riverbed

RIVERBED PRODUCT RELEASE NOTES

PRODUCT: STEELCENTRAL CONTROLLER FOR STEELHEAD

RELEASE DATE: 27-DECEMBER-2023

VERSION: 9.15.0

CONTENTS

riverbed

5) Contacting Riverbed Support

1) SteelCentral Controller for SteelHead Version 9.15.0

1) NEW FEATURES

Aimed at improving usability and compatibility, this release includes features relevant to the Federal space including support for IPv6 and Cisco Secure Group Tagging (SGT). The release also introduces support for new SMB 3.1.1 crypto algorithms (AES-GCM, AES-CCM, AES-GMAC), DISKO support for short domain names, and DISKO performance improvements. In addition, security improvements to the SteelHead Certificate Signing Service provide an easy path for TLS/SSL optimization without the need for an agent.

2) Ipv6 Support

Riverbed is continuing its efforts to make its products fully compatible with Ipv6. Reference the following KB article to understand acceleration product Ipv6 support: https://supportkb.riverbed.com/support/index?page=content&id=S38049&actp=search

3) FIXED PROBLEMS

- **SCC-2160** Symptom: When connecting to the SCC Web UI, the secure cookie and HSTS header will only be included if SCC has HTTPS enabled.

  Condition: If the request from the browser is via HTTP, then SCC will exclude “secure cookie” and “HSTS” in the response header and will only be included if SCC has HTTPS enabled. **HTTPS** can be disabled with the *no web https enable* command, and HTTP can be enabled with the *web http enable* command.

- **SCC-2044** Symptom: An SCC policy push with MAPI signing, WinSec Controller, and replication user configurations may fail at times.

Condition: This issue can occur when MAPI signing configuration is added before WinSec and replication user configurations. A fix has been made to add WinSec/replication user configurations first followed by MAPI signing.

- **SCC-1914** Symptom: After upgrading to SteelHead 9.12.2b, the connection to the SteelCentral Controller may be lost.

  Condition: This issue occurs due to a weaker SSH key algorithms being removed from the SteelHead release. The weaker SSH key algorithms were removed from the SteelCentral Controller so that communication can now be established.

- **SCC-1886** Symptom: On SCC's SSL Main Settings policy page, the option to generate certificates for bypassed servers doesn't work for TLS passthrough servers (TLS blade).

  Condition: This issue occurs because SCC parsing of error codes from the appliance doesn’t cover TLS blade.

- **SCC-1869** Symptom: SteelHead SSL optimization fails with browsers reporting issues with server certificates: {{ERR_CERT_COMMON_NAME_INVALID}}

  Condition: This issue occurs when the SCC CA signed proxy server certificates are added to SteelHeads to achieve SSL optimization.

- **SCC-1713** Symptom: The external backup fails, causing a mount point failure for the SSH server.

  Condition: This issue occurs when the external server unmounts due to a failure during backup.

- **SCC-1534** Symptom: A Client Accelerator (formerly SteelHead Mobile [SHM]) that is a peer to any connected SteelHead is shown in the SteelCentral Controller (SCC) Unmanaged **Appliance** Report page; however, it is designed to manage only SteelHead, Client Accelerator Controller (formerly SteelHead Mobile Controller [SMC]), and Interceptor (IC).

  Condition: This condition appeared beginning in the release 9.12.0.

- **SCC-1136** Symptom: An external backup using CIFS causes the appliance to hang.

Condition: The SMB protocol negotiation fails because of a CIFS version mismatch.

- **SCC-474** Symptom: An SCC CA certificate addition fails with the error "global name 'm' is not defined."

  Condition: This issue occurs when the added SCC CA certificate's chain of trust (Intermediate and Root CA's) has any certificate with validity beyond the year 2050.

2) KNOWN ISSUES

- **SCC-2297** Symptom: When upgrading Virtual SCC, an error is given "image install of <image name> failed. The upgrade image provided does not pass validation."

  Condition: This can occur when upgrading from 9.12.1 and earlier, to 9.15.x and later, due to rootfs space issues. Virtual SCC systems deployed on 9.12.2 and later should not encounter this.

  Public Workaround: One must re-deploy the Virtual SCC VM using an image that is 9.15.x or later. Reference the following KB articles for instructions:
  https://supportkb.riverbed.com/support/index?page=content&id=S37986
  https://supportkb.riverbed.com/support/index?page=content&id=S14439

3) UPGRADING

Upgrading Alert:

9.2.0 Upgrade, Path Selection and QoS: Operators must disable path selection and QoS in SteelHead 9.0.x or SteelHead 9.1.x prior to rebooting into SteelHead 9.2.0, which uses new path identifiers. Please refer to Knowledge Base article S28250 for detailed instructions. Failure to follow this process can block pre-existing connections and render the SteelHead unreachable after the first SCC 9.2.0 Path Selection policy push.

This section describes how to upgrade the SCC appliance software. These instructions assume you are familiar with the SCC appliance, the SCC command-line interface (CLI), and the Management

Console.

NOTE: Riverbed recommends that you upgrade your SCC software from one major version to the next, without skipping intermediate versions. The recommended upgrade path is 5.5.4c > (6.0.1 or 6.1.x) > 6.5.x > (7.0.x or 8.0.x) > 8.5.x > 8.6.x > (9.0.x or 9.1.x or 9.2.x) > (9.5.x or 9.6.x or 9.7.x or 9.8.x) > 9.9.x > (9.10.x > 9.12.x)

Missing the intermediate steps can lead to irrecoverable database corruption. To upgrade the Riverbed SteelCentral Console for SteelHead:

1. Download the software image from the Software tab of the support site to a location such as your desktop.

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

3. Navigate to the Administration Software Upgrade page and choose one of the following options:

a. From URL. Type the URL that points to the software image in the text box.

b. From Local File. Browse your file system and select the software image. c. Click Install Upgrade.

d. Clear the browser cache and cookies to ensure the user interface displays correctly.

4) HARDWARE AND SOFTWARE REQUIREMENTS

The SCC appliance has the following requirements:

- SCC 9.15.0 is compatible with both the model 8151 and the 1000.

- A Computer that supports a Web browser with color image display
- Javascript and cookies must be enabled on your Web browser.

- The SCC supports Mozilla Firefox version 31 ESR (Extended Support Release) and

- Microsoft Internet Explorer version 9.

- NOTE: If you want to encrypt your communication, you must have a Secure Sockets

- Layer (SSL)-capable browser.

The SCC command-line interface has the following requirements:

- An ASCII terminal or emulator that can connect to the serial console (9600 baud, 8 bits, no parity, 1 stop bit, and no flow control) or

- A computer with a Secure Shell (SSH) client that is connected by an IP network to the SteelHead appliance primary interface. Free SSH clients include PuTTY for Windows computers, OpenSSH for many UNIX and UNIX-like operating systems, or Cygwin.

5) CONTACTING RIVERBED SUPPORT

Visit the Riverbed Support site to download software updates and documentation, browse our library of Knowledge Base articles and manage your account. To open a support case, choose one of the options below. **Phone**

Riverbed provides phone support at 1-888-RVBD-TAC (1-888-782-3822). Outside the U.S. dial +1 415 247 7381.

Online

You can also submit a support case online

Email

Send email to support@riverbed.com. A member of the support team will reply as quickly as possible.