

Vertiv™ Avocent® MP1000 Management Platform and Vertiv™ Avocent® MP1000VA Management Platform Virtual Appliance

Release Notes

VERSION R12 (3.96.1), JULY 2026

Release Notes Section Outline

- | | |
|---|--|
| 1. Notes for Updating the Hardware Appliance | 12. Rack UPS Support Information |
| 2. Notes for Updating the Virtual Appliance | 13. Vertiv™ Avocent® MergePoint Unity™ Support Information |
| 3. Update Instructions | 14. Vertiv™ Avocent® MergePoint Unity™ 2 Support Information |
| 4. Appliance Firmware Version Information | 15. Cascaded Device Support Information |
| 5. Features and Enhancements | 16. Port Usage Information |
| 6. Device Support Information | 17. Vertiv™ Avocent® DSView™ Management Software Versions |
| 7. Language Support Information | 18. RESTful API |
| 8. Client Browser Support Information | 19. Vertiv™ Avocent® DSView™ Solution Related Products |
| 9. Viewer Support and Version Information | 20. Known Issues and Limitations |
| 10. Server Processor (SP) Support Information | |
| 11. Power Distribution Unit (PDU) Support Information | |

1. Notes for Updating the Hardware Appliance

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

NOTE: For additional information on this process, refer to the Vertiv™ Avocent® MP1000 Management Platform Quick Installation Guide, which is provided with the management platform and also available on the [Vertiv™ Avocent® MP1000 Management Platform product page](#) under the *Documents & Downloads* tab.

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

2. Notes for Updating the Virtual Appliance

This new release supports upgrading the Vertiv™ Avocent® MP1000 Management Platform Virtual Appliance in both VMware and Hyper-V virtual environments, assuming the virtual appliance is already deployed on the system. If instructions are needed to prepare for and deploy the virtual appliance, or if any additional information related to the initial launch of the virtual appliance is needed, refer to the Vertiv™ Avocent® MP1000VA Installation/Deployment Guide, which is available on the [Vertiv™ Avocent® MP1000 Management Platform Virtual Appliance](#) product page under the *Documents & Downloads* tab. After deploying the virtual appliance and are ready to upgrade to the latest version, proceed to the next section of these release notes.

IMPORTANT NOTE: The initial deployment of the virtual appliance in a VMware virtual environment is done with an Open Virtual Appliance (OVA) file (.ova). The initial deployment of the virtual appliance in a Hyper-V virtual environment is done with a Virtual Hard Disk (VHDX) file (.vhdx). Ensure the file is not used to update the virtual appliance; the upgrade file is an img.xz file. Additionally, the upgrade files for the virtual appliance are NOT interchangeable with those for the hardware appliance. Before

upgrading, verify that files specifically designed for the Vertiv™ Avocent® MP1000VA Management Platform Virtual Appliance are being used.

3. Update Instructions

IMPORTANT NOTE: The Vertiv™ Avocent® MP1000 Management Platform and Vertiv™ Avocent® MP1000VA Management Platform Virtual Appliance (VMware and Hyper-V) must be on firmware version 3.80.3 minimum before upgrading to version R12 (3.96.1). Upgrading directly from a version older than 3.80.3 to version R12 (3.96.1) is not supported and will fail. If your current firmware version is older than 3.80.3, you must first upgrade to version 3.80.3 and then upgrade to version R12 (3.96.1). Once the MP1000 or MP1000VA is successfully upgraded to version R12 (3.96.1), proceed to upgrade the RM1048P Rack Manager and all downstream managed devices per the upgrade order specified below.

NOTE: For virtual appliance deployments, it is recommended to take a VMware snapshot or Hyper-V checkpoint of the current state of the virtual machine before proceeding with the upgrade to provide an additional recovery option in the event the upgrade does not complete successfully.

NOTE: Starting with release R12 (3.96.1) and all subsequent releases, the recommended order of equipment upgrades has changed as follows:

1. Vertiv™ Avocent® MP1000 Management Platform (or MP1000VA Virtual Appliance)
2. Vertiv™ Avocent® RM1048P Rack Manager
3. Vertiv™ Avocent® ACS800/8000 advanced console systems, Vertiv™ Avocent® MergePoint Unity™ switches, Vertiv™ Avocent® MergePoint Unity™ 2 switches, and Vertiv™ Avocent® AutoView™ switches
4. Vertiv™ Avocent® IPIQ IP KVM, Vertiv™ Avocent® IPSL IP serial, and Vertiv™ Avocent® IPUHD 4K IP KVM devices
5. Vertiv™ PowerIT rPDUs, Vertiv™ Geist™ rPDUs, and Vertiv™ Liebert® rack UPS devices

IMPORTANT NOTE: 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 19](#) (Vertiv™ Avocent® DSView™ Solution Related Products) of these release notes.

IMPORTANT NOTE (HA Cluster Mode only): Before upgrading the Primary node, set the HA cluster Standby node(s) to Maintenance Mode to prevent database replication during the upgrade and avoid disruption. It is strongly recommended to have both local backups and/or remote SMB backups on the NTFS folder in place as part of a disaster recovery plan. For further details on High Availability, refer to the [Vertiv™ Avocent® MP1000 High Availability Technical Note](#).

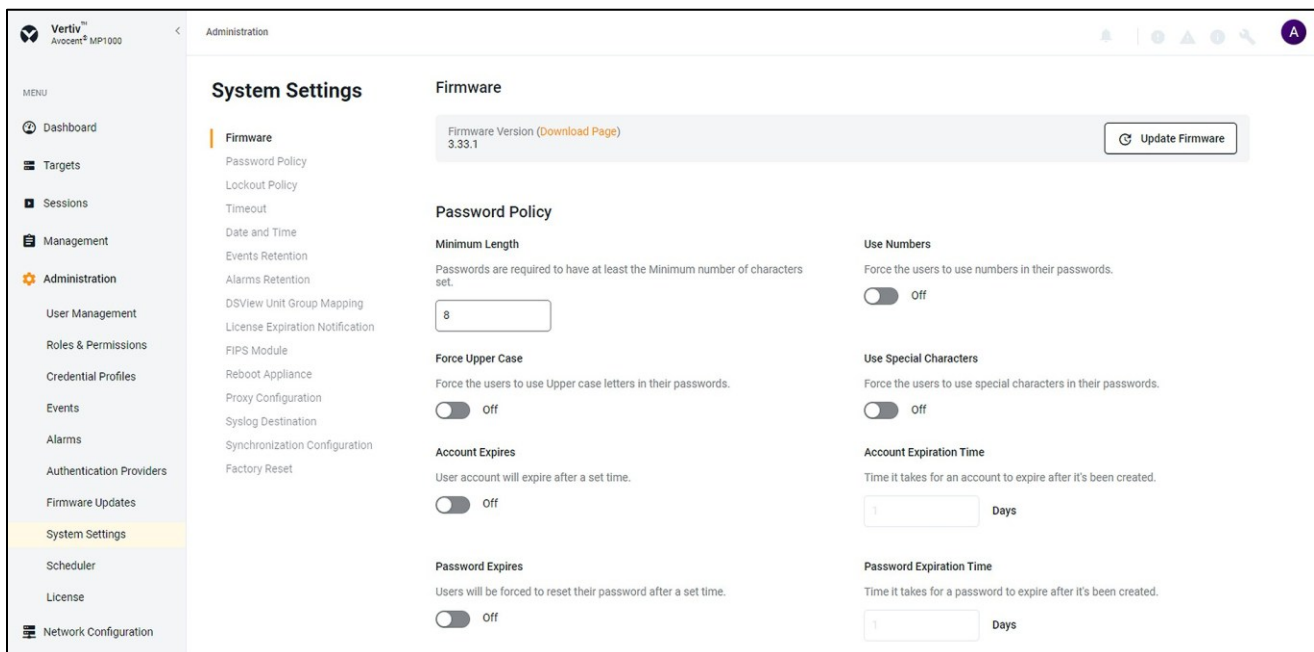
Before upgrading the firmware of a Vertiv™ Avocent® RM1048P Rack Manager appliance that is managed by the Vertiv™ Avocent® MP1000 Management Platform or Vertiv™ Avocent® MP1000VA Management Platform Virtual Appliance, follow the appropriate procedure based on your deployment scenario:

- a) Standalone Mode (MP1000 Management Platform or MP1000VA Management Platform Virtual Appliance NOT part of a cluster): Upgrade the MP1000 Management Platform or MP1000VA Management Platform Virtual Appliance to firmware version R12 (3.96.1) or newer first, then upgrade the RM1048P Rack Manager firmware using the management platform web UI, followed by all remaining downstream managed devices per the upgrade order specified above.
- b) HA Cluster Mode: Once all cluster nodes are on firmware version R12 (3.96.1), place the Standby node(s) in Maintenance Mode, upgrade the RM1048P Rack Manager firmware from the Primary node, then return the Standby node(s) to resume database replication. After the RM1048P Rack Manager upgrade is complete, proceed to upgrade all remaining downstream managed devices per the upgrade order specified above. For further details on HA cluster upgrade procedures, refer to the [Vertiv™ Avocent® MP1000 High Availability Technical Note](#).

NOTE: After upgrading the RM1048P Rack Manager firmware, it is recommended to perform a Resync operation on the rack manager from the management platform web UI to ensure the updated firmware version is displayed correctly in the Appliance View and Targets List pages.

To update the management platform appliance firmware:

1. Visit the management platform firmware download page:
[Vertiv™ Avocent® Management Platform Software Download](#)
2. Download the latest firmware and save it to the local computer, FTP, HTTP, or TFTP server.
NOTE: For information on the latest firmware version, refer to [d](#) (Appliance Firmware Version Information).
3. In a web browser, enter **https://<appliance.IP>** using the IP address for eno1 configured from the management platform console menu.
4. Enter the 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*.

NOTE: After the firmware has been successfully updated, it is strongly advised to clear the browser cache.

NOTE: If the time on the Vertiv™ Avocent® RM1048P Rack Manager and the 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.

4. Appliance Firmware Version Information

APPLIANCE/PRODUCT	VERSION	FILENAME
Vertiv™ Avocent® MP1000 Management Platform	R12 (3.96.1)	obsidian-3.96.1-update.fl
Vertiv™ Avocent® MP1000VA Management Platform Virtual Appliance	R12 (3.96.1)	AvocentADXVirtualAppliance-3.96.1-update.fl

5. Features and Enhancements

The following features and enhancements are available with this release of the Vertiv™ Avocent® MP1000 Management Platform and Vertiv™ Avocent® MP1000VA Management Platform Virtual Appliance:

- Adds the ability to view and configure additional settings for the Vertiv™ Avocent® ACS800 and Vertiv™ Avocent® ACS8000 advanced console systems from the management platform web UI.
- 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
- Enhances the IP Pools feature as follows:
 - Allows a user to centrally manage IP Pools from the management platform web UI, instead of managing IP pools through each Vertiv™ Avocent® RM1048P Rack Manager.
 - Allows a user to assign an external IP address to a target device in the Appliance View or Targets List page.
- 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.
- Adds the ability to apply configuration settings to multiple Vertiv™ Avocent® ACS800 and Vertiv™ Avocent® ACS8000 advanced console systems simultaneously from the management platform web UI as follows:
 - Supports configuration of serial port settings, authentication servers, syslog and NTP server settings, security profiles, event configurations, appliance authentication, security profiles, and local user passwords.
 - Supports configuration of other applicable settings available for advanced console systems.
 - Provides success/failure reporting with retry options for failed operations.

- Adds the ability to backup and restore configuration files for individual Vertiv™ Avocent® ACS800 and Vertiv™ Avocent® ACS8000 advanced console systems from the management platform web UI as follows:
 - Allows users to save ACS configuration files to the management platform, with each backup linked to its source device.
 - Allows users to restore ACS configurations by selecting from device-specific backup files stored on the management platform.
- Adds the ability to centrally monitor and manage events from Vertiv™ Avocent® ACS800 and Vertiv™ Avocent® ACS8000 advanced console systems from the management platform web UI as follows:
 - Allows users to configure advanced console systems to forward event logs to the management platform.
 - Supports configuration of event forwarding protocol.
 - Allows users to view, search, and filter events for individual advanced console systems from the management platform web UI.
- Adds the ability to apply configuration templates to Vertiv™ Avocent® ACS800 and Vertiv™ Avocent® ACS8000 advanced console systems from the management platform web UI as follows:
 - Allows users to select and apply saved configuration templates to one or more advanced console systems on demand.
 - Allows users to automatically apply configuration templates during device enrollment and discovery processes.
 - Provides success and failure reporting of applied configuration templates.
- Adds the ability to upload and manage firmware files for Vertiv™ Avocent® ACS800 and Vertiv™ Avocent® ACS8000 advanced console systems from the management platform web UI as follows:
 - Allows users to upload ACS firmware files to the management platform for secure storage and version tracking.
 - Maintains the current and one previous firmware file with user selection capability.
 - Allows users to select uploaded firmware files when performing firmware updates on one or more advanced console systems.
- Adds the ability to perform bulk firmware updates on multiple Vertiv™ Avocent® RM1048P Rack Manager appliances simultaneously from the management platform web UI, with support for updating up to 10 devices at once.
- Adds a confirmation prompt when removing a Vertiv™ Avocent® RM1048P Rack Manager from the management platform web UI that informs users of data loss and impacts, including details about the reset process and affected configurations, to prevent accidental data removal.
- Enhances the IP Pool functionality to automatically update and display the renewed lease time in the Appliance View without requiring a manual page refresh.

Resolved Issues

- General issues resolved:
 - Fixed issue where high CPU utilization is detected on a management platform virtual appliance with many target devices (CA-0001103865).
 - 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 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 remote connections to Amazon Web Services (AWS) are being observed during an installation of a management platform virtual appliance (CA-0001109078).

- 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 management of a Vertiv™ Avocent® MergePoint Unity™ switch by multiple management platform hardware and virtual appliances is not supported.
- 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 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 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 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 messaging service may fail to start after upgrading to firmware version 3.88.1, preventing users from logging into the web UI.
- 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 an excessive number of login events are logged on Service Processors managed by the management platform within a 30-day period.
- Fixed issue where the IP Pool Retrieved IP Address state shown in the Properties side panel's three-dot menu does not match the state shown in the target device row's three-dot menu for Vertiv™ Avocent® IPUHD 4K IP KVM devices managed through a Vertiv™ Avocent® RM1048P Rack Manager.
- Security vulnerabilities have been resolved (CA-0001100793).
- Authentication Provider issues resolved:
 - Fixed issue where users are unable to create or configure an Azure EntraID SSO authentication provider on the management platform, and existing SSO login attempts fail with error messages (CA-0001171591).
 - Fixed issue where a Single Sign-On (SSO) authentication may fail with the error message "Single Sign-On (SSO) login failed. Please retry again." after the OIDC provider rotates their JSON Web Keys (JWKs) - (CA-0001190660).
 - 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 multiple "Local Users" rows appear under Authentication Providers in the web UI, preventing users from logging in via Active Directory and causing the primary node in an HA cluster to enter Maintenance mode (CA-0001109617).
 - 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).

- Firmware Upgrade issues resolved:
 - Fixed issue where a firmware update initiated using the SCP protocol fails when the FTP server configuration is disabled on the device (CA-0001215691).
 - Fixed issue where firmware upgrades for a Vertiv™ Avocent® IPUHD 4K IP KVM and Vertiv™ Avocent® IPSL IP serial devices that are managed by a Vertiv™ Avocent® RM1048P Rack Manager fail when using the File Upload method.
 - Fixed issue where firmware upgrades for a Vertiv™ Avocent® IPUHD 4K IP KVM or Vertiv™ Avocent® IPIQ IP KVM device fail when using the TFTP file transfer method.
 - Fixed issue where the firmware version on the Appliance View page is not updated correctly after performing an upgrade of the Vertiv™ Avocent® MergePoint Unity™ switch.
- High Availability issues resolved:
 - Fixed issue where an unexpected HA failover occurred during scheduled backup operations, which by default appear at 00:00 UTC (CA-0001047886 and CA-0001109800).
 - Fixed issue where a primary node stays in Maintenance mode and prevents the primary node from switching to Standby or Primary mode during an HA failover operation (CA-0001077669, CA-0001082261, and CA-0001077669).
 - Fixed issue where the cluster reports Standalone mode instead of Primary/Standby mode on startup. This prevented KVM sessions from being established (CA-0001045560).
 - Fixed issue where firmware upgrades on HA cluster nodes resulted in cluster failures. The system now enforces guardrails that only allow firmware upgrades when Primary and Standby nodes are in the correct mode (such as Primary, Standby, or Maintenance).
 - Fixed issue where custom certificates and their signing authorities are not correctly recognized during cluster formation, which prevented clusters from being formed and caused system downtime. The system now verifies certificate acceptance and adds signing authorities to the allowlist during the certificate update process (CA-0001100185, CA-0001082261, CA-0001077689, and CA-0001086148).
 - Fixed issue where the SSL certificate cannot be updated from the web UI of the Standby node in an HA cluster. The Certificate feature is unavailable or disabled when creating or updating on the Standby node's web UI. (CA-0001100185).
- Licensing issues resolved:
 - Fixed issue where the license service may go offline every few days, preventing users from launching KVM sessions (CA-0001056587).
- 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:
 - On the Mass Configuration page, the Filter and Search functionalities do not work in combination. When a filter is applied and a specific configuration name is entered in the Search field, the system ignores the search input and displays all records that match only the filter criteria, rather than narrowing the results based on both the filter and search conditions. To work around this issue, use either the Search or the Filter functionality independently to locate the desired Mass Configuration records.
 - When managing a Vertiv™ Avocent® ACS800/8000 advanced console system from the management platform web UI, navigating to the *Events and Logs - Event List* page and selecting an event, followed by clicking on the event link, causes the Events page to display incorrectly. To work around this issue, navigate away from the Events page and return to it to restore the page view, or access the event details directly from the Vertiv™ Avocent® ACS800/8000 advanced console system web UI.
 - When applying a configuration template during the discovery of a Vertiv™ Avocent® ACS800/8000 advanced console system on the Discoveries page, the configuration template may fail to be fully applied to the device. The Configuration Template Status column on the Discoveries page may incorrectly display "Success" even though the configuration template was only partially applied or not applied at all to the advanced console system. To resolve this issue, manually apply the configuration template to the ACS800/8000 advanced console system after discovery completes using the mass configuration feature on the Targets List or Appliance View page.

- When events are configured to "Send Message to DSView Solution" on the Events and Logs page, the event message information displayed on the Events page is incomplete or not present for sessions launched to a Vertiv™ Avocent® ACS800/8000 advanced console system. To view complete event and session information, access the event logs directly from the ACS800/8000 advanced console system web UI.
- Fixed issue where firmware update file path validation was inconsistent across FTP, SFTP, and SCP protocols when updating a Vertiv™ Avocent® ACS800/8000 advanced console system. The File Location field now provides consistent text with file path examples for each protocol (CA-0001175378).
- Fixed issue where the Network Configuration section does not display in the Properties panel for a Vertiv™ PowerIT rPDU device after it retrieves an external IP address from an IP Pool. Although the system correctly allocates the external IP address, the corresponding network configuration details were not shown when viewing the device from the Appliance View.
- Fixed issue where Vertiv™ Avocent® IPIQ IP KVM devices connected to a managed Vertiv™ Avocent® RM1048P Rack Manager are visible in the rack manager's CLI under attached devices but do not appear in the Appliance View or Targets List on the management platform web UI (CA-0001158555).
- 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 Vertiv™ Avocent® IPIQ IP KVM devices connected to a managed Vertiv™ Avocent® RM1048P Rack Manager incorrectly display "Port 99" instead of the actual port number in the Appliance View and Targets List on the management platform web UI (CA-0001158563 and CA-0001157880).
- Fixed issue where upgrading a Vertiv™ Avocent® MergePoint Unity™ 2 KVM over IP and serial console switch via the management platform virtual appliance causes an error message to appear on the Firmware Updates page, even though the firmware installation completes successfully.
- Fixed issue where an error occurs when attempting to save a custom timezone configuration on the *System - Timezone* page for a Vertiv™ Avocent® ACS800/8000 advanced console system managed by the management platform.
- Fixed issue where multiple validation error messages stating "Server1 Related fields are required" continue to display on the *System - Date and Time* page for a Vertiv™ Avocent® ACS800/8000 advanced console system managed by the management platform, even after successfully entering all required Server1 fields and saving the configuration.
- 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 a Vertiv™ Avocent® RM1048P Rack Manager are missing or displayed as duplicates in the Appliance View and Targets List pages 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 Vertiv™ Avocent® RM1048P 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.
- Fixed issue where a Vertiv™ PowerIT Monitored or Metered-only rPDU 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 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 Vertiv™ Avocent® RM1048P Rack Manager (CA-0001089100 and CA-0001088135).
- Fixed issue where UPS devices connected to a Vertiv™ Avocent® ACS800/8000 advanced console system are duplicated in the Targets - Appliance View whenever a resync operation is performed on the advanced console system (CA-0001070117).
- 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 Vertiv™ Avocent® RM1048P Rack Manager's firmware (CA-0001082261).

6. Device Support Information

The Vertiv™ Avocent® MP1000 Management Platform may manage the following devices:

- Vertiv™ Avocent® RM1048P Rack Manager
- Vertiv™ Avocent® IPUHD 4K IP KVM device
- Vertiv™ Avocent® IPIQ IP KVM device
- Vertiv™ Avocent® ACS800 and/or Vertiv™ Avocent® ACS8000 advanced console systems
- Vertiv™ Avocent® IPSL IP serial device
- Vertiv™ PowerIT rPDUs
- Vertiv™ Liebert® rack UPS devices
- Vertiv™ Avocent® MergePoint Unity™ KVM over IP and serial console switch (firmware version 2.14.0 or higher)
- Vertiv™ Avocent® MPUIQ-VMCHS-G01, MPUIQ-VMCHD, MPUIQ-VMCDV, MPUIQ-VMCDP, and MPUIQ-SRL modules
- Vertiv™ Avocent® MergePoint Unity™ 2 KVM over IP and serial console switch
- Vertiv™ Avocent® AutoView™ switch (cascaded from a Vertiv™ Avocent® MergePoint Unity™ switch) – firmware version 2.10.0 or higher
- 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.

7. Language Support Information

The Vertiv™ Avocent® MP1000 Management Platform software currently supports English and Simplified Chinese.

8. 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+

BROWSER	PREFERRED VERSION	SUPPORTED VERSIONS
Chrome	115+	40+
Safari	16+	12+

9. Viewer Support and Version Information

Supported Viewers

VIEWER	VERSION
KVM Viewer	4.55.1
Serial Viewer	4.29.1
Virtual Machine (VM) Viewer	3.22.1

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

10. 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

SERVICE PROCESSOR	FIRMWARE VERSION	PROTOCOLS
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

11. 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

12. Rack UPS Support Information

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

13. Vertiv™ Avocent® MergePoint Unity™ Support Information

SUPPORTED VERTIV™ AVOCENT® MERGEPOINT UNITY™ SWITCH MODELS

MPU104E

MPU108E

MPU108EDAC

MPU1016

MPU1016DAC

MPU2016

MPU2016DAC

MPU2032

MPU2032DAC

MPU4032

MPU4032DAC

MPU8032

MPU8032DAC

DMPU108E

DMPU1016

DMPU2032

14. Vertiv™ Avocent® MergePoint Unity™ 2 Support Information

SUPPORTED VERTIV™ AVOCENT® MERGEPOINT UNITY™ 2 SWITCH MODELS

MPU2-108DAC-400

MPU2-2016DAC-400

MPU2-2032DAC-400

MPU2-4032DAC-400

15. Cascaded Device Support Information

The following table lists the Vertiv™ Avocent® AutoView™ switch models that can be cascaded via the Vertiv™ Avocent® MergePoint Unity™ switch.

SUPPORTED VERTIV™ AVOCENT® AUTOVIEW™ SWITCH MODELS
AV2108
AV2216
AV3108
AV3216

16. Port Usage Information

PORT	TYPE	PORT TRAFFIC	SOURCE	DESTINATION	SERVICE	REQUIRED	NOTES
20	TCP	OUT	MP1000	ACS 800/8000	FTP - File Transfer Protocol	Required	FTP data channel for file transfers. Use in conjunction with port 21 for firmware updates and file transfers to/from devices.
21	TCP	IN	Corporate Network	MP1000 / Target Devices	FTP - File Transfer Protocol	Required	Use for firmware updates, configuration backups, and file transfers. Inbound for users uploading to MP1000; outbound for MP1000 connecting to device FTP servers.
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.

PORT	TYPE	PORT TRAFFIC	SOURCE	DESTINATION	SERVICE	REQUIRED	NOTES
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.
3871	TCP	OUT	MP1000	ACS 800/8000	Discovery - Device Detection	Required	Automatic device discovery protocol for detecting and registering new devices on the network. Also for TLS encrypted console sessions to Vertiv™ Avocent® ACS800/8000 advanced console systems.
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.
4122	TCP	IN	MP1000	Target Devices	SSH Passthrough	Required	SSH passthrough connections to managed devices through the MP1000 console system (Vertiv™ Avocent® ACS800/8000 advanced console system) for serial device 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

PORT	TYPE	PORT TRAFFIC	SOURCE	DESTINATION	SERVICE	REQUIRED	NOTES
							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 onsole access.
48048	TCP	OUT	MP1000	ACS 800/8000	REST API - Device Management	Required	REST API communications for device configuration, monitoring, and management operations with Vertiv™ Avocent® ACS800/8000 advanced console systems.

17. 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
4.5.0	SP17	June 6, 2024
4.5.0	SP18	March 18, 2025
4.5.0	SP18.1	June 13, 2025
4.5.0	SP18.2	September 23, 2025

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

18. 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® MP1000 Management Platform. 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.

19. Vertiv™ Avocent® DSView™ Solution Related Products

PRODUCT	DOWNLOAD/PRODUCT PAGE
Vertiv™ Avocent® RM1048P Rack Manager, including RESTful API	https://www.vertiv.com/en-us/support/software-download/software/vertiv-avocent-rm1048-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/
Vertiv™ Avocent® ACS800/8000 advanced console systems	https://www.vertiv.com/en-us/support/software-download/it-management/avocent-ac-8000-advanced-control-systems-software-downloads/
Vertiv™ Avocent® MergePoint Unity™ KVM over IP and serial console switch	https://www.vertiv.com/en-us/support/software-download/it-management/avocent-mergepoint-unity-switches-software-downloads/
Vertiv™ Avocent® MergePoint Unity™ 2 KVM over IP and serial console switch	https://www.vertiv.com/en-us/products-catalog/monitoring-control-and-management/ip-kvm/vertiv-avocentmergepointunity-2-kvm-over-ip-switches/
Vertiv™ Avocent® AutoView™ 3108/3216 switch	https://www.vertiv.com/en-us/support/software-download/it-management/avocentautoview-3108-3216-analog-kvm-switches-software-downloads/
Vertiv™ Avocent® AutoView™ 2108/2216 switch	https://www.vertiv.com/en-us/support/software-download/it-management/avocentautoview-21082216-analog-kvm-switches--software-downloads/
Vertiv™ Avocent® DSView™ management software	https://www.vertiv.com/en-us/support/software-download/software/avocent-dsview-software-downloads/

20. Known Issues and Limitations

This release contains the following known issues and limitations:

- **Firmware Update Issues:**
 - A bulk firmware update operation of multiple Vertiv™ Avocent® RM1048P Rack Managers that are managed by the management platform may result in a timeout error when upgrading over a high-latency or low-bandwidth network. To resolve this issue, perform firmware upgrades on fewer Vertiv™ Avocent® RM1048P Rack Managers at a time to reduce concurrent network traffic during the bulk upgrade operation. If the issue persists, upgrade the rack managers individually using the file upload method.
 - Upgrading firmware on a Vertiv™ Avocent® IPUHD 4K IP KVM device occasionally fails with the error message "Failure: retry limit reached for IPXX FW update: error from IPIQ management service" or "Failure: retry limit reached for IPXX FW update." To resolve this issue, perform a "Reset Preserve network and User" operation from the three-dot menu of the 4K IP KVM device and attempt the firmware upgrade again. If the firmware upgrade fails initially, try the upgrade operation again without performing a reset.
 - **[BEFORE UPGRADING rPDU DEVICE]** When a Vertiv™ PowerIT 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.
 - 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.
 - Unable to update the firmware of a Vertiv™ Avocent® MergePoint Unity™ switch using the FTP or TFTP methods from the web UI. The only supported methods for updating firmware are the File Upload and HTTP methods.
- **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 the IP KVM devices that 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 may cause one or more firmware updates to fail. To resolve this issue, wait for at least five minutes after the Vertiv™ Avocent® IPUHD 4K IP KVM Device Bulk Firmware Update operation has failed, and then update the firmware for 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 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 Vertiv™ Avocent® RM1048P Rack Managers that are managed by the 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.

- 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 upgrade or conversion.
 3. Restore the Lease Time to the default value of 86400 seconds (24 hours).
 - When changing the bonding mode configuration from "Ports not bonded" to either "1st and 2nd ports bonded" or "1st fails over to 2nd port" on the *Administration - Network Configuration - Normal/Failover-Bonded Settings* page, the management platform may become unresponsive, preventing access to both the web UI and SSH (CLI) connections for several minutes or indefinitely. To resolve this issue, reboot system after modifying the bonding mode settings.
- 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:
 - **WARNING: Action Required Before February 2027**
R13 is a mandatory update, slated for later release. Once available, please install R13 as soon as possible to avoid service disruption. Appliance communication may become unstable after February 2027 if R13 is not installed.
 - After performing a factory reset on a Vertiv™ Avocent® RM1048 Rack Manager, the appliance reverts to an early release firmware (version 1.9.9) which contains expired certificates. The Vertiv™ Avocent® MP1000 Management Platform discovery in the web UI displays a false positive, indicating successful discovery when enrollment has not been completed. The RM1048P Rack Manager remains in standalone mode and cannot be managed or upgraded through the Vertiv™ Avocent® MP1000 Management Platform. To resolve this issue, upgrade the Vertiv™ Avocent® RM1048P Rack Manager as a standalone device to the latest firmware release (1.82.1) before enrolling it into the Vertiv™ Avocent® MP1000 Management Platform for management and firmware updates.
 - The Vertiv™ Avocent® RM1048P Rack Manager appliance certificate generation fails after configuration of the email, RID, and URI entries in the Subject Alternative Name (SAN) when the management platform manages the appliance.
 - 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 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 page requires a manual refresh of the page to view the updated contents of the certificate.
- High Availability issues:
 - After adding a Standby node to an HA cluster on the management platform virtual appliance, the node may be displayed with an incorrect role status on the High Availability page. The node may initially appear as "Standby" but then change to "Standalone" after a few minutes, or it may be added directly as "Standalone" and remain in that state. To resolve this issue, click on the three-dot menu at the end of the row for the affected node and select the "Set to Standby" option to manually correct the node's role status to "Standby".
 - SSH Passthrough functionality fails to work correctly on the Standby node after it becomes the Primary node during an HA failover. To resolve this issue, disable and then re-enable the SSH Passthrough feature from the web UI on the new Primary node after the failover is complete.

- After updating the management platform firmware, the role for the primary node of a cluster may be displayed as “Maintenance” on the High Availability page. To resolve this issue, follow these steps:
 1. Remove the primary node that is in Maintenance mode from the cluster.
 2. Restart the primary node using the CLI.
 3. Add the primary node to the cluster.
- Adding a node with a DHCP address to a cluster causes synchronization issues. To resolve this issue, configure the node to have the original static IP address when it was first added to the cluster, and then reboot the node on which the static IP address was changed.
- The role in the High Availability list view may display “Standalone” for a node that is added to a cluster as a Standby node. To resolve this issue, click on the three-button menu at the end of the row for the desired node and select the *Set to Standby* option. The role in the High Availability list will be updated to “Standby”.
- A cluster node transition between Primary and Standby may cause the status of target devices managed by the Vertiv™ Avocent® DSVIEW™ management software to show as non-responsive. To resolve this issue, remove the Vertiv™ Avocent® DSVIEW™ management software server from the management platform, then re-add it and wait for the status to update.
- After a cluster is set up or the cluster is deconstructed and then reconstructed, one of the cluster nodes (such as the management platform hardware appliance) may fail to be added to the cluster. To resolve this issue, log in to the management platform hardware appliance that failed to be added to the cluster using the web UI and verify that the High Availability feature is enabled. Then, add the node to the cluster.

If the Add Node operation fails or if unable to log into the management platform hardware appliance that failed to be added to the cluster using the web UI or CLI, perform a factory restore on the management platform hardware appliance using the following steps:

1. Access the console port of the management platform hardware appliance.
 2. Press **Ctrl-Alt-Del** keys to bring up the main menu.
 3. Select the **Maintenance** menu option.
 4. On the following menu, select the **Factory Restore** menu option.
- After a cluster is deconstructed and then reconstructed, one of the cluster nodes (such as the management platform virtual appliance for VMware) may fail to be added to the cluster. To resolve this issue, log in to the virtual appliance that failed to be added to the cluster using the web UI and verify that the High Availability feature is enabled, and then add the node to the cluster.

If the Add Node operation fails or if unable to log into the virtual appliance that failed to be added to the cluster using the web UI or CLI, perform the following steps if the management platform virtual appliance has been previously upgraded to a newer version:

1. Log in to the virtual machine and access the console port of the management platform virtual appliance.
2. Press **Ctrl-Alt-Del** keys to bring up the main menu.
3. Select the **Maintenance** menu option.
4. On the following menu, select the **Force boot previous Image** menu option.

-or-

If the virtual appliance has not been upgraded after installation, delete and reinstall the management platform virtual appliance.

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

- Adding a VM host on the Virtualization page displays an error message even though the VM host is successfully added to the management platform. To avoid this error message, add the VM host from the Appliance View page.

- **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.
- After initial discovery of a Service Processor (SP), the firmware version is not displayed in the Appliance View. To resolve this issue, perform a manual Resync operation on the Service Processor. After the Resync is completed, the firmware version will be displayed correctly in the Appliance View.
- 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).
 - SPs that are connected to a Vertiv™ Avocent® RM1048P Rack Manager, then deleted from the Appliance View page, are not being rediscovered and added to the Appliance View page 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.
 - Unable to add an HP iLO4 device that is configured with a 1-1 NAT rule in the Vertiv™ Avocent® RM1048P Rack Manager to the 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 managed by 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 error popup is not clickable, preventing the user from closing the window. The user must manually close the browser tab or window to exit the pop-up.
 - The Dashboard icon to view multiple viewer sessions is not visible for users assigned the built-in roles. To resolve this issue, create a custom target role and assign the following permissions:
 - View Devices
 - Configure Devices

- 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.
- Unable to start a serial session with a Vertiv™ Avocent® ACS800/8000 advanced console system that is managed through the Vertiv™ Avocent® DSVIEW™ management software on the management platform virtual appliance. To resolve this issue, manage the advanced console system directly through the management platform instead of through the Vertiv™ Avocent® DSVIEW™ management software.
- Launching simultaneous KVM sessions to target devices connected to a Vertiv™ Avocent® RM1048P Rack Manager in proxy mode may cause the web UI to display an error message.
- Sharing a serial session to a target device connected to a Vertiv™ Avocent® MPUIQ-SRL module that is attached to a Vertiv™ Avocent® MergePoint Unity™ switch fails.
- Unable to map Virtual Media files or folders 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 on 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 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 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™ management software device may open an additional browser tab (and leave it open). 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 do not show up correctly in the Dashboard.
- Web UI issues:
 - The Save button in the Mass Configuration page is enabled only when the SSH protocol is selected for serial port configuration. For all other protocol options (Telnet, Raw Mode, Telnet/SSH, Raw Mode Telnet/SSH, Telnet/Raw Mode SSH, and Telnet/SSH/Raw Mode), the Save button remains disabled, preventing the user from saving the configuration.
 - When the FTP server is disabled, and a user attempts to save the configuration of a Vertiv™ Avocent® ACS800/8000 advanced console system, two "File name" input fields are displayed under the Local File option.
 - When no Vertiv™ Avocent® ACS800/8000 advanced console system devices are available in the management platform, the system still allows users to navigate to the Administration - Mass Configuration page and proceed with creating a mass

configuration. Make sure that at least one Vertiv™ Avocent® ACS800/8000 advanced console system has been discovered and is available in the management platform prior to creating a mass configuration.

- When the management platform is configured to forward Vertiv™ Avocent® ACS800/8000 advanced console system syslog messages to the management platform Events page, the ACS device name displayed in the event may be incomplete or may be missing the IP address.
- 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 the FTP server is disabled, and a user attempts to save the configuration of a Vertiv™ Avocent® ACS800/8000 advanced console system, two duplicate "File name" input fields are displayed under the Local File option in the pop-up window. To resolve this issue, disregard the disabled "File name" field and use only the active "File name" field to enter or modify the file name when saving the device configuration.
- 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.
- When a serial port on a Vertiv™ Avocent® ACS800/8000 advanced console system is configured with a device type set to "ServerTech PRO2", the Save Configuration Template operation fails to create the configuration template file.
- When configuring the Vertiv™ Avocent® ACS800/8000 advanced console system pull configuration settings on the management platform web UI, the Save button becomes disabled when certain optional fields are left empty. As a workaround, ensure all configuration fields in the configuration screen are populated, even if they appear to be optional, before attempting to save the configuration. The Save button will become enabled once all required fields contain valid values.
- Unable to access the Properties panel for merged target devices or the legacy Vertiv™ Avocent® MergePoint Unity™ KVM over IP and serial console switches in the Appliance 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 for target devices connected to a Vertiv™ Avocent® MergePoint Unity™ 2 KVM over IP and serial console switch incorrectly displays a Network Configuration section that does not apply to these target devices.
- Duplicate ports and device types are displayed for multiple target devices in the Vertiv™ Avocent® RM1048P Rack Manager web interface after performing Auto Device Cleanup and Auto Discovery operations. To resolve this issue, use the CLI interface instead of the web UI to verify and manage port information and device types for the connected devices.
- At this time, the RSA format SSH keys are the only officially supported SSH key format for the management platform.
- 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.
- Unable to update a target device name from the Properties panel of a Vertiv™ Avocent® ACS800/8000 advanced console system. To resolve this issue, enable the "Push to Target Device" setting under the *Administration – System Settings – Synchronization Configuration* page.
- The socket power control options, device settings, and sensor information for Vertiv™ PowerIT rPDU devices (monitored or metered) connected to a Vertiv™ Avocent® ACS800/8000 advanced console system may not display correctly on the web UI.

- The power outlet status of a monitored or metered Vertiv™ PowerIT rPDU device is not updated correctly (such as Not Responding) on the web UI after successful discovery of the device.
- After a successful discovery of a Vertiv™ Avocent® MergePoint Unity™ KVM over IP and serial console switch device, the Device list displays the discovered device on the Unmanaged tab.
- After removing and manually rediscovering a Vertiv™ Avocent® IPIQ IP KVM device or a Vertiv™ Avocent® IPUHD 4K IP KVM device that is connected to a managed Vertiv™ Avocent® RM1048P Rack Manager using the management platform web UI, duplicate IP KVM device entries are displayed in the Appliance View. To resolve this issue, access the *Show Attached Devices* menu item in the CLI, identify the duplicate entry in the Appliance View by comparing IP addresses, and then remove the duplicate entry from the Appliance View.
- 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.
- 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. 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.
- Deleting a target device from an organization using the vertical ellipsis may occasionally not remove the device from the organization. To resolve this issue, select the target device from the organization and then click the Trash icon located above the table to remove it.
- General issues:
 - Deleting a Vertiv™ Avocent® RM1048P Rack Manager from an Organization group removes the rack manager from the management platform without resetting the management platform IP address in the rack manager appliance. This prevents the rack manager from being re-added to the management platform. To resolve this issue, log into the Vertiv™ Avocent® RM1048P Rack Manager CLI and remove the management platform IP address using the CLI menu options. After the management platform IP address has been removed via the CLI, the rack manager can be re-added to the management platform.
 - When ACS syslog messages are forwarded to MP1000 Events, the ACS device name is missing the IP address and displays incomplete information in the Events list.
 - Vertiv™ Avocent® IPIQ IP KVM IPIQ devices connected to a managed Vertiv™ Avocent® RM1048P Rack Manager may show in the rack manager's CLI under attached devices but do not appear in the management platform web UI under the Appliance View or Targets List page. This issue may occur when many Vertiv™ Avocent® Universal Management Gateway appliance UMIQ modules are auto converted to Vertiv™ Avocent® IPIQ IP KVM devices. To resolve this issue, restart the NATS bridge and IP-management services from the CLI. If the issue persists after a service restart, verify that the system time is synchronized between the management platform and the rack manager, as time synchronization issues can prevent proper device registration. Additionally, ensure that the firmware on the rack manager is compatible with the release on the management platform.
 - The Vertiv™ Avocent® MP1000 Management Platform Virtual Appliance does not allow a Fully Qualified Domain Name (FQDN) as the file location when performing a firmware upgrade of a Vertiv™ Avocent® ACS800/8000 advanced console system over SCP.

- The Restore Factory Defaults operation initiated through the CLI may fail on the Vertiv™ Avocent® MP1000 Management Platform and Vertiv™ Avocent® MP1000VA Management Platform Virtual Appliance. In some cases, selecting the Restore Factory option from the CLI may fail on the first attempt without displaying an error message. To resolve this issue, wait 10 minutes and then retry the Restore Factory operation. The second attempt should be completed successfully.

NOTE: This issue may occur when multiple Vertiv™ Avocent® Universal Management Gateway appliance UMIQ modules are auto converted to Vertiv™ Avocent® IPIQ IP KVM devices.

1. Restart the NATS bridge and IP-management services from the CLI.
 2. If the issue persists after service restarts, verify that the system times are synchronized between the management platform and the rack manager, as time synchronization issues can prevent proper device registration.
 3. Additionally, ensure that the firmware on the rack manager is compatible with the release on the management platform.
- 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.
 - After upgrading the management platform, the discovery of Vertiv™ PowerIT rPDU and Vertiv™ Liebert® rack UPS devices may fail. To resolve this issue, restart the "pd-management" service using the *Diagnostics - Restart Service* menu in the management platform CLI.
 - The Reset to Factory Defaults operation via CLI fails on the management platform virtual appliance. To resolve this issue, perform the factory reset operation using the management platform web UI interface instead of the CLI.
 - When attempting to set up a RADIUS authentication provider on the management platform, the operation fails with the error message "Unknown Error: Contact Administrator". To resolve this issue, restart the "radius-authentication" service using the *Diagnostics - Restart Service* menu in the management platform CLI and add the RADIUS authentication provider.
 - When a Vertiv™ PowerIT rPDU device is connected to a managed Vertiv™ Avocent® RM1048P Rack Manager, deleting the PDU device from the web UI and rebooting the rack manager prevents the PDU device from being rediscovered automatically.
 - SSH passthrough connection fails when an administrator user attempts to connect to a Vertiv™ Avocent® ACS800/8000 advanced console system using port number and public/private key authentication. To work around this issue, use a custom user account instead of the administrator account when establishing SSH passthrough connections.
 - 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 select 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.
 - 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.
 - A Vertiv™ PowerIT rPDU device connected to a Vertiv™ Avocent® RM1048P Rack Manager that the management platform manages is not being automatically rediscovered after deleting the rPDU device from the web UI and rebooting the rack manager. To resolve this issue, perform a resync operation on the rack manager from the web UI to display the rPDU device in the Appliance View.

- 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 page.
- SNMP V3 traps are currently not supported in the management platform hardware or virtual appliance.
- Upgrading a Vertiv™ Avocent® RM1048P Rack Manager appliance that the management platform manages may display the error message *Failure: could not retrieve update status from appliance* after the firmware upgrade has completed successfully. When this occurs, manually reboot the rack manager appliance.
- Upgrading the firmware of a management platform virtual appliance with the firmware of a management platform hardware appliance causes the virtual appliance to become non-operational.
- Unable to discover an older version of a Vertiv™ Avocent® RM1048P Rack Manager appliance using the web UI. To resolve this issue, upgrade the appliance to a newer version and then rediscover it from the web UI.
- A Vertiv™ Avocent® ACS800/8000 advanced console system cannot be re-enrolled into the management platform (CA-0000765879, CAS-70019-J0X8B0, CAS-568010, CAS-568207, and CA-0000823887).
- The outlet groups of a Vertiv™ Liebert® rack UPS device connected to a Vertiv™ Avocent® RM1048P 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.
- 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.
- 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 Vertiv™ PowerIT 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.
- Unable to control outlet groups of a UPS device that is connected to the Vertiv™ Avocent® RM1048P Rack Manager.
- When the FIPS mode of operation is enabled on the Vertiv™ Avocent® MP1000 Management Platform, specific FIPS 140-2 supported cryptographic algorithms can result in a failed connection to an SMB server when trying to perform a Backup and Restore operation. To resolve this issue, disable the FIPS mode of operation on the *Administration - System Settings - FIPS Module* page, and then connect to the SMB server to perform the Backup and Restore operation using the CLI.
- A power loss of an SMB server might cause the 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.
- After restoring a management platform from an existing SMB server backup, any existing credential profiles are not displayed on the web UI of the restored appliance. To resolve this issue, create new credential profiles with unique names using the web UI of the restored appliance.
- 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 highlighted when using Linux; this is not supported in VMware.
- The 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 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 rack manager web UI.
- In some rare cases, the Status column on the Targets List page disappears when using the Google Chrome browser. If this occurs, clear the browser cache and open a new browser window.