

RIVERBED PRODUCT RELEASE NOTES

PRODUCT: CLIENT ACCELERATOR CONTROLLER

RELEASE DATE: 13-DECEMBER-2023

VERSION: 6.4.0

CONTENTS

- 1) Supported Hardware Models
- 2) New Features
- 3) Fixed Problems
- 4) Known Issues
- 5) Alert: SCC Compatibility
- 6) Upgrading SteelCentral Controller for SteelHead Mobile Software
- 7) Hardware and Software Requirements
- 8) Contacting Riverbed Support

1) SUPPORTED HARDWARE MODELS

- Steelhead Mobile Controller version 6.3.0 supports model 8551, 9000, 9001 and the AZURESCCM.
- Steelhead Mobile Controller version 6.4.0 supports model 8551, 9001 and the AZURESCCM.

2) NEW FEATURES

These new features are available in SteelHead Mobile 6.4.0

- Support for TLS 1.3
- Client Accelerator support for IPv6
- Add IPv6 Support to the macOS CA endpoint
- Support for AppGate SDP
- Support for Wireguard VPN
- Support for Cisco Secure Client 5 - AnyConnect VPN
- Enhance customer workflows to support necessary Image Signing cert updates
- Upgrade Windows build to Windows 10 and Visual Studio 2019
- IT Installation of the "internal" CA proxy Certificate
- Drop SMC 9000 upgrade support

3) FIXED PROBLEMS

Problems fixed in version 6.4.0

- **SHMOBILE-4102** Symptom: Client Accelerator fails to connect to HTTP/HTTPS sites when updating Chrome to version 119.0.6045.160 and eventually shows ERR_SSL_KRY_USAGE_INCOMPATIBLE.
Condition: Google Chrome enforces "digital signature" as the default key usage attribute, while legacy RSA decryption cipher suites rely on the "keyEncipherment" key usage option.

Users encounter connection problems in intercepted TLS/SSL traffic due to ERR_SSL_KEY_USAGE_INCOMPATIBLE, linked to the use of "key encipherment" in X.509 key usage during TLS handshake with Client Accelerator or SteelHead interception, resulting in failures. To support X.509 key usage extension for RSA certificates, {{keyusageextn dig-sign}} has been enabled by default in version 6.3.2 and later.

- **SHMOBILE-4069** Symptom: The optimization service crashes while optimizing SaaS traffic. Condition: The crash is triggered by the failure to fetch the IP address of the interface that received the connection. This issue was seen in a lab machine that was tested for various use cases. After a restart of the client machine, the issue was not seen and the SaaS connections were optimized without any optimization crash.
- **SHMOBILE-3641** Symptom: When selecting Preferences from the Client Accelerator menu on macOS 13, the preferences window may not render correctly. Either a previous preferences window is still showing or a blank preferences pane is showing. Condition: The command to open the Client Accelerator preferences no longer works reliably in macOS 13. That command needs to be updated.
- **SHMOBILE-3296** Symptom: Client Accelerator for Mac clients does not optimize connections proxied via Cloud Access Security Broker (CASB). Condition: Since version 6.3.0, Client Accelerator for Mac clients uses a system extension to intercept connections for optimization. Connections proxied via a CASB are not identified for optimization by the system extension. For instance, connections to cloud apps protected by Microsoft Defender for Cloud Apps (previously known as Microsoft Cloud App Security) are not optimized. In version 6.4.0, the system extension is updated to identify connections proxied via a CASB and classify them for optimization.

4) KNOWN ISSUES

Known Issues in version 6.4.0

- **SHMOBILE-4061** The fjid process crashes when FIPS mode is enabled and the hashed user account password is not FIPS compliant.

- **SHMOBILE-4059** The “fips enable” CLI logs an error about non-FIPS-allowed hash but still enables FIPS.
- **SHMOBILE-4057** An untrusted certificate error occurs with optimized connections in Firefox.
- **SHMOBILE-4027** GlobalProtect VPN disconnects when IPv6 connection optimization is enabled on a client running version 6.4.0.
- **SHMOBILE-4018** Connections bypassed by "Hostname-based interception (HNBI)" are not listed in the connection list report of Client Accelerator on macOS.
- **SHMOBILE-3895** Editing a source label results in a new intercept rule being added on the endpoint CA.
- **SHMOBILE-3890** IPv6 connections do not go through the AppGate tunnel when Client Accelerator optimization is enabled.
- **SHMOBILE-3889** IPv6 connections do not go through the WireGuard tunnel when Client Accelerator optimization is enabled.

5) ALERT: SCC COMPATIBILITY

If you use SteelCentral Controller for SteelHead (SCC) to manage your appliances, you must upgrade SCC to a specific version before you upgrade your appliances to this software version. Failure to do so will prevent communication between SCC and your appliances. Go to [Knowledge Base article S27759](#) for complete details.

6) UPGRADING STEELCENTRAL CONTROLLER FOR STEELHEAD MOBILE SOFTWARE

To upgrade the software

1. From the Mobile Controller Management Console, choose Setup to expand the Setup menu.
2. Choose Upgrade Software to display the Software Upgrade page.
3. Under Install Upgrade From, select one of the following options:

- From URL

Click this option and type the URL. If you specify a URL in the URL text box, the image is uploaded, installed, and the system is rebooted at the time you specify.

- From Local File

Click this option and type the path or click Browse to go to the local file directory. If you specify a file to upload in the Local File text box, the image is uploaded immediately; however, the image is installed and the system is rebooted at the time you specify.

- Schedule Upgrade for Later

Schedules the upgrade process. Specify the date and time to run the upgrade. Use the following format: YYYY/MM/DD, HH:MM:SS

- Install Upgrade

Installs the software upgrade on your system

7) HARDWARE AND SOFTWARE REQUIREMENTS

For SHM 6.1.0, Cisco VPN clients are not qualified with this release.

If you are using an Enterprise Software Suite to Distribute SteelHead Mobile Client Packages for MAC OS X Clients, go to [Knowledge Base Article S26379](#).

Virtual SteelCentral Controller for SteelHead Mobile requires at least 3 GB of RAM and at least 20 GB of available storage.

For other hardware and software dependencies, VPN requirements, anti-virus compatibility or firewall requirements, see the *SteelHead Mobile Controller Installation Guide*.

8) 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.

©2023 Riverbed Technology. All rights reserved. Riverbed and any Riverbed product or service name or logo used herein are trademarks of Riverbed Technology. All other trademarks used herein belong to their respective owners. The trademarks and logos displayed herein may not be used without the prior written consent of Riverbed Technology or their respective owners.