



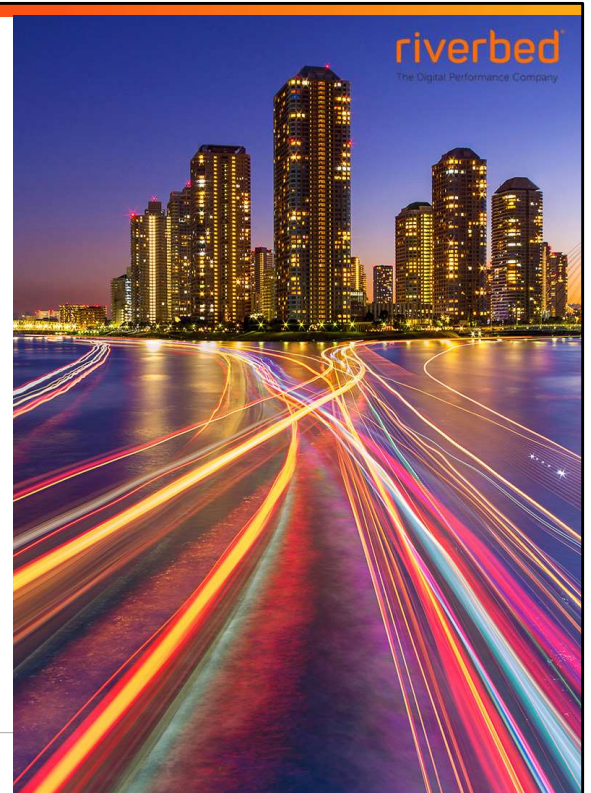
Configure SteelHead SaaS Accelerator

Learning Objectives

After completing this module, you will be able to:

- Describe the Legacy SaaS Accelerator.
- Describe the SaaS Accelerator Service.
- License the SaaS Accelerator.
- Deploy client-side SteelHeads with SaaS Acceleration.
- Deploy SaaS for SteelHead Mobile.
- Verify and troubleshoot SaaS acceleration.

© 2021 Riverbed Technology, Inc. All rights reserved.



Key Points



Cloud adoption is growing fast. It's taking consolidation to the next level.



With more and more data and applications accessed in the cloud, users are more exposed than ever to the limits of the WAN.



With Riverbed SaaS Accelerator, these cloud applications can be optimized, allowing Cloud services to be accessed as if they were local.

Why the Growth in Cloud Services?

Consolidation Taken to the Next Level

- Cloud adoption is growing fast due to a number of key advantages:
 - Flexibility and elasticity
 - Backup and disaster recovery
 - Automatic software updates
 - Reduced capital expend
 - Increased collaboration
 - Flexibility to work from anywhere
 - Increased security due to reduced local footprint

When Riverbed SteelHead appliances were first introduced they were very much an enabler of consolidation, allowing enterprises to remove expensive branch IT while users now accessed applications from branches halfway around the world as if they were sitting next to the server.

This had the 'double whammy' of reducing costs while at the same time improving user productivity. This drove a trend of consolidation which, due in part to advances in virtualization, has now moved to the next stage.

Rather than businesses simply consolidating their infrastructure, increasingly both public and private clouds are being utilized.

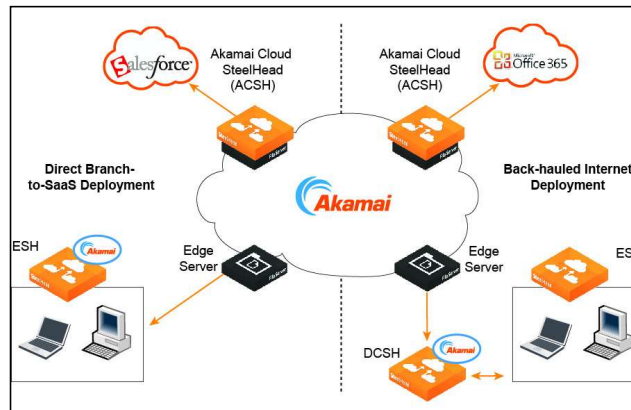
Cloud services are growing fast due to offering elastic provisioning of services and compute, and allowing users to simply pay for resources when they need them. Rather than having to pay for and maintain expensive hardware, cloud services can be implemented with a contract and an SLA.



SteelHead SaaS Configurations – Deployment Types

Deployment Topologies

- Two types of deployment
 - Direct Branch Internet
 - Back-hauled Internet

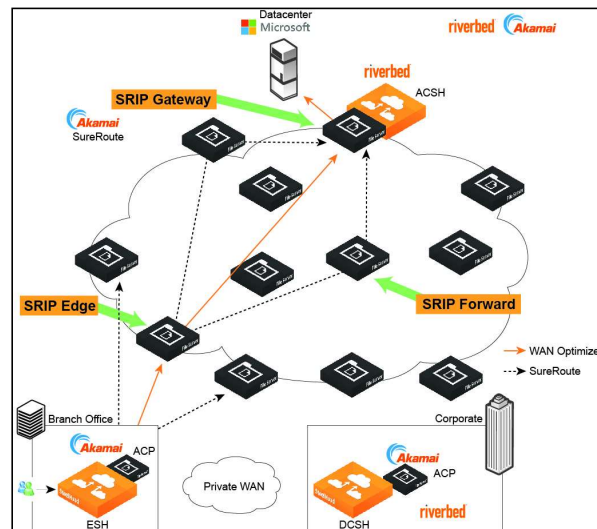


© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 6

An internet link is required in order to access the Akamai network. There are, therefore, two deployment configurations, depending on whether there is a direct breakout at the branch or whether the internet connection is via the datacenter. These two configurations are termed *Direct Branch* or *Back-Hauled* respectively.

Deployment Configurations - Direct Branch Internet



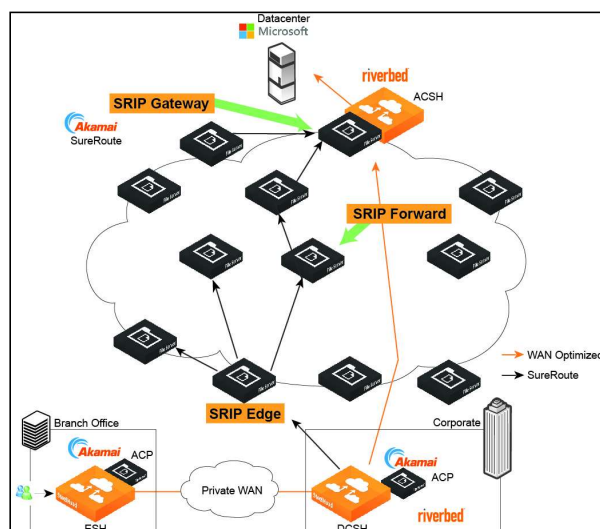
© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 7

After the ESH 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, Direct Branch mode, is very simple with optimization and redirection to the Akamai network both being performed by the ESH.

Deployment Configurations – Back-Hauled Internet



© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 8

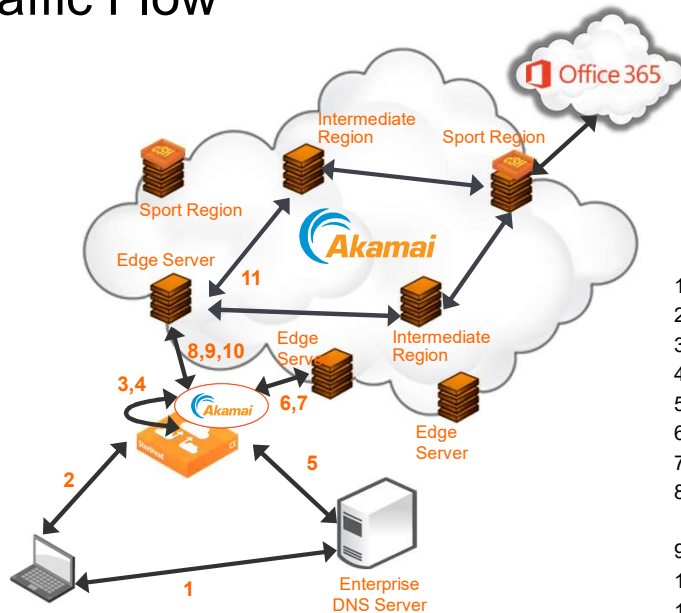
In this topology, the branch does not have its own connection to the Internet. All traffic directed to the Internet is back-hauled over a private WAN or VPN to the organization's datacenter.

For Back-Hauled mode, the optimization is still performed by the ESH, but it adds special information in the inner-channel packets to indicate that this is traffic directed to the SaaS provider. When the Data Center SteelHead (DCSH) 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 DCSH unwraps the inner channel traffic from the tunnel before sending it across the WAN to the ESH appliance.

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

In both cases, the traffic is UDP encapsulated across the Akamai network.

Traffic Flow



Ports

TCP 443 (SSL between ESH and ACSH)
 UDP 53 (DNS requests)
 UDP 9545 (UDP tunnel to SRIP Edge)

1. Client makes DNS req for SaaS URL to DNS Server
2. Client makes TCP connection to SaaS provider
3. SH intercepts connection pkt and checks SaaS list
4. SH passes to ACP software on SteelHead
5. ACP makes DNS req for SRIP Edge to DNS server
6. ACP now makes UDP tunnel with SRIP Edge
7. SRIP *may* redirect to a closer SRIP edge
8. ACP forms UDP tunnel with SRIP Edge and Akamai finds nearest Sport region (ACSH) to destination
9. ACP forwards discovery probe
10. SRIP Edge checks entitlement code, cust, id, cpcode
11. SRIP forwards to ACSH

© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 9

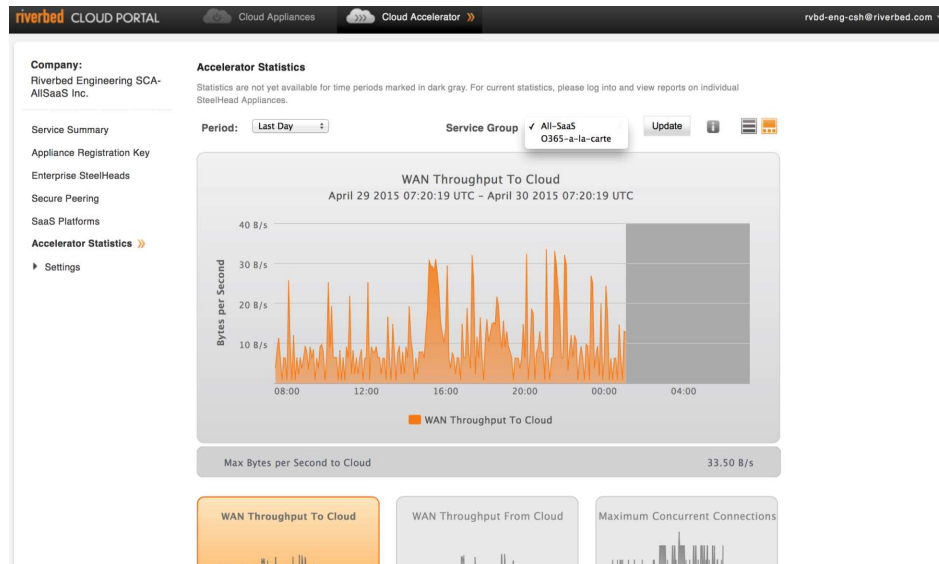
The Riverbed Cloud Portal

- A cloud resource which registers SteelHeads, allowing them to use SteelHead SaaS
- Manages SaaS certificates

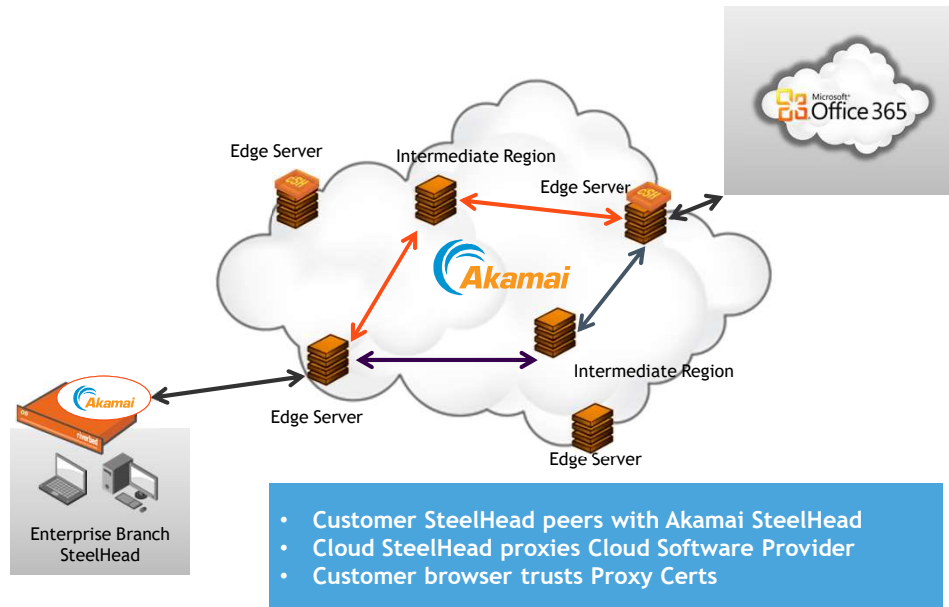
The screenshot displays the Riverbed Cloud Portal interface. The top navigation bar includes the Riverbed logo, 'CLOUD PORTAL', and links for 'Cloud Appliances' and 'Cloud Accelerator'. The left sidebar contains a menu with items like 'Company', 'Service Summary', 'Appliance Registration Key', 'Enterprise SteelHeads', 'Secure Peering', 'SaaS Platforms', 'Accelerator Statistics', 'Settings', 'General Settings', and 'Certificate Settings'. The main content area is divided into two sections: 'Enterprise SteelHead Summary' and 'SaaS Services Summary'. The 'Enterprise SteelHead Summary' section shows statistics: 0 SteelHeads Pending Service, 4 SteelHeads Granted Service, and 0 SteelHeads Denied Service. The 'SaaS Services Summary' section contains a table with columns for Service Group, Application Name (ID), Provider, and Acceleration Service.

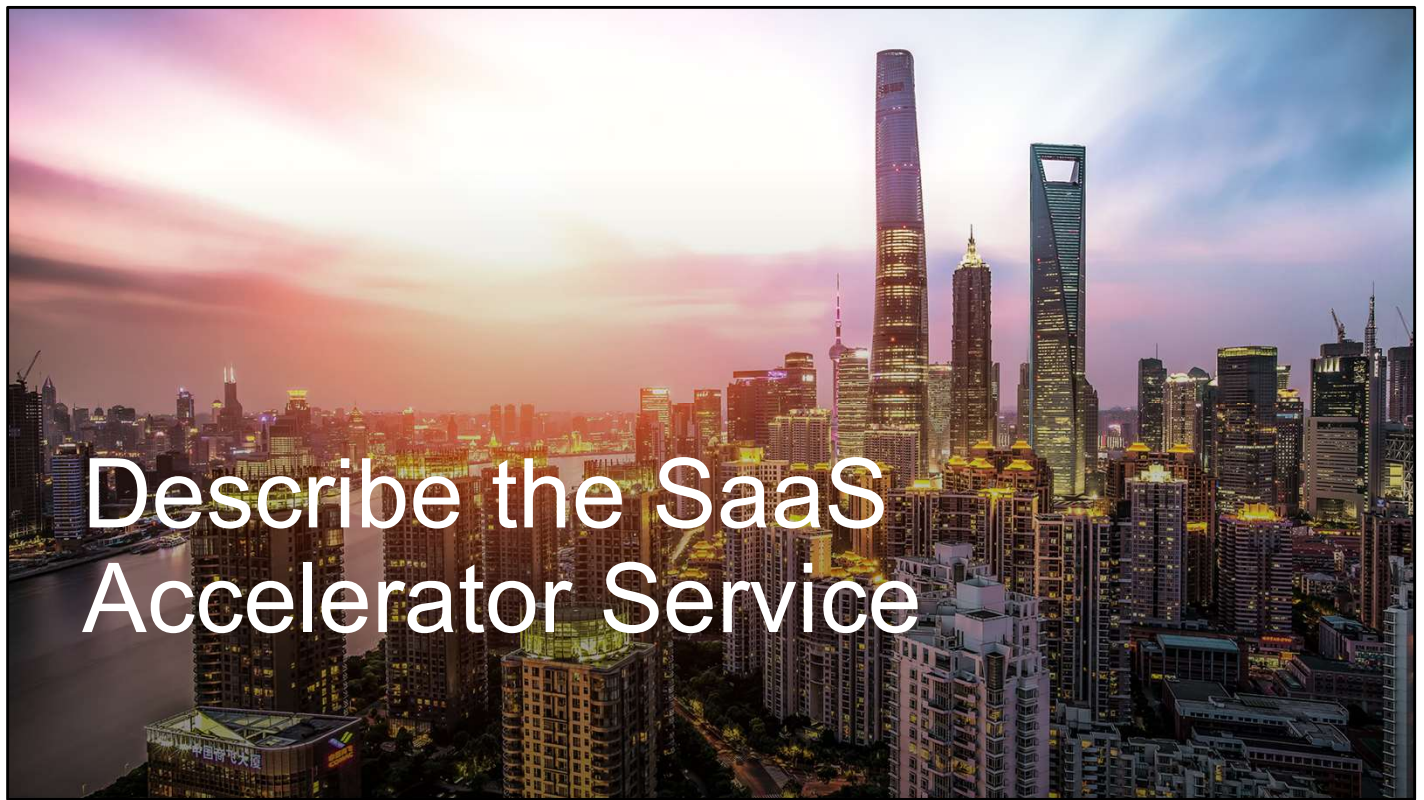
Service Group	Application Name (ID)	Provider	Acceleration Service
All-SaaS	box.net (BOX)	Box Inc	ON
All-SaaS	Office 365 (O365)	Microsoft Inc.	ON
All-SaaS	Salesforce.com (SFDC)	Salesforce.com Inc.	ON
O365-a-la-carte	Office 365 (O365)	Microsoft Inc.	ON

Cloud Portal Statistics



SSL Optimization with SteelHead SaaS





SaaS Accelerator Service – Management

- Riverbed SaaS Accelerator Service is managed by SaaS Accelerator Manager (SAM).
 - Client-side appliances registered with SAM:
 - RiOS client-side SteelHead
 - SteelHead Mobile clients registered through an SCCM
 - SteelHead SD 2.0
 - Server-side managed by Riverbed
- Automatic peering and proxy certificate management

SaaS Accelerator Service – Supported Applications

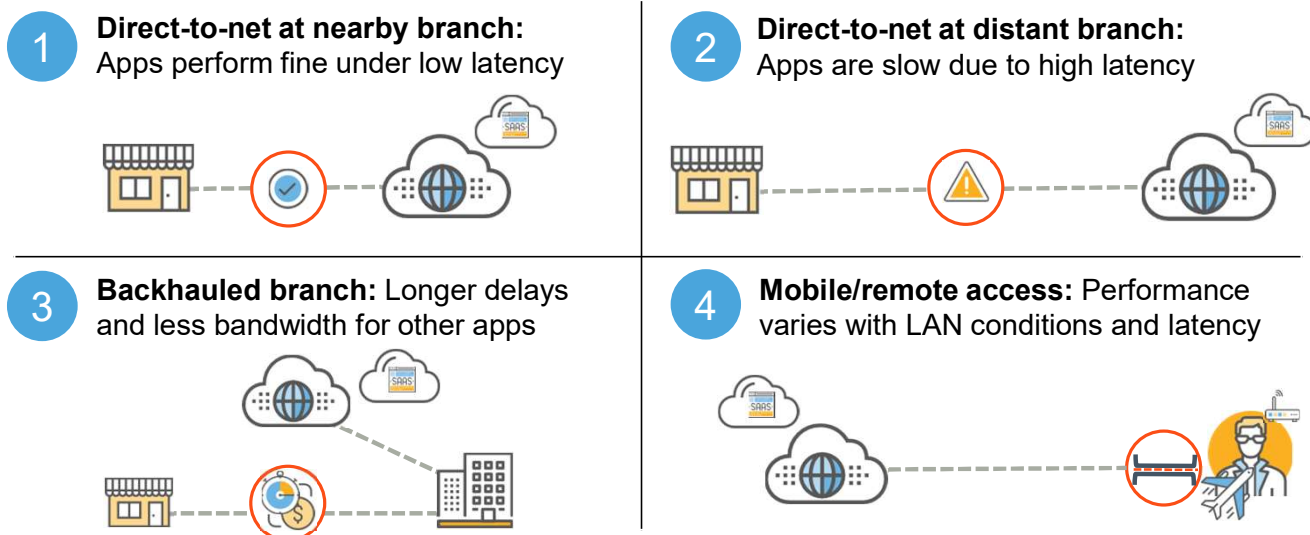
- Supported applications:
 - Microsoft Office 365 (includes Exchange, SharePoint, MS Office WebApps, MS Authentication and Identity services)
 - Box
 - ServiceNow
 - Salesforce
 - Veeva

Required Components to Make this Work

- SaaS Acceleration Manager (SAM), as of March 2020
- A valid license token for SaaS Accelerator
- Riverbed client-side appliances:
 - Client-side SteelHead
 - RiOS SteelHead running 9.8.1/9.9.0 or higher
 - SCCM/SHM running 6.1.0 or higher
 - Steelhead SD 2.0 appliance with vSH running 9.8.1 or higher
 - Open up TCP port 3900 for the SH/SCCM to communicate with SAM

Cover Your SaaS? Performance Varies

Four Scenarios, Four Different User Experiences



© 2021 Riverbed Technology, Inc. All rights reserved.

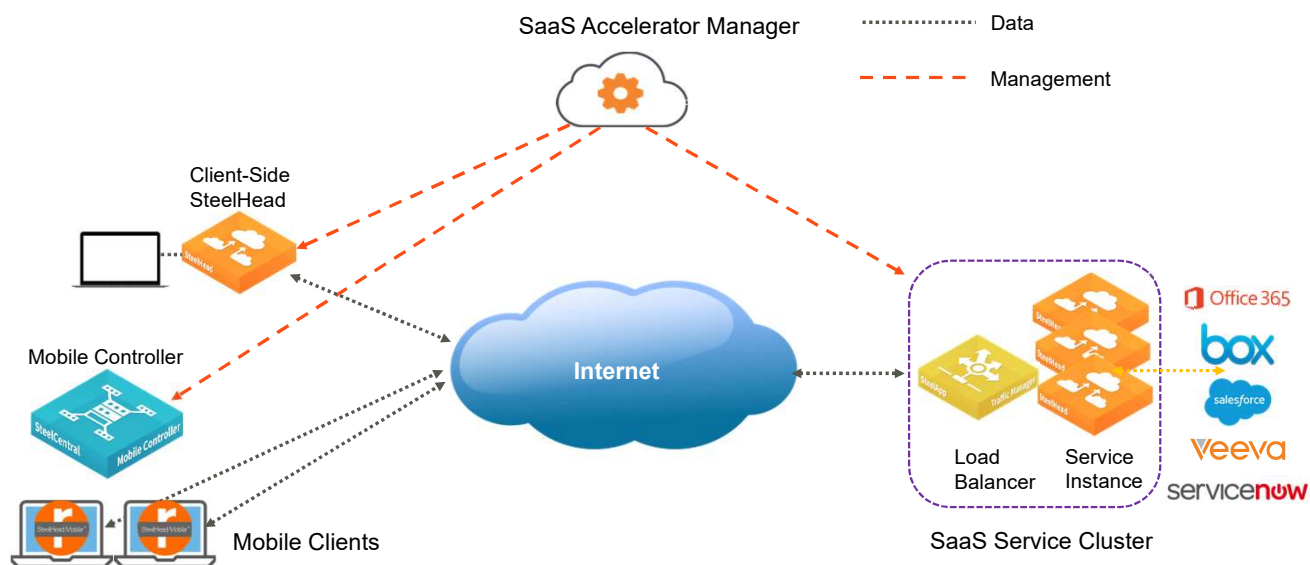
riverbed 17

So we've established that SaaS apps are critical for businesses today, yet the performance of those apps can be problematic to manage. Let's touch a little more upon why this is.

When we consider that companies deliver SaaS apps in different ways depending on a user's location or the company's security posture, among other factors, the user experience can be wildly inconsistent. Let's look a little closer...

- First, as you might expect – sometimes users have direct-to-net access and are doing their work from a branch or Headquarters located very close to a cloud pop. In those cases, most of the time, SaaS should run okay.
- Another example, however, is places where there is high latency for users working at a far away branch. This is going to cause performance slow-downs – and a less than productive user experience.
- Of course on top of that, in some places in the world BW is not so cheap, and so the cloud traffic going through the available pipes slows down.
- Next, there are also many enterprise companies these days who are backhauling SaaS traffic through a datacenter because of a firm security posture – and while there may be a plan to evolve from this, it won't happen overnight. Distance is distance and the speed of light doesn't get any faster. Backhauling creates more distance and causes longer delays, and that greatly hinders performance.
- And last but not least, now we have dynamic and highly mobile workforces logging on from so many different places and networks as they move through their workdays, and this makes predicting performance much more challenging
- Of course, most companies have a combination of these scenarios that impact SaaS performance – and therefore, workforce productivity.

SaaS Acceleration – Overview



© 2021 Riverbed Technology, Inc. All rights reserved.

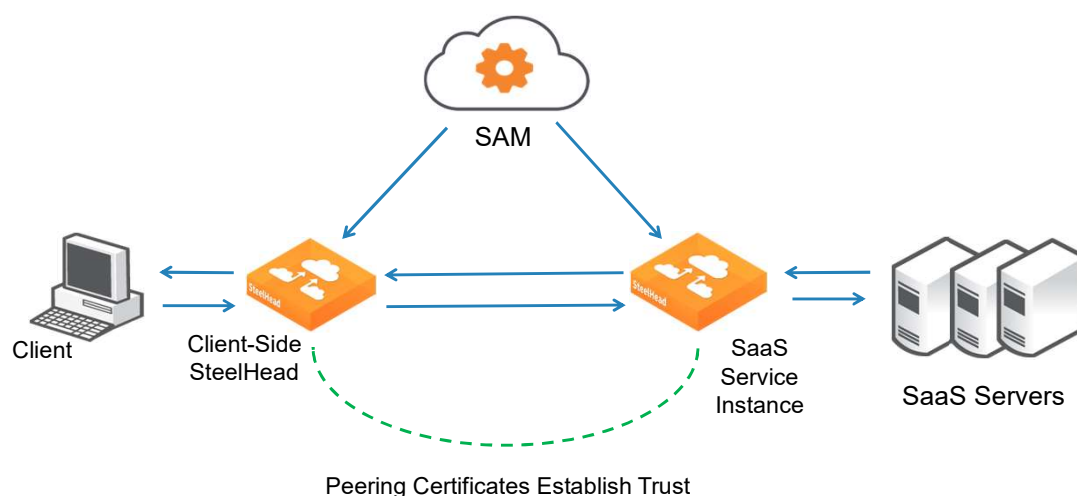
riverbed 18

When you configure a SaaS application for acceleration, SAM 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 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 SAM, the end-user traffic meant for the SaaS server goes to the client-side SteelHead. The client-side SteelHead 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 and the SaaS service cluster is accelerated.

SaaS Accelerator – Peering Trusts



© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 19

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.

The SAM uses the root CA certificate to sign peering and proxy certificates, which it pushes to the SaaS service cluster. When a client-side SteelHead is moved to the SAM white list, the SAM pushes the peering certificate signed by its root CA to the client-side SteelHead and the client-side SteelHead uploads its peering certificate to the SAM which the SAM pushes to the service cluster. This establishes the trust relationship between the client-side SteelHead and the SaaS service cluster.

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



SaaS Accelerator Licensing – AppUnits & AppData

- License includes AppUnits and AppData:
 - AppUnits are tokens that should be bought based on the number of users the customer wants to optimize.
 - AppUnits can be used for accelerating any application.
 - AppData is for the data that will be flowing through the SaaS Accelerator Service.
- Limits on the number of users and data used by the service are enforced based on the available license.

SaaS Accelerator Licensing – AppUnits/User/App

How Many AppUnits Per User?



Question 1: Which application do you want to accelerate?

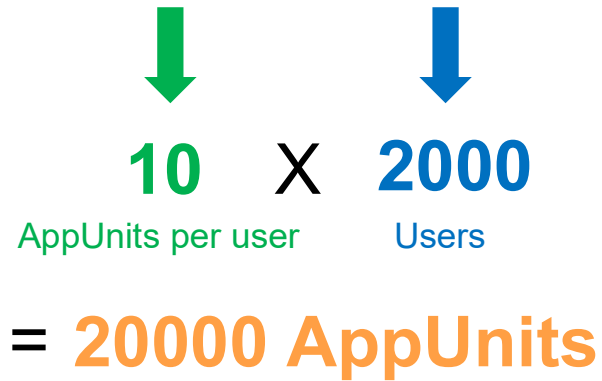
Question 2: How many users do you have?

SaaS Application	AppUnits Per User
Box	5
MS Office 365	10
Salesforce	10
ServiceNow	10
Veeva	20

- Each AppUnit includes 0.3GiB of AppData.
- AppData is pooled for all applications and all users.
- The license is specific to the SAM not per SteelHead.

Example AppUnits Calculation

Customer wants to optimize **Office 365** for **2000** users.


$$\begin{array}{ccc} \downarrow & & \downarrow \\ 10 & \times & 2000 \\ \text{AppUnits per user} & & \text{Users} \\ = & 20000 & \text{AppUnits} \end{array}$$

Configure the SaaS Accelerator

Configure the SAM and Client-Side SteelHead

- There are a number of steps to be performed.
- On the SAM:
 1. Redeem the license token on the SAM.
 2. Generate Root CA Certificate.
 3. Distribute CA to end-user machines.
 4. Configure SaaS applications for acceleration.
- On the branch SteelHead:
 1. Register clients using the SAM registration token.
 2. Enable SSL optimization on the client-side SteelHeads.
 3. Move client-side SteelHead to the white list.
 4. Enable SaaS acceleration.
 5. Add application-based in-path rules.

Redeem the License Token

Enter Token

- Enter the token on the SAM under **Organization > Licenses**.



Redeem the License Token

Verify License

- Once enabled you can view your App units and data.

 SaaS Accelerator



Info

Feature SaaS Accelerator

Serial 1VSDJQOC13DD532A97171

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

Generate Root CA Certificate

Configure Certificate Authority to Sign Peering and Proxy Certificates

- Navigate to **Optimization > SSL Optimization**.
- Click **Generate Root CA Certificate**.
- Enter the details and click **Submit**.

Generate Root CA Certificate

Common name: BredonCA

Organization: Riverbed Education

Organization unit: (Optional)

Locality: Bredon

State: (Optional)

Country: GB

Email address: dave@riverbed.com

RSA cipher bits: 2048

Validity period (days): 730

Cancel Submit

Distribute CA to End-User Machines

CA Certificate Needs to be Trusted on End-User Machines

- Click **Download** to download the certificate and then distribute to all client machines.
- Could use Group Policy in AD

The screenshot shows the Riverbed SteelHead SaaS Accelerator interface. On the left is a navigation menu with the following items: Optimization (selected), SaaS Accelerator, SSL Optimization (highlighted in orange), SaaS Client Appliances, SaaS Connection Count, SaaS Data Usage, SaaS Traffic Summary, Users, Applications, and Rules. The main content area displays the 'address' section with the following information:

- SHA1 hash:** 0b:b5:ac:a5:59:03:f9:f0:e6:fb:ce:c6:cd:00:64:8f:98:b6:8b:48
- Valid from:** 2019-06-19 14:35 UTC
- Expires on:** 2021-06-20 14:35 UTC

Below this is the 'Certificate' section, which includes 'Copy' and 'Download' buttons. The certificate text is displayed in a box:

```
-----BEGIN CERTIFICATE-----
MIIDlDCCAnygAwIBAgIIEM7gZ0qQ9WMwDQYJKoZIhvcNAQELBQAwcDELMAkGA1UE
BhMCR0IxDzANBgNVBACTBkYjZWRvbG9uMRswGQYDQKKEsJSAxZ1cmJlZCBFZHVj
aW9uMRERDwYDVQQDEWhCcMVKb25DQTEgMB4GCScqGSIB3DQEJAwRZGF2ZUByaXZl
cmJlZC5jb20wHhcNMjE5MTQzNTQzWhcNMjE5MTQzNTQzWjBwMQswCQYD
VQQGEWhQjEPMA0GA1UEBxMGQnJlZG9uMRswGQYDQKKEsJSAxZ1cmJlZCBFZHVj
YXRpb24xETAPBgNVBAMTCEYjZWRvbG9uMRswGQYDQKKEsJSAxZ1cmJlZCBFZHVj
-----
```

You need to copy or download the certificate onto the client machines.

Configure SaaS Apps – Create Service Cluster (1/3)

The screenshot shows the Riverbed SteelConnect Manager interface. The left sidebar contains a navigation menu with the following items: Dashboard, Health Check, Organization, Network Design, Routing, Optimization, SaaS Accelerator (highlighted), SSL Optimization, SaaS Client Appliances, SaaS Connection Count, SaaS Data Usage, SaaS Traffic Summary, Users, Applications, Rules, Wi-Fi, and Appliances. The main content area is titled "SaaS Accelerator" and features a table with columns: SaaS Application, Number of Users, Service Endpoint, and Service Status. A red box highlights the "Accelerate Application" button in the top right corner. Below the table, a message states: "The SaaS Accelerator has not been configured."

riverbed SteelConnect Manager

AhmetOrg 1 message Help

SaaS Accelerator

Accelerate Application

SaaS Application	Number of Users	Service Endpoint	Service Status
The SaaS Accelerator has not been configured.			

Configure SaaS Apps – Create Service Cluster (2/3)

Defining the Application Determines the SaaS Service Cluster

Accelerate Application



Application

Microsoft Office 365

Includes SharePoint Online and OneDrive for Business (1st Packet), Exchange Online (1st Packet), Office Online, Web Apps - Excel, PowerPoint, Word (1st packet), Authentication and Identity

Region ?

United States

User limit ?

800

Number of users ?

200

Accelerated SSL/TLS connections ?

2000

Cancel

Submit

© 2021 Riverbed Technology, Inc. All rights reserved.


riverbed 30



Select the region closest to where your data is located for the specified SaaS Application.



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

Configure SaaS Apps – Create Service Cluster (3/3)

Wait for the Cluster to be Created

SaaS Application	Number of Users	Service Endpoint	Service Status
 Microsoft Office 365	200	—	⚙️ Setting up SaaS acceleration. (started 86 seconds ago)

SaaS Application	Number of Users	Service Endpoint	Service Status
 Microsoft Office 365	200	52.185.64.238:7810  Copy	✅ SaaS acceleration is complete. ⚙️ Starting service (started 321 seconds ago).

SaaS Application	Number of Users	Service Endpoint	Service Status
 Microsoft Office 365	200	52.185.64.238:7810  Copy	✅



Register Clients – Copy Token from SAM

riverbed sandbox1 Help

SaaS Accelerator Client Appliances

The SaaS Accelerator license will expire in 8 days . Contact Riverbed to renew your license and benefit from uninterrupted SaaS application acceleration.

Registration Token

Registration token 10OOC13DD532A97171ESCvW7zT1Wc3TzQ2VuQH Copy Regenerate

Appliances

These appliances are registered to peer with the SaaS Accelerator.

Serial Number	Access List	Peering Certificates Status	Date of Last Contact	Hostname
No appliances have registered with this SteelConnect Manager.				

Register Clients – Copy Token to SteelHead

SaaS Accelerator SAAS > 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:

SteelConnect Manager Port:

Registration Token:

Register

Register Clients – Registered SteelHead

SaaS Accelerator SAAS > SaaS Accelerator

SaaS Acceleration

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

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

- ✓ Enable [SSL optimization](#) on this appliance.
- Move this appliance to the SteelConnect Manager's white list (on the SaaS Client Appliances page).
- Configure in-path rules for the SaaS applications that should be accelerated.
- Enable SaaS acceleration on this appliance.

SteelConnect Registration

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

Deregister

Enable SSL Optimization

Enable SSL Optimization (if not Enabled Already)

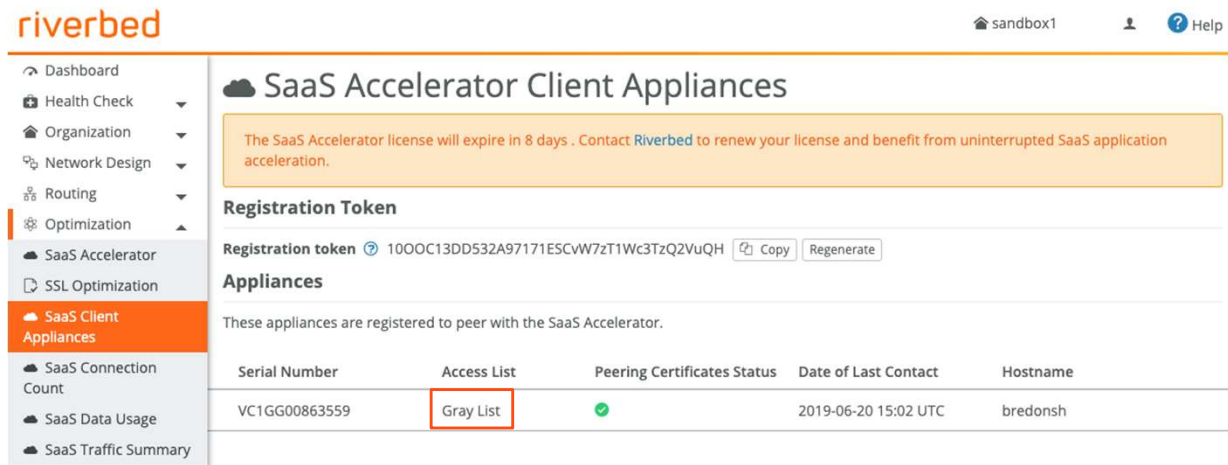
SSL Main Settings SSL > SSL Main Settings ?

General SSL Settings

☒ Enable SSL Optimization

Apply

Whitelist Appliance in SAM – Initially in Gray List



riverbed sandbox1 ? Help

SaaS Accelerator Client Appliances

The SaaS Accelerator license will expire in 8 days . Contact [Riverbed](#) to renew your license and benefit from uninterrupted SaaS application acceleration.

Registration Token

Registration token 10OOC13DD532A97171ESCvW7zT1Wc3TzQ2VuQH [Copy](#) [Regenerate](#)

Appliances

These appliances are registered to peer with the SaaS Accelerator.

Serial Number	Access List	Peering Certificates Status	Date of Last Contact	Hostname
VC1GG00863559	Gray List	✓	2019-06-20 15:02 UTC	bredonsh

Whitelist Appliance in SAM – Move to Whitelist

riverbed sandbox1 Help

SaaS Accelerator

The SaaS Accelerator license will expire

Registration Token

Registration token ⓘ 10OOC13DD532AS

Appliances

These appliances are registered to peer with

Serial Number	Access
VC1GG00863559	Gray

VC1GG00863559

Settings

Peering Certificates

General information

Serial number

VC1GG00863559

Registration time

2019-06-20 14:59 UTC

Time of last contact

2019-06-20 15:03 UTC

Access list

Access list ⓘ

White List

Cancel

Submit

Enable SaaS Acceleration on the SteelHead

SaaS Acceleration Status

Last SteelConnect Data Refresh: 2019/06/20 17:19:40 BST (49 seconds ago) [Refresh Data](#)
Access List: White List

SaaS Applications:

Application	Service Endpoint	In-Path Rule Status
Exchange Online	52.185.64.238:7810	Not configured
Office O365 authentication and identity	52.185.64.238:7810	Not configured
Office Online Web Apps - Excel Powerpoint Word	52.185.64.238:7810	Not configured
SharePoint for Business	52.185.64.238:7810	Not configured

☒ Enable Acceleration

Apply

Add Application-Based In-Path Rules

- Only applications configured in the SAM will be available.
- Ensure that this is above the default rules.
 - Port 443 is passed through by default.

▼ Add a New In-Path Rule ◀ Remove Selected Rules ▶ Move Selected Rules...

Type: Auto Discover

Enable Email Notification: ☐

Ignore Latency Detection: ☐

Source: { Subnet: All IPv4 }

Destination: { Subnet: SaaS Application 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: ☒

Add

☒ Exchange Online
Office 365 authentication and identity
Office Online Web Apps – Excel Powerpoint Word
SharePoint for Business

Application-Based In-Path Rules – Example

⊕ Add a New In-Path Rule ⊖ Remove Selected Rules ⇅ Move Selected Rules...

<input type="checkbox"/>	Rule	Type	Source	Destination	VLAN	Protocol	Preoptimization Policy	Latency Policy	Data Reduction Policy	Cloud Acceleration	Web Proxy	Kickoff	Rule Status	Email Notify	Ignore Latency Detection
<input type="checkbox"/>	1	Auto Discover	All-IPv4:*	SaaS Application SharePoint for Business <small>Port or Port Label: *</small>	All	--	None	Normal	Normal	SaaS	None	No	Enabled	n/a	✖
<input type="checkbox"/>	2	Auto Discover	All-IPv4:*	SaaS Application Office Online Web Apps - Excel Powerpoint Word <small>Port or Port Label: *</small>	All	--	None	Normal	Normal	SaaS	None	No	Enabled	n/a	✖
<input type="checkbox"/>	3	Auto Discover	All-IPv4:*	SaaS Application Office 365 authentication and identity <small>Port or Port Label: *</small>	All	--	None	Normal	Normal	SaaS	None	No	Enabled	n/a	✖
<input type="checkbox"/>	4	Auto Discover	All-IPv4:*	SaaS Application Exchange Online <small>Port or Port Label: *</small>	All	--	None	Normal	Normal	SaaS	None	No	Enabled	n/a	✖

FYI: CLI Commands on the Client-Side SteelHead

- SaaS Accelerator configuration can be done on the SteelHead CLI as well as GUI.
- CLI commands for reference:
 - `show service saas-accel`
 - `show service saas-accel applications`
 - `service saas-accel register scm <scm domain name> token <abcd>`
 - `service saas-accel enable`
 - `in-path rule auto-discover ddst-app <app-name>`
 - `no service saas-accel register`



Register SteelCentral Controller for Mobile (SCCM)

Copy SAM Details into SCCM

A. Obtain from SAM:

- a) it's URL,
- b) Port #,
- c) and Registration Token

B. Click Register

C. Screen should change to reflect registration

Configure > SaaS Accelerator ?

SteelConnect Registration

SteelConnect Manager Hostname or IP Address: scm-zak-test.0re0.de
SteelConnect Manager Port: 3900
Registration Token: *****neNk

De-register

SaaS Acceleration Status

Last SteelConnect Data Refresh: 2019/07/10 11:16:30 GMT (just now)

Refresh Data

Access List: Gray List

Configure SaaS Acceleration

☐ Enable Acceleration

Apply

As for when configuring a SteelHead, you will need the SAM hostname and IP address and the registration token from the SaaS Client Appliances page of the SAM.

On SAM –Whitelist SCCM (1/4 screenshots)

riverbed SteelConnect Manager sandbox2 1 message Help

SaaS Accelerator Client Appliances

Registration Token

Registration token 10O0B956EEE7D117E4BJ1YvYDqG8uRJEUJneNk Copy Regenerate

Appliances

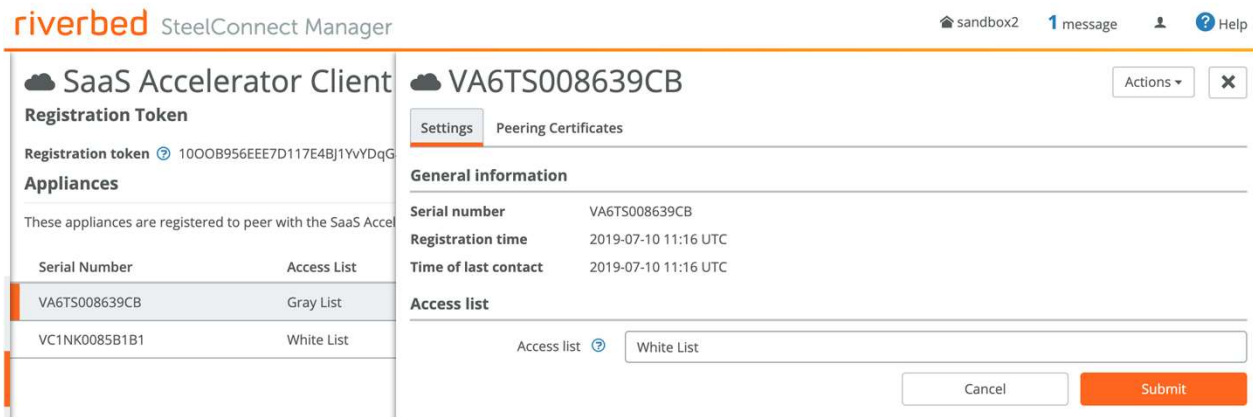
These appliances are registered to peer with the SaaS Accelerator.

Serial Number	Access List	Peering Certificates Status	Date of Last Contact	Hostname
VA6TS008639CB	Gray List	No certificates uploaded	2019-07-10 11:16 UTC	bredonsccm
VC1NK0085B1B1	White List		2019-06-20 18:02 UTC	SHCX99

© 2021 Riverbed Technology, Inc. All rights reserved. **riverbed** 45

Add the SCCM to the Whitelist on the SAM just as you would do for a SteelHead.

On SAM –Whitelist SCCM (2/4 screenshots)



riverbed SteelConnect Manager

sandbox2 1 message Help

SaaS Accelerator Client **VA6TS008639CB** Actions X

Registration Token

Registration token ⓘ 10O0B956EEE7D117E4BJ1YvYDqG

Appliances

These appliances are registered to peer with the SaaS Accelerator

Serial Number	Access List
VA6TS008639CB	Gray List
VC1NK0085B1B1	White List

Settings Peering Certificates

General information

Serial number VA6TS008639CB

Registration time 2019-07-10 11:16 UTC

Time of last contact 2019-07-10 11:16 UTC

Access list

Access list ⓘ White List

Cancel Submit

On SAM –Whitelist SCCM (3/4 screenshots)

Configure > SaaS Accelerator ?

SteelConnect Registration

SteelConnect Manager Hostname or IP Address: scm-zak-test.0re0.de
SteelConnect Manager Port: 3900
Registration Token: *****neNk

[De-register](#)

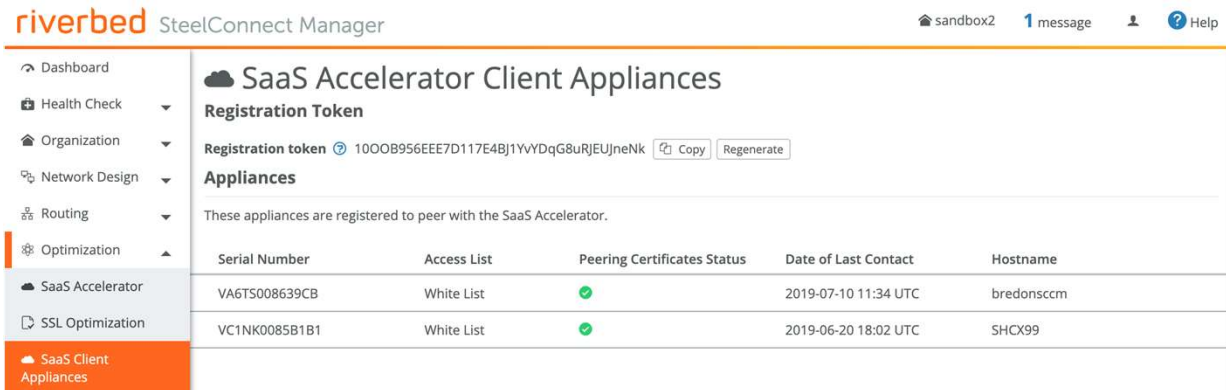
SaaS Acceleration Status

Last SteelConnect Data Refresh: 2019/07/10 11:30:46 GMT (just now) [Refresh Data](#)
Access List: White List

You will need to click the Refresh Data button to see the change.

On SAM –Whitelist SCCM (4/4 screenshots)

Step 2: Whitelist SCCM on SAM



The screenshot displays the 'SaaS Accelerator Client Appliances' page in the Riverbed SteelConnect Manager. The left sidebar shows the navigation menu with 'SaaS Client Appliances' selected. The main content area shows the 'Registration Token' and a table of registered appliances.

Registration Token

Registration token ⓘ 10O0B956EEE7D117E4BJ1YvYDqG8uRJEUjNeNk [Copy](#) [Regenerate](#)

Appliances

These appliances are registered to peer with the SaaS Accelerator.

Serial Number	Access List	Peering Certificates Status	Date of Last Contact	Hostname
VA6TS008639CB	White List	✓	2019-07-10 11:34 UTC	bredonsccm
VC1NK0085B1B1	White List	✓	2019-06-20 18:02 UTC	SHCX99

© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 48

Note the change in Peering Certificates Status once the SCCM is trusted.

On SCCM – Enable SaaS Acceleration

Configure > SaaS Accelerator ?

SteelConnect Registration

SteelConnect Manager Hostname or IP Address: scm-zak-test.0re0.de
SteelConnect Manager Port: 3900
Registration Token: *****neNk

De-register

SaaS Acceleration Status

Last SteelConnect Data Refresh: 2019/07/10 11:30:46 GMT (just now) Refresh Data
Access List: White List

Configure SaaS Acceleration

☒ Enable Acceleration
Apply

SaaS Applications:

Application	Service Endpoint	Policies using Application
Exchange Online	52.230.228.35:7810	Not Configured
Office O365 authentication and identity	52.230.228.35:7810	Not Configured
Office Online Web Apps - Excel Powerpoint Word	52.230.228.35:7810	Not Configured
SharePoint for Business	52.230.228.35:7810	Not Configured

You then need to Enable SaaS Acceleration on the Configure > SaaS Accelerator page. Click Apply.

On SCCM – Add Application-Based In-Path Rule

Manage > Policies [?](#)

[+ Create New Policy](#) [- Remove Selected Policies](#)

Policy	Last Modified Time	Description
Initial	2019/07/10 11:30:46	
zak_testing	2019/07/10 11:38:53	SaaS Accelerator Policy

[General Settings](#) [In-Path Rules](#) [Protocol Settings](#) [SSL](#) [SaaS Acceleration](#) [Location Awareness](#) [Endpoint Settings](#)

Optimization Rules:

[+ Add a New In-Path Rule](#) [- Remove Selected Rules](#) [Move Selected Rules...](#)

Type: [Auto Discover](#)

Position: [Start](#)

Source Subnet: [All-IPv4](#)

Destination Subnet or [Host Label](#) or App Label: [SaaS Application](#) [Office Online Web Apps - Excel Powerpoint Word](#)

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:

[Add](#)

© 2021 Riverbed Technology, Inc. All rights reserved. [riverbed](#) 50

You need to either create a new policy or amend an existing one. You need to perform the following:

- Configure in-path rules
- Enable SSL optimization
- Enable SaaS Acceleration at the policy level
- Ensure the policy is assigned to your mobile clients

On SCCM – Update Policy for SSL Optimization

zak_testing 2019/07/10 11:38:53 SaaS Accelerator Policy

General Settings In-Path Rules Protocol Settings **SSL** SaaS Acceleration Location Awareness Endpoint Settings

General SSL Settings

☒ Enable SSL Optimization

Client Authentication

☐ Enable Client Certificate Support

Proxies

☐ Enable SSL Proxy Support

SSL Secure Peering Settings

Traffic Type:

☒ Fallback to No Encryption

SSL Peering

☒ Trust All Pre-configured Peering Certificates

☐ Trust Selected Peering Certificates

Effective List of all the Peering Certificates:

Trusted Entity	Issued To	Expiration Date
SaaS-Opt_Peering_CA_4387182D525DC93A66E5842D43D8FFE1DB9F8CBD	BredonCA	Jul 10 11:05:34 2021 GMT

© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 51

You need to enable SSL Optimization and ensure that the peering certificate is trusted.

On SCCM – Configure Policy for SaaS Application

Manage > Policies ?

+ Create New Policy — Remove Selected Policies

Policy	Last Modified Time	Description
Initial	2019/07/10 11:30:46	
zak_testing	2019/07/10 11:42:23	SaaS Accelerator Policy

General Settings In-Path Rules Protocol Settings SSL SaaS Acceleration Location Awareness Endpoint Settings

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

Update Policy

On SCCM – Verify SaaS Policy are Listed

Configure > SaaS Accelerator [?](#)

SteelConnect Registration

SteelConnect Manager Hostname or IP Address: scm-zak-test.0re0.de
SteelConnect Manager Port: 3900
Registration Token: *****neNk

[De-register](#)

SaaS Acceleration Status

Last SteelConnect Data Refresh: 2019/07/10 11:44:10 GMT (just now) [Refresh Data](#)

Access List: White List

Configure SaaS Acceleration

☒ Enable Acceleration

[Apply](#)

SaaS Applications:

Application	Service Endpoint	Policies using Application
Exchange Online	52.230.228.35:7810	zak_testing
Office O365 authentication and identity	52.230.228.35:7810	zak_testing
Office Online Web Apps - Excel Powerpoint Word	52.230.228.35:7810	zak_testing
SharePoint for Business	52.230.228.35:7810	zak_testing

On SCCM - Assign Policy to Endpoint & Verify on Client

Group Assignments:

▼ Add Group Assignment — Remove Selected Assignments

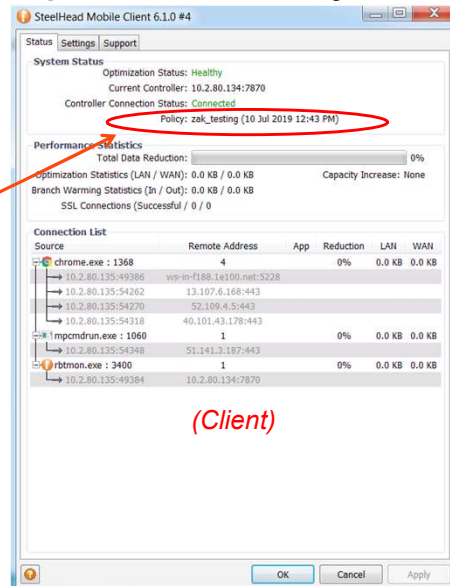
Group: Default

Package: Default (6.1.0 #4) ▾

Policy: **zak_testing** ▾

Add

(SCCM)

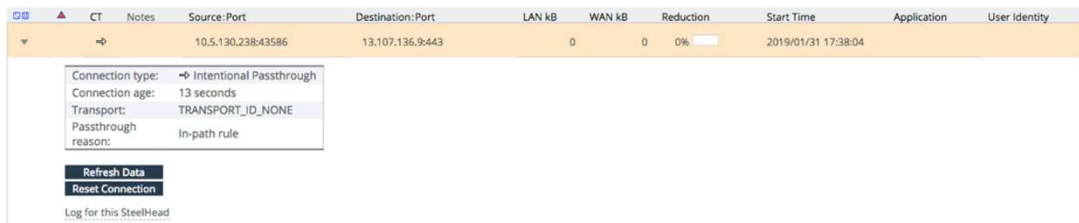


(Client)

You can do this via the Endpoint Report as well.

First Connection on Client-Side SteelHead

- Until the first connection is classified, traffic will not match the new rule.



CT	Notes	Source:Port	Destination:Port	LAN kB	WAN kB	Reduction	Start Time	Application	User Identity
▼	→	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

Refresh Data

Reset Connection

[Log for this SteelHead](#)

- Next, connections are optimized with SSL errors.
- Then, connections are accelerated successfully.

Automatic SSL Certification Generation

- You will initially see protocol errors, even after the traffic has been identified.
- The server-side SteelHead will auto-generate the CSRs for the necessary certificates, but this will take a few minutes to complete.

The screenshot displays the SteelHead SaaS Accelerator interface. At the top, a status bar shows the source IP 10.1.80.143:63609, destination IP 81.130.105.56:443, and connection statistics: 261 bytes, 285 packets, and 0% retransmission. Below this, the connection details are shown:

- Connection type: RIOS
- Connection age: 11 seconds
- Application: HTTP
- Transport: TRANSPORT_ID_SSL
- Transport error: Server is already in the Discovered (bypassed, not optimizable) table on server-side Steelhead
- Notes: In-path, SDR optimized, LZ compressed, Client side, WAN encrypted

Below the connection details, there are three buttons: Refresh Data, Send Keep-Alive, and Reset Connection. A link "Log for this SteelHead" is also present.

On the right side, the source and destination information is displayed:

- Source: 10.1.80.143:63609
- 10.1.80.100:7801
- SteelHead VCX 9.9.0a (YOU ARE HERE)
- 10.1.80.100:11963
- Transparency mode: Correct Addressing
- Congestion control: New Reno
- 52.185.64.238:7810
- SteelHead SaaS-Accelerator Service 1.0.0
- Destination: 81.130.105.56:443

At the bottom right, a table shows the LAN and WAN side statistics:

	LAN side	WAN side
Bytes	3,191,108	3,426,781
Packets	2,544	713
Retransmitted	6	0
Fast retransmitted	5	0
Timeouts	1	0
Congestion window	12	10

Successfully Optimized Connection

10.1.80.143:55836 52.97.145.178:443 105 10 90% 2019/06/20 17:48:25 MS-Office-365

Connection type: RIOS
Connection age: 6 seconds
Application: HTTP > MS-Office-365
Transport: TRANSPORT_ID_SSL
Notes: In-path
SDR optimized
LZ compressed
Client side
WAN encrypted

Refresh Data
Send Keep-Alive
Reset Connection
Log for this SteelHead

Source 10.1.80.143:55836

10.1.80.100:7801
SteelHead VCX 9.9.0a (YOU ARE HERE)
10.1.80.100:12114

Transparency mode: Correct Addressing
Congestion control: New Reno

52.185.64.238:7810
SteelHead SaaS-Accelerator Service 1.0.0

Destination 52.97.145.178:443

	LAN side	WAN side
Bytes	107,841	10,619
Packets	82	22
Retransmitted	0	0
Fast retransmitted	0	0
Timeouts	0	0
Congestion window	18	10

© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 57

Note the application and the SteelHead SaaS-Accelerator Service in the Server-Side SteelHead information.

Endpoint Report for Mobile Client

Reports > Endpoints > Endpoint Report ?

Endpoints

Settings

Filters

Endpoint Operations

Remove Selected Endpoints

User	Status	Controller	IP Address	Version	Group	Policy	Total Reduction	LAN Data	WAN Data	Warmed Data	Connected At
dave-PC\dave	Healthy	10.2.80.134	10.2.80.135	6.1.0 #4	Default	zak_testing	15.84%	1008.4 MB	838.6 MB	0 B	2019/07/10 15:18:07
<div>General InformationStats SummaryCurrent ConnectionsAdaptersAssignmentsDiagnostics</div>											
Connections:											
Type	Process	Source:Port	Dest:Port	Reduction	LAN Data	WAN Data	Warmed Data	Application	Notes		
	outlook.exe : 2368	10.2.80.135:59901	52.97.164.178:443	19.07%	66.3 KB	53.7 KB	0 B	HTTP			
	outlook.exe : 2368	10.2.80.135:59910	52.97.164.178:443	28.14%	32.7 KB	23.5 KB	0 B	HTTP			
	outlook.exe : 2368	10.2.80.135:59923	52.97.164.178:443	0%	2.3 KB	4.5 KB	0 B	HTTP			
Connection Information											
Connected Since:		2019/07/10 15:19:20									
Peer Appliance:		52.230.228.35:7810 (Server Side)									
WAN Visibility Mode:		Correct Addressing									
WAN Congestion Control:		Windows									

The client has Outlook open, connecting to Exchange Online. You can see the application (HTTP) and when you expand the connection you can see the server-side SteelHead and port being used.



Notifications - SAM

riverbed SteelConnect Manager

🏠 sandbox2 1 message ⓘ Help

- Dashboard
- Health Check
- Organization
- Network Design
- Routing
- Optimization
- SaaS Accelerator**
- SSL Optimization
- SaaS Client Appliances
- SaaS Connection Count
- SaaS Data Usage
- SaaS Traffic Summary

SaaS Accelerator

⚡ Accelerate Application

The SaaS Accelerator license will expire in 7 days . Contact [Riverbed](#) to renew your license and benefit from uninterrupted SaaS application acceleration.

SaaS Application	Number of Users	Service Endpoint	Service Status
📌 Microsoft Office 365	200	52.158.212.172:7810 Copy	🟢

AppUnits Usage

SaaS Accelerator

[Accelerate Application](#)[AppUnits usage](#)

The SaaS Accelerator license will expire in 7 days . Contact [Riverbed](#) to renew your license and benefit from uninterrupted SaaS application acceleration.

SaaS Application	Number of Users	Service Endpoint	Service Status
 Box	400	52.230.224.144:7810 View Copy	
AppUnits Usage			
 Microsoft Office			

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 4000
Available AppUnits 4000

SaaS Application	AppUnits Assigned	Number of Users	Number of SSL/TLS Connections
Box	2000	400	2000
Microsoft Office 365	2000	200	2000

SSL/TLS Connection Count

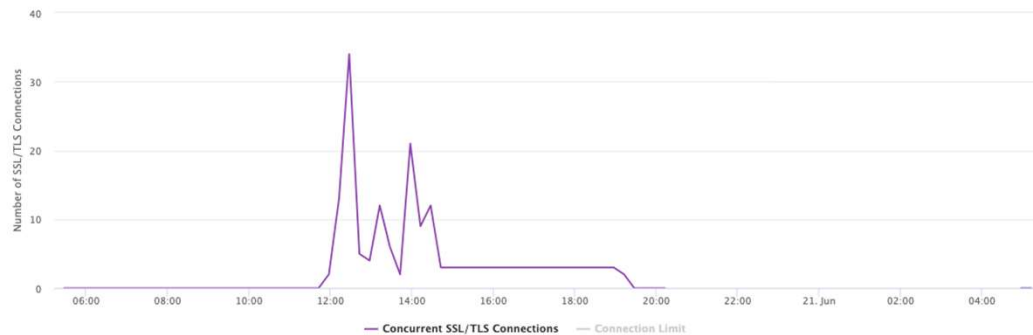
SaaS Accelerator Connection Count

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

Period



© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 62

Period options: Last hour, day, week, 30 days, 60 days, 90 days and year.

Egress Data Usage

SaaS Accelerator Cumulative Egress Data Usage

Total Data Usage

Data Usage Trend

This report shows the amount of egress data used since the SaaS Accelerator feature was licensed on Sep 30, 2018.

SaaS Application	Egress Data Used
Microsoft Office 365	419.02 MiB
Box	0 bytes
Salesforce	1.85 MiB
Veeva	0 bytes
Total data used	420.87 MiB

Egress Data Usage Trend

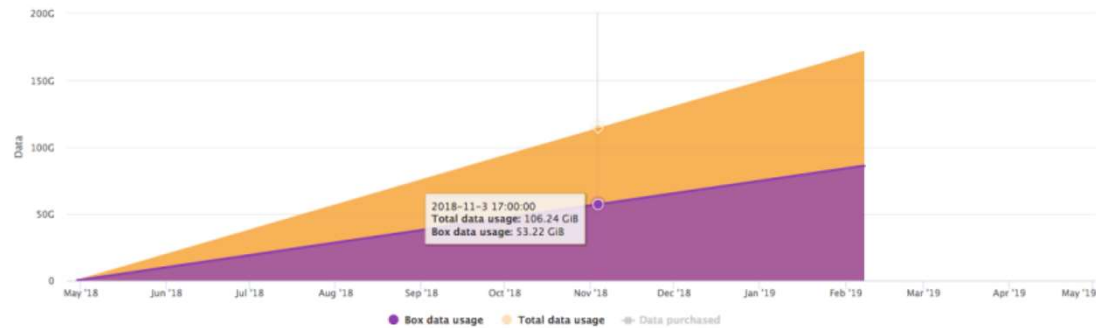
SaaS Accelerator Cumulative Egress Data Usage

Total Data Usage **Data Usage Trend**

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



© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 64

SaaS Traffic Summary

SaaS Traffic Summary

Total Data Reduction

The total data reduction provided by the SaaS Accelerator since it was configured on Mar 9, 2019.

935.74 MiB (69.56%)

Data reduction

Period

SaaS Application	Data Reduction	LAN Data ⓘ	WAN Data ⓘ
Microsoft Office 365	46.02%	34.35 MiB	18.54 MiB
Salesforce	5.41%	1.89 MiB	1.79 MiB
Veeva	0.00%	0 bytes	0 bytes
Total Data Reduction	43.90%	36.24 MiB	20.33 MiB

Putting it all Together - Real World Use Case

Scenario	The customer is a large multinational food company based in Europe, but with offices worldwide, including Australia. Lotus Notes was used for mail with regional datacenters hosting mail servers in each region. They were moving away from Lotus Notes and migrating to Office 365.
Issue	Due to the way Office 365 works, the data is hosted close to the HQ of the subscribing company, i.e., Europe. This resulted in users in APAC now having 300ms of latency and applications were now running much too slowly. Email and SharePoint were now almost unusable for half the company.
Solution	By purchasing SteelHead SaaS Accelerator, they were able to benefit from WAN acceleration for their Office 365 traffic, reducing the access time for applications such as Email and SharePoint by around 30 times in certain locations. This resulted in far less time being wasted by users watching a magnifying glass on their screen, increasing productivity as well as making employees much happier as they could now access their applications.

© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed 66

As an example of this, Riverbed recently worked with a large food company with headquarters in Europe but with offices worldwide, including Australia. This company had just a few regional datacenters around the world, including Hong Kong, South Africa, the UK and the US.

However, when they moved to Office 365, this caused a real problem as their data was now stored in one of Microsoft's European datacenters, meaning users in Australia now had 300-400ms of latency and applications were now running much too slowly. Email and SharePoint were now almost unusable for half the company.

By purchasing SaaS Accelerator, they were able to benefit from WAN acceleration for their Office 365 traffic, reducing the access time for applications such as Email and SharePoint by around 30 times in certain locations.

This resulted in far less time being wasted by users watching a magnifying glass on their screen, increasing productivity as well as making employees much happier as they could now access their applications.

SaaS Accelerator – Video: Optimization of SaaS Applications

In this video, you will view:

- Walk-through configuration of SaaS Accelerator Manager and client-side SteelHead

Duration: **30 minutes**

Demo/Video



*eLab system: link and access details
provided in your course confirmation email*

Module Review

You should now be able to:

- Describe the Legacy SaaS Accelerator.
- Describe the SaaS Accelerator Service.
- License the SaaS Accelerator.
- Deploy client-side SteelHeads with SaaS Acceleration.
- Deploy SaaS for SteelHead Mobile.
- Verify and troubleshoot SaaS acceleration.

© 2021 Riverbed Technology, Inc. All rights reserved.

riverbed
The Digital Performance Company