Avocent® ADX RM1048P Rack Manager

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 RM1048P rack manager is an enterprise class rack manager appliance that serves as a single point for secure local and remote access and administration of target devices. The Avocent ADX RM1048P rack manager provides IP consolidation and network translation to connect to IT devices, PoE, and provide physical aggregation of your devices. It provides keyboard, video, and mouse (KVM) capabilities and can also remotely perform server management tasks, including power control and console access, on managed target devices. It gives you flexible target device management control and secures remote access from anywhere at anytime.

Figure 1.1 Avocent ADX RM1048P Rack Manager Descriptions

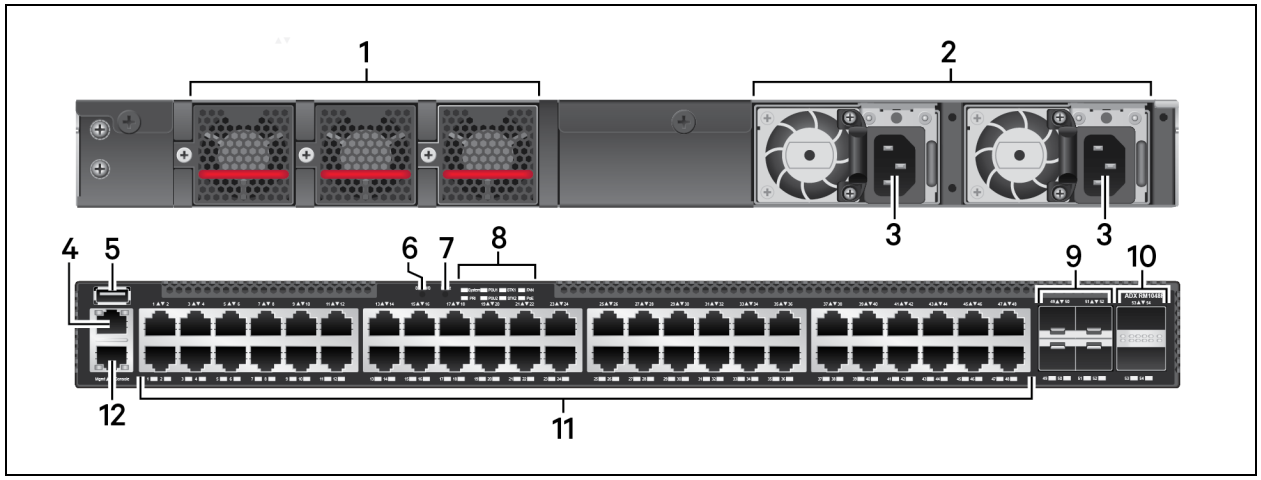


Table 1.1 Avocent ADX RM1048P Rack Manager Descriptions

Item	Description	Item	Description
1	Cooling Fans (2N + 1)	7	Reset button
2	Two redundant power supplies	8	LED indicator lights
3	Two redundant power supplies	9	4 SFP+ ports
4	Management port	10	2 stacking ports (reserved for future use)
5	USB storage port	11	48 1G PoE ports
6	STK M/S button	12	Console port (serial)

1.2 Features and Benefits

The Avocent ADX RM1048P rack manager provides the following benefits for your data center.

- Supports more than 100 simultaneous users on a single all digital rack manager platform to enable scaling without increasing your costs.
- Reduces IP management costs by consolidating IP addresses seamlessly.
- Provides remote and local access to devices from a single IP.
- Reduces power and cabling with Power over Ethernet (PoE).
- Simplifies deployment and configuration with API automation.
- Increases the number of user sessions without the need for more hardware.
- Connects a diverse range of IT devices for rack-level access.
- Provides secure access with a private network.
- Improves reliability with network failover.
- Provides configurable bandwidth to meet digital demand.

1.3 Installation and Initial Setup

For installation and initial setup instructions, see the Avocent ADX RM1048P rack manager Quick Installation Guide provided with your Avocent ADX RM1048P rack manager. This document is also available on the Avocent ADX RM1048P rack manager 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 Rack Manager*.
4. Scroll down and click on *Documents & Downloads* tab.
5. A list of Manuals will be displayed. Click on *Vertiv™ Avocent® ADX RM1048P Rack Manager 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 RM1048P rack manager 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 the Avocent ADX RM1048P rack manager 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 RM1048P rack manager:

1. Make a serial connection to the console port of the Avocent ADX RM1048P rack manager using serial settings of 115200 bps, no parity, 1 stop bit, 8 data bits, and no flow control.
2. From the console menu, login using admin as the username and password. You are prompted to change the password.
3. Select the option to show or configure network settings.
4. Select the *Vrf_app0 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 UI.

5. To assign a static IP address, type .. (Two periods) and press Enter to return to the previous menu.
6. Select the *Vpp0 option*; an IP address must also be assigned to this network interface.
7. Select the *static IP option* and follow the on-screen prompts to configure the IP, subnet, and gateway.
8. Type 0 (zero) and press Enter to exit the main menu.
9. Select the option to reboot the Avocent ADX RM1048P rack manager.
10. Once the Avocent ADX RM1048P rack manager 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 25.

This page intentionally left blank

2 Web User Interface (UI)

Once you have connected the Avocent ADX RM1048P rack manager to a network and configured its IP address, you can access the Avocent ADX RM1048P rack manager with its web UI. The web UI provides direct access to the Avocent ADX RM1048P rack manager and its target devices.

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 RM1048P rack manager https://<appliance.IP> using the IP address for Vrf_app0 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

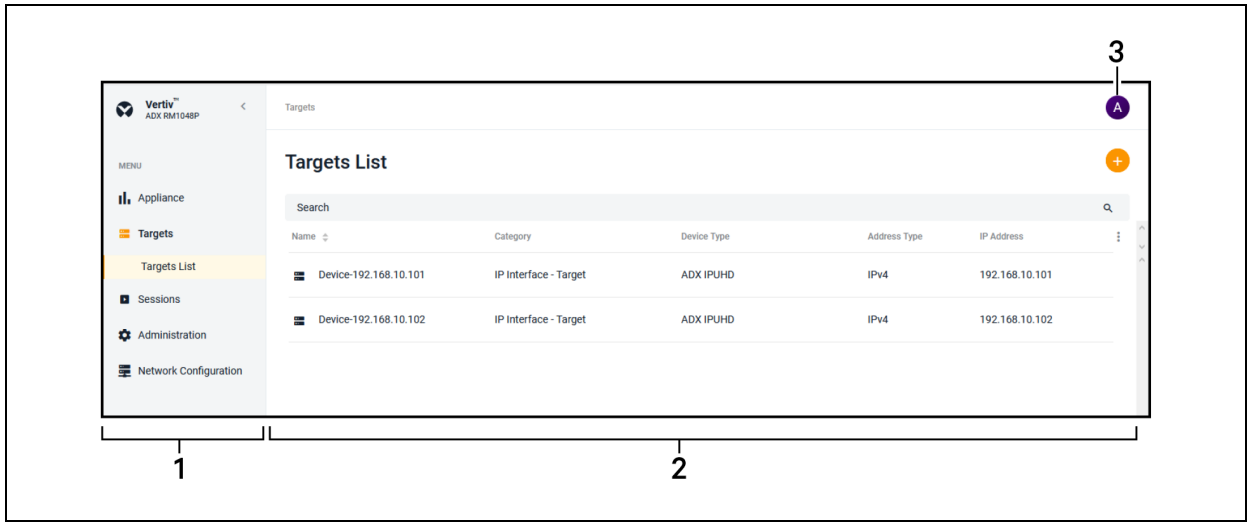


Table 2.1 Web UI Overview Descriptions

Item	Description
1	Sidebar
2	Content Area
3	User Preferences

2.1 Appliance

The Appliance screen displays information about the Avocent ADX RM1048P rack manager and its ports. An administrator can also configure each port from this screen.

2.1.1 Properties

From the Properties heading, you can view the serial number and model of your Avocent ADX RM1048P rack manager. You can also assign a name to your Avocent ADX RM1048P rack manager that will be used to identify it.

2.1.2 Firmware

From the Firmware heading, you can update the firmware for your Avocent ADX RM1048P rack manager or all of its connected targets.

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. From the Appliance, select *overview* screen, and click the *update firmware icon*.
4. Select whether to update the firmware for just the Avocent ADX RM1048P rack manager or to update the firmware for just the connected targets.
5. Select the firmware file and click *Update*.

2.1.3 Ports

An administrator can view the status of, enable and configure the ports on the Avocent ADX RM1048P rack manager.

To configure a port:

1. From the Appliance screen, click *Ports*.
2. Click on the row of the port you want to configure to open its Properties panel.
3. View the properties of a port by expanding the panel or click the *Edit icon* to configure the port.
4. Use the appropriate slider to enable or disable the port or PoE mode. Use the drop-down menu to select the speed of the port.
5. Click *Save Changes* when finished.

2.2 Targets

When logging into the Avocent ADX RM1048P rack manager, the Targets List screen displays a list of targets connected to the Avocent ADX RM1048P rack manager.

The following target types can be managed:

- IP KVM devices.
- Service processors.

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, use the drop-down menu to select your credential profile. For more information, see Credential Profile on page 21.

5. Click on the check-box 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, you are required to enter the credential profile to add or discover it.

2.2.1 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.

2.2.2 Merge targets

You can merge multiple 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.

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 check-box 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 icon* next to the individual target you want to unmerge and click *Unmerge icon* to remove just that target.

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.

Vertiv™ Avocent® ADX MP1000 management platform can manage Geist™ rPDU to provide the following features:

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

To add a Geist™ rPDU into the management platform:

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:

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:

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 KVM Management

The Avocent ADX RM1048P rack manager 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 Avocent® ADX IPUHD	Avocent® ADX MP1000/ Avocent® ADX RM1048P (IPUHD)	Avocent® ADX MP1000/ 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)	✓	✓	×

2.4.1 Video viewer

The Avocent ADX RM1048P rack manager 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 RM1048P rack manager, the target screen appears in a new window. The Avocent ADX RM1048P rack manager allows you to control the target server in person remotely. When you connect to the Avocent ADX RM1048P rack manager, 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 the settings of the Avocent ADX RM1048P rack manager using the *Settings* icon.

2.4.2 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.

2.4.3 Launching an HTML5 video viewer session

Using the web User Interface (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 RM1048P rack manager, 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 below:

- 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*.

2.4.4 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.

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 reserved 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 check-box* 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 check-box will already be enabled and cannot be changed. You might wish to enable the check-box 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.

2.5 Service Processor (SP) Access

The Avocent ADX RM1048P rack manager and Vertiv™ Avocent® ADX MP1000 management platform 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 mentioned benefits:

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

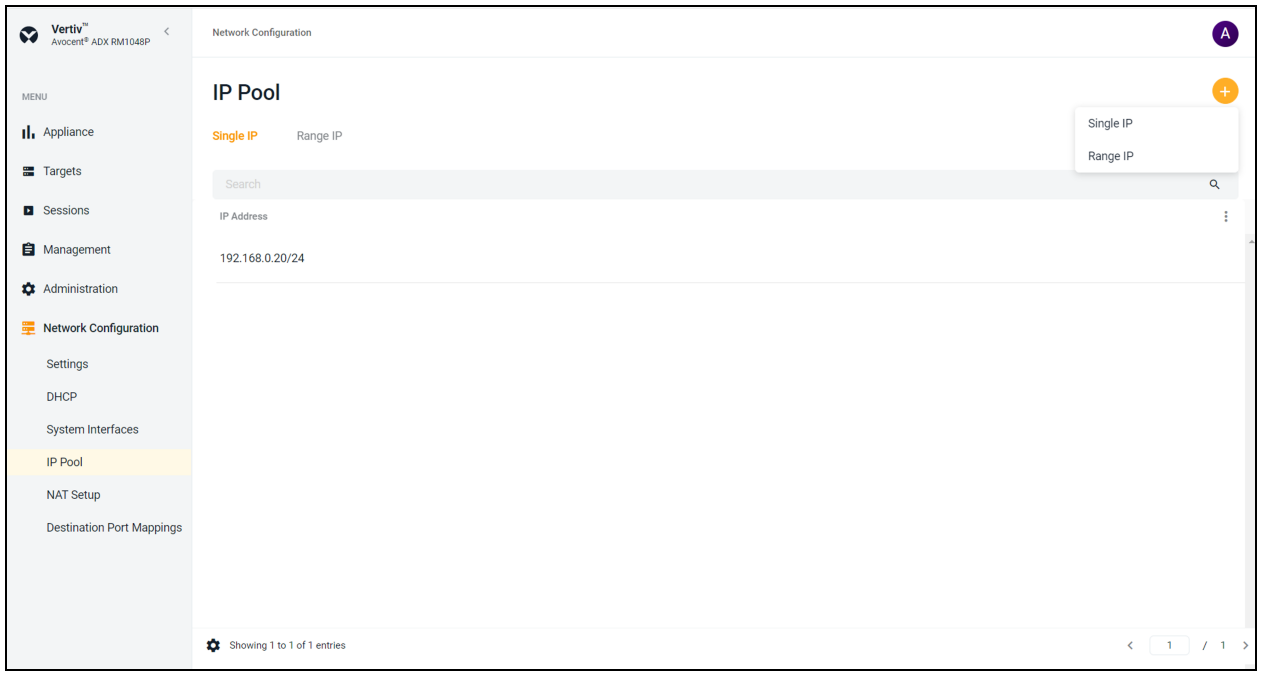
2.5.1 Configuring service processor (SP) web UI access

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

IP Pool

To define an IP Pool:

Figure 2.2 IP Pool Overview



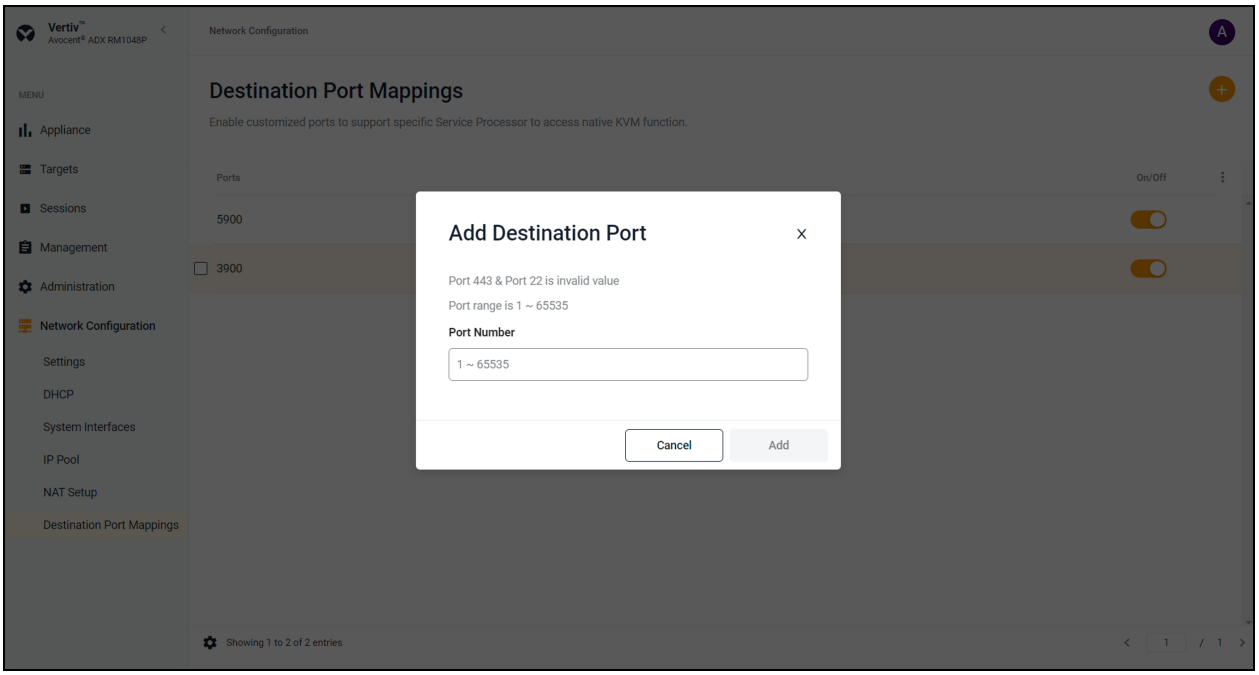
1. From the Network Configuration screen, select *IP Pool*.
2. Click the *plus (+) icon* for below 2 options:
   - Single IP.
   - Range IP.
3. To add a single IP address, click on *Single IP*.
4. Enter the IP Address, then click the *plus (+) icon* to add to the list of addresses. You can enter up to 48 sets of addresses.
5. Click *Add*.
6. To add a range of IP address, click on *Range IP*.
7. Use the Range IP Value from and to fields to enter a range of IP addresses to be added to the network.
8. Click *Add*.

To delete an IP Pool:

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

Defining a Destination Port Mappings

Figure 2.3 Destination Port Mappings Overview



To define the Destination Port Mappings:

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:

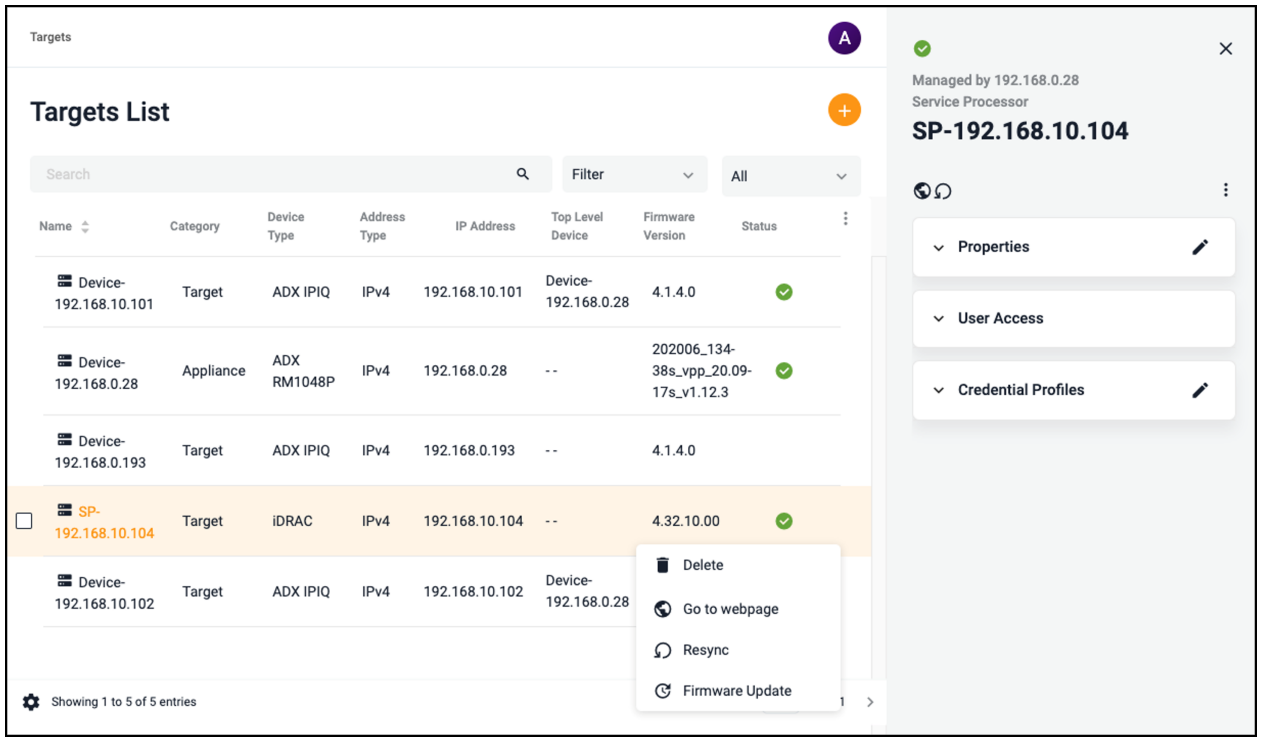
1. Click on the *check-box* to the left of the port.
2. Click the *vertical ellipses* to the right and click *Delete*.

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

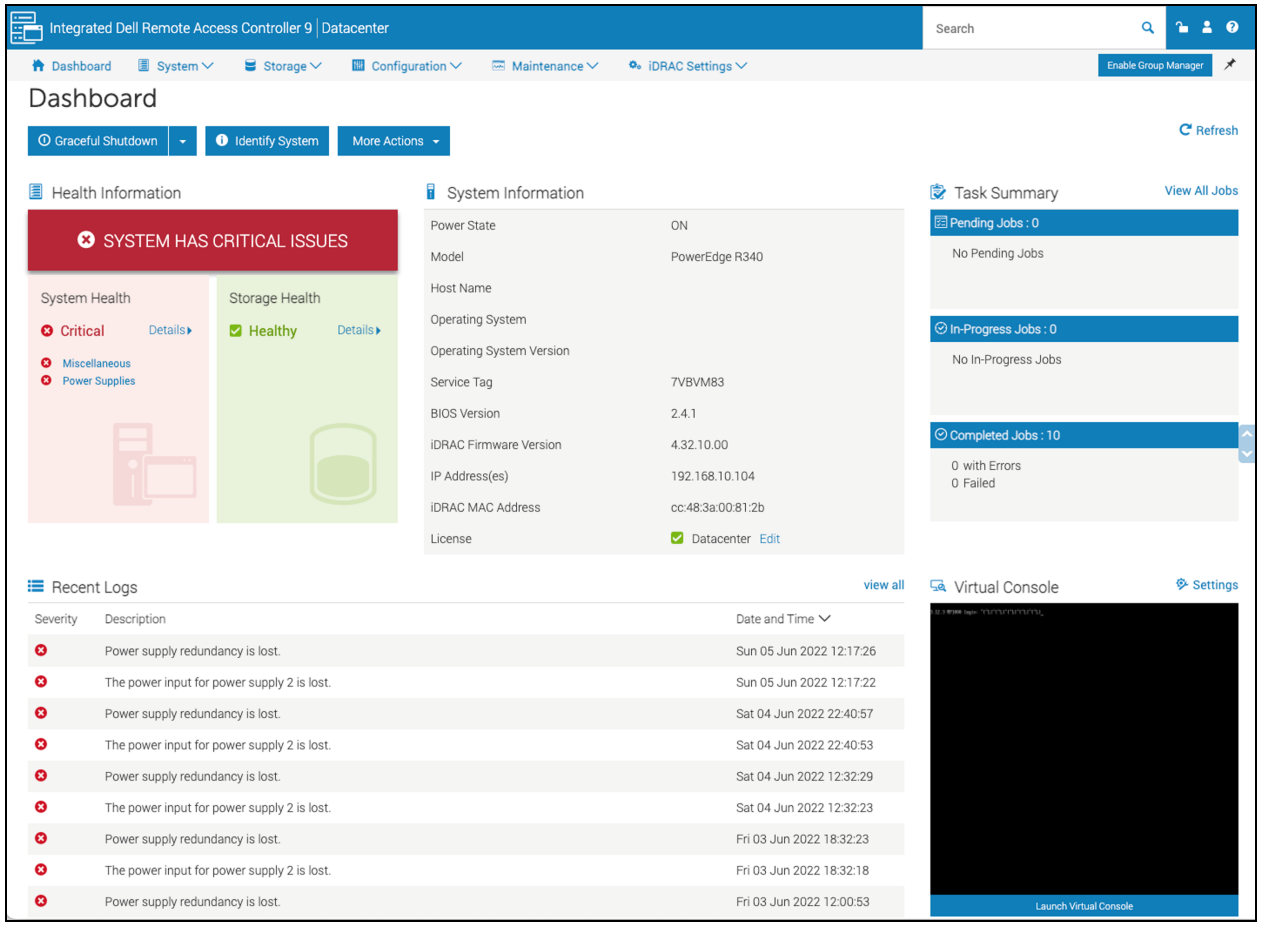
Figure 2.4 Launching Web UI Session



To launch web UI session:

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). See Figure 2.5 on the next page

Figure 2.5 Webpage of the Device (iDRAC) Overview



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

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

2.6.1 Service processor metrics

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

- Click on *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, Update*.

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

2.6.2 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 web page.

2.7 Administration

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

2.7.1 User Management

Access to ports can be optionally restricted, based on permissions an administrator can assign to custom user groups. The Avocent ADX RM1048P rack manager 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 RM1048P rack manager are displayed.

To navigate 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 the check-box 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 of the groups for the Avocent ADX RM1048P rack manager 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.

2.7.2 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 RM1048P rack manager. For example, changing the password for a user on the Avocent ADX RM1048P rack manager.

The Avocent ADX RM1048P rack manager has four default system roles, 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 and 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 check-boxes 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 check-box 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.

2.7.3 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*.

2.7.4 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 (information, warning or critical).
- Use the arrows next to each column to sort each event.
- Click on an event to open its properties sidebar.

2.7.5 Authentication Providers

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

You can Authenticate locally or through AD/LDAP. The Avocent ADX RM1048P rack manager supports remote group authorizations for the LDAP authentication method.

NOTE: The authentication method configured for the Avocent ADX RM1048P rack manager is used for the 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-based 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 RM1048P rack manager 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 RM1048P rack manager, to map your Active Directory remote group to a role on the Avocent ADX RM1048P rack manager.

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.

2.7.6 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 on page 6.

2.7.7 System Settings

From the System Settings screen, you can view and configure system settings for the Avocent ADX RM1048P rack manager.

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:

1. From the System Settings screen, under the FIPS Mode Settings, use the slider to enable or disable FIPS mode.
2. Click *Apply*. 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 RM1048P rack manager.

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.

2.7.8 User Preferences

Click the *icon* in the upper right to open your user profile or log out from the Avocent ADX RM1048P rack manager.

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.

2.7.9 SSL Certificate Replacement

If you wish to replace the SSL certificates in your appliance, please visit Vertiv™ Avocent® ADX RM1048 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.

2.8 Network Configuration

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

2.8.1 Settings

Network Settings

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

Normal/Failover-Bonded Settings

The Avocent ADX RM1048P rack manager has four SFP+ network interface ports. You can configure these ports for bonded and/or failover. The two ports on the left can be bonded to each other as can the two ports on the right. The ports on the right can be used as failover for the left.

To configure the SFP ports:

1. From the sidebar, click *Network Configuration - Settings*.
2. Under the Normal/Failover-Bonded Settings heading, use the drop-down menu to enable one SFP, two SFPs (bonded), two SFPs (failover) or four SFPs (bonded and failover).

Ethernet interfaces

The Avocent ADX RM1048P rack manager has three physical network interfaces (eth1, vrf_app0, Vpp0). 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*.

2.8.2 System Interfaces

From the System Interfaces screen, you can view information about the system interfaces. Use the vertical ellipses to configure the table.

2.8.3 IP Pool

An IP pool is a range of dedicated IP addresses within your network. IP pool addresses are necessary for 1 to 1 NAT setup. From the IP Pool screen, you can view configured IP pools as well as create new pools from a single IP address or from a range of IP addresses. To create/delete an IP pool, see IP Pool on page 15

2.8.4 Network Address Translation (NAT) Setup

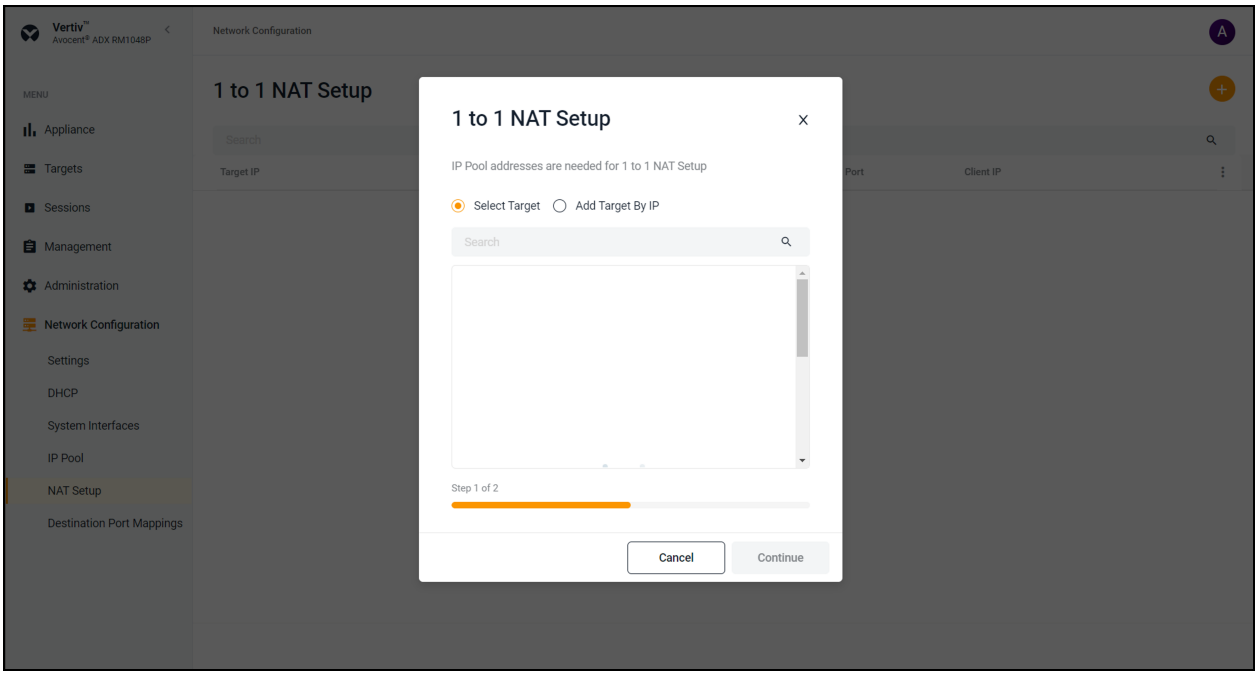
From the NAT Setup screen, you can add and configure NAT rules to perform address translations.

To configure a NAT setup:

NOTE: To add and configure NAT rule, you have to create IP Pool to be used for the NAT rule. See Service Processor (SP) Access on page 14

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.

Figure 2.6 1 to 1 NAT Setup Overview



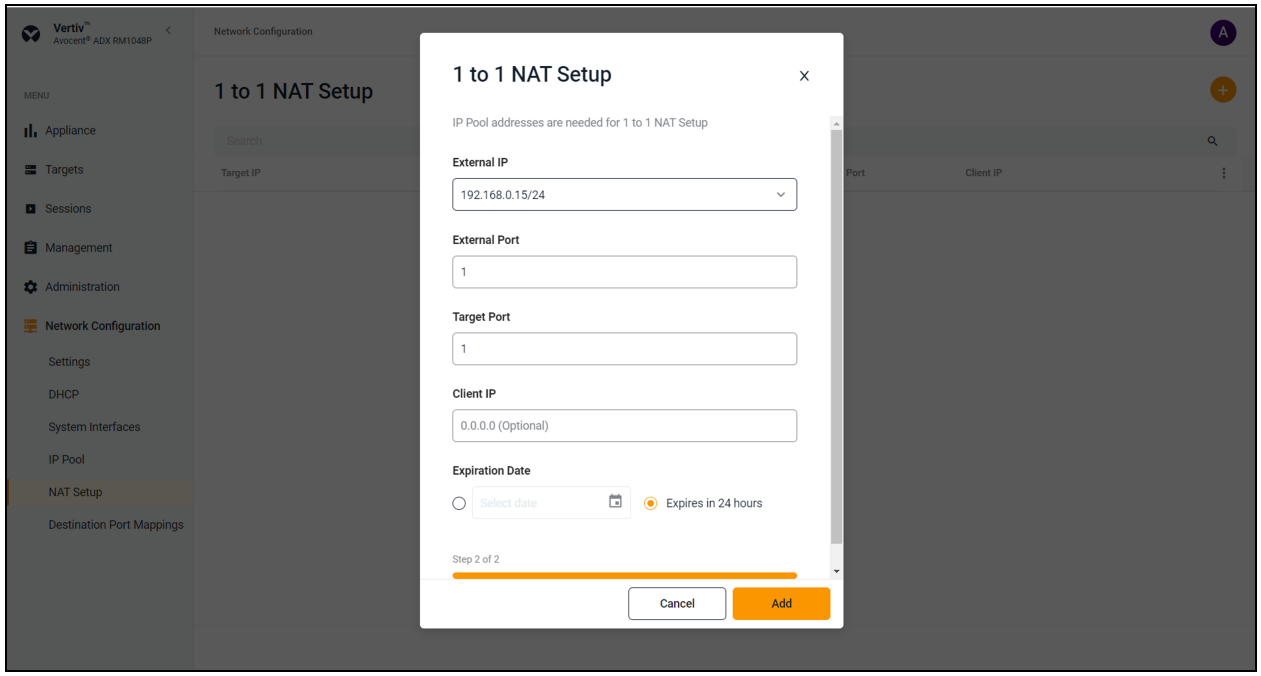
3. To add target from the Target List, select the radio button of *Select Target* and choose a target in the list below.

   -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.

Figure 2.7 1 to 1 NAT Setup Options



5. Use the drop-down menu to select the external IP.
6. Define the applicable number for the external port, 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*.

2.8.5 Destination Port Mappings

From the destination port mappings screen, you can enable customized ports to support specific Service Processor (SP) to access native KVM function. To define the destination port mappings, see Defining a Destination Port Mappings on page 16.

This page intentionally left blank

Appendices

Appendix A: Technical Specifications

Table 3.1 Technical Specifications Avocent ADX RM1048P rack manager

Item	Value
Ports	
Device	48 X 1G PoE ports
SFP	4 X SFP + uplink ports
Management	1 X management 1 X console
PoE	IEEE 802.3at
Fan Units	3 X fans
Power	
Power Supplies	Redundant/Dual power
Power Usage	1800 watts maximum
Input Voltage	100 VAC to 240 VAC at 50/60 Hz
Dimensions	
Form Factor	Rack (1U or 21U)
Height x Width x Depth	1.72 in. X 17.24 in. X 17.40 in. (43.7 mm x 438 mm x 42 mm)
Weight	16.91 lbs (7.67 kg)
Environmental	
Storage Temperature	-40° C to 70° C (-40° F to 158° F)
Operating Temperature	0° C to 45° C (32° F to 113° F)
Storage Humidity	
Operating Humidity	5-90% non-condensing
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: CMN (Certification Model Number), MPN (Manufacturer's Part Number) or Sales Level Model 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

590-2356-501C