VERTIV™

Avocent® 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.

The products covered by this instruction manual are manufactured and/or sold by Vertiv. This document is the property of Vertiv and contains confidential and proprietary information owned by Vertiv. Any copying, use or disclosure of it without the written permission of Vertiv is strictly prohibited.

Names of companies and products are trademarks or registered trademarks of the respective companies. Any questions regarding usage of trademark names should be directed to the original manufacturer.

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

NOTE: At this time, the former Vertiv™ Avocent® ADX platform is transitioning into the Vertiv™ Avocent® DSView™ solution. During this transition, there may temporarily still be references to "ADX" within product-related features and documentation.

The Avocent 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 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 RM1048P Rack Manager Descriptions

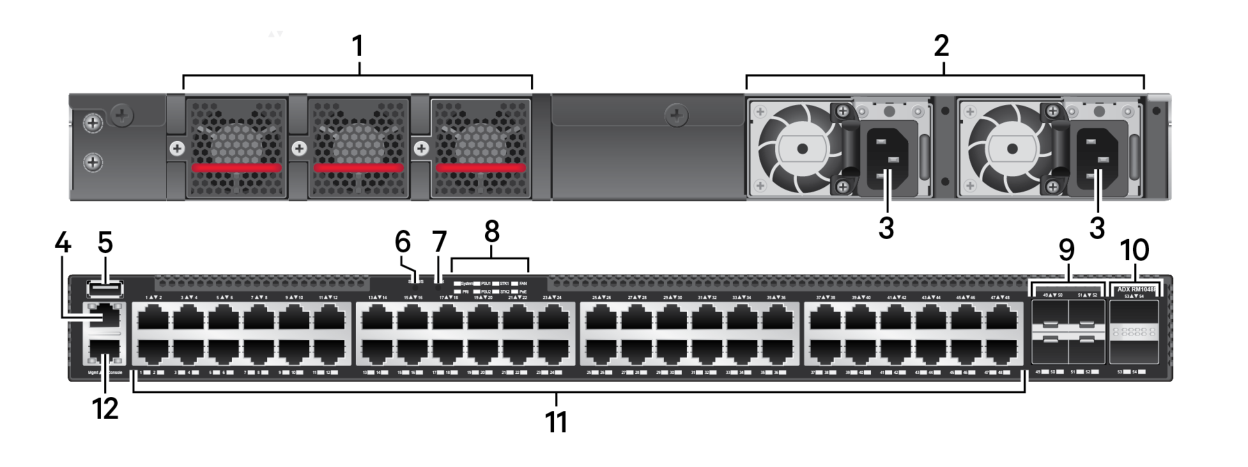


Table 1.1 Avocent RM1048P Rack Manager Descriptions

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 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 Vertiv™ Avocent® RM1048P Rack Manager Quick Installation Guide provided with your rack manager. This document is also available on the Avocent RM1048P Rack Manager product page.

To navigate to the product page:

1. Go to www.Vertiv.com.
2. On the Search bar, type **RM1048P** and press **Enter**.
3. Click on *Vertiv™ Avocent® RM1048P Rack Manager*.
4. Scroll down and click the *Documents & Downloads* tab.
5. Under Manuals, click the *Vertiv™ Avocent® RM1048P Rack Manager Quick Installation Guide*. The PDF file will open in the new tab.

2 SSL Certificate Replacement

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

This page intentionally left blank

3 Web User Interface (UI)

Once you have connected the Avocent RM1048P Rack Manager to a network and configured its IP address, you can access the rack manager and target devices via the web UI.

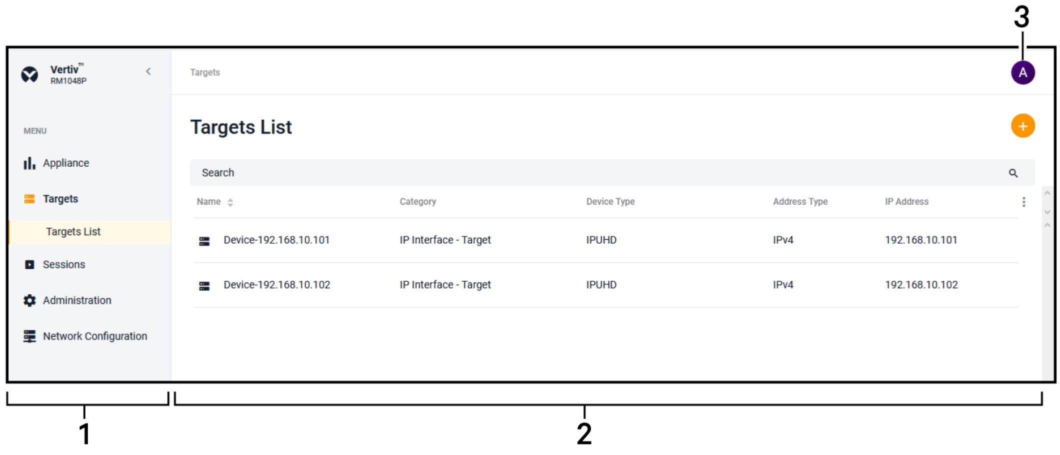
The web UI is compatible with the latest 32-bit and 64-bit versions of the following web browsers:

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

To log into the web UI:

1. Open a web browser and enter the Vrf_app0 IP address for the rack manager that you previously configured. The IP address should be entered in the following format: **https://**<appliance.IP>
2. At the login screen, enter your username and password. The web UI opens into the Targets List screen.

Figure 3.1 Web UI Overview



Name	Category	Device Type	Address Type	IP Address
Device-192.168.10.101	IP Interface - Target	IPUHD	IPv4	192.168.10.101
Device-192.168.10.102	IP Interface - Target	IPUHD	IPv4	192.168.10.102

Table 3.1 Web UI Overview Descriptions

Item	Description
1	Sidebar
2	Content Area
3	User Preferences

3.1 Account Settings

To open your account settings, click the profile icon in the top right corner of the web UI. The drop-down menu allows you to choose from User Preferences, Help and Log Out.

User Preferences

This option provides access to the following tabs: User Profile, Localization and Color Theme. The capabilities of these tabs have been provided in the remainder of this section.

User Profile

Configure the profile name and email address.

Localization

- Measuring System - Select either the Metric or Imperial radio button to determine the measuring system for the rack manager.
- Time Zone - Use the drop-down menu to select your time zone for alarms and notifications.
- Time Number Separators - Use the Digit Grouping drop-down menu and the Decimals drop-down menu to select the appropriate values.
- Data Format - Select either the Day/Month/Year or Month/Day/Year radio button to determine the format for all dates in the web UI.
- Time Format - Select either the 12-hours or 24-hour radio button to determine the format for all times in the web UI.
- Language - Use the drop-down menu to select the language used in the web UI.

Color Theme

Select the radio button for your desired color theme.

Help

This option redirects you to the Online Help provided for the Avocent RM1048P Rack Manager.

Log Out

This option immediately logs you out of the web UI.

3.2 Appliance

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

3.2.1 Overview

The Overview screen provides the following functions for the rack manager:

- View the serial number and model of your appliance
- Assign a name for easy device identification
- Update the firmware version

To update the firmware:

1. From the left-hand sidebar, click *Appliance - Overview - Firmware*.
2. Under the Firmware heading, click *(Download Page)* to go to the Vertiv™ Avocent® RM1048 Software Downloads page.
3. Download the most recent firmware version.
4. Save the firmware to your local PC, FTP, HTTP, or TFTP server.
5. From the *Appliance - Overview - Firmware* screen, click the *Update Firmware* button.
6. Select whether to update the firmware for just the Avocent RM1048P Rack Manager or to update the firmware for just the connected targets.
7. Select the firmware file and click *Update*.

3.2.2 Ports

The Ports screen allows an administrator to enable, configure and view the status of the ports on the Avocent RM1048P Rack Manager.

To configure a port:

1. From the *Appliance - Ports* screen, click on the desired port to open its Properties panel.
2. Click *Port Properties* to expand the menu.

   -or-

   Click the Edit icon (pencil) to configure the port.
3. Use the appropriate slider to enable or disable the Port Status or PoE Mode options.
4. Click *Save Changes*.

3.3 Targets

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

The following target types can be managed:

- IP KVM devices
- Service Processors
- Vertiv™ Uninterruptible Power Supplies (UPSes)
- Vertiv™ Power Distribution Units (PDUs)

IP KVM devices

KVM devices can be discovered and managed when connected via a Vertiv™ Avocent® IPIQ IP KVM device or a Vertiv™ Avocent® IPUHD 4K IP KVM device. The Avocent 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 allows for flexible target device management control and secure remote access from anywhere at anytime.

The KVM over IP functionality of the appliance provides the following features and benefits:

- 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

Service Processors (SPs)

Connecting an SP to a rack manager provides the following features and benefits:

- Ability to centrally access the web UI of the server
- Ability to launch embedded KVM viewer
- Secures the servers when connected to a private network
- Provides multiple server space management options
- Unrestricted, secure access to server interface

Vertiv™ Uninterruptible Power Supplies (UPSes)

Vertiv™ UPSes provide power conditioning and battery backup for business critical IT equipment to ensure your applications are protected in the event of an unanticipated loss of power or an unprecedented power surge. Adding a UPS to the rack manager improves input power quality and equipment protection and provides a battery mode that allows the power supply to continue without interruption if the input power fails.

Vertiv™ Power Distribution Units (PDUs)

Vertiv™ PDUs distribute reliable, electric power to data centers and monitor the system's power status. Avocent RM1048P Rack Manager can manage PDUs to provide the following features:

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

3.3.1 Targets List

Configure targets

Target devices can be added to the rack manager via a single IP or a range of IP addresses.

NOTE: Some devices require a credential profile in order to be added to the rack manager. See Credential Profiles on page 27 to create a credential profile.

NOTE: To access the web UI of a connected SP, you must first configure the SP as described in Service Processors (SPs) on the next page.

To add a single device or a range of devices:

1. From the *Targets* - *Targets List* screen, click the Add icon (+) in the top right corner. An Add Device dialogue box appears.
2. Select the Single IP radio button to add a single device.

   -or-

   Select the Range IP radio button to add a range of devices.
3. Enter the discovery name.
4. If you selected the Single IP radio button, enter the IP address.

   -or-

   If you select the Range IP radio button, enter the IP address range.
5. Use the Device Type drop-down menu to select the device type.
6. Based on your selection, fill out the appropriate fields.

NOTE: Credential profiles are required for the following device types: Rack Managers, Service Processors, Rack PDUs and Rack UPS. All of these devices require Username/Password credentials, except for the Rack UPS. The Rack UPS requires SNMPv1/v2 credentials.

7. Click *Discover*. It may take several minutes for the device(s) to be successfully added to the rack manager. Once added, the target devices appear on the Targets - Targets List screen.

To delete a target device:

1. From the *Targets* - *Targets List* screen, click on the vertical ellipses next to the individual device you want to delete.
2. Click the *Delete* icon. It may take several minutes for the device to fully delete.

To view target properties and network configuration:

1. From the *Targets* - *Targets List* screen, click a target to open its sidebar.
2. Click the Edit icon (pencil) to configure the target's properties.

To activate Maintenance Mode:

1. From the *Targets* - *Targets List* screen, hover the mouse over the desired target and click the vertical ellipses.
2. Use the slider button to enable the In Maintenance Mode setting.

Manage targets

To manage target devices:

1. Hover the mouse over the desired target and click the vertical ellipses.
2. Different functions appear for each target device type. Click the appropriate function.

Merge targets

You can merge multiple target devices into a single merged target device. This allows you to conveniently launch actions on a set of targets that are merged to behave as one. You can merge KVM, SP and serial targets, as well as all outlets on a Vertiv™ Geist™ Rack Power Distribution Unit (rPDU). Additionally, power operations are now included in overall user activities.

NOTE: You cannot merge VMs.

To merge targets:

1. From the *Targets - Targets 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 *Merge*. A plus (+) icon displays to show the merged targets. Click the icon to expand the merged target and show each individual target.

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

To unmerge targets:

1. From the *Targets - Targets List* screen, 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 next to the individual target you want to unmerge and click *Unmerge* to remove just that target.

3.3.2 Discoveries

The Discoveries screen allows you to discover target devices by entering a range of IP addresses. There are two tabs on this page: Range and Appliance. The Range tab displays the different range discovery tasks that are currently being performed. The Appliance tab shows the target devices that have been discovered as a result of the range discovery tasks.

To navigate around the Discoveries screen:

From the left-hand sidebar, click *Targets - Discoveries*.

- Click the *Range* or *Appliance* tab to switch between views.
- Use the Search bar to search for specific tasks or target devices.
- Use the Start IP and End IP bars to conduct searches based on IP addresses.
- Use the All Status drop-down menu to filter searches by discovery status.

3.3.3 Service Processors (SPs)

To access the web UI of an SP connected to a rack manager, you must first create an IP pool for the SP to obtain an available IP address. Once the IP pool has been created, the Destination Port Mapping setting should be configured.

NOTE: Web UI sessions cannot be launched for the SP until these configurations have been completed.

Supported processors

The Avocent RM1048P Rack Manager support the following SPs:

- Dell iDRAC 7, 8, and 9
- HPE iLO4 and iLO5

- Lenovo XCC
- OpenBmc

Creating an IP pool

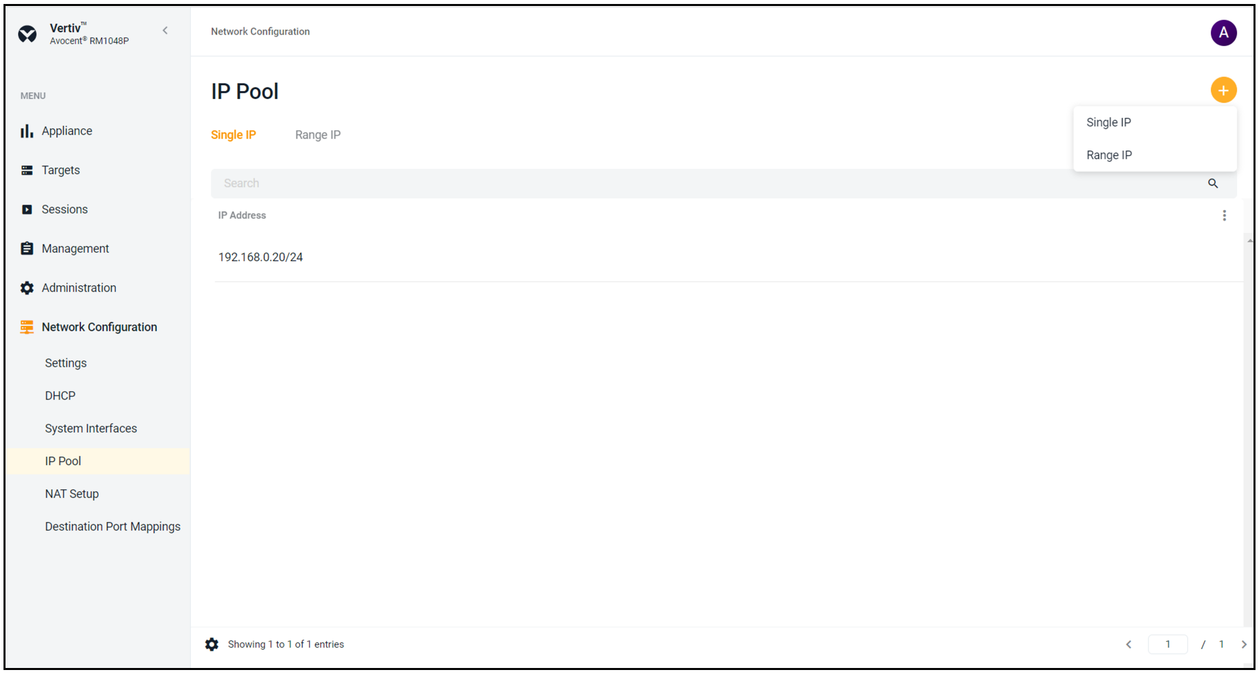
To create an IP pool:

1. From the *Network Configuration - IP Pool* screen, click the plus (+) icon.
2. To add a single IP address, click the *Single IP* button.

   -or-

   To add a range of IP addresses, click the *Range IP* button.

Figure 3.2 IP Pool Overview



IP Address
192.168.0.20/24

Showing 1 to 1 of 1 entries

3. Enter the appropriate information and click *Add*.

NOTE: You can enter up to 48 single IP addresses and 1 range of IP addresses.

To delete an IP Pool:

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

Configuring destination ports

To define a destination port:

1. From the *Network Configuration - Destination Port Mappings* screen, click the plus (+) icon. An Add Destination Port dialogue box will appear.
2. Enter the port number and click *Add*.

NOTE: Use the On/Off button to enable or disable the port.

NOTE: The port must be enabled 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*.

Viewing device metrics and management options

Once discovered, an SP appears on the Targets - Targets List with its SP type and IP address. To view SP metrics, click on the desired SP. From the Metrics screen, you can perform the following functions:

- View the status, temperature, fan speed, power and properties of the SP
- Upgrade the SP firmware
- Control the LED and power functions of the SP
- Navigate to the SP web UI
- Reboot the device
- Drag and drop to rearrange the boot order

NOTE: Depending on the model, the SP may require a reboot for the rearranging of the boot order to take effect.

3.4 Sessions

3.4.1 Sessions List

The Avocent RM1048P Rack Manager allows you to launch multiple sessions simultaneously to access your target devices via the rack manager web UI. The Sessions List screen displays a log of the active and closed sessions that have been launched from your rack manager.

To navigate through the Sessions List screen:

From the left-hand sidebar, click *Sessions - Sessions List*.

- Use the *Active*, *Closed* and *All* tabs to view the session log based on status.
- Use the Search bar to search for specific sessions.
- Click a target name to view its sidebar, which includes the Properties and User Sessions drop-down menus.

3.4.2 KVM sessions

The Avocent RM1048P Rack Manager conducts KVM sessions using HTML5 Video Viewer with one or more target devices attached to one or more KVM switches. When a target device connects to the rack manager, the target screen appears in a new window, and the target server can be controlled remotely. In addition to controlling each target device, you can 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.

Supported browsers and processors

KVM sessions use the web-based HTML5 Video Viewer. The following web browsers are supported by the Video Viewer:

- Google Chrome

- Microsoft Edge
- Apple Safari
- Mozilla Firefox

The following table highlights the processors supported by the rack manager for launching KVM sessions.

Table 3.2 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

Launch KVM sessions

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

NOTE: You must have assigned rights or belong to a user group with assigned rights to launch a KVM session.

To launch a KVM session:

From the *Targets - Targets List* screen, hover the mouse over the desired target and click the Launch Session icon.

-or-

Click on the desired target to open its sidebar, then click the Launch Session icon.

To close a KVM session:

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

Exclusive Mode

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 KVM session:

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

HTML5 Video Viewer

Connecting the target devices via the rack manager allows you to centrally manage computer settings, access files, and launch virtual media sessions for the target devices from the rack manager's web UI.

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 for the Avocent RM1048P Rack Manager using the *Settings* icon.

Table 3.3 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 3.4 Feature Comparison for Vertiv™ Avocent® IPUHD 4K IP KVM Device and Vertiv™ Avocent® IPIQ IP KVM Device Viewer

Feature	Stand-Alone Vertiv™ Avocent® IPUHD 4K IP KVM device	Vertiv™ Avocent® MP1000 Management Platform/ Avocent RM1048P Rack Manager (Vertiv™ Avocent® IPUHD 4K IP KVM device)	Vertiv™ Avocent® MP1000 Management Platform/ Avocent RM1048P Rack Manager (Vertiv™ Avocent® IPIQ IP KVM device)
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)	✓	✓	×

HTML5 Video Viewer menu

Using the Video Viewer menu, you can configure active KVM sessions. This section describes the capabilities of the Video Viewer menu options.

File

- Copy and paste text to the target
- Open a server-side recording file

View

- Configure display options for the video viewer
- Maximize the screen size
- Enable single-cursor modes
- View KVM statistics
- Hide the status bar at the bottom of the screen

Video Options

- Display more color options to optimize fidelity or less colors to reduce the volume of data transferred on the network

NOTE: The maximum speed is Grayscale 16 Shades, and the maximum video quality is Color 24 bit.

- Enable noise reduction for VGA or disable it for a digital video source

Scaling

The Scaling tab allows you to adjust the appearance of the target's screen in the Video Viewer using the following features:

- Maintain Aspect Ratio - Enable this feature to maintain the aspect ratio of the target's screen.
- Stretch to Window - Select this feature to fit the target screen to your display.
- Zoom - Use this drop-down menu to select the zoom percentage of the display.

Max Resolution

Select the maximum target resolution for your KVM session(s).

NOTE: This setting affects the actual video resolution of your target system's OS.

NOTE: Changes made to this setting affect all sessions and will remain until changed again.

Macros

The Macros tab provides access to a list of supported OSes that your target device may use. After selecting the desired OS, you can access the list of command strings that are valid for the selected OS. You can also define macros using the Manage Macros tab. If you are looking for a command string that does not appear in the list, verify you have selected the correct OS in the Macro Manage drop-down list.

NOTE: It is recommended that you use the Macros tab to send a command string to a server. This saves time and eliminates the risk of errors. Your client server will not be affected.

To send a command to the target server:

1. From the Video Viewer menu, click the *Macros* drop-down list and select a command string from the Static Macros list.
2. Click *Send*.

Tools

- Select the keyboard language
- Perform a screen capture

- Send an instant message
- Select the mouse mode
- Reset the keyboard and mouse
- Enable a virtual keyboard - When enabled, the keyboard displays on the client's workstation and can be positioned anywhere in the window. Use the up and down arrows in the top right to change the size of the keyboard.
- Enable exclusive mode
- Optimize network bandwidth
- Schedule the reduction of the update rate

Virtual Media

The Virtual Media feature allows you to map a physical drive on the client machine as a virtual drive on a target device. Also, you can use the client workstation to add and map an .iso and .img file as a virtual drive on a target device.

NOTE: Only one Virtual Media session can be active on a target device at a time.

NOTE: VMs do not have the Virtual Media feature.

Prerequisites

Before using the Virtual Media feature, ensure the following prerequisites are met:

- The target device must be connected to a KVM switch using an IQ module, with both supporting Virtual Media.
- The target device must be able to use the types of USB2 compatible media that you virtually map.
- The target device must support a portable USB memory device to map it on a client machines as a Virtual Media drive on the target device.
- You (or the user group to which you belong) must have permission to establish Virtual Media sessions and/or reserve Virtual Media sessions to the target device.

To map a Virtual Media drive:

1. In the Virtual Media section of the client navigational toolbar, click *Connect*.
2. After the session is activated, use the Virtual Media drop-down menu to select the type of file to map. Select *Map ISO image* or *Files/Folder* to map a .iso file.

   -or-

   Select *Map Removable Disk Image* to map a .img file.
3. If you wish to reset the USB connection, select *Virtual Media - Reset USB*.
4. Read the instructions, then click *OK*.
5. Select a file from the Open dialog box with the proper file extension (.iso or .img), then click *Open*.
6. If you wish to limit the mapped drive to read-only access, check the Read Only box in the Virtual Disk Management dialogue 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. If the session setting has read and write access enabled, you may check the Read Only box to limit a particular drive's access. 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.

7. Click *Map Drive*, then click *Close*. Mapping is now complete, and the drive 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*.

3.4.3 Serial sessions

The Avocent RM1048P Rack Manager provides serial management via a Vertiv™ Avocent® IPSL IP serial device.

To launch a serial session:

1. From the *Targets - Targets List* screen, hover the mouse over the desired serial device.
2. On the right of the column, click the Launch Serial Session 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*.

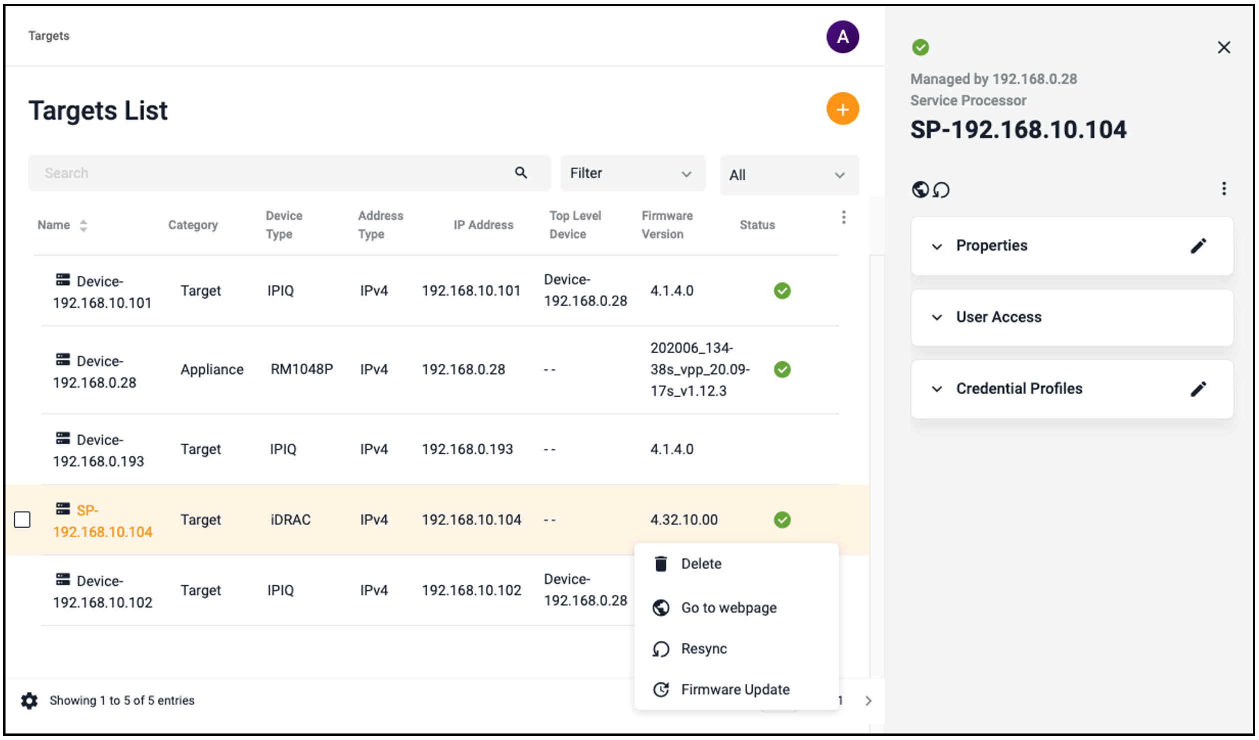
3.4.4 Web UI sessions

Service Processors (SPs) can be remotely accessed from the rack manager by launching web UI sessions.

To launch the web UI session:

1. From the *Targets - Targets List* screen, navigate to the desired SP.

Figure 3.3 Launching Web UI Session



Targets List

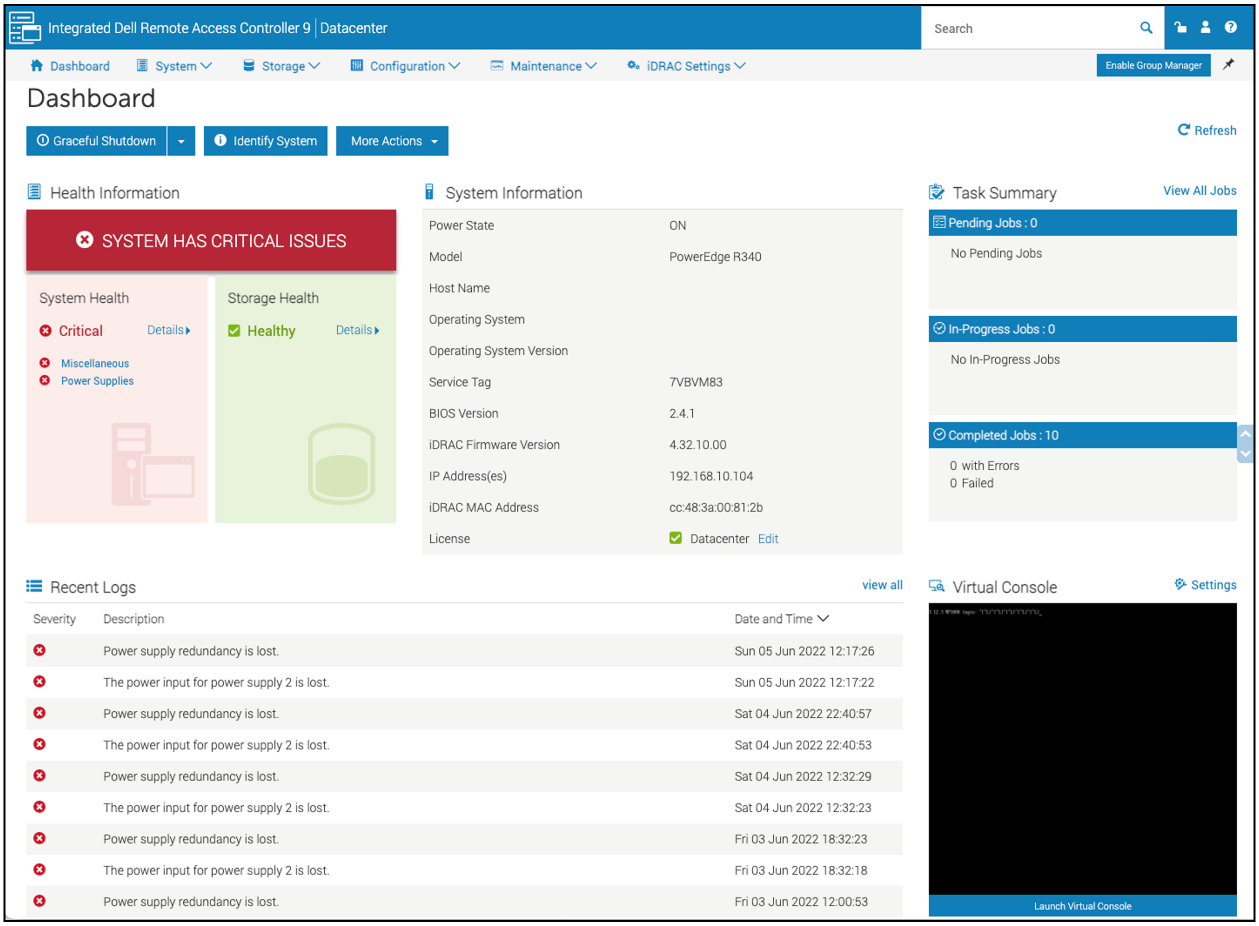
Name	Category	Device Type	Address Type	IP Address	Top Level Device	Firmware Version	Status
Device-192.168.10.101	Target	IPIQ	IPv4	192.168.10.101	Device-192.168.0.28	4.1.4.0	✓
Device-192.168.0.28	Appliance	RM1048P	IPv4	192.168.0.28	- -	202006_134-38s_vpp_20.09-17s_v1.12.3	✓
Device-192.168.0.193	Target	IPIQ	IPv4	192.168.0.193	- -	4.1.4.0	
□ SP-192.168.10.104	Target	iDRAC	IPv4	192.168.10.104	- -	4.32.10.00	✓
Device-192.168.10.102	Target	IPIQ	IPv4	192.168.10.102	Device-192.168.0.28		

Showing 1 to 5 of 5 entries

✓
Managed by 192.168.0.28
Service Processor
SP-192.168.10.104

2. Select the management card (for example iDRAC) and click *Go to webpage*.
3. Enter the username and password, then click *Log In*. You are redirected to the webpage of the SP.

Figure 3.4 Webpage of the Device (iDRAC) Overview



Dashboard

Health Information

SYSTEM HAS CRITICAL ISSUES

System Health: Critical (Details)
- Miscellaneous
- Power Supplies

Storage Health: Healthy (Details)

System Information

Power State	ON
Model	PowerEdge R340
Host Name	
Operating System	
Operating System Version	
Service Tag	7VBVM83
BIOS Version	2.4.1
iDRAC Firmware Version	4.32.10.00
IP Address(es)	192.168.10.104
iDRAC MAC Address	cc:48:3a:00:81:2b
License	☑ Datacenter Edit

Task Summary

Pending Jobs : 0
No Pending Jobs

In-Progress Jobs : 0
No In-Progress Jobs

Completed Jobs : 10
0 with Errors
0 Failed

Recent Logs

Severity	Description	Date and Time
☒	Power supply redundancy is lost.	Sun 05 Jun 2022 12:17:26
☒	The power input for power supply 2 is lost.	Sun 05 Jun 2022 12:17:22
☒	Power supply redundancy is lost.	Sat 04 Jun 2022 22:40:57
☒	The power input for power supply 2 is lost.	Sat 04 Jun 2022 22:40:53
☒	Power supply redundancy is lost.	Sat 04 Jun 2022 12:32:29
☒	The power input for power supply 2 is lost.	Sat 04 Jun 2022 12:32:23
☒	Power supply redundancy is lost.	Fri 03 Jun 2022 18:32:23
☒	The power input for power supply 2 is lost.	Fri 03 Jun 2022 18:32:18
☒	Power supply redundancy is lost.	Fri 03 Jun 2022 12:00:53

Virtual Console

3.5 Management

The Management screen displays the managed and unmanaged target devices connected to the rack manager.

To navigate through the Management screen:

From the left-hand sidebar, click *Management*. On this screen, you can perform the following functions:

- Use the *Managed* or *Unmanaged* tab to see the appropriate list of target devices.
- Click the plus (+) icon to add a new device, then fill out the required fields.

3.6 Administration

With Administrator login rights, you can access the Administration screen to configure and manage the rack manager and target devices.

3.6.1 User Management

The User Management screen allows you to view and configure the user and group accounts.

Based on your assigned permissions, access to ports may be restricted by an administrator. By default, the user is admin and the following are the pre-defined user groups:

- System-Administrators
- System-Maintainers
- User-Administrators
- Users

NOTE: Only administrator users can view all target devices. If non-administrator users wish to view target devices, the user must be added to a user group, then an administrator must add the target devices to the user group. For instructions, please see User groups on the facing page.

Users

From the left-hand sidebar, click the *Administration - User Management - Users* tab to view all users for the Avocent RM1048P Rack Manager.

To navigate through the Users tab:

Click a user to open its sidebar. On this screen, you can perform the following functions:

- Click the vertical ellipses to the right of the device to change the selected user's password or delete or disable the user.
- View the Properties and Device Access menus.
- Expand *Properties* and click the Edit icon (pencil) to configure the user's name, email and password expiration time.

To configure a user's password expiration time:

1. Click the desired user to open the sidebar.
2. Click *Properties* to expand the menu.
3. Under the Password Expiration Time section, use the slider to enable the field.
4. Use the calendar feature to select a date and time.
5. (Optional) Check the 24h Clock box to set the time in the 24-hour clock format, if desired.
6. Click *Done*, then click *Save*.

To create a new user:

1. Click the Add icon (+) in the top right corner. An Add User dialogue box appears.
2. Enter the full name, user name and temporary password.

NOTE: The password must have a minimum of eight characters.

3. Click *Add User*.

To delete a user:

1. Hover the mouse over the desired target and check the box of the left.
2. Click the Delete icon (trash can) above the list of users.
3. At the confirmation screen, click *Yes* to delete.

User groups

A user group defines what the user can do within the web UI and CLI, regarding appliance settings and administration. From the left-hand sidebar, click the *Administration - User Management - Groups* tab to view all groups for the Avocent RM1048P Rack Manager.

To navigate through the Groups tab:

Click a group to open its properties sidebar. On this screen, you can perform the following functions:

- Click the vertical ellipses to delete the selected user group.
- Expand *Group Properties* to view and configure the group name, preemption level and assigned system roles.
- Expand *Users* to view and configure the assigned users.
- Expand *Targets* to view and configure the assigned target devices.
- Expand *External Groups* to view and configure the assigned external groups.

To create a user group:

1. Click the Add icon (+). An Add New Group dialogue box appears.
2. Enter the group name and check the boxes for each user you want to add to the group.
3. Click *Add Group*.

NOTE: By default, user groups have no assigned permissions. After adding the user group, you must assign at least one system role to gain permissions for functionality purposes.

4. Click the newly added user group to open its side panel, then click the Edit (pencil) icon next to the Group Properties heading.
5. Under the System Roles heading, select the desired system role(s) to assign them to the user group. If you wish to create a new system role, please see Roles & Permissions.
6. Click *Save Changes*. The user group has now been created and assigned permissions.

To assign target devices to a user group:

NOTE: Target devices can be assigned to non-administrative users to provide limited access to the devices, depending on the system roles of the user.

1. Click the desired user group to open its side panel, then click the Edit (pencil) icon next to the Targets heading.
2. Check the box(es) for the target devices you wish to add to the user group.
3. Click *Save Changes*.

To delete a user group:

1. Hover the mouse over the desired target and check the box of the left.
2. Click the *Delete* icon (trash can) above the list of groups.
3. At the confirmation screen, click *Yes* to delete.

Group mapping

Multiple users on the same network can be added to the rack manager by mapping the Active Directory (external) group to the local user group. For group mapping, the authentication provider for the external group must first be added to the web UI. To add an authentication provider, see the procedure in Authentication Providers on page 28.

Once the authentication provider has been added, the external group can be mapped to the local user group.

To perform group mapping:

1. From the *Administration - User Management - Groups* screen, click on the desired local user group. The side panel appears.
2. Click *External Groups* to expand the menu.
3. Select the desired external group from the list.
4. Click *Assign to External Group*.
5. Click *Save Changes*.

3.6.2 Roles & Permissions

The Roles & Permissions screen displays the roles and permissions of the targets and system. A user permission authorizes a user to perform a specific operation on a target or system. A role is a collection of user permissions. There are four default system roles and two default target roles.

System Roles

A system role is a collection of user permissions that can be applied to a system. These roles can be configured and applied to a user group to permit specific system operations. For example, a system administrator with a system role that includes the permission to change the user password is allowed to change user passwords from the web UI. The following list highlights the four default roles and their associated user groups:

- System Administrator Role – System Administrators
- System Maintainer Role – System Maintainers
- User Administrator Role – User Administrators
- User Role – Users

User groups can be configured with one or more system roles. The system role permissions assigned to a user group are available for any user within the user group. For more information on user group configurations, please see User groups on the previous page.

Target Roles

A target role is a collection of user permissions that can be applied to a target device. These roles can be configured and applied to a user group to permit specific operations on a target device. For example, a user with a target role that includes the user permission to establish KVM sessions is allowed to launch KVM sessions to target devices from the web UI. User groups can be associated with one or more target roles. The following list highlights the two default target roles:

- User Target Role
- System Maintainer Target Role

The following table describes the user permissions allowed for each system and target role. A checkmark indicates the permission listed in the left-hand column is allowed for the role. An "x" indicates the permission is not allowed.

Table 3.5 Roles and Permissions

	System Roles				Target Roles	
User Permission	System Administrator Role	System Maintainer Role	User Administrator Role	User Role	User Target Role	System Maintainer Target Role
Configure Local User Accounts and User Groups	✓	✘	✓	✘	✘	✘
View Local User Accounts and User Groups	✓	✘	✓	✘	✘	✘
Configure Roles and Resource Groups	✓	✘	✓	✘	✘	✘
View Roles and Resource Groups	✓	✘	✓	✘	✘	✘
Configure External Authentication Providers	✓	✘	✓	✘	✘	✘
View External Authentication Providers	✓	✘	✓	✘	✘	✘
Configure Appliance Settings	✓	✓	✘	✘	✘	✓
View Appliance Settings	✓	✓	✘	✘	✘	✓
Reboot Appliance	✓	✓	✘	✘	✘	✓
Reset Appliance To Factory Defaults	✓	✓	✘	✘	✘	✓
Update Appliance SSL Certs	✓	✘	✘	✘	✘	✘
View Appliance SSL Certs	✓	✘	✘	✘	✘	✘
View Event Log	✓	✓	✘	✘	✘	✘
Configure Event Data Retention Policy	✓	✓	✘	✘	✘	✘
View Event Data Retention Policy	✓	✓	✘	✘	✘	✘
View System Logs	✓	✓	✘	✘	✘	✘
Configure Licensing	✓	✓	✘	✘	✘	✘
View Licensing	✓	✓	✘	✘	✘	✘
Configure User Profile	✓	✓	✘	✘	✘	✘
View User Profile	✓	✓	✘	✘	✘	✘
Configure User Policy	✓	✓	✓	✓	✘	✘
View User Profile	✓	✓	✓	✓	✘	✘

Table 3.5 Roles and Permissions (continued)

	System Roles				Target Roles	
User Permission	System Administrator Role	System Maintainer Role	User Administrator Role	User Role	User Target Role	System Maintainer Target Role
Configure User Policy	✓	✗	✓	✗	✗	✗
View User Policy	✓	✗	✓	✗	✗	✗
Change User Password	✓	✓	✓	✓	✗	✗
Configure Devices	✓	✓	✗	✗	✗	✓
View Devices	✓	✓	✓	✓	✓	✓
Upgrade Firmware	✓	✓	✗	✗	✗	✓
Configure KVM Session	✓	✗	✗	✗	✗	✗
Establish KVM Session	✓	✓	✓	✓	✓	✓
Establish VKVM Session	✓	✓	✗	✓	✓	✓
Establish Exclusive Session	✓	✗	✗	✗	✗	✗
Establish Stealth Session	✓	✗	✗	✗	✗	✗
Configure Serial Session	✓	✗	✗	✗	✗	✗
Establish Serial Session	✓	✓	✓	✓	✓	✓
Establish SSH Session	✓	✓	✓	✓	✓	✓
Establish Viewer Session To VM	✓	✓	✗	✓	✓	✓
Establish VNC Session	✓	✓	✗	✓	✓	✓
Launch standalone passive session	✓	✓	✓	✓	✓	✓
Terminate active standalone passive sessions	✓	✓	✓	✓	✓	✓
View Target Sessions	✓	✓	✗	✗	✗	✓
Terminate Target Session	✓	✗	✗	✗	✗	✗
Establish Virtual Media Session	✓	✓	✓	✓	✓	✓
KVM Clipboard paste	✓	✓	✗	✗	✗	✓
KVM Paste text from file	✓	✓	✗	✗	✗	✓
KVM Screen capture	✓	✓	✗	✗	✗	✓

Table 3.5 Roles and Permissions (continued)

	System Roles				Target Roles	
User Permission	**System Administrator Role**	**System Maintainer Role**	**User Administrator Role**	**User Role**	**User Target Role**	**System Maintainer Target Role**
KVM Screen recording	✓	✓	✘	✘	✘	✓
KVM Remote Audio	✓	✓	✘	✘	✘	✓
Browse Virtual Media Disk Image	✓	✓	✓	✓	✓	✓
Write to Virtual Media Disk Image	✓	✓	✓	✓	✓	✓
Create ISO image file in KVM session	✓	✓	✘	✘	✘	✘
Manage VM	✓	✘	✘	✘	✘	✓
View VM	✓	✓	✘	✘	✘	✘
Configure Connection ESX Host	✓	✘	✘	✘	✘	✘
View Connection Settings ESX Host	✓	✘	✘	✘	✘	✘
View User Sessions	✓	✘	✓	✘	✘	✘
Configure Data Points	✓	✘	✘	✘	✘	✘
Create, Update and Delete Organization Information	✓	✓	✘	✘	✘	✓
View Organization Information	✓	✓	✓	✓	✓	✓
Configure Shutdown profiles	✓	✓	✘	✘	✘	✘
View Shutdown profiles	✓	✓	✓	✓	✘	✘
Run Shutdown profiles	✓	✓	✘	✘	✘	✘
Configure Service Processor	✓	✓	✘	✘	✘	✓
View Service Processor	✓	✓	✘	✘	✓	✓
View Service Processor Metrics	✓	✓	✘	✘	✓	✓
View Preferences	✓	✓	✓	✓	✘	✘
Configure Preferences	✓	✓	✓	✓	✘	✘
Configure Sys Log	✓	✓	✘	✘	✘	✘

Table 3.5 Roles and Permissions (continued)

	System Roles				Target Roles	
User Permission	System Administrator Role	System Maintainer Role	User Administrator Role	User Role	User Target Role	System Maintainer Target Role
View Sys Log	✓	✓	✗	✗	✗	✗
Posts to Event Log	✓	✓	✗	✗	✗	✗
Purge Event Log	✓	✗	✗	✗	✗	✗
Reboot Server	✓	✗	✗	✗	✗	✗
Shutdown Server	✓	✗	✗	✗	✗	✗
Power Control	✓	✓	✗	✗	✗	✓
Reset Control	✓	✓	✗	✗	✗	✓
Boot order Control	✓	✓	✗	✗	✗	✓
Restart Control	✓	✓	✗	✗	✗	✓
Led Control	✓	✓	✗	✗	✗	✓
Configure Scheduled Jobs	✓	✓	✗	✗	✗	✗
View Scheduled Jobs	✓	✓	✗	✗	✗	✗
Configure Nodes for High Availability	✓	✓	✓	✗	✗	✗
View Nodes for High Availability	✓	✓	✓	✗	✗	✗
Configure Notification Settings	✓	✓	✗	✗	✗	✗
View Notification Settings	✓	✓	✗	✗	✗	✗

Users can also create a custom system or target role to which user permissions can be assigned from the web UI. To create a custom role, please refer to the following procedure.

To add a new role:

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

   -or-

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

2. Click the Add icon (+) in the top right corner.
3. Enter a name and description for the role.
4. Check the desired box(es) to add permissions.

   -or-

   Check the Select All box to add all permissions.

5. Click *Add Role*.

To configure an existing role:

NOTE: The default roles cannot be configured.

1. From the *Administration - Roles & Permissions* screen, click a role to open its sidebar.
2. Expand *Properties* and click the Edit icon (pencil) to configure the description for the role.
3. Expand *Permissions* and click the Edit icon (pencil) to configure the permissions for the role.
4. Click *Save*.

To view role properties and permissions:

From the left-hand sidebar, click *Administration - Roles & Permissions*, then click a role to open its sidebar.

To delete a role:

NOTE: The default roles cannot be deleted.

1. From the *Administration - Roles & Permissions* screen, hover the mouse over the desired target and check the box to the left.
2. Click the Delete icon (trash can).
3. At the confirmation screen, click *Yes* to delete.

3.6.3 Credential Profiles

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

The Credential Profiles screen displays the credential profiles of your target devices. 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 the following device types: Service Processors, Rack PDUs, and Rack UPSes. All of these devices require Username/Password credentials, except for the Rack UPS. The Rack UPS requires SNMPv1/v2 credentials.

NOTE: 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 - Credential Profiles* screen, click the Add icon (+) in the top right corner. An Add credential profile dialogue box appears.
2. Enter a profile name and type, username and port.
3. Enter the password, then confirm the password.
4. (Optional) Add a note, if desired.
5. Click *Add credential profile*.

3.6.4 Events

The Events screen displays the saved log of events that have occurred.

To view more options in the Events screen:

From the left-hand sidebar, click *Administration - Events*. On this screen, you can perform the following functions:

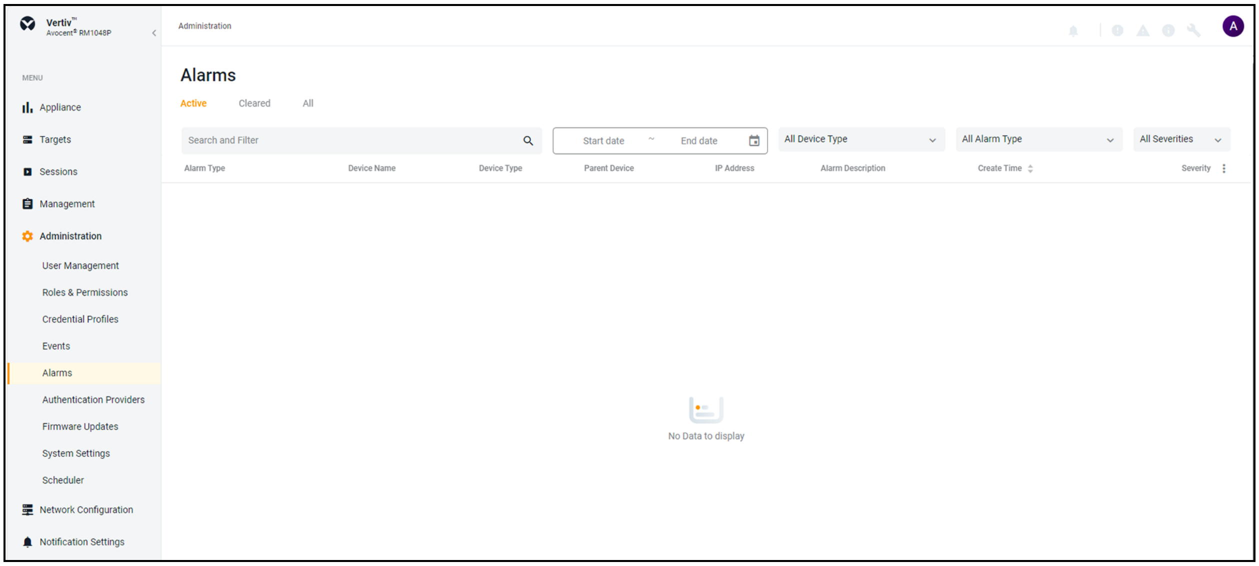
- Use the Search bar to search for a specific event.

- Use the Filters drop-down menu to filter events by severity (*All Severities, Info, Warning* or *Critical*).
- Use the arrows next to each column to sort each event.
- Click on an event to open its sidebar and view the properties.

3.6.5 Alarms

The Alarms screen displays the types of alarm alerts for the target devices.

Figure 3.5 Alarms Screen



To navigate through the Alarms screen:

From the left-hand sidebar, click *Administration - Alarms*. On this screen, you can perform the following functions:

- Use the Search and Filter bar to search or filter for a specific alarm alerts by using the IP address or device name.
- Use the calendar feature to filter alarms by date.
- Use the All Device Type drop-down menu to filter alarms by device type.
- Use the All Alarm Type drop-down menu to filter alarms by alarm types.
- Use the All Severities drop-down menu to filter alarms by severity (*All Severities, Info, Warning* or *Critical*).
- Navigate between the *Active, Cleared* and *All* tabs to view the different list of alarms.

To clear the alarms manually:

1. Hover the mouse over the desired alarms and check the box to the left for each one.

   -or-

   Click the vertical ellipses to the right of the individual alarm.
2. Click the *Clear Alarms* icon. A Clear Alarm dialogue box will appear.
3. Click *Continue*.

3.6.6 Authentication Providers

The Authentication Providers screen displays the list of configured authentication providers.

Providers can be authenticated locally or via AD/LDAP, TACACS+ or RADIUS. For the LDAP method, the Avocent RM1048P Rack Manager supports remote group authorizations.

NOTE: The authentication method chosen to configure the rack manager is used for authenticating every user that attempts to log in through SSH or the web UI.

To add an authentication provider:

1. From the *Administration - Authentication Providers* screen, click the Add icon (+) in the top right corner.
2. Use the drop-down menu to select *AD/LDAP, TACACS+* or *RADIUS* as the authentication type. A dialogue box appears for the chosen authentication type.
3. Enter the required configuration information for your authentication server.
4. When finished, click *Add Provider*.

To enable an authentication provider:

1. From the *Administration - Authentication Providers* screen, click the vertical ellipses next to the desired provider.
2. Click *Enable*.

To delete an authentication provider:

1. From the *Administration - Authentication Providers* screen, click the vertical ellipses next to the desired provider.
2. Click the *Delete* icon.
3. At the confirmation screen, click *Yes* to delete.

To update the providers order:

1. From the *Administration - Authentication Providers* screen, click the Add icon (+) in the top right corner.
2. Select *Update providers order* in the drop-down menu.
3. Use the right-hand drag icon to rearrange the providers as desired.
4. When finished, click *Update Order.*

Active directory

You can enable role-based security on the Avocent RM1048P Rack Manager to map your Active Directory remote group to a role on the rack manager.

NOTE: When you are mapped to any local role and have enabled and configured the related security, 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 Add 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.

3.6.7 Firmware Updates

The Firmware Updates screen shows the scheduled firmware updates. The Status column reflects the current status of the firmware updates.

NOTE: If needed, click the Refresh icon in the top right corner to refresh the page.

For information on updating the firmware, see Appliance on page 6.

3.6.8 System Settings

From the System Settings screen, you can view and configure the system settings for the Avocent RM1048P Rack Manager. Click *Administration - System Settings*, then use the sidebar menu to navigate through the various sections.

Password Policy

From here, you can perform the following functions:

- Configure global password rules for all user accounts
- Use the drop-down menus and sliders to set the global password policy

NOTE: When the global password policy is updated for enhanced security, all local user accounts will be flagged to change the password at the next login.

- Configure the account expiration settings

NOTE: By default, passwords must have a minimum of eight characters and all other password expiration rules are pre-defined.

Lockout Policy

An administrator can configure global lockout rules to all user accounts. By default, lockout is enabled after three failed login attempts, accounts are automatically unlocked after 20 minutes and the login retry timeout is disabled.

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

From here, you can perform the following functions:

- View the current date and time
- Manually configure the date and time

  -or-

  Use an NTP server

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

To archive events before deleting them, click the Archive and Delete radio button.

-or-

To delete events without archiving them, click the Delete radio button.

Alarms Retention

Retention Policy

Define the number of days to delete the alarm from the system.

Viewer Settings

Use the slider to determine if users will be automatically logged out after the Video Viewer session has been inactive for a set time. If this setting is enabled, use the Minutes field to configure the amount of time a user can be inactive before being logged out.

Standalone KVM Viewer Settings

Use the different settings to configure the standalone KVM sessions.

FIPS Module

By default, the FIPS mode of operation is disabled but can be enabled using the slider.

Email Server Configuration

Click the Edit icon (pencil) to configure the primary or secondary email server information. To receive email notifications, you must enable the Sending Email setting under the Notification Configuration heading.

Notification Configuration

Use the Sending Email slider to enable or disable email notifications from the rack manager. To configure the email notification, see Notification Settings on page 37.

Reboot Appliance

Click *Reboot* to reboot the appliance.

NOTE: Upon reboot, you will be logged out of the system.

Factory Reset

To perform a factory reset:

From the *Administration - System Settings - Factory Reset* screen, click the *Reset To Default Setting* button to remove all data from your equipment.

3.6.9 Scheduler

The Scheduler screen displays the schedule of events set to occur based on your configurations.

3.7 Network Configuration

The Network Configuration screen allows you to view and configure network settings.

NOTE: The Avocent RM1048P Rack Manager requires at least two IP addresses to access the web UI and launch target sessions. For more information, please see Ethernet Interfaces on the facing page.

3.7.1 Settings

Network Settings

The Network Settings tab displays the following items:

- Hostname
- Primary DNS
- Secondary DNS
- Domain Name

To configure the Hostname:

1. From the left-hand sidebar, click *Network Configuration - Settings*.
2. Under the Network Settings heading, enter the new value in the Hostname field.
3. Click *Save*.

Normal/Failover-Bonded Settings

The Avocent 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 left-hand 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).

Failover-Routed IPv4 Trigger Mode

The Failover-Routed IPv4 Trigger Mode tab allows you to configure the trigger for initiating failover.

To configure the trigger mode for failover:

1. From the left-hand sidebar, click *Network Configuration - Settings*.
2. Under the Failover-Routed IPv4 Trigger Mode, select either the *Primary Interface Down,Unreachable Default Gateway* or *Unreachable IP* radio button. If you select *Unreachable IP*, then fill out the IP Address field.

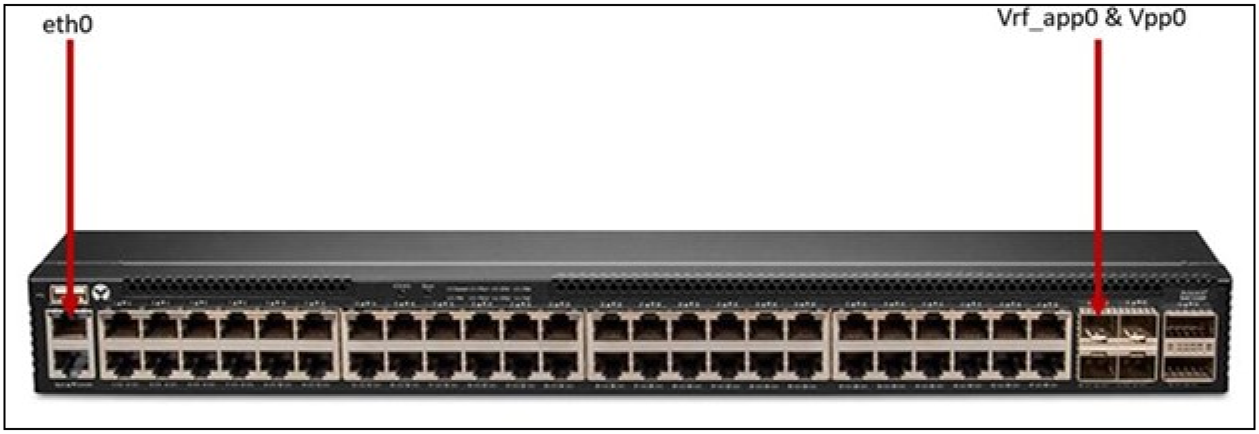
NOTE: For the changes to take effect, you must reboot the device.

Ethernet Interfaces

The Avocent RM1048P Rack Manager has three physical network interfaces (eth0, vrf_app0, Vpp0). Each interface has an individual MAC address and can be assigned an IP address statically or via DHCP. The eth0 interface (RJ45 port) is the management port reserved for system failure to perform network firmware updates from the rack manager's Open Network Install Environment (ONIE) boot menu. It is not required to assign an IP address to the eth0 interface; however, the rack manager does require the vrf_app0 and Vpp0 interfaces to be assigned IP addresses. The vrf_app0 interface provides access to the rack manager's web UI or CLI via an SSH session. The Vpp0 interface allows you to launch KVM sessions to target devices from the web UI. For instructions on configuring the vrf_app0 and Vpp0 interfaces, please see the Vertiv™ Avocent® RM1048P Rack Manager Quick Installation Guide.

NOTE: If assigning an IP address statically, the vrf_app0 and Vpp0 interfaces cannot be assigned the same IP addresses.

Figure 3.6 Avocent RM1048P Rack Manager Interface Ports



To configure a static IP address:

1. From the left-hand sidebar, click *Network Configuration - Settings*.
2. Under the Ethernet Interfaces heading, click the desired interface to open its sidebar.
3. Expand *Network Configuration* to view the settings for the selected interface.
4. Click the Edit icon (pencil) to configure the selected interface.
5. For assigning a static IP, enter the IP address, prefix length and gateway address in the appropriate fields and click *Save*.

3.7.2 DHCP

From the DHCP screen, you can configure the range of IP addresses available to target devices that are plugged into the rack manager ports. You can also alter how long leases last for the assigned IP addresses.

To navigate through the DHCP screen:

From the left-hand sidebar, click *Network Configuration - DHCP*.

- Under the Dynamic Ranges heading, use the Seconds field to configure the number of seconds the lease time lasts.
- Refer to the Lease IP Address List to view the non-expired or all leased IP addresses.
- Under the Reserved IP Configuration heading, click the Add (+) icon to reserve specific IP addresses for target devices.

3.7.3 System Interfaces

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

3.7.4 IP Pool

An IP pool is a range of reserved 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 Creating an IP pool on page 11

3.7.5 Network Address Translation (NAT) Setup

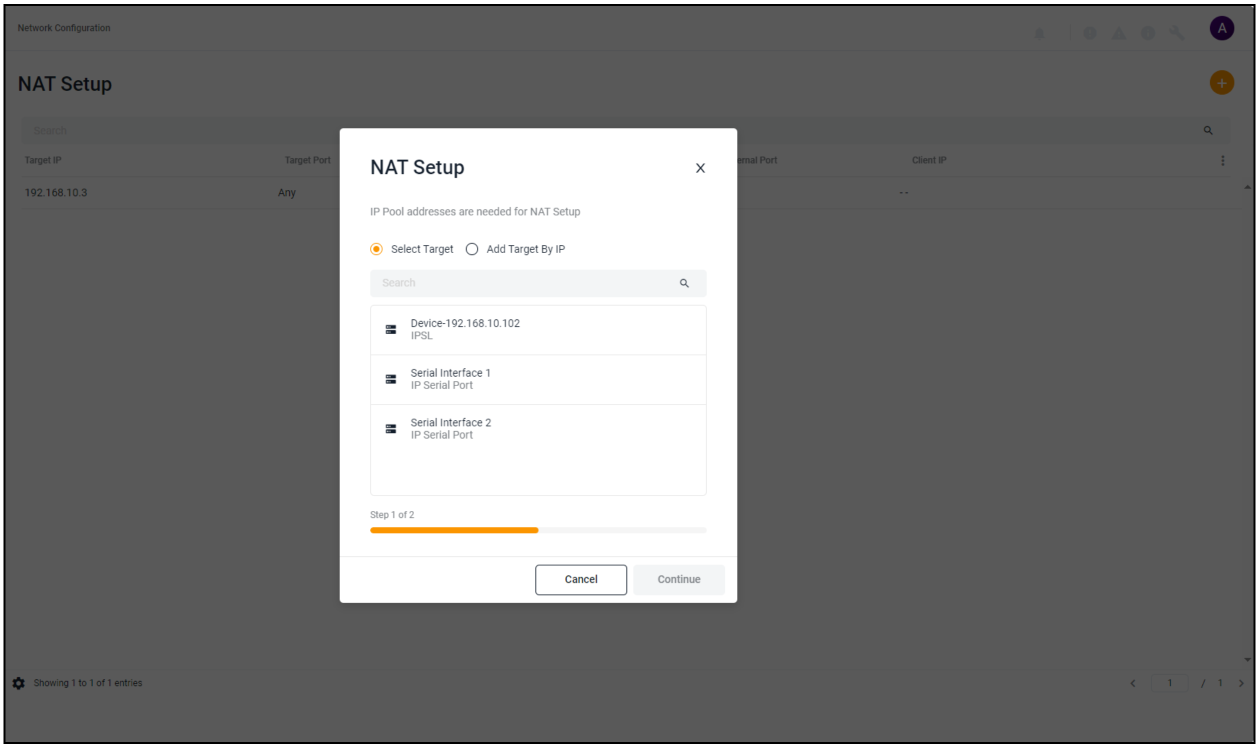
From the NAT Setup screen, you can add and configure NAT rules to perform address translations.

NOTE: To add and configure a NAT rule, you must create an IP pool to be used for the NAT rule. For instructions on configuring IP pools, please see Creating an IP pool on page 11.

To configure a 1 to 1 NAT setup:

1. From the *Network Configuration - NAT Setup* screen, click the plus (+) icon.

Figure 3.7 1 to 1 NAT Setup Overview



Target IP	Target Port	ernal Port	Client IP
192.168.10.3	Any		--

IP Pool addresses are needed for NAT Setup

● Select Target ○ Add Target By IP

Device-192.168.10.102
IPSL

Serial Interface 1
IP Serial Port

Serial Interface 2
IP Serial Port

Step 1 of 2

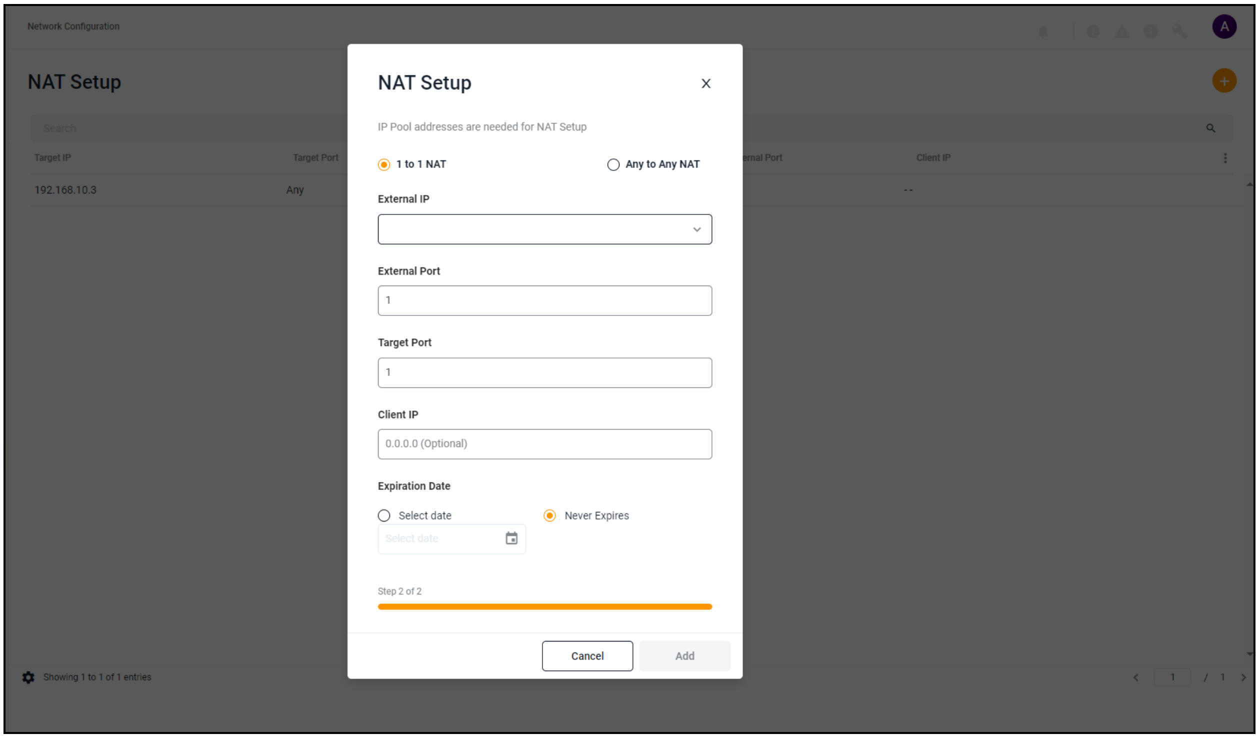
2. To add a target from the Targets List, select the *Select Target* radio button and choose the appropriate device.

   -or-

   To add a target that is not in the Targets List, select the *Add Target by IP* radio button and enter the IP address of the new target.

3. Click *Continue*. A 1 to 1 NAT Setup dialogue box appears.

Figure 3.8 1 to 1 NAT Setup Options



Network Configuration

NAT Setup

Target IP	Target Port	...rnal Port	Client IP
192.168.10.3	Any		--

Showing 1 to 1 of 1 entries

NAT Setup

IP Pool addresses are needed for NAT Setup

● 1 to 1 NAT ○ Any to Any NAT

External IP:

External Port: 1

Target Port: 1

Client IP: 0.0.0.0 (Optional)

Expiration Date

○ Select date ● Never Expires

Select date

Step 2 of 2

4. Use the drop-down menu to select the external IP.
5. Define the applicable number for the external port, target port. If required, enter the client IP.
6. To manually set the expiration date, select the Select date radio button and use the calendar feature.

   -or-

   To set a 24 hour expiration date, click the radio button for Expires in 24 hours.
7. Click *Add*.

To configure an Any to Any NAT setup:

NOTE: If a target device is set to 1 to 1 NAT, then it cannot be converted to Any to Any NAT.

1. From the *Network Configuration - NAT Setup* screen, click the plus (+) symbol in the top right corner.
2. Click the Select Target radio button to choose a target from the list.

   -or-

   Click the Add Target by IP radio button to add a target by its IP address.
3. Click *Continue*.
4. Use the External IP drop-down menu to select the external IP address.
5. In the Expiration Date section, click the Select date radio button and use the calendar feature to set an expiration date.

   -or-

   Click the Never Expires radio button.
6. Click *Add*.

3.7.6 Destination Port Mappings

From the *Network Configuration - Destination Port Mappings* screen, you can enable customized ports to support specific Service Processors (SPs) for access to the native KVM function. To define the destination port mappings, see Configuring destination ports on page 11.

3.8 Notification Settings

3.8.1 Notification Policy

To create a notification policy:

1. From the *Notification Settings - Notification Policy* screen, click the Add Notification Policy icon (+) in the top right corner. An Add Notification Policy dialogue box appears.
2. Enter the name for the notification policy.

NOTE: The Name field has a limit of 30 characters.

3. Check one of the following boxes for the Alarm Severities section: Critical, Warning or Information.
4. Use the slider to enable or disable the Alarm Cleared Notification setting.
5. In the Distribution List section, enter the appropriate information into the To or the CC field.
6. (Optional) Add a description for the notification policy, if desired.

NOTE: The Description field has a limit of 300 characters.

7. Click *Add*.

This page intentionally left blank

Appendices

Appendix A: Technical Specifications

Table 4.1 Technical Specifications Avocent 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

Appendix B: UMIQ to IPIQ Conversion

The Vertiv™ Avocent® Universal Management IQ (UMIQ) can now be upgraded to a Vertiv™ Avocent® IPIQ IP KVM device. The upgrade must be performed from the Avocent RM1048P Rack Manager Command Line Interface (CLI). Please refer to the following procedure for upgrading instructions.

To convert a Vertiv™ Avocent® UMIQ to a Vertiv™ Avocent® IPIQ IP KVM device:

1. Log into the rack manager's CLI with your username and password.
2. Enter **10** to select the Diagnostics option.
3. Enter **12** to select the Manage UMIQ to IPIQ conversion option.
4. Enter **1** to select the Enable conversion service option.

NOTE: After enabling the conversion service, it may take a few minutes for the system to register the change.

5. To view the change, enter **3**. The following information appears: the port number, MAC address, IP address and the conversion status.

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, 505 N Cleveland Ave, Westerville, OH, 43085, USA

While every precaution has been taken to ensure accuracy and completeness here, Vertiv Group Corp. assumes no responsibility, and disclaims all liability, for damages resulting from use of this information or for any errors or omissions.