Avocent® ADX MP1000 Management Platform

Installer/User Guide

The information contained in this document is subject to change without notice and may not be suitable for all applications. While every precaution has been taken to ensure the accuracy and completeness of this document, Vertiv assumes no responsibility and disclaims all liability for damages resulting from use of this information or for any errors or omissions. Refer to other local practices or building codes as applicable for the correct methods, tools, and materials to be used in performing procedures not specifically described in this document.

Technical Support Site

If you encounter any installation or operational issues with your product, check the pertinent section of this manual to see if the issue can be resolved by following outlined procedures.

Visit https://www.vertiv.com/en-us/support/ for additional assistance.

TABLE OF CONTENTS

1 Getting Started

1.1 Product Overview

The Vertiv™ Avocent® ADX MP1000 management platform is a secure centralized enterprise management solution that allows you to remotely access, manage, monitor and control target devices through managed appliances. You can also launch a session to a target device with a single point of access. The Avocent ADX MP1000 management platform provides simplified management and control of both virtual and physical infrastructure. It provides efficient, secure, and auditable access to devices for your IT operators.

Figure 1.1 Avocent ADX MP1000 Management Platform Description

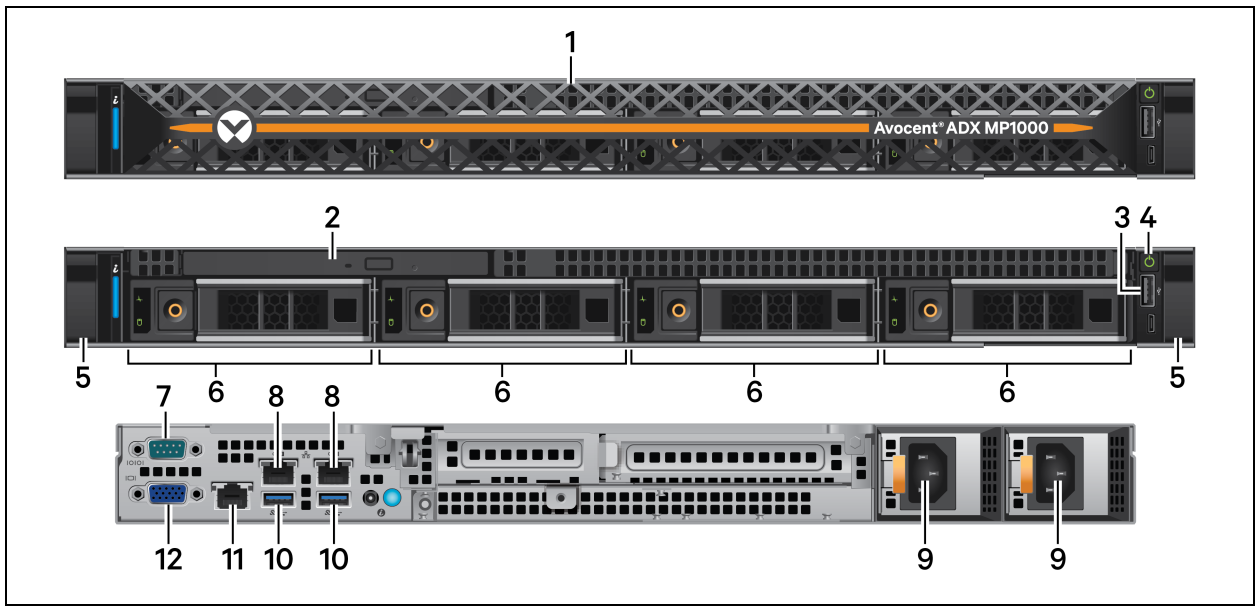


Table 1.1 Avocent ADX MP1000 Management Platform Description

Item	Description	Item	Description
1	Removable front bezel	7	Console port
2	Optional optic drive	8	1G uplink ports
3	USB 2.0 port	9	Redundant dual power supplies
4	Power button	10	USB 3.0 ports for mouse and keyboard
5	Release latch	11	Management port
6	3.5 in. hard drive bays	12	VGA port

1.2 Features and Benefits

The Avocent ADX MP1000 management platform provides the following benefits for your data center:

- Provides and combines control of your KVM over IP, service processor, and virtual machine devices to manage your entire infrastructure across enterprise and edge sites.
- Designed for scalability so that you can easily scale from small to large and uniform complex infrastructure with a single management platform.
- Simplifies your infrastructure and improves productivity with automation of deployment and configuration tasks on your IT equipment.
- Improves efficiency by standardizing your management of service processors and using a common set of APIs to manage your entire IT infrastructure.
- Enhances security with centralized firmware updates and safeguarded access to your IT devices.
- Minimizes service disruption by being able to always remotely access your IT infrastructure.
- Control and restrict operations to your devices and keep track of detailed user history.
- Minimizes downtime for upgrades.

1.3 Installation and Initial Setup

For installation and initial setup instructions, see the Avocent ADX MP1000 management platform Quick Installation Guide provided with your Avocent ADX MP1000 management platform. This document is also available on the Avocent ADX MP1000 management platform product page.

To navigate to the product page:

1. Go to www.Vertiv.com.
2. On the Search bar, type ADX and press Enter.
3. Click on *Vertiv™ Avocent® ADX MP1000 Management Platform*.
4. Scroll down and click on *Documents & Downloads tab*.
5. A list of Manuals will be displayed. Click on *Vertiv™ Avocent® ADX MP1000 Management Platform Quick Installation Guide*. The PDF file will open in the new tab.

To navigate to the Release Notes page for Vertiv™ Avocent® ADX IPIQ IP KVM Device:

1. Go to www.Vertiv.com.
2. On the Search bar, type ADX and press Enter.
3. Click on *Vertiv™ Avocent® ADX IPIQ IP KVM*.
4. Scroll down and click on *Documents & Downloads tab*.
5. Scroll down and click on link for *Vertiv™ Avocent® ADX IPIQ IP KVM Software Downloads*.

1.3.1 Assigning an IP address

The Avocent ADX MP1000 management platform uses the IP addresses to uniquely identify itself to IP-based target devices. It supports both Dynamic Host Configuration Protocol (DHCP) and static IP addresses.

NOTE: An IP address is always obtained via DHCP.

For the first time, you will need to access Avocent ADX MP1000 management platform via its console menu to view the DHCP assigned IP address or configure a static IP address.

To view or configure the IP address of the Avocent ADX MP1000 management platform:

1. From the console menu, login using *admin* as the username and password. You are prompted to change the password.
2. Select the option to show or configure network settings.
3. Select the *eno1 option*.

NOTE: The IP address assigned by the DHCP server is visible once this option is selected. The address can be entered into a web browser to access the web User Interface (UI).

4. To assign a static IP address, select the applicable option and follow the on-screen prompts to configure the IP, subnet, and gateway.
5. Type **0 (zero)** and press **Enter** to exit the main menu.
6. Select the option to reboot the Avocent ADX MP1000 management platform.
7. Once the Avocent ADX MP1000 management platform reboots, enter the static IP address to access the web UI.

NOTE: For information on configuring your network from the web UI, see Network Configuration on page 32.

This page intentionally left blank

2 Web User Interface (UI)

Once you have connected the Avocent ADX MP1000 management platform to a network and configured its IP address, you can access the Avocent ADX MP1000 management platform with its web UI. The web UI provides direct access to the Avocent ADX MP1000 management platform and its appliances.

The web UI is compatible with the latest 32-bit and 64-bit versions of the following web browsers:

- Google Chrome.
- Microsoft Edge.
- Apple Safari.
- Mozilla Firefox.

To login the web UI:

1. Open a web browser to the address of the Avocent ADX MP1000 management platform https://<appliance.IP> using the IP address for eno1 you configured from the console menu.
2. At the login screen, enter your username and password.
3. Once you login, the Targets List screen will appear.

Figure 2.1 Web UI Overview

Table 2.1 Web UI Overview Descriptions

Item	Description
1	Sidebar
2	Content Area
3	User Preferences

2.1 Targets

When logging into the Avocent ADX MP1000 management platform, the Targets List screen displays a list of targets connected to the Avocent ADX MP1000 management platform.

The following target types can be managed:

- IP KVM devices.
- Service processors.
- Virtual machines.
- Serial devices.
- RM1048P rack managers.

You can manage targets from the Avocent ADX MP1000 management platform through a Vertiv™ Avocent® ADX RM1048P rack manager and then enroll the rack manager into your Avocent ADX MP1000 management platform. You can also discover and manage KVM devices connected via a Vertiv™ Avocent® ADX IPIQ IP KVM device or Vertiv™ Avocent® ADX IPUHD 4K IP KVM device. Serial devices can be discovered and managed via an Vertiv™ Avocent® ACS 800/8000 Advanced Console System. The Avocent ADX MP1000 management platform can manage service processors logically over the network or via an SP connected to an enrolled rack manager.

To enroll a single rack manager into the Avocent ADX MP1000 management platform:

1. From the Management screen, click the *plus (+) icon*.
2. Click *Add Device*.
3. Enter the IP address for the rack manager and click *Add Device*. You can also assign a name to the rack manager from this screen.

To discover a range of rack managers:

1. From the Management screen, click the *plus (+) icon*.
2. Click *IP Range Discovery*.
3. Use the IP From and IP To fields to enter a range for your rack managers to be discovered on the network.
4. Click on the checkbox to add and manage the discovered rack managers. If checked, all discovered rack managers are automatically added to the list as managed devices.
5. Click *Start Discovery*.

NOTE: It may take 10-15 minutes for the rack manager to be fully enrolled. Once it is fully enrolled, the rack manager and all its targets are visible in the web UI of the Avocent ADX MP1000 management platform.

NOTE: Once enrolled, a rack manager is only accessible from the web UI of the Avocent ADX MP1000 management platform. To access a rack manager from its own web UI again, you will have to unenroll the rack manager from the Avocent ADX MP1000 management platform.

To unenroll a rack manager:

1. From the Management screen, move your mouse to the row with the rack manager you want to delete and click the checkbox next to the rack manager.

   -or-

   Click the *ellipses* at the far right of the row with the rack manager you want to delete.

2. Click the *Delete icon*.

NOTE: It may take 10-15 minutes for the rack manager to unenroll from the Avocent ADX MP1000 management platform.

Connected targets display in a table in the content area. Click the *vertical ellipses icon* to configure the table.

To add a single target:

1. From the Targets List screen, click the *plus (+) icon*.
2. Click *Add Device*.
3. Enter the IP address for the device and click *Add Device*. You can also assign a name to the target.

To discover a range of targets:

1. From the Targets List screen, click the *plus (+) icon*.
2. Click *IP Range Discovery*.
3. Use the IP Start and IP End fields to enter a range for your targets to be discovered on the network.
4. Use the drop-down menu to select the type of target and enter your username and password in the appropriate fields.

   -or-

   For service processors and virtual machines, use the drop-down menu to select your credential profile. For more information, see Credential Profile on page 25.
5. Click on the checkbox to add and manage the discovered devices. If checked, all discovered devices are automatically added to the list as managed devices.
6. Click *Discover*.

NOTE: For service processors and virtual machines, you are required to enter the credential profile to add or discover it.

2.1.1 Target properties

To view target properties and network configuration:

1. Click a *target* to open its properties sidebar.
2. Click the *Edit icon* to change the name or serial number of the target.

2.1.2 Merge targets

You can merge multiple target devices into a single merged target device. This provides you a convenient method to launch actions on a set of targets that are really the same target. You can merge KVM, SP, and serial targets. You cannot merge virtual machines.

The user can now merge all the outlets on a Vertiv™ Geist™ rPDU, and power operations are now included in the user's overall activities.

To merge targets:

1. From the Target List screen, select the targets you want to merge by hovering your mouse over each target and clicking the box to the left of each one.
2. Click *Merge Targets*, then click *Apply*.

A plus (+) icon displays to show the merged targets. Click the icon to expand the merged target and show each individual target.

To unmerge targets:

1. Click the checkbox next to the merged target.
2. Click the *Unmerge icon* to unmerge all the targets.

   -or-

   If you have more than two targets merged, click the *vertical ellipses* next to the individual target you want to unmerge and click *Unmerge* to remove just that target.

2.1.3 Resource groups

Resource groups may be used to organize your targets. You may create nested resource groups (groups within groups) to organize targets hierarchically. Targets may belong to multiple groups.

Nested groups

To create a resource group:

1. From the Resource Groups screen, click the *plus (+) icon*.
2. Enter a name for your resource group.
3. Click a target to add it to the group.

   -or-

   Check the *Select All box* to add all targets to the group.

NOTE: You can use the search field to filter targets.

4. Click Add *Resource Group* when you are finished adding targets.

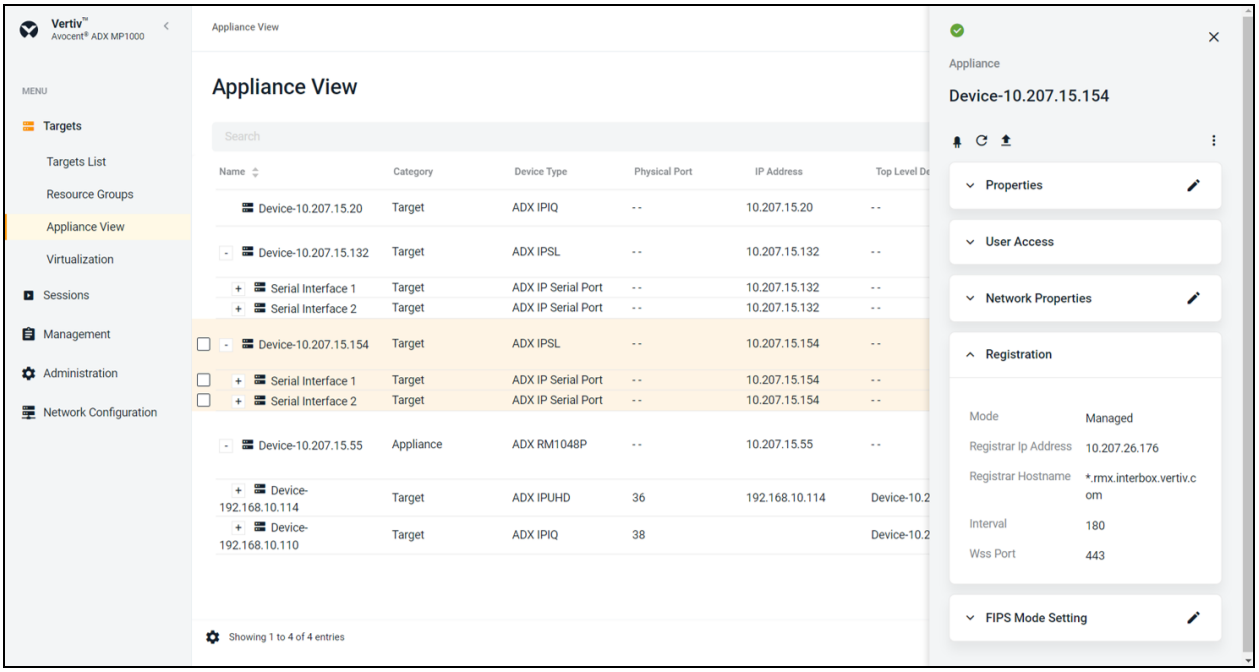
To delete a resource group:

You can either click the *vertical ellipses* to the right of the group or click the checkbox next to the group folder and then click the *delete icon*. You can delete multiple groups at the same time by checking the boxes next to the group name and then clicking the *delete icon*.

2.2 Appliance View

Appliance view organizes the devices under the appliance they are physically or logically associated. This includes RM1048P, Geist™ Rack PDUs, DSView™, ACS Appliance, IPIQ, IPUHD, and Virtualization. The devices by default are sorted by Port number. Appliance View can perform the same operations as Target List such as launching a KVM session, etc. The only difference is that Appliance View organises the devices to the apparent appliance that they belong to.

Figure 2.2 Appliance View Overview



To navigate to the Appliance View, follow the below steps:

1. From the Targets screen, select *Appliance View*.
2. The Appliance View screen shows the list of devices that are added to the Target List.
3. Click the *plus (+) icon* and it shows the list of appliances that are physically connected to the rack manager.
4. Click on any device in the Targets List, and the information of the device is displayed on the right-side panel that is listed below:
    - Properties.
    - User Access.
    - Network Properties.
    - Registration.
    - FIPS Mode Setting.
5. Click on the *drop-down arrow* for detailed information.

To launch a KVM session, follow the below steps:

1. Click on the *play icon* to the right of the individual device you want to launch a KVM session.
2. A pop-up message Connecting to KVM Viewer will be displayed.
3. A KVM session is launched in a new tab.

To delete a device from the Appliance View, follow the below steps:

1. Click on the *vertical ellipses* next to the individual device you want to delete.
2. It shows the below-listed options:
    - Delete.
    - Resynchronization.
    - Firmware Update.
3. Click the *Delete icon*.

2.3 Vertiv™ Geist™ Rack Power Distribution Units (rPDU)

A Geist™ Rack Power Distribution Unit (rPDU) is a device for controlling electrical power in a data center. Geist™ rPDU is basically a power strip designed to provide standard electrical outlets for data center equipment.

Avocent ADX MP1000 management platformcan manage Geist™ rPDUs to provide the following features:

- View power consumption.
- Provides the ability to power cycle devices (Power Off, Power On, and Cycle).

To add a Geist™ rPDU into the Avocent ADX MP1000 management platform, follow the below steps:

1. From the Targets screen, select *Targets List*.
2. Click the *plus (+) icon* and click *Add Device*.
3. Enter the IP address for the Geist™ rPDU. You can also assign a name to the Geist™ rPDU from this screen.
4. Click *Add Device*.

To discover a range of Geist™ rPDU, follow the below steps:

1. From the Targets screen, select *Targets List*.
2. Click the *plus (+) icon* and click *IP Range Discovery*.
3. Use the IP Range *Start* and *End* fields to enter a range for your Geist™ rPDU to be discovered on the network.
4. Using the drop-down, enter the Device Type and Credentials (Username and Password).
5. Click *Discover*.

NOTE: When the Geist™ rPDU is added to the Targets List, it will appear in the Appliance View as the Geist™ rPDU. If you expand that, 42 entries with their respective port numbers will be displayed.

To manage and control a Geist™ rPDU, follow the below steps:

1. Click on the *vertical ellipses* next to the individual Geist™ rPDU.
2. It shows the below-listed control functions:
    - Power Off.
    - Power On.
    - Power Cycle.
3. Click on appropriate option to manage and control the device.

2.4 Dashboard

Dashboard feature allows the user to launch multiple KVM sessions simultaneously into one dashboard. This feature supports sessions for Vertiv™ Avocent® ADX IPUHD 4K IP KVM device (KVM preview).

Capabilities - This feature has the capability to:

- View multiple previews in one view.
- Drag and drop.

Value - This equipment provides below benefits:

- Reduce time to provision systems remotely.
- View system health in a NoC.
- Improve the productivity of test teams.
- Single dashboard to remotely manage IT.

To launch a dashboard, follow the below steps:

1. From the Targets screen, select *Targets List*.
2. Select the *checkbox* to the left of the individual device in the Targets List.

NOTE: The user can select one or more devices to launch a dashboard.

3. Click on the *play icon* (Launch Dashboard) at the top. The Dashboard is launched in the new tab in the preview mode.
4. The Dashboard window displays widgets in the preview mode for the number of devices that are virtually connected through KVM.

NOTE: The dashboard feature will update every 7 to 10 seconds.

5. In the Dashboard screen, you can access the following features:
    a. Click on *play icon* to launch a live KVM session.
    b. Click on the *full screen icon* to expand the screen to full screen.
    c. Click on the *delete icon* to remove the widget from the dashboard.
    d. Click on the checkbox for Maintain Aspect Ratio to get the desired aspect ratio for the widgets.
    e. Click on the *drop-down arrow* to the right of the Maintain Aspect Ratio checkbox to re-size the configuration of the dashboard.

2.5 KVM Management

The Avocent ADX MP1000 management platform provides flexible, centralized control of data center servers and virtual media of remote branch offices where trained operators may be unavailable. KVM over IP gives you flexible target device management control and secure remote access from anywhere at anytime.

The KVM over IP functionality of the appliance provides enterprise customers with the following features and options:

- Keyboard, video, and mouse (KVM) capabilities, configurable for digital (remote) connectivity.
- HTML5 KVM Viewer.
- Serial Viewer.
- Session management.
- Session sharing.
- Screen capture.
- Screen recording.
- Control over color depth.
- Zoom.
- Virtual keyboard.
- Copy and paste.
- Network bandwidth optimization.
- Macros.
- Virtual media.

Table 2.2 KVM Viewer Feature Compatibility

Feature	Menu	Google Chrome	Microsoft Edge (Chromium Based)	Mozilla Firefox	Apple Safari
Recording	Tools -> Start Recording	✓	✓	✓	×
Create ISO image	Tools -> Create Image or drag and drop in canvas	✓	✓	×	×
Map files and folders as ISO image	Virtual Media -> Map ISO image or drag and drop in canvas	✓	✓	×	×
Map removable disk or floppy disk images by drag and drop	Virtual Media -> Map Removable Disk/ Floppy Disk image	✓	✓	×	×

Table 2.3 Feature Comparison for Vertiv™ Avocent® ADX IPUHD 4K IP KVM Device and Vertiv™ Avocent® ADX IPIQ IP KVM Device Viewer

Feature	Stand-Alone Vertiv™ Avocent® ADX IPUHD	Avocent ADX MP1000/ Vertiv™ Avocent® ADX RM1048P (IPUHD)	Avocent ADX MP1000/ Vertiv™ Avocent® ADX RM1048P (IPIQ)
Option to play server-side recorded file (File -> Open Server-side Recording File)	✓	×	×
Video Noise Filter (View -> Audio and Video Options)	✓	✓	×
Video Lane Settings (View -> Audio and Video Options)	✓	✓	×
Remote Audio Support (View -> Audio and Video Options) Tools -> Remote Audio)	✓	✓	×
Max Resolution Settings (View -> Max Resolution)	✓	✓	×
User Information (View -> User Information)	✓	×	×
Instant Message (Tools -> Instant Message)	✓	×	×
Optimize Network Bandwidth (Tools -> Optimize Network Bandwidth)	✓	✓	×

2.5.1 Video viewer

The Avocent ADX MP1000 management platform is used to conduct a KVM session with one or more target devices attached to one or more KVM switches. When you connect to a device using the Avocent ADX MP1000 management platform, the target screen appears in a new window. The Avocent ADX MP1000 management platform allows you to control the target server in person remotely. When you connect to the Avocent ADX MP1000 management platform, your session can be confined to a window on your desktop or expanded to fit your entire desktop. You can manage computer settings, access files, and launch virtual media sessions from the client.

You can use the menu located at the top of the window to access features such as screen capture, refresh, and virtual keyboard. Although you can use the virtual keyboard to enter text to the target server, you can use the macros feature to send multi-key commands to make sure the command string is accurate. Depending on the operating system selected in the Macros settings, the command options will change. You can also configure settings of the Avocent ADX MP1000 management platform using the *Settings* icon.

2.5.2 HTML5 session

The web-based HTML5 Video Viewer is compatible with the latest versions of the following browsers:

- Google Chrome.
- Microsoft Edge.
- Apple Safari.
- Mozilla Firefox.

To launch an HTML5 session, you must have assigned rights or belong to a user group with assigned rights.

2.5.3 Launching an HTML5 video viewer session

Using the Web (UI), you can connect to each target, access target server files, manage software updates, and execute operating system commands. Each target server has a device information panel that contains data about the device.

NOTE: You may need to disable your browser's pop-up blocker to launch an HTML5 session.

To launch a video viewer session:

1. From the sidebar of the Avocent ADX MP1000 management platform, click *Targets List*.
2. Hover your mouse over the row with the target you want to access and click the *Launch Session icon*.

   -or-

   Click on the target you want to access to open its properties sidebar. Then click the *Launch Session icon*.

To close a video viewer session:

Click the *user icon* in the upper right-hand corner and select *Exit Viewer*.

Session sharing

When you connect to a target server that is currently being accessed by another user, the video viewer presents you with options that allow you to choose how to connect to the server. The four options include:

- Active Sharing - You, as well as other users, an interact with the target.
- Passive Sharing - Grants access to the target in read-only mode. The other user knows you are viewing the session.
- Preempt - Interrupts and terminates the previous user's session.
- Stealth - Grants access to the target as a viewer only. The other user does not know you are viewing the session.

If you are currently connected to a target server and another user attempts to share the session with you, the video viewer allows you to select how you want the user to connect. You have the option to:

- Approve.
- Reject.
- Allow as read-only.

Launching an exclusive HTML5 session

An exclusive connection is used when you need to access a target while excluding all other users. When a target is selected with the Exclusive Mode setting enabled, no other user in the system can switch to that target.

To enable an exclusive session:

Launch a session and click *Tools - Exclusive Mode*.

2.5.4 Video viewer menu

From the menu, at the top of the screen, you can configure your video viewer session.

File menu

From the File menu, you can copy text and paste it to the target. You can also open a server-side recording file.

View options

Click *View* to configure display options for the video viewer as well as enable full-screen and single-cursor modes. You can also view KVM statistics and display or hide the status bar at the bottom of the screen.

Video options

You can display more colors for the best fidelity, or fewer colors to reduce the volume of data transferred on the network. The choices range from Grayscale 16 Shades (maximum speed) to Color 24 bit (maximum video quality). You can also enable noise reduction for VGA or disable it for a digital video source.

To select a color depth for the video viewer:

1. From the toolbar, click *View*.
2. Click *Video Options*.
3. Use the slider to select the color depth.
4. Click the *radio button* to enable or disable noise reduction.
5. Click *Apply*.

Scaling

From the Scaling tab, you can adjust the appearance of the target's screen in the KVM Viewer by using the below options:

1. Enable *Maintain Aspect Ratio* to maintain the aspect ratio of the Target screen.
2. Select *Stretch to Window* to fit the Target screen to your display.
3. Select *Zoom* and use drop-down menu to select the zoom percentage of the display.

Max Resolution

From the Max resolution tab, you can select the maximum target resolution for your KVM session. This setting affects all sessions and remains until changed again.

NOTE: This setting causes a change of the actual video resolution on your target system's OS.

Macros

The Macros tab provides access to a list of supported operating systems that your target device may use. After you select the applicable operating system, you can access the list of command strings that are valid for the selected operating system.

NOTE: It is recommended that you use the macros feature to send a command string to a server. Using the macros feature when sending a command string such as Ctrl-Alt-Delete to a target device will not affect your client server. Selecting from the available keystrokes saves time and eliminates the risk of errors.

From the Macros section of the status bar, you can send a string of commands with one click to the target computer. The options in the drop-down list are predetermined based on the macro set you select by accessing the Macros tab. If you are looking for a command string that does not appear in the list, be sure to verify that you have the correct operating system selected in the Macro Manage drop-down list.

You can also define macros using the Manage Macros tab.

To send a command to the target computer:

1. Click the *Macros drop-down list* at the top of the screen and select a command string from the Static Macros list.
2. Click *Send*.

Tools

From the Tools tab, you can select the keyboard language, capture a screenshot, send an instant message, select the mouse mode, reset the keyboard and mouse, and enable a virtual keyboard. You can also enable exclusive mode, optimize network bandwidth and choose when to reduce the update rate.

Virtual Keyboard

When the Virtual keyboard is enabled, the keyboard is displayed on the client's workstation and can be positioned anywhere inside the window. The up and down directional arrows in the top right corner of the virtual keyboard are used to increase or decrease the size of the keyboard, respectively.

2.5.5 Virtual media

Use the virtual media feature on the client workstation to map a physical drive on the client machine as a virtual drive on a target device. You can also use the client workstation to add and map an .iso or .img file as a virtual drive on the target device.

Requirements

The virtual media feature has the following requirements:

- The target device must be connected to a KVM switch that supports virtual media with an IQ module that supports virtual media.
- The target device must be able to use the types of USB2 compatible media that you virtually map.
- If the target device does not support a portable USB memory device, you cannot map it on a client machine as a virtual media drive on the target device.
- The user (or user group to which the user belongs) must have permission to establish virtual media sessions and/or reserve virtual medial sessions to the target device.
- Only one virtual media session can be active on a target device at one time.

To map a virtual media drive:

1. In the virtual media section of the client navigational toolbar, click *Connect*.
2. After the virtual media session is activated, use the Virtual Media drop-down menu to select the type of file to map. Select *Map ISO image* to map an .iso file or select either *Map Removable Disk* or *Map Floppy Disk* to map an .img file.
3. Select a file from the Open dialog box with an .iso or .img file extension, depending on your selection in step 2, then click *Open*.

4. If you wish to limit the mapped drive to read-only access, click the *Read Only checkbox* in the Virtual Disk Management dialog box.

NOTE: If the virtual media session settings were previously configured so that all mapped drives must be read only, the Read Only checkbox will already be enabled and cannot be changed. You might wish to enable the checkbox if the session settings enabled read and write access, but you wish to limit a particular drive's access to read only.

5. Click *Map Drive*, then click *Close*.

NOTE: After a physical drive or image is mapped, it can be used on the target device.

To unmap a virtual media drive:

1. From the Virtual Media menu, click the mapped drive to unmap that drive.

   -or-

   Click *Deactivate* to unmap all the drives.

2. At the prompt, click *Yes* to unmap the drive.

2.6 Service Processor (SP) Access

The Avocent ADX MP1000 management platform and Vertiv™ Avocent® ADX RM1048P rack manager connects to the client server.

Capabilities - This equipment have the capability to:

- Access management web UI of the server.
- Launch embedded KVM viewer.
- Dynamic proxy to the server management interface.

Value - This equipment provides below benefits:

- Keeps the servers secure when connected to a private network.
- Provides multiple server space management options.
- Unrestricted yet secure access to server interface.

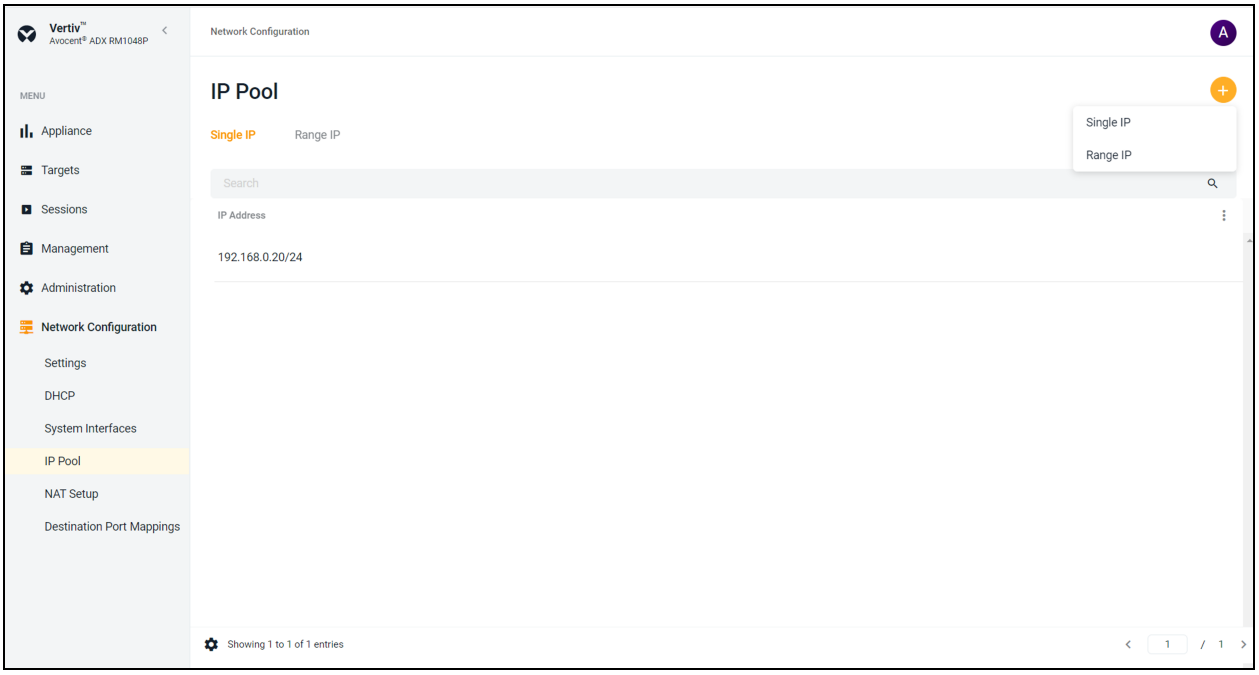
2.6.1 Configuring service processor web UI access

NOTE: To configure service processor web UI access on Vertiv™ Avocent® RM1048P rack manager, you should first navigate to the Vertiv™ Avocent® RM1048P rack manager from the Management menu in Avocent ADX MP1000 management platform web UI.

NOTE: To configure service processor web UI access, you must define IP Address Pool and Destination Port Mappings before launching the web UI session.

Defining an IP Pool

Figure 2.3 IP Pool Overview



To define an IP Pool, follow the below steps:

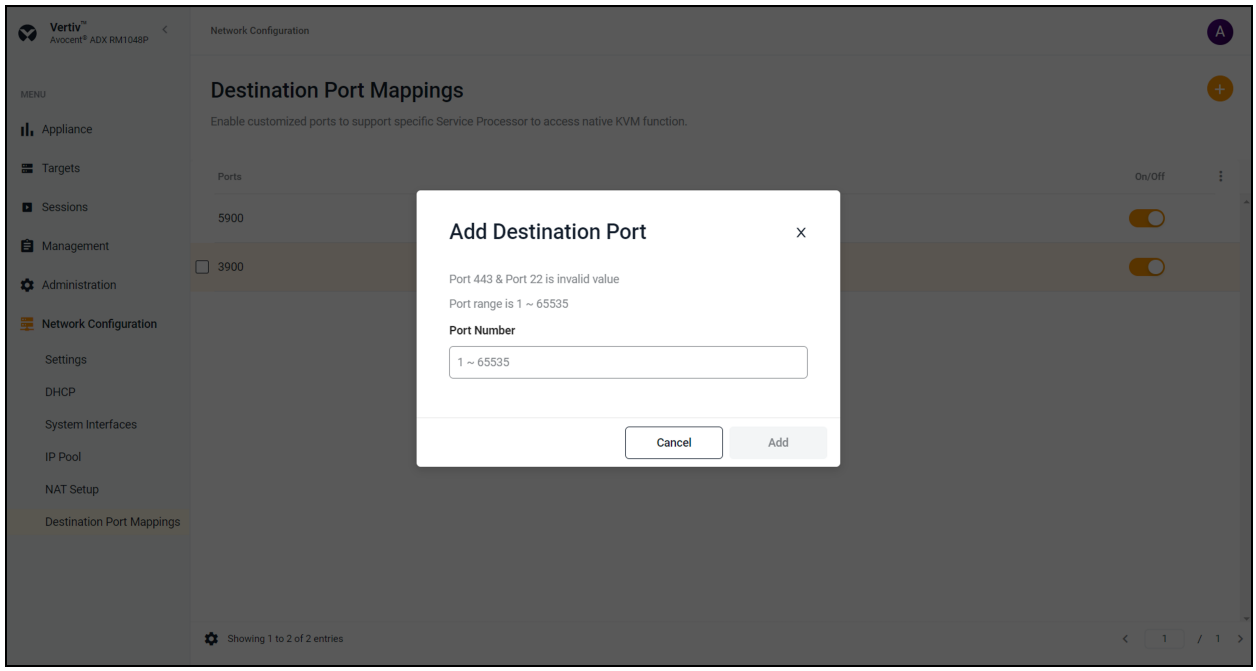
1. From the Network Configuration screen, select *IP Pool*.
2. Click the *plus (+) icon* for the below 2 options:
   - Single IP.
   - Range IP.
3. To add a single IP address, click on *Single IP*.
4. Enter the IP Address and click *Add*.
5. To add a range of IP address, click on *Range IP*.
6. Use the Range IP Value *From* and *To* fields to enter a range of IP addresses to be added to the network.
7. Click *Add*.

To delete an IP Pool, follow the below steps:

1. Click on the checkbox to the left of the pool.
2. Click the *vertical ellipses* to the right and click *Delete*.

Defining Destination Port Mappings

Figure 2.4 Destination Port Mappings Overview



To define the Destination Port Mappings, follow the below steps:

1. From the Network Configuration screen, select *Destination Port Mappings*.
2. Click the *plus (+) icon* and a window Add Destination Port will appear.
3. Enter the Port Number and click *Add*.

NOTE: The user has the ability to enable or disable the port by clicking on the On/Off button.

NOTE: The port must be enabled if the user needs to access vKVM.

To delete a destination port:

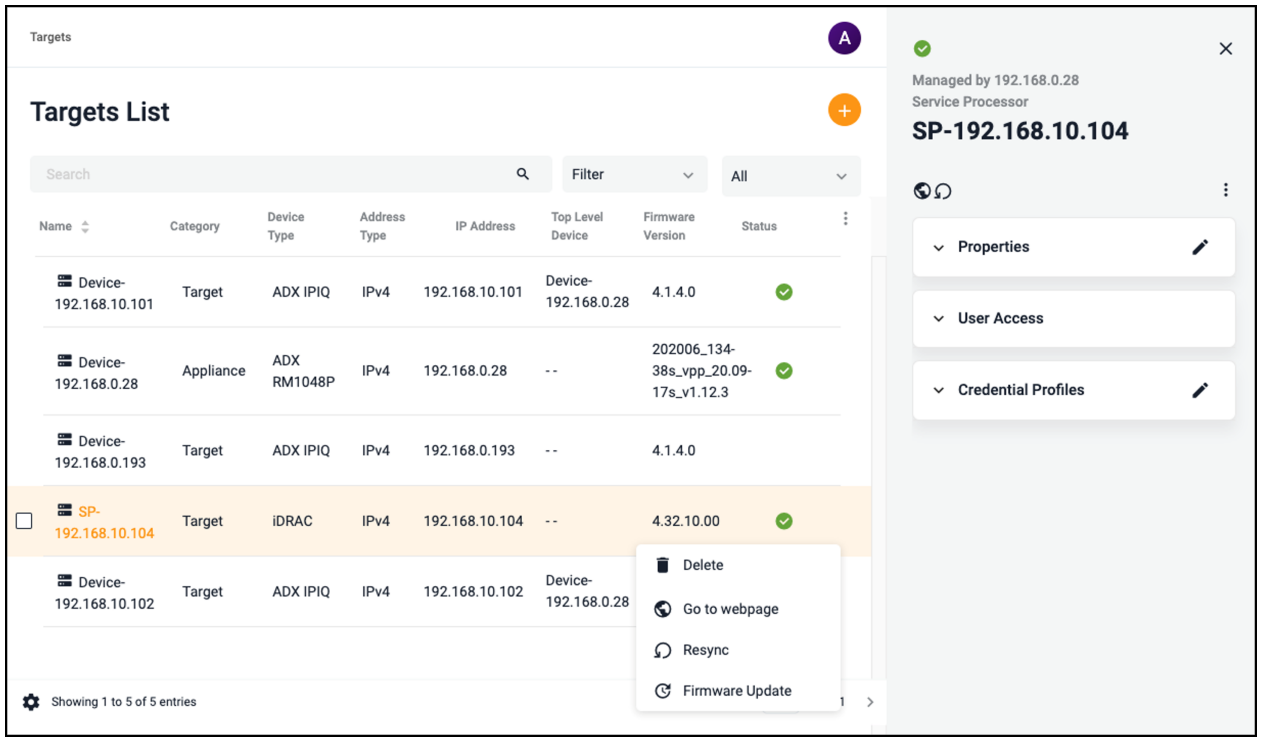
1. Click on the checkbox to the left of the port.
2. Click the *vertical ellipses* to the right and click *Delete*.

Table 2.4 Supported Processors/Servers for Launching KVM Sessions

Service Processor	Port
Dell iDRAC7	5900
Dell iDRAC8	5900
Dell iDRAC9	5900
HP iLO 4	5900 (Firmware<2.8) 443 (Firmware>2.8)
HP iLO 5	443
XCC	3900

Launching web UI session

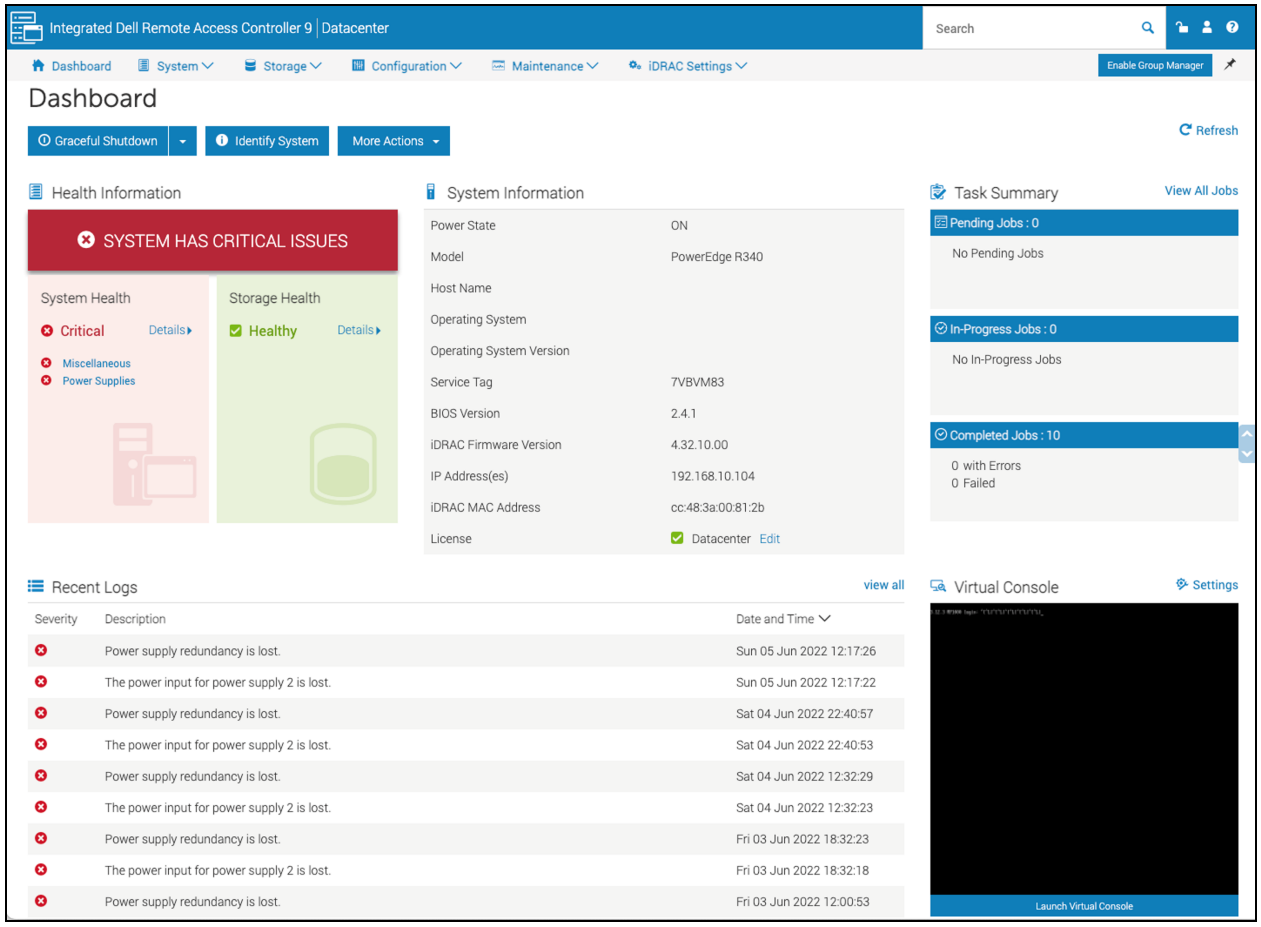
Figure 2.5 Launching Web UI Session



To launch the Web UI session, follow the below steps:

1. From the Targets screen, navigate to the Service Processor in the Targets List.
2. Select the management card (for example iDRAC) and click on the *Globe icon*.
3. Select *Go to webpage*.
4. Enter the Username and Password and click *Log In*.
5. The user is then navigated to the webpage of the device (iDRAC).

Figure 2.6 Webpage of the Device (iDRAC) Overview



2.7 Service Processor (SP) Management

A Service Processor (SP) can be connected physically via a rack manager or logically over a network to the management platform.

The Avocent ADX MP1000 management platform can discover SPs over the network, provided the SPs have an IP address and are connected to the same network as the management platform.

NOTE: Users that do not have Administrator access will only see devices to which they have access.

The Avocent ADX MP1000 management platform and Vertiv™ Avocent®ADX RM1048P rack manager support the following SPs:

- Dell iDRAC 7, 8 and 9.
- HPE iLO4 and iLO5.
- Lenovo XCC.
- OpenBmc.

2.7.1 Service processor metrics

Once discovered, an SP displays in the Target List with its SP type and IP address.

- Click an *SP* to view its metrics.
- From the Metrics screen, you can view the SPs status, temperature, fan speed, power, and properties.
- You can also upgrade the SP firmware and change the boot order.
- Drag and drop to re-arrange the boot order as desired. At the confirmation screen, click *Yes*, U*pdate*.

NOTE: SP reboot can be required for the re-order to take effect, depending on the model.

2.7.2 Service processor control

From the Metrics page, you can also control the LED and power functions of the SP as well as reboot the SP or go to the SP web UI.

- From the upper right-hand corner, click *LED* to view the LED controls. From here, you can turn the LED On or Off or make it blink.
- Click *Power* to view the power controls. From here, you can perform a graceful shutdown, turn off the system or power cycle the system.
- Click the *vertical ellipses* to view more control options. From here, you can reboot the SP or go to its webpage.

2.8 Serial Management

The Avocent ADX MP1000 management platform provides serial management via an Vertiv™ Avocent® ACS 800/8000 advanced console system and an Vertiv™ Avocent® ADX IPUHD 4K IP KVM device.

NOTE: The ACS console system should not be enrolled with any other platform, such as the DSView software, when enrolling with a Avocent ADX MP1000 management platform.

To launch a serial session:

1. From the Targets List screen, under Serial Interfaces, move your mouse over the device you want to access.
2. On the right of the column, click the *Launch Console icon* or Click the *vertical ellipses* and select whether to launch the serial session in a new tab or new window.

To end a serial session:

Click the *user icon* in the upper right-hand corner and select *Exit Serial Viewer*.

2.9 Administration

With Administrator login rights, you can access Administration screen, configure and manage the appliances and the associated targets.

2.9.1 User management

Access to ports can be optionally restricted, based on permissions an administrator can assign to custom user groups. The Avocent ADX MP1000 management platform has a default user of admin and four pre-defined user groups listed below:

- System-administrator.
- System-maintainer.
- User-administrator.
- User.

Users

When the Users tab is selected, all the users for the Avocent ADX MP1000 management platform are displayed.

To view more options in the Users tab:

- Click a *user* to open its properties sidebar.
- Click the *vertical ellipses* to the right of the device to change the selected user's password or delete or disable.

NOTE: From this sidebar, you can also view user properties and groups.

- Click the *Edit icon* to configure the user's name and email and enable account and password expiration rules.
- Click *Groups* to assign the user to groups.

To create a new user:

1. From the User Management screen, select the *Users* tab.
2. Click the *plus (+) icon* to add a new user.
3. Enter the full name, username, and temporary password for the user.
4. Click *Add User*.

To delete a user:

1. Click on the checkbox next to the user you want to delete.
2. Click the *Delete icon* above the list of users.
3. At the confirmation screen, click *Yes* to delete.

User groups

When the Groups tab is selected, all the groups for the Avocent ADX MP1000 management platform are displayed. A user group defines the view and what the user can do within the web UI and CLI, regarding appliance settings and administration.

To navigate more options in the Users groups screen:

- Click a *group* to open its properties sidebar.
- Click the *vertical ellipses* to delete the selected user group.
- Click *Group Properties* to view and configure the group. From here, you can name the group and assign both the pre-emption level and system role for the group.
- Expand the Users drop-down menu to view users assigned to the selected group.
- Click the *Edit icon* to assign more users to the group.

To create a new group:

1. From the User Management screen, select the *Groups* tab.
2. Click the *plus (+) icon* to add a new group.
3. Enter the name for the group and check the boxes for each user you want to add to the group.
4. Click *Add Group*.

To delete a group:

1. Check the box next to the group you want to delete.
2. Click the *Delete icon* above the list of groups.
3. At the confirmation screen, click *Yes* to delete.

2.9.2 Roles and Permissions

This screen displays the roles and permissions of the target and system.

NOTE: A permission is an individual operation a user can have on a target or system. A role is a collection of those permissions. A role is a convenient way to assign a set of permissions to a user group. Roles can also be assigned to the binding between users groups and resource groups.

- Target roles are a set of permissions applicable to a target device. For example, launching a KVM session.
- System roles are a set of permissions applicable to the Avocent ADX MP1000 management platform. For example, changing the password for a user on the Avocent ADX MP1000 management platform.

The Avocent ADX MP1000 management platform has four system roles by default as listed below:

1. System-Administrator.
2. System-Maintainer.
3. User-Administrator.
4. User-Role.

Click a *role* to open its properties sidebar.

To add a new role:

1. From the Roles & Permissions screen, select the *Target Roles* tab to create a target role.

   -or-

   Select the *System Roles* tab to create a new system role.

2. Click the *plus (+) icon*.
3. Enter a name and description for the role.
4. Click the checkbox to add desired permissions.

   -or-

   Click *Select All* to add all permissions.

5. Click *Add Role*.

To configure an existing role:

1. Click a *role* to open its properties sidebar.
2. Under the properties drop-down menu, click the *Edit icon* to configure the description for the role.
3. Under the permissions drop-down menu, click the *Edit icon* to configure the permissions for the role.

NOTE: The user cannot edit the properties and permissions of the four default system roles.

To delete a role:

1. Click the checkbox of the role you want to delete.
2. Click the *Delete icon*.
3. At the confirmation screen, click *Yes* to delete.

NOTE: The user cannot delete the four default system roles.

2.9.3 Credential Profile

NOTE: An administrator can view and create profiles to access your targets.

A credential profile stores the user ID and password for a single user and can be used across different target device types. Credential profiles are required for SPs. Before enrolling a rack manager with an SP, you must define the credential profile for each one with unique credentials.

To create a credential profile:

1. From the Administration screen, select *Credential Profile*.
2. Click the *plus (+) icon* in the upper right.
3. Create a name for the profile.
4. Add the username and password for the profile.
5. Click *Add credential profile*.

2.9.4 Events

When an event occurs, it is saved in the event log that can be viewed from the Events screen.

To navigate more options in an Events screen:

- Use the search bar to search for a specific event.
- Use the Filters drop-down menu to filter events by severity (info, warning or critical).
- Use the arrows next to each column to sort each event.
- Click on an event to open its properties sidebar.

2.9.5 Authentication Providers

From the sidebar, click to view a list of configured authentication providers.

You can Authenticate locally or through AD/LDAP. The Avocent ADX MP1000 management platform supports remote group authorizations for the LDAP authentication method.

NOTE: The authentication method configured for the Avocent ADX MP1000 management platform is used for authentication of any user who attempts to login through SSH or the web UI.

To add an authentication provider:

1. From the Authentication Providers screen, click the *plus (+) icon*.
2. Use the drop-down menu to select either LDAP or Active Directory (AD) as the authentication type.
3. Enter the configuration information for your authentication server.
4. If desired, use the slider to enable SSL mode to create a secure connection.
5. Under the Advanced heading, you can also configure user- and group-based searches.
6. When you are done, click *Add Provider*.

To configure an LDAP server

1. Use the slider to enable LDAP.
2. Enter the server address and server port in the appropriate fields. To add more than one server, click the *plus (+) icon*.
3. Select the binding method for the LDAP service. Using the login credential uses the Avocent ADX MP1000 management platform credentials. To configure different credentials, select *Use Configured Credential* and enter the username and password.
4. For search settings, enter the Base DN and UID attributes.
5. Click *Apply* at the bottom of the screen.

To delete an LDAP server:

Click the *Delete icon* under the Remove icon.

Active Directory

You can enable role-based security on the Avocent ADX MP1000 management platform, to map your Active Directory remote group to a role on the Avocent ADX MP1000 management platform.

NOTE: When you are mapped to any local role, and the related security is enabled and configured, Active Directory remote group provides you the related permission after login.

To enable role mapping:

1. From the LDAP screen, use the slider under Active Directory Settings to enable role-based security.
2. Click the *plus (+) icon*.
3. Enter the name of your Active Directory remote group in the appropriate field.
4. Use the drop-down menu to select the local role the remote group will be mapped with.
5. Click *Apply*.

To delete a role mapping:

Click the *Remove icon* next to the group you want to remove.

2.9.6 Firmware updates

From the Firmware Updates screen, you can view scheduled firmware updates. Click the *Refresh icon* to refresh the page.

For information on updating the firmware, see Firmware below.

2.9.7 System Settings

From the System Settings screen, you can view and configure system settings for the Avocent ADX MP1000 management platform.

Firmware

To update the firmware:

1. Download the new firmware from the product page at www.Vertiv.com.
2. Save the firmware to your local PC, FTP, HTTP or TFTP server.
3. On the Avocent ADX MP1000 management platform, from the System Settings screen, click the *Update Firmware icon*.
4. Select the firmware file and click *Update*.

Password Policy

You can configure global password rules for all the user accounts. Use the drop-down menus and sliders to set the global password policy. When the global password policy is update for enhanced security, all local user accounts will be flagged to change the password at next login.

You can also configure account expiration settings. Password with minimum eight characters and all other password expiration rules are default.

FIPS Mode Settings

The FIPS mode of operation can be enabled or disabled via the web UI and is executed after a reboot.

The FIPS mode of operation is disabled as default and needs to be enabled to change/update.

To enable or disable FIPS mode:

From the System Settings screen, under the FIPS Mode Settings, use the slider to enable or disable FIPS mode. The mode changes on the next reboot.

NOTE: The selected FIPS mode gets enabled even after performing a factory reset.

Lockout Policy

An administrator can configure global lockout rules to all user accounts. When lockout is enabled, a user will be locked out of the Avocent ADX MP1000 management platform.

By default, lockout is enabled on three failed login attempts and accounts are automatically unlocked after 20 minutes. The login retry timeout is disabled by default.

Timeout

An administrator can configure the global inactivity timeout for the application and the viewer. When the inactivity threshold is reached, the user session will be disconnected. By default, both the application and viewer timeout is enabled with a time limit of 30 minutes.

Date and Time

Shows the current date and time. You can use an NTP service or manually configure the date and time.

Events Retention

Purge Events

Use the slider to determine the length of time in days (1-59) before events are purged from the system.

Events Archiving

Check the appropriate button to archive events before deleting or delete without archiving them.

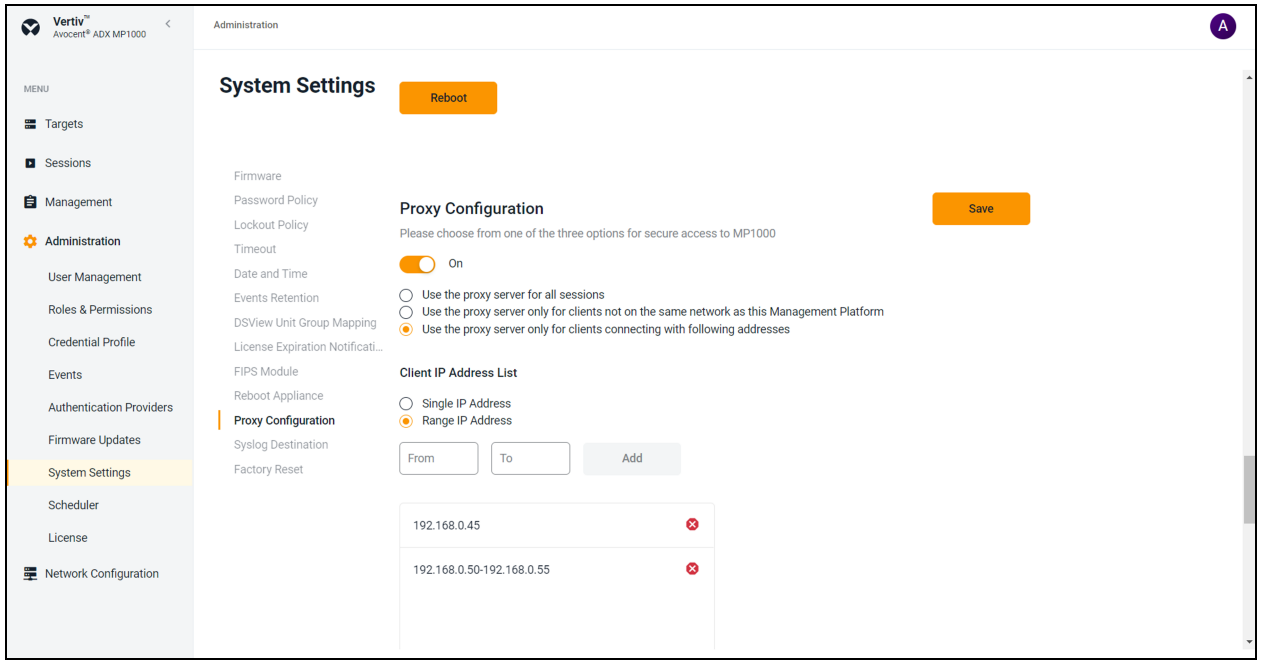
2.9.8 SSL Certificate Replacement

If you wish to replace the SSL certificates in your appliance, please visit Vertiv™ Avocent® ADX MP1000 Software Downloads for a script and release notes to assist you with this process. If you need additional assistance, please contact your Vertiv technical support representative.

2.9.9 Proxy Configuration

Proxy Configuration allows the customers to access all KVM/Serial session traffic through the Avocent ADX MP1000 management platform.

Figure 2.7 Proxy Configuration Overview



To turn on the Proxy Configuration, follow the below steps:

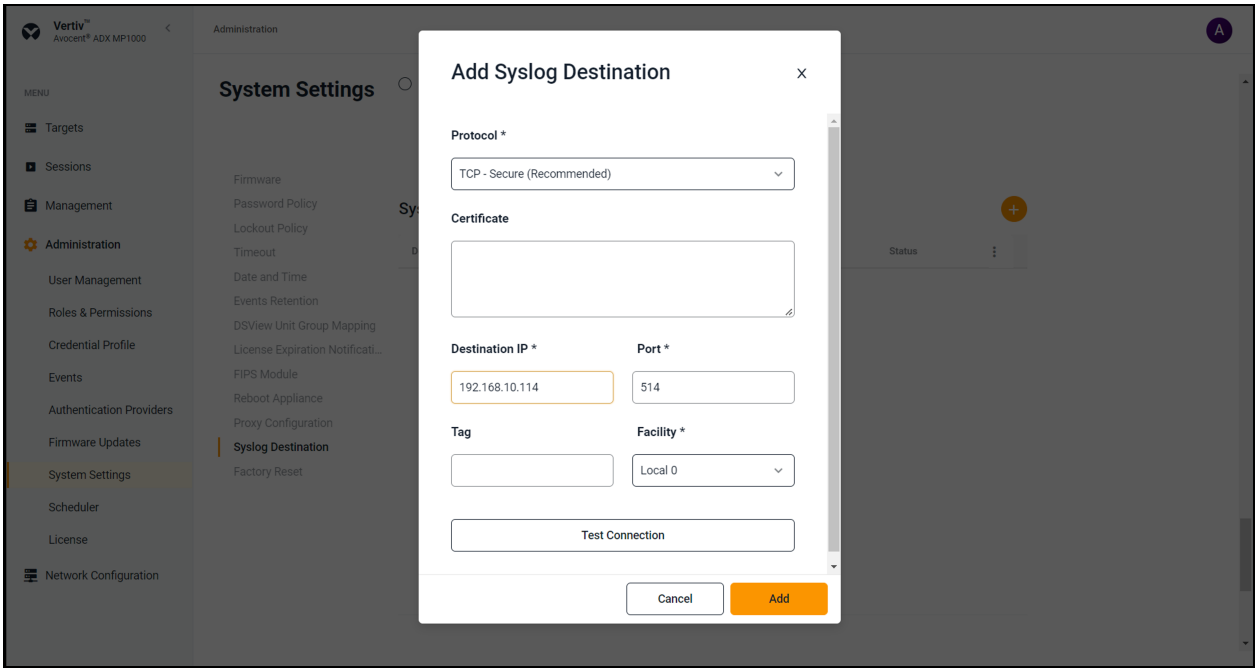
1. From the Administration screen, select *System Settings*.
2. In the System Settings screen, click *Proxy Configuration*.
3. Enable the Proxy Configuration by clicking on the *On/Off button*.
4. For secure access, the user can select one of the three options mentioned below:
    a. Use the proxy server for all sessions: This option allows all the traffic through the MP1000 IP address for any KVM sessions that are launched.
    b. Use the proxy server only for clients not on the same network as this Management Platform: This option allows the use of proxy for all those client machines that are not on the same network as MP1000. This option is used when the client network segment is at different location than MP1000.
    c. Use the proxy server only for clients connecting with following addresses: This option allows the use of proxy for specific IP addresses. The user can select one of the two options to enter the IP Address:
    - Single IP Address.
    - Range IP Address.
5. Click *Save*.

2.9.10 Syslog Destination

Syslog Destination enables a customer to configure the application such that it sends all the audit events to the customer's Syslog server. Syslog server acts as the aggregation point for various different applications.

NOTE: The Audit Events page logs all the user activities such as user login, user log out, logging to KVM session, creating user etc.

Figure 2.8 Add Syslog Destination Overview



To setup Syslog Destination, follow the below steps:

1. From the Administration screen, select *System Settings*.
2. In the System Settings screen, click *Syslog Destination*.
3. Click the *plus (+) icon* and a new dialog Add Syslog Destination appears.
4. Click on the *drop-down arrow* and select the *Protocol*. For Example TCP-Secure (Recommended).

NOTE: The recommended secure option for the Syslog Remote Destination setting is TCP with TLS support.

5. Enter the IP Address of the Syslog server.

NOTE: Port 514 is the standard port for the Syslog server, and this field need not be edited.

NOTE: The Tag field is optional, and the user can add any name in that field.

6. Click on the *drop-down arrow* and select the appropriate *Syslog Facility*.
7. Click on *Test Connection*. If the IP Address is valid, a message will pop-up Test Connection Successful or else a message will pop-up Test Connection Failed.
8. Click *Add*.
9. Enable the Syslog Connection by clicking on the *On/Off button*.

2.9.11 License

This screen displays licensing information for the Avocent ADX MP1000 management platform. You can view the total number of licenses used and the total number of targets.

License management

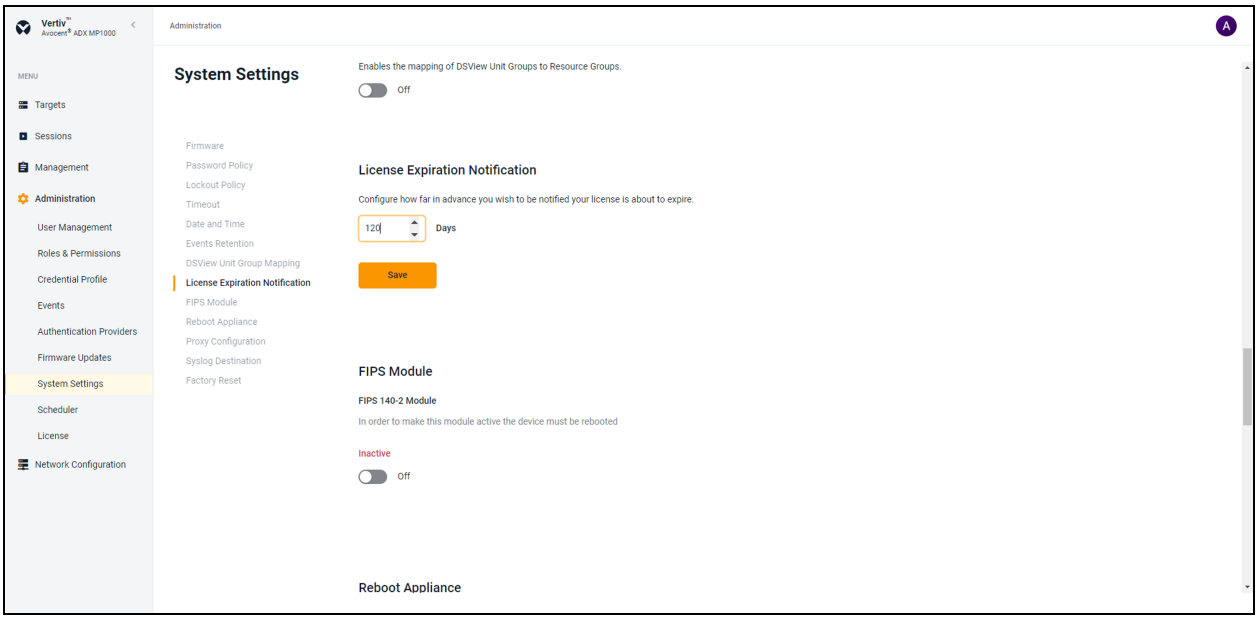
To add a license:

1. From the Administration screen, select *License*.
2. Click on *Expand License*.

3. In the Number field, enter the License Key.
4. Click *Add License*.

License expiration notification

Figure 2.9 License Overview



To set the license expiration notification:

1. From the Administration screen, select *System Settings*.
2. Click on *License Expiration Notification*.
3. In the Days field, enter the number of days you want to be notified in advance about the license expiry.

NOTE: The default value to be entered in the Days field is 120.

4. Click *Save*.

NOTE: If the system is not licensed or the license expires, all the buttons are disabled (grayed out) and the user cannot add devices, upgrade firmware, add users, launch remote sessions, etc.

NOTE: The user cannot add any new devices if the device count exceeds the specified limit (number of licenses), however the user can still launch sessions, upgrade firmware, add users, launch remote sessions, etc. until the license expires.

2.9.12 User Preferences

Click the *icon* in the upper right to open your user profile or log out from the Avocent ADX MP1000 management platform.

User profile

Enter the name and email address for the logged in user.

Localization

Select *measuring system*, *date format*, *time zone*, *language*, and *time number separators* as per preference.

Color theme

Select the color theme for the web UI.

2.9.13 Network Configuration

From this screen, you can view and configure network settings.

Network Settings

You can view the hostname, primary and secondary DNS addresses and the domain name under this tab.

Ethernet Interfaces

The Avocent ADX MP1000 management platform has two physical network interfaces (eno1, eno2). Each interface has an individual MAC address and can be assigned an IP address via DHCP or statically.

To configure the ethernet interface:

1. From the sidebar, click *Network Configuration - Settings*.
2. Under the Ethernet Interfaces, click on the interface you want to configure to open its properties panel.
3. Expand the Network Configuration to view the settings for the selected interface. Click the *Edit icon* to configure the selected interface.
4. For assigning a static IP, enter the IP address, prefix length and gateway address in the appropriate fields and click *Save*.

2.9.14 Network Address Translation (NAT) Setup

From the NAT Setup screen on Vertiv™ Avocent® RM1048P rack manager, you can add and configure NAT rules to perform address translations.

NOTE: To configure a NAT rules on Vertiv™ Avocent® RM1048P rack manager, you should first navigate to the Vertiv™ Avocent® RM1048P rack manager from the Management menu in MP1000 web UI.

To configure a NAT setup:

NOTE: To add and configure the NAT rule, you have to create IP Pool to be used for the NAT rule. See Defining an IP Pool on page 18

1. From the Network Configuration screen, select *NAT Setup*.
2. Click the *plus (+) icon* in the upper right for below 2 options:
   - Select Target.
   - Add Target By IP.
3. To add target from the Target List, select the radio button of *Select Target* and choose a target in the list below.

   -or-

   To add a target that is not added to Target List, select the radio button of *Add Target by IP* and enter the IP address of the new target.
4. Click *Continue* and a window of 1 to 1 NAT Setup will appear.
5. Use the drop-down menu to select the external IP.
6. Define the applicable number for the external port and target port. If required, enter the client IP.
7. To define the expiration date, select the first option to set the manual date.

8. To set the default setting for the expires select the second option, it will be removed after 24 hours.
9. Click *Add*.

2.10 Avocent ADX MP1000 management platform Vertiv™ Avocent® DSView™ Management Software Integration

Avocent ADX MP1000 management platform and Vertiv™ Avocent®DSView™ management software integration is required to provide the user all the devices in one system so they can be run simultaneously. To display all the devices in a single system, the Avocent ADX MP1000 management platform and Avocent® DSView™ management software are connected using API Integration. Both the list of devices included in Avocent® DSView™ management software and the list of devices included in Avocent ADX MP1000 management platform are displayed in the Targets List.

2.10.1 Benefits

- Avocent ADX MP1000 management platform can show Avocent® DSView™ management software devices.
- Great user experience - use single platform.
- Launch KVM or Serial sessions to devices in Avocent® DSView™ management software.
- Protects customer investment in Avocent gear.
- Creates a pathway to Avocent ADX MP1000 management platform migration.

2.10.2 Avocent® DSView™ management software integration

To add a Avocent® DSView™ management software device into the Avocent ADX MP1000 management platform:

1. From the Targets screen, select *Targets List*.
2. Click the *plus (+) icon* and select *Add Device*.
3. Enter the IP address and click *Add Device*.
4. As soon as you click on *Add Device*, it will go through the discovery process and the Targets List will show the information that comes from the Avocent® DSView™ management software system.

To discover a range of Avocent® DSView™ management software devices:

1. From the Targets screen, select *Targets List*.
2. Click the *plus (+) icon* and select *IP Range Discovery*.
3. Enter the IP Range Start and IP Range End fields to enter a range for your targets to be discovered on the network.
4. Using the drop-down, enter the Device Type and Credentials (Username and Password).
5. Click *Discover*.

NOTE: The Targets List displays all the devices that are discovered on the network. The category column in the Targets List shows the device type.

NOTE: The Top Level Device column indicates device is managed by Avocent® DSView™ management software.

To delete a Avocent® DSView™ management software device:

1. Click on the checkbox to the left of the device.
2. Click the *vertical ellipses* to the right and click *Delete*.

To launch a session, follow the below steps:

1. Click on the *play icon* to the right of the individual Avocent® DSView™ management software device you want to launch a KVM session.
2. A pop-up message Connecting to KVM Viewer will be displayed.
3. A Avocent® DSView™ management software HTML5 KVM session or Serial Session is launched in a new tab.

2.10.3 Avocent® DSView™ management software synchronization

Default schedule

The system automatically synchronizes daily at 12:00 am.

Schedule modification

To edit the schedule:

1. Click on any Avocent® DSView™ management software device for which you want to edit the schedule, and the information of the device is displayed on the right-side panel that is listed below:
   - Properties.
   - User Access.
   - Scheduler.
2. Click on the *edit icon* to the right of the Scheduler to edit the fields as below:
   - Repeat Day: The user can modify the schedule either daily or choose specific weekdays.
   - Repeat Time: The user can modify the schedule by choosing a specific time of day.
3. Click *Save*.

On demand resynchronization

To resynchronization the system on demand:

1. Click the *vertical ellipses* to the right.
2. Click *Resynchronization*.

NOTE: The device will automatically resynchronization daily at 12:00 am or the schedule that has been specified by the user.

3 Virtual Appliance

3.1 Requirements

The Vertiv™ Avocent® ADX MP1000VA Virtual Appliance supports the following virtualization products:

- VMware vSphere Hypervisor (ESXi) 7.0.
- VMware vCenter Server 7.0.

3.1.1 Resources

The following minimum hardware resources must be provided, preferably without oversubscribing the host server's resources and reserved for the Avocent ADX MP1000VA Virtual Appliance, where possible.

- Processors (higher or equivalent to the following):
  - Intel Xeon Scalable Generation 1+ 6-Core+.
  - Intel Xeon Processor E5-1650 v4 [6C/12T @ 3.6GHz (4.0GHz)].
  - Intel Xeon Silver 4309Y [8C/8T @2.8GHz (3.6GHz)].
  - AMD EPYC 72F3 [8C/16T @ 3.7GHz (4.1GHz)].
- 4x vCPU.
- 16GB Memory.
- 1TB Storage.

3.2 Deploying the Virtual Appliance

Vertiv distributes the Avocent ADX MP1000VA Virtual Appliance as an Open Virtual Appliance (OVA) file that includes all the necessary components in a single convenient package designed for loading into the VMware vSphere and the VMware vSphere Hypervisor (ESXi). Detailed instructions on deploying your virtual appliance are available in the VMware vCenter. Visit https://www.vmware.com/products/vcenter.html and select *Access Product Documentation*.

3.3 VM Network Configuration

The Avocent ADX MP1000VA Virtual Appliance supports only one virtual network interface.

WARNING! Although additional interfaces may be added, they are not recognized by the application and can cause adverse effects, depending on the DHCP client/route metrics.

3.4 Initial Network Configuration using the Command Line Interface (CLI)

3.4.1 Accessing the VM console

To access the VM console:

1. Click on the thumbnail to open the VM console once the virtual machine has started running.
2. Enter **admin** as the username and **admin** as the password to login for the first time at the Avocent ADX MP1000VA Virtual Appliance login screen.

NOTE: When booting up, it may take time for the services to start before the CLI responds. If the Still Starting message appears, wait for it to clear before proceeding.

3. Change the admin password by following the instructions, then log in again using the new password.
4. To view/set the network IP address, proceed to the next section (Assigning an IP address).

3.4.2 Assigning an IP address

The Avocent ADX MP1000VA Virtual Appliance uses IP addresses to uniquely identify itself to IP-based target devices. It supports both Dynamic Host Configuration Protocol (DHCP) and static IP addressing. An IP address is always obtained via DHCP.

To view or configure the IP address of the Avocent ADX MP1000 management platform:

1. Ensure you have completed the steps in the previous section to access the VM console and change your password.
2. Select the option to show or configure network settings.
3. Select the ethernet interface to configure (not bond 0).

NOTE: The IP address assigned by the DHCP server is visible once this option is selected. This address can be entered into a web browser to access the web UI.

4. To assign a static IP address, select the applicable option and follow the on-screen prompts to configure the IP, subnet and gateway.
5. Type 0 (zero) and press Enter to exit the main menu.
6. Select the option to reboot the Avocent ADX MP1000 management platform.
7. When the Avocent ADX MP1000 management platform reboots, enter the static IP address into a web browser to access the web UI.

NOTE: For information on configuring your network from the web user interface, see Network Configuration (External Link).

3.4.3 Accessing the web UI

To access the web UI:

1. Using your virtual appliance IP address, enter https://<appliance.IP> in a web browser.
2. At the login screen, enter your username and password. The Targets List screen appears.

Appendices

Appendix A: Technical Specifications

Table 2.5 Technical Specifications - Avocent ADX MP1000 Management Platform

Item	Value
Ports	
Networking	2 X 1 GbE
Rear	2 X USB 3.0 1 X VGA 1 X serial connector
Power	
Power Supplies	Dual 350W (platinum) hot-plug redundant power supplies
Input Voltage	100 VAC to 240 VAC at 50 HZ/60 Hz
Dimensions	
Form Factor	Rack (1U)
Height x Width x Depth	1.68 in. X 17.08 in. X 18.98 in. (42.8 mm X 434 mm X 482 mm)
Weight	29.98 lbs (13.6 KG)
Security	Secure Boot
Environmental	
Storage Temperature	-40° C to 65° C (-40° F to 149° F)
Operating Temperature	10° C to 35° C (50° F to 95° F)
Storage Humidity	5%-95% relative humidity with 33° C (91° F) max dew point
Operating Humidity	10%-80% relative humidity with 29° C (84.2° F) max dew point
Safety and EMC Standards, Approvals and Markings	Safety certifications and EMC certifications for this product are obtained under one or more of the following designations: Certification Model Number(CMN), Manufacturer's Part Number (MPN) or Sales Level Model (SLM) designation. The designation that is referenced in the EMC and/or safety reports and certificates are printed on the label applied to this product.
Warranty	Two years standard limited warranty
Maintenance (Optional)	One, two or four years of Silver or Gold

This page intentionally left blank

Connect with Vertiv on Social Media

https://www.facebook.com/vertiv/

https://www.instagram.com/vertiv/

https://www.linkedin.com/company/vertiv/

https://www.twitter.com/Vertiv/

Vertiv.com | Vertiv Headquarters, 1050 Dearborn Drive, Columbus, OH, 43085, USA

590-2355-501C