SteelHead™ EX Installation and Configuration Guide

Includes RiOS®, SteelFusion™ Edge, and VSP

Version 5.0
March 2017
## Contents

Welcome .................................................................................................................................................. 7
   Audience ........................................................................................................................................... 7
   Document conventions .................................................................................................................. 8
Documentation and release notes ........................................................................................................ 8
   Contacting Riverbed ..................................................................................................................... 8

1 - Overview of SteelHead EX ........................................................................................................... 11
   Introducing SteelHead EX ............................................................................................................. 11
   SteelHead technology .................................................................................................................... 12
   SteelHead behavior in the network ............................................................................................... 13
   Fail-to-wire (bypass) mode ........................................................................................................... 14
   Fail-to-block (disconnect) mode .................................................................................................. 14
Safety guidelines .................................................................................................................................. 15
Virtual Services Platform .................................................................................................................... 15
SteelFusion storage ............................................................................................................................ 15
   SteelFusion-dedicated target mode ............................................................................................... 16
Product dependencies and compatibility .......................................................................................... 16
   Software dependencies ................................................................................................................. 17
   SCC compatibility .......................................................................................................................... 17
   Virtual Services Platform support ............................................................................................... 18
   Firewall requirements .................................................................................................................... 18
   Ethernet network compatibility ..................................................................................................... 18
   SNMP-based management compatibility ..................................................................................... 19
New features in 5.0 ............................................................................................................................... 19
Upgrading to SteelHead EX 5.0 ......................................................................................................... 19
   Managing the ESXi upgrade ......................................................................................................... 20
   Upgrading SteelHead EX software ............................................................................................... 21
   Reclaiming disk space ............................................................................................................... 22
   Downgrading the software ........................................................................................................... 23

2 - Managing Riverbed Licenses ......................................................................................................... 25
   Riverbed licensing methods ........................................................................................................... 25
   Automatic licensing ....................................................................................................................... 26
### Contents

Manual licensing using the Riverbed Licensing Portal ........................................................... 27  
Retrieving licenses using the Riverbed Licensing Portal .................................................. 27  
Installing your license keys ............................................................................................. 27  

#### 3 - Installing and Configuring SteelHead EX ............................................................... 29  
Choosing a network deployment........................................................................................ 29  
Checking your inventory .................................................................................................... 32  
Preparing your site for installation .................................................................................. 32  
Site requirements ........................................................................................................... 32  
SteelHead ports .............................................................................................................. 33  
Avoiding duplex mismatch............................................................................................... 33  
Bypass card interface naming conventions ..................................................................... 34  
Completing the configuration checklist .......................................................................... 35  
Powering on the system..................................................................................................... 35  
Configuring in-path SteelHead EX appliances ................................................................ 36  
Connecting the SteelHead EX to your network............................................................... 37  
Running the configuration wizard.................................................................................... 38  
Verifying you are connected to the SteelHead ............................................................... 42  
Connecting to the Management Console ....................................................................... 44  
Verifying WAN optimization ........................................................................................... 45  
Checking for speed and duplex errors.......................................................................... 45  
Configuring out-of-path SteelHead EX appliances .......................................................... 45  
Connecting out-of-path SteelHead EX appliances to your network .................................. 46  
Configuring the server-side SteelHead ........................................................................... 46  
Configuring the client-side SteelHead ............................................................................. 49  

#### 4 - Troubleshooting........................................................................................................ 53  
Cables .............................................................................................................................. 53  
Solution ........................................................................................................................... 53  
Duplex mismatch............................................................................................................. 54  
Possible cause .................................................................................................................. 54  
In-path SteelHead connection.......................................................................................... 55  
Possible cause .................................................................................................................. 55  
Oplock issues .................................................................................................................... 55  
Possible causes ................................................................................................................ 55  
CIFS overlapping open optimization denies multi-user access ....................................... 57  
Solution ........................................................................................................................... 57  
IP address configuration.................................................................................................... 58  
Solutions........................................................................................................................... 58  
Asymmetric routing.......................................................................................................... 59  
Possible cause .................................................................................................................. 59  
Packet ricochet ................................................................................................................ 59  
Possible cause .................................................................................................................. 60
Packet ricochet—Internet Control Messaging Protocol (ICMP) redirects ........................................... 60
  Possible causes ........................................................................................................................... 60
Simplified routing ...................................................................................................................... 60
Autodiscovery failure ................................................................................................................ 62
  Possible causes ........................................................................................................................ 62
Protocol optimization errors ...................................................................................................... 62
  Solutions .................................................................................................................................. 63
Server-side out-of-path connection caveats .............................................................................. 63
Specific problems ...................................................................................................................... 63
Resetting a lost password .......................................................................................................... 64

A - Series EX xx60 Technical Specifications ............................................................................ 67
EX560 and EX760 specifications ............................................................................................... 68
  Status lights and ports .......................................................................................................... 68
  Technical specifications ........................................................................................................ 70
  Power specifications .......................................................................................................... 70
  Environmental specifications ............................................................................................. 71
EX1160 specifications .............................................................................................................. 71
  Status lights and ports .......................................................................................................... 71
  Technical specifications ........................................................................................................ 72
  Power specifications .......................................................................................................... 73
  Environmental specifications ............................................................................................. 74
EX1260 specifications .............................................................................................................. 74
  Status lights and ports .......................................................................................................... 75
  Technical specifications ........................................................................................................ 76
  Power specifications .......................................................................................................... 77
  Environmental specifications ............................................................................................. 77
EX1360 specifications .............................................................................................................. 77
  Status lights and ports .......................................................................................................... 78
  Technical specifications ........................................................................................................ 79
  Power specifications .......................................................................................................... 80
  Environmental specifications ............................................................................................. 80
SteelHead EX hardware allocation ........................................................................................... 81
VSP and SteelFusion storage specifications .............................................................................. 83
Welcome

Welcome to the SteelHead EX Installation and Configuration Guide. This guide describes how to install and configure the SteelHead. It also describes the status lights and specifications for the system. The SteelHead EX Installation and Configuration Guide provides an overview of SteelHead features, specifications, terminology, and deployment scenarios. This document also describes how to install and connect a SteelHead to your network.

 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.

This guide includes information relevant to these products:

- Riverbed Optimization System (RiOS)
- Riverbed SteelHead (SteelHead)
- Riverbed SteelHead EX (SteelHead EX)
- Riverbed SteelCentral Controller for SteelHead (SCC)
- Riverbed command-line interface (CLI)
- Riverbed Virtual Services Platform (VSP)

This guide is intended to be used with the following documentation:

- SteelHead Management Console User’s Guide for SteelHead EXs (includes RiOS, SteelFusion Edge, and VSP information)
- SteelHead Deployment Guide (for SteelHead EX deployment scenarios)
- SteelFusion Core Installation and Configuration Guide
- SteelFusion Deployment Guide (for SteelFusion Core and SteelFusion Edge deployment scenarios)
- SteelFusion Core Getting Started Guide
- SteelFusion Core Management Console User’s Guide
Document conventions

This guide uses the following standard set of typographical conventions.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>italics</em></td>
<td>Within text, new terms and emphasized words appear in italic typeface.</td>
</tr>
<tr>
<td><strong>boldface</strong></td>
<td>Within text, CLI commands, CLI parameters, and REST API properties appear in bold typeface.</td>
</tr>
<tr>
<td>Courier</td>
<td>Code examples appear in Courier font:</td>
</tr>
<tr>
<td></td>
<td>amnesiac &gt; enable</td>
</tr>
<tr>
<td></td>
<td>amnesiac # configure terminal</td>
</tr>
<tr>
<td>&lt;&gt;</td>
<td>Values that you specify appear in angle brackets: interface &lt;ip-address&gt;</td>
</tr>
<tr>
<td>[]</td>
<td>Optional keywords or variables appear in brackets: ntp peer &lt;ip-address&gt; [version &lt;number&gt;]</td>
</tr>
<tr>
<td>{}</td>
<td>Elements that are part of a required choice appear in braces: {&lt;interface-name&gt;</td>
</tr>
<tr>
<td></td>
<td>The pipe symbol separates alternative, mutually exclusive elements of a choice. The pipe symbol is used in conjunction with braces or brackets; the braces or brackets group the choices and identify them as required or optional: {delete &lt;filename&gt;</td>
</tr>
</tbody>
</table>

Documentation and release notes

The most current version of all Riverbed documentation can be found on the Riverbed Support site at https://support.riverbed.com.

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

Each software release includes release notes. The release notes list new features, known issues, and fixed problems. To obtain the most current version of the release notes, go to the Software and Documentation section of the Riverbed Support site at http://www.riverbed.com/services/index.html.

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

Contacting Riverbed

This section describes how to contact departments within Riverbed.

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

- **Professional services** - Need help with planning a migration or implementing a custom design solution? Contact Riverbed Professional Services. Email proserve@riverbed.com or go to http://www.riverbed.com/services/index.html.

- **Documentation** - Have suggestions about Riverbed’s online documentation or printed materials? Send comments to techpubs@riverbed.com.
Overview of SteelHead EX

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

- “Introducing SteelHead EX” on page 11
- “Safety guidelines” on page 15
- “Virtual Services Platform” on page 15
- “SteelFusion storage” on page 15
- “Product dependencies and compatibility” on page 16
- “New features in 5.0” on page 19
- “Upgrading to SteelHead EX 5.0” on page 19

Introducing SteelHead EX

With SteelHead EX, you can consolidate branch office services into a converged infrastructure solution combining optimization, storage delivery, and virtualization for complete branch consolidation. SteelHead EX optimizes the performance of applications across the hybrid network, including on-premise, cloud, and Software-as-a-Service (SaaS) applications.

The SteelHead EX provides these features:

- The Riverbed Virtual Services Platform (VSP) that consolidates branch services onto the vSphere virtualization platform.
- Centralizes branch data to the data center with Riverbed BlockStream technology for storage delivery.
- Acts as a SteelCentral probe, making it easy to provide branch application-level visibility and troubleshooting.
- Seamlessly integrates with NetProfiler for end-to-end network monitoring and reporting, and with AppResponse for end-user experience monitoring for web and SaaS applications.
- Integrates seamlessly with SteelCentral NetShark-V for continuous captures of packet and flow data to improve network troubleshooting.
SteelHead technology

All SteelHead solutions offer a combination of data, transport, and application streamlining, and path selection. These technologies, along with SteelHead management capabilities, provide a comprehensive solution for the hybrid enterprise.

Data streamlining

- Uses patented, scalable, data referencing technology to reduce the bandwidth used to transmit data by up to 99%.
- Provides industry-leading scalability and patented deduplication.
- Works with TCP-based protocols and applications, including file sharing (CIFS/SMB), web applications (HTTP and HTTPS), database software (Oracle), and collaboration tools (CAD, SharePoint, email).
- Works with UDP-based file transfer applications, including Signiant, Aspera, and Symantec's Veritas Volume Replicator.

Transport streamlining

- Reduces the number of TCP packets required to transfer data by 65-98%.
- Enables the acceleration of SSL-encrypted traffic to eliminate the security versus performance trade-offs.
- Enables greater utilization of high bandwidth links (long, fat networks, such as OC3, OC12, and metro-fiber) for HS-TCP and MX-TCP.
- Supports satellite optimization for TCP links (based on SCPS extensions) over satellite connections that tend to be high latency, dynamic bandwidth, or lossy due to signal-to-noise ratio.

Application streamlining

- Offers the broadest support for application-specific modules to provide performance improvements on top of the data and transport streamlining optimization performed on all TCP traffic.
- Reduces application protocol chattiness up to 98%.
- Minimizes application overhead to provide massive throughput increases to applications such as file sharing (CIFS, SMB2/3, and NFS), collaboration software (SharePoint), email (Exchange and IBM Lotus Notes), cloud-based SaaS offerings (Office 365 and Salesforce), web applications (HTTP and HTTPS), database (Oracle), and storage and disaster recovery (NetApp SnapMirror and EMC SRDF/A).

Management streamlining

- Enables easy deployment through auto-discovery of peers and auto-interception of traffic—with no reconfiguration of clients, servers, or routers.
- Simplifies ongoing management by providing simple but powerful web-based (SteelCentral SteelCentral Controller for SteelHead, Management Console) and command-line interfaces, in-depth reporting, and real-time NetFlow export.
Introducing SteelHead EX

- Supports a vast array of network environments and topologies, including but not limited to MPLS, VoIP, video conferencing, QoS, VPN, satellite infrastructure, ATM, frame relay, microwave, and wireless.
- Automates configuration and deployment of hybrid networking and path selection with application-aware, business intent-based policies.

SteelHead behavior in the network

You configure optimization of traffic using the 5.0 or the Riverbed CLI. You configure the type of traffic a SteelHead optimizes and specify the type of action it performs using:

- **In-Path rules** - In-path rules determine the action a SteelHead takes when a connection is initiated, usually by a client. In-path rules are used only when a connection is initiated. Because connections are usually initiated by clients, in-path rules are configured for the initiating, or client-side SteelHead. You configure one of these types of in-path rule actions:
  - **Auto Discover** - Use the autodiscovery process to determine if a remote SteelHead is able to optimize the connection attempting to be created by this SYN packet.
  - **Fixed-Target** - Skip the autodiscovery process and use a specified remote SteelHead as an optimization peer. Fixed-target rules require the input of at least one remote target SteelHead; an optional backup SteelHead might also be specified.
  - **Fixed-Target (Packet Mode Optimization)** - Skip the autodiscovery process and uses a specified remote SteelHead as an optimization peer to perform bandwidth optimization on TCPv4, TCPv6, UDPv4, or UDPv6 connections. Packet-mode optimization rules support both physical in-path and master/backup SteelHead configurations. For details, see the SteelHead Management Console User’s Guide.
  - **Pass-Through** - Allow the SYN packet to pass through the SteelHead. No optimization is performed on the TCP connection initiated by this SYN packet.
  - **Discard** - Drop the SYN packet silently.
  - **Deny** - Drop the SYN packet and send a message back to its source.

- **Peering rules** - Peering rules determine how a SteelHead reacts when it sees a probe query. Peering rules are an ordered list of fields a SteelHead uses to match with incoming SYN packet fields. For example, source or destination subnet, IP address, VLAN, or TCP port, as well as the IP address of the probing SteelHead. This is especially useful in complex networks. These types of peering rule are available:
  - **Auto** - If the receiving SteelHead isn’t using enhanced autodiscovery, this has the same effect as the Accept peering rule action. If enhanced autodiscovery is enabled, the SteelHead only becomes the optimization peer if it is the last SteelHead in the path to the server.
  - **Accept** - The receiving SteelHead responds to the probing SteelHead and becomes the remote-side SteelHead (that is, the peer SteelHead) for the optimized connection.
  - **Pass-through** - The receiving SteelHead doesn’t respond to the probing SteelHead, and allows the SYN+ probe packet to continue through the network.

For detailed information about in-path and peering rules and how to configure them, see the SteelHead Management Console User’s Guide.
Overview of SteelHead EX

Introducing SteelHead EX

Fail-to-wire (bypass) mode

All SteelHead models and in-path network interface cards support a fail-to-wire mode. In the event of a failure or loss of power, the SteelHead goes into bypass mode and the traffic passes through uninterrupted.

If the SteelHead is in bypass mode, you are notified in the following ways:

- The Intercept/Bypass status light on the bypass card is triggered. For detailed information about bypass card status lights, see Appendix A, “Series EX xx60 Technical Specifications.”
- The Home page of the Management Console displays Critical in the Status bar.
- SNMP traps are sent (if you have set this option).
- The event is logged to system logs (syslog).
- Email notifications are sent (if you have set this option).

When the fault is corrected, new connections receive optimization; however, connections made during the fault do not. To force all connections to be optimized, enable the *kickoff* feature. Generally, connections are short-lived and kickoff isn't necessary. For detailed information about enabling the kickoff feature, see the *SteelHead Management Console User's Guide*.

When the SteelHead is in bypass mode the traffic passes through uninterrupted. Traffic that was optimized might be interrupted, depending on the behavior of the application-layer protocols. When connections are restored, they succeed, even without optimization.

In an out-of-path deployment, if the server-side SteelHead fails, the first connection from the client fails. After detecting that the SteelHead isn't functioning, a ping channel is set up from the client-side SteelHead to the server-side SteelHead. Subsequent connections are passed through unoptimized. When the ping succeeds, processing is restored and subsequent connections are intercepted and optimized.

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

Fail-to-block (disconnect) mode

With fail-to-block mode enabled in a redundant network path environment, traffic is blocked and rerouted to an optimized backup path in the event of a failure.

This feature is useful only if the network has a routing or switching infrastructure that can automatically divert traffic off the link to the optimized backup path. In an active-backup redundant network setup, the active path is configured to use fail-to-block, and the backup path is configured to use fail-to-bypass, thus traffic continues to be optimized on the backup path if there is a failure on the active path. In the event of a failure, the LAN and WAN interfaces power down and from a connected router or switch perspective those devices do not detect a link.

SteelHead EX supports fail-to-block mode on all cards.

The following events trigger fail-to-block if the feature is enabled:

- Kernel crash
- Hardware failure
Safety guidelines

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

**Note:** 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.

Virtual Services Platform

The Virtual Services Platform (VSP) is a VMware-based virtualization platform that lets you run multiple virtual machines on a SteelHead EX. With VSP, you can consolidate multiple basic services in the branch such as print, DNS, and DHCP. In VSP, you install and run virtual machines directly from a dedicated partition of the SteelHead EX. VSP supports running up to five virtual machines on a single SteelHead EX.

VSP is included in the native SteelHead EX functionality and doesn't require a separate download or license. VSP in SteelHead EX 5.0 includes ESXi 6.0 Patch 3 as the virtualization platform.

For details on configuring and using VSP, see the SteelHead Management Console User’s Guide for the SteelHead EX.

SteelFusion storage

SteelFusion is a converged infrastructure solution, encompassing all branch services such as server, storage, networking, and WAN optimization. It is a dual-ended system comprised of: SteelFusion Enabled SteelHead EX or SteelFusion Edge and SteelFusion Core.

SteelFusion Core is a physical or virtual appliance in the data center that mounts all LUNs that need to be made available to applications and servers at a remote location from the back-end storage array. SteelFusion Enabled SteelHead EX or SteelFusion Edge provides a virtualized environment that hosts the branch application servers. Core appliances communicate across the WAN with the Edge appliances at the branch.
SteelFusion delivers local user performance while enabling data centralization, instant recovery, and lower total operating costs. Unlike traditional converged infrastructures, SteelFusion enables stateless branch services. You can access applications that run locally in your branch while the primary data is centralized in your data center. Decoupling computation from its underlying storage allows your applications to run in a stateless mode, which reduces your branch footprint and centralizes management of your branch services.

With SteelFusion, you can extend a data center storage array to a remote location, even over a low-bandwidth link. This enables you to effectively deliver global storage infrastructure anywhere you need it.

SteelFusion provides the following functionality:

- Innovative block storage optimization ensures that you can centrally manage data storage while keeping that data available to business operations in the branch, even in the event of a WAN outage.
- A local authoritative cache ensures LAN-speed reads and fast cold writes at the branch.
- Integration with Microsoft Volume Shadow Copy Service enables consistent point-in-time data snapshots and seamless integration with backup applications.
- Integration with the snapshot capabilities of the storage array enables you to configure application-consistent snapshots through the SteelFusion Core Management Console.
- Integration with industry-standard Challenge-Handshake Authentication Protocol (CHAP) authenticates users and hosts.
- A secure vault protects sensitive information using AES 256-bit encryption.
- Solid-state disks (SSDs) that guarantee data durability and performance.
- An active-active high-availability (HA) deployment option for Core ensures the availability of storage array logical unit numbers (LUNs) for remote sites.
- Customizable reports provide visibility to key utilization, performance, and diagnostic information.

For detailed information about how SteelFusion works, see the SteelFusion Core Installation and Configuration Guide.

SteelFusion-dedicated target mode

SteelFusion-dedicated target mode refers to a SteelFusion-enabled SteelHead EX that provides VSP functionality but doesn’t include WAN optimization.

Appliances in SteelFusion-dedicated target mode are intended to be used in conjunction with existing SteelHead deployments, thereby enabling customers to take advantage of SteelFusion functionality without upgrading their existing SteelHeads.

Product dependencies and compatibility

This section provides information about product dependencies and compatibility. It includes this information:

- “Software dependencies” on page 17
Software dependencies

This table summarizes the software requirements for the SteelHead.

<table>
<thead>
<tr>
<th>Riverbed component</th>
<th>Hardware and software requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>SteelHead Management Console, SteelCentral Controller for SteelHead</td>
<td>Any computer that supports a web browser with a color image display.</td>
</tr>
<tr>
<td></td>
<td>The Management Console has been tested with Chrome, Mozilla Firefox Release 38, and Microsoft Internet Explorer 11.</td>
</tr>
<tr>
<td></td>
<td>The SteelCentral Controller for SteelHead has been tested with Mozilla Firefox Release 38 and Microsoft Internet Explorer 11.</td>
</tr>
<tr>
<td></td>
<td>Internet Explorer 9.0 must refresh reports every 4 minutes due to performance issues. Consider using a different browser to view reports.</td>
</tr>
<tr>
<td></td>
<td>JavaScript and cookies must be enabled in your web browser.</td>
</tr>
</tbody>
</table>

SCC compatibility

The SteelHead EX has been tested with the following SteelCentral Controller for SteelHead (SCC) versions.

<table>
<thead>
<tr>
<th>EX version</th>
<th>SteelHead RiOS version</th>
<th>Recommended SCC version</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0</td>
<td>9.5.0a</td>
<td>9.5.1</td>
</tr>
<tr>
<td>4.6</td>
<td>9.2.1</td>
<td>9.2.2</td>
</tr>
<tr>
<td>4.5</td>
<td>9.2.1</td>
<td>9.2</td>
</tr>
<tr>
<td>4.3</td>
<td>9.1.2</td>
<td>9.1.0e</td>
</tr>
<tr>
<td>4.2</td>
<td>9.1.1a</td>
<td>9.1.0d</td>
</tr>
<tr>
<td>4.1</td>
<td>9.1</td>
<td>9.1</td>
</tr>
<tr>
<td>3.6</td>
<td>9.0</td>
<td>9.0</td>
</tr>
<tr>
<td>3.5.3</td>
<td>8.6</td>
<td>8.6.0</td>
</tr>
<tr>
<td>3.1</td>
<td>8.5.1</td>
<td>8.5.0</td>
</tr>
</tbody>
</table>

Note: As a result of updating the version of SSH, older releases of SCC can’t connect to newer software on managed appliances. If you plan to upgrade your EX appliances to 4.3 or later, first upgrade the SCC to 9.1.0e or later to avoid disconnections. See knowledge base article S27759 for complete details.
**Virtual Services Platform support**

Virtual Services Platform (VSP) isn’t supported on the Series xx55 hardware platforms. VSP is supported only on the SteelHead EX Series xx60 hardware platforms.

**Firewall requirements**

We recommend that you deploy the SteelHead behind your firewall. These firewall settings are required for the SteelHead:

- Ports 7800 and 7810 must be open.
- Make sure your firewall doesn’t strip TCP options.

Secure transport requires communication on the management plane, control plane, and data plane. Consider the following port usage:

- The management plane requires communication between the SteelHead and the SCC on TCP port 9443 and TCP port 22.
- The control plane between the SteelHead acting as the controller and the SteelHeads acting as group members is over TCP port 9443.
- Encryption service flows over ESP (IP protocol 50). Or, if the network is public, over UDP port 4500.

**Note:** The secure transport feature must be configured on the SCC. For detailed information, see the SteelCentral Controller for SteelHead User’s Guide.

**Ethernet network compatibility**

The SteelHead supports these networking standards. A SteelHead with a Gigabit Ethernet card supports jumbo frames on in-path and primary ports.

<table>
<thead>
<tr>
<th>Ethernet standard</th>
<th>IEEE standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet Logical Link Control (LLC)</td>
<td>IEEE 802.2 - 1998</td>
</tr>
<tr>
<td>Fast Ethernet 100BASE-TX</td>
<td>IEEE 802.3 - 2008</td>
</tr>
<tr>
<td>Gigabit Ethernet over Copper 1000BASE-T (All copper interfaces are autosensing for speed and duplex.)</td>
<td>IEEE 802.3 - 2008</td>
</tr>
<tr>
<td>Gigabit Ethernet over Fiber 1000BASE-SX (LC connector)</td>
<td>IEEE 802.3 - 2008</td>
</tr>
<tr>
<td>Gigabit Ethernet over Fiber 10GBASE-LR Single Mode</td>
<td>IEEE 802.3 - 2008</td>
</tr>
<tr>
<td>Gigabit Ethernet over 10GBASE-SR Multimode</td>
<td>IEEE 802.3 - 2008</td>
</tr>
</tbody>
</table>

The SteelHead ports support these connection types and speeds:

<table>
<thead>
<tr>
<th>Port</th>
<th>Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary (PRI)</td>
<td>10/100/1000BASE-T, auto-negotiating</td>
</tr>
<tr>
<td>Auxiliary (AUX)</td>
<td>10/100/1000BASE-T, auto-negotiating</td>
</tr>
</tbody>
</table>
The SteelHead supports VLAN Tagging (IEEE 802.3-2008). It doesn't support the Inter-Switch Link (ISL) protocol.

The SteelHead autonegotiates speed and duplex mode for all data rates and supports full duplex mode and flow control (IEEE 802.3-2008).

**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 5.0**

These new features are available in 5.0:

- **Parity with RiOS 9.5 and SteelFusion Core 5.0** - EX 5.0 includes the features in RiOS 9.5 and SteelFusion Core 5.0 (Exception: SteelHead EX doesn't support the Web Proxy feature.)

**Upgrading to SteelHead EX 5.0**

This section describes how to upgrade, reclaim disk space, and how to downgrade your software. It includes these sections:

- “Managing the ESXi upgrade” on page 20
- “Upgrading SteelHead EX software” on page 21
- “Reclaiming disk space” on page 22
- “Downgrading the software” on page 23

SteelHead EX reserves a portion of the datastore so that non-ESX-based virtual machines can be converted, on the SteelHead EX, to ESX virtual machine format. You can reclaim that datastore space for other purposes.

SteelHead EX software 5.0 is compatible with previous SteelHead EX software versions. However, to obtain the full benefits of the new features in 5.0, you must upgrade the client-side and server-side SteelHeads on any given WAN link. After you have upgraded all appliances, all the benefits of the new features and enhancements are available.
If you mix software versions in your network, the releases might support different optimization features and you can’t take full advantage of the features that aren’t part of the older software versions.

For information on compatibility between RiOS, Edge, Core, and vSphere releases, see the knowledge base article RiOS, SteelFusion Edge, SteelFusion Core and vSphere Release Matrix https://supportkb.riverbed.com/support/index?page=content&id=S:S27472.

Managing the ESXi upgrade

Because the SteelHead EX software image includes the ESXi software, the image upgrade might upgrade the ESXi version used by VSP. If you haven't changed the ESXi version outside of SteelHead EX, the ESXi version will be updated to match the new install image, if necessary. If you have modified the ESXi version for VSP independently of the SteelHead EX image, the software upgrade does one of the following:

- If the existing version of ESXi is older than the version in the image file, the image upgrade updates the ESXi version. The configuration won’t be affected.
- If the existing version of ESXi is newer than the version in the image file, the image upgrade doesn’t change ESXi. The configuration won’t be affected.
- If the version can’t be determined, ESXi will be upgraded to the version in the image file. The ESXi configuration might be lost. As a best practice, back up your existing configuration before proceeding.

If your running ESXi version is fully supported, meaning the version reported by ESXi matches the version of ESXi bundled with the RiOS image, the upgrade process performs a backup of the existing ESXi configuration before the upgrade.

Note: You can verify the version number and the support status of the running ESXi installation on the Help page of the Management Console.

Known issues

Upgrading hypervisor to ESXi 6.0 includes the following known issues:

- vCenter licenses need to be reinstalled.
  The EX upgrade to ESXi 6.0 applies a new embedded license to the hypervisor. If ESXi isn’t managed by vCenter, there is no need to upgrade the default license. However, if you added a custom license in 5.5 that supported vCenter, you will lose that functionality. After the upgrade, you need to add a new 6.0 license that supports vCenter. You add the custom license from either vSphere or vCenter.

- You need to use vCenter or vSphere v6.0 to manage SteelHead EX 5.0 virtual machines. If you use vCenter 5.5 or lower to manage ESXi, you must upgrade vCenter to 6.0 or higher before upgrading the SteelHead EX appliance.

- ESXi 6.0 requires enhanced password complexity.
  You can find the new password requirements here: https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.security.doc/GUID-DC96FFDB-F5F2-43EC-8C73-05ACDAE6BE43.html
  If you upgrade from an earlier version of ESXi, you can continue to use your old password even if it doesn’t meet the new requirements. However, if you change your password or reinstall ESXi, your new password must satisfy the new requirements.
- iSCSI connections fail and datastores become inaccessible when IQN changes.

  This problem can occur if you change the IQN of an iSCSI adapter while iSCSI sessions on the adapter are still active.

  **Workaround:** When you change the IQN of an iSCSI adapter, no session should be active on that adapter. Remove all iSCSI sessions and all targets on the adapter before changing the IQN.

- Active Directory settings aren't retained.

  The Active Directory settings configured in the ESXi host before upgrade aren't retained when the host is upgraded to ESXi 6.0.

  **Workaround:** Add the host to the Active Directory Domain after the upgrade if the pre-upgrade ESXi version is 5.1 or later. Do not add the host to the Active Directory Domain after upgrade if the pre-upgrade ESXi version is ESXi 5.0.x.

- Hosts that were previously added to the domain are no longer joined to the domain.

  When upgrading from vSphere 5.5 to vSphere 6.0 for the first time, the Active Directory configuration isn't retained. After the upgrade, rejoin the hosts to the vCenter Server domain.

### Upgrading SteelHead EX software

Follow these steps to upgrade your software. These instructions assume you are familiar with the SteelHead EX and the Management Console.

Riverbed has tested and qualified EX upgrades within two major releases. To perform a qualified upgrade, you might need to upgrade to an intermediary release first.

**To upgrade the EX software**

1. Download the software image from the Riverbed Support site to a location such as your desktop. Optionally, you can download a delta image directly from the Riverbed Support site to the SteelHead. The delta downloaded image includes only the incremental changes. The smaller file size means a faster download and less load on the network.

2. Log in to the Management Console using the Administrator account (admin).

3. Choose Configure > Maintenance: Software Upgrade and choose one of the following options:
   - **From URL** - Type the URL that points to the software image. Use one of the following 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
Overview of SteelHead EX Upgrading to SteelHead EX 5.0

- **From Riverbed Support Site** - 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 your file system and select the software image.

- **Schedule Upgrade for Later** - Select this check box to schedule an upgrade for a later time. Type the date and time in the Date and Time text boxes using these formats: YYYY/MM/DD and HH:MM:SS.

4. Click **Install** to immediately upload and install the software upgrade on your system, unless you schedule it for later.

   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.

5. Choose Configure > Maintenance: Reboot/Shut Down and click **Reboot**.

   The appliance can take a few minutes to reboot. This is normal behavior as 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 Home page, Software Upgrade, and Help pages of the Management Console display the software version upgrade.

### Reclaiming disk space

Follow the steps in this section to reclaim the disk space that was reserved for converting virtual machines. These instructions assume that you have performed the upgrade procedure described in “Upgrading SteelHead EX software” on page 21.

By default, the upgrade process doesn't automatically alter the existing disk layout. Disk space must be manually reclaimed.

**Note:** Changing the disk layout erases SteelFusion and VSP data from the disk and destroys the ESXi datastore. The appliance is rebooted as part of the process. Back up your SteelFusion, VSP, and datastore data prior to changing the disk layout.

For details about the amount of space that can be recovered, and about maximum allocations, see “Series EX xx60 Technical Specifications” on page 67.
To reclaim datastore space
1. Ensure that you have upgraded the appliance to EX 2.1 or greater.
2. Launch the Management Console.
3. Enter login credentials.
5. In the Disk Layout area, select one of the two available extended modes.
6. Click Apply.
7. At the prompt, click OK to confirm your intention to change the disk layout and reboot the device.

Downgrading the software
If you want to downgrade to a previous version of the SteelHead software, you must downgrade to a version of the software that has previously run on your machine.

When you downgrade the software, RiOS reverts the ESXi version to the version supported in the installation image. If you upgraded the ESXi using vCenter (separate from the EX installation), the system can't restore the state and ESXi starts with the initial configuration.
Managing Riverbed Licenses

This chapter describes the Riverbed licensing methods and how to manage Riverbed licenses. It includes these sections:

- “Riverbed licensing methods” on page 25
- “Automatic licensing” on page 26
- “Manual licensing using the Riverbed Licensing Portal” on page 27

Riverbed licensing methods

A license is a string issued by Riverbed that embeds information that ties the license to data to prevent tampering. After you install the license, the system saves it in the configuration database and enables the functionality associated with the license. Riverbed employs the following licensing methods:

- **Automatic licensing** - After you connect your SteelHead to the network, the appliance automatically contacts the Riverbed Licensing Portal and downloads and installs the licenses. This option requires Internet access from the SteelHead.

- **Manual licensing** - You can manually fetch and activate licenses for Riverbed products using the Riverbed Licensing Portal. To retrieve license keys, follow the instruction at the following location: https://licensing.riverbed.com/index.htm.

- **Token method** - You use tokens to activate Riverbed software. For detailed information, see the installation guides for these products.

- **Factory licensing** - You can have all your Riverbed licenses installed at the factory for a small fee.
Automatic licensing

Automatic licensing allows the SteelHead, once connected to the network, to automatically contact the Riverbed Licensing Portal to retrieve and install license keys onto the appliance. Automatic licensing simplifies inventory management and provides an automated mechanism of fetching licenses for Riverbed products without having to manually activate individual appliances and licenses.

If you are behind a firewall, you can retrieve licenses at the Riverbed Licensing Portal using the email option or by downloading and XML file to the SteelCentral Controller for SteelHead. For detailed information, see “Retrieving licenses using the Riverbed Licensing Portal” on page 27.

Automatic licensing also works over a web proxy. For details on setting up a web proxy, see the SteelHead Management Console User’s Guide.

Note: If automatic licensing fails, an error message is displayed in the Management Console. Go to the Riverbed Licensing Portal and follow the instructions for retrieving your licenses.

To view licenses on a new SteelHead

- Connect the new SteelHead to the network.
  
  The SteelHead automatically contacts the Riverbed Licensing Portal, which downloads and installs the licenses. The Management Console Licensing page displays a success message, or the Alarm Status page reports an actionable error message.

To replace expired licenses

- Purchase new downloadable licenses to replace the expired license.
  
  At the time of the next scheduled automatic license fetch, the SteelHead automatically contacts the Riverbed License Portal and downloads the new licenses. The Management Console Licensing page displays a success message or the Alarm Status page reports an actionable error message. You do not need to delete the expired license. The system uses the license with the latest expiration date.

To fetch a license on demand

1. In the Management Console, choose Configure > Maintenance: Licenses to display the Licenses page.

2. Click Fetch Updates Now.
  
  The Management Console Licensing page displays a success message or the Alarm Status page reports an actionable error message.

Note: Only administrator users can fetch and install licenses. For detailed information on administrator and monitor users, see the SteelHead Management Console User’s Guide.
Manual licensing using the Riverbed Licensing Portal

You can retrieve and manage Riverbed licenses using the Riverbed Licensing Portal. Once you retrieve a license from the Riverbed Licensing Portal, you need to install it.

Retrieving licenses using the Riverbed Licensing Portal

The Licensing Portal requires a unique product identifier to retrieve a license. Depending on the product, the identifier can be a serial number, a license request key (activation code), or a token. The steps to retrieve a license vary based on the product identifier. Online instructions guide you through the process.

To retrieve your licenses for an appliance using a serial number

2. Enter your appliance serial number as your unique product identifier. The serial number is on a label located on your appliance, and it also appears in the Support tab of the Management Console.
3. Click Next.
4. Provide the contact information for the license, including your name and email.
5. Click Submit. The Licensing Portal displays license information for all the products purchased with the serial number you specified.
6. 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.
7. Optionally, if you are behind a firewall, click Download XML to download an XML file. 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 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
   write memory

   where <license-key> is the license key you retrieved from the Riverbed Licensing Portal

To install a license using the Management Console

1. Connect to the Management Console of the appliance.
   For details, see the SteelHead Management Console User’s Guide.

2. Choose Administration > Maintenance: Licenses to display the Licenses Page.

3. Copy and paste the license key provided by Riverbed Licensing Portal into the text box. Separate multiple license keys with a space, Tab, or Enter.
Installing and Configuring SteelHead EX

This chapter describes how to install and configure SteelHead EX. It includes these sections:

- “Choosing a network deployment” on page 29
- “Checking your inventory” on page 32
- “Preparing your site for installation” on page 32
- “Powering on the system” on page 35
- “Configuring in-path SteelHead EX appliances” on page 36
- “Configuring out-of-path SteelHead EX appliances” on page 45

Caution: Read and follow the safety guidelines described in the Safety and Compliance Guide. Failure to follow these safety guidelines can result in damage to the equipment.

Choosing a network deployment

Typically, the SteelHead is deployed on a LAN, with communication between appliances taking place over a private WAN or VPN. Because optimization between SteelHeads usually takes place over a secure WAN, it isn’t necessary to configure company firewalls to support SteelHead-specific ports.

Note: 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 autodiscovery to function properly.

For optimal performance, minimize latency between SteelHeads and their respective clients and servers. Position SteelHeads as close as possible to your network endpoints (that is, client-side SteelHeads should be as close to your clients as possible, and server-side SteelHeads should be as close to your servers as possible).

Ideally, SteelHeads optimize only traffic that is initiated or terminated at their local site. The best and easiest way to achieve this optimization is to deploy the SteelHeads where the LAN connects to the WAN, and not where any LAN-to-LAN or WAN-to-WAN traffic can pass through (or be redirected to) the SteelHead.

For detailed information about your deployment options and best practices for deploying SteelHeads, see the SteelHead Deployment Guide.

Before you begin the installation and configuration process, you must select a network deployment:
- **Physical in-path** - In a physical in-path deployment, the SteelHead is physically in the direct path between clients and servers. The clients and servers continue to see client and server Internet Protocol (IP) addresses. In-path designs are the simplest to configure and manage, and the most common type of SteelHead deployment, even for large sites.

![Figure 3-1. Physical In-Path deployment](image)

- **Virtual in-path** - In a virtual in-path deployment, the SteelHead is virtually in the path between clients and servers. Traffic moves in and out of the same WAN interface, and the LAN interface isn’t used. This deployment differs from a physical in-path deployment in that a packet redirection mechanism, such as a SteelHead Interceptor, WCCP, policy based routing (PBR), or Layer-4 switching, directs packets to SteelHeads that aren’t in the physical path of the client or server. For details on the redirection mechanisms, see the SteelHead Deployment Guide.

![Figure 3-2. Virtual In-Path: WCCP deployment](image)

- **Out-of-path** - In an out-of-path deployment, the server-side SteelHead isn’t in the direct path between the client and the server. In an out-of-path deployment, the SteelHead acts as a proxy. This type of deployment might be suitable for locations where physical in-path or virtual in-path configurations aren’t possible. This deployment requires only a SteelHead primary interface to connect to the network. The SteelHead can be connected anywhere in the LAN.
An out-of-path SteelHead deployment doesn’t use a redirecting mechanism. You configure fixed-target in-path rules for the client-side SteelHead. The fixed-target in-path rules point to the primary IP address of the out-of-path SteelHead. The out-of-path SteelHead uses its primary IP address when communicating to the server. The remote SteelHead must be deployed either in a physical or virtual in-path mode.

**Figure 3-3. Out-of-Path deployment**

![Out-of-Path deployment diagram](image)

### Deployment benefits summary

This table summarizes the benefits of the various deployment options.

<table>
<thead>
<tr>
<th>Deployment type</th>
<th>Benefits</th>
<th>Requires</th>
<th>Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical In-Path</td>
<td>Simple to configure and uses automatic discovery of peers.</td>
<td>In-path rules.</td>
<td>Scaling, availability, cabling.</td>
</tr>
<tr>
<td>Virtual In-Path</td>
<td>Limited physical disruption, routing forces traffic to WAN, automatic discovery of peers.</td>
<td>External setup to use PBR, WCCP, a SteelHead Interceptor, or Layer-4 switching.</td>
<td>Dependent on the external configuration.</td>
</tr>
<tr>
<td>Out-of-Path</td>
<td>The client-side SteelHead sends directly to the server-side SteelHead with no physical disruption. This configuration is typically used as a way to rapidly deploy a SteelHead in a site with very complex or numerous connections to the WAN.</td>
<td>Fixed-target rules.</td>
<td>Requires explicit manual configuration. Connections initiated from the site with the out-of-path SteelHead can’t be optimized. Servers at the site detect the optimized traffic coming from the out-of-path SteelHead primary IP address instead of a client IP address.</td>
</tr>
</tbody>
</table>
Checking your inventory

Your shipping carton contains these items:

- The SteelHead
- One standard Ethernet straight-through cable
- One standard Ethernet crossover 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 SteelHead) 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 SteelHead 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 can't connect a SteelHead 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
- Rails (preinstalled on the EX Series xx60 platforms)
- 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

The SteelHead ships completely assembled, with all the equipment parts in place and securely fastened.

Site requirements

Before you install the SteelHead, make sure that your site meets these requirements:

- It is a standard electronic environment where the ambient temperature doesn't exceed 40°C (104°F) and the relative humidity doesn't exceed 80% (noncondensing). For detailed information, see the appendices that follow.

- 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.
Preparing your site for installation

Installing and Configuring SteelHead EX

- 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:** We recommend that you use a four-post mounting rack for 2U systems.

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

### SteelHead ports

The following table summarizes the ports used to connect the SteelHead to your network.

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console</td>
<td>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.</td>
</tr>
</tbody>
</table>
| Primary (PRI) | The management interface that connects the SteelHead to a LAN switch. This management interface enables you to connect to the Management Console and the SteelHead CLI.  
  - The primary and auxiliary ports can't share the same network subnet.  
  - The primary and in-path interfaces can share the same subnet.  
  - You must use the primary port on the server-side for out-of-path deployments. |
| Auxiliary (AUX) | An optional port that provides an additional management interface for a secondary network.  
  - The primary and auxiliary ports can't share the same network subnet.  
  - The auxiliary and in-path interfaces can't share the same network subnet.  
  - You can't use the auxiliary port for out-of-path SteelHeads. |
| WAN      | Connects the WAN port of the SteelHead and the WAN router using a crossover cable. |
| LAN      | Connects the LAN port of the SteelHead and the LAN switch using a straight-through cable.  
  **Note:** If the SteelHead is deployed between two switches, both the LAN and WAN ports must be connected with straight-through cables. |

### Avoiding duplex mismatch

Before you begin the configuration process, ensure that your LAN and WAN interfaces have the same duplex settings.

The SteelHead automatically negotiates duplex settings. If one end of the link is set to autonegotiate and the other end of the link isn't set to autonegotiate, the duplex settings on the network device default to half-duplex. This duplex mismatch passes traffic, but it causes late collisions and results in degraded optimization. To achieve maximum optimization, set your network devices to **100** and **full**.

To avoid duplex mismatches, manually configure the duplex settings on your:

- router.
- switch.
Installing and Configuring SteelHead EX Preparing your site for installation

- SteelHead WAN interface.
- SteelHead LAN interface.
- SteelHead primary interface.

The following can be signs of a duplex mismatch:

- On the Reports > Diagnostics: System Logs page, you see errors for sends, receives, cyclic redundancy check (CRC), and short sends.
- You can’t connect to an attached device.
- You can connect to a device when you choose auto-negotiation, but you can’t connect to that same device when you manually set the speed or duplex.
- Slow performance across the network.

For detailed information about checking for duplex mismatches, see “Duplex mismatch” on page 54.

Bypass card interface naming conventions

The interface names for the bypass cards are a combination of the slot number and the port pairs (<slot>_<pair>, <slot>_<pair>). For example, if a four-port bypass card is located in slot 0 of your appliance, the interface names are lan0_0, wan0_0, lan0_1, and wan0_1, respectively. Alternatively, if the bypass card is located in slot 1 of your appliance, the interface names are lan1_0, wan1_0, lan1_1, and wan1_1, respectively.

For detailed information about installing additional bypass cards, see the Network and Storage Card Installation Guide.
Completing the configuration checklist

The following table lists the parameters you specify to complete the initial configuration of the SteelHead. Be prepared to provide values for these parameters.

<table>
<thead>
<tr>
<th>Appliance</th>
<th>Parameter</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SteelHead (the Primary Interface)</td>
<td>Hostname</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IP address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Netmask</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Default gateway (the WAN gateway)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS IP address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Domain name for the system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Administrator password</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SMTP server IP address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Events and failures notification email address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Primary interface speed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Primary interface duplex</td>
<td></td>
</tr>
<tr>
<td>In-Path Deployments</td>
<td>In-path interface IP address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In-path netmask</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In-path gateway</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In-path: LAN interface speed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In-path: LAN interface duplex</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In-path: WAN interface speed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In-path: WAN interface duplex</td>
<td></td>
</tr>
</tbody>
</table>

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 it is in the off position on the rear of the SteelHead.
2. Plug the AC power cord into the SteelHead.

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

Figure 3-4. Connecting the AC power

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

4. Press the system power switch on.

   If the SteelHead doesn’t immediately power on, press the power switch off, then press the power switch on again.

5. Check the status lights on the SteelHead.

   For detailed information about the status lights, see Appendix A, “Series EX xx60 Technical Specifications.”

Note: The 1U and 2U SteelHead EXs (Series xx60) take 15 minutes to start. The EX560 and EX760 take about 7 minutes to start.

Configuring in-path SteelHead EX appliances

In a physical in-path deployment, the SteelHead is physically in the direct path between clients and servers. The clients and servers continue to see client and server IP addresses. Physical in-path configurations are suitable for any location where the total bandwidth is within the limits of the installed SteelHead. For more information about in-path configurations, see “Choosing a network deployment” on page 29.

For detailed information about in-path deployments, see the SteelHead Deployment Guide.

You use standard Ethernet straight-through and crossover cables to connect to your network in an in-path configuration. Make sure that you use the correct cables to establish your network connections:

- **Straight-through cables** - Primary and LAN ports on the appliance to the LAN switch.
- **Crossover cable** - WAN port on the appliance to the WAN router.
Connecting the SteelHead EX to your network

You use standard Ethernet straight-through and crossover cables to connect to your network in an in-path configuration. Make sure that you use the correct cables to establish your network connections:

- **Straight-through cables** - Primary and LAN ports on the appliance to the LAN switch.
- **Crossover cable** - WAN port on the appliance to the WAN router.

To connect to the SteelHead to your network

1. 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 3-5. Connecting the primary port to the LAN switch](image1)

   **Figure 3-5. Connecting the primary port to the LAN switch**

2. Identify the straight-through cable that connects your LAN switch to your WAN router. Unplug the end connected to the WAN router.

   ![Figure 3-6. Disconnecting the WAN router](image2)

   **Figure 3-6. Disconnecting the WAN router**

3. Plug the straight-through cable that you disconnected from the WAN router into the LAN port of the SteelHead.

   ![Figure 3-7. Connecting the LAN switch to the LAN port](image3)

   **Figure 3-7. Connecting the LAN switch to the LAN port**
4. Using the provided crossover cable, plug the cable into the WAN port of the SteelHead and the WAN router.

Figure 3-8. Connecting the WAN port to the WAN router

Note: If you have a four-port or six-port bypass card, repeat Step 1 through Step 4. For detailed information about installing additional bypass cards, see the Network and Storage Card Installation Guide.

Running the configuration wizard

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

To run the configuration wizard

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

Figure 3-9. Connecting to the SteelHead

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

   - Baud rate: 9600 bps
   - Data bits: 8
   - Parity: none
   - Stop bits: 1
   - vt100 emulation
   - No flow control

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

   We recommend that you connect the console port to a device that logs output. Even though this isn't 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 SteelHead using the configuration wizard.

4. If you have a SteelCentral Controller for SteelHead (SCC) appliance installed in your network to manage multiple SteelHeads, you can use it to automatically configure them:

Do you want to auto-configure using a SCC? no

If you answer yes, you are prompted for the SCC hostname or IP address. The hostname or IP address is used to contact the SCC. The default value is riverbedcmc. If you enter no, the wizard continues.

**Note:** If you mistakenly answer yes, to return to the wizard from the CLI, enter the configuration jump-start command from configuration mode. For detailed information, see the “To restart the configuration wizard” on page 42.

5. To start the configuration wizard, enter yes at the system prompt.

Do you want to use the configuration wizard for initial configuration? yes

Press Enter to enter the default value; press ? for help; press Ctrl+B to go back to the previous step.

6. Complete the configuration wizard steps on the client-side and the server-side SteelHeads as described in the following table.

<table>
<thead>
<tr>
<th>Wizard prompt</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: Host name?</td>
<td>Enter the host name for the SteelHead.</td>
<td>hostname? amnesiac</td>
</tr>
<tr>
<td>Step 2: Use DHCP on the primary interface?</td>
<td>You are given the option to enable the DHCP to automatically assign an IP address to the primary interface for the SteelHead.</td>
<td>Use DHCP? no</td>
</tr>
<tr>
<td></td>
<td>We recommend that you do not set DHCP.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The default value is no.</td>
<td></td>
</tr>
<tr>
<td>Step 3: Primary IP address?</td>
<td>Enter the IP address for the SteelHead.</td>
<td>Primary IP address? 10.10.10.6</td>
</tr>
<tr>
<td>Step 4: Netmask?</td>
<td>Enter the netmask address.</td>
<td>Netmask? 255.255.0.0</td>
</tr>
<tr>
<td>Step 5: Default gateway?</td>
<td>Enter the default gateway for the SteelHead.</td>
<td>Default gateway? 10.0.0.1</td>
</tr>
<tr>
<td>Step 6: Primary DNS server?</td>
<td>Enter the primary DNS server IP address.</td>
<td>Primary DNS server? 10.0.0.2</td>
</tr>
<tr>
<td>Wizard prompt</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>Step 7: Domain name?</td>
<td>Enter the domain name for the network where the SteelHead is to reside. If you set a domain name, you can enter hostnames in the system without the domain name.</td>
<td>Domain name? example.com</td>
</tr>
<tr>
<td>Step 8: Admin password?</td>
<td>We strongly recommend that you change the default administrator password at this time. The password must be a minimum of six characters.</td>
<td>Admin password? xxxyyy</td>
</tr>
<tr>
<td>Step 9: SMTP server?</td>
<td>Enter the name of the SMTP server. External DNS and external access for SMTP traffic is required for email notification of events and failures to function.</td>
<td>SMTP server? natoma</td>
</tr>
<tr>
<td></td>
<td><strong>Important:</strong> Make sure that you provide a valid SMTP server to ensure that the email notifications for events and failures are sent to the correct destinations.</td>
<td></td>
</tr>
<tr>
<td>Step 10: Notification email address?</td>
<td>Enter a valid email address to which notification of events and failures are to be sent.</td>
<td>Notification email address? <a href="mailto:example@example.com">example@example.com</a></td>
</tr>
<tr>
<td>Step 11: Set the primary interface speed?</td>
<td>Enter the speed on the primary interface (that is, the SteelHead). Make sure that this value matches the setting on your router or switch. The default value is auto.</td>
<td>Set the primary interface speed? [auto] auto</td>
</tr>
<tr>
<td>Step 12: Set the primary interface duplex?</td>
<td>Enter the duplex mode on the primary interface. Make sure that this value matches the setting on your router or switch. The default value is auto.</td>
<td>Set the primary interface duplex? [auto] auto</td>
</tr>
</tbody>
</table>
Wizard prompt | Description | Example
--- | --- | ---
Step 13: Would you like to activate the in-path configuration? | Enter yes at the system prompt to configure in-path support. An in-path configuration is a configuration in which the SteelHead is in the direct path of the client and server. For detailed information about in-path configurations, see the SteelHead Deployment Guide. | Would you like to activate the in-path configuration? yes

Step 14: In-Path IP address? | Enter the in-path IP address for the SteelHead. | In-Path IP address? 10.11.11.6

Step 15: In-Path Netmask? | Enter the in-path netmask address. | In-Path Netmask? 255.255.0.0

Step 16: In-Path Default gateway? | Enter the in-path default gateway (the WAN gateway). | In-Path Default Gateway? 10.11.11.16

Step 17: Set the in-path: LAN interface speed? | Enter the in-path, LAN interface speed. Make sure that this value matches the setting on your router or switch. The default value is auto. | Set the in-path: LAN interface speed? [auto] auto

Step 18: Set the in-path: LAN interface duplex? | Enter the in-path, LAN duplex value. Make sure that this value matches the setting on your router or switch. The default value is auto. | Set the in-path: LAN interface duplex? [auto] auto

Step 19: Set the in-path: WAN interface speed? | Enter the in-path, WAN interface speed. Make sure that this value matches the setting on your router or switch. The default value is auto. | Set the in-path: WAN interface speed? [auto] auto

Step 20: Set the in-path: WAN interface duplex? | Enter the in-path, WAN duplex speed. Make sure that this value matches the setting on your router or switch. The default value is auto. | Set the in-path: WAN interface duplex? [auto] auto

7. The system confirms your settings.

You have entered the following information:
1. Hostname: amnesiac
2. Use DHCP on primary interface: no
3. Primary IP address: 10.10.10.6
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: xxxxyyy
9. SMTP server: natoma
10. Notification email address: example@example.com
11. Set the primary interface speed: auto
12. Set the primary interface duplex: auto
13. Would you like to activate the in-path configuration: yes
14. In-Path IP address: 10.11.11.6
15. In-Path Netmask: 255.255.0.0
16. In-Path Default gateway: 10.11.11.16
17. Set the in-path:LAN interface speed: auto
18. Set the in-path:LAN interface duplex: auto
19. Set the in-path:WAN interface speed: auto
20. Set the in-path:WAN interface duplex: auto

To change an answer, enter the step number to return to. Otherwise hit <enter> to save changes and exit.

Choice:

The SteelHead configuration wizard automatically saves your configuration settings.

8. To log out of the system, enter the following command at the system prompt:
   ```plaintext
   amnesiac> exit
   ```

To restart the configuration wizard

- Enter the following set of commands at the system prompt:
  ```plaintext
  > enable
  # configure terminal
  (config) # configuration jump-start
  ```

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

**Verifying you are connected to the SteelHead**

Perform the following tasks to verify that you have properly connected the SteelHead.

**To verify you are connected to the SteelHead**

1. Verify that you can connect to the CLI using one of the following devices:
   - An ASCII terminal or emulator that can connect to the serial console. It must have the following 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 SteelHead primary port.

2. At the system prompt, enter the following command:
   ```plaintext
   ssh admin@host.domain
   ```
   or
   ```plaintext
   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:
   ```plaintext
   ping -I <primary-IP-address> <primary-default-gateway>
   ```

5. At the system prompt, ping from the in-path default gateway:
   ```plaintext
   ping -I <in-path-IP-address> <in-path-default-gateway>
   ```
If you have problems connecting to the SteelHead, use the following flow chart to troubleshoot issues.

Figure 3-10. Resolving IP connectivity
Connecting to the Management Console

After you configure the SteelHead, you can check and modify your configuration settings and view performance reports and system logs in the Management Console. You can connect to the Management Console through any supported web browser.

To connect to the Management 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.

To connect to the Management Console

1. Specify the URL for the Management Console in the location box of your web browser:

   \[ protocol://host.domain \]

   *protocol* is http or https. HTTPS uses the SSL protocol to ensure a secure environment. When you connect using HTTPS, the system prompts you to inspect and verify the SSL certificate. This is a self-signed certificate that provides encrypted web connections to the Management Console. The system re-creates the certificate when you change the appliance hostname or when the certificate expires.

   The secure vault doesn’t protect the self-signed certificate used with HTTPS connections.

   *host* is the hostname you assigned to the SteelHead primary interface in the configuration wizard. If your DNS server maps that IP address to a name, you can specify the DNS name.

   *domain* is the full domain name for the appliance.

   Note: Alternatively, you can specify the IP address instead of the host and domain name.

   The Management Console appears, displaying the Sign In page.

   Figure 3-11. Sign in page

2. In the Username text box, specify the user login: admin, monitor, a login from a RADIUS or TACACS+ database, or any local accounts created using the Role-Based Accounts feature. The default login is admin.

   Users with administrator (admin) privileges can configure and administer the SteelHead. Users with monitor (monitor) privileges can view the SteelHead reports, user logs, and change their own password. A monitor user can’t make configuration changes.
3. In the Password text box, type the password you assigned in the configuration wizard of the SteelHead. (The default administrator password for the SteelHead is **password**.)

4. Click **Sign In** to display the Dashboard.

### Verifying WAN optimization

Perform the following tasks to verify that you have properly configured the SteelHead.

**To verify optimization**

1. Go to the Reports > Optimization: Bandwidth Optimization in the Management Console to verify optimization.

2. Map a remote drive on a client machine.

3. Drag and drop a 1-MB file from the client to the remote server.
   
   Ensure that the server is located across the WAN.

4. Drag and drop the 1-MB file again.
   
   Performance improves significantly.

### Checking for speed and duplex errors

If you selected autonegotiation (auto) for your in-path and primary interfaces, you must ensure that the SteelHead negotiated the speed and duplex at the rate your devices expect. For example, ensure settings are **auto** on the LAN and WAN and **100 FULL** on the LAN and WAN. You can verify your speed and duplex settings in the Configure > Networking: Inpath0_0 page and the Configure > Networking: Base Interfaces page of the Management Console.

**To check for speed and duplex errors**

1. In the Management Console, go to the Reports > Diagnostics: System Logs page.

2. Check the system logs for duplex or speed errors.


4. Check for duplex and speed errors.
   
   If you find errors, change the speed and duplex settings on your LAN and WAN interface in the Configure > Networking: Inpath 0_0 page.

### Configuring out-of-path SteelHead EX appliances

In an out-of-path deployment, the SteelHead isn't in the direct path between the client and the server. Servers see the IP address of the server-side SteelHead rather than the client-side IP address.
An out-of-path configuration is suitable for data center locations where physical in-path or logical in-path configurations aren't possible. For a detailed figure, see “Choosing a network deployment” on page 29.

For detailed information about out-of-path deployments, see the SteelHead Deployment Guide.

**Connecting out-of-path SteelHead EX appliances to your network**

You use a standard Ethernet straight-through cable to connect the primary port of the SteelHead to the LAN switch in an out-of-path configuration.

**To connect an out-of-path SteelHead 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 that is configured to connect to a host.

**Figure 3-12. Connecting the primary port and LAN switch**

![Diagram of connecting primary port and LAN switch](image)

**Configuring the server-side SteelHead**

The configuration wizard automatically starts when you log in to the SteelHead CLI for the first time. For detailed information about the configuration wizard and how to start it, see “To run the configuration wizard” on page 38.

In an out-of-path configuration, the client-side SteelHead is configured as an in-path device and the server-side SteelHead is configured as an out-of-path device.

**To configure the server-side SteelHead**

1. Check the duplex and speed settings on the router and switch that connects to your SteelHead. Make sure that the settings on the router, switch, and the SteelHead match. For example, ensure that settings are auto speed and duplex on the LAN and WAN or 100 FULL on the LAN and WAN. If the settings do not match, optimization might be degraded.

2. Connect to the CLI.
3. If you have a SteelCentral Controller for SteelHead appliance installed in your network to manage multiple SteelHeads, you can use it to automatically configure them.

Do you want to auto-configure using a SCC? no

If you enter yes, you are prompted for the SCC hostname or IP address. The hostname or IP address is used to contact the SCC. The default value is set to riverbedcmc. If you enter no, the wizard continues.

4. To start the configuration wizard, enter yes at the system prompt.

Do you want to use the configuration wizard for initial configuration? yes

Note: If you mistakenly answer no, to return to the wizard from the CLI, enter the configuration jump-start command from configuration mode. For detailed information, see the “To restart the configuration wizard” on page 42.

5. Complete the configuration wizard steps on the client side and server side.

<table>
<thead>
<tr>
<th>Wizard prompt</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: Host name?</td>
<td>Enter the hostname for the SteelHead.</td>
<td>Hostname? amnesiac</td>
</tr>
<tr>
<td>Step 2: Use DHCP on the primary interface?</td>
<td>You are given the option to enable the DHCP to automatically assign an IP address to the primary interface for the SteelHead. We recommend that you do not set DHCP. The default value is no.</td>
<td>Use DHCP? no</td>
</tr>
<tr>
<td>Step 3: Primary IP address?</td>
<td>Enter the IP address for the SteelHead.</td>
<td>Primary IP address? 10.10.10.6</td>
</tr>
<tr>
<td>Step 4: Netmask?</td>
<td>Enter the netmask address.</td>
<td>Netmask? 255.255.0.0</td>
</tr>
<tr>
<td>Step 5: Default gateway?</td>
<td>Enter the default gateway for the SteelHead.</td>
<td>Default gateway? 10.0.0.1</td>
</tr>
<tr>
<td>Step 6: Primary DNS server?</td>
<td>Enter the primary DNS server IP address.</td>
<td>Primary DNS server? 10.0.0.2</td>
</tr>
<tr>
<td>Step 7: Domain name?</td>
<td>Enter the domain name for the network where the SteelHead is to reside. If you set a domain name, you can enter hostnames in the system without the domain name.</td>
<td>Domain name? example.com</td>
</tr>
<tr>
<td>Step 8: Admin password?</td>
<td>We strongly recommend that you change the default administrator password at this time. The password must be a minimum of six characters. The default administrator password is password.</td>
<td>Admin password? xxxyyy</td>
</tr>
<tr>
<td><strong>Wizard prompt</strong></td>
<td><strong>Description</strong></td>
<td><strong>Example</strong></td>
</tr>
<tr>
<td>------------------</td>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Step 9: SMTP server?</td>
<td>Enter the SMTP server. External DNS and external access for SMTP traffic is required for email notification of events and failures.</td>
<td>SMTP server? natoma</td>
</tr>
<tr>
<td><strong>Important:</strong> Make sure that you provide a valid SMTP server to ensure that the email notifications for events and failures.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 10: Notification email address?</td>
<td>Enter a valid email address to receive email notification of events and failures.</td>
<td>Notification email address? <a href="mailto:example@example.com">example@example.com</a></td>
</tr>
<tr>
<td>Step 11: Set the primary interface speed?</td>
<td>Enter the speed on the primary interface (that is, the SteelHead). Make sure that this value matches the setting on your router or switch. The default value is auto.</td>
<td>Set the primary interface speed? [auto] auto</td>
</tr>
<tr>
<td>Step 12: Set the primary interface duplex?</td>
<td>Enter the duplex mode on the primary interface, and type a value at the system prompt. Make sure that this value matches the setting on your router or switch. The default value is auto.</td>
<td>Set the primary interface duplex? [auto] auto</td>
</tr>
<tr>
<td>Step 13: Would you like to activate the in-path configuration?</td>
<td>Enter <strong>no</strong> at the system prompt to configure in-path support. An in-path configuration is a configuration in which the SteelHead is in the direct path of the client and server. For detailed information about in-path configurations, see the <em>SteelHead Deployment Guide</em>.</td>
<td>Would you like to activate the in-path configuration? no</td>
</tr>
<tr>
<td>Step 14: Would you like to activate the out-of-path configuration?</td>
<td>Enter <strong>yes</strong> at the system prompt to configure out-of-path support. An out-of-path configuration is a configuration in which the SteelHead isn’t in the direct path of the client and server. For detailed information about in-path configurations, see the <em>SteelHead Deployment Guide</em>.</td>
<td>Would you like to activate the out-of-path configuration? [no] yes</td>
</tr>
</tbody>
</table>
The system confirms your settings:

You have entered the following information:
Step 1: Hostname? amnesiac
Step 2: Use DHCP on primary interface? no
Step 3: Primary IP address? 10.10.10.6
Step 4: Netmask? 255.255.0.0
Step 5: Default gateway? 10.0.0.1
Step 6: Primary DNS server? 10.0.0.2
Step 7: Domain name? example.com
Step 8: Admin password? xxyyyy
Step 9: SMTP server? natoma
Step 10: Notification email address? example@example.com
Step 11: Set the primary interface speed? auto
Step 12: Set the primary interface duplex? auto
Step 13: Would you like to activate the in-path configuration: no
Step 14: Would you like to activate the out-of-path configuration? yes

To change an answer, enter the step number to return to. Otherwise hit <enter> to save changes and exit.

The SteelHead configuration wizard automatically saves your settings.

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

   For details on restarting the configuration wizard, see “To restart the configuration wizard” on page 42.

Configuring the client-side SteelHead

In an out-of-path configuration, you configure the client-side SteelHead in the same way as in an in-path configuration. For optimization to occur, you must define a fixed-target rule on the client-side SteelHead that points to the out-of-path, server-side SteelHead. You can define fixed-target rules using the Management Console or the CLI.

For detailed information about the Management Console, see the SteelHead Management Console User’s Guide.

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

The following procedures describe how to configure in-path rules using the Management Console.

To configure the client-side SteelHead

1. Follow the procedures for an in-path configuration.
   For details, see “Configuring in-path SteelHead EX appliances” on page 36.

2. Connect to the Management Console.
   For details, see “Connecting to the Management Console” on page 44.
3. Choose the Optimization > Network Services: In-Path Rules page.

4. Under In-Path Rules, click Add a New In-Path Rule to display the in-path rule configuration options.

5. For Type, select Fixed-Target from the drop-down list.

6. For Target Appliance IP Address, specify the IP address and port number for the peer SteelHead.
   Use one of these formats:
   XXX.XXX.XXX.XXX/XX (IPv4)
   X:X::X/XXX (IPv6)
   The IP address must be the primary Port IP address on the target SteelHead. The default port is 7810.

7. (Optional) If you have a backup (out-of-path) SteelHead in your system (for failover support), note the following:
   For the Backup Appliance IP Address, specify the IP address and port for the backup appliance in the Backup IP and Port text boxes. Use one of these formats:
   XXX.XXX.XXX.XXX/XX (IPv4)
   X:X::X/XXX (IPv6)
   The default port is 7810.

8. Click Add to apply the rule to the running configuration.
9. Click **Save** to write your settings to memory.

   For detailed information about verifying your connections and configuration settings, see “Verifying you are connected to the SteelHead" on page 42 and “Verifying WAN optimization” on page 45.

You can now optimize WAN traffic using the SteelHead.
Troubleshooting

This chapter describes how to troubleshoot the SteelHead installation and describes how to investigate and solve issues with the following common problems:

- “Cables” on page 53
- “Duplex mismatch” on page 54
- “In-path SteelHead connection” on page 55
- “Oplock issues” on page 55
- “CIFS overlapping open optimization denies multi-user access” on page 57
- “IP address configuration” on page 58
- “Asymmetric routing” on page 59
- “Packet ricochet” on page 59
- “Packet ricochet—Internet Control Messaging Protocol (ICMP) redirects” on page 60
- “Simplified routing” on page 60
- “Autodiscovery failure” on page 62
- “Protocol optimization errors” on page 62
- “Server-side out-of-path connection caveats” on page 63
- “Specific problems” on page 63
- “Resetting a lost password” on page 64

Cables

Improper cabling prevents smooth traffic flows between the SteelHead and the router or switch.

Solution

To ensure that the traffic flows when the SteelHead is optimizing traffic, and when the SteelHead transitions to bypass mode, use the appropriate crossover or straight-through cable to connect the SteelHead to a router or switch. Verify the cable selection by removing the power cable from the appliance, and then test connectivity through it.
Make sure that you have connected your cables as follows:

- SteelHead to router: crossover cable
- SteelHead to switch: straight-through cable
- SteelHead to SteelHead: crossover cable
- SteelHead to a host: crossover cable

**Duplex mismatch**

The following symptoms occur due to a duplex mismatch:

- Access isn't faster after configuring the SteelHead.
- The interface counters display error messages. An alarm or log message about error counts appears.
- The pass through rule is ineffective. (This is a definite indication of duplex mismatch.)
- There are many retransmissions in packet traces.
- You can't connect to an attached device.
- You can connect with a device when you choose auto-negotiation, but you can't connect with the same device when you manually set the speed or duplex.
- Good performance for one direction of data flow, but poor performance in the opposite direction.

**Possible cause**

- You have probably set the duplex value for your router to 100Full (fixed) and for the SteelHead to Auto.

**Example**

The following example shows applications that appear slower with SteelHeads configured in an in-path deployment. The timed performance numbers to transfer a 20 MB file over FTP are:

- no SteelHead – 3:16
- cold SteelHead – 5:08
- warm SteelHead – 3:46

Adding a pass through rule for an application doesn't help. Slow connections appear as optimized in the Management Console on the Current Connections report page. However, stopping the SteelHead service while leaving the system powered on and an in-path configuration returns performance to original levels.

**Solutions**

To resolve the duplex mismatch error:

- Connect to the SteelHead CLI and enter the flood-ping command to check the duplex mismatch:

  ```
  ping -f -I >in-path-ip> -s 1400 <clientIP>
  ```
- Change the interface speed and duplex to match.
- Ensure there is a speed and duplex match between each in-path interface and its peer network interface. If they do not match, you might have a large number of errors on the interface when it is in the bypass mode, because the switch and the router aren’t set with the same duplex settings. Also, ensure connectivity when service is down.
  
  If matching speed and duplex do not reduce collisions or errors, try hard-setting one end and auto-setting the other. Try the half-duplex mode.
- If all combinations fail, as a last resort, add an intermediary hub or switch that is more compatible with both network interfaces.

**In-path SteelHead connection**

When there are SteelHeads with in-path connection issues, the two sites are connected in-path and you can ping them, but they can’t connect to each other to optimize data.

**Possible cause**

The firewall is running port filtering and drops your probe packets. The firewall is filtering the IP and port address of the source and destination (bandwidth limitation) systems.

**Solutions**

To resolve the SteelHead connection issue:

- open port 7800 on both firewalls.
- use the port visibility mode.
- if there is no encryption, place the SteelHead after the firewall.

**Oplock issues**

The following symptoms occur due to opportunistic lock (oplock) issues:

- File access isn't faster or tasks such as drag-and-drop are fast but applications might benefit from acceleration.
- The Current Connections report page in the Management Console (select Reports > Networking: Current Connections) displays slow connections as optimized.

**Possible causes**

- The client is running an old anti-virus software such as McAfee v4.5, the most common type, which competes with the application for an oplock instead of opening as read-only. The antivirus causes multiple file opens.
- The server has oplocks disabled.
Example
You can open a previously-accessed file in 5 seconds on PC1, but you can’t open the same file under 24 seconds on PC2. If you close the file on PC1, you can open it in 5 seconds on PC2. However, it takes you 24 seconds to open the same file on PC1.

Solutions
Windows Common Internet File System (CIFS) uses oplock to determine the level of safety the OS or the application has in working with a file. Oplock is a lock that a client requests on a file in a remote server. An oplock controls the consistency of optimizations such as read-ahead. Oplock levels are reduced when you make conflicting opens to a file.

To prevent any compromise to data integrity, the SteelHead only optimizes data when a client has exclusive access to the data.

When an oplock isn’t available, the SteelHead doesn’t perform application-level latency optimization but still performs Scalable Data Referencing (SDR) and data compression as well as TCP optimization. Therefore, even without the benefits of latency optimization, SteelHeads still increase WAN performance, but not as effectively as when application optimizations are available.

To resolve oplock issues:

- Upgrade your anti-virus software to the latest version.
- Use Filemon (sysinternals) to check for file access.
- Enable CIFS Overlapping Opens (by default, this function is enabled). For details, see “CIFS overlapping open optimization denies multi-user access” on page 57.
- Ensure that the server has oplock enabled by verifying registry settings on Windows servers or the Filer configuration (for NetApp or EMC servers).
- Run a network analyzer such as Riverbed SteelCentral Pilot, which is fully integrated with Wireshark, and determine that the server grants oplocks when the client opens a file.
- Check whether the client is running an anti-virus software that is scanning the files over the WAN or that the anti-virus software doesn’t break the oplock.
CIFS overlapping open optimization denies multi-user access

The CIFS overlapping open optimization issue prevents a client from accessing a file when different clients access the file at the same time.

Solution

To resolve the CIFS overlapping open optimization issue, configure CIFS overlapping open optimization on the client-side SteelHead as follows:

1. Connect to the SteelHead Management Console.
   For details, see the SteelHead Management Console User’s Guide.

2. On the client-side SteelHead, choose Optimization > Protocols: CIFS (SMB1) to display the CIFS (SMB1) page.

Figure 4-1. CIFS (SMB1) page
3. Under Overlapping Open Optimization (Advanced), complete the configuration as described in the following table.

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Overlapping Open Optimization</td>
<td>Enables overlapping opens to obtain better performance with applications that perform multiple opens on the same file: for example, CAD applications. By default, this setting is disabled.</td>
</tr>
<tr>
<td>Note</td>
<td>Enable this setting on the client-side SteelHead.</td>
</tr>
<tr>
<td></td>
<td>With overlapping opens enabled, the SteelHead optimizes data where exclusive access is available (when locks are granted). When an oplock isn’t available, the SteelHead doesn’t perform application-level latency optimizations but still performs SDR and compression on the data as well as TCP optimizations.</td>
</tr>
<tr>
<td></td>
<td>Note: If a remote user opens a file that is optimized using the overlapping opens feature and a second user opens the same file, they might receive an error message if the file fails to go through a v3.x.x or later SteelHead or if it doesn't go through a SteelHead: for example, certain applications that are sent over the LAN. If this occurs, you should disable overlapping opens for such applications.</td>
</tr>
<tr>
<td></td>
<td>Use the radio buttons to set either an include list or exclude list of file types subject to overlapping opens optimization.</td>
</tr>
</tbody>
</table>

4. Click **Apply** to apply your settings to the current configuration.

5. Click **Save** to save your settings permanently.

### IP address configuration

If you haven’t configured IP addresses correctly, the SteelHeads can’t connect to each other or to your network.

### Solutions

To verify the IP address has been configured correctly:

- Ensure the SteelHeads are reachable through the IP address, by pinging their primary and in-path interfaces.
- Ensure that the SteelHeads in the network can reach each other through their own interfaces.

Connect to the SteelHead CLI. For details, see the *Riverbed Command-Line Interface Reference Manual*. Enter the following command to ping from a specific in-path interface on a SteelHead to another in-path interface:

```
ping -f -I (Local-SteelHead-Inpath-IP) -s 1400 (Remote-SteelHead-Inpath-IP)
```

- Ensure that the default gateways, both for the SteelHead and for its in-path interfaces, are correct.
Asymmetric routing

If there is an asymmetric routing issue, many connections fail during data transfer or they fail to start.

Possible cause

Asymmetric routing occurs when a TCP connection takes one path to the destination and another when returning to the source. If the SteelHead sees only the LAN to WAN or only the WAN to LAN packets, it can’t optimize the data.

Solutions

To resolve the asymmetric routing issue, do one of the following:

- Rank the following solutions from most to least preferable with respect to complexity and cost and select one:
  - configure a fixed-target rule.
  - use a logical in-path configuration such as WCCP or PBR.
  - use four-port or six-port SteelHead.
  - configure connection-forwarding with two SteelHeads.
- Remove the asymmetry.

Packet ricochet

The following symptoms occur due to packet ricochet:

- Performance is less than expected
- The following log message appears:

  ```
  » [fionr taelrcreeapdt/ y lnoactaltekde rnceoln/neiccotireo. n c:119426.316] 8.n7a3t._1c5h:e1c6k1: 1 SYN ==> packet 192.168.208.12:80 ==> 192.168.72.9:7801
  ```
**Possible cause**
Traffic to the LAN is travelling to the WAN router on the way to the LAN.

**Solutions**
To resolve packet ricochet issues:
- Change the in-path gateway to the LAN router.
- Add static routes to LAN subnets through the LAN router.
- Enable in-path simplified routing.

**Packet ricochet—Internet Control Messaging Protocol (ICMP) redirects**
The following symptoms occur due to packet ricochet ICMP redirects:
- Connections fail on first attempt, but succeed on second attempt.
- On one or both sites, the in-path interface on the SteelHead is on a different network than the local host.
- There are no in-path routes defined.

**Possible causes**
- Traffic to the LAN is travelling to the WAN router on the way to the LAN, but the router drops the packet.
- Outer connections to clients or servers are routed through the WAN interface to the WAN gateway, and then routed through the SteelHead to the next hop LAN gateway.
- The WAN router is probably dropping the SYN from the SteelHead before issuing an ICMP redirect.

**Solutions**
To resolve the packet ricochet ICMP redirects issue, do one of the following:
- Change the router ICMP configuration to forward the packet or turn off ICMP redirect.
- Change the in-path gateway to the LAN router.
- Add static routes to LAN subnets through the LAN router.
- Enable in-path simplified routing. For details, see “Simplified routing” on page 60.
- Add in-path routes to local destinations to prevent the ICMP redirect and subsequent drop.

**Simplified routing**
Simplified routing changes the process used to select the destination Ethernet address for packets transmitted from in-path interfaces.
Simplified routing collects the IP address for the next hop MAC address from each packet it receives to address traffic. With simplified routing, you can use either the WAN or LAN-side device as a default gateway. The SteelHead learns the right gateway to use by watching where the switch or router sends the traffic, and by associating the next-hop Ethernet addresses with IP addresses. Enabling simplified routing eliminates the need to add static routes when the SteelHead is in a different subnet from the client and the server.

Without simplified routing, if a SteelHead is installed in a different subnet from the client or server, you must define one router as the default gateway and static routes for the other routers so that traffic isn't redirected back through the SteelHead. In some cases, even with the static routes defined, the Access Control List (ACL) on the default gateway can still drop traffic that should have gone through the other router. Enabling simplified routing eliminates this issue.

Simplified routing has the following constraints:

- You can't enable WCCP.
- The default route must exist on each SteelHead in your network.

**Note:** For detailed information, see the *SteelHead Deployment Guide*.

**To enable simplified routing**


**Figure 4-2. Simplified Routing page**

![Simplified Routing page](image)

2. Under Mapping Data Collection Setting, complete the configuration as described in the following table.
3. Click **Apply** to save your settings to the running configuration.

4. Click **Save** to save your settings permanently.

### Autodiscovery failure

When autodiscovery fails, all traffic passes through with the SteelHead in-path (physically or logically).

#### Possible causes
- Cisco PIX 7.x or Raptor firewalls
- Satellite
- Intrusion Detection System (IDS) or Intrusion Prevention System (IPS)

#### Solutions
- Create a fixed-target rule on the client-side SteelHead.
  - Specify the **Target Appliance IP Address** and its port as 7800 on the opposite SteelHead (in-path without autodiscovery).
- Configure end nodes (firewalls) to allow your probe to pass through.
- Configure the SteelHead IP address as the friendly IP address for IDS or IPS.
- Cisco PIX Firewall IOS v7.0 might block the autodiscovery probe. Some firewall configurations strip TCP options or drop packets with these options. You can keep this configuration and switch to fixed-target rules or change the configuration on the firewall.

### Protocol optimization errors

When there are protocol optimization errors, the SteelHead does not optimize expected protocols.
Solutions
To resolve protocol optimization errors, check:
- that connections have been successfully established.
- that SteelHeads on the other side of a connection are turned on.
- for secure or interactive ports that are preventing protocol optimization.
- for any pass through rules that could be causing some protocols to pass through the SteelHeads unoptimized.
- that the LAN and WAN cables aren’t inadvertently swapped.

Server-side out-of-path connection caveats
The following are the caveats for a server-side out-of-path (OOP) SteelHead connection:
- OOP configuration doesn’t support autodiscovery. You must create a fixed-target rule on the client-side SteelHead.
- You must create an OOP connection from an in-path or logical in-path SteelHead and direct it to port 7810 on the primary interface of the server-side SteelHead. This setting is mandatory.
- Interception isn’t supported on the primary interface.
- An OOP configuration provides non-transparent optimization from the server perspective. Clients connect to servers, but servers treat it like a server-side SteelHead connection. This affects:
  - log files.
  - server-side ACLs.
  - bi-directional applications such as rsh.
- You can use OOP configurations along with in-path or logical in-path configurations.

Specific problems
The following section describes specific problems you might encounter in the SteelHead.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The <code>show interfaces</code> CLI command displays 4294967295 as the number of errors on an interface.</td>
<td>The bypass card isn’t properly installed; reinstall it. For details, see the Network and Storage Card Installation Guide.</td>
</tr>
<tr>
<td>The SteelHead blocks traffic when going into bypass mode.</td>
<td>If a SteelHead blocks traffic when going into bypass mode, verify that connections to its neighboring devices are correctly configured. Ensure that the cable from the SteelHead to the switch is a straight-through cable and the cable from the SteelHead to the router is a crossover cable. Also, ensure that there are no network speed or duplex mismatches.</td>
</tr>
</tbody>
</table>
Troubleshooting

## Resetting a lost password

To reset your password, you must have access to the serial console or monitor and must be able to see the entire boot process to perform these steps:

1. Start, or reboot the appliance.

2. When prompted, press any key to continue.

3. Immediately press E.

   A GNU GRUB menu appears.

   - For a SteelHead upgraded to 4.0 from 2.0 or 3.0, the menu prompts you to select the Riverbed SteelHead, diagnostics, or a restore/recovery image. Select Riverbed SteelHead and skip to Step 5.

   - For a SteelHead manufactured with 4.0 (that has not had previous versions), the menu prompts you to select the disk image to use. Continue with Step 4.

   - For software versions prior to 4.0, the menu displays root and kernel parameters. Skip to Step 6.

4. Press V or ^ to select the disk image to boot.

---

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
</table>
| The SteelHead doesn’t come out of bypass mode when the network connection is restored. | If a SteelHead doesn’t come out of bypass mode, verify that:  
- The in-path interface has an IP address. For example, at the system prompt, enter the `show interfaces` CLI command.  
- In-path interception is enabled. For example, at the system prompt, enter the `show in-path` CLI command. Expected results are:  
  - Enabled: yes  
  - Optimizations Enabled On: inpath0_0  
- The bypass service is running. For example, at the system prompt, enter the `show service` CLI command. To enable the SteelHead service if it isn’t running, use the CLI command `service enable`.
- You have a valid and active SH10BASE license. Your license file should also contain entries for SH10CIFS and SH10EXCH licenses, even if they haven’t been activated. For example, at the system prompt, enter the `show licenses` CLI command. For questions about licenses, contact Riverbed Support at https://support.riverbed.com |

| The SteelHead fails to boot. | Ensure that:  
- The power strip or the uninterruptable power supply (UPS) the SteelHead is plugged into is turned on and is functioning properly.  
- The rocker switch on the back of the SteelHead (Series xx20) is turned on. (When on, the rocker switch is in the depressed, or 1 position.) |
5. Press E. A GRUB menu appears, with options similar to the following:

```
0: root (hd0,1)
1: kernel /vmlinuz ro root=/dev/sda5 console=tty0 console=ttyS0,9600n8
```

6. Press V or ^ to select the kernel boot parameters entry.

7. Press E to edit the kernel boot parameters. The CLI displays a partially completed line of text similar to the following:

```
kernel /vmlinuz ro root=/dev/sda5 console=tty0 console=ttyS0,9600n8
```

8. The line of text contains two console= entries. Modify this line as follows:
   - If you are accessing the SteelHead remotely, delete `console=tty0`
   - If you are accessing the SteelHead directly (through a keyboard and monitor connected to the appliance), delete `console=ttyS0`
   - At the end of the line, type a space and append the line with `single fastboot`
     - You must include a space before the word `single`.

   **Note:** Use the arrow keys to access the entire command line.


10. Press B to continue booting. The system starts.

11. At the command prompt, enter `/sbin/resetpw.sh`. The password is blank.

12. Type `reboot` and press Enter to reboot the appliance.
Troubleshooting

Resetting a lost password
Series EX xx60 Technical Specifications

This appendix describes the status lights and ports, and the technical and environmental specifications. It includes these sections:

- “EX560 and EX760 specifications” on page 68
- “EX1160 specifications” on page 71
- “EX1260 specifications” on page 74
- “EX1360 specifications” on page 77
- “SteelHead EX hardware allocation” on page 81
- “VSP and SteelFusion storage specifications” on page 83
EX560 and EX760 specifications

This section describes the status lights and ports, and it provides technical and environmental specifications.

Status lights and ports

The following figures illustrate the EX560 and EX760 status light and port locations. For detailed information, see the *Series EX560 and EX760 Systems Owner's Manual*.

**Figure A-1. Front panel**

![Front panel diagram]

**Figure A-2. Back panel**

![Back panel diagram]

The following table summarizes the EX560 and EX760 system LEDs.

<table>
<thead>
<tr>
<th>LED</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power On/Power Button</td>
<td>The power-on indicator lights when the system power is on.</td>
</tr>
<tr>
<td></td>
<td>When the system bezel is installed, the power button isn't accessible.</td>
</tr>
<tr>
<td>HDD</td>
<td>Lights when the hard disk drive (HDD) is in use.</td>
</tr>
</tbody>
</table>
### System Diagnostics (4)

<table>
<thead>
<tr>
<th>LED</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 2 3 4</td>
<td>The system is in a normal off condition or a possible pre-BIOS failure has occurred. Plug the system into a working electrical outlet and press the power button. The diagnostic lights aren't lit after the system successfully boots to the operating system. The system is in a normal operating condition after POST.</td>
</tr>
</tbody>
</table>

### BIOS checksum failure detected; system is in recovery mode. Contact Riverbed Support at [https://support.riverbed.com](https://support.riverbed.com).

### Possible processor failure. Contact Riverbed Support at [https://support.riverbed.com](https://support.riverbed.com).

### Memory failure. Contact Riverbed Support at [https://support.riverbed.com](https://support.riverbed.com).

### Possible NIC card failure. Contact Riverbed Support at [https://support.riverbed.com](https://support.riverbed.com).

### Possible video failure. Contact Riverbed Support at [https://support.riverbed.com](https://support.riverbed.com).

### Hard drive failure. Contact Riverbed Support at [https://support.riverbed.com](https://support.riverbed.com).

### Possible USB failure. Contact Riverbed Support at [https://support.riverbed.com](https://support.riverbed.com).

### Other failure. Contact Riverbed Support at [https://support.riverbed.com](https://support.riverbed.com).

### System Status

(On both the front and back panels) Lights blue when the system hardware is operating normally. Lights orange when the system needs attention due to a problem.

To determine the current status of the Management Console software, check the Management Console status bar.

### System ID Button

(On both the front and back panels) Enables you to locate a system within a rack. When you push either of the buttons, the system status indicators on the front and back panels light blue until you push one of the buttons again.

### SSD

Lights when the solid state drive (SSD) is in use.

### LAN-WAN Ports

<table>
<thead>
<tr>
<th>Link/Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>Green = LAN or WAN link is up.</td>
</tr>
<tr>
<td>Blinks green</td>
<td>Blinks green = LAN or WAN link is active.</td>
</tr>
<tr>
<td>Disconnect</td>
<td>Green = LAN or WAN link is in disconnect mode.</td>
</tr>
<tr>
<td>Bypass</td>
<td>Green = LAN or WAN link is in bypass mode.</td>
</tr>
</tbody>
</table>
Technical specifications

The following table summarizes the technical specifications for the systems.

<table>
<thead>
<tr>
<th></th>
<th>EX560 G/L/M/H</th>
<th>EX760 L/M/H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Form Factor</td>
<td>1U</td>
<td>1U</td>
</tr>
<tr>
<td>HDD / SSD</td>
<td>1 TB HDD</td>
<td>1 TB HDD</td>
</tr>
<tr>
<td></td>
<td>1 x 80 GB SSD</td>
<td>1 x 160 GB SSD</td>
</tr>
<tr>
<td>Data Store</td>
<td>40–70 GB</td>
<td>140 GB</td>
</tr>
<tr>
<td></td>
<td>380 GB VSP</td>
<td>380 GB VSP</td>
</tr>
<tr>
<td>Dimensions (LxWxH)</td>
<td>17.09 x 15.52 x 1.66 in (434.0 x 394.3 x 42.4 mm)</td>
<td>17.09 x 15.52 x 1.66 in (434.0 x 394.3 x 42.4 mm)</td>
</tr>
<tr>
<td>Weight (without packaging)</td>
<td>17.76 lbs (8.058 kg)</td>
<td>17.76 lbs (8.058 kg)</td>
</tr>
<tr>
<td>PCIe Slots</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Onboard Bypass Ports/Max # Ports</td>
<td>4/4</td>
<td>4/4</td>
</tr>
</tbody>
</table>

For more information about SteelFusion and VSP disk allocation, see “VSP and SteelFusion storage specifications” on page 83.

Power specifications

The following table summarizes the power specifications for the systems. The systems are rated at the following power characteristics when operating at nominal AC input voltages (120 V and 230 V).

<table>
<thead>
<tr>
<th>System</th>
<th>EX560/760</th>
<th>EX560/760</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration</td>
<td>All (G/L/M/H)</td>
<td>All (G/L/M/H)</td>
</tr>
<tr>
<td>PSU Type</td>
<td>1x250W</td>
<td>1x250W</td>
</tr>
<tr>
<td></td>
<td>100–240Vac, 50/60Hz, 2-1 A</td>
<td>100–240Vac, 50/60Hz, 2-1 A</td>
</tr>
<tr>
<td>AC Input</td>
<td>120V (100–127VAC)</td>
<td>230V (200–240VAC)</td>
</tr>
<tr>
<td>Max. Amps.</td>
<td>1.2</td>
<td>0.6</td>
</tr>
<tr>
<td>Max. Watts</td>
<td>135</td>
<td>135</td>
</tr>
<tr>
<td>Typical Watts</td>
<td>85</td>
<td>80</td>
</tr>
<tr>
<td>Max VA</td>
<td>140</td>
<td>140</td>
</tr>
<tr>
<td>Power Factor</td>
<td>97</td>
<td>97</td>
</tr>
<tr>
<td>Heat Dissipation in BTU/hour (Typical)</td>
<td>295</td>
<td>280</td>
</tr>
</tbody>
</table>
Environmental specifications

The following table summarizes the environmental requirements for the systems.

<table>
<thead>
<tr>
<th>EX560, EX760</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating Acoustic</td>
</tr>
<tr>
<td>Temperature (Operating)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Temperature (Storage)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Relative Humidity</td>
</tr>
<tr>
<td>Storage Humidity</td>
</tr>
<tr>
<td>Operating Altitude</td>
</tr>
</tbody>
</table>

EX1160 specifications

This section describes the status lights and ports, and it provides technical and environmental specifications for the EX1160 appliance.

Status lights and ports

The following figures illustrate the status lights and ports.

Figure A-3. Front panel

Figure A-4. Back panel
The following table summarizes the system LEDs.

<table>
<thead>
<tr>
<th>LED</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYSTEM</td>
<td>Normal = Blue</td>
</tr>
<tr>
<td></td>
<td>System Boot = Red</td>
</tr>
<tr>
<td>PRI = Primary</td>
<td>Link and Traffic = Blinks Blue</td>
</tr>
<tr>
<td>AUX = Auxiliary</td>
<td></td>
</tr>
<tr>
<td>REM = Remote</td>
<td></td>
</tr>
<tr>
<td>LAN-WAN</td>
<td>Link and Traffic = Blinks Blue</td>
</tr>
<tr>
<td>BYP/BLK</td>
<td>Normal = No Light</td>
</tr>
<tr>
<td>BYP = Bypass</td>
<td>Bypass or Block (Disconnect) = Orange</td>
</tr>
<tr>
<td>BLK = Block (Disconnect)</td>
<td></td>
</tr>
<tr>
<td>HDDs/SSDs</td>
<td>Disk Connected = Blue</td>
</tr>
<tr>
<td></td>
<td>Read/Write Activity = Blinks Blue</td>
</tr>
<tr>
<td></td>
<td>Failed Disk = Orange</td>
</tr>
<tr>
<td>Back Panel</td>
<td>Left LED</td>
</tr>
<tr>
<td>PRI = Primary</td>
<td>Link = Green</td>
</tr>
<tr>
<td>AUX = Auxiliary</td>
<td>Activity = Blinks Green</td>
</tr>
<tr>
<td>REM = Remote</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Right LED</td>
</tr>
<tr>
<td></td>
<td>GB = Orange</td>
</tr>
<tr>
<td></td>
<td>100 MB = Green</td>
</tr>
<tr>
<td></td>
<td>10 MB = No Light</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Back Panel</td>
<td>Left LED</td>
</tr>
<tr>
<td>LAN-WAN</td>
<td>Link = Green</td>
</tr>
<tr>
<td></td>
<td>Activity = Blinks Green</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Right LED</td>
</tr>
<tr>
<td></td>
<td>GB = Orange</td>
</tr>
<tr>
<td></td>
<td>100 MB = Green</td>
</tr>
<tr>
<td></td>
<td>10 MB = No Light</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>BYP/BLK</td>
</tr>
<tr>
<td></td>
<td>Normal = No Light</td>
</tr>
<tr>
<td></td>
<td>Bypass or Block (Disconnect) = Orange</td>
</tr>
</tbody>
</table>

**Technical specifications**

The following table summarizes the technical specifications for the systems.

<table>
<thead>
<tr>
<th></th>
<th>EX1160 G/L/M/H</th>
<th>EX1160 VH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Form Factor</td>
<td>1U</td>
<td>1 U</td>
</tr>
<tr>
<td>HDD / SSD</td>
<td>2 x 1 TB HDD</td>
<td>2 x 1 TB HDD</td>
</tr>
<tr>
<td></td>
<td>2 x 80 GB SSD</td>
<td>2 x 160 GB SSD</td>
</tr>
<tr>
<td>Data Store</td>
<td>140 GB SSD</td>
<td>280 GB SSD</td>
</tr>
<tr>
<td></td>
<td>415 GB VSP</td>
<td>415 GB VSP</td>
</tr>
</tbody>
</table>
EX1160 specifications

<table>
<thead>
<tr>
<th></th>
<th>EX1160 G/L/M/H</th>
<th>EX1160 VH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dimensions (LxWxH)</td>
<td>25.4 x 17.2x1.71 in</td>
<td>25.4 x 17.2x1.71 in</td>
</tr>
<tr>
<td></td>
<td>(645.4 x 436x43.5 mm)</td>
<td>(645.4 x 436 x 43.5 mm)</td>
</tr>
<tr>
<td>Weight (without packaging)</td>
<td>36 lbs (16.36 kg)</td>
<td>36 lbs (16.36 kg)</td>
</tr>
<tr>
<td>PCIe Slots</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Onboard Bypass Ports/ Max # Ports</td>
<td>4/8</td>
<td>4/8</td>
</tr>
</tbody>
</table>

For more information about SteelFusion and VSP disk allocation, see “VSP and SteelFusion storage specifications” on page 83.

Note: This table indicates the SSD disk capacity available to the system: disks in newer appliance models or replacement disks might be capable of a higher capacity (such as 100 GB instead of 80 GB or 200 GB instead of 160 GB), but the system still limits them to the capacity expected by the system and defined in this table.

Power specifications

The following table summarizes the power specifications for the systems. The systems are rated at the following power characteristics when operating at nominal AC input voltages (120 V and 230 V).

<table>
<thead>
<tr>
<th>System</th>
<th>EX1160</th>
<th>EX1160</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration</td>
<td>All (G/L/M/H/VH)</td>
<td>All (G/L/M/H/VH)</td>
</tr>
<tr>
<td>PSU Type</td>
<td>2 x 450 W</td>
<td>2 x 450 W</td>
</tr>
<tr>
<td></td>
<td>100 - 127 Vac</td>
<td>200 - 240 Vac</td>
</tr>
<tr>
<td></td>
<td>8A, 50/60 Hz</td>
<td>4A, 50/60 Hz</td>
</tr>
<tr>
<td>AC Input</td>
<td>120 V (100 - 127 VAC)</td>
<td>230 V (200 - 240 VAC)</td>
</tr>
<tr>
<td>Max. Amps.</td>
<td>4.1</td>
<td>3.4</td>
</tr>
<tr>
<td>Max. Watts</td>
<td>220</td>
<td>220</td>
</tr>
<tr>
<td>Typical Watts</td>
<td>175</td>
<td>180</td>
</tr>
<tr>
<td>Max VA</td>
<td>225</td>
<td>265</td>
</tr>
<tr>
<td>Power Factor</td>
<td>97</td>
<td>92</td>
</tr>
<tr>
<td>Heat Dissipation in BTU/hour (Typical)</td>
<td>605</td>
<td>610</td>
</tr>
</tbody>
</table>
Environmental specifications

The following table summarizes the environmental requirements for the systems.

<table>
<thead>
<tr>
<th></th>
<th>EX1160</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating Acoustic</td>
<td>61.5 dBA Sound pressure (Typical)</td>
</tr>
<tr>
<td>Temperature (Operating)</td>
<td>10º - 40ºC</td>
</tr>
<tr>
<td></td>
<td>50º - 104ºF</td>
</tr>
<tr>
<td>Temperature (Storage)</td>
<td>-40º - 65ºC</td>
</tr>
<tr>
<td></td>
<td>-40º - 149ºF</td>
</tr>
<tr>
<td>Relative Humidity</td>
<td>20% - 80%</td>
</tr>
<tr>
<td></td>
<td>noncondensing</td>
</tr>
<tr>
<td>Storage Humidity</td>
<td>5% - 95%</td>
</tr>
<tr>
<td></td>
<td>noncondensing</td>
</tr>
<tr>
<td>Operating Altitude</td>
<td>-50 ft - 10,000 ft</td>
</tr>
<tr>
<td></td>
<td>(-15.24 m - 3048 m)</td>
</tr>
</tbody>
</table>

EX1260 specifications

This section describes the status lights, ports, technical, and environmental specifications for EX1260 appliances.
Status lights and ports

The following figures illustrate the status lights and ports and identify the disk numbers and PCIe slots.

Figure A-5. Front panel

Figure A-6. Back panel

The following table summarizes the system LEDs.

<table>
<thead>
<tr>
<th>LED</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYSTEM</td>
<td>Normal = Blue</td>
</tr>
<tr>
<td></td>
<td>System Boot = Red</td>
</tr>
<tr>
<td>PRI</td>
<td>Link and Traffic = Blinks Blue</td>
</tr>
<tr>
<td>AUX</td>
<td></td>
</tr>
<tr>
<td>REM</td>
<td></td>
</tr>
<tr>
<td>LAN-WAN</td>
<td>Link and Traffic = Blinks Blue</td>
</tr>
<tr>
<td>BYP/BLK</td>
<td>Normal = No Light</td>
</tr>
<tr>
<td>BYP</td>
<td>Bypass or Block (Disconnect) = Orange</td>
</tr>
<tr>
<td>BLK</td>
<td></td>
</tr>
<tr>
<td>HDDs/SSDs</td>
<td>Disk Connected = Blue</td>
</tr>
<tr>
<td></td>
<td>Read/Write Activity = Blinks Blue</td>
</tr>
<tr>
<td></td>
<td>Failed Disk = Orange</td>
</tr>
</tbody>
</table>
### Technical specifications

The following table summarizes the technical specifications for the systems.

<table>
<thead>
<tr>
<th></th>
<th>EX1260-2 G/L/M/H</th>
<th>EX1260-2 VH</th>
<th>EX1260-4 G/L/M/H</th>
<th>EX1260-4 VH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Form Factor</td>
<td>2U</td>
<td>2U</td>
<td>2U</td>
<td>2U</td>
</tr>
<tr>
<td>HDD / SSD</td>
<td>4 x1 TB HDD</td>
<td>4 x1 TB HDD</td>
<td>8 x1 TB HDD</td>
<td>8 x1 TB HDD</td>
</tr>
<tr>
<td></td>
<td>2 x 80 GB SSD</td>
<td>4 x 80 GB SSD</td>
<td>2 x 80 GB SSDs</td>
<td>4 x 80 GB SSD</td>
</tr>
<tr>
<td>Data Store</td>
<td>140 GB</td>
<td>280 GB</td>
<td>140 GB</td>
<td>280 GB</td>
</tr>
<tr>
<td></td>
<td>860 GB VSP</td>
<td>860 GB VSP</td>
<td>1850 GB VSP</td>
<td>1850 GB VSP</td>
</tr>
<tr>
<td>Dimensions (LxWxH)</td>
<td>25.4 x 17.2 x 3.43 in (645.4 x 436 x 87.1 mm)</td>
<td>25.4 x 17.2 x 3.43 in (645.4 x 436 x 87.1 mm)</td>
<td>25.4 x 17.2 x 3.43 in (645.4 x 436 x 87.1 mm)</td>
<td>25.4 x 17.2 x 3.43 in (645.4 x 436 x 87.1 mm)</td>
</tr>
<tr>
<td>Weight (without packaging)</td>
<td>58 lbs (23.36 kg)</td>
<td>58 lbs (23.36 kg)</td>
<td>58 lbs (23.36 kg)</td>
<td>58 lbs (23.36 kg)</td>
</tr>
<tr>
<td>PCIe Slots</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Onboard Bypass Ports/Max # Ports</td>
<td>4/8</td>
<td>4/8</td>
<td>4/8</td>
<td>4/8</td>
</tr>
</tbody>
</table>

For more information about SteelFusion and VSP disk allocation, see “VSP and SteelFusion storage specifications” on page 83.

**Note:** This table indicates the SSD disk capacity available to the system. Disks in newer appliance models or replacement disks might be capable of a higher capacity (such as 100 GB instead of 80 GB or 200 GB instead of 160 GB), but the system still limits them to the capacity expected by the system and defined in this table.
Power specifications

The following table summarizes the power specifications for the systems. The systems are rated at the following power characteristics when operating at nominal AC input voltages (120 V and 230 V).

<table>
<thead>
<tr>
<th>System</th>
<th>EX1260 (2TB)</th>
<th>EX1260 (2TB)</th>
<th>EX1260 (4TB)</th>
<th>EX1260 (4TB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration</td>
<td>All (G, L, M, H, VH)</td>
<td>All (G, L, M, H, VH)</td>
<td>All (G, L, M, H, VH)</td>
<td>All (G, L, M, H, VH)</td>
</tr>
<tr>
<td>PSU Type</td>
<td>2 x 770W 100 - 127Vac 8A, 50/60Hz</td>
<td>2 x 770W 200 - 240Vac 4A, 50/60Hz</td>
<td>2 x 770W 100 - 127Vac 8A, 50/60Hz</td>
<td>2 x 770W 200 - 240Vac 4A, 50/60Hz</td>
</tr>
<tr>
<td>AC Input</td>
<td>120V (100-127VAC)</td>
<td>230V (200-240VAC)</td>
<td>120V (100-127VAC)</td>
<td>230V (200-240VAC)</td>
</tr>
<tr>
<td>Max. Amps.</td>
<td>4.5</td>
<td>2.1</td>
<td>5.2</td>
<td>3.2</td>
</tr>
<tr>
<td>Max. Watts</td>
<td>419</td>
<td>400</td>
<td>445</td>
<td>430</td>
</tr>
<tr>
<td>Typical Watts</td>
<td>330</td>
<td>320</td>
<td>335</td>
<td>345</td>
</tr>
<tr>
<td>Max VA</td>
<td>419</td>
<td>490</td>
<td>445</td>
<td>515</td>
</tr>
<tr>
<td>Power Factor</td>
<td>98</td>
<td>94</td>
<td>97</td>
<td>94</td>
</tr>
<tr>
<td>Heat Dissipation in BTU/hour (Typical)</td>
<td>1130</td>
<td>1190</td>
<td>1726</td>
<td>1175</td>
</tr>
</tbody>
</table>

Environmental specifications

The following table summarizes the environmental requirements for the systems.

<table>
<thead>
<tr>
<th>EX1260</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating Acoustic</td>
</tr>
<tr>
<td>Temperature (Operating)</td>
</tr>
<tr>
<td>Temperature (Storage)</td>
</tr>
<tr>
<td>Relative Humidity</td>
</tr>
<tr>
<td>Storage Humidity</td>
</tr>
<tr>
<td>Operating Altitude</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

EX1360 specifications

This section describes the status lights and ports, and it provides technical and environmental specifications.
Status lights and ports

The following figures illustrate the status light and port locations and identify the disk numbers and PCIe slot locations.

Figure A-7. Front panel

Disks 0 through 19 are HDD disks. Disks 20 through 23 are SSD disks.

Figure A-8. Back panel

The following table summarizes the SteelHead EX 1360 system LEDs.

<table>
<thead>
<tr>
<th>LED</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYSTEM</td>
<td>Normal = Blue</td>
</tr>
<tr>
<td></td>
<td>System Boot = Yellow</td>
</tr>
<tr>
<td>PRI = Primary</td>
<td>Link and Traffic = Blinks Blue</td>
</tr>
<tr>
<td>AUX = Auxiliary</td>
<td></td>
</tr>
<tr>
<td>REM = Remote</td>
<td></td>
</tr>
<tr>
<td>LAN-WAN</td>
<td>Link and Traffic = Blinks Blue</td>
</tr>
<tr>
<td>BYP/BLK</td>
<td>Normal = No Light</td>
</tr>
<tr>
<td>BYP = Bypass</td>
<td>Bypass or Block (Disconnect) = Orange</td>
</tr>
<tr>
<td>BLK = Block (Disconnect)</td>
<td></td>
</tr>
</tbody>
</table>
**Technical specifications**

The following table summarizes the technical specifications for the systems.

<table>
<thead>
<tr>
<th></th>
<th>EX1360 G/L/M</th>
<th>EX1360P G/L/M</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Form Factor</strong></td>
<td>2U</td>
<td>2U</td>
</tr>
<tr>
<td><strong>HDD / SSD</strong></td>
<td>20 x 1 TB HDD</td>
<td>20 x 1 TB HDD</td>
</tr>
<tr>
<td></td>
<td>4 x 100 GB SSD</td>
<td>4 x 400 GB SSD</td>
</tr>
<tr>
<td><strong>Data Store</strong></td>
<td>320 GB</td>
<td>320 GB</td>
</tr>
<tr>
<td></td>
<td>4000 GB VSP</td>
<td>4000 GB VSP</td>
</tr>
<tr>
<td><strong>Dimensions (LxWxH)</strong></td>
<td>25.4 x 17.2 x 3.43 in</td>
<td>25.4 x 17.2 x 3.43 in</td>
</tr>
<tr>
<td></td>
<td>(645.4 x 436 x 87.1 mm)</td>
<td>(645.4 x 436 x 87.1 mm)</td>
</tr>
<tr>
<td><strong>Weight (without packaging)</strong></td>
<td>58 lbs (23.36 kg)</td>
<td>58 lbs (23.36 kg)</td>
</tr>
<tr>
<td><strong>PCIe Slots</strong></td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td><strong>Onboard Bypass Ports/Max # Ports</strong></td>
<td>4/8</td>
<td>4/8</td>
</tr>
</tbody>
</table>

For more information about SteelFusion and VSP disk allocation, see “VSP and SteelFusion storage specifications” on page 83.
Power specifications

The following table summarizes the power specifications for the systems. The systems are rated at the following power characteristics when operating at nominal AC input voltages (120 V and 230 V).

<table>
<thead>
<tr>
<th>System</th>
<th>EX1360</th>
<th>EX1360</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Configuration</td>
<td>EX1360</td>
</tr>
<tr>
<td></td>
<td>All (G, L, M)</td>
<td>All (G, L, M)</td>
</tr>
<tr>
<td>PSU Type</td>
<td>2 x 770W</td>
<td>2 x 770W</td>
</tr>
<tr>
<td></td>
<td>100 - 127Vac</td>
<td>200 - 240Vac</td>
</tr>
<tr>
<td></td>
<td>8A, 50/60Hz</td>
<td>4A, 50/60Hz</td>
</tr>
<tr>
<td>AC Input</td>
<td>120V (100 - 127VAC)</td>
<td>230V (200 - 240VAC)</td>
</tr>
<tr>
<td>Max. Amps.</td>
<td>6.4</td>
<td>3.3</td>
</tr>
<tr>
<td>Max. Watts</td>
<td>635</td>
<td>630</td>
</tr>
<tr>
<td>Typical Watts</td>
<td>505</td>
<td>500</td>
</tr>
<tr>
<td>Max VA</td>
<td>650</td>
<td>464590</td>
</tr>
<tr>
<td>Power Factor</td>
<td>98</td>
<td>97</td>
</tr>
<tr>
<td>Heat Dissipation in BTU/hour (Typical)</td>
<td>1726</td>
<td>1712</td>
</tr>
</tbody>
</table>

Environmental specifications

The following table summarizes the environmental requirements for the systems.

<table>
<thead>
<tr>
<th>EX1360</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating Acoustic</td>
</tr>
<tr>
<td>Temperature (Operating)</td>
</tr>
<tr>
<td>Temperature (Storage)</td>
</tr>
<tr>
<td>Relative Humidity</td>
</tr>
<tr>
<td>Storage Humidity</td>
</tr>
<tr>
<td>Operating Altitude</td>
</tr>
</tbody>
</table>
SteelHead EX hardware allocation

With SteelHead EX, part of the memory is dedicated to RiOS and part of the memory is dedicated to virtualization. The memory isn’t shared. CPU cores are dedicated to either RiOS or VSP. The processors aren’t shared.

The following table describes the hardware specifications for the xx60 series models. The “RAM, Available to VSP/ESXi” column in this table indicates the amount of available physical memory. Deploy virtual machines on ESXi in accordance with VMware Performance Best Practices for vSphere, which you can find at the following URL: http://www.vmware.com/pdf/Perf_Best_Practices_vSphere5.0.pdf.

Note: On April 1, 2014, the amount of memory shipped in EX1160 and EX1260 appliances increased. The following table displays the memory amounts for both the new models and the earlier versions. The models are identified by their orderable part number.

<table>
<thead>
<tr>
<th>Series</th>
<th>Part number</th>
<th>Minimum CPU</th>
<th>Allocation</th>
<th>HDD/SSD</th>
<th>RAM, shipped</th>
<th>RAM, available to VSP/ESXi</th>
</tr>
</thead>
<tbody>
<tr>
<td>EX560</td>
<td>EXA-00560-B010</td>
<td>1 x 4 cores 3.1 GHz 2 cores / 2 cores</td>
<td>1 TB HDD 1 x 80 GB SSD</td>
<td>8 GB (16 GB with SteelFusion-licensed model)</td>
<td>4 GB (9 GB)</td>
<td></td>
</tr>
<tr>
<td>All versions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EX760</td>
<td>EXA-00760-B010</td>
<td>1 x 4 cores 3.1 GHz 2 cores / 2 cores</td>
<td>1 TB HDD 1 x 160 GB SSD</td>
<td>16 GB</td>
<td>8 GB</td>
<td></td>
</tr>
<tr>
<td>All versions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EX1160</td>
<td>EXA-01160-B030</td>
<td>2 x 4 cores 2.2 GHz 1 x 4 cores / 1x 4 cores</td>
<td>2 x 1 TB HDD 2 x 80 GB SSD</td>
<td>20 GB</td>
<td>10 GB</td>
<td></td>
</tr>
<tr>
<td>G/L/M/H versions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EX1160</td>
<td>EXA-01160-B035</td>
<td>2 x 4 cores 2.2 GHz 1 x 4 cores / 1x 4 cores</td>
<td>2 x 1 TB HDD 2 x 80 GB SSD</td>
<td>48 GB</td>
<td>32 GB</td>
<td></td>
</tr>
<tr>
<td>G/L/M/H versions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EX1160</td>
<td>EXA-01160-B020</td>
<td>2 x 4 cores 2.2 GHz 1 x 4 cores / 1x 4 cores</td>
<td>2 x 1 TB HDD 2 x 160 GB SSD</td>
<td>24 GB</td>
<td>12 GB</td>
<td></td>
</tr>
<tr>
<td>VH version</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EX1160</td>
<td>EXA-01160-B025</td>
<td>2 x 4 cores 2.2 GHz 1 x 4 cores / 1x 4 cores</td>
<td>2 x 1 TB HDD 2 x 160 GB SSD</td>
<td>48 GB</td>
<td>32 GB</td>
<td></td>
</tr>
<tr>
<td>VH version</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EX1260-2</td>
<td>EXA-01260-B010</td>
<td>2 x 6 cores 2.6 GHz 1 x 6 cores / 1x 6 cores</td>
<td>4 x 1 TB HDD 2 x 80 GB SSD</td>
<td>24 GB (upgradeable to 32 GB)</td>
<td>11 GB (upgradeable to 19 GB)</td>
<td></td>
</tr>
<tr>
<td>Series</td>
<td>Part number</td>
<td>Minimum CPU</td>
<td>Allocation RiOS / VSP</td>
<td>HDD/SSD</td>
<td>RAM, shipped</td>
<td>RAM, available to VSP/ESXi</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------</td>
<td>-------------</td>
<td>----------------------</td>
<td>---------</td>
<td>--------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>EX1260-2</td>
<td>EXA-01260-B025</td>
<td>2 x 6 cores 2.6 GHz</td>
<td>1 x 6 cores / 1 x 6 cores</td>
<td>4 x 1 TB HDD 2 x 80 GB SSD</td>
<td>72 GB</td>
<td>48 GB</td>
</tr>
<tr>
<td>G/L/M/H versions</td>
<td>EXA-01260-B030 (EXA-01260-B040)</td>
<td>2 x 6 cores 2.6 GHz</td>
<td>1 x 6 cores / 1 x 6 cores</td>
<td>4 x 1 TB HDD 4 x 80 GB SSD</td>
<td>24 GB (upgradeable to 32 GB)</td>
<td>7 GB (upgradeable to 15 GB)</td>
</tr>
<tr>
<td>VH version</td>
<td>EXA-01260-B045</td>
<td>2 x 6 cores 2.6 GHz</td>
<td>1 x 6 cores / 1 x 6 cores</td>
<td>4 x 1 TB HDD 4 x 80 GB SSD</td>
<td>72 GB</td>
<td>48 GB</td>
</tr>
<tr>
<td>EX1260-4</td>
<td>EXA-01260-B065</td>
<td>2 x 6 cores 2.6 GHz</td>
<td>1 x 6 cores / 1 x 6 cores</td>
<td>4 x 1 TB HDD 2 x 80 GB SSD</td>
<td>88 GB</td>
<td>64 GB</td>
</tr>
<tr>
<td>G/L/M/H versions</td>
<td>EXA-01260-B050 (EXA-01260-B060)</td>
<td>2 x 6 cores 2.6 GHz</td>
<td>1 x 6 cores / 1 x 6 cores</td>
<td>4 x 1 TB HDD 4 x 80 GB SSD</td>
<td>32 GB (upgradeable to 64 GB)</td>
<td>14 GB (upgradeable to 45 GB)</td>
</tr>
<tr>
<td>VH version</td>
<td>EXA-01260-B070 (EXA-01260-B060)</td>
<td>2 x 6 cores 2.6 GHz</td>
<td>1 x 6 cores / 1 x 6 cores</td>
<td>4 x 1 TB HDD 4 x 80 GB SSD</td>
<td>32 GB (upgradeable to 64 GB)</td>
<td>10 GB (upgradeable to 41 GB)</td>
</tr>
<tr>
<td>EX1260-4</td>
<td>EXA-01260-B085</td>
<td>2 x 6 cores 2.6 GHz</td>
<td>1 x 6 cores / 1 x 6 cores</td>
<td>4 x 1 TB HDD 4 x 80 GB SSD</td>
<td>88 GB</td>
<td>64 GB</td>
</tr>
<tr>
<td>VH version</td>
<td>EXA-01360-B010</td>
<td>2 x 8 cores 3.0 GHz</td>
<td>1 x 8 core / 1 x 8 cores</td>
<td>20 x 1 TB HDD 4 x 100 GB SSD</td>
<td>128 GB</td>
<td>64 GB</td>
</tr>
<tr>
<td>EX1360</td>
<td>EXA-01360-B030</td>
<td>2 x 8 cores 3.0 GHz</td>
<td>1 x 8 core / 1 x 8 cores</td>
<td>20 x 1 TB HDD 4 x 400 GB SSD</td>
<td>128 GB</td>
<td>64 GB</td>
</tr>
<tr>
<td>G/L/M versions</td>
<td>EXA-01360-B010</td>
<td>2 x 8 cores 3.0 GHz</td>
<td>1 x 8 core / 1 x 8 cores</td>
<td>20 x 1 TB HDD 4 x 100 GB SSD</td>
<td>128 GB</td>
<td>64 GB</td>
</tr>
</tbody>
</table>

**Note:** This table indicates the SSD disk capacity available to the system. Disks in newer appliance models or replacement disks might be capable of a higher capacity (such as 100 GB instead of 80 GB or 200 GB instead of 160 GB), but the system still limits them to the capacity expected by the system and defined in this table.

**Note:** The RAM available to VSP/ESXi is the host physical memory available to vSphere. The memory available to guests is less. (ESXi uses approximately 2 GB of memory and the remainder is available for virtual machines.)
VSP and SteelFusion storage specifications

The following table summarizes the following information:
- Possible disk space allocations between VSP and SteelFusion on xx60 model appliances.
- SteelFusion Input/Output Operations Per Second (IOPS) on xx60 model appliances.

You aren't constrained by the VSP and SteelFusion disk allocation. You can use the local LUN feature on SteelFusion to allocate as much disk space as you want for the VM local datastore and use the rest for the SteelFusion block store. To do this, select SteelFusion Only mode. Then, set up a local LUN in that space for VSP, format it using VMFS, and add the VM datastore. (The VM datastore provides storage for VM files.) You can use the rest of the space for the SteelFusion block store.

**Note:** For optimal performance, we recommend direct storage and not iSCSI unless disk sizing flexibility is absolutely necessary.

**Note:** For SteelFusion-only allocations, the system reserves a small amount of disk space for VSP for local swap space.

**Note:** You need a SteelFusion license for SteelFusion-only allocations, for VSP-only allocations, and to access the disk space allocated for SteelFusion storage in a mixed allocation.

Numbers in parenthesis represent the maximum amount of space available for the component when the appliance's disk layout is set to an extended mode. See “Reclaiming disk space” on page 22.

<table>
<thead>
<tr>
<th>Series</th>
<th>SteelFusion-only allocation (extended disk layout)</th>
<th>VSP-only allocation (extended disk layout)</th>
<th>Mixed allocation (extended disk layout)</th>
<th>SteelFusion IOPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>EX560/EX760</td>
<td>380 (380)</td>
<td>380 (600)</td>
<td>190 (300)</td>
<td>85</td>
</tr>
<tr>
<td>EX1160</td>
<td>760 (760)</td>
<td>415 (830)</td>
<td>275 (415)</td>
<td>170</td>
</tr>
<tr>
<td>EX1260-2</td>
<td>1580 (1580)</td>
<td>860 (1700)</td>
<td>575 (860)</td>
<td>350</td>
</tr>
<tr>
<td>EX1260-4</td>
<td>3.6TB (3.6TB)</td>
<td>1.86TB (3.7TB)</td>
<td>1230 (1860)</td>
<td>700</td>
</tr>
<tr>
<td>EX1360</td>
<td>10TB</td>
<td>10TB</td>
<td>4TB (5TB)</td>
<td>1700</td>
</tr>
</tbody>
</table>