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. In addition to providing physical aggregation of your devices, the rack manager enables you to connect to IT devices and Power over Ethernet (PoE) via IP consolidation and network translation. The appliance also offers keyboard, video, and mouse (KVM) capabilities and can remotely perform server management tasks, including power control and console access, on managed target devices. With the rack manager, you can benefit from flexible target device management control and secure remote access from anywhere at anytime.

Figure 1.1 Avocent RM1048P Rack Manager Descriptions

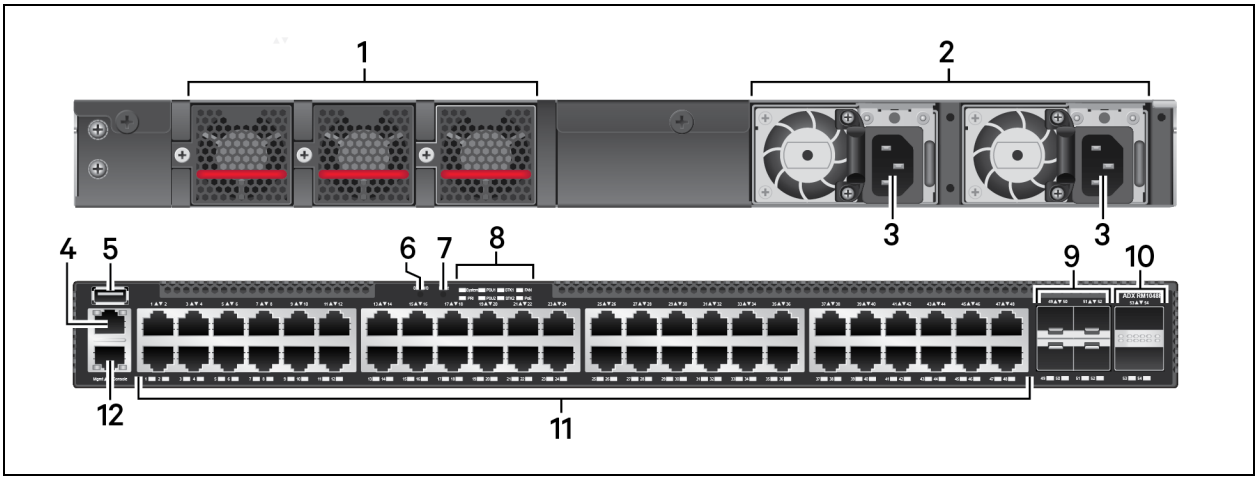


Table 1.1 Avocent RM1048P Rack Manager Descriptions

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)

The Avocent RM1048P Rack Manager operates as a managing appliance within the Vertiv™ Avocent® DSView™ Solution. The following figure and table describes the system configuration of the Vertiv™ Avocent® DSView™ Solution.

Figure 1.2 Vertiv™ Avocent® DSView™ Solution System Configuration

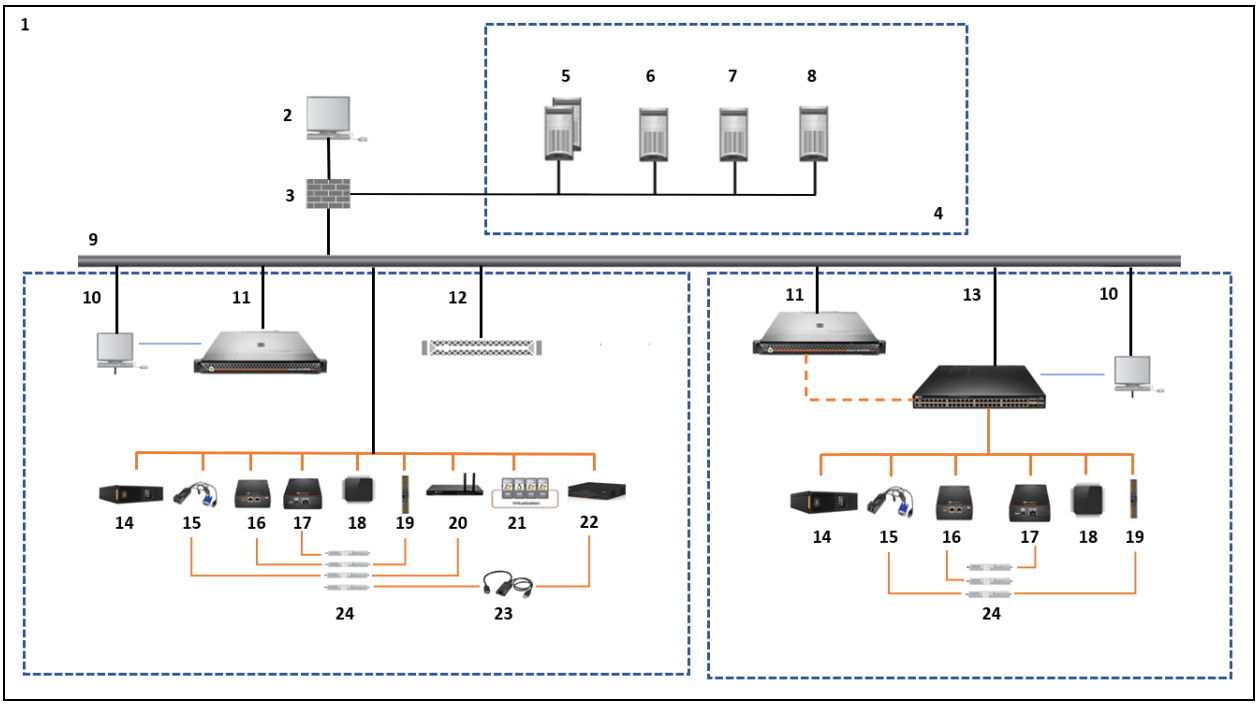


Table 1.2 Vertiv™ Avocent® DSView™ Solution System Configuration Descriptions

Number	Description	Number	Description
1	Corporate Network	13	Avocent RM1048P Rack Manager
2	Vertiv™ Avocent® DSView™ Solution Software Client	14	Uninterruptible Power Supply (UPS)
3	Firewall	15	Vertiv™ Avocent® IPIQ IP KVM Device
4	DMZ/Extranet	16	Vertiv™ Avocent® IPUHD 4K IP KVM Device
5	External Authentication Servers (Optional)	17	Vertiv™ Avocent® IPSL IP Serial Device
6	SMTP Mail Server	18	Service Processor (SP)
7	NTP Time Server	19	Power Distribution Unit (PDU)
8	Syslog Server	20	Vertiv™ Avocent® ACS800/8000 Advanced Console System
9	Private Network	21	Virtual Machines (VM)
10	CLI Client	22	Vertiv™ Avocent® MergePoint Unity™ KVM over IP and serial console switch
11	Vertiv™ Avocent® MP1000 Management Platform	23	Vertiv™ Avocent® MPUIQ module
12	Vertiv™ Avocent® MP1000 Management Platform Virtual Appliance	24	Target Devices

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, entirely digital rack manager platform to enable scaling without increasing 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 Application Programming Interface (API) automation.
- Increases the number of user sessions without the need for additional 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. In 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 opens in the new tab.

This page intentionally left blank

2 SSL Certificate Replacement

When you enter the rack manager's IP address into a web browser, you may receive an error message indicating that the SSL certificates are not recognized. 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.

3 Web User Interface (UI)

Once you have connected the Avocent RM1048P Rack Manager to a network and configured the IP addresses, you can access it via its web UI. The web UI provides direct access to the rack manager and its targets.

NOTE: The Avocent RM1048P Rack Manager requires at least two IP addresses to access the web UI and launch target sessions. For more information, refer to Ethernet interfaces on page 49.

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 IP address you previously configured for the Vrf_app0 interface. 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 Appliance View screen.

Figure 2.1 Web UI Overview

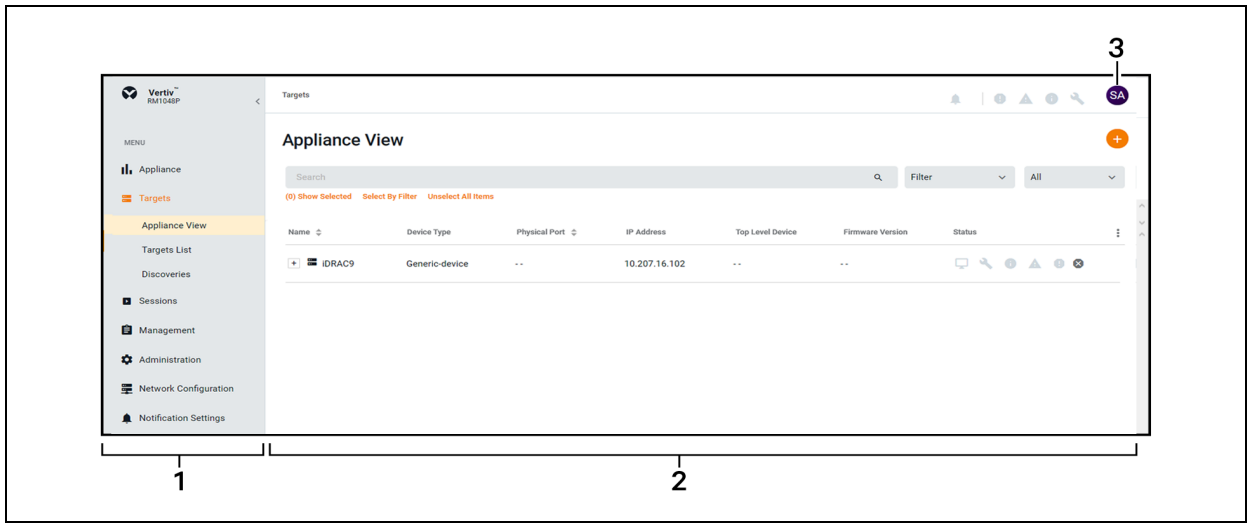


Table 2.1 Web UI Overview Descriptions

Number	Description
1	Sidebar
2	Content Area
3	User Preferences

3.1 Account Settings

You can view your account settings by clicking the profile icon in the top right corner of the web UI. The pop-up 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 following table describes the capabilities of these tabs.

Table 2.2 User Preferences

Tab	Description
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 - Select your time zone for alarms and notifications from the drop-down menu. • Time Number Separators - Select the digit grouping and decimal values from the respective drop-down menus. • 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 - Select the language to be used in the web UI from the drop-down menu.
Color Theme	Select the radio button for your desired color theme.

Help

This option redirects you to a digital copy of the Vertiv™ Avocent® RM1048P Rack Manager Installer/User Guide.

Log Out

This option immediately logs you out of the web UI.

3.2 Appliance

The Appliance tab contains two sub-menu items - Overview and Ports - from which you can view appliance information about the Avocent RM1048P Rack Manager and its ports, such as the properties and the firmware version. You can also perform general appliance functions, including resetting to factory defaults and updating firmware. Additionally, administrators can configure individual ports.

3.2.1 Overview

From the Overview screen, you can perform the following functions:

- View the serial number, model and asset tag of your appliance.
- Assign a name for easy device identification.
- Reset the appliance to factory settings.
- Update the firmware version.

To reset the appliance to factory settings:

1. From the left-hand sidebar, click *Appliance - Overview*.
2. Click the vertical ellipsis in the top right corner, then click *Reset to Factory Settings*.

To update the firmware:

1. From the left-hand sidebar, click *Appliance - Overview*.
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. Return to the Overview screen in the web UI and click the *Update Firmware* button.
6. Select whether to update the firmware for only the Avocent RM1048P Rack Manager or to update the firmware for only the connected targets.
7. Select the firmware file and click *Update*.

3.2.2 Ports

From the Ports screen, administrators can enable, configure and view the status of the ports on the Avocent RM1048P Rack Manager.

To configure a port:

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

   -or-

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

3.3 Targets

The Targets tab contains three sub-menu items - Appliance View, Targets List and Discoveries - from which you can manage your target devices. The Avocent RM1048P Rack Manager supports the following target device types:

- IP KVM devices
- Serial devices
- Service processors
- UPSes
- PDUs
- Generic devices

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 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

Refer to KVM sessions on page 18 for initial prerequisites and configurations, as well as information on launching and configuring KVM sessions.

For more information on the IP KVM devices, refer to the Vertiv™ Avocent® IPUHD 4K IP KVM Installer/User Guide and the Vertiv™ Avocent® IPIQ IP KVM Quick Installation Guide available on www.vertiv.com.

Serial devices

The Vertiv™ Avocent® IPSL IP serial device provides an innovative serial IP solution for simplifying remote access and troubleshooting devices while seamlessly scaling from edge to enterprise.

The serial management functionality of the appliance provides the following features and benefits:

- Secure remote serial access to IT devices for quick troubleshooting.
- Simultaneous management of up to four serial devices.
- Reduced power costs and simplified cabling by leveraging Power over Ethernet (PoE).
- Centralization and protection of your expensive IT equipment on-site while permitting remote access.
- Remote firmware updates of your IT devices.
- HTML5 serial viewer
- Virtual media
- Configure serial communication
- Parameters
- Data logging
- Serial over SSH

Refer to Serial sessions on page 24 for information on launching and configuring serial sessions.

For more information about the IP serial device, refer to the Vertiv™ Avocent® IPSL IP Serial Device Installer/User Guide available on www.vertiv.com.

Service processors

The Avocent RM1048P Rack Manager supports the following SPs:

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

Connecting a service processor (SP) to a rack manager provides the following features and benefits:

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

Refer to Web UI sessions on page 25 for initial prerequisites and configurations, as well as information on launching and configuring web UI sessions.

Vertiv™ 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™ PDUs

Vertiv™ PDUs distribute reliable, electric power to data centers and monitor the system's power status. Managing PDUs with the rack manager provides the following features:

- View power consumption

- Ability to power cycle devices (Power Off, Power On, Cycle)

Generic devices

NOTE: Generic devices are not supported on rack managers that are managed by the Vertiv™ Avocent® MP1000 Management Platform.

A generic device refers to any network device that can physically connect to back of the rack manager. Generic devices can be added to the rack manager's network via their IP address but cannot actively communicate with the rack manager. The support for generic devices allows for the consolidation of IP addresses in your data center and enables you to centrally access the web pages of the devices from the rack manager.

Since no communication is being established between the rack manager and generic devices, limited functionality is available for generic devices. The only available functionality for generic devices is launching the web page of the device.

Refer to Web UI sessions on page 25 to open the web page of a generic device via the rack manager.

3.3.1 Appliance view

NOTE: The Appliance View screen and Targets List screens perform the same operations; however, the Appliance View screen organizes the targets based on the appliance with which they are physically or logically associated. By default, this screen sorts the list of target devices by port number.

From the Appliance View screen, you can view and manage the target devices managed by the rack manager. You can also perform the following functions:

- Add and delete devices
- Modify device information
- Perform maintenance activities
- Merge devices
- Launch KVM, serial or web sessions
- Launch a session dashboard

Adding and deleting devices

You can discover a single or a range of target devices. Generic devices can also be added to the appliance. Adding a generic device differs from discovering other target devices because only an IP address is required to add a generic device. Therefore, the appliance cannot actively communicate with generic devices, which limits the functions you can perform on the generic device from the rack manager web UI.

Devices can be discovered manually or you can configure the Auto Discovery feature for devices to be discovered automatically once they are physically connected to the back of the rack manager. To configure Auto Discovery, refer to Auto discovery on page 46.

NOTE: To discover devices for the rack manager, you must create credential profiles 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. To create a credential profile, refer to Credential profiles on page 35.

To discover a single device or a range of devices:

1. From the left-hand sidebar, click *Targets - Appliance View*.
2. Click the Add Device icon (+) in the top right corner. The Device dialogue box appears.

3. Click the *Discover* tab.
4. Select the Single IP radio button to add a single device.

   -or-

   Select the Range IP radio button to add a range of devices.

5. Enter the discovery name.
6. If you selected the Single IP radio button, enter the IP address.

   -or-

   If you selected the Range IP radio button, enter the IP address range.

7. Select the device type from the Device Type drop-down menu.
8. Based on your selection, fill out the appropriate fields.
9. 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 Appliance View and Targets List screens.

To add a generic device:

1. From the left-hand sidebar, click *Targets - Appliance View*.
2. Click the Add Device icon (+) in the top right corner. The Device dialogue box appears.
3. Click the *Add* tab.
4. Enter the device name and IP address.
5. Click *Add*. The device is added to the Appliance View and Targets List screens.

To delete a target device:

1. From the left-hand sidebar, click *Targets - Appliance View*.
2. Click the vertical ellipsis next to the individual device you want to delete.
3. Click the *Delete* icon. It may take several minutes for the device to fully delete.

Modifying device information

You can view the properties and other device specific information via the device's information panel. The information displayed in the panel varies by device type. You can view a device's information panel by clicking on the row of the desired device. Upon selection, the panel will pop out on the right side of the screen. Any editable information will contain a pencil icon on the right side of the tab.

To modify device properties and other information:

1. From the left-hand sidebar, click *Targets - Appliance View*.
2. Click on the row of the desired device. The information panel opens.
3. Click the Edit icon (pencil) to configure the device properties.
4. When finished, click *Save*.
5. Perform steps 2 and 3 for any other editable tabs in the panel.

NOTE: If rearranging the boot order for an SP target device, you may be required to reboot the device depending on the SP model.

Performing maintenance activities

You can perform a variety of functions for each target device. Functions may include device removal, firmware updates, device reboot, resynchronization and more. The types of functions available vary by device type. To access these functions, click on the vertical ellipsis on the right side of the device row.

When performing maintenance activities such as firmware upgrades, the device can be set to Maintenance Mode.

To activate Maintenance Mode:

From the left-hand sidebar, click *Targets - Appliance View*, then hover the mouse over the desired target and click the vertical ellipsis. Click the In Maintenance Mode toggle button to enable the setting.

-or-

From the left-hand sidebar, click *Targets - Appliance View*, then click on the row of the desired device to open its information panel and click the Tool icon below the device name.

Merging devices

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, service processor 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: VMs cannot be merged.

To merge targets:

1. From the left-hand sidebar, click *Targets - Appliance View*.
2. Select the targets you want to merge by hovering your mouse over each target and clicking the box to the left of each one.
3. Click *Merge Targets*, then click *Merge*.
4. The connected targets display in a table in the content area of the web UI. A plus icon (+) appears next to the merged targets. Click the icon to expand the merged target and show each individual target. If you wish to configure the table, click the vertical ellipsis icon.

To unmerge targets:

1. From the left-hand sidebar, click *Targets - Appliance View*.
2. Check the box next to the merged target.
3. Click the *Unmerge* icon to unmerge all the targets.

   -or-

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

Launching sessions

You can launch KVM, serial or web UI sessions from two different areas of the Appliance View or Targets List screens. For more information about the different session types and activities, refer to Sessions on page 15.

NOTE: To access the web UI of a connected service processor, it must first be configured as described in Web UI sessions on page 25.

Launching a dashboard

The Launch Dashboard feature allows for multiple KVM sessions to be launched simultaneously into one dashboard. Sessions are supported for the Vertiv™ Avocent® IPIQ IP KVM device and the Vertiv™ Avocent® IPUHD 4K IP KVM device (KVM preview). This feature adds the following benefits:

- Reduced time to provision systems remotely.
- Increased awareness of system health through a NoC
- Improved productivity of test teams.
- Increased efficiency through single dashboard for remote IT management.

To launch a dashboard:

1. From the left-hand sidebar, click *Targets - Appliance View*.
2. Hover the mouse over the desired device(s) and check the box next to the device name.
3. From the top of the screen, click the Launch Dashboard icon (play symbol). The dashboard launches into a new tab in preview mode for the number of devices virtually connected through KVM.
4. The Dashboard preview screen updates every 7 to 10 seconds and provides the following features:
    - A Launch Viewer icon (play symbol) to launch a live KVM session.
    - A Full Screen icon to maximize the screen size.
    - A Delete icon (trash can) to remove the widget from the dashboard.
    - A Maintain Aspect Ratio check box to configure the desired aspect ratio for the widgets.
    - A drop-down menu to configure the size of the widgets.

3.3.2 Targets list

From the Targets List screen, you can perform the same operations that are available from the Appliance View screen. Unlike the Appliance View screen, the targets are not organized by the appliance to which they are associated.

3.3.3 Discoveries

From the Discoveries screen, you can discover target devices by entering a range of IP addresses. Two tabs are displayed on this page: Range and Appliance. The Range tab displays the different range discovery tasks that are currently being performed. The Appliance tab displays the target devices that have been discovered as a result of the range discovery tasks.

To navigate the Discoveries screen:

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

- View the different discovery logs by clicking the *Range* or *Appliance* tab.
- Search for specific tasks or target devices using the search bar.
- Conduct searches based on an IP address using the Start IP and End IP bars .
- Filter searches by discovery status using the All Status drop-down menu.

3.4 Sessions

The Sessions tab contains one sub-menu item - Sessions List - from which you can view session information for past and current sessions. The Avocent RM1048P Rack Manager allows you to launch multiple sessions simultaneously to access your target devices via the rack manager web UI.

3.4.1 Sessions list

From the Sessions List screen, you can view the log of active and closed sessions that have been launched from your rack manager.

To navigate the Sessions List screen:

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

- View the session log based on status by clicking the *Active*, *Closed* and *All* tabs.
- Search for specific sessions using the search bar.
- View a device's information panel, which includes the Properties and User Sessions drop-down menus, by clicking the target name.
- Sort the columns in ascending or descending order by clicking the arrows next to the column name. Columns can be sorted by target name, start time, user and target IP address.
- Export data as a CSV file.

Exporting data

You can easily export and share your session data information as a comma-separated values (CSV) file. Before exporting data, ensure the appropriate email server has been set up on the system.

To export data as a CSV file:

1. From the left-hand sidebar, click *Sessions – Sessions List*.
2. (Optional) Filter the list of sessions, as desired.
3. Click the Export icon in the right corner to export the Active, Closed, or All page. The Export List to CSV dialogue box appears.
4. Review the dialogue box and verify once more that the CSV file is set to be sent to the correct email address.
5. Click *Export*. The CSV file is sent to the specified email address.

The following table provides descriptions of the columns in the CSV file.

Table 2.3 CSV File Field Descriptions

Column Name	Description
Id	Unique identification of the session
Name	Name of the session
TargetId	SIP (Session Initiation Protocol) address of the session target
TargetName	Name of the session target
TargetIpAddress	IP address of the session target
DeviceId	Unique identification of the device
ParentId	Unique identification of the parent session ("NA" if not applicable)
MergedGroupId	Unique identification of the merged group
ConnectionPath	Connection path of the session ("NA" if not applicable)
StartTime	Start time of the session
EndTime	End time of the session
Status	Status of the session
SessionMode	Mode of the session
CreateTime	Creation time of the session
UpdateTime	Last update time of the session
DeleteTime	Deletion time of the session ("NA" if not applicable)
UsersSessions	List of user session details associated with the session
Username	Username of the user associated with the session
Mode	Mode of the user session: • SM_UNDEFINED = session is not yet defined • SM_NORMAL = normal active session that maybe shared with other users • SM_SHARING_ACTIVE = active sharing session (multiple users control keyboard and mouse. This session got approved by the primary user.) • SM_SHARING_PASSIVE = passive sharing session (No keyboard/mouse interaction and no Virtual Media, video only. This session got approved by the primary user.) • SM_STANDALONE_PASSIVE = standalone passive session. (No keyboard/mouse interaction and no Virtual Media, video only.). Session will not be interrupted for any sharing request. • SM_STEALTH = shared session in stealth mode (No keyboard/mouse interaction and no Virtual Media, video only and the session will be hidden to other shared users. When primary user closes the session, this session will be closed automatically.) • SM_EXCLUSIVE = private session that does not allow sharing by other users. While setting session as exclusive session, if there are any shared sessions then those sessions will be closed automatically.) • SM_PREEMPT = preempt session. Existing session will be preempted and this session will become primary session. • SM_LOCAL_PORT = sessions involving the local port (may not be shared/stealthed/anything)
State	State of the user session: • SS_PENDING = session is defined but not yet connected • SS_INITIATED = session initiated in the process to be connected • SS_CONNECTED = session is connected

Table 2.3 CSV File Field Descriptions (continued)

Column Name	Description
	• SS_TERMINATED = session was terminated by another user • SS_EXPIRED = session was terminated (based on session timeout interval) • SS_REJECTED = session request to share read-only or interactive was rejected, session was never connected • SS_RECONNECTING = session got interrupted by network. Session is in re-connecting state • SS_RECONNECTED = failed to reconnect the session

Type	Type of user session:
	• ST_UNSPECIFIED = 0; // the value has not been specified
	• ST_KVM = remote Keyboard/Video/Mouse session
	• ST_VIRTUAL_MEDIA = remote Virtual Media session
	• ST_SERIAL = remote serial (such as RS-232) session
	• ST_VIRTUAL_MACHINE = remote Virtual Machine session
	• ST_SSH = remote SSH session
	• ST_NATIVE_WEB = allows user to access device's web interface
	• ST_SSH_PASSTHROUGH = remote SSH passthrough session
	• ST_LOCAL_KVM = remote Keyboard/Video/Mouse session (using local port)
	• ST_LOCAL_VM = remote Virtual Media session (using local port)
	• ST_LOCAL_SERIAL = remote serial (such as RS-232) session (using local port)

Client	IP address of the client
StartTime	Start time of the user session
EndTime	End time of the user session

3.4.2 KVM sessions

The Avocent RM1048P Rack Manager conducts KVM sessions using the web-based 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 centrally managing 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.

This section covers the following topics for KVM sessions:

- Supported browsers and processors
- Launching KVM sessions
- Configuring KVM sessions
- Using virtual media
- Sharing KVM sessions
- Reconnecting to KVM sessions

Supported browsers and processors

The HTML5 Video Viewer supports the following web browsers:

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

The following table describes the compatibility of the HTML5 Video Viewer capabilities for each supported browser.

Table 2.4 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	✓	✓	×	×
Browse disk image	Tools -> Browse Disk Image	✓	✓	×	×

The following table specifies which service processors and ports are supported by the rack manager for launching KVM sessions.

Table 2.5 Supported Processors and Servers

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 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:

1. From the left-hand sidebar, click *Targets - Appliance View*.
2. Hover the mouse over the desired target and click the Launch KVM Session icon.

   -or-

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

To close a KVM session:

From the Video Viewer session, click the user icon in the upper right-hand corner and select *Exit Viewer*.

Configuring KVM sessions

After launching a KVM session, you can use the menu located at the top of the Video Viewer window to access the features described in the following table. You can also configure the settings for the Avocent RM1048P Rack Manager using the *Settings* icon. Table 2.6 on the next page provides descriptions of the various KVM features. The availability of the KVM Video Viewer features varies by device type.

Table 2.6 KVM Video Viewer Features

Tab	Feature	Description
File	Open Server-side Recording File	Open a server-side recorded file to play.
	Paste Text From File	Copy text content from a text file and send it to the target.
View	Audio & Video Options	**NOTE: These settings apply to all users.** • *Audio Configuration* - Configure the number of audio channels and audio quality level. • *Video Color Settings* - Display more color options to optimize fidelity or less colors to reduce the volume of data transferred on the network. The maximum speed is Grayscale 16 Shades, and the maximum video quality is Color 24 bit. • *Video Noise Filter* - Enable noise filter for VGA or disable it for a digital video source. • *Video Lane Settings* - Configure USB-C lane speed and view the number of current video lanes.
	Refresh	Refresh the session.
	Full Screen	Enable Full Screen mode with or without single-cursor mode.
	Scaling	Adjust the size of the ratios of the session screen by configuring or selecting the Fit to Window, Stretch to Window or Zoom setting.
	Max Resolution	Select the maximum target resolution for your KVM session. This setting applies to all users and affects the actual video resolution of your target systems OS.
	Single Cursor	Enable single-cursor mode.
	Statistics	View KVM statistics.
	User Information	View general user information.
	Status Bar	Display or hide the status bar at the bottom of the screen.
Macros	Static Macros	Send multi-key commands to make sure the command string is accurate. After you select the applicable operating system, select *Static Macros* to access the list of command strings that are valid for the selected operating system. Send a string of commands by clicking the desired string from the Static Macros list and clicking *Send*. The options in the drop-down list are pre-determined based on the macro set you select. If you are looking for a command string that does not appear in the list, verify that you have selected the correct operating system in the Manage Macros window. **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.**
	Manage	Define macros from the Manage Macros window.
Tools	User Preferences	Select the keyboard language and configure the settings for pasting text, dragging and dropping files/folders and recording.
	Instant Message	Send a message to all users currently logged in.
	Capture Screen	Capture a screenshot of the session.
	Mouse Modes	Select a mouse mode: Absolute, Relative (no acceleration) or Relative
	Align Local Cursor	Align the cursor with the view orientation of the session.
	Reset Keyboard/Mouse USB	If you begin experiencing issues with your keyboard or mouse, you can reset the device.
	Exclusive Mode	Enable Exclusive Mode when you need to access a target while excluding all other users. When a target is

Table 2.6 KVM Video Viewer Features (continued)

Tab	Feature	Description
		selected with the Exclusive Mode setting enabled, no other user in the system can switch to that target.
Tools (continued)	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.
	Start Recording	Begin recording a video of the session.
	Optimize Network Bandwidth	Optimize your network bandwidth for better session performance.
	Remote Audio	Enable or disable remote audio.
	Create ISO Image	Create an ISO image to store data from the target session.
	Browse Disk Image	Browse to a saved disk image.
Virtual Media	See Using virtual media on the next page.	

The following table compares the HTML5 Video Viewer features available for the standalone and managed Vertiv™ Avocent® IPUHD 4K IP KVM device and the managed Vertiv™ Avocent® IPIQ IP KVM device.

Table 2.7 Feature Comparison for IP KVM Device Viewers

Feature	Standalone 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 (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)	✓	✓	×

Using 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. From the KVM Video Viewer session, click the *Virtual Media* tab, then click *Connect*.
2. After the session is activated, use the Virtual Media drop-down menu to select the type of file to map. Click *Map ISO image or Files/Folder* to map an .iso file.

   -or-

   Click *Map Removable Disk Image* to map an .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 KVM Video Viewer session, click the *Virtual Media* tab, then click the mapped drive to unmap that drive.

   -or-

   Click *Deactivate* to unmap all the drives.
2. At the prompt, click *Yes*.

Sharing KVM sessions

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 are as follows:

Table 2.8 Session Sharing Options

Option	Description
Active Sharing	You, as well as other users, can interact with the target.
Passive Sharing	Access is granted to the target in read-only mode. The other user knows you are viewing the session.
Preempt	The previous user's session is interrupted and terminated.
Stealth	Access is granted to the target in viewer-only mode. 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. The following options are available: Approve, Reject or Allow as read-only.

Reconnecting to KVM sessions

When a KVM session disconnects from the target device but still maintains a connection to the managing appliance, the viewer will automatically attempt to re-establish a connection to the target device. Viewer Reconnect is a session capability available for the Avocent RM1048P Rack Manager, the Vertiv™ Avocent® MP1000 Management Platform, and the Vertiv™ Avocent® MP1000VA Management Platform Virtual Appliance. Supported target devices for Viewer Reconnect include the Vertiv™ Avocent® IPIQ IP KVM device and the Vertiv™ Avocent® IPUHD 4K IP KVM device.

3.4.3 Serial sessions

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

Launching serial sessions

To launch a serial session:

1. From the left-hand sidebar, click *Targets - Appliance View*.
2. Hover the mouse over the desired serial device.
3. On the right of the column, click the Launch Serial Session icon.

   -or-

   Click the vertical ellipsis and select whether to launch the serial session in a new tab or new window.

To end a serial session:

From the serial session menu, click the user icon in the upper right-hand corner and select *Exit Serial Viewer*.

Configuring serial sessions

Upon launching a serial session, you are presented with the CLI of the target serial device.

Some basic and useful keys include:

- Press **Tab** (once/twice) to show the next possible command(s) or option(s).
- Press the up/down arrows to navigate the command history.
- Enter **ls** to show the list of sub-nodes.
- Enter **show** to show the available configuration in the node.
- Press **ctrl** + **E** to get the current parameter value for editing.
- Press **** to escape spaces, '\' and other control characters when assigning values to parameters.

You can use the menu located at the top of the Serial Viewer window to access the features described in the following table.

Table 2.9 Serial Viewer Features

Tab	Feature	Description
File	Save As...	Save a copy of the log file.
Edit	Copy	Copy, paste, select all or clear the text of the CLI.
	Paste	
	Select All	
	Clear	
Tools	Start Logging	Begin logging the serial session. When finished, click Stop Logging and the log file will automatically downloaded to your local system.

3.4.4 Web UI sessions

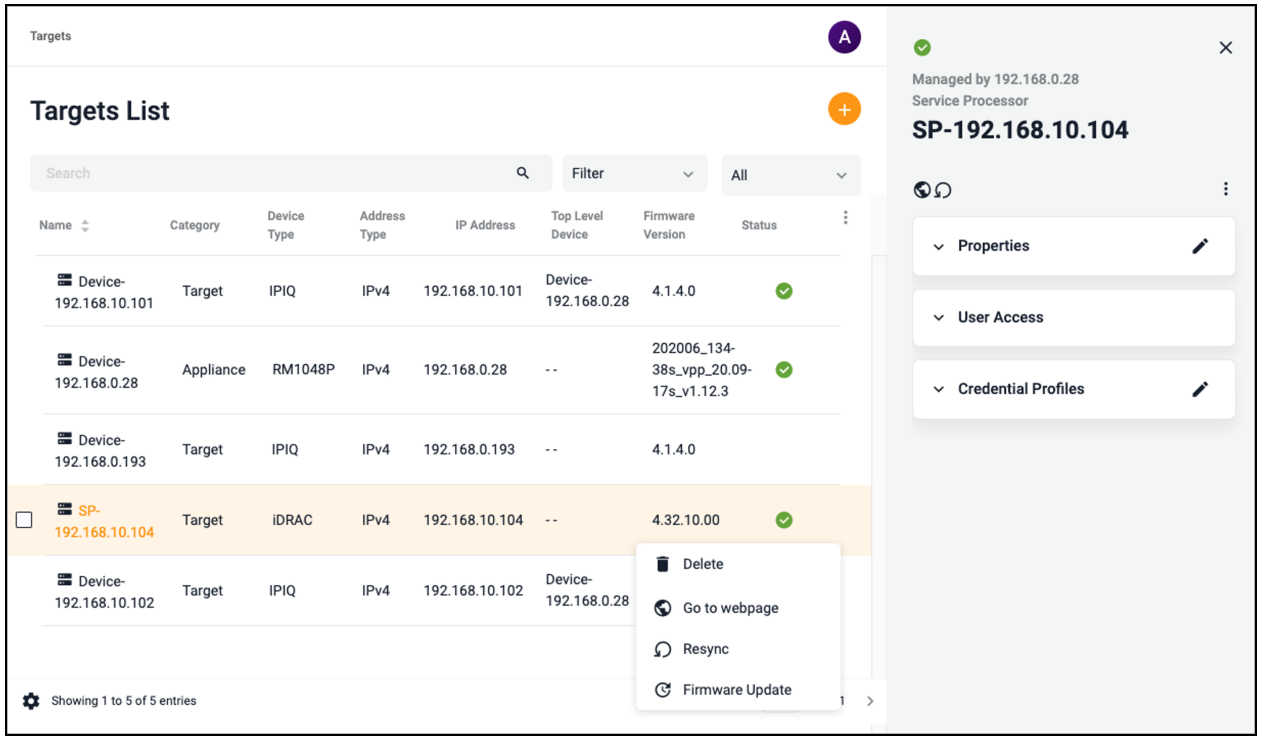
Service Processors (SPs) and generic devices can be remotely accessed from the rack manager by launching web UI sessions.

NOTE: Before launching a web UI session for an SP, ensure that you have created an IP pool and configured the destination port mapping. For more information, refer to IP pool on page 50 and Destination port mappings on page 53.

To launch a web UI session:

1. From the left-hand sidebar, click *Targets - Appliance View*.
2. Click on the row of the desired device. The device's side information panel opens on the right side of the screen.

Figure 2.2 SP Target Device



3. Click the *Go to webpage* icon (globe). You are redirected to the webpage of the device.

3.5 Management

The Management tab contains one sub-menu item - Devices - from which you can view general management information about connected target devices. The Avocent RM1048P Rack Manager maintains a log of connected target devices, in which the devices are categorized as either managed or unmanaged and split into separate tabs respectively.

3.5.1 Devices

From the Devices screen, you can view the log of managed and unmanaged target devices connected to the rack manager.

To navigate the Devices screen:

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

- View the different logs of target devices by clicking the *Managed* or *Unmanaged* tab.
- Add a new device by clicking the Add icon (+) and filling out the required fields.
- View a managed device's settings by clicking on the orange link in the Name column.

3.6 Administration

The Administration tab contains nine sub-menu items - User Management, Roles & Permissions, Credential Profiles, Events, Alarms, Authentication Providers, Firmware Updates, System Settings and Scheduler - from which administrators can access the advanced settings to configure and manage the rack manager and its target devices.

3.6.1 User management

From the User Management screen, you can view and configure the user and group accounts. The User Management screen contains two individual tabs for Users and Groups. For more information about these tabs, see Users below and Groups on the next page.

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, refer to Groups on the next page.

Users

From the Users tab, you can view all users and user specific information for the Avocent RM1048P Rack Manager. You can also create and delete users and configure user password expiration settings.

To navigate the Users tab:

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

- Add or delete a user.
- Configure the user by hovering your mouse over the user and clicking the vertical ellipsis on the right.
- Configure the columns displayed in the table by clicking the vertical ellipsis in the right corner of the table and clicking *Table Configuration*.
- Open the user's information panel by clicking on the user. From the information panel, you can:
  - View user properties and other information, if applicable.
  - Configure the user's name, email and password expiration time by expanding the Properties menu and clicking the Edit icon (pencil).

To add a new user:

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

To configure a user's password expiration time:

1. From the *Users* tab, click the desired user to open the information panel.
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*.

Groups

From the Groups tab, you can view all groups for the Avocent RM1048P Rack Manager. A user group defines what the user can do within the web UI and CLI, regarding appliance settings and administration. You can also create and delete user groups, assign target devices to groups and perform group mapping.

To navigate the Groups tab:

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

- Add or delete a user group.
- Open the group's information panel by clicking on the group. From the information panel, you can:
  - 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 add a user group:

1. From the *Groups* tab, 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 icon (pencil) 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, refer to Configuring roles and permissions on page 34.
6. Click *Save Changes*. The user group has now been created and assigned permissions.

To delete a user group:

1. From the *Groups* tab, hover the mouse over the desired group and check the box on the left.

2. Click the Delete icon (trash can) above the list of groups.
3. At the confirmation screen, click *Yes* to delete.

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. From the *Groups* tab, click the desired user group to open its information panel, then click the Edit icon (pencil) 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*.

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, refer to Authentication providers on page 40.

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 *Groups* tab, click on the desired local user group. The information 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 and permissions

From the Roles & Permissions screen, you can configure 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. For more information on the default roles, refer to System roles below and Target roles below.

For information on adding, deleting or editing roles and permissions for the Avocent RM1048P Rack Manager, refer to Configuring roles and permissions on page 34.

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, refer to Groups on page 28.

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

Table 2.10 on the facing page 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 2.10 Roles and Permissions

User Permission	System Roles				Target Roles	
	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 User Profile	✓	✓	✗	✗	✗	✗
View User Profile	✓	✓	✗	✗	✗	✗
Configure User Policy	✓	✓	✓	✓	✗	✗
View User Profile	✓	✓	✓	✓	✗	✗
Configure User Policy	✓	✗	✓	✗	✗	✗
View User Policy	✓	✗	✓	✗	✗	✗

Table 2.10 Roles and Permissions (continued)

User Permission	System Roles				Target Roles	
	System Administrator Role	System Maintainer Role	User Administrator Role	User Role	User Target Role	System Maintainer Target Role
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	✓	✓	✗	✗	✗	✓
KVM Screen recording	✓	✓	✗	✗	✗	✓
KVM Remote Audio	✓	✓	✗	✗	✗	✓

Table 2.10 Roles and Permissions (continued)

User Permission	System Roles				Target Roles	
	System Administrator Role	System Maintainer Role	User Administrator Role	User Role	User Target Role	System Maintainer Target Role
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	✓	✓	✗	✗	✗	✗
View Sys Log	✓	✓	✗	✗	✗	✗
Posts to Event Log	✓	✓	✗	✗	✗	✗

Table 2.10 Roles and Permissions (continued)

User Permission	System Roles				Target Roles	
	System Administrator Role	System Maintainer Role	User Administrator Role	User Role	User Target Role	System Maintainer Target Role
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	✓	✓	✗	✗	✗	✗

Configuring roles and permissions

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, refer to the following procedure.

To add a new role:

1. From the left-hand sidebar, click *Administration - Roles & Permissions*.
2. Select the *Target Roles* tab to create a target role.

   -or-

   Select the *System Roles* tab to create a system role.
3. Click the Add icon (+) in the top right corner.
4. Enter a name and description for the role.
5. Check the desired box(es) to add permissions.

   -or-

   Check the Select All box to add all permissions.

6. Click *Add Role*.

To configure an existing role:

NOTE: The default roles cannot be configured.

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

To delete a role:

NOTE: The default roles cannot be deleted.

1. From the left-hand sidebar, click *Administration - Roles & Permissions*.
2. Hover the mouse over the desired role and check the box to the left.
3. Click the Delete icon (trash can).
4. 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.

From the Credential Profiles screen, you can view and create the credential profiles that will allow you to access 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.

Creating a credential profile

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 with Username/Password credentials:

1. From the left-hand sidebar, click *Administration - Credential Profiles*.
2. Click the Add icon (+) in the top right corner. An Add credential profile dialogue box appears.
3. Enter a profile name.
4. From the Profile Type drop-down menu, click *Username/Password*.
5. Enter the username and port number.
6. Enter and confirm the password.
7. (Optional) Add a note.
8. Click *Add credential profile*.

To create a credential profile with SNMPv1/v2 credentials:

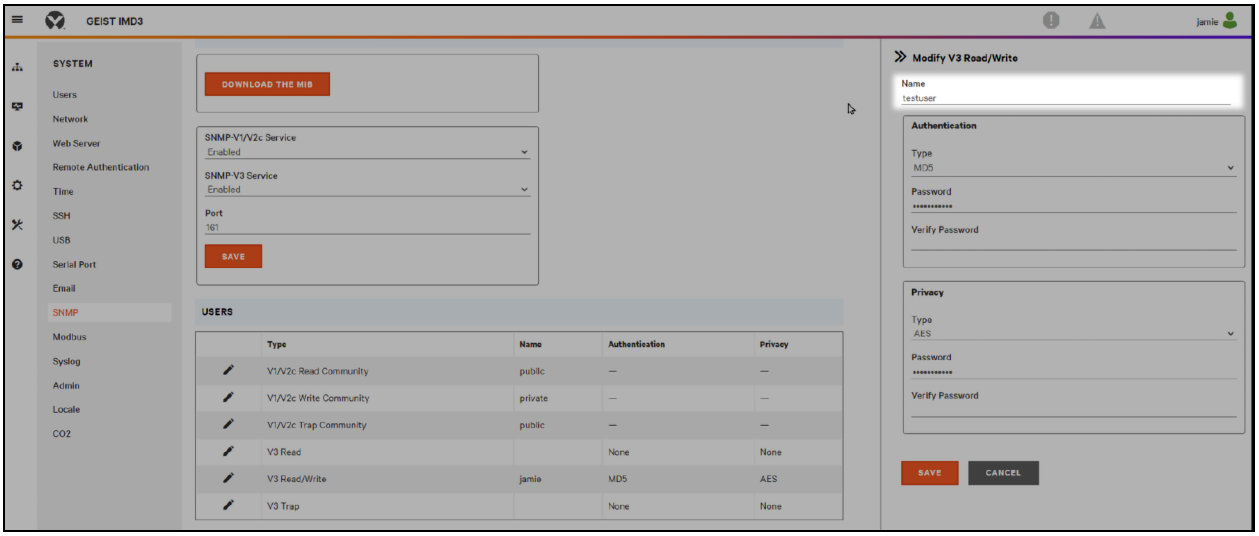
1. From the left-hand sidebar, click *Administration - Credential Profiles*.
2. Click the Add icon (+) in the top right corner. An Add credential profile dialogue box appears.

3. Enter a profile name.
4. From the Profile Type drop-down menu, click *SNMPv1/v2*.
5. Specify the version in the Version field: *SNMPv1* or *SNMPv2*.
6. Enter the port number.
7. Enter the read community.
8. (Optional) Enter the write community, trap community and any notes you wish.
9. In the Firmware Update Credentials section, enter the username and password.
10. Click *Add credential profile*.

To create a credential profile with SNMPv3 credentials:

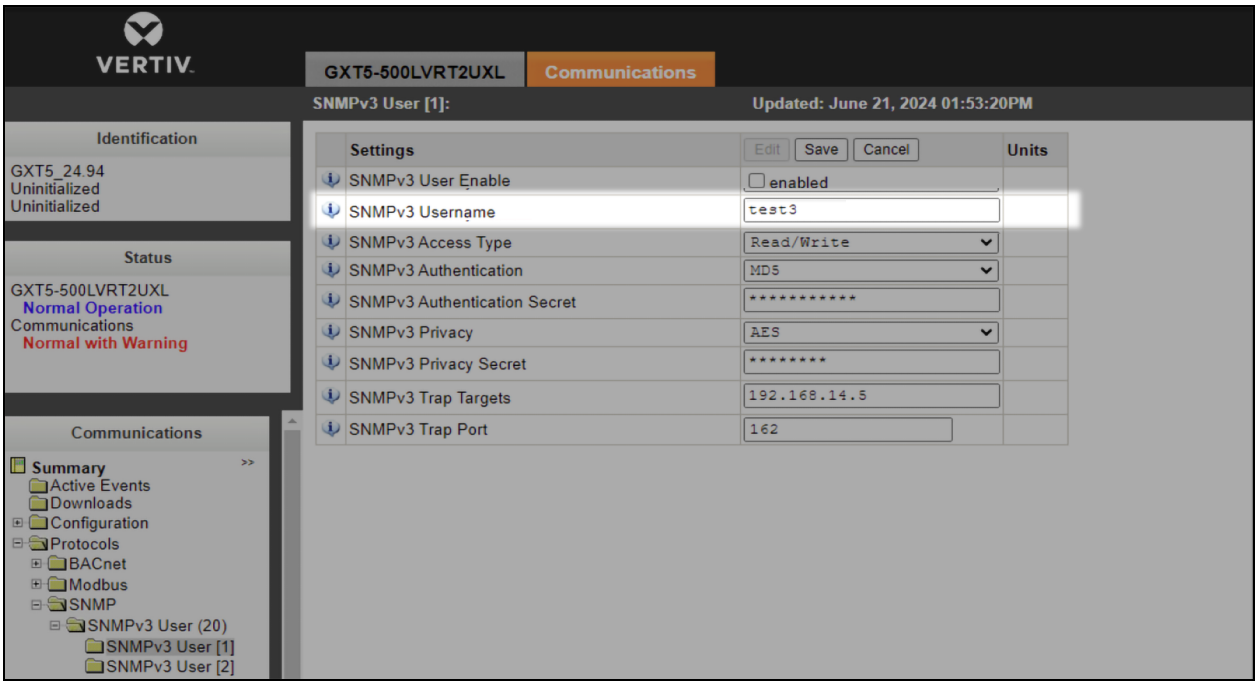
1. From the left-hand sidebar, click *Administration - Credential Profiles*.
2. Click the Add icon (+) in the top right corner. An Add credential profile dialogue box appears.
3. Enter a profile name.
4. From the Profile Type drop-down menu, click *SNMPv3*.
5. Enter a valid username.
    - Vertiv™ Geist™ rPDUs require the username to match the existing SNMPv3 username configured on the device. For example, refer to Figure 2.3 below.

Figure 2.3 Rack PDU Username Example



- Vertiv™ Liebert® rack UPSes require the username to match the existing SNMPv3 username configured on the device. For example, refer to Figure 2.4 on the facing page.

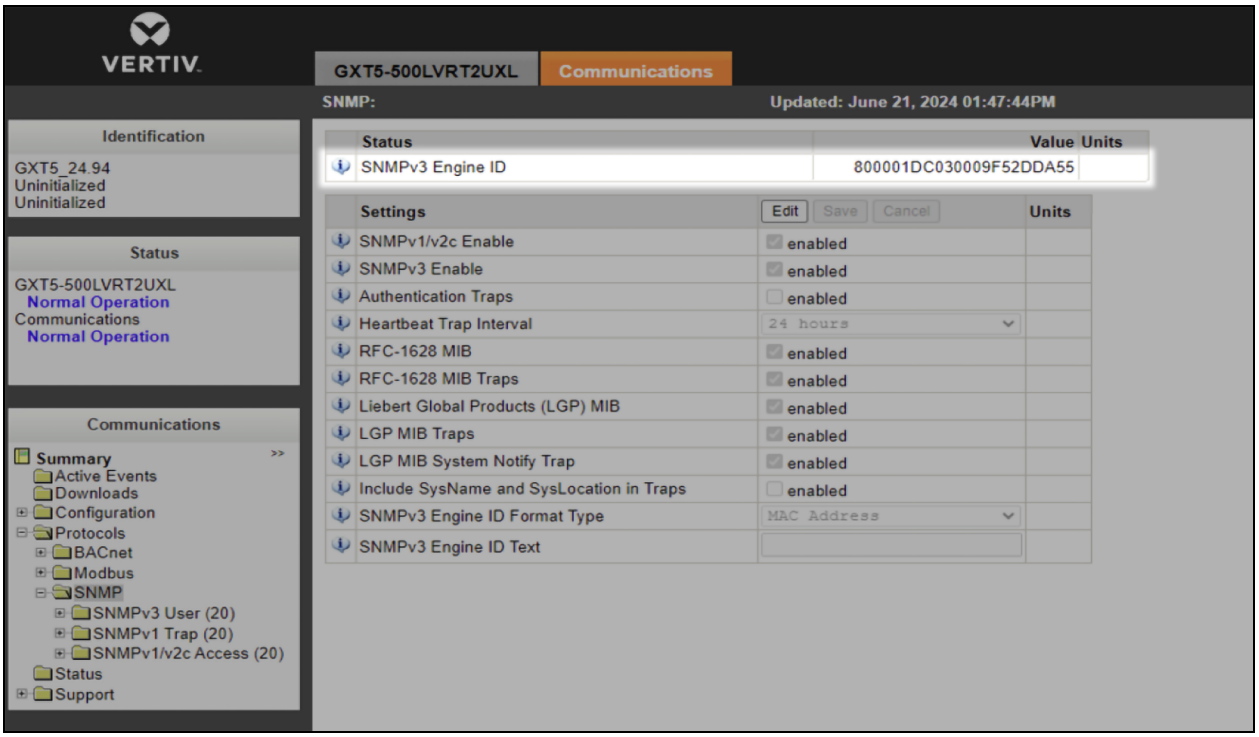
Figure 2.4 Rack UPS Username Example



6. (Optional) Enter an engine identification number in the Engine ID field. The engine ID is required by the managing appliance to receive and process SNMPv3 traps from the device.
   - For Vertiv™ Geist™ rPDUs, the engine ID follows this pattern: 80001F8803 + MAC address without including any colons in the MAC address. For example, if the device's MAC address is 00:19:85:0A:A8:17, then the engine ID is 80001F88030019850AA817.
   - For Vertiv™ Liebert® rack UPSes, the engine ID follows this pattern: 800001DC03 + MAC address without including any colons in the MAC address. For example, if the device's MAC address is 00:02:99:2C:77:A8, then the engine ID is 800001DC030002992C77A8.

NOTE: The engine ID is configurable for the rack UPS device. For example, refer to Figure 2.5 on the next page.

Figure 2.5 Rack UPS Engine ID Example

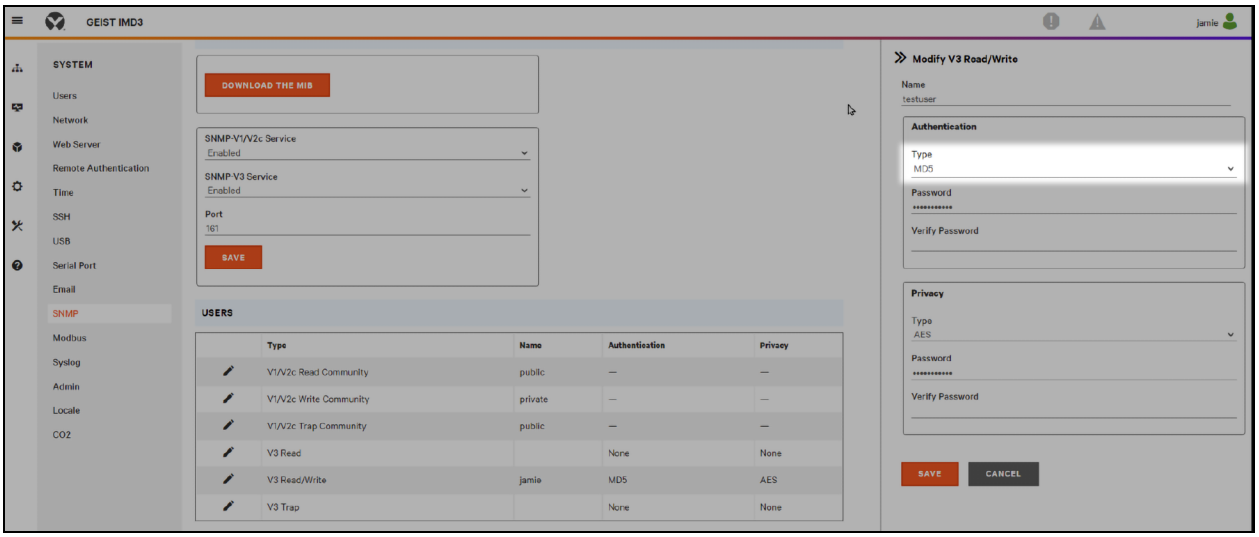


7. Enter a port associated with SNMPv3 in the Port field. The default port is 161.
8. (Optional) Enter the context name in the Context Name field. The SNMPv3 context allows multiple instances of the same SNMP object on a device.
9. (Optional) Enter the context ID in the Context ID field.

NOTE: When connecting to a Vertiv™ Geist™ rPDU using the SNMPv3 protocol, the network connection may be slow and may require multiple attempts to discover the device.

NOTE: If an error occurs with authenticating the Vertiv™ Geist™ rPDU using the SHA1 cryptography hash function, it is recommended to configure the device with the MD5 cryptography hash function. For example, refer to Figure 2.6 on the facing page.

Figure 2.6 MD5 Cryptography Hash Function Example



3.6.4 Events

From the Events screen, you can view the saved log of system events that have occurred.

To navigate the Events screen:

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

- Search for a specific event using the search bar.
- Filter events by severity (*All Severities, Info, Warning* or *Critical*) using the Filters drop-down menu.
- Sort events in ascending or descending order by clicking the arrows next to each column.
- View the information panel for each event by clicking on the desired event.
- Configure the columns displayed in the table by clicking the vertical ellipsis in the right corner of the table and clicking *Table Configuration*.

3.6.5 Alarms

From the Alarms screen, you can view the types of alarm alerts for the target devices. You can also clear alarms manually.

To navigate the Alarms screen:

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

- Search and filter for a specific alarm alert by IP address or device name using the Search and Filter bar.
- Filter alarms:
    - By date using the calendar feature.
    - By device type using the All Device Type drop-down menu.
    - By alarm type using the All Alarm Type drop-down menu.
    - By severity (*All Severities, Info, Warning* or *Critical*) using the All Severities drop-down menu.
- View the different alarm statuses by clicking the *Active, Cleared* and *All* tabs.
- Configure the columns displayed in the table by clicking the vertical ellipsis in the right corner of the table and clicking *Table Configuration*.

To clear the alarms manually:

1. From the left-hand sidebar, click *Administration - Alarms*.
2. Hover the mouse over the desired alarms and check the box to the left for each one.

   -or-

   Click the vertical ellipsis to the right of the individual alarm.
3. Click the *Clear Alarms* icon. A Clear Alarm dialogue box appears.
4. Click *Continue*.

3.6.6 Authentication providers

From the Authentication Providers screen, you can view the list of configured authentication providers. You can also add and enable a new provider, delete an existing provider, update the order of providers and configure role mapping for Active Directory.

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 left-hand sidebar, click *Administration - Authentication Providers*.
2. Click the Add Authentication Provider icon (+) in the top right corner.
3. Select *AD/LDAP, TACACS+* or *RADIUS* as the authentication type from the pop-up menu. A dialogue box appears for the chosen authentication type.
4. Enter the required configuration information for your authentication server.
5. When finished, click *Add Provider*.

To enable an authentication provider:

1. From the left-hand sidebar, click *Administration - Authentication Providers*.
2. Click the vertical ellipsis next to the desired provider.
3. Click *Enable*.

To delete an authentication provider:

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

To update the providers order:

1. From the left-hand sidebar, click *Administration - Authentication Providers*.
2. Click the Add icon (+) in the top right corner.
3. Select *Update providers order* in the drop-down menu.
4. Use the right-hand drag icon to rearrange the providers as desired.
5. 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. Select the local role that the remote group will be mapped with from the drop-down menu.
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

From the Firmware Updates screen, you can view the status of the scheduled firmware updates.

To navigate the Firmware Updates screen:

- View the status of the firmware update by clicking the plus symbol (+) on the left side of the row.
- Refresh the page by clicking the Refresh icon in the top right corner.
- Configure the columns displayed in the table by clicking the vertical ellipsis in the right corner of the table and clicking *Table Configuration*.

For information on updating the firmware, refer to Overview on page 8.

3.6.8 System settings

From the System Settings screen, administrators can view and configure the system settings for the Avocent RM1048P Rack Manager. System settings include the following:

- Password policy
- Lockout policy
- Timeout
- Date and time
- Events retention
- Alarms retention
- Viewer settings
- Standalone KVM viewer settings
- Federal Information Processing Standards (FIPS) module
- Email server configuration
- Notification configuration
- SSH passthrough

- Auto discovery
- Auto device cleanup
- Certificate
- Reboot appliance
- Factory reset

NOTE: All configurations described in this section can be performed from the *Administration - System Settings* screen. You can use the sidebar menu to navigate through the System Settings page.

Password policy

You can configure global password rules for all user accounts and configure expiration settings. By default, passwords must have a minimum of eight characters and all other password expiration rules are pre-defined. The maximum number of characters permitted is 64.

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.

To configure the password policy:

1. From the sidebar of the System Settings screen, click *Password Policy*.
2. Use the toggle buttons and provided fields to configure the password settings.

Lockout policy

You can configure global lockout rules for all user accounts. By default, a user is locked out of the UI after three failed login attempts. After 20 minutes, the user's account is unlocked, and they may attempt to login again.

To configure the lockout policy:

1. From the sidebar of the System Settings screen, click *Lockout Policy*.
2. Click the Lockout toggle button to enable or disable lockout. If enabled, the user account will be locked out after a set number of failed login attempts.
3. In the Failed Login Attempts field, enter the number of failed login attempts a user is permitted before their account is locked.
4. Click the Login Retry Timeout toggle button to enable or disable a timeout that will force the user to wait before logging in after each failed login attempt.
    a. If you enabled the Login Retry Timeout button, enter the duration of the timeout in the Retry Timeout field.
5. Click the Automatically Unlock Account toggle button to unlock the account that was locked out after a set amount of time.
    a. If you enabled the Automatically Unlock Account button, enter the duration of time before the account is automatically unlocked in the Automatic Unlock Time field.

Timeout

You 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.

To configure the inactivity timeout settings:

1. From the sidebar of the System Settings screen, click *Timeout*.

2. Click the toggle button to enable or disable automatic log out of a user account after a set time of inactivity.
3. If enabled, enter the duration of time a user can be inactive before the viewer session times out and closes.
4. Click *Save*.

Date and time

You can view the current date and time, manually configure the date and time settings or use an Network Time Protocol (NTP) server.

To configure the date and time settings:

1. From the sidebar of the System Settings screen, click *Date and Time*.
2. Click the Configure Date and Time radio button to manually set the date and time.

   -or-

   Click the Use NTP Server radio button to synchronize the date and time with the server.
3. Click *Save*.

Events retention

You can determine the number of days (1-60) before events are automatically purged from the system.

To configure the events retention policy:

1. From the sidebar of the System Settings screen, click *Events Retention*.
2. In the Purge events section, use the slider to set the number of days before the events are purged.
3. In the Events Archiving section, click the Archive and delete radio button to archive the events before they are deleted.

   -or-

   Click the Delete radio button to delete the events after the set number of days for purging events passes.
4. Click *Save*.

Alarms retention

You can determine the number of days before alarms are purged from the system.

To configure the alarms retention policy:

1. From the sidebar of the System Settings screen, click *Alarms Retention*.
2. Enter the number of days (1-60) for which the alarms are saved. After the set period, the alarms are deleted.
3. Click *Save*.

Viewer settings

You can configure the global inactivity timeout for the Video Viewer. When the inactivity threshold is reached, the viewer session will be disconnected. By default, the viewer timeout is enabled with a time limit of 30 minutes.

To configure the inactivity timeout settings for the Video Viewer:

1. From the sidebar of the System Settings screen, click *Viewer Settings*.

2. Click the toggle button to enable or disable automatic log out from a viewer session after a set time of inactivity.
3. If enabled, enter the duration of time a user can be inactive before the viewer session times out and closes.
4. Click *Save*.

Standalone KVM viewer settings

You can allow the system to launch standalone KVM sessions through the API, terminate standalone KVM sessions after a set time or inactivity, preempt standalone KVM sessions, and run standalone KVM sessions while running an exclusive KVM session.

To configure the standalone KVM viewer settings:

1. From the sidebar of the System Settings screen, click *Standalone KVM Viewer Settings*.
2. Click the Allow Standalone KVM Sessions toggle button to enable or disable the system to launch standalone KVM sessions through the API.
3. Click the Allow Preemption of Standalone KVM Sessions to enable or disable other users from interrupting active sessions.
4. Click the Standalone KVM Viewer Inactivity Timeout toggle button to enable or disable the system to terminate the session after a set time of inactivity.
    a. If the Standalone KVM Viewer Inactivity Timeout button is enabled, enter the duration of time a user can be inactive before the viewer sessions times out and closes.
5. Click the Allow Exclusive Sessions with Standalone KVM sessions toggle button to enable or disable the system to run standalone KVM session while simultaneously running an exclusive KVM session.
6. Click *Save*.

FIPS module

You can enhance the security of your rack manager, particularly for protecting sensitive data, by enabling FIPS mode. By default, the FIPS mode of operation is disabled.

NOTE: Enabling FIPS mode requires the appliance to be rebooted.

To enable FIPS mode:

1. From the sidebar of the System Settings screen, click *FIPS Module*.
2. Click the toggle button to enable FIPS mode.
3. From the sidebar, click *Reboot Appliance*.
4. Click the *Reboot* button. Upon reboot of the appliance, the FIPS mode is now enabled.

Email server configuration

You can enter email server information for both a primary and secondary account. This information will be used for sending system notifications.

To configure email server information:

1. From the sidebar of the System Settings screen, click *Email Server Configuration*.
2. Click the Edit icon (pencil) to configure either the primary or secondary email server information.
3. (Optional) After entering all required information, you can send a test email by entering an email address in the Test Email Server Configuration field and clicking the *Send Test Email* button.
4. Click *Save*.

NOTE: After configuring the email server information, you must enable the Sending Email setting to receive email notifications. For instructions, refer to Notification configuration below.

Notification configuration

You can enable or disable the system to send email notifications to the email address specified on the Email Server Configuration tab.

To configure email notifications:

1. From the sidebar of the System Settings screen, click *Notification Configuration*.
2. Click the toggle button to enable or disable the system to send email notifications.
3. Click *Save*.

For information on configuring notification policies, refer to Notification Settings on page 54.

SSH passthrough

You can launch a serial session without the use of web browser by using SSH passthrough. From an SSH client, a user with the appropriate device and sessions permissions can establish a connection to Vertiv™ Avocent® AC8000 advanced console systems and its targets that are managed by the rack manager.

SSH passthrough is only accessible for administrator users. Other user roles must be given the appropriate permissions to start an SSH session. While SSH passthrough supports both internal and external users, external users must have specified permissions to access the device. However, external users do not need sessions permissions as these settings are not available in rack managers for external users.

NOTE: Each target device used for SSH passthrough must have a unique name. If multiple targets have the same name, an error will occur and prevent a successful connection. SSH passthrough will only attempt to connect to the first target matching that name.

To configure SSH passthrough:

1. From the sidebar of the System Settings screen, click *SSH Passthrough*.
2. Click the toggle button to enable or disable SSH passthrough.
3. Specify the SSH server port on the rack manager to connect an SSH session. The default port is 2222.
4. Click *Save*.

To establish an SSH connection:

1. Open the SSH client.
2. Using the following format, enter the command to establish an SSH connection: **ssh -t** <appliance.IP> **-l "**<username>**:**<target device name>**" -p** <ssh server port>
   - appliance.IP - The IP address of the rack manager.
   - username - The username for the rack manager.
   - target device name - The name of the target device to which you wish to establish an SSH connection.
   - ssh server port - The port number specified when SSH passthrough was enabled on the System Settings screen of the rack manager web UI.
3. When prompted, enter your password for the rack manager.

NOTE: If connecting to a target device of the Vertiv™ Avocent® ACS8000 advanced console system, then you may be prompted for the login credentials of that target device.

Auto discovery

You can enable the Auto Discovery feature to allow devices that are physically connected to the rack manager to be automatically discovered. This feature reduces the need for manually discovering devices. By default, this feature is disabled.

NOTE: Auto Discovery is only available for SPs, UPSes, PDUs and generic devices.

NOTE: Before enabling Auto Discovery, ensure that you have already created the necessary credential profiles for the devices you wish to connect to the rack manager. Once Auto Discovery is enabled, all existing credential profiles will be used to help discover the devices. If an auto-discovered device has no credential profile (or the credential profile is inaccurate), the device will be added as a generic device, which has limited functionality within the rack manager.

To enable and configure Auto Discovery:

1. From the sidebar of the System Settings screen, click *Auto Discovery*.
2. Click the Auto Discovery toggle button to enable it. Once enabled, physically connected devices are discovered automatically and the remaining feature parameters become configurable.
3. (Optional) Click the Add Unidentified Devices as Generic Devices toggle button. When enabled, devices that appear for Auto Discovery but do not have a credential profile will be added as generic devices.
4. (Optional) Click the Add Service Processors as Generic Devices toggle button. When enabled, SPs that appear for Auto Discovery are added as generic devices.
5. Click *Save*.

Auto device cleanup

You can enable the Auto Device Cleanup feature to automatically remove offline devices after a set period of inactivity. The timer for device inactivity starts once the device status on the Targets List and Appliance View screens shows as unresponsive. By default, this feature is disabled.

To enable and configure Auto Device Cleanup:

1. From the sidebar of the System Settings screen, click *Auto Device Cleanup*. Once enabled, the remaining feature parameters become configurable.
2. (Optional) In the Device Inactive Time field, enter the duration of time (in minutes) that a device must be inactive to be deleted on the next cleanup cycle. The default setting is 10 minutes.
3. (Optional) In the Cleanup Frequency field, enter how often (in minutes) inactive devices will be automatically deleted from the appliance. The default setting is every 30 minutes.
4. Click *Save*.

You can also perform on-demand cleanup of all inactive devices. To perform an on-demand device cleanup, click the *Cleanup Now* button. Any device that has exceeded the threshold specified in the Device Inactive Time field will be immediately removed.

Certificate

You can generate a new certificate signing request (CSR), as well as update or download the certificate currently installed on the appliance.

NOTE: These functions can also be performed from the Targets List screen by clicking on the orange link in the Name column for the desired device. The Certificate page will appear and allow you to generate, install and download a certificate.

NOTE: Updating the certificate for a Vertiv™ Avocent® IPUHD 4K IP KVM device from the Targets List requires a manual refresh of the page to view the updated contents of the certificate.

To generate a new certificate:

1. From the sidebar of the System Settings screen, click *Certificate*.
2. Click the Generate signing request icon in the right corner. The Generate Certificate Signing Request dialogue box appears.
3. Enter the required information: Common Name, Country.
4. (Optional) Enter additional information: State, City, Organization, Organization Unit, and Email. You can also optionally add a subject alternative name.
5. Click *Generate*. The CSR downloads as a .pem file and is now ready to be uploaded on the appliance.

To upload the certificate:

1. From the sidebar of the System Settings screen, click *Certificate*.
2. Click the Update certificate icon in the right corner.
3. Browse to and select the .pem file to upload.
4. Click *Open*. The .pem file uploads to the appliance.

To download the certificate currently installed on the appliance:

1. From the sidebar of the System Settings screen, click *Certificate*.
2. Click the Download certificate icon in the right corner. The CSR downloads as a .pem file to your local system.

Reboot appliance

You can reboot the appliance. Rebooting the appliance will log you out of the system.

To reboot the appliance:

1. From the sidebar of the System Settings screen, click *Reboot Appliance*.
2. Click the *Reboot* button.
3. A message appears, prompting you to confirm your reboot request. Click *Reboot*.

3.6.9 Scheduler

From the Scheduler screen, you can view the schedule of events set to occur based on your configurations. You can configure the table displaying the scheduled events by clicking the vertical ellipsis in the right corner and clicking *Table Configuration*. Select or deselect the Completed Time or State check box to configure the information displayed in the table.

3.7 Network Configuration

The Network Configuration tab contains six sub-menu items - Settings, DHCP, System Interfaces, IP Pool, NAT Setup and Destination Port Mappings - from which you can view and configure general network settings, as well as port settings, trigger mode, interface settings and more.

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

3.7.1 Settings

From the Settings screen, you can configure the following:

- Network settings
- Normal/failover-bonded settings
- Failover-routed IPv4 trigger mode
- Ethernet interfaces. For information on other system interfaces, refer to System interfaces on page 50.

NOTE: All configurations described in this section can be performed from the *Network Configuration - Settings* screen. You can use the sidebar menu to navigate through the Settings page.

Network settings

You can view the hostname, primary DNS, secondary DNS and domain name. The hostname is configurable.

To configure the hostname:

1. From the sidebar of the Settings screen, click *Network 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.

NOTE: Configuring the SFP ports requires the appliance to be rebooted.

To configure the SFP ports:

1. From the sidebar of the Settings screen, click *Normal/Failover Bonded 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). The Update Uplinks dialogue box appears.
3. Click *Yes, Update*.

Failover-routed IPv4 trigger mode

You can use the failover-routed IPv4 trigger mode to configure the trigger for initiating failover.

To configure the trigger mode for failover:

1. From the sidebar of the Settings screen, click *Failover-Routed IPv4 Trigger Mode*.

2. Under the Failover-Routed IPv4 Trigger Mode, select either the *Primary Interface Down, Unreachable Default Gateway* or *Unreachable IP* radio button.
    a. If you select *Unreachable IP*, then fill out the IP Address field.
3. Reboot the device for the changes to take effect. From the left-hand sidebar, click *Administration - System Settings*.
4. Click the *Reboot Appliance* tab.
5. Click the *Reboot* button, and then click *Reboot* to confirm your request.

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.

NOTE: For instructions on configuring the vrf_app0 and Vpp0 interfaces, refer to the Vertiv™ Avocent® RM1048P Rack Manager Quick Installation Guide shipped with the appliance.

The following figure and table provides descriptions of the rack manager's physical network interfaces.

Figure 2.7 Avocent® RM1048P Rack Manager Interface Ports

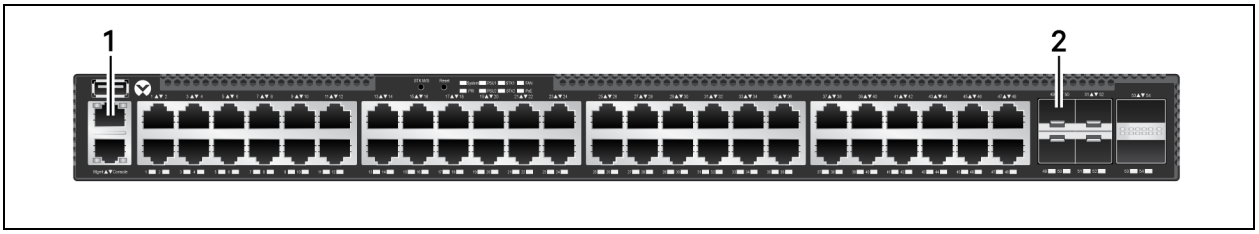


Table 2.11 Avocent® RM1048P Rack Manager Interface Ports

Number	Interface	Description
1	eth0 (RJ54 port)	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.
2	Vrf_app0	Provides access to the rack manager's web UI or CLI via an SSH session.
	Vpp0	Allows you to launch KVM sessions to target devices from the web UI.

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

To configure a static IP address:

1. From the sidebar of the Settings screen, click *Ethernet Interfaces*.
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 connected to the rack manager ports. You can also alter how long leases last for the assigned IP addresses.

To navigate the DHCP screen:

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

- Configure the number of seconds the lease time lasts by adjusting the Seconds field under the Dynamic Ranges heading.
- Refer to the Lease IP Address List to view the non-expired or all leased IP addresses.
- Reserve IP addresses for target devices by clicking the Add icon (+) under the Reserved IP Configuration heading and entering the device's MAC address and the desired IP address.

3.7.3 System interfaces

From the System Interfaces screen, you can view information about the system interfaces. You can configure the table displaying the interface information by clicking the vertical ellipsis in the right corner.

3.7.4 IP pool

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. An IP pool is a range of reserved IP addresses within your network. IP pool addresses are necessary for 1-to-1 NAT setup.

To create an IP pool:

1. From the left-hand sidebar, click *Network Configuration - IP Pool*.
2. Click the Add icon (+) in the top right corner.
3. To add a single IP address, click the *Single IP* button.

   -or-

   To add a range of IP addresses, click the *Range IP* button.
4. 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. From the left-hand sidebar, click *Network Configuration - IP Pool*.
2. Check the box to the left of the desired IP pool.
3. Click the vertical ellipsis to the right and click *Delete*.

3.7.5 NAT setup

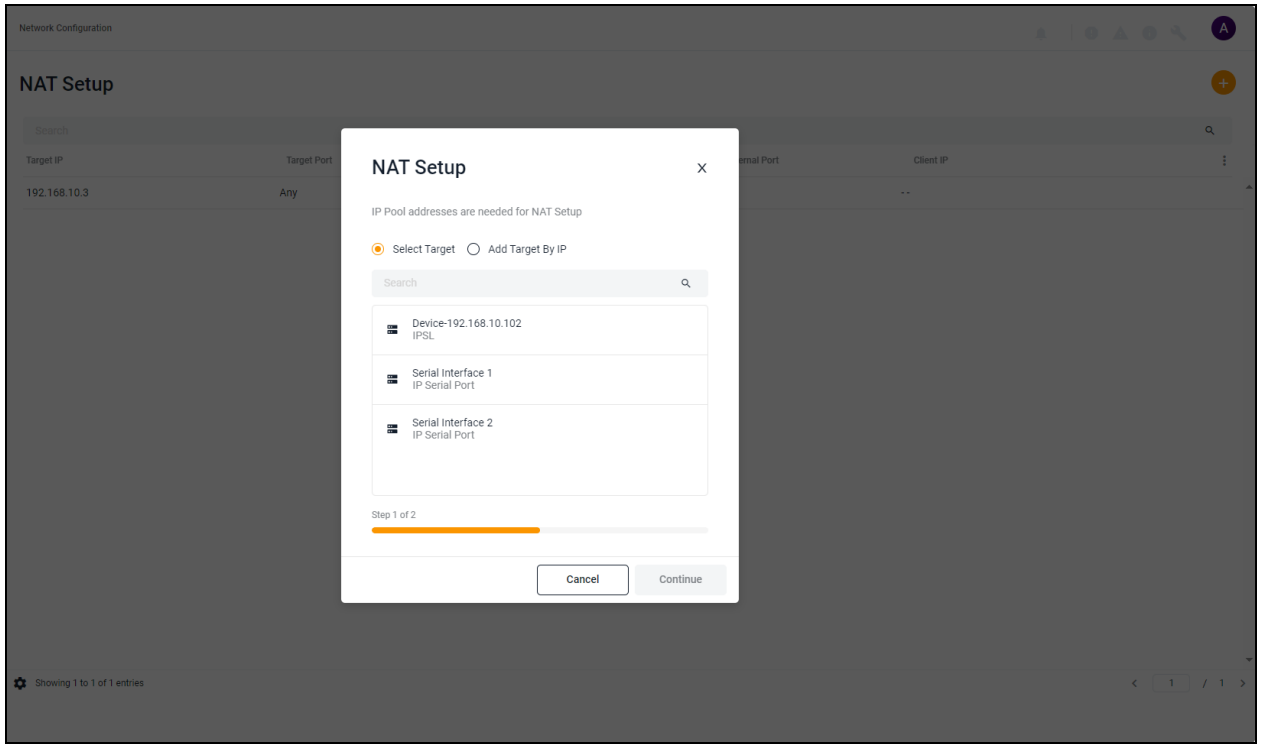
From the NAT Setup screen, you can add and configure NAT rules to perform address translations.

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, refer to IP pool above.

To configure a 1-to-1 NAT setup:

1. From the left-hand sidebar, click *Network Configuration - NAT Setup*.
2. Click the Add icon (+) in the top right corner.

Figure 2.8 1-to-1 NAT Setup Overview



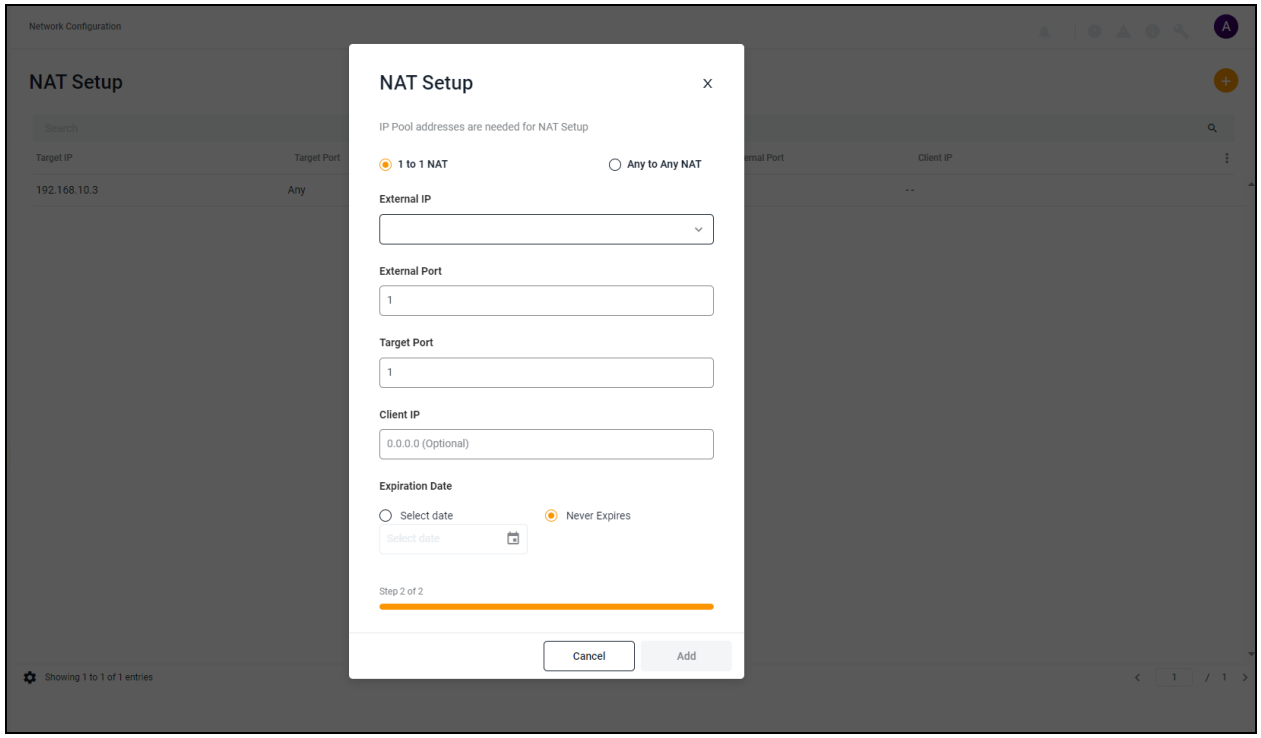
3. To add a target from the Targets List, click the Select Target radio button and select the appropriate device.

   -or-

   To add a target by its IP address, click the Add Target By IP radio button and enter the IP address.

4. Click *Continue*.

Figure 2.9 1-to-1 NAT Setup Options



5. Click the 1 to 1 NAT radio button.
6. Select the external IP address from the External IP drop-down menu.
7. Specify the external port and target port in the respective fields.
8. (Optional) Enter the client IP address in the Client IP field.
9. To manually set the expiration date, click the Select date radio button and use the calendar feature to set the date.

   -or-

   To set no expiration date, click the Never Expires radio button.
10. Click *Add*.

To configure an Any-to-Any NAT setup:

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

1. From the left-hand sidebar, click *Network Configuration - NAT Setup*.
2. Click the Add icon (+) in the top right corner.
3. To add a target from the Targets List, click the Select Target radio button and select the appropriate device.

   -or-

   To add a target by its IP address, click the Add Target By IP radio button and enter the IP address.
4. Click *Continue*.
5. Click the Any to Any NAT radio button.
6. Select the external IP address from the External IP drop-down menu.

7. To manually set the expiration date, click the Select date radio button and use the calendar feature to set the date.

   -or-

   To set no expiration date, click the Never Expires radio button.

8. Click *Add*.

3.7.6 Destination port mappings

From the Destination Port Mappings screen, you can enable customized ports to support specific Service Processors (SPs) for access to the native KVM function.

To define a destination port:

1. From the left-hand sidebar, click *Network Configuration - Destination Port Mappings*.
2. Click the Add icon (+) in the top right corner. An Add Destination Port dialogue box appears.
3. Enter the port number and click *Add*.
4. 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. From the left-hand sidebar, click *Network Configuration - Destination Port Mappings*.
2. Check the box to the left of the port.
3. Click the vertical ellipsis to the right and click *Delete*.

3.8 Notification Settings

The Notification Settings tab contains one sub-menu item - Notification Policy - from which you can configure the policies for the notifications sent from the appliance.

3.8.1 Notification policy

From the Notification Policy screen, you can customize the severity, distribution and other settings for your appliance's notification policy.

To create a notification policy:

1. From the left-hand sidebar, click *Notification Settings - Notification Policy*.
2. Click the Add Notification Policy icon (+) in the top right corner. An Add Notification Policy dialogue box appears.
3. Enter the name for the notification policy. The Name field has a limit of 30 characters.
4. Check one of the following boxes for the Alarm Severities section: Critical, Warning or Information.
5. Use the slider to enable or disable the Alarm Cleared Notification setting.
6. In the Distribution List section, enter the appropriate information into the To or the CC field.
7. (Optional) Add a description for the notification policy, if desired. The Description field has a limit of 300 characters.
8. Click *Add*.

Appendices

Appendix A: Technical Specifications

Table 3.1 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: Backup and Restore

Using the Avocent RM1048P Rack Manager Command Line Interface (CLI), you can enter **5** to select the Backup and Restore option to perform the following functions:

- Perform a remote backup (on-demand or scheduled)
- Configure the retention policy to preserve storage space
- Configure a schedule for backup automation
- View a list of all backups in the appliance
- Delete a backup
- Restore a previous configuration of the appliance

B.1 Limitations and Notes

Note the following information and limitations about the Backup and Restore capability of the rack manager:

- The Backup and Restore feature does not support backing up one rack manager and restoring it on a different appliance. If you perform a backup and restore of the appliance to a different host, the hardware will fail.
- If you have custom SSL certificates and the primary rack manager's IP address changes, you will have to replace the certificates for the rack manager.
- There is no limit on the number of remote backups you can retain.

B.2 Performing a Remote Backup

Backups can be saved remotely using a SMB/CIFS server. There is no limit on the number of remote backups you can retain. Before performing a remote backup, you must configure the host server.

To configure the SMB host server:

NOTE: Before continuing, ensure you are using SMB protocol version 2.0 or greater.

1. From the Backup and Restore menu, enter **2** for the SMB option.
2. Enter **1** to select the Configure option, then enter **1** to select the Configure SMB Host option.
3. Enter the IP address, username, password and directory path for the SMB host server.

To create an on demand backup:

1. From the Backup and Restore menu, enter **1**for the SMB option to back up the appliance remotely.
2. A list appears and displays the number of backups retained, the backup schedule, the backup status, and the restore status. From the Options section, enter **3** to select the On Demand Backup option. The following message appears: *Create a new backup of the current system state?*
3. Enter **yes**. The Backup Status line indicates it is in progress.
4. Press **Enter** to refresh the screen. The Backup Status line displays *Success*, and the backup has been created.

B.3 Configuring the Retention Policy

NOTE: After configuring a retention policy, you must create a new backup for the system to register the change.

1. From the Backup and Restore menu, enter **1**for the SMB option to back up the appliance remotely.
2. Enter **1** to select the Configure option.
3. Enter **1** to select the Change Retention Policy option.

4. Enter the number of backups you wish to retain. You can retain a maximum of five backups locally. The Backups Retained line updates and reflects the number of backups being retained.

B.4 Configuring a Schedule for Backup Automation

1. From the Backup and Restore menu, enter 1for the SMB option to back up the appliance remotely.
2. A list appears and displays the number of backups retained, the backup schedule, the backup status, and the restore status. From the Options section, enter 1 to select the Configure option.
3. Enter 2 to select the Change Backup Schedule option.
4. Enter the appropriate number to select the No Schedule, Daily, Weekly or Monthly option.

NOTE: If you select the No Schedule option, you will be returned to the Configure menu. If you select the Weekly option, select which day you wish for the backup to begin. If you select the Monthly option, enter the day of the month (1-28) you wish for the backup to begin.

5. Enter the time (HH:MM) you wish for the backup to begin. The backup has been successfully scheduled.

NOTE: The time value should be in the 24 hour clock format.

B.5 Viewing a List of All Backups

1. From the Backup and Restore menu, enter 1for the SMB option to back up the appliance remotely.
2. Enter 2 to select the List option.

B.6 Deleting a Backup

1. From the Backup and Restore menu, enter 1for the SMB option to back up the appliance remotely.
2. Enter 4 to select the Delete Backup option. An index of existing backups appears.
3. Enter the appropriate number for the backup you wish to delete.
4. Enter yes to delete the selected backup. The backup has been deleted.

B.7 Restoring a Previous Backup Configuration

NOTE: Backup restoration requires the backup to be the same firmware version as the primary rack manager.

NOTE: Restoring a backup will initiate a reboot of the appliance.

1. From the Backup and Restore menu, enter 1for the SMB option to back up the appliance remotely.
2. Enter 5 to select the Restore option. An index of deleted backups appears.
3. Enter the appropriate number for the backup you wish to restore.
4. Enter yes to reboot the appliance. Once the system comes back online, the backup has been successfully restored.

Appendix C: 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 43082 USA

590-2356-501J