Vertiv™ Avocent® RM1048P Rack Manager

Release Notes

VERSION 1.82.1, JUNE 2026

Release Notes Section Outline

1. Update Instructions

The Vertiv™ Avocent® RM1048P Rack Manager firmware may be updated through the web user interface (UI). To access the rack manager web UI, enter the assigned IP address into a web browser, which is provided during the initial setup of the rack manager.

NOTE: For additional information on this process, refer to the Vertiv™ Avocent® RM1048P Rack Manager Quick Installation Guide, which is provided with the rack manager and also available on the Vertiv™ Avocent® RM1048P product page under the *Documents & Downloads* tab.

IMPORTANT NOTE: Prior to updating the firmware, ensure the hardware will have full integration software support with this release. For more information, contact your Vertiv Technical Support representative.

NOTE: Before upgrading the firmware of a Vertiv™ Avocent® RM1048P Rack Manager appliance that is managed by the Vertiv™ Avocent® MP1000 Management Platform or Vertiv™ Avocent® MP1000VA Management Platform Virtual Appliance, you must first upgrade the MP1000 or MP1000VA management platform appliance to firmware version 3.96.1 or newer version. After the management platform appliance has been successfully upgraded to 3.96.1, you may then proceed to upgrade the Vertiv™ Avocent® RM1048P Rack Manager firmware using the management platform web UI.

NOTE: Before updating the firmware, ensure that all downstream Vertiv equipment is upgraded to the latest firmware release. The recommended order of equipment upgrades is as follows:

1. **Vertiv™ Avocent® IPIQ IP KVM, Vertiv™ Avocent® IPSL IP serial, and Vertiv™ Avocent® IPUHD 4K IP KVM devices**
2. **Vertiv™ PowerIT rPDUs, Vertiv™ Geist™ rPDUs, and Vertiv™ Liebert® rack UPS devices**
3. **Vertiv™ Avocent® RM1048P Rack Manager and Vertiv™ Avocent® MP1000 Management Platform (or MP1000VA Virtual Appliance)**

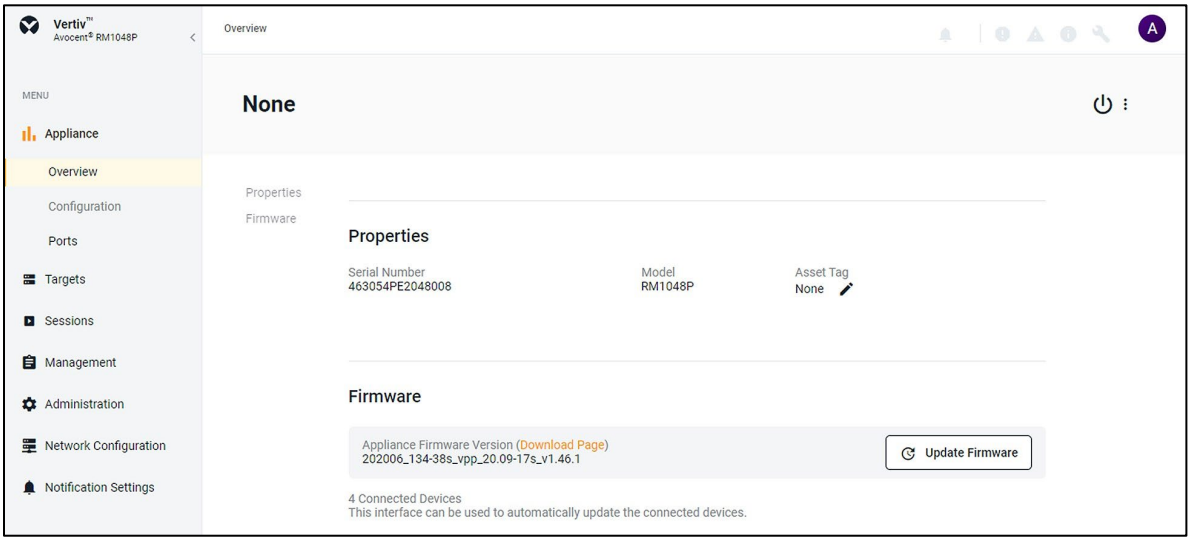
IMPORTANT: The Vertiv™ Avocent® RM1048P Rack Manager and the management platform (hardware or virtual appliance) must be upgraded within the same maintenance window to ensure proper compatibility and system functionality.

For firmware download locations for each product, refer to Section 13 (Vertiv™ Avocent® DSView™ Solution Related Products) of these notes.

To update the rack manager firmware:

1. Visit the Vertiv™ Avocent® RM1048P **rack manager firmware download page**
2. Download the latest firmware and save it to the local computer, FTP, or HTTP server.
   NOTE: For information on the latest firmware version, refer to Section 2 (Appliance Firmware Version Information).
3. In a web browser, enter **https://**<appliance.IP> using the IP address for Vrf_app0 from the configured rack manager console menu.

4. Enter the username and password at the login screen. The Targets List screen opens.
5. In the sidebar, select *Appliance - Overview* and click the *Update Firmware* button.



6. Select whether to update the firmware for just the rack manager or to update the firmware for just the connected targets.
7. Select the firmware file and click *Update*.

   NOTE: FTP and HTTP are the only supported protocols for updating the firmware. The TFTP protocol is not supported.
8. After the firmware has been successfully updated, it is strongly advised to clear the browser cache.

   NOTE: If the time on the rack manager and the Vertiv™ Avocent® MP1000 Management platform differ by more than a few seconds, the management platform will be unable to discover and manage the rack manager. It is recommended to configure both appliances with the same NTP server to establish a shared time setting and allow for proper discovery.

2. Appliance Firmware Version Information

APPLIANCE/PRODUCT	VERSION	FILENAME
Vertiv™ Avocent® RM1048P Rack Manager	1.82.1	SONiC-202006_134-40s_vpp_20.09-17s_v1.82.1.bin

3. Features and Enhancements

The following features and enhancements are available with this release of the Vertiv™ Avocent® RM1048P Rack Manager:

- Enhances the SSH Passthrough feature as follows:
  - Supports both public/private key authentication and username/password authentication for SSH passthrough sessions.
  - Allows connections to devices with SSH servers. Examples of these devices include, but are not limited to:
    - Vertiv™ Avocent® IPSL IP serial devices
    - Vertiv™ PowerIT rPDU devices
    - Vertiv™ Liebert® rack UPS devices
    - Generic target devices
    - Devices connected to the Vertiv™ Avocent® RM1048P Rack Manager appliance

- Improves the device status in the Appliance View and the Targets List pages.
- Provides system logging and diagnostics capabilities as follows:
    - Adds diagnostic functionality to capture and analyze system and network connectivity data for the management platform and managed devices using the web UI, including support for ping, traceroute, TCP connection, and NTP connection tests.
    - Adds the ability to export system logs via the web UI for the management platform and managed devices, including service logs, container logs, and system-level diagnostic information.
    - Adds the ability to configure log levels for services via the web UI to support troubleshooting and diagnostics.

Resolved Issues

- General issues resolved:
    - Fixed issue where Vertiv™ Avocent® IPIQ IP KVM, Vertiv™ Avocent® IPUHD 4K IP KVM, and Vertiv™ Avocent® IPSL IP serial devices that are managed by the management platform would stop responding and display a non-responsive status after a short period of time following discovery or firmware upgrade.
    - Fixed issue where the status shows as Offline for all Vertiv™ Avocent® IPIQ IP KVM and Vertiv™ Avocent® IPUHD 4K IP KVM devices in the Appliance View or Targets List page (CA-000110648, CA-0001056784, and CA-0001106484).
    - Fixed issue where a Vertiv™ PowerIT rPDU Monitored or Metered-only PDU incorrectly presents row menu options to control sockets in the Appliance View for the Vertiv™ Avocent® ACS8000 advanced console system. These socket control options are not supported for a metered-only PDU.
    - Fixed issue where a previous discovery process continues indefinitely on the Discoveries page even though the target device has been added at a later date (CA-0000998448).
    - Fixed issue where a discovery of a Vertiv™ PowerIT rPDU device after upgrading the firmware shows that it was not successful. However, the device is successfully added to the Appliance View.
    - Fixed issue where firmware upgrade of a Vertiv™ Avocent® IPUHD 4K IP KVM or a Vertiv™ Avocent® IPIQ IP KVM device fails when using the TFTP file transfer method.
    - Fixed issue where email notifications for active alarms are not being sent when the notification policy is configured due to certificate validation errors with IP SANs (CA-0001096635).
    - Fixed issue where the discovery of a Vertiv™ PowerIT rPDU device with firmware 6.x is not working correctly when using a credential profile that is configured with username and password.
    - Fixed issue where outlet name changes made to one Vertiv™ PowerIT rPDU device would incorrectly propagate to other managed rPDU devices after performing a Resync operation (CA-0001097576).
    - Fixed issue where the automatic conversion of Vertiv™ Avocent® Universal Management Gateway appliance UMIQ-v2 modules to operate as Vertiv™ Avocent® IPIQ IP KVM devices fails intermittently, with approximately 10% of conversions failing on the first attempt when converting multiple devices simultaneously on a Vertiv™ Avocent® RM1048P Rack Manager (CA-0001177845).
    - Fixed issue where Vertiv™ Avocent® IPIQ IP KVM device discovery performance degraded on the Vertiv™ Avocent® RM1048P Rack Manager compared to previous firmware versions, with devices taking longer to be discovered and initially reporting incorrect port numbers (port 99) before eventually displaying the correct port assignments.
    - Fixed issue where an excessive number of login events are logged on Service Processors managed by the management platform within a 30-day period.
- Authentication Provider issues resolved:
    - Fixed issue where Active Directory or LDAP authentication experiences login performance degradation from an Active Directory or LDAP provider with many groups (CA-0001081049).
    - Fixed issue where a user may not be able to authenticate with Azure single sign-on (SSO) after the configuration of the Azure SSO has been completed on the web UI (CA-0001076222).
    - Fixed issue where SSO login fails with a custom certificate using FQDN due to redirect URI being automatically generated with an IP address instead of FQDN. Users can now specify a custom redirect URI to match their certificate's FQDN (CA-0001122546).

- Fixed issue where authorization failed for Active Directory users with a custom Group Base DN filter configured, even though authentication was successful (CA-0001177848).
- Fixed issue where user-entered information in the "Add AD/LDAP Provider" dialog is lost when accidentally clicking outside the dialog area before completing the configuration.
- Fixed issue where multiple duplicate "Local Users" rows appear under the Authentication Providers page, preventing users from successfully logging in via Active Directory authentication and causing the Primary node in a High Availability cluster to enter Maintenance mode (CA-0001109617).

- Session/Viewer Issues resolved:
  - Fixed issue where a user with a lower permission level can view the list of all viewer sessions.
- CLI Issues resolved:
  - Fixed issue where the CLI session terminates unexpectedly when rapidly configuring the Vpp0 network interface on a Vertiv™ Avocent® RM1048P Rack Manager (CA-0001157192).
- Web UI issues resolved:
  - Fixed issue where Vertiv™ Avocent® IPIQ IP KVM devices connected to a Vertiv™ Avocent® RM1048P Rack Manager intermittently fail to register with the management platform or display an offline status after initially appearing online (CA-0001177851).
  - Fixed issue where Vertiv™ Avocent® IPIQ IP KVM devices connected to a Vertiv™ Avocent® RM1048P Rack Manager show an offline status in the management platform web UI after upgrading the management platform firmware to version 3.88.1 (CA-0001183450).
  - Fixed issue where network properties are not displayed correctly in the Properties panel when viewing managed devices such as Vertiv™ Avocent® RM1048P Rack Manager, Vertiv™ Avocent® MergePoint Unity™ 2 switches, Vertiv™ PowerIT rPDU devices, Service Processors, and Vertiv™ Avocent® IPIQ IP KVM, Vertiv™ Avocent® IPSL IP serial, and Vertiv™ Avocent® IPUHD 4K IP KVM devices from the Appliance View (CA-0001158561).
  - Fixed issue where device management action buttons are not visible for custom users with full permissions when selecting Vertiv™ Avocent® IPUHD 4K IP KVM or Vertiv™ Avocent® IPIQ IP KVM devices from the Appliance View.
  - Fixed issue where devices connected to the rack manager are missing or displayed as duplicates in the Appliance View or Targets List page after a firmware upgrade. The duplicate devices had the same port and IP address but different names, preventing KVM sessions from being opened.
  - Fixed issue where Vertiv™ Liebert® rack UPS and Vertiv™ PowerIT rPDU devices that are connected to a rack manager, then deleted from the Appliance View, may not be rediscovered and added to the Appliance View after performing a resync operation.
  - Fixed issue where the web UI displays an incorrect power outlet status when an invalid credential profile is configured for the discovery of a Vertiv™ PowerIT rPDU device.
  - Fixed issue where the Device Discovery page does not correctly validate IP address ranges, allowing invalid IP address entries during IP Range Discovery operations (CA-0001087739).
  - Fixed issue where the web UI does not update to reflect the correct firmware version after updating a rack manager (CA-0001089100 and CA-0001088135).
  - Fixed issue where the Notification Policy does not accept a dash (-) in the email address domain name in the Distribution List (CA-0001038642).
  - Fixed issue where the Targets - Appliance View and Administration - Firmware Updates pages do not display the correct firmware version after updating a rack manager's firmware (CA-0001082261).

4. Device Support Information

The Vertiv™ Avocent® RM1048P Rack Manager may manage the following devices:

- Vertiv™ Avocent® IPUHD 4K IP KVM device
- Vertiv™ Avocent® IPIQ IP KVM device
- Vertiv™ Avocent® IPSL IP serial device

- Vertiv™ PowerIT rPDUs
- Vertiv™ Liebert® rack UPS devices
- Vertiv™ Avocent® Universal Management Gateway appliance UMIQ-v2 module converted to operate as a Vertiv™ Avocent® IPIQ IP KVM device

  NOTE: For this functionality, contact your Vertiv Technical Support representative.

5. Language Support Information

The Vertiv™ Avocent® RM1048P Rack Manager software currently supports English and Simplified Chinese.

6. Client Browser Support Information

NOTE: Unless noted otherwise, both 32-bit and 64-bit browsers are supported.

BROWSER	PREFERRED VERSION	SUPPORTED VERSIONS
Edge	115+	79+
Firefox (Windows, MacOS, Linux)	115+	35+
Chrome	115+	40+
Safari	16+	12+

7. Viewer Support and Version Information

Supported Viewers

VIEWER	VERSION
KVM Viewer	4.55.1
Serial Viewer	4.29.1

Viewer Features and Browser Support

VIEWER FEATURE	MICROSOFT EDGE	MOZILLA FIREFOX	GOOGLE CHROME	APPLE SAFARI
Create ISO Image	Yes	No	Yes	No
Map Files or Folders in Virtual Media	Yes	No	Yes	No
Browse Disk Image	Yes	No	Yes	No

8. Server Processor (SP) Support Information

Tested SPs/Servers and Firmware

NOTE: Other SPs that support IPMI 2.0 may also be supported.

SERVICE PROCESSOR	FIRMWARE VERSION	PROTOCOLS
Dell iDRAC6 (R)	2.92	IPMI 2.0
Dell iDRAC7	2.65.65.65	Redfish, IPMI 2.0

SERVICE PROCESSOR	FIRMWARE VERSION	PROTOCOLS
Dell iDRAC8	2.84.84.84	Redfish, IPMI 2.0
Dell iDRAC9	6.10.80.00	Redfish, IPMI 2.0
HP iLO 2	iLO 2 v2.33	IPMI 2.0
HP iLO 3	iLO 3 v1.92	IPMI 2.0
HP iLO 4	iLO 4 v2.82	Redfish, IPMI 2.0
HP iLO 5	iLO 5 v2.91	Redfish, IPMI 2.0
Lenovo IMM2	TCOO60A 5.90	IPMI 2.0
Lenovo XCC	CDI3A8N 9.40	Redfish, IPMI 2.0
FSC iRMCS4	9.62F	IPMI 2.0
ACI	v4.3-2022-r08	Redfish, IPMI 2.0
OpenBMC	2.9, 2.11	Redfish, IPMI 2.0

Supported SPs/Servers for Launching KVM Sessions

SERVICE PROCESSOR	PORT	PORT TRAFFIC
Dell iDRAC7	5900	Inbound
Dell iDRAC8	5900	Inbound
Dell iDRAC9	5900 (default), 443 (configured with racadm)	Inbound
HP iLO 4	5900 (firmware < 2.8), 443 (firmware > 2.8)	Inbound
HP iLO 5	443	Inbound
XCC	3900	Inbound

9. Power Distribution Unit (PDU) Support Information

PRODUCT FAMILY	FIRMWARE VERSION
Vertiv™ PowerIT rPDU with I-03	6.3.0
Vertiv™ PowerIT rPDU with I-05M	6.3.0

10. Rack UPS Support Information

SUPPORTED VERTIV RACK UPS PRODUCT
Vertiv™ Liebert® GXT4 and Vertiv™ Liebert® GXT5 UPS
Vertiv™ Liebert® PSI5 UPS

Vertiv™ Edge UPS

Vertiv™ Liebert® APS UPS

11. Port Usage Information

PORT	TYPE	PORT TRAFFIC	SOURCE	DESTINATION	SERVICE	REQUIRED	NOTES
22	TCP	IN	Corporate Network	MP1000	SSH - Secure Shell Access	Required	Secure command-line access to MP1000 for administration, configuration, and CLI management. Use key-based authentication for enhanced security.
22	TCP	OUT	MP1000	Target Devices	SSH - Device Management	Required	SSH connections from MP1000 to managed devices (Vertiv™ Avocent® ACS800/8000 advanced console systems, switches, service processors) for configuration and management.
49	TCP	OUT	MP1000	TACACS+ Servers	TACACS+ Authentication	Optional	Terminal Access Controller Access-Control System Plus for centralized authentication, authorization, and accounting (AAA). Provides granular command authorization and full packet encryption.
123	UDP	OUT	MP1000	NTP Servers	NTP - Network Time Protocol	Required	Time synchronization with external or internal NTP servers. Accurate time is critical for logging, certificates, and time-based authentication (Kerberos, time-based OTP).
161	UDP	OUT	MP1000	Target Devices	SNMP - Monitoring Queries	Required	Outbound SNMP queries for device monitoring, status checks, and management information retrieval from managed infrastructure.
162	UDP	IN	Target Devices	MP1000	SNMP Trap - Alert Reception	Required	Inbound SNMP traps for receiving alerts, notifications, and events from managed devices (power events, device status changes, threshold alerts).
389	TCP	OUT	MP1000	LDAP Servers	LDAP - Lightweight Directory Access Protocol	Optional	User authentication and authorization against corporate directory services (Active Directory, LDAP). Used for centralized user management. Not encrypted; use LDAPS (636) when possible.
443	TCP	IN	Corporate Network	MP1000	HTTPS - Web Interface	Required	Secure web browser access to MP1000 management interface and REST API calls from external clients.
443	TCP	OUT	MP1000	Target Devices / Identity Providers	HTTPS - REST API & SSO	Required	Outbound HTTPS connections for REST API communications with managed devices and SSO authentication providers (Azure Entra ID, OKTA, etc.).
445	TCP	OUT	MP1000	Corporate Network	SMB - File Sharing	Optional	Server Message Block protocol for network file sharing, backup operations, and configuration file storage on network shares.
636	TCP	OUT	MP1000	LDAP Servers	LDAPS - LDAP over SSL/TLS	Recommended	Secure LDAP authentication with SSL/TLS encryption. Preferred over port 389 for directory services authentication. Provides encrypted credentials transmission.

1812	UDP	OUT	MP1000	RADIUS Servers	RADIUS Authentication	Optional	Remote Authentication Dial-In User Service for centralized authentication. Used for user authentication against RADIUS servers. Port 1812 is for authentication requests.
1813	UDP	OUT	MP1000	RADIUS Servers	RADIUS Accounting	Optional	RADIUS accounting for user session tracking, audit logging, and billing information. Port 1813 is for accounting requests. Typically used in conjunction with port 1812.
3900	TCP	OUT	MP1000	Service Processors	KVM Sessions - XCC	Optional	Remote KVM access to servers with XClarity Controller (XCC) - typically Lenovo servers. Provides remote console and keyboard/video/mouse access.
5900	TCP	OUT	MP1000	Service Processors	VNC/KVM Sessions	Optional	Virtual Network Computing protocol for KVM access to Dell iDRAC 7, 8, 9 and other VNC-based management interfaces. Standard VNC port for remote console sessions.
17988	TCP	OUT	MP1000	Service Processors	Virtual Media - HPE iLO	Optional	Virtual media connections for remote ISO/image mounting to HPE iLO managed servers. Enables remote OS installation and recovery operations.
17990	TCP	OUT	MP1000	Service Processors	KVM Sessions - HPE iLO	Optional	Remote KVM access sessions to HPE iLO managed servers (iLO 4, iLO 5, iLO 6). Provides integrated remote console access.

12. RESTful API

The Vertiv™ Avocent® DSView™ Solution RESTful API provides the ability to manage resources (i.e., users, devices, events, and more) that are included in the Vertiv™ Avocent® RM1048P Rack Manager. To view the RESTful API documentation, visit the **API User Guide**.

API Compatibility and Depreciation Notices
The diagnostic API endpoints introduced in this release are provisional and may undergo significant changes in future releases, potentially impacting backward compatibility. These endpoints are not yet documented in the official API documentation and should be used with caution in production environments.

13. Vertiv™ Avocent® DSView™ Solution Related Products

PRODUCT	DOWNLOAD PAGE
Vertiv™ Avocent® MP1000 Management Platform and Vertiv™ Avocent® MP1000VA Management Platform Virtual Appliance	https://www.vertiv.com/en-us/support/software-download/software/vertiv-avocent-mp1000-software-download-page/
Vertiv™ Avocent® IPIQ IP KVM device	https://www.vertiv.com/en-us/support/software-download/software/vertiv-avocent-ipiq-software-downloads/
Vertiv™ Avocent® IPUHD 4K IP KVM device	https://www.vertiv.com/en-us/support/software-download/software/vertiv-avocent-ipuhd-4k-ip-kvm-software-download-page/
Vertiv™ Avocent® IPSL IP serial device	https://www.vertiv.com/en-us/support/software-download/software/vertiv-avocent-ipsl-ip-serial-device-software-download-page/

14. Known Issues and Limitations

This release contains the following known issues and limitations:

- Firmware Update Issues:
  - [**BEFORE UPGRADING rPDU DEVICE]** When a Vertiv™ PowerIT rPDU device is connected to a rack manager and configured to obtain an IP address from a DHCP server, a firmware upgrade of the rPDU device causes the device to obtain a new IP address after it is rebooted. To resolve this issue, configure the rack manager to reserve an IP address for the rPDU device.
  - When updating firmware on Vertiv™ Avocent® IPUHD 4K IP KVM devices, the web UI may incorrectly display a successful update message even though the firmware update has failed. Note that firmware downgrades from version 3.x to 2.x are not supported on 4K IP KVM devices.
  - After restarting or upgrading the rack manager, the web UI may temporarily show devices on port 99. The system uses port 99 as a placeholder and will automatically display the correct port number when the port information is available. If port 99 persists on the web UI for a Vertiv™ Avocent® IPIQ IP KVM, Vertiv™ Avocent® IPUHD 4K IP KVM, or Vertiv™ Avocent® IPSL IP serial device, delete the device and allow it to be automatically added back to the system on the next registration.
- Bulk Firmware Update issues:
  - A bulk firmware update operation of several Vertiv™ Avocent® IPIQ IP KVM devices that are physically connected to the back of a rack manager may cause one or more firmware updates to fail. To resolve this issue, wait at least five minutes after the Vertiv™ Avocent® IPIQ IP KVM Device Bulk Firmware Update operation has failed, and then attempt to update the firmware for the IP KVM devices that have previously failed.
  - A bulk firmware update operation of several Vertiv™ Avocent® IPUHD IP KVM devices that are physically connected to the back of a rack manager may cause one or more firmware updates to fail. To resolve this issue, wait at least five minutes after the Vertiv™ Avocent® IPUHD IP KVM Device Bulk Firmware Update operation has failed, and then update the firmware for the 4K IP KVM devices that have previously failed. If the bulk update operation continues to fail, delete and re-add the 4K IP KVM device from the *Targets – Appliance View* or *Targets – Targets List* page, and then update the firmware for the 4K IP KVM devices. If the bulk firmware update operation issue is not resolved, follow these steps:
  - Disconnect the 4K IP KVM device from the back of the rack manager.
  - Delete the 4K IP KVM device from the *Targets – Appliance View* or *Targets – Targets List* page.
  - Restart both the SIP-Docker and IP-Management services using the CLI.
  - Update the firmware in the 4K IP KVM device.

- A bulk firmware update operation of several rack managers that are managed by the Vertiv™ Avocent® MP1000 Management Platform may cause one or more firmware updates to fail. To resolve this issue, follow these steps:
- Delete and re-add the rack manager from the *Targets - Appliance View* page.
- Re-add the rack manager.
- Update the firmware in the rack manager.

- Network Issues:
  - When connecting, disconnecting, and reconnecting large numbers (i.e., 40+) of Vertiv™ Avocent® IPIQ IP KVM devices to a Vertiv™ Avocent® RM1048P Rack Manager in a short period of time. To resolve this issue:
    1. Temporarily reduce the DHCP Lease Time through the rack manager web UI .
    2. Conduct a bulk device update or conversion.
    3. Restore the Lease Time to the default value of 86400 seconds (24 hours).
- Authentication Provider issues:
  - After upgrading the management platform firmware, Active Directory users configured with FQDN may be logged out and unable to authenticate. To resolve this issue, a local administrator must restart the 'egress-ldap' service using the *Diagnostics - Restart Service* menu in the CLI console and verify the service status before attempting to log in again.
- Certificate Issues:
  - The rack manager certificate generation fails after configuration of the email, RID, and URI entries in the Subject Alternative Name (SAN) when the appliance is managed by the Vertiv™ Avocent® MP1000 Management Platform.
  - The SAN (Subject Alternative Name) field is not included in a CSR (Certificate Signing Request) generated by a Vertiv™ Avocent® IPUHD 4K IP KVM or Vertiv™ Avocent® IPSL IP serial device that is managed by either the Vertiv™ Avocent® MP1000 Management Platform or the rack manager. A security warning will be presented in the browser after launching a KVM or serial session to the device.
  - Updating the certificate for a Vertiv™ Avocent® IPUHD 4K IP KVM device from the Targets List requires a manual refresh of the page to view the updated contents of the certificate.
- SP issues:
  - Power control options (Push button, Graceful Shutdown, Power off, and Power on System) for Dell iDRAC and Lenovo XCC service processors may fail. To resolve this issue, restart the Spider service using the *Diagnostics - Restart Service* menu in the management platform CLI.
  - Users are unable to access the web UI for iDRAC 8/9 service processors with firmware version 5.10.50.00 or higher from the Targets List view. To resolve this issue, follow these steps:
    1. Log in to the iDRAC 8/9 service processor from a console window.
    2. Execute the **racadm get idrac.webserver.HostHeaderCheck** command and verify that the host header check is enabled.
    3. Execute the **racadm set idrac.webserver.HostHeaderCheck 0** command and verify it is successfully executed.
    4. Execute the **racadm get idrac.webserver.HostHeaderCheck** command and verify that the host header check is disabled.
    5. Launch the web UI for the iDRAC 8/9 service processor from the Targets List view.
  - Accessing details for SPs that were discovered using invalid Credential Profile information results in an error message, and no device details are shown. The workaround for this is to update the Credential Profile in the SP's Properties panel and perform a Resync operation, or rediscover one or more SPs with an IP Range Discovery operation using the correct Credential Profile(s).
  - OpenBMC SPs do not support virtual media, sensor, power, or thermal data.
  - Virtual media resources are not supported in the XCC SP.
  - Mounting virtual media on iDRAC7/8 SPs behaves inconsistently.

- CIFS and NFS are not operational for HP iLO4 and iLO5 SPs.
- Unable to add an HP iLO4 device that is configured with a 1-1 NAT rule to the Vertiv™ Avocent® MP1000 Management Platform.
- No access is given to archived events on an HP iLO5 SP.
- The default system roles (User-Role, User-Administrator-Role and System-Maintainer-Role) do not include access to SPs.

- Session/Viewer issues:
  - When attempting to launch a KVM session to a target device connected to a Vertiv™ Avocent® MergePoint Unity™ 2 KVM over IP and serial console switch without sufficient permissions, the error message "You do not have permission to launch this viewer. Please close this window." is displayed as expected; however, the "OK" button in the popup is not clickable, preventing the user from closing the window. To resolve this issue, manually close the browser tab or window to exit the pop-up.
  - Launching simultaneous KVM sessions to target devices connected to a rack manager in proxy mode may cause the web UI to display an error message.
  - A user with a lower permission level can view the list of all viewer sessions.
  - Unable to map files or folders in Virtual Media using the Firefox client browser. This feature is only supported by Google Chrome and Microsoft Edge client browsers.
  - The icon to launch viewer sessions at the row level of the Appliance View and Targets List pages is missing for serial target devices that are managed by the Vertiv™ Avocent® DSView™ management software and displayed on the management platform web UI. The icon to launch viewer sessions is available on the Properties side panel.
  - Renaming a target device that is managed by the Vertiv™ Avocent® DSView™ management software and displayed on the Vertiv™ Avocent® MP1000 Management Platform web UI prevents launching a viewer session to the target device.
  - After the initial discovery of a Vertiv™ Avocent® IPIQ IP KVM device, the launch KVM icon in the Targets List and Appliance View remains disabled until the device completes the registration process. The Targets List View page can be refreshed after a few minutes to access the launch KVM icon for the device.
  - VM sessions are not cleared after exiting the KVM Viewer.
  - A KVM session to a Vertiv™ Avocent® IPUHD 4K IP KVM device that goes into sleep mode due to user inactivity does not respond to keyboard or mouse input.
  - Session timeout modifications do not take effect until a logout occurs; no message is forthcoming.
  - Viewer sessions for a Vertiv™ Avocent® IPUHD 4K IP KVM device connected to a rack manager do not show up correctly in the Dashboard.
- Web UI issues:
  - When NAT is configured for multiple devices connected to a Vertiv™ Avocent® RM1048P Rack Manager, launching the "Open Web Page" option for a Service Processor (SP) may incorrectly open the web interface of another device. On subsequent attempts, an "Unknown Error: Contact Administrator" message may appear, or the correct Service Processor web page may load inconsistently. To resolve this issue, review and correct the NAT configuration for each device in the *Network Configuration - NAT Setup* page to ensure unique and non-conflicting mappings are assigned to each device.
  - The System Settings page does not load and continues to display a loading state indefinitely when accessed by a newly created user, even after the user has been assigned the required roles and permissions. To resolve this issue, log in using an administrator account and verify that all required roles and permissions have been correctly assigned to the user and their associated groups.
  - When attempting to open the web page for a Service Processor (SP) connected to a Vertiv™ Avocent® RM1048P Rack Manager using the hyperlink in the SP view, an error message "No available IP" is displayed. To resolve this issue, use the "Open Web Page" option available in the three-dot menu from either the Appliance View or Targets List page instead of using the hyperlink in the SP view.
  - When 200 items are selected for viewing in the Appliance View page, the action row containing the three icons (Assign to Groups, Delete, and Firmware Update) may not be displayed. To resolve this issue, refresh the browser session to restore visibility of the action icons.
  - The Properties panel is inaccessible for Vertiv™ PowerIT rPDU outlets and Vertiv™ Liebert® rack UPS groups, which impacts a user's ability to change port names. To resolve this issue, change the port name using the web UI in the rPDU or rack UPS device, and then delete and rediscover the device using the rack manager web UI.

- The Factory Reset function for the rack manager does not work from the *Administrator - System Settings - Factory* Reset page in the web UI. When clicking the Factory Reset button, no action occurs. To resolve this issue, access the Command Line Interface (CLI) of the rack manager and use the CLI commands to perform the Factory Reset operation. The Factory Reset operation will complete successfully through the CLI interface.
- The three-dot menu (ellipsis) for IP Pool options is not visible in the Properties panel when viewing the details of a Vertiv™ Liebert® rack UPS device. To access these IP Pool options, use the three-dot menu available in the device row of the Appliance View, rather than the Properties panel.
- When attempting to delete a list of users that includes the default system administrator user, none of the selected users are deleted from the system.
- The scroll bar on the Targets List view is hidden when the browser window is resized to a smaller size.
- Clicking away from the Device Properties panel before the properties are fully loaded generates several errors for Vertiv™ Avocent® IPSL IP serial devices and the Vertiv™ Avocent® IPUHD 4K IP KVM devices.
- On the Organizations page, the Launch KVM Session icon may overlap with the Device Status icon. To resolve this issue and properly align both icons, zoom out on the browser page.
- Creating a new organization or filtering devices on organizations without any devices occasionally generates an error message; however, the new organization is successfully created.

- General issues:
  - When converting many Vertiv™ Avocent® Universal Management Gateway appliance UMIQ-v2 modules to operate as Vertiv™ Avocent® IPIQ IP KVM devices simultaneously using a Vertiv™ Avocent® RM1048P Rack Manager, one or more modules may fail to complete the conversion successfully. To resolve this issue, convert no more than twenty UMIQ-v2 modules at a time, waiting for each batch to complete successfully before proceeding with the next group of modules.
  - When disabling the Network Time Protocol (NTP) setting via the web UI on the management platform or Vertiv™ Avocent® RM1048P Rack Manager, the web UI logs out automatically after saving. Upon re-login, the NTP setting does not persist as disabled and reverts to its previous enabled state. To resolve this issue, disable the NTP setting using the *Show/Configure Manager – Turn NTP Off* menu in the management platform CLI or rack manager CLI.
  - When a Vertiv™ PowerIT rPDU device is connected to a managed rack manager, deleting the PDU device from the web UI and rebooting the rack manager prevents the PDU device from being rediscovered automatically.
  - During system startup, the CLI interface on the management platform hardware, virtual appliance or rack manager may display the Troubleshooting menu instead of the main CLI menu. This occurs when a service is still starting up or experiencing startup issues. The Troubleshooting menu provides diagnostic options to help identify and resolve service-related problems. To resolve this issue:
    1. Select Option 0 from the Troubleshooting menu to access the main CLI menu if services have completed startup.
    2. Use the Show Services option in the Troubleshooting menu to identify which service may be experiencing issues and view its logs.
    3. If the main CLI menu does not become accessible after a reasonable waiting time (i.e., 5 or 10 minutes), contact Vertiv Technical Support for assistance.
  - The Vertiv™ Avocent® RM1048P Rack Manager may experience intermittently high fan speeds and elevated CPU usage, even when no devices are connected to the rack manager.
  - When editing a Credential Profile in the Properties panel, the web UI may incorrectly show an option to select the same credential that is already assigned. Attempting to choose and save this duplicate credential results in an error message. To avoid this issue, do not select the duplicate credential option when editing Credential Profiles.
  - After updating the serial port name from the Vertiv™ Avocent® IPSL IP serial device user interface, the serial port name is not synchronized in the Appliance View or Targets List pages.
  - Unable to access the CLI of the rack manager with older SSH clients due to an encryption error. To resolve this issue, update the SSH client to the latest version.

- SNMP V3 traps are currently not supported in the rack manager.
- Upgrading the rack manager may display the upgrade status “In Progress” for an extended period of time even after the upgrade has completed successfully. When this occurs, manually reboot the rack manager appliance.
- A power cycle of a Vertiv™ Liebert® rack UPS device outlet group using the web UI does not work correctly when the outlet group is already turned off.
- The outlet groups of a Vertiv™ Liebert® rack UPS device that is connected to a rack manager may not be synchronized in the Appliance View or Targets List page after an appliance firmware upgrade. To resolve this issue, delete the UPS device and then re-add it to the Appliance View or Targets List page.
- Unable to discover a Vertiv™ PowerIT rPDU device with a Credential Profile that is configured with a specific port number. To resolve this issue, leave the port field blank and rediscover the rPDU device.
- Changing the assigned DHCP IP address of a Vertiv™ PowerIT rPDU device to a reserved IP address causes the status of the device to show incorrectly. To resolve this issue, delete the rPDU device from the web UI and rediscover the device using the reserved IP address.
- The Credential Profile assigned to a target device cannot be modified after the target device is discovered and added to the Targets List page. To modify the Credential Profile, rediscover the target device.
- The Appliance View may show duplicate entries for Vertiv™ PowerIT rPDUs after discovery of rPDUs with the following Credential Profile Configurations:
  - If there is one Credential Profile configured with SNMP V2 and firmware update credentials.

    -or-

    If there are two Credential Profiles, where the first is configured with SNMP v2 and the second is configured with username/password.

  If this situation occurs and an rPDU listing is duplicated in the Appliance View, the rPDU power outlet status will not display correctly. To resolve the duplicate entry scenario, delete one of the duplicate listings. After the duplicate listing is deleted, wait a few minutes and refresh the web page. This should then correct the rPDU power outlet status information as well.
- The scheduled Daily Alarm Purge operation only purges alarms that are cleared and older than the configured retention period.
- The alarm drop-down list in the upper right corner of the page does not update correctly when new alarms are generated. To resolve this issue, log out and log back into the application to view the updated list of alarms in the drop-down list.
- Device name synchronization is not available for Vertiv™ PowerIT rPDUs discovered via SNMP.
- Unable to change the power state of a Vertiv™ Liebert® PSI5 UPS outlet group.
- An attempt to establish a remote Virtual Media session to a Vertiv™ Avocent® IPUHD 4K IP KVM device managed by a rack manager using the NFS Transfer Protocol fails with an error message.
- Changing network settings from DHCP to Static on the Properties panel requires wait at least one minute, then refresh the page to view updated changes.
- The Kingston USB device is not supported and not displayed in the Boot Manager.
- Power Control is non-functional for unlicensed VMware targets.
- The Virtual Machine Viewer Caps Lock (and other keys) are not highlighted when using Linux; this is not supported in VMware.

- The changed time (from the CLI) is not maintained through a reset. BIOS overrides time and must be set via BIOS.
- Deleting an unmanaged rack manager in the Vertiv™ Avocent® MP1000 Management Platform does not trigger the rack manager to go into Standalone mode; it must be done manually.
- In some rare cases, the Status column in the Targets List view disappears when using the Google Chrome browser. If this occurs, clear the browser cache and open a new browser window.