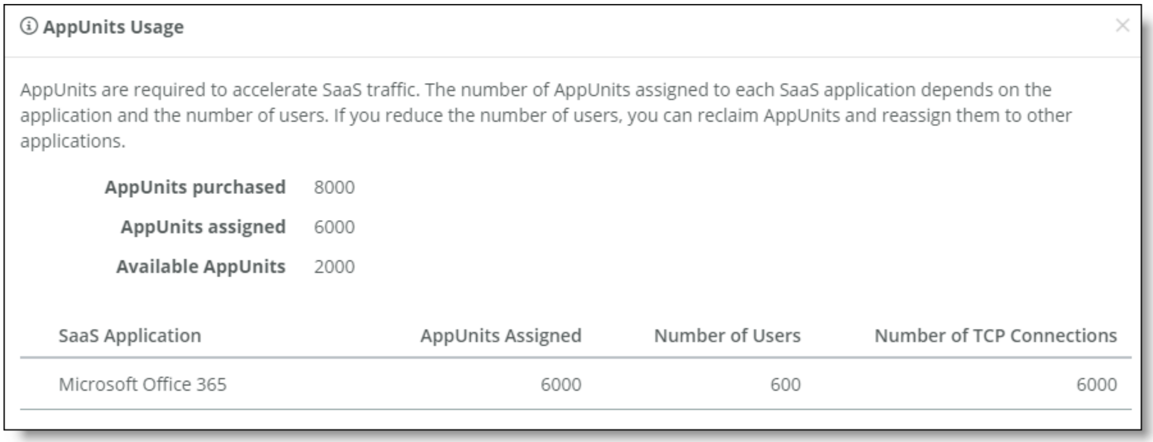
1. Choose Optimization > SaaS Accelerator.
2. From the Accelerate Application drop-down list, choose AppUnits Usage.

Figure 4-2. AppUnits Usage from Accelerate Application drop-down list



The AppUnits Usage dialog box shows the AppUnits purchased, the AppUnits assigned, and the available AppUnits.

Figure 4-3. AppUnit usage



AppUnits are required to accelerate SaaS traffic. The number of AppUnits assigned to each SaaS application depends on the application and the number of users. If you reduce the number of users, you can reclaim AppUnits and reassign them to other applications.

AppUnits purchased	8000
AppUnits assigned	6000
Available AppUnits	2000

SaaS Application	AppUnits Assigned	Number of Users	Number of TCP Connections
Microsoft Office 365	6000	600	6000

This dialog box also shows the current assignments for configured SaaS applications.

Monitoring SaaS connections

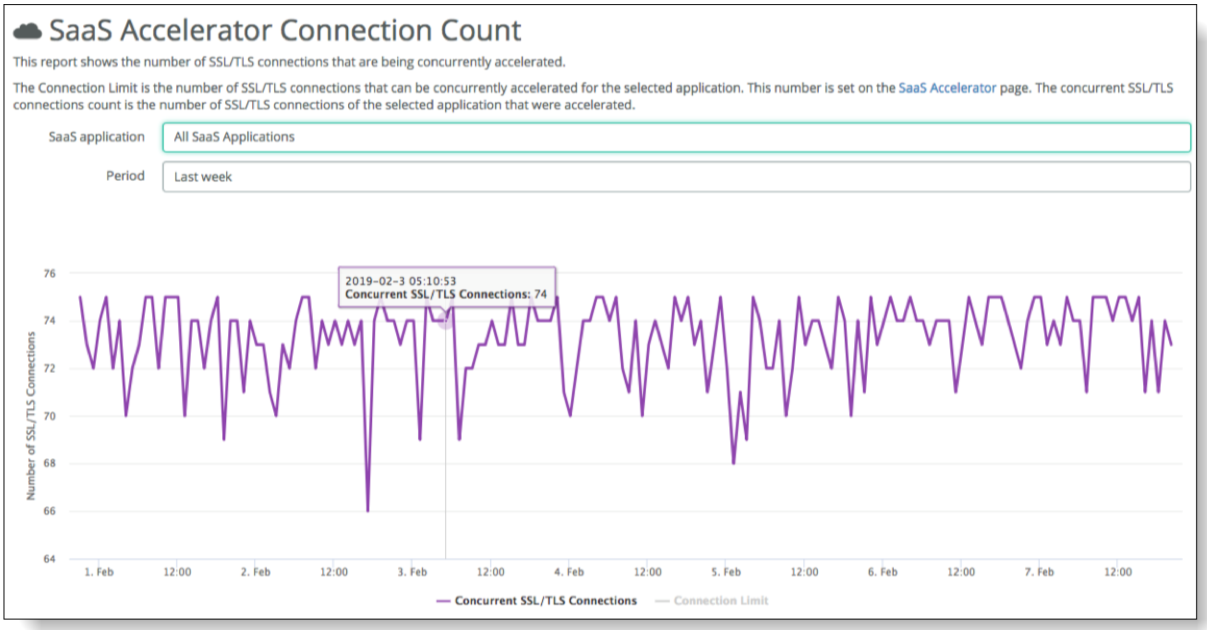
The SaaS Accelerator Connection Count report shows information about SSL/TLS connections for accelerated applications. Monitor this page to ensure your connection count remains below your connection limit.

To view connection usage

1. Choose Optimization > SaaS Connection Count.

   The SaaS Accelerator Connection Count page appears.

Figure 4-4. SaaS Accelerator Connection Count report



SaaS Accelerator Connection Count

This report shows the number of SSL/TLS connections that are being concurrently accelerated.

The Connection Limit is the number of SSL/TLS connections that can be concurrently accelerated for the selected application. This number is set on the SaaS Accelerator page. The concurrent SSL/TLS connections count is the number of SSL/TLS connections of the selected application that were accelerated.

SaaS application: All SaaS Applications

Period: Last week

2. From the SaaS Application drop-down list, select to view all application connections or select a specific application.

3. Specify a time period for the report.

   This can range from the last hour to the last year.

The report shows the concurrent SSL/TLS connections count for the selected application. Click the Connection Limit link at the bottom of the chart to display the connection limit based on the user limit specified on the SaaS Accelerator page when you configured the acceleration for the application.

Monitoring SaaS data usage

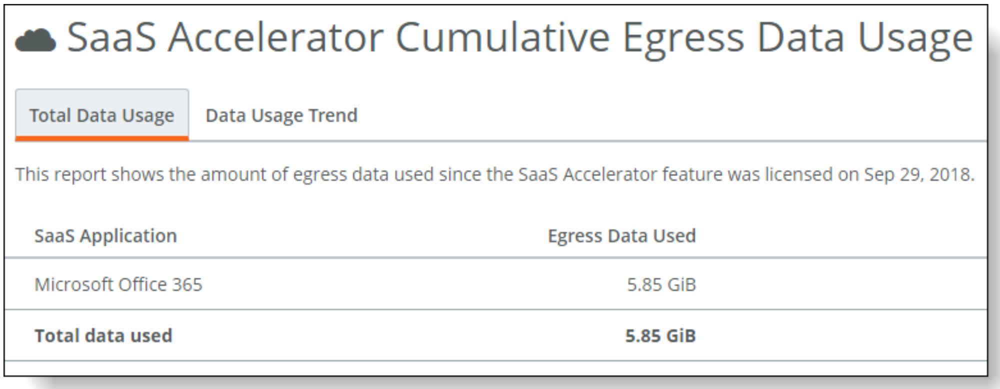
The SaaS Data Usage report shows the amount of SaaS service data used since the SaaS Accelerator feature was licensed.

To view data usage

1. Choose Optimization > SaaS Data Usage.

The SaaS Accelerator Cumulative Egress Data Usage page shows the usage history.

Figure 4-5. SaaS total data usage



SaaS Accelerator Cumulative Egress Data Usage

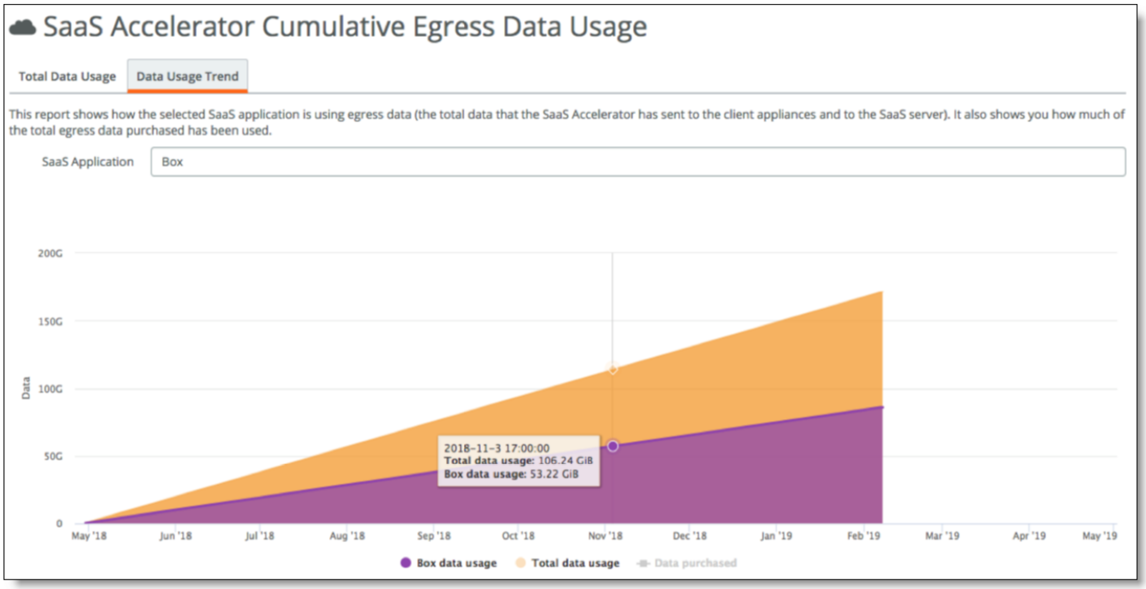
This report shows the amount of egress data used since the SaaS Accelerator feature was licensed on Sep 29, 2018.

SaaS Application	Egress Data Used
Microsoft Office 365	5.85 GiB
Total data used	**5.85 GiB**

2. Select the Data Usage Trend tab to view application-specific data usage and see how application usage compares to overall usage.

   Select Data Purchased (under the graph) to show how your data usage compares to the data limit provided by your license.

Figure 4-6. SaaS data usage trend



SaaS Accelerator Cumulative Egress Data Usage

This report shows how the selected SaaS application is using egress data (the total data that the SaaS Accelerator has sent to the client appliances and to the SaaS server). It also shows you how much of the total egress data purchased has been used.

SaaS Application: Box

Monitoring data reduction for accelerated SaaS traffic

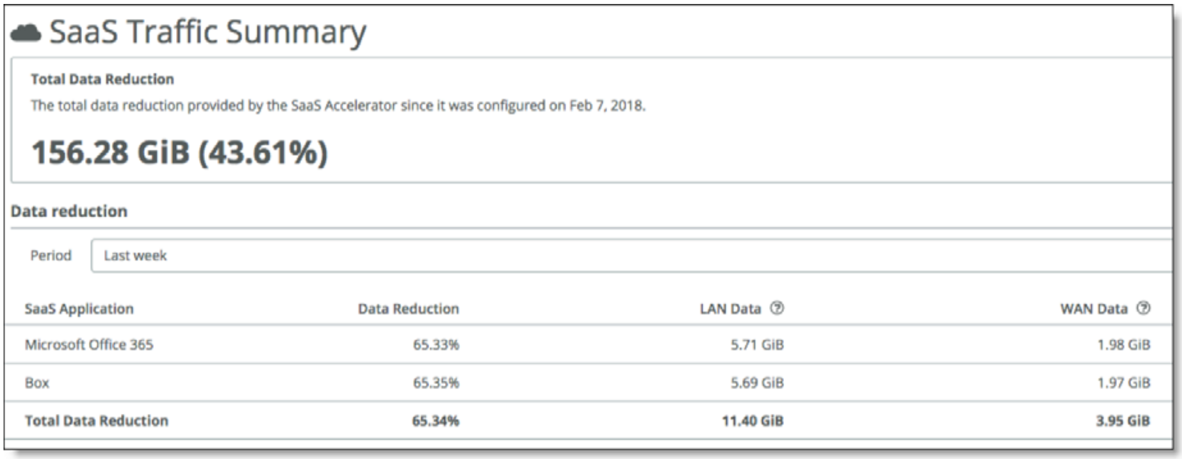
The SaaS Traffic Summary reports shows the total data reduction provided by SaaS Accelerator since it was configured and lets you filter it by time period. The report also shows the data reduction for each configured SaaS application.

To view data reduction

- Choose Optimization > SaaS Traffic Summary.

The SaaS Traffic Summary page shows the overall data reduction and application details.

Figure 4-7. SaaS Data Reduction report



SaaS Traffic Summary

Total Data Reduction

The total data reduction provided by the SaaS Accelerator since it was configured on Feb 7, 2018.

156.28 GiB (43.61%)

Data reduction

Period: Last week

SaaS Application	Data Reduction	LAN Data	WAN Data
Microsoft Office 365	65.33%	5.71 GiB	1.98 GiB
Box	65.35%	5.69 GiB	1.97 GiB
Total Data Reduction	**65.34%**	**11.40 GiB**	**3.95 GiB**

You can filter the results by time period ranging from the last hour to the last year.

The LAN Data column displays the amount of data transferred between the SaaS service cluster and the SaaS servers. The LAN data includes ingress and egress traffic on the SaaS LAN side.

The WAN Data column displays the amount of data transferred between the SaaS service cluster and the SteelHead clients. The WAN data includes ingress and egress traffic on the WAN side.

Data Reduction is a percentage based on LAN data compared to WAN data.

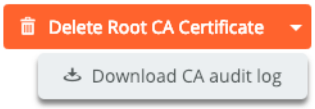
Monitoring certificate signing activity

From SCM, you can download a compressed archive of log files that shows the history and details of the certificate signing operations for SaaS acceleration. The log includes information for root CA, proxy, and peering certificates.

To review the certificate activity and log

1. In SCM, choose Optimization > SSL Optimization.
2. Click the arrow to the right of Delete Root CA Certificate and click **Download CA audit log**.

Figure 4-8. Downloading the CA audit log



Your browser downloads a ZIP-format archive file to your computer. Depending on your browser configuration, it might prompt you for a location to store the file or simply store the file in your default Downloads folder. The default name for this file is *Organization*_SteelConnect_CA_Audit_Log.zip where *Organization* is the short name of your organization.

Opening the archive displays a text file with a name in the format:

SteelSecure_org-*Organization*-xxxxxxxxxxxxxxxx_audit.txt where *Organization-xxxxxxxxxxxxxxxx* identifies your organization. This is the most recent audit log of certificate activity. There might be additional files with a date/time string appended. Each of these files contains audit log records for a previous period up to the date and time in the filename.

Each audit log consists of multiple lines of text that provide you the following details:

- A log line that includes:
  - The date and time (in UTC) that the operation occurred.
  - The Certificate Authority operation that was performed (create a CA, delete a CA, sign a peering certificate, or sign a proxy certificate).
  - The organization or SaaS Accelerator service instance for the operation.
  - The common name (CN=) of the certificate.
- The full text of the certificate in base-64 (PEM) format.

When signing certificates for a SaaS Accelerator service instance, the log line includes the Service Endpoint IP address. This enables you to easily correlate proxy certificates with the accelerated SaaS service in case the common name is not self-explanatory.

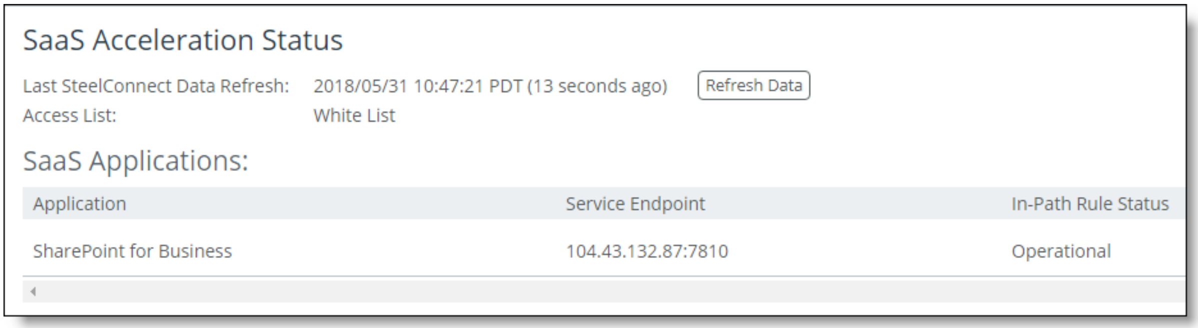
Monitoring SaaS acceleration from the SteelHead

From the SteelHead, you can use the SaaS Acceleration Status pane to monitor activity. This pane shows all SaaS applications configured for acceleration and shows the status of their in-path rules.

To display the SaaS Acceleration Status pane

- On the SteelHead appliance, choose Optimization > SaaS: SaaS Accelerator.

Figure 4-9. SaaS Acceleration Status pane



SaaS Acceleration Status

Last SteelConnect Data Refresh: 2018/05/31 10:47:21 PDT (13 seconds ago)
Access List: White List

SaaS Applications:

Application	Service Endpoint	In-Path Rule Status
SharePoint for Business	104.43.132.87:7810	Operational

If the In-Path Rule Status is Operational, an in-path rule has been configured for this application. If the In-Path Rule Status is Not Configured, an in-path rule has not been configured. If the feature has been disabled, all SaaS applications display Not Configured.

The SteelHead gets data from SCM every five minutes and shows the time for the displayed data. Click **Refresh Data** to get the latest information.

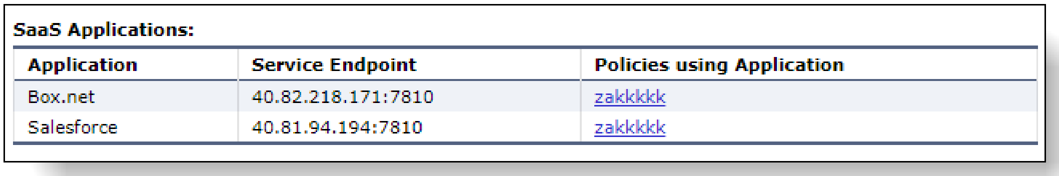
Monitoring SaaS acceleration on Mobile Controllers

From the Mobile Controller, you can use the SaaS Acceleration Status pane to monitor activity. This pane shows all SaaS applications configured for acceleration and the list of policies for which in-path rules have been set up for SaaS acceleration.

To display the SaaS Acceleration Status pane on a Mobile Controller

- On the Mobile Controller, choose Configure > SaaS Accelerator.

Figure 4-10. SaaS Acceleration status pane



SaaS Applications:

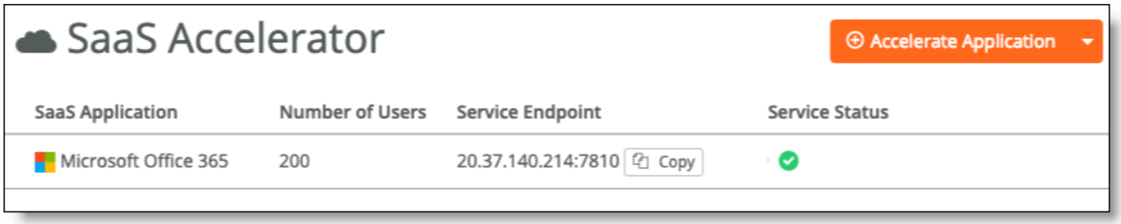
Application	Service Endpoint	Policies using Application
Box.net	40.82.218.171:7810	zakkkkk
Salesforce	40.81.94.194:7810	zakkkkk

The SteelHead Mobile gets data from SteelConnect Manager every five minutes and shows the time for the displayed data. Click **Refresh Data Now** to get the latest data.

Monitoring SaaS service cluster status

From SCM, you can monitor the status of the SaaS service cluster for each accelerated application. Choose Optimization > SaaS Accelerator page to display the status.

Figure 4-11. SaaS service cluster status



SaaS Application	Number of Users	Service Endpoint	Service Status
Microsoft Office 365	200	20.37.140.214:7810	✓

The service status can be one of these values:

- **Healthy (Green)** - The service cluster is operating normally and is capable of acceleration.
- **Degraded (Yellow)** - The service cluster is not functioning at full capacity.
- **Critical (Red)** - The service cluster is unavailable and is not accelerating SaaS traffic.

5

License Enforcement

The SaaS Accelerator requires licenses to control the number of users and the amount of accelerated data. This chapter describes license enforcement considerations, including these topics:

License expiring

As you approach your license expiration date, warning emails are sent to realm and organization administrators and an alert is posted to the SaaS Accelerator page.

If your license expires and you exceed your 30-day grace period, the configuration is undeployed and deleted. (You will need to completely reconfigure the SaaS Accelerator to restart the service.)

We recommend renewing your license when the warnings begin. You can review your license expiration dates on the Organization > Licenses page in SCM.

Exceeding data license limits

As you approach your data license limits, warning emails are sent to realm and organization administrators and an alert is posted to the SaaS Accelerator page.

If an organization exceeds the data limit, Riverbed will invoice the customer for data overage fees. For more information, see the this document:
https://www.riverbed.com/document/legal/saas-accelerator-data-overage-fees.pdf

If an organization exceeds the data limit, the SaaS service cluster stops acceleration. To resume service, purchase more data within the grace period.

You can monitor your AppUnit and data usage from SCM. For details, see "Monitoring AppUnit usage" on page 38.

As you approach your license limits, we recommend increasing your usage limits with add-on licenses.

Reaching connection limits

When the SaaS Accelerator service reaches the number of connections for its configured limits, it enters admission control and new connections matching the SaaS application defined in the client-side appliance in-path rule will not be accelerated.

The SaaS Accelerator service accelerates new connections after it exits admission control.

6

Troubleshooting

This chapter describes how to troubleshoot issues, including these topics:

- "Client-side SteelHead troubleshooting" on page 47
- "SteelHead Mobile client troubleshooting" on page 48

Client-side SteelHead troubleshooting

This section includes troubleshooting suggestions for SteelHead and SteelHead SD on the client side.

Verify SaaS acceleration is running

SaaS Accelerator uses a new method to classify application traffic and the client appliance needs to recognize this type of application traffic. (The SaaS Accelerator uses the DPI classification engine.)

If you do not see accelerated SaaS connections, use the **show service saas-accel application cache** command. SaaS acceleration will not happen until an entry appears in the output of this command.

To troubleshoot application classification, ensure the logging level is set to info (this is the default level).

To set the log level to info

- Enter these commands on the SteelHead command line:

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

If you don't want to make this change globally, you can also set the log level specifically for the application classification logs.

To set application classification logs to the info level

- From the CLI, run this command:

```
logging filter qosd level info
```

When application classification is successful, log messages for the classification service appear:

```
“Doing appctrl query dst:... ”
"Snoopy: Classified app for dst:..."
"Snoopy: Appid # found in cache ..."
```

If application classification is failing, the following message appears in the logs:

```
   "Snoopy: Failed to resolve appctrl server..."
```

To correct application classification failure, make sure the client SteelHead can resolve hostnames and DNS is working properly. Application classification relies on the appcs.x.riverbed.cc server and the client-side SteelHead must be able to resolve this hostname and reach this server.

Displaying SaaS service cluster peers for client-side appliances

To see details of the SaaS service cluster peered with the client-side SteelHead appliance

- From the SteelHead web interface, choose Reports > Peers.
- From the CLI, run the **show peers** command.

```
amnesiac > show peers
S IP              Name             Model   Version Licenses
- --------------- ---------------- ------- ------- ----------------------------
O 20.37.127.226   XNFD25BAE78DF17A SaaS-   1.0.0   CIFS/MAPI/SSL
O 172.16.2.3      steelhead-1      VCX     9.8.1   CIFS/MAPI/SSL/ORACLE-FORMS

O = online, U = unknown
Total appliances: 2
Connected appliances: 2
```

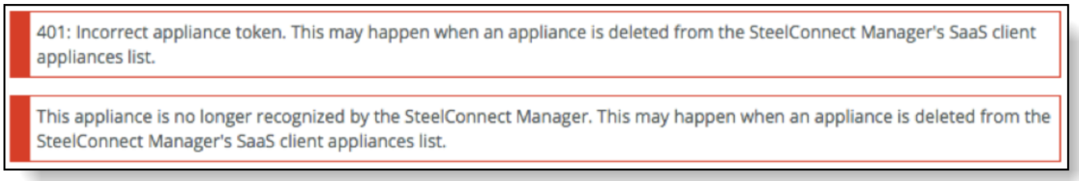
Client-side SteelHead splice logs also indicate the SaaS service cluster peer.

SteelHead error messages

These errors appear on the SteelHead if an appliance is deleted from the SCM list of SaaS appliances.

- 401: Incorrect appliance token.
- This appliance is no longer recognized by the SteelConnect Manager.

Figure 6-1. SaaS registration errors



401: Incorrect appliance token. This may happen when an appliance is deleted from the SteelConnect Manager's SaaS client appliances list.

This appliance is no longer recognized by the SteelConnect Manager. This may happen when an appliance is deleted from the SteelConnect Manager's SaaS client appliances list.

To clear these errors, you need to deregister the appliance using the client SaaS acceleration interface. For details, see "Canceling SaaS acceleration" on page 25.

SteelHead Mobile client troubleshooting

SaaS acceleration uses a new method to classify application traffic, and the SteelHead Mobile clients need to recognize this type of application traffic. (The SaaS Accelerator service runs as part of the qosd process.)

Application classification relies on the appcs.x.riverbed.cc server and SteelHead Mobile clients must be able to resolve this hostname and reach this server.

If you do not see accelerated SaaS connections, use the **rbtdebug -f dns_table** command to review the DNS mapping between hostnames and IP addresses and the **rbtdebug -f app** command to review the list of applications the SteelHead Mobile has classified.