Vertiv™ Avocent® ADX MP1000 Management Platform
Release Notes

VERSION 3.17.8, OCTOBER 2022

Release Notes Section Outline

1. Update Instructions
2. Appliance Firmware Version Information
3. Features and Enhancements
4. Device Support Information
5. Language Support Information
6. Client Browser Support Information
7. Viewer Support and Version Information
8. Dashboard Support Information
9. Server Processor (SP) Support Information
10. Power Distribution Unit (PDU) Support Information
11. TCP Port Usage Information
12. Known Issues and Limitations

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 & Download*s tab.

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

To update the Vertiv™ Avocent® 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.
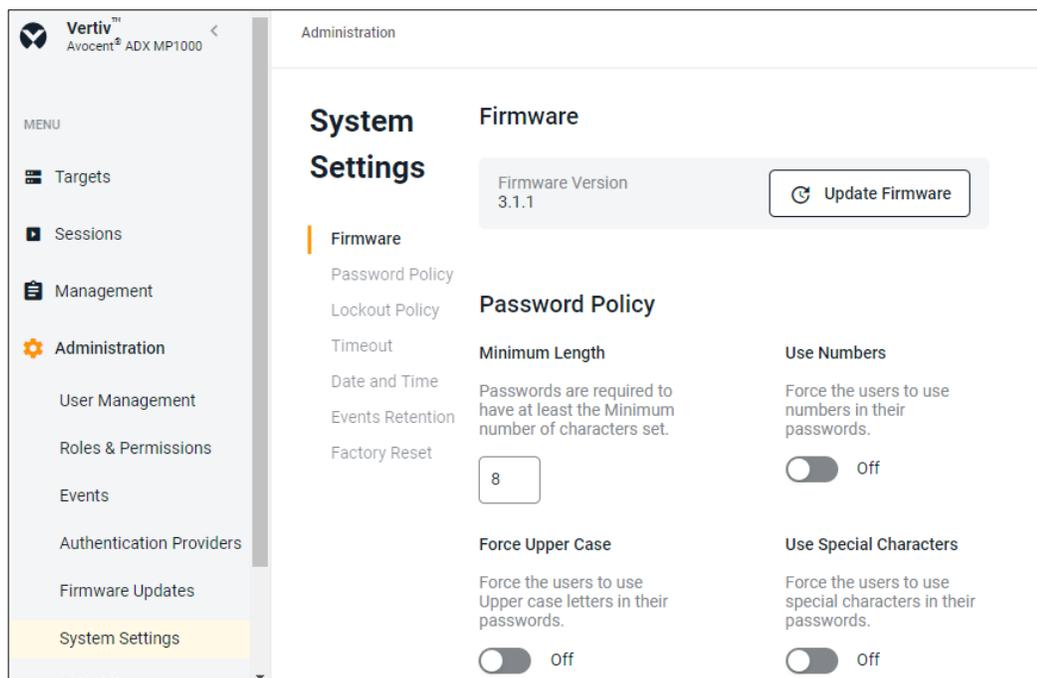
6. Select the firmware file and click *Update*.

2. Appliance Firmware Version Information

APPLIANCE/PRODUCT	VERSION	FILENAME
Vertiv™ Avocent® ADX MP1000 Management Platform	3.17.8	obsidian-3.17.8-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.

New Features

- The new Proxy feature allows network traffic for a remote target device session from a browser client on port 443 to be redirected from the Vertiv™ Avocent® ADX MP1000 Management Platform to the appropriate Vertiv™ Avocent® ADX Ecosystem device. The Proxy feature may be enabled or disabled from the web user interface (UI); it is disabled by default.

  NOTE: The Proxy feature currently supports KVM and Serial sessions.

- The new Syslog feature allows events in the Event Viewer to be forwarded to a Syslog server. This capability allows you to configure the Syslog server in the web UI and also disable connection to it.

- The new Appliance view displays the list of appliances and connected targets in a hierarchical format and allows you to search for and access details about both.

- The new Dashboard view allows you to view and create pages that include content side-by-side on a single screen. This capability allows you to perform the following operations:

  - View static images for multiple KVM, serial, virtual machine and SSH sessions on a single dashboard page.

  - Launch sessions (KVM, serial, virtual machine and SSH) from the Dashboard page.

  - Configure and arrange content on the Dashboard.

- The new SSL Certificate Replacement feature allows you to create a CSR request that can be sent to a certificate authority to obtain a signed certificate which may then be uploaded to a Vertiv™ Avocent® ADX MP1000 Management Platform appliance. For additional information on this process, see the release notes that accompany the Certificate Replacement Script.

Enhancements

- This release adds support for discovering Vertiv™ Geist™ rack Power Distribution Units (rPDUs) and then adding them to the Target List view. This capability allows you to perform the following operations:
  - View power consumption on the rPDU and perform power operations on rPDUs or rPDU outlets.
  - Merge rPDU outlets with other devices.
- This release adds IPMI protocol support for service processors (SPs). This capability allows you to perform power/reset operations, control LED status and monitor sensor information on targets that support IPMI functionality.
- With this release, the Event Name property of an event in the Properties panel is renamed to "Description".

Resolved Issues

- General issues resolved:
  - Fixed issue where there was no indication of the actual powered state of a virtual machine.
  - Fixed issue where some operations for a Vertiv™ Avocent® ADX IPIQ IP KVM device (control LED, restart, and reset, for example) could not be performed.
- Resource Group issues resolved:
  - Fixed issue where adding a device from the second page on the Resource Group list caused the device to be duplicated in the Resource Group list.
  - Fixed issue where a device could not be removed from a resource group.
  - Fixed issue where removing a target from a resource group caused the target to be removed from all other resource groups associated with the target.
- Serial issues resolved (serial appliances/ports/sessions):
  - Fixed issue where the links to launch a Vertiv™ Avocent® ACS advanced console system web page and Command Line Interface (CLI) were not available.
  - Fixed issue where the link to launch a serial session for a Vertiv™ Avocent® ACS advanced console system port was missing.
  - Fixed issue where you are allowed to delete an active Vertiv™ Avocent® ACS advanced console system serial session.
  - Fixed issue where the link to launch a KVM session was showing twice for a virtual machine.
  - Fixed issue where the KVM Viewer displayed an error when running in Full Screen and Single Cursor mode using Chrome, Firefox and Edge browsers.
  - Fixed issue where the statistics panel in the KVM Viewer showed resolution when there was no signal at startup.
  - Fixed issue where the KVM Viewer was not closing when clicking on the *Exit* button using Firefox version 105.
  - Fixed issue where the status bar showed as Inactive after successfully mapping a folder in a virtual media connection to a Vertiv™ Avocent® ADX IPUHD 4K IP KVM and Vertiv™ Avocent® ADX IPIQ IP KVM device.
- Service processor (SP) issues resolved:
  - Fixed issue where firmware upgrade was failing for Dell iDRAC8, Dell iDRAC9 and XCC SPs.
- Licensing issues resolved:
  - Fixed issue where an event was not being added to the event log when a license was added.
  - Fixed issue where an invalid license expiration notification value (such as 1 day) was being allowed.

- Resync issues resolved:
  - Fixed issue where a resync operation on an SP was adding a duplicate entry in the Target List view.
  - Fixed issue where the Resync option was being displayed incorrectly for Vertiv™ Avocent® ADX IPUHD 4K IP KVM and Vertiv™ Avocent® ADX IPIQ IP KVM devices.

- Configuration issues resolved:
  - Fixed issue where the date format for the 24-hour clock was incorrect under System Settings.
  - Fixed issue where changing user properties under User Management was not successful.
  - Fixed issue where the Prefix Length field could not be set to a number greater than 24 on the Static Network Configuration page.
  - Fixed issue where the destination port mapping setting was missing.
  - Fixed issue where changing the Network Configuration settings for a Vertiv™ Avocent® ADX RM1048P Rack Manager was generating an error message.
  - Fixed issue where the settings for a Vertiv™ Avocent® ADX IPIQ IP KVM device could not be modified.
  - Fixed issue where *Unknown* error was displayed after changing Credential Profile notes or DHCP settings.
  - Fixed issue where enabling the Vertiv™ Avocent® DSView management software "DSView Unit Group" mapping setting required toggling the ON and OFF option twice.
  - Fixed issue where the Security Profile settings for a Vertiv™ Avocent® ACS8000 advanced console system appliance did not match the settings on the On-board Web Interface (OBWI).

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® 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	2.22.1
Serial Viewer	2.15.1
Virtual Machine (VM) Viewer	1.9.1

8. Dashboard Support Information

ITEM	VERSION
Dashboard	1.10.1

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	2.82.82.82	Redfish, IPMI 2.0
Dell iDRAC9	5.00.00.00	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 v2.80	Redfish, IPMI 2.0
HP iLO 5	iLO 5 v2.71	Redfish, IPMI 2.0
Lenovo IMM2	TCOO60A 5.90	IPMI 2.0
Lenovo XCC	CDI394N 8.40	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	5.6.0

11. 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)

12. Known Issues and Limitations

This release contains the following known issues and limitations:

- SP issues:
    - 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:
    - 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 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.

- General issues:
  - 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® ACS800/8000 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.