



Avocent[®] MP1000 Management Platform

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
1.1 Product Overview	1
1.2 Prerequisites	3
1.3 Features and Benefits	3
2 System Licensing	5
3 SSL Certificate Replacement	7
4 Web User Interface (UI)	9
4.1 Account Settings	10
4.2 Dashboard	11
4.2.1 Edge Management	11
4.3 Targets	12
4.3.1 Appliance view	15
4.3.2 Organizations	19
4.3.3 Targets list	20
4.3.4 Resource groups	20
4.3.5 Virtualization	21
4.3.6 Discoveries	21
4.4 Sessions	22
4.4.1 Sessions List	22
4.4.2 KVM sessions	25
4.4.3 Serial sessions	31
4.4.4 Web UI sessions	32
4.5 Management	33
4.5.1 Devices	33
4.5.2 High availability	33
4.6 Administration	42
4.6.1 User management	42
4.6.2 Roles and permissions	44
4.6.3 Credential profiles	50
4.6.4 Events	54
4.6.5 Alarms	54
4.6.6 Authentication providers	54
4.6.7 Firmware updates	55
4.6.8 System settings	56
4.6.9 Scheduler	64
4.6.10 License	64
4.7 Network Configuration	67
4.7.1 Network settings	67
4.7.2 Normal/Failover-bonded settings	67

4.7.3 Failover-routed IPv4 trigger mode	67
4.7.4 Ethernet interfaces	68
4.8 Notification Settings	69
4.8.1 Notification policy	69
Appendices	71
Appendix A: Technical Support and Contacts	71
Appendix B: Technical Specifications	73
Appendix C: Backup and Restore	75

1 Getting Started

1.1 Product Overview

NOTE: 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 MP1000 Management Platform is a secure, centralized enterprise management solution that allows users to remotely access, manage, monitor and control target devices through managed appliances. Additionally, this product simplifies IT management and control of physical and virtual infrastructures by allowing target devices to be launched from a single, central access point.

The following figure and table describe the various components of the management platform hardware appliance.

Figure 1.1 Avocent MP1000 Management Platform Description

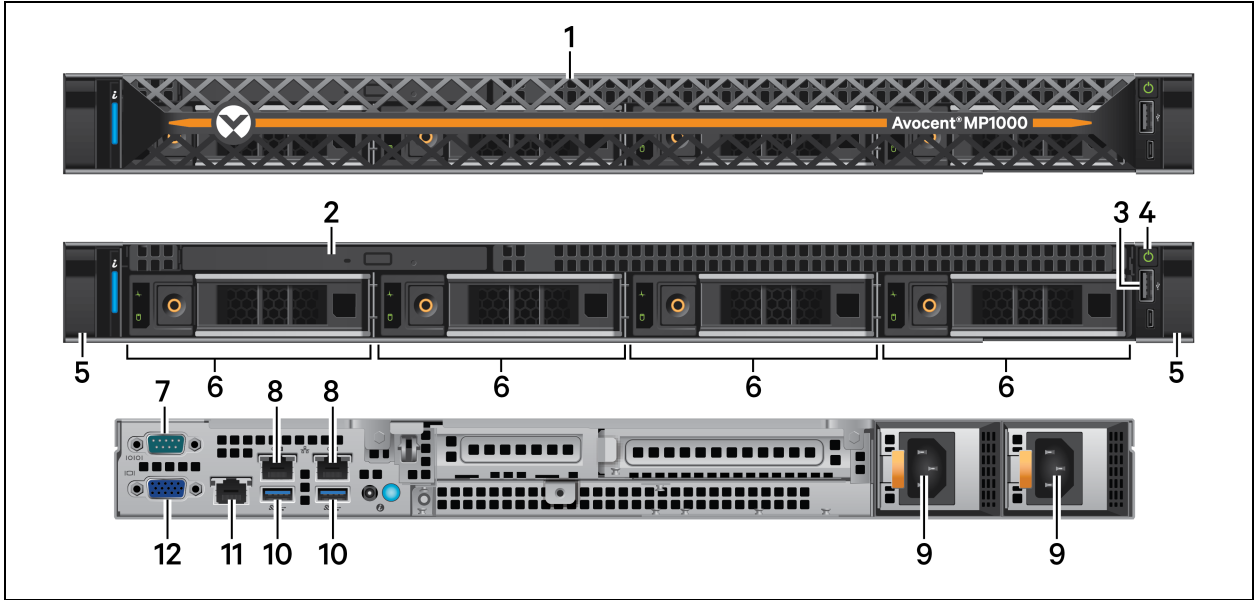


Table 1.1 Avocent MP1000 Management Platform Description

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

The Avocent MP1000 Management Platform 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

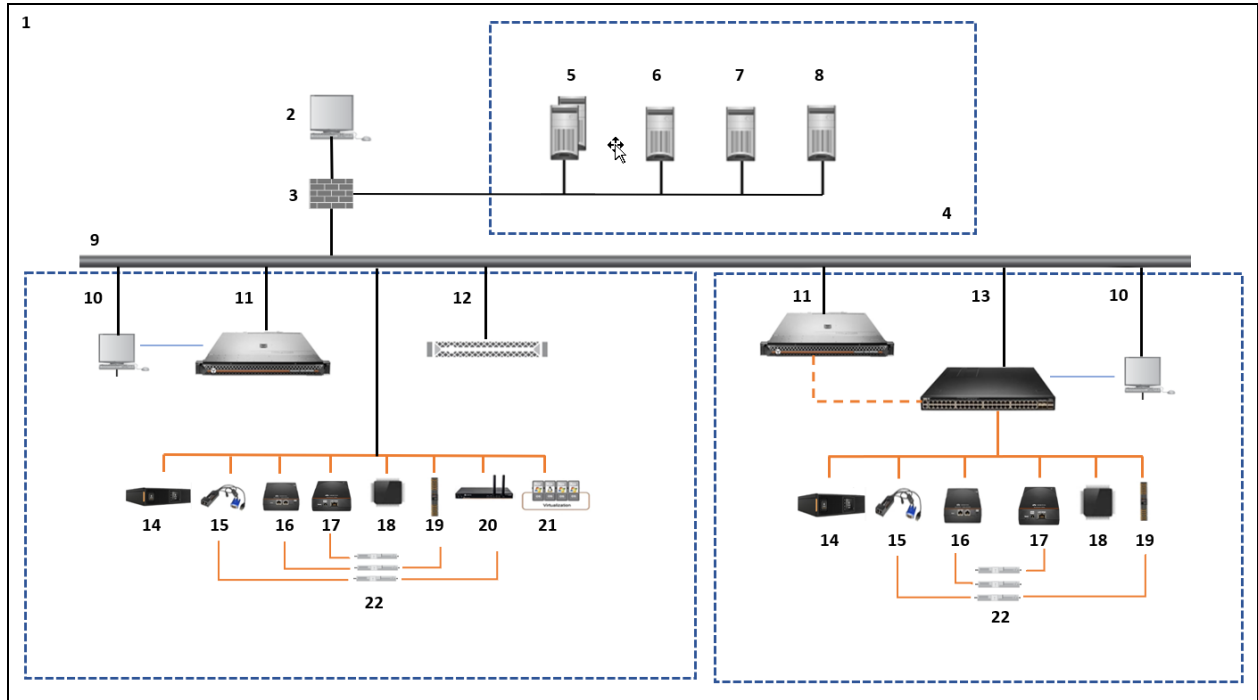


Table 1.2 Vertiv™ Avocent® DSView™ Solution System Configuration Descriptions

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

1.2 Prerequisites

To support both physical and virtual infrastructures, the management platform is offered as a hardware appliance and a virtual appliance. Both appliances offer remote access to the management platform, but they follow different installation and deployment processes. The hardware appliance requires a physical setup of equipment to support its functions and therefore must be physically installed. Comparatively, the virtual appliance is distributed as a disk image that must be virtually installed and deployed on one of the virtualization platforms supported by the management platform.

Prior to beginning operations, ensure you have reviewed and completed the appropriate documentation for your appliance type as specified in the following table.

Table 1.3 Documentation By Appliance Type

Appliance Type	Documentation
Hardware	Vertiv™ Avocent® MP1000 Management Platform Quick Installation Guide
Virtual	Vertiv™ Avocent® MP1000VA Management Platform Virtual Appliance Getting Started Guide (to be completed first)
	Vertiv™ Avocent® MP1000VA Management Platform Virtual Appliance Installation/Deployment Guide

To find product documentation for the management platform, go to the [Vertiv™ Avocent® MP1000 Management Platform](#) or the [Vertiv™ Avocent MP1000 Management Platform Virtual Appliance](#) product page. Scroll down and click the *Documents & Downloads* tab. Click the appropriate link to open a PDF version of the documentation.

1.3 Features and Benefits

The Avocent MP1000 Management Platform provides the following benefits for your data center:

- Combined control of your KVM over IP, Service Processors (SPs) and Virtual Machines (VMs) to manage your entire infrastructure across enterprise and edge sites
- Network scalability to easily expand into a large, complex and uniform infrastructure with a single management platform
- Simplified infrastructure and improved productivity with the automation of deployment and configuration tasks on your IT equipment
- Improved efficiency through the standardized management of SPs and use of common API sets to manage the entire IT infrastructure
- Enhanced security with centralized firmware updates and safeguarded access to your IT devices
- Minimal service disruption for your IT infrastructure due to the remote access option
- Controlled and restricted operations to your devices and detailed monitoring system that maintains record of user history
- Minimal downtime for upgrades

This page intentionally left blank

2 System Licensing

NOTE: The Avocent MP1000 Management Platform is currently transitioning licensing management processes. Starting at firmware version 3.69.6, the management platform will use the third-party Thales system for license management and activation. Licenses from the old process (legacy licenses) will remain valid until they expire or are removed. If you remove a legacy license, it cannot be re-added to the appliance. Only Thales licenses can be added to an updated management platform.

After completing the initial installation and setup for the Avocent MP1000 Management Platform, you must purchase and activate your licenses for the management platform in order to launch target sessions and access the full functionality of the appliance. After submitting your order, you will receive an email from the Vertiv Entitlement Portal Team with a link to create an account for the customer portal. Follow the steps detailed in the email. Once your account has been activated, you are ready to activate your licenses and add them to the management platform.

For instructions on activating and adding licenses to the management platform, refer to [License](#) on page 64.

For instructions on configuring the expiration notification for your license, refer to [License expiration notification](#) on page 59.

This page intentionally left blank

3 SSL Certificate Replacement

When you enter the management platform'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, please visit [Vertiv™ Avocent® MP1000 Software Downloads](#) for a script and release notes for assistance with this process. If you need additional assistance, please contact your Vertiv Technical Support representative.

This page intentionally left blank

4 Web User Interface (UI)

Once you have connected the Avocent MP1000 Management Platform to a network and configured its IP address, you can access it via its web UI. The web UI provides direct access to the management platform and its targets.

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 for the Avocent MP1000 Management Platform that you previously configured. The IP address should be entered in the following format: **https://<appliance.IP>**
2. At the login screen, enter your username and password. The web UI opens into the Appliance View screen.

Figure 4.1 Web UI Overview

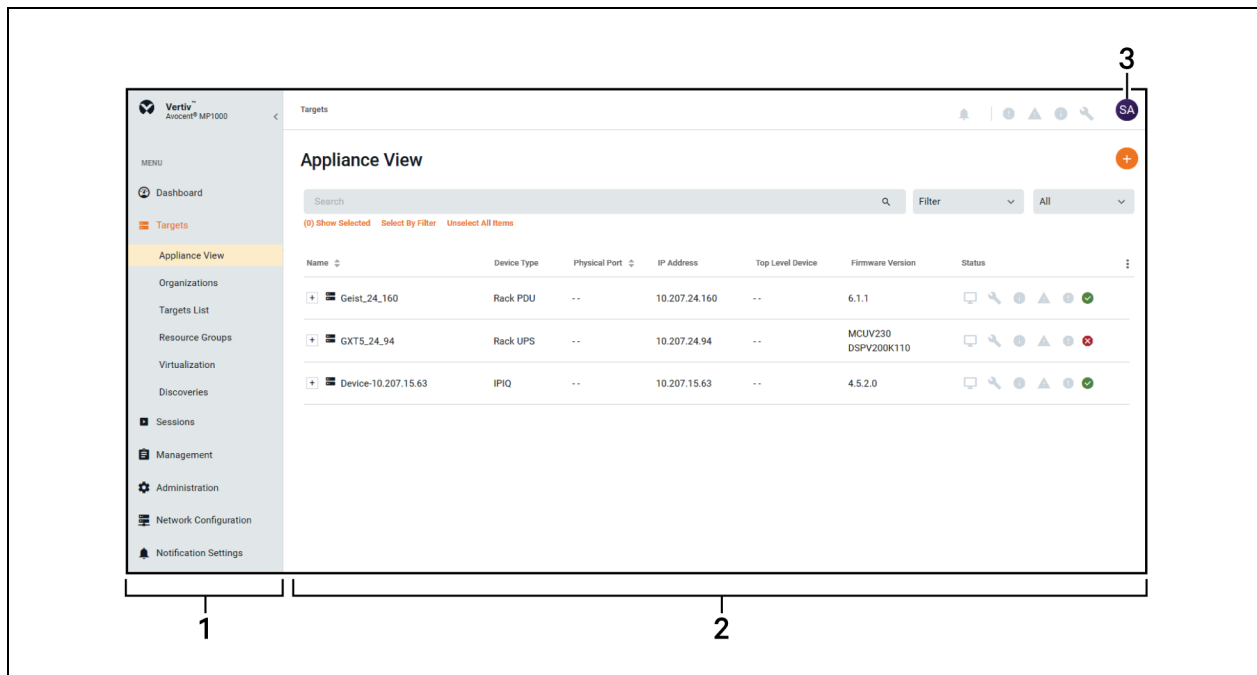


Table 4.1 Web UI Overview Description

Item	Description
1	Sidebar
2	Content area
3	Account settings

4.1 Account Settings

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

User Preferences

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

Table 4.2 User Preferences

Tab	Description
User Profile	Configure the profile name, password and email address.
Localization	<ul style="list-style-type: none"> Measuring System - Select either the Metric or Imperial radio button to determine the measuring system for the management platform. 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 menu. 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® MP1000 Management Platform User Guide.

Log Out

This option immediately logs you out of the web UI.

4.2 Dashboard

The Dashboard tab contains one sub-menu item - Edge Management - from which you can centrally manage and control IT equipment and physical infrastructure devices, such as Vertiv™ Uninterruptible Power Supplies (UPSes) and Vertiv™ Power Distribution Units (PDUs).

4.2.1 Edge Management

From the Edge Management screen, you can perform the following functions:

- View the alarm status for sites and devices
- Deeper drill down into device data
- View key device metrics
- Remotely recover via the KVM device, serial device, SP, and the cycle power via the Vertiv™ UPSes and Vertiv™ PDUs

To navigate the Edge Management screen:

From the left-hand sidebar, click *Dashboard - Edge Management*. On this screen, you can access the following features:

- Organizations - A list of all available organizations and ungrouped devices. Use the Search field to search for specific organizations. Use the Filter drop-down menu to filter organizations by All, No Devices, Has Devices, Has No Sub Orgs or Has Sub Orgs. Upon selecting the organization in this view, the associated list of devices and alarms appear in the Device Locator and Alarms views. For more information, refer to [Organizations](#) on page 19.
- Device Locator - A list of all the devices associated with the specific organization. Select the device to view its associated alarms and device metrics. Use the Search field to search for specific devices. Use the Filter drop-down menu to filter devices by All, Rack PDU, Power Outlet and IPIQ. Use the All drop-down menu to search for devices by the following status options: Responding, On and Off.
- Device Metrics - A description of device metrics, including Energy, Real Power (W), Apparent Power (VA) and Power Factor. This view appears after selecting the device in the Device Locator view.
- Alarms - A list of alarms associated with the selected device. Click the vertical ellipsis to clear the alarm. For more information, refer to [Alarms](#) on page 54.

4.3 Targets

The Targets tab contains six sub-menu items - Appliance View, Organizations, Targets List, Resource Groups, Virtualization and Discoveries - from which you can manage your target devices. The number of target devices permitted for a single management platform ranges from 50-5,000. The Avocent MP1000 Management Platform supports the following target device types:

- [Vertiv™ Avocent® RM1048P Rack Manager](#)
- [Vertiv™ Uninterruptible Power Supplies \(UPSes\)](#)
- [Vertiv™ Power Distribution Units \(PDUs\)](#)
- [Service Processors \(SPs\)](#)
- [IP KVM devices](#)
- [Vertiv™ Avocent® ACS 800/8000 advanced console system](#)
- [Vertiv™ Avocent® DSView™ management software](#)
- [Virtual Machines \(VMs\)](#)
- [Generic devices](#)

NOTE: Users without Administrator access can only see devices to which they have access.

Vertiv™ Avocent® RM1048P Rack Manager

Adding a rack manager to the management platform allows you to centrally connect multiple devices for increased network scalability. The following devices can be added to the rack manager, then managed by the management platform:

- Vertiv™ UPSes
- Vertiv™ PDUs
- Services Processors
- IP KVM devices

NOTE: These devices can be added individually to the management platform without requiring a rack manager; however, the rack manager allows you to maximize the number of managed devices.

NOTE: Once added, a rack manager can only be accessed via the Avocent MP1000 Management Platform web UI. To access the rack manager via its own web UI again, the rack manager must be removed from the management platform web UI.

Vertiv™ Uninterruptible Power Supplies (UPSes)

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

Vertiv™ Power Distribution Units (PDUs)

Vertiv™ PDUs distribute reliable, electric power to data centers and monitor the system's power status. PDUs only consume a single license as a target for the management platform; therefore, adding a Vertiv™ PDU to the management platform allows you to add multiple devices via the outlets while minimizing your license consumption.

Service Processors (SPs)

SPs can be connected physically via a rack manager or logically over a network to the management platform. The Avocent MP1000 Management Platform can discover SPs over the network, provided the SPs have an IP address and are connected to the same network as the management platform.

The Avocent MP1000 Management Platform and Vertiv™ Avocent® RM1048P rack manager support the following SPs:

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

Connecting a service processor to a management platform or rack manager provides the following features and benefits:

- Ability to access the management web UI of the server
- Ability to launch embedded KVM viewer
- Configure dynamic proxy to the server management interface
- 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 32 for initial prerequisites and configurations, as well as information on launching and configuring web UI sessions.

IP KVM devices

KVM devices can be discovered and managed when connected via a Vertiv™ Avocent® IPIQ IP KVM device or a Vertiv™ Avocent® IPUHD 4K IP KVM device. The Avocent MP1000 Management Platform provides flexible, centralized control of data center servers and virtual media of remote branch offices where trained operators may be unavailable. KVM over IP 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 25 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 IP KVM Installer/User Guide and the Vertiv™ Avocent® IPIQ IP KVM Quick Installation Guide available on www.vertiv.com.

Vertiv™ Avocent® ACS 800/8000 advanced console system

Serial devices can be discovered and managed by the management platform when connected via a Vertiv™ Avocent® ACS 800/8000 advanced console system. The console system serves as a single point for access and administration of connected devices, such as serial consoles.

Vertiv™ Avocent® DSView™ management software

The Vertiv™ Avocent® DSView™ management software can be added to the management platform to provide access to all the devices in one system, so they can be run simultaneously. To display all the devices in a single system, the Avocent MP1000 Management Platform and Vertiv™ Avocent® DSView™ management software are connected using API integration. Once the management software has been added to the Avocent MP1000 Management Platform, the Targets List screen displays the list of devices for both the management software and the management platform.

The management software provides the following features and benefits:

- Display of Vertiv™ Avocent® DSView™ management software devices on management platform web UI
- Enhanced user experience via a single platform for central access and control
- Target session launching to devices in the Vertiv™ Avocent® DSView™ management software
- Protection of customer investment in Avocent gear
- Pathway to Avocent MP1000 Management Platform migration
- Allows for the integration of Vertiv™ Avocent® DSView™ management software zones as part of the login, which enables you to view all target devices within the zone, rather than just top-level devices.

Virtual Machines (VMs)

VMs can be added to the management platform via Virtual Machine Managers or Hypervisors to increase efficiency through centralized management. The management platform uses APIs to seamlessly integrate the VMs into the system.

Generic devices

A generic device refers to any device that is connected to the management platform over the network. Generic devices are added to the management platform's network via their IP address but cannot actively communicate with the management platform. The support for generic devices allows for the consolidation of IP addresses in your data center and provides central access to the web pages of the devices from the management platform.

Since no communication is being established between the management platform 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 32 to open the web page of a generic device via the management platform.

4.3.1 Appliance view

NOTE: The Appliance View screen and the Targets List screen 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 connected to the management platform. You can also perform the following functions:

- [Add and delete devices](#)
- [Modify device information](#)
- [Perform maintenance activities](#)
- [Synchronize devices](#)
- [Merge devices](#)
- [Launch KVM, serial or web UI 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 management platform web UI.

NOTE: To discover devices for the management platform, you must create credential profiles for the following device types: Service Processors, ACS, Rack PDUs, Rack UPS, DSView and Virtual Machines. 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 50.

NOTE: To add an SP that is connected to a rack manager, you must first configure the SP to remotely access it. For SP configuration instructions, see the [Vertiv™ Avocent® RM1048P Rack Manager Installer/User Guide](#) shipped with the rack manager and located on www.vertiv.com. This does not apply if you are adding an SP independently.

To discover a single device or a range of devices:

1. From the left-hand sidebar, click *Targets - Appliance View* or *Discoveries*.
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 management platform. 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* or *Discoveries*.
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* or *Discoveries*.
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.

Performing maintenance activities

You can perform a variety of functions for each target device. Functions may include activating maintenance mode, removing devices, updating firmware, rebooting devices, resynchronizing devices, 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.

To perform a bulk firmware update for multiple devices:

NOTE: Bulk updates are only possible for devices of the same device type.

1. From the left-hand sidebar, click *Targets - Appliance View*.
2. Select the devices of the same device type.
3. Click the Firmware Update icon above the list of targets. A Firmware Update dialogue box appears.
4. Click *Choose File* and browse to the file from your local drive.
5. Select the firmware file and click *Open*.

-or-

Drag and drop the file from your local drive.

NOTE: If you wish to update the firmware from TFTP, FTP or HTTP, fill in the required information.

6. Click *Update* to update the firmware.

Synchronizing devices

To change and sync the device name from ADX to Device:

1. From the left-hand sidebar, click *Targets - Appliance View*.
2. Click on the desired device to open its information panel.
3. In the panel, click the Edit icon (pencil).
4. Edit the Device Name field.
5. Click *Save*.

NOTE: It takes around 30-40 seconds to complete the synchronization process. Wait a few seconds for the system to reflect the changes.

6. Go to the device's web UI to verify that the device name is changed.

-or-

To change and sync the device name from Device to ADX:

1. Change the device name in the Device web UI.

NOTE: It takes around 30-40 seconds to complete the synchronization process. Wait a few seconds for the system to reflect the changes.

2. Go to the ADX to verify that the device name is changed.

To resynchronize the system on demand:

1. From the left-hand sidebar, click *Targets - Appliance View*.
2. Click the vertical ellipsis to the right, then click *Resynchronization*.

By default, the system automatically synchronizes daily at 12:00am. If desired, you can configure the schedule.

To configure the synchronization schedule:

1. From the left-hand sidebar, click *Targets - Appliance View*.
2. Click on any Vertiv™ Avocent® DSView™ management software device to open its information panel. The panel displays the following tabs:
 - Properties
 - User Access
 - Scheduler

3. Click the Edit icon (pencil) to the right of the Scheduler to edit the following fields:
 - Repeat Day: Modify the schedule by day.
 - Repeat Time: Modify the schedule by time.
4. Click *Save*.

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, SP and serial targets, as well as all outlets on a Vertiv™ Geist™ Rack Power Distribution Unit (rPDU). Additionally, power operations are now included in the overall activities.

NOTE: You cannot merge VMs.

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

NOTE: Connected targets display in a table in the content area of the web UI. Click the vertical ellipsis to configure the table.

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 Targets List screen or the Appliance View screen. For more information about the different session types and activities, refer to [Sessions](#) on page 22.

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.

NOTE: The Dashboard preview screen updates every 7 to 10 seconds.

4. The Dashboard preview screen 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.

4.3.2 Organizations

From the Organizations screen, you can view a list of organizations and ungrouped devices in a table. The Status column displays the status for Maintenance Mode, alarm aggregation and device alarm severities. You can also perform the following functions:

- Organize devices by location
- Configure automatic alarm aggregation
- View display of global alarm counts and source alarms
- View the alarm summary
- Navigate to the alarm
- Create, configure and delete organizations

To create a new organization:

1. From the left-hand sidebar, click *Targets - Organizations*.
2. Click the Add icon (+). An Organization Editor dialogue box appears.
3. On the right side of the Organization Editor, click the Add icon (+). An Add Organization dialogue box appears.
4. Enter the required details to add the organization.
5. Click *Save*. After adding an organization, you can click the plus symbol (+) on the left side of the table to locate the devices and their associated alarms.

To edit an existing organization:

1. From the left-hand sidebar, click *Targets - Organizations*.
2. Click on the organization or device you want to edit to open its information panel.
3. Click on the *Properties* tab to expand the menu and click the Edit icon (pencil) to change the following details:
 - Organization Name
 - Longitude
 - Latitude
 - Description
4. Click *Save*.

To move an organization using the Organization Editor:

1. From the left-hand sidebar, click *Targets - Organizations*.
2. Check the box to the left side of the organization you want to move.
3. Click the *Move* button to shift the organization from left-to-right or right-to-left.

To delete an organization using the Organization Editor:

1. From the left-hand sidebar, click *Targets - Organizations*.
2. Hover the mouse over the row with the organization you want to delete and click on the vertical ellipsis.
3. Click *Delete*.
4. At the confirmation screen, click *Delete* again.

4.3.3 Targets list

From the Targets List screen, you can perform the same functions 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. For more information, refer to [Appliance view](#) on page 15.

4.3.4 Resource groups

From the Resource Groups screen, you can organize targets in a hierarchy by creating nested resource groups (groups within groups).

NOTE: To assign targets that are managed by another device (such as the Vertiv™ Avocent® RM1048P Rack Manager) to a resource group, you must assign the managing device to the resource group.

NOTE: Targets may belong to multiple groups.

To create a nested resource group:

1. From the left-hand sidebar, click *Targets - Resource Groups*.
2. Click the Add icon (+). An Add Resource Group dialogue box appears.
3. Enter a name for your resource group.
4. Check the box(es) for the desired target(s) you wish to add to the group.

-or-

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

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

5. When finished, click *Add Resource Group*.

To delete a resource group:

1. From the left-hand sidebar, click *Targets - Resource Groups*.
2. Click the vertical ellipses to the right of the group.

-or-

Check the box next to the group folder, then click the Delete icon (trash can).

NOTE: To delete multiple groups simultaneously, check all desired boxes.

4.3.5 Virtualization

From the Virtualization screen, you can view the list of Virtual Machine Managers and Hypervisors that are managed by the management platform. You can also add Virtual Machines (VMs).

NOTE: VMs can also be added from the Appliance View or Targets List screen. For more information, refer to [Adding and deleting devices](#) on page 15.

To add a VM as a target device:

1. From the left-hand sidebar, click *Targets - Virtualization*.
2. Click the Add Hosts icon (+) in the top right corner. An Add Host(s) dialogue box appears.
3. Enter the IP address of the Virtual Machine Manager or Hypervisor.
4. Enter the username and password credentials.
5. Click *Add Host(s)*.

4.3.6 Discoveries

From the Discoveries screen, you can discover target devices by entering a range of IP addresses. Two tabs are presented 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.
- Discover and add devices by clicking the Add Device icon (+) in the top right corner. For further instructions, refer to [Adding and deleting devices](#) on page 15.

4.4 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 MP1000 Management Platform allows you to launch multiple sessions simultaneously to access your target devices via the management platform web UI.

4.4.1 Sessions List

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

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, IP address or start time.
- 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 4.3 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

Table 4.3 CSV File Field Descriptions (continued)

Column Name	Description
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	<p>Mode of the user session:</p> <ul style="list-style-type: none"> 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	<p>State of the user session:</p> <ul style="list-style-type: none"> SS_PENDING = session is defined but not yet connected SS_INITIATED = session initiated in the process to be connected SS_CONNECTED = session is connected 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	<p>Type of user session:</p> <ul style="list-style-type: none"> ST_UNSPECIFIED = 0; // the value has not been specified ST_KVM = remote Keyboard/Video/Mouse session

Table 4.3 CSV File Field Descriptions (continued)

Column Name	Description
	<ul style="list-style-type: none"> • 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

4.4.2 KVM sessions

The Avocent MP1000 Management Platform 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 management platform, the target screen appears in a new window, and the target server can be controlled remotely. In addition to controlling each target device, you can access target server files, manage software updates and execute operating system commands. Each target server has a device information panel that contains data about the device.

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 4.4 KVM Viewer Feature and Browser 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 management platform for launching KVM sessions.

Table 4.5 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 - Targets List*.
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 MP1000 Management Platform using the *Settings* icon. **Table 4.6** below provides descriptions of the various KVM features. The availability of the KVM Video Viewer features varies by device type.

Table 4.6 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	<p>NOTE: These settings apply to all users.</p> <ul style="list-style-type: none"> • <i>Audio Configuration</i> - Configure the number of audio channels and audio quality level.

Table 4.6 KVM Video Viewer Features (continued)

Tab	Feature	Description
View (continued)	Audio & Video Options (continued)	<ul style="list-style-type: none"> <i>Video Color Settings</i> - 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. <i>Video Noise Filter</i> - Enable noise filter for VGA or disable it for a digital video source. <i>Video Lane Settings</i> - 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	<p>Send multi-key commands to make sure the command string is accurate.</p> <p>After you select the applicable operating system, select <i>Static Macros</i> 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 <i>Send</i>. 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.</p> <p>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.</p>
	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 selected with the Exclusive Mode setting enabled, no other user in the system can switch to that target.
	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	Optimize your network bandwidth for better session performance.

Table 4.6 KVM Video Viewer Features (continued)

Tab	Feature	Description
	Bandwidth	
Tools (continued)	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 below.	

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 4.7 Feature Comparison for IP KVM Device Viewers

Feature	Standalone Vertiv™ Avocent® IPUHD 4K IP KVM device	Avocent MP1000 Management Platform/ Vertiv™ Avocent® RM1048P Rack Manager (Vertiv™ Avocent® IPUHD 4K IP KVM device)	Avocent MP1000 Management Platform/ Vertiv™ 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, click *Reset Virtual Media 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 particular drive.

-or-

Click *Disconnect* 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 4.8 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 MP1000 Management Platform, the Vertiv™ Avocent® MP1000VA Management Platform Virtual Appliance and the Vertiv™ Avocent® RM1048P Rack Manager. Supported target devices for Viewer Reconnect include the Vertiv™ Avocent® IPIQ IP KVM device and the Vertiv™ Avocent® IPUHD 4K IP KVM device.

4.4.3 Serial sessions

The Avocent MP1000 Management Platform provides serial management via the Vertiv™ Avocent® ACS 800/8000 advanced console system or an Vertiv™ Avocent® IPSL IP serial device.

NOTE: When adding to the management platform, the advanced console system should not be enrolled with any other platform, such as the Vertiv™ Avocent® DSView™ management software.

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 side of the column, click the Launch Console 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 4.9 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.

4.4.4 Web UI sessions

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

To launch the web UI session:

1. From the left-hand sidebar, click *Targets - Appliance View*.
2. Hover your mouse over the desired device (for example, iDRAC) and click the vertical ellipsis on the right side of the row.

Figure 4.2 SP Target Device

The screenshot displays the 'Targets List' interface. The table below represents the data shown in the 'Targets List' table:

Name	Category	Device Type	Address Type	IP Address	Top Level Device	Firmware Version	Status
Device-192.168.10.101	Target	ADX IPIQ	IPv4	192.168.10.101	Device-192.168.0.28	4.1.4.0	✓
Device-192.168.0.28	Appliance	ADX RM1048P	IPv4	192.168.0.28	--	202006_134-38s_vpp_20.09-17s_v1.12.3	✓
Device-192.168.0.193	Target	ADX IPIQ	IPv4	192.168.0.193	--	4.1.4.0	✓
<input type="checkbox"/> SP-192.168.10.104	Target	iDRAC	IPv4	192.168.10.104	--	4.32.10.00	✓
Device-192.168.10.102	Target	ADX IPIQ	IPv4	192.168.10.102	Device-192.168.0.28		

The detailed view on the right shows the device 'SP-192.168.10.104' managed by 192.168.0.28. The view includes sections for Properties, User Access, and Credential Profiles. A context menu is open over the selected device, showing options: Delete, Go to webpage, Resync, and Firmware Update.

3. Click *Go to webpage*.
4. Enter the username and password, then click *Log In*. You are redirected to the webpage of the device.

4.5 Management

The Management tab contains two sub-menu items - Devices and High Availability - from which you can view general management information about connected target devices and configure server redundancy for the appliance.

4.5.1 Devices

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

To navigate through the Devices tab:

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 and configure a managed device's settings by clicking on the orange link in the Name column.

4.5.2 High availability

From the High Availability screen, you can configure up to three nodes for server redundancy. The High Availability (HA) feature enables you to reduce downtime and ensures continuous data replication by synchronizing a maximum of three nodes within a cluster. A cluster contains a primary node that replicates its data to one or two standby nodes. Standby nodes are promoted to Primary mode if any system service fails or can be promoted manually to allow for maintenance operations, such as firmware upgrades.

NOTE: While multiple clusters can exist on a single subnet, nodes can only belong to a single cluster at a time.

This section covers the following topics for HA:

- [Prerequisites](#)
- [Creating and configuring server redundancy](#)
- [Accessing the HA cluster](#)
- [Configuring and initiating failover](#)
- [Removing nodes and deleting the cluster](#)
- [Resetting a node](#)

Prerequisites

Before creating a cluster for server redundancy, ensure the nodes meet the following requirements:

- Must be the same appliance type. For example, if the primary node is a management platform hardware appliance, then you cannot add a standby node that is a management platform virtual appliance. All nodes must be either a hardware appliance or a virtual appliance.
- Must use the latest firmware version. To upgrade to the latest firmware, refer to [Firmware](#) on page 56.
- Must be configured with a static IP address. This is because if the node is configured with DHCP, it may receive a different IP address when restarted and become unavailable to the cluster. To configure a static IP address, refer to [Ethernet interfaces](#) on page 68.

- Must have the Network Time Protocol (NTP) enabled on the same NTP server to ensure the time settings are consistent for all nodes. If the time settings are not synchronized, the Vertiv™ Avocent® RM1048P Rack Managers that are enrolled on the management platform may not transition properly during failover.
- Must have a High Availability license uploaded on the primary node. The HA license specifies how many nodes are permitted on a single cluster, excluding the Primary node. You cannot add more nodes to a cluster than specified by the license. HA licenses can only be applied to the Primary node in a cluster; Standby and Maintenance nodes do not need their own independent licenses. During failover, the HA license is transferred to the new acting Primary node. While the HA license remains valid for the new Primary node, any future licenses being added to the system will need to use the new Primary node's product lock code. To activate and add an HA license to the primary node, refer to [License](#) on page 64.
- Must have the High Availability Policy setting enabled to allow a Standby node to be added to the cluster. To enable the HA settings, refer to [High availability](#) on page 57.

Creating and configuring server redundancy

The management platform supports up to three nodes within a cluster. A cluster must contain at least two nodes (one primary and one standby) for server redundancy. For additional reliability, a second standby node may be added to the cluster. Four different server modes are available for the management platform:

- Primary - The managing server in a cluster.
- Standby - A non-managing server in a cluster to which data is replicated.
- Maintenance - A server undergoing maintenance operations.
- Standalone - An independent server not included in a cluster.

NOTE: To avoid data collisions, all new data entries, except for maintenance operations, should be entered on the Primary node only.

NOTE: Maintenance mode is intended only for service activities such as firmware upgrades. Data replication does not occur on nodes when set to Maintenance mode. If any changes are made to a node while in Maintenance mode, data may be lost.

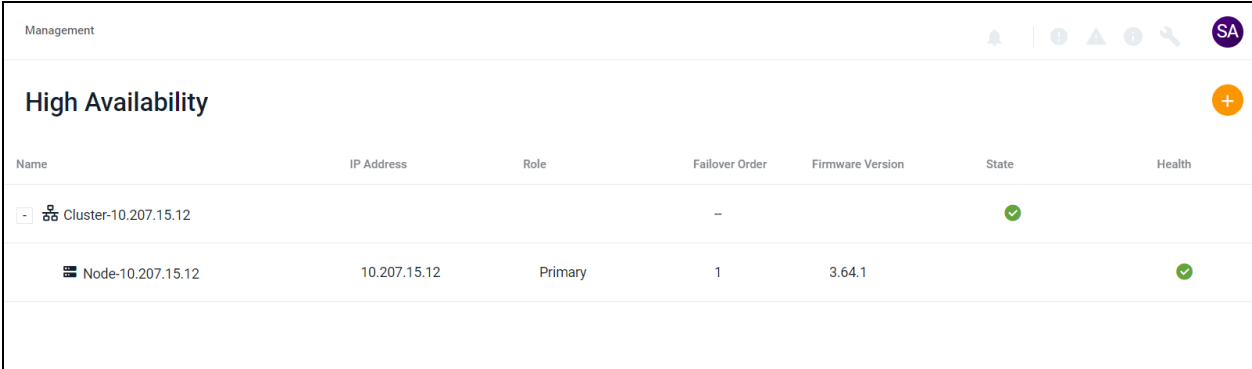
Clusters should be created from the Primary node's web UI. When a cluster is created, the management platform you are currently logged into automatically becomes the Primary node. Any nodes added afterward become Standby nodes, which are reserved for system failover.

To create a cluster:

1. From the left-hand sidebar, click *Management - High Availability*.
2. Click the plus icon (+) in the top right corner, then click the *Create Cluster* button.
3. A Create Cluster dialog box appears. Click the Continue box.

- The cluster appears on the High Availability screen with a green checkmark status indicating that the cluster is healthy. The Primary node (the appliance on which the cluster was originally created) is automatically added to the cluster. After creating a cluster with a Primary node, at least one Standby node should be added.

Figure 5.1 Cluster Created



The screenshot shows the 'High Availability' management page. At the top, there is a 'Management' header and a 'High Availability' title with a plus icon. Below the title is a table with columns: Name, IP Address, Role, Failover Order, Firmware Version, State, and Health. The table contains two rows: a cluster entry and a primary node entry.

Name	IP Address	Role	Failover Order	Firmware Version	State	Health
Cluster-10.207.15.12			--		✓	
Node-10.207.15.12	10.207.15.12	Primary	1	3.64.1		✓

To add a node to the cluster:

- From the left-hand sidebar, click *Management - High Availability*.
- Click the plus icon (+) in the top right corner, then click *Add Node*.



CAUTION: The following warning message appears: *This will add a new node to the cluster in Standby mode. All data will be erased from the host during this operation. Additionally, only administrator users can access a node in Standby mode.*

- Check the Continue box, then click *Add Node*.

4. Enter the static IP address and admin credentials for the Standby node, then click *Add Node*.

NOTE: If the standby node does not already have a static IP address, then one must be configured.

Figure 5.2 Add Node Data

Add Node ×

This will add a new node to the cluster in Standby mode. All data will be erased from the host during this operation.

IP Address:

The administrator login credentials for the remote host are required for the initial communication and conversion of the remote host.

Username

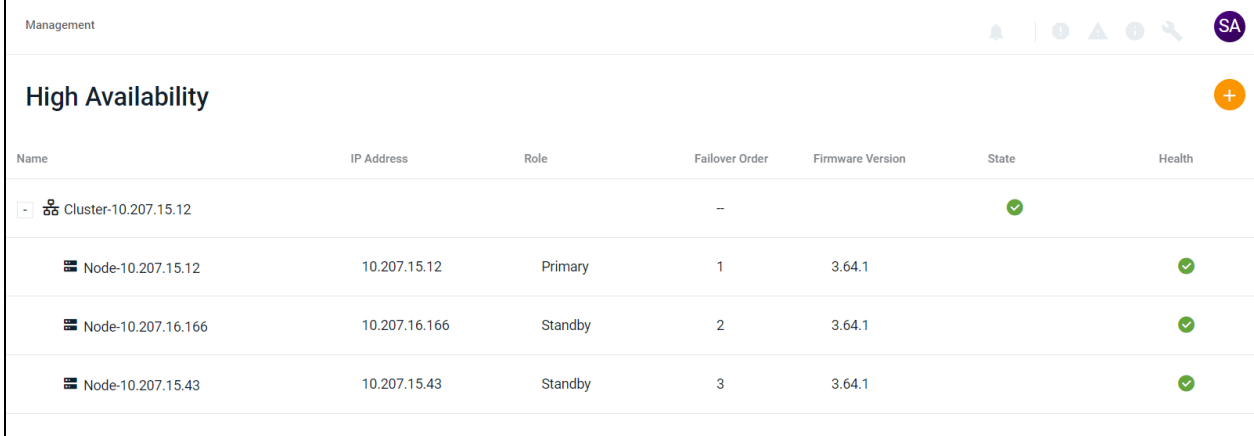
Password

Cancel Add Node

- The Primary node's data begins replicating to share and synchronize with the Standby node. When the Health icons turn green, data replication is established. This can take several minutes. When complete, the cluster should look similar to the following figure, depending on how many Standby nodes were added.

NOTE: You must wait several minutes after the Health icon turns green before attempting to perform failover operations. If data has not been fully replicated and failover is initiated, data may be lost.

Figure 5.3 Complete Cluster



Name	IP Address	Role	Failover Order	Firmware Version	State	Health
Cluster-10.207.15.12			--		✓	
Node-10.207.15.12	10.207.15.12	Primary	1	3.64.1		✓
Node-10.207.16.166	10.207.16.166	Standby	2	3.64.1		✓
Node-10.207.15.43	10.207.15.43	Standby	3	3.64.1		✓

Accessing the HA cluster

After configuring the system for HA, you should now have a Primary node and at least one Standby node within a cluster. Each node maintains its own unique IP address. The cluster can be accessed via the primary node's IP address. Open a web browser, then enter the IP address of the Primary node in the following format: <https://<appliance.IP>>. You are directed to the web UI of the current managing node in the cluster.

NOTE: The IP address used to access the cluster will change in the event of failover. Ensure you are always connecting to the current Primary node's IP address when attempting to access the cluster.

Configuring and initiating failover

If the HA cluster contains more than one Standby node, you can configure the Failover Order setting to establish which node will be promoted if the Primary goes down.

To configure the failover order:

- From the left-hand sidebar, click *Management - High Availability*.
- Click the plus icon (+) in the top right corner, then click *Update Failover Order*. A dialogue box appears.
- Drag and drop the nodes into the desired failover order using the two horizontal lines on the right side of the row.
- Click *Update Order*. The failover order has been successfully configured and implemented.

To promote/demote a node:

- From the left-hand sidebar, click *Management - High Availability*.
- Hover the mouse over the desired node and click the vertical ellipsis.
 - To demote a primary node to a standby, select the *Set to Standby* option and confirm the selection.
 - To promote a standby node to a primary, select the *Set to Primary* option and confirm the selection.

NOTE: It may take several minutes for the node to fully change modes.

Removing nodes and deleting the cluster

Removing a node from the cluster clears the HA license from the system and reverts the node back to its original Standalone mode.

NOTE: Primary nodes should not be removed from the cluster. For this reason, the Remove From Cluster option is not available in the primary node configuration options. If you wish to remove the primary node, then it should be demoted to a standby node and one of the standby nodes should be promoted to the new primary. Then, the original node may be removed.

NOTE: Removing a node with licenses bound to its product code will cause the licenses to become invalid. To resolve this, add a replacement license to the cluster and adjust as needed. After a valid replacement is added, delete the old invalid license.

To remove a standby node from the cluster:

1. From the left-hand sidebar, click *Management - High Availability*.
2. Hover the mouse over the desired standby node and click the vertical ellipsis.
3. Click the *Remove From Cluster* option.
4. On the confirmation screen, click the appropriate button to complete the operation.

To delete a cluster:

1. From the left-hand sidebar, click *Management - High Availability*.
2. Hover the mouse over the standby node and click the vertical ellipsis.
3. Click the *Remove From Cluster* option.
4. Perform steps 1 and 2 for any additional standby nodes, if applicable.
5. Hover the mouse over the primary node and click the vertical ellipsis.
6. Click *Delete Cluster*. The cluster has been successfully deleted.

Resetting a node

If a node is not fulfilling normal functions, such as mode transition requests, refer to the following procedure to reset the node.

To reset a node:

1. Log into the management platform's CLI using your admin credentials.
2. When the Root Menu appears, enter **12** to select the Diagnostics option.

Figure 5.4 Root Menu

```
admin's Password>
MP1000VA CLI

:: / (ROOT MENU)
enp11s0      : 10.207.16.166 (static)
Member of Cluster : 8af9b779-dac5-4816-9354-3271351b77ca
# Service Root
Product      : Avocent MP1000VA
UUID        : 96dc4d56-0b98-8f0f-c9f3-a5a89b44c74e
Software Version : 1.117.1
Firmware Version : 3.64.1
Serial Number  : VMware-56 4d dc 96 98 0b 0f 8f-c9 f3 a5 a8 9b 44 c7 4e
# Chassis
Asset Tag    : No Asset Tag
Location    :
SKU         : Not Specified
# Manager
Enrollment  : UNENROLLABLE
Current Date/Time : 2024-04-11T15:27:22+0000
Options:
0 Exit the CLI
1 Show/Configure Network Settings
2 Show Thermal and Power Data
3 Show/Configure Chassis
4 Show/Configure Manager
5 Backup and Restore
6 High Availability
7 Account Settings
8 Update Firmware
9 Reset to Factory Defaults
10 Shutdown
11 Reboot
12 Diagnostics
Select an option:
/> 12|
```

3. Enter **4** to restart a service on the node.

Figure 5.5 Diagnostics Options

```

:: /diagnostics
Options:
0 Root Menu. ENTER to Refresh Menu. ".." For Previous Menu.
1 Show Logs
2 Save Logs to USB
3 Show Services
4 Restart Service
5 Set Logging Level for a Service
6 Ping an Address
7 Trace Route
8 TCP Connect
9 Test connection to NTP servers
10 Show Enrolled Managers
Select an option:
/diagnostics> 4|

```

4. From the Restart Service list, locate the system-management option, then enter the associated number.

Figure 5.6 Restart Service List

```

49 scheduler Up 5 days (healthy)
50 serial-viewer Up 5 days
51 sessionmgt Up 5 days (healthy)
52 sip-docker Up 5 days
53 sp-management Up 34 minutes (healthy)
54 spider-pkg Up 34 minutes
55 symmetricds Up 28 minutes
56 symmetricds Exited (129) 28 minutes ago
57 symmetricds Exited (129) 28 minutes ago
58 symmetricds Exited (129) 28 minutes ago
59 symmetricds Exited (137) 28 minutes ago
60 system-management Up 34 minutes (healthy)
61 tacacs-authentication Up 34 minutes (healthy)
62 tftp Up 5 days
63 tor-management Up 5 days (healthy)
64 ui Up 5 days (healthy)
65 ui-redirect-management Up 5 days
66 unleash-server Up 5 days
67 unleash-server Exited (1) 5 days ago
68 updater Up 5 days
69 user-management-local Up 5 days (healthy)
70 vm-viewer Up 5 days
71 vmsync Up 34 minutes (healthy)
72 ws-proxy Up 5 days
Service number> 60|

```


5. The service has been restarted, and the node has been reset. Wait a minute to allow the system to reconnect to other services. If you wish to view the status of the restart, enter **3** to select the Show Services option.

Figure 5.7 Service Restarted

```
** Service has been restarted. **  
  
** Please allow the system a minute to reconnect to other services. **  
  
** Select 'Show Services' in the diagnostic menu to check the status. **  
  
:: /diagnostics  
Options:  
0 Root Menu. ENTER to Refresh Menu. ".." For Previous Menu.  
1 Show Logs  
2 Save Logs to USB  
3 Show Services  
4 Restart Service  
5 Set Logging Level for a Service  
6 Ping an Address  
7 Trace Route  
8 TCP Connect  
9 Test connection to NTP servers  
10 Show Enrolled Managers  
Select an option:  
/diagnostics> |
```

If the issue persists, perform one of the following procedures:

Select a new primary node. Once all nodes within the cluster display a Normal status (green checkmark), you may switch back to the previous primary node.

-or-

Remove the malfunctioning node from the cluster, then re-add it.

4.6 Administration

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

4.6.1 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 facing 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, an administrator must place the target devices into a resource group, then assign the resource group to user groups. For instructions, refer to [Groups](#) on the facing page.

Users

From the Users tab, you can view all users and user specific information for the Avocent MP1000 Management Platform. 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.
- 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 target and check the box of the left.

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

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 MP1000 Management Platform. A user group defines the view and 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 *Resource Groups* to view and configure the assigned resource groups.
 - 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.

To assign system roles to a user group:

1. From the *Groups* tab, click the newly added user group to open its side panel, then click the Edit icon (pencil) next to the *Group Properties* heading.
2. Under the *System Roles* heading, select the desired system role(s) to be added to the user group. If you wish to create a new system role, refer to [Roles and permissions](#) on the next page.
3. Click *Save Changes*. The user group has now been created and assigned permissions.

NOTE: After adding the system role to the user group, you must define the resource group. To create a resource group, refer to [Resource groups](#) on page 20. Then, you must assign the user group to the desired resource group.

To assign a user group to a resource group:

1. From the *Groups* tab, click on the desired user group to open its side panel.
2. Click *Resource Groups* to expand its menu, then click the Edit icon (pencil).
3. Check the box for the appropriate resource group and click *Save Changes*.
4. The resource group must be assigned at least one target role. If you wish to create a new target role rather than use a pre-configured one, refer to [Roles and permissions](#) below.
5. Once the changes have been saved, hover the mouse over the resource group to select the Edit Roles icon.
6. Check the box for the appropriate target role(s), then click *Save Changes*. Non-administrator users within the configured user group can now view all target devices assigned to that resource group.

To delete a user group:

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

NOTE: Multiple users on the same network can be added to the management platform by mapping the Active Directory (external) group to the local user group. To perform group mapping, refer to the [Vertiv™ Avocent® Mapping Local User Groups to External Authentication Provider User Groups Technical Note](#), which can be found on the [Vertiv™ Avocent® MP1000 Management Platform product page](#) under the *Documents & Downloads* tab.

4.6.2 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](#) on the facing page.

For information on adding, deleting or editing roles and permissions for the Avocent MP1000 Management Platform, refer to [Configuring roles and permissions](#) on page 49.

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 User Interface (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

NOTE: Only administrator users can view all target devices. If non-administrator users wish to view target devices, an administrator must place the target devices into a resource group, then assign the resource group to user groups. For more instructions, please see [User management](#) on page 42.

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 [User management](#) on page 42.

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. The following list highlights the two default target roles:

- User Target Role
- System Maintainer Target Role

User groups can be associated with one or more target roles. Additionally, the user group may be associated with a collection of targets called resource groups. Resource groups can include one or more target roles that define the user permissions allowed for the target devices within the group. For more information on resource groups, please see [Resource groups](#) on page 20.

Table 5.1 below 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 5.1 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	✓	✗	✗	✗	✗	✗

Table 5.1 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
View Appliance SSL Certs	✓	✗	✗	✗	✗	✗
View Event Log	✓	✓	✗	✗	✗	✗
Configure Event Data Retention Policy	✓	✓	✗	✗	✗	✗
View Event Data Retention Policy	✓	✓	✗	✗	✗	✗
View System Logs	✓	✓	✗	✗	✗	✗
Configure Licensing	✓	✓	✗	✗	✗	✗
View Licensing	✓	✓	✗	✗	✗	✗
Configure User Profile	✓	✓	✗	✗	✗	✗
View User Profile	✓	✓	✗	✗	✗	✗
Configure User Policy	✓	✓	✓	✓	✗	✗
View User Profile	✓	✓	✓	✓	✗	✗
Configure User Policy	✓	✗	✓	✗	✗	✗
View User Policy	✓	✗	✓	✗	✗	✗
Change User Password	✓	✓	✓	✓	✗	✗
Configure Devices	✓	✓	✗	✗	✗	✓
View Devices	✓	✓	✓	✓	✓	✓
Upgrade Firmware	✓	✓	✗	✗	✗	✓
Configure KVM Session	✓	✗	✗	✗	✗	✗
Establish KVM Session	✓	✓	✓	✓	✓	✓
Establish VKVM Session	✓	✓	✗	✓	✓	✓
Establish Exclusive Session	✓	✗	✗	✗	✗	✗
Establish Stealth Session	✓	✗	✗	✗	✗	✗
Configure Serial Session	✓	✗	✗	✗	✗	✗
Establish Serial Session	✓	✓	✓	✓	✓	✓

Table 5.1 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
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	✓	✓	✗	✗	✗	✓
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	✓	✗	✗	✗	✗	✗

Table 5.1 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
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	✓	✓	✗	✗	✗	✗
Purge Event Log	✓	✗	✗	✗	✗	✗
Reboot Server	✓	✗	✗	✗	✗	✗
Shutdown Server	✓	✗	✗	✗	✗	✗
Power Control	✓	✓	✗	✗	✗	✓
Reset Control	✓	✓	✗	✗	✗	✓
Boot order Control	✓	✓	✗	✗	✗	✓
Restart Control	✓	✓	✗	✗	✗	✓
Led Control	✓	✓	✗	✗	✗	✓
Configure Scheduled Jobs	✓	✓	✗	✗	✗	✗
View Scheduled Jobs	✓	✓	✗	✗	✗	✗

Table 5.1 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
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 target and check the box to the left.
3. Click the Delete icon (trash can).
4. At the confirmation screen, click Yes to delete.

4.6.3 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 of your target devices. A credential profile stores the user ID and password for a single user and can be used across different target device types. Credential profiles are required for the following device types: Service Processors, ACS, Rack PDUs, Rack UPS, DSView and Virtual Machines. 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:

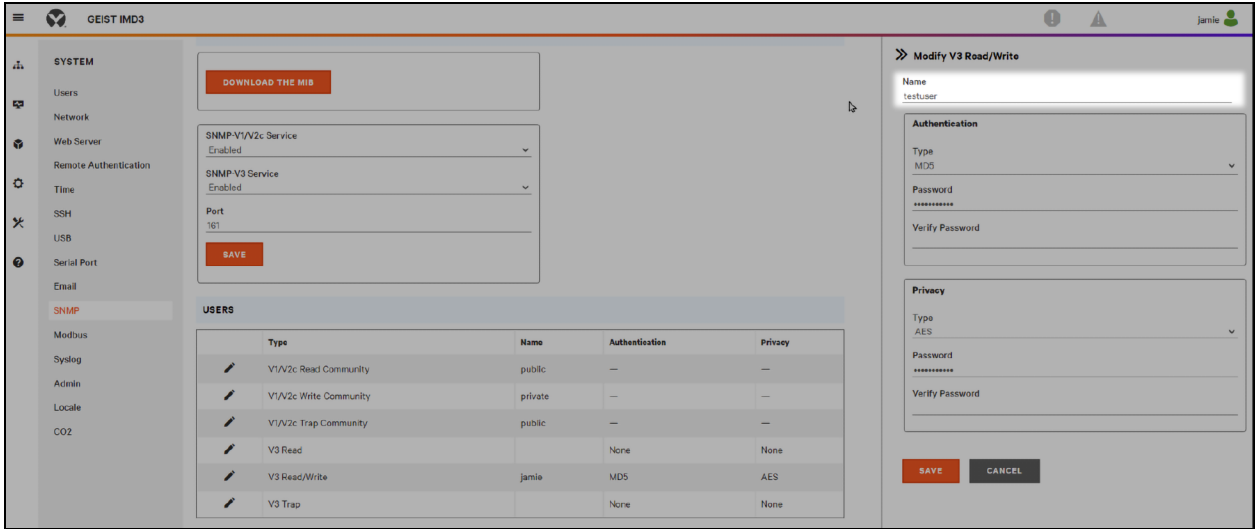
1. From the left-hand sidebar, click *Administration - Credential Profiles*.
2. Click the Add icon (+) in the top right corner. An Add credential profile dialogue box appears.
3. Enter a profile name.
4. From the Profile Type drop-down menu, click *SNMPv1/v2*.
5. Specify the version in the Version field: *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*.

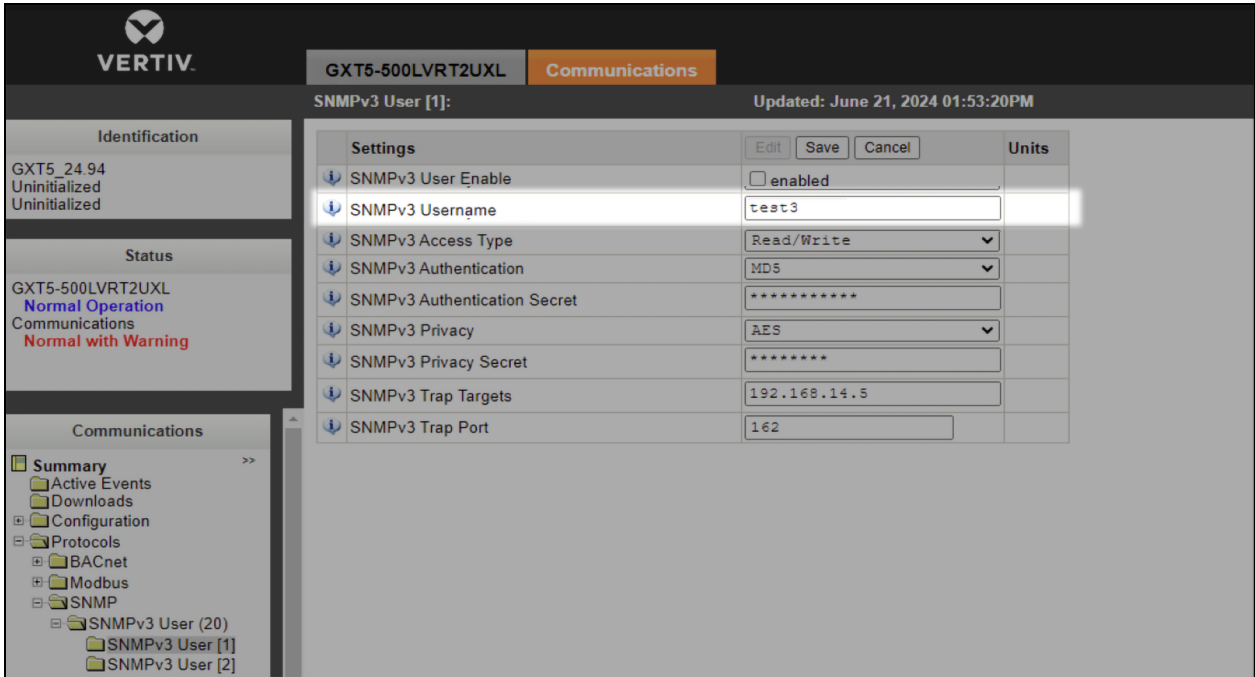
- 5. Enter a valid username.
 - Vertiv™ Geist™ rPDUs require the username to match the existing SNMPv3 username configured on the device.

Figure 5.8 Rack PDU Username Example



- Vertiv™ Liebert® rack UPSes require the username to match the existing SNMPv3 username configured on the device.

Figure 5.9 Rack UPS Username Example

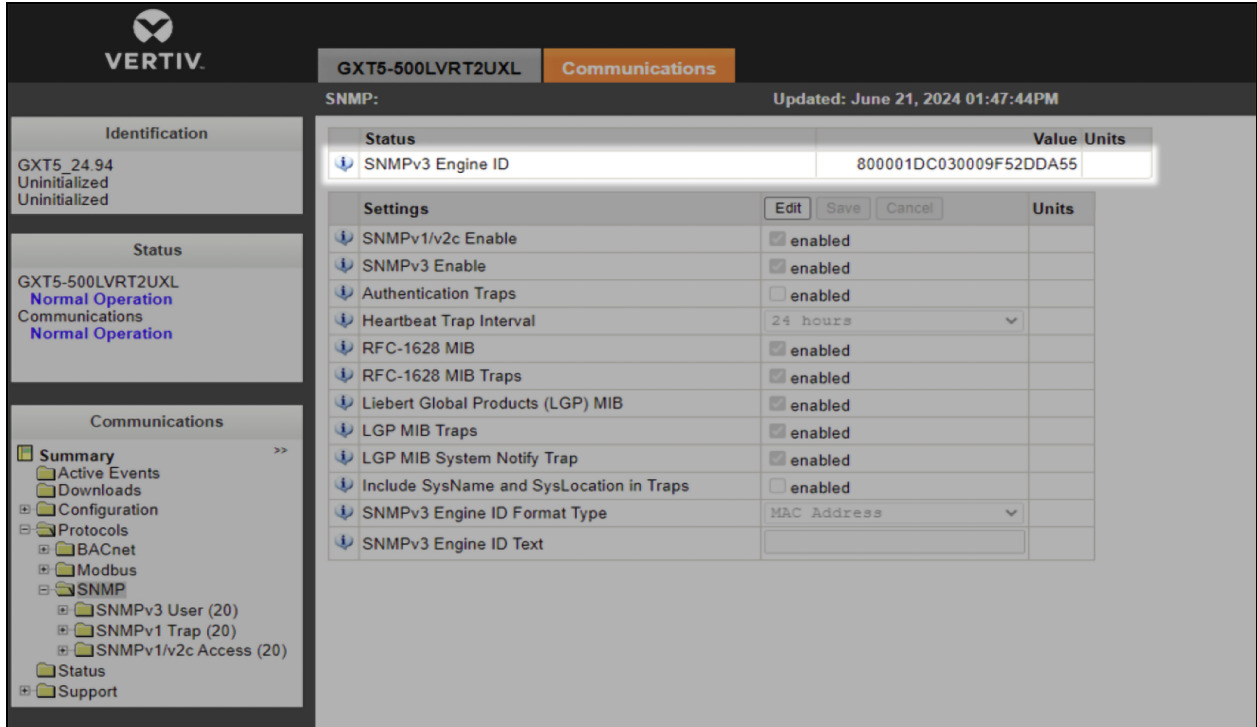


- 6. (Optional) Enter an engine identification number in the Engine ID field to create a unique credential profile for a single device. If the credential profile will be used for multiple devices, an engine ID is not needed.

- 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 5.10 below .

Figure 5.10 Rack UPS Engine ID Example

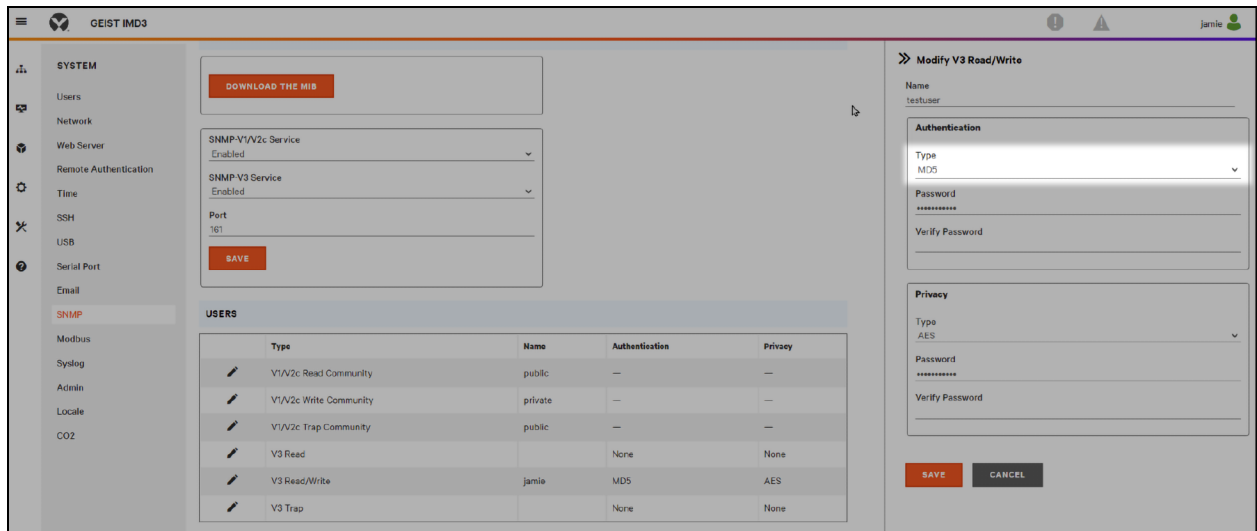


7. Enter a port associated with SNMPv3 in the Port field. The default port is 161.
8. (Optional) Enter the context name in the Context Name field. The SNMPv3 context allows multiple instances of the same SNMP object on a device.
9. (Optional) Enter the context ID in the Context ID field.

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 5.11 on the facing page.

Figure 5.11 MD5 Cryptography Hash Function Example



Adding a Vertiv™ Avocent® DSView™ 4.5 management software zone

The Vertiv™ Avocent® DSView™ 4.5 management software uses zones to provide multitenancy capabilities for your data center. Zones allow for the virtual segregation of server resources, including appliances, target devices and virtual machines. Each zone operates as an independent subset of the management software and maintains its own user administration. Adding a Vertiv™ Avocent® DSView™ 4.5 management software zone to the management platform enables you to view all target devices within that zone. For more information on the management software zones, please see the Vertiv™ Avocent® DSView™ 4.5 Management Software Installer/User Guide located on www.vertiv.com.

NOTE: The Avocent MP1000 Management Platform only supports top level zones. Sub-level zones are not supported.

To add a zone to the management platform:

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. Select *Username/Password* from the Profile Type drop-down menu.
5. Enter the username and password, then confirm the password.
6. Enter the port number.
7. Enter the appropriate zone.

NOTE: If a zone is not specified, the system will attempt to manage the software using only the username and password.

8. (Optional) Add a note, if desired.
9. Click *Add credential profile*. The credential profile has been created and now must be discovered by the management platform. To discover the zone, refer to [Discoveries](#) on page 21.

4.6.4 Events

From the Events screen, you can view the saved log of 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.

4.6.5 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.

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*.

4.6.6 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 MP1000 Management Platform supports remote group authorizations. For more information, see the following sections:

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

Adding and configuring authentication providers

To add an authentication provider:

1. From the left-hand sidebar, click *Administration - Authentication Providers*.
2. Click the Add icon (+) in the top right corner.
3. Select *AD/LDAP*, *TACACS+* or *RADIUS* as the authentication type from the drop-down 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 (trash can).
4. At 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*.

Mapping local user groups

You can map local user groups to user groups from an external authentication provider such as Active Directory (AD) or LDAP, which simplifies administration by allowing you to centrally manage user permissions and access. After the mapping is completed, members of the external authentication provider user group will have the same target permissions as the users from the local user group.

To map local user groups to AD or LDAP user groups:

Refer to the Vertiv™ Avocent® Mapping Local User Groups to External Authentication Provider User Groups Technical Note, which can be found on the [Vertiv™ Avocent® MP1000 Management Platform product page](#) under the *Documents & Downloads* tab.

4.6.7 Firmware updates

From the Firmware Updates screen, you can view the scheduled firmware updates. The Status column reflects the current status of the firmware updates. If needed, click the Refresh icon in the top right corner to refresh the page. For information on updating the firmware for the management platform, refer to [Firmware](#) on the next page.

For information on updating the firmware for target devices, refer to [Performing maintenance activities](#) on page 16.

4.6.8 System settings

From the System Settings screen, administrators can view and configure the system settings for the Avocent MP1000 Management Platform. System settings include the following:

- [Firmware](#)
- [Password policy](#)
- [High availability](#)
- [Lockout policy](#)
- [Timeout](#)
- [Date and time](#)
- [Events retention](#)
- [Alarms retention](#)
- [Viewer settings](#)
- [Standalone KVM viewer settings](#)
- [DSView unit group mapping](#)
- [License expiration notification](#)
- [FIPS module](#)
- [Proxy configuration](#)
- [Synchronization configuration](#)
- [Syslog destination](#)
- [Email server configuration](#)
- [Notification configuration](#)
- [SSH passthrough](#)
- [Certificate](#)
- [Reboot appliance](#)
- [Factory reset](#)

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

Firmware

You can update the firmware for the management platform to the latest version. Firmware updates can also be performed for target devices from the Targets List or Appliance View screen.

To update the firmware:

1. From the sidebar of the System Settings screen, click *Firmware*.
2. Click (*Download Page*). The [Vertiv™ Avocent® MP1000 Software Downloads](#) page opens in a new tab.
3. Download the latest firmware version for your appliance type (hardware or virtual).
4. Save the firmware to your local PC, FTP, HTTP or TFTP server.
5. Return to the *System Settings* screen of the web UI and click the *Update Firmware* button.
6. Select the firmware file and click *Update*.

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.

High availability

If you have a High Availability license, you can create High Availability clusters with one primary and up to two standby nodes for server redundancy. Adding a node to a cluster is a protected operation that requires you to enable the explicit permission. It is highly recommended to enable both the High Availability and Manual Role Control settings before adding a node to the cluster.

To enable the HA permissions for creating a cluster:

1. From the sidebar of the System Settings screen, click *High Availability*.
2. Click the High Availability toggle button to allow the host server to join a cluster.
3. Click the Manual Role Control toggle button to allow authorized users to initiate High Availability mode transitions.
4. Click *Save*.

For more information about creating and configuring HA clusters, refer to [High availability](#) on page 33.

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 attempt.
5. If you enabled the Login Retry Timeout button, enter the duration of the timeout in the Retry Timeout field.
6. Click the Automatically Unlock Account toggle button to unlock the account that was locked out after a set amount of time.
7. 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.

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.
5. 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.
6. 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.
7. Click *Save*.

DSView unit group mapping

You can enable the mapping of Vertiv™ Avocent® DSView™ 4.5 management software groups to resource groups for the management platform.

To enable group mapping for Vertiv™ Avocent® DSView™ units:

1. From the sidebar of the System Settings screen, click *DSView Unit Group Mapping*.
2. Click the toggle button to enable group mapping.
3. Click *Save*.

License expiration notification

You can configure how far in advance you wish to be notified about the expiration of your system license(s). By default, an expiration notification for licenses appears 120 days prior to the expiration date.

To configure the license expiration notification:

1. From the sidebar of the System Settings screen, click *License Expiration Notification*.

2. In the Days field, enter the number of days you want to be notified in advance about the license expiry.
3. Click *Save*.

NOTE: If the system does not have a valid license, all the buttons are disabled (grayed out). You cannot perform any functions within the web UI until new licenses have been obtained.

NOTE: If the target device count exceeds the number of reserved licenses, no new devices can be added; however, regular functions can still be performed until the license expires.

FIPS module

You can enhance the security of your management platform, 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.

Proxy configuration

You can configure a proxy server to access all KVM/serial session traffic through the Avocent MP1000 Management Platform

To enable proxy configuration:

1. From the sidebar of the System Settings screen, click *Proxy Configuration*.
2. Click the toggle button to enable the Proxy Configuration setting.
3. For secure access, select one of the following options:
 - a. **Use the proxy server for all sessions:** permits all traffic through the management platform IP address for any KVM sessions that are launched.
 - b. **Use the proxy server only for clients not on the same network as this Management Platform:** allows the use of proxy for all those client machines that are not on the same network as the management platform. This option is used when the client network segment is at different location than management platform.
 - c. **Use the proxy server only for clients connecting with following addresses:** allows the use of proxy for specific IP addresses. You can select the radio button for either Single IP Address or Range IP Address. Enter the IP address, then click *Add*.
4. Click *Save*.

Syslog destination

You can configure the application to send all the audit events to your syslog server. The syslog server acts as the aggregation point for various different applications.

NOTE: The Audit Events page logs all user activities.

To set up Syslog Destination:

1. From the sidebar of the System Settings page, click *Syslog Destination*.

2. Click the plus icon (+) in the top right corner. An Add Syslog Destination dialogue box appears.
3. Select the protocol from the Protocol drop-down menu.

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

4. (Optional) If using the TCP - Secure protocol option, enter a valid TLS certificate in the Certificate field.
5. In the Destination IP field, enter the IP address of the syslog server.

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

6. (Optional) Add a name to the Tag field, if desired.
7. Select the appropriate syslog facility from the Facility drop-down menu.
8. Click *Test Connection*. If the IP Address is valid, a *Test Connection Successful* message pops up. If invalid, a *Test Connection Failed* message pops up.
9. Click *Add*.
10. Click the toggle button to enable the syslog connection.

Synchronization configuration

You can synchronize the device name and data between the management platform and targets. Before synchronizing devices, you must enable and configure the synchronization settings.

NOTE: The web UI may refer to the management platform as 'ADX' and the targets as 'Device.'

To prepare for device synchronization:

1. From the left-hand sidebar, click *Administration - System Settings - Synchronization Configuration*.
2. Click the toggle button to enable the Synchronization Configuration setting.
3. For the Synchronization Direction field, select the appropriate radio button:
 - Device to ADX
 - ADX to Device
4. Select the device daily sync time (GMT+5.5).

NOTE: By default, it shows the real time of your location.

5. Click *Save*. Once saved, you can now synchronize your devices. For more information, refer to [Synchronizing devices](#) on page 17.

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 policy](#) on page 69.

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® ACS8000 advanced console systems and its targets that are managed by the management platform.

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 management platforms for external users.

NOTE: Each target device used for SSH passthrough must have a unique name. If there are multiple targets with 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 enable or disable SSH passthrough:

1. From the sidebar of the System Setting screen, click *SSH Passthrough*.
2. Click the toggle button to enable or disable SSH passthrough.
3. Specify the SSH server port on the management platform to connect an SSH session. The default port is 4122.
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 management platform.
 - username - The username for the management platform.
 - 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 management platform web UI.
3. When prompted, enter your password for the management platform.

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.

Certificate

You can generate and install new certificate signing requests (CSRs), as well as 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.

To generate a new CSR:

1. From the sidebar of the System Settings screen, click *Certificate*.
2. Click the Generate Certificate 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 installed on the appliance.

To install a CSR:

1. From the sidebar of the System Settings screen, click *Certificate*.
2. Click the Install Certificate icon in the right corner.
3. Browse to and select the .pem file to upload.
4. Click *Upload*.

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*.

Factory reset

You can perform a factory reset on your appliance, which will remove all data from the equipment.

To perform a factory reset:

1. From the sidebar of the System Settings screen, click *Factory Reset*.
2. Click *Reset To Default Setting*.

4.6.9 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 in the table.

4.6.10 License

From the License screen, you can view the total number of licenses used, total number of targets managed, and the license expiration date. Additionally, you can add and delete licenses from this screen. For more information, see the following sections:

NOTE: To view and configure licensing, user accounts must be set up as either a System Administrator Role or System Maintainer Role. For more information, refer to Roles and permissions on page 44.

NOTE: For instructions on configuring the expiration notification for your license, refer to License expiration notification on page 59.

Activating and add licenses

NOTE: The Appliance license must be uploaded to the management platform first.



CAUTION: If you perform a backup and restore of the management platform to a different host, the added licenses will become invalid and the hardware will fail.

To activate and add a license:

1. From the left-hand sidebar, click *Administration – License*.
2. Click the Add icon (+) in the top right corner. The Add License dialogue box appears.
3. Copy the unique Product Lock Code.
4. Click the *Customer portal* link to access the portal where you will activate the license.
5. Log into the portal using the credentials you created from the email by the Vertiv Entitlement Portal Team. Upon login, a list of your purchased licenses appears. Depending on your purchase, these licenses may include Appliance, Demo, High Availability (HA) and/or Targets.
6. From the list of licenses, click the arrow on the left side of the license you wish to activate.

Figure 5.12 License List

Product	Activated	Available						
DSVS_APPLIANCE L10	26	31						
Entitlement ID	Order Date	Vertiv Order Number	Reseller PO Number	Nodes	Service Level	Activated	Available	Actions
c8049d69-4963-4114-a5c3-26fa882b807b	9/24/2024			1	-	0	5	ACTIVATE
123b2f8-519-4e8f-8fa3-7702f4c1445	9/23/2024			1	-	2	4	ACTIVATE
e67ec0c4-d55e-41d7-b810-f1bc2c76d815	8/1/2024	KLH		0	-	24	22	ACTIVATE

7. Click the orange *Activate* button on the right-hand side of the column. You are redirected to the Order Activation screen.

Figure 5.13 Order Activation Screen

Order ID: c8049d69-4961-4114-a5c3-26fa582b801b Customer Name: KLH

Activating For Myself | Activating For Another User Activate Email: kharper@no-company-i-think.com

Products | Downloads

Product	Activated	Available	Quantity To Activate
<input checked="" type="checkbox"/> DSVS_TARGETS 1.0 Expiration: 1744416000000	0	5	<input type="text" value="1"/>
<input checked="" type="checkbox"/> DSVS_HA_NODES 1.0 Expiration: 1744416000000	0	5	<input type="text" value="1"/>
<input checked="" type="checkbox"/> DSVS_APPLIANCE 1.0 Expiration: None	0	5	<input type="text" value="1"/>

Product Lock Code

Device: Available | New

Device Name: *UUID:

CANCEL | ACTIVATE

8. Ensure the box next to the appropriate license is checked.
9. Ensure the Quantity to Activate field reflects the correct value.
10. In the Device Name field, enter a device name, if desired.
11. In the UUID field, enter the product lock code you copied from the management platform web UI.
12. Click the orange *Activate* button in the bottom right corner. A window appears indicating that the activation was successful.

Figure 5.14 Activation Completed Successfully

Order ID: c8049d69-4961-4114-a5c3-26fa582b801b Customer Name: KLH

License file has been e-mailed to: kharper@no-company-i-think.com

Product	Activated
DSVS_TARGETS 1.0	1
DSVS_HA_NODES 1.0	1
DSVS_APPLIANCE 1.0	1

DOWNLOAD LICENSE FILE | CLOSE

Device: Available | New

Device Name: *UUID:

CANCEL | ACTIVATE

13. Upon activation, a License File is generated. Click the *Download License File* button to download the License File to your local system.

NOTE: You can also download your license files from the Activations page of the customer portal.

14. Open the License File in a text editor, such as Notepad, and copy the contents of the file.
15. Return to the management platform web UI to upload the license.
16. In the Add License dialogue box, paste the contents of the License File into the provided text box.

17. Click *Submit*. The license is now uploaded. Repeat this procedure for all licenses that need to be activated and added to your appliance.

Deleting licenses

NOTE: Deleting an active Appliance license is not allowed if there are other active licenses on the system. To delete the Appliance license, you must delete all other active licenses, and then delete the Appliance license.

To delete a license:

1. From the left-hand sidebar, click *Administration – License*.
2. In the License Details section, check the box on the left side of the license you wish to delete.
3. Click the Delete icon (trash can) above the licenses. The Delete License dialogue box appears.
4. Verify that you have selected the appropriate license to delete.
5. Click *Delete*. A warning message appears: Deleting Active License(s) will reduce the available quantity for use. Are you sure you want to delete?
6. Click *Yes, Delete*.

4.7 Network Configuration

The Network Configuration tab contains one sub-menu item - Settings - from which you can view and configure the network settings for the management platform, including the hostname, failover-bonded settings, failover-routed IPv4 routed trigger mode and Ethernet interfaces.

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.

4.7.1 Network settings

You can view and configure the hostname, primary DNS, secondary DNS and domain name.

To configure the network settings:

1. From the sidebar of the Settings screen, click *Network Settings*.
2. Under the Network Settings heading, adjust the settings as needed.
3. Click *Save*.

4.7.2 Normal/Failover-bonded settings

NOTE: The management platform virtual appliance only has one virtual network interface and does not support failover. While additional interfaces can be added, they will not be recognized and may cause adverse effects, depending on the DHCP client/route metrics. Therefore, this section is not included in the web UI for the virtual appliance.

The Avocent MP1000 Management Platform hardware appliance has two physical network interface ports. You can configure these ports for bonding and/or failover.

To configure failover for the network interface ports:

NOTE: The device must be rebooted for changes to take effect.

1. From the sidebar of the Settings screen, click *Normal/Failover-Bonded Settings*.
2. Using the Uplinks drop-down menu, select either *Ports not bonded*, *1st and 2nd ports bonded* or *1st fails over to 2nd port*.
3. A message appears, prompting you to confirm your selection. Click *Yes, Update*. To determine when failover is initiated, refer to [Failover-routed IPv4 trigger mode](#) below.

4.7.3 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. If you select *Unreachable IP*, then fill out the IP Address field.

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

4.7.4 Ethernet interfaces

The Avocent MP1000 Management Platform has two physical network interfaces (eno1, eno2). Each interface has an individual MAC address and can be assigned an IP address via DHCP or statically. The Ethernet Interfaces tab allows you to configure the static IP address for the management platform.

To configure a static IP address:

1. From the sidebar of the Settings screen, click *Ethernet Interfaces*.
2. Click the desired interface to open its information panel.
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*.

Adding multi-Ethernet support

NOTE: This section applies only to the Vertiv™ Avocent® MP1000 Management Platform Virtual Appliance.

When adding a second ethernet interface to the virtual appliance, you must ensure the route metric is correctly set for each interface. By default, the route metric sets to 200 for each interface to provide equal weighting to routing. The default setting is only acceptable if all targets are reachable from all interfaces. However, if some targets are on a different network segment or following different routing rules per interface, then the route metric must be increased for the private or segmented networks. This ensures the primary network (with the lowest metric) is used for clients, ancillary services such as SMTP or Active Directory, and so on. All other ethernet interfaces (with higher route metrics) are used for their respective subnets. To set the route metric, refer to the Vertiv™ Avocent® DSView™ Updating Ethernet Interface Route Metric Tech Note located on the Avocent MP1000 Management Platform product page at www.vertiv.com.

4.8 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.

4.8.1 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. Click the toggle button 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*.

This page intentionally left blank

Appendices

Appendix A: Technical Support and Contacts

A.1 Technical Support/Service in the United States

Vertiv Group Corporation

24x7 dispatch of technicians for all products.

1-800-543-2378

Avocent Software and Hardware Products

Website: www.vertiv.com/en-asia/support/warranty/it-management-hardware-support-contacts/

A.2 Locations

United States

Vertiv Headquarters

505 N Cleveland Ave

Westerville, OH 43082

Europe

Via Leonardo Da Vinci 8 Zona Industriale Tognana

35028 Piove Di Sacco (PD) Italy

Asia

7/F, Dah Sing Financial Centre

3108 Gloucester Road, Wanchai

Hong Kong

This page intentionally left blank

Appendix B: Technical Specifications

Table 7.1 Technical Specifications - Avocent MP1000 Management Platform

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

This page intentionally left blank

Appendix C: Backup and Restore

Using the Avocent MP1000 Management Platform Command Line Interface (CLI), you can enter **5** to select the Backup and Restore option to perform the following functions:

- [Perform a backup \(on-demand or scheduled\) to a local or remote server](#)
- [Configure the retention policy to preserve storage space](#)
- [Configure a schedule for backup automation](#)
- [View a list of all backups in the management platform system](#)
- [Delete a backup](#)
- [Restore a previous configuration of the management platform](#)

C.1 Limitations and Notes

Note the following information and limitations about the Backup and Restore capability of the management platform:

- The Backup and Restore feature does not support backing up one management platform and restoring it on a different appliance.
- If you have custom SSL certificates and the primary management platform's IP address changes, you will have to replace the certificates for the management platform.
- If you perform a backup and restore of the appliance to a different host, the system licenses will become invalid and the hardware will fail.
- A maximum of five local backups can be retained at once, whereas there is no limit on the number of remote backups you can retain.

C.2 Performing a Backup to a Local or Remote Server

If you wish to save the backup to a remote server, you must first configure the SMB host in the CLI. The SMB protocol must be version 2.0 or greater.

To configure the SMB host server:

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 Local option if you wish to backup the management platform locally.

-or-

Enter **2** for the SMB option if you wish to back up the management platform 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.

C.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 Local option if you wish to backup the management platform locally.

-or-

Enter **2** for the SMB option if you wish to back up the management platform 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.

C.4 Configuring a Schedule for Backup Automation

1. From the Backup and Restore menu, enter **1** for the Local option if you wish to backup the management platform locally.

-or-

Enter **2** for the SMB option if you wish to back up the management platform 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.

C.5 Viewing a List of All Backups

1. From the Backup and Restore menu, enter **1** for the Local option if you wish to backup the management platform locally.

-or-

Enter **2** for the SMB option if you wish to back up the management platform remotely.
2. Enter **2** to select the List option.

C.6 Deleting a Backup

1. From the Backup and Restore menu, enter **1** for the Local option if you wish to backup the management platform locally.

-or-

Enter **2** for the SMB option if you wish to back up the management platform 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.

C.7 Restoring a Previous Backup Configuration

NOTE: Backup restoration requires the backup to be the same firmware version as the primary management platform.

NOTE: Restoring a backup will initiate a reboot of the management platform.

1. From the Backup and Restore menu, enter **1** for the Local option if you wish to backup the management platform locally.

-or-

Enter **2** for the SMB option if you wish to backup the management platform 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 management platform. Once the system comes back online, the backup has been successfully restored.

This page intentionally left blank

Connect with Vertiv on Social Media



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



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



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



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



Vertiv.com | Vertiv Headquarters, 505 N Cleveland Ave, Westerville, OH 43082 USA

©2024 Vertiv Group Corp. All rights reserved. Vertiv™ and the Vertiv logo are trademarks or registered trademarks of Vertiv Group Corp. All other names and logos referred to are trade names, trademarks or registered trademarks of their respective owners. While every precaution has been taken to ensure accuracy and completeness here, Vertiv Group Corp. assumes no responsibility, and disclaims all liability, for damages resulting from use of this information or for any errors or omissions.

590-2355-501J