# Vertiv™ Avocent® MP1000 Management Platform
## Release Notes

### VERSION 3.50.8, NOVEMBER 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. Vertiv™ Avocent® DSView™ Management Software Versions
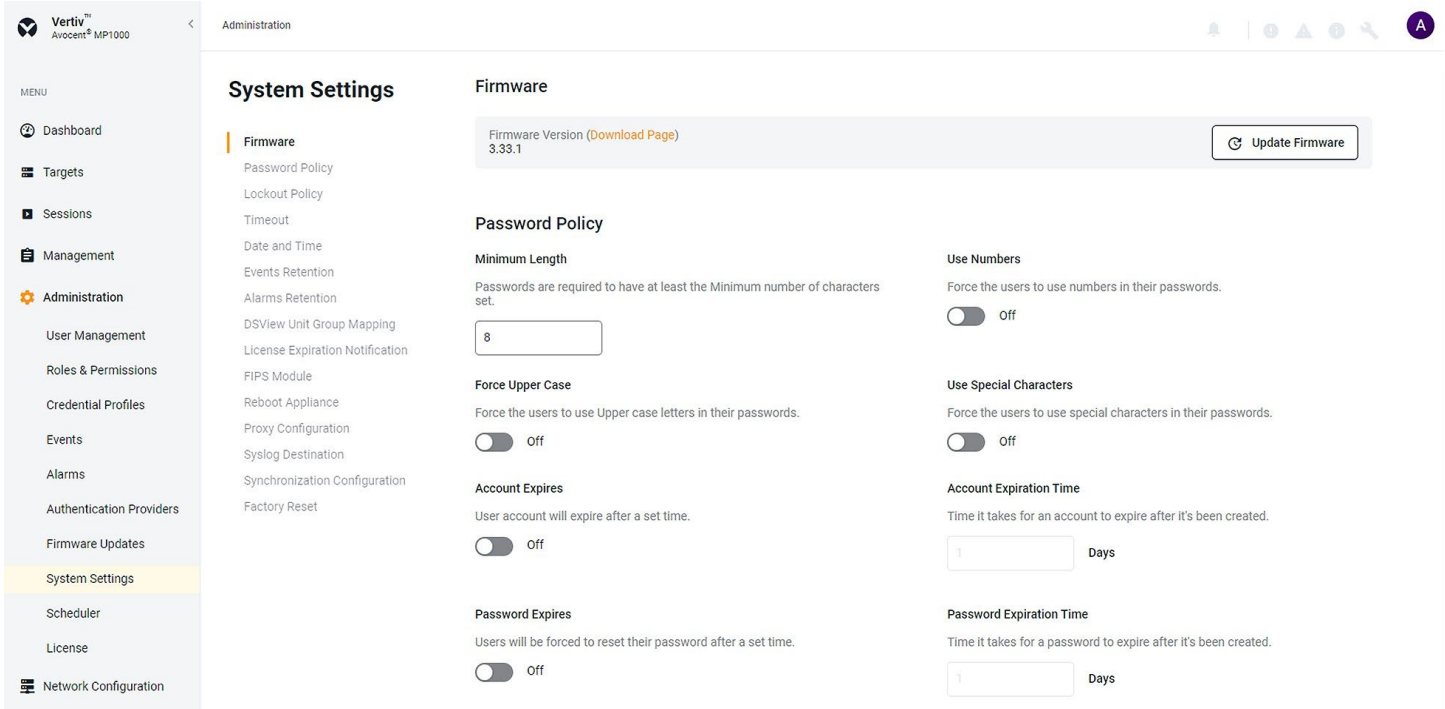14. Known Issues and Limitations

## 1. Update Instructions

The Vertiv™ Avocent® MP1000 Management Platform firmware may be updated through the web user interface (UI). To access the Vertiv™ Avocent® MP1000 Management Platform web UI, enter your assigned IP address into a web browser (this IP address is provided upon initial set up of the management platform).

**NOTE: For additional information on this process, see the Vertiv™ Avocent® MP1000 Management Platform Quick Installation Guide that is provided with the platform and also available at** www.vertiv.com/Management-Platform **under the** *Documents & Download*s **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® MP1000 Management Platform firmware:

1. Visit the Vertiv™ Avocent® MP1000 Management Platform firmware download page located here:
   Vertiv™ Avocent® Management Platform Software Download
2. Download the latest firmware and save it to your local computer, FTP, HTTP or TFTP 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 eno1 that you configured from the Vertiv™ Avocent® MP1000 Management Platform console menu.
4. Enter your username and password at the login screen; the Targets List screen opens.
5. In the sidebar, select *Administration - System Settings* and click the *Update Firmware* button.

6. Select the firmware file and click *Update*.

## 2. Appliance Firmware Version Information

| APPLIANCE/PRODUCT | VERSION | FILENAME |
|---|---|---|
| Vertiv™ Avocent® MP1000 Management Platform | 3.50.8 | obsidian-3.50.8-update.img.xz |

## 3. Features and Enhancements

The following features and enhancements are available with this release of the Vertiv™ Avocent® MP1000 Management Platform:

- This release adds support to manage discovery requests, which allows the user to perform the following operations:
  - View the list of discovery requests created by all users.
  - View the details and progress of each discovery request, including the status of each IP address in the discovery range.
- This release adds support for the following operations on Vertiv™ Rack UPS devices:
  - View and power cycle UPS device outlet groups.
  - Synchronize UPS devices and UPS device outlet names.
- This release adds support for the following operations on Vertiv™ Geist™ rack Power Distribution Units (rPDUs):
  - Synchronize Rack PDU devices.
  - Manage daisy chained Rack PDU devices.
- This release adds support for email notifications, which allows the user to perform the following operations:
  - Enable or disable email notification based on alarm severity.
  - Select the alarm severity to use for sending email notifications to multiple recipients.
- This release adds the following firmware update enhancements:
  - Add a Firmware Update History view to show a history of firmware updates including the current status for ongoing firmware updates.

- Allow the selection of multiple devices of the same type and perform a bulk firmware update.
- This release adds support for user authentication with an external RADIUS authentication provider.
- This release adds support to allow a user to launch a KVM Viewer session in Standalone Passive or read-only mode which does not require approval for subsequent users to join the same KVM viewer session.
- This release adds the ability to select and clear all entries across multiple pages with or without a filter in the Target List, Appliance View, and Organization View.
- This release adds support to perform a backup of the management platform. This feature allows the user to perform the following operations using the Command Line Interface (CLI):
  - View the list of backups and the status of the last backup.
  - Schedule time for backups.
  - Change the remote location and credentials to store a backup file (CIFS mount).
- This release adds support to restore the management platform from a backup. This feature allows the user to perform the following operations using the CLI:
  - Specify the remote location where the backup file is stored (CIFS mount).
- This release adds support to convert a Vertiv™ Avocent® UMIQ KVM device to a Vertiv™ Avocent® IPIQ IP KVM device. This feature allows the user to perform the following operations using the CLI:
  - View the list of Vertiv™ Avocent® UMIQ KVM devices including MAC address and port information.
  - Upgrade the Vertiv™ Avocent® UMIQ device firmware to convert it to an Vertiv™ Avocent® IPIQ IP KVM device.
  - View the status of the Vertiv™ Avocent® UMIQ device firmware upgrade operation.
- This release adds support to manage discovery requests. This feature allows the user to perform the following operations:
  - Create and run discovery requests.
  - View details of all discovery requests in the new Discovery View.
  - Track progress status of discovery requests in the Discovery View upon refreshing the page or moving from another page to the Discovery View. This includes the discovery starting and completion time, discover status, and the list of device IP addresses that have been discovered.
  - Search and sort discovery request information in the Discovery View.
  - Update configuration for discovery requests from the Discovery View.
- This release adds the ability to configure a NAT rule with a target port and external port set to "any" when mapping the private IP address of the target to a public IP address on the network. The target is connected to a port on the Vertiv™ Avocent® RM1048P Rack Manager.

## Resolved Issues

- General issues resolved:
  - Fixed issue where filtering devices by "Power Outlet" is not displaying correctly in the Appliance View for Vertiv™ Geist™ rPDUs that are managed by Vertiv™ Avocent® ACS800 and/or ACS8000 advanced console system appliances.
  - Fixed issue where filtering devices by "Power Outlet" across multiple pages in the Appliance View is not displaying the correct device count on the last page.
  - Fixed issue where the Device Locator widget in the Dashboard is not showing the top-level devices in the organization hierarchy for a selected device in the Organizations widget.
  - Fixed issue where the Appliance View and Target List do not display the firmware version for Vertiv™ Avocent® Geist™ rPDUs that are discovered using SNMP.
  - Fixed issue where a resync operation does not bring back a previously deleted Vertiv™ Avocent® ACS800/ACS8000 advanced console system appliance or a Vertiv™ Geist™ rPDU on the Appliance View.
  - Fixed issue where the icon that represents the maintenance mode for a Vertiv™ Geist™ rPDU or Vertiv™ Rack UPS device in the Appliance View does not get updated correctly after the user enables the Maintenance Mode for the device.
  - Fixed issue where the user is unable to launch the device web page from the Target List for Vertiv™ Geist™ rPDU and Vertiv™ Rack UPS devices that are connected to the Vertiv™ Avocent® RM1048P Rack Manager and discovered via SNMP.
  - Fixed issue where an attempt to upgrade an OpenBMC device is not successful.

- Fixed issue where continuous invalid log in attempts using the RESTful API generated an excessive number of events which consumed disk space on the Vertiv™ Avocent® MP1000 Management Platform appliance.
- Fixed issue where the Edit (pencil) icon is missing for the default user group on the Users panel.
- Fixed issue where the details for a Vertiv™ Geist™ PDU device show an incorrect value for the PDU accumulated energy setting on the Appliance View properties panel.
- Fixed issue where the PDU Info tab is empty on the Appliance View properties panel for a Vertiv™ Geist™ PDU device that is discovered using the SNMP protocol.
- Fixed issue where the Search and Filter edit box contains Chinese characters when the Device List page is refreshed several times (CAS-69076-M5W7K7).
- Fixed issue where a search for a very large number of LDAP entries generates an error message indicating the size limit has been exceeded (CAS-61819-L7X2S8).
- Fixed issue where the resync operation is not working correctly for a Vertiv™ Geist™ PDU device that is attached to a Vertiv™ Avocent® ACS800 and/or ACS8000 advanced console appliance (CAS-58436-G3M5G5).
- Fixed issue where an attempt to unmap an external authentication group from an internal user group generates an error message (CAS-69078-R7Y0D8).
- Fixed issue where the firmware version is not being updated on the Appliance View or Target List view after a resync operation has been performed on a Vertiv™ Geist™ PDU device (CAS-58432-D5N0V8).
- Fixed issue where the process to discover devices on the network by IP range runs continuously on the background and sometimes it gets stuck (CAS-66795-L6J0H5).
- Fixed issue where the status of a Vertiv™ Avocent® DSView™ server on the Appliance View shows as not responding a few minutes after the server has been added to the Appliance View or Target List view (CAS-66436-P9Z8L5).
- Fixed issue where clicking the SP name link (hyperlink) on the Targets List view produces error messages.
- Fixed issue where the firmware updates for the managed Vertiv™ Avocent® RM1048P Rack Manager and Vertiv™ Avocent® IPUHD 4K IP KVM fail with an error message via the new managed device drill-down page.
- Fixed issue where the changed time (from the CLI) is not maintained through a reset. BIOS overrides time and must be set via BIOS.
- Fixed issue where the asset tag for a Vertiv™ Avocent® RM1048P Rack Manager cannot be changed using the web UI; however, it can be changed using the CLI.
- Organization issues resolved:
  - Fixed issue where devices moved from the Ungrouped Devices section of the Organization Editor to a specific organization are still being left in the Ungrouped Devices section.
  - Fixed issue where the Organization Editor is missing the checkboxes that allow organizations to be moved into other organizations.
  - Fixed issue where the Dashboard link appears incorrectly when a Vertiv™ Geist™ PDU or Vertiv™ Rack UPS device is selected on the Organizations page.
  - Fixed issue where a user without the proper permissions is able to create a new organization (CAS-68543-G1S4L9).
- Virtual Appliance issues resolved:
  - Fixed issue where an attempt to unmap an external authentication group from an internal user group is not successful.
  - Fixed issue where selecting a target to merge with a power outlet from the Appliance View or Target List generates an error message.
- Serial issues resolved (serial appliances/ports/sessions):
  - Fixed issue where the "RxON Software" flow control option is missing on the Physical Settings page of a Vertiv™ Avocent® ACS800 and/or ACS8000 advanced console system appliance connected to the Vertiv™ Avocent® MP1000 Management Platform appliance.
- Configuration issues resolved:
  - Fixed issue where an attempt to map several groups from different external authentication providers to an internal user group generates an error message.
  - Fixed issue where disabling the API HTTP Access option on the Security Profile configuration page of a Vertiv™ Avocent® ACS800 and/or ACS8000 advanced console system appliance connected to the Vertiv™ Avocent® MP1000 Management Platform appliance does not take effect.
  - Fixed issue where the Lockout Policy system settings are not being saved (CAS-67485-X2S0G4).

## 4. Device Support Information

The following devices may be managed by the Vertiv™ Avocent® MP1000 Management Platform:

- Vertiv™ Avocent® RM1048P Rack Manager
- Vertiv™ Avocent® IPUHD 4K IP KVM device
- Vertiv™ Avocent® IPIQ IP KVM device
- Vertiv™ Avocent® ACS800 and/or ACS8000 advanced console systems
- Vertiv™ Avocent® 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® IPIQ IP KVM device
  **NOTE: For this functionality, contact your Vertiv Technical Support representative.**

## 5. Language Support Information

The Vertiv™ Avocent® MP1000 Management Platform 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 | 115+ | 35+ |
| Chrome | 115+ | 40+ |
| Safari | 16+ | 12+ |

## 7. Viewer Support and Version Information

### Supported Viewers

| VIEWER | VERSION |
|--------|---------|
| KVM Viewer | 4.21.1 |
| Serial Viewer | 4.7.1 |
| Virtual Machine (VM) Viewer | 3.9.1 |

## 8. Dashboard Support Information

| ITEM | VERSION |
|------|---------|
| Dashboard | 1.26.1 |

# 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. Vertiv™ Avocent® DSView™ Management Software Versions

| SOFTWARE VERSION | SERVICE PACK | RELEASE DATE |
| --- | --- | --- |
| 4.5.0 | SP15 | July 15, 2022 |
| 4.5.0 | SP16 | December 9, 2022 |

**NOTE: Launching KVM and serial sessions to devices managed by the Vertiv™ Avocent® DSView™ software requires the activation of a Vertiv™ Avocent® DSView™ Software Development Edition license on the Vertiv™ Avocent® DSView™ software system.**

## 14. Known Issues and Limitations

This release contains the following known issues and limitations:

- Virtual Machine issues:
  - The status and power control for virtual machines running in Hyper-V are not displayed correctly in the Appliance View.
- 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).

- SPs that are connected to a Vertiv™ Avocent® RM1048P Rack Manager, then deleted from the Appliance View are not being rediscovered and added to the Appliance View after performing a resync operation.
- OpenBMC SPs do not support virtual media, sensor, power or thermal data.
- 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.
- The default system roles (User-Role, User-Administrator-Role and System-Maintainer-Role) do not include access to SPs.
- Session/Viewer issues:
  - 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 has completed 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.
  - After changing the time zone or enabling NTP on the Vertiv™ Avocent® IPUHD 4K IP KVM device, launching a KVM session to the device fails with a timeout error.
  - 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.
  - Launching a KVM or serial session to a Vertiv™ Avocent® DSView™ software device may open an additional browser tab (and leave it opened). You must manually close the additional browser tab after the session is closed.
  - KVM or serial sessions to Vertiv™ Avocent® DSView™ software devices connected to a Vertiv™ Avocent® MergePoint Unity™ KVM over IP and serial console switch or a Vertiv™ Avocent® Universal Management Gateway appliance are not listed in the Sessions list page.
  - 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:
  - The names for target devices that are managed by the Vertiv™ Avocent® DSView™ management software and displayed on the web UI are not being synchronized correctly.
  - When the list of email address on the Distribution List of the Notification Policy settings are separated by a carriage return, the save operation generates an error message. To resolve this issue, the list of email addresses should be separated by a semicolon and not a carriage return.
  - When the list of email address on the Add Notification Policy panel are separated by a carriage return, the add operation generates an error message. To resolve this issue, the list of email addresses should be separated by a semicolon and not a carriage return.
  - 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.
  - The web UI displays virtual machines managed by VMWare ESXi and vCenter 6.5.x, 6.7.x and 7.x versions only.
  - Unable to change a full name in the User Preferences view.
  - On the Organizations page, the Launch KVM Session icon may overlap with the Device Status icon. Zooming out on the browser page to properly align both icons resolves this issue.

- 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:
    - 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.
    - Unable to control outlet groups of a UPS device that is connected to the Vertiv™ Avocent® RM1048P Rack Manager.
    - A power loss of an SMB server might cause the Vertiv™ Avocent® MP1000 Management Platform to generate HTTP 500 errors when performing backup and restore operations. To resolve this issue, connect the power to the SMB server and reconfigure the SMB server credentials and path using the CLI.
    - 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.
    - When a serial USB adapter is not plugged into the micro-USB port of a Vertiv™ Avocent® IPUHD 4K IP KVM device, the Properties panel for the device displays *No Information* with no additional details.
    - 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 Vertiv™ Avocent® MP1000 Management Platform uses FTP as the only mechanism to upgrade a Vertiv™ Avocent® ACS 800/8000 advanced console system unit.
    - 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.
    - Unable to change settings for Vertiv™ Avocent® IPIQ IP KVM devices discovered through a Vertiv™ Avocent® RM1048P Rack Manager; settings may be updated using the Vertiv™ Avocent® RM1048P Rack Manager web UI.
    - 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.