Vertiv™ Avocent® RM1048P Rack Manager

Release Notes

VERSION 1.74.1, DECEMBER 2025

Release Notes Section Outline

1. Update Instructions

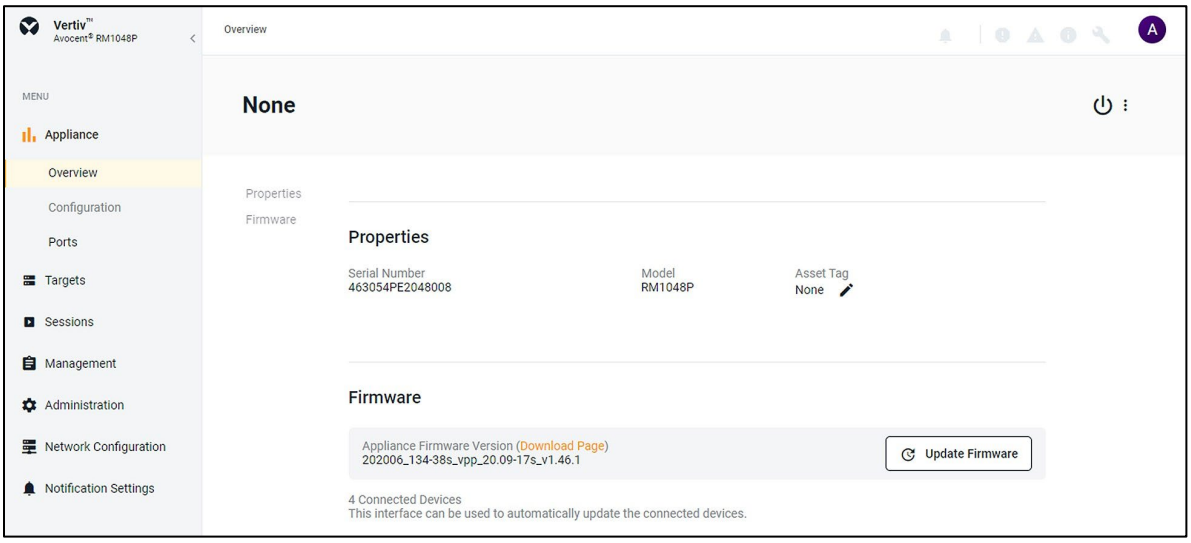
The Vertiv™ Avocent® RM1048P Rack Manager firmware may be updated through the web user interface (UI). To access the rack manager web UI, enter your assigned IP address into a web browser, which is provided during the initial setup of the rack manager.

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 Rack Manager product page 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 rack manager firmware:

1. Visit the 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 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.
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	1.74.1	SONiC-202006_134-40s_vpp_20.09-17s_v1.74.1.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.

Resolved Issues

- General issues resolved:
  - 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.

- 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).
- Session/Viewer Issues resolved:
  - Fixed issue where a user with a lower permission level can view the list of all viewer sessions.
- Web UI issues resolved:
  - 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
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

SERVICE PROCESSOR	FIRMWARE VERSION	PROTOCOLS
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. TCP Port Usage Information

PORT	TYPE	PORT TRAFFIC	DESCRIPTION
443	TCP	Inbound, Outbound	General Communications (TCP)
22	TCP	Inbound	General Communications (TCP)

12. 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/

13. 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:
    1. Disconnect the 4K IP KVM device from the back of the rack manager.
    2. Delete the 4K IP KVM device from the *Targets – Appliance View* or *Targets – Targets List* page.
    3. Restart both the SIP-Docker and IP-Management services using the CLI.
    4. 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:
    1. Delete and re-add the rack manager from the *Targets - Appliance View* page.
    2. Re-add the rack manager.
    3. Update the firmware in the rack manager.
- 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 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 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 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:
  - 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:
  - 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 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 or after deleting a rack manager from the Vertiv™ Avocent® MP1000 Management Platform, the CLI interface on the rack manager may display the Troubleshooting menu instead of the main CLI menu. To resolve this issue, you can select Option **0** from the Troubleshooting menu to access the main CLI menu.
  - 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, you need to 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 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 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.