riverbed

RIVERBED PRODUCT RELEASE NOTES

PRODUCT: CLIENT ACCELERATOR CONTROLLER

RELEASE DATE: 02-SEPTEMBER-2024

VERSION: 6.4.1a

CONTENTS

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

No New features are available in SteelHead Mobile 6.4.1a

These new features are available in SteelHead Mobile 6.4.1

- Qualification of macOS 14 (Sonoma)
- Qualification of Windows 11 23H2 feature update
- Support for Microsoft Always On VPN
- Get HTTP Framework and HTTP/2 Traffic working on Windows
- Deprecation of obsolete optimizations: phase 1
- Feasibility of enabling int bypass command by default
- IPv6 support for host labels - Internal: Remove obsolete support for Akamai Cloud Proxy (ACP)
- Internal: Build CA Controller with OPENSSL_3.x

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 6.4.1a

- **SHMOBILE-4446** Symptom: Closed connections are not being purged from the delayed connection list.
  Condition: Moved the closed connection to the delete list after the timer expires.

- **SHMOBILE-4319** Symptom: Closed connections are not being purged from delayed connection list.
  Condition: Moved the closed connection to delete list after few timer expires.

Problems fixed in version 6.4.1

- **SHMOBILE-4059** Symptom: When trying to enable FIPS mode when the hashed user account password is not FIPS compliant, the CLI logs an error but still enables FIPS post reload.
  Condition: This issue occurs when the hashed user account password is not FIPS compliant.

- **SHMOBILE-4057** Symptom: In recent macOS versions, an untrusted certificate warning occurs with optimized connections in Firefox.
  Condition: This issue occurs when certain Firefox configuration files enforced by macOS fail to copy. See the following sample log message. As a result, the Client Accelerator's proxy certificate is not added to Firefox's certificate store. {noformat}sandboxd: [com.apple.sandbox.reporting:violation] System Policy: rbtmond(26556) deny(1) filewrite-create /Applications/Firefox.app/Contents/Resources/firefox_shmobile.cfg{noformat}

- **SHMOBILE-3895** Symptom: Editing a source label added to a policy results in adding a new intercept rule on the endpoint CA rather than editing the already existing rule with the updated value.
  Condition: This issue occurs when editing a source label added to a policy. For more details, go to Knowledge Base article [S37948|http://supportkb.riverbed.com/support/index?page=content&id=S37948] on the Riverbed support website.

- **SHMOBILE-3890** Symptom: IPv6 connections do not go through the AppGate tunnel. Condition: This issue occurs when Client Accelerator optimization is enabled. Cannot ping the IPv6 server over the AppGate tunnel created using IPv6. Also, IPv6 connections are not optimized. For more details, go to Knowledge Base article [S37946|https://supportkb.riverbed.com/support/index?page=content&id=S37946&actp=search] on the Riverbed Support site.

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 6.4.1

- **SHMOBILE-4240** The CA certificate 1024-bit key size is not compatible with the latest OpenSSL standards.

- **SHMOBILE-4061** The fijid 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-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.

Known Issues in version 6.4.0

- **SHMOBILE-4061** The fijid 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.