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

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

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

Figure 1.1 Vertiv Avocent MP1000 Management PlatformDescription

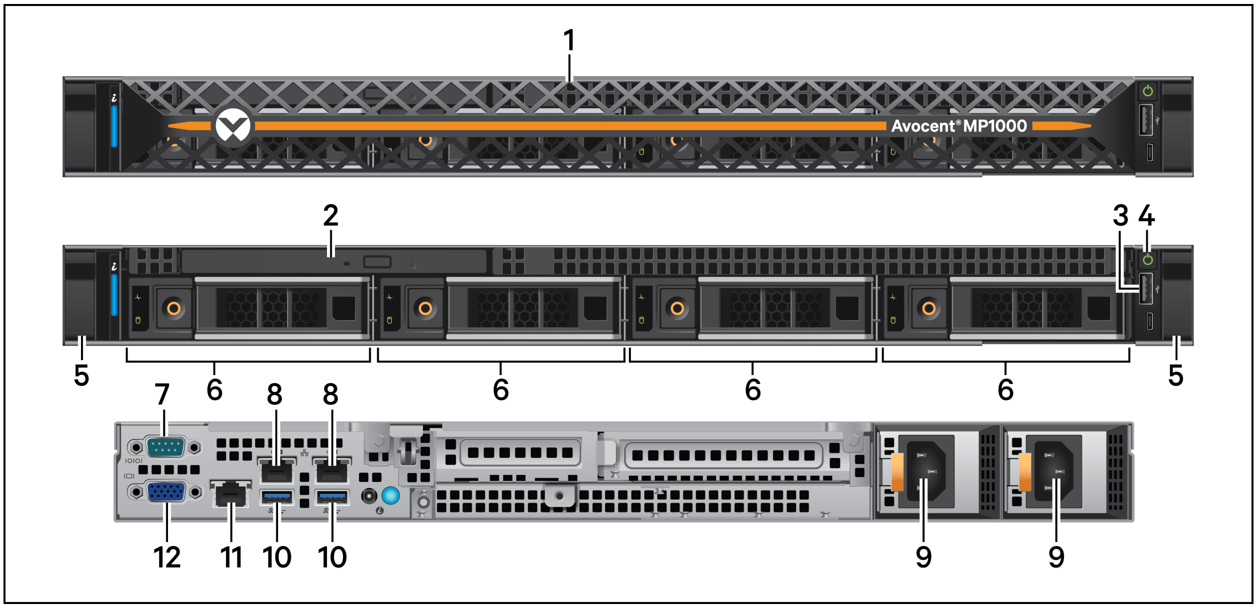


Table 1.1 Vertiv Avocent MP1000 Management PlatformDescription

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

The management platform operates as a managing appliance within the Vertiv™ Avocent® DSView™ solution. The following figure and table describes the system configuration of the Vertiv™ Avocent® DSView™ solution.

Figure 1.2 Vertiv™ Avocent® DSView™ Solution System Configuration

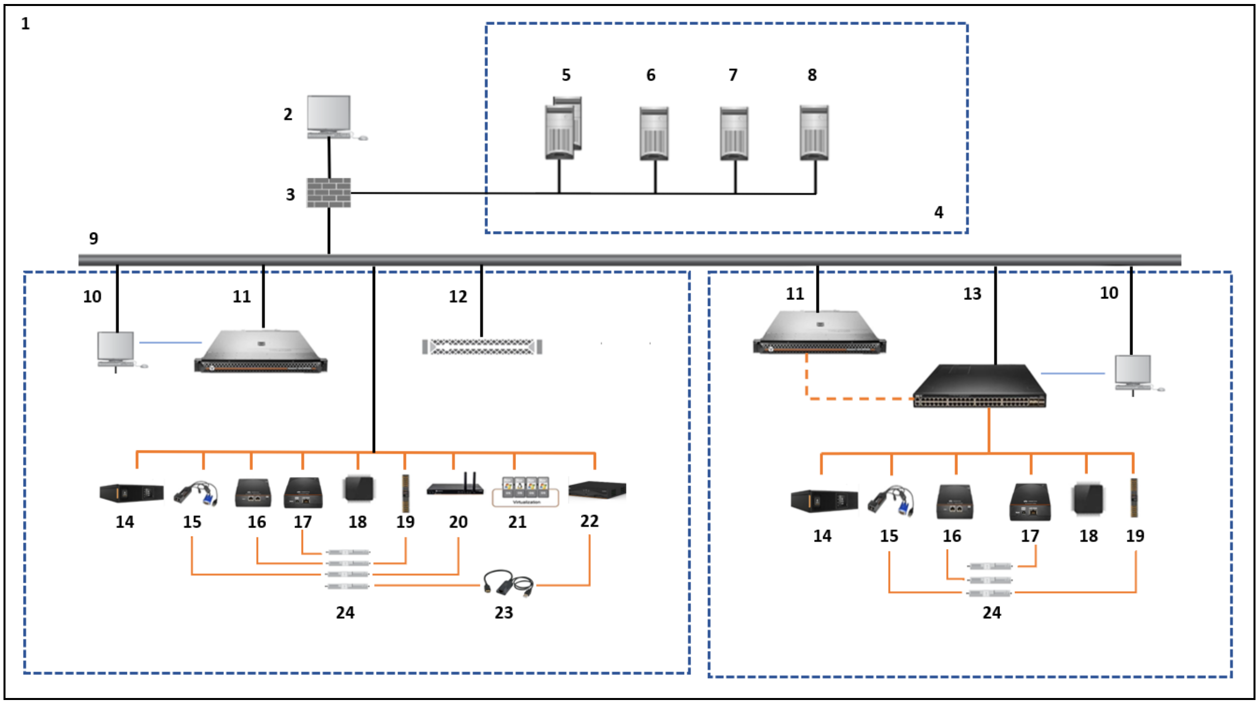


Table 1.2 Vertiv™ Avocent® DSView™ Solution System Configuration Descriptions

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

1.2 Prerequisites

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

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

Table 1.3 Documentation By Appliance Type

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

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

1.3 Features and Benefits

The Vertiv 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

1.4 Physical Security

This product is designed and intended to be deployed and operated in a physically secure and network firewall-protected location. Vertiv recommends a review of the physical security and operating environment of the unit. Since an attacker or disgruntled user can cause serious disruption, below are some recommended best practices that include, but are not limited to:

- Restrict access to areas, racks, and units with encrypted card RFID/badges, unique multi-factor passcode authentication for access, man traps, and biometric scanners for physical access to the equipment.

- Have trusted and background-checked security guards with 24x7x365 physical presence and written logs to help document and note physical access to a data center, building, rack, and so on.
- Restrict physical access to telecommunications equipment and network cabling. Physical access to the telecommunications lines and network cabling should be restricted to protect against attempts to intercept or sabotage communications. Best practices include use of metal conduits for the network cabling running between equipment cabinets.
- All USB, RJ45, and/or any other physical ports should be restricted on the units.
- Do not connect removable media (such as USB devices, SD cards, and so on) for any operation (such as firmware upgrade, configuration change, or boot application change) unless the origin of media is known and trusted. Before connecting any portable device through a USB port or SD card slot, scan the device for malware and viruses.

2 System Licensing

NOTE: The Vertiv Avocent MP1000 Management Platform is transitioning its licensing management processes. Starting with firmware version 3.69.8, the platform will utilize the third-party Thales system for license management and activation. Legacy licenses from the old process will remain valid until they expire or are removed. However, once a legacy license is removed, it cannot be re-added to the appliance. Only Thales licenses can be added to an updated management platform.

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

For instructions on activating and adding licenses to the management platform, refer to License on page 66.

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

2.1 License Usage with Target Devices

Rack manager

Adding the Vertiv™ Avocent® RM1048P Rack Manager as a proxy between the management platform and devices (such as the Vertiv™ Avocent® IPIQ, Vertiv™ Avocent® 4K IPUHD, and Vertiv™ Avocent® IPSL devices) provides centralized management, enhanced functionality, compliance with licensing requirements, failover capabilities, and scalability.

When the rack manager needs to act as a proxy between devices and the management platform, the management platform must have enough Target Licenses to add or enroll the rack manager. Once enrolled, the rack manager will be managed by the management platform. This process deducts 49 counts from the management platform's Target licenses, accounting for the 48 ports and the rack manager appliance itself.

Advanced console system

When a Vertiv™ Avocent® ACS8000 advanced console system is connected to the management platform, all ports on the console system are enabled by default. Therefore, this process deducts counts from the management platform's Target licenses, accounting for the number of enabled ports and the advanced console system itself, even if there are no devices connected to the ports. If you wish to prevent unnecessary license usage, you can disable the ports as needed from the console system's web UI before connecting it to the management platform.

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.

You can also replace the certificates from within the appliance's web UI on the Administration - System Settings - Certificate page. For more information, refer to Certificate on page 64.

If you need additional assistance, please contact your Vertiv Technical Support representative.

This page intentionally left blank

4 Web User Interface (UI)

Once you have connected the Vertiv 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:

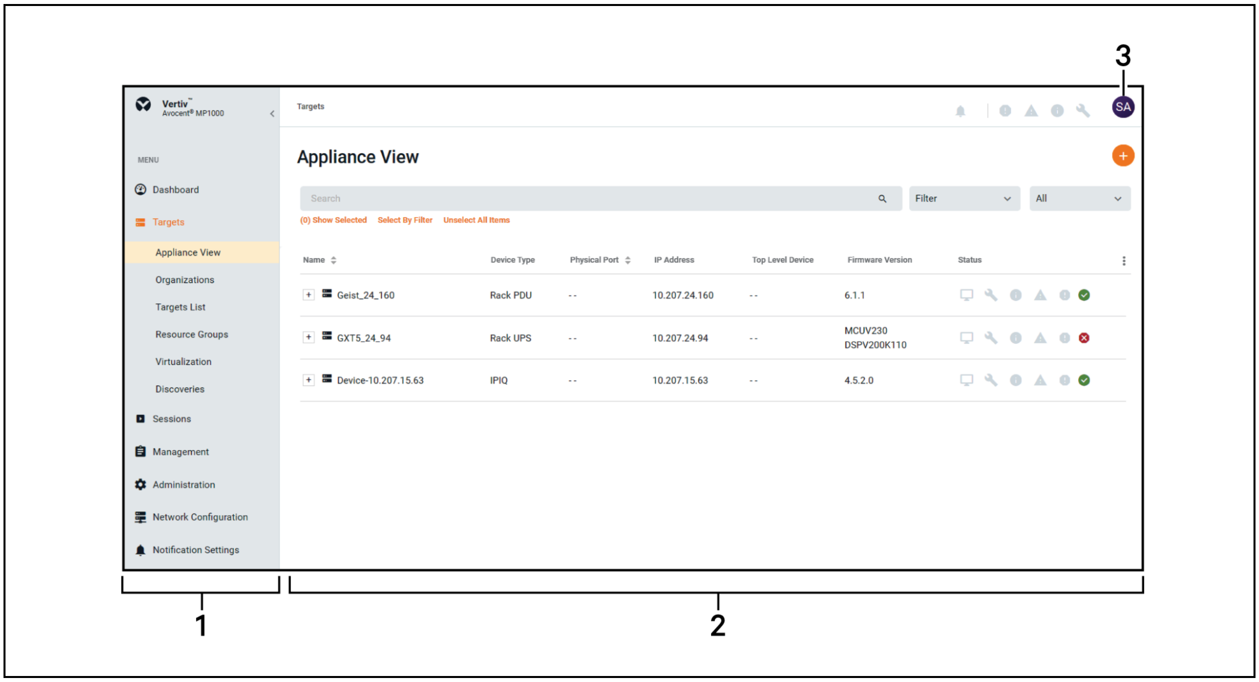
- Google Chrome
- Microsoft Edge
- Apple Safari
- Mozilla Firefox

To log into the web UI:

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

NOTE: Once you've logged in for the first time, you can set up Single-Sign On (SSO) for streamlined authentication. For more information, refer to Setting up Single-Sign On on page 54.

Figure 4.1 Web UI Overview



Name	Device Type	Physical Port	IP Address	Top Level Device	Firmware Version	Status
Geist_24_160	Rack PDU	--	10.207.24.160	--	6.1.1	✓
GXT5_24_94	Rack UPS	--	10.207.24.94	--	MCUV230 DSPV200K110	✗
Device-10.207.15.63	IPIQ	--	10.207.15.63	--	4.5.2.0	✓

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, Color Theme, and SSH Public Key. The following table provides descriptions of these tabs.

Table 4.2 User Preferences

Tab	Description
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 - Select your time zone for alarms and notifications from the drop-down menu. • Time Number Separators - Select the digit grouping and decimal values from the respective drop-down menu. • Data Format - Select either the Day/Month/Year or Month/Day/Year radio button to determine the format for all dates in the web UI. • Time Format - Select either the 12-hours or 24-hour radio button to determine the format for all times in the web UI. • Language - Select the language to be used in the web UI from the drop-down menu.
Color Theme	Select the radio button for your desired color theme.
SSH Public Key	Upload or delete your public key for SSH passthrough. **NOTE: SSH passthrough is accessible only to administrator users; other user roles must be assigned the appropriate permissions to initiate an SSH session. For more information, refer to SSH passthrough on page 62.**

Help

This option redirects you to the web-based version of the Vertiv™ Avocent® MP1000 Management Platform User Guide.

Log Out

This option immediately logs you out of the web UI.

4.2 Dashboard

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

4.2.1 Edge management

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

- View the alarm status for sites and devices.
- Drill deeper into device data.
- View key device metrics.
- Remotely recover via the KVM device, serial device, SP, and the cycle power via the UPSes and PDUs.

To navigate the Edge Management screen:

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

- Organizations - A list of all available organizations and ungrouped devices. Use the Search field to search for specific organizations. Use the Filter drop-down menu to filter organizations by All, No Devices, Has Devices, Has No Sub Orgs or Has Sub Orgs. Upon selecting the organization in this view, the associated list of devices and alarms appear in the Device Locator and Alarms views. For more information, refer to Organizations on page 21.
- Device Locator - A list of all the devices associated with the specific organization. Select the device to view its associated alarms and device metrics. Use the Search field to search for specific devices. Use the Filter drop-down menu to filter devices by All, Rack PDU, Power Outlet and IPIQ. Use the All drop-down menu to search for devices by the following status options: Responding, On and Off.
- Device Metrics - A description of device metrics, including Energy, Real Power (W), Apparent Power (VA) and Power Factor. This view appears after selecting the device in the Device Locator view.
- Alarms - A list of alarms associated with the selected device. Click the vertical ellipsis to clear the alarm. For more information, refer to Alarms on page 53.

4.3 Targets

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

- Vertiv™ Avocent® RM1048P Rack Manager
- Uninterruptible Power Supplies (UPSes)
- Power Distribution Units (PDUs)
- Service Processors (SPs)
- Vertiv™ Avocent® MergePoint Unity™ KVM over IP and serial console switch
- Vertiv™ Avocent® MergePoint Unity™ 2 KVM over IP and serial console switch
- Vertiv™ Avocent® AutoView™ switch
- IP KVM devices
- Vertiv™ Avocent® ACS 800/8000 advanced console system
- Vertiv™ Avocent® DSView™ management software
- Virtual Machines (VMs)
- Generic devices

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

Vertiv™ Avocent® RM1048P Rack Manager

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

- Vertiv™ Liebert® rack UPSes
- Vertiv™ Power IT rack PDUs
- Service Processors
- IP KVM devices

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

NOTE: Once added, a rack manager can only be accessed via the 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.

Uninterruptible Power Supplies (UPSes)

Vertiv™ Liebert® rack 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.

Power Distribution Units (PDUs)

Vertiv™ PowerIT rPDUs 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 an rPDU 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 management platform can discover SPs over the network, provided the SPs have an IP address and are connected to the same network as the management platform.

The Vertiv Avocent MP1000 Management Platform and Vertiv™ Avocent® RM1048P Rack Manager support the following SPs:

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

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

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

Refer to Web UI sessions on page 33 to launch a session to the SP device via the management platform.

Vertiv™ Avocent® MergePoint Unity™ KVM over IP and serial console switch

The Vertiv™ Avocent® MergePoint Unity™ switch combines analog and digital technology to provide flexible, centralized control of data center servers and virtual media, and to facilitate the operations, activation, and maintenance of remote branch offices where trained operators may be unavailable. The IP-based switch provides flexible target device management control and secure remote access from anywhere at any time.

The switch supports IQ modules that are powered directly from the target device and provide Keep Alive functionality when the switch is not powered. For a list of supported IQ modules, please refer to the Vertiv™ Avocent® Cables and Server Interface Modules sheet.

Additionally, the Vertiv™ Avocent® MergePoint Unity™ switch also supports the Vertiv™ Avocent® MPUIQ-SRL module, which provides true serial capabilities through SSH and serial viewer sessions.

When connected to the management platform, the Vertiv™ Avocent® MergePoint Unity™ switch supports the following capabilities:

- Launch KVM and serial sessions, with session sharing permitted
- Launch the web page of the switch appliance
- Perform maintenance activities, including rebooting, resynchronization, and firmware upgrades
- Two-tier expansion, with the Vertiv™ Avocent® AutoView™ switch or the Vertiv™ Avocent® MergePoint Unity™ switch

Vertiv™ Avocent® MergePoint Unity™ 2 KVM over IP and serial console switch

The Vertiv™ Avocent® MergePoint Unity™ 2 switch is a next-generation KVM over IP and serial console switch designed for secure, high-performance remote management of servers and network devices. The management platform supports the following switch models:

- MPU2-108DAC-400
- MPU2-2016DAC-400
- MPU2-2032DAC-400
- MPU2-4032DAC-400

Vertiv™ Avocent® AutoView™ switch

The Vertiv™ Avocent® AutoView™ 2108/2216/3108/3216 switch is an analog keyboard, video and mouse (KVM) switch that provides flexible, centralized local access to data center servers. The switch also provides centralized remote access to data center servers.

NOTE: The 2108/2216 models require the optional Remote Access Key for remote access.

The switch supports IQ modules that are powered directly from the target device and provide Keep Alive functionality when the switch is not powered. For a list of supported IQ modules, please refer to the Vertiv™ Avocent® Cables and Server Interface Modules sheet.

When connected to the management platform, the Vertiv™ Avocent® AutoView™ switch supports the following capabilities:

- Launch KVM sessions, with session sharing permitted
- Launch the web page of the switch appliance
- Perform maintenance activities, including rebooting, resynchronization, and firmware upgrades
- Two-tier expansion, with the Vertiv™ Avocent® AutoView™ switch or the Vertiv™ Avocent® MergePoint Unity™ switch

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 management platform provides flexible, centralized control of data center servers and virtual media of remote branch offices where trained operators may be unavailable. KVM over IP allows for flexible target device management control and secure remote access from anywhere at anytime.

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

- Keyboard, video, and mouse (KVM) capabilities, configurable for digital (remote) connectivity
- HTML5 KVM Viewer
- Serial Viewer
- Session management
- Session sharing
- Screen capture
- Screen recording
- Control over color depth
- Zoom
- Virtual keyboard
- Copy and paste
- Network bandwidth optimization
- Macros
- Virtual media

Refer to KVM sessions on page 27 for initial prerequisites and configurations, as well as information on launching and configuring KVM sessions.

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

Vertiv™ Avocent® ACS 800/8000 advanced console system

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

Vertiv™ Avocent® DSView™ management software

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

NOTE: In order to connect the management software with the management platform, a Web Services API license is required. To check if your system is already equipped with the license, log into the web UI of the Vertiv™ Avocent® DSView 4.5 management software and navigate to the *System - Licenses* page. The license will be listed as Web Services API. Contact Vertiv Technical Support if you do not have the license key currently installed.

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 Vertiv Avocent MP1000 Management Platform migration
- Allows for the integration of Vertiv™ Avocent® DSView™ management software zones as part of the login, which enables you to view all target devices within the zone, rather than just top-level devices.

Virtual Machines (VMs)

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

Generic devices

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

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

Refer to Web UI sessions on page 33 to launch a session to the generic device via the management platform.

4.3.1 Appliance view

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

From the Appliance View screen, you can view and manage the target devices connected to the management platform. You can perform the following functions:

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

Adding and deleting devices

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

NOTE: To discover devices for the management platform, you must create credential profiles for the following device types: Service Processors, Rack PDUs, Rack UPS, Vertiv™ Avocent® DSView™ management software, and Virtual Machines. All of these devices require Username/Password credentials, except for the Rack UPS. The Rack UPS requires SNMPv1/v2 credentials. To create a credential profile, refer to Credential profiles on page 48.

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

To discover a single device or a range of devices:

1. From the left-hand sidebar, click *Targets - Appliance View* or *Discoveries*.
2. Click the Add Device icon (+) in the top right corner. The Device dialog box appears.
3. Click the *Discover* tab.
4. Select the Single IP radio button to add a single device.

   -or-

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

   -or-

   If you selected the Range IP radio button, enter the IP address range.
7. Select the device type from the Device Type drop-down menu.
8. Based on your selection, fill out the appropriate fields.
9. Click *Discover*. It may take several minutes for the device(s) to be successfully added to the management platform. Once added, the target devices appear on the Appliance View and Targets List screens.

To add a generic device:

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

To delete a target device:

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

Modifying device information

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

To modify device properties and other information:

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

Performing maintenance activities

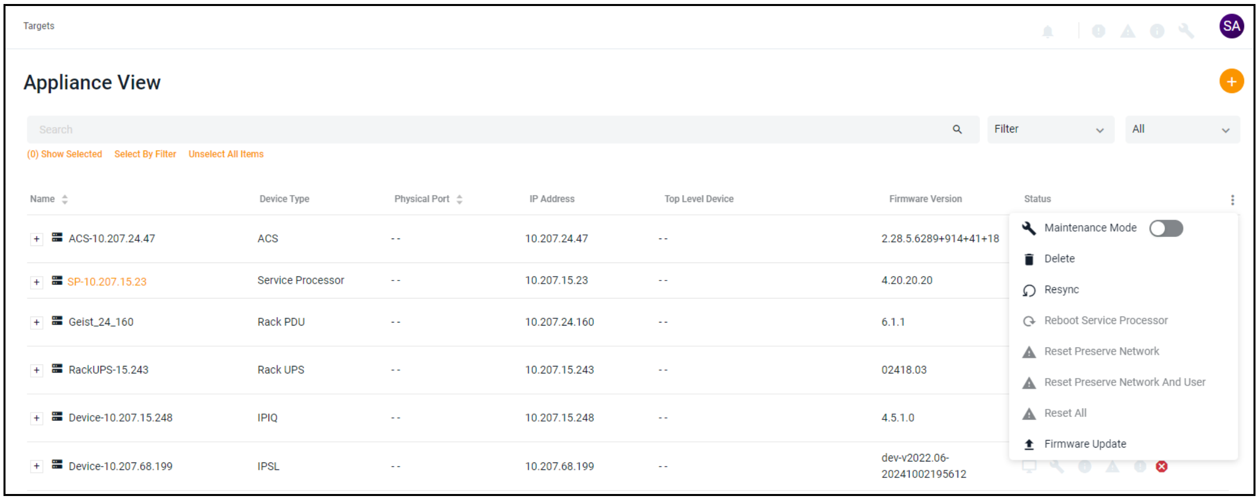
You can perform a variety of maintenance activities for each target device such as:

- Activating maintenance mode
- Removing devices
- Updating firmware for one or more devices
- Rebooting devices
- Resynchronizing devices
- Powering on/off outlets
- Power cycling outlets

The types of maintenance activities that are available may vary by device type. To access these functions, click on the vertical ellipsis on the right side of the device row.

The following figure shows an example of the possible maintenance activities that can be performed for a Service Processor.

Figure 4.2 Maintenance Activities



Name	Device Type	Physical Port	IP Address	Top Level Device	Firmware Version	Status
ACS-10.207.24.47	ACS	--	10.207.24.47	--	2.28.5.6289+914+41+18	
SP-10.207.15.23	Service Processor	--	10.207.15.23	--	4.20.20.20	
Geist_24_160	Rack PDU	--	10.207.24.160	--	6.1.1	
RackUPS-15.243	Rack UPS	--	10.207.15.243	--	02418.03	
Device-10.207.15.248	IPIQ	--	10.207.15.248	--	4.5.1.0	
Device-10.207.68.199	IPSL	--	10.207.68.199	--	dev-v2022.06-20241002195612	

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

To activate Maintenance Mode:

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

   -or-

Click on the row of the desired device to open its information side panel and click the Tool icon below the device name.

To remove a target device:

1. From the left-hand sidebar, click *Targets - Appliance View.*
2. Hover the mouse over the desired device row and click the vertical ellipsis on the right side.
3. Click *Delete*. The Delete Device dialog box appears.
4. Click *Yes, Delete* to verify the removal of the device.

To update the firmware for one or more devices:

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

1. From the left-hand sidebar, click *Targets - Appliance View*.
2. To perform an update for a single device, hover over the row, click the vertical ellipsis on the right side, and click *Firmware Update*.

   -or-

   To perform a bulk update for multiple devices, hover over each row, check the box on the left side for all devices, and click the Firmware Update icon above the list of targets.
3. The Firmware Update dialog box appears. Choose whether to update the firmware via one of the following servers: local, TFTP, FTP, HTTP, SFTP, or SCP.

NOTE: The availability of update methods varies by device type. Refer to Table 4.3 below for more information.

4. If you selected the *Upload File* tab, then click *Choose File* and browse to the firmware file. You can also drag and drop the firmware file.

   -or-

   If you selected the *TFTP, FTP, HTTP, SFTP,* or *SCP* tab, fill in the provided fields.
5. Click *Update*.

Table 4.3 Supported Firmware Update Methods Per Device Type

Device Type	Update Method					
	Upload File	TFTP	FTP	HTTP	SFTP	SCP
Rack Managers	Yes	Yes	Yes	Yes	No	No
Console Systems	No	No	Yes	No	Yes	Yes
Legacy KVM Switches	Yes	No	No	Yes	No	No
Service Processors	Yes	Yes	Yes	Yes	No	No
IP KVM and IP Serial Devices	Yes	Yes	Yes	Yes	No	No
Rack PDUs	Yes	Yes	Yes	Yes	No	No
Rack UPSes	Yes	Yes	Yes	Yes	No	No
Virtual Machines	No	No	No	No	No	No
Legacy Management Software	No	No	No	No	No	No

To reboot a target device:

1. From the left-hand sidebar, click *Targets - Appliance View*.
2. Hover the mouse over the desired device row and click the vertical ellipsis on the right side.
3. Click *Reboot*. The Reboot Device dialog box appears.
4. Click *Yes, Reboot* to confirm the rebooting of the device.

To resynchronize a target device:

1. From the left-hand sidebar, click *Targets - Appliance View*.
2. Hover the mouse over the desired device row and click the vertical ellipsis on the right side.
3. Click *Resync*. The Resync Device dialog box appears.
4. Click *Yes, Resync* to confirm the rebooting of the device.

To power on/off all outlets for rack PDU target devices:

1. From the left-hand sidebar, click *Targets - Appliance View*.
2. Hover the mouse over the desired device row and click the vertical ellipsis on the right side.
3. Click *Power On All Outlets*.

   -or-

   Click *Power Off All Outlets*.

To power cycle all outlets for rack PDU target devices:

1. From the left-hand sidebar, click *Targets - Appliance View*.
2. Hover the mouse over the desired device row and click the vertical ellipsis on the right side.
3. Click *Power Cycle All Outlets*.

Securing device connections

You can enable Secure mode when connecting to Vertiv™ Avocent® MergePoint Unity™ switch appliances. When this setting is enabled, users can only access the appliance from the management platform. Sessions can still be launched, but users will no longer be able to access the web UI of the switch appliance.

To enable Secure mode for connecting switch appliances:

1. From the left-hand sidebar, click *Targets - Appliance View*.
2. Click on the row of the desired appliance to open the information side panel.
3. Click the Edit (pencil) icon for the MergePoint Unity Settings section.
4. Click the toggle button to enable Secure mode, and then click *Apply*.

Synchronizing devices

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

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

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

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

-or-

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

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

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

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

To resynchronize the system on demand:

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

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

To configure the synchronization schedule:

1. From the left-hand sidebar, click *Targets - Appliance View*.
2. Click on any Vertiv™ Avocent® DSView™ management software device to open its information panel. The panel displays the following tabs::
   - Properties
   - User Access
   - Scheduler
3. Click the Edit icon (pencil) to the right of the Scheduler to edit the following fields:
   - Repeat Day: Modify the schedule by day.
   - Repeat Time: Modify the schedule by time.
4. Click *Save*.

Merging devices

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

NOTE: You cannot merge VMs.

To merge targets:

1. From the left-hand sidebar, click *Targets - Appliance View*.
2. Select the targets you want to merge by hovering your mouse over each target and clicking the box to the left of each one.
3. Click *Merge Targets*, then click *Merge*. A plus icon (+) displays to show the merged targets. Click the + to expand the merged target and show each individual target.

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

To unmerge targets:

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

   -or-

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

Launching sessions

You can launch KVM, serial, or web UI sessions from two different areas of the Targets List screen or the Appliance View screen. For more information about the different session types and activities, refer to Sessions on page 25.

Launching a dashboard

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

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

To launch a dashboard:

1. From the left-hand sidebar, click *Targets - Appliance View*.
2. Hover the mouse over the desired device(s) and check the box next to the device name.
3. From the top of the screen, click the Launch Dashboard icon (play symbol). The dashboard launches into a new tab in preview mode for the number of devices virtually connected through KVM.

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

4. The Dashboard preview screen provides the following features:
   - A Launch Viewer icon (play symbol) to launch a live KVM session.
   - A Full Screen icon to maximize the screen size.
   - A Delete icon (trash can) to remove the widget from the dashboard.
   - A Maintain Aspect Ratio check box to configure the desired aspect ratio for the widgets.
   - A drop-down menu to configure the size of the widgets.

4.3.2 Organizations

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

- Organize devices by location
- Configure automatic alarm aggregation

- View display of global alarm counts and source alarms
- View the alarm summary
- Navigate to the alarm
- Create, configure, and delete organizations

Creating an organization

To create a new organization:

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

Managing an organization

To edit an existing organization:

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

To move an organization using the Organization Editor:

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

Deleting an organization

To delete an organization using the Organization Editor:

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

4.3.3 Targets list

From the Targets List screen, you can perform the same functions that are available from the Appliance View screen. Unlike the Appliance View screen, the targets are not organized by the appliance to which they are associated. For more information, refer to Appliance view on page 15.

4.3.4 Resource groups

From the Resource Groups screen, you can organize targets in a hierarchy by creating nested resource groups (groups within groups). A resource group is a collection of target devices that can be centrally managed. These groups allow administrators to apply specific roles and permissions to multiple devices simultaneously, simplifying the management process. Resource groups can also be linked to local user groups or external authentication provider user groups, such as Active Directory or LDAP.

NOTE: Targets may belong to multiple resource groups.

NOTE: A resource group can only be a child to one parent resource group at a time. When you want to add child resource groups to a parent resource group, you can choose from all available resource groups. If a resource group is already assigned to a different parent, it can still be selected to become a child of the new parent resource group. In this case, it will be automatically moved from its current parent to the new parent without any notification.

Setting up resource groups

Before you can create a resource group, ensure the following prerequisites have been met:

- A local user group has been created for the resource group with the necessary system role assigned to the group. For more information, see Groups on page 41.
- A target role has been created for the resource group with the necessary device permissions assigned to the role. For more information, see Configuring roles and permissions on page 48.

Once the local user group and target role have been configured, you are ready to create the resource group.

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 dialog 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. You can use the Search field to filter targets.

   -or-

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

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.

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

Enabling inherited permissions

By enabling Inherited Permissions, you can configure the appliance to automatically pass down the permissions of parent groups to child groups or devices. Any updates or changes to the parent group's permissions are immediately reflected in the child groups and devices. This feature simplifies the management of permissions by ensuring that changes made at a higher level are consistently applied to all subordinate devices.

To enable Inherited Permissions on a parent group:

1. From the left-hand sidebar, click *Administration – System Settings*.
2. Click on the *Inherited Settings* tab.
3. Click on the toggle button to enable Inherited Permissions. By default, this setting is disabled.
4. Click *Save*.

If necessary, you can override the Inherited Permissions settings for a group of target devices. By overriding the setting, permissions will no longer be automatically applied to the devices. You can also override the setting on specific devices, rather than the entire group, without affecting its siblings within the group.

To override Inherited Permissions:

1. From the left-hand sidebar, click *Targets – Appliance View* or *Targets - Resource Groups*.
2. Click on the device for which you want to override the setting. The device panel opens on the right-hand side.
3. On the Properties drop-down menu, click on the Edit icon (pencil).
4. Click on the Allow Inherit toggle button to disable the setting.
5. Click *Save*.

Deleting resource groups

To delete a resource group:

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

   -or-

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

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

4.3.5 Virtualization

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

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

To add a VM as a target device:

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

5. Click *Add Host(s)*.

4.3.6 Discoveries

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

To navigate the Discoveries screen:

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

- View the different discovery logs by clicking the *Range* or *Appliance* tab.
- Search for specific tasks or target devices using the search bar.
- Conduct searches based on an IP address using the Start IP and End IP bars.
- Filter searches by discovery status using the All Status drop-down menu.
- Discover and add devices by clicking the Add Device icon (+) in the top right corner. For further instructions, refer to Adding and deleting devices on page 15.

4.4 Sessions

The Sessions tab contains one sub-menu item - Sessions List - from which you can view session information for past and current sessions. The Vertiv Avocent MP1000 Management Platform allows you to launch multiple sessions simultaneously to access your target devices via the management platform web UI.

4.4.1 Sessions list

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

To navigate the Sessions List screen:

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

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

Exporting data

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

To export data as a CSV file:

1. From the left-hand sidebar, click *Sessions – Sessions List*.
2. (Optional) Filter the list of sessions, as desired.

3. Click the Export icon in the right corner to export the Active, Closed, or All page. The Export List to CSV dialog box appears.
4. Review the dialog box and verify once more that the CSV file is set to be sent to the correct email address.
5. Click *Export*. The CSV file is sent to the specified email address.

Table 4.4 below provides descriptions of the columns in the CSV file.

Table 4.4 CSV File Field Descriptions

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

Table 4.4 CSV File Field Descriptions (continued)

Column Name	Description
	• SM_LOCAL_PORT = sessions involving the local port (may not be shared/stealthed/anything)
State	State of the user session: • SS_PENDING = session is defined but not yet connected • SS_INITIATED = session initiated in the process to be connected • SS_CONNECTED = session is connected • SS_TERMINATED = session was terminated by another user • SS_EXPIRED = session was terminated (based on session timeout interval) • SS_REJECTED = session request to share read-only or interactive was rejected, session was never connected • SS_RECONNECTING = session got interrupted by network. Session is in re-connecting state • SS_RECONNECTED = failed to reconnect the session

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

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

4.4.2 KVM sessions

The Vertiv Avocent MP1000 Management Platform conducts KVM sessions using the web-based HTML5 Video Viewer with one or more target devices attached to one or more KVM switches. When a target device connects to the management platform, the target screen appears in a new window, and the target server can be controlled remotely. In addition to controlling each target device, you can access target server files, manage software updates and execute operating system commands. Each target server has a device information panel that contains data about the device.

This section covers the following topics for KVM sessions:

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

Supported browsers and processors

The HTML5 Video Viewer supports the following web browsers:

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

The following table describes the compatibility of the HTML5 Video Viewer capabilities for each supported browser. For more information about the KVM video viewer features, refer to Table 4.7 on the facing page.

Table 4.5 KVM Viewer Feature and Browser Compatibility

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

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

Table 4.6 Supported Processors and Servers

Service Processor	Port
Dell iDRAC7	5900
Dell iDRAC8	5900
Dell iDRAC9	5900
HP iLO 4	5900 (Firmware<2.8), 443 (Firmware>2.8)
HP iLO 5	443
XCC	3900

Launching KVM sessions

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

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

To launch a KVM session:

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

-or-

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

To close a KVM session:

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

Configuring KVM sessions

After launching a KVM session, you can use the menu located at the top of the Video Viewer window to access the features described in the following table. You can also configure the settings for the Vertiv Avocent MP1000 Management Platform using the *Settings* icon. Table 4.7 below provides descriptions of the various KVM features.

NOTE: The availability of the KVM Video Viewer features varies by device type.

Table 4.7 KVM Video Viewer Features

Feature	Menu	Description
Open Server-side Recording File	*File - Open Server-side Recording File*	Open a server-side recorded file to play.
Paste Text From File	*File - Paste Text From File*	Copy text content from a text file and send it to the target.
Audio Configuration	*View - Audio & Video Options - Audio Configuration*	Configure the number of audio channels and audio quality level. Applies to all users.
Video Color Settings	*View - Audio & Video Options - Video Color Settings*	Display more color options to optimize fidelity or less colors to reduce the volume of data transferred on the network. The maximum speed is Grayscale 16 Shades, and the maximum video quality is Color 24 bit. Applies to all users.
Video Noise Filter	*View - Audio & Video Options - Video Noise Filter*	Enable noise filter for VGA or disable it for a digital video source. Applies to all users.
Video Lane Settings	*View - Audio & Video Options - Video Lane Settings*	Configure USB-C lane speed and view the number of current video lanes. Applies to all users.
Refresh	*View - Refresh*	Refresh the session.
Full Screen	*View - Full Screen*	Enable Full Screen mode with or without single-cursor mode.
Scaling	*View - Scaling*	Adjust the size of the ratios of the session screen by configuring or selecting the Fit to Window, Stretch to Window or Zoom setting.
Max Resolution	*View - Max Resolution*	Select the maximum target resolution for your KVM session. This setting applies to all users and affects the actual video resolution of your target systems OS.
Single Cursor	*View - Single Cursor*	Enable single-cursor mode.
Statistics	*View - Statistics*	View KVM statistics.
User Information	*View - User Information*	View general user information.
Status Bar	*View - Status Bar*	Display or hide the status bar at the bottom of the screen.
Static Macros	*Macros - Static Macros*	Send multi-key commands to make sure the command string is accurate. After you select the applicable operating system, select *Static Macros* to access the list of command strings that are valid for the selected operating system. Send a string of commands by clicking the desired string from the Static

Table 4.7 KVM Video Viewer Features (continued)

Feature	Menu	Description
		Macros list and clicking *Send*. The options in the drop-down list are pre-determined based on the macro set you select. If you are looking for a command string that does not appear in the list, verify that you have selected the correct operating system in the Manage Macros window. **NOTE: It is recommended that you use the Macros tab to send a command string to a server. This saves time and eliminates the risk of errors. Your client server will not be affected.**
Manage Macros	*Macros - Manage*	Define macros from the Manage Macros window.
User Preferences	*Tools - User Preferences*	Select the keyboard language and configure the settings for pasting text, dragging and dropping files/folders and recording.
Instant Message	*Tools - Instant Messages*	Send a message to all users currently logged in.
Capture Screen	*Tools - Capture Screen*	Capture a screenshot of the session.
Mouse Modes	*Tools - Mouse Modes*	Select a mouse mode: Absolute, Relative (no acceleration) or Relative
Align Local Cursor	*Tools - Align Local Cursor*	Align the cursor with the view orientation of the session.
Reset Keyboard/Mouse USB	*Tools - Reset Keyboard/Mouse USB*	If you begin experiencing issues with your keyboard or mouse, you can reset the device.
Exclusive Mode	*Tools - Exclusive Mode*	Enable Exclusive Mode when you need to access a target while excluding all other users. When a target is selected with the Exclusive Mode setting enabled, no other user in the system can switch to that target.
Virtual Keyboard	*Tools - Virtual Keyboard*	When enabled, the keyboard displays on the client's workstation and can be positioned anywhere in the window. Use the up and down arrows in the top right to change the size of the keyboard.
Start Recording	*Tools - Start Recording*	Begin recording a video of the session.
Optimize Network Bandwidth	*Tools - Optimize Network Bandwidth*	Optimize your network bandwidth for better session performance.
Remote Audio	*Tools - Remote Audio*	Enable or disable remote audio.
Create ISO Image	*Tools - Create ISO Image*	Create an ISO image to store data from the target session.
Browse Disk Image	*Tools - Browse Disk Image*	Browse to a saved disk image.
Map Removable Disk/Floppy Disk Image	*Virtual Media - Map Removable Disk/Floppy Disk Image*	See Using virtual media on the facing page.

Table 4.8 below compares the HTML5 Video Viewer features available for the Vertiv™ Avocent® IPUHD 4K IP KVM device standalone and the Vertiv™ Avocent® IPIQ IP KVM device when they are operated as either standalone devices or managed by the management platform or the Vertiv™ Avocent® RM1048P Rack Manager.

Table 4.8 Feature Comparison for IP KVM Device Viewers

Feature	Standalone Vertiv™ Avocent® IPUHD 4K IP KVM device	Managed Vertiv™ Avocent® IPUHD 4K IP KVM device	Managed Vertiv™ Avocent® IPIQ K IP KVM device
Option to play server-side recorded file (File - Open Server-side Recording File)	✓	×	×
Video Noise Filter (View - Audio and Video Options)	✓	✓	×
Video Lane Settings (View - Audio and Video Options)	✓	✓	×
Remote Audio Support (Tools - Remote Audio)	✓	✓	×
Max Resolution Settings (View - Max Resolution)	✓	✓	×
User Information (View - User Information)	✓	×	×
Instant Message (Tools - Instant Message)	✓	×	×
Optimize Network Bandwidth (Tools - Optimize Network Bandwidth)	✓	✓	×

Using virtual media

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

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

NOTE: VMs do not have the Virtual Media feature.

Prerequisites

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

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

To map a Virtual Media drive:

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

-or-

Click *Map Removable Disk Image* to map an .img file.

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

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

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

To unmap a Virtual Media drive:

1. From the KVM Video Viewer session, click the *Virtual Media* tab, then click the mapped drive to unmap that particular drive.

   -or-

   Click *Disconnect* to unmap all the drives.

2. At the prompt, click *Yes*.

Sharing KVM sessions

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

Table 4.9 Session Sharing Options

Option	Description
Active Sharing	You, as well as other users, can interact with the target.
Passive Sharing	Access is granted to the target in read-only mode. The other user knows you are viewing the session.
Preempt	The previous user's session is interrupted and terminated.
Stealth	Access is granted to the target in viewer-only mode. The other user does not know you are viewing the session.

If you are currently connected to a target server and another user attempts to share the session with you, the Video Viewer allows you to select how you want the user to connect. The following options are available: Approve, Reject or Allow as read-only.

NOTE: When a Vertiv™ Avocent® MergePoint Unity™ switch is added to the management platform, the Automatic Sharing is enabled by default. This feature must be enabled to allow for session sharing on the management platform with the switch.

Reconnecting to KVM sessions

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

4.4.3 Serial sessions

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

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

Launching serial sessions

To launch a serial session:

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

   -or-

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

To end a serial session:

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

4.4.4 Web UI sessions

Service Processors (SPs), generic devices, and Vertiv™ Avocent® MergePoint Unity™ switches can be remotely accessed from the management platform by launching the web UI of the target device.

To launch the web UI of the target device:

1. From the left-hand sidebar, click *Targets - Appliance View*.
2. Hover your mouse over the desired device and click the vertical ellipsis on the right side of the row.
3. Click *Open Web Page*. You are redirected to the webpage of the device.

4.5 Management

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

4.5.1 Devices

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

To navigate through the Devices tab:

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

- View the different logs of target devices by clicking the *Managed* or *Unmanaged* tab.
- Add a new device by clicking the Add icon (+) and filling out the required fields.
- View and configure a managed device's settings by clicking on the orange link in the Name column. For more information, refer to Updating configuration settings for managed devices below.
- Save and restore specific configurations for the Vertiv™ Avocent® ACS800/8000 advanced console system. For more information, refer to Saving and restoring a specific configuration on the facing page.
- Save and restore configuration templates for the Vertiv™ Avocent® ACS800/8000 advanced console system. For more information, refer to Saving and applying a configuration template on page 36.

Updating configuration settings for managed devices

You can directly access and update specific configuration settings for the following target devices:

- Vertiv™ Avocent® ACS8000 advanced console system
- Vertiv™ Avocent® IPSL IP serial device
- Vertiv™ Avocent® RM1048P Rack Manager

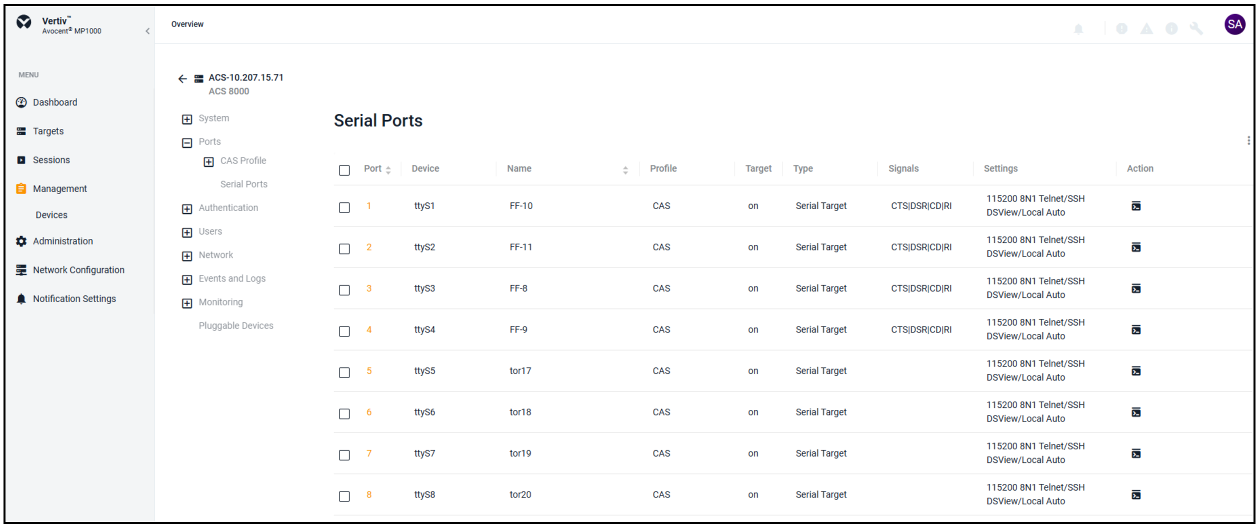
For detailed configuration instructions for each target device UI, refer to the respective product's user guide, which is available at www.vertiv.com.

To configure the UI settings for managed devices:

1. From the left-hand sidebar, click *Management - Devices*.
2. Click on the orange device name link.
3. The Appliance Settings page appears. The following figure shows the UI settings for the advanced console system.

NOTE: Available UI settings vary depending on the device type.

Figure 4.3 Appliance Settings



Serial Ports

□	Port	Device	Name	Profile	Target	Type	Signals	Settings	Action
□	1	ttyS1	FF-10	CAS	on	Serial Target	CTS|DSR|CD|RI	115200 8N1 Telnet/SSH DSView/Local Auto	▣
□	2	ttyS2	FF-11	CAS	on	Serial Target	CTS|DSR|CD|RI	115200 8N1 Telnet/SSH DSView/Local Auto	▣
□	3	ttyS3	FF-8	CAS	on	Serial Target	CTS|DSR|CD|RI	115200 8N1 Telnet/SSH DSView/Local Auto	▣
□	4	ttyS4	FF-9	CAS	on	Serial Target	CTS|DSR|CD|RI	115200 8N1 Telnet/SSH DSView/Local Auto	▣
□	5	ttyS5	tor17	CAS	on	Serial Target		115200 8N1 Telnet/SSH DSView/Local Auto	▣
□	6	ttyS6	tor18	CAS	on	Serial Target		115200 8N1 Telnet/SSH DSView/Local Auto	▣
□	7	ttyS7	tor19	CAS	on	Serial Target		115200 8N1 Telnet/SSH DSView/Local Auto	▣
□	8	ttyS8	tor20	CAS	on	Serial Target		115200 8N1 Telnet/SSH DSView/Local Auto	▣

NOTE: For the Vertiv™ Avocent® ACS8000 advanced console system, the following features are supported starting from specific firmware versions of the console system:

Table 4.10 Required Firmware Versions for Console System Features

Feature	Supported From Firmware Version
Non-blocking firmware update	v2.24.2
Non-blocking certificate	v2.24.1
Save and restore configuration	v2.29.3
Export file and diagnostic	v2.31.0

Saving and restoring a specific configuration

NOTE: This capability is available only for the Vertiv™ Avocent® ACS800/8000 advanced console system.

You can initiate a backup of the advanced console system’s current settings, choosing to save locally or to a remote server using a specified protocol. This is useful for preserving the exact state of a specific unit. You can also restore the settings from a previously saved configuration file, which helps quickly recover from incorrect configurations or device failures.

To save a configuration:

1. From the left-hand sidebar, click *Management – Devices*.
2. Locate the advanced console system devices from the list, and click the vertical ellipsis on the right-hand side of the row.
3. Click *Save Configuration*. The Save Configuration dialog box appears.
4. Choose the desired method for saving the configuration, either as a compressed file or a CLI script.
5. Select the file transfer method for the configuration file: Local File, SFTP, FTP, or SCP.

NOTE: If you chose CLI Script as the saving method, you also have the option to scrub the configuration of sensitive data. This option should only be enabled when generating a configuration file for third-party distribution, as it will remove key configuration elements.

6. Enter the required information for the transfer method.
7. Click *Save*.

To restore a configuration:

1. From the left-hand sidebar, click *Management – Devices*.
2. Locate the advanced console system devices from the list, and click the vertical ellipsis on the right-hand side of the row.
3. Click *Restore Configuration*. The Restore Configuration dialog box appears.
4. Select the file transfer method for the configuration file: Local File, SFTP, FTP, or SCP.
5. Enter the required information for the transfer method.
6. Click *Restore*.

Saving and applying a configuration template

NOTE: This capability is available only for the Vertiv™ Avocent® ACS800/8000 advanced console system.

You can create a reusable template of configuration settings for the advanced console system, which can then be applied to one or more console systems. This enables the streamlining of bulk configuration and ensures consistency across units. Templates are automatically saved to the Administration - File Management tab in the management platform.

For a list of settings that will be applied to the advanced console system via the configuration template, refer to Configuration Template Settings on page 85.

To save a configuration template:

1. From the left-hand sidebar, click *Management – Devices*.
2. Locate the device from the list whose configuration settings you'd like to create a template from, and click the vertical ellipsis on the right-hand side of the row.
3. Click *Save Configuration Template*.
4. Enter a name for the template.
5. (Optional) Enter a description for the template.
6. Click *Save*. After roughly one minute, the template will appear in the Administration - File Management tab.

To apply a configuration template:

1. From the left-hand sidebar, click *Management – Devices*.
2. Locate the device from the list that to which the template should be applied, and click the vertical ellipsis on the right-hand side of the row.
3. Click *Apply Configuration Template*. The Apply Configuration Template dialog box appears.
4. From the drop-down list, choose your desired template.
5. Click *Apply*.

4.5.2 High availability

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

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

This section covers the following topics for HA:

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

Prerequisites

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

- Must be the same appliance type. For example, if the primary node is a management platform hardware appliance, then you cannot add a standby node that is a management platform virtual appliance. All nodes must be either a hardware appliance or a virtual appliance.
- Must use the latest firmware version. To upgrade to the latest firmware, refer to Firmware on page 56.
- Must be configured with a static IP address. This is because if the node is configured with DHCP, it may receive a different IP address when restarted and become unavailable to the cluster. To configure a static IP address, refer to Ethernet interfaces on page 74.
- Must have the Network Time Protocol (NTP) enabled on the same NTP server to ensure the time settings are consistent for all nodes. If the time settings are not synchronized, the Vertiv™ Avocent® RM1048P Rack Managers that are enrolled on the management platform may not transition properly during failover.
- Must have a High Availability license uploaded on the primary node. The HA license specifies how many nodes are permitted on a single cluster, excluding the Primary node. You cannot add more nodes to a cluster than specified by the license. HA licenses can only be applied to the Primary node in a cluster; Standby and Maintenance nodes do not need their own independent licenses. During failover, the HA license is transferred to the new acting Primary node. While the HA license remains valid for the new Primary node, any future licenses being added to the system will need to use the new Primary node’s product lock code. To activate and add an HA license to the primary node, refer to License on page 66.
- Must have the High Availability Policy setting enabled to allow a Standby node to be added to the cluster. To enable the HA settings, refer to High availability on page 57.

Creating and configuring server redundancy

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

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

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

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

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

To create a cluster:

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

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

To add a node to the cluster:

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

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

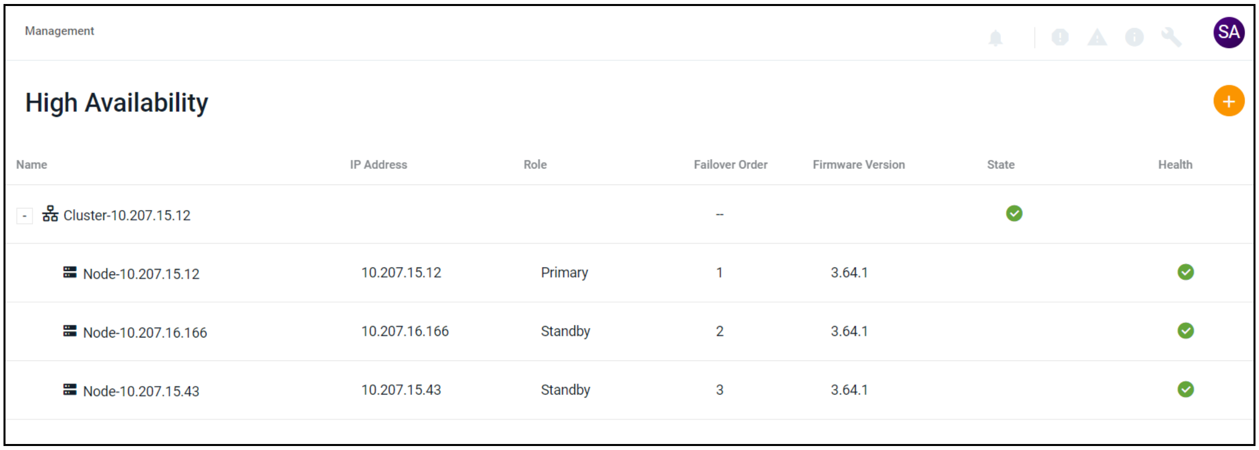
3. Check the Continue box, then click *Add Node*.
4. Enter the static IP address and admin credentials for the Standby node, then click *Add Node*.

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

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

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

Figure 4.4 Complete Cluster



High Availability

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

Accessing the HA cluster

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

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

Configuring and initiating failover

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

To configure the failover order:

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

To promote/demote a node:

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

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

Removing nodes and deleting the cluster

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

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

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

To remove a standby node from the cluster:

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

To delete a cluster:

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

Resetting a node

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

To reset a node:

1. Log into the management platform's CLI using your admin credentials.
2. When the Root Menu appears, enter **12** to select the Diagnostics option.
3. Enter **4** to restart a service on the node.
4. From the Restart Service list, locate the system-management option, then enter the associated number.
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.

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

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

     -or-

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

4.6 Administration

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

4.6.1 User management

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

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

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

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

Users

From the Users tab, you can view all users and user specific information for the Vertiv Avocent MP1000 Management Platform. You can also create and delete users and configure user password expiration settings.

To navigate the Users tab:

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

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

To add a new user:

1. From the *Users* tab, click the Add icon (+) in the top right corner. An Add User dialog box appears.
2. Enter the full name, user name and temporary password.

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

3. Click *Add User*.

To delete a user:

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

To configure a user's password expiration time:

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

Groups

From the Groups tab, you can view all groups for the Vertiv Avocent MP1000 Management Platform. A user group defines the view and what the user can do within the web UI and CLI, regarding appliance settings and administration. You can also create and delete user groups, assign target devices to groups and perform group mapping.

To navigate the Groups tab:

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

- Add or delete a user group.
- Open the group's information panel by clicking on the group. From the information panel, you can:
    - Expand *Group Properties* to view and configure the group name, preemption level and assigned system roles.
    - Expand *Users* to view and configure the assigned users.

- Expand *Resource Groups* to view and configure the assigned resource groups.
- Expand *External Groups* to view and configure the assigned external groups.

To add a user group:

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

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

To assign system roles to a user group:

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

NOTE: After adding the system role to the user group, you must define the resource group. To create a resource group, refer to Resource groups on page 23. Then, you must assign the user group to the desired resource group.

To assign a user group to a resource group:

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

To delete a user group:

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

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

4.6.2 Roles and permissions

From the Roles & Permissions screen, you can configure the roles and permissions of the targets and system.

A user permission authorizes a user to perform a specific operation on a target or system. A role is a collection of user permissions. There are four default system roles and two default target roles. For more information on the default roles, refer to System Roles on the facing page and Target Roles on the facing page.

For information on adding, deleting or editing roles and permissions for the management platform, refer to Configuring roles and permissions on page 48.

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 Groups on page 41.

User groups can be configured with one or more system roles. The system role permissions assigned to a user group are available for any user within the user group. For more information on user group configurations, refer to Groups on page 41.

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 23.

Table 4.11 on the next 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 4.11   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 Policy	✓	✗	✓	✗	✗	✗

Table 4.11 Roles and Permissions (continued)

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

Table 4.11 Roles and Permissions (continued)

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

Table 4.11 Roles and Permissions (continued)

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

Configuring roles and permissions

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

To add a new role:

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

   -or-

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

   -or-

   Check the Select All box to add all permissions.
6. Click *Add Role*.

To configure an existing role:

NOTE: The default roles cannot be configured.

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

To delete a role:

NOTE: The default roles cannot be deleted.

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

4.6.3 Credential profiles

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

From the Credential Profiles screen, you can view and create the credential profiles of your target devices. A credential profile stores the user ID and password for a single user and can be used across different target device types. Credential profiles are required for the following device types: Service Processors, Rack PDUs, Rack UPSes, DSView, and Virtual Machines. The type of credentials required for each device type are as follows:

- Rack PDU devices must use either Username/Password credentials or SNMPv1, v2, or v3 credentials.
- Rack UPS devices must use either SNMPv1 or v2 credentials.

- All other device types require Username/Password credentials.

Creating a credential profile

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

To create a credential profile with Username/Password credentials:

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

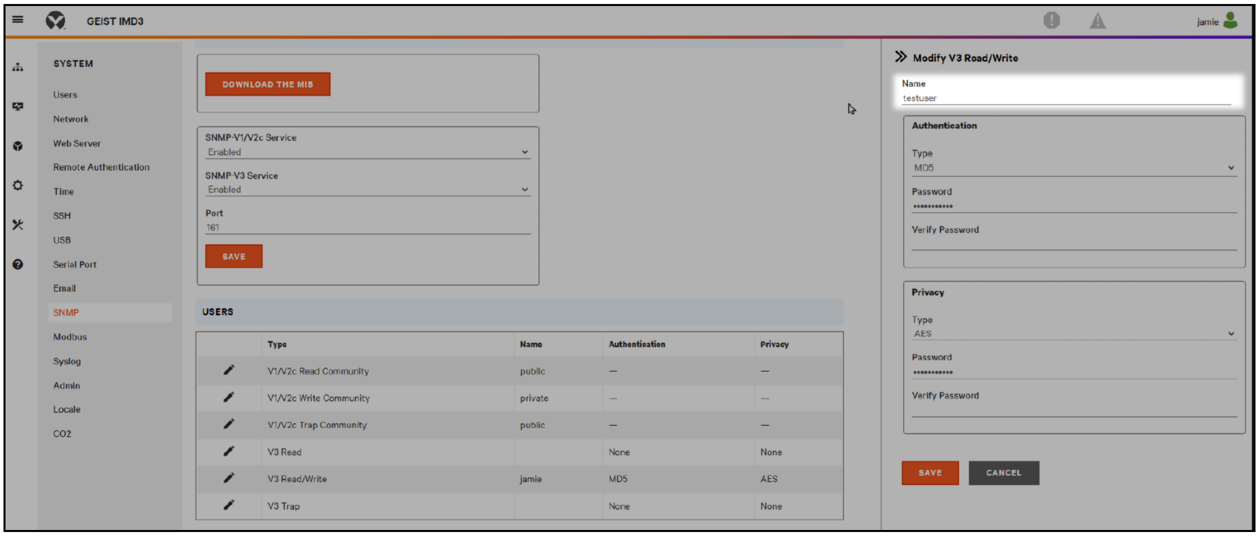
To create a credential profile with SNMPv1/v2 credentials:

1. From the left-hand sidebar, click *Administration - Credential Profiles*.
2. Click the Add icon (+) in the top right corner. An Add credential profile dialog box appears.
3. Enter a profile name.
4. From the Profile Type drop-down menu, click *SNMPv1/v2*.
5. Specify the version in the Version field: *SNMPv1* or *SNMPv2*.
6. Enter the port number.
7. Enter the read community.
8. (Optional) Enter the write community, trap community and any notes you wish.
9. In the Firmware Update Credentials section, enter the username and password.
10. Click *Add credential profile*.

To create a credential profile with SNMPv3 credentials:

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

Figure 4.5 Rack PDU Username Example



SNMP-V1/V2c Service: Enabled

SNMP-V3 Service: Enabled

Port: 161

USERS

Type	Name	Authentication	Privacy
V1/V2c Read Community	public	—	—
V1/V2c Write Community	private	—	—
V1/V2c Trap Community	public	—	—
V3 Read		None	None
V3 Read/Write	jamie	MD5	AES
V3 Trap		None	None

Modify V3 Read/Write

Name: testuser

Authentication

Type: MD5

Password: ••••••••••••

Verify Password:

Privacy

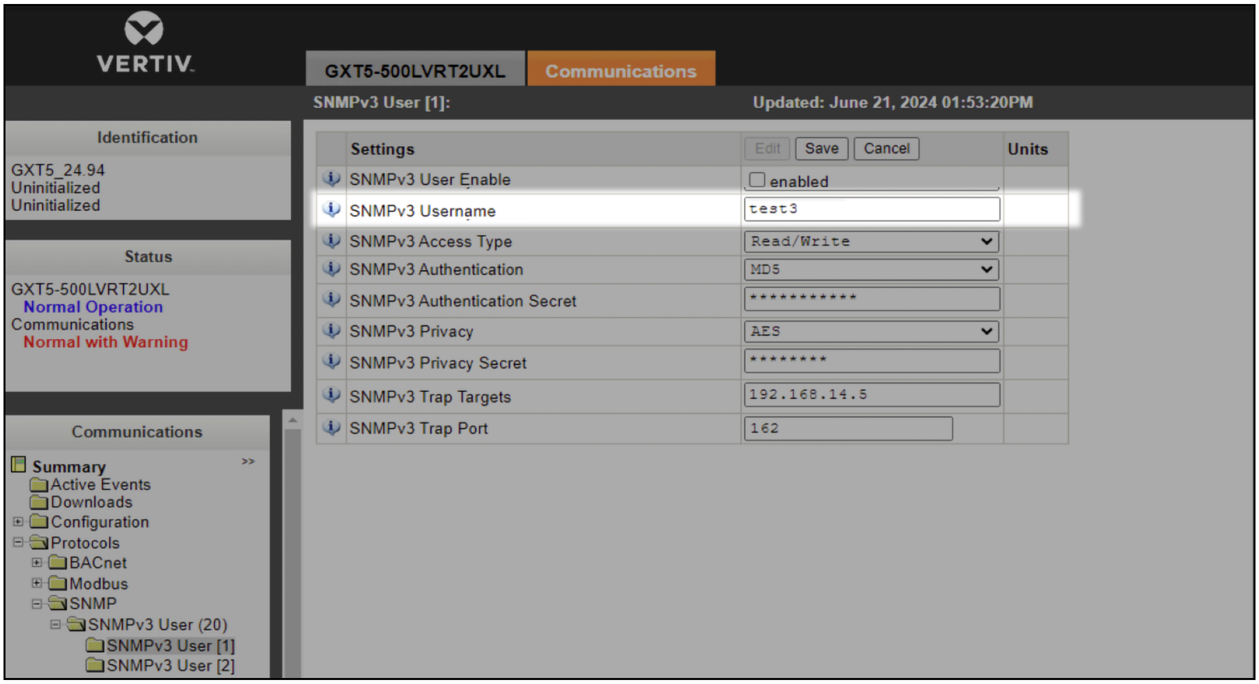
Type: AES

Password: ••••••••••••

Verify Password:

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

Figure 4.6 Rack UPS Username Example



SNMPv3 User [1]:

Updated: June 21, 2024 01:53:20PM

Identification: GXT5_24.94
Uninitialized
Uninitialized

Status: GXT5-500LVRT2UXL Normal Operation; Communications Normal with Warning

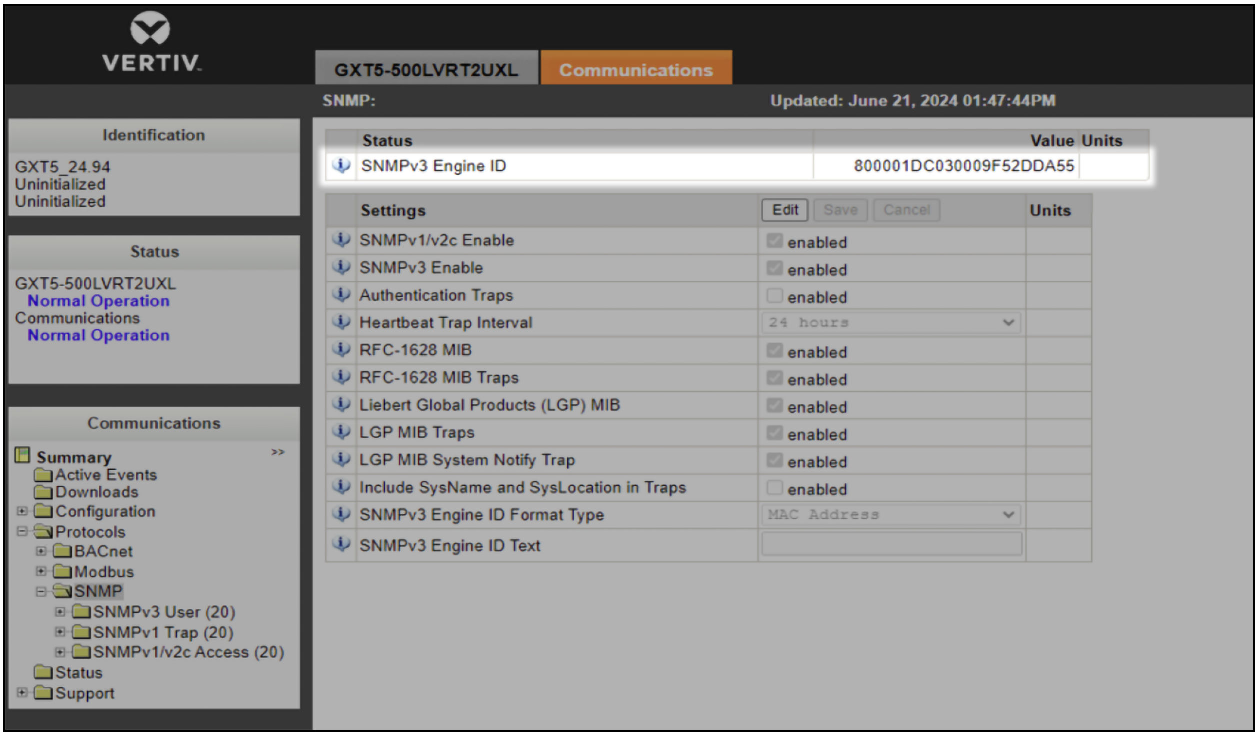
Settings		Units
SNMPv3 User Enable	□ enabled	
SNMPv3 Username	test3	
SNMPv3 Access Type	Read/Write	
SNMPv3 Authentication	MD5	
SNMPv3 Authentication Secret	***********	
SNMPv3 Privacy	AES	
SNMPv3 Privacy Secret	********	
SNMPv3 Trap Targets	192.168.14.5	
SNMPv3 Trap Port	162	

6. (Optional) Enter an engine identification number in the Engine ID field to create a unique credential profile for a single device. If the credential profile will be used for multiple devices, an engine ID is not needed.
   - For Vertiv™ PowerIT rPDUs, the engine ID follows this pattern: 80001F8803 + MAC address without including any colons in the MAC address. For example, if the device's MAC address is 00:19:85:0A:A8:17, then the engine ID is 80001F88030019850AA817.

- For Vertiv™ Liebert® rack UPSes, the engine ID follows this pattern: 800001DC03 + MAC address without including any colons in the MAC address. For example, if the device's MAC address is 00:02:99:2C:77:A8, then the engine ID is 800001DC030002992C77A8.

NOTE: The engine ID is configurable for the rack UPS device. For example, refer to Figure 4.7 below.

Figure 4.7 Rack UPS Engine ID Example



SNMP: Updated: June 21, 2024 01:47:44PM

Identification

GXT5_24.94
Uninitialized
Uninitialized

Status

GXT5-500LVRT2UXL
Normal Operation
Communications
Normal Operation

Communications

Summary >>
Active Events
Downloads
Configuration
Protocols
BACnet
Modbus
SNMP
SNMPv3 User (20)
SNMPv1 Trap (20)
SNMPv1/v2c Access (20)
Status
Support

Status	Value	Units
SNMPv3 Engine ID	800001DC030009F52DDA55	

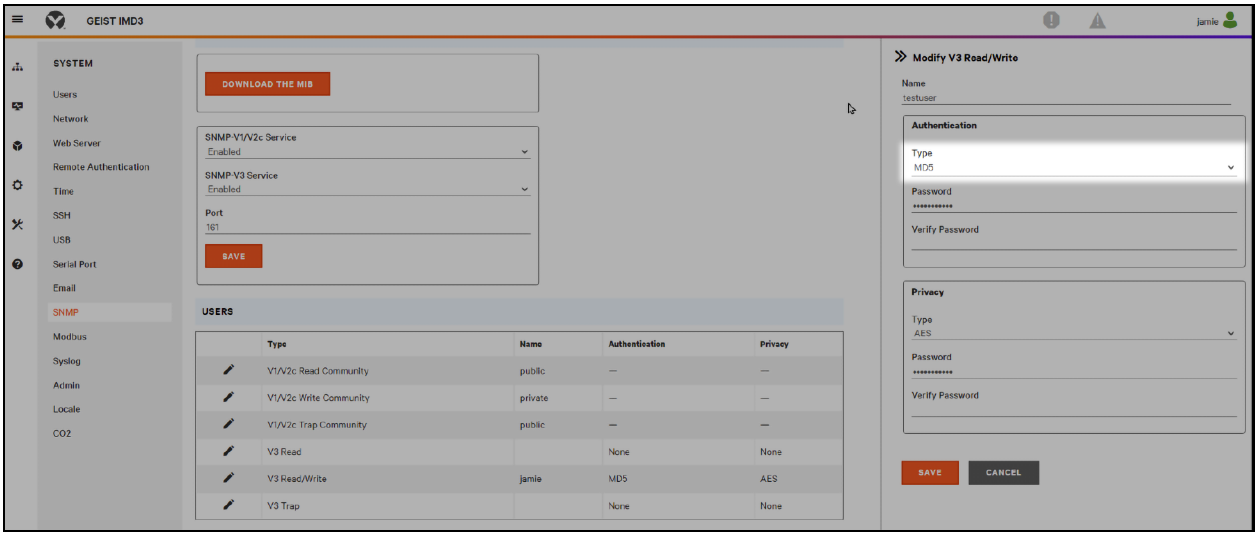
Settings	Edit Save Cancel	Units
SNMPv1/v2c Enable	☑ enabled	
SNMPv3 Enable	☑ enabled	
Authentication Traps	□ enabled	
Heartbeat Trap Interval	24 hours	
RFC-1628 MIB	☑ enabled	
RFC-1628 MIB Traps	☑ enabled	
Liebert Global Products (LGP) MIB	☑ enabled	
LGP MIB Traps	☑ enabled	
LGP MIB System Notify Trap	☑ enabled	
Include SysName and SysLocation in Traps	□ enabled	
SNMPv3 Engine ID Format Type	MAC Address	
SNMPv3 Engine ID Text		

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

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

NOTE: If an error occurs with authenticating the Vertiv™ PowerIT rPDU using the SHA1 cryptography hash function, it is recommended to configure the device with the MD5 cryptography hash function. For example, refer to Figure 4.8 on the next page.

Figure 4.8 MD5 Cryptography Hash Function Example



SNMP-V1/V2c Service: Enabled

SNMP-V3 Service: Enabled

Port: 161

USERS

	Type	Name	Authentication	Privacy
✎	V1/V2c Read Community	public	—	—
✎	V1/V2c Write Community	private	—	—
✎	V1/V2c Trap Community	public	—	—
✎	V3 Read		None	None
✎	V3 Read/Write	jamie	MD5	AES
✎	V3 Trap		None	None

Modify V3 Read/Write

Name: testuser

Authentication

Type: MD5

Password: •••••••••••

Verify Password

Privacy

Type: AES

Password: •••••••••••

Verify Password

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

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

NOTE: The management platform only supports top level zones. Sub-level zones are not supported.

To add a zone to the management platform:

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

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

8. (Optional) Add a note, if desired.
9. Click *Add credential profile*. The credential profile has been created and now must be discovered by the management platform. To discover the zone, refer to Discoveries on page 25.

4.6.4 Events

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

To navigate the Events screen:

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

- Search for a specific event using the search bar.
- Filter events by severity (*All Severities, Info, Warning* or *Critical*) using the Filters drop-down menu.
- Sort events in ascending or descending order by clicking the arrows next to each column.
- View the information panel for each event by clicking on the desired event.

NOTE: The maximum retention period for event data is 60 days. Events and related records can be stored for up to 60 days before being automatically deleted or purged from the system.

4.6.5 Alarms

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

To navigate the Alarms screen:

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

- Search and filter for a specific alarm alert by IP address or device name using the Search and Filter bar.
- Filter alarms:
  - By date using the calendar feature.
  - By device type using the All Device Type drop-down menu.
  - By alarm type using the All Alarm Type drop-down menu.
  - By severity (All Severities, Info, Warning or Critical) using the All Severities drop-down menu.

NOTE: The maximum retention period for alarm policy data is 60 days. Alarms and related records can be stored for up to 60 days before being automatically deleted or purged from the system.

To clear the alarms manually:

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

   -or-

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

4.6.6 Authentication providers

From the Authentication Providers screen, you can view the list of configured authentication providers. You can also add and enable a new provider, delete an existing provider, update the order of providers and configure role mapping for Active Directory. Providers can be authenticated locally or via AD/LDAP, TACACS+, or RADIUS. For the LDAP method, the 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.

Adding and configuring authentication providers

To add an authentication provider:

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

To enable an authentication provider:

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

To delete an authentication provider:

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

To update the providers order:

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

Setting up Single-Sign On

The management platform supports Single Sign-On (SSO). This feature allows you to authenticate once and gain access to multiple systems without needing to log in separately to each one.

NOTE: A management platform can only have one assigned SSO provider at a time.

NOTE: The user group names in the SSO provider must match the user group names as configured in the SSO provider in order for proper roles and permissions to be assigned.

To set up SSO:

1. From the left-hand sidebar, click *Administration – Authentication Provider.*
2. Click on the Add Authentication Provider (+) icon in the top right corner and click the *Single Sign-On (SSO)* option. The Add SSO Provider dialog box appears.
3. Enter the name, issuer URL, client ID, and client secret in the provided fields.

NOTE: You can obtain the issuer URL, client ID, and client secret from your SSO provider.

4. Click *Add Provider*.
5. After the provider has been added, test the connection to ensure it is successful.
    a. Click the vertical ellipsis on the right side of the row and click *Test*.
    b. The Test Authentication Provider dialog box appears. Click *Test*. The status of the test will appear in the lower text box.
6. After verifying the connection is successful, you must enable the SSO provider. Click the vertical ellipsis on the right side of the row and click *Enable*.
7. Once enabled, the login page will display the SSO option. At the login page, click *Single Sign-On (SSO)*, and log in with your SSO provider credentials.

Mapping local user groups

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

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

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

4.6.7 Firmware updates

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

For information on updating the firmware for target devices, refer to Performing maintenance activities on page 17.

4.6.8 System settings

From the System Settings screen, administrators can view and configure the system settings for the management platform. System settings include the following:

- Firmware
- Password policy
- High availability
- Lockout policy
- Timeout
- Date and time
- Events retention
- Alarms retention
- Viewer settings
- Standalone KVM viewer settings
- DSView unit group mapping

- License expiration notification
- FIPS module
- Proxy configuration
- Synchronization configuration
- Syslog destination
- Email server configuration
- Notification configuration
- SSH passthrough
- Certificate
- Inherited settings
- Custom fields
- Reboot appliance
- Factory reset

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

Firmware

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

To update the firmware from the System Settings screen:

1. From the sidebar of the System Settings screen, click *Firmware*.
2. Click *(Download Page)*. The Vertiv™ Avocent® MP1000 Software Downloads page opens in a new tab.
3. Download the latest firmware version for your appliance type (hardware or virtual).
4. Save the firmware to one of the following servers: local, TFTP, FTP, HTTP, SFTP, or SCP.

NOTE: The availability of update methods varies by device type. Refer to Table 4.3 on page 18 for more information.

5. Return to the *System Settings* screen of the web UI and click the *Update Firmware* button.
6. Select the firmware file and click *Update*.

Password policy

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

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

To configure the password policy:

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

High availability

If you have a High Availability license, you can create High Availability clusters with one primary and up to two standby nodes for server redundancy. Adding a node to a cluster is a protected operation that requires you to enable the explicit permission.

NOTE: It is strongly recommended to enable both the High Availability and Manual Role Control settings before adding a node to the cluster.

To enable the HA permissions for creating a cluster:

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

For more information about creating and configuring HA clusters, refer to High availability on page 36.

Lockout policy

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

To configure the lockout policy:

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

Timeout

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

To configure the inactivity timeout settings:

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

Date and time

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

NOTE: If the time on the rack manager and the management platform vary by more than a few seconds, the management platform will be unable to discover and manage the rack manager. It is recommended to configure both appliances with the same NTP server to establish a shared time setting and allow for proper discovery.

To configure the date and time settings:

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

   -or-

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

Events retention

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

To configure the events retention policy:

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

   -or-

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

   Click *Save*.

Alarms retention

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

To configure the alarms retention policy:

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

Viewer settings

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

To configure the inactivity timeout settings for the Video Viewer:

1. From the sidebar of the System Settings screen, click *Viewer Settings*.
2. Click the toggle button to enable or disable automatic log out from a viewer session after a set time of inactivity.

3. If enabled, enter the duration of time a user can be inactive before the viewer session times out and closes.
4. Click *Save*.

Standalone KVM viewer settings

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

To configure the standalone KVM viewer settings:

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

DSView unit group mapping

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

To enable group mapping for management software groups:

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

License expiration notification

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

To configure the license expiration notification:

1. From the sidebar of the System Settings screen, click *License Expiration Notification*.
2. In the Days field, enter the number of days you want to be notified in advance about the license expiry.
3. Click *Save*.

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

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

FIPS module

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

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

To enable FIPS mode:

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

Proxy configuration

You can configure a proxy server to access all KVM and serial session traffic through the management platform.

To enable proxy configuration:

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

Syslog destination

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

NOTE: The Audit Events page logs all user activities.

To set up Syslog Destination:

1. From the sidebar of the System Settings page, click *Syslog Destination*.
2. Click the plus icon (+) in the top right corner. The Add Syslog Destination dialog box appears.
3. Select the protocol from the Protocol drop-down menu.

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

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

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

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

Synchronization configuration

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

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

To prepare for device synchronization:

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

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

5. Click *Save*. Once saved, you can now synchronize your devices. For more information, refer to Synchronizing devices on page 19.

Email server configuration

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

To configure email server information:

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

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

Notification configuration

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

To configure email notifications:

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

2. Click the toggle button to enable or disable the system to send email notifications.
3. Click *Save*.

For information on configuring notification policies, refer to Notification policy on page 75.

SSH passthrough

You can launch a serial session without using a web browser by connecting to the target device through an SSH client. Supported target devices for SSH passthrough include:

- Vertiv™ Avocent® ACS800/8000 advanced console systems
- Vertiv™ Avocent® IPSL IP serial device
- Vertiv™ PowerIT PDUs
- Vertiv™ Liebert® rack UPSes
- Generic devices with SSH servers
- Service processors
- Target devices managed by the Vertiv™ Avocent® RM1048P Rack Manager

Prerequisites

The following prerequisites must be met to enable SSH passthrough:

- SSH passthrough is accessible only to administrator users; other user roles must be assigned the appropriate permissions to initiate an SSH session.
- External users need specific device permissions but do not require session permissions, as these settings are not available for external users in the management platform.
- Each target device must have a unique name. If multiple targets share a name, only the first matching device will be connected, and an error will occur for the remaining devices.

Enabling SSH passthrough

To enable or disable SSH passthrough:

1. From the sidebar of the System Setting screen, click *SSH Passthrough*.
2. Click the toggle button to enable or disable SSH passthrough.
3. Specify the SSH server port on the management platform to connect an SSH session. The default port is 4122. The following ports cannot be set as the SSH server port: 80, 443, 22220, 25, and 5432.
4. Click *Save*.

Using public/private key authentication

You can generate public/private key pairs and upload the public key for SSH passthrough sessions, allowing authentication to be performed without entering a password.

NOTE: Each user can upload and manage their own public keys. Additionally, administrators can upload keys for other users.

To upload your own public key:

1. From the top right-hand corner, click the profile icon and click *User Preferences*. The User Preferences page appears.

2. From the left-hand sidebar, click the *SSH Public Key* tab.
3. Click the *Update* button.
4. Upload your public key by either dragging and dropping the file or browsing for the file.
5. Click *Add*.

To upload a public key for another user (administrative capability):

1. From the left-hand sidebar, click *Administration – User Management*.
2. From the Users tab, click on the user account to open the side panel.
3. Click the Edit icon (the pencil) for the SSH Public Key.
4. Drag and drop your file into the box or browse for the file to upload your public key.
5. Click *Update SSH Public Key*. After uploading the key, basic information about the key will be displayed in the side panel, including the type and bit length.

To delete your own public key:

1. From the top right-hand corner, click the profile icon and click *User Preferences*. The User Preferences page appears.
2. From the left-hand sidebar, click the *SSH Public Key* tab.
3. Click the *Delete* button and confirm the selection.

To delete another user's public key (administrative capability):

1. From the left-hand sidebar, click *Administration – User Management*.
2. From the Users tab, click on the user account to open the side panel.
3. Click the Edit icon (the pencil) for the SSH Public Key.
4. Click *Delete SSH Public Key*.
5. The Delete SSH Public Key confirmation message appears. Click *Delete*.

Establishing an SSH connection

To establish an SSH connection via password authentication:

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

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

To establish an SSH connection via key authentication:

1. Open the SSH client.
2. Using the following format, enter the command to establish an SSH connection: **ssh -t** <appliance.IP> **-l "**<username>**:**<target device name>**" -p** <ssh server port>**-i**<path_to_key>
   - appliance.IP - The IP address of the management platform.
   - username - The username for the management platform.
   - target device name - The name of the target device to which you wish to establish an SSH connection.
   - ssh server port - The port number specified when SSH passthrough was enabled on the System Settings screen of the management platform web UI.
   - path_to_key – The path to the private key configured for key-based authentication. Omit if you are not using key-based authentication.

Certificate

You can generate and install new certificate signing requests (CSRs), as well as download the certificate currently installed on the appliance.

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

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

To generate a new CSR:

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

To install a CA-signed certificate:

1. From the sidebar of the System Settings screen, click *Certificate*.
2. Click the Install Certificate icon in the right corner.
3. Browse to and select the .pem file assigned by a CA (Certificate Authority) with base64 PEM.
4. Click *Upload*.

To download the currently installed certificate:

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

Inherited settings

You can enable Inherited Permissions on your target devices or groups, which will automatically assign permissions from parent groups to child groups or devices. For more information about inherited permissions, refer to Enabling inherited permissions on page 24.

Custom fields

You can add custom fields, which are unique, user-defined data fields, to the management platform to store additional information that is not covered by the default fields. Custom fields are particularly useful for configuring the appliance to meet specific organizational needs.

To add a custom field:

1. From the left-hand sidebar, click *Administration – Systems Settings*.
2. Click the *Custom Field Labels* tab.
3. Click the Add Custom Field icon (+) in the top right corner. The Add Custom Field dialog box appears.
4. Enter the display label for the custom field.
5. Click the Status toggle button to enable the custom field.
6. Click *Add*.

Custom field values for specific devices can be modified.

To edit custom fields for specific devices:

1. From the left-hand sidebar, click *Targets – Appliance View* or *Targets – Targets List*.
2. Click on the desired device. The device's information panel opens.
3. Click on the Edit icon (the pencil) for the Custom Fields menu.
4. Edit the values as needed.
5. Click *Save*.

Additionally, custom fields associated with devices can be configured to be displayed as columns in the Targets – Appliance View or Targets – Targets List page.

To add a Custom Fields column to the target device list:

1. From the left-hand sidebar, click *Targets – Appliance View* or *Targets – Targets List*.
2. Above the list of target devices, click the vertical ellipsis and click *Table Configuration*.
3. Check the box for Custom Fields.
4. Click *Done*.

Reboot appliance

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

To reboot the appliance:

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

Factory reset

Resetting the firmware of the management can be useful in various scenarios, such as troubleshooting, re-purposing the device, or preparing it for a new user. You can reset your management platform by one of three options: clearing the current firmware image, restoring the previous firmware image, or restoring factory settings. You can also choose to preserve the current network settings during the reset, if desired.

To perform a factory reset:

1. From the sidebar of the System Settings screen, click on the *Factory Reset* tab.
2. Click the orange *Factory Reset* button. The Factory Reset dialog box appears.
3. If you wish to retain your current network settings, click the Preserve Network Settings radio button.

   -or-

   If you wish to delete all current configuration settings and files, click the Reset All radio button.
4. Under the Firmware Image heading, select the radio button for the firmware image that will be restored or retained.
   - Retain Current: If selected, this option clears all data on the current firmware image.
   - Restore Previous: If selected, this option restores the firmware image that was previously running on the appliance. If the firmware has not yet been updated to a new version, then this option will be grayed out.
   - Restore Factory: If selected, this option clears all data and restores the factory firmware image.
5. Click *Continue*. A confirmation page appears.
6. Review your selections and click *Yes, Reset*. The system will reboot, and your changes will be reflected.

4.6.9 Scheduler

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

4.6.10 License

From the License screen, you can view the total number of licenses used, total number of targets managed, and the license expiration date. Additionally, you can add and delete licenses from this screen.

NOTE: To view and configure licensing, user accounts must be set up as either a System Administrator Role or System Maintainer Role. For more information, refer to Roles and permissions on page 42.

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

Activating and adding licenses

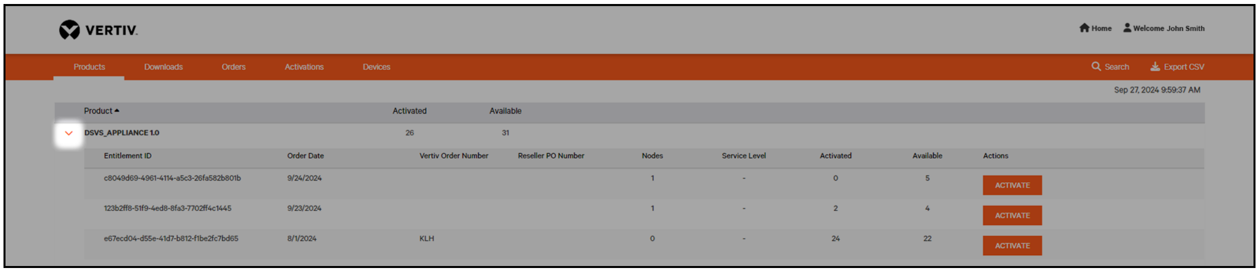
NOTE: The Appliance license must be uploaded to the management platform first.

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

To activate and add a license:

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

Figure 4.9 License List



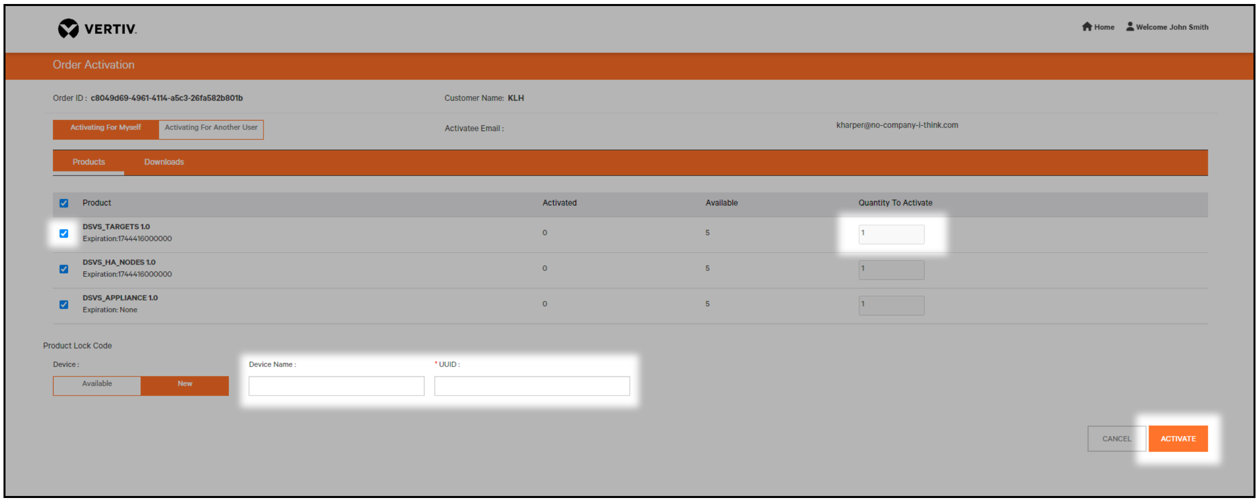
Sep 27, 2024 9:59:37 AM

Product ▲	Activated	Available
DSVS_APPLIANCE 1.0	26	31

Entitlement ID	Order Date	Vertiv Order Number	Reseller PO Number	Nodes	Service Level	Activated	Available	Actions
c8049d69-4961-4114-a5c3-26fa582b801b	9/24/2024			1	-	0	5	ACTIVATE
123b2ff8-51f9-4ed8-8fa3-7702ff4c1445	9/23/2024			1	-	2	4	ACTIVATE
e67ecd04-d55e-41d7-b812-f1be2fc7bd65	8/1/2024	KLH		0	-	24	22	ACTIVATE

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

Figure 4.10 Order Activation Screen



Order ID : c8049d69-4961-4114-a5c3-26fa582b801b

Customer Name: KLH

Activatee Email : kharper@no-company-i-think.com

☑	Product	Activated	Available	Quantity To Activate
☑	DSVS_TARGETS 1.0 Expiration:1744416000000	0	5	1
☑	DSVS_HA_NODES 1.0 Expiration:1744416000000	0	5	1
☑	DSVS_APPLIANCE 1.0 Expiration: None	0	5	1

Product Lock Code

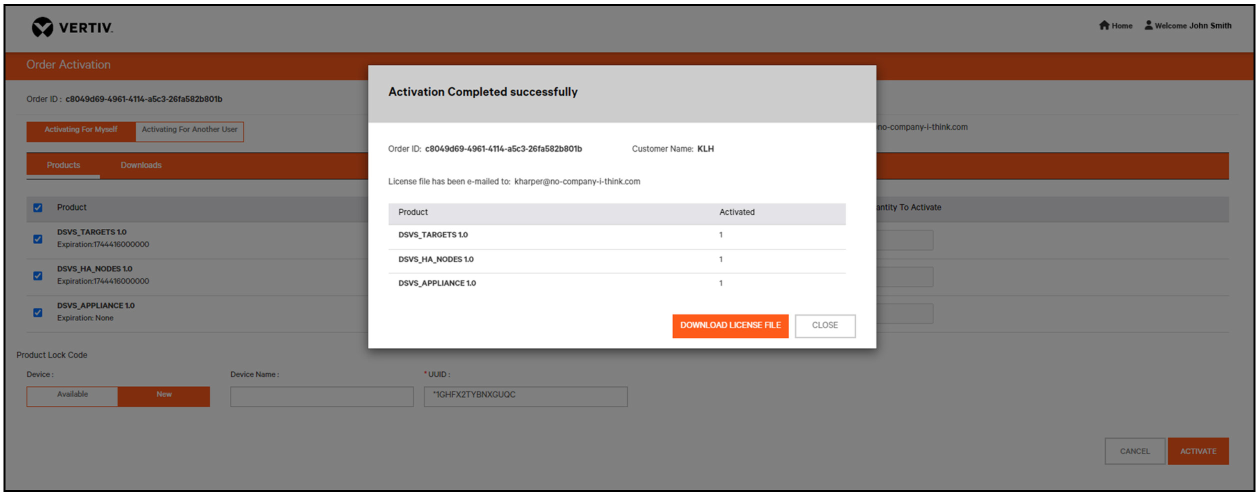
Device :

Device Name :

* UUID :

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

Figure 4.11 Activation Completed Successfully



Order ID : c8049d69-4961-4114-a5c3-26fa582b801b

no-company-i-think.com

☑ DSVS_TARGETS 1.0 Expiration:1744416000000

☑ DSVS_HA_NODES 1.0 Expiration:1744416000000

☑ DSVS_APPLIANCE 1.0 Expiration: None

UUID: *1GHFX2TYBNXGUQC

Activation Completed successfully

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

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

Product	Activated
DSVS_TARGETS 1.0	1
DSVS_HA_NODES 1.0	1
DSVS_APPLIANCE 1.0	1

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

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

14. Open the License File in a text editor, such as Notepad, and copy the contents of the file.
15. Return to the management platform web UI to upload the license.
16. In the Add License dialog box, paste the contents of the License File into the provided text box.
17. Click *Submit*. The license is now uploaded. Repeat this procedure for all licenses that need to be activated and added to your appliance.

Deleting licenses

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

To delete a license:

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

4.6.11 IP pool

From the IP Pool screen, you can allocate and manage IP addresses for targets managed by a rack manager from a centralized location. This feature streamlines network configuration, especially for larger deployments, by allowing administrators to create, assign, and manage IP address pools from a single interface. The key features available from this page include:

- Create and manage IP pools directly on the management platform, eliminating the need to configure pools individually on each rack manager.

- Assign a single IP pool to multiple rack managers, or designating different pools for different sets of rack managers to suit your network architecture.
- Open a target's web interface directly from the management platform through NAT-based access.
- Reduce manual setup and repetitive tasks through the automatic distribution of IP pools configured on the management platform to rack managers in Managed mode.

NOTE: It is recommended to keep a record of pool configurations and associations for troubleshooting and future reference.

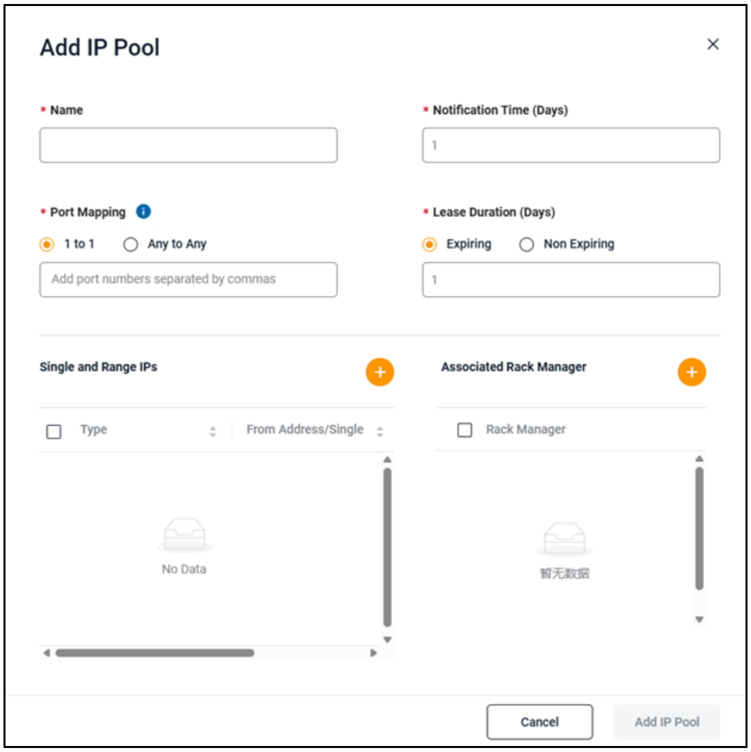
NOTE: In standalone mode, IP pools are configured on individual rack manager devices. In managed mode, all IP management is performed via the management platform.

Creating an IP pool

To create an IP pool:

1. From the left-hand sidebar, click *Administration – IP Pools*.
2. Click the Add IP Pool (+) icon in the top right corner. The Add IP Pool dialog box appears.

Figure 4.12 Add IP Pool



Add IP Pool

* Name:

* Notification Time (Days): 1

* Port Mapping: ● 1 to 1 ○ Any to Any

Add port numbers separated by commas

* Lease Duration (Days): ● Expiring ○ Non Expiring

1

Single and Range IPs

□	Type	From Address/Single

No Data

Associated Rack Manager

□	Rack Manager

暂无数据

3. Fill out the fields accordingly:
   a. Name: Enter a unique name for your IP pool.
   b. Notification Time (Days): Specify the number of days before lease expiration when notification should be sent.
   c. Port Mapping:

- Choose 1 to 1 to map a single source IP address to a single destination IP address for specific ports only. You must specify one or more port numbers, separated by commas. Traffic will be permitted only on the specified ports.

-or-

- Choose Any to Any to map one IP address to target device's IP address without port restrictions. The port input is disabled for this option because all ports are implicitly open.

d. Lease Duration (Days):

- Choose Expiring and enter the number of days for the lease duration.

-or-

- Choose Non Expiring if you do not want the lease to expire.

4. In the Single and Range IPs section:
   a. Click the orange plus (+) button.
   b. Enter the individual IP addresses or specify a range as needed. The added IP addresses will appear in the list below.
5. In the Associated Rack Manager section:
   a. Click the orange plus (+) button.
   b. Select one or more rack managers to associate with this IP pool. The selected rack managers will appear in the list below.
6. Click *Add IP Pool* to save and create the new pool.
7. After creating the IP pool, verify that the associated IP addresses and rack managers are correctly listed. You can edit or delete the pool later if changes are needed.

Retrieving external IP addresses

Upon defining an IP pool for targets managed by a rack manager, you must retrieve the target's external IP address from the Appliance View or Targets List page.

To retrieve the external IP address for a target device:

1. From the left-hand sidebar, click *Administration – Appliance View* or *Administration – Targets List*.
2. Click on the vertical ellipsis for the target or click on the target's row to open the side panel.
3. Click *Retrieve External IP*.
4. After successful retrieval, the globe icon becomes click-able and you can open to the target's web page. You can also view the NAT rules from the IP Pool screen.

After allowing sufficient time and refreshing the UI, you can view the retrieved IP address from the target's side panel. Navigate to the *Appliance View* screen, click on the respective target to open its side panel, and expand the Network Configuration section. This section will contain the external IP address assigned to the target, the mapped port, and the lease time in days.

Opening a target's web page

After you've retrieved a target's external IP address, you can directly access its web page from the Appliance View or Targets List page.

To open a target's web page:

1. From the left-hand sidebar, click *Administration – Appliance View* or *Administration – Targets List*.
2. Click on the vertical ellipsis for the target or click on the target's row to open the side panel.
3. Click the globe icon to open the web page in a new tab.

Viewing NAT rules

After you've retrieved a target's external IP address, you can view the NAT rules from the IP Pool page.

To view NAT rules:

1. From the left-hand sidebar, click *Administration – IP Pools*.
2. Click on the orange link of the IP pool name. The settings of the IP pool appear.
3. Scroll down to the Usage section.

NOTE: Upon lease expiration, NAT rules are deleted automatically.

Managing IP leases

You can manage your IP leases by either releasing external IP addresses or renewing the leases.

Releasing the external IP removes the assigned external IP address from the target and returns it to the IP pool for reuse. When this action is performed, the NAT rule associated with that IP is deleted, the target no longer has external access to its web page through that IP, and the IP becomes available for other targets in the same pool.

To release an external IP address:

1. From the left-hand sidebar, click *Administration – Appliance View* or *Administration – Targets List*.
2. Click on the vertical ellipsis for the target or click on the target's row to open the side panel.
3. Click *Release External IP*.

When an external IP address's lease is close to expiring, you can renew the lease to keep the same IP assigned to the target without interruption. This prevents the address from being automatically released and the NAT rules from being deleted.

To renew an external IP address's lease:

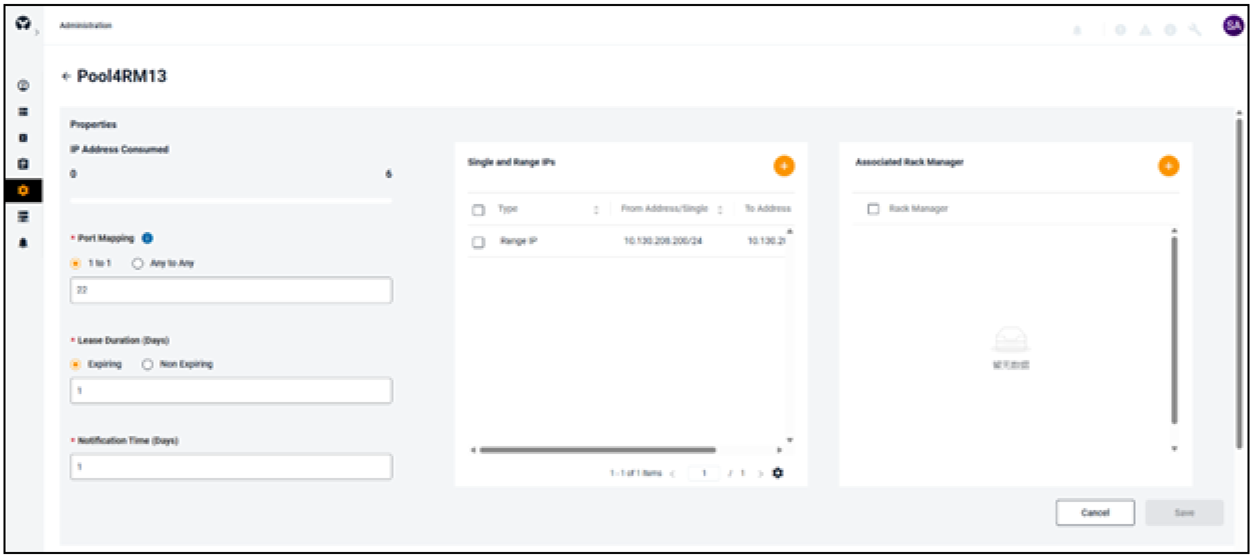
1. From the left-hand sidebar, click *Administration – Appliance View* or *Administration – Targets List*.
2. Click on the vertical ellipsis for the target or click on the target's row to open the side panel.
3. Click *Renew Lease*.

Editing an IP pool

To edit an IP pool:

1. From the left-hand sidebar, click *Administration – IP Pools*.
2. Click on the orange link of the IP pool name. The settings of the IP pool appear.

Figure 4.13 Edit IP Pools



Pool4RM13

Properties

IP Address Consumed

0 6

* Port Mapping

● 1 to 1 ○ Any to Any

22

* Lease Duration (Days)

● Expiring ○ Non Expiring

1

* Notification Time (Days)

1

Single and Range IPs

□	Type	From Address/Single	To Address
□	Range IP	10.130.208.200/24	10.130.2

1 - 1 of 1 items 1 / 1

Associated Rack Manager

□ Rack Manager

3. Edit the settings as needed and click *Save*.

Adding or removing rack manager associations

After configuring an IP pool, you can add or remove an associated rack manager as needed.

NOTE: If the rack manager is unenrolled from the management platform entirely, then all associated configurations, including associations and NAT rules, will be automatically cleared. For more information about deleting target devices, refer to Adding and deleting devices on page 15.

To add a new rack manager association to an IP pool:

1. From the left-hand sidebar, click *Administration – IP Pools*.
2. Click on the orange link of the IP pool name. The settings of the IP pool appear.
3. In the Associated Rack Manager section, click the orange plus (+) icon. The Add Rack Manager dialog box appears.
4. Choose the desired rack manager(s) from the list that you wish to associated with the IP pool.
5. Click *Add*.
6. Click *Save*.

To remove an existing rack manager association from an IP pool:

NOTE: Associated rack managers with active IP addresses cannot be removed. The associated IP addresses must first be released from the Targets List page. For more information, refer to Managing IP leases on the previous page.

1. From the left-hand sidebar, click *Administration – IP Pools*.
2. Click on the orange link of the IP pool name. The settings of the IP pool appear.
3. In the Associated Rack Manager section, check the box on the left-hand side for the rack manager(s) you wish to remove.
4. Click the Delete icon (the trash can) that appears above the list.
5. Confirm deletion and click *Save*.

Deleting an IP pool

NOTE: IP pools with active IP addresses cannot be deleted. The IP address must first be released from the Targets List page. For more information, refer to Managing IP leases on page 71.

To delete an IP pool:

1. From the left-hand sidebar, click *Administration – IP Pools*.
2. Click the check box on the left-hand side of the IP pool you wish to delete.
3. Click the Delete icon (the trash can).

4.6.12 File management

From the File Management screen, you can view the log of configuration templates created for the Vertiv™ Avocent® ACS800/8000 advanced console system devices. For more information, refer to Saving and applying a configuration template on page 36.

4.7 Network Configuration

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

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

4.7.1 Network settings

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

To configure the network settings:

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

4.7.2 Normal/Failover-bonded settings

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

The management platform hardware appliance has two physical network interface ports. You can configure these ports for bonding and/or failover.

To configure failover for the network interface ports:

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

1. From the sidebar of the Settings screen, click *Normal/Failover-Bonded Settings*.
2. Using the Uplinks drop-down menu, select either *Ports not bonded*, *1st and 2nd ports bonded* or *1st fails over to 2nd port*.

3. A message appears, prompting you to confirm your selection. Click *Yes, Update*. To determine when failover is initiated, refer to Failover-routed IPv4 trigger mode below.

4.7.3 Failover-routed IPv4 trigger mode

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

To configure the trigger mode for failover:

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

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

4.7.4 Ethernet interfaces

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

To configure a static IP address:

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

Adding multi-Ethernet support

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

When adding a second Ethernet interface to the virtual appliance, you must ensure the route metric is correctly set for each interface. By default, the route metric sets to 200 for each interface to provide equal weighting to routing. The default setting is suitable only if all targets are reachable from all interfaces.

However, if some targets are on different network segments or following different routing rules per interface, then the route metric must be increased for the private or segmented networks. This ensures the primary network (with the lowest metric) is used for clients, ancillary services such as SMTP or Active Directory, and so on. All other Ethernet interfaces, with higher route metrics, are used for their respective subnets.

To set the route metric, refer to the Vertiv™ Avocent® DSView™ Updating Ethernet Interface Route Metric Tech Note, which can be found on the management platform product page at www.vertiv.com.

4.8 Notification Settings

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

4.8.1 Notification policy

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

To create a notification policy:

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

This page intentionally left blank

Appendices

Appendix A: Technical Support and Contacts

A.1 Technical Support/Service in the United States

Vertiv Avocent IT Management Software and Hardware Support Contacts

Phone: 1-888-793-8763

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

Email: support.avocent@vertiv.com

A.2 Locations

United States

Vertiv Headquarters

505 N Cleveland Ave

Westerville, OH 43082

Europe

Via Leonardo Da Vinci 8 Zona Industriale Tognana

35028 Piove Di Sacco (PD) Italy

Asia

7/F, Dah Sing Financial Centre

3108 Gloucester Road, Wanchai

Hong Kong

This page intentionally left blank

Appendix B: Technical Specifications

Table B.1 Technical Specifications - Avocent MP1000 Management Platform

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

This page intentionally left blank

Appendix C: Backup and Restore

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

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

C.1 Limitations and Notes

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

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

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

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

To configure the SMB host server:

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

To create an on demand backup:

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

   -or-

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

C.3 Configuring the Retention Policy

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

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

   -or-

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

2. Enter **1** to select the Configure option.
3. Enter **1** to select the Change Retention Policy option.
4. Enter the number of backups you wish to retain. You can retain a maximum of five backups locally. The Backups Retained line updates and reflects the number of backups being retained.

C.4 Configuring a Schedule for Backup Automation

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

   -or-

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

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

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

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

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

C.5 Viewing a List of All Backups

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

   -or-

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

2. Enter **2** to select the List option.

C.6 Deleting a Backup

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

   -or-

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

2. Enter **4** to select the Delete Backup option. An index of existing backups appears.
3. Enter the appropriate number for the backup you wish to delete.
4. Enter **yes** to delete the selected backup. The backup has been deleted.

C.7 Restoring a Previous Backup Configuration

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

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

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

   -or-

   Enter **2** for the SMB option if you wish to backup the management platform remotely.
2. Enter **5** to select the Restore option. An index of deleted backups appears.
3. Enter the appropriate number for the backup you wish to restore.
4. Enter **yes** to reboot the management platform. Once the system comes back online, the backup has been successfully restored.

This page intentionally left blank

Appendix D: Configuration Template Settings

The following settings will be applied to the Vertiv™ Avocent® ACS8000 advanced console system via the configuration template:

- System Security Profile
- Ports CAS Profile Auto Discovery
- Ports Dial-In Profile Settings
- System Date and Time
  - Date and Time
  - Time Zone
- Network
  - IPSec (VPN)
  - SNMP
  - Firewall IPv4 Filter Table
- Serial Ports
  - CAS/Physical
- Authentication
  - Appliance Authentication
  - Authentication Servers (except for the Vertiv™ Avocent® DSView™ management software)
    - RADIUS
    - TACACS+
    - LDAP(S) | AD
    - Kerberos
    - Duo
- Users
  - Local Accounts
  - Authorization
- Events and Logs
  - Event List
  - Event Destinations (except for the Vertiv™ Avocent® DSView™ management software)
  - Trap Forward
  - Data Buffering
  - Appliance Logging
- Power Management
  - Network PDUs
  - Network UPS

- Internal Appliance Sensors
- Monitoring
  - Scheduled Tasks

Connect with Vertiv on Social Media

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

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

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

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

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