VERTIV™

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 Product Overview

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

The Avocent 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.

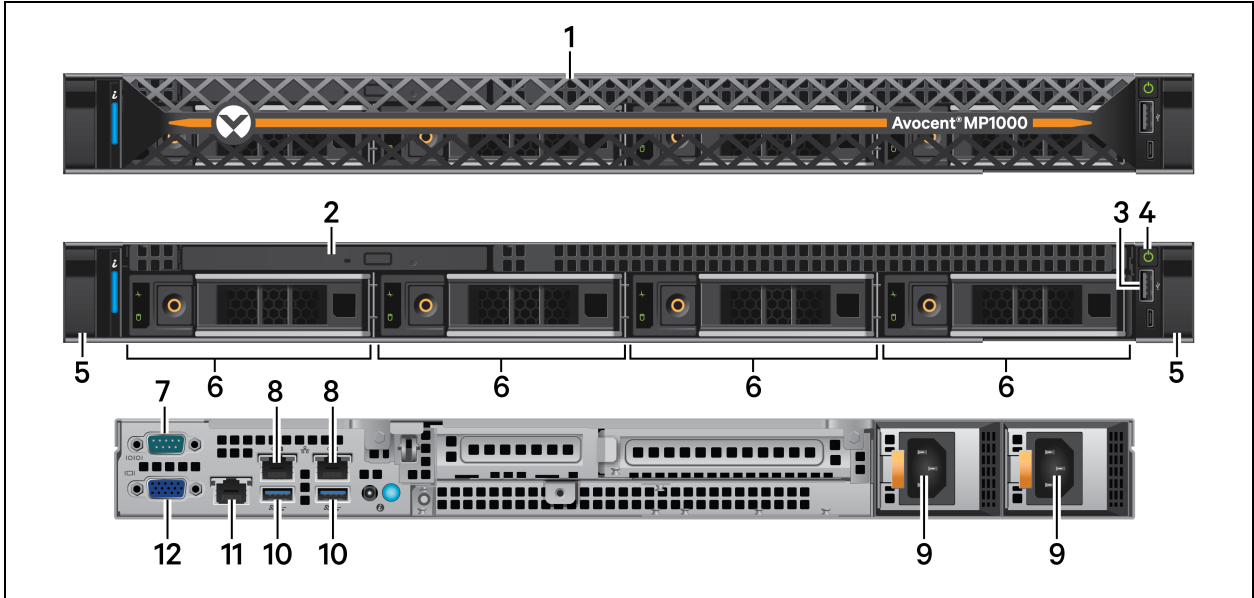**Figure 1.1   Avocent MP1000 Management Platform Description**

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

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 have 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. See the following section to ensure you have reviewed and completed all accompanying documentation for your appliance type.

1.2 Prerequisites

Before continuing, ensure you have reviewed and completed the appropriate documentation for your appliance type. The following descriptions highlight which documentation you should refer to for each appliance type.

Avocent MP1000 Management Platform hardware appliance:

- Vertiv™ Avocent® MP1000 Management Platform Quick Installation Guide

Avocent MP1000 Management Platform virtual appliance:

- Vertiv™ Avocent® MP1000VA Management Platform Virtual Appliance Getting Started Guide
- Vertiv™ Avocent® MP1000VA Management Platform Virtual Appliance Installation/Deployment Guide.

NOTE: The getting started guide should be completed before the installation/deployment guide.

To view product documentation for the management platform:

1. Go to the Vertiv™ Avocent® MP1000 Management Platform product page.
2. Scroll down and click *Documents & Downloads*.
3. Under Manuals, click on the appropriate document.

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

Once you have completed the initial documentation for the Avocent MP1000 Management Platform, you must obtain the appropriate licenses for the management platform as each appliance type has different licensing requirements. The hardware appliance requires a Base license and a Targets license. The virtual appliance only requires a Virtual Appliance License Key. These licenses allow you to launch target sessions and access the full functionality of the management platform. Additionally, if you wish to use the High Availability feature for server redundancy, each server must have a High Availability license.

The license keys are generated using the unique serial number associated with your management platform and can be obtained from your Vertiv representative or reseller. To generate the license keys, your Vertiv representative or reseller must have the management platform's serial number and a copy of your Purchase Order, which will contain the number of target devices requiring registration and the desired duration of the licenses. You may be asked to provide this information.

NOTE: The number of target devices permitted for a single management platform ranges from 50-5,000.

After receiving the license keys, you must upload them to the Avocent MP1000 Management Platform web UI. Proceed to the next section for instructions on locating the serial number for your appliance type.

2.1 Serial Number Location

2.1.1 Hardware appliance

For license key generation, you may be asked to supply your Vertiv representative or reseller with the serial number associated with your Avocent MP1000 Management Platform. Please refer to the following procedure for instructions on accessing the serial number. Then, supply your Vertiv representative or reseller with the serial number to obtain your license keys.

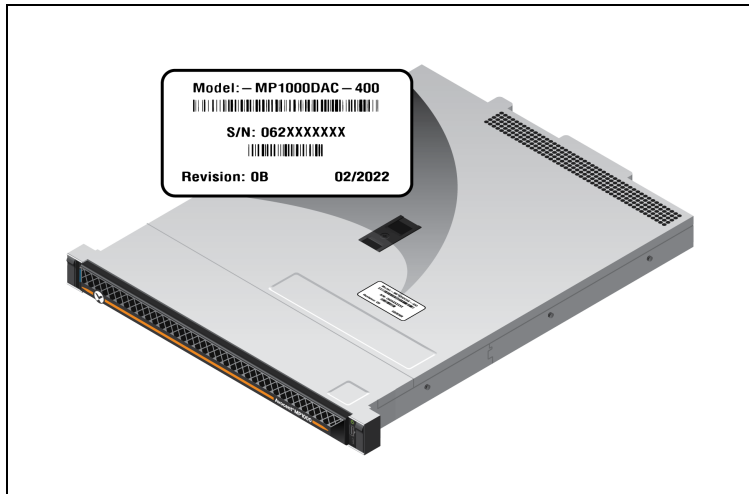NOTE: The email containing your license key information should be retained for future reference.

To locate the serial number:

1. Check the side of the packaging box in which the management platform was shipped.
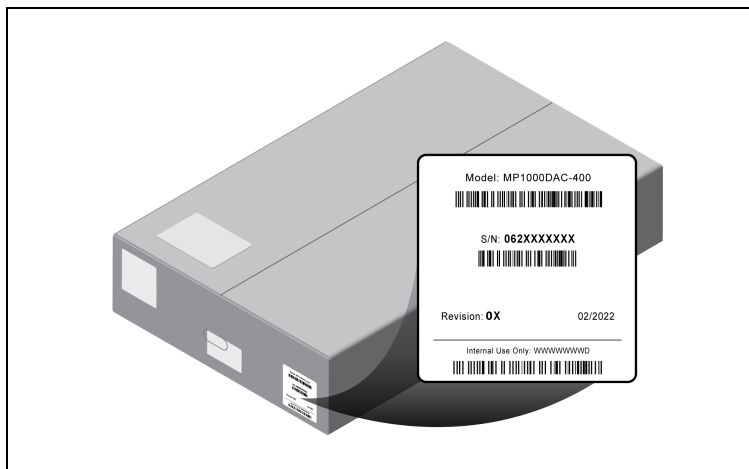
-or-

Check the top of the physical unit.

-or-

Check the extended warranty for the management platform.

2. Contact your Vertiv representative or reseller to supply them with your serial number and obtain the license keys. Then, refer to License Upload on page 8 to upload the licenses to the web UI.

2.1.2 Virtual appliance

For license key generation, ensure the VA is deployed on one of the supported virtualization platforms and assigned an IP address to access the management platform's serial number. The serial number for the VA can be found within the Vertiv™ Avocent® MP1000VA Management Platform Virtual Appliance Command Line Interface (CLI). The CLI may be accessed via SSH or the VM console. Please refer to the following procedures for instructions on accessing the serial number. Then, supply your Vertiv representative or reseller with the serial number to obtain your license keys.

NOTE: The email containing your license key generation information should be retained for future reference.

NOTE: The following procedures contain figures referencing VMware in the Serial Number information line. However, if you are using a different virtualization platform, the serial number may appear differently.

To access the serial number via SSH:

1. Open a terminal window on your computer and enter **ssh** <username>**@**<appliance ip>. Press **Enter**.
2. When the Avocent MP1000 Management Platform login screen appears, enter **admin** as the username and enter the password you created when you first accessed the VA.

3. When the CLI opens, the serial number appears in the Serial Number information line.

Figure 2.1 Serial Number Information Line

4. Contact your Vertiv representative or reseller to supply them with your serial number and obtain your license keys. After obtaining the license keys, proceed to the next section to upload them to the web UI.

-or-

To access the serial number via the VM console:

1. In the virtualization platform's client, select the Console icon to open the CLI.

2. When the Avocent MP1000 Management Platform login screen appears, enter **admin** as the username and enter the password you created when you first accessed the VA.

3. When the CLI opens, the serial number appears in the Serial Number information line.

Figure 2.2   Serial Number Information Line

4. Contact your Vertiv representative or reseller to supply them with your serial number and obtain the license keys. Then, refer to the next section to upload the licenses to the web UI.

2.2 License Upload

To upload the license keys:

NOTE: For the hardware appliance, you must upload the Base License first.

1. From the Vertiv™ Avocent® MP1000 Software Downloads page, download the latest firmware version of the Avocent MP1000 Management Platform.

Proprietary and Confidential ©2024 Vertiv Group Corp. 2 System Licensing

2. Log into the Avocent MP1000 Management Platform web UI with administrator privileges. Enter **admin** as the username and the password you created when you first logged in.

Figure 2.3 Login Screen
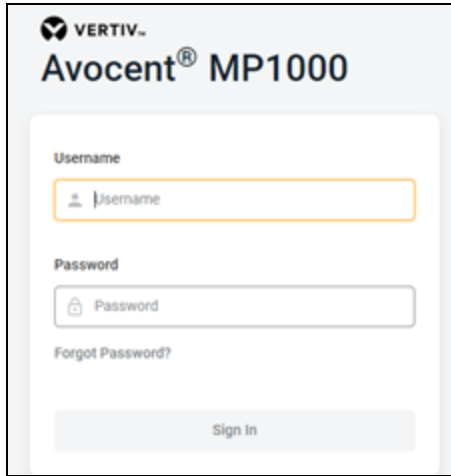
3. In the left-hand sidebar, select *Administration - License*.

Figure 2.4 Administration Options
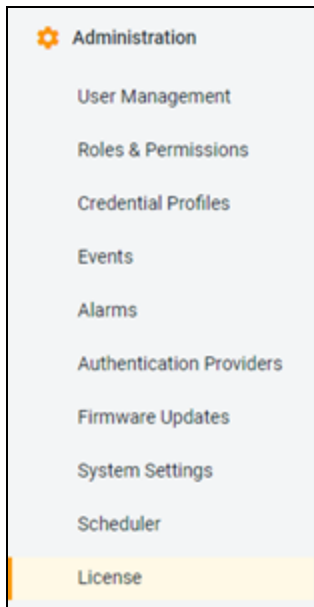
4. Click *Add License*.

Figure 2.5 Add License
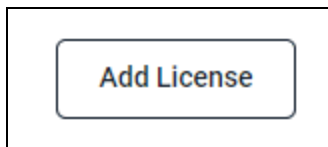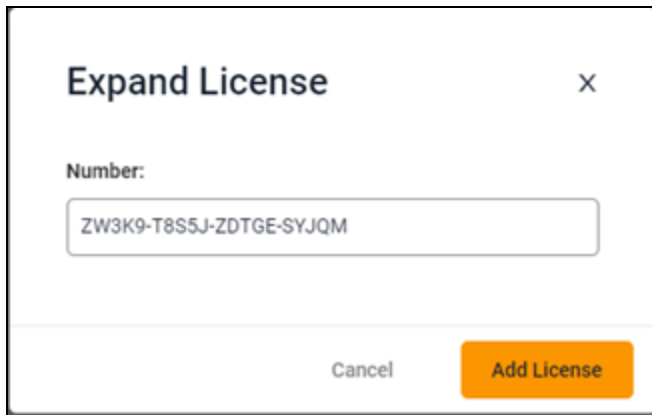
5. In the Number field, enter the Base License for the hardware appliance.

-or-

Enter the Virtual Appliance License Key for the virtual appliance. At this point, all licensing requirements have been met for the virtual appliance.

6. After the Base License key is added for the hardware appliance, the Add License button changes to an Expand License button. The Targets license must now be uploaded for the hardware appliance. The High Availability license can also be added at this point, if desired. Select the *Expand License* button.

7. In the Number field, enter the appropriate license key and select *Add License*. When finished, the uploaded licenses appear on the screen.

Figure 2.6   Targets or High Availability License Key

2.3 License Expiration

By default, an expiration notification for licenses appears 120 days prior to the expiration date. If you wish to change this time frame, see the following procedure.

To configure the license expiration notification:

1. Go to the *Administration - System Settings - License Expiration Notification* screen.

Figure 2.7   License Overview
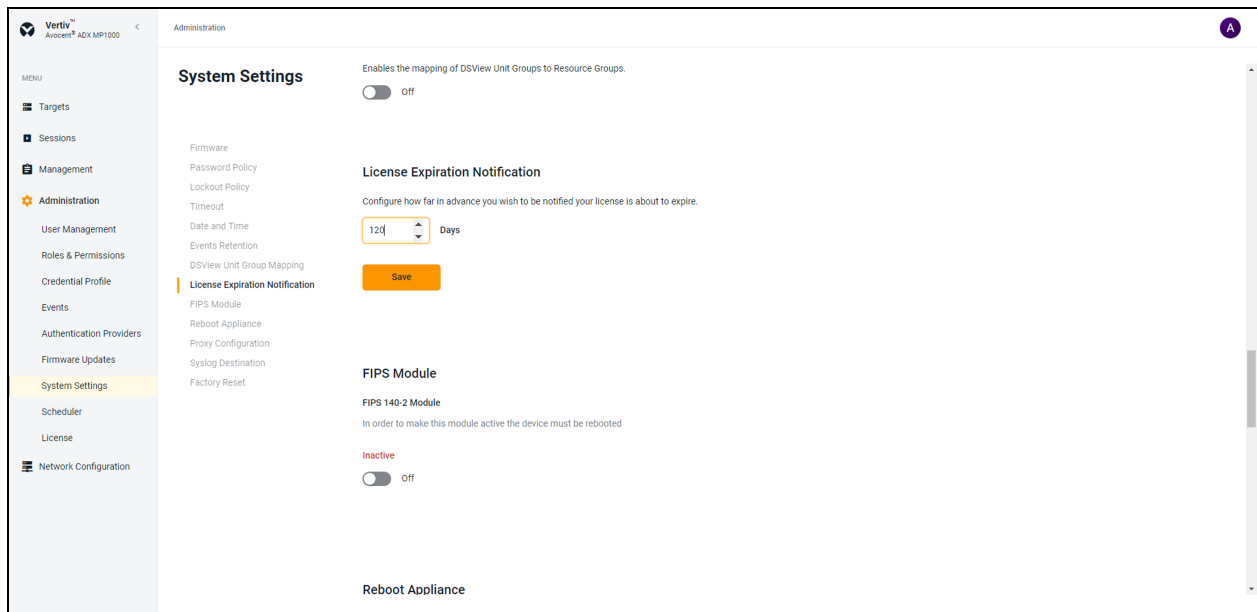
2. In the Days field, enter the number of days you want to be notified in advance about the license expiry.
3. Click *Save*.

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.

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

Proprietary and Confidential ©2024 Vertiv Group Corp.

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 Targets List 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.

User Profile

Configure the profile name, password and email address.

Localization

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

Color Theme

Select the radio button for your desired color theme.

Help

This option redirects you to the Online Help provided for the Avocent MP1000 Management Platform.

Log Out

This option immediately logs you out of the web UI.

4.2 Dashboard

4.2.1 Edge Management

The Edge Management dashboard is a single platform on 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). The Dashboard - Edge Management screen displays the views for the Organizations, Device Locator and Alarms. The following capabilities are supported by the Edge Management screen:

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

Figure 4.2   Dashboard - Edge Management

To navigate through the Edge Management screen:

From the left-hand sidebar, click *Dashboard - Edge Management*. On the Edge Management 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, see Organizations on page 24

- **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 ellipses to clear the alarm. For more information, see Alarms on page 56

4.3 Targets

The following target device types can be managed by the Avocent MP1000 Management Platform:

- Vertiv™ Avocent® RM1048P Rack Managers
- Vertiv™ Uninterruptible Power Supplies (UPSes)
- Vertiv™ Power Distribution Units (PDUs)
- Service Processors (SPs)
- IP KVM devices, such as the Vertiv™ Avocent® IPIQ IP KVM device and the Vertiv™ Avocent® IPUHD 4K IP KVM device
- Vertiv™ Avocent® ACS 800/8000 advanced console system
- Serial devices, such as the Vertiv™ Avocent® IPSL IP serial device
- Vertiv™ Avocent® DSView™ management software
- Virtual Machines (VMs)

These target device types are described further in the remainder of this section.

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
- SPs
- 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.

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

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

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

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

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.

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.

The Appliance View screen displays a list of targets sorted by port number by default. From this screen, you can configure, merge and manage targets, as well as launch target sessions.

Figure 4.3   Appliance View
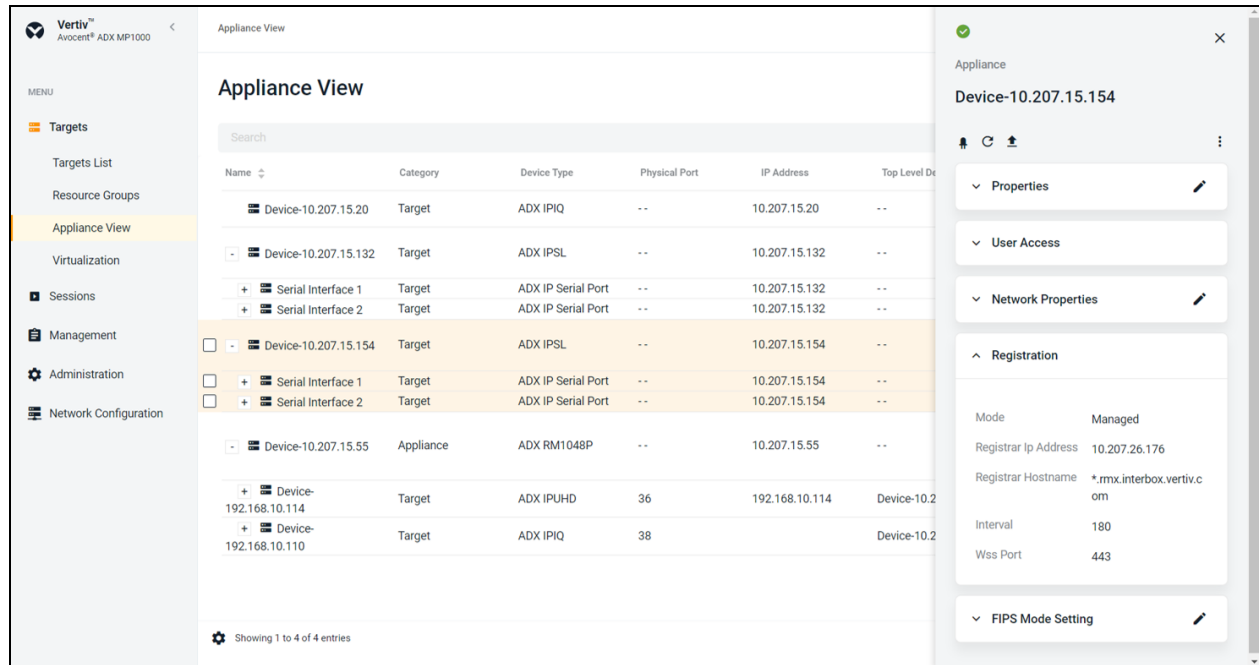
To navigate through the Appliance View screen:

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

- Click the plus icon (+) next to each device name to view the list of appliances physically connected to the rack manager.
- Click the desired device to open its sidebar. This sidebar may include drop-down menus for Properties, User Access, Settings and more. Click the appropriate menu to expand it and view the information.

Configure targets

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

NOTE: Some devices require a credential profile in order to be added to the management platform. See Credential Profiles on page 55 to create a credential profile.

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. This does not apply if you are adding an SP independently.

To add a single device or a range of devices:

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

   -or-

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

   -or-

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

5. Use the Device Type drop-down menu to select the device type.

6. Based on your selection, fill out the appropriate fields.

NOTE: Credential profiles are required for the following device types: 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.

7. 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 Targets - Appliance View screen or the Targets - Targets List screen.

To delete a target device:

1. From the *Targets - Appliance View* screen, click on the vertical ellipses next to the individual device you want to delete. The following options appear: Delete, Resynchronization and Firmware Update.

2. Click the *Delete* icon. It may take several minutes for the device to fully delete.

To view target properties and network configuration:

1. From the *Targets - Appliance View* screen, click a target to open its sidebar.

2. Click the Edit icon (pencil) to configure the target's properties.

To activate the Maintenance Mode:

1. From the *Targets - Appliance View* screen, click on the device to open its sidebar.

   -or-

   Hover the mouse over the row of the desired device and click on the vertical ellipse.

2. Click on the Maintenance Mode icon.

   -or-

   Use the slider to activate the Maintenance Mode.

3. A dialogue box appears. Click *Continue*.

Merge targets

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

NOTE: You cannot merge VMs.

To merge targets:

1. From the *Targets - Appliance View* screen, select the targets you want to merge by hovering your mouse over each target and clicking the box to the left of each one.

2. Click *Merge Targets*, then click *Merge*. A plus (+) icon displays to show the merged targets. Click the icon to expand the merged target and show each individual target.

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

To unmerge targets:

1. From the *Targets - Appliance View* screen, click the checkbox next to the merged target.

2. Click the *Unmerge* icon to unmerge all the targets.

-or-

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

Manage targets

Vertiv™ UPSes

To manage and control a Vertiv™ UPS:

1. Hover the mouse over the desired Vertiv™ UPS device and click on the vertical ellipses. The following functions appear:
   - Open Web Page
   - In Maintenance Mode
   - Clear Alarm
   - Delete
   - Resync
   - Power On All Outlets
   - Power Off All Outlets
   - Power Cycle All Outlets
2. Click on the appropriate option to manage and control the device.

To configure the properties for a Vertiv™ UPS:

1. Click on the desired UPS to open its sidebar. The sidebar displays the following tabs: Properties, Outlets, Sensor's data, User Access, and Credential Profiles and a global icon to navigate to the Vertiv™ UPS web UI.
2. Click the Edit icon (pencil) to edit the Device Name field.
3. Use the Credential Profiles drop-down menu to add a credential profile.

   -or-

   Click on Edit icon (pencil) to add a credential profile.

Vertiv™ PDUs

To manage and control a Vertiv™ PDU:

1. Hover the mouse over the desired Vertiv™ PDU and click on the vertical ellipses. The following functions appear:
   - Open Web Page
   - In Maintenance Mode
   - Clear Alarm
   - Delete
   - Resync
   - Firmware Update
   - Power On All Outlets
   - Power Off All Outlets
   - Power Cycle All Outlets
2. Click on the appropriate option to manage and control the device.

To configure the properties for a Vertiv™ PDU:

1. Click on the desired PDU to open its sidebar. The sidebar displays the following tabs: Properties, Outlets, Sensors, PDU Info, User Access and Credential Profiles.
2. Click the Edit icon (pencil) to edit the Device Name field.
3. Use the Credential Profiles drop-down menu to add a credential profile.

   -or-

   Click on Edit icon (pencil) to add a credential profile.

Launch 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 possesses the following capabilities and value:

Capabilities

- View multiple previews in one screen
- Drag and drop

Value

- Reduce time to provision systems remotely
- Remain aware of system health through a NoC
- Improve the productivity of test teams
- Increase efficiency through single dashboard for remote IT management

To launch a dashboard:

1. From the left-hand sidebar, click *Targets - Appliance View*.

   -or-

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

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 (the 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

The Organizations screen shows a list of organizations and ungrouped devices. The following capabilities are provided:

- Device organization by location

- Automatic alarm aggregation

- Display of global alarm counts and source alarms

- Alarm summary

- Ability to navigate to the alarm

Figure 4.4 Organization Screen
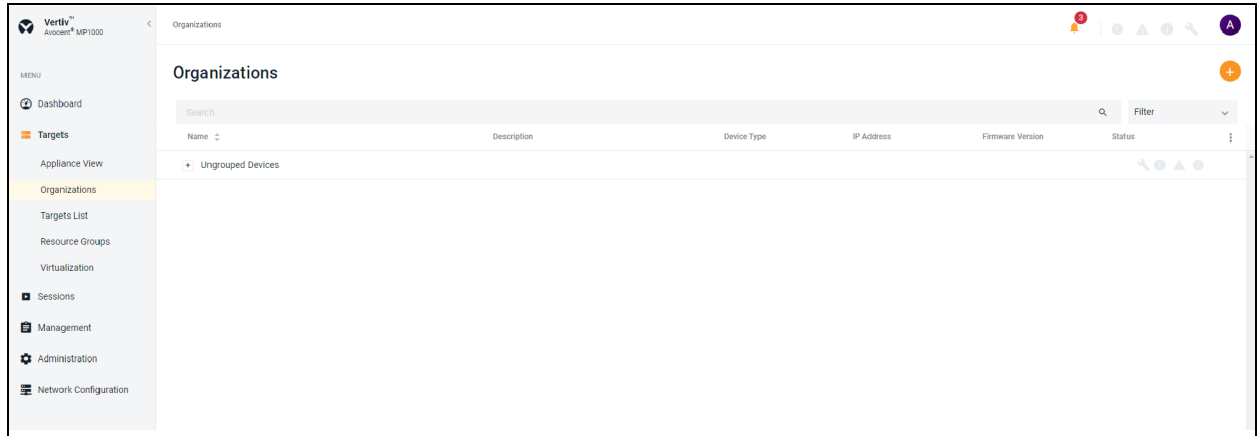
To navigate through the Organizations screen:

From the left-hand sidebar, click *Targets - Organizations*. On this screen, you can access the following features:

- Status: The Status column displays the status for Maintenance Mode, alarm aggregation and device alarm severities.

- Device List: Click the plus icon (+) to the left to the individual organization to locate the devices and their associated alarms.

To create a new organization:

1. From the top of the *Targets - Organizations* screen, click the Add icon (+). An Organization Editor dialogue box appears.

2. On the right side of the Organization Editor, click the Add icon (+) . An Add Organization dialogue box appears.

Figure 4.5   Adding Organization
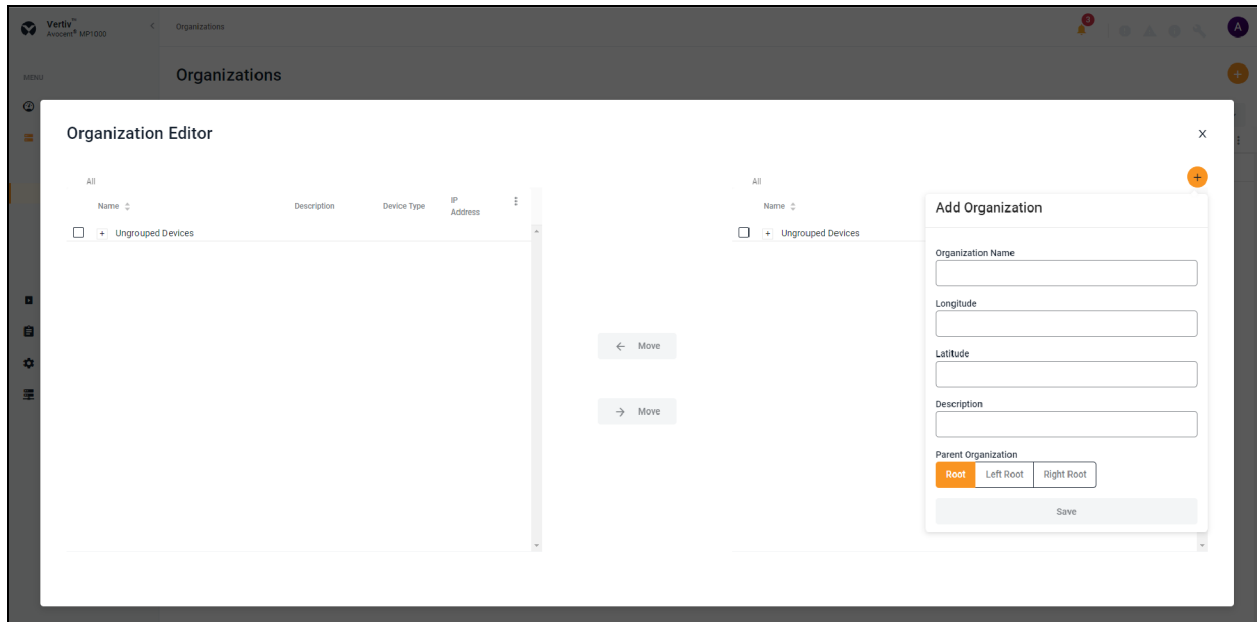
3.   Enter the required details to add the organization.

4.   Click *Save*.

To edit an existing organization:

1.   Click on the organization or device you want to edit to open its sidebar.

2.   Expand *Properties* and click the Edit icon (pencil) to change the following details:

- Organization Name

- Longitude

- Latitude

- Description

3.   Click *Save*.

To move an organization using the Organization Editor:

1.   Click on the check box to the left side of the organization which you want to move.

2.   Click the *Move* button to shift the organization from left to right or vice versa.

Figure 4.6   Organization Editor
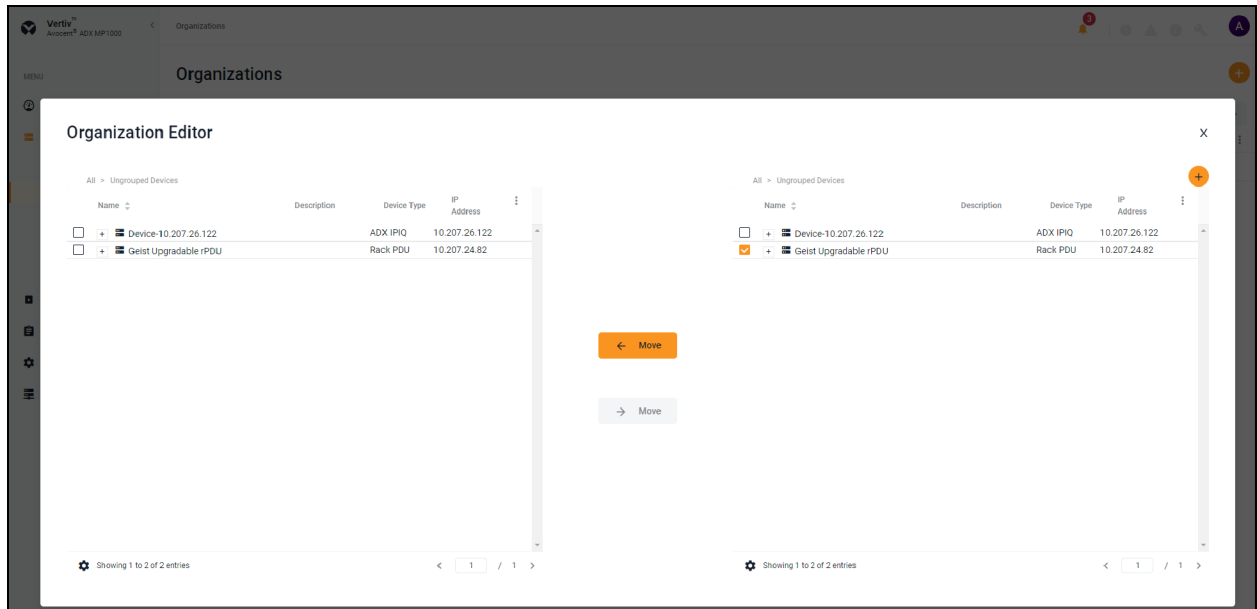
To delete an organization using the Organization Editor:

1. Hover the mouse over the row with the organization you want to delete and click on the vertical ellipses.
2. Click *Delete*.
3. At the confirmation screen, click *Delete*.

4.3.3 Targets List

The Targets List screen displays the list of targets connected to the Avocent MP1000 Management Platform. Unlike the Appliance View screen, the targets are not organized by the appliance to which they are associated. From here, you can perform the same functions that are available from the Appliance View screen.

4.3.4 Resource Groups

The Resource Groups screen allows you to 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:

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: You can delete multiple groups simultaneously by checking the boxes next to the group name, then clicking the Delete icon (trash can).

4.3.5 Virtualization

The Targets - Virtualization screen displays only the list of Virtual Machine Managers and Hypervisors that are being managed by the management platform. From this screen, you can add Virtual Machines (VMs).

NOTE: VMs can also be added from the Targets - Appliance View and Targets - List screens.

To add a VM as a target device:

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

4.3.6 Discoveries

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

Figure 4.7 Discoveries Page
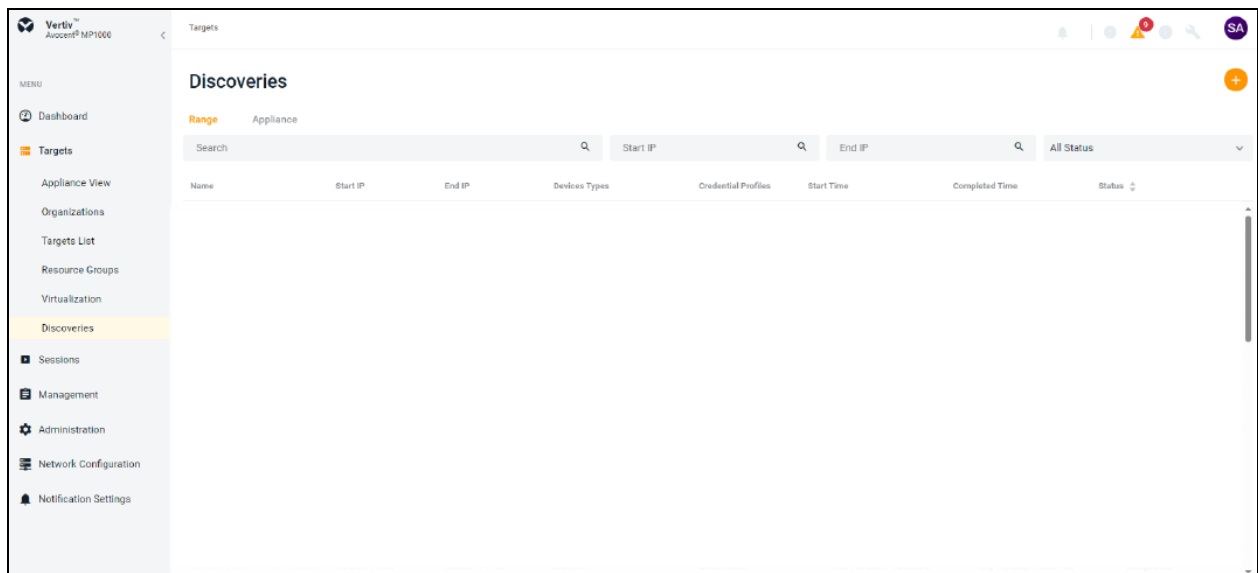
To navigate through the Discoveries screen:

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

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

To discover a device:

NOTE: A credential profile is required for the device to be discovered. To create a credential profile, refer to Credential Profiles on page 55 .

1. From the *Targets - Discoveries* page, click the Add icon (+) in the top right corner. The Add Device dialogue box opens.

Figure 4.8 Add Device

2. Click the Single IP radio button to discover a single IP address.

-or-

Click the Range IP radio button to discover a range of IP addresses.

3. Enter the discovery name and IP address.

4. Select the appropriate device type from the Device Type drop-down menu.

5. Select the credential profile you created for the device from the Credential Profile drop-down menu.

6. Enter the port number.

7. Click *Discover*. Once discovered, the device appears on the Appliance View page.

4.4 Sessions

4.4.1 Sessions List

The Avocent MP1000 Management Platform allows you to launch multiple sessions simultaneously to access your target devices via the management platform web UI. The Sessions List screen displays a log of the active and closed sessions that have been launched from your management platform appliance.

To navigate through the Sessions List screen:

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

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

4.4.2 KVM sessions

The Avocent MP1000 Management Platform conducts KVM sessions using HTML5 Video Viewer with one or more target devices attached to one or more KVM switches. When a target device connects to the 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.

Supported browsers

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

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

Launch KVM sessions

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

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

To launch a KVM session:

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

-or-

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

To close a KVM session:

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

Exclusive Mode

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

To enable an exclusive KVM session:

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

Viewer Reconnect

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 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.

HTML5 Video Viewer

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

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

Table 4.2   KVM Viewer Feature Compatibility

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

Table 4.3   Feature Comparison for Vertiv™ Avocent® IPUHD 4K IP KVM Device and Vertiv™ Avocent® IPIQ IP KVM Device Viewer

Feature	Stand-Alone Vertiv™ Avocent® IPUHD 4K IP KVM device	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 (View -> Audio and Video Options) Tools -> Remote Audio)	✓	✓	✗
Max Resolution Settings (View -> Max Resolution)	✓	✓	✗
User Information (View -> User Information)	✓	✗	✗
Instant Message (Tools -> Instant Message)	✓	✗	✗
Optimize Network Bandwidth (Tools -> Optimize Network Bandwidth)	✓	✓	✗

HTML5 Video Viewer menu

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

File

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

View

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

Video Options

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

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

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

Scaling

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

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

Max Resolution

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

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

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

Macros

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

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

To send a command to the target server:

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

Tools

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

Virtual Media

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

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

NOTE: VMs do not have the Virtual Media feature.

Prerequisites

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

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

To map a Virtual Media drive:

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

   -or-

   Select *Map Removable Disk Image* to map a .img file.

3. If you wish to reset the USB connection, select *Virtual Media - Reset USB*.
4. Read the instructions, then click *OK*.
5. Select a file from the Open dialog box with the proper file extension (.iso or .img), then click *Open*.
6. If you wish to limit the mapped drive to read-only access, check the Read Only box in the Virtual Disk Management dialogue box.

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

7. Click *Map Drive*, then click *Close*. Mapping is now complete, and the drive can be used on the target device.

To unmap a Virtual Media drive:

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

   -or-

   Click *Deactivate* to unmap all the drives.

2. At the prompt, click *Yes*.

Session sharing

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

- **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.

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.

To launch a serial session:

1. From the *Targets - Appliance View* screen, hover the mouse over the desired serial device.
2. On the right of the column, click the Launch Console icon.

    -or-

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

To end a serial session:

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

4.4.4 Web UI sessions

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

To launch the web UI session:

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

Figure 4.9 Launching Web UI Session

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

Figure 4.10   Webpage of the Device (iDRAC) Overview

4.5 Management

4.5.1 Devices

The Devices tab displays the 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:

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

4.5.2 High Availability

The High Availability tab allows you to configure up to three nodes for server redundancy. Through the High Availability (HA) feature, the management platform reduces 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.

NOTE: All nodes within a cluster must be the same appliance type. If using a management platform hardware appliance, then all nodes must also be hardware appliances. If using a management platform virtual appliance, then all nodes must also be virtual appliances.

To navigate through the High Availability tab:

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

- Create and configure a cluster with one primary and up to two standby nodes.
- View the name, IP address, role, firmware version, status and health of the cluster and each individual node.
- Click on a node entry to view its side panel for information about the properties and node status.
- Configure the server mode.

Prerequisites

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

- Must use the latest firmware version. To upgrade to the latest firmware, refer to Firmware on page 59 .
- Must be configured with a static IP address. To configure a static IP address, refer to Ethernet Interfaces on page 67 .

NOTE: If the node is configured with DHCP, it may receive a different IP address when restarted and become unavailable to the cluster.

- Must have the Network Time Protocol (NTP) enabled on the same NTP server to ensure the time settings are consistent for all nodes. If time settings are not synchronized, the Vertiv™ Avocent® RM1048P Rack Managers enrolled on the management platform may not transition properly during failover.
- Must be licensed for High Availability. The HA feature cannot be accessed nor configured until the license has been uploaded. Please see System Licensing on page 5 for instructions on how to obtain and upload the license.

NOTE: At minimum, the primary node must be licensed for HA. If the standby node(s) does not have an HA license, it acquires the primary node's license automatically when it is promoted.

- Must have the High Availability Policy setting enabled to allow a standby node to be added to the cluster. From the left-hand sidebar, click *System Settings - High Availability*, then use the slider to enable the setting. Click *Save*.

Server Redundancy Configuration

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.
- 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 web UI of the management platform you wish to act as the primary node. When a cluster is created, the management platform you are currently logged into becomes the primary automatically. Any nodes added afterward become standby nodes, reserved for system failover. If the 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 create a cluster:

1. From the left-hand sidebar, click *Management - High Availability*. The High Availability page opens, as shown below.

Figure 4.11   High Availability Screen
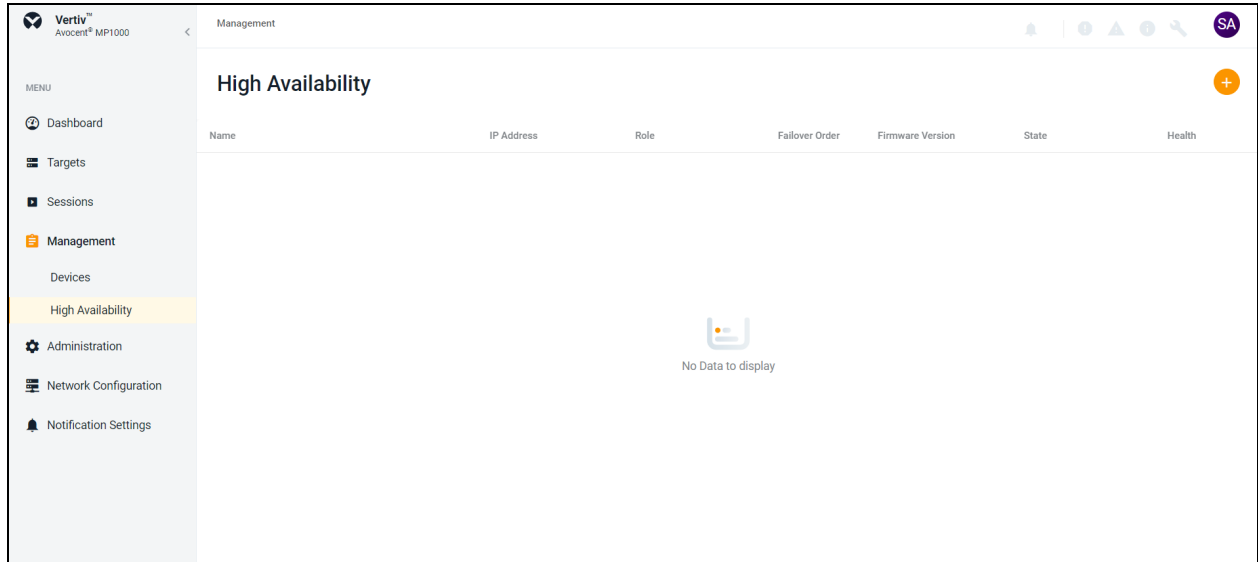
2. Click the plus (+) icon in the top right corner, then click the *Create Cluster* button.
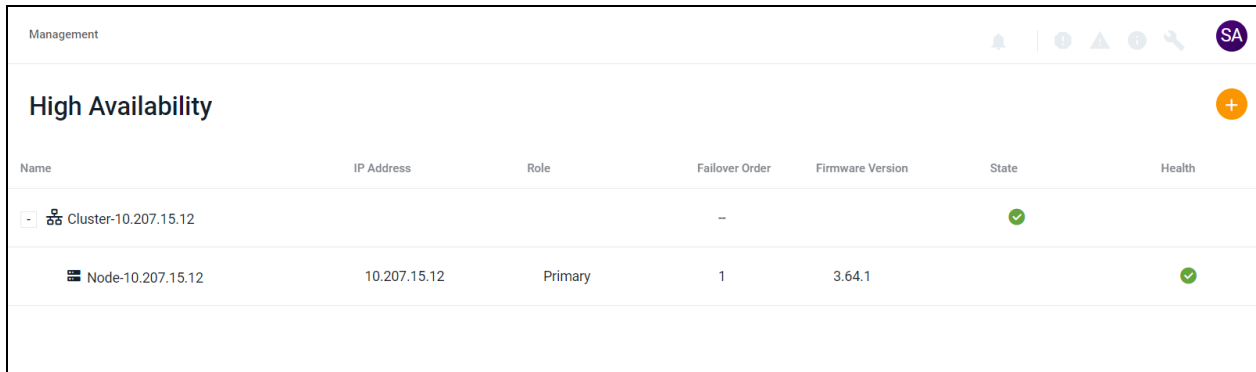
Figure 4.12   Create Cluster
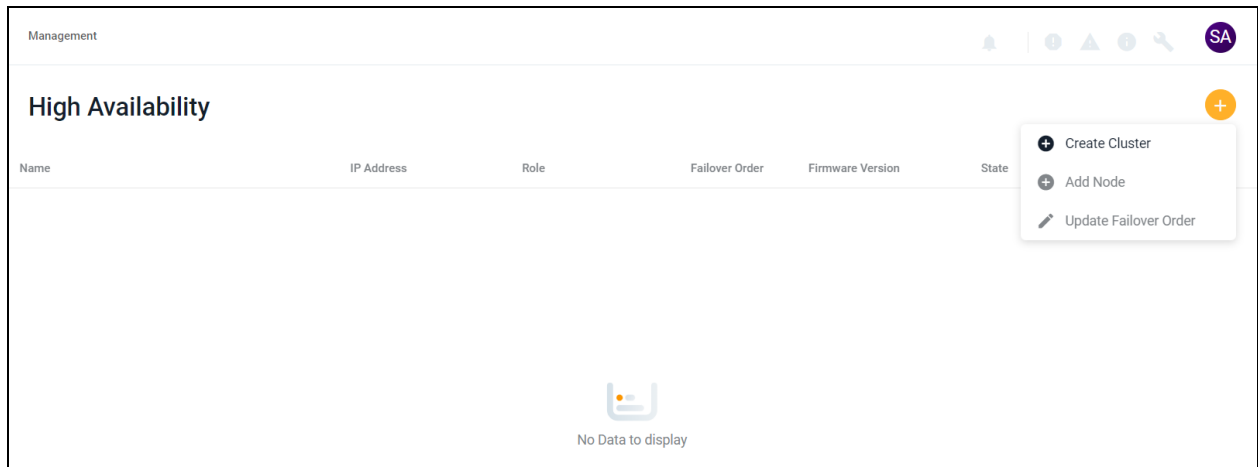
3. A Create Cluster dialog box appears. Click the Continue box.

4. The cluster appears on the High Availability screen with a green checkmark status indicating that the cluster is healthy.

Figure 4.13   Cluster Created

To add a node to the cluster:

1. After creating a cluster with a primary node, at least one standby node should be added. From the *Management - High Availability* tab, click the plus (+) icon in the top right corner, then click *Add Node*.

Figure 4.14   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.**

Figure 4.15   Add Node Warning Message
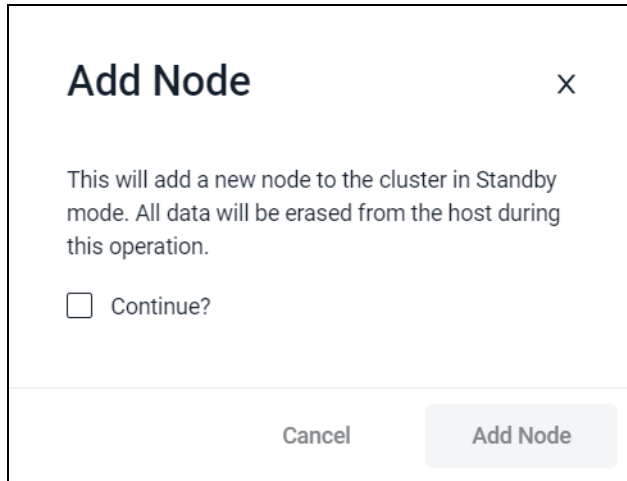
2.   Check the Continue box, then click *Add Node*.

3.   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 4.16   Add Node Data

4. The primary node's data begins replicating to share and synchronize with the standby node. When the nodes' Health icon turns 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 4.17   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		✓

To access the 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.

To configure the failover order:

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

To promote/demote a node:

From the *Management - High Availability* screen, 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.

To remove a standby node from the cluster:

NOTE: 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.

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

To delete a cluster:

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

High Availability Troubleshooting

If a node is malfunctioning and not fulfilling normal functions, such as mode transition requests, please 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 4.18   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 4.19   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 4.20   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 4.21   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> |
```

NOTE: 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

From the Administration tab, you can customize the functions of the management platform to better suit your needs. This section provides descriptions and instructions for configuring the settings under this tab.

4.6.1 User Management

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

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

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

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

Users

From the left-hand sidebar, click the *Administration - User Management - Users* tab to view all users for the Avocent MP1000 Management Platform.

To view more options in the Users tab:

Click a user to open its sidebar. From here, you can perform the following functions:

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

To configure a user's password expiration time:

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

To create a new user:

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

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

3. Click *Add User*.

To delete a user:

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

User groups

A user group defines the view and what the user can do within the web UI and CLI, regarding appliance settings and administration. From the left-hand sidebar, click the *Administration - User Management - Groups* tab to view all groups for the Avocent MP1000 Management Platform.

To view more options in the Groups tab:

Click a group to open its properties sidebar. From here, you can perform the following functions:

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

To create a new group:

1. Click the Add icon (+). An Add New Group dialogue box appears.

2. Enter the group name and check the boxes for each user you want to add to the group.

3. Click *Add Group.*

To assign a user group to a resource group:

1. Click on the desired user group to open its side panel.

2. Click *Group Properties* to expand the menu, then click the Edit (pencil) icon.

3. Under the System Roles section, check the box(es) for the system role you wish to assign. If you wish to create a new system role rather than use a pre-configured one, please see Roles & Permissions on the next page

4. Click *Save Changes.*

5. After adding the system role to the user group, you must define the resource group. See Resource Groups on page 27 for instructions on creating a resource group.

6. From the *Administration - User Management - Groups* tab, click on the desired user group to open its side panel.

7. Click *Resource Groups* to expand its menu, then click the Edit (pencil) icon.

8. Check the box for the appropriate resource group and click *Save Changes.*

9. 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, please see Roles & Permissions on the next page

10. Once the changes have been saved, hover the mouse over the resource group to select the Edit Roles icon.

11. 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 group:

1. Hover the mouse over the desired target and check the box of the left.

2. Click the Delete icon (trash can) above the list of groups.

3. At the confirmation screen, click *Yes* to delete.

Group mapping

Multiple users on the same network can be added to the management platform by mapping the Active Directory (external) group to the local user group. For group mapping, the authentication provider for the external group must first be added to the web UI. To add an authentication provider, see the procedure in Authentication Providers on page 57

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

To perform group mapping:

1. From the *Administration - User Management - Groups* screen, click on the desired local user group. The side panel appears.

2. Click *External Groups* to expand the menu.

3. Select the desired external group from the list.

4. Click *Assign to External Group.*

5. Click *Save Changes.*

4.6.2 Roles & Permissions

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

System Roles

A system role is a collection of user permissions that can be applied to a system. These roles can be configured and applied to a user group to permit specific system operations. For example, a system administrator with a system role that includes the permission to change the user password is allowed to change user passwords from the web 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 groups on page 48

User groups can be configured with one or more system roles. The system role permissions assigned to a user group are available for any user within the user group. For more information on user group configurations, please see User groups on page 48

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 27 .

 Table 4.4   on the facing page describes the user permissions allowed for each system and target role. A checkmark indicates the permission listed in the left-hand column is allowed for the role. An "x" indicates the permission is not allowed.

Table 4.4   Roles and Permissions

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

Table 4.4   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 User Policy	✓	✗	✓	✗	✗	✗
Change User Password	✓	✓	✓	✓	✗	✗
Configure Devices	✓	✓	✗	✗	✗	✓
View Devices	✓	✓	✓	✓	✓	✓
Upgrade Firmware	✓	✓	✗	✗	✗	✓
Configure KVM Session	✓	✗	✗	✗	✗	✗
Establish KVM Session	✓	✓	✓	✓	✓	✓
Establish VKVM Session	✓	✓	✗	✓	✓	✓
Establish Exclusive Session	✓	✗	✗	✗	✗	✗
Establish Stealth Session	✓	✗	✗	✗	✗	✗
Configure Serial Session	✓	✗	✗	✗	✗	✗
Establish Serial Session	✓	✓	✓	✓	✓	✓
Establish SSH Session	✓	✓	✓	✓	✓	✓
Establish Viewer Session To VM	✓	✓	✗	✓	✓	✓
Establish VNC Session	✓	✓	✗	✓	✓	✓
Launch standalone passive session	✓	✓	✓	✓	✓	✓
Terminate active standalone passive sessions	✓	✓	✓	✓	✓	✓
View Target Sessions	✓	✓	✗	✗	✗	✓
Terminate Target Session	✓	✗	✗	✗	✗	✗
Establish Virtual Media Session	✓	✓	✓	✓	✓	✓
KVM Clipboard paste	✓	✓	✗	✗	✗	✓
KVM Paste text from file	✓	✓	✗	✗	✗	✓
KVM Screen capture	✓	✓	✗	✗	✗	✓
KVM Screen recording	✓	✓	✗	✗	✗	✓
KVM Remote Audio	✓	✓	✗	✗	✗	✓

Table 4.4   Roles and Permissions (continued)

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

Table 4.4   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
Reboot Server	✓	✗	✗	✗	✗	✗
Shutdown Server	✓	✗	✗	✗	✗	✗
Power Control	✓	✓	✗	✗	✗	✓
Reset Control	✓	✓	✗	✗	✗	✓
Boot order Control	✓	✓	✗	✗	✗	✓
Restart Control	✓	✓	✗	✗	✗	✓
Led Control	✓	✓	✗	✗	✗	✓
Configure Scheduled Jobs	✓	✓	✗	✗	✗	✗
View Scheduled Jobs	✓	✓	✗	✗	✗	✗
Configure Nodes for High Availability	✓	✓	✓	✗	✗	✗
View Nodes for High Availability	✓	✓	✓	✗	✗	✗
Configure Notification Settings	✓	✓	✗	✗	✗	✗
View Notification Settings	✓	✓	✗	✗	✗	✗

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

To add a new role:

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

   -or-

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

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

   -or-

   Check the Select All box to add all permissions.

5. Click *Add Role*.

To configure an existing role:

NOTE: The default roles cannot be configured.

1. From the *Administration - Roles & Permissions* screen, click a role to open its sidebar.

2. Expand *Properties* and click the Edit icon (pencil) to configure the description for the role.

3. Expand *Permissions* and click the Edit icon (pencil) to configure the permissions for the role.

4. Click *Save*.

To view role properties and permissions:

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

To delete a role:

NOTE: The default roles cannot be deleted.

1. From the *Administration - Roles & Permissions* screen, hover the mouse over the desired target and check the box to the left.

2. Click the Delete icon (trash can).

3. At the confirmation screen, click *Yes* to delete.

4.6.3 Credential Profiles

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

The Credential Profiles screen displays the credential profiles of your target devices. A credential profile stores the user ID and password for a single user and can be used across different target device types. Credential profiles are required for the following device types: Service Processors, 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.

NOTE: Before enrolling a rack manager with an SP, you must define the credential profile for each one with unique credentials.

To create a credential profile:

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

2. Enter a profile name and type, username and port.

3. Enter the password, then confirm the password.

4. (Optional) Add a note.

5. Click *Add credential profile.*

Management software zone support

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 *Administration - Credential Profiles* screen, click the Add icon (+) in the top right corner. An Add credential profile dialogue box appears.

Figure 4.22   Add Credential Profile: Username/Password Profile Type

2. Enter a profile name.

3. Select *Username/Password* from the Profile Type drop-down menu.

4. Enter the username and password, then confirm the password.

5. Enter the port number.

6. 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.

7. (Optional) Add a note.

8. 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 28 .

4.6.4 Events

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

To view more options in the Events screen:

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

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

-   Use the Filters drop-down menu to filter events by severity (*All Severities, Info, Warning* or *Critical*).

-   Use the arrows next to each column to sort each event.

-   Click on an event to open its sidebar and view the properties.

4.6.5 Alarms

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

Figure 4.23   Alarms Overview

To view more options in the Alarms screen:

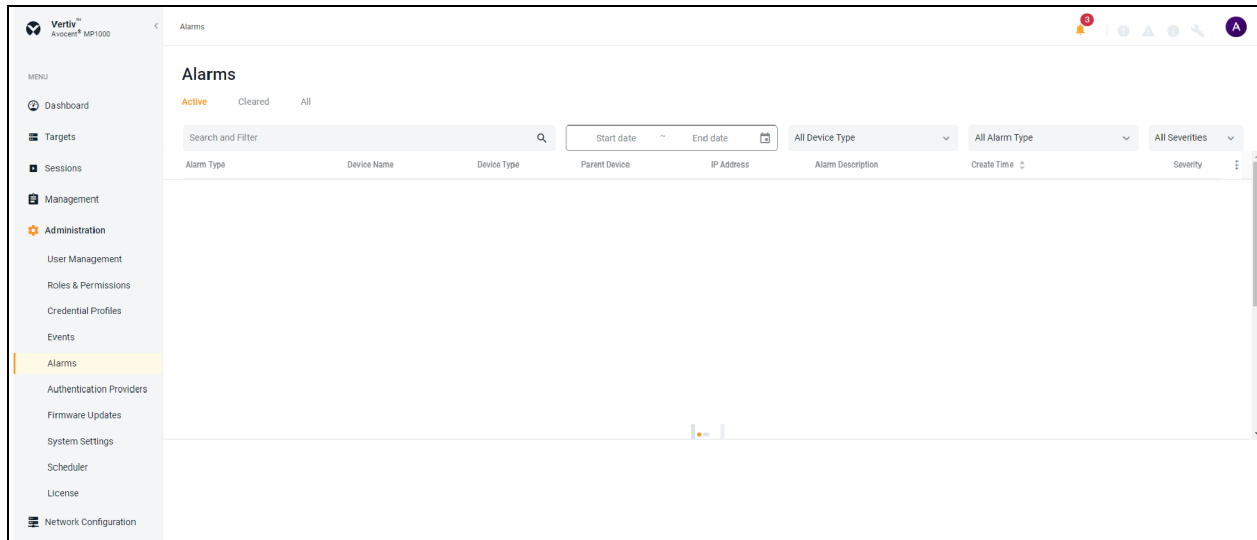From the left-hand sidebar, click *Administration - Alarms.* On this screen, you can perform the following functions:

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

To clear the alarms manually:

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

   -or-

   Click the vertical ellipses to the right of the individual alarm.

2. Click the *Clear Alarms* icon. A Clear Alarm dialogue box appears.

3. Click *Continue*.

4.6.6 Authentication Providers

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

Providers can be authenticated locally or via AD/LDAP, TACACS+ or RADIUS. For the LDAP method, the Avocent MP1000 Management Platform supports remote group authorizations.

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.

To add an authentication provider:

1. From the *Administration - Authentication Providers* screen, click the Add icon (*+*) in the top right corner.

2. Use the drop-down menu to select *AD/LDAP, TACACS+* or *RADIUS* as the authentication type. A dialogue box appears for the chosen authentication type.

3. Enter the required configuration information for your authentication server.

NOTE: The following figure references the Add TACACS+ Provider dialogue box. If you choose a different provider, the dialogue box will contain different information.

Figure 4.24   Add TACACS+ Provider

4. When finished, click *Add Provider*.

To enable an authentication provider:

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

2. Click *Enable*.

To delete an authentication provider:

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

2. Click the Delete icon.

3. At confirmation screen, click *Yes* to delete.

To update the providers order:

1. From the *Administration - Authentication Providers* screen, click the Add icon (+) in the top right corner.

2. Select *Update providers order* in the drop-down menu.

3. Use the right-hand drag icon to rearrange the providers as desired.

4. When finished, click *Update Order*.

Active directory

You can enable role-based security on the Avocent MP1000 Management Platform to map your Active Directory remote group to a role on the Avocent MP1000 Management Platform.

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

To enable role mapping:

1. From the LDAP screen, use the slider under Active Directory Settings to enable role-based security.

2. Click the Add icon (+).

3. Enter the name of your Active Directory remote group in the appropriate field.

4. Use the drop-down menu to select the local role the remote group will be mapped with.

5. Click *Apply*.

To delete a role mapping:

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

4.6.7 Firmware Updates

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

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

For more information on updating the firmware, see Firmware below .

4.6.8 System Settings

From the System Settings screen, you can view and configure the system settings for the Avocent MP1000 Management Platform. Use the System Settings sidebar menu to navigate through the various sections.

Firmware

To update the firmware:

1. From the *Administration - System Settings - Firmware* screen, click *(Download Page)*. The Vertiv™ Avocent® MP1000 Software Downloads page opens in a new tab.

2. Download the latest firmware version for your appliance type (hardware or virtual).

3. Save the firmware to your local PC, FTP, HTTP or TFTP server.

4. From the *System Settings* screen of the web UI, click the *Update Firmware* button.

5. Select the firmware file and click *Update*.

Figure 4.25   Firmware Updates Screen
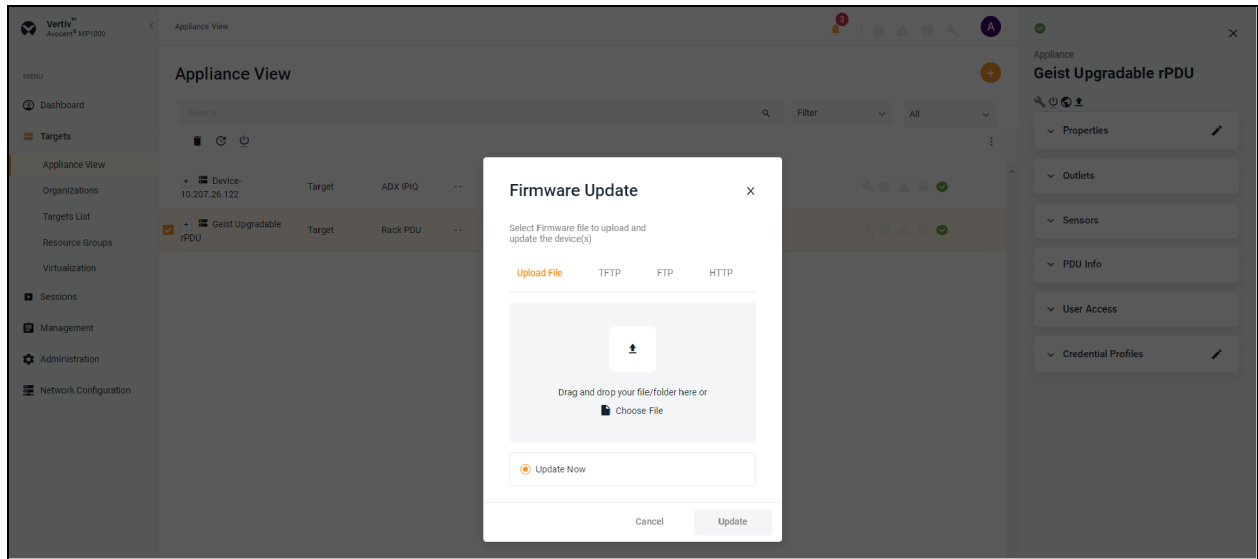
To update the firmware for the multiple devices:

1. From the *Targets - Appliance View* screen, select the devices of the same device type.

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

2. Click the Firmware Update icon above the list of targets. A Firmware Update dialogue box appears.
3. Click *Choose File* and browse to the file from your local drive.
4. 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.

5. Click *Update* to update the firmware.

Password Policy

From here, you can perform the following functions:

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

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

*   Configure the account expiration settings

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

Lockout Policy

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

Timeout

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

Date and Time

From here, you can perform the following functions:

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

    -or-

    Use an NTP server

Events Retention

Purge Events

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

Events Archiving

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

-or-

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

Alarms Retention

Retention Policy

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

Viewer Settings

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

Standalone KVM Viewer Settings

Use the different settings to configure the standalone KVM sessions.

DSView Unit Group Mapping

Use the slider to enable or disable the mapping of the Vertiv™ Avocent® DSView™ unit groups to Resource Groups.

License Expiration Notification

Configure the number of days you wish to be notified of license expiry. For more information, see License Expiration on page 11

FIPS Module

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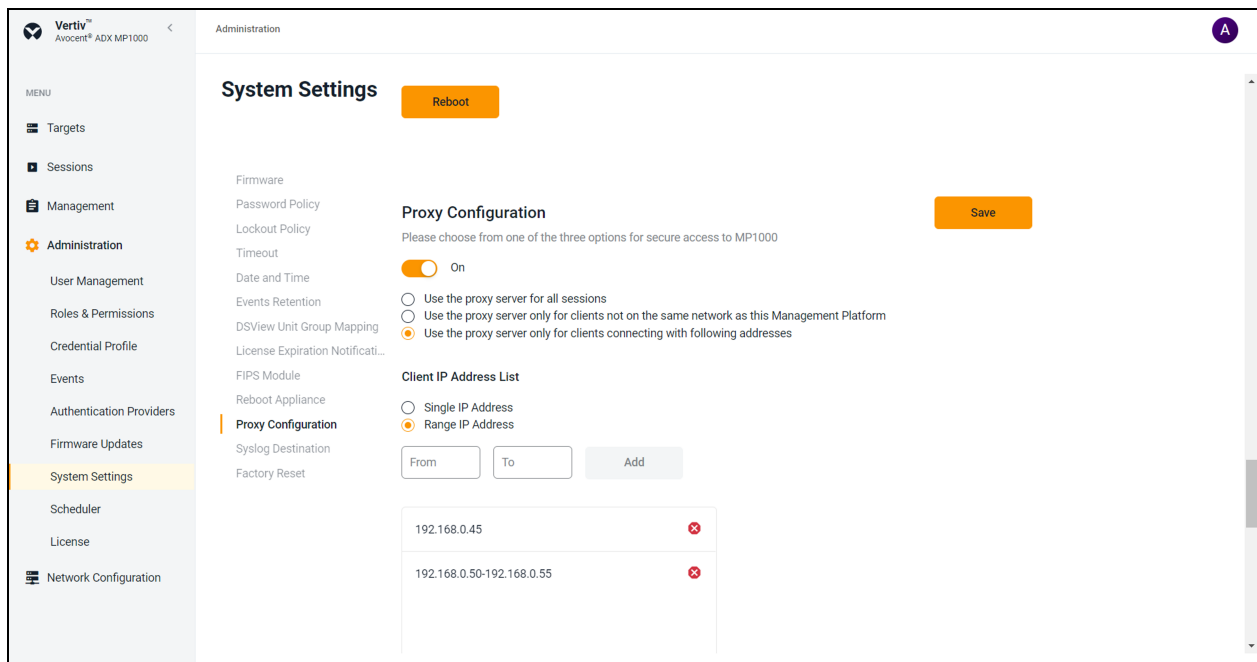
Reboot Appliance

Click *Reboot* to reboot the appliance.

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

Proxy Configuration

Proxy configuration allows you to access all KVM/serial session traffic through the Avocent MP1000 Management Platform.

Figure 4.26   Proxy Configuration Overview


To enable proxy configuration:

1. From the left-hand sidebar, click *Administration - System Settings - Proxy Configuration*.

2. Use the slider to enable the Proxy Configuration setting.

3. For secure access, the user can select one of the following three 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*.

         4 Web User Interface (UI)

Syslog Destination

The Syslog Destination setting enables you to 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.

Figure 4.27   Add Syslog Destination Overview
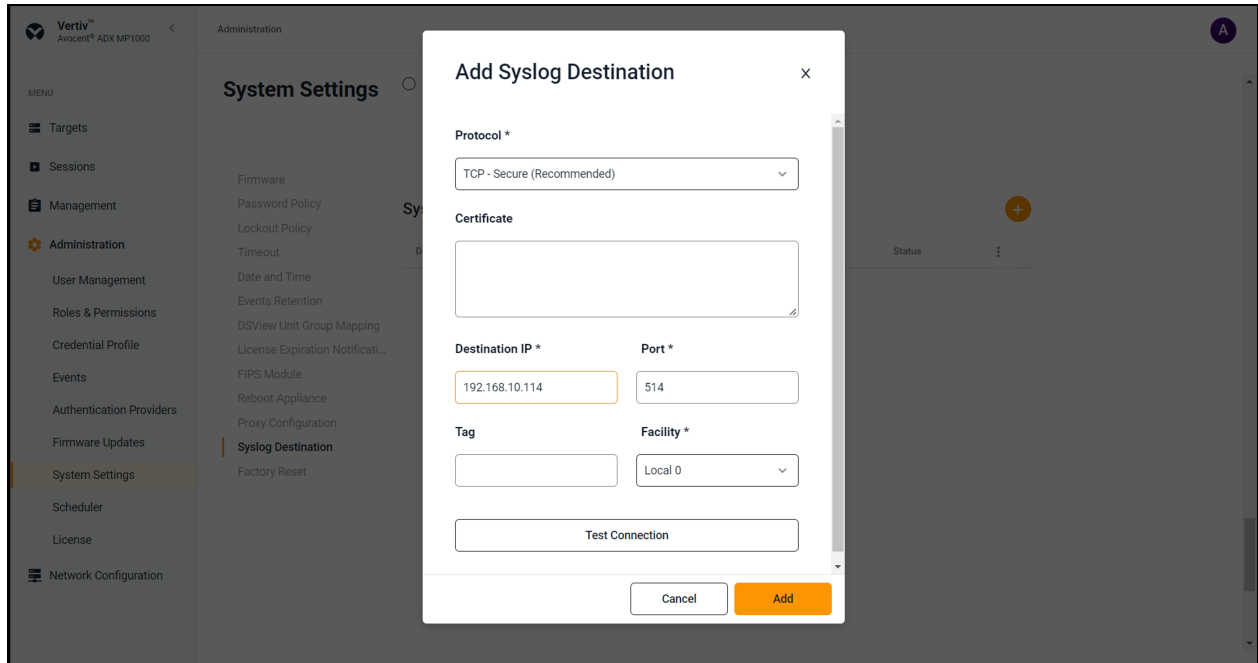
To set up Syslog Destination:

1. From the left-hand sidebar, click *Administration - System Settings - Syslog Destination*.

2. Click the Add icon (+). An Add Syslog Destination dialogue box appears.

3. Use the Protocol drop-down menu to select the protocol.

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

4. 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.

5. (Optional) Add a name to the Tag field, if desired.

6. Use the Facility drop-down menu to select the appropriate syslog facility.

7. 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.

8. Click *Add*.

9. Use the slider to enable the syslog connection.

Synchronization Configuration

The Synchronization Configuration setting allows you to synchronize the device name and data between the management platform and targets.

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

Prerequisite

To prepare for device synchronization:

1. From the left-hand sidebar, click *Administration - System Settings - Synchronization Configuration.*
2. Use the slider 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, proceed to applicable procedure, depending on your selection in step 2.

Device synchronization

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

1. From the *Targets - Appliance View* screen, click on the desired device. The sidebar opens.
2. In the Properties panel, click the Edit icon (pencil).
3. Edit the Device Name field.
4. 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.

5. 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.

On demand resynchronization

To resynchronize the system on demand:

From the *Targets - Appliance View* screen, click the vertical ellipses to the right, then click *Resynchronization*.

NOTE: The device automatically resynchronizes daily at 12:00 am or at the scheduled time.

Synchronization schedule

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

To configure the synchronization schedule:

1. From the *Targets - Appliance View* screen, click on any Vertiv™ Avocent® DSView™ management software device to open its sidebar. The sidebar displays the following tabs:
   - Properties

- User Access
- Scheduler

2. 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.

3. Click *Save*.

Factory Reset

To perform a factory reset:

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

SSH Passthrough

SSH passthrough is a serial session opened to a unit without the use of a web browser. 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 left-hand sidebar, click *Administration – System Settings – SSH Passthrough*.
2. Use 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. Use the following command structure: **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 in System Settings.

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.

4.6.9 Scheduler

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

4.6.10 License

The License screen shows the total number of licenses used, total number of targets managed, and the license expiration date. Additionally, licenses can be uploaded from this screen.

For licensing instructions, see System Licensing on page 5

4.7 Network Configuration

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

4.7.1 Network Settings

The Network Settings tab displays the following items:

- Hostname
- Primary DNS
- Secondary DNS
- Domain Name

To configure the Hostname:

In the Hostname field, enter the new value, then 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. The Normal/Failover-Bonded Settings tab allows you to configure these ports for bonding and/or failover.

To configure failover for the network interface ports:

Using the Uplinks drop-down menu, select either *Ports not bonded, 1st and 2nd ports bonded* or *1st fails over to 2nd port*. Proceed to the next section to determine when you would like the failover to occur.

4.7.3 Failover-Routed IPv4 Trigger Mode

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

To configure the trigger mode for failover:

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 left-hand sidebar, click *Network Configuration - Ethernet Interfaces*.

2. Click the desired interface to open its sidebar.

3. Expand *Network Configuration* to view the settings for the selected interface.

4. Click the Edit icon (pencil) to configure the selected interface.

5. For assigning a static IP, enter the IP address, prefix length and gateway address in the appropriate fields and click *Save*.

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, please refer to the technical note located on the Vertiv™ Avocent® MP1000 Management Platform Virtual Appliance product page.

5 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 local or remote backup
- 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
- Create a backup on demand
- Delete a backup
- Restore a previous configuration of the management platform

NOTE: The Backup and Restore feature does not support backing up one management platform and restoring it on a different appliance.

NOTE: 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.

Backups can be saved to either the local server or a remote server. 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. If you wish to save the backup to a remote server, you must first configure the SMB host in the CLI.

To configure the SMB host server:

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

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

To create an on demand backup:

1. From the Backup and Restore menu, enter **1** for the 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.

To create a scheduled 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 **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.

To view a list of all backups in the management platform system:

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.

To configure 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.

To delete 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.

To restore a backup:

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.

Appendices

Appendix A: Technical Specifications

Table 5.1   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

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/