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

Release Notes

VERSION 3.58.4, FEBRUARY 2024

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

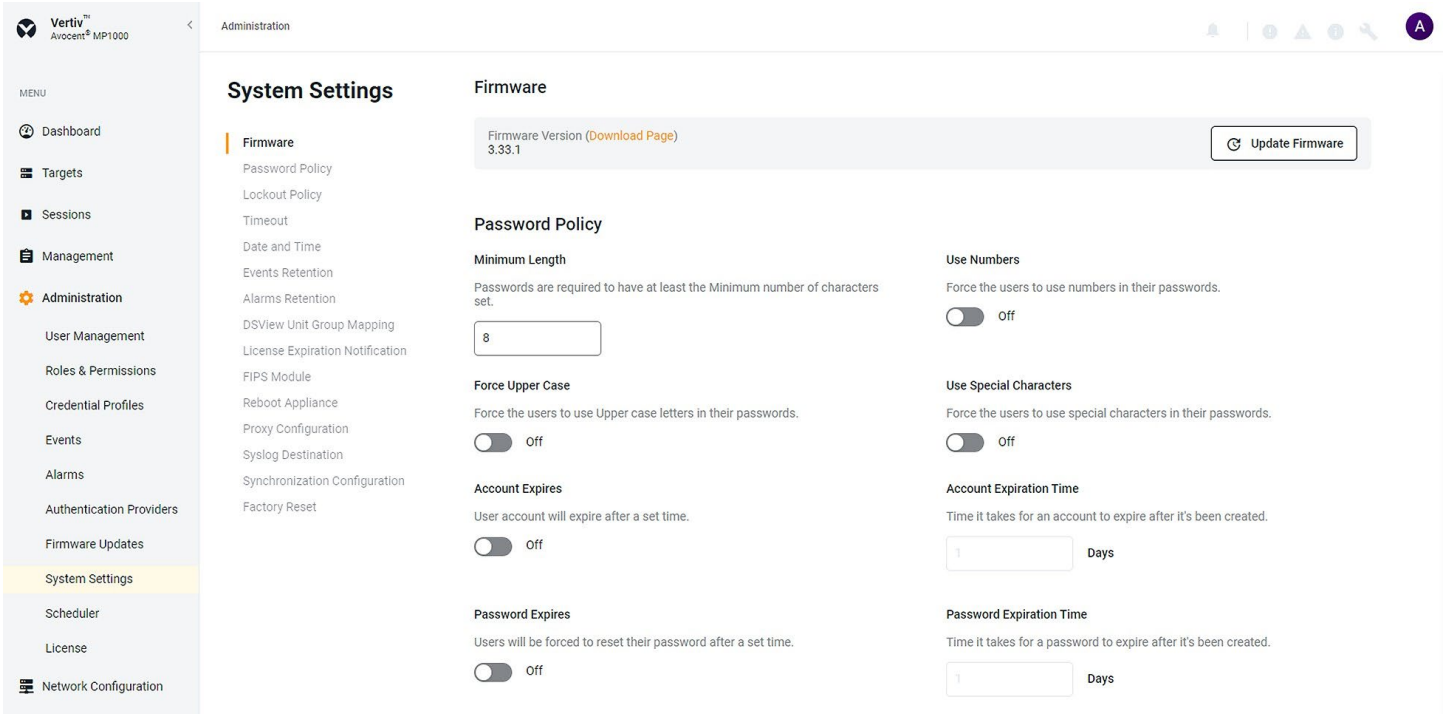
This new release supports upgrading the Vertiv™ Avocent® MP1000 Management Platform Virtual Appliance in both VMware and Hyper-V virtual environments, and it assumes the virtual appliance is already deployed on your system. If you need instructions on preparing for and deploying the virtual appliance, 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

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*.

4. Appliance Firmware Version Information

APPLIANCE/PRODUCT	VERSION	FILENAME
Vertiv™ Avocent® MP1000 Management Platform	3.58.4	obsidian-3.58.4.img.xz
Vertiv™ Avocent® MP1000VA Management Platform Virtual Appliance	3.58.4	AvocentADXVirtualAppliance3.58.4-update.img.xz

5. Features and Enhancements

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

- This release adds support for High Availability (HA) of management platform nodes in a cluster. This feature allows a user to perform the following operations:
    - Manage HA cluster configuration
    - Enable the HA feature on the management platform.
    - Add a management platform node to the HA cluster.
    - Remove a management platform node from the HA cluster.
    - Configure a management platform as a primary or standby node in the HA cluster.
    - View the health and status of each node in the HA cluster.
    - Manage failover between the primary and standby node in the HA cluster
    - Configure the response timeout to invoke an automatic failover from the standby to primary node.
    - Manually switch from the standby to the primary node using the web UI.

Resolved Issues

- General issues resolved:
    - Fixed issue where the firmware upgrade of a Vertiv™ Avocent® IPIQ IP KVM device or Vertiv™ Avocent® IPUHD 4K IP KVM device using the Upload File method generates an error message.
    - Fixed issue where the generation of a CSR with the asterisk symbol (*) in the Common Name and SAN attribute causes an HTTP 500 error (CAS-67981-J1F1B3).
    - Fixed issue where the Physical Port column heading on the Appliance View is not aligned correctly when scrolling to the right side of the page (CAS-56629-W3W6N2).
    - Fixed issue where clicking several times on a row that displays a Vertiv™ Avocent® IPSL IP serial device on the Target List causes several error messages to be displayed.
    - Fixed issue where the session list panel is incorrectly displayed for a user with the User Administrator role.
    - Fixed issue where the connection to an external authentication provider that is configured with an FQDN name is not successful (CAS-66019-Z7G5Z9).
    - Fixed issue where a Vertiv™ Avocent® IPUHD 4K IP KVM device that is connected to a Vertiv™ Avocent® RM1048P Rack Manager is not being discovered.
    - Fixed issue where Vertiv™ Geist™ rPDU or Vertiv™ Liebert® rack UPS devices are not being rediscovered after being deleted from the Appliance View.
- Resync issues resolved:
    - Fixed issue where the names for target devices that are managed by the Vertiv™ Avocent® DSView™ management software and displayed on the web UI are not being synchronized correctly.
- Organization issues resolved:
    - Fixed issue where a user without the proper permissions is able to create a new organization (CAS-68543-G1S4L9).
- User Group issues resolved:
    - Fixed issue where users who are members of an Active Directory nested group are unable to login to the management platform (CAS-69079-B2L7Q6).
    - Fixed issue where adding nested resource groups to an existing user group displays an SQL error message (CAS-68640-D2P8G2).
    - Fixed issue where the state of the “Select All” check box for System Roles is inconsistent when selecting a user group on the User Management page.
- Configuration issues resolved:
    - Fixed issue where modifying the external IP address of a NAT rule on the Properties panel displays an error message.
    - Fixed issue where updating the static IP address on the properties panel for a Vertiv™ Avocent® IPUHD 4K IP KVM device displays an error message.

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® 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	4.28.1
Serial Viewer	4.12.1
Virtual Machine (VM) Viewer	3.15.1

10.Dashboard Support Information

ITEM	VERSION
Dashboard	1.29.1

11. Server Processor (SP) Support Information

Tested SPs/Servers and Firmware

NOTE: Other SPs that support IPMI 2.0 may also be supported.

SERVICE PROCESSOR	FIRMWARE VERSION	PROTOCOLS
Dell iDRAC6 (R)	2.92	IPMI 2.0
Dell iDRAC7	2.65.65.65	Redfish, IPMI 2.0
Dell iDRAC8	2.84.84.84	Redfish, IPMI 2.0
Dell iDRAC9	6.10.80.00	Redfish, IPMI 2.0
HP iLO 2	iLO 2 v2.33	IPMI 2.0
HP iLO 3	iLO 3 v1.92	IPMI 2.0
HP iLO 4	iLO 4 v2.82	Redfish, IPMI 2.0
HP iLO 5	iLO 5 v2.91	Redfish, IPMI 2.0
Lenovo IMM2	TCOO60A 5.90	IPMI 2.0
Lenovo XCC	CDI3A8N 9.40	Redfish, IPMI 2.0
FSC iRMCS4	9.62F	IPMI 2.0
ACI	v4.3-2022-r08	Redfish, IPMI 2.0
OpenBMC	2.9, 2.11	Redfish, IPMI 2.0

Supported SPs/Servers for Launching KVM Sessions

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

12. Power Distribution Unit (PDU) Support Information

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

13. Rack UPS Support Information

SUPPORTED VERTIV RACK UPS PRODUCT
Vertiv™ Liebert® GXT5 UPS
Vertiv™ Liebert® PSI5 UPS
Vertiv™ Edge UPS
Vertiv™ Liebert® APS UPS

14. TCP Port Usage Information

NOTE: TCP port usage is bidirectional unless otherwise noted.

PORT	TYPE	DESCRIPTION
443	TCP	General Communications (TCP)
22	TCP	General Communications (TCP)
3871	TCP	Vertiv™ Avocent® ACS800/8000 advanced console systems
445	TCP	The SMB host port must be open for the management platform to connect to the SMB device.
31417	TCP	This port is required to support replication between nodes in the HA cluster.

15. Vertiv™ Avocent® DSView™ Management Software Versions

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

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

16. Known Issues and Limitations

This release contains the following known issues and limitations:

- Virtual Machine issues:
  - The status and power control for virtual machines running in Hyper-V are not displayed correctly in the Appliance View.
  - 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.
  - The Network Configuration page displays an error message when entering a period character in the Domain Name field.
- SP issues:
  - Users are unable to access the web UI for iDRAC 8/9 service processors with firmware version 5.10.50.00 or higher from the Target List view.

    To resolve this issue:

    1. Log in to the iDRAC 8/9 service processor from a console window.

2. Execute the **racadm get idrac.webserver.HostHeaderCheck** command and verify the host header check is enabled.
3. Execute the **racadm set idrac.webserver.HostHeaderCheck 0** command and verify it is successfully executed.
4. Execute the **racadm get idrac.webserver.HostHeaderCheck** command and verify the host header check is disabled.
5. Launch the web UI for the iDRAC 8/9 service processor from the Target List view.

- Accessing details for SPs that were discovered using invalid Credential Profile information results in an error message and no device details are shown. The workaround for this is to update the Credential Profile in the SP's Properties panel and perform a Resync operation, or you can rediscover one or more SPs with an IP Range Discovery operation using the correct Credential Profile(s).
- SPs that are connected to a Vertiv™ Avocent® RM1048P Rack Manager, then deleted from the Appliance View are not being rediscovered and added to the Appliance View after performing a resync operation.
- OpenBMC SPs do not support virtual media, sensor, power or thermal data.
- Mounting virtual media on iDRAC7/8 SPs behaves inconsistently.
- CIFS and NFS are not operational for HP iLO4 and iLO5 SPs.
- No access is given to archived events on an HP iLO5 SP.
- The default system roles (User-Role, User-Administrator-Role and System-Maintainer-Role) do not include access to SPs.

- Session/Viewer issues:
  - The icon to launch viewer sessions at the row level of the Appliance and Target List Views is missing for serial target devices that are managed by the Vertiv™ Avocent® DSView™ management software and displayed on the Management Platform web UI. The icon to launch viewer sessions is available on the Properties side panel.
  - Renaming a target device that is managed by the Vertiv™ Avocent® DSView™ management software and displayed on the Management Platform web UI prevents launching a viewer session to the target device.
  - After the initial discovery of a Vertiv™ Avocent® IPIQ IP KVM device, the launch KVM icon in the Targets List and Appliance View remains disabled until the device has completed the registration process. The Targets List View page can be refreshed after a few minutes to access the launch KVM icon for the device.
  - VM sessions are not cleared after exiting the KVM Viewer.
  - After changing the time zone or enabling NTP on the Vertiv™ Avocent® IPUHD 4K IP KVM device, launching a KVM session to the device fails with a timeout error.
  - A KVM session to a Vertiv™ Avocent® IPUHD 4K IP KVM device that goes into sleep mode due to user inactivity does not respond to keyboard or mouse input.
  - Launching a KVM or serial session to a Vertiv™ Avocent® DSView™ software device may open an additional browser tab (and leave it opened). You must manually close the additional browser tab after the session is closed.
  - KVM or serial sessions to Vertiv™ Avocent® DSView™ software devices connected to a Vertiv™ Avocent® MergePoint Unity™ KVM over IP and serial console switch or a Vertiv™ Avocent® Universal Management Gateway appliance are not listed in the Sessions list page.
  - Session timeout modifications do not take effect until a logout occurs; no message is forthcoming.
  - Viewer sessions for a Vertiv™ Avocent® IPUHD 4K IP KVM device connected to a Vertiv™ Avocent® RM1048P Rack Manager does not show up correctly in the Dashboard.
- Web UI issues:
  - When the list of email address on the Distribution List of the Notification Policy settings are separated by a carriage return, the save operation generates an error message. To resolve this issue, the list of email addresses should be separated by a semicolon and not a carriage return.
  - When the list of email address on the Add Notification Policy panel are separated by a carriage return, the add operation generates an error message. To resolve this issue, the list of email addresses should be separated by a semicolon and not a carriage return.
  - The scroll bar on the Target List view is hidden when the browser window is resized to a smaller size.
  - Clicking away from the Device Properties panel before the properties are fully loaded generates several errors for Vertiv™ Avocent® IPSL IP serial devices and the Vertiv™ Avocent® IPUHD 4K IP KVM devices.
  - The RS422 and RS485 RJ-45 pin-out value options on the Physical Port Settings panel only apply to ports 1 and 2 of the Vertiv™ Avocent® ACS8000 advanced console system.
  - The web UI displays virtual machines managed by VMWare ESXi and vCenter 6.5.x, 6.7.x and 7.x versions only.
  - Unable to change a full name in the User Preferences view.

- On the Organizations page, the Launch KVM Session icon may overlap with the Device Status icon. To resolve this issue and properly align both icons, zoom out on the browser page.
- Creating a new organization or filtering devices on organizations without any devices occasionally generates an error message; however, the new organization is successfully created.

- General issues:
  - 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.
  - The Primary and Secondary DNS values are lost after performing an appliance firmware upgrade. To resolve this issue, add the Primary and Secondary DNS values using the web UI.
  - Unable to discover a Vertiv™ Geist™ rPDU device with a Credential Profile that is configured with a specific port number. To resolve this issue, leave the port field blank and re-discover the rPDU device.
  - Changing the assigned DHCP IP address of a Vertiv™ Geist™ rPDU device to a reserved IP address causes the status of the device to show incorrectly. To resolve this issue, delete the Vertiv™ Geist™ rPDU device from the web UI and rediscover the device using the reserved IP address.
  - The Credential Profile assigned to a target device cannot be modified after the target device is discovered and added to the Target List page. To modify the Credential Profile, you need to rediscover the target device.
  - The Appliance View may show duplicate entries for Vertiv™ Geist™ rPDUs after discovery of rPDUs with the following Credential Profile Configurations:
    - If there is one Credential Profile configured with SNMP V2 and firmware update credentials.
      -or-
      If there are two Credential Profiles where the first Profile is configured with SNMP V2 and the second is configured with username/password.

    If this situation occurs and an rPDU listing is duplicated in the Appliance View, the rPDU power outlet status will not display correctly. To resolve the duplicate entry scenario, delete one of the duplicate listings. Once the duplicate listing is deleted, wait a few minutes and refresh the web page. This should then correct the rPDU power outlet status information as well.
  - The scheduled Daily Alarm Purge operation only purges alarms that are cleared and older than the configured retention period.
  - The alarm drop-down list in the upper right corner of the page does not update correctly when new alarms are generated. To resolve this issue, log out and log back into the application to view the updated list of alarms in the drop-down list.
  - Device name synchronization is not available for Vertiv™ Geist™ rPDUs discovered via SNMP.
  - Unable to change the power state of a Vertiv™ Liebert® PSI5 UPS outlet group.
  - Unable to control outlet groups of a UPS device that is connected to the Vertiv™ Avocent® RM1048P Rack Manager.
  - A power loss of an SMB server might cause the Vertiv™ Avocent® MP1000 Management Platform to generate HTTP 500 errors when performing backup and restore operations. To resolve this issue, connect the power to the SMB server and reconfigure the SMB server credentials and path using the CLI.
  - An attempt to establish a remote Virtual Media session to a Vertiv™ Avocent® IPUHD 4K IP KVM device managed by a Vertiv™ Avocent® RM1048P Rack Manager using the NFS Transfer Protocol fails with an error message.
  - When a serial USB adapter is not plugged into the micro-USB port of a Vertiv™ Avocent® IPUHD 4K IP KVM device, the Properties panel for the device displays *No Information* with no additional details.
  - The Kingston USB device is not supported and not displayed in the Boot Manager.
  - Power Control is non-functional for unlicensed VMWare targets.
  - The Virtual Machine Viewer Caps Lock (and other keys) are not highlighting when using Linux; this is not supported in VMWare.
  - The Vertiv™ Avocent® MP1000 Management Platform uses FTP as the only mechanism to upgrade a Vertiv™ Avocent® ACS 800/8000 advanced console system unit.
  - Deleting an unmanaged Vertiv™ Avocent® RM1048P Rack Manager in the Vertiv™ Avocent® MP1000 Management Platform does not trigger the rack manager to go into Standalone mode; it must be done manually.

- Unable to change settings for Vertiv™ Avocent® IPIQ IP KVM devices discovered through a Vertiv™ Avocent® RM1048P Rack Manager; settings may be updated using the Vertiv™ Avocent® RM1048P Rack Manager web UI.
- In some rare cases, the Status column in the Target List view disappears using the Chrome browser. If this occurs, clear the browser cache and open a new browser window.