Vertiv™ Avocent® RM1048P Rack Manager

Release Notes

VERSION 1.66.1, FEBRUARY 2025

Release Notes Section Outline

1. Update Instructions
2. Appliance Firmware Version Information
3. Features and Enhancements
4. Device Support Information
5. Language Support Information
6. Client Browser Support Information
7. Viewer Support and Version Information
8. Server Processor (SP) Support Information
9. Power Distribution Unit (PDU) Support Information
10. Rack UPS Support Information
11. TCP Port Usage Information
12. Known Issues and Limitations

1. Update Instructions

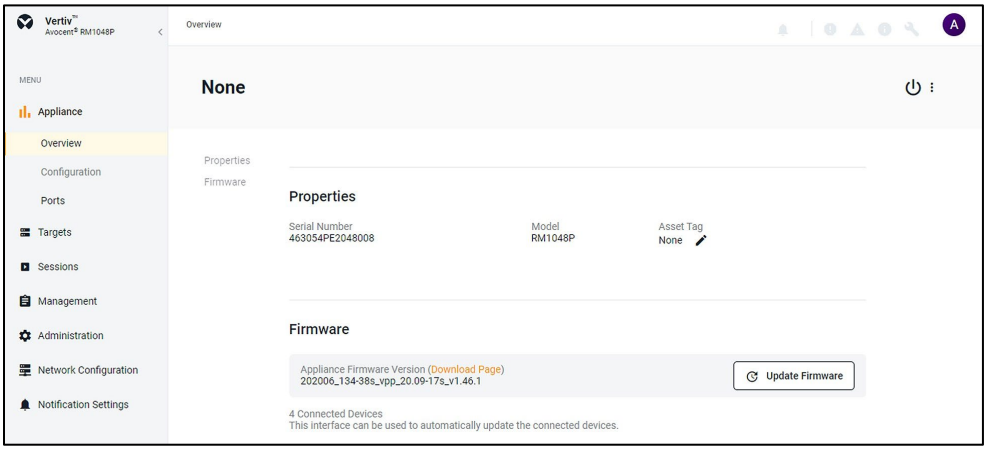
The Vertiv™ Avocent® RM1048P Rack Manager firmware may be updated through the web user interface (UI). To access the rack manager web UI, enter your assigned IP address into a web browser (this IP address is provided upon initial set up of the Vertiv™ Avocent® RM1048P Rack Manager).

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

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

To update the Vertiv™ Avocent® RM1048P Rack Manager firmware:

1. Visit the Vertiv™ Avocent® RM1048P Rack Manager firmware download page located here: Vertiv™ Avocent® RM1048P Rack Manager Software Download
2. Download the latest firmware and save it to your local computer, FTP or HTTP server.
   NOTE: The latest firmware version is listed in the Appliance Firmware Version Information section of these release notes.
3. In a web browser, enter **https://**<appliance.IP> using the IP address for Vrf_app0 that you configured from the Vertiv™ Avocent® RM1048P Rack Manager console menu.
4. Enter your 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 if you'd like to update the firmware for just the rack manager or if you'd like 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.

2. Appliance Firmware Version Information

APPLIANCE/PRODUCT	VERSION	FILENAME
Vertiv™ Avocent® RM1048P Rack Manager	1.66.1	SONiC-202006_134-40s_vpp_20.09-17s_v1.66.1.bin

3. Features and Enhancements

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

- Adds the ability to replace self-signed certificates with Certificate Authority (CA) generated certificates via the web UI.
  - To establish a secure connection with the web UI, you must include the FQDN (Fully Qualified Domain Name) in the SAN (Subject Alternate Name) field of the CSR request.
  - If you receive the signed certificate from the CA (certificate authority) in a format that is different than the required PEM format (such as pb7), you must convert the CA signed certificate to PEM format before replacing the self-signed certificate with the CA signed certificate.
- Adds support for backup and restore of the Vertiv™ Avocent® RM1048P Rack Manager via the CLI.
- Adds support for auto discovering devices that are connected to a Vertiv™ Avocent® RM1048P Rack Manager.
- Adds support for adding generic devices via the web UI.
- Adds support for displaying a hierarchical view of devices connected to the Vertiv™ Avocent® RM1048P Rack Manager.
- Enhances the Session List page as follows:
  - Adds support for sorting and filtering session list data.
  - Adds ability to export session list data to a comma-separated value (CSV) file.
- Enhances the ability to perform bulk firmware upgrades.

Resolved Issues

- General issues resolved:
  - Fixed issue where a user with access to devices in a resource group who is assigned the System Administrators role is restricted to have access only to the devices in the resource group instead of having access to all devices.
  - Fixed issue where testing of a user that belongs to an AD or LDAP external authentication provider fails during the configuration of the external authentication provider (CA-0000909025).
  - Fixed issue where the Network Configuration page displays an error message when entering a period character in the Domain Name field (CA-0000855098).
  - Fixed issue where after discovery of a Vertiv™ Liebert® rack UPS or Vertiv™ Geist™ rPDU device that is connected to a Vertiv™ Avocent® RM1048P Rack Manager, the power outlets may not be displayed on the web UI.
  - Fixed issue where inactive devices from a Vertiv™ Avocent® RM1048P Rack Manager that is managed by the Vertiv™ Avocent® MP1000 Management Platform may not be removed properly during the scheduled auto device cleanup operation.
  - Fixed security issues (CA-0000860138).
- SP issues resolved:
  - Fixed issue where retrieving metric information from service processors may fail within a specific period of time (for example, 30 minutes) after an initial request to obtain metric information has been initiated.
- CLI issues resolved:
  - Fixed issue where searching for a DNS entry from the CLI displays an error message (CA-0000893427).

- Fixed issue where displaying the list of SMB backups from the CLI displays an error message (CA-0000828618).
- Fixed issue where the *No Such file or directory* error message is displayed after selecting the CLI Diagnostics option (CA-0000893446)

- Viewer issues resolved:
  - Fixed issue where a copy and paste operation to a file that is opened on a KVM session to a target device is not working properly (CA-0000948620).
- Web UI issues resolved:
  - Fixed issue where the firmware version in the Appliance View is not updated correctly after performing an upgrade of the Vertiv™ Avocent® RM1048P Rack Manager (CA-0000826005).

4. Device Support Information

The following devices may be managed by the Vertiv™ Avocent® RM1048P Rack Manager:

- Vertiv™ Avocent® IPUHD 4K IP KVM device
- Vertiv™ Avocent® IPIQ IP KVM device
- Vertiv™ Avocent® IPSL IP serial device
- Vertiv™ Geist™ 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	4.41.1
Serial Viewer	4.17.1

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
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

SERVICE PROCESSOR	PORT	PORT TRAFFIC
XCC	3900	Inbound

9. Power Distribution Unit (PDU) Support Information

PRODUCT FAMILY	FIRMWARE VERSION
Vertiv™ Geist™ I-03 PDU	5.10.4

10. Rack UPS Support Information

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

11. TCP Port Usage Information

PORT	TYPE	PORT TRAFFIC	DESCRIPTION
443	TCP	Inbound, Outbound	General Communications (TCP)
22	TCP	Inbound	General Communications (TCP)
3871	TCP	Outbound	Vertiv™ Avocent® ACS800/8000 advanced console systems
48048	TCP	Outbound	The default port for RESTful API communication with a Vertiv™ Avocent® ACS800/8000 advanced console system. This port is configurable on the advanced console system.

12. Known Issues and Limitations

This release contains the following known issues and limitations:

- 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 Vertiv™ Avocent® RM1048P Rack Manager may cause one or more firmware updates to fail. To resolve this issue, wait for 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 Vertiv™ Avocent® IPIQ 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 Vertiv™ Avocent® RM1048P Rack Manager appliance may cause one or more firmware updates to fail. To resolve this issue, wait for at least five minutes after the Vertiv™ Avocent® IPUHD IP KVM Device Bulk Firmware Update operation has failed and then update the firmware for Vertiv™ Avocent® IPUHD IP KVM devices that have previously failed. If the bulk update operation continues to fail, delete and re-add the Vertiv™ Avocent® IPUHD IP KVM device from the *Targets – Appliance View* or *Targets – Target List* page and then update the firmware for Vertiv™ Avocent® IPUHD IP KVM devices. If the bulk firmware update operation issue is not resolved, follow these steps:
    1. Disconnect the Vertiv™ Avocent® IPUHD IP KVM device from the back of the Vertiv™ Avocent® RM1048P Rack Manager.

2. Delete the Vertiv™ Avocent® IPUHD IP KVM device from the *Targets – Appliance View* or *Targets – Target List* page.
3. Restart both the sip-docker and ip-management services using the CLI.
4. Update the firmware in the Vertiv™ Avocent® IPUHD IP KVM device.

- A bulk firmware update operation of several Vertiv™ Avocent® RM1048P Rack Managers that are managed by the Vertiv™ Avocent® MP1000 Management Platform appliance may cause one or more firmware updates to fail. To resolve this issue, follow these steps:

1. Delete and re-add the Vertiv™ Avocent® RM1048P Rack Manager appliance from the *Targets - Appliance View* page.
2. Re-add the Vertiv™ Avocent® RM1048P Rack Manager.
3. Update the firmware in the Vertiv™ Avocent® RM1048P Rack Manager.

- Certificate Issues:
  - 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 Vertiv™ Avocent® RM1048P Rack Manager. A security warning will be presented on 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:
  - 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 Target 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 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 the host header check is disabled.
5. Launch the web UI for the iDRAC 8/9 service processor from the Target 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 you can 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:
  - Unable to map files or folders in Virtual Media using the Firefox client browser. This feature is only supported by Chrome and Edge client browsers.
  - The icon to launch viewer sessions at the row level of the Appliance and Target List Views 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 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 Vertiv™ Avocent® RM1048P Rack Manager does not show up correctly in the Dashboard.

- Web UI issues:
  - 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 Target 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.
  - The RS422 and RS485 RJ-45 pin-out value options on the Physical Port Settings panel only apply to ports 1 and 2 of the Vertiv™ Avocent® ACS8000 advanced console system.
  - 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:
  - 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 Targets – Appliance View or Targets – Target List page.
  - Unable to access the CLI of the Vertiv™ Avocent® RM1048P 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 being supported in the Vertiv™ Avocent® RM1048P Rack Manager.
  - When a Vertiv™ Geist™ rPDU device is connected to a Vertiv™ Avocent® RM1048P 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.
  - Upgrading the Vertiv™ Avocent® RM1048P Rack Manager appliance may display the upgrade status “In Progress” for a long 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 properly when the outlet group is already turned off.
  - The outlet groups of a Vertiv™ Liebert® rack UPS device that is connected to a Vertiv™ Avocent® RM1048P Rack Manager may not be synchronized in the Appliance View or Target List page after an appliance firmware upgrade. To resolve this issue, delete the UPS device and add it back to the Appliance View or Target List page.
  - Unable to discover a Vertiv™ Geist™ rPDU device with firmware 6.x using a credential profile that is configured with username and password. To resolve this issue, enable the Aggregation feature and set the HTTP Interface to “Enabled” on the rPDU device. Then, re-discover the rPDU device using the web UI.
  - Unable to discover a Vertiv™ Geist™ rPDU device with a Credential Profile that is configured with a specific port number. To resolve this issue, leave the port field blank and re-discover the rPDU device.
  - Changing the assigned DHCP IP address of a Vertiv™ Geist™ rPDU device to a reserved IP address causes the status of the device to show incorrectly. To resolve this issue, delete the Vertiv™ Geist™ 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 Target List page. To modify the Credential Profile, you need to rediscover the target device.
  - The Appliance View may show duplicate entries for Vertiv™ Geist™ 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 Profile 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. Once 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™ Geist™ 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 Vertiv™ Avocent® RM1048P Rack Manager using the NFS Transfer Protocol fails with an error message.
- Changing network settings from DHCP to Static on the Properties panel requires you to 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 highlighting 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 Vertiv™ Avocent® RM1048P 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 Target List view disappears using the Chrome browser. If this occurs, clear the browser cache and open a new browser window.