



Avocent® Matrix Manager Software

Installer/User Guide

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. For additional assistance, visit <https://www.VertivCo.com/en-us/support/>

TABLE OF CONTENTS

1 Product Overview	1
1.1 Features and Benefits	1
1.1.1 Multiple cascaded systems management	1
1.1.2 Network troubleshooting	1
1.1.3 Web-based access and control	1
1.1.4 Secure authentication and communication	1
1.1.5 Group management	1
1.1.6 External Application Program Interfaces (APIs)	1
1.1.7 Auto failover	2
1.2 Basic System Configuration	2
2 Installation and Setup	3
2.1 System Minimum Requirements	3
2.1.1 PostgreSQL database configuration	3
2.1.2 Installation prerequisites	3
2.2 Microsoft Windows Installation	3
2.3 Red Hat Linux Installation	4
2.4 License Activation	4
2.5 Launching the Dashboard	6
2.6 Understanding the Information Flow	8
2.6.1 Matrix Manager software information chain	8
2.7 Setting up Your System	9
2.7.1 Adding devices to the system	10
2.7.2 Creating device groups	11
2.7.3 Creating roles for device groups	12
2.8 Next Steps	12
3 Administration, Access and Monitoring	13
3.1 Customizing Basic Matrix Manager Software Settings	13
3.2 Using Matrix Manager Software Online Help	13
3.3 Configuring Password Settings	13
3.4 Scheduling Backups and Firmware Upgrades	14
3.5 Streamlined Operations	14
3.5.1 Using third-party authentication	15
3.5.2 Using an external API	16
3.6 Monitoring Activities	16
3.6.1 Using notifications	17
3.6.2 Scheduling event tasks	18
4 Expanding Your System	21
4.1 User Operations	21
4.1.1 Using user OSD profiles	23
4.2 Device Operations	23
4.2.1 General device settings	24
4.2.2 General device activities	24
4.2.3 Customizing device properties	25
4.2.4 Managing device sessions	25
4.3 Managing Extended Display Identification Data (EDID)	26
5 Advanced Operations	29
5.1 Macro Operations	29

5.1.1 Using switched presets macros	29
5.1.2 Using follow the leader macros	29
5.1.3 Using multi-video macros	29
5.2 High Availability Operations	30
5.2.1 Using a peer manager for your system	30
5.2.2 Using a peer switch	31
5.3 External KVM	31
5.3.1 External KVM users	32
5.3.2 KVM device bridge	33
6 Appendices	35
6.1 Appendix A: External KVM Best Practices	37
6.1.1 AMWorks™ software recommendations	37
6.1.2 AMX™ switching system recommendations	37
6.1.3 Matrix Manager software recommendations	37

1 PRODUCT OVERVIEW

The Vertiv™ Avocent® Matrix Manager software is a secure, web browser-based, centralized enterprise management solution that provides remote management and monitoring of multiple Vertiv™ Avocent Matrix High Performance KVM switching systems. The Matrix switching system is the next generation of Vertiv keyboard, video and mouse (KVM) products that provides a high-performance, reliable desktop extension experience and offers a way to migrate to a digital solution while leveraging existing infrastructure. In a typical scenario, the Matrix switching system connects numerous transmitters and receivers in a matrix fashion to communicate through the proprietary central switch or a network of switches.

As you expand and cascade your Matrix switching systems, the Matrix Manager software provides a streamlined user interface for administration activities and serves as a connection broker to manage, authenticate and authorize sessions between your receivers and transmitters in the Matrix system. The Matrix Manager software links users to computers across the matrix to connect video, USB peripherals and audio from a target computer to a receiver where users can then operate as if the computer is directly connected to their own monitors, USB peripherals and speakers. The software then handles all administration, access control, monitoring and firmware upgrades across the Matrix switching system.

NOTE: For more information on the Matrix switching system, see the Vertiv™ Avocent® Matrix High Performance KVM Switching System Installer/User Guide.

1.1 Features and Benefits

1.1.1 Multiple cascaded systems management

Multiple Matrix High Performance KVM switches can be interconnected to create a cascaded switching system that is capable of supporting more receivers and transmitters. Within each cascaded system, one switch is configured as a master and the remaining switches are configured as slaves. The purpose of the Matrix Manager software is to communicate to each system component through the master switch. For instructions to cascade your Matrix switches, see the Vertiv™ Avocent® Matrix High Performance KVM Switching System Installer/User Guide.

1.1.2 Network troubleshooting

The Matrix Manager software uses industry standard IP connections so you can easily troubleshoot issues within the system from the Network Operations Center (NOC), from any location in the world. With the Matrix Manager software, you can access all of your devices from a single screen.

1.1.3 Web-based access and control

As a web browser-based management solution, the Matrix Manager software provides a centralized secure database for storing user, device, configuration and system information, allowing administrators to organize, add, configure, remove, and delete managed devices and users. It also enables authentication, access control and monitoring of any target computers.

1.1.4 Secure authentication and communication

The Secure Sockets Layer (SSL) over a TCP/IP connection encrypts Matrix Manager software data. Users are authenticated using the Matrix Manager software internal database and/or one of the external authentication methods available such as Active Directory. See [Administration, Access and Monitoring](#) on page 13 for more information.

1.1.5 Group management

The Matrix Manager software streamlines processes across large Matrix switching systems by allowing administrators to designate permissions, assign access/control rights and schedule tasks via groups. Through creation of user groups and device groups, an administrator assigns roles to each, which then designates all aspects of access to the system. This creates an additional seamless layer of security across the switching system.

1.1.6 External Application Program Interfaces (APIs)

The Matrix Manager software eases device data integration through a REpresentational State Transfer (REST) Web Service API and a Telnet API. The external API service handles certain core functionality and provides transparent cacheability that leads to increased performance, reduced server load and statelessness on the server, making failover easy. See [Administration, Access and Monitoring](#) on page 13 for more information.

1.1.7 Auto failover

The more complex your Matrix switching system is, the more critical it is to ensure that the Matrix Manager software is functional and protected from a system failure. The Matrix Manager software provides access to a high availability backup Matrix Manager software system (known as a peer manager) to keep the system protected and running. The Matrix switch provides the ability to designate and configure a slave switch as the backup controller for the cascade. See [Advanced Operations](#) on page 29 for more information.

1.2 Basic System Configuration

The following figure shows an example system configuration using the Matrix Manager software. Descriptions are listed in [Example System with Software Descriptions](#) on page 2.

Figure 1.1 Example Matrix Switching System with Matrix Manager Software

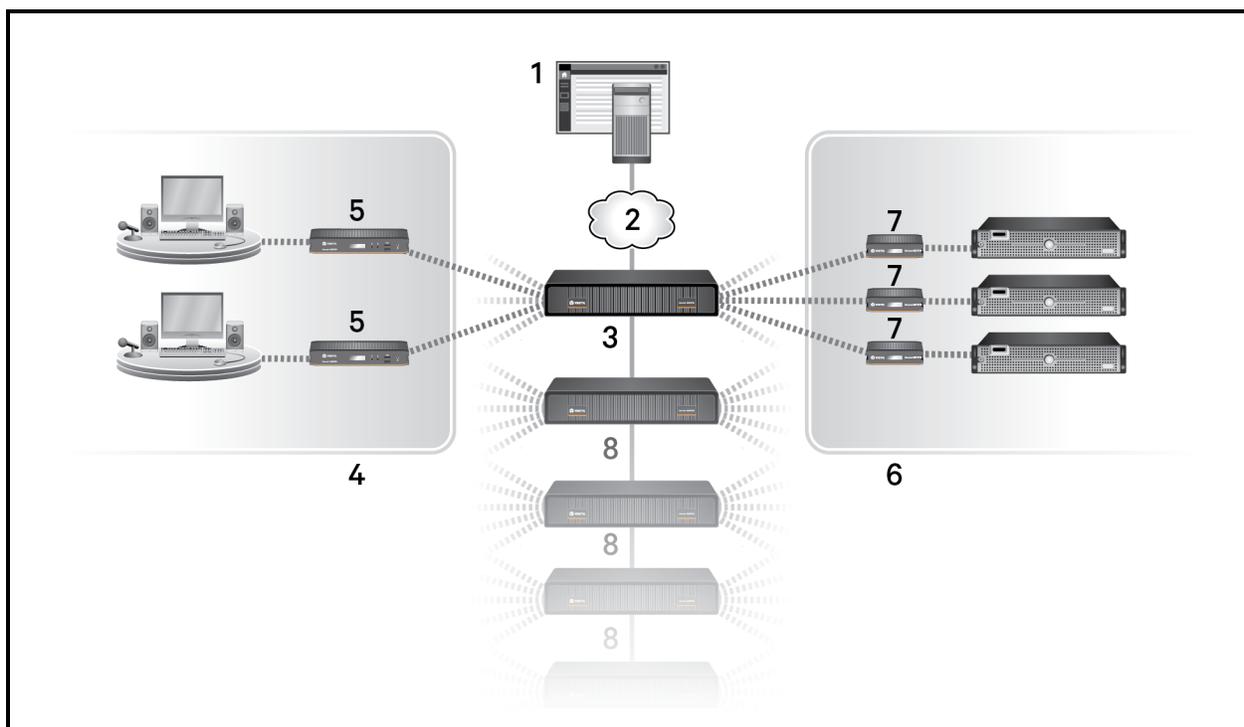


Table 1.1 Example System with Software Descriptions

NUMBER	DESCRIPTION
1	Matrix Manager software
2	Ethernet
3	Matrix master switch
4	Work stations
5	Matrix switching system receivers
6	Server room
7	Matrix switching system transmitters
8	Cascaded Matrix slave switches

2 INSTALLATION AND SETUP

The Matrix Manager software is provided by Technical Support and may be installed on either a Microsoft® Windows® or Red Hat® Linux® operating system. For users without direct Internet access, the installer is provided by Technical Support on physical media such as a DVD or USB thumb drive.

However, before beginning installation, ensure you have met the system requirements and have the license IDs, default usernames and passwords provided by your Vertiv representative. When you purchased the software, you were given an Entitlement ID that corresponds to your software version, as well as your feature Activation IDs. Available features include: an evaluation copy, a primary Matrix Manager software license and a maintenance agreement subscription.

2.1 System Minimum Requirements

Please refer to the latest release notes for the minimum system requirements. For additional information and tips on installation, see [Appendix A: External KVM Best Practices](#) on page 37.

2.1.1 PostgreSQL database configuration

NOTE: The Matrix Manager software only supports PostgreSQL version 9.0.13 at this time and cannot be installed on a server running another version.

If you are already using PostgreSQL, you must modify it in order to use the Matrix Manager software. During installation, when PostgreSQL 9.0.13 is detected, you will be prompted to enter the existing port number and credentials. The `custom_variable_classes= 'symmetric'` entry must then be appended to the contents of the `postgresql.conf` file and the PostgreSQL service must be restarted.

2.1.2 Installation prerequisites

There are several prerequisites that must be complete prior to installing the Matrix Manager software, such as libraries that must be installed for use with Red Hat Linux. See the release notes that accompany this product for more information.

2.2 Microsoft Windows Installation

To install on a Microsoft Windows OS:

1. After getting the Matrix Manager software files from Technical Support, run the `setup.exe` installation file as an administrator. The installation wizard is displayed.
2. On the Introduction screen, click *Next*.
3. Accept the terms of the License Agreement, enable License Agreement terms and click *Next*.
4. Verify the installation folder or change the installation to another folder and click *Next*.
5. Accept the default port or enter a different port, and click *Next*.
6. On the PostgreSQL screen, verify the port number and click *Next*.
7. Enter the password twice and click *Next*.
8. Review the inputs and click *Install*.
9. Click *Done* when complete and proceed to [License Activation](#) on page 4.

To uninstall from a Microsoft Windows OS:

NOTE: You must be logged in as an administrator to uninstall the software.

1. Before uninstalling the Matrix Manager software, perform a system backup to retain your data. See [Administration, Access and Monitoring](#) on page 13 for back up instructions.
2. If you are installing the Matrix Manager software on another server with existing licenses or if you no longer intend to use a server for the Matrix Manager software, you must deactivate the licenses first. See [License Activation](#) on page 4 for information on license deactivation.
3. After you have backed up your system and deactivated licenses, navigate to the Control Panel and select *Programs – Features – Matrix Manager*.
4. Click *Uninstall/Change*.

-or-

On your local drive, navigate to *Program Files – Matrix Manager – Uninstall*.

5. Double-click the UninstallMatrixManager.exe file.
6. At the Uninstall Matrix Manager wizard, click *Uninstall*, then click *Done*.
7. When complete, navigate to your local directory and select *Program Files*.
8. Delete the EmersonNetworkPower folder, the Matrix Manager folder or the Matrix Manager installation folder where the software was installed and the PostgreSQL folder.
9. In your local directory, double-click *Users*, delete the postgres folder and reboot the server.

2.3 Red Hat Linux Installation

To install on a Red Hat Linux operating system:

1. After getting the Matrix Manager software files from Technical Support, log in as the root user of the Linux server.
2. Execute the installer .bin file, enter the `./install.bin` command and press **Enter**.
3. When the welcome message appears, follow the prompts on the screen, and select option 1 to begin.
4. Review the License Agreement and enter **Y** to agree and continue.
5. Verify or change the default installation folder location, port number for the application, username, password and port number for the PostgreSQL database and complete the installation.

To uninstall on a Red Hat Linux operating system:

1. Before uninstalling the Matrix Manager software, perform a system backup to retain your data. See [Administration, Access and Monitoring](#) on page 13 for back up instructions.
2. Navigate to the Manager installation folder: `CD /usr/local/Matrix_Manager/`.
3. Within the Manager installation folder, enter the `./Uninstall_Matrix_manager` command and follow the prompts on the screen.
4. Delete the EmersonNetworkPower folder, the Matrix Manager folder or the Matrix Manager installation folder where the software was installed and the PostgreSQL folder.
5. At the Linux terminal console, type the `userdel postgres` command. This will delete the Postgres user account if it exists.
6. Reboot the Linux server.

2.4 License Activation

After installing the Matrix Manager software, licenses must be activated before you can see the Dashboard and begin using the software. The following types of licenses are available.

Table 2.1 License Types

LICENSE	DESCRIPTION
Evaluation	An evaluation license can be purchased to allow access to the Matrix Manager software for a limited amount of time. With an evaluation license, you also get primary and subscription license access for the same amount of time. Those temporary licenses can be upgraded to permanent primary and subscription licenses.
Primary	A primary license is necessary for the Matrix Manager software system to run. When you upgrade from an evaluation license to a permanent primary license, the services it provides never expire.
Subscription	A subscription license allows you to do firmware upgrades to the Avocent Matrix High Performance KVM Switching System and can be purchased in yearly increments.

The following licensing rules apply:

- You must have a license for each Matrix Manager software instance.
- Licenses can be activated online or offline.
- (Optional) You can set the license expiration notification. The default is 15 days before expiration.

- If your evaluation or primary Matrix Manager software license expires, the Matrix Manager software will no longer be accessible. In addition, communication with the devices in your system will also not be allowed.

To log in and begin license activation:

1. After the Matrix Manager software is installed, enter `https://<IP>:<Port>/` into your browser.

NOTE: If your port number is changed during the installation, the communication port number must be updated for the system to work properly. For more information, see the Vertiv™ Avocent® Matrix High Performance KVM Switching System Installer/User Guide.

2. At the log in screen, enter the default username and password provided by your Vertiv representative and click *Login*.

NOTE: Be sure to change your default password for security purposes.

Figure 2.1 Licensing Window

Activated Licenses

Feature Name	Feature Version	Expiration Date	Activation ID	Fulfillment ID	Status
Matrix Manager Primary	1.2	Mon Feb 08 05:00:00 EST 2016	170a-3ab0-8f19-45c7-80cc	FID__4cc975f4_14ccb9ccec7__7c13	expired
Matrix Manager Subscription	1.2	Mon Feb 08 05:00:00 EST 2016	1c28-8d89-8375-40d6-9522	FID__4cc975f4_14ccb9ccec7__7c12	expired
Matrix Manager Primary	1.2	Fri Oct 07 05:00:00 EDT 2016	670a-98f5-7e21-471b-806e	FID__5b26bb65_15249bbcd0a__61d2	expired
Matrix Manager Subscription	1.2	Fri Oct 07 05:00:00 EDT 2016	91d7-b52d-eba4-4298-98b0	FID__5b26bb65_15249bbcd0a__61d1	expired
Matrix Manager Primary	1.2	Tue Sep 19 05:00:00 EDT 2017	1ed5-c41c-4481-40fe-b28b	FID__190dda1d_156832c4db1__521b	valid
Matrix Manager Subscription	1.2	Tue Sep 19 05:00:00 EDT 2017	5579-ae92-b509-4636-97d2	FID__190dda1d_156832c4db1__5219	valid

Page 1 of 3

DEACTIVATE

Activation

Entitlement ID: SUBMIT

Activation File: BROWSE ACTIVATE

License Expiration Notification

Expiry Warning Period (days): UPDATE

To activate your license:

1. (Optional) Set the License Expiration Notification and click *Update*.
3. Enter the Entitlement ID (with no spaces) and click *Submit*.
4. Select *Evaluation, Primary and/or Subscription* from the Available Features pop-up box, then click *Submit*.
5. If a network connection is not detected, proceed to the next section to activate the license offline.

-or-

If the network connection is stable, the license information appears in the Activated Licenses pane.

6. Log off and log in again for the licenses to take effect.

To complete activation offline:

1. When a network connection is not detected, an Offline Activation pop-up box appears. Enter the Activation IDs and click *Add* for each feature to be activated.
2. Select *Generate* and at the prompt, download the system generated .xml file to your local machine.
3. After you have downloaded the file, contact Technical Support. They will provide you with another file containing an .xml file for each requested feature.
4. In the Licensing pane, select *Browse* in the Activation File section to navigate to and open an activation file.
5. When the file name appears in the Activation File field, click *Activate*.
6. After activation, verify all of the licenses are listed in the Activated Licenses section. Log out and log back in to get started with the Matrix Manager software Dashboard.

To deactivate a license:

1. Select a license and click *Deactivate*.
2. If the Matrix Manager software has connectivity to the Emerson Licensing Center, then deactivation will be successful and the Activated Licenses section updates. You have completed deactivation.

-or-

If the Emerson Licensing Center is unreachable, the following message appears: *Do you want to generate offline deactivate request file?*

3. Select *Generate* and you are prompted to download a system generated .xml file to your local machine.
4. After you have downloaded the file, contact Technical Support to complete the deactivation.

2.5 Launching the Dashboard

NOTE: The Dashboard is accessible after your licenses are activated.

The Matrix Manager software Dashboard is a one-stop location to see the activities taking place in your system. From the Dashboard, you can see connections, metrics, users and devices that are working in your system. From the side navigation bar (shown in the following figure), you can select specific options that allow you to customize your system details.

To access the Dashboard:

1. Enter **https://<IP>:<Port>/** into your browser.

NOTE: If your port number is changed during the installation, the communication port number of the switch will also need to be updated in order for the system to work properly.

2. Upon entering your log in credentials, the Dashboard appears. It will not have any content populating the fields until after you've completed your set up process.

Figure 2.2 Dashboard

The screenshot shows the Avocent Matrix Manager dashboard. At the top, it says 'Avocent® Matrix Manager' with a help icon and a lock icon. On the left is a navigation sidebar with icons for Dashboard, Sessions, Users, Devices, Settings, Events, and External-System. The main content area is divided into several sections:

- Events:** A table with columns: Date/Time, Device Name/Association, User, Type, and Description. It lists four events from 2017-08-23.
- Sessions:** A table with columns: User, Receiver, Transmitter, Action, and Time Stamp. It shows 'No records found.'
- Discovered Devices:** A table with columns: Name, Eid, Type, and IP Address. It shows 'No records found.'
- Enrolled Devices:** A table with columns: Name, Eid, Type, and IP Address. It shows 'No records found.'
- System Metrics:** A summary box showing 'Manager Uptime: 12 Days : 01 Hours : 13 Minutes'. Below it is a table with columns: Login (Count, Peak Concurrence), Session (Count, Peak Concurrence), and Connection Authorization (Count). It shows 'No records found.'
- User Creations:** A table with columns: Username, Date/Time, Created By, and Expiration Date. It shows 'No records found.'

Table 2.2 Dashboard Descriptions

NUMBER	NAME	DESCRIPTION
1	Side Navigation bar	Used to select the type of information to display or edit in the main content area.
2	Events pane	Displays the details for the last five events. Selecting <i>Events</i> in the side navigation bar will allow you to edit this information.
3	Sessions pane	Displays the history of receiver log ins and connections to transmitters. Selecting <i>Sessions</i> in the side navigation bar will allow you to view and manage current sessions.
4	Discovered Devices pane	Displays device information for master switches that have been discovered. Selecting <i>Devices</i> in the side navigation bar will allow you to view and enroll currently discovered devices and discover new devices.
5	Enrolled Devices pane	Displays information for enrolled devices. Selecting <i>Devices</i> in the side navigation bar will allow you to edit this information.
6	System Metrics pane	Displays metrics for services that are continuously running, plus log in and connections information.
7	User Creations pane	Displays details on internal users added to the system. A list of internal users added to the system. Selecting <i>Users</i> in the side navigation bar will allow you to edit this information.
8	Question Mark icon	Selecting this icon will access the online help system. If you do not have Internet access, the help files can be downloaded offline.
9	Padlock icon	Indicates that you are securely logged into the Matrix Manager software. Clicking this icon will allow you to log off.
10	Top Option bar	From the Dashboard, this serves as a Welcome notification and changes depending on your

NUMBER	NAME	DESCRIPTION
		selection from the side navigation bar. When you select an option, the name of the opened window is displayed and where applicable, additional tabs to further customize your system.

2.6 Understanding the Information Flow

Now that you've accessed the Dashboard for the first time, it is important that you understand the flow of information within the Matrix Manager software before proceeding to set up your system. The Matrix Manager software operates within the parameters of the following definitions:

- Users - Each person that will access the software and the Matrix switching system.
- Devices - Each switch, transmitter and receiver that are in your system.
- Groups (user groups and device groups) - A streamlined way to organize the users, transmitters and receivers in the system. The goal of grouping within the Matrix Manager software is that you will eventually have a complete categorized list of the system components (users, transmitters and receivers), the resource privileges of each and which permissions (roles) are assigned to each group. Once the component framework is established, adding new users or devices to an existing group becomes simple, seamless and quick.
- Roles - Roles define the permissions of each group.

2.6.1 Matrix Manager software information chain

Within the Matrix Manager software, you will be defining users, user groups, roles, device groups and devices. The following figure illustrates the possible paths you can take to define each. The table after the figure lists the information type and then defines how the paths flow.

Figure 2.3 The Information Chain

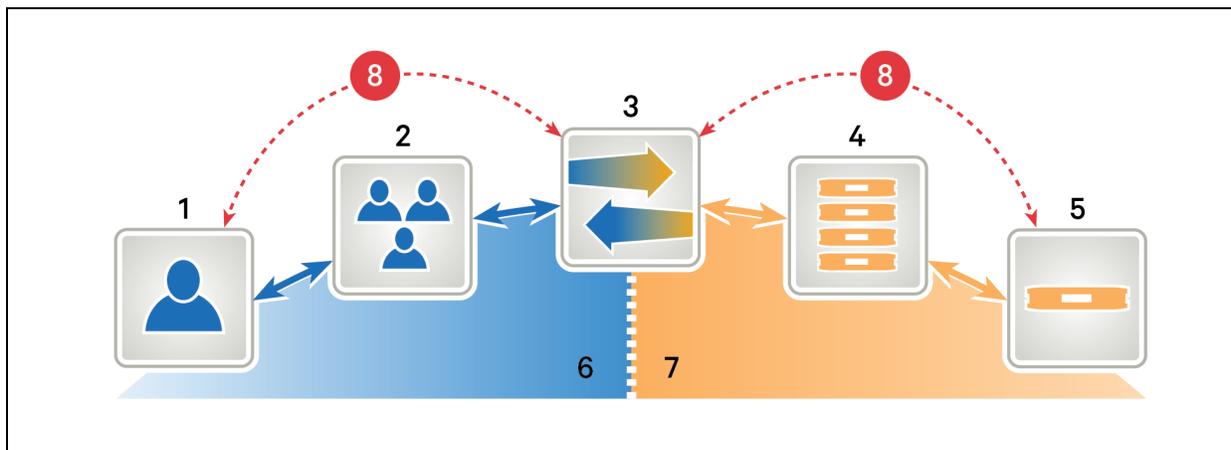


Table 2.3 Information Chain Descriptions

ROLES	DESCRIPTIONS
1	Users
2	User groups
3	Roles
4	Device Groups
5	Devices
6	User path: There are three variations of the user path. Option 1: Add users, assign them to user groups, and then define user group roles. Option 2: Define roles, apply them to user groups, and then add users to the user groups. Option 3: Create a user group, assign users to that user group and then define roles for the user group.

ROLES	DESCRIPTIONS
7	Device path: There are three variations of the device path. Option 1: Add devices, assign them to device groups, and then define device group roles. Option 2: Define roles, apply them to device groups, and then add devices to the device groups. Option 3: Create a device group, assign devices to that user group and then define roles for the device group.
8	Prohibited paths: Matrix Manager software operates in a group-based system. Regardless of whether you follow the user path or device path, you must pass through the group set up in order to proceed. This means that you cannot define roles for users or devices specifically. You can only define roles for user groups or device groups. You cannot add users or devices to a role. You can only add users or devices to a group.

2.7 Setting up Your System

Later sections of this user guide will detail more advanced operations for your Matrix Manager software. To get started, however, this section will help you get your basic system up and running with the software. The user and device paths described in the previous table are interchangeable and both must be followed, but either path can be followed first. For the Matrix Manager software to operate properly, users, user groups, devices, device groups and roles for both group types must be added/created and defined.

When you access the Dashboard the first time, the following defaults for the user, group and role are already established:

NOTE: For security purposes, change your default passwords once you access the Dashboard.

- One internal user (Admin)
- One user group (Administrators)
- One role (AdminRole) with full privileges
- One device group (AdminDeviceGroup) designated as default group

This section will use the default information to meet the criteria for users, user groups and user group roles.

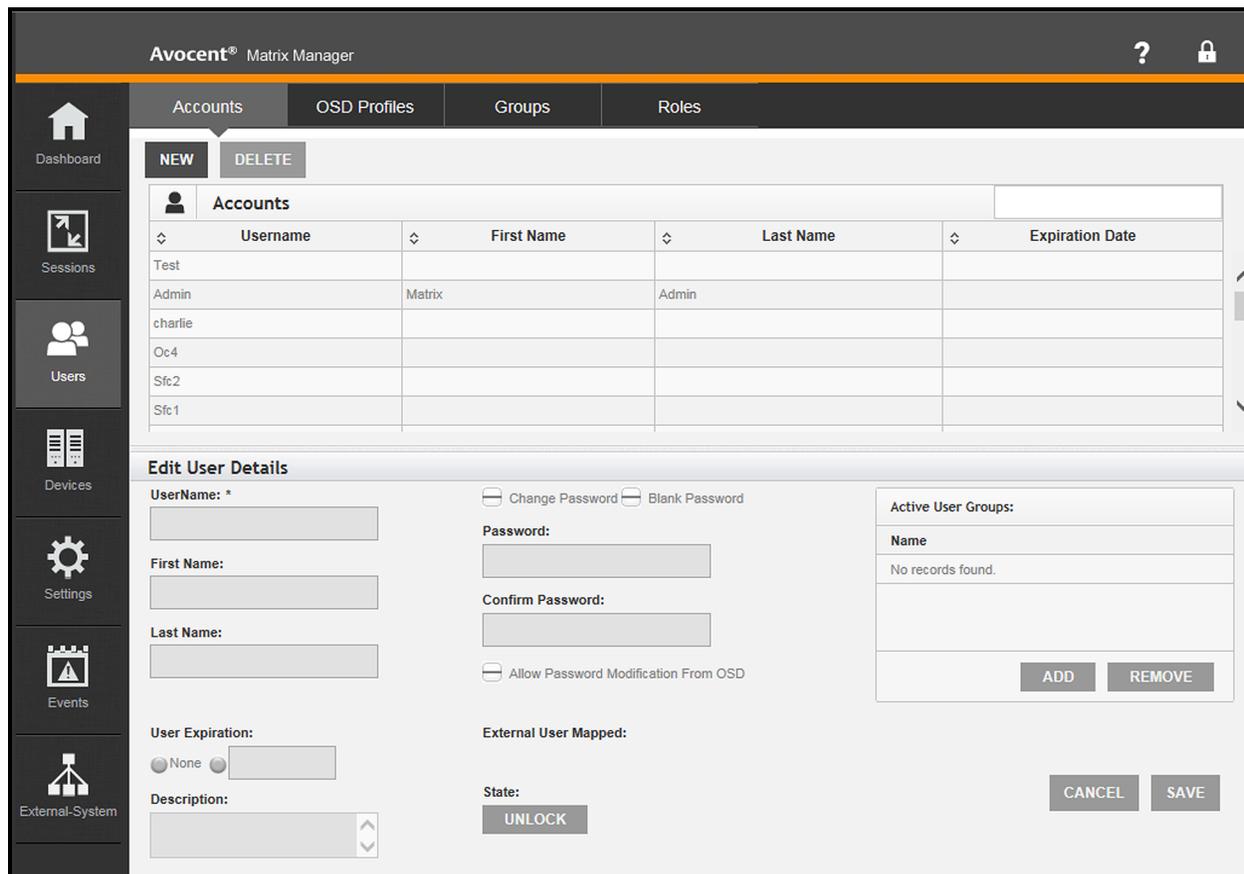
NOTE: For system set up purposes, this section only describes how to view the current established information. To learn how to edit or add users, user groups and user group roles, see [Expanding Your System](#) on page 21.

All that must be done to complete basic system set up is adding/creating/defining the devices, device groups and device group roles.

To see the details for the established user, group and role:

1. From the Dashboard side navigation bar, select *Users – Accounts* tab. In the *Accounts* pane, information for the internal user (Admin) is listed.

Figure 2.4 Users – Accounts Tab



2. Select the *Groups* tab in the top option bar. In the Groups pane, information for the user group (Administrators) is listed.
3. Select the *Roles* tab in the top option bar. In the Roles pane, information for the role (AdminRole) is listed.

2.7.1 Adding devices to the system

To continue with system set up, the Matrix Manager software needs to discover and enroll the connected Matrix High Performance KVM master switches. For more detailed operations, see [Expanding Your System](#) on page 21.

To manually discover and enroll the master switch:

1. From the Dashboard side navigation bar, select *Devices – Unmanaged* tab – *Discovery* button.

Figure 2.5 Devices - Units Tab

Name	Type	IP Address	Status	Firmware Version	Description
MXS5132-SX-32-3032C6	Switch (Controller)	10.207.67.245 fd40:db8:4:4:217:ebff:fe30:32c6	Ready	1.8.8.5590	
MXT5120-TX-VGA-E01011	Transmitter (VGA)		Ready	01.07.00.5326	
MXT5120-TX-VGA-000095	Transmitter (VGA)		Ready	01.07.00.5326	
MXR5110-RX-DVI-I-E00005	Receiver (G1)		Ready	01.08.02.5563	
MXT5110-TX-DVI-D-E00002	Transmitter (DVI)		Ready	01.08.01.5563	
MXR5110-RX-DVI-I-E05006	Receiver (G1)		Ready	01.08.02.5563	
MXS5132-SX-32-DA0C84	Switch	10.207.67.246 fd40:db8:4:4:218:32ff:fedc:c84	Ready	1.8.7.5587	
MXT5110-TX-DVI-D-E00001	Transmitter (DVI)		Ready	01.08.01.5563	
MXT5110-TX-DVI-D-E04022	Transmitter (DVI)		Ready	01.08.01.5563	
MXT5110-TX-DVI-D-E04036	Transmitter (DVI)		Ready	01.08.01.5563	
MXS5120-SX-20-861D6A	Switch (Controller)	10.207.67.241 fd40:db8:4:4:867e:40ff:fe86:1d6a	Ready	1.8.7.5587	
MXT5110-TX-DVI-D-E04103	Transmitter (DVI)		Ready	01.08.01.5563	
MXT5110-TX-DVI-D-E04028	Transmitter (DVI)		Ready	01.08.01.5563	
MXT5110-TX-DVI-D-E04029	Transmitter (DVI)		Ready	01.08.01.5563	
MXR5110-RX-DVI-I-E05103	Receiver (G1)		Ready	01.08.02.5563	
MXR5110-RX-DVI-I-E05139	Receiver (G1)		Ready	01.08.02.5563	
MXR5110-RX-DVI-I-E00003	Receiver (G1)		Ready	01.08.02.5563	

2. In the Manual Discovery pop-up box, select an IP Type, enter an IP address or a range of IP addresses and click *Discover*. Once discovered, the device information will appear in the Unmanaged tab within the Units pane.

NOTE: This information should be specific to the device you are discovering. In this case, enter the information for the master switch.

3. Select the master switch and click *Enroll*.
4. After the switch is enrolled, the master switch information will appear in the Units pane. Select the *Units* tab in the Devices top option bar to view the enrolled master switch and the matrix of devices managed under it.

To enable auto discovery upon device installation:

1. From the Dashboard side navigation bar, select *Settings – System* tab – *Manager Settings* tab.
2. In the General Settings pane, select *Enable* in the Device Auto Discovery field.
3. Enter a duration in the Auto Discovery Frequency field and click *Save*.

2.7.2 Creating device groups

Device groups allow administrators to sort and organize switches, receivers and transmitters into specific categories with defined rules and permissions for each. These groups have no hierarchy and devices can be members of more than one group. To continue the system set up process, you must create groups for the devices that you just added. One or more device groups can be set up as default groups. A default group is a device group to which all new switches, receivers and transmitters will be automatically added.

NOTE: This section describes creating basic device groups. To learn how to customize device settings and edit or delete device groups and device group roles, see [Expanding Your System](#) on page 21.

To create a device group with active units:

1. From the Dashboard side navigation bar, select *Devices – Groups* tab – *New*.
2. In the Add Unit Group pane, enter a name and description.
3. Click *Add* on the Active Units pane to assign an available unit.
4. Select the Default group checkbox to configure the group as a default group for new devices.
5. On the Available Units pop-up box, select devices to add to the device group.
6. Click *Add*. When you select a device group in the Groups pane, the associated devices are now listed in the Units: Active Units pane.
7. Click *Add* on the Active Roles pane to assign an available role.
8. On the Available Roles pop-up box, select roles to add to the device group.
9. In the Available Unit Groups pop-up box, select a device group and click *Add*.
10. Click *Save*. When you select a device group in the Groups pane, the associated roles are now listed in the Roles: Active Roles pane.

2.7.3 Creating roles for device groups

Roles define the boundaries and permissions for groups. When you establish roles within the software, you are provided with various permission levels that you can assign to each role.

NOTE: For system set up purposes, this section only describes how to get started with device group roles. Procedures for creating other types of roles are covered later in this user guide.

To create a role with a specific device group:

1. From the Dashboard side navigation bar, select *Users – Roles* tab –*New*.
2. In the Add Role pane, enter the role name and description.
3. Select a USB mode from the drop-down list.
4. Enable one or more permissions for this role. Permissions are listed in the following table.

Table 2.4 Role Permissions

PERMISSION NAME	ACCESS LEVEL DESCRIPTION
Manager Access	Allows full access to the Matrix Manager software. Within the software, you can view and manage all devices. However, this permission does not give access for you to log in to a receiver or connect to a transmitter. Device Access is required for this.
Manager API Access	Allows you to execute actions on a target device using external REST API Web Service calls.
Device Access	Allows you to log in to a receiver and connect to a transmitter, but you cannot log into the Matrix Manager software. By default, you have access to Share mode. For more information on Share mode, see the Vertiv™ Avocent® Matrix High Performance KVM Switching System Installer/User Guide.
Private Access Allowed	Allows you to connect to a target device in Private mode. For more information on Private mode, see theVertiv™Avocent® Matrix High Performance KVM Switching System Installer/User Guide.

5. Click *Add* in the Active Unit Groups: Device Group Name pane.
6. In the Available Unit Groups pop-up box, select a device group and click *Add*.
7. Click *Save*. When you select a role in the Roles pane, the associated device groups are now listed in the Active Unit Groups: Device Group Name pane. Also, when you select a device group by selecting *Devices- Groups* tab from the Dashboard, the roles associated with that device group are listed in the Roles: Active Roles pane.

2.8 Next Steps

Now that your basic system is installed, you can begin expanding and customizing components with the Matrix Manager software. You are now ready to begin authenticating and authorizing sessions between receivers and transmitters in the system, as well as handle all administration, access control, monitoring and firmware upgrade activities across the Matrix switching system.

3 ADMINISTRATION, ACCESS AND MONITORING

Now that your basic system is installed, the Matrix Manager software allows you to expand and customize the components. You are now ready to begin authenticating and authorizing sessions between receivers and transmitters in the system, as well as handling all administration, access control, monitoring and firmware upgrade activities across the Matrix switching system.

While working with the Matrix Manager software, you can perform general operations such as customizing software configurations, accessing online help and creating tasks to tailor the system to your needs.

3.1 Customizing Basic Matrix Manager Software Settings

Selecting *Settings* from the Dashboard, then clicking the *System* tab and the *Manager Settings* tab provides options to adjust general software settings. The General Settings, Lockout Policy and Inactivity Timeout panes allow you to reset the Matrix Manager software to factory defaults and determine durations for lockout (in case of repeated unauthorized attempts to log in) and time-outs. After you enter information within these panes, click *Save* to retain your settings. From the Manager Settings tab, you can also configure online help and passwords.



CAUTION: If you reset the software, it returns to the original state at installation and all data and activated licenses are removed unless you select the option to not release the licenses during the reset.

By selecting *Settings – System* tab – *System Restore* tab from the Dashboard, you can restore the Matrix Manager software system to a previous state using a generated backup.

3.2 Using Matrix Manager Software Online Help

Online help is available when you select the question mark icon on the top-right of the Dashboard. The online help provides a way to search for answers to questions you may have while working in the Matrix Manager software. The online help is hosted on the Vertiv web site. If you do not have continuous access to the Internet, you may wish to install the help on the local server running the Matrix Manager software.

To select your help configuration:

1. From the Dashboard side navigation bar, select *Settings – System – Manager Settings* tab.
2. In the Help Configuration pane, select a radio button in the Show Help From section for the option you wish to select.
3. In the Download Help From section, select a radio button for the option you wish to select.
4. If downloading from a Local Device, select *Browse* to locate and select the file, and then click *Download*.

-or-

If downloading from the Vertiv website, click *Save*.

3.3 Configuring Password Settings

The default administrator password is provided by Technical Support. After initial software log in, passwords for administrators and users can be changed. Changing passwords is described later in this user guide, but password configuration is done within the Settings window.

To select your password configuration:

1. From the Dashboard side navigation bar, select *Settings – System* tab – *Manager Settings* tab.
2. In the Password Configuration pane, select *Yes* or *No* in the Password Required field.

NOTE: Selecting *No* means that when creating a user, you have the option to add a password if desired, or enable the Blank Password checkbox to allow users to be created without a password. Selecting *Yes* means that a password is required when you create a user.

3. Click *Save*.

3.4 Scheduling Backups and Firmware Upgrades

Creating tasks is helpful because it uses the Matrix Manager software to automate important system activities such as backing up your system and upgrading your firmware.

To schedule a backup task:

1. From the Dashboard side navigation bar, select *Settings – Tasks* tab. The Tasks pane appears.
2. Click *Add*, then select *Backup* from the Task Type drop-down list.
3. Enable the *Run Now* checkbox.

-or-

Disable the *Run Now* checkbox and click the *Calendar* icon to change the start date.
 - a. Enable the *End By* checkbox and enter a date.
 - b. Set the Frequency by hours or minutes or click the *Run Once* radio button.
4. Enter the file location or a remote path to store the information, but the Matrix Manager software must have access to this path.
5. Enable the *Password Protect Backup File* checkbox.
6. Enable the *Add Date and Time* to the file name checkbox.
7. Enter a Password for the backup file and confirm it. A password is required only if Password Protect Backup File is enabled.
8. If required to access the backup location, the Login Required option must be used. Enable the radio button, enter a login username and password, then click *Save*.

To schedule firmware upgrade tasks for devices:

NOTE: You cannot upgrade firmware if the subscription license (maintenance agreement) has expired.

1. From the Dashboard side navigation bar, select *Settings – Tasks* tab – *Add* button.
2. Select *Firmware Upgrade* from the Task Type drop-down list.
3. Enable the *Run Now* checkbox.

-or-

Disable the *Run Now* checkbox and click the *Calendar* icon to change the start date.
4. Select a protocol type, *Local File* or *FTP*.

If *Local File* is selected, enter the file location on your local or shared drive where the firmware is located.

-or-

If *FTP* is selected, enter the FTP server IP address, the location of the file on the server and log in credentials for the server.
5. Select a device type to upgrade in the Update field.

-or-

Select a unit group to update all devices in the unit group.
6. Click *Add* on the Devices or Groups: Available Devices or Groups pane and select a device.
7. Click *Add – Save*.

3.5 Streamlined Operations

The Matrix Manager software provides authentication and API options that ease device data integration and streamline system performance.

3.5.1 Using third-party authentication

Matrix Manager software is delivered with an internal authentication service which verifies the login username and password against user account information stored in the internal database of the server. In addition the software also supports authentication of users using one or more external Active Directory (AD) systems.

If the Matrix Manager server is configured with one or more third-party authentication systems, login requests are first checked against the internal database. If no match is found then the request is re-directed to the configured external authentication servers. If authenticated successfully, the Manager software obtains the external group name for the corresponding user account and looks in the internal database for a matching user group name. All further rights and permissions are based on the matching internal user group.

To add a third-party authentication service:

1. From the Dashboard side navigation bar, select *Settings – 3rdParty* tab. The 3rdParty pane appears.
2. Select *New*.
3. In the Authentication Name field, enter a name for the AD server.
4. In the Directory Service URL field, enter the IP address of the AD server or the Domain Name of the AD server.
5. In the AD Domain name field, type the Active Directory Domain Name for the domain you wish to add.
6. In the optional User Container field, specify the name of the container to search for user accounts. This will limit the search scope to that container. The name may be entered in several forms.

Example:

Assume an Active Directory domain name of “sunrise.mycompany.com” with users in subfolder “sun/myusers.” The User Container field may be entered as:

Example 1 (no sub-domain): “sun.myusers”

Example 2 (no sub-domain): “ou=myusers,ou=sun”

If users are contained in a sub-domain such as “mktg.sunrise.mycompany.com”, valid forms are:

Example 1 (with sub-domain): “mktg.sunrise.mycompany.com/sun/myusers”

Example 2 (with sub-domain and no container specified): “mktg.sunrise.mycompany.com/”

Example 3 (with sub-domain): “ou=myusers,ou=sun,dc=mktg,dc=sunrise,dc=mycompany,dc=com”

7. In the optional Group Container field, specify the name of the container to search for user groups. This will limit the search scope to that container.
8. Enter the username and password for an Active Directory account that has browse rights in the User Name field.
9. Specify a Secure Socket Layer (SSL) encryption mode:
 - Click Do Not Use SSL to have authentication performed using unencrypted clear text instead of SSL encryption. This method is the least secure.
 - Click Use SSL in Trust All mode to use SSL encryption for data transmission. All server certificates will be trusted and automatically accepted by the Matrix Manager software for transmitting data. This SSL method provides medium security.

NOTE: This encryption mode is not recommended for wide area networks (WANs).

- Click Use SSL in Certificate-based Trust mode to use SSL encryption for data transmission. The Matrix Manager software will approve the server and then the certificate before transmitting data. This SSL method provides maximum security.
10. Click *Save*. The Matrix Manager server will use the above details and try to establish a connection with the third-party authentication server.

To setup user account access and permissions:

1. Setup the user accounts and user groups in the AD system.

2. Create User Groups in the Manager software with the same name of the user group in the AD system. The syntax of the AD Group name and the Manager software must be the same.
3. Assign the appropriate roles and permissions to the user group in the Matrix Manager software.

NOTE: The permissions, access rights and roles for external users are based on the rights given to the internal user group that is mapped to the external user group.

To edit a third-party authentication:

1. From the Dashboard side navigation bar, select *Settings – 3rdParty* tab. The 3rdParty pane appears.
2. Select the authentication name, make necessary changes and click *Save*.

To delete a third-party authentication:

1. From the Dashboard side navigation bar, select *Settings – 3rdParty* tab. The 3rdParty pane appears.
2. Select the authentication name, click *Delete* and click *Save*.

To schedule a third-party profile cleanup task:

NOTE: If a third-party user or system is deleted, you can schedule a cleanup of external third-party user profiles in the system.

1. From the Dashboard side navigation bar, select *Settings – Tasks* tab – *Add* button.
2. Select *User Cleanup* from the Task Type drop-down list.
3. Enable the *Run Now* checkbox.

-or-

Disable the *Run Now* checkbox and click the *Calendar* icon to change the start date.

- a. Enable the *End By* checkbox and enter a date.
 - b. Set the *Frequency* by hours or minutes or click the *Run Once* radio button.
4. Click *Save*.

3.5.2 Using an external API

The Matrix Manager software provides a REpresentational State Transfer (REST) Web Service API and a Telnet API to perform core functionality such as forced log in/out of receivers and establishing/disconnecting sessions between the receiver and transmitter managed by the software. If you are interested in using the API, enable access within the Matrix Manager software. See the Vertiv™ Avocent® Matrix Manager Software API Technical Bulletin for more information.

To enable external API access:

1. From the Dashboard side navigation bar, select *Settings – System* tab – *External API*. The External API pane appears.
2. Enable access for the Web or Telnet API and click *Save*. For the Telnet API, the default port is 9000.

NOTE: The firewall on the Manager server must be configured to allow communication on port 9000 or the Telnet API access port must be configured.

3.6 Monitoring Activities

With the Matrix Manager software running, you may want to monitor system activities. Events monitoring is available from the Dashboard to view dates, times, severity, usernames, types of activities and descriptions. An event can be designated as informational, critical or a warning that requires attention. The Event Log provides a list of system-related events and the Event Monitor checks for the overflow of events in the system.

To access the event log:

From the Dashboard side navigation bar, select *Events*.

From the event log, you can enable event counts that will generate an alert from the Matrix Manager software if the count is exceeded. While you can set the alert in the following procedure, you will not receive any email alerts until notifications are established in the next section.

To enable alerts:

1. From the Dashboard side navigation bar, select *Events – Log tab – Monitor* button.
2. In the Event Monitor pop-up box, click the *Enable* radio button and enter a number in the Event Counts field.
3. Click *Save*.

3.6.1 Using notifications

Notifications can be configured to send emails and/or Simple Network Management Protocol (SNMP) traps with information regarding specific events. A notification policy establishes which events are included in email alerts and/or SNMP traps.

A notification list establishes the users and email addresses to be alerted. Email notifications use Simple Mail Transfer Protocol (SMTP), so the SMTP server must be configured.

To configure the SMTP server for email notifications:

1. From the Dashboard side navigation bar, select *Settings – System tab – SMTP Server*. The SMTP Server pane appears.
2. Enter the address of the server and enable *Login Required for Access*, if applicable.
3. Enter the username and password of the SMTP server, if applicable, and click *Save*.

NOTE: For additional information on the SNMP traps sent by the Manager software, contact Technical Support to request an MIB file.

To configure SNMP trap send policy:

1. From the Dashboard side navigation bar, select *Events – Policies* and click *New*.
2. Enter the policy name in the Name field.
3. Enter the description of this policy in the Description field.
4. Click *Add* to add the event which you want to send SNMP Trap in the Event List.
5. Click *Add* to add the SNMP Server.
6. Click *Save*.

To add a notification list:

NOTE: Notifications lists can contain one or more email addresses, separated by a comma. Email addresses must be accessible from the SMTP server and associated with a notification policy.

1. From the Dashboard side navigation bar, select *Events – Notification List tab – New* button.
2. In the Add Notification List pane, enter a List name and one or more email addresses for users to be notified of an event.
3. Click *Save*.

To edit or delete a notification list:

1. From the Dashboard side navigation bar, select *Events – Notification List tab*. The Notification List pane appears.
2. In the Notification List pane, select a notification.
3. If editing a notification, edit the list in the Edit Notification List and click *Save*.

-or-

If deleting a notification, click the *Delete* button once, then again on the confirmation pop-up box.

The SNMP list screen can be used to configure the SNMP servers that can receive the trap notifications.

To configure the SNMP server for trap notifications:

1. From the Dashboard side navigation bar, select *Events –SNMP List*. Click *New*.
2. Enter a name for this SNMP server.
3. Enter the IP address of the SNMP server.

NOTE: Only IPv4 is supported.

4. Enter the SNMP trap port. The default port is 162.
5. In SNMP Version field, select the SNMP version. The Manager software supports all SNMP versions, but the configuration for each is different.
6. Enter a description of the server in the description field.
7. If SNMP v1 or v2c is selected, the Community field is available. Select a community from the drop-down menu. The default for this field is "public".
8. For SNMP v3, select a security level and then complete the following:
 - a. If security level AUTH_NOPRIV or AUTH_PRIV is selected, complete the following:

Enter the configured SNMP V3 server authentication username.

Select the Auth protocol.

Enter the SNMP V3 server authentication password.

- b. If security level AUTH_PRIV is selected, complete the following:

Select the privacy protocol from the drop-down menu.

Enter the SNMP v3 server privacy password.

To create a notification policy for a specific event (task) and notification list:

1. From the Dashboard side navigation bar, select *Events – Policies* tab – *New* button.
2. In the Add Policy pane, enter a name and description.
3. Click *Add* in the Event: Event pane.
4. In the Available Events pop-up box, select an event and click *Add*.
5. In the Notification List pane, click *Add*.
6. In the Available Lists pop-up box, select a list and click *Add*.
7. In the SNMP Servers List pane, click *Add*.
8. In the Available SNMP servers pop-up menu, select a server and click *Add*.
9. Click *Save*.

NOTE: When you select a policy in the Policies pane, the associated events and notification lists are listed in the Event: Event and Notification List panes.

To edit or delete a notification policy:

1. From the Dashboard side navigation bar, select *Events – Policies* tab. The Policies pane appears.
2. If editing a notification policy, you can change information in the Edit Policy, Event: Event or Notification List panes and click *Save*.

-or-

If deleting a policy, click *Delete* once, then again on the confirmation pop-up box.

3.6.2 Scheduling event tasks

The Matrix Manager software allows you to create tasks to export event information to a designated location or to cleanup events tracked.

To schedule an event export task:

1. From the Dashboard side navigation bar, select *Settings – Tasks* tab. The Tasks pane appears.
2. Click *Add* and select *Event Export* from the Task Type drop-down list.
3. Enable the *Run Now* checkbox.

-or-

Disable the *Run Now* checkbox and click the *Calendar* icon to change the start date.

- a. Enable the *End By* checkbox and enter a date.
 - b. Set the *Frequency* by hours or minutes or click the *Run Once* radio button.
4. Enter the file location where the information is to be stored. The file location can be a remote path, but the Matrix Manager software must have access to this path..
 5. Enable the *Login Required* checkbox.
 6. Enter a Login User, then enter your password twice.
 7. Select your Event Category from the drop-down list.
 8. Enable the *Add Date and Time to the file name* checkbox.
 9. Click *Save*.

To add an event cleanup task:

NOTE: Event cleanup permanently deletes events from the system. Ensure an event export task is set up if you wish to archive events before purging the content during cleanup.

1. From the Dashboard side navigation bar, select *Settings – Tasks* tab. The Tasks pane appears.
2. Click *Add* and select *Event Cleanup* from the Task Type drop-down list.
3. Enable the *Run Now* checkbox.

-or-

Disable the *Run Now* checkbox and click the *Calendar* icon to change the start date.

- a. Enable the *End By* checkbox and enter a date.
 - b. Set the *Frequency* by hours or minutes or click the *Run Once* radio button.
4. Enter the *Age (Days)* the events are kept or click *Default*.
 5. Click *Save*.

This page intentionally left blank.

4 EXPANDING YOUR SYSTEM

Your basic Matrix Manager software should be set up at this point and ready for you to begin expanding with additional users and devices. As long as you follow the pattern described in the Matrix Manager software information chain section in [Understanding the Information Flow](#) on page 8, you can add user or device information first.

4.1 User Operations

When you first log in to the Matrix Manager software, an internal user is already set up for you. Before you begin adding additional users, determine the privileges and permissions necessary for each user through user groups and user group roles. The best practice sequence to add a user to the system is to create a user group, define a role for that user group and then add a user that will be associated with that group and role.

NOTE: When logged into a receiver, if the user permissions are changed in the manager, the updated permissions will not take affect until the user logs out of the receiver OSD and back in.

When a user changes the effective access rights/permissions (by changing the user group or role or unit groups), it is not immediately effected in active logins at the receiver. So if someone is already logged into a receiver, and then if the permissions are changed in Manager software, the updated permissions will not take effect until the user logs out of the receiver OSD and logs back in.

To create a user group:

1. From the Dashboard side navigation bar, select *Users – Groups* tab.
2. Click *New*, enter the group name and description.
3. Click *Add* under the Active Users pane.
4. In the Available Users pop-up box, select user(s) and click *Add*.
5. Click *Add* under the Active Roles pane.
6. In the Available Roles pop-up box, select role(s) and click *Add*.
7. Click *Save*.

To edit or delete a user group:

1. From the Dashboard side navigation bar, select *Users – Groups* tab.
2. Select a user group.
3. If editing a user group, you can change the information in the Active Users or Active Roles panes and click *Save*.

-or-

If deleting a user group, click *Delete* once, then again on the confirmation pop-up box.

To create a role:

1. From the Dashboard side navigation bar, select *Users – Roles* tab – *New*.
2. Enter the role name and description.
3. Select a USB Connectivity option from the drop-down list.
4. Enable one or more permissions for this role. See Role Permissions table in [Installation and Setup](#) on page 3 for more information.
5. Select *Add* in the Active User Groups pane and select the appropriate user group name.
6. Click *Save*.

To edit or delete a role:

1. From the Dashboard side navigation bar, select *Users – Roles* tab.
2. Select a role.
3. If editing a role, you can change information in the Active User Groups pane and click *Save*.

-or-

If deleting a role, click *Delete* once, then again on the confirmation pop-up box.

To associate a user group with a role:

1. From the Dashboard side navigation bar, select *Users – Groups* tab.
2. Select a user group.
3. Select a role in the Edit User Group Details – Active Roles pane, and click *Save*.

To create a user:

1. From the Dashboard side navigation bar, select *Users*. Ensure that the Users window opens to the Accounts tab.
2. Click *New*.
3. Enter a unique username. Usernames can contain spaces, alpha/numeric and the following special characters:

~!@#\$\$%^&*O+=?_<>.\/-

Names are case sensitive, spaces are allowed, but duplicates are not allowed.

4. Enter the first and last name of the user. If desired, enable the *User Expiration* checkbox and select a date from the calendar.
5. Add a description.
6. Enter a password and enter the password again to confirm.

-or-

Enable the Blank Password checkbox.

NOTE: Earlier in this user guide, you selected your password configuration. If you selected *No* in the Password Required field, then you can enable the Blank Password checkbox to allow users to log in without a password.

7. The Allow Password Modification From OSD allows users to change their own passwords from the receiver OSD. If unchecked, this user will not be allowed to modify the password from receiver OSD. By default, this field is enabled.
8. Click *Save*.

To change a user password:

NOTE: This section only applies to user passwords. If you forget the administrator password, contact Technical Support.

1. From the Dashboard side navigation bar, select *Users – Accounts* tab.
2. Select a user.
3. Enable the *Change Password* checkbox under the Edit User Details pane.

NOTE: An account locks automatically based on the Lockout Policy defined in the Settings window. If an account is locked, the State: Unlock button is enabled. The administrator can unlock the account or wait until the Lockout Policy duration passes.

4. Enter the new password and enter the password again to confirm it.
5. Click *Save*.

To edit or delete a user:

1. From the Dashboard side navigation bar, select *Users – Accounts* tab.
2. Select a user.
3. If you are editing a user, you can change the information in the Edit User Details pane and click *Save*.

-or-

If you are deleting a user, click *Delete* once, then again on the confirmation pop-up box.

To associate a user with a user group:

NOTE: If a user group has already been associated with a role, the user is automatically assigned the role associated with corresponding user group.

1. From the Dashboard side navigation bar, select *Users – Accounts* tab.
2. Select a user.
3. In the Active User Groups pane, and click *Add*.
4. Select a user group, click *Add* and then click *Save*.

4.1.1 Using user OSD profiles

The receivers in your Matrix switching system have an on-screen display (OSD) that allows you to perform activities within the switching system. OSD profiles allow individual users logging into the receiver to have their own custom settings such as OSD hotkeys, OSD timeout, favorite transmitter and shortcut key configurations. Profiles can be configured for internal and external users. Internal profiles are automatically generated when a user is added to the Matrix Manager software. External profiles are automatically generated when a user logs in to the receiver OSD for the first time. For each Matrix Manager user, you can modify the user's OSD profile settings. For more information on the receiver OSD, see the Vertiv™ Avocent® Matrix High Performance KVM Switching System Installer/User Guide.

To edit user OSD profile settings:

1. From the Dashboard side navigation bar, select *Users – OSD Profiles* tab.
2. Select a username in the OSD Profiles pane and a hotkey sequence from the drop-down list in the Details pane. The option to enable or disable can only be entered by an administrator.

NOTE: When *Disable* is selected, the user can no longer have a user assigned hotkey selection, the system default hotkey will apply.

3. In the Timeout field, enter a number of minutes or hours. The time-out is disabled when it is set to zero.

NOTE: If your receiver OSD times-out, the hotkey sequence you selected in the previous step must be used to activate it again.

4. Select one or more transmitters in the Favorite Transmitter List pane and click *Save*.

NOTE: The transmitters in this list are modified and added by a user in the Matrix switching system. A favorite transmitter is one that is frequently accessed. For more information on the favorites list, see the Vertiv™ Avocent® High Performance KVM Switching System Installer/User Guide.

4.2 Device Operations

The Installation and Setup chapter describes how to get a basic system up and running, including adding devices, device groups and roles. Follow the steps in that chapter for each device that you add to your system. As you expand your system by adding more devices, groups and roles, you can begin customizing your device information.

To edit or delete a device group:

1. From the Dashboard side navigation bar, select *Devices – Groups* tab.
2. Select a device group.
3. If you are editing a user group, you can change the information under the Edit Device Group Details pane and click *Save*.

-or-

If you are deleting a user group, click *Delete* once, then again on the confirmation pop-up box.

To edit or delete a device from the Offline Units tab:

1. From the Dashboard side navigation bar, select *Devices – Offline Units* tab.
2. Select an offline device.
3. Click *Delete* once, then again on the confirmation pop-up box.

To edit or delete a device group role:

1. From the Dashboard side navigation bar, select *Users – Roles* tab.
2. Select a role.
3. If you are editing a role, you can change the information in the Edit Role pane and click *Save*.

-or-

If you are deleting a role, click *Delete* once, then again on the confirmation pop-up box.

4.2.1 General device settings

From the Settings window, at the System tab, you can select the *Device Settings* tab to modify general device settings. Adding information within the panes on this tab allows you to manage system defaults for USB permissions, transmitter USB/video priority and the OSD inactivity time-out. These defaults are applied not only to existing devices, but also to new devices. Click *Save* after entering information to retain your changes.

NOTE: The OSD inactivity time-out is disabled when it is set to zero.

4.2.2 General device activities

From the Devices window – Units tab, you can select several buttons to perform general activities including disenrolling master switches, rebooting, restoring and locating devices, and viewing physical connections to each. Devices are selected in the Units pane.

To disenroll a master switch:

1. Select a master switch and select *Disenroll* to remove it. When you disenroll a master switch, it becomes unmanaged and all devices cascaded off of it become offline.
2. To see the disenrolled master switch information, select the *Unmanaged* tab.
3. To see the offline cascaded device information, select the *Offline Units* tab.

NOTE: Devices that are turned off or not responding to the Matrix Manager software or master switch will also show as offline.

To view the physical connections, locate or reboot a device:

1. Select a device.
2. To see a list of physical connections to and from the device, select *Topology*. For more detailed Topology information, click the *Topology* tab.

-or-

If having trouble locating a device, select the device and select *LCD Flash*.

-or-

To reboot a device, select *Reboot*.

To restore a device to factory default settings:

1. Select a device and select *Restore*. When a device is restored, you no longer have access to its current settings. A warning pop-up box will provide an option to restore to full or partial factory default settings.



WARNING! You will not receive a confirmation pop-up box, so ensure that you want to complete the restore process before you proceed.

2. Select the full option to restore master switches to factory default settings at installation. Full restoration moves all devices cascaded off the restored one to an Offline status in the Units pane. Information for these offline cascaded devices can be found by selecting the *Offline Units* tab from the Devices window. Reconfiguring the devices must be done from the Matrix switching system. See the Avocent Matrix High Performance KVM Switching System Installer/User Guide for information on configuring your devices.

-or-

Select the partial option to restore factory default settings to master switches, with the exception of network settings. You do not have to reconnect to the device using a different IP address.

Topology

From the Topology tab, you can see a graphical representation of all of the switches associated with the Manager software. You can drag the nodes (switches) and zoom in and out on the diagram. The numbers displayed on each line indicate the number of physical connections between two switches. By double-clicking on a switch in the diagram or by selecting one or more switches in the tree view, the switch port table with all of the receivers and transmitters that are connected to that switch is displayed. Selecting a receiver or transmitter alone in the tree will display information associated with that receiver/transmitter, including the status. Click on *Export* to export the topology information in .csv format.

4.2.3 Customizing device properties

From the Devices window – Units tab, you can customize properties for switches, transmitters and receivers in your system. Select a device in the Units pane and a Details pane appears below it with the information on your device. Each Details pane has tabs for customization depending on your device type (switch, transmitter or receiver). These options are listed in the following table.

Table 4.1 Details Tabs for Customization

TAB NAME	DEVICE TYPE	DESCRIPTION
Management	Switch	Allows you to view cascade participation and role. You can select a preferred manager for the cascade (in high availability mode) and view the current manager of the cascade.
Attributes	Switch, Transmitter and Receiver	Allows you to view/change device name, electronic ID (EID) and part number information, change location and add notes.
Settings	Switch, Transmitter and Receiver	For the master switch, this allows you to enable/disable banners, set an inactivity time-out for the Matrix switch on-board web interface (OBWI) and enter Syslog destination information. For the transmitter and receivers, you are provided numerous options to enable/disable and can also set a variety of inactivity time-outs.
IPv4	Switch	Allows you to choose the configuration method, IP and gateway addresses, subnet mask and DNS.
IPv6	Switch	Allows you to choose the configuration method, IP and gateway addresses, subnet mask and DNS.
Unit Group	Switch, Transmitter and Receiver	Allows you to see device groups associated with a specific device. Select <i>Add</i> in the Groups: Active Groups pane to add a device group.
EDID	Transmitter and Receiver	Allows you to choose USB video traffic priority, microphone input and icon usage.
Cascade	Switch	Allows you to view the current master switch and peer switch cascade roles. You can also manage the master switch redundancy setup. For more information on master switch redundancy, see the Vertiv™ Avocent® Matrix High Performance KVM Switching System Installer/User Guide.

4.2.4 Managing device sessions

The Matrix Manager administrator can use the Sessions screen to view and manage the active receiver logins and connections. The administrator can force a user to log in or log out of a receiver and connect/disconnect to a transmitter.

To force a user log in to a receiver:

1. From the Dashboard side navigation bar, select *Sessions*.
2. Click *Login*. In the Force Login pop-up box, select a user and receiver, then click *Login* again.

To force a user to log out from a receiver:

1. From the Dashboard side navigation bar, select *Sessions*.

2. Select a valid session and click *Logout*.

NOTE: If a connection exists, the connection will be terminated by the system before log out.

To force a connection to a transmitter:

1. From the Dashboard side navigation bar, select *Sessions*.
2. Select a user and click *Connect*. In the Force Connect pop-up box, select the connection mode required (*Private or Shared*), a transmitter, and then click *Connect* again.

NOTE: Only the transmitter and receiver to which the user has access is displayed. Data is context sensitive.

If a Matrix user is mapped to an external user, then the transmitter list will include the external targets to which he can connect. Matrix transmitters marked as "bridge" will not be displayed in the target list. If the user is not mapped to an external user, then the transmitter list will not show any external targets. However, the transmitter list will show any bridge transmitter if the user has access to the transmitter based on groups and roles permissions. For more information on external KVM and the KVM device bridge, see [External KVM](#) on page 31.

NOTE: Some users must be logged in to a receiver to complete a forced connect.

To force a disconnect from a transmitter:

1. From the Dashboard side navigation bar, select *Sessions*.
2. Click *Disconnect*. In the Force Disconnect pop-up box, select a transmitter, then click *Disconnect* again.

To view the connection path:

1. From the Dashboard side navigation bar, select a session.
2. Click *Connection Path* to view the all of the connections for the session.

Verify sessions

The Matrix Manager software shows up-to-date session information, but you can manually verify if a session still exists.

To verify sessions:

1. From the Dashboard side navigation bar, select *Sessions*.
2. Click the *Verify* button. A message is displayed advising that one or more sessions are verified.
3. Check the event log for details.
4. Click *Close*.

4.3 Managing Extended Display Identification Data (EDID)

EDID is provided by a digital display to describe its capabilities to a video source, such as a graphics card. It enables a device to know what type of monitor is connected to it and lists the monitor name, manufacturer ID, description and product code. The Matrix Manager software allows you to pull this information from master switches and receivers and then push it to transmitters. Decoded EDID is viewed from the side navigation bar by selecting *Devices – EDID* tab.

To customize EDID:

1. From the Dashboard side navigation bar, select *Devices – EDID*.
2. Select the device and select the *Attributes* tab.
3. Customize EDID name and description as needed.
4. Click *Save*.

To view decoded EDID:

1. From the Dashboard side navigation bar, select *Devices – EDID*.
2. Select the device and select the *Decoded EDID* tab. The read-only decoded EDID and raw hexadecimal EDID can be viewed.

To pull EDID:

1. From the Dashboard side navigation bar, select *Devices – EDID* tab – *Pull*.
2. Select a device on the Active Devices pop-up box, click *OK* once and then again to confirm.

NOTE: EDID cannot be pulled from multiple devices simultaneously.

To push EDID:

1. From the Dashboard side navigation bar, select *Devices – EDID* tab.
2. Select the monitor with the EDID to be pushed and click *Push*.
3. Select a device on the Active Devices pop-up box, click *OK* once and then again to confirm.

NOTE: EDID can be pushed to multiple transmitters simultaneously. VGA and DVI EDIDs are not intercompatible.

To delete EDID from the Manager software:

NOTE: This will only delete the EDID from the Manager software. The information can still be pulled from any switch or receiver.

1. From the Dashboard side navigation bar, select *Devices – EDID* tab.
2. Select a monitor and click *Delete* once, then again to confirm.

This page intentionally left blank.

5 ADVANCED OPERATIONS

Now that you have a basic understanding of your Matrix Manager software and have customized it for your system needs, you can increase and streamline current functionality by adding macros and a peer manager to your system.

5.1 Macro Operations

Macros are predefined instructions for designated device connections and are triggered to perform a sequence of actions. Three types of macros (switched presets, follow the leader and multi-video) can be added, edited and deleted within your system. Macro activity is treated as an event by the Matrix Manager software and is logged in the Events log.

5.1.1 Using switched presets macros

Switched presets macros utilize any user logged into a receiver at the time the macro is executed. This macro can be manually executed by the user on the Matrix switch side via the receiver OSD, or from the Matrix Manager software. The following rules apply to a switched presets macro:

- A user must be logged in to a receiver for this macro to be applied. If no user is logged into the receiver, the corresponding connection is skipped.
- A user must have access rights to the transmitter that is designated for a connection by the macro.
- The transmitter designated by the macro cannot be in Private mode.
- Within a macro, no transmitters and receivers should be duplicated.
- Receivers with an active connection must be disconnected before applying a macro. Otherwise, the receiver will be forced to disconnect by the macro.

5.1.2 Using follow the leader macros

With the follow the leader macro, the Matrix Manager software administrator designates a certain transmitter and receiver as “leaders,” known as a trigger pair. When the macro is executed, up to eight receivers can be forced to connect to the same transmitter in the trigger pair. For example, if the trigger pair is Receiver A and Transmitter B, then Receivers C, D and E will all be forced to connect to Transmitter B also. The following rules apply to a follow the leader macro:

- Only one trigger pair is allowed per macro.
- The connection to the trigger pair must be established before other connections are initiated.
- The transmitter in the trigger pair must be set to Share mode to allow other connections.

5.1.3 Using multi-video macros

Multi-video macros allow the administrator to force each receiver in a list to connect to a corresponding transmitter after the trigger pair is established. For example, if the trigger pair is Receiver A and Transmitter B, then the macro can force Receiver C to connect to Transmitter D and force Receiver E to connect to Transmitter F. The following rules apply to a multi-video macro:

- There can only be one trigger pair per macro.
- The connection to the trigger pair must be established before other connections are initiated.

To add a macro:

1. From the Dashboard side navigation bar, select *Devices – Macros tab – New*.
2. Enter a name and description, and select your macro type (*Switched Presets, Follow the Leader or Multi-video macros*) from the drop-down list.
3. If you selected *Switched Presets*, click *New* to add a connection.
4. Enter a Connection Name, select the receiver and transmitter and click *Save*.
5. Next, click *Add* in the Roles pane, select a role, and then click *Add – Save*.

-or-

If you selected *Follow the Leader*, select the receiver and transmitter in the Trigger Connections pane. In the Available Receivers pane, select a receiver and move it to the Assigned column. Click *Save*.

-or-

If you selected *Multi-video mode*, select a receiver and transmitter in the Trigger Connections pane. Then, you can add, edit or delete connections in the Additional Connections pane and click Save.

To delete a macro:

1. From the Dashboard side navigation bar, select *Devices – Macros* tab.
2. Select a macro and click *Delete once*, then again to confirm.

To execute a switched preset macro:

1. From the Dashboard side navigation bar, select *Devices – Macros* tab.
2. Select a macro and click *Execute*.

5.2 High Availability Operations

When using the Matrix Manager software, you can add an additional layer of security and protection to your system to guard from a system failure. A high availability backup instance of the Matrix Manager software is called a peer manager and will automatically take over if failure occurs in your initial system.

5.2.1 Using a peer manager for your system

To use the peer manager, you must install and enroll another instance of the Matrix Manager software. Install the peer version of the Matrix Manager software the same way as the initial version, ensuring the same https ports are used, as detailed in [Installation and Setup](#) on page 3. The default https port is 8443.



WARNING! Before enrolling the peer manager, generate a backup of your data. During enrollment, all data in the peer manager instance will be deleted.

To enroll a peer manager:

1. From the Dashboard side navigation bar, select the *Settings – System* tab – *High Availability* tab.
2. Enter an IP Address/Hostname and the administrator username and password for the peer manager.
3. In the Database Synchronization Frequency field select/enter how often for the peer manager database to synchronize with the initial Matrix Manager software version.
4. Click *Save*.
5. Click *Enroll*. The data between the two instances of the Matrix Manager software is immediately replicated.

To disenroll a peer manager:

1. From the Dashboard side navigation bar, select *Settings – System* tab – *High Availability* tab.
2. Enter the IP Address/Hostname and the administrator username/password of the peer manager to disenroll.
3. Click *Disenroll*.

When the peer manager is enrolled, the status will be displayed in the High Availability Configuration pane. The following table lists the types of status options.

Table 5.1 Peer Manager Status Options

STATUS	DESCRIPTION
Not Applicable	The current Matrix Manager software instance is not in a high availability configuration.
Responding	The current Matrix Manager software instance is in a high availability configuration and is synchronized with the peer manager.
Not Responding	The current Matrix Manager software instance is unable to synchronize with the peer manager.
Certificate Mismatch	Both instances of the Matrix Manager software are unable to synchronize because of a certificate mismatch. Disenroll and enroll the peer manager again.

5.2.2 Using a peer switch

The Matrix High Performance KVM switching system provides the ability to set up a slave switch to be configured as a peer to the master switch. This configuration protects the system against a failure of the master switch. For more information on using a peer switch, see the Vertiv™ Avocent® Matrix High Performance KVM Switching System Installer/User Guide.

The Matrix Manager software can be used to view and manage the current master, peer and slave switches.

To view the cascade roles:

1. From the Dashboard side navigation bar, select the *Devices – Units* tab. Select a switch.
2. From the Management tab, you can view the current cascade participation and current Cascade Role.
3. If a switch that is currently the cascade controller is selected, you will see Cascade tab in the device details. The Cascade tab can be used to view and manage the cascade controller and peer controller roles. The following options are available:
 - Link Peer – Enabled when there is no switch configured as a peer (or backup controller) switch. It allows you select a slave switch to be the peer.
 - Unlink Peer – This is enabled when there is a peer switch enabled. It allows you to unlink the peer switch.
 - Force Role Switch – This enables the user to force a cascade role switch of the current controller and the backup controller.
 - Promote Peer – This is enabled only when the peer switch is acting as the current controller. It allows you to promote the peer switch to the new master switch.

5.3 External KVM

With the Matrix Manager software, you can add an external KVM system and connect to its targets from the Matrix Manager receivers. Currently, the Manager software only supports the AMX™ switch with AMWorks™ java based administration tool software. The AMWorks software can be installed on the same server as the Manager software or on a separate server that the Matrix Manager server can communicate with. In order for the Matrix Manager software to communicate with the AMWorks software server, the AMWorks software system must be configured with all device and user data and be synchronized with the AMX switch. Only one instance of the AMWorks and AMX software switch can be integrated with the Matrix Manager software.

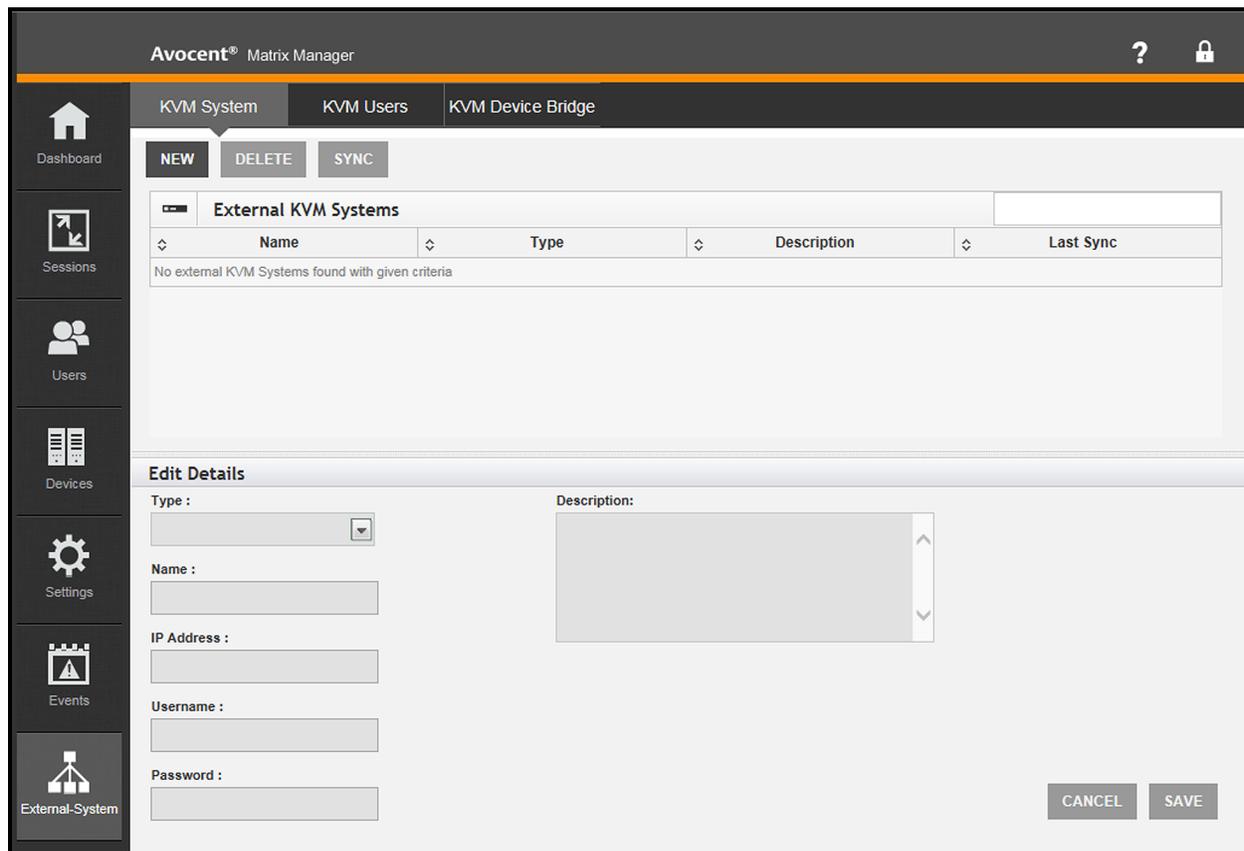
To add an external KVM system:

1. From the Dashboard side navigation bar, select the *External System – KVM System* tab - *New*.
2. On the Add details section, select *AMX* as the type.
3. Enter a name for the external system, then enter the IP address and password to access the AMWorks software system.
4. Enter an optional description and click *Save*.

NOTE: The firewall on the external KVM system must be configured to allow access to port 9734.

5. After the external KVM system is added, you will need to synchronize the user and device information. Click on the *Sync* button to obtain the external KVM system information.

Figure 5.1 Adding an External KVM System



A sync is a one-time operation. If the external KVM system data already exists in the Manager software, then the new information from the sync operation will be used to add, merge or delete external system information in the Matrix Manager software.

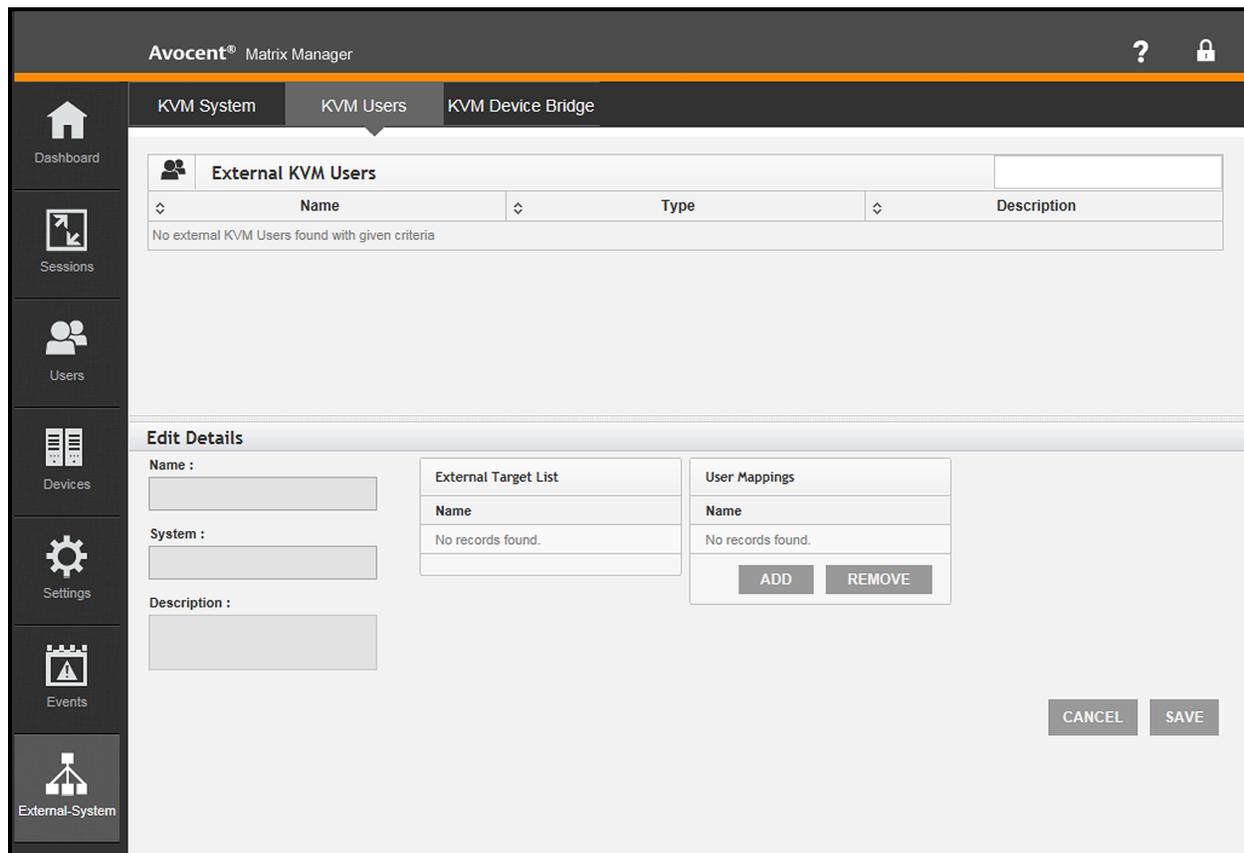
NOTE: It is recommended to perform a sync operation once all data in the external KVM system has been set up. If there is any change in the external system (such as new users or devices) then a sync operation must be performed again in order to update information in the Matrix Manager software.

If a sync operation is initiated when the AMWorks software system is not synchronized with the AMX switch, then all the external system data will be removed from the Manager software.

5.3.1 External KVM users

From the Dashboard side navigation bar, select the *External System – KVM Users* tab. This screen lists all the external users that were retrieved from the external KVM system during the last sync operation. Click on a user to view the details and map the external user to an internal Matrix Manager software user.

Figure 5.2 KVM Users Screen



The Edit Details section of the external KVM Users screen can be used to view the external username, corresponding external system and the list of external targets/transmitters which the user can access.

NOTE: The list of external targets which an external user can access is based on data from the time of last sync operation and may not reflect current information from the external system.

The User Mapping field can be used to map the external user to one or more internal Matrix Manager users. This mapping is necessary and will be used to connect from the Matrix receiver to external targets. When a Matrix user logs into a Matrix receiver, the corresponding external user will be used to calculate the list of external targets that can be accessed.

If a Matrix user is not mapped to any external user then the user cannot access any external KVM targets. However, if a Matrix transmitter that a user has access to is configured as a bridge transmitter, then they can view the external system receiver OSD and can login and connect to external targets.

NOTE: One external user can be mapped to more than one Matrix Manager software internal user, but one Matrix Manager software internal user can be mapped to only one external user.

5.3.2 KVM device bridge

A bridge is a physical setup/connection between a Matrix transmitter and an external KVM system receiver. The bridge is required in order for the Matrix receiver to be able to connect with the external transmitters. The bridge must be set up the same way both physically and logically. An incorrect setup might end up giving connections and access to the wrong external targets.

If a Matrix transmitter is selected to be a bridge transmitter, then it cannot be part of any macros in the Matrix system. If the corresponding transmitter exists as part of any macro, it will be removed from the macro connection.

From the Dashboard side navigation bar, select the *External System – KVM device bridge* tab. Based on the data from the last sync, all of the external KVM receivers are listed. For each receiver the following information is displayed:

- Name (Read Only) – Device name of the external receiver from the external system.
- System (Read Only) – Name of the external KVM system to which this receiver belongs.
- Bridge Status (Read Only) – The value will be N/A unless this receiver is configured to be a bridge.
- Description – Optional description for this external receiver/bridge.
- Device Mapping – If this receiver is physically set up to be a bridge, then a corresponding logical mapping is required to be made in the Manager software. One external receiver can be mapped to one Matrix transmitter. The transmitter and receiver also need to be physically configured as a bridge.

6 APPENDICES

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. For additional assistance, visit <https://www.VertivCo.com/en-us/support/>

This page intentionally left blank.

6.1 Appendix A: External KVM Best Practices

This section should be read, if applicable, before installing Matrix Manager software. The following additional information is recommended for adding an external KVM system into the Matrix Manager software. For firmware requirements, refer to the product release notes.

The AMWorks™ software, AMX™ devices and switches, Matrix Manager software and Matrix devices and switches must all be in the same network and must be able to communicate with each other at all times.

NOTE: Disable the firewall or open the firewall ports to https port 8443 for the Matrix Manager software and to TCP port 9734 on the AMX switching system.

6.1.1 AMWorks™ software recommendations

The following are recommendations for AMWorks software integration with Matrix Manager software.

- It is recommended after set up that the network settings or the IP address of any of the software servers or devices are not changed. Do not change the AMWorks software IP address or the Matrix Manager software IP address after adding the AMWorks software into the Matrix Manager software. If the IP changes, then the AMWorks software system must be deleted and added to the Manager software.
- Before adding AMWorks software into the Matrix Manager software, all configurations and data establishment should be set up in the Matrix Manager software. Initiate a manual sync process to gather the updated device, user and access rights information from the AMWorks software system.
- The new AMWorks software system must be running at all times to serve the remote API call from the Matrix system.
- In order to be able to communicate with the AMWorks, Matrix Manager software should be running in an IPv4 supported environment because the AMWorks system works only in an IPv4 environment.

Shared, exclusive and private mode guidelines

- Shared mode will be only available within the AMWorks software system.
- The Matrix system connection to AMX switching system targets will always be in private mode.
- Since the bridge runs in exclusive mode, the number of bridges must be equivalent to the number of simultaneous connections required to AMX switching system targets.

6.1.2 AMX™ switching system recommendations

The following are recommendations for AMX switching system integration with Matrix Manager software.

- All bridge receivers in the AMX switching system must be directly connected to the AMX master switch.
- The new AMWorks software system must always be in sync with the master AMX switch.



CAUTION: Do not attempt to perform a sync operation when the AMWorks software system is not synchronized with the AMX switch. This may lead to deleting all AMX switch user and device records in the Manager software.

- The connection time will take an average of 3 to 12 seconds when connecting to AMX switch targets or when switching targets with AMX switch targets involved.
- Do not perform firmware upgrades when there is an active connection to AMX switch target. Reboot or turn off any of the involved and corresponding switches or devices.
- Changes made in the AMX switching system are not automatically reflected in Matrix system.

6.1.3 Matrix Manager software recommendations

The following are recommendations for AMWorks software and AMX switching system (together) integration with Matrix Manager software.

- It is recommended that only one Matrix Manager software system administrator perform all tasks related to adding the AMX switching system, including performing the sync and bridge set up.

- During the process of adding the external KVM system or performing the sync operations, it is recommended that no other changes occur in either Matrix or the external KVM systems.
- When performing user mapping in the Manager software, please verify and note of the permissions of the user in the Manager software and the AMWorks software system. If MatrixUser1 is mapped to AMXUser1, then access to all AMX targets of AMXUser1 will be available when MatrixUser1 logs into the Matrix receiver.

NOTE: The permissions from the AMX™ switching system are not real-time; they correspond to the permissions at last user-initiated sync time.

Bridge set up recommendations

- Physically set up bridges before adding to the Matrix Manager system.

NOTE: When logically mapping the devices in the Manager software, ensure the Manager software matches the physical bridge.

- The Matrix VGA transmitter connected to the AMX bridged receiver must be turned on first.
- After the Matrix VGA transmitter connected to the AMX bridged receiver is discovered and connected to the Matrix switch, then connect the AMX receiver. USB control of the Matrix VGA transmitter connected to the AMX bridged receiver will be available via AMX switch OSD functionally or directly to the selected target connected through the AMIQ module.



VertivCo.com | Vertiv Headquarters, 1050 Dearborn Drive, Columbus, OH, 43085, USA

© 2017 Vertiv Co. All rights reserved. Vertiv and the Vertiv logo are trademarks or registered trademarks of Vertiv Co. All other names and logos referred to are trade names, trademarks or registered trademarks of their respective owners. While every precaution has been taken to ensure accuracy and completeness herein, Vertiv Co. assumes no responsibility, and disclaims all liability, for damages resulting from use of this information or for any errors or omissions. Specifications are subject to change without notice.

590-1739-501A