Deploy the SteelCentral Controller for SteelHead

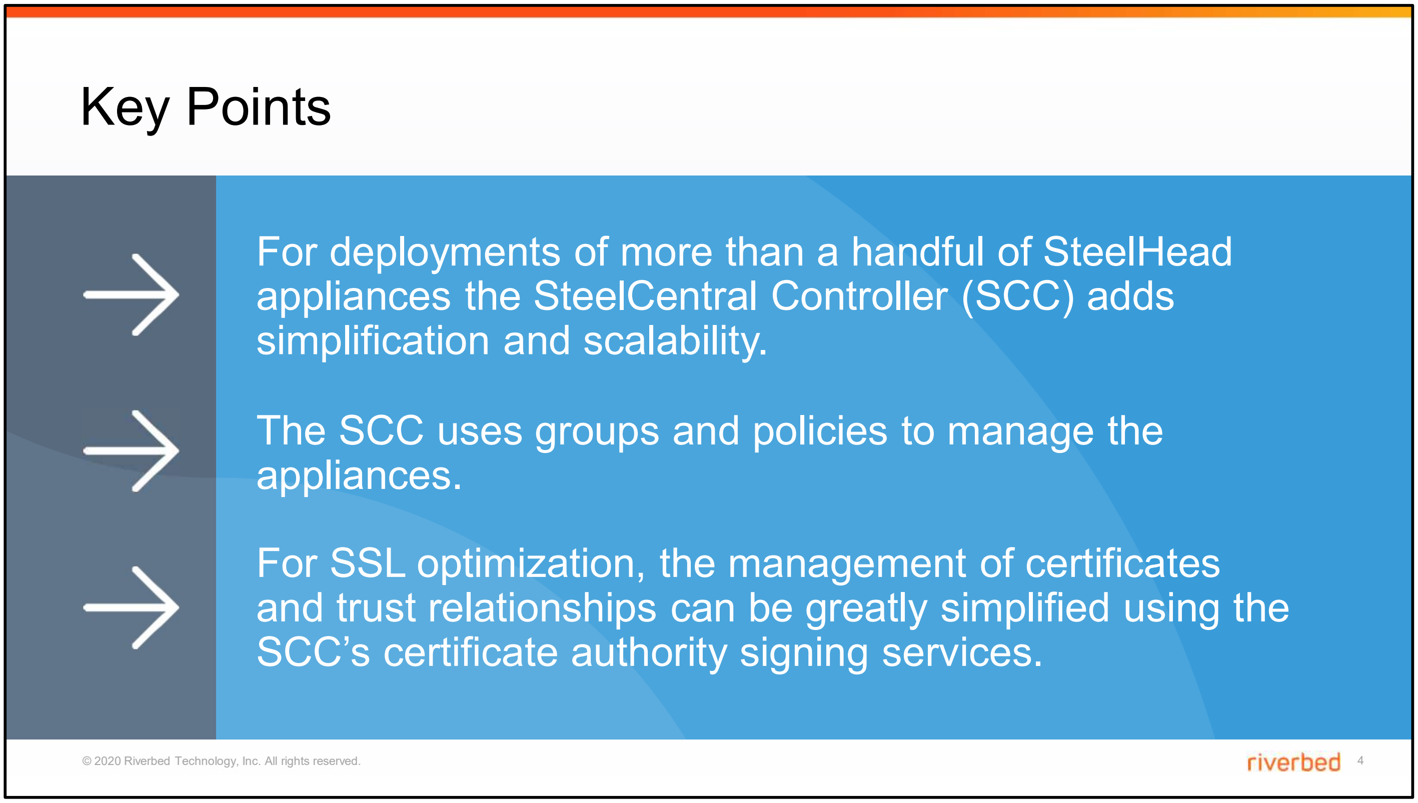
Learning Objectives

After completing this module, you will be able to:

- Describe the SteelCentral Controller for SteelHead (SCC).
- Setup and operate the SCC.
- Manage your configurations with the SCC.
- Manage your software with the SCC.

riverbed
The Digital Performance Company

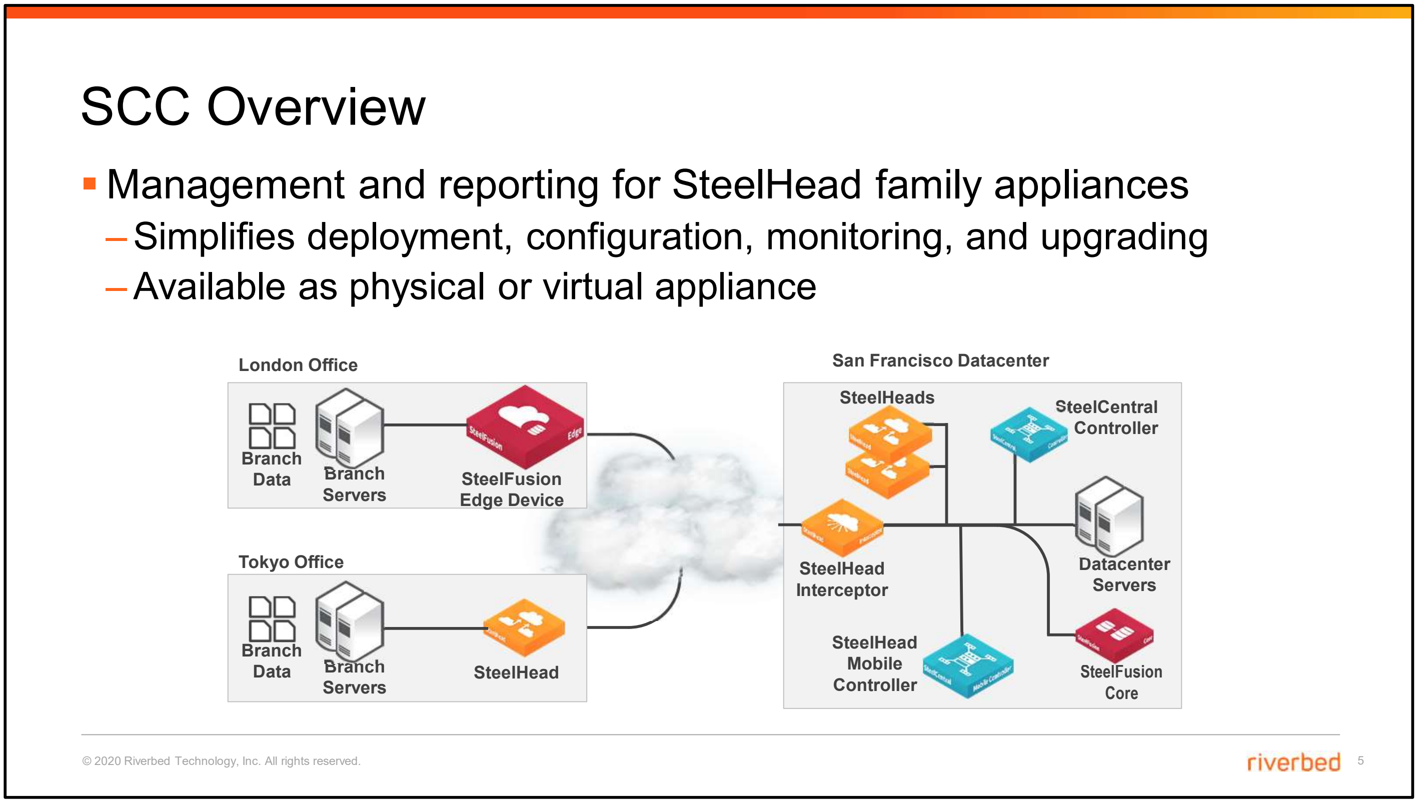
Describe the SteelCentral® Controller for SteelHead (SCC)



Key Points

- For deployments of more than a handful of SteelHead appliances the SteelCentral Controller (SCC) adds simplification and scalability.
- The SCC uses groups and policies to manage the appliances.
- For SSL optimization, the management of certificates and trust relationships can be greatly simplified using the SCC's certificate authority signing services.

The SCC's Certificate Authority capability greatly simplifies SteelHead peering trusts, and can generate proxy certificates for bypassed servers.



SCC Overview

- Management and reporting for SteelHead family appliances
  - Simplifies deployment, configuration, monitoring, and upgrading
  - Available as physical or virtual appliance

riverbed 5

Configuration: The SteelCentral Controller (SCC) enables you to automatically configure new appliances or to send configuration settings to appliances in remote offices. The SCC utilizes configuration objects (policies and groups) to facilitate centralized configuration and reporting.

Monitoring: The SCC provides both high-level status and detailed statistics of the performance of appliances and enables you to configure event notification for managed appliances.

Management: The SCC enables you to start, stop, restart, and reboot remote appliances. You can also schedule jobs to send software upgrades and configuration changes to remote appliances or to collect logs from remote appliances.

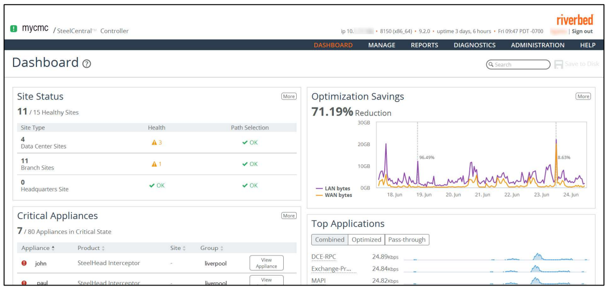
Partial Federation: You can put any appliance into branch-managed mode to prevent configuration changes or maintenance operations from the SCC. The SCC continues to monitor and gather statistics from appliances that are branch managed.

Operations History: The Operations History page lists all of the actions related to configuring SteelHead appliances that have been performed and tells you if they were successful or not.

SCC Highlights

Overview

- Configures SteelHeads & Interceptors
- Status info for SteelHead Mobile Controllers and SteelFusion devices
- Monitoring: both high-level status and detailed statistics
- Maintenance: image updates, restarts, reboots, & more
- Troubleshooting: centralized system & TCP dumps



ip 10.[redacted] • 8150 (x86_64) • 9.2.0 • uptime 3 days, 6 hours • Fri 09:47 PDT -0700 [redacted] | Sign out

Dashboard

Site Status

11 / 15 Healthy Sites

Site Type	Health	Path Selection
4 Data Center Sites	⚠ 3	✓ OK
11 Branch Sites	⚠ 1	✓ OK
0 Headquarters Site	✓ OK	✓ OK

Optimization Savings

71.19% Reduction

Critical Appliances

7 / 80 Appliances in Critical State

	Appliance	Product	Site	Group	
!	john	SteelHead Interceptor	-	liverpool	View Appliance
!	paul	SteelHead Interceptor	-	liverpool	View

Top Applications

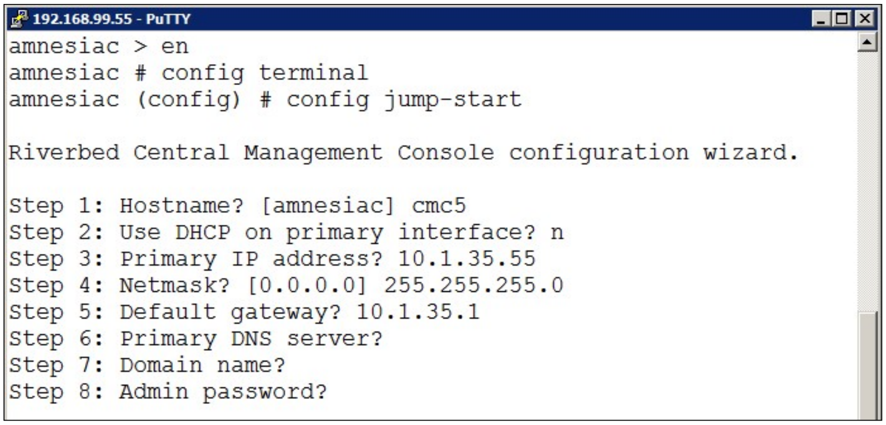
DCE-RPC	24.89Kbps
Exchange-Pr...	24.84Kbps
MAPI	24.82Kbps

- Operation History
- SteelHead firmware library for centralized updates
- Import existing SteelHead configurations
- CLI command broadcasting
- Touchless SteelHead configuration
- Secure appliance communications
  - HTTPS access to CMC
  - SH to CMC communications over SSH
  - Radius / TACACS+ authentication

Setup and Operate the SCC

SCC Startup & Operations (Op’s) – Jumpstart Wizard

- Wizard from the console for initial Primary interface configuration

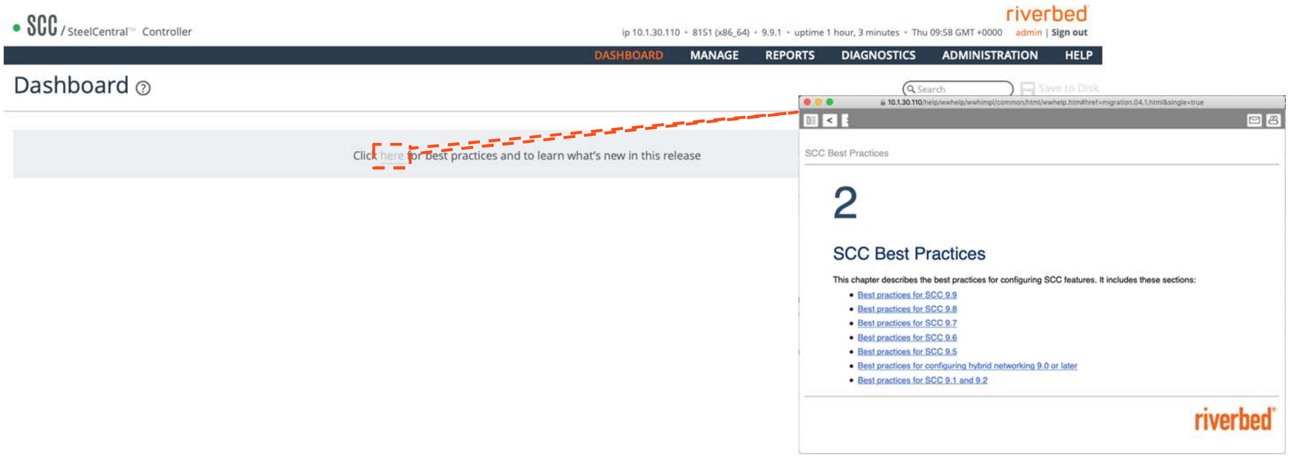


```
amnesiac > en
amnesiac # config terminal
amnesiac (config) # config jump-start

Riverbed Central Management Console configuration wizard.

Step 1: Hostname? [amnesiac] cmc5
Step 2: Use DHCP on primary interface? n
Step 3: Primary IP address? 10.1.35.55
Step 4: Netmask? [0.0.0.0] 255.255.255.0
Step 5: Default gateway? 10.1.35.1
Step 6: Primary DNS server?
Step 7: Domain name?
Step 8: Admin password?
```

SCC Startup & Op’s – SCC Best Practices/RIs Notes


SCC / SteelCentral Controller
riverbed
ip 10.1.30.110 • 8151 (x86_64) • 9.9.1 • uptime 1 hour, 3 minutes • Thu 09:58 GMT +0000
admin | Sign out
DASHBOARD
MANAGE
REPORTS
DIAGNOSTICS
ADMINISTRATION
HELP
Dashboard
Search
Save to Disk
10.1.30.110/help/wwhelp/wwhimpl/common/html/wwhelp.htm#href=migration.04.1.html&single=true

Click here for best practices and to learn what’s new in this release

SCC Best Practices

2

SCC Best Practices

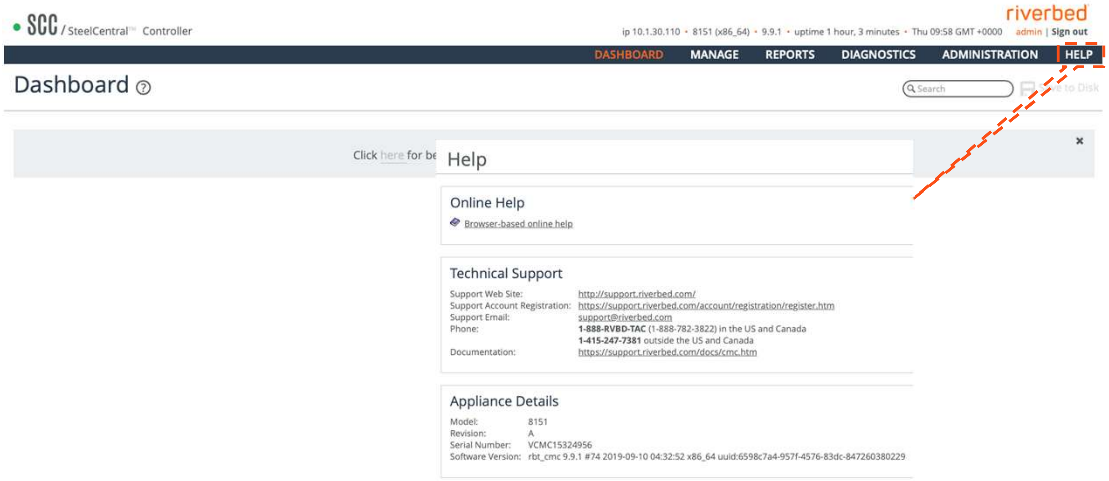
This chapter describes the best practices for configuring SCC features. It includes these sections:

- Best practices for SCC 9.9
- Best practices for SCC 9.8
- Best practices for SCC 9.7
- Best practices for SCC 9.6
- Best practices for SCC 9.5
- Best practices for configuring hybrid networking 9.0 or later
- Best practices for SCC 9.1 and 9.2

Welcome Widget - Click Learn More to view migration best practices for 9.0 and later, including how to set up sites, applications, path selection, QoS, and pushing configurations. Click the X to hide the widget.

SCC Startup & Op's – Help Menu

Documentation and Help



Help

Online Help

Browser-based online help

Technical Support

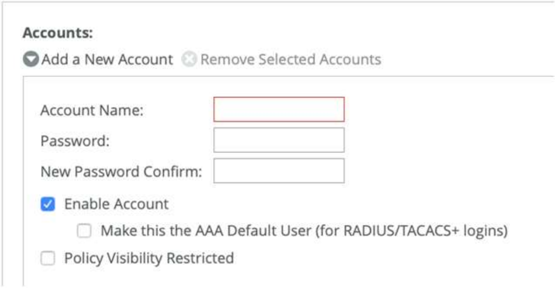
Support Web Site:	http://support.riverbed.com/
Support Account Registration:	https://support.riverbed.com/account/registration/register.htm
Support Email:	support@riverbed.com
Phone:	**1-888-RVBD-TAC** (1-888-782-3822) in the US and Canada **1-415-247-7381** outside the US and Canada
Documentation:	https://support.riverbed.com/docs/cmc.htm

Appliance Details

Model:	8151
Revision:	A
Serial Number:	VCMC15324956
Software Version:	rbt_cmc 9.9.1 #74 2019-09-10 04:32:52 x86_64 uuid:6598c7a4-957f-4576-83dc-847260380229

SCC Startup & Op's – Role Based Administration (RBA)

- Administration > Security > User Permissions
- Allows specific privilege levels
- Supported authentication integration methods:
  - Local (on SCC, the default)
  - RADIUS
  - TACACS
  - SAML



Accounts:

Add a New Account | Remove Selected Accounts

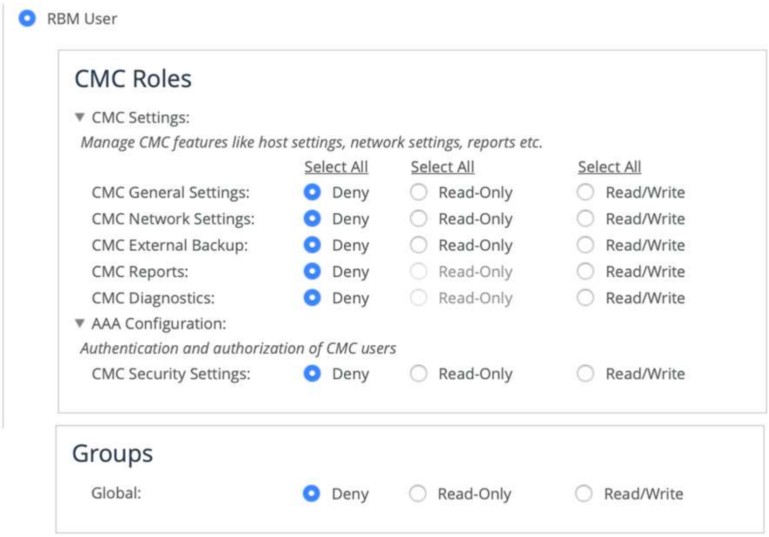
Account Name:	
Password:	
New Password Confirm:	

☑ Enable Account

□ Make this the AAA Default User (for RADIUS/TACACS+ logins)

□ Policy Visibility Restricted

SCC Startup & Op’s – RBA & SCC Settings



● RBM User

CMC Roles

▼ CMC Settings:

Manage CMC features like host settings, network settings, reports etc.

	Select All	Select All	Select All
CMC General Settings:	● Deny	○ Read-Only	○ Read/Write
CMC Network Settings:	● Deny	○ Read-Only	○ Read/Write
CMC External Backup:	● Deny	○ Read-Only	○ Read/Write
CMC Reports:	● Deny	○ Read-Only	○ Read/Write
CMC Diagnostics:	● Deny	○ Read-Only	○ Read/Write

▼ AAA Configuration:

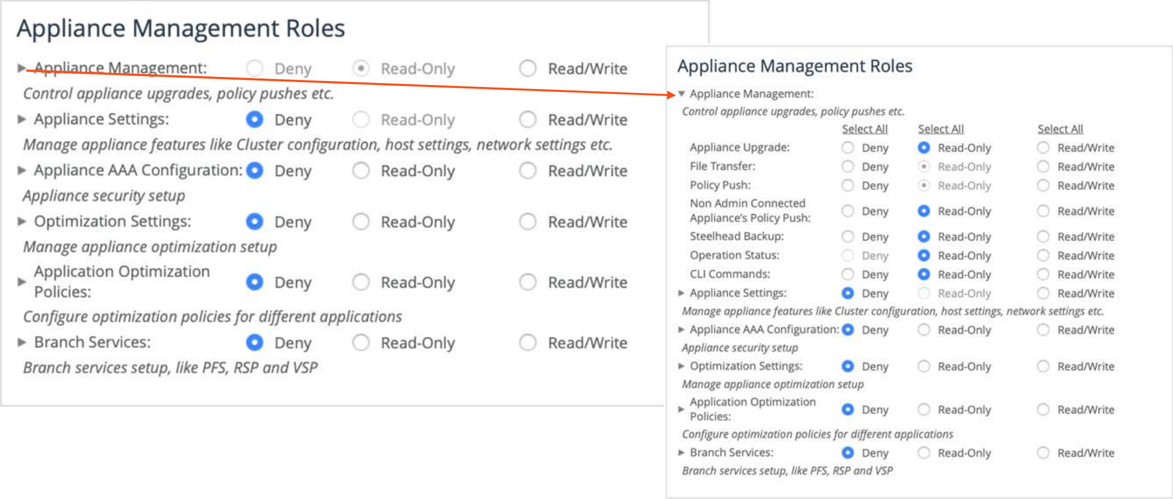
Authentication and authorization of CMC users

CMC Security Settings:	● Deny	○ Read-Only	○ Read/Write

Groups

Global:	● Deny	○ Read-Only	○ Read/Write

SCC Startup & Op’s – RBA & Appliance Settings

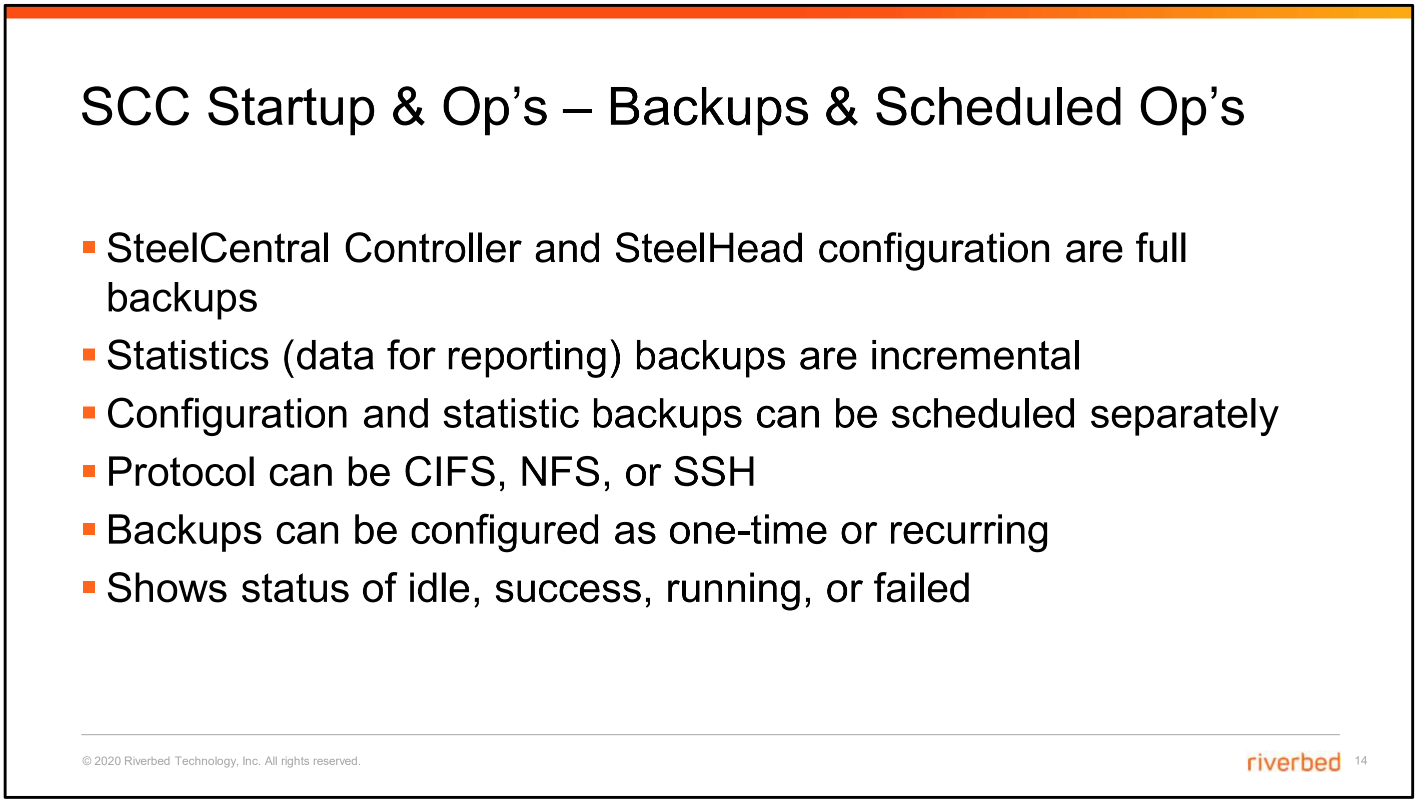


Appliance Management Roles

▸ Appliance Management:	○ Deny	● Read-Only	○ Read/Write
Control appliance upgrades, policy pushes etc.			
▸ Appliance Settings:	● Deny	○ Read-Only	○ Read/Write
Manage appliance features like Cluster configuration, host settings, network settings etc.			
▸ Appliance AAA Configuration:	● Deny	○ Read-Only	○ Read/Write
Appliance security setup			
▸ Optimization Settings:	● Deny	○ Read-Only	○ Read/Write
Manage appliance optimization setup			
▸ Application Optimization Policies:	● Deny	○ Read-Only	○ Read/Write
Configure optimization policies for different applications			
▸ Branch Services:	● Deny	○ Read-Only	○ Read/Write
Branch services setup, like PFS, RSP and VSP			

Appliance Management Roles

▾ Appliance Management:			
Control appliance upgrades, policy pushes etc.			
	Select All	Select All	Select All
Appliance Upgrade:	○ Deny	● Read-Only	○ Read/Write
File Transfer:	○ Deny	● Read-Only	○ Read/Write
Policy Push:	○ Deny	● Read-Only	○ Read/Write
Non Admin Connected Appliance's Policy Push:	○ Deny	● Read-Only	○ Read/Write
Steelhead Backup:	○ Deny	● Read-Only	○ Read/Write
Operation Status:	○ Deny	● Read-Only	○ Read/Write
CLI Commands:	○ Deny	● Read-Only	○ Read/Write
▸ Appliance Settings:	● Deny	○ Read-Only	○ Read/Write
Manage appliance features like Cluster configuration, host settings, network settings etc.			
▸ Appliance AAA Configuration:	● Deny	○ Read-Only	○ Read/Write
Appliance security setup			
▸ Optimization Settings:	● Deny	○ Read-Only	○ Read/Write
Manage appliance optimization setup			
▸ Application Optimization Policies:	● Deny	○ Read-Only	○ Read/Write
Configure optimization policies for different applications			
▸ Branch Services:	● Deny	○ Read-Only	○ Read/Write
Branch services setup, like PFS, RSP and VSP			



SCC Startup & Op’s – Backups & Scheduled Op’s

- SteelCentral Controller and SteelHead configuration are full backups
- Statistics (data for reporting) backups are incremental
- Configuration and statistic backups can be scheduled separately
- Protocol can be CIFS, NFS, or SSH
- Backups can be configured as one-time or recurring
- Shows status of idle, success, running, or failed

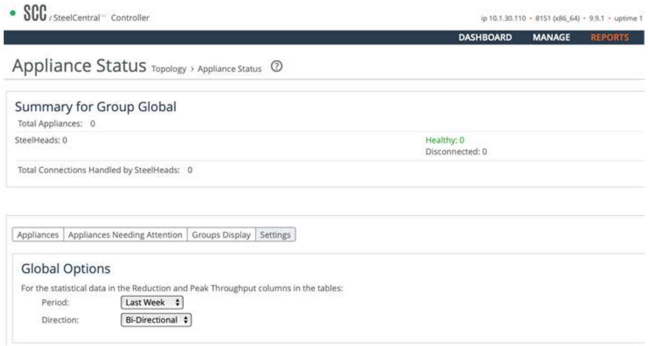
For SteelCentral Controller - typically, you do not need to use backups. Riverbed recommends that you restore an appliance to health by resending its configuration policies.

Backup/Restore Enhancement
The SteelCentral Controller now makes a distinction between the SteelCentral Controller's own configuration and nightly appliance backups (now called Appliance Configuration Snapshots) when backing up to or restoring from an external location. Additionally, nightly backups are only copied incrementally if SteelCentral Controller external appliance backups have a recurrence defined.

A status of idle indicates that there is no backup or restore history. The system does not retain a record of backup and restore statuses from prior to system startup (including reboots).

SCC Startup & Op's – SCC Dashboard

- Contains an overview of the current status
- Customizable per user, (Under Reports >Topology > Appliance Status > Settings)


SCC / SteelCentral™ Controller
ip 10.1.30.110 • 8151 (x86_64) • 9.9.1 • uptime 1
DASHBOARD
MANAGE
REPORTS
Appliances
Appliances Needing Attention
Groups Display
Settings

Appliance Status Topology › Appliance Status

Summary for Group Global

Total Appliances: 0

SteelHeads: 0 Healthy: 0 Disconnected: 0

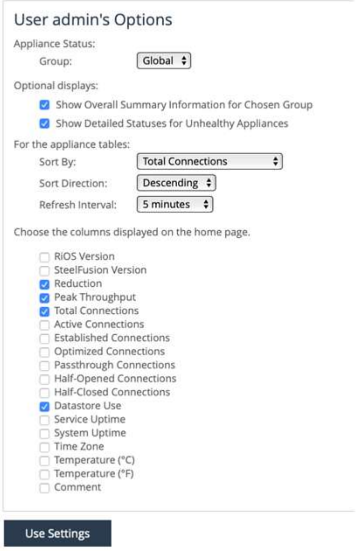
Total Connections Handled by SteelHeads: 0

Global Options

For the statistical data in the Reduction and Peak Throughput columns in the tables:

Period: Last Week

Direction: Bi-Directional



User admin's Options

Appliance Status:

Group: Global

Optional displays:

☑ Show Overall Summary Information for Chosen Group
☑ Show Detailed Statuses for Unhealthy Appliances

For the appliance tables:

Sort By: Total Connections

Sort Direction: Descending

Refresh Interval: 5 minutes

Choose the columns displayed on the home page.

☐ RiOS Version
☐ SteelFusion Version
☑ Reduction
☑ Peak Throughput
☑ Total Connections
☐ Active Connections
☐ Established Connections
☐ Optimized Connections
☐ Passthrough Connections
☐ Half-Opened Connections
☐ Half-Closed Connections
☑ Datastore Use
☐ Service Uptime
☐ System Uptime
☐ Time Zone
☐ Temperature (°C)
☐ Temperature (°F)
☐ Comment

After you connect to the SCC Management Console, the Dashboard appears. The Dashboard provides a general overview regarding the status of your SCC, including site status, the status of configured appliances, and optimization savings.

Site Status - Displays the health status of sites by site type; for example branch office or data center and its location. In addition, it lists the path selection status for each site.

Optimized Savings - Summarizes the overall inbound and outbound bandwidth improvements for your network at specified time intervals.

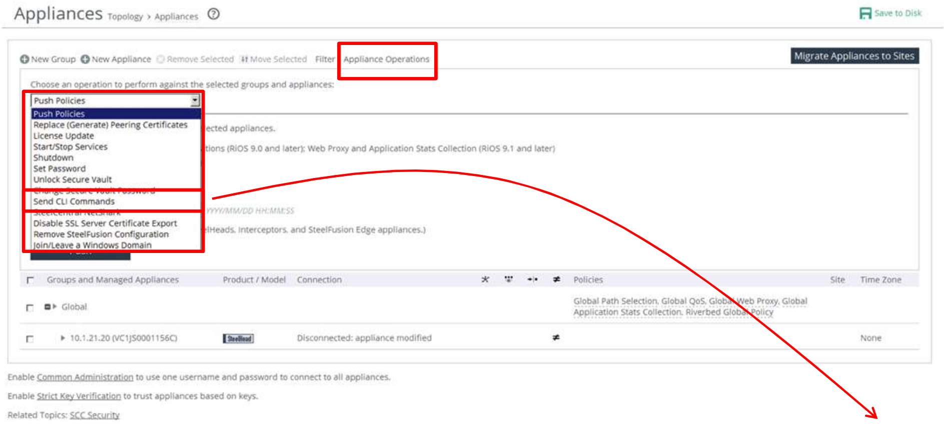
Top Applications - Top Applications on the Dashboard provide you with a summary of bandwidth reduction across applications for optimized, pass-through, and combined (optimized and pass through) traffic for the top ten applications in the network. Application statistics help you make optimization policy decisions and allocate resources appropriately. Top Applications provides historical data for up to one week for the entire network.

Byte counts - Refers to Layer 3 packet size (that is, the IP header plus the payload) without the potential tunnel overhead or higher layer retransmissions. Mouse over the data for each application to view the WAN throughput. Click the application name to go to the Applications Details page where you can view throughput data.

Critical Appliances - Provides a table of configured appliances that are currently in a Critical state. The table lists the appliance name, Riverbed appliance type (for example SteelHead or SteelHead EX), the hardware model, software version, site, and group. To view appliance details, click View Appliance. To connect to the appliance, click Console.

Appliance Administration

Perform actions on appliances / groups of appliances



Appliances Topology › Appliances ⓘ

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

Push Policies

- Push Policies
- Replace (Generate) Peering Certificates
- License Update
- Start/Stop Services
- Shutdown
- Set Password
- Unlock Secure Vault
- Change Secure Vault Password
- Send CLI Commands
- SteelCentral NetShark
- Disable SSL Server Certificate Export
- Remove SteelFusion Configuration
- Join/Leave a Windows Domain

...ected appliances.

...tions (RiOS 9.0 and later): Web Proxy and Application Stats Collection (RiOS 9.1 and later)

YYYY/MM/DD HH:MM:SS

...lHeads, Interceptors, and SteelFusion Edge appliances.)

☐	Groups and Managed Appliances	Product / Model	Connection	✲	⁂	⇥	≠	Policies	Site	Time Zone
☐	▸ Global							Global Path Selection, Global QoS, Global Web Proxy, Global Application Stats Collection, Riverbed Global Policy		
☐	▸ 10.1.21.20 (VC1JS0001156C)	SteelHead	Disconnected: appliance modified				≠			None

Enable Common Administration to use one username and password to connect to all appliances.

Enable Strict Key Verification to trust appliances based on keys.

Related Topics: SCC Security

Next slide…

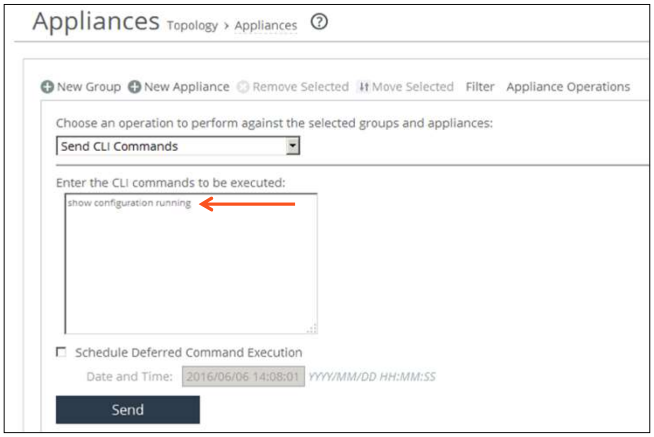
© 2020 Riverbed Technology, Inc. All rights reserved.

riverbed 16

You can perform different appliance operations in the **Manage > Appliances page - Appliance Operations** tab.

Appliance Administration – CLI Broadcasting

- Quickly send CLI commands to a group of SteelHead appliances
- Send immediately or schedule for later
- Assumes a “conf t” mode



Choose an operation to perform against the selected groups and appliances: Send CLI Commands

Enter the CLI commands to be executed:

show configuration running

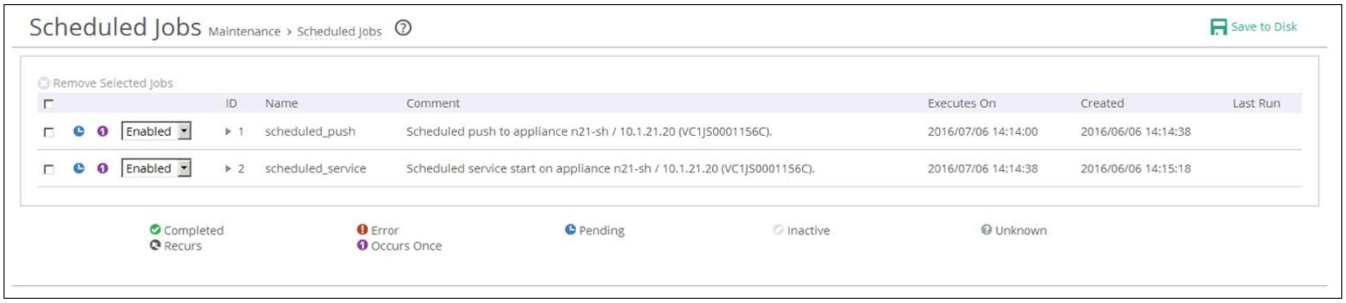
□ Schedule Deferred Command Execution

Date and Time: 2016/06/06 14:08:01 YYYY/MM/DD HH:MM:SS

You can send CLI commands to selected appliances and appliance groups in the **Manage > Topology > Appliances** page.

Scheduled Jobs

- Ability to schedule any configuration push
- Scheduler built into software upgrade mechanism
- Job Management interface for job status



□			ID	Name	Comment	Executes On	Created	Last Run
□	◔ ❶	Enabled ▾	▸ 1	scheduled_push	Scheduled push to appliance n21-sh / 10.1.21.20 (VC1JS0001156C).	2016/07/06 14:14:00	2016/06/06 14:14:38	
□	◔ ❶	Enabled ▾	▸ 2	scheduled_service	Scheduled service start on appliance n21-sh / 10.1.21.20 (VC1JS0001156C).	2016/07/06 14:14:38	2016/06/06 14:15:18	

riverbed 18

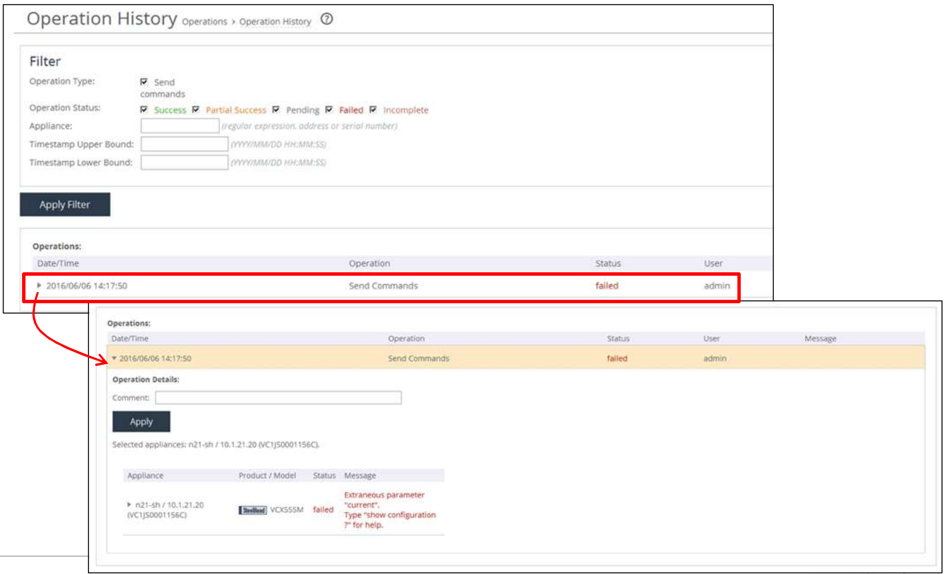
You can view completed, pending and inactive jobs, as well as jobs that were not completed because of an error in the **Administration > Maintenance > Scheduled Jobs** page.

Jobs are CLI commands that execute at a time you specify.

The only jobs you can schedule using the SteelCentral Controller GUI are software upgrades and configuration pushes; for all other jobs, you must use the CLI.

Operation History

- View operations applied to SteelHead appliances and groups
- Search filter by date/time, event, or type



Operation History Operations › Operation History

Filter

Operation Type: ☑ Send commands

Operation Status: ☑ Success ☑ Partial Success ☑ Pending ☑ Failed ☑ Incomplete

Appliance: (regular expression, address or serial number)

Timestamp Upper Bound: (YYYY/MM/DD HH:MM:SS)

Timestamp Lower Bound: (YYYY/MM/DD HH:MM:SS)

Apply Filter

Operations:

Date/Time	Operation	Status	User
▸ 2016/06/06 14:17:50	Send Commands	failed	admin

Operations:

Date/Time	Operation	Status	User	Message
▾ 2016/06/06 14:17:50	Send Commands	failed	admin	

Operation Details:

Comment:

Apply

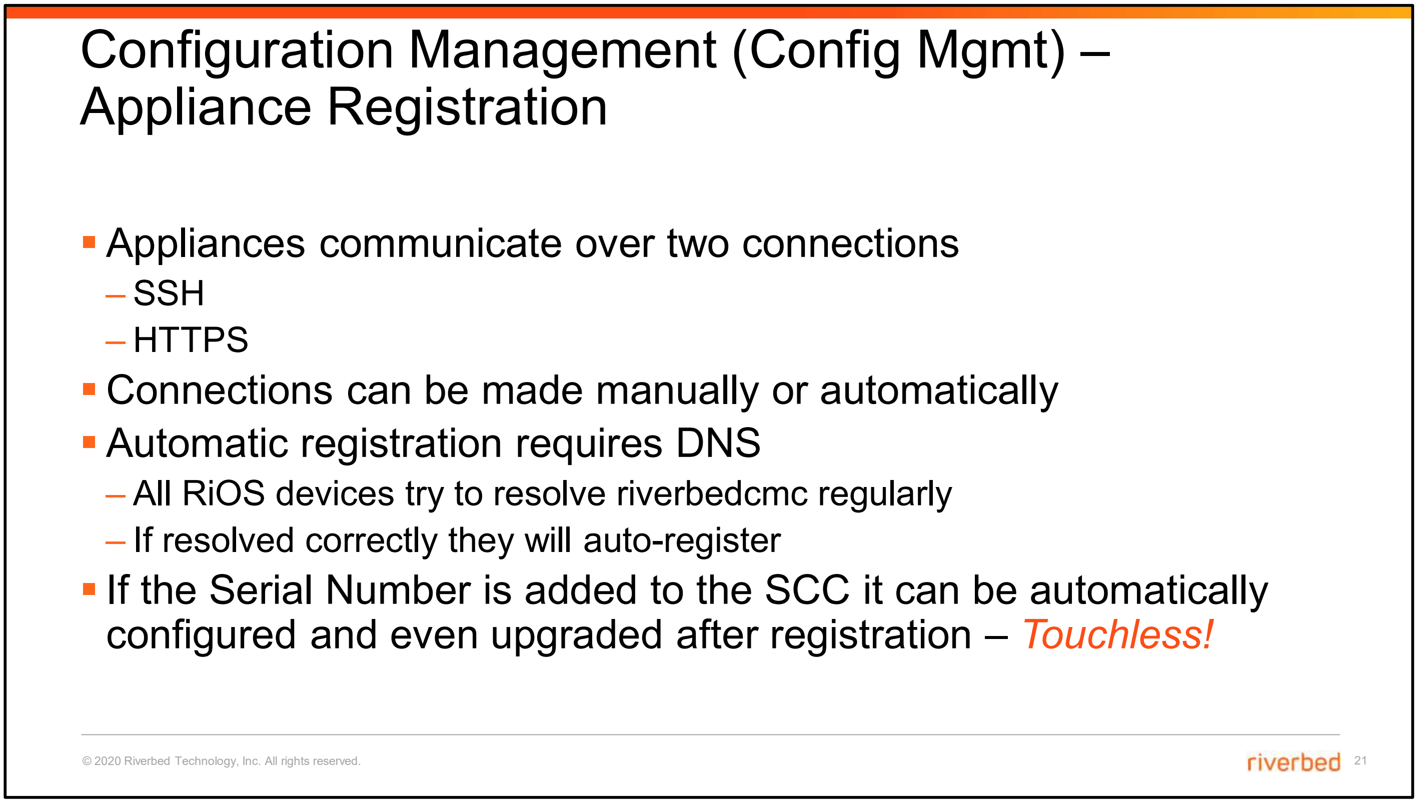
Selected appliances: n21-sh / 10.1.21.20 (VC1JS0001156C).

Appliance	Product / Model	Status	Message
▸ n21-sh / 10.1.21.20 (VC1JS0001156C)	SteelHead VCX555M	failed	Extraneous parameter "current". Type "show configuration ?" for help.

You can view the operation history for the system, including the ID, time stamp, type, and the status of the operation in the **Manage > Operation History** page. You can open each operation in the history to view operation details, including the serial number of the appliance, current status of the operation for the appliance, and messages associated with the operation. For more information, see the *SteelHead Management Console User's Guide*.

Users can view the operation history of only those appliances and appliance groups for which they have permission.

Manage Your Configuration with the SCC



Configuration Management (Config Mgmt) – Appliance Registration

- Appliances communicate over two connections
  - SSH
  - HTTPS
- Connections can be made manually or automatically
- Automatic registration requires DNS
  - All RiOS devices try to resolve riverbedcmc regularly
  - If resolved correctly they will auto-register
- If the Serial Number is added to the SCC it can be automatically configured and even upgraded after registration – *Touchless!*

riverbed 21

You can manage remote appliances in the Appliances page. SteelHeads must be registered with the SCC so that you can monitor and manage them with the SCC.

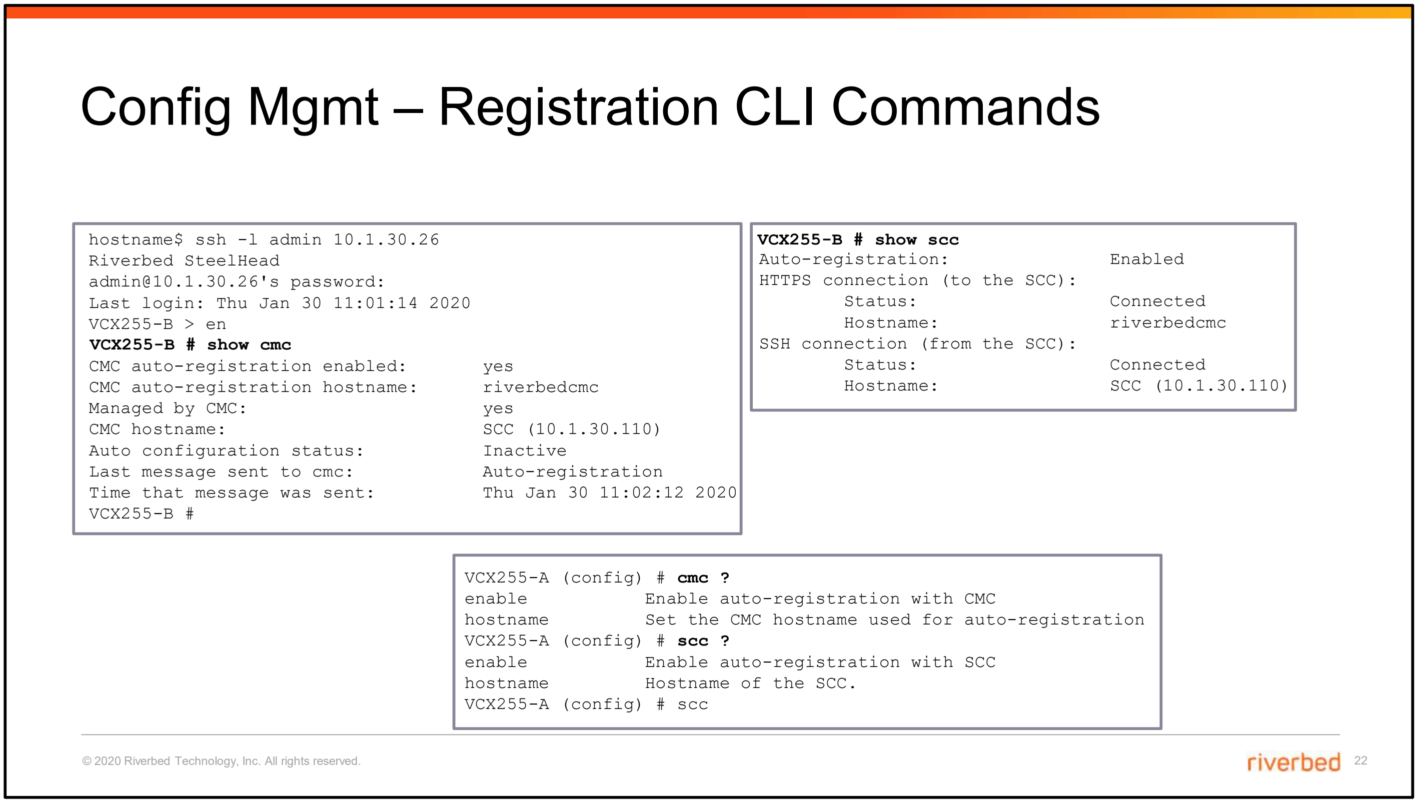
SteelHeads are designed to send a registration request periodically to the SCC so that they're automatically registered. If can take up to an hour for all registered SteelHeads to appear in the Appliances page.

An unregistered SteelHead appears on the Appliances page with the error “NO ADDRESS SPECIFIED.” You can manually add the SteelHead in the Appliances page.

Adding a Riverbed appliance creates a connection between the SCC and the appliance.

After you have registered an appliance, you can configure features and push configurations to remote appliances by group or for individual appliances using the SCC. The SCC collects statistics, health, and connection history information from registered appliances.

If you have SteelHeads that are behind a firewall you can run a CLI command that creates an SSL authorized port.



Config Mgmt – Registration CLI Commands

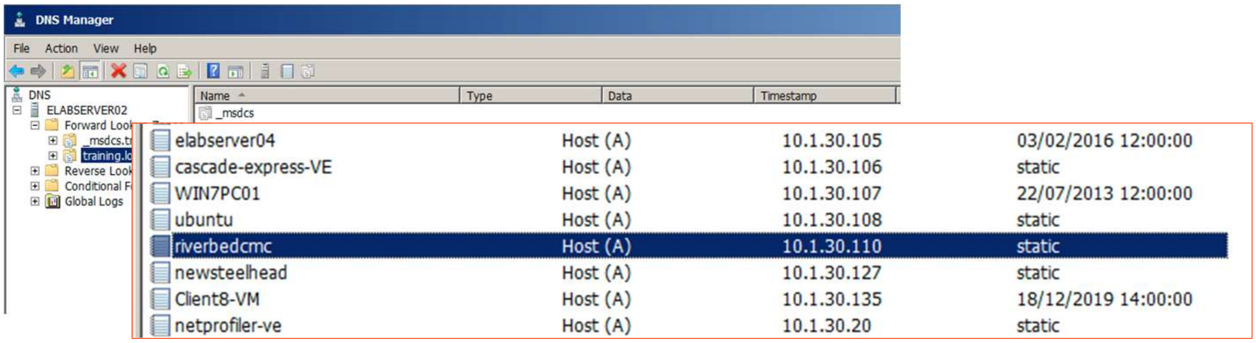
```
hostname$ ssh -l admin 10.1.30.26
Riverbed SteelHead
admin@10.1.30.26's password:
Last login: Thu Jan 30 11:01:14 2020
VCX255-B > en
VCX255-B # show cmc
CMC auto-registration enabled:       yes
CMC auto-registration hostname:      riverbedcmc
Managed by CMC:                      yes
CMC hostname:                        SCC (10.1.30.110)
Auto configuration status:           Inactive
Last message sent to cmc:            Auto-registration
Time that message was sent:          Thu Jan 30 11:02:12 2020
VCX255-B #
```

```
VCX255-B # show scc
Auto-registration:                 Enabled
HTTPS connection (to the SCC):
        Status:                    Connected
        Hostname:                  riverbedcmc
SSH connection (from the SCC):
        Status:                    Connected
        Hostname:                  SCC (10.1.30.110)
```

```
VCX255-A (config) # cmc ?
enable           Enable auto-registration with CMC
hostname         Set the CMC hostname used for auto-registration
VCX255-A (config) # scc ?
enable           Enable auto-registration with SCC
hostname         Hostname of the SCC.
VCX255-A (config) # scc
```

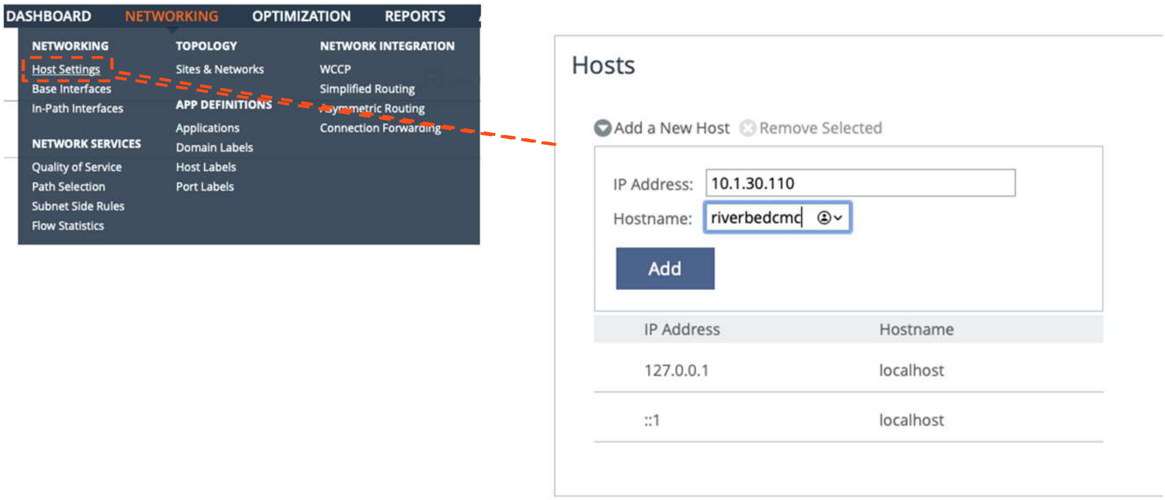
Config Mgmt – Auto-Registration: Using DNS

- DNS or Hostname Configuration is required
- Best Practice use NTP as well



Name	Type	Data	Timestamp
elabserver04	Host (A)	10.1.30.105	03/02/2016 12:00:00
cascade-express-VE	Host (A)	10.1.30.106	static
WIN7PC01	Host (A)	10.1.30.107	22/07/2013 12:00:00
ubuntu	Host (A)	10.1.30.108	static
riverbedcmc	Host (A)	10.1.30.110	static
newsteelhead	Host (A)	10.1.30.127	static
Client8-VM	Host (A)	10.1.30.135	18/12/2019 14:00:00
netprofiler-ve	Host (A)	10.1.30.20	static

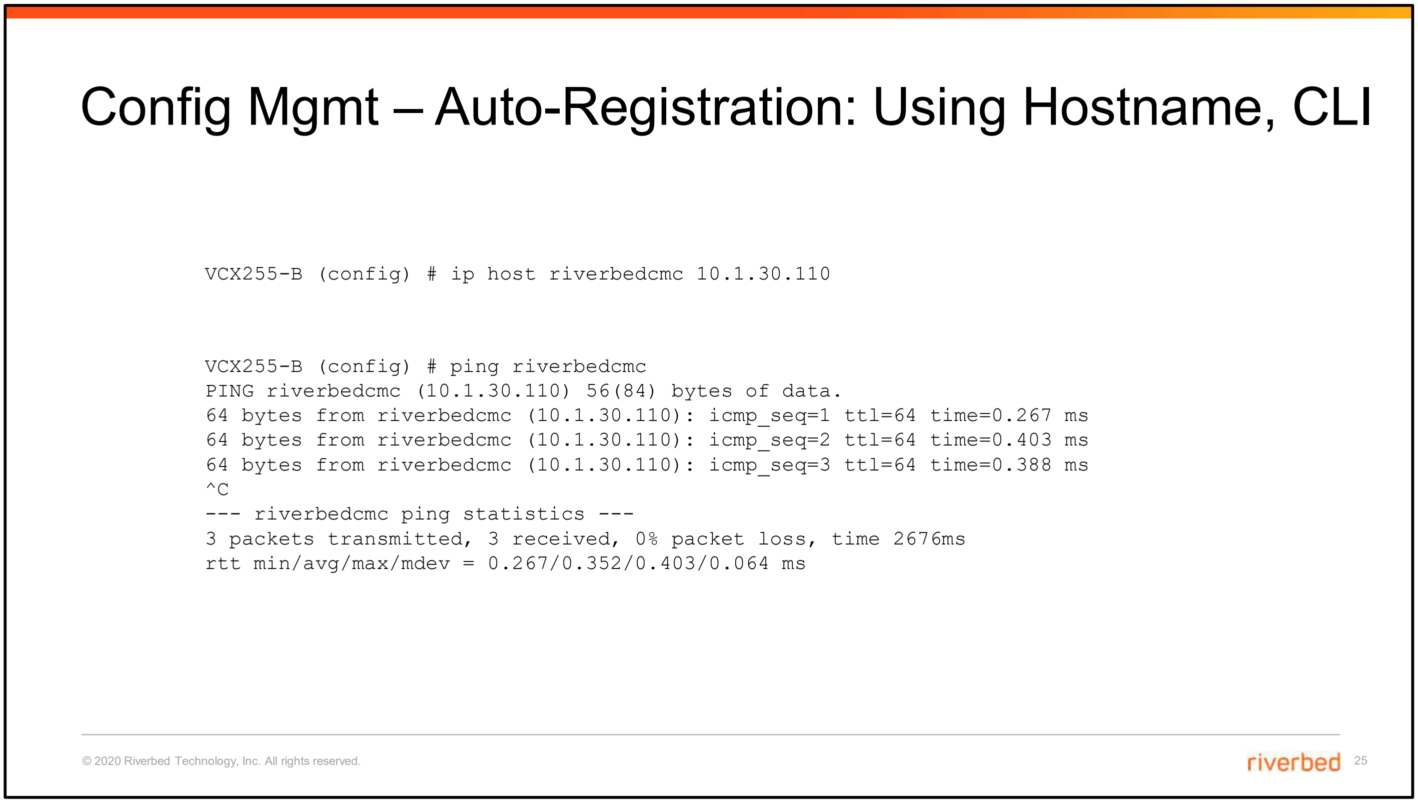
Config Mgmt – Auto-Registration: Using Hostname, GUI



IP Address: 10.1.30.110

Hostname: riverbedcmc

IP Address	Hostname
127.0.0.1	localhost
::1	localhost

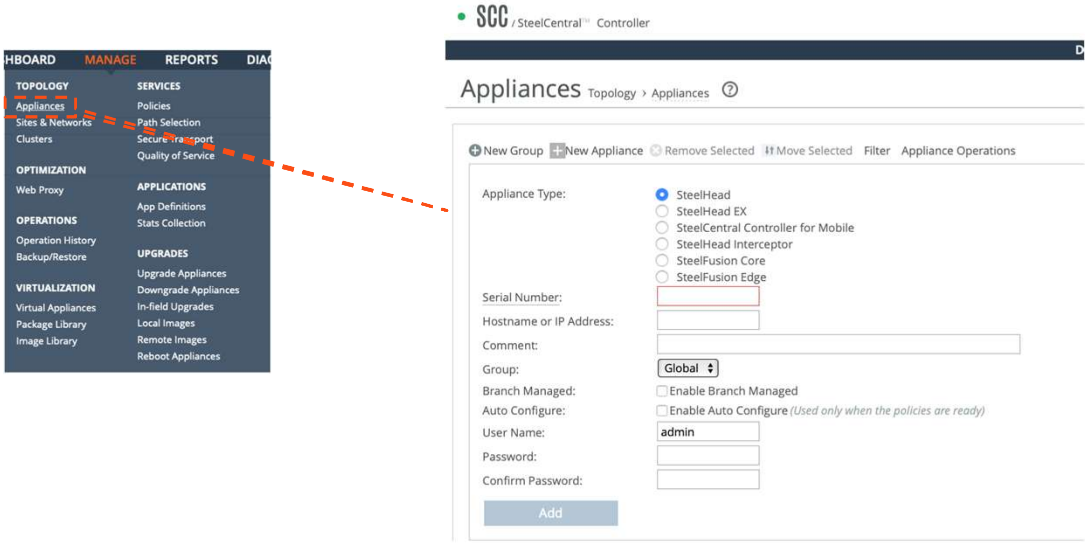


Config Mgmt – Auto-Registration: Using Hostname, CLI

```
VCX255-B (config) # ip host riverbedcmc 10.1.30.110
```

```
VCX255-B (config) # ping riverbedcmc
PING riverbedcmc (10.1.30.110) 56(84) bytes of data.
64 bytes from riverbedcmc (10.1.30.110): icmp_seq=1 ttl=64 time=0.267 ms
64 bytes from riverbedcmc (10.1.30.110): icmp_seq=2 ttl=64 time=0.403 ms
64 bytes from riverbedcmc (10.1.30.110): icmp_seq=3 ttl=64 time=0.388 ms
^C
--- riverbedcmc ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2676ms
rtt min/avg/max/mdev = 0.267/0.352/0.403/0.064 ms
```

Config Mgmt – Manual Registration



Appliance Type:
● SteelHead
○ SteelHead EX
○ SteelCentral Controller for Mobile
○ SteelHead Interceptor
○ SteelFusion Core
○ SteelFusion Edge

Serial Number:

Hostname or IP Address:

Comment:

Group: Global

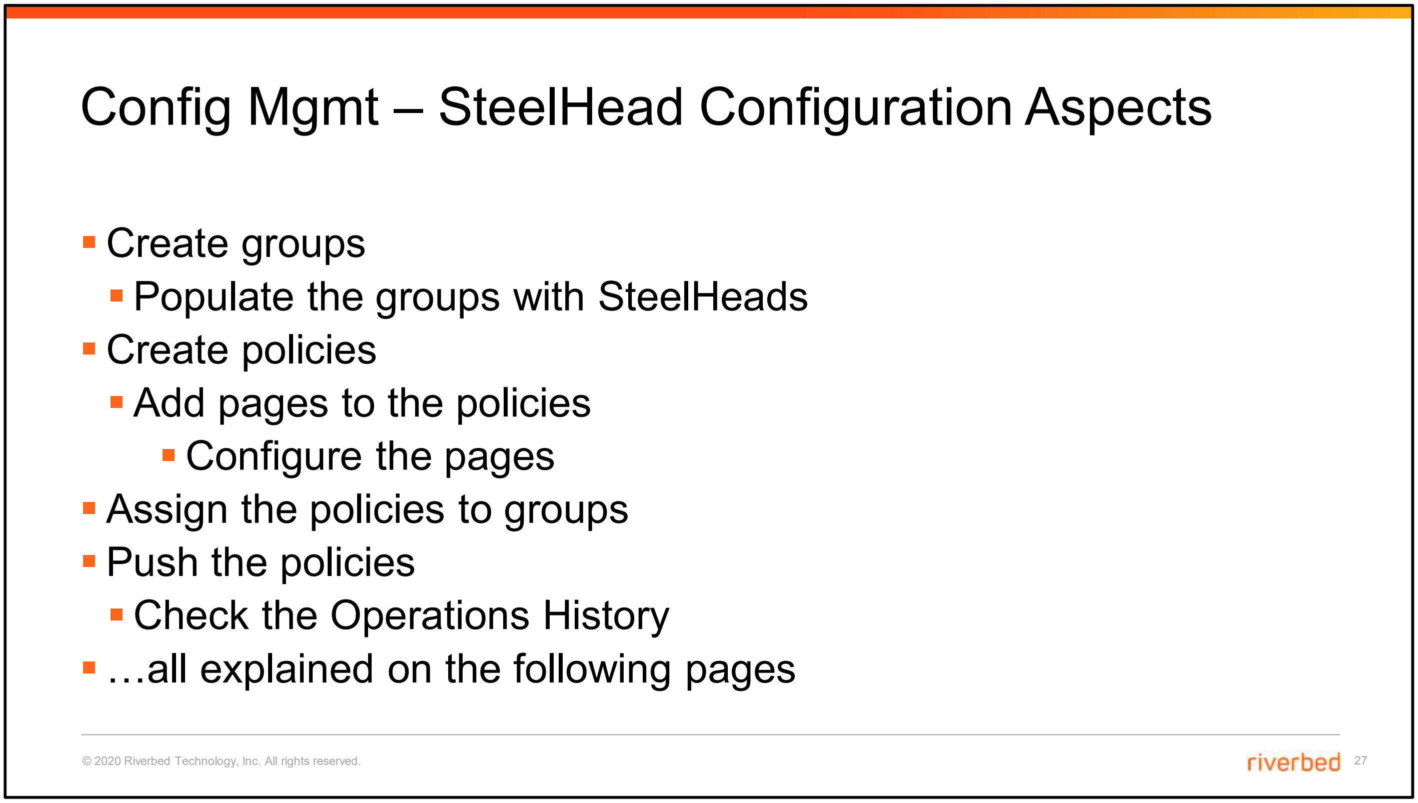
Branch Managed: □ Enable Branch Managed

Auto Configure: □ Enable Auto Configure *(Used only when the policies are ready)*

User Name: admin

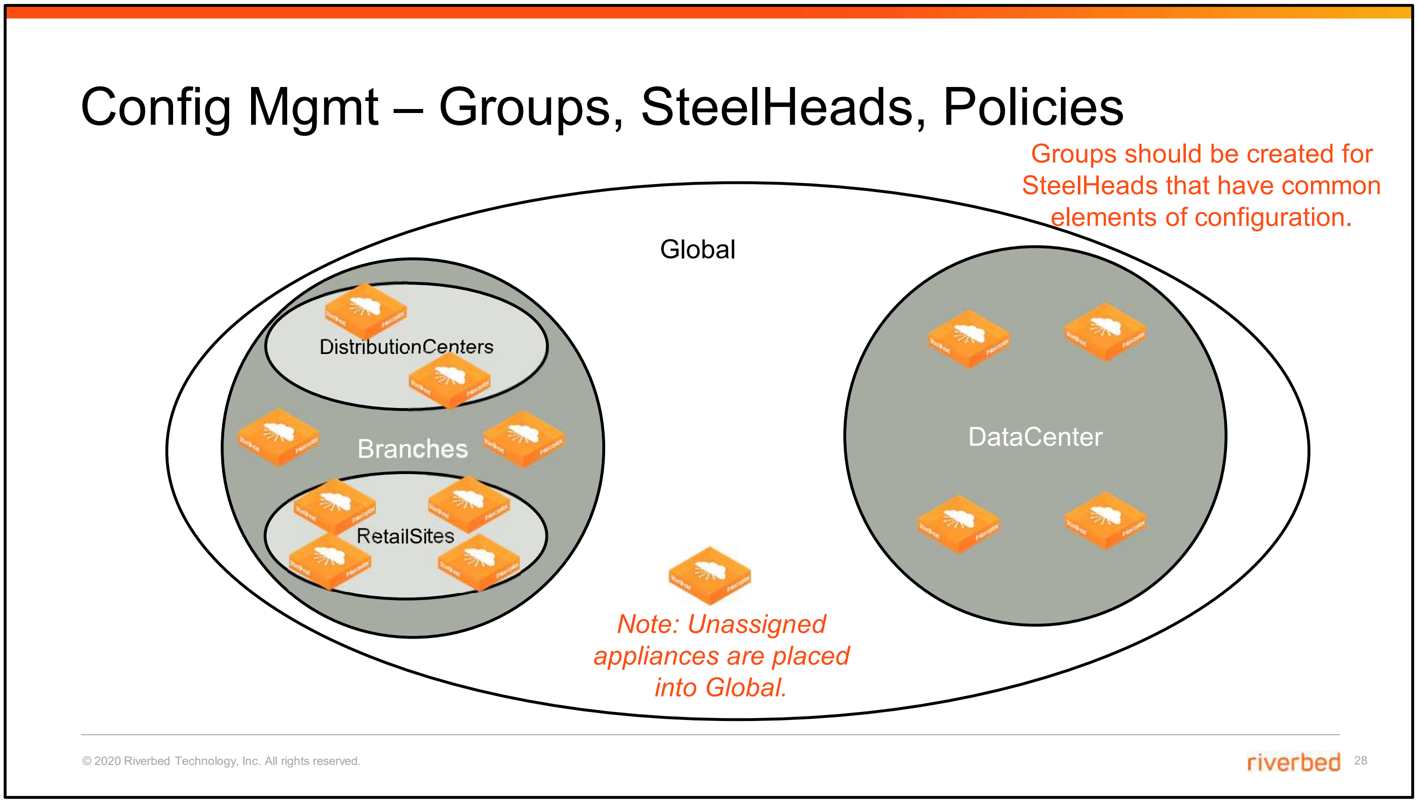
Password:

Confirm Password:



Config Mgmt – SteelHead Configuration Aspects

- Create groups
  - Populate the groups with SteelHeads
- Create policies
  - Add pages to the policies
    - Configure the pages
- Assign the policies to groups
- Push the policies
  - Check the Operations History
- …all explained on the following pages



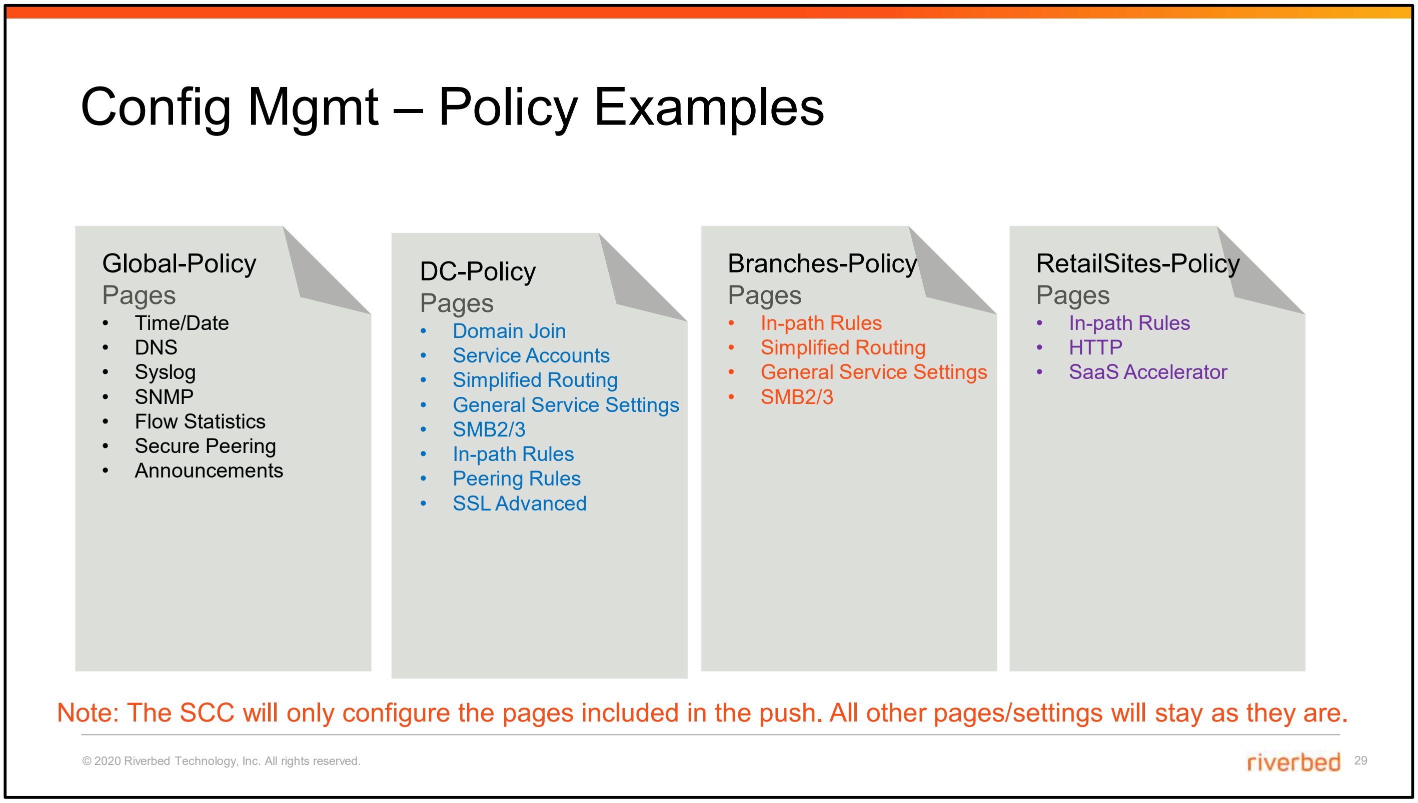
Config Mgmt – Groups, SteelHeads, Policies

Groups should be created for SteelHeads that have common elements of configuration.

Note: Unassigned appliances are placed into Global.

riverbed 28

There is a limit of 256 groups… if you call that a limitation.



Config Mgmt – Policy Examples

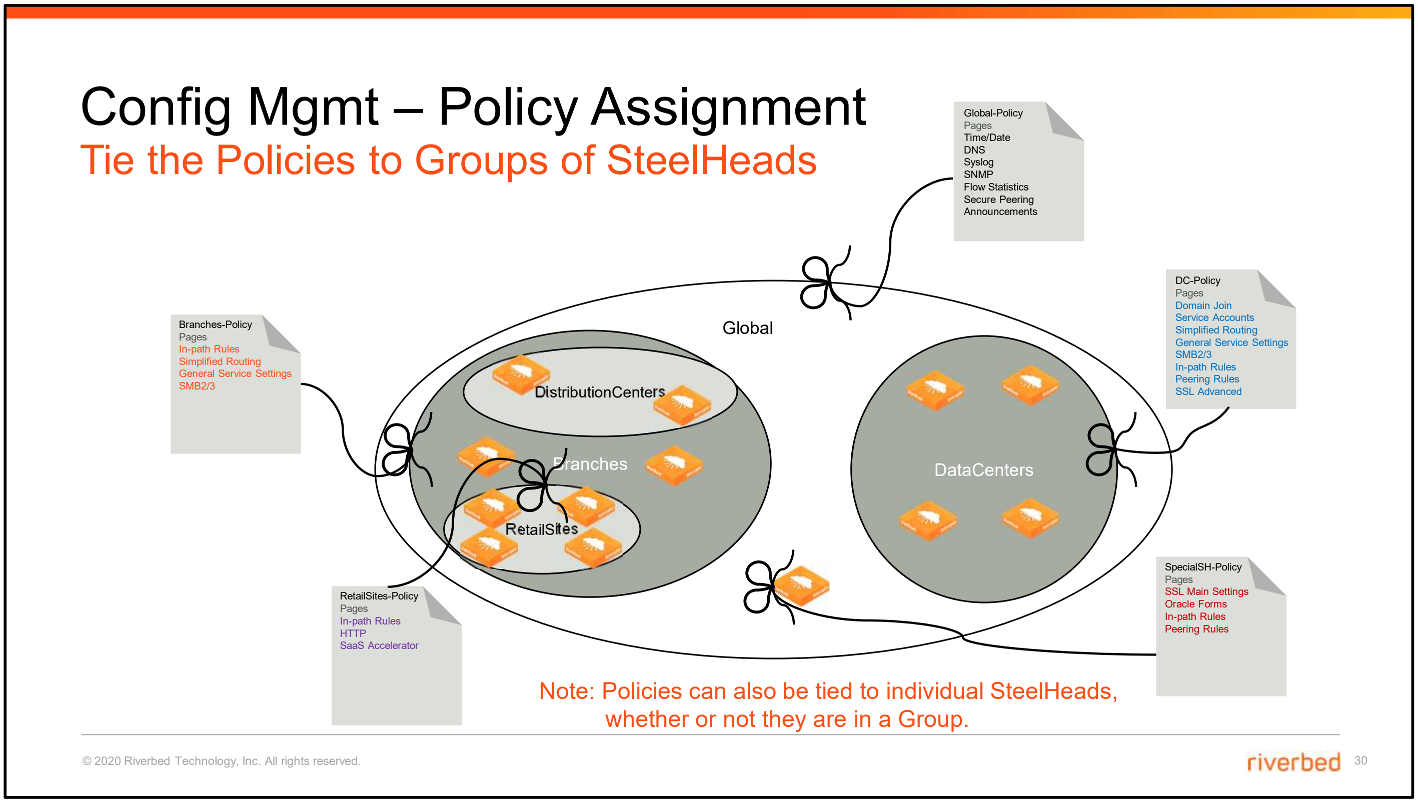
Global-Policy
Pages
- Time/Date
- DNS
- Syslog
- SNMP
- Flow Statistics
- Secure Peering
- Announcements

DC-Policy
Pages
- Domain Join
- Service Accounts
- Simplified Routing
- General Service Settings
- SMB2/3
- In-path Rules
- Peering Rules
- SSL Advanced

Branches-Policy
Pages
- In-path Rules
- Simplified Routing
- General Service Settings
- SMB2/3

RetailSites-Policy
Pages
- In-path Rules
- HTTP
- SaaS Accelerator

Note: The SCC will only configure the pages included in the push. All other pages/settings will stay as they are.



Config Mgmt – Policy Assignment

Tie the Policies to Groups of SteelHeads

Global-Policy
Pages
Time/Date
DNS
Syslog
SNMP
Flow Statistics
Secure Peering
Announcements

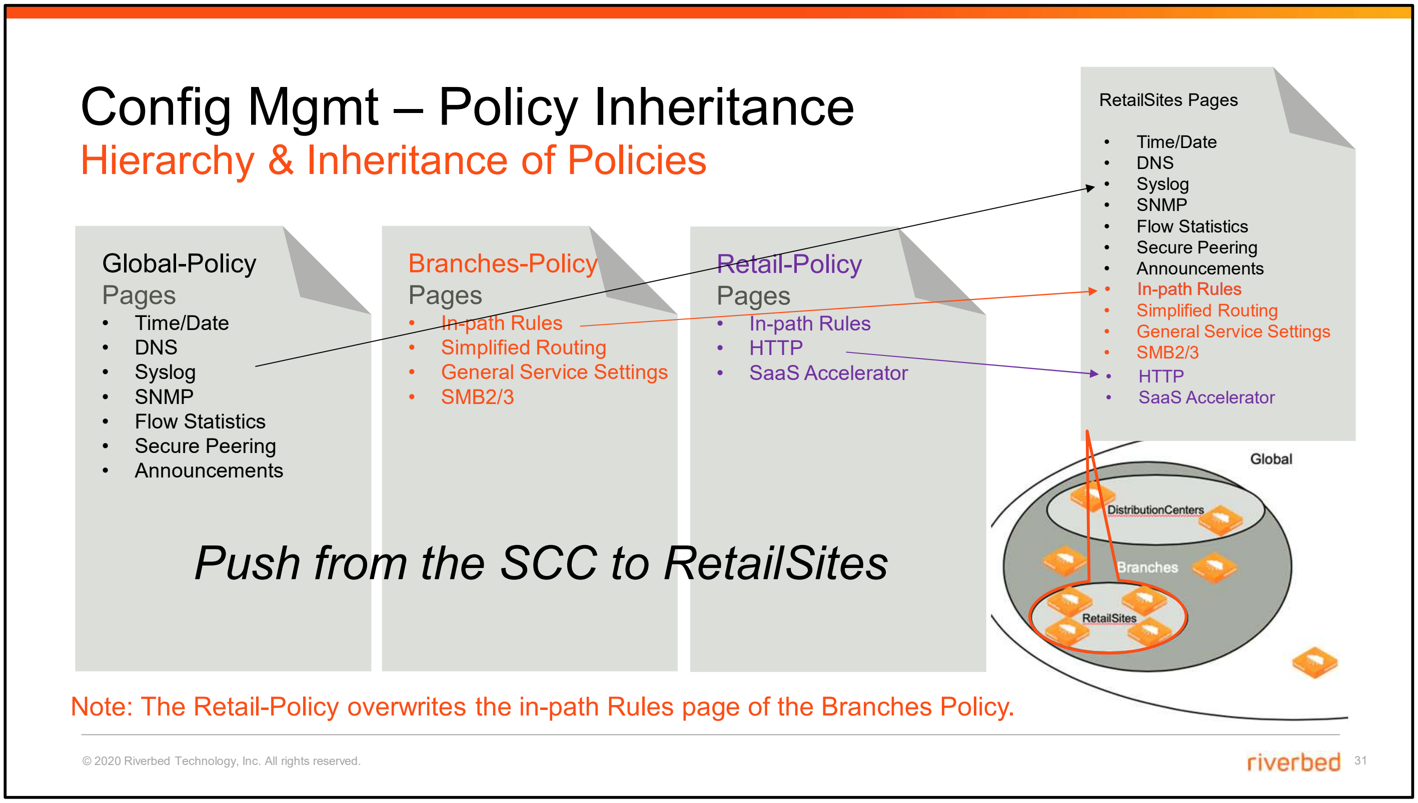
DC-Policy
Pages
Domain Join
Service Accounts
Simplified Routing
General Service Settings
SMB2/3
In-path Rules
Peering Rules
SSL Advanced

Branches-Policy
Pages
In-path Rules
Simplified Routing
General Service Settings
SMB2/3

RetailSites-Policy
Pages
In-path Rules
HTTP
SaaS Accelerator

SpecialSH-Policy
Pages
SSL Main Settings
Oracle Forms
In-path Rules
Peering Rules

Note: Policies can also be tied to individual SteelHeads, whether or not they are in a Group.



Config Mgmt – Policy Inheritance

Hierarchy & Inheritance of Policies

Global-Policy
Pages

- Time/Date
- DNS
- Syslog
- SNMP
- Flow Statistics
- Secure Peering
- Announcements

Branches-Policy
Pages

- In-path Rules
- Simplified Routing
- General Service Settings
- SMB2/3

Retail-Policy
Pages

- In-path Rules
- HTTP
- SaaS Accelerator

RetailSites Pages

- Time/Date
- DNS
- Syslog
- SNMP
- Flow Statistics
- Secure Peering
- Announcements
- In-path Rules
- Simplified Routing
- General Service Settings
- SMB2/3
- HTTP
- SaaS Accelerator

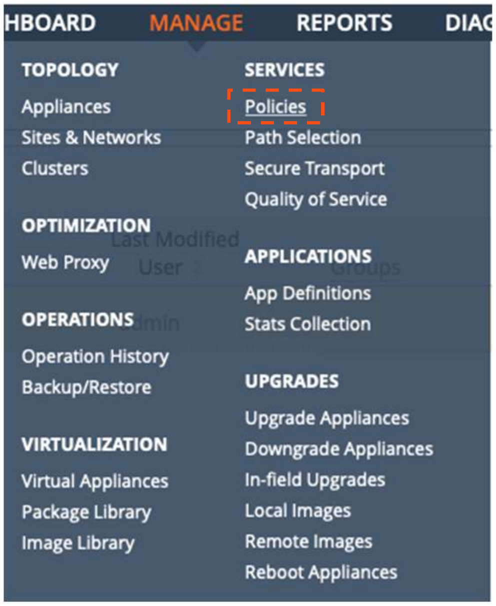
Push from the SCC to RetailSites

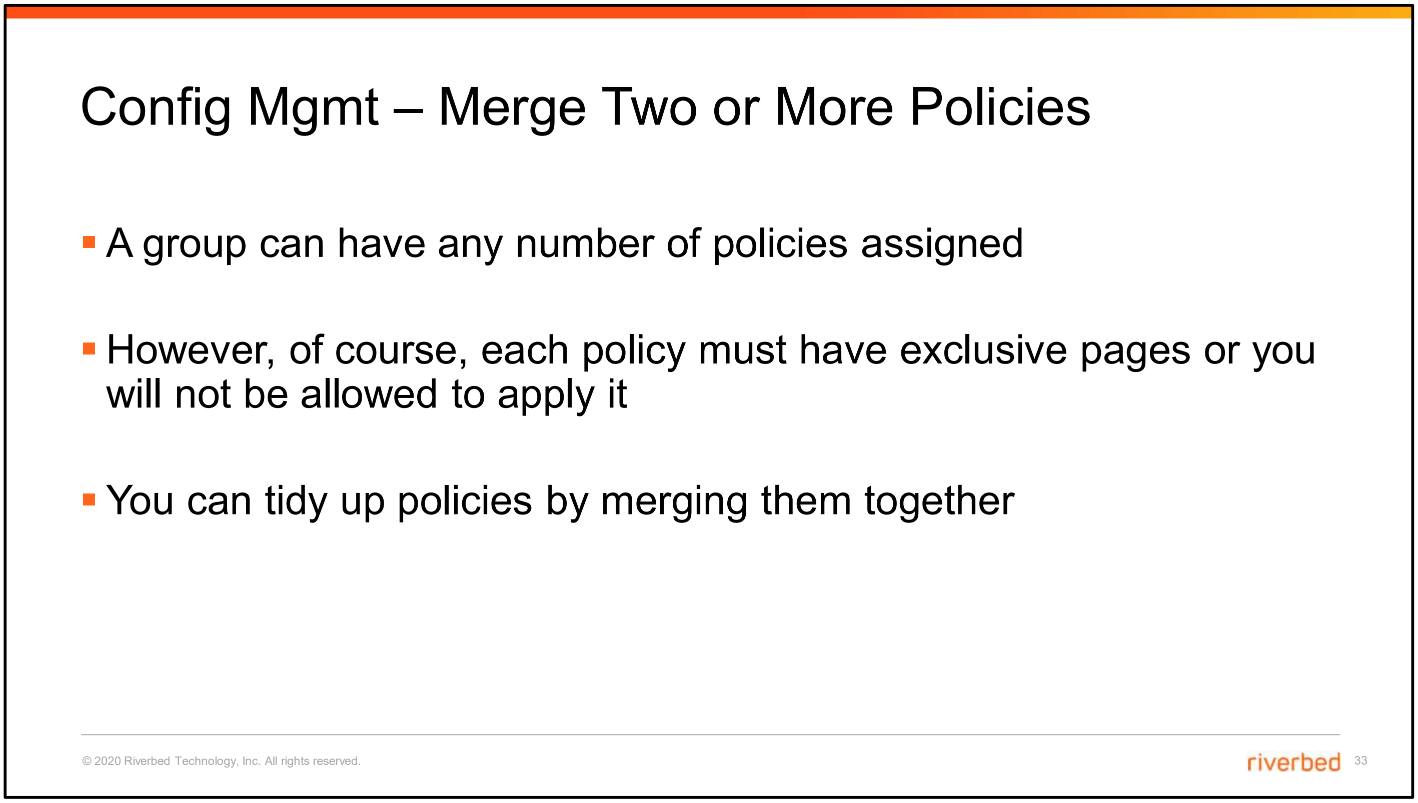
Note: The Retail-Policy overwrites the in-path Rules page of the Branches Policy.

Config Mgmt – Policy Creation

Create a Policy

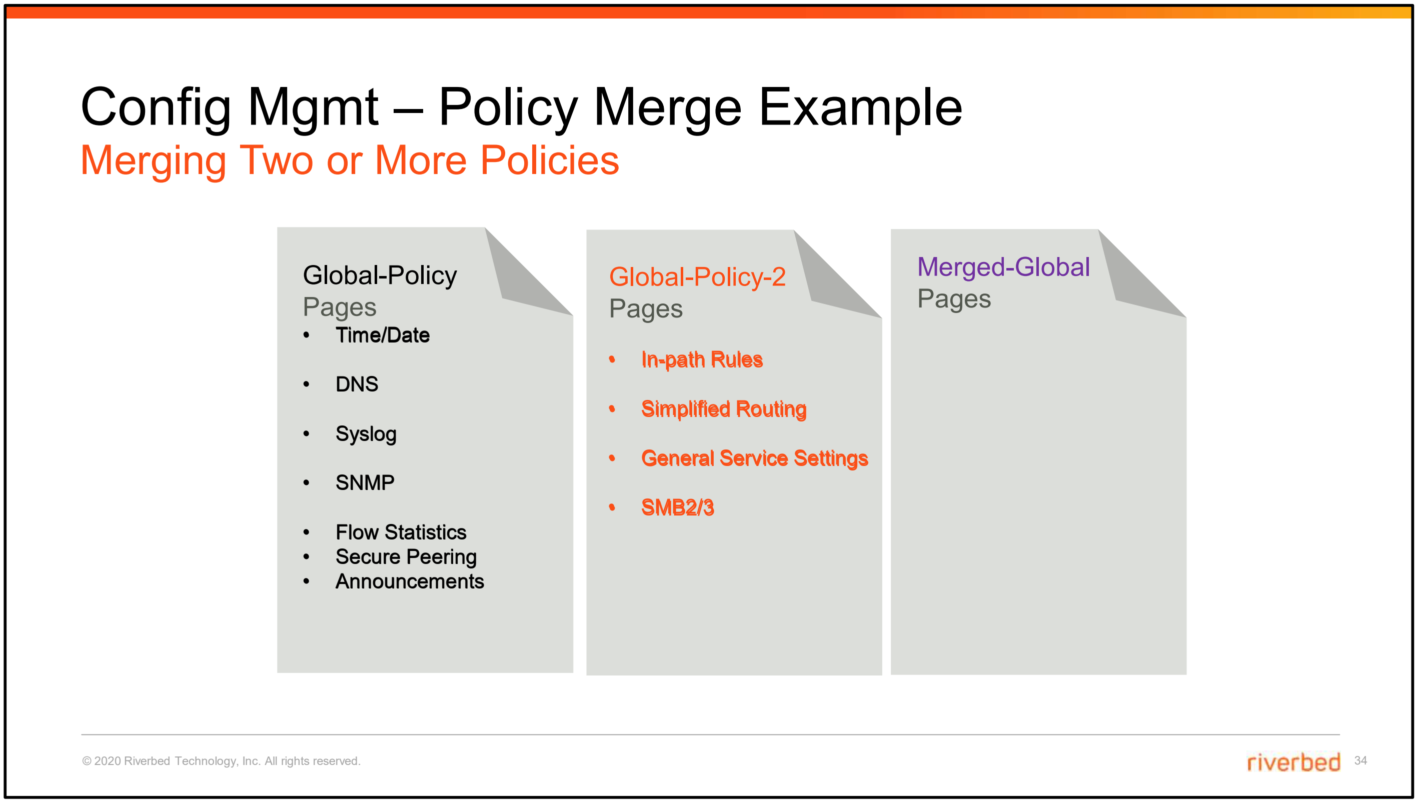
- Manually
- Copy an existing policy and adjust it
- Import from a SteelHead
- Merge existing policies together





Config Mgmt – Merge Two or More Policies

- A group can have any number of policies assigned
- However, of course, each policy must have exclusive pages or you will not be allowed to apply it
- You can tidy up policies by merging them together



Config Mgmt – Policy Merge Example

Merging Two or More Policies

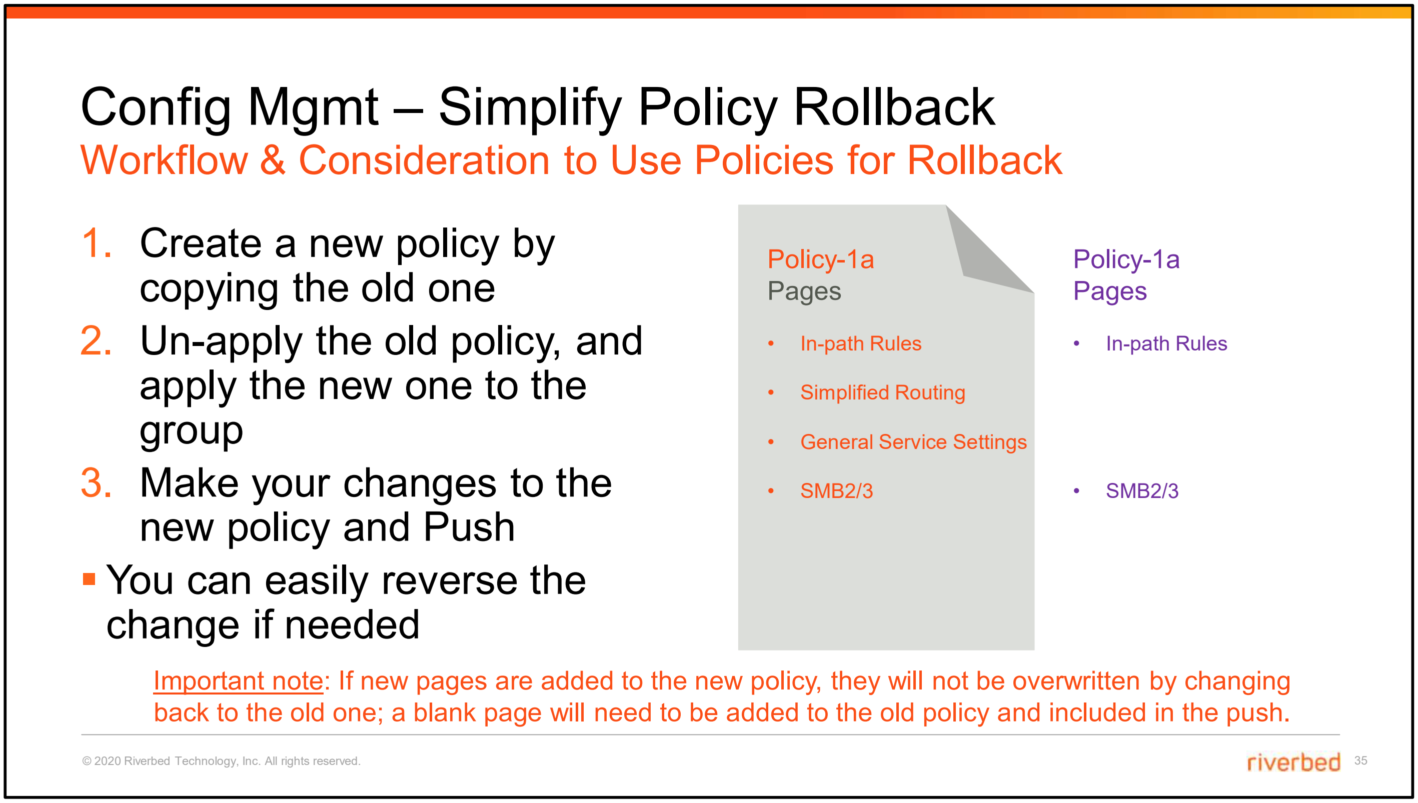
Global-Policy
Pages

- Time/Date
- DNS
- Syslog
- SNMP
- Flow Statistics
- Secure Peering
- Announcements

Global-Policy-2
Pages

- In-path Rules
- Simplified Routing
- General Service Settings
- SMB2/3

Merged-Global
Pages



Config Mgmt – Simplify Policy Rollback

Workflow & Consideration to Use Policies for Rollback

1. Create a new policy by copying the old one
2. Un-apply the old policy, and apply the new one to the group
3. Make your changes to the new policy and Push

- You can easily reverse the change if needed

Policy-1a
Pages

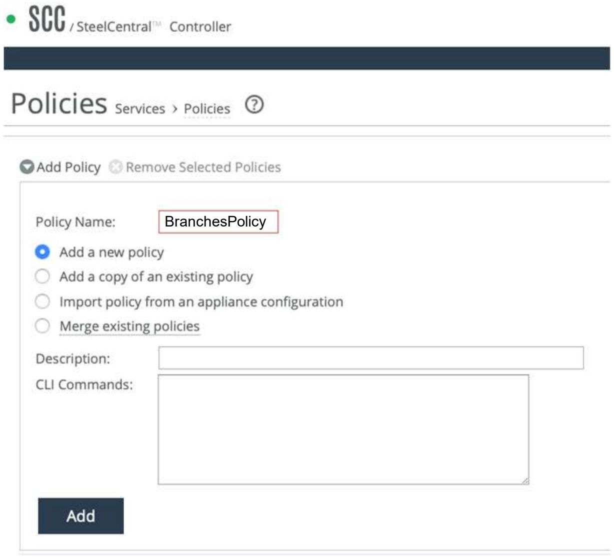
- In-path Rules
- Simplified Routing
- General Service Settings
- SMB2/3

Policy-1a
Pages

- In-path Rules
- SMB2/3

Important note: If new pages are added to the new policy, they will not be overwritten by changing back to the old one; a blank page will need to be added to the old policy and included in the push.

Config Mgmt – Add a New Policy



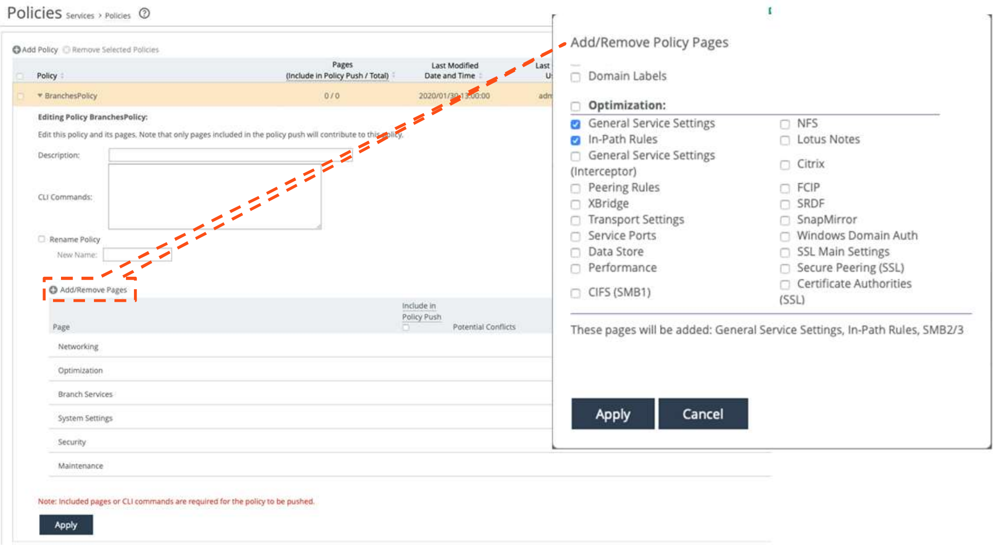
Policy Name: BranchesPolicy

● Add a new policy
○ Add a copy of an existing policy
○ Import policy from an appliance configuration
○ Merge existing policies

Description:

CLI Commands:

Config Mgmt – Adding Pages to a Policy



Policies Services › Policies

Add Policy | Remove Selected Policies

	Policy	Pages (Include in Policy Push / Total)	Last Modified Date and Time	Last U
□	▾ BranchesPolicy	0 / 0	2020/01/30 13:00:00	adm

Editing Policy BranchesPolicy:

Edit this policy and its pages. Note that only pages included in the policy push will contribute to this policy.

Description:

CLI Commands:

□ Rename Policy

New Name:

Add/Remove Pages

Page	Include in Policy Push □	Potential Conflicts
Networking		
Optimization		
Branch Services		
System Settings		
Security		
Maintenance		

Note: Included pages or CLI commands are required for the policy to be pushed.

Apply

Add/Remove Policy Pages

□ Domain Labels

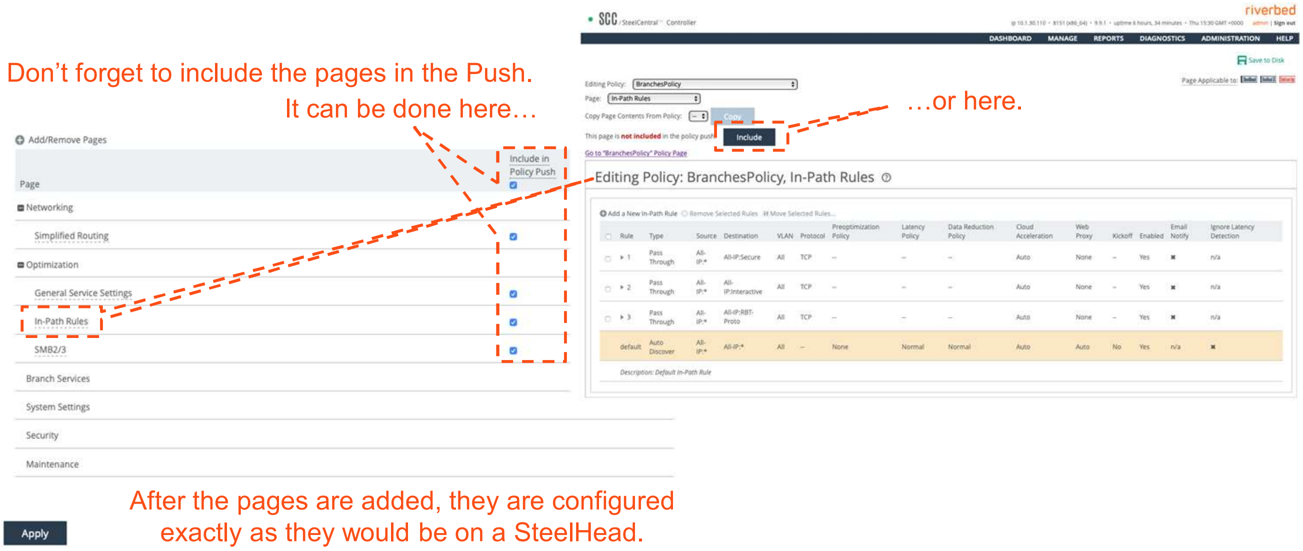
□ **Optimization:**

- ☑ General Service Settings
- ☑ In-Path Rules
- □ General Service Settings (Interceptor)
- □ Peering Rules
- □ XBridge
- □ Transport Settings
- □ Service Ports
- □ Data Store
- □ Performance
- □ CIFS (SMB1)
- □ NFS
- □ Lotus Notes
- □ Citrix
- □ FCIP
- □ SRDF
- □ SnapMirror
- □ Windows Domain Auth
- □ SSL Main Settings
- □ Secure Peering (SSL)
- □ Certificate Authorities (SSL)

These pages will be added: General Service Settings, In-Path Rules, SMB2/3

Apply | Cancel

Config Mgmt – Editing Page Settings



Don't forget to include the pages in the Push.
It can be done here…

…or here.

SCC / SteelCentral™ Controller
riverbed
@ 10.1.30.110 • 8151 (x86_64) • 9.9.1 • uptime 6 hours, 34 minutes • Thu 15:30 GMT +0000
admin | Sign out
DASHBOARD
MANAGE
REPORTS
DIAGNOSTICS
ADMINISTRATION
HELP
Save to Disk
Page Applicable to:

Editing Policy: BranchesPolicy

Page: In-Path Rules

Copy Page Contents From Policy: --

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

Go to "BranchesPolicy" Policy Page

Editing Policy: BranchesPolicy, In-Path Rules

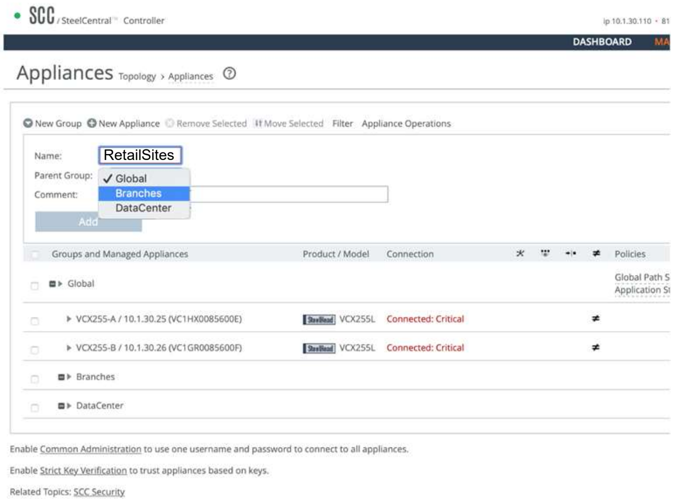
	Rule	Type	Source	Destination	VLAN	Protocol	Preoptimization Policy	Latency Policy	Data Reduction Policy	Cloud Acceleration	Web Proxy	Kickoff	Enabled	Email Notify	Ignore Latency Detection
□	▸ 1	Pass Through	All-IP:*	All-IP:Secure	All	TCP	--	--	--	Auto	None	--	Yes	✖	n/a
□	▸ 2	Pass Through	All-IP:*	All-IP:Interactive	All	TCP	--	--	--	Auto	None	--	Yes	✖	n/a
□	▸ 3	Pass Through	All-IP:*	All-IP:RBT-Proto	All	TCP	--	--	--	Auto	None	--	Yes	✖	n/a
	default	Auto Discover	All-IP:*	All-IP:*	All	--	None	Normal	Normal	Auto	Auto	No	Yes	n/a	✖

Description: Default In-Path Rule

Page	Include in Policy Push
	☑
⊟ Networking	
Simplified Routing	☑
⊟ Optimization	
General Service Settings	☑
In-Path Rules	☑
SMB2/3	☑
Branch Services	
System Settings	
Security	
Maintenance	

After the pages are added, they are configured exactly as they would be on a SteelHead.

Config Mgmt – Creating Groups



Appliances Topology › Appliances

Name: RetailSites

Parent Group: ✓ Global

Comment:

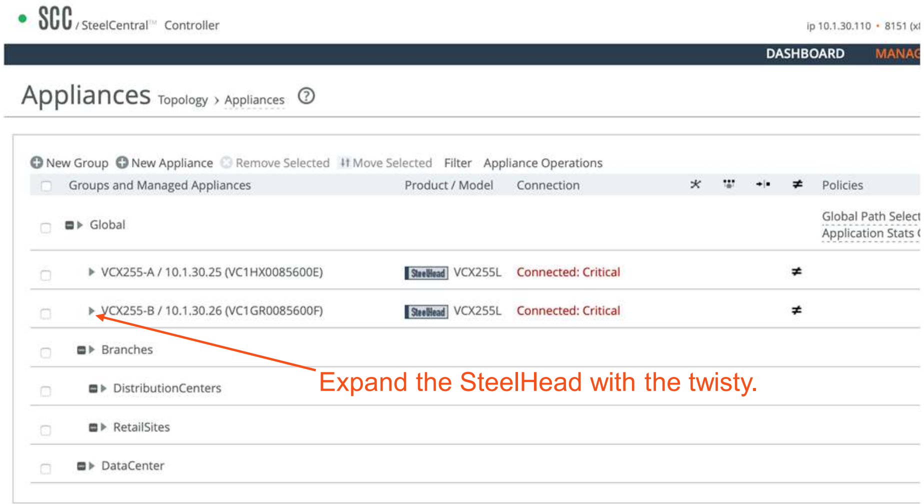
Groups and Managed Appliances	Product / Model	Connection				≠	Policies
Global							Global Path S Application S
VCX255-A / 10.1.30.25 (VC1HX0085600E)	SteelHead VCX255L	Connected: Critical				≠	
VCX255-B / 10.1.30.26 (VC1GR0085600F)	SteelHead VCX255L	Connected: Critical				≠	
Branches							
DataCenter							

Enable Common Administration to use one username and password to connect to all appliances.

Enable Strict Key Verification to trust appliances based on keys.

Related Topics: SCC Security

Config Mgmt – Add Existing SteelHead to Group (1/3)



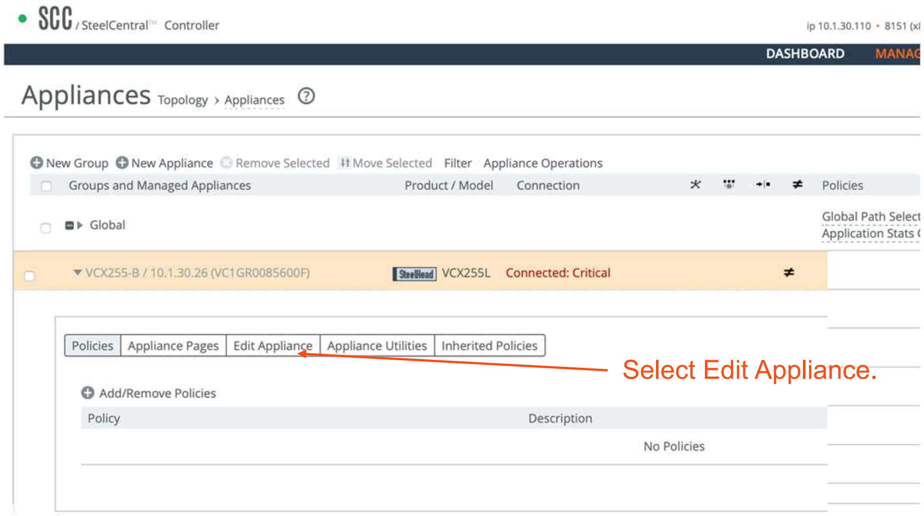
Appliances Topology › Appliances ⓘ

⊕ New Group ⊕ New Appliance Remove Selected Move Selected Filter Appliance Operations

□	Groups and Managed Appliances	Product / Model	Connection	⚹	⠿	→|•	≠	Policies
□	▸ Global							Global Path Select Application Stats (
□	▸ VCX255-A / 10.1.30.25 (VC1HX0085600E)	SteelHead VCX255L	Connected: Critical				≠	
□	▸ VCX255-B / 10.1.30.26 (VC1GR0085600F)	SteelHead VCX255L	Connected: Critical				≠	
□	▸ Branches							
□	▸ DistributionCenters							
□	▸ RetailSites							
□	▸ DataCenter							

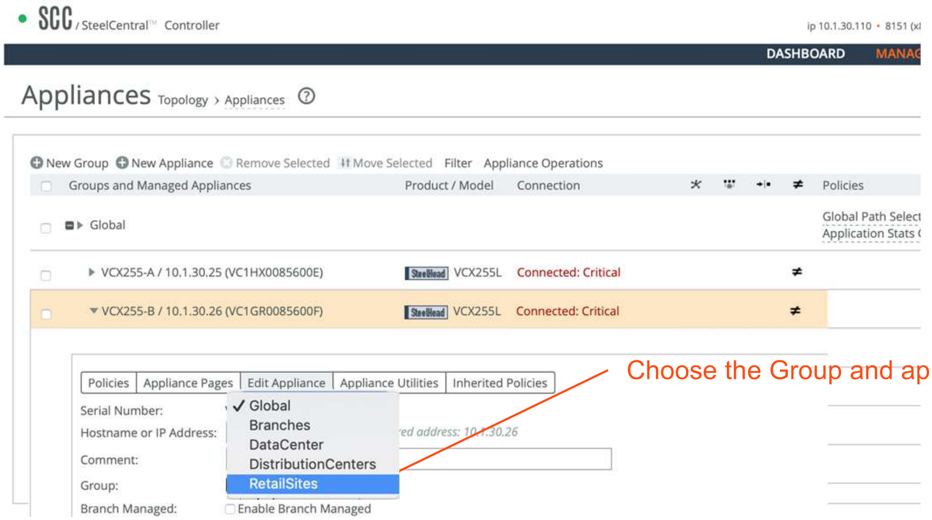
Expand the SteelHead with the twisty.

Config Mgmt – Add Existing SteelHead to Group (2/3)



Select Edit Appliance.

Config Mgmt – Add Existing SteelHead to Group (3/3)



SCC / SteelCentral™ Controller   ip 10.1.30.110 • 8151 (x

DASHBOARD MANAG

Appliances Topology › Appliances

New Group | New Appliance | Remove Selected | Move Selected | Filter | Appliance Operations

Groups and Managed Appliances	Product / Model	Connection	Policies
Global			Global Path Select Application Stats (
VCX255-A / 10.1.30.25 (VC1HX0085600E)	SteelHead VCX255L	Connected: Critical	
VCX255-B / 10.1.30.26 (VC1GR0085600F)	SteelHead VCX255L	Connected: Critical	

Policies | Appliance Pages | Edit Appliance | Appliance Utilities | Inherited Policies

Serial Number:

Hostname or IP Address: ...red address: 10.1.30.26

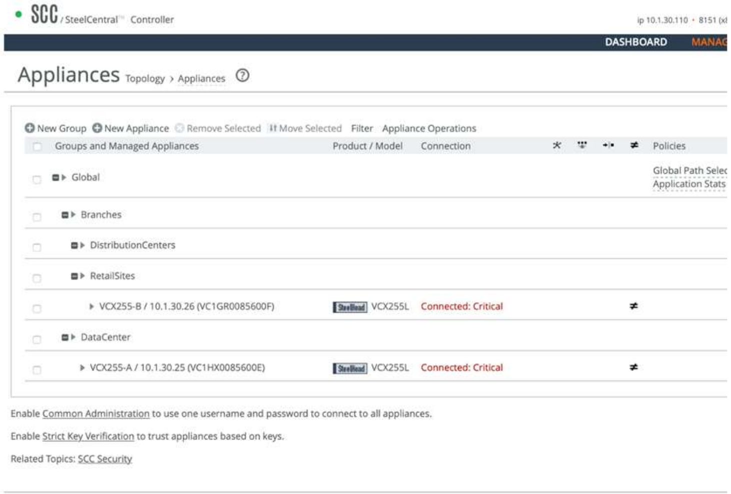
Comment:

Group: RetailSites

Branch Managed: □ Enable Branch Managed

Choose the Group and apply.

Config Mgmt – Hierarchical Group Display



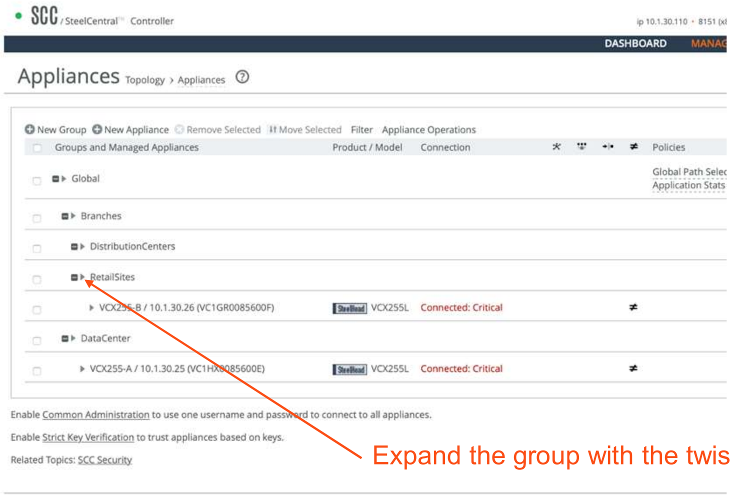
□	Groups and Managed Appliances	Product / Model	Connection	≠	Policies
□	Global				Global Path Selec Application Stats
□	Branches				
□	DistributionCenters				
□	RetailSites				
□	VCX255-B / 10.1.30.26 (VC1GR0085600F)	SteelHead VCX255L	Connected: Critical	≠	
□	DataCenter				
□	VCX255-A / 10.1.30.25 (VC1HX0085600E)	SteelHead VCX255L	Connected: Critical	≠	

Enable Common Administration to use one username and password to connect to all appliances.

Enable Strict Key Verification to trust appliances based on keys.

Related Topics: SCC Security

Config Mgmt – Add Policy to Group, or SteelHead (1/2)



Groups and Managed Appliances	Product / Model	Connection	≠	Policies
Global				Global Path Selec Application Stats
Branches				
DistributionCenters				
RetailSites				
VCX255-B / 10.1.30.26 (VC1GR0085600F)	SteelHead VCX255L	Connected: Critical	≠	
DataCenter				
VCX255-A / 10.1.30.25 (VC1HX0085600E)	SteelHead VCX255L	Connected: Critical	≠	

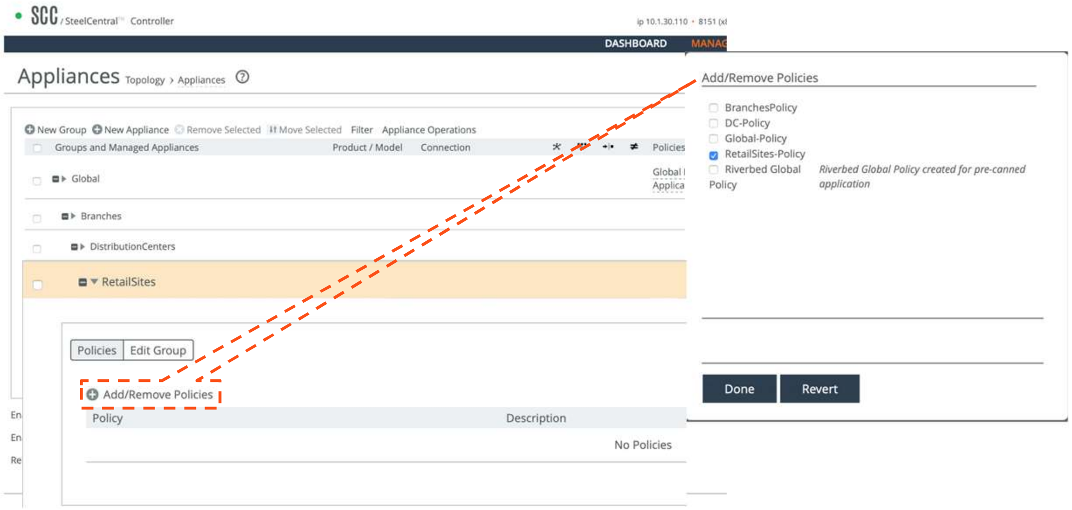
Enable Common Administration to use one username and password to connect to all appliances.

Enable Strict Key Verification to trust appliances based on keys.

Related Topics: SCC Security

Expand the group with the twisty.

Config Mgmt – Add Policy to Group, or SteelHead (2/2)



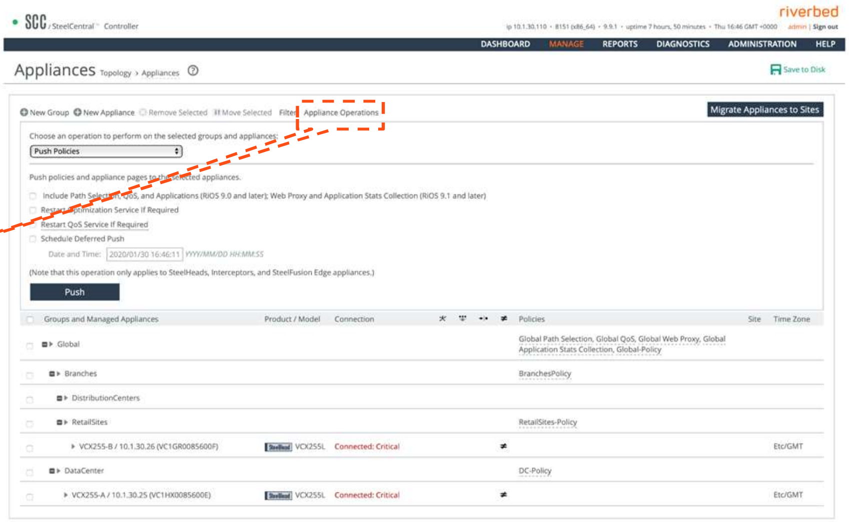
□	Groups and Managed Appliances	Product / Model	Connection	Policies
□	Global			Global I Applica
□	Branches			
□	DistributionCenters			
□	RetailSites			

Policy	Description
	No Policies

Add/Remove Policies

- □ BranchesPolicy
- □ DC-Policy
- □ Global-Policy
- ☑ RetailSites-Policy
- □ Riverbed Global Policy — *Riverbed Global Policy created for pre-canned application*

Config Mgmt – Push Policy/Config from SCC (1/2)



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

Push Policies

Push policies and appliance pages to the selected appliances.

□ Include Path Selection, QoS, and Applications (RiOS 9.0 and later); Web Proxy and Application Stats Collection (RiOS 9.1 and later)

□ Restart Optimization Service If Required

□ Restart QoS Service If Required

□ Schedule Deferred Push

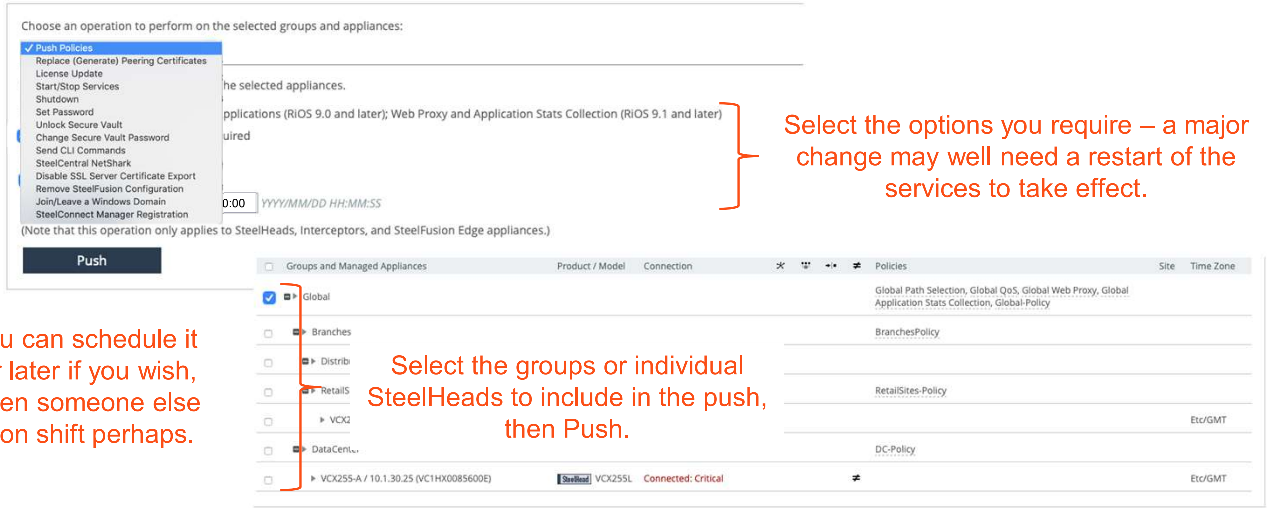
Date and Time: 2020/01/30 16:46:11 YYYY/MM/DD HH:MM:SS

(Note that this operation only applies to SteelHeads, Interceptors, and SteelFusion Edge appliances.)

Groups and Managed Appliances	Product / Model	Connection				≠	Policies	Site	Time Zone
Global							Global Path Selection, Global QoS, Global Web Proxy, Global Application Stats Collection, Global-Policy		
Branches							BranchesPolicy		
DistributionCenters									
RetailSites							RetailSites-Policy		
VCX255-B / 10.1.30.26 (VC1GR0085600F)	SteelHead VCX255L	Connected: Critical				≠			Etc/GMT
DataCenter							DC-Policy		
VCX255-A / 10.1.30.25 (VC1HX0085600E)	SteelHead VCX255L	Connected: Critical				≠			Etc/GMT

On the Manage Appliances page, select Appliance Operations.

Config Mgmt – Push Policy/Config from SCC (2/2)



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

✓ Push Policies
Replace (Generate) Peering Certificates
License Update
Start/Stop Services
Shutdown
Set Password
Unlock Secure Vault
Change Secure Vault Password
Send CLI Commands
SteelCentral NetShark
Disable SSL Server Certificate Export
Remove SteelFusion Configuration
Join/Leave a Windows Domain
SteelConnect Manager Registration

he selected appliances.

pplications (RiOS 9.0 and later); Web Proxy and Application Stats Collection (RiOS 9.1 and later)

uired

0:00 YYYY/MM/DD HH:MM:SS

(Note that this operation only applies to SteelHeads, Interceptors, and SteelFusion Edge appliances.)

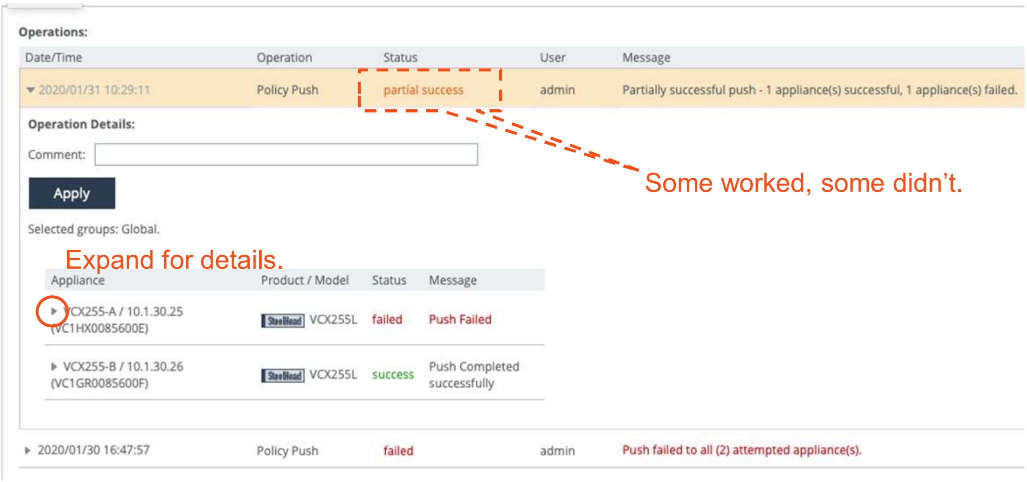
□	Groups and Managed Appliances	Product / Model	Connection				≠	Policies	Site	Time Zone
☑	Global							Global Path Selection, Global QoS, Global Web Proxy, Global Application Stats Collection, Global-Policy		
□	Branches							BranchesPolicy		
□	Distrib									
□	RetailS							RetailSites-Policy		
□	VCX2									Etc/GMT
□	DataCent..							DC-Policy		
□	VCX255-A / 10.1.30.25 (VC1HX0085600E)	SteelHead VCX255L	Connected: Critical				≠			Etc/GMT

Select the options you require – a major change may well need a restart of the services to take effect.

You can schedule it for later if you wish, when someone else is on shift perhaps.

Select the groups or individual SteelHeads to include in the push, then Push.

Config Mgmt – Operation History, Partial Success



Operations:

Date/Time	Operation	Status	User	Message
▾ 2020/01/31 10:29:11	Policy Push	partial success	admin	Partially successful push - 1 appliance(s) successful, 1 appliance(s) failed.

Operation Details:

Comment:

Selected groups: Global.

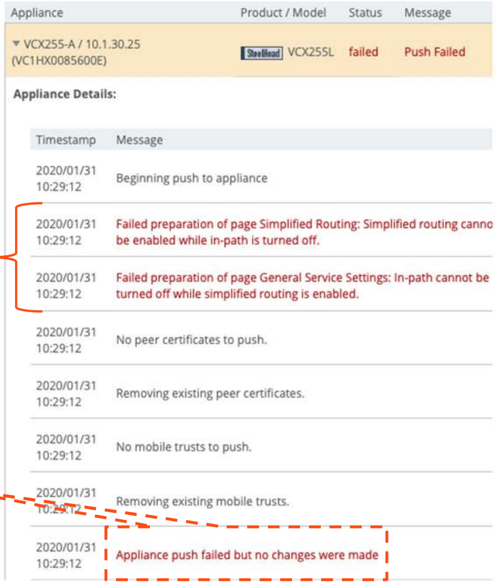
Appliance	Product / Model	Status	Message
▸ VCX255-A / 10.1.30.25 (VC1HX0085600E)	SteelHead VCX255L	failed	Push Failed
▸ VCX255-B / 10.1.30.26 (VC1GR0085600F)	SteelHead VCX255L	success	Push Completed successfully

Date/Time	Operation	Status	User	Message
▸ 2020/01/30 16:47:57	Policy Push	failed	admin	Push failed to all (2) attempted appliance(s).

Some worked, some didn't.

Expand for details.

Config Mgmt – Operation History, Details



Appliance	Product / Model	Status	Message
▾ VCX255-A / 10.1.30.25 (VC1HX0085600E)	SteelHead VCX255L	failed	Push Failed

Appliance Details:

Timestamp	Message
2020/01/31 10:29:12	Beginning push to appliance
2020/01/31 10:29:12	Failed preparation of page Simplified Routing: Simplified routing canno be enabled while in-path is turned off.
2020/01/31 10:29:12	Failed preparation of page General Service Settings: In-path cannot be turned off while simplified routing is enabled.
2020/01/31 10:29:12	No peer certificates to push.
2020/01/31 10:29:12	Removing existing peer certificates.
2020/01/31 10:29:12	No mobile trusts to push.
2020/01/31 10:29:12	Removing existing mobile trusts.
2020/01/31 10:29:12	Appliance push failed but no changes were made

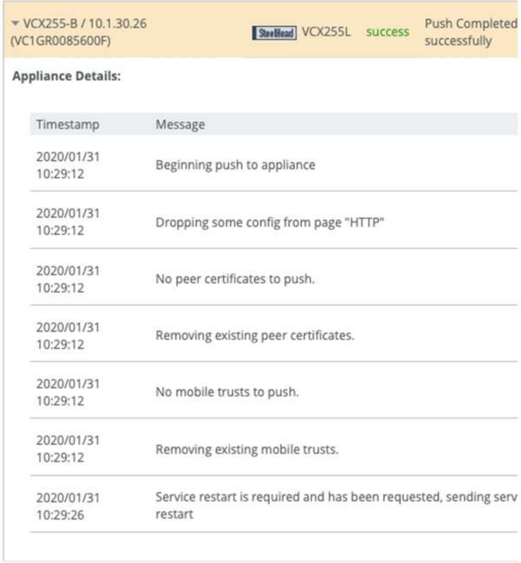
The issues are listed here.

Important point: If a push fails nothing at all is changed.

riverbed 49

Config Mgmt – Operation History, Successful Push

A more successful one.

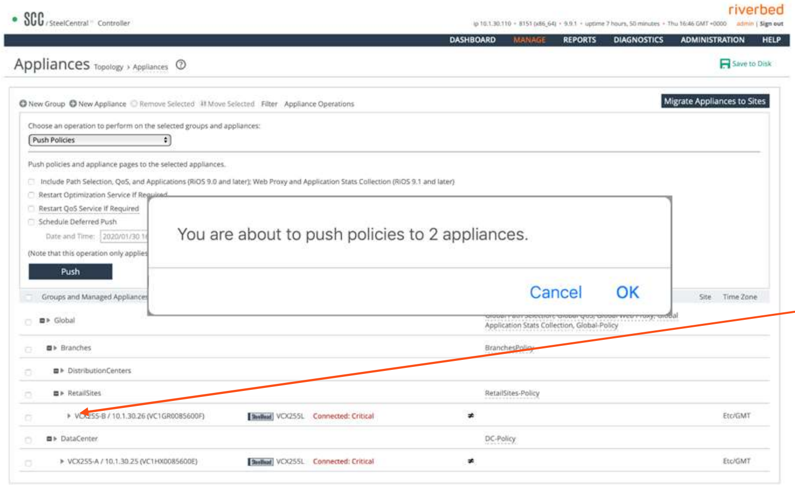


▾ VCX255-B / 10.1.30.26 (VC1GR0085600F) SteelHead VCX255L success Push Completed successfully

Appliance Details:

Timestamp	Message
2020/01/31 10:29:12	Beginning push to appliance
2020/01/31 10:29:12	Dropping some config from page "HTTP"
2020/01/31 10:29:12	No peer certificates to push.
2020/01/31 10:29:12	Removing existing peer certificates.
2020/01/31 10:29:12	No mobile trusts to push.
2020/01/31 10:29:12	Removing existing mobile trusts.
2020/01/31 10:29:26	Service restart is required and has been requested, sending serv restart

Config Mgmt – Push Policies


SCC / SteelCentral Controller
riverbed
ip 10.1.30.110 • 8151 (x86_64) • 9.9.1 • uptime 7 hours, 50 minutes • Thu 16:46 GMT +0000 admin | Sign out
DASHBOARD
MANAGE
REPORTS
DIAGNOSTICS
ADMINISTRATION
HELP
Appliances Topology › Appliances
Save to Disk
New Group
New Appliance
Remove Selected
Move Selected
Filter
Appliance Operations
Migrate Appliances to Sites
Push
Cancel
OK

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

Push policies and appliance pages to the selected appliances.

- □ Include Path Selection, QoS, and Applications (RiOS 9.0 and later); Web Proxy and Application Stats Collection (RiOS 9.1 and later)
- □ Restart Optimization Service If Required
- □ Restart QoS Service If Required
- □ Schedule Deferred Push

Date and Time: 2020/01/30 1

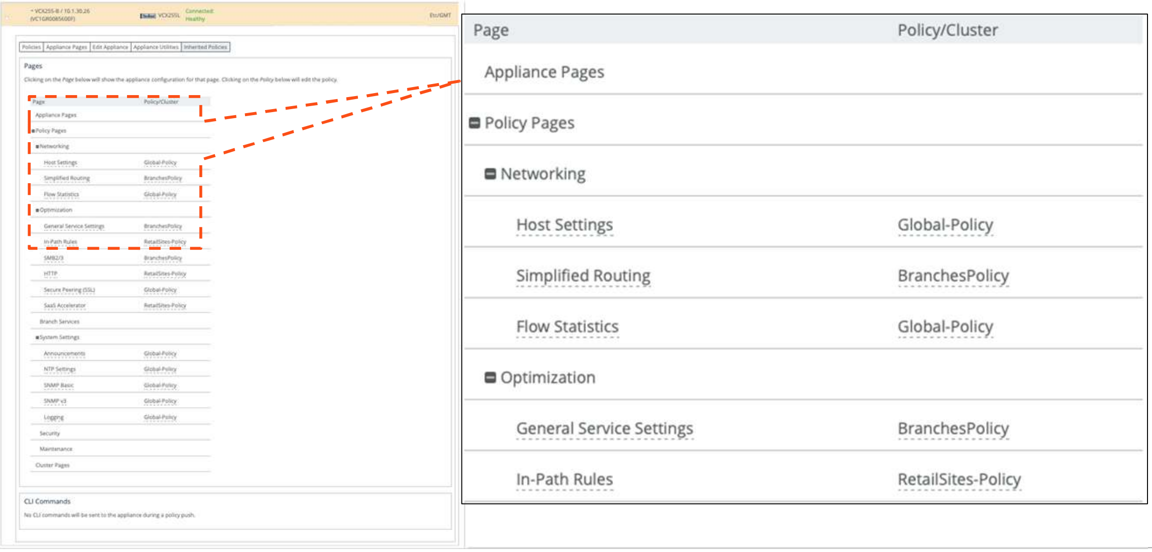
(Note that this operation only applies

You are about to push policies to 2 appliances.

□ Groups and Managed Appliances					Site	Time Zone
□ Global				Global Path Selection, Global QoS, Global Web Proxy, Global Application Stats Collection, Global-Policy		
□ Branches				BranchesPolicy		
□ DistributionCenters						
□ RetailSites				RetailSites-Policy		
□ VCX255-B / 10.1.30.26 (VC1GR0085600F)	SteelHead VCX255L	Connected: Critical	≠			Etc/GMT
□ DataCenter				DC-Policy		
□ VCX255-A / 10.1.30.25 (VC1HX0085600E)	SteelHead VCX255L	Connected: Critical	≠			Etc/GMT

This would be a scary moment if you were not sure what was being pushed. You can check by using the twisty on the individual appliances.

Config Mgmt – Appliance > Policy Inheritance Page



• VCX255-B / 10.1.30.26 (VC1GR00085600F) Global VCX255L Connected: Healthy Etc/GMT

Pages

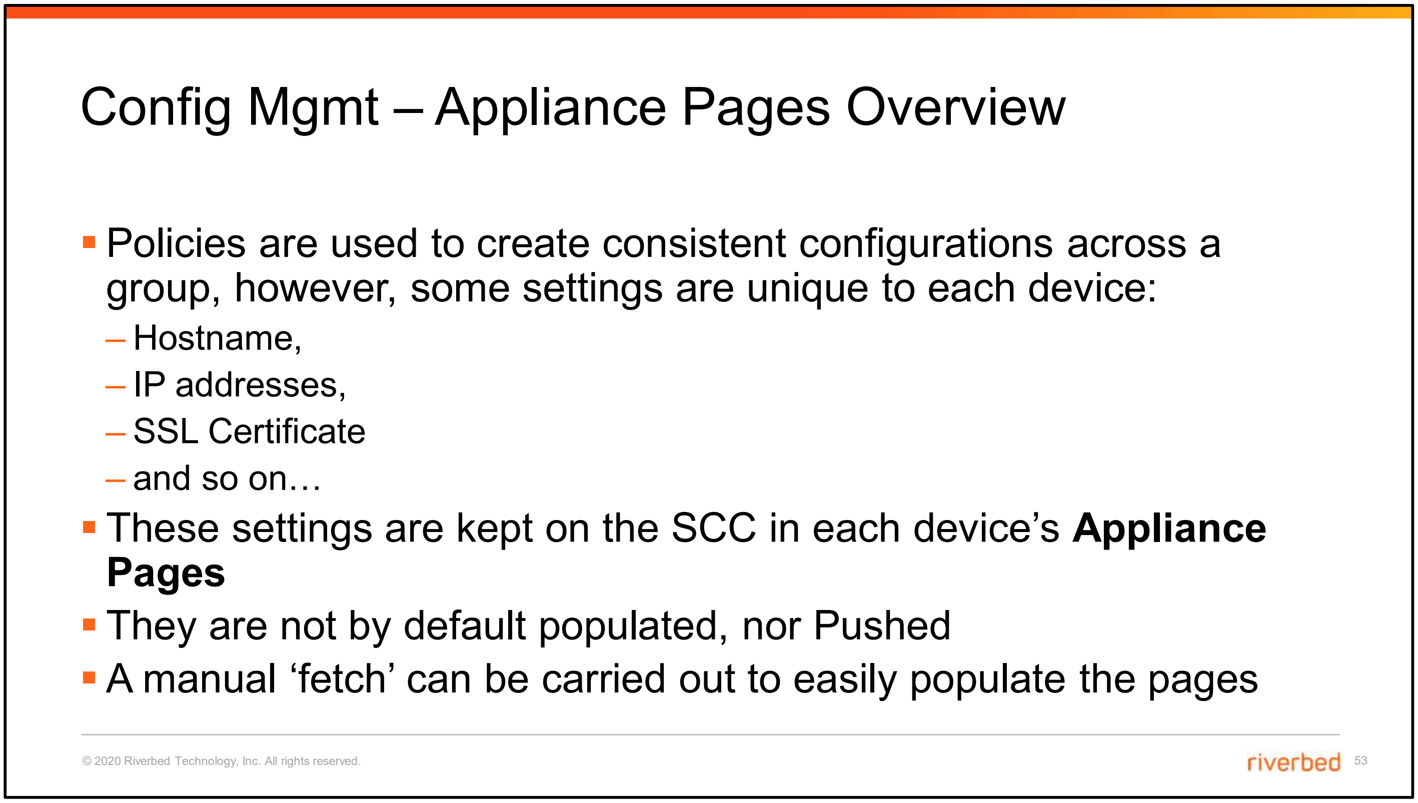
Clicking on the *Page* below will show the appliance configuration for that page. Clicking on the *Policy* below will edit the policy.

Page	Policy/Cluster
Appliance Pages	
■ Policy Pages	
■ Networking	
Host Settings	Global-Policy
Simplified Routing	BranchesPolicy
Flow Statistics	Global-Policy
■ Optimization	
General Service Settings	BranchesPolicy
In-Path Rules	RetailSites-Policy
SMB2/3	BranchesPolicy
HTTP	RetailSites-Policy
Secure Peering (SSL)	Global-Policy
SaaS Accelerator	RetailSites-Policy
Branch Services	
■ System Settings	
Announcements	Global-Policy
NTP Settings	Global-Policy
SNMP Basic	Global-Policy
SNMP v3	Global-Policy
Logging	Global-Policy
Security	
Maintenance	
Cluster Pages	

CLI Commands

No CLI commands will be sent to the appliance during a policy push.

Page	Policy/Cluster
Appliance Pages	
⊟ Policy Pages	
⊟ Networking	
Host Settings	Global-Policy
Simplified Routing	BranchesPolicy
Flow Statistics	Global-Policy
⊟ Optimization	
General Service Settings	BranchesPolicy
In-Path Rules	RetailSites-Policy

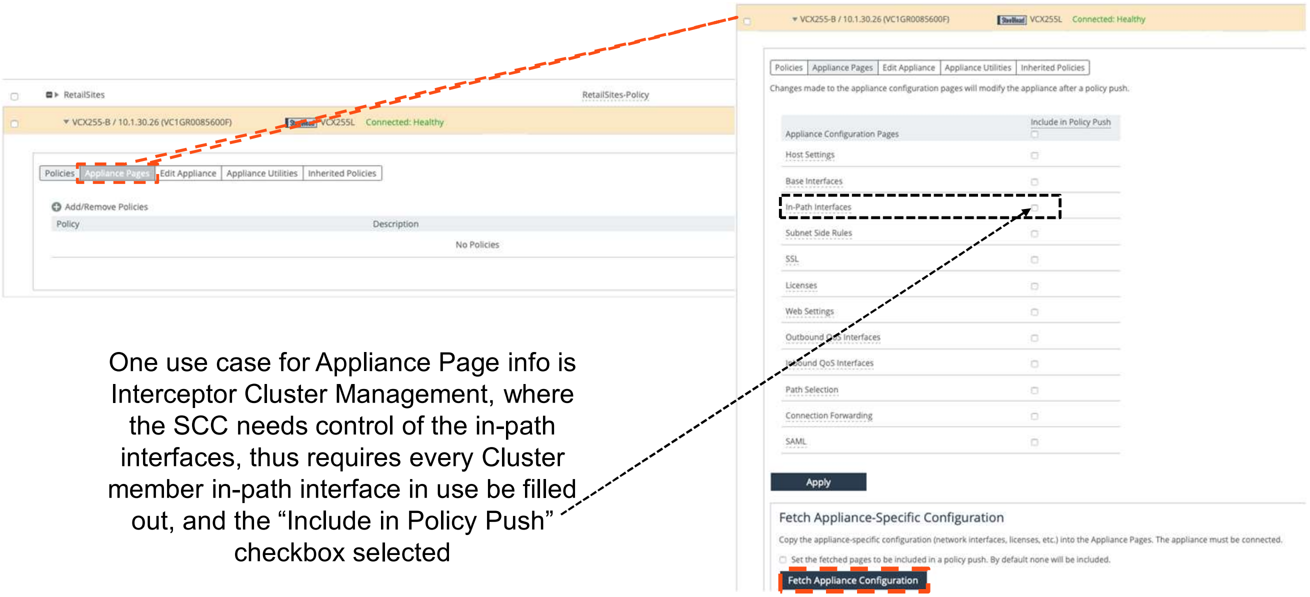


Config Mgmt – Appliance Pages Overview

- Policies are used to create consistent configurations across a group, however, some settings are unique to each device:
  - Hostname,
  - IP addresses,
  - SSL Certificate
  - and so on…
- These settings are kept on the SCC in each device's **Appliance Pages**
- They are not by default populated, nor Pushed
- A manual 'fetch' can be carried out to easily populate the pages

riverbed 53

Config Mgmt – Appliance Pages GUI



□ RetailSites RetailSites-Policy

□ ▾ VCX255-B / 10.1.30.26 (VC1GR0085600F) SteelHead VCX255L Connected: Healthy

Policy	Description
No Policies	

□ ▾ VCX255-B / 10.1.30.26 (VC1GR0085600F) SteelHead VCX255L Connected: Healthy

Changes made to the appliance configuration pages will modify the appliance after a policy push.

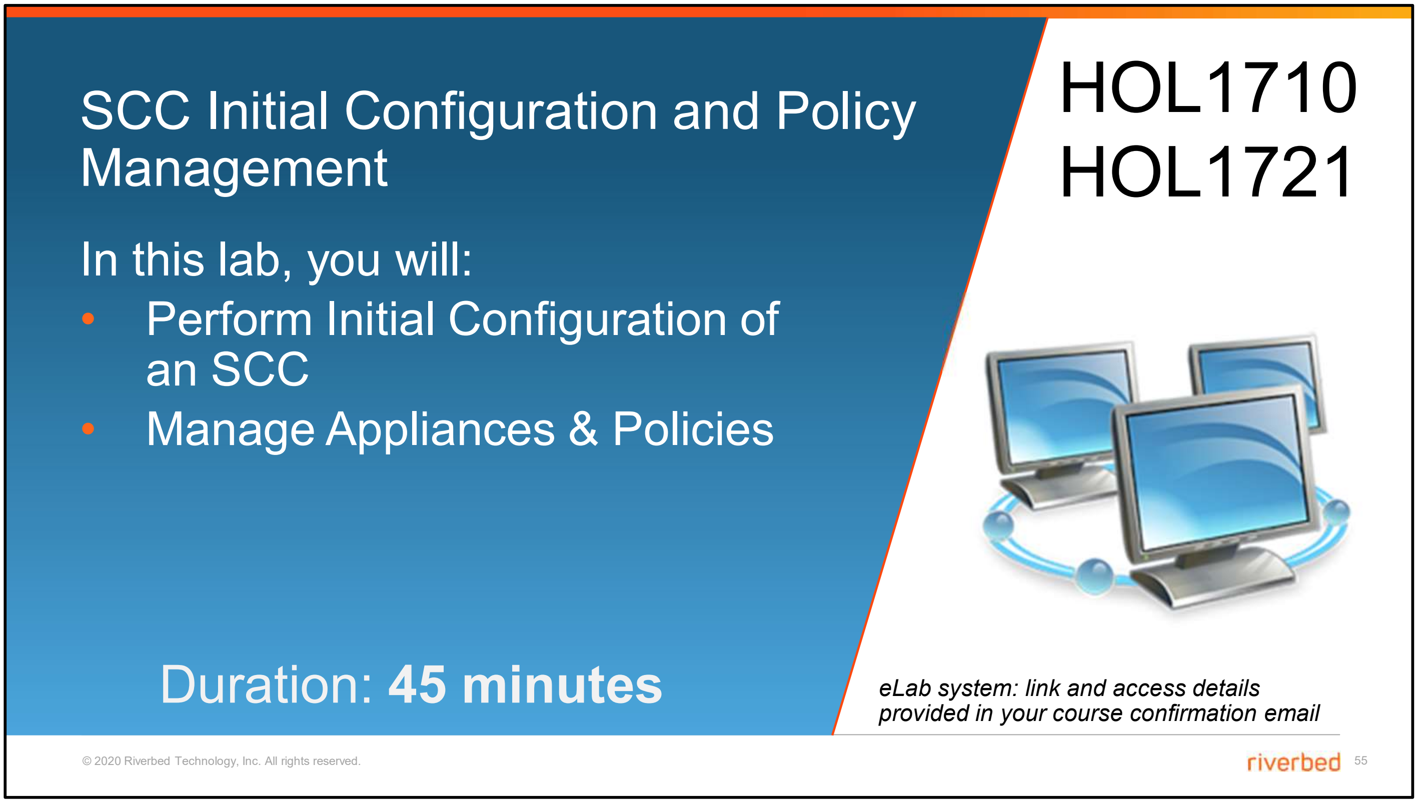
Appliance Configuration Pages	Include in Policy Push □
Host Settings	□
Base Interfaces	□
In-Path Interfaces	□
Subnet Side Rules	□
SSL	□
Licenses	□
Web Settings	□
Outbound QoS Interfaces	□
Inbound QoS Interfaces	□
Path Selection	□
Connection Forwarding	□
SAML	□

Fetch Appliance-Specific Configuration

Copy the appliance-specific configuration (network interfaces, licenses, etc.) into the Appliance Pages. The appliance must be connected.

□ Set the fetched pages to be included in a policy push. By default none will be included.

One use case for Appliance Page info is Interceptor Cluster Management, where the SCC needs control of the in-path interfaces, thus requires every Cluster member in-path interface in use be filled out, and the “Include in Policy Push” checkbox selected



SCC Initial Configuration and Policy Management

HOL1710
HOL1721

In this lab, you will:

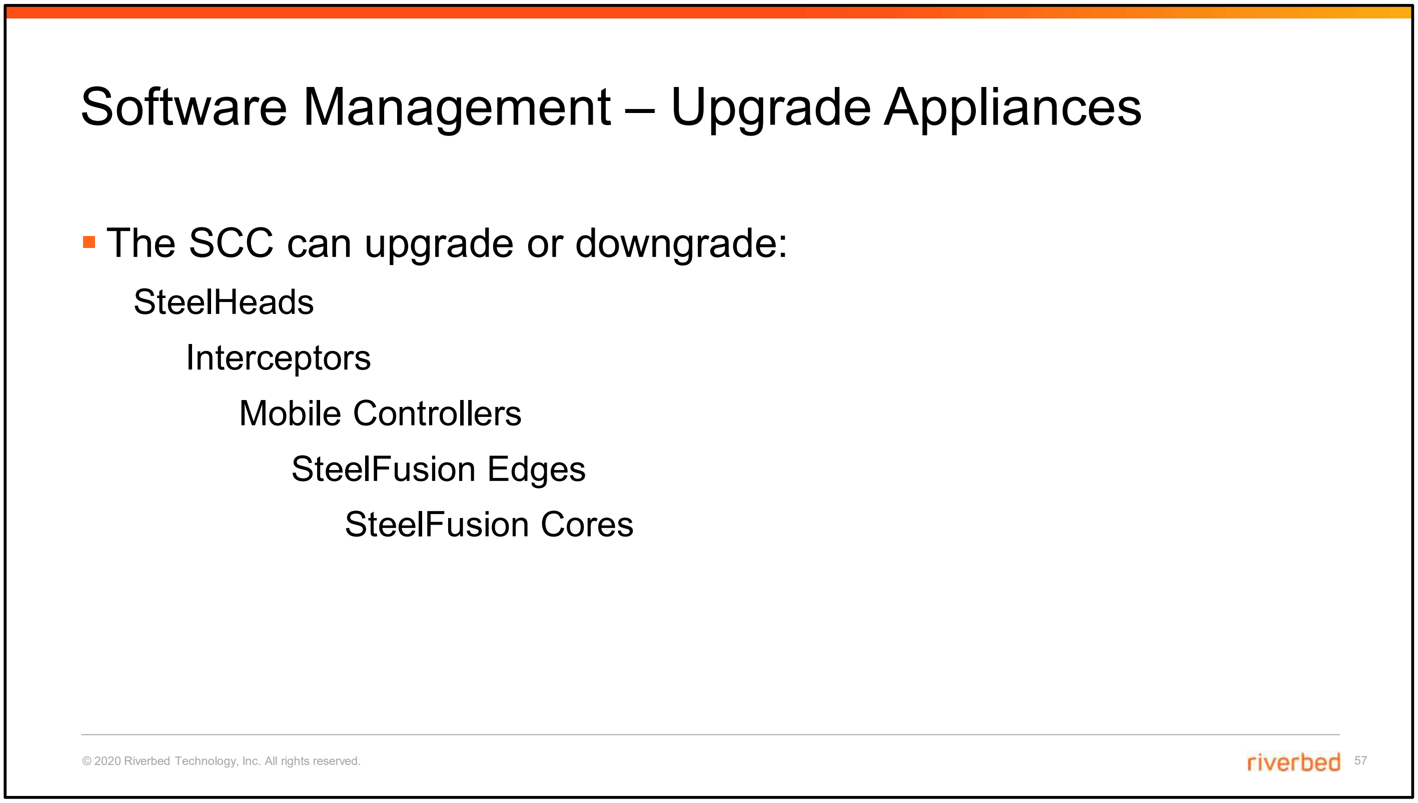
- Perform Initial Configuration of an SCC
- Manage Appliances & Policies

Duration: **45 minutes**

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

riverbed 55

Manage Your Software with the SCC



Software Management – Upgrade Appliances

- The SCC can upgrade or downgrade:

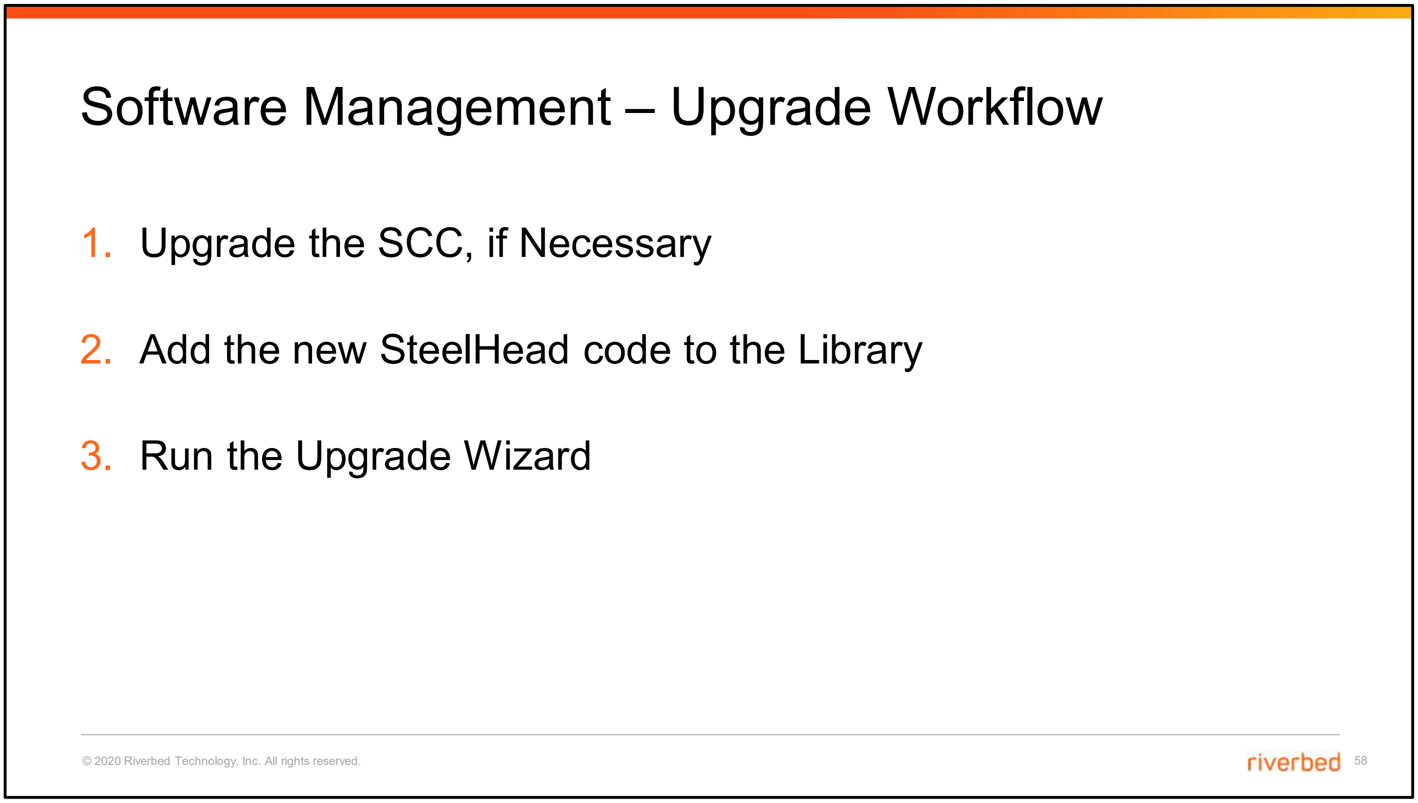
SteelHeads

Interceptors

Mobile Controllers

SteelFusion Edges

SteelFusion Cores



Software Management – Upgrade Workflow

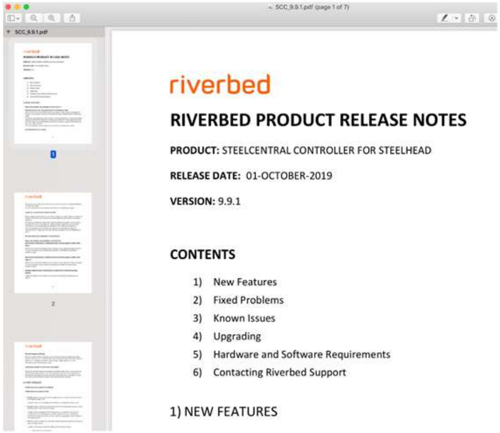
1. Upgrade the SCC, if Necessary

2. Add the new SteelHead code to the Library

3. Run the Upgrade Wizard

Software Management – Obtain SCC Upgrade Image

- This procedure is the same for all RiOS devices
- Visit the Support Website
- Go to appliance (SCC, in this case)
- Download the code and check the Release Notes



riverbed

RIVERBED PRODUCT RELEASE NOTES

PRODUCT: STEELCENTRAL CONTROLLER FOR STEELHEAD

RELEASE DATE: 01-OCTOBER-2019

VERSION: 9.9.1

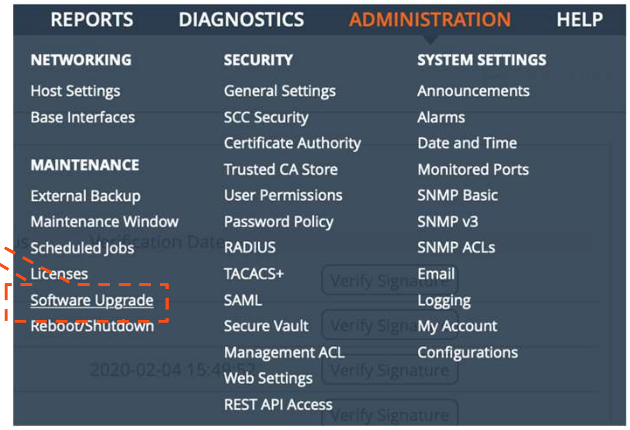
CONTENTS

1) New Features
2) Fixed Problems
3) Known Issues
4) Upgrading
5) Hardware and Software Requirements
6) Contacting Riverbed Support

1) NEW FEATURES

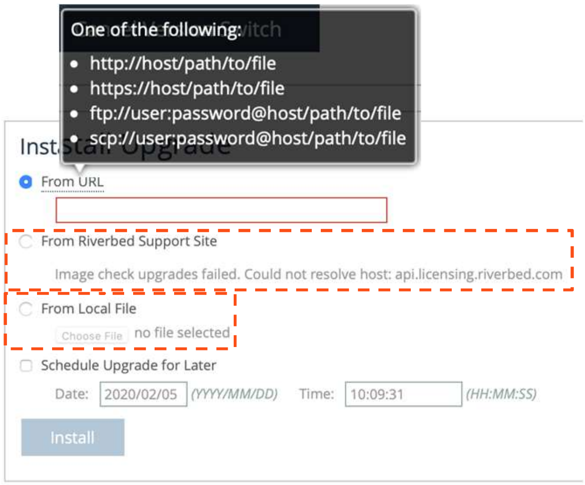
Software Management – Access SCC Upgrade Page

- Logon to the SCC and select **Software Upgrade** under Administration.



Software Management – Options to Download Code

- "From Local File", if you are doing the upgrade locally from your workstation.
- "From URL", if your image is on a networked Server.
- "From Riverbed Support Site"; the SCC (or any RiOS device) can 'call home', if it has Internet access.
- Choose the file and press **Install** when ready, then reboot.



One of the following:

- http://host/path/to/file
- https://host/path/to/file
- ftp://user:password@host/path/to/file
- scp://user:password@host/path/to/file

Install Upgrade

● From URL

○ From Riverbed Support Site

Image check upgrades failed. Could not resolve host: api.licensing.riverbed.com

○ From Local File

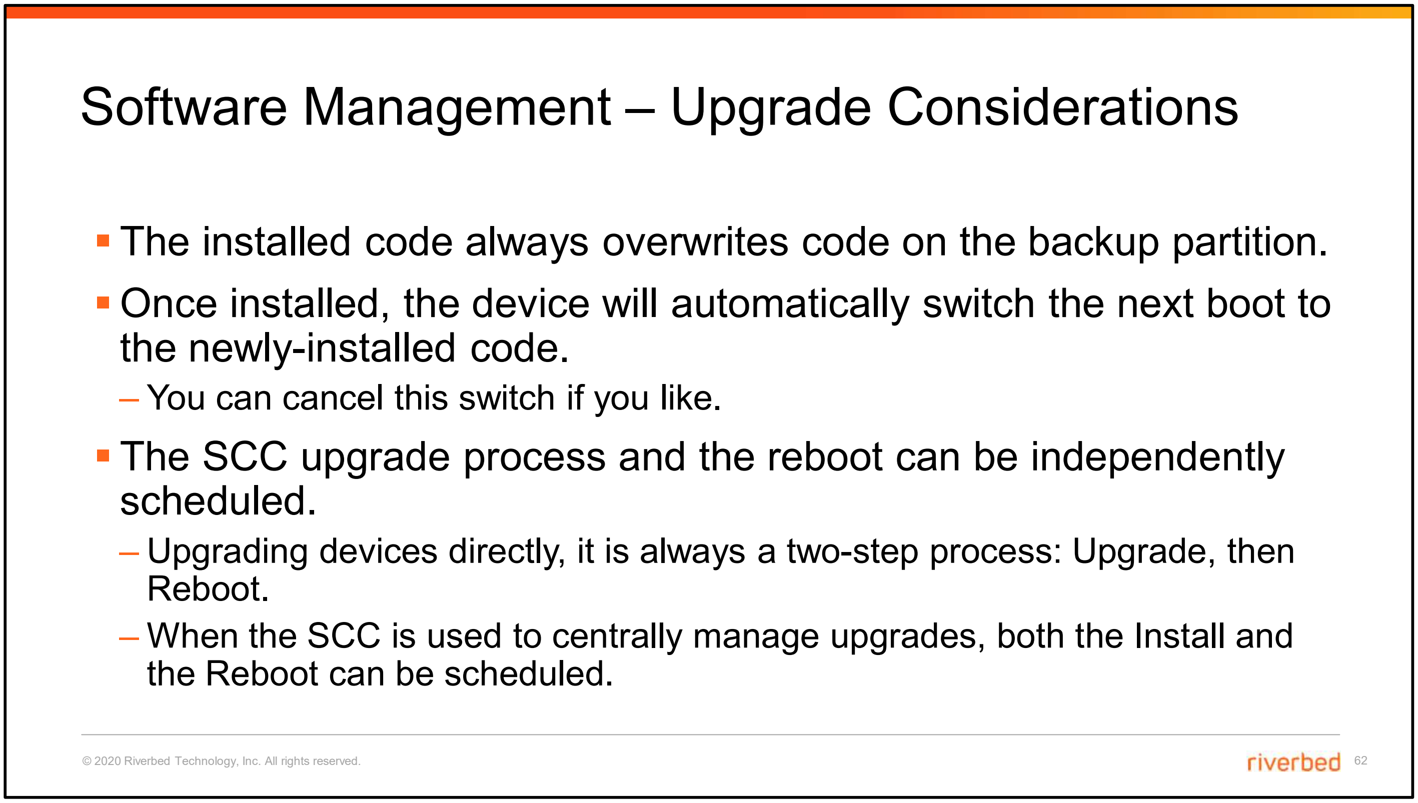
Choose File no file selected

□ Schedule Upgrade for Later

Date: 2020/02/05 (YYYY/MM/DD) Time: 10:09:31 (HH:MM:SS)

You can upgrade or revert to a backup version of the software in the Software Upgrade page. The bottom of the page displays the software version history, including the version number and the software installation date.

To find allowed upgrades between RiOS versions and recommended upgrade paths, use the Software Upgrade tool on the Riverbed Support site at https://support.riverbed.com. The tool includes all of the
recommended intermediate RiOS versions.

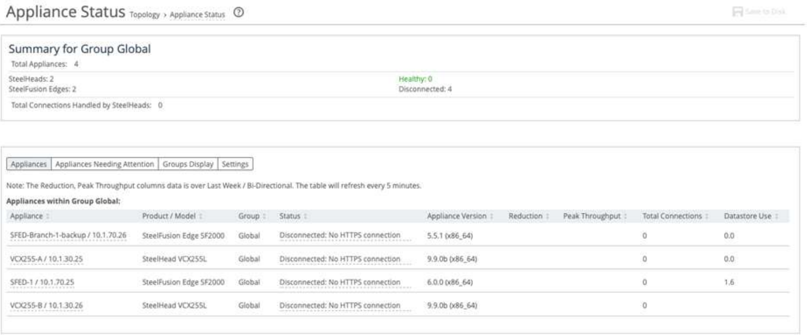


Software Management – Upgrade Considerations

- The installed code always overwrites code on the backup partition.
- Once installed, the device will automatically switch the next boot to the newly-installed code.
  - You can cancel this switch if you like.
- The SCC upgrade process and the reboot can be independently scheduled.
  - Upgrading devices directly, it is always a two-step process: Upgrade, then Reboot.
  - When the SCC is used to centrally manage upgrades, both the Install and the Reboot can be scheduled.

Software Management – Upgrade Appliances with SCC

- Wizard-driven process for upgrade and downgrade
- Strict rules apply when downgrading
- The Appliance Status Report shows the code that your appliances are currently running



Appliance Status Topology › Appliance Status

Summary for Group Global

Total Appliances: 4

SteelHeads: 2
SteelFusion Edges: 2

Healthy: 0
Disconnected: 4

Total Connections Handled by SteelHeads: 0

Appliances | Appliances Needing Attention | Groups Display | Settings

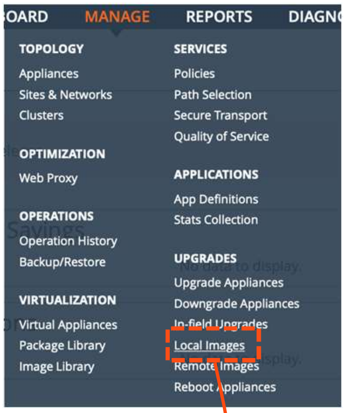
Note: The Reduction, Peak Throughput columns data is over Last Week / Bi-Directional. The table will refresh every 5 minutes.

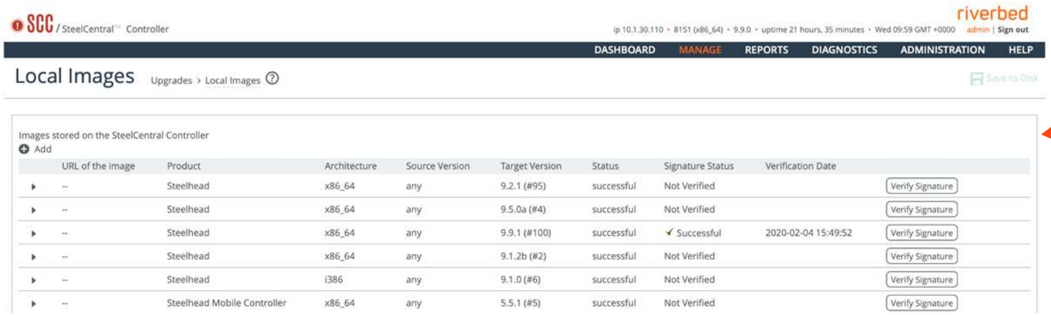
Appliances within Group Global:

Appliance	Product / Model	Group	Status	Appliance Version	Reduction	Peak Throughput	Total Connections	Datastore Use
SFED-Branch-1-backup / 10.1.70.26	SteelFusion Edge SF2000	Global	Disconnected: No HTTPS connection	5.5.1 (x86_64)			0	0.0
VCX255-A / 10.1.30.25	SteelHead VCX255L	Global	Disconnected: No HTTPS connection	9.9.0b (x86_64)			0	0.0
SFED-1 / 10.1.70.25	SteelFusion Edge SF2000	Global	Disconnected: No HTTPS connection	6.0.0 (x86_64)			0	1.6
VCX255-B / 10.1.30.26	SteelHead VCX255L	Global	Disconnected: No HTTPS connection	9.9.0b (x86_64)			0	

Software Management - SCC Library

- For configuration of SteelHeads, the SCC must be equal or newer in release, check the release notes
- The SCC has a library of code images, and knows which images are valid for each appliance




SCC / SteelCentral™ Controller
riverbed
ip 10.1.30.110 • 8151 (x86_64) • 9.9.0 • uptime 21 hours, 35 minutes • Wed 09:59 GMT +0000 admin | Sign out
DASHBOARD
MANAGE
REPORTS
DIAGNOSTICS
ADMINISTRATION
HELP
Save to Disk

Local Images Upgrades › Local Images

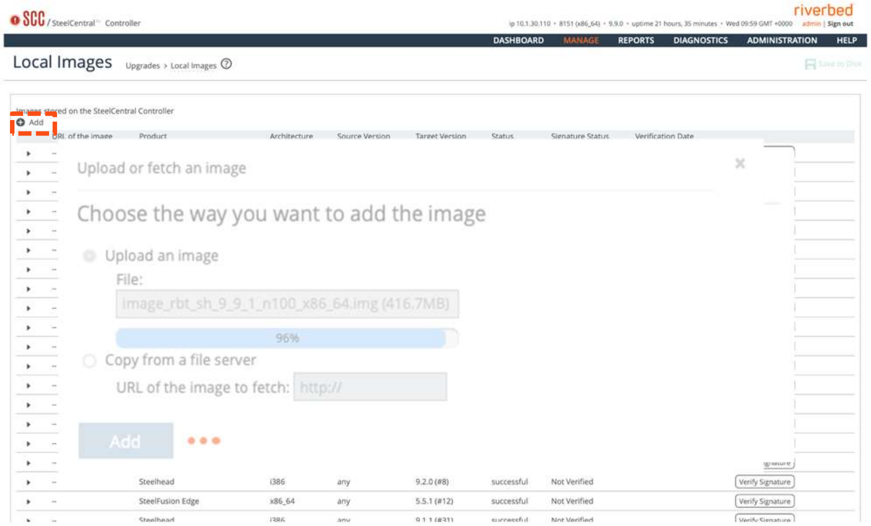
Images stored on the SteelCentral Controller

Add

	URL of the image	Product	Architecture	Source Version	Target Version	Status	Signature Status	Verification Date	
▸	--	Steelhead	x86_64	any	9.2.1 (#95)	successful	Not Verified		Verify Signature
▸	--	Steelhead	x86_64	any	9.5.0a (#4)	successful	Not Verified		Verify Signature
▸	--	Steelhead	x86_64	any	9.9.1 (#100)	successful	✓ Successful	2020-02-04 15:49:52	Verify Signature
▸	--	Steelhead	x86_64	any	9.1.2b (#2)	successful	Not Verified		Verify Signature
▸	--	Steelhead	i386	any	9.1.0 (#6)	successful	Not Verified		Verify Signature
▸	--	Steelhead Mobile Controller	x86_64	any	5.5.1 (#5)	successful	Not Verified		Verify Signature

riverbed 64

Software Management – Add Image to the Library


SCC / SteelCentral Controller
riverbed
ip 10.1.30.110 • 8151 (x86_64) • 9.9.0 • uptime 21 hours, 35 minutes • Wed 09:59 GMT +0000 admin | Sign out
DASHBOARD
MANAGE
REPORTS
DIAGNOSTICS
ADMINISTRATION
HELP
Save to Disk

Local Images Upgrades > Local Images

Images stored on the SteelCentral Controller

Add

Upload or fetch an image

Choose the way you want to add the image

○ Upload an image

File: image_rbt_sh_9_9_1_n100_x86_64.img (416.7MB)

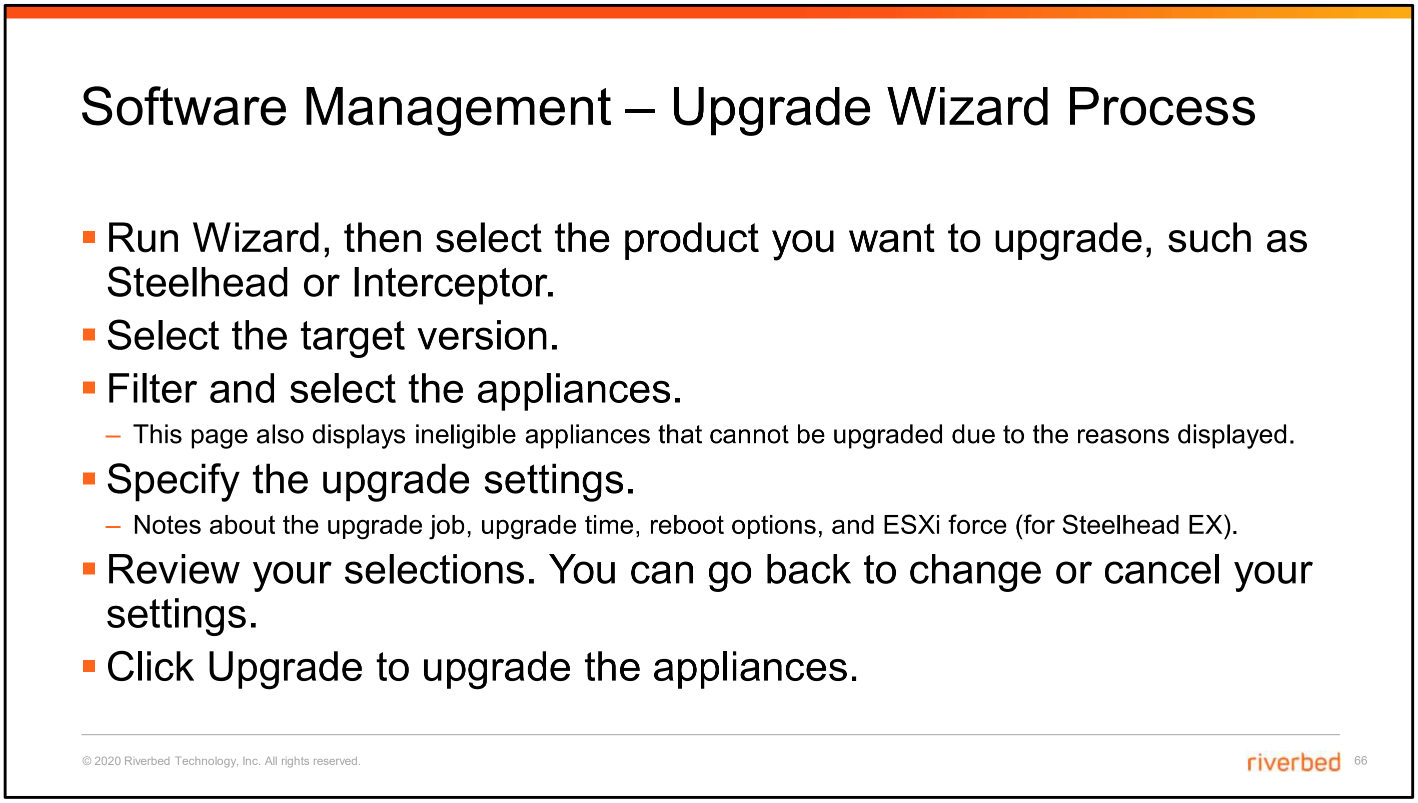
96%

○ Copy from a file server

URL of the image to fetch: http://

Add

URL of the image	Product	Architecture	Source Version	Target Version	Status	Signature Status	Verification Date	
–	Steelhead	i386	any	9.2.0 (#8)	successful	Not Verified		Verify Signature
–	SteelFusion Edge	x86_64	any	5.5.1 (#12)	successful	Not Verified		Verify Signature
–	Steelhead	i386	any	9.1.1 (#31)	successful	Not Verified		Verify Signature

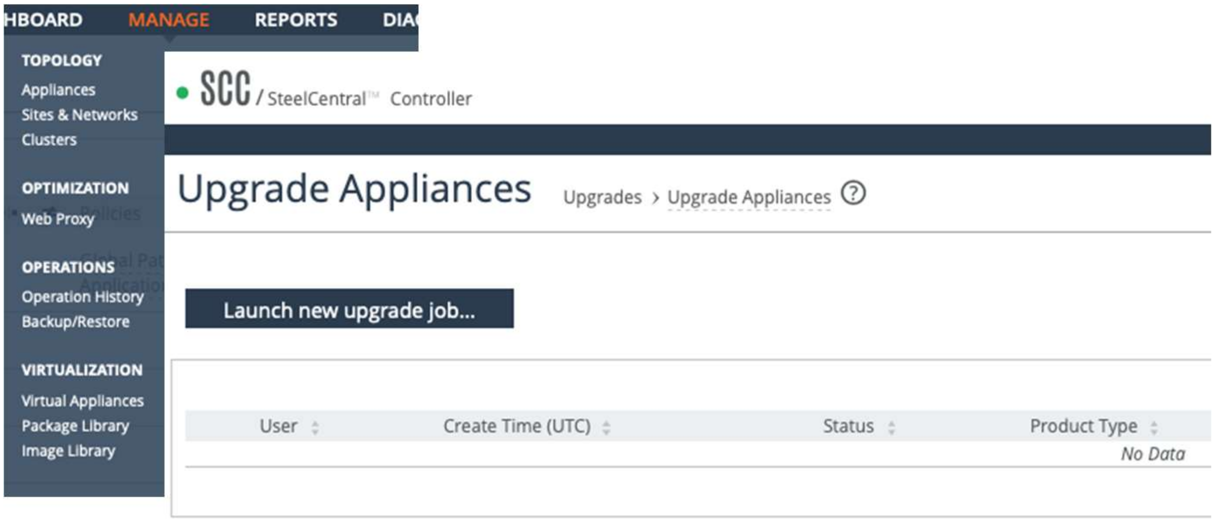


Software Management – Upgrade Wizard Process

- Run Wizard, then select the product you want to upgrade, such as Steelhead or Interceptor.
- Select the target version.
- Filter and select the appliances.
  - This page also displays ineligible appliances that cannot be upgraded due to the reasons displayed.
- Specify the upgrade settings.
  - Notes about the upgrade job, upgrade time, reboot options, and ESXi force (for Steelhead EX).
- Review your selections. You can go back to change or cancel your settings.
- Click Upgrade to upgrade the appliances.

riverbed 66

Software Management – Run the Upgrade Wizard

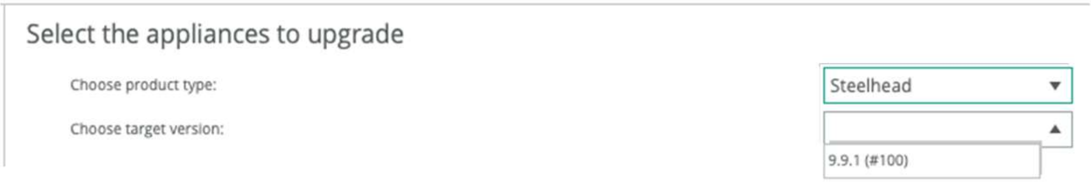


User	Create Time (UTC)	Status	Product Type
			No Data

riverbed 67

Software Management – Select Appliance Type

- Once selected the code can be chosen
- The SCC knows current the versions of the appliances
- It will only show the valid code in the list



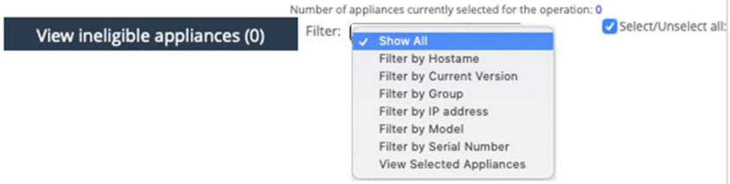
Select the appliances to upgrade

Choose product type: Steelhead

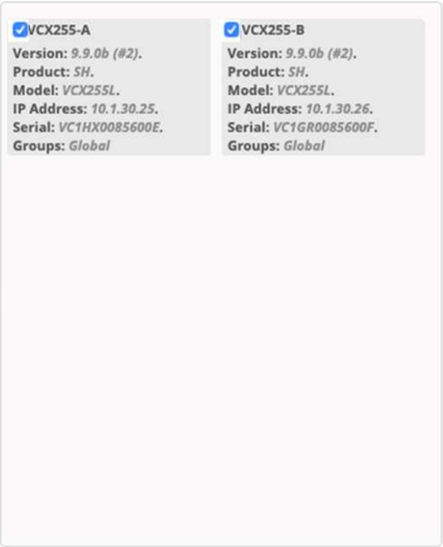
Choose target version: 9.9.1 (#100)

Software Management – Choose Your Appliances

- Only eligible appliances are listed
- If it's a large number, you can filter the list



Number of appliances currently selected for the operation: 0



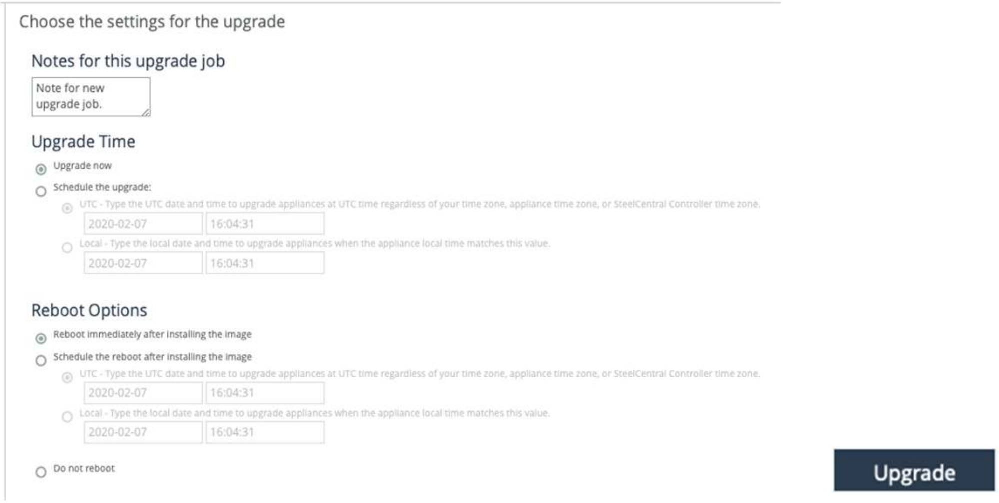
☑ VCX255-A

Version: 9.9.0b (#2).
Product: SH.
Model: VCX255L.
IP Address: 10.1.30.25.
Serial: VC1HX0085600E.
Groups: Global

☑ VCX255-B

Version: 9.9.0b (#2).
Product: SH.
Model: VCX255L.
IP Address: 10.1.30.26.
Serial: VC1GR0085600F.
Groups: Global

Software Management – Choose Upgrade Settings



Choose the settings for the upgrade

Notes for this upgrade job

Note for new upgrade job.

Upgrade Time

● Upgrade now

○ Schedule the upgrade:

● UTC - Type the UTC date and time to upgrade appliances at UTC time regardless of your time zone, appliance time zone, or SteelCentral Controller time zone.

2020-02-07 16:04:31

○ Local - Type the local date and time to upgrade appliances when the appliance local time matches this value.

2020-02-07 16:04:31

Reboot Options

● Reboot immediately after installing the image

○ Schedule the reboot after installing the image

● UTC - Type the UTC date and time to upgrade appliances at UTC time regardless of your time zone, appliance time zone, or SteelCentral Controller time zone.

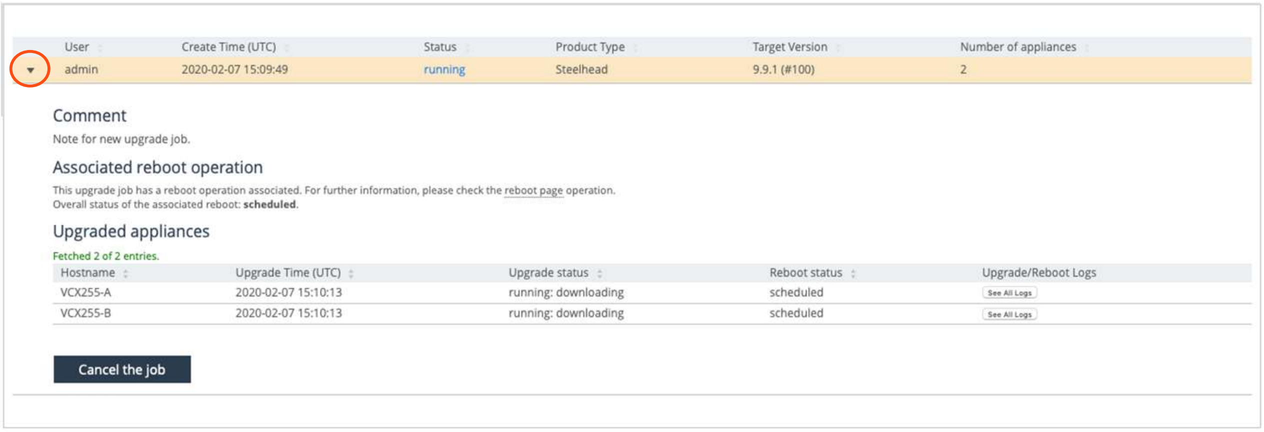
2020-02-07 16:04:31

○ Local - Type the local date and time to upgrade appliances when the appliance local time matches this value.

2020-02-07 16:04:31

○ Do not reboot

Software Management – View Upgrade Status



User	Create Time (UTC)	Status	Product Type	Target Version	Number of appliances
admin	2020-02-07 15:09:49	running	Steelhead	9.9.1 (#100)	2

Comment

Note for new upgrade job.

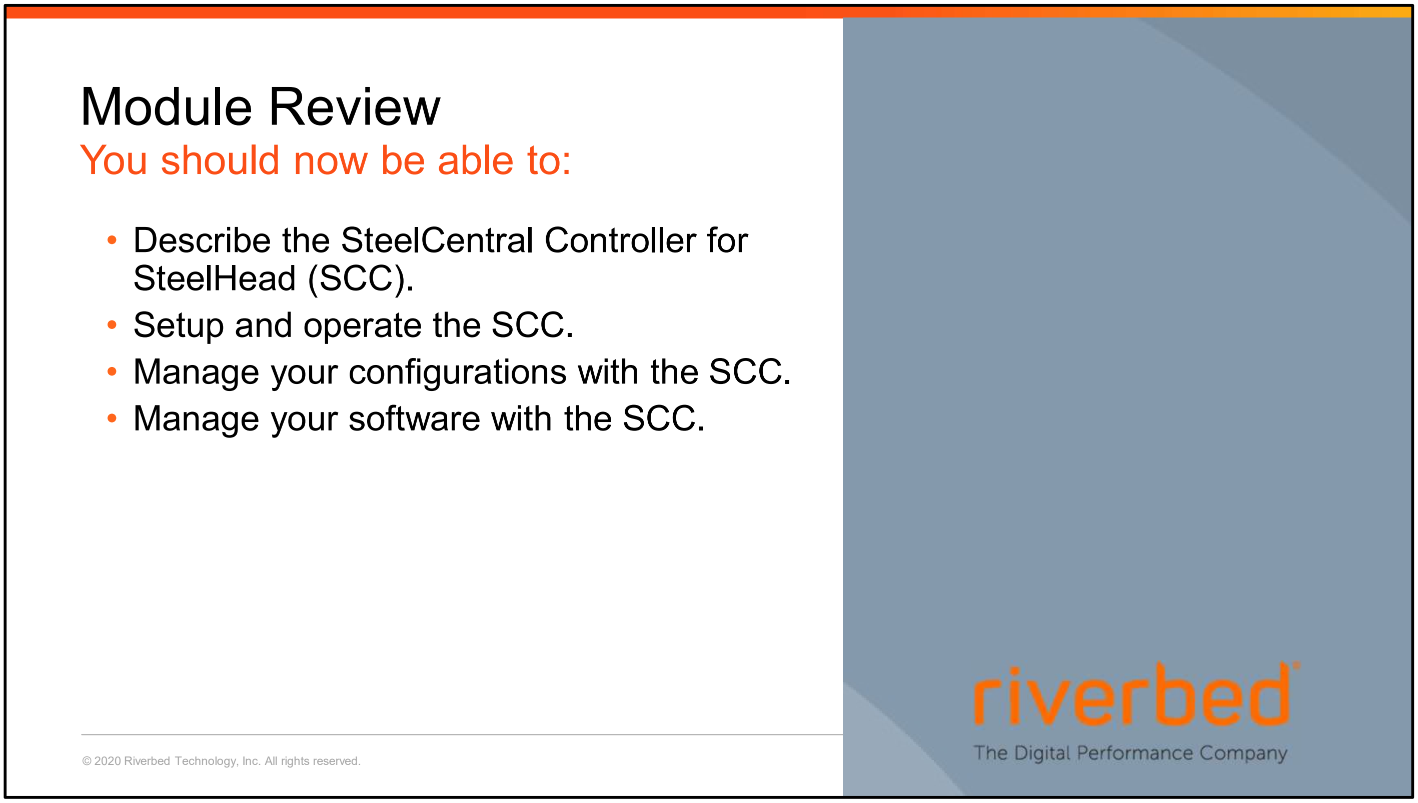
Associated reboot operation

This upgrade job has a reboot operation associated. For further information, please check the reboot page operation.
Overall status of the associated reboot: **scheduled**.

Upgraded appliances

Fetched 2 of 2 entries.

Hostname	Upgrade Time (UTC)	Upgrade status	Reboot status	Upgrade/Reboot Logs
VCX255-A	2020-02-07 15:10:13	running: downloading	scheduled	See All Logs
VCX255-B	2020-02-07 15:10:13	running: downloading	scheduled	See All Logs



Module Review

You should now be able to:

- Describe the SteelCentral Controller for SteelHead (SCC).
- Setup and operate the SCC.
- Manage your configurations with the SCC.
- Manage your software with the SCC.

The Digital Performance Company