

# Vertiv™ Avocent® ADX RM1048P Rack Manager

## Release Notes

VERSION 1.33.6, JULY 2023

### 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. Dashboard Support Information
9. Server Processor (SP) Support Information
10. Power Distribution Unit (PDU) Support Information
11. Rack UPS Support Information
12. TCP Port Usage Information
13. Known Issues and Limitations

### 1. Update Instructions

The Vertiv™ Avocent® ADX 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® ADX RM1048P Rack Manager).

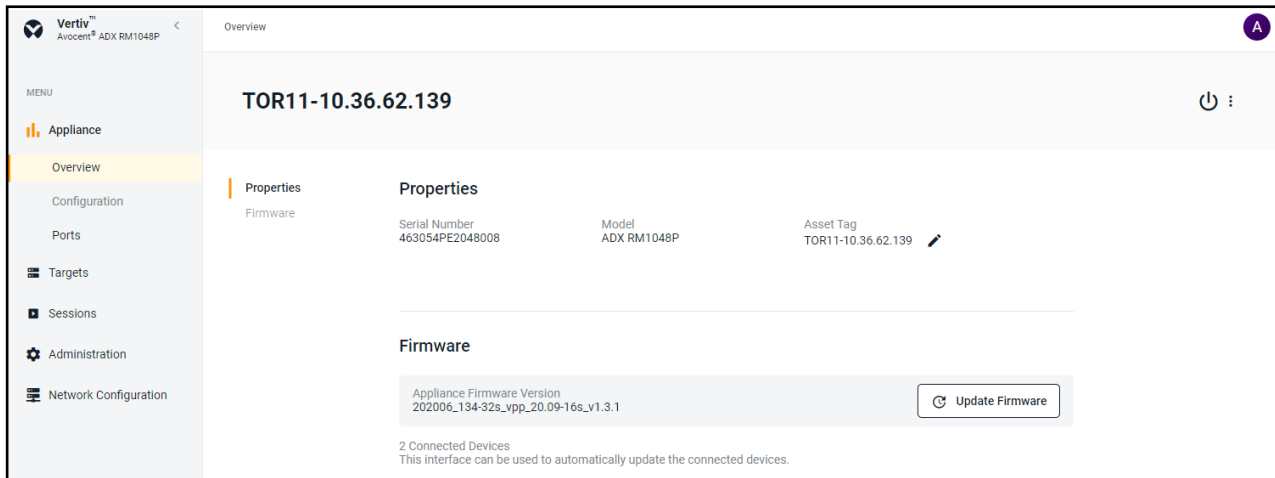
**NOTE:** For additional information on this process, see the Vertiv™ Avocent® ADX RM1048P Rack Manager Quick Installation Guide that is provided with the rack manager and also available at [Vertiv™ Avocent® ADX Rack Manager](#) under the *Documents & Downloads* tab.

**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® ADX RM1048P Rack Manager firmware:

1. Visit the Vertiv™ Avocent® ADX RM1048P Rack Manager firmware download page located here:  
[Vertiv™ Avocent® ADX 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® ADX RM1048P Rack Manager console menu.
4. Enter your username and password at the login screen; the Targets List screen opens.

- In the sidebar, select *Appliance-Overview* and click the *Update Firmware* button.



- 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.
- 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® ADX RM1048P Rack Manager	1.33.6	SONiC-202006_134-38s_vpp_20.09-17s_v1.33.6.bin

## 3. Features and Enhancements

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

- This release adds support for discovering Vertiv™ Avocent® IPSL IP serial devices and then adding them to the Target List view.
- This release adds support for discovering Vertiv™ Geist™ rack Power Distribution Units (rPDUs) and then adding them to the Target List view. This capability allows you to perform the following operations:
  - View power metrics on rPDU device and perform power operations.
  - Merge rPDU outlets with other devices.
  - Synchronize rPDU outlet names.
  - Update the firmware on the rPDU.

**NOTE: In the Vertiv™ Avocent® ADX RM1048P Rack Manager web UI, Vertiv™ Geist™ rPDUs may be referred to as “Geist™ PDUs” or “Rack PDUs”.**

- This release adds support for discovering Vertiv™ rack UPS devices and then adding them to the Target List view. This capability allows you to perform the following operations:
  - View power metrics on the rack UPS device.
- This release adds support for viewing and managing device alarms. This functionality includes the following operations:
  - Search, sort, and filter device alarms.
  - Manually clear device alarm status.
  - Set a device in maintenance mode.
  - Configure alarm retention policy.
  - Display alarm count and alarm severity status.

- This release adds support for updating the Vertiv™ Geist™ rPDU firmware through the Vertiv™ Avocent® RM1048P Rack Manager web UI.
- This release adds support for a user to be notified in a pop-up notification panel when new devices have been discovered.
- This release adds support for configuring Cross-Origin Resource Sharing (CORS) through the Command Line Interface (CLI).
- This release adds API support to launch KVM, serial and Virtual Machine sessions.
- This release adds support for mapping a disk image as writable in KVM Viewer virtual media.
- This release adds the capability for updating the firmware for multiple devices in bulk mode.
- This release adds support for a TACACS+ external authentication provider.

## Resolved Issues

- General issues resolved:
  - Fixed issue where the firmware update operation from the Targets List was not working properly.
  - Fixed issue where a reboot operation after configuring a NAT rule on the Vertiv™ Avocent® ADX RM1048P Rack Manager causes the NAT rule IP address to be unreachable.
  - Fixed issue where the user is unable to assign multiple roles to a resource group that belongs to a user group when the length of all combined roles exceeds 69 characters.
  - Fixed issue where a new user assigned to a default user group is unable to access the Appliance View.
  - Fixed issue where a login attempt fails when multiple external authentication providers are configured in the Vertiv™ Avocent® ADX Platform system (CAS-56844-V1Q6K2 and CAS-55832-Z6Z8LO).
  - Fixed issue where a connection to a secure AD or LDAP authentication provider requires client certificate verification (CAS-59302-K5D5R7).
  - Fixed issue where merging a port on an Vertiv™ Avocent® ACS800 and/or ACS8000 device with another device creates duplicate launch serial icons on the Target List (CAS-55823-Z2H0C0).
  - Fixed issue where duplicate entries of a Vertiv™ Avocent® ADX IPIQ IP KVM device can be added to the Target List (CAS-56469-M8W4H9).
  - Fixed issue where the web UI was unable to retrieve groups from an external authentication provider with a large number of external groups (CAS-61819-L7X2S8).
  - Fixed issue where a user cannot drill down to a service processor from the Target List to access detailed information for the service processor (CAS-57036-W6J7S8).
  - Fixed issue where a Vertiv™ Avocent® ADX IPIQ IP KVM device in the Target List cannot be rediscovered after the device has been deleted from the Target List (CAS-60870-Q8K1X6).
  - Fixed issue where the username is not displayed for closed sessions on the Session List panel (CAS-59092-T5P0J8).
  - Fixed issue where a loss of communication occurs when the failover does not match the primary interface (CAS-56062-L9V2M0).
  - Fixed issue where the disk space on a Vertiv™ Avocent® ADX RM1048P Rack Manager was getting full due to a large number of database core dump files.
  - Fixed issue where a firmware update on the Vertiv™ Avocent® ADX RM1048P Rack Manager appliance with a large database causes the system to be non-operational.
- Viewer issues resolved:
  - Fixed issue where a user was unable to join an existing KVM session from the Sessions List page when the virtual media session was active on the KVM Viewer.
  - Fixed issue where a user was unable to download an ISO image file after being mapped to a file or folder in a virtual media session.
  - Fixed issue where a user attempts to change the default filename during creation of an ISO image file and the new filename does not take effect.
  - Fixed issue where launching a passive or stealth KVM session behaves as an active KVM session when the system proxy is enabled.
  - Fixed issue where a connection to a KVM session for a Vertiv™ Avocent® IPIQ IP KVM device drops after a few seconds when the system proxy is enabled.
- Configuration issues resolved:
  - Fixed issue where a reboot operation after configuring a NAT rule on the Vertiv™ Avocent® ADX RM1048P Rack Manager causes the NAT rule configuration to disappear.

- Fixed issue where the FIPS option was missing from the properties panel for a selected Vertiv™ Avocent® ADX IPUHD 4K IP KVM device on the Target List page.
- Fixed issue where a user from an external authentication provider was unable to login after changing the external authentication provider from insecure to secure mode.
- Fixed issue where a user is unable to change the domain name of a Vertiv™ Avocent® ADX RM1048P Rack Manager in the Network Settings page (CAS-56499-N0G3V8 and CAS-56531-K3D3P9).
- Fixed issue where the MAC Address for a Vertiv™ Avocent® ADX IPIQ IP KVM device is not displayed on the Network Configuration panel (CAS-59056-P5T1X2).

## 4. Device Support Information

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

- Vertiv™ Avocent® ADX IPUHD 4K IP KVM device
  - Vertiv™ Avocent® ADX IPIQ IP KVM device
  - Vertiv™ Avocent® ADX IPSL IP serial device
  - Vertiv™ Geist™ rPDUs
  - Vertiv™ and Vertiv™ Liebert® rack UPS devices
  - Vertiv™ Avocent® Universal Management Gateway appliance UMIQ-v2 module converted to operate as a Vertiv™ Avocent® ADX IPIQ IP KVM device
- NOTE: For this functionality, contact your Vertiv Technical Support representative.**

## 5. Language Support Information

The Vertiv™ Avocent® ADX 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	99+	79+
Firefox (Windows, MacOS, Linux)	97+	35+
Chrome	99+	40+
Safari	15+	12+

## 7. Viewer Support and Version Information

### Supported Viewers

VIEWER	VERSION
KVM Viewer	4.11.1
Serial Viewer	4.5.1

## 8. Dashboard Support Information

ITEM	VERSION
Dashboard	1.25.1

## 9. 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
Dell iDRAC7	5900
Dell iDRAC8	5900
Dell iDRAC9	5900 (default), 443 (configured with racadm)
HP iLO 4	5900 (firmware < 2.8), 443 (firmware > 2.8)
HP iLO 5	443
XCC	3900

## 10. Power Distribution Unit (PDU) Support Information

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

## 11. Rack UPS Support Information

### SUPPORTED VERTIV RACK UPS PRODUCT

Vertiv™ Liebert® GXT5 UPS

Vertiv™ Liebert® PSI5 UPS

Vertiv™ Edge UPS

Vertiv™ Liebert® APS UPS

## 12. TCP Port Usage Information

**NOTE:** TCP port usage is bidirectional unless otherwise noted.

PORT	TYPE	DESCRIPTION
443	TCP	General Communications (TCP)
22	TCP	General Communications (TCP)
3871	TCP	Vertiv™ Avocent® ACS800/8000 advanced console systems

## 13. Known Issues and Limitations

This release contains the following known issues and limitations:

- 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:
    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.
  - No access is given to archived events on an HP iLO5 SP.
  - Clicking the SP name link (hyperlink) on the Targets List view produces error messages.
  - The default system roles (User-Role, User-Administrator-Role and System-Maintainer-Role) do not include access to SPs.
- Session/Viewer issues:
  - After the initial discovery of a Vertiv™ Avocent® ADX 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® ADX 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® ADX IPUHD 4K IP KVM device connected to a Vertiv™ Avocent® ADX RM1048P Rack Manager does not show up correctly in the Dashboard.
- Web UI issues:
  - 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® ADX 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.
  - With the option to add another resource group to a resource group, there are only options to add existing resource groups.
  - Unable to change a full name in the User Preferences view.
- General issues:
  - 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.
  - Device name synchronization is not available for Vertiv™ Geist™ rPDUs discovered via SNMP.
  - An attempt to establish a remote Virtual Media session to a Vertiv™ Avocent® ADX IPUHD 4K IP KVM device managed by a Vertiv™ Avocent® ADX 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.
  - Managed Vertiv™ Avocent® ADX RM1048P Rack Manager and Vertiv™ Avocent® ADX IPUHD 4K IP KVM device firmware updates via the new managed device drill-down page fail with an error message.
  - Deleting an unmanaged Vertiv™ Avocent® ADX RM1048P Rack Manager in the Vertiv™ Avocent® ADX 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.