Vertiv™ Avocent® ADX MP1000 Management Platform
Release Notes

VERSION 3.5.3, DECEMBER 2021

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. Server Processor Support Information
9. TCP Port Usage
10. 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 was provided with the platform.

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 www.vertiv.com/ADX-Management-Platform , select the *Documents & Downloads* tab, then select the Management Platform software downloads link.

2. Download the new firmware and save it to your local computer, FTP, HTTP or TFTP server.

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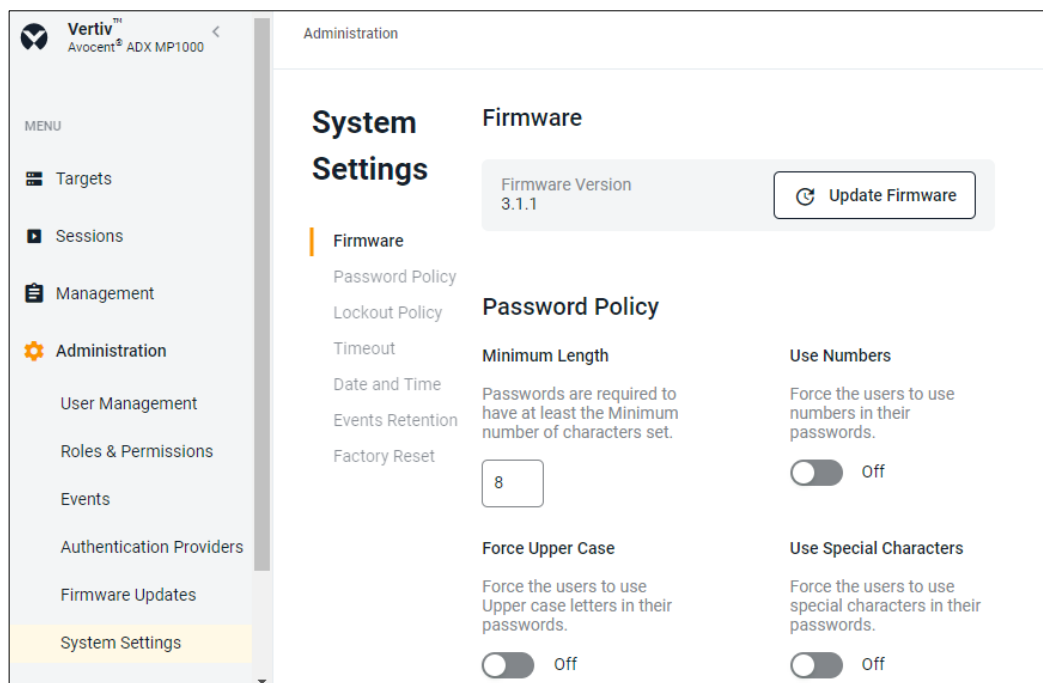
6. Select the firmware file and click *Update*.

2. Appliance Firmware Version Information

APPLIANCE/PRODUCT	VERSION	FILENAME
Vertiv™ Avocent® ADX MP1000 Management Platform	3.5.3	docker-image-obsidian-3.5.3-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:

- Service processor (SP) enhancements:
    - Added support for managing server processors subtending from a managed Vertiv™ Avocent® ADX RM1048P Rack Manager; you can access service processors managed within the rack manager's private IP network.
    - Extended support via Redfish for XCC, ILO4 and Vertiv™ ACI-based OpenBMC service processors.
    - Added firmware update capability for service processors.
- New feature support for Vertiv™ Avocent® UMIQ-v2 modules converted to operate as a Vertiv™ Avocent® ADX IPIQ IP KVM device:
  NOTE: See the Device Support section of this release note for more information.
    - Added support for managing converted Vertiv™ Avocent® UMIQ-v2 modules subtending from a managed Vertiv™ Avocent® ADX RM1048P Rack Manager. With this new feature, you may:
        - Launch KVM sessions from the web UI.
        - Support VMedia from an IQ session.
        - Operate with the converted Vertiv™ Avocent® UMIQ-v2 module as an auto DHCP-addressable Vertiv™ Avocent® ADX IPIQ IP KVM device.
        - Update the IQ firmware.
        - Support a location LED.

- KVM Viewer enhancements:
  - Added support for remote audio from a Vertiv™ Avocent® ADX IPUHD 4K IP KVM device with recording capabilities.
  - Improved general web UI usability (for example, pop-ups were removed) and updated the Viewer to the latest version.
- Web UI enhancements:
  - Added the ability to change the hostname, DNS nameservers and the domain name in order to support FQDN services
  - Improved resource group management
- General enhancements:
  - Enhanced diagnostics overall (for example, the show and save logs functionality was improved)

Resolved Issues

- Virtual Machine Viewer now able to be launched to VMs that are not part of vCenter.

- NAT routes now modified when managing a Vertiv™ Avocent® ADX RM1048P Rack Manager.

- Adding a target to a user group no longer fails Fine-Grained Authorization (FGA).

- Location and Asset tags are no longer cleared after a management platform firmware update.

- Changed VM Sync to better handle event messages from VMWare.

- Removed support for SSL protocol versions earlier than TLS 1.2 (TLS 1.2 and 1.3 supported).

- Removed Port 8880.

- Improved credential UX and changed the credential API endpoint.

- Adjusted system roles to now be able to bulk delete.

- The sp-management service is now updated to not delete the SP log and to also include the power control type (in Status).

- Adjusted the KVM Viewer window to now close after a reconnection attempt fails.

- Corrected issues with Administration/System Settings- Password Expires and the Password Expiration Reminder; both are now functional.

- Fixed issue where changing the bonding port settings results in the Vertiv™ Avocent® ADX MP1000 Management Platform not being able to enroll a Vertiv™ Avocent® ADX RM1048P Rack Manager.

- Fixed issue with the serial output during the re-imaging of the management platform.

- Fixed issue where factory reset was exposed in the web UI of the Vertiv™ Avocent® ADX MP1000 Management Platform.

- Fixed issue where opening the KVM Viewer after a rack manager re-enrollment sometimes took up to 10 minutes.

- Fixed issue where a managed Vertiv™ Avocent® ADX RM1048P Rack Manager firmware update via a new managed device link page previously failed with an error message. Now, a managed rack manager firmware update via a Managed Devices 2 DOT link passes and works as designed.

- Fixed issue where the Add Group dialog box did not actually assign the users to the group. Clicking the Select All checkbox in the Add Group dialog box now assigns the users to the group.

- Fixed issue where the user was unable to launch a KVM Session to a target without view permissions to the associated rack manager.

- Fixed issue where the Add Group to Group option from within an existing resource group launches a modal to select from existing resource groups.

- Fixed API call used to retrieve password expiration value.

- Fixed issue where no content was displayed in the mapped drive after mapping the VMedia folder.

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® 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 RM1048P Rack Manager 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	96	79+
Firefox	94	35+
Chrome	96	40+
Safari	15	12+

7. Viewer Support and Version Information

The following table lists browser/viewer combinations successfully tested with a representative selection of client operating systems.

Tested Browser and Viewer Combinations (64-bit versions)

CLIENT SYSTEM	HTML5 KVM VIEWER SUPPORT?	VIEWER VERSION
Chrome	YES	2.6.1
Firefox (Windows Client)	YES	2.6.1
Firefox (Linux Client)	YES	2.6.1
Firefox (Mac OS Client)	YES	2.6.1
Microsoft Edge	YES	2.6.1
Safari	YES	2.6.1

8. Server Processor Support Information

Tested Service Processors/Servers and Firmware

SERVICE PROCESSOR	FIRMWARE VERSION
Dell iDRAC7	2.65.65.65
Dell iDRAC8	2.75.75.75
Dell iDRAC9	3.30.30.30
HP iLO 4	iLO 4 v2.30
HP iLO 5	iLO 5 v1.40
XCC	CDI346L 3.60 2020-01-02
ACI	v4.1-2021-r07

9. TCP Port Usage

NOTE: TCP port usage is bidirectional unless otherwise noted

PORT	TYPE	DESCRIPTION
443	TCP	General Communications (TCP)
22	TCP	General Communications (TCP)

10. Known Issues and Limitations

This release contains the following known issues:

- VM sessions are not cleared after exiting the viewer.

- The Virtual Machine Viewer Caps Lock (and other keys) are not highlighting when using Linux; this is not supported in VMWare.

- The SP virtual media connection sync is not functional.

- The changed time [from the Command Line Interface (CLI)] is not maintained through a reset. BIOS overrides time and must be set via BIOS.

- The Kingston USB in the front panel is not recognized and is causing the Boot Manager to not display.

- The default system roles (User-Role, User-Administrator-Role and System-Maintainer-Role) do not include access to service processors.

- 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.

- A Vertiv™ Avocent® ADX MP1000 Management Platform enrolling a Vertiv™ Avocent® ADX RM1048P Rack Manager does not require an account and password but is still accessible in the web UI. The Vertiv™ Avocent® MP1000 Management Platform can enroll a Vertiv™ Avocent® ADX RM1048P Rack Manager with an invalid account/password.

- SP version not updated after the SP firmware is updated.

- Error adding target to user group: SQL error.

- Unable to launch a KVM Session to a target without view permission to the associated Vertiv™ Avocent® ADX RM1048P Rack Manager; users must have access to modify the rack manager.

- No access is given to archived Events.

- iLO5 SP issue: Cannot control the power state of the server.

- Clicking the SP name link (hyperlink) on the Target page produces error messages.

- From the API, the Vertiv™ Avocent® ADX RM1048P Rack Manager does not register, so "is_registered" parameters remain "false" after enrollment into the Vertiv™ Avocent® ADX MP1000 Management Platform.

- Enrollment issue: If adding a rack manager to the management platform fails, it is displayed in Unmanaged Devices but is still listed as a target.

- Deleting an unmanaged rack manager in the management platform does not trigger the rack manager to go into standalone mode; it must be done manually.

- Opening the KVM Viewer after rack manager re-enrollment may cause the KVM viewer to produce a 500 server message while authorization is being initialized.

- Session Timeout modifications do not take effect until a logout occurs; no message is forthcoming.

- The HTML5 KVM Viewer displays an incorrect resolution due to Windows 10 interaction for resolutions set as static 3840 x 2160.

- With the option to add a resource group to a resource group, there are only options to add existing resource groups.

- Power Control is non-functional for unlicensed VMWare targets.