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

Release Notes

VERSION 3.80.3, AUGUST 2025

Release Notes Section Outline

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 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 & Downloads* tab.**

IMPORTANT NOTE: Prior to updating the hardware appliance firmware, ensure your 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, and it assumes the virtual appliance is already deployed on your system. If you need instructions on preparing for and deploying the virtual appliance, or if you need any additional information related to the initial launch of the virtual appliance, see the Vertiv™ Avocent® MP1000VA Installation/Deployment Guide that is available on the product page under the *Documents & Downloads* tab (Vertiv™ Avocent® MP1000 Management Platform Virtual Appliance). Once you have deployed the virtual appliance and are ready to upgrade to the latest version, proceed to the next section of these release notes.

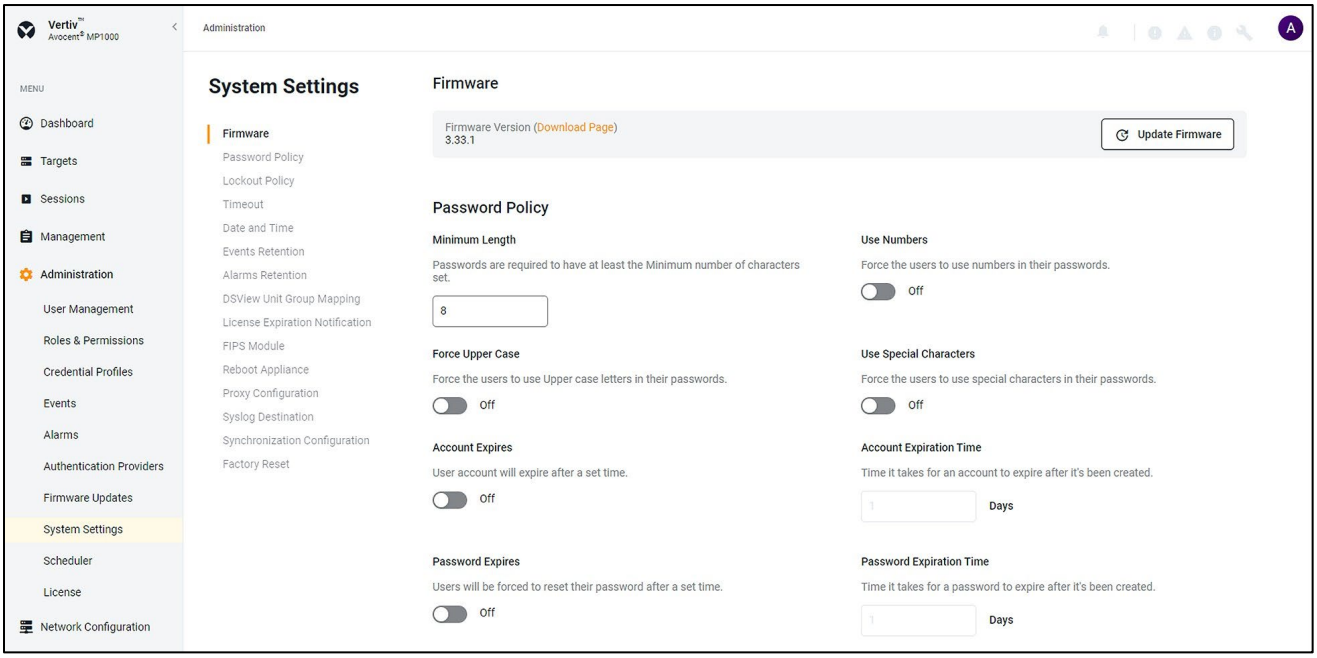
IMPORTANT NOTE: Initial deployment of the virtual appliance in a VMware virtual environment is done with an Open Virtual Appliance (OVA) file (.ova). Similarly, initial deployment of the virtual appliance in a Hyper-V virtual environment is done with a Virtual Hard Disk (VHDX) file (.vhdx). Ensure you do not attempt to update the virtual appliance with that file; the upgrade file is an img.xz file. Additionally, the upgrade files for the virtual appliance are NOT interchangeable with the hardware appliance upgrade files. Prior to upgrading, verify you are using files specifically for the Vertiv™ Avocent® MP1000VA Management Platform Virtual Appliance.

3. Update Instructions

NOTE: If you have previously configured a cluster with either a management platform hardware or virtual appliance with a firmware version prior to v3.66.8, the node must be deconstructed to successfully perform a firmware upgrade. To deconstruct the node from the web UI, navigate to the *Management - High Availability* screen. First, remove the Standby node from the cluster, then remove the Primary node. Once the cluster has been torn down, you may proceed to the below procedure to upgrade the firmware. For further details on High Availability, refer to the Vertiv™ Avocent® MP1000 High Availability Technical Note.

To update the management platform appliance 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*.

   NOTE: If the time on the rack manager and the management platform vary by more than a few seconds, the management platform will be unable to discover and manager 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

NOTE: Starting with appliance firmware version 3.66.8, the file extension has been changed from .img.xz to .fl for both the hardware and virtual appliance.

NOTE: Before upgrading the management platform hardware or virtual appliance with a firmware version prior to 3.58.4, you must first upgrade the appliance to firmware version 3.58.4 (released in February 2024).

APPLIANCE/PRODUCT	VERSION	FILENAME
Vertiv™ Avocent® MP1000 Management Platform	3.80.3	obsidian-3.80.3-update.fl
Vertiv™ Avocent® MP1000VA Management Platform Virtual Appliance	3.80.3	AvocentADXVirtualAppliance-3.80.3-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 support for logging in to the management platform web UI using the single sign-on (SSO) feature. This includes the following:
  - Enable or disable the SSO feature.
  - Add and configure an SSO authentication provider that supports the OpenID Connect (OIDC) protocol.
  - Test the connection to the SSO authentication provider with connection status feedback provided in the web UI.
- Adds support for custom fields associated with devices. This includes the following:
  - Add up to twenty custom fields and define a label for each custom field.
  - Configure a set of custom fields to be displayed as columns in the *Targets – Appliance View* or *Targets – Targets List* page.
  - Allow a user to modify custom field values for a specific device.
- Adds support for child devices to inherit resource group membership from the top-level device (i.e., an appliance). When this feature is enabled in the management platform web UI, the following operations are automatically performed:
  - Update the resource group membership of all devices based on their top-level device resource group membership.
  - New devices added to the management platform will inherit the resource group membership from their top-level device.
  - Any changes in the resource group membership for a top-level device will be applied to the child devices.
  - The user is informed that the resource group membership has been inherited by child devices of a top-level device.
- Adds support for Vertiv™ Avocent® MergePoint Unity™ 2 KVM over IP and serial console switches. This will include the following operations:
  - Automatically enroll the KVM over IP and serial console switch in the management platform when the user registers the switch with the management platform.
  - Launch KVM, Virtual Media, and Serial sessions to target devices connected to the KVM over IP and serial console switch.
  - View properties of the KVM over IP and serial console switch.
  - Access the KVM over IP and serial console switch web UI from the management platform web UI.
  - Upgrade the KVM over IP and serial console switch firmware.
  - Reboot the KVM over IP and serial console switch.
  - Reset the KVM over IP and serial console switch to factory default settings.
- Adds support for Vertiv™ Avocent® AutoView™ switches. This will allow a user to perform the following operations:
  - Discover Vertiv™ Avocent® AutoView™ switches on the network and add them to the platform management web UI.
  - Launch KVM, Virtual Media, and Serial sessions to target devices connected to a Vertiv™ Avocent® AutoView™ switch.

- Perform resync operations on the Vertiv™ Avocent® AutoView™ switch.
- Access the Vertiv™ Avocent® AutoView™ switch web UI from the management platform web UI.
- Upgrade the Vertiv™ Avocent® AutoView™ switch firmware.
- Reboot the Vertiv™ Avocent® AutoView™ switch.
- Enable or disable secure mode when connection to the Vertiv™ Avocent® AutoView™ switch.

- Adds the ability to view and configure settings for Vertiv™ Avocent® ACS800 and ACS8000 advanced console systems from the management platform web UI.
- Allows a user with the appropriate permissions to reset the firmware on the Vertiv™ Avocent® MP1000 Management Platform appliance. This includes the following options:
  - Retain the current firmware version.
  - Restore to the previous firmware version.
  - Restore to the factory default firmware version.
- Enhances the licensing feature as follows:
  - Adds the ability to view the same entitlement ID from the management platform web UI as it is displayed in the licensing customer portal.
  - Provides a mechanism to distinguish between legacy license keys and license entitlement IDs in the management platform web UI.
- Enhances the Bulk Firmware Update feature as follows:
  - Perform the bulk firmware update operation on several Vertiv™ Avocent® ACS800 or ACS8000 advanced console systems from the management platform web UI.

Resolved Issues

- General issues resolved:
  - Fixed issue where a user may not able to authenticate with Azure single sign-on (SSO) after the configuration of the Azure SSO has been successfully completed on the web UI (CA-0001076222).
  - Fixed issue where alarms associated with low current on the Vertiv™ Geist™ rPDU device are not being displayed on the *Administration - Alarms* page of the management platform web UI (CA-0001003684).
  - Fixed issue where a user with a View Device permission is allowed view and perform certain management operations (i.e., update appliance settings) that the user should not be allowed to perform on the Vertiv™ Avocent® RM1048P Rack Manager appliance (CA-0001021720).
  - Fixed issue where an extra additional text “DNS:” is added to the beginning of each subject alternate name when generating a certificate signing request.
  - Fixed issue where the search feature of the Appliance View is case sensitive.
- High Availability issues resolved:
  - Fixed issue where a primary node stays in Maintenance mode and prevents the primary node from switching to Standby mode (CA-0001082261 and CA-0001077669)
  - Fixed issue where data from a cluster node is not being replicated after a cluster has been reconstructed or a node failover has been performed (CA-0001045561).
  - Fixed issue where a cluster node does not report the correct server mode (i.e., Primary, Standby, Maintenance or Standalone) after the cluster node has been restarted (CA-0001045560).
  - Fixed issue where the status of devices that support the SNMP protocol is displayed as not responding in the web UI after a successful node failover.
  - Fixed issue where a cluster node transition from a primary node to a standby node causes the status of existing Vertiv™ Avocent® MergePoint Unity™ switches to show as non-responsive and the devices are no longer manageable.
- Firmware Update issues resolved:
  - Fixed issue where several attempts to update the Vertiv™ Avocent® MP1000VA Management Platform Virtual Appliance firmware failed without providing details to the user about the reason for the failure.

- Viewer issues resolved:
  - Fixed issue where launching a KVM session to a target device connected to a Vertiv™ Avocent® RM1048P Rack Manager fails in proxy mode (CA-0000989255).
  - Fixed issue where a KVM session to a target device from the Dashboard is unable to connect to the target device and the Dashboard shows a session timeout.
  - Fixed issue where KVM and serial viewer sessions to a target device connected to a Vertiv™ Avocent® MergePoint Unity™ switch cannot be stopped from the Sessions List page.
- Web UI issues resolved:
  - Fixed issue where a user may not be able to change network settings under bonded mode (CAS-569292).
  - Fixed issue where devices may be missing from the Appliance View after upgrading the management platform firmware (CA-0000998434, CA-0001008917, and CA-0001010858).
  - Fixed issue where changes to the domain name on the device network settings is not being saved (CA-0001005725 and CA-0001017960).
  - Fixed issue where ports associated with devices connected to Vertiv™ Avocent® RM1048P Rack Manager appliances are shown as duplicates on the platform management web UI and the ports are being set with the default names instead of customer supplied names (CA-0000998455).
- Licensing issues resolved:
  - Fixed issue where the launching of a KVM session from the *Targets – Appliance View* or *Targets – Targets List* page shows incorrectly that one or more licenses have expired (CA-0001056587).
  - Fixed issue where a non-administrator user who is not allowed to view licensing information is prevented from launching a KVM session to a target device (CA-0000982623 and CA-0001008284).

6. 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™ 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+
Chrome	115+	40+
Safari	16+	12+

9. Viewer Support and Version Information

Supported Viewers

VIEWER	VERSION
KVM Viewer	4.50.1
Serial Viewer	4.23.1
Virtual Machine (VM) Viewer	3.20.1

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

SERVICE PROCESSOR	FIRMWARE VERSION	PROTOCOLS
HP iLO 3	iLO 3 v1.92	IPMI 2.0
HP iLO 4	iLO 4 v2.82	Redfish, IPMI 2.0
HP iLO 5	iLO 5 v2.91	Redfish, IPMI 2.0
Lenovo IMM2	TCOO60A 5.90	IPMI 2.0
Lenovo XCC	CDI3A8N 9.40	Redfish, IPMI 2.0
FSC iRMCS4	9.62F	IPMI 2.0
ACI	v4.3-2022-r08	Redfish, IPMI 2.0
OpenBMC	2.9, 2.11	Redfish, IPMI 2.0

Supported SPs/Servers for Launching KVM Sessions

SERVICE PROCESSOR	PORT	PORT TRAFFIC
Dell iDRAC7	5900	Inbound
Dell iDRAC8	5900	Inbound
Dell iDRAC9	5900 (default), 443 (configured with racadm)	Inbound
HP iLO 4	5900 (firmware < 2.8), 443 (firmware > 2.8)	Inbound
HP iLO 5	443	Inbound
XCC	3900	Inbound

11. Power Distribution Unit (PDU) Support Information

PRODUCT FAMILY	FIRMWARE VERSION
Vertiv™ Geist™ rPDU with I-03	6.3.0
Vertiv™ Geist™ rPDU with I-05M	6.3.0

12. Rack UPS Support Information

SUPPORTED VERTIV™ RACK UPS PRODUCTS
Vertiv™ Liebert® GXT4 and 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. Cascaded Device Support Information for Vertiv™ Avocent® MergePoint Unity™ and AutoView™ Switches

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

15. TCP Port Usage Information

PORT	TYPE	PORT TRAFFIC	DESCRIPTION
443	TCP	Inbound, Outbound	General Communications (TCP)
22	TCP	Inbound	General Communications (TCP)
3871	TCP	Outbound	Vertiv™ Avocent® ACS800/8000 advanced console systems Vertiv™ Avocent® MergePoint Unity™ KVM over IP and serial console switch
445	TCP	Outbound	The SMB host port must be open for the management platform to connect to a remote network drive for backup and restore operations.
4122	TCP	Outbound	This port is required only when the SSH Passthrough feature is enabled.
48048	TCP	Outbound	The default port for RESTful API communication with a Vertiv™ Avocent® ACS800/8000 advanced console system. This port is configurable on the advanced console system.

16. 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

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.

17. Vertiv™ Avocent® DSView™ Solution Related Products

PRODUCT	DOWNLOAD PAGE
Vertiv™ Avocent® RM1048P Rack Manager	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-acs-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® 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/

18. Known Issues and Limitations

This release contains the following known issues and limitations:

- Firmware Update Issues:
  - **[BEFORE UPGRADING rPDU DEVICE]** When a Vertiv™ Geist™ rPDU device is connected to a Vertiv™ Avocent® RM1048P Rack Manager and configured to obtain an IP address from a DHCP server, a firmware upgrade of the rPDU device causes the device to obtain a new IP address after it is rebooted. To resolve this issue, configure the rack manager to reserve an IP address for the rPDU device.
  - The firmware version on the Appliance View page is not updated correctly after performing an upgrade of the Vertiv™ Avocent® MergePoint Unity™ switch.
  - 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 Vertiv™ Avocent® IPIQ IP KVM devices that have previously failed.
  - A bulk firmware update operation of several Vertiv™ Avocent® IPUHD IP KVM devices that are physically connected to the back of a Vertiv™ Avocent® RM1048P Rack Manager may cause one or more firmware updates to fail. To resolve this issue, wait for at least five minutes after the Vertiv™ Avocent® IPUHD IP KVM Device Bulk Firmware Update operation has failed and then update the firmware for Vertiv™ Avocent® IPUHD IP KVM devices that have previously failed. If the bulk update operation continues to fail, delete and re-add the Vertiv™ Avocent® IPUHD IP KVM device from the *Targets – Appliance View* or *Targets – Target List* page and then update the firmware for Vertiv™ Avocent® IPUHD IP KVM devices. If the bulk firmware update operation issue is not resolved, follow these steps:

1. Disconnect the Vertiv™ Avocent® IPUHD IP KVM device from the back of the Vertiv™ Avocent® RM1048P Rack Manager.
2. Delete the Vertiv™ Avocent® IPUHD IP KVM device from the *Targets – Appliance View* or *Targets – Target List* page.
3. Restart both the sip-docker and ip-management services using the CLI.
4. Update the firmware in the Vertiv™ Avocent® IPUHD IP KVM device.

- A bulk firmware update operation of several Vertiv™ Avocent® RM1048P Rack Managers that are managed by the Vertiv™ Avocent® MP1000 Management Platform may cause one or more firmware updates to fail. To resolve this issue, follow these steps:
  1. Delete and re-add the Vertiv™ Avocent® RM1048P Rack Manager from the *Targets - Appliance View* page.
  2. Re-add the Vertiv™ Avocent® RM1048P Rack Manager.
  3. Update the firmware in the Vertiv™ Avocent® RM1048P Rack Manager.

- Certificate Issues:
  - The 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 appliance is managed by the Vertiv™ Avocent® MP1000 Management Platform.
  - The SAN (Subject Alternative Name) field is not included in a CSR (Certificate Signing Request) generated by a Vertiv™ Avocent® IPUHD 4K IP KVM or Vertiv™ Avocent® IPSL IP serial device that is managed by either the Vertiv™ Avocent® MP1000 Management Platform or 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 Target List requires a manual refresh of the page to view the updated contents of the certificate.
- High Availability issues:
  - After updating the Vertiv™ Avocent® MP1000 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 the node was first added to the cluster and then reboot the node in 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 3-button menu at the end of the row of the node you want to correct and select the *Set to Standby* option. The role in the High Availability list view 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™ server from the management platform, then re-add it and wait for the status to update.
  - After a cluster is setup or the cluster is deconstructed and then reconstructed, one of the cluster nodes (i.e., Vertiv™ Avocent® MP1000 Management Platform hardware appliance) may fail to be added to the cluster. To resolve this issue, login 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 and then add the node to the cluster.

    If the Add Node operation fails or you are 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 next menu, select the **Factory Restore** menu option.

- After a cluster is deconstructed and then reconstructed, one of the cluster nodes (i.e., Vertiv™ Avocent® MP1000VA Management Platform Virtual Appliance for VMware) may fail to be added to the cluster. To resolve this issue, login 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 you are 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. Login 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 next menu, select the **Force boot previous Image** menu option.

  -or-

  If the virtual appliance has been installed without being upgraded, you will need to delete and re-install the MP1000VA virtual appliance.

- Virtual Machine issues:
  - The status and power control for virtual machines running in Hyper-V are not displayed correctly in the Appliance View.
  - 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, you can add the VM host from the Appliance View page.
- SP issues:
  - Users are unable to access the web UI for iDRAC 8/9 service processors with firmware version 5.10.50.00 or higher from the Target List view.

    To resolve this issue, follow these steps:

    1. Log in to the iDRAC 8/9 service processor from a console window.
    2. Execute the **racadm get idrac.webserver.HostHeaderCheck** command and verify the host header check is enabled.
    3. Execute the **racadm set idrac.webserver.HostHeaderCheck 0** command and verify it is successfully executed.
    4. Execute the **racadm get idrac.webserver.HostHeaderCheck** command and verify the host header check is disabled.
    5. Launch the web UI for the iDRAC 8/9 service processor from the Target List view.
  - Accessing details for SPs that were discovered using invalid Credential Profile information results in an error message and no device details are shown. The workaround for this is to update the Credential Profile in the SP's Properties panel and perform a Resync operation, or you can rediscover one or more SPs with an IP Range Discovery operation using the correct Credential Profile(s).
  - 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.
  - 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:
  - 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.
  - A user with a lower permission level is able to view the list of all viewer sessions.

- 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 Chrome and Edge client browsers.
- The icon to launch viewer sessions at the row level of the Appliance and Target List Views is missing for serial target devices that are managed by the Vertiv™ Avocent® DSView™ management software and displayed on the Management Platform web UI. The icon to launch viewer sessions is available on the Properties side panel.
- Renaming a target device that is managed by the Vertiv™ Avocent® DSView™ management software and displayed on the Management Platform web UI prevents launching a viewer session to the target device.
- After the initial discovery of a Vertiv™ Avocent® IPIQ IP KVM device, the launch KVM icon in the Targets List and Appliance View remains disabled until the device 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:
  - Unable to update a target device name from the Properties panel of a Vertiv™ Avocent® ACS800 and ACS8000 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™ Geist™ 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™ Geist™ rPDU device is not updated correctly (i.e., 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 Vertiv™ Avocent® MP1000 or Vertiv™ Avocent® MP1000VA 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 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. 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 on the *Trash* icon located above the table to remove the target device.

- General issues:
  - Management of a Vertiv™ Avocent® MergePoint Unity™ switch by multiple Vertiv™ Avocent® MP1000 Management Platform and Vertiv™ Avocent® MP1000VA Management Platform Virtual appliances is not supported.
  - After updating the serial port name from the Vertiv™ Avocent® IPSL IP serial device user interface, the serial port name is not synchronized in the Targets – Appliance View or Targets – Target List page.
  - SNMP V3 traps are currently not being supported in the Vertiv™ Avocent® MP1000 Management Platform or Vertiv™ Avocent® MP1000VA Management Platform Virtual Appliance.
  - Upgrading a Vertiv™ Avocent® RM1048P Rack Manager appliance that is managed by the Vertiv™ Avocent® MP1000 Management Platform 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 Vertiv™ Avocent® MP1000VA Management Platform Virtual Appliance with the firmware of a Vertiv™ Avocent® MP1000 Management Platform 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 re-discover the appliance from the web UI.
  - Unable to discover a Vertiv™ Geist™ rPDU device with firmware 6.x using a credential profile that is configured with username and password. To resolve this issue, enable the Aggregation feature and set the HTTP Interface to “Enabled” on the rPDU device. Then, re-discover the rPDU device using the web UI.
  - 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).
  - Vertiv™ Liebert® rack UPS and Vertiv™ Geist™ 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. To resolve this issue, you can remove and re-add the UPS or rPDU devices to the Appliance View.
  - 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 Target List page after an appliance firmware upgrade. To resolve this issue, delete the UPS device and add it back to the Appliance View or Target List page.
  - A power cycle of a Vertiv™ Liebert® rack UPS device outlet group using the web UI does not work properly when the outlet group is already turned off.
  - 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.
- When the FIPS mode of operation is enabled on the Vertiv™ Avocent® MP1000 Management Platform, certain 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 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.
- After restoring a Vertiv™ Avocent® MP1000 Management Platform appliance 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 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 on the Target List page disappears using the Chrome browser. If this occurs, clear the browser cache and open a new browser window.