Vertiv™ Avocent® ADX MP1000 Management Platform

Release Notes

VERSION 3.33.5, JULY 2023

Release Notes Section Outline

1. Update Instructions

The Vertiv™ Avocent® ADX MP1000 Management Platform firmware may be updated through the web user interface (UI). To access the Vertiv™ Avocent® ADX 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).

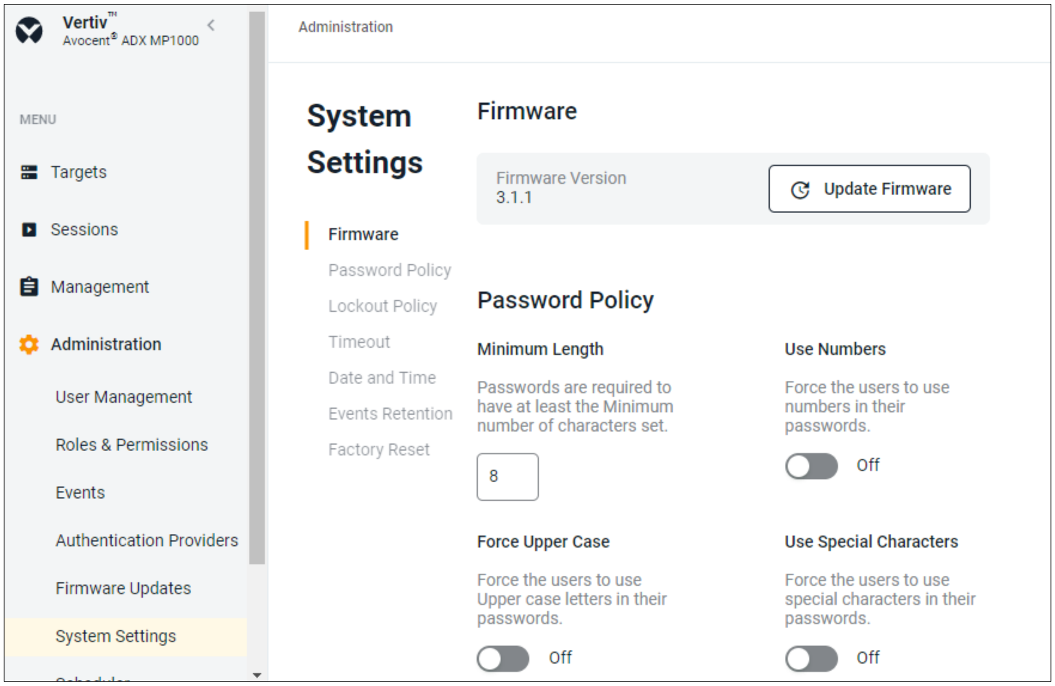
NOTE: For additional information on this process, see the Vertiv™ Avocent® ADX MP1000 Management Platform Quick Installation Guide that is provided with the platform and also available at www.vertiv.com/ADX-Management-Platform under the *Documents & Downloads* tab.

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

To update the Vertiv™ Avocent® ADX MP1000 Management Platform firmware:

1. Visit the Vertiv™ Avocent® ADX MP1000 Management Platform firmware download page located here:
   Vertiv™ Avocent® ADX 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® ADX 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.



Firmware

Firmware Version
3.1.1

Password Policy

Minimum Length

Passwords are required to have at least the Minimum number of characters set.

8

Use Numbers

Force the users to use numbers in their passwords.

Off

Force Upper Case

Force the users to use Upper case letters in their passwords.

Off

Use Special Characters

Force the users to use special characters in their passwords.

Off

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

2. Appliance Firmware Version Information

APPLIANCE/PRODUCT	VERSION	FILENAME
Vertiv™ Avocent® ADX MP1000 Management Platform	3.33.5	obsidian-3.33.5-update.img.xz

3. Features and Enhancements

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

- This release adds support for discovering Vertiv™ Avocent® IPSL IP serial devices and then adding them to the Target List view.
- This release adds support for discovering Vertiv™ rack UPS devices and then adding them to the Target List view. This capability allows you to perform the following operations:
  - View power metrics on the rack UPS device.
- This release adds support for synchronizing Vertiv™ Geist™ rack Power Distribution Unit (rPDU) outlet names.
- This release adds support for managing devices in an organization hierarchy. This capability allows you to perform the following operations:
  - Manage organizations by adding or removing an organization (or nested organization), adding or removing devices within an organization, and/or moving devices and organizations within the organization hierarchy.
  - Within an organization or nested organization, you can search and filter devices, and also view aggregated alarms for devices within an organization.
- This release adds support for viewing and managing device alarms. This functionality includes the following operations:
  - Search, sort, and filter device alarms.
  - Manually clear device alarm status.
  - Set a device in maintenance mode.
  - Configure alarm retention policy.
  - Display alarm count and alarm severity status.

- This release adds a new Edge Management dashboard allowing users to view the overall status of devices located on different sites to help diagnose issues. This includes status and metrics for devices discovered by the Vertiv™ Avocent® ADX MP1000 Management Platform.
- This release adds support for updating the Vertiv™ Geist™ rPDU firmware through the Vertiv™ Avocent® MP1000 Management Platform web UI.
- This release adds support for a user to be notified in a pop-up notification panel when new devices are discovered.
- This release adds support for configuring Cross-Origin Resource Sharing (CORS) through the Command Line Interface (CLI).
- This release adds API support to launch KVM, serial and Virtual Machine sessions.
- This release adds support for mapping a disk image as writable in KVM Viewer virtual media.
- This release adds the capability for updating the firmware for multiple devices in bulk mode.
- This release adds support for a TACACS+ external authentication provider.

Resolved Issues

- General issues resolved:
  - Fixed issue where the reboot operation on a Vertiv™ Avocent® ACS800 and/or ACS8000 advanced console system was not working properly.
  - Fixed issue where the firmware update operation from the Targets List was not working properly.
  - Fixed issue where an attempt to change the order in the list of external authentication providers caused an error to display to the user.
  - Fixed issue where a new user assigned to a default user group is unable to access the Appliance View.
  - Fixed issue where the user is unable to assign multiple roles to a resource group that belongs to a user group when the length of all combined roles exceeds 69 characters.
  - Fixed issue where a login attempt fails when multiple external authentication providers are configured in the Vertiv™ Avocent® ADX Platform system (CAS-56844-V1Q6K2 and CAS-55832-Z6Z8L0).
  - Fixed issue where a connection to a secure AD or LDAP authentication provider requires client certificate verification (CAS-59302-K5D5R7).
  - Fixed issue where merging a port on an Vertiv™ Avocent® ACS800 and/or ACS8000 device with another device creates duplicate launch serial icons on the Target List (CAS-55823-Z2H0C0).
  - Fixed issue where duplicate entries of a Vertiv™ Avocent® ADX IPIQ IP KVM device can be added to the Target List (CAS-56469-M8W4H9).
  - Fixed issue where the web UI was unable to retrieve groups from an external authentication provider with a large number of external groups (CAS-61819-L7X2S8).
  - Fixed issue where a user cannot drill down to a service processor from the Target List to access detailed information for the service processor (CAS-57036-W6J7S8).
  - Fixed issue where a Vertiv™ Avocent® ADX IPIQ IP KVM device in the Target List cannot be rediscovered after the device is deleted from the Target List (CAS-60870-Q8K1X6).
  - Fixed issue where the username is not displayed for closed sessions on the Session List panel (CAS-59092-T5P0J8).
  - Fixed issue where a firmware update on the Vertiv™ Avocent® ADX MP1000 Management Platform appliance with a large database causes the system to be non-operational.
  - Fixed issue where the KVM link in the Appliance View is disabled after initial discovery of a Vertiv™ Avocent® ADX IPIQ IP KVM device from the Vertiv™ Avocent® ADX MP1000VA virtual appliance.
- Virtual Appliance issues resolved:
  - Fixed issue where the certificate replacement script is unable to update the certificate for the Vertiv™ Avocent® ADX MP1000VA virtual appliance (CAS-58874-K4X5S5).
  - Fixed issue where launching a second KVM session to an Vertiv™ Avocent® ADX IPIQ IP KVM device fails when the system proxy configuration is enabled on the Vertiv™ Avocent® ADX MP1000VA virtual appliance (CAS-57611-M9Q0P8).
  - Fixed issue where the shutdown operation on a Vertiv™ Avocent® ADX MP1000 Management Platform appliance was not working properly.
- Viewer issues resolved:
  - Fixed issue where a user was unable to join an existing KVM session from the Sessions List page when the virtual media session was active on the KVM Viewer.
  - Fixed issue where a user was unable to download an ISO image file after being mapped to a file or folder in a virtual media session.
  - Fixed issue where a user attempts to change the default filename during creation of an ISO image file and the new filename does not take effect.

- Fixed issue where launching a passive or stealth KVM session behaves as an active KVM session when the system proxy is enabled.
- Fixed issue where a connection to a KVM session for a Vertiv™ Avocent® IPIQ IP KVM device drops after a few seconds when the system proxy is enabled.

- Serial issues resolved (serial appliances/ports/sessions):
  - Fixed issue where deleting an active serial session on a Vertiv™ Avocent® ACS800 and/or ACS8000 advanced console system device from the Sessions List page did not terminate the active serial session.
- Configuration issues resolved:
  - Fixed issue where the FIPS option was missing from the properties panel for a selected Vertiv™ Avocent® ADX IPUHD 4K IP KVM device on the Target List page.
  - Fixed issue where a user from an external authentication provider was unable to login after changing the external authentication provider from insecure to secure mode.
  - Fixed issue where a user is unable to change the domain name of a Vertiv™ Avocent® ADX RM1048P Rack Manager in the Network Settings page (CAS-56499-N0G3V8 and CAS-56531-K3D3P9).
  - Fixed issue where a user is unable to change the device name of a Vertiv™ Avocent® ADX RM1048P Rack Manager from the Management properties panel (CAS-56395-B9Q7W2).
  - Fixed issue where the MAC Address for a Vertiv™ Avocent® ADX IPIQ IP KVM device is not displayed on the Network Configuration panel (CAS-59056-P5T1X2).

4. Device Support Information

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

- Vertiv™ Avocent® ADX RM1048P Rack Manager
- Vertiv™ Avocent® ADX IPUHD 4K IP KVM device
- Vertiv™ Avocent® ADX IPIQ IP KVM device
- Vertiv™ Avocent® ACS800 and/or ACS8000 advanced console systems
- Vertiv™ Avocent® ADX IPSL IP serial device
- Vertiv™ Geist™ rPDUs
- Vertiv™ and Vertiv™ Liebert® rack UPS devices
- Vertiv™ Avocent® Universal Management Gateway appliance UMIQ-v2 module converted to operate as a Vertiv™ Avocent® ADX IPIQ IP KVM device
  NOTE: For this functionality, contact your Vertiv Technical Support representative.

5. Language Support Information

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

6. Client Browser Support Information

NOTE: Unless noted otherwise, both 32-bit and 64-bit browsers are supported.

BROWSER	PREFERRED VERSION	SUPPORTED VERSIONS
Edge	99+	79+
Firefox	97+	35+
Chrome	99+	40+
Safari	15+	12+

7. Viewer Support and Version Information

Supported Viewers

VIEWER	VERSION
KVM Viewer	4.11.1
Serial Viewer	4.5.1
Virtual Machine (VM) Viewer	3.8.1

8. Dashboard Support Information

ITEM	VERSION
Dashboard	1.25.1

9. Server Processor (SP) Support Information

Tested SPs/Servers and Firmware

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

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

Supported SPs/Servers for Launching KVM Sessions

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

10. Power Distribution Unit (PDU) Support Information

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

11. Rack UPS Support Information

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

12. TCP Port Usage Information

NOTE: TCP port usage is bidirectional unless otherwise noted.

PORT	TYPE	DESCRIPTION
443	TCP	General Communications (TCP)
22	TCP	General Communications (TCP)
3871	TCP	Vertiv™ Avocent® ACS800/8000 advanced console systems

13. Vertiv™ Avocent® DSView™ Management Software Versions

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

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

14. Known Issues and Limitations

This release contains the following known issues and limitations:

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

    To resolve this issue:

    1. Log in to the iDRAC 8/9 service processor from a console window.
    2. Execute the **racadm get idrac.webserver.HostHeaderCheck** command and verify the host header check is enabled.
    3. Execute the **racadm set idrac.webserver.HostHeaderCheck 0** command and verify it is successfully executed.
    4. Execute the **racadm get idrac.webserver.HostHeaderCheck** command and verify the host header check is disabled.
    5. Launch the web UI for the iDRAC 8/9 service processor from the Target List view.
  - Accessing details for SPs that were discovered using invalid Credential Profile information results in an error message and no device details are shown. The workaround for this is to update the Credential Profile in the SP's Properties panel and perform a Resync operation, or you can rediscover one or more SPs with an IP Range Discovery operation using the correct Credential Profile(s).
  - 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.
  - Clicking the SP name link (hyperlink) on the Targets List view produces error messages.
  - The default system roles (User-Role, User-Administrator-Role and System-Maintainer-Role) do not include access to SPs.
- Session/Viewer issues:
  - After the initial discovery of a Vertiv™ Avocent® ADX 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® ADX IPUHD 4K IP KVM device, launching a KVM session to the device fails with a timeout error.
  - A KVM session to a Vertiv™ Avocent® ADX 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® ADX IPUHD 4K IP KVM device connected to a Vertiv™ Avocent® ADX RM1048P Rack Manager does not show up correctly in the Dashboard.

- Web UI issues:
    - 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® ADX 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.
    - The asset tag for a Vertiv™ Avocent® ADX RM1048P Rack Manager cannot be changed using the web UI; it can be changed using the Command Line Interface (CLI), however.
    - With the option to add another resource group to a resource group, there are only options to add existing resource groups.
    - Unable to change a full name in the User Preferences view.
    - On the Organizations page, the Launch KVM Session icon may overlap with the Device Status icon. Zooming out on the browser page to properly align both icons resolves this issue.
- General issues:
    - 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.
    - Device name synchronization is not available for Vertiv™ Geist™ rPDUs discovered via SNMP.
    - An attempt to establish a remote Virtual Media session to a Vertiv™ Avocent® ADX IPUHD 4K IP KVM device managed by a Vertiv™ Avocent® ADX 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® ADX 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 changed time (from the CLI) is not maintained through a reset. BIOS overrides time and must be set via BIOS.
    - Managed Vertiv™ Avocent® ADX RM1048P Rack Manager and Vertiv™ Avocent® ADX IPUHD 4K IP KVM device firmware updates via the new managed device drill-down page fail with an error message.
    - The Vertiv™ Avocent® ADX 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® ADX RM1048P Rack Manager in the Vertiv™ Avocent® ADX 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® ADX IPIQ IP KVM devices discovered through a Vertiv™ Avocent® ADX RM1048P Rack Manager; settings may be updated using the Vertiv™ Avocent® ADX 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.