SteelCentral Controller for SteelHead Installation Guide

Version 9.0

December 2014

riverbed®

Riverbed Technology
680 Folsom Street
San Francisco, CA 94107

Phone: 415.247.8800
Fax: 415.247.8801
Web: http://www.riverbed.com

Part Number
712-00117-15

Contents

Preface

Welcome to the *SteelCentral Controller for SteelHead Installation Guide*. Read this preface for the documentation conventions, additional reading, and contact information. This preface includes the following sections:

About This Guide

This guide describes how to install and configure the SteelCentral Controller for SteelHead (SCC).

This guide includes information relevant to the following products:

- Riverbed SteelCentral Controller for SteelHead (SCC)
- Riverbed SteelHead (SteelHead)
- Riverbed SteelHead CX (SteelHead CX)
- Riverbed SteelHead EX (SteelHead EX)
- Riverbed SteelHead Mobile (SteelHead Mobile)
- Riverbed SteelHead Interceptor (SteelHead Interceptor)
- Riverbed Granite Core/SteelFusion Core (Granite Core/SteelFusion Core)
- Riverbed Granite Edge/SteelFusion Edge (Granite Edge/SteelFusion Edge)
- Riverbed Optimization System (RiOS)

Audience

This guide is written for storage and network administrators who are familiar with administering and managing WANs using common network protocols such as TCP, CIFS, HTTP, FTP, and NFS.

Document Conventions

This table summarizes the document conventions used in this guide.

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

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

< >	Values that you specify appear in angle brackets: **interface <ip-address>**
[ ]	Optional keywords or variables appear in brackets: **ntp peer <ip-address> [version <number>]**
{ }	Elements that are part of a required choice appear in braces: **{<interface-name> | ascii <string> | hex <string>}**
|	The pipe symbol represents a choice to select one keyword or variable to the left or right of the symbol. The keyword or variable can be either optional or required: **{delete <filename> | upload <filename>}**

Safety Guidelines

Follow the safety precautions outlined in the *Safety and Compliance Guide* when installing and setting up your equipment.

Important: Failure to follow these safety guidelines can result in injury or damage to the equipment. Mishandling of the equipment voids all warranties. Read and follow safety guidelines and installation instructions carefully.

Many countries require the safety information to be presented in their national languages. If this requirement applies to your country, consult the *Safety and Compliance Guide*. Before you install, operate, or service the Riverbed products, you must be familiar with the safety information. Refer to the *Safety and Compliance Guide* if you do not clearly understand the safety information provided in the product documentation.

Contacting Riverbed

This section describes how to contact departments within Riverbed.

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

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

CHAPTER 1 Product Overview

This chapter provides hardware and software requirements, new features, and upgrade instructions. It includes the following sections:

Hardware and Software Dependencies

This section provides information about product dependencies and compatibility.

Hardware and Software Requirements

The following tables summarize the hardware and software requirements for the SCC.

SCC Component	Hardware and Software Requirements
SCC appliance	19-inch (483 mm) two or four-post rack.
SCC Web Interface	Any computer that supports a Web browser with a color image display. The SCC has been tested with Mozilla Firefox Extended Support Release (ESR) v24.0 and Microsoft Internet Explorer (IE) v9.0. When you upgrade to v9.0, clear the browser cache and cookies to ensure the user interface displays correctly. JavaScript and cookies must be enabled in your Web browser.

SCC v9.0 Product Support

SCC supports the following Riverbed products and software versions.

Product	Required Software Version	SCC Feature Support
SteelHead CX	Version 8.0 or higher	Configuration and monitoring support. SCC v9.0 requires you to migrate legacy QoS policies. You must reconfigure your path selection rules in v9.0.
SteelHead EX	Version 3.6 or higher	Configuration and monitoring support.
SteelHead Interceptor	Version 3.x or higher	Configuration and monitoring support. Pushing configurations to appliances is limited to XBridge, system settings, security settings, and in-path and load balancing rules for clusters.
SteelHead Mobile	Version 4.0 or higher	Monitoring only.
SteelFusion Core	Version 2.5 or higher	Monitoring only.
SteelStore	Version 3.0 or higher	Monitoring only.

SteelHead Compatibility

The SteelHead has been tested with the following SCC software versions:

SteelHead RiOS Version	Recommended Version	SCC Appliance v8.6.x	SCC Appliance v8.5.x	SCC Appliance v8.0.x
SteelHead v9.0	SCC v9.0	Parity	Parity	Not supported
SteelHead v8.6 SteelHead CX v8.6 SteelHead EX v3.5	SCC v8.6	Parity	Parity	Not supported
SteelHead v8.5.x SteelHead CX v8.5.x SteelHead EX v2.5.x	SCC v8.5.x	Parity	Parity	Not supported
SteelHead v8.0.x SteelHead CX v8.0.x SteelHead EX v2.1.x SteelHead EX v2.0.x	SCC v8.5.x; Edge High Availability only for SteelHead EX v2.0 or later	Parity	Parity	Parity

Version 9.0 Legacy Policy Push Restrictions

This table summarizes the legacy policy push restrictions in SCC v9.0.x.Theses restrictions only apply to policies configured with software versions prior SCC v9.0.x.

SCC Feature	SteelHead CX Software	SteelHead EX Software	SteelHead Interceptor
Outbound QoS (Basic)	v8.0.x only supported v9.0 or higher not supported	v2.0.x only supported v3.6.x or higher not supported	—
Outbound QoS (Advanced)	v8.0.x only supported v9.0 or higher not supported	v2.0.x only supported v3.6.x or higher not supported	—
Outbound QoS Interfaces	v9.0 or higher not supported	v3.6.x or higher not supported	—
Inbound QoS	v9.0 or higher not supported	v3.6.x or higher not supported	—
Inbound QoS Interfaces	v9.0 or higher not supported	v3.6.x or higher not supported	—
Path Selection (legacy)	v8.0.x not supported v9.0 or higher not supported	v2.0.x not supported v3.6.x or higher not supported	—
Host Labels	v8.0.x not supported	v2.0.x not supported	—
SnapMirror	v8.0.x not supported	v2.0.x not supported	—
REST API Access	v8.0.x not supported	v2.0.x not supported	—
Management ACL			v3.x.x not supported

Firewall Requirements

For the SCC CLI, port 22 must be passed through for the firewall to function properly.

Because optimization between SteelHeads typically takes place over a secure WAN, it is not necessary to configure company firewalls to support SteelHead specific ports. If there are one or more firewalls between two SteelHeads, ports 7800 and 7810, must be passed through firewall devices located between the pair of SteelHeads. Also, SYN and SYN/ACK packets with the TCP option 76 must be passed through firewalls for auto-discovery to function properly.

SNMP-Based Management Compatibility

This product supports a proprietary Riverbed MIB accessible through SNMP. SNMPv1 (RFCs 1155, 1157, 1212, and 1215), SNMPv2c (RFCs 1901, 2578, 2579, 2580, 3416, 3417, and 3418), and SNMPv3 are supported, although some MIB items might only be accessible through SNMPv2 and SNMPv3.

SNMP support enables the product to be integrated into network management systems such as Hewlett-Packard OpenView Network Node Manager, BMC Patrol, and other SNMP-based network management tools.

New Features in SCC v9.0

SCC v9.0 delivers an application-centric approach to optimizing and managing appliances. It delivers new centralized, business-intent-based policies and intuitive control and management of users, applications, and networks based on your business requirements.

The SCC automatically derives all network path possibilities and, based on business policies, prioritizes, secures, and delivers critical applications over the faster networks and less-critical recreational applications and bulk backups over the Internet. This solution simplifies application and path management and ensures secure service-level delivery for business critical applications. Using a wizard-like process for defining application policies based on customer business requirements, the SCC enables you to easily leverage and control hybrid networks for accelerated application delivery.

Hybrid networks typically combine private networks (MPLS links) with public networks such as the Internet. The SCC provides application-aware Quality of Service (QoS) and path selection to control network consumption and prioritize critical and latency sensitive applications, while minimizing use by noncritical applications.

The following new features are available in the SCC v9.0:

- **Sites and Site Migration** - In previous versions of the SCC, the management paradigm was appliances and appliance groups. SCC v9.0 introduces the concept of sites, networks, and uplinks to organize appliances that you are managing using the SCC. Sites use a new location property that enables you to manage your networks based on the physical location of your appliances. With defined sites, you can easily track user issues based on the location of the appliance and troubleshoot problems. Sites are an important part of path selection, QoS, and secure transport. Version 9.0 includes a migration wizard with comma separated values (CSV) import and export so that you can easily migrate appliances to sites.
- **Easy Path Selection** - Path Selection gives you fine-grained control of application traffic flow across multiple WAN circuits connecting SteelHeads at your various locations. Version 9.0 uses the concept of application groups to define path selection rules that include the global performance for an application, including the latency priority. SCC v9.0 includes a path selection setup wizard that enables you to define path selection rules for application groups, such as business bulk (file transfer applications and protocols), business critical (low latency, transactional applications and protocols), business productivity (general business-level applications and protocols), business video, and so on. (You cannot migrate your previously defined path selection rules when you upgrade to SCC v9.0. For details about creating new path selection rules, see the *SteelCentral Controller for SteelHead User's Guide*.)
- **Streamlined QoS and QoS Migration** - Version 9.0 simplifies QoS configuration, troubleshooting, and customization. It includes an improved QoS user interface to handle basic and advanced modes, including a QoS class hierarchy editor. Version 9.0 includes configuration of QoS rules based on applications and application groups and introduces the concept of QoS profiles, which replace QoS policies. QoS profiles provide a way to fine-tune QoS rules for application groups. Version 9.0 also includes a basic and advanced QoS migration wizard for migrating existing QoS policies to QoS profiles.

- **Secure Transport** - Secure transport enables simple, secure, and manageable group encryption for inter-SteelHead communication in path selection deployments. A secure transport controller is a centralized service deployed on a reachable SteelHead, configured as a controller, that controls and manages secure transport key generation, distribution of local site subnets and rekeying between secure transport peers, and uses a centralized portal for configuring and reporting. All appliances that have a securable uplink are added to a secure transport group.
- **SteelCentral AppResponse Integration** - In SteelHead-based deployments where a SteelCentral AppResponse version 9.5 appliance is present, you can use the SCC to configure the communication between the SteelHeads and the AppResponse appliances. This integrated solution provides visibility into a wide variety of issues, such as where the service delays are occurring on the network and how well the SteelHead is performing.
- **New Dashboard** - Version 9.0 includes a new dashboard that contains announcements, site status, critical appliance summaries, and an optimization savings graph. The dashboard also includes a welcome widget that describes how to migrate previous versions of the SCC to v9.0, including links to migrating appliances to sites, setting up path selection, migrating QoS profiles, and pushing configurations.
- **Context Sensitive Search Box** - Version 9.0 includes that ability to search for sites, networks, regions, applications, and uplink types. For example, you can enter a single letter, and a drop-down list displays with matches for sites, networks, regions, applications, and uplink Types.
- **Parity with SteelHead v9.0** - SCC v9.0 includes feature and configuration parity with SteelHead v9.0, including path selection, QoS, secure transport, SMB v3.0.2, and signed SMB resiliency.

Upgrading the SCC

You can upgrade SCC only to the next major version. Do not skip intermediate major versions. Multi-version upgrades and downgrades can result in database incompatibilities, potentially leading to data corruption.

Upgrade Considerations

Consider the following guidelines before upgrading SCC:

- The SCC does not support upgrades from SCC lower than v8.5. If you are running an SCC release lower than v8.5 you must perform a multi-step upgrade; that is, first upgrade to a release 8.5 or above and then to v9.0. A multi-step upgrade ensures that auto-migration of statistics occurs correctly.
- Upgrading from RiOS v8.6.x (or earlier) to v9.0 does not automatically migrate previous QoS rules to a new configuration. Version 9.0 provides a QoS migration wizard to assist you in migrating your QoS rules.
- You cannot migrate previous path selection rules from SCC v8.6.x (or earlier) to v9.0.
- If you mix RiOS software versions in your network, the releases might not fully support certain features (for example, QoS) and you cannot take full advantage of the v9.0 features that are not part of the prior software versions.

Recommended Upgrade Paths

To find allowed upgrades between software versions and recommended upgrade paths, see Riverbed Support at https://support.riverbed.com. The tool includes the recommended intermediate software versions.

- The SCC must be upgraded to v8.6 before it can be upgraded to v9.0.
- The SCC must be upgraded to v8.5 before it can be upgraded to v8.6.
- The SCC must be upgraded to v8.0 before it can be upgraded to v8.5.

If you are running a version of the SCC prior to v8.0, please contact Riverbed Support regarding acceptable upgrade paths.

Upgrading the SCC Software Version

Follow these steps to upgrade your software. These instructions assume you are familiar with the SCC, the CLI, and the SCC console.

To upgrade SCC software

1. Download the software image from Riverbed Support to a location such as your desktop.
2. Log in to the SCC using the administrator account (admin).
3. Choose Administration > Maintenance: Software Upgrade to display the Software Upgrade page.
4. Under Install Upgrade, choose one of the following options:
   - **From URL** - Type the URL that points to the software image that you want to upgrade to. Use one of these formats:

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

   - **From Riverbed Support Site** - Before you begin, make sure you have created a support account at https://support.riverbed.com. Select the target release number from the drop-down list to download a delta image directly to the appliance from the Riverbed Support site. The downloaded image includes only the incremental changes. You do not need to download the entire image. The system downloads and installs the new image immediately after you click **Install**. To download and install the image later, schedule another date or time before you click **Install**.
   - **From Local File** - Browse to your file system and select the software image.
   - **Schedule Upgrade for Later** - Type the date and time using the following format: YYYY/MM/DD HH:MM:SS.
5. Click **Install** to upgrade your SCC software.

   The software image can be quite large; uploading the image to the system can take a few minutes. Downloading a delta image directly from the Riverbed Support site is faster because the downloaded image includes only the incremental changes and is downloaded directly to the appliance.

   As the upgrade progresses, status messages appear.

   After the installation is complete, you are reminded to reboot the system to switch to the new version of the software.

6. Choose Administration > Maintenance: Reboot/Shutdown and click **Reboot**.

   The appliance can take a few minutes to reboot. This behavior is normal because the software is configuring the recovery flash device. Do not press Ctrl+C, unplug, or otherwise shut down the system during this first boot. There is no indication displayed during the system boot that the recovery flash device is being configured.

   After the reboot, the Dashboard, Software Upgrade, and Help pages in the console display the RiOS version upgrade.

Downgrading the SCC Software Version

If you are downgrading to a previous version of the RiOS software, you must downgrade to a version of the software that has previously run on your system.

Managing Licenses

You can retrieve and manage Riverbed licenses using the Riverbed Licensing Portal. After you retrieve a license key from the Riverbed Licensing Portal, you need to install to activate your appliance.

Retrieving Licenses Using the Riverbed Licensing Portal

The Riverbed Licensing Portal requires a unique identifier to retrieve a license such as, a serial number, a license request key (activation code), or a token. These steps describe how to retrieve a license using a serial number.

To retrieve your licenses for an appliance using a serial number

1. Go to the License page in the Riverbed Licensing Portal at https://licensing.riverbed.com/index.htm.
2. Enter your appliance serial number as your unique product identifier.

   The serial number is on a label located on your appliance. It also appears in the Help tab of the SCC Console.
3. Click **Next**.
4. Provide the contact information for the license, including your name and email.
5. Click **Submit** to display license information for all the products purchased with the serial number you specified.
6. Click a serial number to see license details.
7. Optionally, if you are behind a firewall, type the email address in the Email address text box and click **Email Keys** to have the license keys emailed to you.

8. Optionally, if you are behind a firewall, click **Download XML** to download an XML file with the license key. The XML file can be imported by the SteelCentral Controller for SteelHead.

Note: Click **New Search** to look for additional license records.

Installing Your License Keys

Because each license key is generated for a specific appliance, ensure that you install your license key on the appropriate appliance.

To install a license using the SCC console

1. Connect to the SCC Management Console of the appliance. For details, see the *SteelCentral Controller for SteelHead User's Guide*.
2. Choose Administration > Maintenance: Licenses to display the Licenses page.
3. Click + **Add New License** to expand the page.
4. Copy and paste the license key provided by the Riverbed Licensing Portal into the text box. Separate multiple license keys with a space, Tab, or Enter.
5. Click **Add** to display the license in the table.

You can also install a license key using the SCC command-line interface (CLI).

To install a license using the CLI

1. Connect to the CLI of the appliance and enter configuration mode.

   For details see the *Riverbed Command-Line Interface Reference Manual*.
2. At the system prompt, enter the following commands:

```
license install <license key>
write memory
```

CHAPTER 2 Installing the SCC

This chapter describes how to install and configure the SCC. It includes the following sections:

Checking Your Inventory

This section describes the contents of the SCC shipping carton.

Check your shipment to ensure that it contains the following items:

- The SCC
- One standard Ethernet straight-through cable
- One serial null-modem cable
- One or two power cables (depending on your order)

  Aside from country-specific requirements, all systems ship with the same power cable. The power cable has an IEC 60320 C13 plug on one end (to connect to the SCC) and a country-specific plug that fits the wall socket for that country. If a system has two power supplies, it ships with two suitable cables.

  You must always connect the SCC using either the cable in the accessories box or another cable that is approved for use by the IEC in the country in which the appliance is connected.

  You cannot connect an SCC directly to multiphase outlets. You must use a rack PDU or power strip that provides the appropriate three-prong outlet (hot/neutral/ground). For details, see the Knowledge Base solution number 1301.
- One Phillips screwdriver
- One mounting kit

- Documentation kit

If any items are damaged or missing, notify Riverbed Support at https://support.riverbed.com for replacement or repair.

Preparing Your Site for Installation

Before you install the SCC, make sure that your site meets the following requirements:

- It is a standard electronic environment where the ambient temperature does not exceed 40° C (104° F) and the relative humidity does not exceed 80% (noncondensing). For detailed information, see the appendix that follows.
- Ethernet connections are available within the standard Ethernet limit.
- There is available space on a two-post or four-post 19-inch rack. For details about installing the SteelHead to a rack, see the *Rack Installation Guide* or the printed instructions that were shipped with the system.
- A clean power source is available, dedicated to computer devices and other electronic equipment.
- The rack is a standard 19-inch Telco-type mounting rack.

Note: If your rack requires special mounting screws, contact your rack manufacturer.

The SCC is completely assembled, with all the equipment parts in place and securely fastened. The SCC is ready for installation with no further assembly required.

SCC Ports

This table summarizes the ports used to connect the SCC to your network.

Port	Description
Console	Connects the serial cable to a terminal device. You establish a serial connection to a terminal emulation program for console access to the configuration wizard and the SteelHead CLI.
Primary (PRI)	The management interface that connects the SCC to a LAN switch. This management interface enables you to connect to the SCC console and the SCC CLI. The primary and auxiliary ports cannot share the same network subnet.
Auxiliary (AUX)	An optional port that provides an additional management interface for a secondary network. You cannot have the primary and auxiliary ports on the same subnet. The auxiliary and in-path interfaces cannot share the same network subnet.

Completing the Configuration Checklist

This section lists the parameters you specify to complete the initial configuration of the SCC and to register remote SteelHeads.

Be prepared to provide values for the parameters listed in the following checklist.

Appliance	Parameter	Your Value
SCC	Hostname	
	IP address	
	Netmask	
	Default gateway	
	DNS server	
	Domain name	
Remote SteelHeads	Serial number	
	Version	
	IP address or hostname	
	User name	
	Password	

Powering On the System

This section describes how to connect the AC power and how to power on the system.

Caution: In European electrical environments you must ground (earth) the Green/Yellow tab on the power cord, or risk electrical shock.

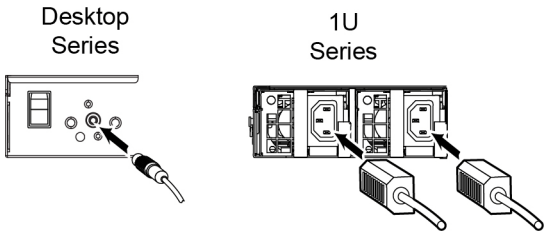
To power on the system

1. If your system has a master power switch, ensure that the system and master power switch is in the off position on the rear of the SCC.

2. Plug the AC power cord into the SCC.

Note: If your model has multiple power supplies, you must plug in all the power cords or you will hear an alarm.

Figure 2-1. Connecting the Power



3. Plug the AC power cord into an uninterrupted AC power source.

4. Press the system power switch on. If the SCC does not immediately power on, press the power switch off, then press the power switch on again.

5. Check the status lights on the SCC. For detailed information about the status lights, see the appendix at the end of this guide.

Securing the Power Cord on Desktop Systems

The Model 1000 include a power cord retention module. You can install this module to reduce the risk of accidentally unplugging the power.

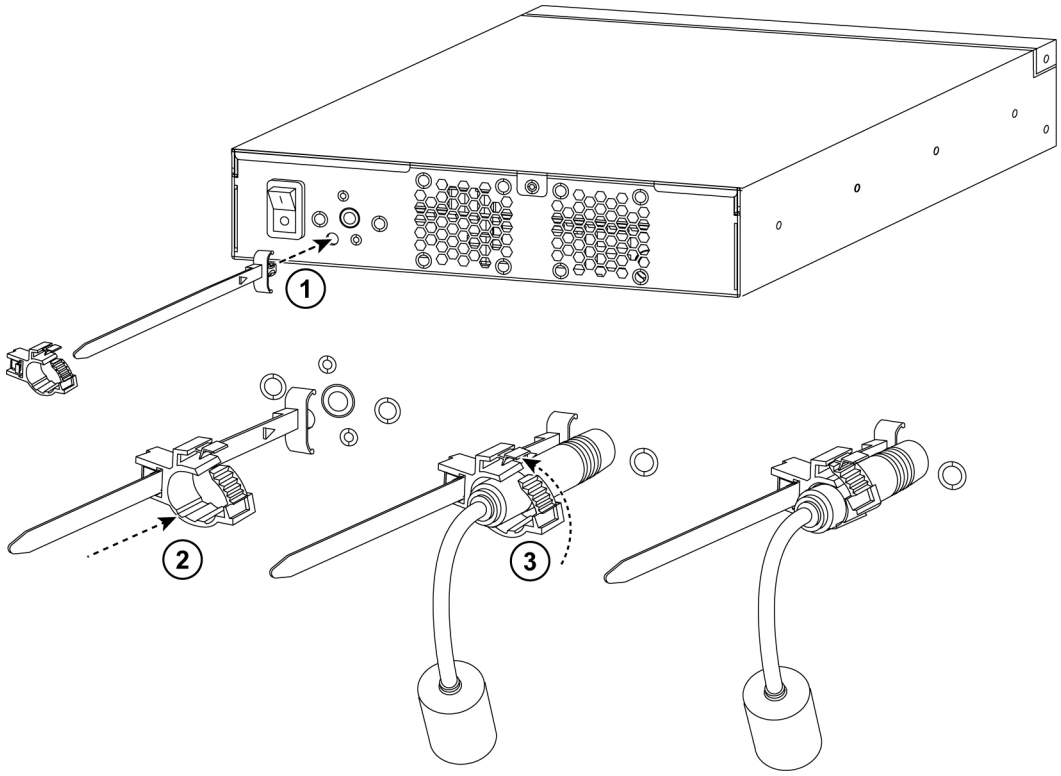
To install the power cord retention module

1. Push the retention module into the socket near the power connection.

   The socket is left of the power supply.

2. Attach the retention fastener to the module and tighten it around the power cable.

Figure 2-2. Attaching the Power Cord



The retention module does not prevent accidental pulls from removing the power cord, but it does provide increased protection.

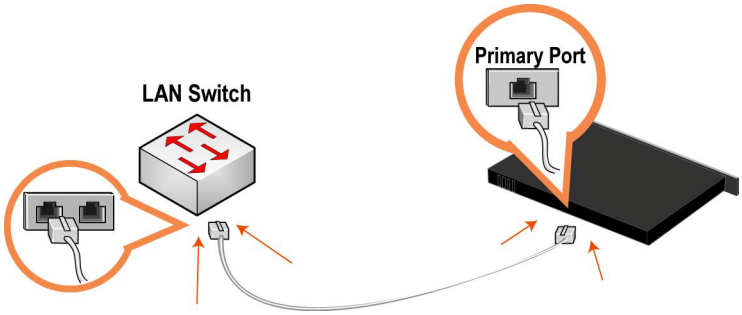
Connecting the SCC to Your Network

This section describes how to connect the SCC to your network.

To connect the SCC to your network

- Plug the straight-through cable into the primary port of the SteelHead and the LAN switch. This can be any port on your LAN switch configured to connect to a host.

Figure 2-3. Connecting the Primary Port and LAN Switch



Running the Configuration Wizard

To access the configuration wizard and the SCC CLI, you establish a serial connection using a terminal emulator program.

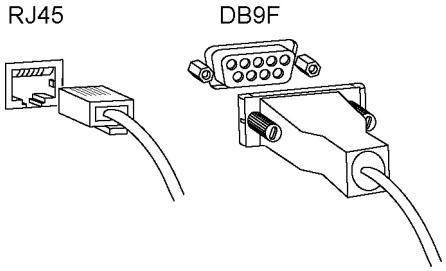
To run the configuration wizard

1. Plug the serial cable into the Console port and a terminal.

   Depending on your appliance, the Console port is either a DB9F port or an RJ45 port. (For port details for your appliance model, see the specification appendix in the installation guide for your product.)

   The appropriate console cable ships with your appliance.

Figure 2-4. Connecting to the SCC



2. Start your terminal emulation program, such as Tera Term Pro. The terminal device must have these settings:

- Baud rate: 9600 bps
- Data bits: 8
- Parity: none
- Stop bits: 1

- vt100 emulation
- No flow control

  If you are using the SCC with a terminal server, the terminal server must use hardware flow control for the port connected to the SCC.

  Riverbed recommends that you connect the console port to a device that logs output. Even though this is not a requirement, it can help you to identify problems with the system.

3. Log in as administrator user (admin) and enter the default password (password). For example:

```
login as: admin
Sent username "admin"
password: password
```

   The configuration wizard automatically starts after you have entered the login and default password. After you have established a connection, you configure the SCC using the configuration wizard.

4. Complete the configuration wizard steps as described in the following table.

Note: Press Enter to enter the default value. If you mistakenly answer **no**, you can start the configuration wizard by entering **configuration jump-start** at the system prompt.

Note: Press? for help. Press Ctrl-B to go back to the previous step.

Wizard Prompt	Description	Example
Step 1: Host Name?	Enter the hostname for the SCC.	`Step 1: Hostname? minna`
Step 2: Use DHCP?	You are given the option to enable the DHCP to automatically assign an IP address to the primary interface for the SCC. Riverbed recommends that you do not set DHCP. The default value is no.	`Step 2: Use DHCP? no`
Step 3: Primary IP address?	Enter the IP address for the SCC.	`Step 3: Primary IP address? 10.0.0.74`
Step 4: Netmask?	Enter the netmask for the network on which the SCC is to reside.	`Step 4: Netmask? 255.255.0.0`
Step 5: Default gateway?	Enter the default gateway for the network on which the SCC is to reside.	`Step 5: Default gateway? 10.0.0.1`
Step 6: Primary DNS server?	Enter the primary DNS server for the network on which the SCC is to reside.	`Step 6: Primary DNS server? 10.0.0.2`

Wizard Prompt	Description	Example
Step 7: Domain name?	Enter the domain name for the network on which the SCC is to reside. If you set a domain name, you need not specify the domain names when you set up remote appliances to be managed by the SCC. **Note:** When you configure DNS server settings, map **riverbedcmc** to the IP address for the SCC.	`Step 7: Domain name? example.com`
Step 8: Admin password?	Riverbed strongly recommends that you change the default password at this time. The password must be minimum of six characters. The default administrator password is password.	`Step 8: Admin password? xxxyyy`

5. The system confirms your settings:

```
You have entered the following information:
    1. Hostname: minna
    2. Use DHCP: no
    3. Primary IP address: 10.0.0.74
    4. Netmask: 255.255.0.0
    5. Default gateway: 10.0.0.1
    6. Primary DNS server: 10.0.0.2
    7. Domain name: example.com
    8. Admin password: xxxyyy
To change an answer, enter the step number to return to.
Otherwise hit <enter> to save changes and exit.
Choice:
```

   The SCC configuration wizard automatically saves your initial configuration settings.

6. To log out of the system, enter the following command at the system prompt:

```
# exit
```

7. If your model has a front bezel, replace the bezel on the SCC.

To restart the configuration wizard

- Enter these commands at the system prompt:

```
> enable
# configure terminal
(config) # configuration jump-start
```

For detailed information about the CLI, see the *Riverbed Command-Line Interface Reference Manual*.

Verifying Your Connections to the System

This section describes how to verify that you have properly connected the SCC.

Perform this tasks to verify that you have properly connected the SCC.

To verify you are connected to the SCC

1. Verify that you can connect to the CLI using one of these devices:

- An ASCII terminal or emulator that can connect to the serial console. It must have these settings: 9600 baud, 8 bits, no parity, 1 stop bit, vt100, and no flow control.
- A computer with a Secure Shell (SSH) client that is connected to the SCC primary port.

2. At the system prompt, enter this command:

```
ssh admin@host.domain
```

or

```
ssh admin@ipaddress
```

3. You are prompted for the administrator password. This is the password you set in the configuration wizard.

4. At the system prompt, ping from the management interface:

```
ping -I <primary-IP-address> <primary-default-gateway>
```

5. At the system prompt, ping from the in-path default gateway:

```
ping -I <in-path-IP-address> <in-path-default-gateway>
```

Connecting to the SCC Console

After you configure the SCC, you can check and modify your configuration settings and view performance reports and system logs in the SCC console. You can connect to the console through any supported Web browser.

To connect to the console, you must know the host, domain, and administrator password that you assigned in the configuration wizard.

Note: Cookies and JavaScript must be enabled in your Web browser.

Note: Before you begin, clear your browser cache and cookies to ensure the user interface displays correctly.

To connect to the SCC console

1. Enter the URL for the SCC in the location box of your browser:

`protocol://host.domain`

protocol is http or https. The secure HTTPS uses the SSL protocol to ensure a secure environment. When you connect using HTTPS, you are prompted to inspect and verify the SSL certificate. This is a self-signed certificate used to provide encrypted Web connections to the SCC.

host is the IP address or hostname you assigned the SCC during initial configuration. If your DNS server maps the IP address to a name, you can specify the DNS name.

domain is the full domain name for the SCC.

The SCC Login page appears.

2. In the text box, specify the user login: admin, monitor or a login from a RADIUS or a TACACS+ database, or a previously configured RBM account.

   The default login is admin. Users with administrator privileges can configure and administer the SCC. Users with monitor (monitor) privileges can view SCC reports but they cannot configure the system.

3. In the Password text box, specify the password you assigned in the configuration wizard of the SCC.

   The SCC is shipped with password as the default password.

4. Click **Log In** to log in to display the dashboard.

APPENDIX A Appliance Technical Specifications

This appendix describes technical and environmental specifications and explains the status lights on the SCC. This chapter includes the following sections:

Technical Specifications

The following tables summarize the physical and power specifications for the SCC.

	Model 8150	Model 1000
Form Factor	1 U	Desktop
Height, Width, and Depth	1.71 x 17.2 x 25.41 in (4.35 x 43.6 x 64.54 cm)	13 x 8 x 1.73 in. (33.02 x 20.32 x 4.4 cm)
Weight	30 lbs. (13.6 kg)	6 lb (2.7 kg)
Voltage	110-220 V	100-240V 50-60 Hz
Frequency	50-60 Hz	50 W
Power (Watts)	151 W	50 W
Amps	1.8 A	1.3 A
VA	153 V	—
BTU	515 BTU (per hour maximum)	165 BTU
Hard Disk	1 TB	1 x 500 GB HDD 1 x 480 GB SSD
Data Store	400 GB	—

	Model 8150	Model 1000
Power Requirement	151 W	50 W
Power Supply	Single 650 W The dual power supplies are optional.	I/P: 100-240 VAC, 1.3 A, 50-60 Hz O/P: 12 VAC, 7 A, max

Environmental Specifications

The following table summarizes the environmental requirements for the SCC.

The temperature refers to the outside ambient temperature of the appliance. It does not refer to the internal temperature of the appliance. Internal temperatures might be higher than the values stated here.

	Model 8150	Model 1000
Temperature (Operating) (outside, ambient)	10° - 40°C 50° - 95°F	0º - 45º C 32° - 113° F
Temperature (Storage) (outside, ambient)	-40° - 65°C -40° - 149°F	-40° - 65° C -40° - 149° F
Relative Humidity	20% - 80% noncondensing	20% - 80% noncondensing
Storage Humidity	5% to 95% noncondensing	5% - 95% noncondensing
Operating Altitude	Up to 10,000 ft	Up to 10,000 ft
Operating Acoustic	45 dBA Sound pressure (Typical)	45 dBA Sound pressure (Typical)

SCC Status Lights and Ports

This section illustrates the status lights, ports, and power switches for the following SCC models:

Model 8150

The following figures show the Model 8150 status lights and port locations.

Figure A-1. Front Panel

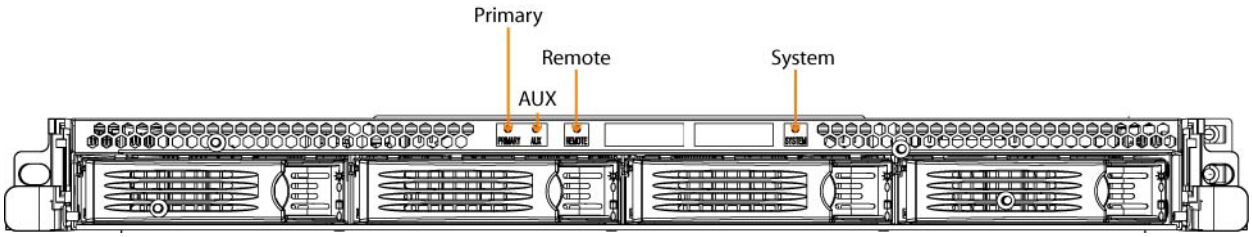
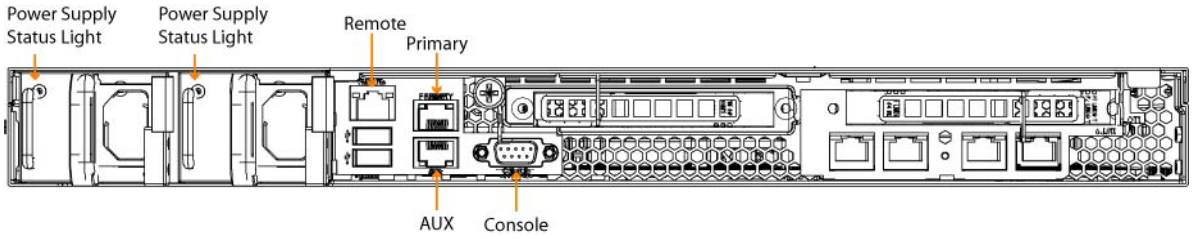


Figure A-2. Back Panel



The following table summarizes the system LEDs.

LED	Status
SYSTEM LEDs	Healthy = Blue Degraded = Yellow Critical = Red System Boot = Yellow
NETWORK STATUS LEDs (Front LAN-WAN LEDs)	Link = Blue Activity = Blinks Blue
BYP/BLK (Bypass or Block (Disconnect) Mode)	Normal = No Light Bypass or Block (Disconnect) = Orange
HDD LEDs	Disk Connected = Blue Read/Write Activity = Blinks Blue Failed Disk = Orange
LAN-WAN LEDs	Left LED Link = Green Activity = Blinks Green Right LED GB = Orange 100-MB = Green 10-MB = No Light

The following table summarizes the power supply LEDs.

LED	Condition
Solid Green	Healthy power supply with AC power connected.
Blinks Green	Unit is halted, but the power supplies are still connected to AC power.
Solid Orange	AC power is not connected to this power supply, but the unit is still powered on due to the other power supply. Occurs when the power supply automatically shuts off due to some error condition, such as an overheat.
Blinks Orange	Indicates a power supply predictive-fail condition, such as a fan failure. The power supply may then shut itself off, which changes the LED to solid orange. A log entry of this predictive-fail can be viewed using the **show hardware error-log all** command in the Riverbed Command-Line Interface.
No LED	No AC power connected.

Model 1000

The following figures show the Model 1000 status lights and port locations on the front and back panels.

Figure A-3. Front Panel

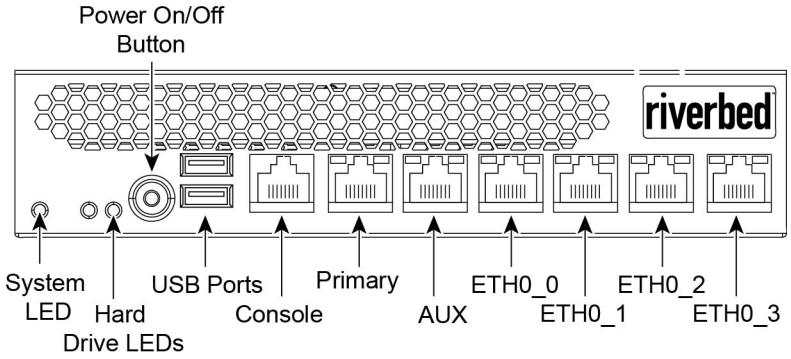
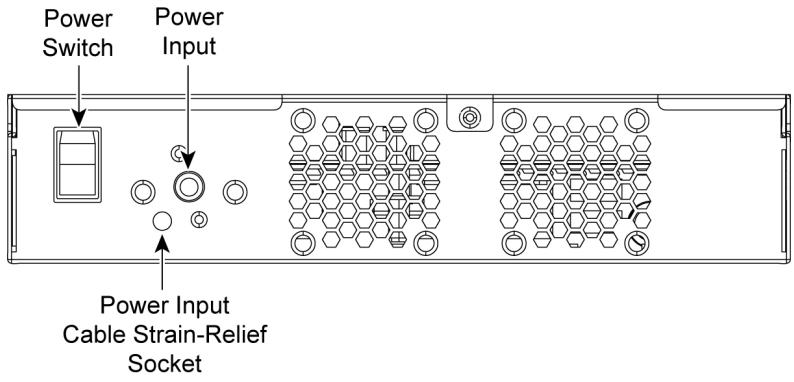


Figure A-4. Back Panel



The following table summarizes the LEDs.

LED	Status
System	Healthy = Blue Degraded = Yellow Critical = Red Power Off = None
Power Button LED	System Off = No Light Standby Mode = Yellow Power On = Blue
Hard Drive LED	Activity = Blinks Blue Failed Disk = Orange
Primary LED	Left LED Link = Green Activity = Blinks Green Right LED GB = Yellow 100 MB = Green 10 MB = No Light (with link on left LED)
LAN/WAN LEDs	Left LED Link = Green Activity = Blinks Green Bypass/Disconnect = Yellow Right LED GB = Yellow 100 MB = Green 10 MB = No Light (with link on left LED)

Index