USER MANUAL

BXAMGR-R2

BOXILLA® KVM MANAGER

FOR BOXILLA 5.1.5 AND LATER

BLACK BOX®

TABLE OF CONTENTS

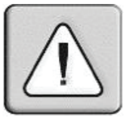
TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

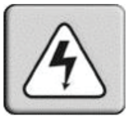
SYMBOLS USED IN THIS MANUAL

INSTRUCTIONS



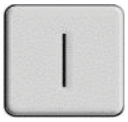
This symbol is intended to alert the user to the presence of important operating and maintenance (servicing) instructions in the literature accompanying the appliance.

DANGEROUS VOLTAGE



This symbol is intended to alert the user to the presence of uninsulated dangerous voltage within the product's enclosure that may be of sufficient magnitude to constitute a risk of electric shock to persons.

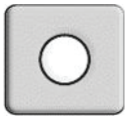
POWER ON



This symbol indicates the principal on/off switch is in the on position.

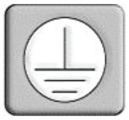
SYMBOLS USED IN THIS MANUAL

POWER OFF



This symbol indicates the principal on/off switch is in the off position.

PROTECTIVE GROUNDING TERMINAL



This symbol indicates a terminal that must be connected to earth ground prior to making any other connections to the equipment.

CHAPTER 1: SPECIFICATIONS

TABLE 1-1. SPECIFICATIONS

SPECIFICATION	DESCRIPTION
Approvals	FCC, ICES-003 ISSUE7, CE, UKCA, CB, BIS
Connectors	(2) 10/100/1000 Ethernet (RJ-45) network connectors, Serial (RJ-45), (2) USB 2.0 (USB Type A), VGA
Power	AC input: 120–240 V, 50–60 Hz
Power Dissipation	<75 W (PSU rated for 250 W)
Dimensions	1.7” H x 17.25” W x 17.5” D (4.3 x 43.8 x 44.5 cm)
BTU	255.75 (Avg), 852.5 (Max)
Weight	Unit: 12.6 lb. (5.7 kg)
MTBF	55,019 Calculated Hours at 40°C (Telcordia SR-332)
Compatibility	Works with Emerald® Unified KVM (EMD200DV-T, EMD200DP-T, EMD4000R, EMD4000T, EMD2000SE-T, EMD2002SE-T, EMD2000SE-R, EMD2002SE-R, EMD2000PE-T, EMD2002PE-T, EMD2000PE-R-P, EMD2002PE-R-P, EMD2000SE-DP-T, EMD2002SE-DP-T, EMD2000SE-DP-R, EMD2002SE-DP-R, EMD2000PE-DP-T, EMD2002PE-DP-T, EMD2000PE-DP-R, EMD2002PE-DP-R, EMD2000SE-T-R2, EMD2000PE-T-R2. EMD2002PE-T-R2, EMD5004-R, EMD5104-R, EMD5004PE-R, and EMD3000GE) and DKM (multiple part numbers), EMS 1G/10G/100G Network Switches, and EMD100USB
Serial Port Configuration	115,200 baud, 1 Stop bit, No Parity, No Handshake
Default IP Address	192.168.1.24
Default Username	admin
Default Password	admin

WARNING: Unit does not contain any user serviceable parts inside. Do not open product, risk of electrical shock.

CHAPTER 2: PRODUCT OVERVIEW

Boxilla® is a state-of-the-art KVM Manager designed to provide pro-active support to the System Manager and enable efficient operation of KVM and AV systems. Its core focus is to provide simple mechanisms to discovery, configure, upgrade and monitor the deployed systems. It provides insight into performance of the deployed system and alerts the System Manager to potential performance or security issues. Comprehensive features include:

- automatic search and detection of Black Box® products (discovery),
- device configuration across multiple sites (if using the right network architecture and configuration)
- configuration backup,
- central upgrades,
- performance and security statistics with user-defined triggers for alerts.

Using the intuitive Boxilla web-based interface, one or more administrators can manage potentially thousands of users who are interacting with an almost unlimited number of devices. Boxilla operates as a self-contained compact server unit that can be located anywhere within your network. Boxilla is supplied pre-loaded and is straightforward to deploy, requiring only a network connection and a power input to begin operation.

The current version of Boxilla provides management of Black Box's Emerald® GE, DESKVUE, and Emerald system, Modular and Compact DKM KVM Matrix Switches, DESKVUE, EMD100 USB 2.0 Switching Extenders, and Black Box EMS L2 Network Switches. The Emerald GE, Emerald, or DESKVUE system provides users with a seamless desktop experience anywhere on a TCP/IP network, while allowing the actual hardware to be securely housed in a corporate data center or in the cloud.

IMPORTANT: Going forward through this manual, we will reference the term Appliances, which will encompass the Emerald GE, DESKVUE, and Emerald transmitters and receivers. If only one or a few apply, they will be called out individually.

The appliances enable the same high-fidelity experience of a desktop PC even for media-rich applications, for example, watching videos, photo editing with Photoshop or 3D design with AutoCAD. The remote desktops may be hosted on a physical PC / workstation or may be a virtual desktop hosted on a private server or in the cloud. The appliances provide its users with Receivers that communicate with target computer nodes (whether physical PC or virtual desktop) over a standard TCP/IP network. Physical PCs/Workstations/Servers have an Emerald Transmitter unit physically connected to provide communication over the TCP/IP network. The performance of the appliances allows them to be deployed on standard corporate networks and even across Wide-Area-Networks (WANs).

Desktop users can use remote keyboard, mouse, video, audio, USB mass storage devices, headsets and other USB devices from the Receiver unit to the remote PC/workstations or Virtual Desktop via the appliances.

The appliances can be composed of just Receivers and Transmitters without a Boxilla manager. In these types of systems—called unmanaged— there is no central management. Each device needs to be configured and upgraded individually. Often to keep the system in sync, the admin exports the configuration from one Receiver and imports it to all other Receivers using a USB Flash Drive formatted as FAT32.

For larger configurations, a central manager is needed—Boxilla. Boxilla operates as a central manager for a "managed domain." A managed domain is a collection of appliances managed by a Boxilla. Once a Receiver or Transmitter has been added to a managed domain, it can only communicate with other Receivers or Transmitters within this managed domain. They are not able to communicate to "unmanaged" devices or devices that are part of a different managed domain (i.e., a domain managed by a different manager). Boxilla is used to configure users, connections, hotkeys and other parameters. The database created on the Boxilla is synchronized to each Receiver on a Boxilla user login. If the Boxilla for the managed domain is not reachable (e.g. powered-down), the Receiver will use the last updated database. This ensures that there is no single point of failure in the managed domain. Users can login and connections can be made even if the manager of the domain is not reachable.

When a Receiver is managed, most of the configuration options on the OSD are disabled (i.e., grayed out). These configuration options can only be updated on the manager.

CHAPTER 2: PRODUCT OVERVIEW

A Boxilla® system can also include IP network switches. Black Box offers the following:

- 24-Port 1G Fiber IP Network Switch (EMS1G24F)
- 48-Port 1G IP Network Switch (EMS1G48)
- 12-Port 10G IP Network Switch (EMS10G12)
- 28-Port 10G IP Network Switch (EMS10G28)
- 32-Port 100G IP Network Switch (EMS100G32-R2)

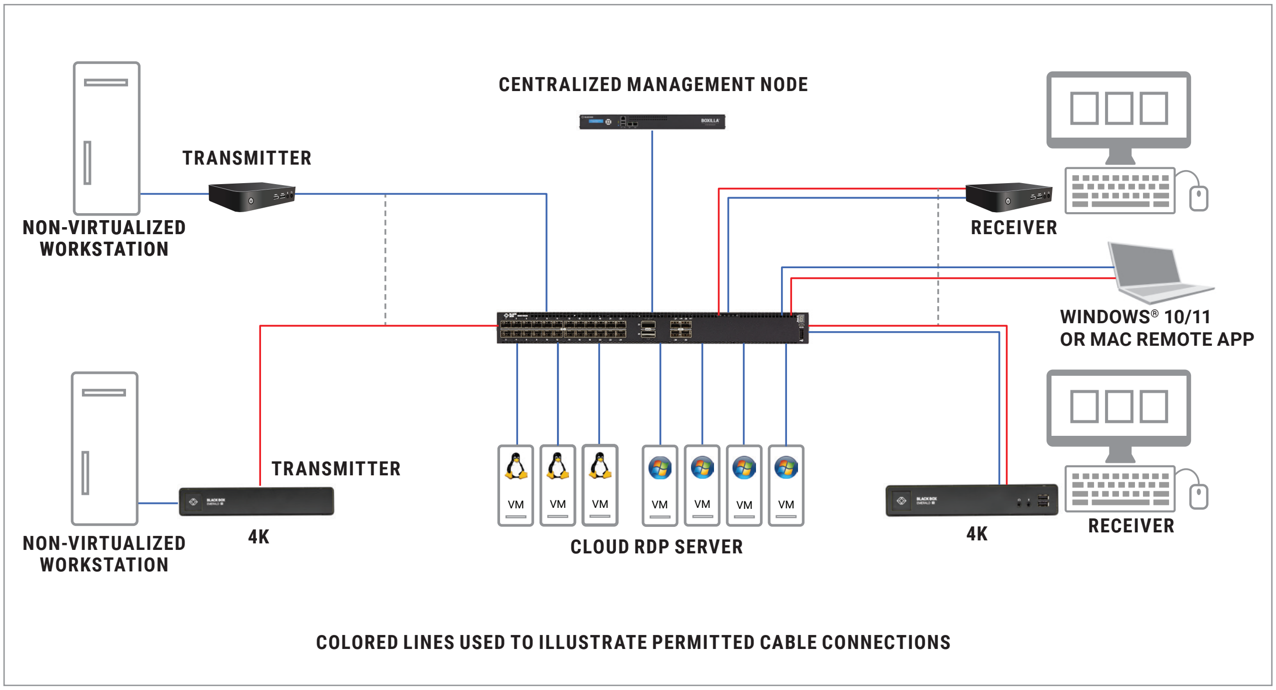

CENTRALIZED MANAGEMENT NODE
TRANSMITTER
NON-VIRTUALIZED WORKSTATION
RECEIVER
WINDOWS® 10/11 OR MAC REMOTE APP
TRANSMITTER
4K
NON-VIRTUALIZED WORKSTATION
VM
VM
VM
VM
VM
VM
VM
CLOUD RDP SERVER
4K
RECEIVER
COLORED LINES USED TO ILLUSTRATE PERMITTED CABLE CONNECTIONS

FIGURE 2-1. BASIC APPLIANCE NETWORK INCLUDING THE EMS NETWORK SWITCH

2.1 OVERVIEW OF BOXILLA CONCEPTS

The product family is composed of Receivers, Transmitters, USB 2.0 extenders, virtual machine brokers, multiviewer, and network switches. DESKVUE is a Multiviewer Receiver that can connect to existing Emerald Transmitters, Virtual Machines, and other types of AV streams. Boxilla is the Enterprise class Manager for the appliances (which are Emerald GE, DESKVUE, and Emerald), Modular and Compact DKM KVM Matrix Switches, Black Box IP Network Switches, and EMD100USB USB 2.0 Transmitters and Receivers. The core design of the appliance architecture is that there is no single point of failure. This means that even if Boxilla goes off-line, the appliances will continue to function—allowing users to login, make connections and operate the system as normal. When the Boxilla manager comes back on line, the various devices will update Boxilla with their performance and security statistics from the period it was offline.

2.2 BOXILLA MANAGED DOMAIN

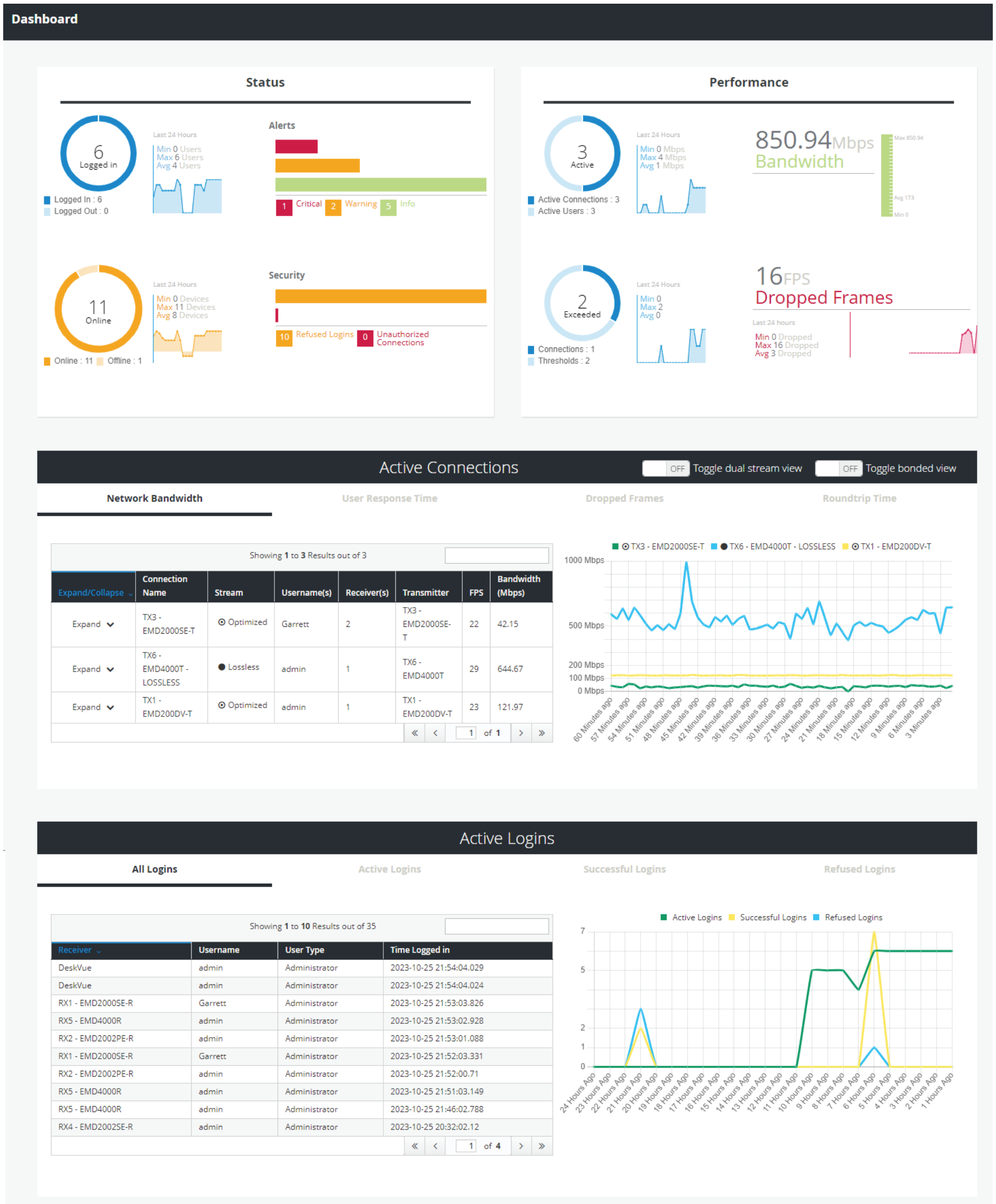
Boxilla® creates a managed domain—a set of devices it manages. Devices that are members of this managed domain can only be managed by this Boxilla unit. Devices in a managed domain can only connect to other devices in the managed domain. No other manager or unmanaged device can configure or connect to devices in this managed domain.

A managed domain is composed of:

- Boxilla Manager—to centrally create, configure and monitor domain;
- Appliances—KVM and AV appliances that can communicate with each other. In the current release, Emerald GE, Emerald, and DESKVUE devices, DKM KVM Matrix Switches, Black Box IP Network Switches, and EMD1000 USB 2.0 Extenders are supported;
- Users—provides various login rights for different users such as their access rights (what connections they can make, level of control they have to change configurations);
- Connections—defines how a Receiver can connect to a Transmitter or a Virtual Machine with properties such as private or share mode, USB redirection enabled or disabled among others;
- Alerts—events detected by Boxilla in the managed domain (such as new device added, firmware upgrade, connection made) and classified as critical, warning or info based on nature of event.

As part of creating a managed domain, the administrator will add Devices to the domain, create Users, define Connections and set Alerts. The following sections will describe how to do this with Boxilla.

Once a domain has been defined (devices, users, connections, etc.) Boxilla monitors the operation of the domain, reports on its performance and indicates any security events detected. The monitoring of the system is presented to the user in advanced graphical and tabular formats. Typically the dashboard is used to get an overview of the domain's operation. An example of the Dashboard is shown in Figure 2-2. From the dashboard the administrator can drill down for more detail on activity, errors and individual devices.



Dashboard

Status

Performance

Active Connections

Showing **1** to **3** Results out of 3

Expand/Collapse	Connection Name	Stream	Username(s)	Receiver(s)	Transmitter	FPS	Bandwidth (Mbps)
Expand	TX3 - EMD2000SE-T	⊙ Optimized	Garrett	2	TX3 - EMD2000SE-T	22	42.15
Expand	TX6 - EMD4000T - LOSSLESS	● Lossless	admin	1	TX6 - EMD4000T	29	644.67
Expand	TX1 - EMD200DV-T	⊙ Optimized	admin	1	TX1 - EMD200DV-T	23	121.97

« ‹ 1 of **1** › »

Active Logins

Showing **1** to **10** Results out of 35

Receiver	Username	User Type	Time Logged in
DeskVue	admin	Administrator	2023-10-25 21:54:04.029
DeskVue	admin	Administrator	2023-10-25 21:54:04.024
RX1 - EMD2000SE-R	Garrett	Administrator	2023-10-25 21:53:03.826
RX5 - EMD4000R	admin	Administrator	2023-10-25 21:53:02.928
RX2 - EMD2002PE-R	admin	Administrator	2023-10-25 21:53:01.088
RX1 - EMD2000SE-R	Garrett	Administrator	2023-10-25 21:52:03.331
RX2 - EMD2002PE-R	admin	Administrator	2023-10-25 21:52:00.71
RX5 - EMD4000R	admin	Administrator	2023-10-25 21:51:03.149
RX5 - EMD4000R	admin	Administrator	2023-10-25 21:46:02.788
RX4 - EMD2002SE-R	admin	Administrator	2023-10-25 20:32:02.12

« ‹ 1 of **4** › »

FIGURE 2-2. DASHBOARD EXAMPLE

A Manager's User Profile is protected by a username and password to permit different users to access the same unit securely. It maintains the central database that is distributed to all Receivers in the "domain" of the Manager (i.e. discovered and added to manager)— called the "managed domain." This distribution ensures that there is no single point of failure in the appliances—each Receiver has a copy of the database. This enables each Receiver to continue operation—log users in, make connections as required—even if the Manager goes off-line.

NOTE: At this time the Boxilla® Administrator can only be configured/edited within Boxilla and cannot use an Active Directory user account.

2.3 BOXILLA SCREEN LAYOUT

Boxilla is designed to provide quick access to key operational functions. This is achieved by the use of the Main Menu and Quick Access Toolbar as shown in Figure 2-3. The Main Menu provides access to:

- Dashboard
- Devices
- Switches
- Peripherals
- Zones
- Connections
- Users
- DKM
- System
- License
- Cluster
- Discovery
- Alerts

The Quick Access toolbar provides access to active Alerts, access to Help and access to Logout.

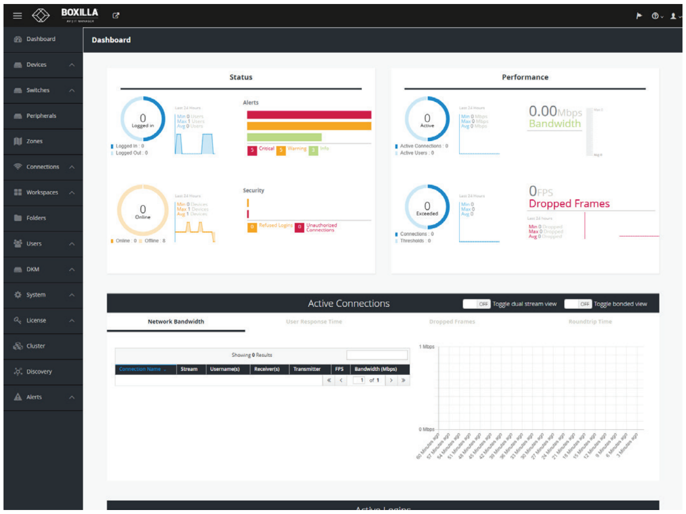
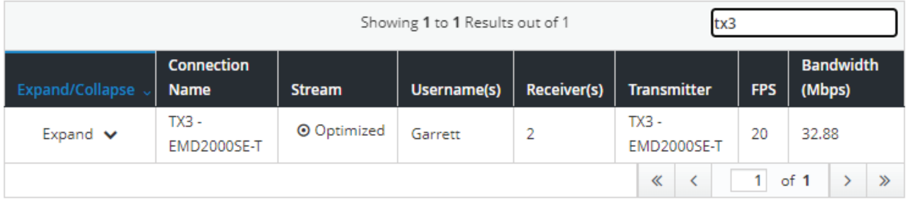


FIGURE 2-3. SCREEN LAYOUT

A common feature of tables in Boxilla® is that they can be sorted by each column (alphabetically either ascending or descending). Click on the column's label (e.g. Connection Name) and the table will be sorted by that column in ascending order. Click on the same column label again and the order will be reversed. Also, a filter can be applied to the values in the column to pick out a subset of rows in the table. For example, typing in tx3 into the filter box in the Network Bandwidth table in Active Connection section of the Dashboard in Figure 2-4 would result in three instead of four rows being displayed as shown in Figure 2-4.



Showing **1** to **1** Results out of 1

tx3

Expand/Collapse	Connection Name	Stream	Username(s)	Receiver(s)	Transmitter	FPS	Bandwidth (Mbps)
Expand	TX3 - EMD2000SE-T	⦿ Optimized	Garrett	2	TX3 - EMD2000SE-T	20	32.88

« ‹ 1 of **1** › »

FIGURE 2-4. FILTERING TABLE

2.4 MODES OF OPERATION

The DESKVUE and Emerald® system has various modes of operation, such as Auto-Login, Auto-Connect, Private Connection, Shared Connection, View Only, and Exclusive Connection Modes. They can obtain their IP address data from a DHCP server in any of these modes or use static addresses. For stable operation with Boxilla, we strongly recommend that Static IP addresses are assigned to the appliances or that you use DHCP addresses with "infinite time-outs."

2.4.1 AUTO LOGIN

In Auto-Login Mode, turning on the receiver appliance automatically causes a login as a pre-defined user. The user is presented with the permitted connections that have been predefined.

2.4.2 AUTO CONNECT

In Auto-Connect Mode, when a user logs-in to the receiver appliance, it causes an automatic connection to their pre-allocated workstation or virtual desktop. Auto-Login and Auto-Connect are defined independently of each other.

2.4.3 PRIVATE CONNECTION

In Private Connection Mode, when a user makes a connection to a target workstation/virtual desktop, this connection is only accessible by this user. All other users will receive a "busy" message if they attempt to connect to the same workstation/virtual machine. This is the default mode for connections.

2.4.4 SHARED CONNECTION

In Shared Connection Mode, multiple users can connect to the audio and video of the same target computer over the network. They arbitrate for control of the keyboard and mouse of that computer. Non-keyboard and mice devices are not supported on shared connections.

2.4.5 VIEW ONLY MODE

A connection can be configured for View Only mode, which allows a user to make a connection and only have viewing access, keeping their keyboard, mouse, and any input devices disabled. This connection mode is good for monitoring systems, without adding risk of disrupting the session.

2.4.6 EXCLUSIVE MODE

The Boxilla® administrator can define a connection parameter of Exclusive mode for physical transmitters and receivers only. This Exclusive connection (Exclusive Shared connection) allows for a single user to have full keyboard and mouse control while seeing video, and it supports USB redirection. Additional users on the same connection are in view-only mode. This connection can support one user who has full control and up to seven view-only-mode users. The view-only-mode users are able to use the keyboard and mouse hot-keys only to go back to the OSD or connect to another target using Favorites without affecting the existing session. If a user connects using "Shared" Exclusive to an existing shared only connection, the user who used the "Shared" Exclusive connection will have keyboard and mouse control, and the other users revert back to a view-only mode.

Upon terminating a "Shared" Exclusive connection, the remaining active users in that same connection will revert back to shared mode.

NOTE: Exclusive Connections are supported on every Emerald transmitter and receiver, but they are not supported on RemoteApp, DESKVUE, or when connecting to a virtual machine.

CHAPTER 3: APPLICATIONS

The appliances are architected to be flexible so they can be deployed in many different types of applications such as basic extension, switching applications (sometimes called matrix), cloud-based desktops, control rooms, digital signage and kiosk applications among others in banking, financial services, broadcast, network operations, industrial, government and enterprise computing sectors. These devices provide state-of-the art performance by:

- using digital sources for video and audio, hence removing analog noise issues or other potential environmental issues;
- using advanced optimized compression to enable visually lossless video over standard low-bandwidth networks rather than a proprietary connection or dedicated gigabit networks of many systems.

3.1 VIDEO, AUDIO, AND USB SWITCHING

Numerous applications require being able to switch between different target PCs or Virtual Desktops. The user wants to be able to change the source of Video, Audio or USB extension (or all three together).

Connections can be made to a target using the receiver appliance’s intuitive On-Screen-Display (OSD) and/or the Emerald RemoteApp. Figure 2-1 in the previous section shows an example of a switching or matrix type of deployment. In this deployment, there are several Receivers and Transmitters and a Boxilla manager as well as virtual desktops.

See www.blackbox.com for the full catalog of available appliances.

CHAPTER 4: INITIAL INSTALLATION

4.1 HARDWARE DESCRIPTION

A Boxilla® manager is supplied with the items shown in Table 4-1. (1) Boxilla Manager, 1RU

TABLE 4-1. WHAT'S INCLUDED

ITEM
Boxilla Unit
(1) US power cord
(1) DB9-F to RJ-45 console cable
(1) Network cable, RJ-45 to RJ-45
(4) rubber feet
(2) Brackets with pull loops
(16) Screws
(2) Rackmount rails

Once the contents of the Boxilla package have been verified, the first task is to configure the IP address of the unit. This can be set in two ways: (1) using the serial port and (2) using the network port via a browser. It is recommended and easier to configure the Boxilla IP address by using the web interface by setting your laptop/computer to a 192.168.1.x (not .24), then trying to connect to the Boxilla using 192.168.1.24, then logging in, and changing the IP settings.

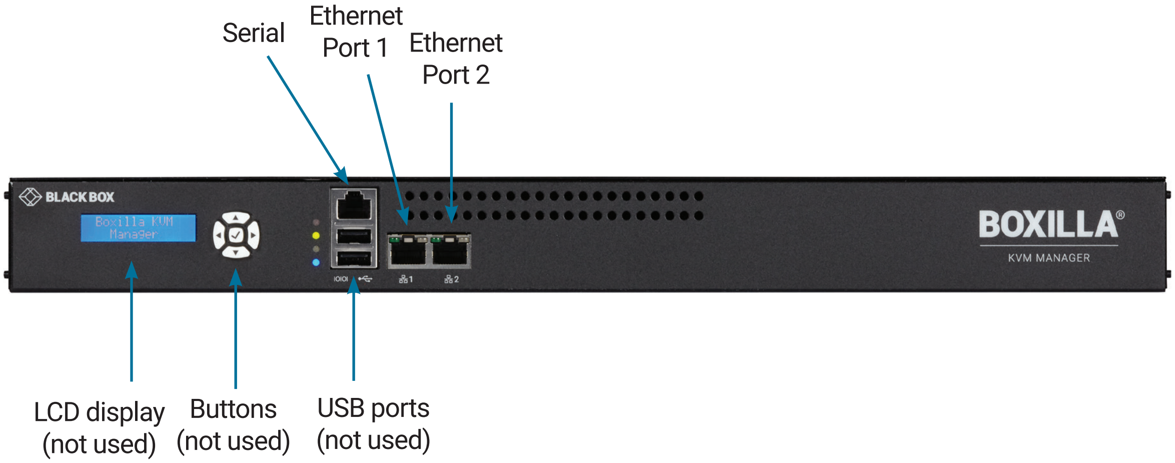


FIGURE 4-1. BOXILLA FRONT PANEL

CONNECTORS NEEDED FOR INSTALLATION

- Serial Port (RS-232 access port to display Boxilla menus using the included adapter; can be used to find the IP or factory reset the controller)

Note: The Serial / RS-232 port is not required for setup if able to access/configure the Boxilla through a web browser.

- Ethernet Network Ports (1 = Primary/default network port; 2 = Secondary network port)
- Power connector (on back of unit)

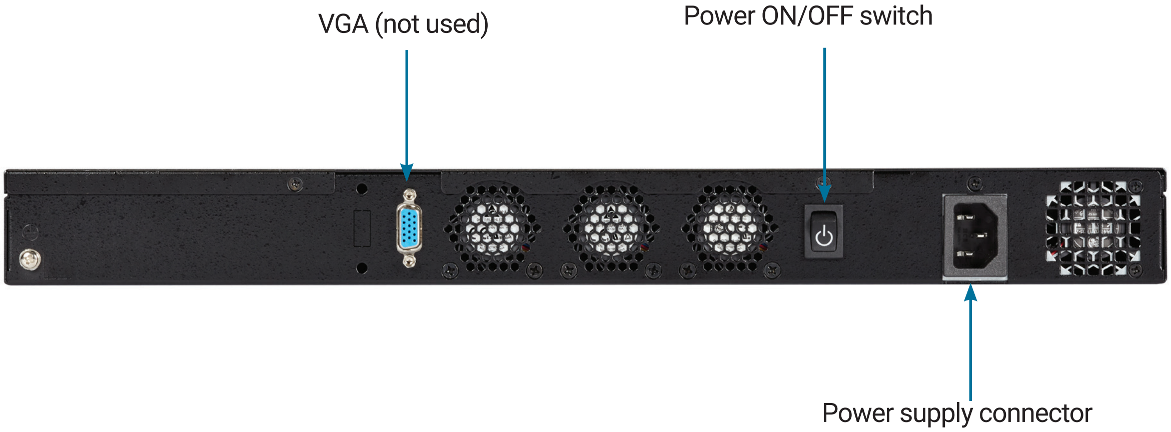


FIGURE 4-2 BOXILLA REAR PANEL

TABLE 4-2. PANEL COMPONENTS

COMPONENT	DESCRIPTION
HD15 female port	Not used
(2) Network ports	1G Ethernet RJ-45 connectors
Power switch	ON/OFF switch
IEC 320 C14	100–240 VAC, 50-60 Hz

CONNECT THE POWER

1. Locate the AC power cord.
2. Attach the AC power cord to the power supply connector on the rear of the unit.
3. Power up the unit by turning on the power switch on the back of the unit.

4.2 LED IDENTIFICATION

Two LEDs are built into the RJ-45 connectors on the Boxilla® Manager. The definition of the operation of these LEDs is shown in Table 4-3.

TABLE 4-3. RJ-45 CONNECTOR LEDS

LED	INDICATION	MEANING
Speed	Green ON	1 Gbps link
	Amber ON	100 Mbps link
	OFF	10 Mbps link
Activity	Amber blinking	Valid link
	OFF	No link

CHAPTER 4: INITIAL INSTALLATION

4.3 MOUNTING BOXILLA IN A RACK

The Boxilla® unit is designed to be easy to mount within a standard 19" rack. The unit requires just a 1U space within the rack.

To mount the Boxilla unit within a rack:

1. Release and detach the inner member from the slide.

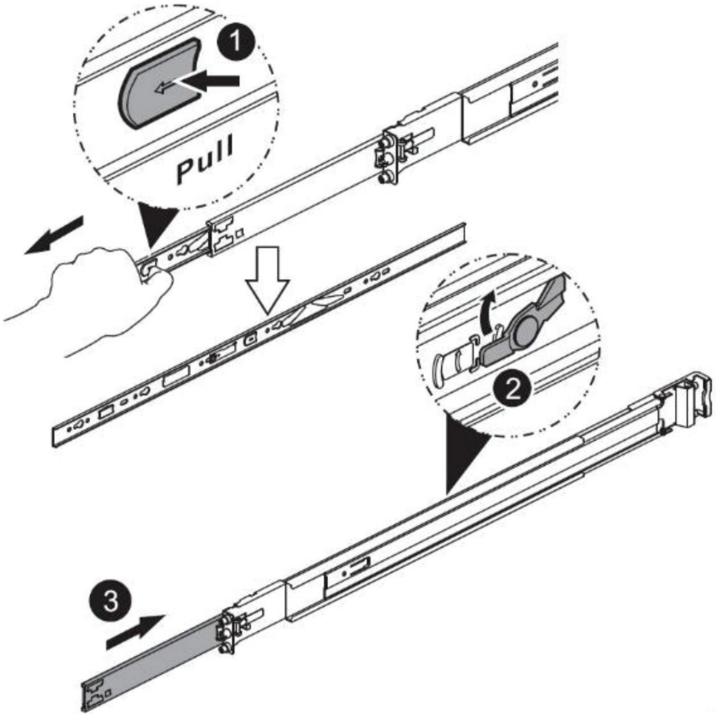


FIGURE 4-3. MOUNTING BOXILLA STEP 1

2. Attach the inner member to the system. For safety, the user can fasten the screw on the end of the inner rail while assembling the chassis.

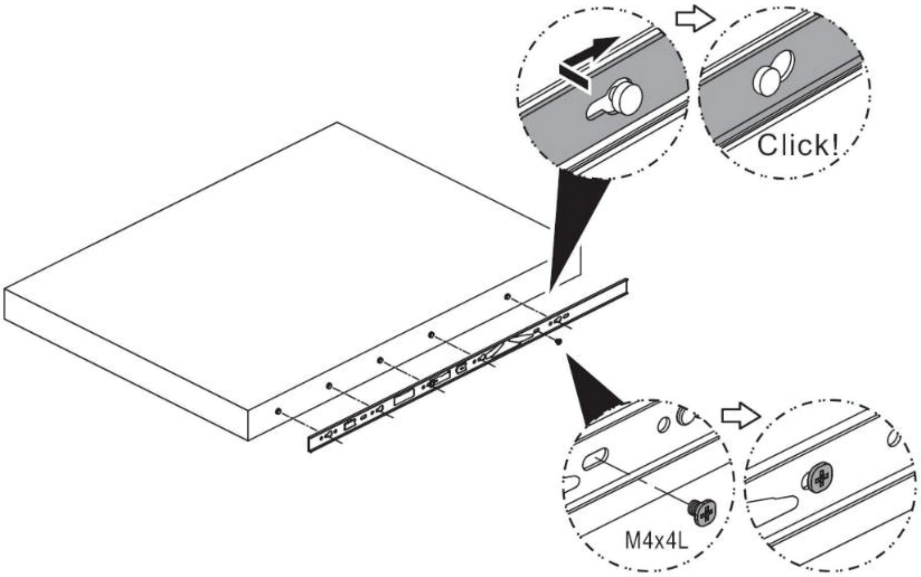


FIGURE 4-4. MOUNTING BOXILLA STEP 2

3. Attach the outer member to the rack.

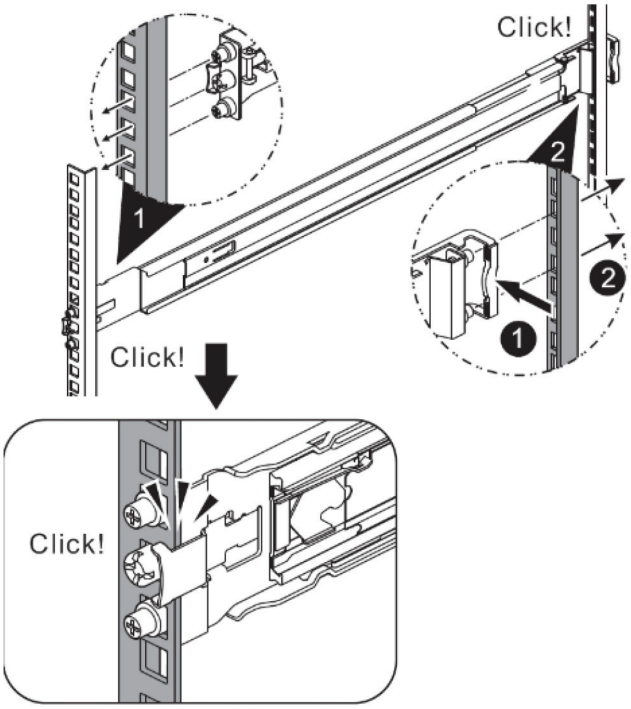


FIGURE 4-5. MOUNTING BOXILLA STEP 3

4. CAUTION: Verify that the ball bearing retainer is locked forward.

5. Horizontally install the system half way into the side rail.

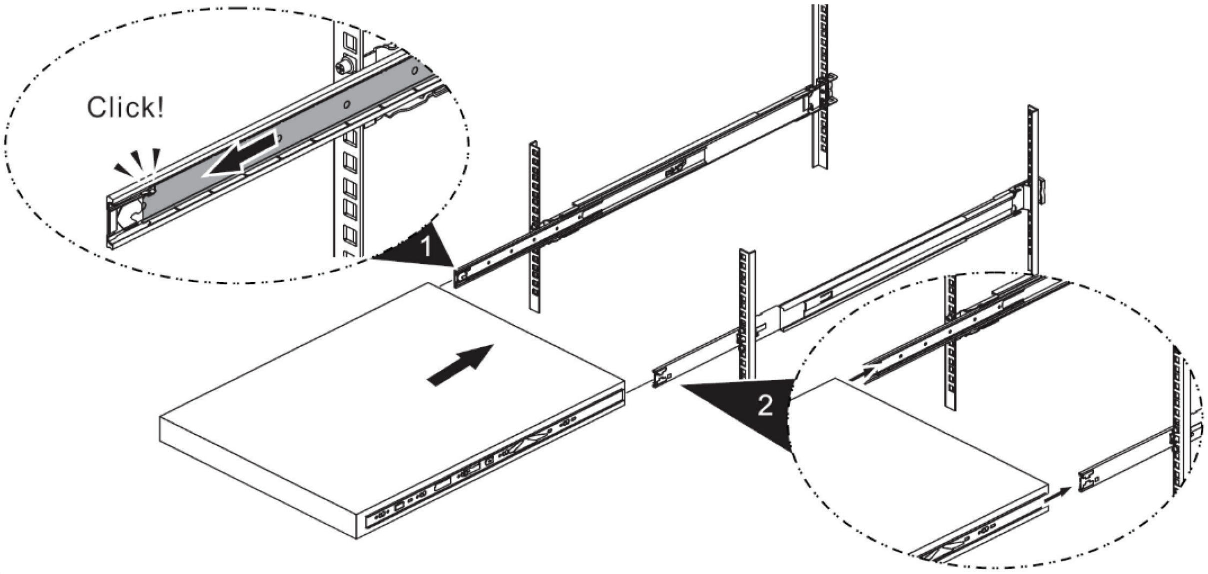


FIGURE 4-6. MOUNTING BOXILLA STEPS 4 & 5

6. Slide the release tab and push the system into the rack.

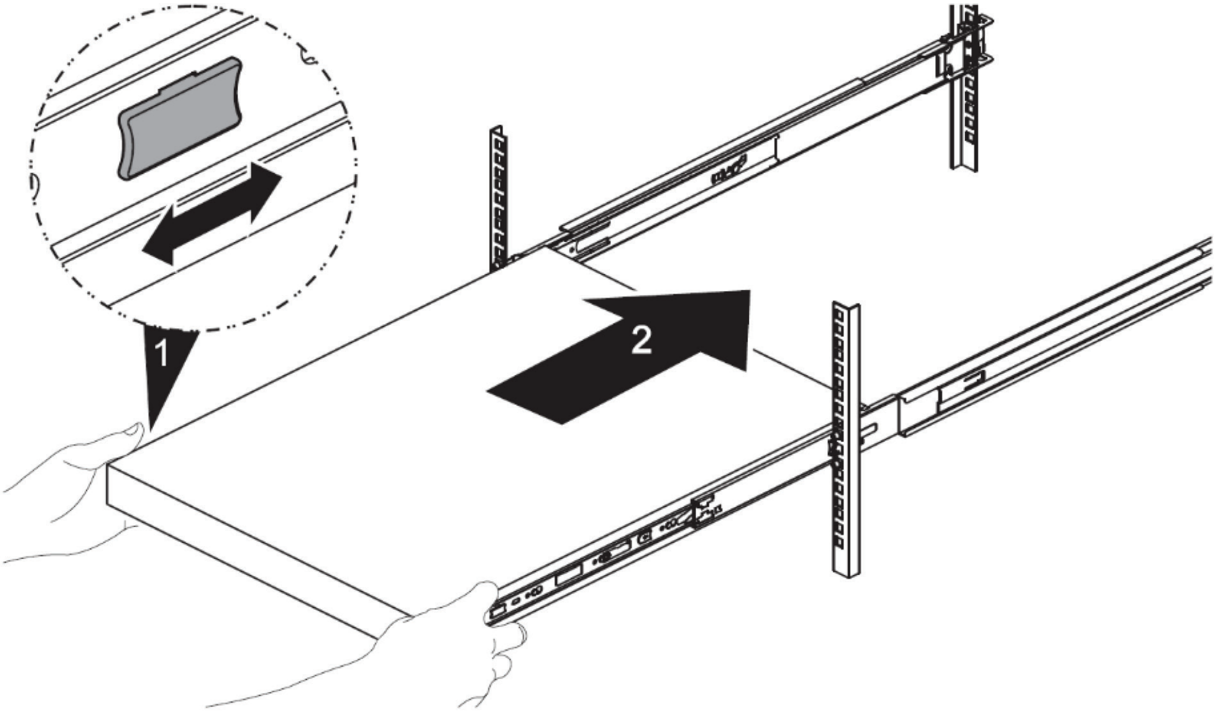


FIGURE 4-7. MOUNTING BOXILLA STEP 6

Rack Mount Bracket

1. Identify the correct orientation for your right and left mount bracket.

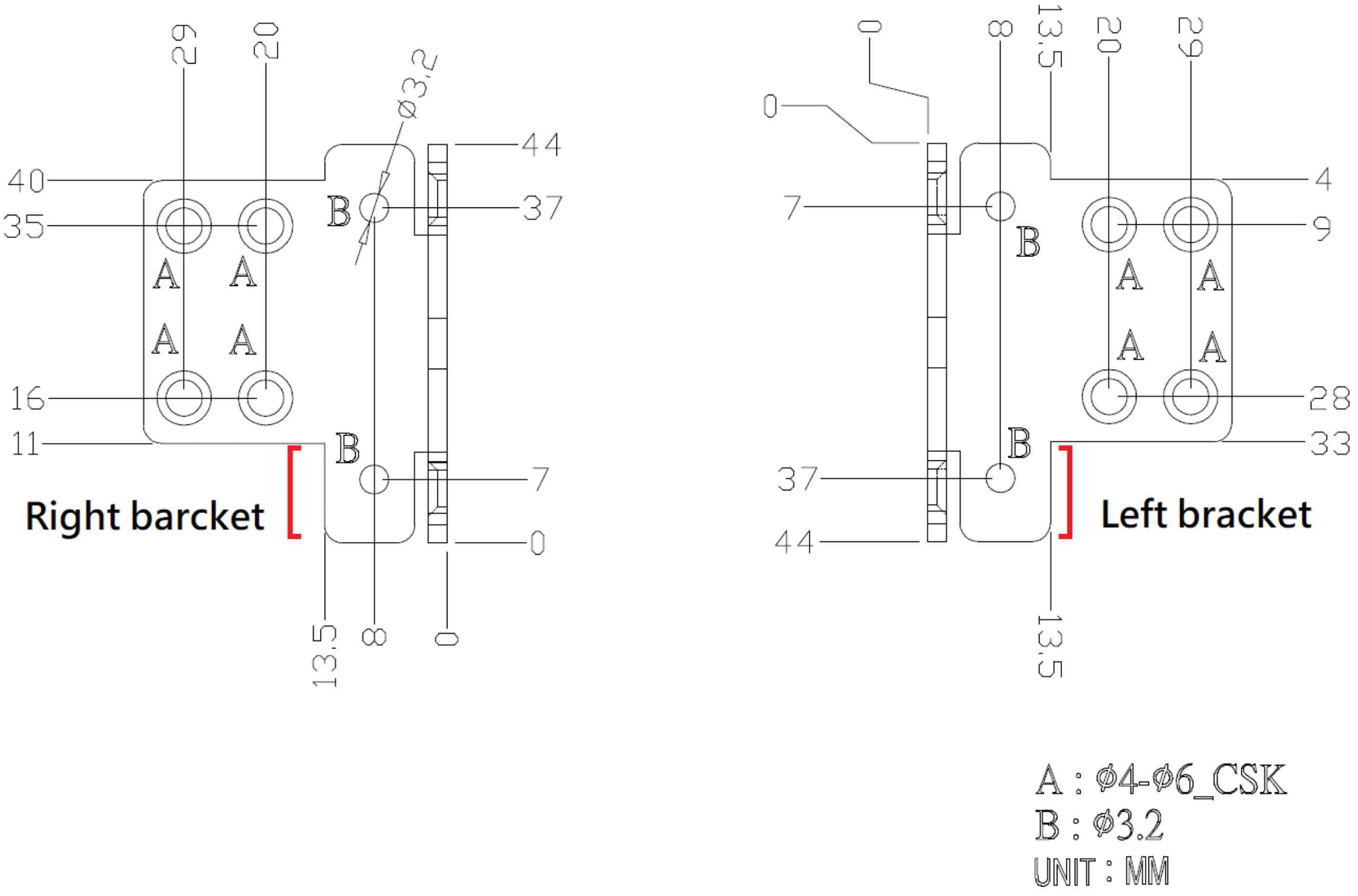


FIGURE 4-8. BRACKET ORIENTATION

2. Fasten the two brackets by tightening four screws per side.

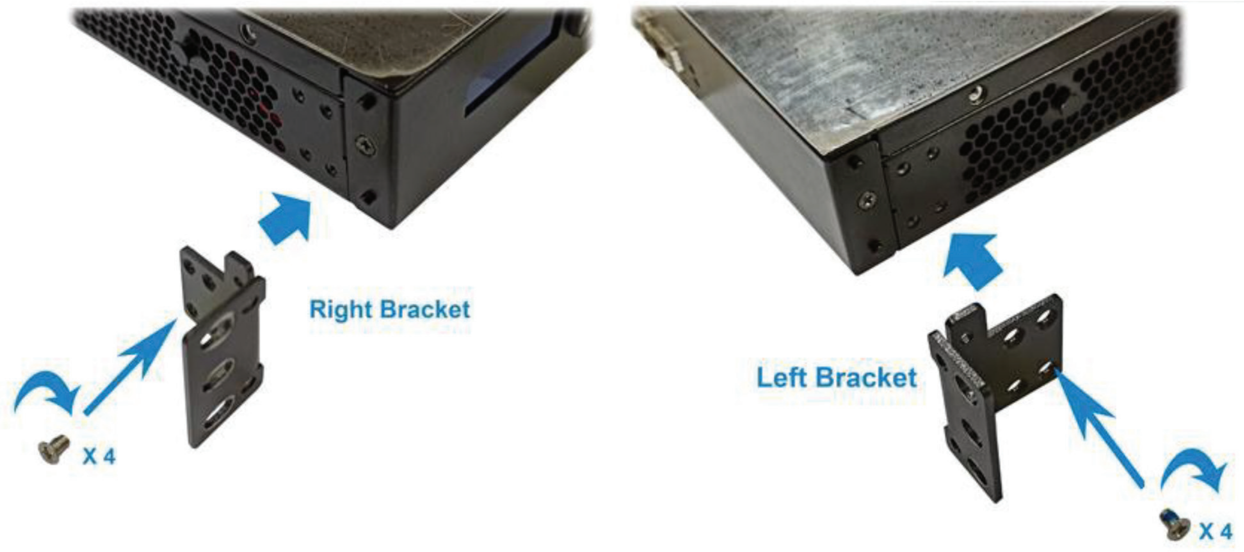


FIGURE 4-9. BRACKET ATTACHMENT

To protect the unit, please use the ground point on the Boxilla® unit on the rear of the Boxilla unit shown in Figure 4-10 (using the provided screw) for connecting to the ground point of the rack or cabinet.

4.3.1 RACKMOUNT SAFETY CONSIDERATIONS

- Elevated Ambient Temperature: If installed in a closed rack assembly, the operating temperature of the rack environment may be greater than room ambient. Use care not to exceed the rated maximum ambient temperature of the Boxilla® unit.
- Reduced Air Flow: Installation of the equipment in a rack should be such that the amount of airflow required for safe operation of the equipment is not compromised.
- Mechanical Loading: Mounting of the equipment in the rack should be such that a hazardous condition does not exist due to uneven mechanical loading.
- Circuit Overloading: Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of circuits might have on overcurrent protection and supply wiring. Consider equipment ratings for maximum current.
- Reliable Earthing: Reliable earthing of rack mounted equipment should be maintained. Pay particular attention to supply connections other than direct connections to the branch circuit (for example, use of power strips).

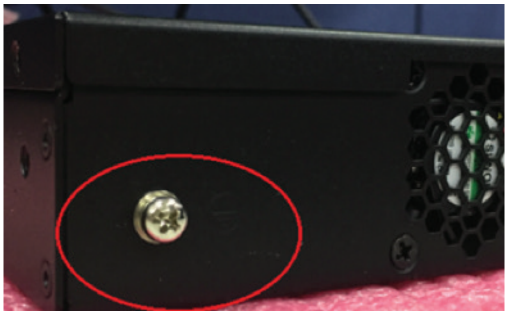


FIGURE 4-10. GROUND CONNECTION

4.4 INSTALLATION SAFETY

To avoid a potentially fatal shock hazard and possible damage to equipment, please observe the following precautions:

- Test AC outlets at the workstation and monitor for proper polarity and grounding.

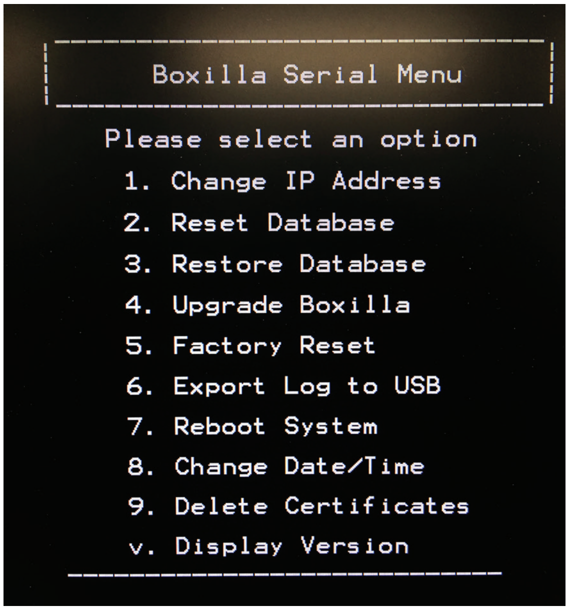
NOTE: The AC inlet is the main disconnect.

4.5 SERIAL CONFIGURATION OF IP ADDRESS

The default IP address for Boxilla® on leaving the factory is 192.168.1.24 and needs to be configured to an appropriate address for where it will be deployed. Open your web browser and navigate to 192.168.1.24 to change the IP address. As a secondary option to configure the IP address, the serial menu can be used. To access the serial menu, connect to the DB9 connector on the front of the unit. The serial port has a fixed configuration of:

- Baud-Rate: 115,200 Baud
- Data: 8 bits
- Stop-Bits: 1
- Parity: None
- XON/XOFF: None

Once the connecting PC has the correct configuration, the following menu should appear when connected to Boxilla's serial port. Make sure you turn echo on for the terminal to see the output.



```
 ---------------------------------
|                                 |
|       Boxilla Serial Menu       |
|_________________________________|

      Please select an option
       1. Change IP Address
       2. Reset Database
       3. Restore Database
       4. Upgrade Boxilla
       5. Factory Reset
       6. Export Log to USB
       7. Reboot System
       8. Change Date/Time
       9. Delete Certificates
       v. Display Version
    ----------------------------
```

FIGURE 4-11. BOXILLA SERIAL MENU

Select "Change IP address" by entering 1. Then follow the prompts to set the new IP address, Net Mask and Gateway IP address.

NOTE: To find the currently configured IP address, select the option "Change IP Address" to view the current IP. You can cancel this menu once you find it.

4.6 IMPORTANT FIRST CONFIGURATION STEPS

There are several important configuration steps that must be carried out when starting a new Boxilla® server for the first time.

1. Set the IP address for the Boxilla Server.
2. Change the default password for the default user "admin" (for security).
3. Configuring/resetting the SSL Certificates under System -> Administration -> Certificates

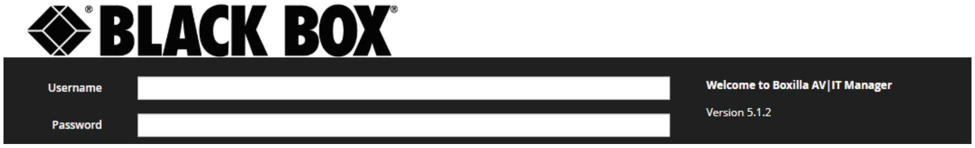
NOTE: Make sure that your computer can view the new IP address; otherwise, the Boxilla server will appear to be offline. Depending on your network configuration and that of the computer, you may need to change the computer's configuration to be able to see Boxilla server's new network address.

IMPORTANT NOTE: If an existing Boxilla server must be replaced, follow the important advice given within Appendix A: Replacing your Boxilla.

4.7 BROWSER CONFIGURATION OF IP ADDRESS

The default IP address for Boxilla on leaving the factory is https://192.168.1.24 and needs to be configured to an appropriate address for where it will be deployed. Use a computer located within the local network that can address the default IP address and ensure that Boxilla is connected to this network via its Ethernet Port 1 (RJ-45) as shown in Figure 4-1, open a web-browser and enter the default IP address for the Boxilla AV/IT Manager: https://192.168.1.24. This should bring up the Boxilla login screen shown below in Figure 4-12.

IMPORTANT: Boxilla requires https:// before the IP address or the web page will not display. Using HTTP:// does not work. To access Boxilla for the first time, use https://192.168.1.24



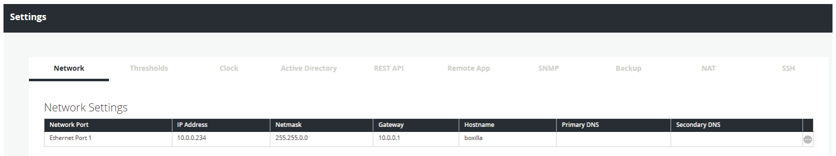
Welcome to Boxilla AV|IT Manager

Version 5.1.2

FIGURE 4-12. BOXILLA LOGIN SCREEN

When the login screen appears, enter the default username "admin" and the default password "admin." This will bring you to the Boxilla dashboard screen. On the Boxilla menu (see the menu on the left in Figure 4-13), select the menu item "System" on the left of the screens.

On the tabs that appear on the main section of the screen, click System —> Settings —> Network. Now you will be presented with the current IP settings for the system. Enter the new IP settings into the supplied fields and click "submit." Boxilla will be updated with the new network settings. From now on, you need to point your Browser to the new IP address.



Network Settings

Network Port	IP Address	Netmask	Gateway	Hostname	Primary DNS	Secondary DNS
Ethernet Port 1	10.0.0.234	255.255.0.0	10.0.0.1	boxilla		

FIGURE 4-13. SYSTEM —> SETTINGS —> NETWORK SCREEN

CHAPTER 5: BOXILLA CONFIGURATION

This section covers the configuration of Boxilla® for administrators.

5.1 SUPPORTED BROWSERS

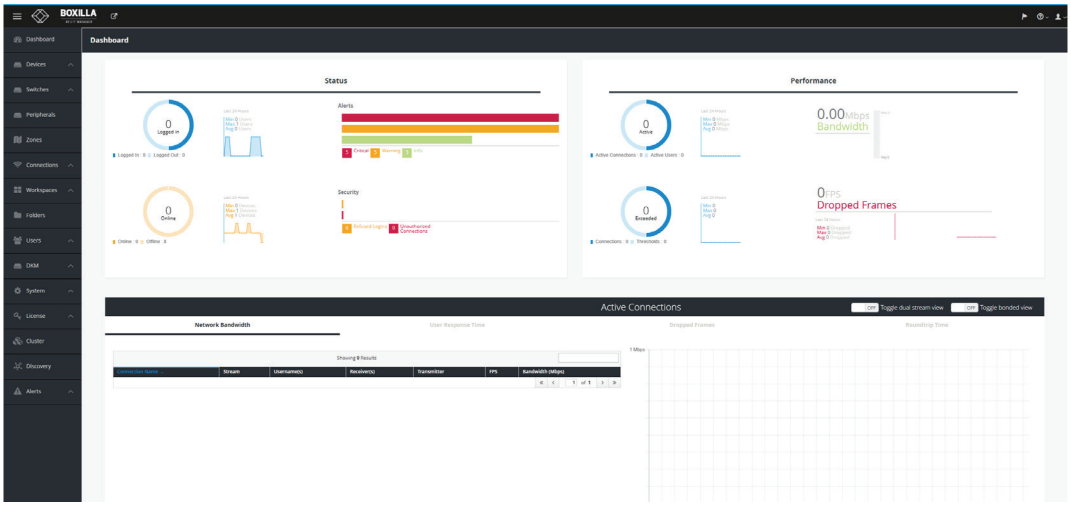
Boxilla will operate with most modern client browsers. It requires the browser to have JavaScript enabled. The list of supported browsers is as follows:

- Google Chrome
- Firefox
- Safari

NOTE: For the best experience, always use the latest versions of supported browsers.

5.2 LOGIN

Logging into the Boxilla® is straight forward and explained in the previous section. Once logged in, you will be presented with a Dashboard detailing a high level summary of statistics for the Boxilla and appliances, as shown in Figure 5-1.



Connection Name	Stream	Username(s)	Receiver(s)	Transmitter	FPS	Bandwidth (Mbps)

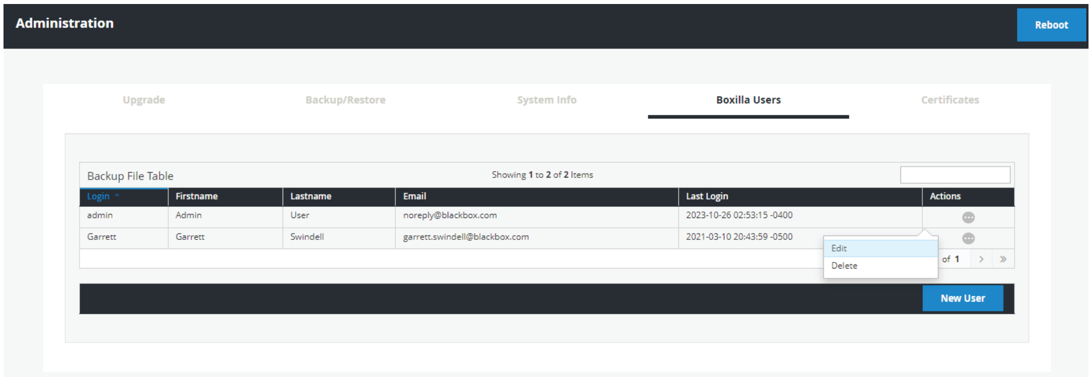
FIGURE 5-1. BOXILLA INITIAL SCREEN ON LOGIN

TABLE 5-1. BOXILLA INITIAL SCREEN MENU COMPONENTS

MENU OPTION	DESCRIPTION
Dashboard	The dashboard is divided into three main areas: Status & Performance Indicators, Active Connections and Active Logins.
Devices	Under the Devices drop-down menu on the left of the Dashboard screen, you will see four options: Settings, Upgrades, Global and Statistics. This is where you will find all of your appliances and each appliance's firmware.
Switches	The "Switches" menu has two subheadings: Status and Upgrades. These all link to individual pages. The status page initially shows a list of all the switches in the KVM Network. Clicking on a particular switch then brings you to a page displaying all the ports of that particular switch. This page also allows you to perform certain actions on the switch. The Upgrades page is similar to the DESKVUE/Emerald® Upgrade page. This shows a list of all the switches in the KVM network plus their current firmware version. If there is a mismatch to the activated firmware release, this will be flagged. You can also upload a release from this page.
Peripherals	Boxilla® uses USB Hub bonding using the EMD100USB to support external USB switching at speeds up to 480 Mbps or to support more complicated USB devices, such as Devlin keyboards.
Zones	Zones enable the administrator to setup unique zones (or groups) of Connections, Physical Receivers, and Users so that a large system can be more easily managed. DESKVUE and Emerald both support zoning.
Connections	Connections define the properties for the flow of keyboard, mouse, video, audio and USB traffic between the appliances, computers, and virtual machines. Connections are created and then allocated to Users to provide them access to Transmitters or Virtual Machines. A connection is a definition and can be allocated to multiple users. When a user logs into an appliance's receiver, they are presented with their allocated connections on the Connections Tab of the OSD on that Receiver.
Workspaces (DESKVUE only)	Workspaces enable the organization and management of display layouts. These layouts, which can be either system-defined or user-created, provide a wide range of configuration options to optimize user workflows.
Folders	Folders contains all the Connection & Workspace elements within the Boxilla and gives a way to organize how they are presented to the KVM user which is independent of Users and Receiver settings. The hierarchy created under this section will be displayed the same across all Emerald Receivers and for all the users depending on their access rights to those connections and workspaces contained.
Users	Users are defined in the Boxilla, then shared with the appliances to provide rights to manage the system, rights to connect to different target devices and rights to set parameters for connections.
DKM	This option enables you to integrate your DKM system with Boxilla and appliances. It includes the configuration elements for Boxilla and DKM.
System	The System button in the main menu brings up the System —> Administration —> Upgrade page. This page allows the Boxilla unit itself to be managed.
License	The License tab enables you to add/manage licenses for Boxilla and remote applications.
Cluster	Boxilla offers a redundancy feature for fail-safe operation. Your system can contain two Boxilla units, one as the primary Boxilla and one as a backup. If the first Boxilla cannot be found, the system will use a backup Boxilla to get the information. The primary and backup Boxilla are known as a cluster.
Discovery	The process of adding devices to Boxilla to manage is known as discovery. The discovery process can be automatic or can be manual.
Alerts	Alert history is a time-stamped log of events across the system.

You are strongly encouraged to change the default admin password as one of your first actions:

- Click on System button on the main menu and then select the Users tab as shown in Figure 5-2.
- Click the "..." icon on the Admin row and click on the edit option.



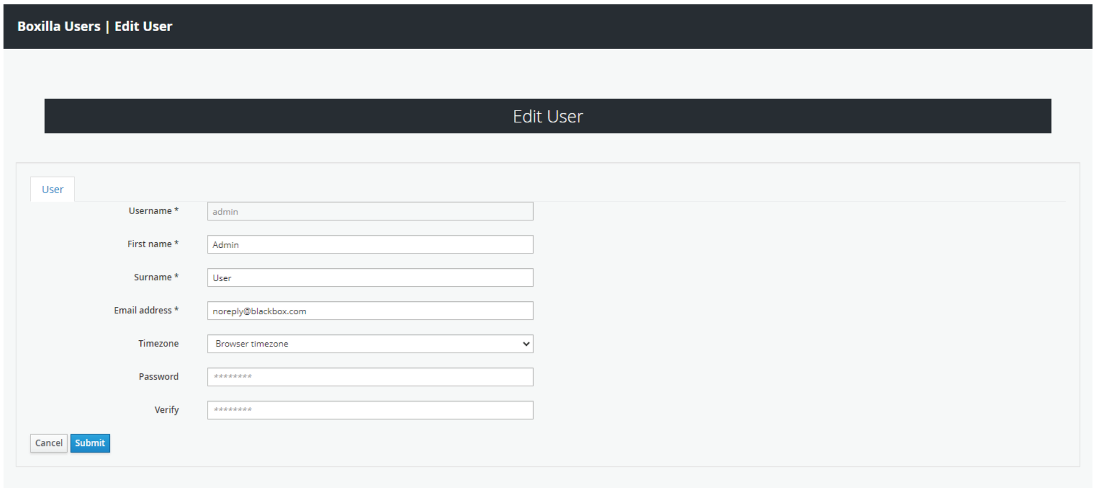
Backup File Table

Showing **1** to **2** of **2** Items

Login ^	Firstname	Lastname	Email	Last Login	Actions
admin	Admin	User	noreply@blackbox.com	2023-10-26 02:53:15 -0400	⋯
Garrett	Garrett	Swindell	garrett.swindell@blackbox.com	2021-03-10 20:43:59 -0500	⋯

FIGURE 5-2. CHANGING ADMIN USER PASSWORD

This allows the Admin user to be edited. The default password would be changed for security. The other properties can be used as required.



Boxilla Users | Edit User

Edit User

Username *	admin
First name *	Admin
Surname *	User
Email address *	noreply@blackbox.com
Timezone	Browser timezone
Password	********
Verify	********

FIGURE 5-3. EDIT ADMIN USER

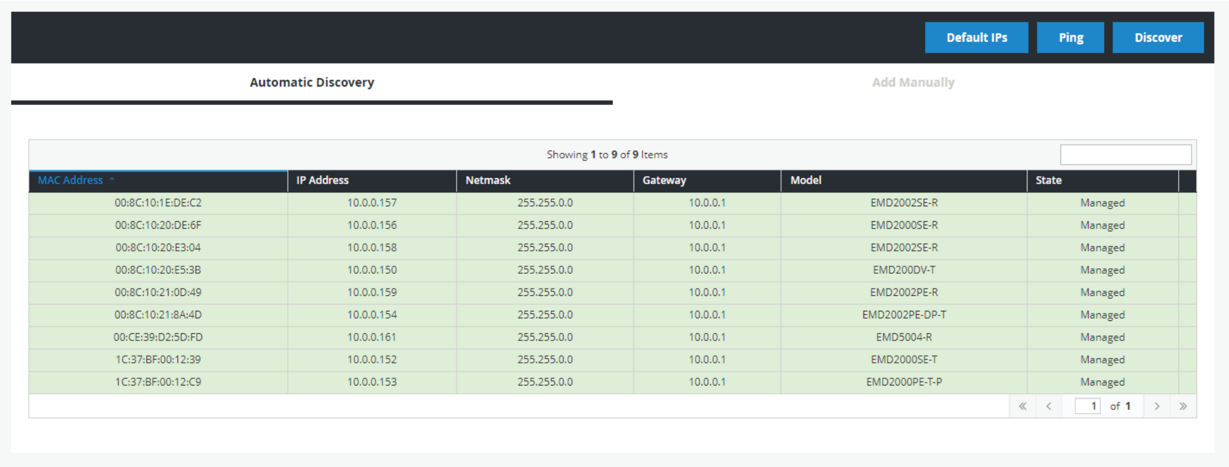
CHAPTER 6: DISCOVERY—ADDING DEVICES

The process of adding devices to Boxilla® to manage is known as discovery. The discovery process can be automatic or can be manual.

6.1 DISCOVERY—AUTOMATICALLY FINDING DEVICES

Boxilla uses a discovery protocol to automatically find devices to be managed on the network to support up to 4,000 devices. This discovery protocol can span across subnets. To allow automatic discovery protocol to operate across subnets, multicast routing should be enabled in the routers in the network, and the IP address of 192.168.1.1 should be available and open. Black Box's discovery protocol is not required for the appliances to operate but it is recommended to enable Boxilla to search for devices across multiple subnets. If the appliance's discovery protocol is not working, i.e. routers do not have multicast routing enabled, the administrator will have to manually add in devices not on its subnet, i.e. add in each device individually by its IP address.

To start adding devices to Boxilla, click on the Discovery button on the main menu. The Discovery page is displayed as shown in Figure 6-1. The example page already has some devices "discovered." The devices are listed in a table as shown in Figure 6-1.



Showing **1** to **9** of **9** Items

MAC Address ^	IP Address	Netmask	Gateway	Model	State
00:8C:10:1E:DE:C2	10.0.0.157	255.255.0.0	10.0.0.1	EMD2002SE-R	Managed
00:8C:10:20:DE:6F	10.0.0.156	255.255.0.0	10.0.0.1	EMD2000SE-R	Managed
00:8C:10:20:E3:04	10.0.0.158	255.255.0.0	10.0.0.1	EMD2002SE-R	Managed
00:8C:10:20:E5:3B	10.0.0.150	255.255.0.0	10.0.0.1	EMD200DV-T	Managed
00:8C:10:21:0D:49	10.0.0.159	255.255.0.0	10.0.0.1	EMD2002PE-R	Managed
00:8C:10:21:8A:4D	10.0.0.154	255.255.0.0	10.0.0.1	EMD2002PE-DP-T	Managed
00:CE:39:D2:5D:FD	10.0.0.161	255.255.0.0	10.0.0.1	EMD5004-R	Managed
1C:37:BF:00:12:39	10.0.0.152	255.255.0.0	10.0.0.1	EMD2000SE-T	Managed
1C:37:BF:00:12:C9	10.0.0.153	255.255.0.0	10.0.0.1	EMD2000PE-T-P	Managed

FIGURE 6-1. DISCOVERY PAGE

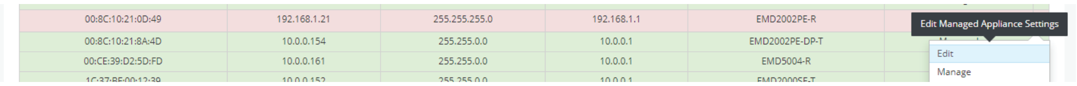
This table shows all devices "discovered" automatically or manually added. To discover devices automatically, click on the "discover" button on the page. This causes the Black Box Discovery protocol to be run where a "discovery" packet is broadcasted to network and devices respond to Boxilla by sending a UDP unicast back to Boxilla. See Appendix C: Protocols for more details on the actual protocol sequence.

The state of a device shown in the table can be one of the following:

- UnManaged—this device is currently not part of any managed domain and should be easily manageable
- Managed—this device is part of the domain managed by this Boxilla manager and should be easily manageable
- ManagedOther—this device is part of a domain managed by another Manager—and cannot be managed by this Boxilla manager
- Orphaned—there is a conflict between the reported state on the Manager and that of the device. This may occur where the device was removed from the Manager's database when the device was off-line, or if the Manager was restored to factory default settings. A device in the orphaned state can be set back to "Managed" by selecting the Manage button and following the same process as for unmanaged devices

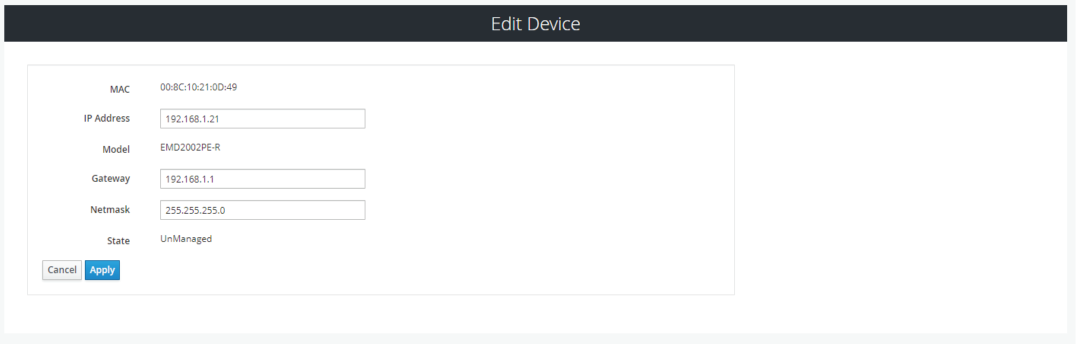
To edit a discovered device, click on the "•••" icon on the row for the device and select the Edit option. This allows the Network configuration of a device to be changed as shown in Figure 6-2. Typically, this is used to change a device from its default IP address to a unique address.

The administrator should be aware that the IP address should be changed to one reachable by Boxilla® (i.e. if moved to a subnet different to Boxilla manager, a router is required to enable communication).



00:8C:10:21:0D:49	192.168.1.21	255.255.255.0	192.168.1.1	EMD2002PE-R	
00:8C:10:21:8A:4D	10.0.0.154	255.255.0.0	10.0.0.1	EMD2002PE-DP-T	
00:CE:39:D2:5D:FD	10.0.0.161	255.255.0.0	10.0.0.1	EMD5004-R	
1C:37:BF:00:12:39	10.0.0.152	255.255.0.0	10.0.0.1	EMD2000SE-T	

FIGURE 6-2. EDIT AND MANAGE OPTIONS



Edit Device

MAC 00:8C:10:21:0D:49

IP Address 192.168.1.21

Model EMD2002PE-R

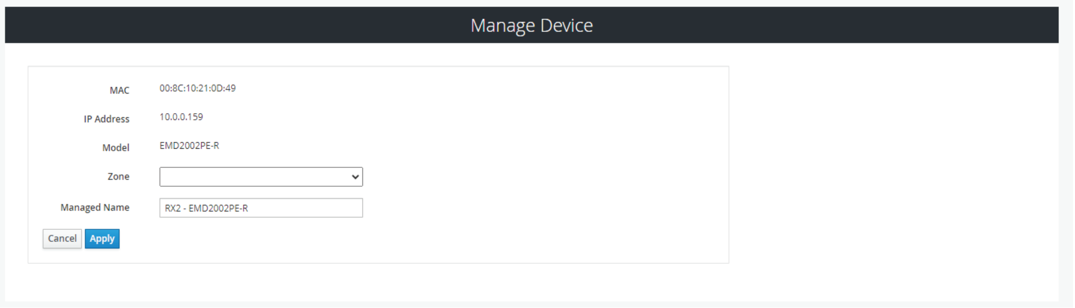
Gateway 192.168.1.1

Netmask 255.255.255.0

State UnManaged

FIGURE 6-3. EDIT DEVICE SCREEN

Once the IP address has been specified, an unmanaged device can now be set to be part of this Boxilla's managed domain. This is done by clicking on the Manage option under the ellipses (...) menu.



Manage Device

MAC 00:8C:10:21:0D:49

IP Address 10.0.0.159

Model EMD2002PE-R

Zone

Managed Name RX2 - EMD2002PE-R

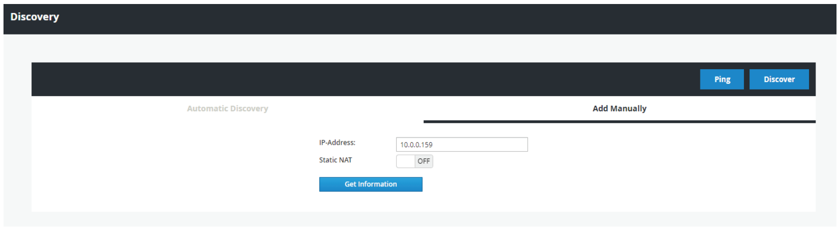
FIGURE 6-4. EDIT DEVICE SCREEN

This causes the device's state to change from UnManaged to Managed. The device is given a name as part of the process of making it managed. This name is used to make it easier for administrators and users to refer to the device (e.g. ControlRoom1 to name a device in Control Room 1). Once managed by Boxilla, this device cannot be managed or configured by any other manager.

6.2 DISCOVERY—MANUALLY ADDING DEVICES

Sometimes an administrator may want to add a device manually, for example, where a device is on a different subnet to the Boxilla® Manager and multicast routing is not enabled to this subnet.

To manually add a device, click on the "Add Manually" tab on the discovery page. This brings up the page shown in Figure 6-5. Enter the IP address of the device to be added and click on "Get Information." This causes Boxilla to retrieve the device's information if reachable. If Boxilla has no valid path on the network to the device (or IP address is not for an appliance), the system will return a message of "device not reachable."

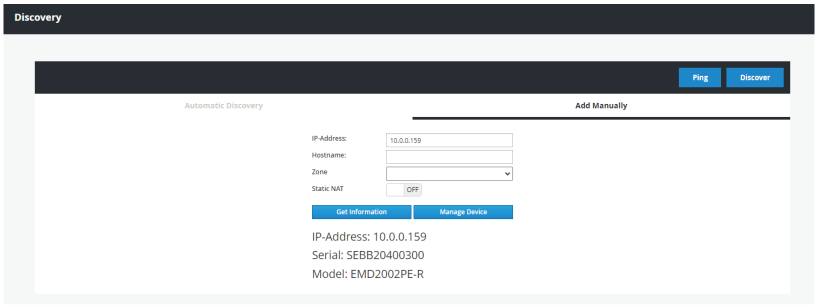


IP-Address: 10.0.0.159

Static NAT OFF

FIGURE 6-5. DISCOVERY—MANUAL ADD

The administrator can give the device a name, check that the device's details are correct if required to ensure it is the correct device (IP address, Serial Number and Model type), and assign the device to a Zone if appropriate. To manage this device, click on "Manage Device" button as shown in Figure 6-6. Refer to Section 14.16.4 if using a Static NAT.



IP-Address: 10.0.0.159

Hostname:

Zone

Static NAT OFF

IP-Address: 10.0.0.159
Serial: SEBB20400300
Model: EMD2002PE-R

FIGURE 6-6. DISCOVERY MANUAL ADD & MANAGE DEVICE

6.3 DISCOVERY—WHAT HAPPENS TO A DEVICE WHEN MANAGED

The appliances can be configured locally when in UnManaged state. When a unit becomes "Managed," its local database is replaced with the database from Boxilla®. The IP address of the device is preserved—but can be changed from Boxilla. The administrator can no longer change users, connections and various properties locally on the device—these can only be changed on Boxilla.

Once a device is managed by Boxilla, Boxilla's database is "synchronized" to the device when a user logs in to the device. The following sections outline how to use Boxilla to configure and monitor devices.

There are operating options that can only be configured locally for this current release. These are:

- Power-Mode— whether an Emerald Receiver powers up automatically when power is applied or needs the power button to be pressed;
- Auto-Login—whether an Emerald Receiver will automatically login as a specific user on power up;
- OSD Resolution—resolution that the OSD is displayed at when on screen;

See the Emerald or DESKVUE device manual for full details of these options.

6.4 DISCOVERY—IF A DEVICE IS NOT FOUND

There can be several reasons why a device has not been discovered by Boxilla:

- The device may be turned off.
- The device may not be reachable on the network— no valid path to device. This can happen if device is on a different network subnet to Boxilla and no router is between the two subnets. Use PING to verify the device can be reached.
- Automatic discovery may not find the device if it is on a different subnet to Boxilla and the router does not allow Multicast UDP packets to be forwarded to it. The router path to subnet manual addition should work.
- There is a potential cabling problem between the device and the Boxilla Manager. Check and where necessary, replace faulty cables.
- Ethernet port 1 on the Boxilla unit is not connected to the KVM network. Discovery messages are ONLY set on Ethernet port 1. Ethernet Port 2 does not support KVM traffic. All KVM traffic is routed through Ethernet Port 1.
- A device exists on the network with an IP address of 192.168.1.1 All Emerald appliances ship with a default gateway configuration of 192.168.1.1 If there is a device on the network with an IP address of 192.168.1.1, Boxilla will be unable to discover Emerald devices with default IP configurations (e.g. 192.168.1.21, 192.168.1.22). To resolve this issue, please reconfigure the device from 192.168.1.1 to an alternative IP address, e.g. 192.168.1.50
- The discovery process requires UDP Multicast, using Multicast Address 224.0.1.249, UDP port 39150. Please ensure your network supports UDP Multicast and the specified multicast address and UDP port is not blocked.
- For DESKVUE only: DESKVUE needs firmware V1.1.0r94 or later installed in order to be discovered and managed by Boxilla.

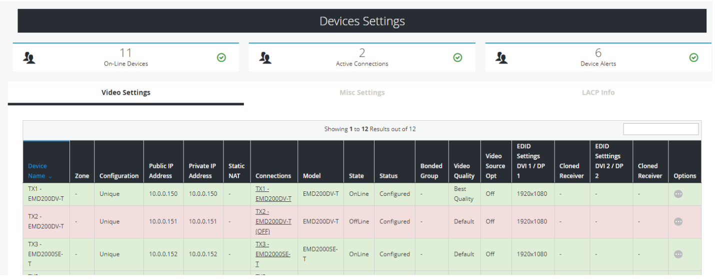
CHAPTER 7: DEVICES

Devices part of the managed domain can be reviewed, upgraded and configured. These actions are performed by clicking the devices' options from the main menu. Figure 7-1 shows the Device—Settings Page. This page shows all the devices that are part of the managed domain.

Boxilla® constantly polls devices to determine their state and operational statistics. The state of a device in the table can be:

- Online—means the device is contactable from Boxilla during recent polling cycles;
- Offline—means the device did not respond during any of the last few polling cycles. This can mean the device is powered-down or is not reachable on the network;
- Demo—means the device is a simulated device for demonstration purposes;

Under the Devices drop-down menu on the left of the Dashboard screen, you will see five options: Settings, Groups, Upgrades, Global and Statistics. These options are described in the following sections. Click on Settings and the following screen appears.



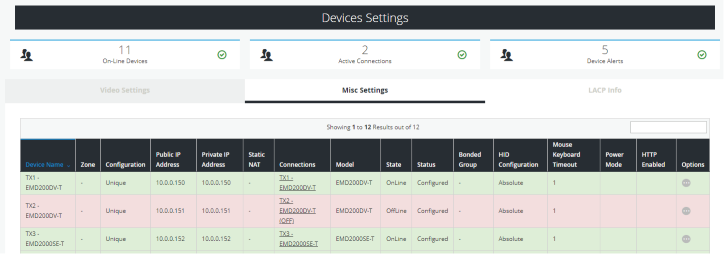
Showing **1** to **12** Results out of 12

Device Name	Zone	Configuration	Public IP Address	Private IP Address	Static NAT	Connections	Model	State	Status	Bonded Group	Video Quality	Video Source Opt	EDID Settings DVI 1 / DP 1	Cloned Receiver	EDID Setttings DVI 2 / DP 2	Cloned Receiver	Options
TX1 - EMD200DV-T	-	Unique	10.0.0.150	10.0.0.150	-	TX1 - EMD200DV-T	EMD200DV-T	OnLine	Configured	-	Best Quality	Off	1920x1080	-	-	-	⋯
TX2 - EMD200DV-T	-	Unique	10.0.0.151	10.0.0.151	-	TX2 - EMD200DV-T (OFF)	EMD200DV-T	OffLine	Configured	-	Default	Off	1920x1080	-	-	-	⋯
TX3 - EMD2000SE-T	-	Unique	10.0.0.152	10.0.0.152	-	TX3 - EMD2000SE-T	EMD2000SE-T	OnLine	Configured	-	Default	Off	1920x1080	-	-	-	⋯

FIGURE 7-1. SETTINGS SCREEN

By default, the Video Settings tab will be open when loading Settings and will show the Device Name, Zone, Configuration, IP Address, NAT details, Connections, Models, State, Status, and other important information.

Click on Misc Settings in the middle of this screen to see the Device Name, Configuration, IP Address, Model, State, Status, HID Configuration, Shared Mouse Timer, Power Mode, HTTP Enabled and Options settings for each TX or RX unit.

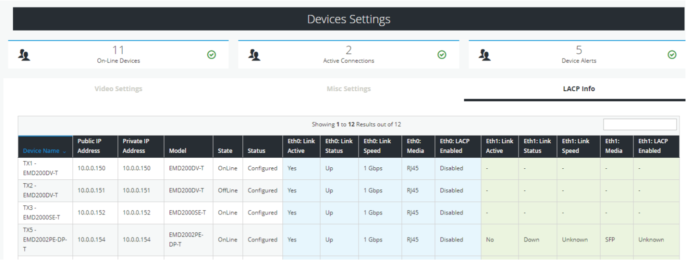


Showing **1** to **12** Results out of 12

Device Name	Zone	Configuration	Public IP Address	Private IP Address	Static NAT	Connections	Model	State	Status	Bonded Group	HID Configuration	Mouse Keyboard Timeout	Power Mode	HTTP Enabled	Options
TX1 - EMD200DV-T	-	Unique	10.0.0.150	10.0.0.150	-	TX1 - EMD200DV-T	EMD200DV-T	OnLine	Configured	-	Absolute	1			⋯
TX2 - EMD200DV-T	-	Unique	10.0.0.151	10.0.0.151	-	TX2 - EMD200DV-T (OFF)	EMD200DV-T	OffLine	Configured	-	Absolute	1			⋯
TX3 - EMD2000SE-T	-	Unique	10.0.0.152	10.0.0.152	-	TX3 - EMD2000SE-T	EMD2000SE-T	OnLine	Configured	-	Absolute	1			⋯

FIGURE 7-2. MISC SETTINGS ON SETTINGS SCREEN

Click on LACP in the middle of this screen to provide additional details about each device's Link Status, including state, speed, media, and if LACP info is detected.



Showing **1** to **12** Results out of 12

Device Name	Public IP Address	Private IP Address	Model	State	Status	Eth0: Link Active	Eth0: Link Status	Eth0: Link Speed	Eth0: Media	Eth0: LACP Enabled	Eth1: Link Active	Eth1: Link Status	Eth1: Link Speed	Eth1: Media	Eth1: LACP Enabled
TX1 - EMD200DV-T	10.0.0.150	10.0.0.150	EMD200DV-T	OnLine	Configured	Yes	Up	1 Gbps	RJ45	Disabled	-	-	-	-	-
TX2 - EMD200DV-T	10.0.0.151	10.0.0.151	EMD200DV-T	OffLine	Configured	Yes	Up	1 Gbps	RJ45	Disabled	-	-	-	-	-
TX3 - EMD2000SE-T	10.0.0.152	10.0.0.152	EMD2000SE-T	OnLine	Configured	Yes	Up	1 Gbps	RJ45	Disabled	-	-	-	-	-
TX5 - EMD2002PE-DP-T	10.0.0.154	10.0.0.154	EMD2002PE-DP-T	OnLine	Configured	Yes	Up	1 Gbps	RJ45	Disabled	No	Down	Unknown	SFP	Unknown

FIGURE 7-3. LACP ON SETTINGS SCREEN

NOTE: A user can configure the HTTP_Enable attribute for Emerald RX devices, but it is not possible to configure the Power Mode setting for Emerald RX devices.

7.1 DEVICES—SETTINGS

You now have the option to configure unique, template or system-wide settings. Here you can:

- Create/edit/delete device templates
- Edit system properties
- Edit individual device settings
- Apply bulk updates to appliances

The configuration of RX and TX settings is managed via an internal workflow reflected in the Status field in the Device Settings screen. Valid values include: Waiting, Configuring, Configured, Failed, Retrieving, Failed_Retrieve and Idle.

Idle – State is pretty much unnoticeable. The appliance gets this state right after it is being managed. Then, after an XML file is pushed to the appliance (as part of the managing process), it changes the state to Retrieving.

Once retrieve is successful, state changes to Configured. Otherwise, it changes to Failed_Retrieve.

When a device is managed, the workflow for the Status field is Retrieving, Configured. It may be necessary to use the "Retrieve" option under the device Video Settings tab in order to synchronize it, but it is not common to need to do this.

The Configuration field is set to Unique.

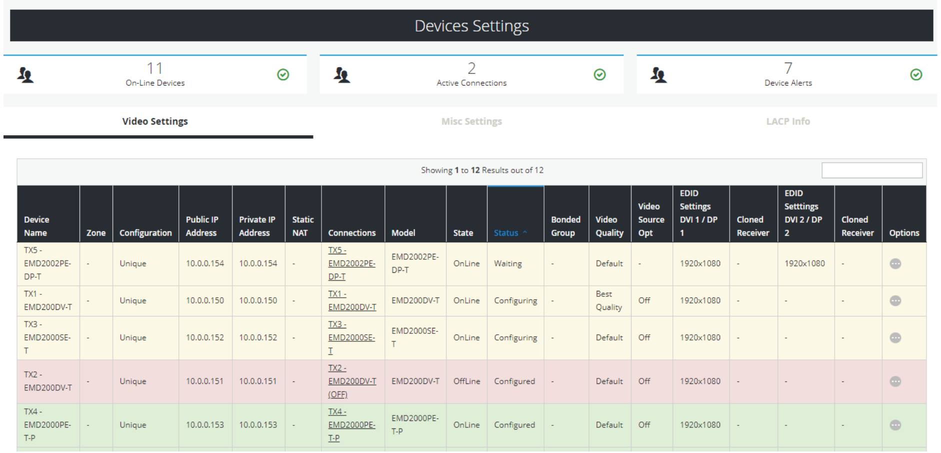
You can change the settings of an individual device (to Unique, Template or System) via the Edit Settings option. The workflow for the Status field here is: Waiting, Configuring, Configured | Failed.

If you Edit a Template, the updated template is applied to all devices that use that Template. The workflow for the Status field here is: Waiting, Configuration, Configuring | Failed.

If you Edit the System Properties, the update System Property is applied to all devices that use the System Property. The workflow for the Status field here is: Waiting, Configuring, Configured | Failed.

You can also apply Bulk updates to devices, e.g., you can apply a Template or System Properties to one or more devices at the same time.

NOTE: Updates to Transmitter devices result in the device rebooting.



Devices Settings

11 On-Line Devices

2 Active Connections

7 Device Alerts

Video Settings | Misc Settings | LACP Info

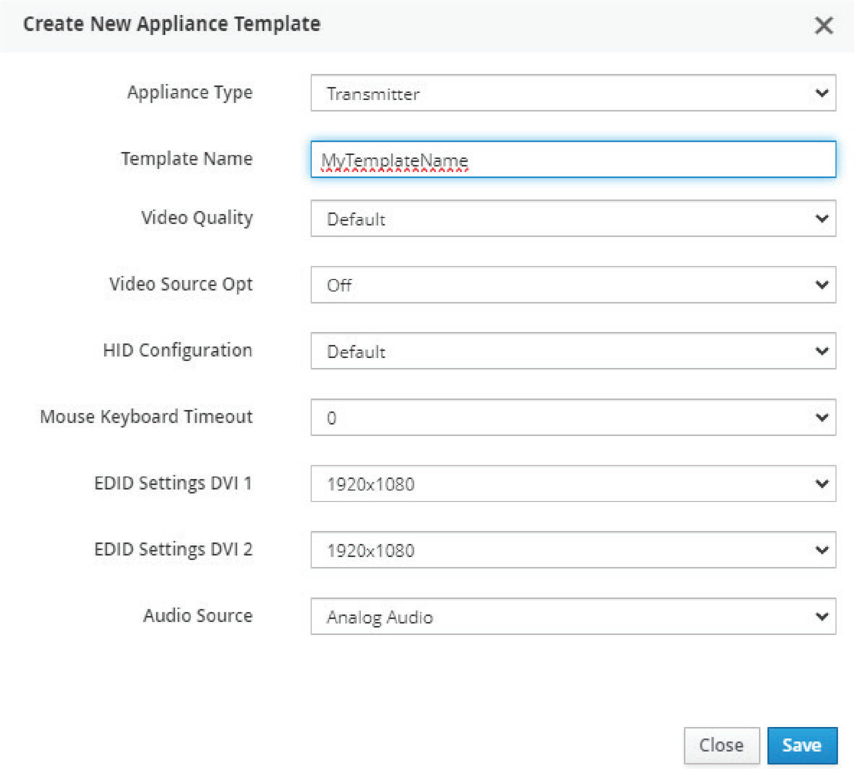
Showing **1** to **12** Results out of 12

Device Name	Zone	Configuration	Public IP Address	Private IP Address	Static NAT	Connections	Model	State	Status ^	Bonded Group	Video Quality	Video Source Opt	EDID Settings DVI 1 / DP 1	Cloned Receiver	EDID Setttings DVI 2 / DP 2	Cloned Receiver	Options
TX5 - EMD2002PE-DP-T	-	Unique	10.0.0.154	10.0.0.154	-	TX5 - EMD2002PE-DP-T	EMD2002PE-DP-T	OnLine	Waiting	-	Default	-	1920x1080	-	1920x1080	-	⋯
TX1 - EMD200DV-T	-	Unique	10.0.0.150	10.0.0.150	-	TX1 - EMD200DV-T	EMD200DV-T	OnLine	Configuring	-	Best Quality	Off	1920x1080	-	-	-	⋯
TX3 - EMD2000SE-T	-	Unique	10.0.0.152	10.0.0.152	-	TX3 - EMD2000SE-T	EMD2000SE-T	OnLine	Configuring	-	Default	Off	1920x1080	-	-	-	⋯
TX2 - EMD200DV-T	-	Unique	10.0.0.151	10.0.0.151	-	TX2 - EMD200DV-T (OFF)	EMD200DV-T	OffLine	Configured	-	Default	Off	1920x1080	-	-	-	⋯
TX4 - EMD2000PE-T-P	-	Unique	10.0.0.153	10.0.0.153	-	TX4 - EMD2000PE-T-P	EMD2000PE-T-P	OnLine	Configured	-	Default	Off	1920x1080	-	-	-	⋯

FIGURE 7-4. HIGHLIGHTED INFORMATION ON DEVICE SETTINGS SCREEN

7.1.1 CREATE/EDIT/DELETE DEVICE TEMPLATES

To create a new device template, click on the blue +Add Template button at the top right of the Devices Settings screen. The Create New Appliance Template screen pops up.



Create New Appliance Template

Appliance Type	Transmitter
Template Name	MyTemplateName
Video Quality	Default
Video Source Opt	Off
HID Configuration	Default
Mouse Keyboard Timeout	0
EDID Settings DVI 1	1920x1080
EDID Settings DVI 2	1920x1080
Audio Source	Analog Audio

FIGURE 7-5. CREATE NEW DEVICE TEMPLATES SCREEN

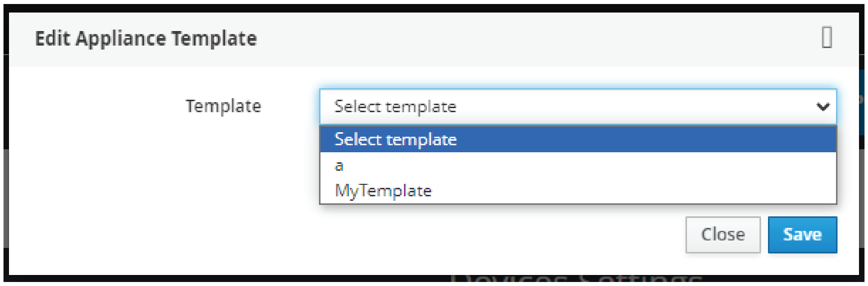
The Create New Device Templates screen fields are described next.

- Appliance Type: Choose Transmitter or Receiver.
- Template Name: Type in a unique name for the template.
- Video Quality: Select from these options: Best Quality, 2, Default, 4, or Best Compression.
- Video Source Opt: Select from Off, DVI Optimized, VGA - High-Performance, VGA - Optimized, VGA - Low Bandwidth (only applied in case of a single-head transmitter).
- HID Configuration: Select from Default, Basic, MAC, Absolute, Absolute Basic, or Absolute MAC. The Absolute Mouse feature can be used to enable interoperability with KM switches with built-in “Glide & Switch” capability such as ServSwitchTC and Freedom. If the target systems are MAC OS, you can use the Absolute MAC setting for best user experience. If the connection uses Transmitter Pair then Absolute, Absolute Basic, or Absolute Mac will need to be used in order for the mouse to work.
- Mouse Keyboard Timeout: Choose an option from 0 to 5 seconds.
- EDID Settings DVI 1: Choose from 1920 x 1080, 1920 x 1200, 1680 x 1050, 1280 x 1024, 1024 x 768, or clone.
- EDID Settings DVI 2: Choose from 1920 x 1080, 1920 x 1200, 1680 x 1050, 1280 x 1024, 1024 x 768, or clone.
- Audio Source: Choose between Analog audio using the 3.5mm connectors, or, if using DisplayPort™ Transmitters and Receivers, you can choose DisplayPort audio.

To save the settings, click the Save button. Otherwise, click the Cancel button.

To edit a device template, click on the blue Edit Template button at the top of the Devices —> Settings screen. The Edit Appliance Template screen pops up. Select the desired template from the drop-down menu, then select the desired options for the Template Name, Video Quality, Video Source Opt, HID Configuration, Mouse Keyboard Timeout, EDID Settings DVI 1 and EDID Settings DVI 2 settings. Click the Save button to save your changes, or click the Cancel button to cancel the settings.

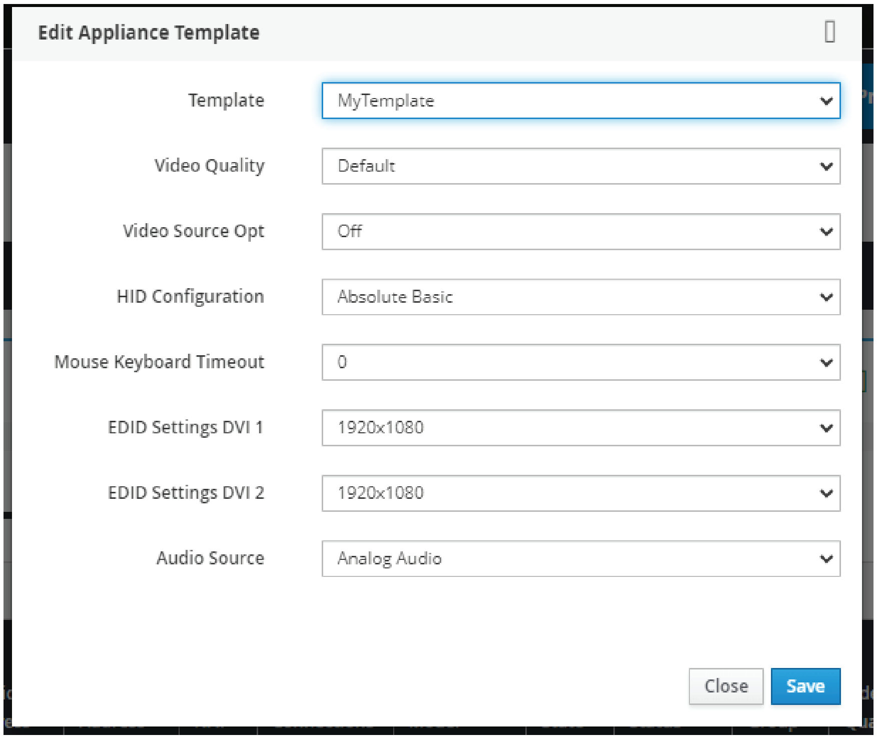
NOTE: The EDID of the remote display can also be copied instead of using the built-in resolutions. This can be done from the receiver menu by connecting to the transmitter and cloning the EDID.



Edit Appliance Template

Template: Select template

FIGURE 7-6. EDIT TEMPLATE SCREEN



Edit Appliance Template

Template: MyTemplate

Video Quality: Default

Video Source Opt: Off

HID Configuration: Absolute Basic

Mouse Keyboard Timeout: 0

EDID Settings DVI 1: 1920x1080

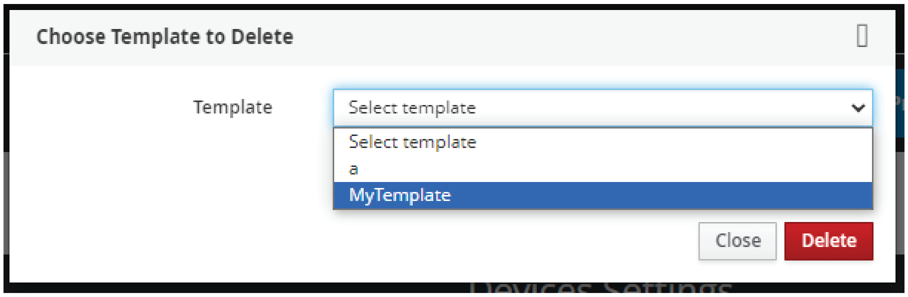
EDID Settings DVI 2: 1920x1080

Audio Source: Analog Audio

FIGURE 7-7. EDIT TEMPLATE FIELDS

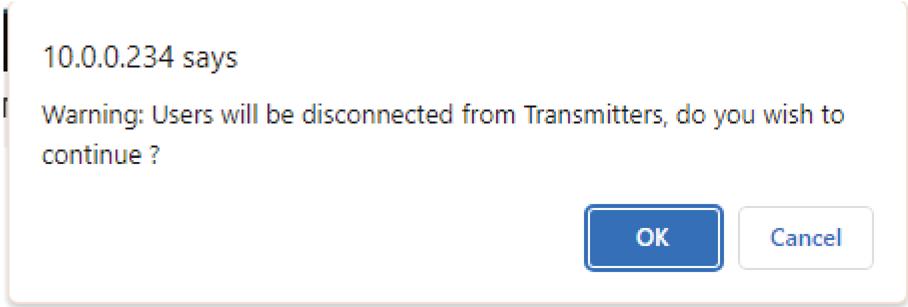
To delete a device template, click on the red -Template button at the top of the Devices —> Settings screen. The Delete Appliance Template screen pops up. Select the template you want to delete from the drop-down menu, then click the Delete button to delete the template, or click the Cancel button to cancel the deletion.

NOTE: You can only delete a template that is currently not in use. Therefore, you will be prompted for a decision regarding disconnecting all users who are actively using the template, as shown in Figure 7-9 below.



Choose Template to Delete

FIGURE 7-8. DELETE TEMPLATE SCREEN



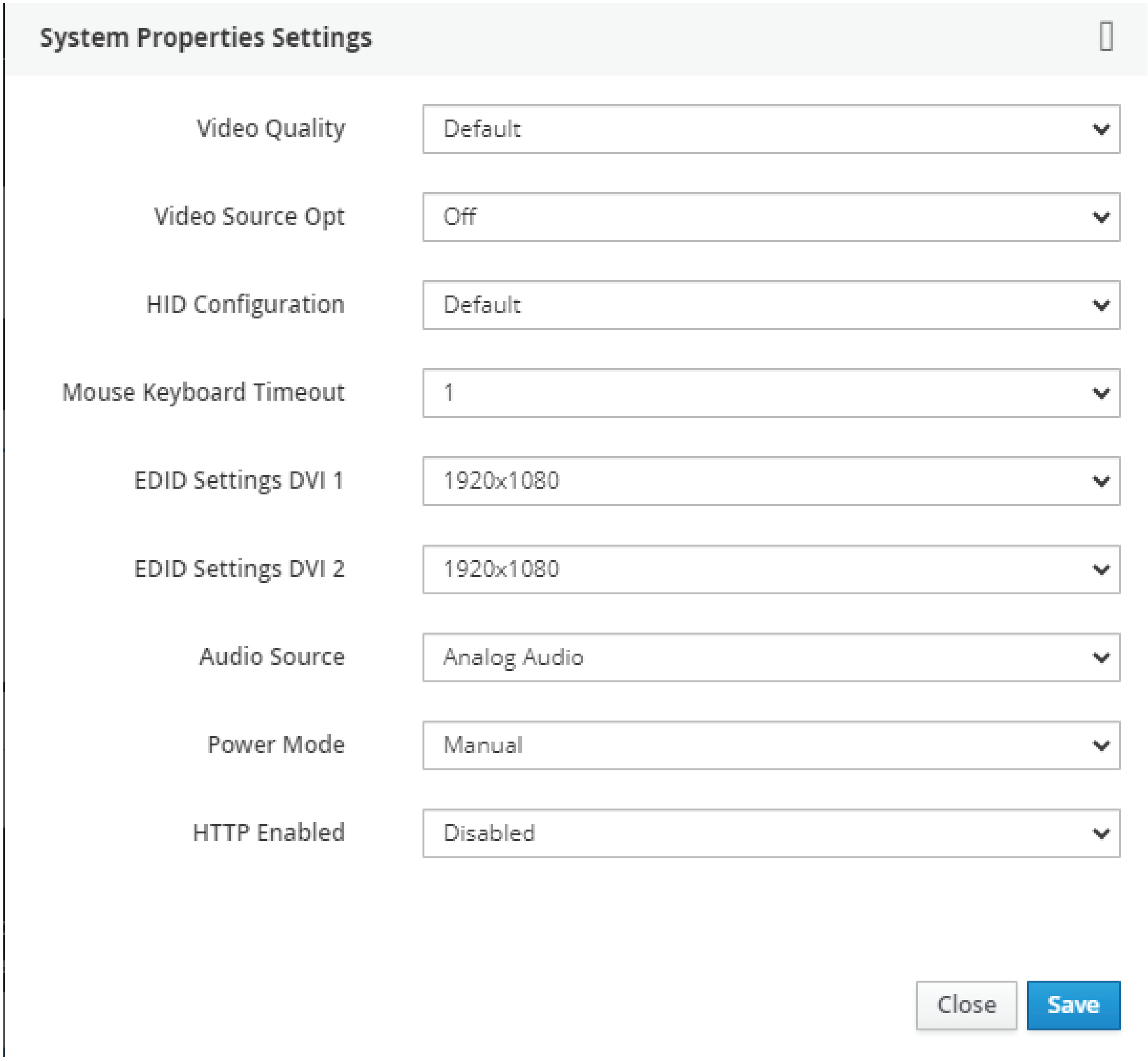
10.0.0.234 says

Warning: Users will be disconnected from Transmitters, do you wish to continue ?

FIGURE 7-9. CONFIRMATION SCREEN

7.1.2 EDIT SYSTEM PROPERTIES

To edit the system properties, click on the blue System Properties button at the top right of the Devices Settings screen. The System Properties Settings screen with editable options pops up. Changes can be saved or canceled.



System Properties Settings

Video Quality	Default
Video Source Opt	Off
HID Configuration	Default
Mouse Keyboard Timeout	1
EDID Settings DVI 1	1920x1080
EDID Settings DVI 2	1920x1080
Audio Source	Analog Audio
Power Mode	Manual
HTTP Enabled	Disabled

FIGURE 7-10. EDIT SYSTEM PROPERTIES SCREEN

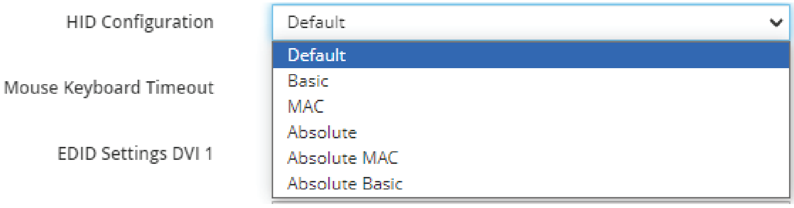
- Video Quality: Select from these options: Best Quality, 2, Default, 4, or Best Compression.
- Video Source Opt: Select from Off, DVI Optimized, VGA - High-Performance, VGA - Optimized, VGA - Low Bandwidth (only applied in the case of a single-head transmitter).
- HID Configuration: Select from Default, Basic, MAC, Absolute, Absolute MAC, or Absolute Basic..

Absolute mouse:

This feature can be used to enable interoperability with KVM switches with built-in “Glide & Switch” capability such as ServSwitchTC and Freedom. RemoteApp and DESKVUE connections also require the HID Configuration to be set for Absolute, Absolute Mac, or Absolute Basic. For normal usage, where mouse is directly connected to Receiver, then the Default or Basic options should be used. If using a Transmitter Pair connection method, then again the transmitter devices must have an Absolute mouse mode enabled.

If the target computers are MAC OS, you can use the Absolute MAC HID configuration for the best user experience.

OSD option:



HID Configuration: Default

Mouse Keyboard Timeout

EDID Settings DVI 1

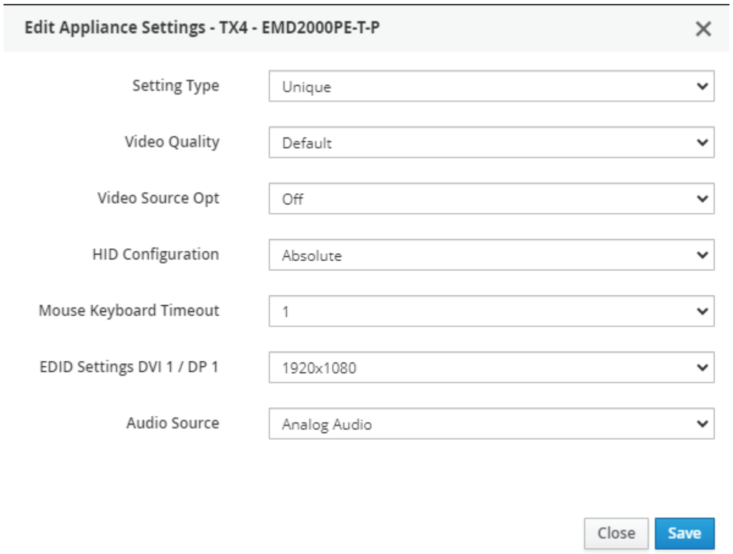
FIGURE 7-11. ABSOLUTE MOUSE SCREEN

- Mouse Keyboard Timeout: Choose an option from 0 to 5 seconds.
- EDID Settings DVI 1: Choose from 1920 x 1080, 1920 x 1200, 1680 x 1050, 1280 x 1024, 1024 x 768, or clone.
- EDID Settings DVI 2: Choose from 1920 x 1080, 1920 x 1200, 1680 x 1050, 1280 x 1024, 1024 x 768, or clone.
- Audio Source: Choose between analog audio using the 3.5mm connectors, or if using DisplayPort™ Transmitters and Receivers, you can choose DisplayPort Audio.
- Power Mode: Choose Manual or Auto.
- HTTP Enabled: Choose Enabled or Disabled.

To save the settings, click the Save button. Otherwise, click the Cancel button.

7.1.3 EDIT INDIVIDUAL DEVICE SETTINGS

To edit the individual device settings, click on the Video Settings or Misc Settings in the middle of the Devices page —> Settings screen. Then click on the Device Name that you want to edit. Select each of the settings you want to change from the drop-down boxes. Options include Setting Type, Video Quality, Video Source, HID Configuration, Mouse Keyboard Timeout, EDID Settings DVI 1 / DP 1 and EDID Settings DVI 2 / DP 2. Click Save, or click Cancel to cancel the changes without saving.



Edit Appliance Settings - TX4 - EMD2000PE-T-P

Setting Type	Unique
Video Quality	Default
Video Source Opt	Off
HID Configuration	Absolute
Mouse Keyboard Timeout	1
EDID Settings DVI 1 / DP 1	1920x1080
Audio Source	Analog Audio

FIGURE 7-12. EDIT INDIVIDUAL DEVICE SETTINGS SCREEN

An individual device can have various operations performed on it by clicking on the "•••" icon on the row for the device as shown in Figure 7-13 (Transmitters) and 7-14 (Receivers). These are:

- Details — get summary details on the device, including its Network configuration, Operational Status, Firmware Version and Serial Number
- Ping — tests the reachability of the device on the network
- Edit Settings — Edit device settings
- Retrieve — Retrieve device settings
- Force Logout — logs out the current user attached to this unit (if any)
- Edit Network - Edit the TCP/IP network settings for the device
- Retrieve logs - Request the log files from the endpoint for support purposes
- Service Access (for developer use only) - Will enable SSH access to the transmitter / receiver units for more advanced troubleshooting by development (disabled by default)
- Change Device Zone - allows the device zone to be modified
- UnManage — removes the device from the managed domain and restores the device back to factory defaults
- Change Device Name — allows the endpoint name to be changed
- Reboot — power cycles the device
- Send Power LED Command — allows the flashing of the onboard LED of the TX/RX to quickly identify them physically

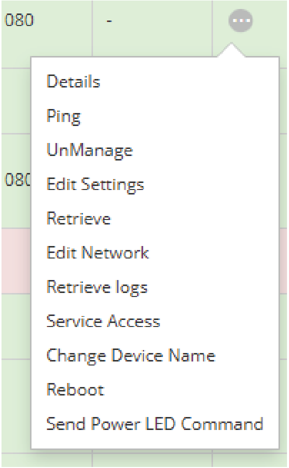


FIGURE 7-13. DEVICE OPTIONS (TRANSMITTER)

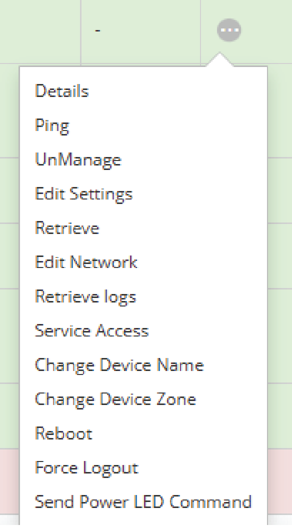
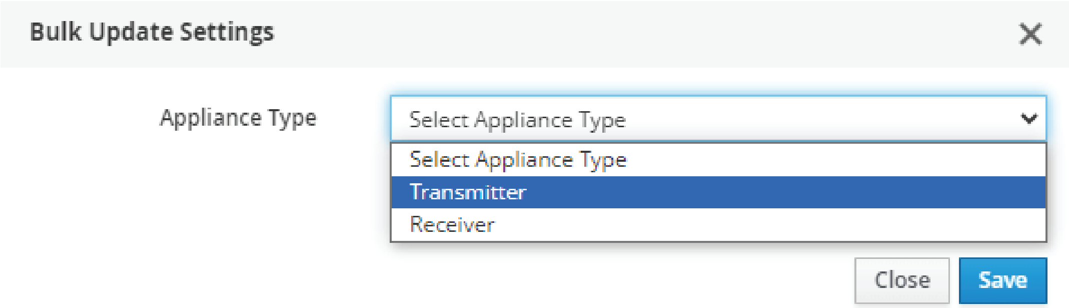


FIGURE 7-14. DEVICE OPTIONS (RECEIVER)

7.1.4 APPLY BULK UPDATE SETTINGS

To update the individual device settings all at once, click on the Bulk Update button in the middle of the Devices —> Settings screen. From the drop-down menu, select the appliance type: Transmitter or Receiver. Click the Save button to apply the updates to all Transmitters or all Receivers, or click cancel to Cancel without saving.


Bulk Update Settings

Appliance Type: Select Appliance Type

FIGURE 7-15. BULK UPDATE SETTINGS SCREEN

7.2 DEVICES—GROUPS

Groups can be created in order to use Bonded Switching. The purpose of the bonding feature (described in Section 11.1.2) is to switch multiple receivers to multiple connections quickly and simply from one user station. A typical example is where a user has a dual head 4K system; the user will have two 4K monitors and 4K receivers on their desk but only one keyboard and mouse. The user will select the "bonded connection" from their OSD and both receivers (up to 8 receivers in a Bonded Connection) will switch to their pre-configured 4K transmitters. Typically this will be set up in extended desktop and the user can move mouse and keyboard activity between both screens. We described 2 head setup above but the same applies for up to 8 bonded connections.

With Boxilla®, it is possible to create a Bonded Connection. This is a group of 2 to 8 connections that have been added to form a "bonded connection." The bonded connection is treated just like any other connection, where users must be assigned access to this connection. A bonded connection can be launched on any bonded receiver. Each connection in a group is assigned a number in order 1 to 8 and these will be matched with the receiver with the receiver bonded group.

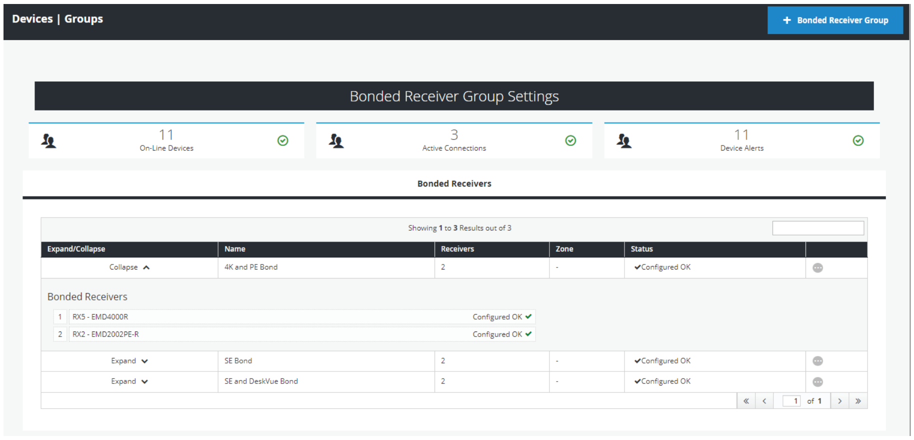
You can also create a Receiver Bonded Group. This is a group of 2 to 8 Receivers that have been added to a group to set up bonding. Their order in the group is critical as they will be matched with a connection in a connection group based on that order (1 to 8).

NOTE: A Receiver device can only be assigned to 1 Bonded Receiver Group.

All receiver types can be mixed and matched within a "receiver bonded group" and again standard interoperability rules will apply.

NOTE: We recommend using a Glide and Switch solution if you want to use one keyboard and mouse across multiple systems.

NOTE: All connections within a bonded connection group and the bonded connection group itself must be in the same zone (if using zones).



Bonded Receiver Group Settings

11 On-Line Devices

3 Active Connections

11 Device Alerts

Bonded Receivers

Showing 1 to 3 Results out of 3

Expand/Collapse	Name	Receivers	Zone	Status	
Collapse ^	4K and PE Bond	2	-	✓Configured OK	⋯

Bonded Receivers

1	RX5 - EMD4000R	Configured OK ✓
2	RX2 - EMD2002PE-R	Configured OK ✓

Expand/Collapse	Name	Receivers	Zone	Status	
Expand ⌄	SE Bond	2	-	✓Configured OK	⋯
Expand ⌄	SE and DeskVue Bond	2	-	✓Configured OK	⋯

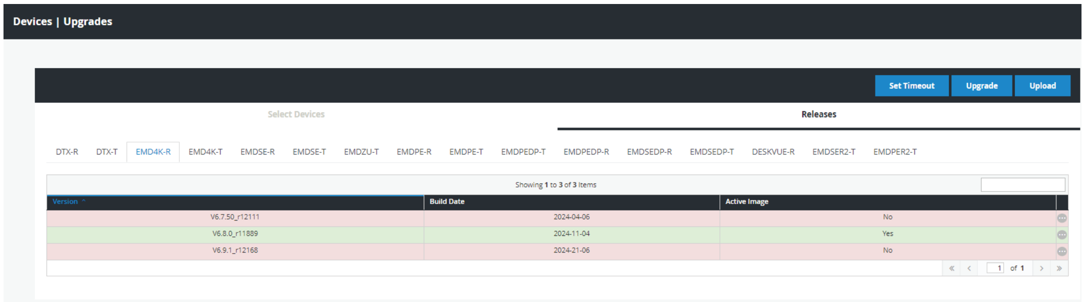
FIGURE 7-16. DEVICES —> GROUPS

7.3 DEVICES—UPGRADE

Boxilla® centrally upgrades devices that are part of its managed domain. The administrator performs this via the Devices— Upgrade page shown in Figure 7-17. Firmware is extremely important since not all versions are compatible with other parts of the system if they are not on the same version. A RemoteApp release is specific to what firmware it is compatible with.

7.3.1 DEVICES— UPGRADE—RELEASES

The Releases tab shows the list of available versions of firmware that can be used to upgrade devices. The administration selects the firmware to be used for upgrades. To select a specific firmware release, click the "Activate" button for the specific version of firmware from the Release options ("•••" icon). This needs to be done for both Receivers (EMD4K-R, EMDSE-R, EMDPE-R, EMDPEDP-R, EMDSEDP-R, DESKVUE-R, and DTX-R) and Transmitters (EMD4K-T, EMDSE-T, EMDZU-T, EMDPE-T, EMDPEDP-T, EMDSEDP-T, EMDSER2-T, EMDPER2-T, EMDDP-T, DTX-T).



Showing 1 to 3 of 3 Items

Version	Build Date	Active Image
V6.7.50_r12111	2024-04-06	No
V6.8.0_r11889	2024-11-04	Yes
V6.9.1_r12168	2024-21-06	No

FIGURE 7-17. DEVICE UPGRADE PAGE

The Administrator loads a new version of firmware by clicking on the "Upload" button on the page and choosing the file(s) to be uploaded. The upload file can be stored anywhere the client browser can access (on local hard-drive, USB thumb-drive, a network file, etc.). Single and Bulk uploads are supported. This new firmware version will be added to appropriate Device list (i.e. Receiver or Transmitter list).

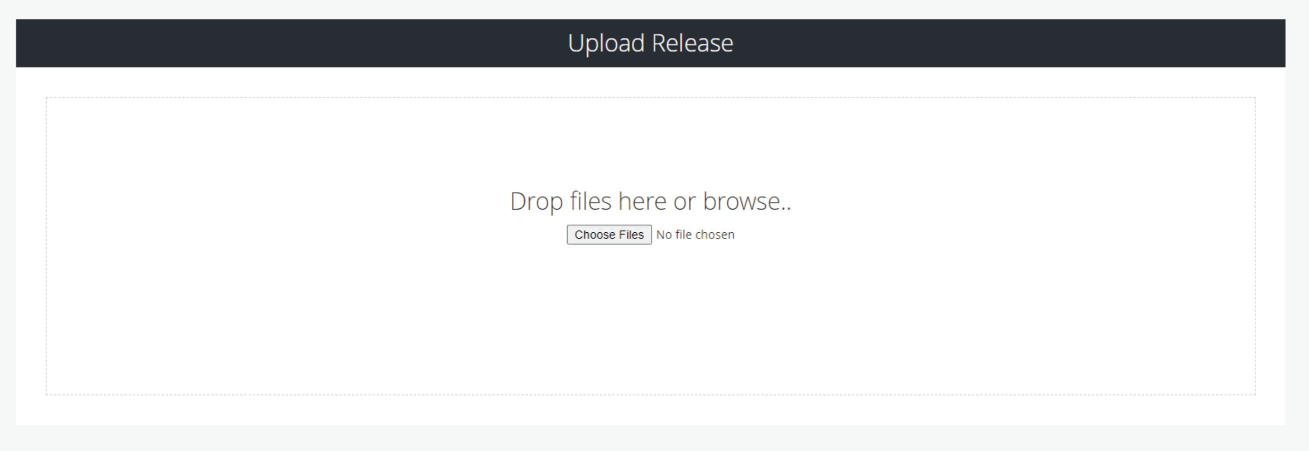


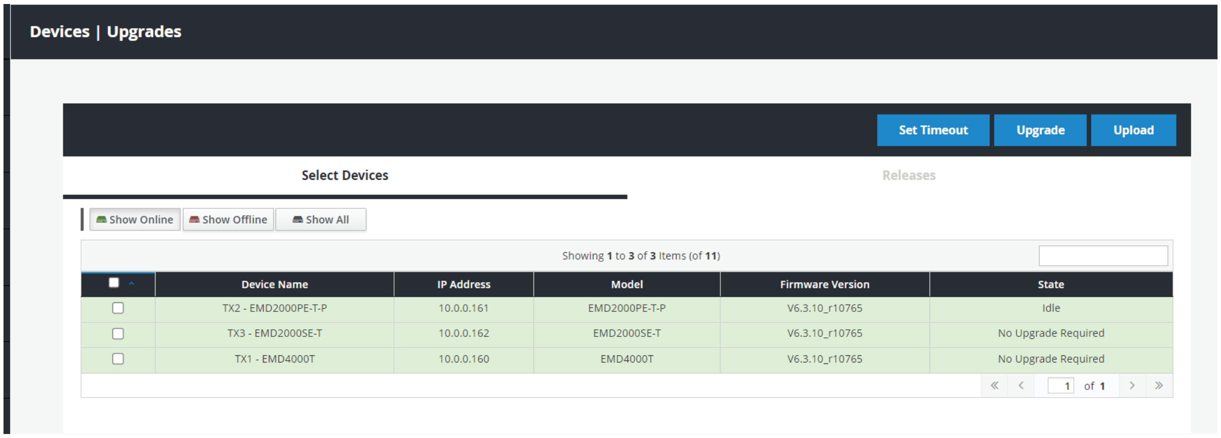
FIGURE 7-18. UPLOAD RELEASE PAGE

To delete a firmware version, the administrator just needs to click on the “delete” option for that release.

7.3.2 DEVICES— UPGRADE—SELECT DEVICES

The administrator needs to select devices to be upgraded to the active firmware versions. The “Select Devices” tab provides a table of all managed devices and allows the administrator to define devices to be upgraded.

The State column shows which devices do not match the active firmware version selected—by showing “Mis-match to Active Firmware Version.” Devices with firmware that match the active firmware version selection will show a “No Upgrade Required” state. The “Idle” state refers to devices that have recently been managed, where no version information has been retrieved from the devices for upgrade purposes.



Showing **1** to **3** of **3** Items (of **11**)

□	Device Name	IP Address	Model	Firmware Version	State
□	TX2 - EMD2000PE-T-P	10.0.0.161	EMD2000PE-T-P	V6.3.10_r10765	Idle
□	TX3 - EMD2000SE-T	10.0.0.162	EMD2000SE-T	V6.3.10_r10765	No Upgrade Required
□	TX1 - EMD4000T	10.0.0.160	EMD4000T	V6.3.10_r10765	No Upgrade Required

FIGURE 7-19. DEVICE UPGRADE SELECTION

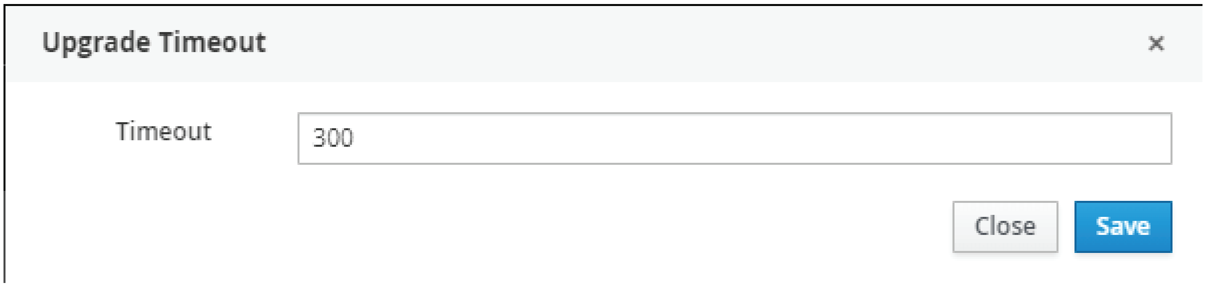
Once the administrator has selected devices to be upgraded (typically all devices that mis-match the active firmware version), the administrator clicks the Upgrade button on the page to initiate the upgrade. All devices can be selected by clicking the tick-box on the top of the column.

The Upgrade button is clicked to initiate the upgrade of all selected devices. Devices that match the “active” firmware version will return “No Upgrade Required” and no upgrade will take place. The rest of the selected devices will be upgraded with various “states” of upgrade being communicated to the administrator during the upgrade process.

NOTE: We recommend that the administrator not move to a different page once starting an upgrade to allow the upgrade process to be monitored. It the administrator does change to a different page, the upgrade will continue in the background. What is mandatory is that Boxilla® and devices being upgraded stay powered up.

7.3.3 DEVICES— UPGRADE—TIMEOUT

Set Timeout button provides the option to configure the Upgrade Timeout period for appliances. This option is useful when upgrading appliances over slow network links where the Upgrade Timeout value may need to be extended. The default Upgrade Timeout Value is set to 300 seconds while the maximum configurable value is 1800 seconds.



Upgrade Timeout

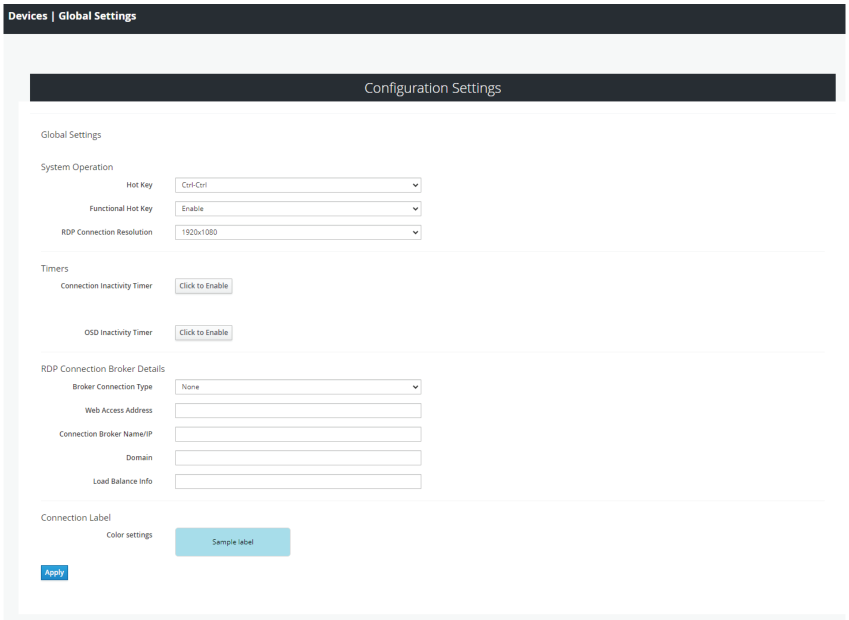
Timeout: 300

FIGURE 7-20. DEVICE UPGRADE TIMEOUT

7.4 DEVICES—GLOBAL

Boxilla® controls global configuration settings for the managed domain. These are settings that apply across all devices in the same way. The administrator changes the parameters to the desired settings and clicks apply to have the changes take effect. This is done on the Devices—Global Settings page. The admin changes the settings and then clicks “Apply.” Changes only take effect when “Apply” is clicked. The properties that can be changed are described in the following sections.

The appliances only pick up the changes to the settings when a user logs in to the device. To ensure global settings are changed on all units at the same time, the Administrator should log out all Users.



Devices | Global Settings

Configuration Settings

Global Settings

System Operation

Hot Key: Ctrl-Ctrl

Functional Hot Key: Enable

RDP Connection Resolution: 1920x1080

Timers

Connection Inactivity Timer: Click to Enable

OSD Inactivity Timer: Click to Enable

RDP Connection Broker Details

Broker Connection Type: None

Web Access Address:

Connection Broker Name/IP:

Domain:

Load Balance Info:

Connection Label

Color settings: Sample label

FIGURE 7-21. DEVICE SETTINGS—CONFIGURATION SETTINGS

Connection Labels: Labels can be configured to display once a connection is established. The position of the Connection Label text and the period of time that the Connection Label text is displayed are configured on each Receiver unit.

Connection Label Display Timeout: This can be set for Always On or for 5 seconds after a connection is established.

Connection Label Location: The location can be configured for the Top Center, Top Right, Bottom Center, or Bottom Right of the screen.

NOTE: Connection Labels are not supported on the Emerald SE Receivers.

7.4.1 HOTKEY

The hotkey is used with the “o” key to terminate the current connection and bring up the OSD on an appliance Receiver. The hotkey with “p” key is used to switch to the previous connection without loading the OSD.

The default hotkey is Print-Screen (PrntScrn). The alternatives are shown in the table below.

In order to support Favorites hotkeys, the Functional Hot Key must be enabled.

TABLE 7-1. HOTKEY SEQUENCES

SEQUENCE	DESCRIPTION
Print Screen (Default)	press Prnt Scrn key
Ctrl + Ctrl	press Ctrl key twice within 1 second
Alt + Alt	press Alt key twice within 1 second
Shift + Shift	press Shift key twice within 1 second
Mouse-Left + Right	press mouse left and right buttons at the same time for 2 seconds (may be required for custom firmware releases, where applicable)

Open OSD: “Hotkey” O

Switch to previous target: “Hotkey” P

The “Functional Hot-Key” is used to enable or disable the use of function keys after the hot-key. When the Functional Hot-key is disabled, only the Hot-Key is required to bring up the OSD on an Emerald Receiver, but Favorites will not work. This means only CTRL-CTRL needed to bring up OSD if CTRL-CTRL selected as hot-key rather than CTRL-CTRL-O when Functional Hot-Key is enabled. It also means the “Hotkey” P, switch to previous target, is no longer is enabled.

The Enable Function key is set by default.

7.4.2 RDP CONNECTION RESOLUTION

This defines the resolution to be requested from the Server when a connection is defined to be to a virtual machine. The actual resolution that the connection actually uses will depend on the Server configuration (see Microsoft documentation).

7.4.3 TIMER SETTINGS

There are two timer settings available. By default they are turned off. The Administrator clicks enable to turn them on and set the timer value required. The two timer settings are:

1. OSD Inactivity Timer—This sets a limit on how long a user can be logged on to the Emerald OSD without any keyboard or mouse activity. Once the user reaches the inactivity timer limit, the user will be logged out of the OSD.
2. Connection Inactivity Timer—This sets a limit on how long a user can be connected to a source (Transmitter) without any keyboard or mouse activity. Once the session reaches the inactivity timer limit, the user will be logged out of the connection and return to the OSD on the Receiver appliance.

NOTE: Inactivity occurs when the mouse or keyboard is not moved or pressed respectively for a set period of time. The Connection Inactivity Timer and OSD Inactivity Timer can be used together.

7.4.4 RDP BROKER SETTINGS

There are two types of Broker types—Connection Broker Server and Web Access Server. The default is none, which means the system uses a connection broker. The Broker type is used to validate the User Credentials (username and password) and determine where the user will be connected to.

The Connection Broker type causes the User Credentials to be sent to the specified Connection Broker. If accepted, then the broker will return the IP address of a local VM from the pool, and this is the IP address used for a connection from the appliance Receiver.

NOTE: We do not support hostnames, so use the IP of the connection broker server.

When “Connection Broker Server” type is selected, the following settings should be set by the Administrator:

1. Enter in the domain name as defined on the local network.
2. Enter in your load balance address as defined in the local server configured, e.g. tsv://VMResource.1.Win7Pool.

The “Web Access Server” setting is used to allow access to a local copy of Active Domain server. If this setting is configured correctly, then if a user who is not configured in the local database attempts to login, the device will redirect the username and password to the local active directory installation and validate the user credentials.

CHAPTER 7: DEVICES

If the user is validated, the Active Directory Server will return a valid VM pool-name to the device. The device sends this pool-name information to the Connection Broker which then allocates a Virtual Machine to the User provided a VM is available.

The following settings need to be set when “Web Access Server” is selected as Broker Connection Type:

1. The Web Access Address should be the login page of the local RD Web Access Server using its IP address, e.g. https://192.168.10.7/RDWeb/Pages/en-US/login.aspx.

NOTE: We currently do not cater for hostnames in the web address, so please use the IP of the Web Access server. You must place the full address in the login page of the RD Web Access server (https://*************.apsx).

2. Enter the local Connection Broker IP address.

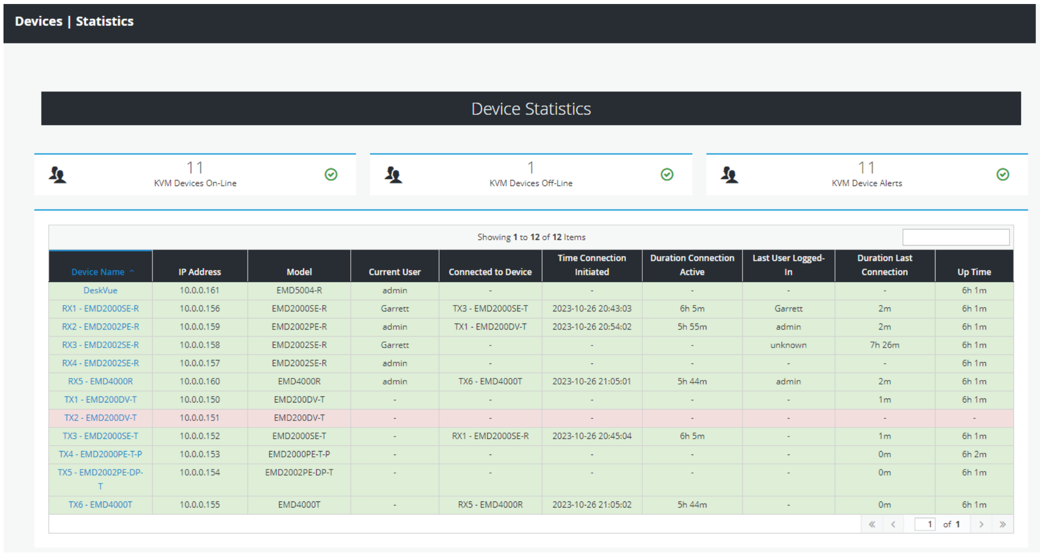
3. Enter the local domain name.

On the Receiver appliance, when the user attempts to log in, the login will now take the following steps in this order:

1. The login credentials are checked to see if the user is configured locally on the Receiver. If the user exists, they will be logged in as normal. If not, then step two will occur. If Broker Connection Type is set to “None,” the Receiver appliance at login will only attempt to authenticate the user locally. This is the default setting.
2. If the Broker Connection Type is set to “Web Access Server,” the Receiver will attempt to launch a connection to an RD Web Access server. This will allow the user to be Authenticated against the Domain Controller (Active Directory), allowing the user to access Virtual Desktop Pools and Personal Virtual desktops.

7.5 DEVICES—STATISTICS

The Device Statistics page provides an overview of the operation of the managed domain as shown in Figure 7-21. It provides an overview of the device on-line and off-line (not contactable). Then a table of devices is displayed showing what user is logged in to what device, when they logged in and how long they were logged in.



Devices | Statistics

Device Statistics

11 KVM Devices On-Line

1 KVM Devices Off-Line

11 KVM Device Alerts

Showing **1** to **12** of **12** Items

Device Name ˄	IP Address	Model	Current User	Connected to Device	Time Connection Initiated	Duration Connection Active	Last User Logged-In	Duration Last Connection	Up Time
DeskVue	10.0.0.161	EMD5004-R	admin	-	-	-	-	-	6h 1m
RX1 - EMD2000SE-R	10.0.0.156	EMD2000SE-R	Garrett	TX3 - EMD2000SE-T	2023-10-26 20:43:03	6h 5m	Garrett	2m	6h 1m
RX2 - EMD2002PE-R	10.0.0.159	EMD2002PE-R	admin	TX1 - EMD200DV-T	2023-10-26 20:54:02	5h 55m	admin	2m	6h 1m
RX3 - EMD2002SE-R	10.0.0.158	EMD2002SE-R	Garrett	-	-	-	unknown	7h 26m	6h 1m
RX4 - EMD2002SE-R	10.0.0.157	EMD2002SE-R	admin	-	-	-	-	-	6h 1m
RX5 - EMD4000R	10.0.0.160	EMD4000R	admin	TX6 - EMD4000T	2023-10-26 21:05:01	5h 44m	admin	2m	6h 1m
TX1 - EMD200DV-T	10.0.0.150	EMD200DV-T	-	-	-	-	-	1m	6h 1m
TX2 - EMD200DV-T	10.0.0.151	EMD200DV-T	-	-	-	-	-	-	-
TX3 - EMD2000SE-T	10.0.0.152	EMD2000SE-T	-	RX1 - EMD2000SE-R	2023-10-26 20:45:04	6h 5m	-	1m	6h 1m
TX4 - EMD2000PE-T-P	10.0.0.153	EMD2000PE-T-P	-	-	-	-	-	0m	6h 2m
TX5 - EMD2002PE-DP-T	10.0.0.154	EMD2002PE-DP-T	-	-	-	-	-	0m	6h 1m
TX6 - EMD4000T	10.0.0.155	EMD4000T	-	RX5 - EMD4000R	2023-10-26 21:05:02	5h 44m	-	0m	6h 1m

FIGURE 7-22. DEVICE STATISTICS

CHAPTER 8: SWITCHES

The “Switches” menu has three subheadings:

- Status
- Upgrades
- Connections

These all link to individual pages.

The Status page initially shows a list of all the Black Box branded switches in the KVM Network. Clicking on a particular switch brings you to a page displaying all the ports of that particular switch. This page also allows you perform certain actions on the switch as detailed below.

Black Box offers the following IP Network Switches:

- 24-Port 1G Fiber Switch (EMS1G24F)
- 48-Port 1G IP Network Switch (EMS1G-48)
- 12-Port 10G IP Network Switch (EMS10G-12)
- 28-Port 10G IP Network Switch (EMS10G-28)
- 32-Port 100G IP Network Switch (EMS100G-32)

The Upgrades page is similar to the appliance Upgrade page. This shows a list of all the Black Box branded switches in the KVM network plus their current firmware version. If there is a mismatch to the activated firmware release, this is flagged. You can also upload a release from this page. NOTE: Uploading a release takes about 15 minutes, including the reboot.

The Connections page provides a list of all active KVM connections from Transmitter devices to Receiver devices across all Black Box branded switches that are managed by Boxilla®. The list correlates the KVM devices with the relevant switch ports and also provides statistics for each switch port.

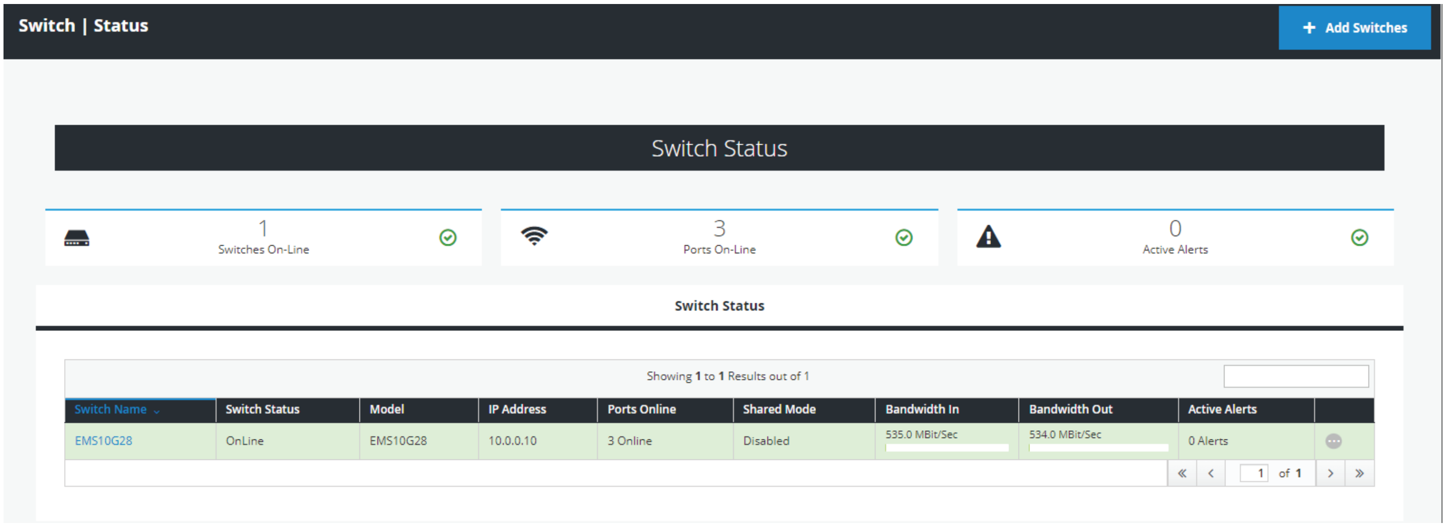
Only the EMS switches mentioned above are compatible with Boxilla, and they require a special firmware to allow them to be managed. If the special firmware was not applied to the EMS switch, you will need to do that first before getting Boxilla to manage it.

CHAPTER 8: SWITCHES

8.1 SWITCHES — STATUS

8.1.1 STATUS PAGE - SWITCH VIEW

The status page when clicked shows a list of the active switches in the KVM network. This has three summary info cards on the top of the screen that detail the number of switches currently online managed by Boxilla®, how many ports have a cable connected and are active, and how many alerts are across the whole Boxilla system relating to switches. In the table, we display the Switch Name, Switch Status, Model, IP Address, how many ports online per switch, whether or not Shared Mode is enabled, the bandwidth in and out figures/graph, the number of alerts on that switch and an option menu. The switch names will be hyperlinks that take you to another page where you get a drill-down of the ports on that switch.



Switch | Status

Switch Status

1 Switches On-Line

3 Ports On-Line

0 Active Alerts

Switch Status

Showing **1** to **1** Results out of 1

Switch Name	Switch Status	Model	IP Address	Ports Online	Shared Mode	Bandwidth In	Bandwidth Out	Active Alerts	
EMS10G28	OnLine	EMS10G28	10.0.0.10	3 Online	Disabled	535.0 MBit/Sec	534.0 MBit/Sec	0 Alerts	

FIGURE 8-1. SWITCH STATUS SCREEN

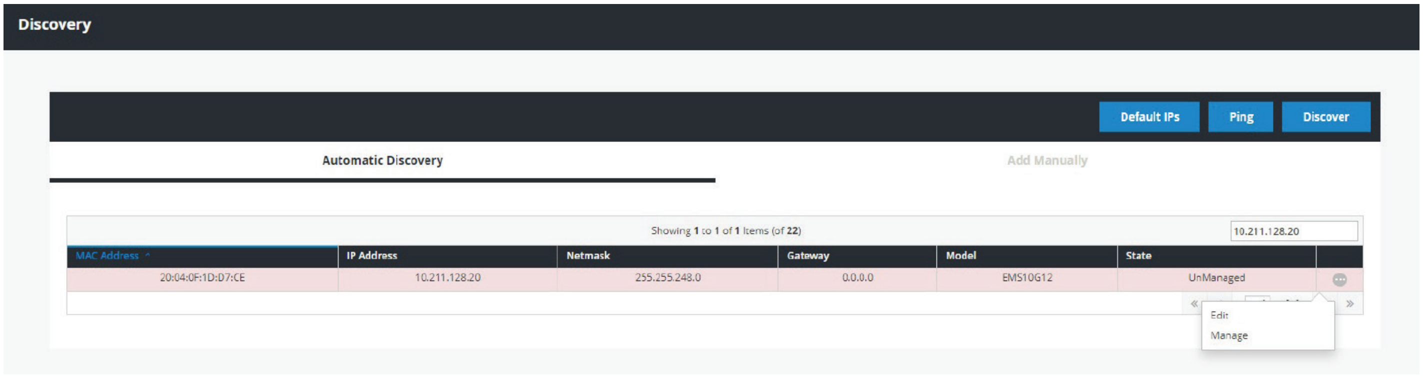
8.1.2 ADDING A SWITCH

There are two ways you can add a switch to be managed. You can automatically discover it by clicking on the Discovery tab in the main menu, or you can click on the + Switch button on the top of the switch status page to add it manually into the Boxilla system.

NOTE: This feature currently does not allow the network switch password to be entered and assumes it is using the default setting. If you changed the Network Switch password, you need to change it back to the default password to continue operation.

AUTOMATIC DISCOVERY

Click on the Discovery tab from the main menu. A screen showing the Automatic Discovery tab appears. On this screen an UnManaged switch appears shaded in pink and a managed switch appears in green.



Showing 1 to 1 of 1 Items (of 22)

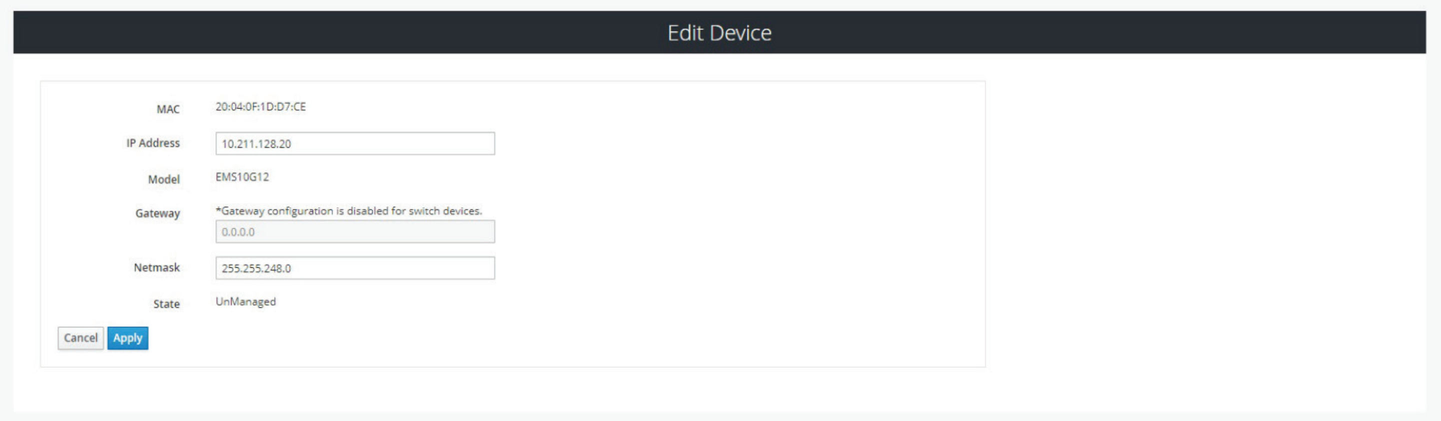
10.211.128.20

MAC Address	IP Address	Netmask	Gateway	Model	State	
20:04:0F:1D:D7:CE	10.211.128.20	255.255.248.0	0.0.0.0	EMS10G12	UnManaged	•••

FIGURE 8-2. AUTOMATIC DISCOVERY TAB

Click on the ellipsis "•••" icon and the drop-down menu to Edit or Manage the switch.

If you select Edit, the Edit Device screen appears.



Edit Device

MAC 20:04:0F:1D:D7:CE

IP Address 10.211.128.20

Model EMS10G12

Gateway *Gateway configuration is disabled for switch devices. 0.0.0.0

Netmask 255.255.248.0

State UnManaged

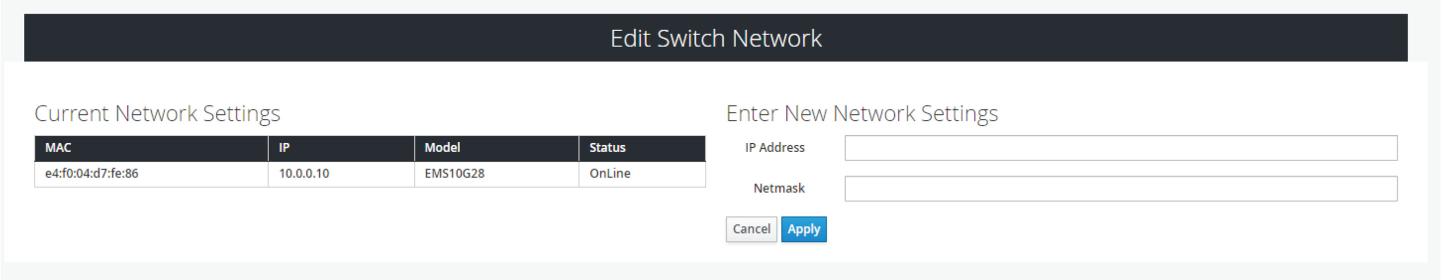
FIGURE 8-3. EDIT DEVICE SCREEN

Enter the IP address and net mask.

Click on Apply to confirm the changes or Cancel to cancel the changes.

When you click on Apply, a popup box tells you that editing network settings will reboot the device.

NOTE: The switch takes about 5 minutes to reboot.



Edit Switch Network

Current Network Settings

MAC	IP	Model	Status
e4:f0:04:d7:fe:86	10.0.0.10	EMS10G28	OnLine

Enter New Network Settings

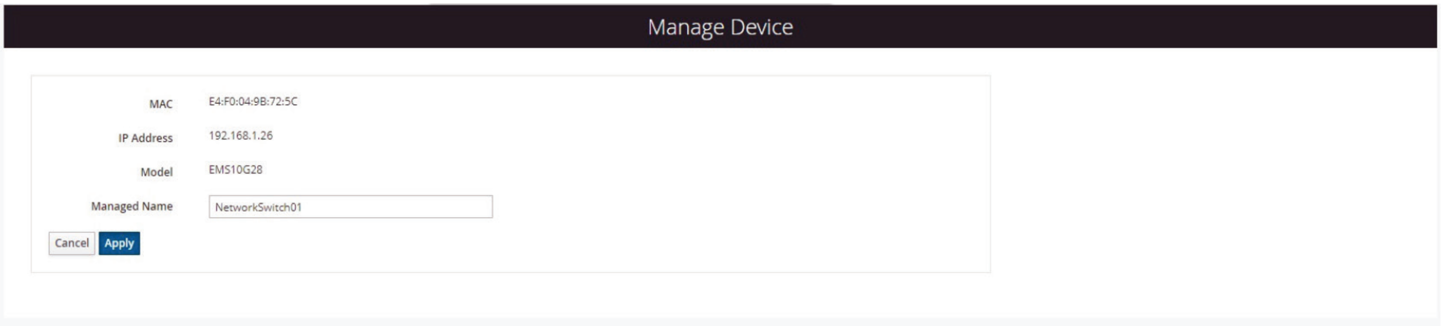
IP Address

Netmask

FIGURE 8-4. ENTER NEW NETWORK SETTINGS SCREEN

Manage

If you select Manage, the Manage Device screen appears.



Manage Device

MAC E4:F0:04:9B:72:5C

IP Address 192.168.1.26

Model EMS10G28

Managed Name NetworkSwitch01

FIGURE 8-5. MANAGE DEVICE SCREEN

Enter the Managed Name and click on Apply.

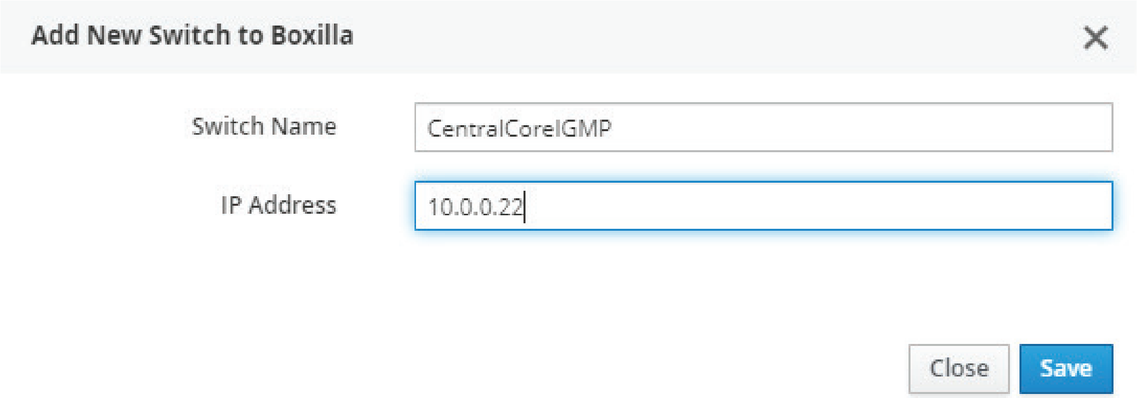
A popup box asks: Are you sure you want to manage this device?

Click on OK to continue or Cancel to stop.

TIP: If the Boxilla® cannot discover the network switch, try adding it manually using the next step. Not being able to discover may be common, but manually adding should work if the switch is configured and reachable.

ADDING A SWITCH VIA THE +SWITCH BUTTON

Clicking the blue "+ Switch" button on the top right corner of the Switch status page pops up a window with the following editing options for the details of the switch to be added:



Add New Switch to Boxilla

Switch Name: CentralCoreIGMP

IP Address: 10.0.0.22

FIGURE 8-6. ADD NEW SWITCH TO THE BOXILLA SCREEN

Clicking "Apply" adds the switch into the table on the status page. As part of the manage process, we first ensure that it is a Black Box switch by studying the bbx.info file to ensure it has the correct data. You then query the switch and get the port information and switch properties and populate our database with the new information. You also copy our domain token to the switch so the switch is then managed by that Boxilla®.

Switch Actions/Options menu

Clicking the “options” elliipsis button on the right-hand side of each switch row will give you a drop-down with some options. These are as below:

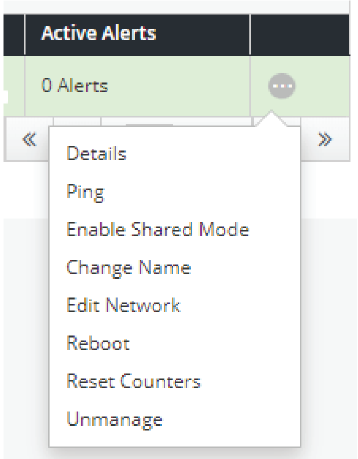
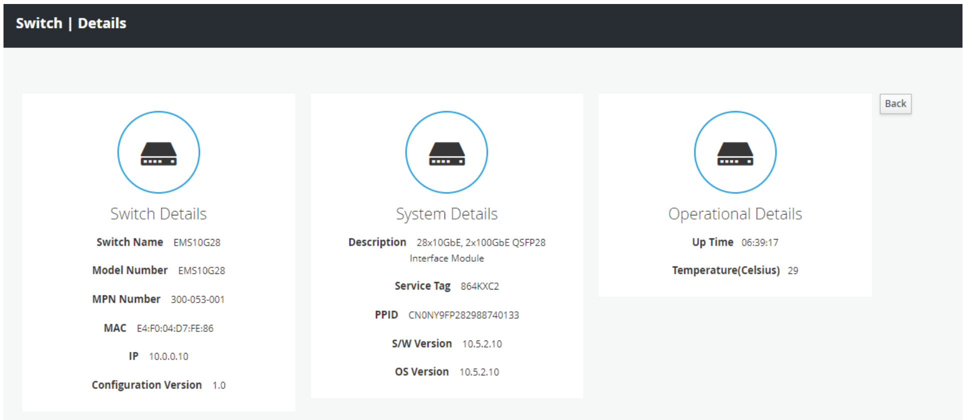


FIGURE 8-7. OPTIONS LIST

• Details: This retrieves details about the switch. Example display below.



Switch Details

Switch Name EMS10G28

Model Number EMS10G28

MPN Number 300-053-001

MAC E4:F0:04:D7:FE:86

IP 10.0.0.10

Configuration Version 1.0

System Details

Description 28x10GbE, 2x100GbE QSFP28 Interface Module

Service Tag 864KXC2

PPID CN0NY9FP282988740133

S/W Version 10.5.2.10

OS Version 10.5.2.10

Operational Details

Up Time 06:39:17

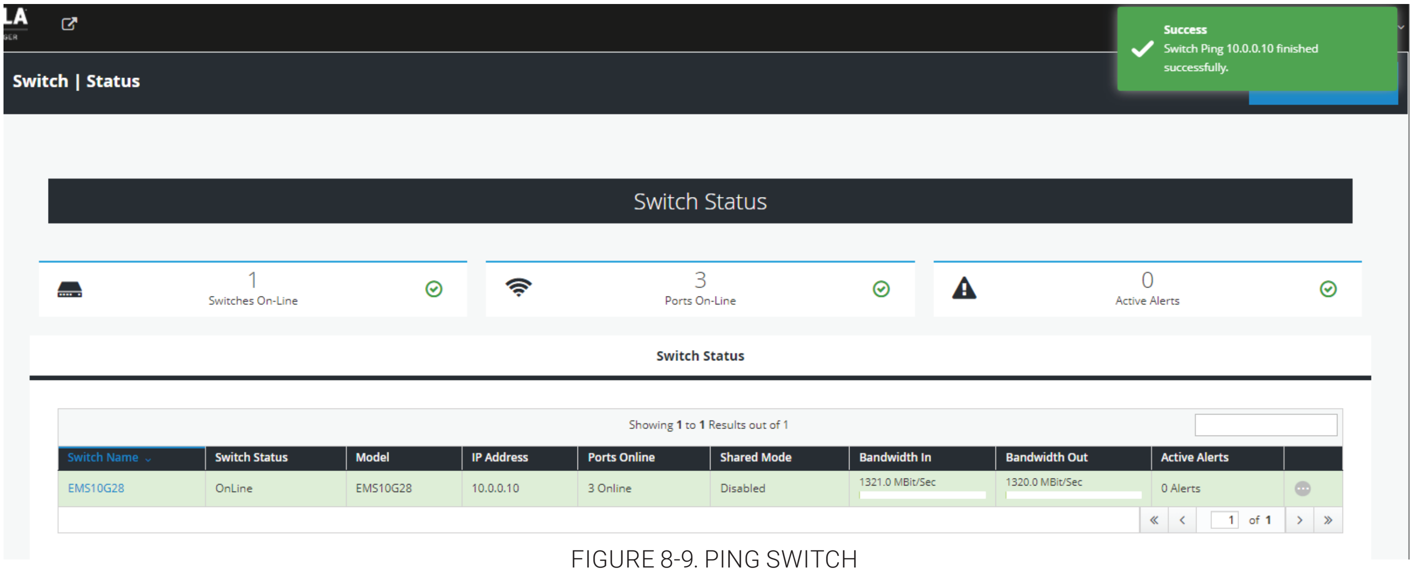
Temperature(Celsius) 29

FIGURE 8-8. SWITCH DETAILS PAGE

- Ping: This pings the management port of the network switch to verify it is powered up and connected.
- Enable/Disable Shared Mode: If you enable shared mode, Boxilla creates VLAN 1003, Boxilla moves all ports into that VLAN and globally enables IGMP Snooping on the switch. Shared analog audio is enabled when shared mode is enabled. When disabling shared mode, Boxilla disables IGMP Snooping and removes VLAN 1003 which moves all ports back into VLAN 1. This functionality is automatically completed once the Enable/Disable Share Mode option is selected. By enabling Shared Mode, Boxilla performs these operations in the background automatically.
- Change Name: Change the name of the switch in the Boxilla® database. This also renames all alerts to the new name.
- Edit Network: This allows the user to change the IP address of the switch.
- Reboot: Reboot the switch.
- Reset Counters: This will reset all of the statistics shown in the table so that fresh data can be viewed.
- Unmanage: This disables IGMP Snooping, MRouter details and the custom VLAN 1003 and moves all ports back to VLAN 1 and then deletes the switch from our database. It also removes the domain token from the switch. If you lose communication with the switch but still wish to unmanage it, you have the option to locally unmanage. Unmanaging also sets the switch in a factory default state. If you wish to keep the switch settings but remove it from Boxilla, you will need to disconnect the network switch first completely from the setup and then in Boxilla you can Unmanage it.

PING SWITCH

To ping this switch, click on the ellipsis “•••” icon and a drop-down menu appears. Click on the Ping option and wait for the results.



Success
Switch Ping 10.0.0.10 finished successfully.

Switch | Status

Switch Status

1 Switches On-Line

3 Ports On-Line

0 Active Alerts

Switch Status

Showing **1** to **1** Results out of 1

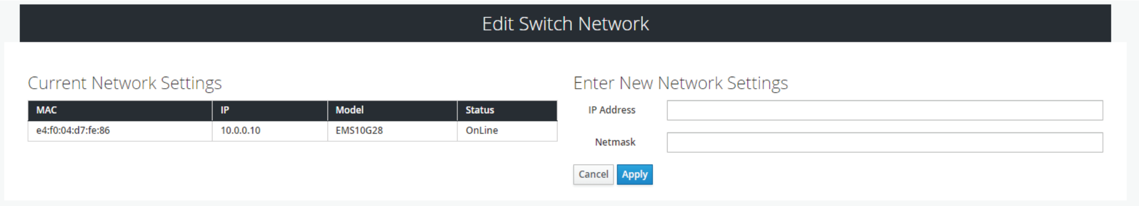
Switch Name	Switch Status	Model	IP Address	Ports Online	Shared Mode	Bandwidth In	Bandwidth Out	Active Alerts	
EMS10G28	OnLine	EMS10G28	10.0.0.10	3 Online	Disabled	1321.0 MBit/Sec	1320.0 MBit/Sec	0 Alerts	•••

1 of **1**

FIGURE 8-9. PING SWITCH

EDIT NETWORK

To Edit the Switch Network switch, click on the ellipsis “•••” icon and a drop-down menu appears. Click on the Edit Network option and enter the changes. When finished making changes, click on the Apply button to confirm changes or the Cancel button to discard the changes. If confirming changes, the switch will reboot, which requires approximately 5 minutes to finish.



Edit Switch Network

Current Network Settings

MAC	IP	Model	Status
e4:f0:04:d7:fe:86	10.0.0.10	EMS10G28	OnLine

Enter New Network Settings

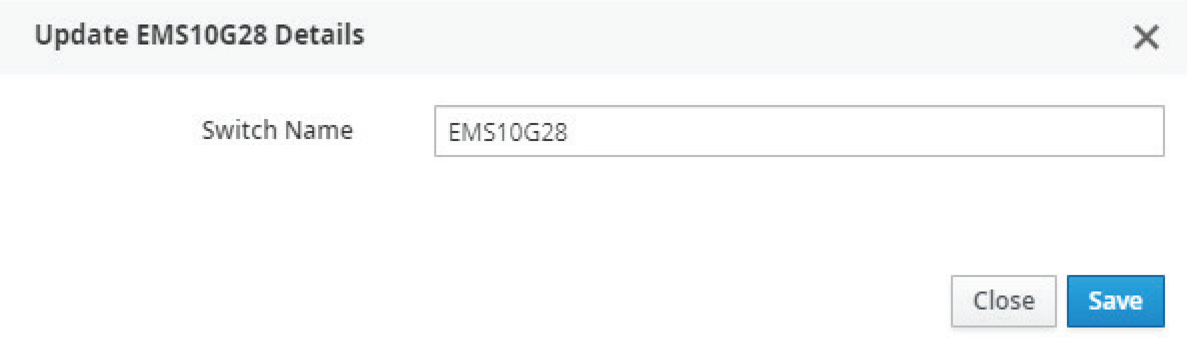
IP Address

Netmask

FIGURE 8-10. SWITCH VIEW STATUS

CHANGE NAME

To change the name of the switch, click on the Change Name option in the drop-down menu and enter a new name for the switch. Once complete, click on the Save button to save your changes or click on the Close button to discard the changes.


Update EMS10G28 Details

Switch Name: EMS10G28

FIGURE 8-11. UPDATE NETWORK SWITCH

SHARED MODE

To enable Shared mode on a switch from the Switch Status screen, click on Enable Shared Mode from the drop-down menu. Shared analog audio is enabled when shared mode is enabled.

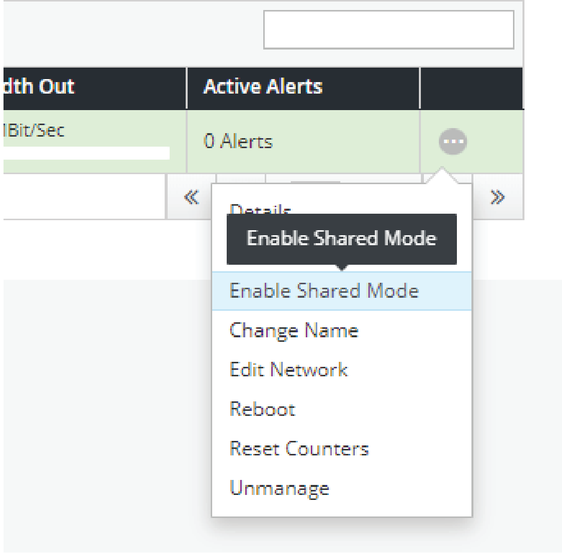


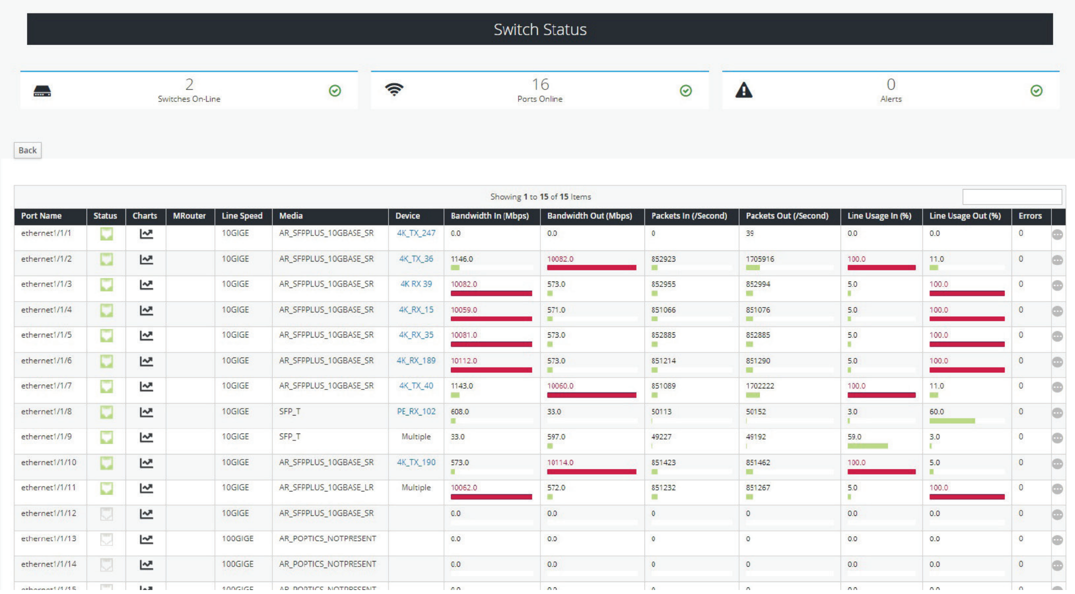
FIGURE 8-12. ENABLE SHARED MODE

The set of operations are performed automatically once the option has been selected.

8.1.3 STATUS PAGE - PORTS VIEW

Once you click a switch name, you are presented with a table view of all the ports on that particular switch. This shows some summary information of that port similar to the active connection table. This table tells you the following:

- PortName
- The status of the switch. Green means it’s online. Grey means it’s offline. Red means it’s disabled.
- The Media type as reported by the Black Box Switch.
- The Bandwidth In and Out (integer and bar chart)
- Packets In and Out (integer and bar chart)
- Line Usage in and Out (integer and chart)
- Port Errors
- Port Options
- Enable/Disable Port
- Enable MRouter
- *(EMS100G-R2 only) Option to Enable or Disable Breakout Module



Switch Status

2 Switches On-Line	16 Ports Online	0 Alerts

Showing **1** to **15** of **15** Items

Port Name	Status	Charts	MRouter	Line Speed	Media	Device	Bandwidth In (Mbps)	Bandwidth Out (Mbps)	Packets In (/Second)	Packets Out (/Second)	Line Usage In (%)	Line Usage Out (%)	Errors	
ethernet1/1/1	🟩	📈		10GIGE	AR_SFPPLUS_10GBASE_SR	4K_TX_247	0.0	0.0	0	39	0.0	0.0	0	⋯
ethernet1/1/2	🟩	📈		10GIGE	AR_SFPPLUS_10GBASE_SR	4K_TX_36	1146.0	10082.0	852923	1705916	100.0	11.0	0	⋯
ethernet1/1/3	🟩	📈		10GIGE	AR_SFPPLUS_10GBASE_SR	4K RX 39	10082.0	573.0	852955	852994	5.0	100.0	0	⋯
ethernet1/1/4	🟩	📈		10GIGE	AR_SFPPLUS_10GBASE_SR	4K_RX_15	10059.0	571.0	851066	851076	5.0	100.0	0	⋯
ethernet1/1/5	🟩	📈		10GIGE	AR_SFPPLUS_10GBASE_SR	4K_RX_35	10081.0	573.0	852885	852885	5.0	100.0	0	⋯
ethernet1/1/6	🟩	📈		10GIGE	AR_SFPPLUS_10GBASE_SR	4K_RX_189	10112.0	573.0	851214	851290	5.0	100.0	0	⋯
ethernet1/1/7	🟩	📈		10GIGE	AR_SFPPLUS_10GBASE_SR	4K_TX_40	1143.0	10060.0	851089	1702222	100.0	11.0	0	⋯
ethernet1/1/8	🟩	📈		10GIGE	SFP_T	PE_RX_102	608.0	33.0	50113	50152	3.0	60.0	0	⋯
ethernet1/1/9	🟩	📈		10GIGE	SFP_T	Multiple	33.0	597.0	49227	49192	59.0	3.0	0	⋯
ethernet1/1/10	🟩	📈		10GIGE	AR_SFPPLUS_10GBASE_SR	4K_TX_190	573.0	10114.0	851423	851462	100.0	5.0	0	⋯
ethernet1/1/11	🟩	📈		10GIGE	AR_SFPPLUS_10GBASE_LR	Multiple	10062.0	572.0	851232	851267	5.0	100.0	0	⋯
ethernet1/1/12	□	📈		10GIGE	AR_SFPPLUS_10GBASE_SR		0.0	0.0	0	0	0.0	0.0	0	⋯
ethernet1/1/13	□	📈		100GIGE	AR_POPTICS_NOTPRESENT		0.0	0.0	0	0	0.0	0.0	0	⋯
ethernet1/1/14	□	📈		100GIGE	AR_POPTICS_NOTPRESENT		0.0	0.0	0	0	0.0	0.0	0	⋯
ethernet1/1/15	□	📈		100GIGE	AR_POPTICS_NOTPRESENT		0.0	0.0	0	0	0.0	0.0	0	⋯

FIGURE 8-13. SWITCH STATUS PORTS VIEW

This information is polled every minute and the page updates on the next page refresh.

PORT OPTIONS—ENABLE/DISABLE PORTS

The drop-down menu has two options: Disable Port and Enable MRouter. Click on the ellipsis "•••" icon and a drop-down menu appears.

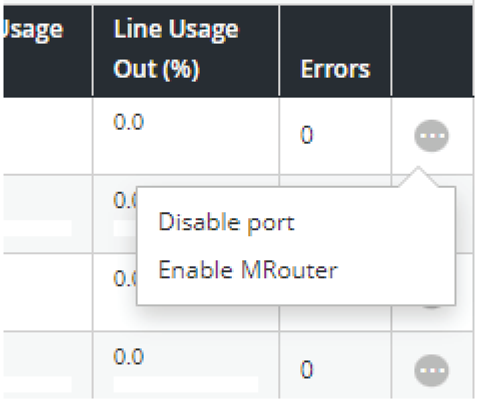


FIGURE 8-14. ENABLE/DISABLE PORT OPTIONS

If you click on Disable Port, the relevant port is disabled and you get a confirmation screen.

To enable a port again, click on the ellipsis "•••" icon next to a port that has status red.

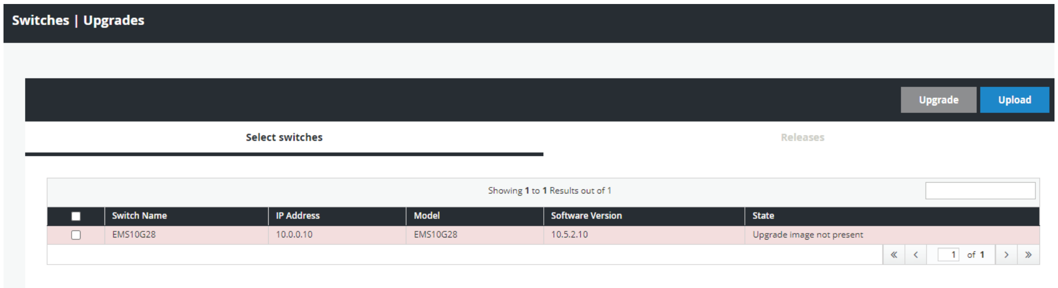
MROUTER

When you select MRouter it goes to the switch and issues the MRouter command. You only want one port to be the MRouter at any time on the switch, so any time the user selects an MRouter, you remove the current MRouter and select the new one.

If you click on Enable MRouter, a pop-up box appears, and you can click on OK to confirm or Leave to cancel the action.

8.2 SWITCHES - UPGRADES

The upgrades page is similar to the appliance upgrades page. It lists the switches currently in the database and also indicates "active release" in the database. Any switch that does not match this release is highlighted in red. You can then select multiple switches and upgrade them in parallel. The upgrade state changes dynamically as the switch goes through different stages of the upgrade process. It transfers the file to the switch, upgrades the switch, then reboots and verifies the upgrade. If all is successful, the switch is now be highlighted in green. If there has been an error, the switch row is highlighted in red with the error state displaying. NOTE: The switch takes about 15 minutes to upgrade and restart.



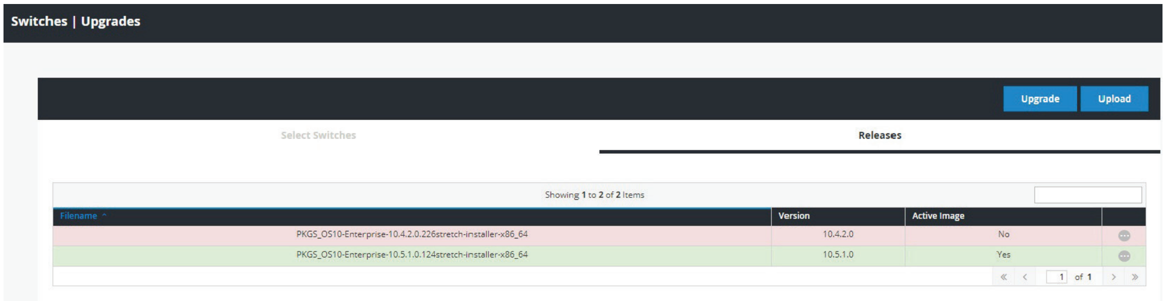
Showing 1 to 1 Results out of 1

■	Switch Name	IP Address	Model	Software Version	State
□	EMS10G28	10.0.0.10	EMS10G28	10.5.2.10	Upgrade image not present

FIGURE 8-15. SWITCH UPGRADES PAGE

Activate Release

Click on the Releases tab, then click on the drop-down menu item and Activate or delete the release.



Filename ˄	Version	Active Image	
PKGS_OS10-Enterprise-10.4.2.0.226stretch-installer-x86_64	10.4.2.0	No	⋯
PKGS_OS10-Enterprise-10.5.1.0.124stretch-installer-x86_64	10.5.1.0	Yes	⋯

FIGURE 8-16. ACTIVATE RELEASE

To upload a new release for the switch, click on the blue Upload button in the top right hand corner and follow the steps.

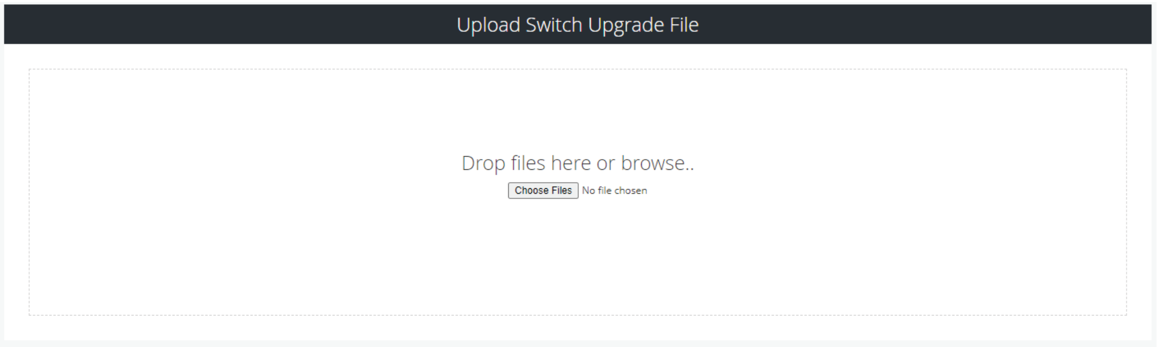
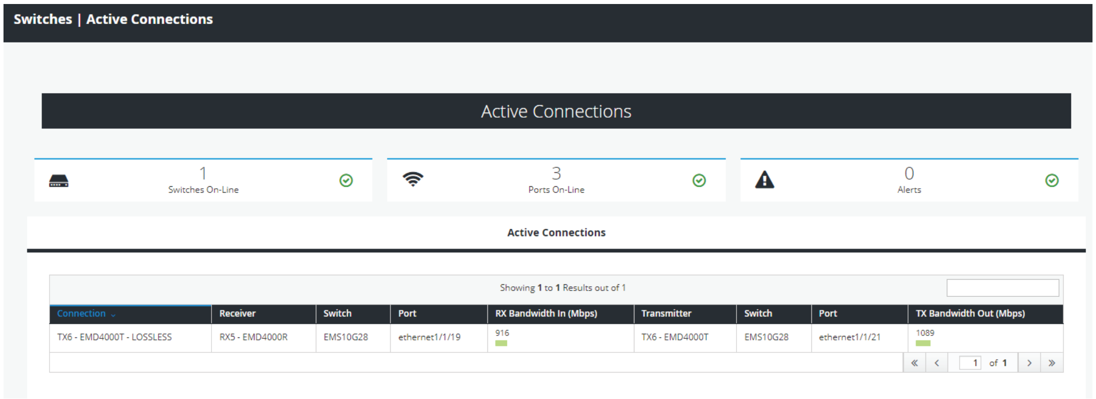


FIGURE 8-17. UPLOAD RELEASE

It is possible to upgrade the EMS network switches without Boxilla® by using the network switch's command line. Those steps are not outlined in this user manual, but they are included in the EMS network switch manual and EMS network switch support guides.

8.3 SWITCHES — CONNECTIONS

The Connections page when clicked shows a list of all the active KVM Transmitter to Receiver connections across all Black Box branded switches managed by Boxilla® in the KVM network. This has three summary info cards on the top of the screen that detail the number of switches currently online managed by Boxilla, how many ports have a cable connected and are active, and how many alerts are across the whole Boxilla system relating to switches.



Switches | Active Connections

Active Connections

1 Switches On-Line

3 Ports On-Line

0 Alerts

Active Connections

Showing **1** to **1** Results out of 1

Connection ⌄	Receiver	Switch	Port	RX Bandwidth In (Mbps)	Transmitter	Switch	Port	TX Bandwidth Out (Mbps)
TX6 - EMD4000T - LOSSLESS	RX5 - EMD4000R	EMS10G28	ethernet1/1/19	916	TX6 - EMD4000T	EMS10G28	ethernet1/1/21	1089

FIGURE 8-18. ACTIVE CONNECTIONS

Each Active Connection is displayed in the table. The contents of each row in the Active Connections table includes:

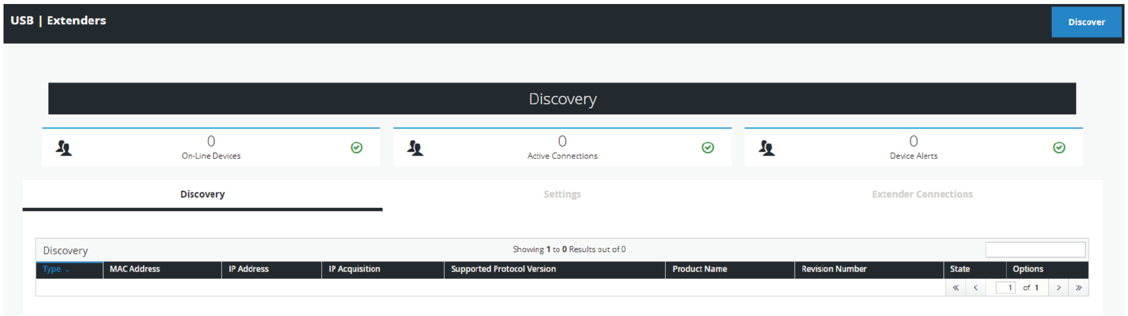
- Connection Name.
- From a Receiver device perspective:
  - The name of the KVM Receiver device.
  - The Black Box branded Switch name and Port number where the KVM Receiver device is attached to.
  - Receiver Bandwidth in Mbps (integer and bar chart) at the Switch Port.
- From a Transmitter device perspective:
  - The name of the KVM Transmitter device.
  - The Black Box branded Switch name and Port number where the KVM Transmitter device is attached to.
  - Transmitter Bandwidth in Mbps (integer and bar chart) at the Switch Port.

CHAPTER 9: PERIPHERALS

To support external USB switching that can handle speeds up to 480 Mbps (USB High Speed), additional USB hubs can be bonded with the Emerald technology. To configure the USB Hub bonding, the Boxilla® will need to be part of the application.

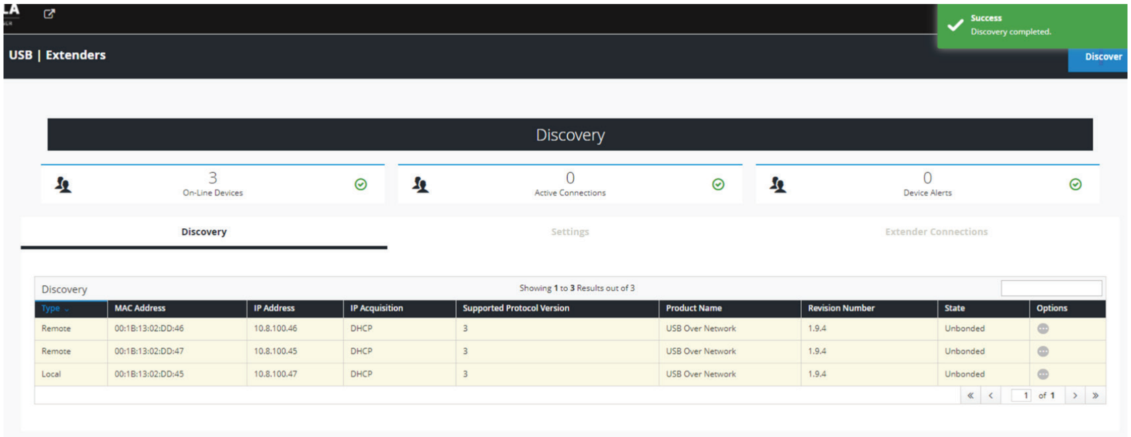
Connect the USB 2.0 Transmitters and Receivers to the Emerald/Boxilla network. In Boxilla, the administrator can navigate to the "Peripherals" tab and discover the USB 2.0 Transmitters and Receivers. The EMD100USB extenders are the only USB 2.0 devices that are supported for Boxilla bonding. A total of 200 EMD100USB devices can be configured within Boxilla to support USB 2.0 switching up to 480Mbps.

9.1 PERIPHERALS - DISCOVERY TAB



Type	MAC Address	IP Address	IP Acquisition	Supported Protocol Version	Product Name	Revision Number	State	Options

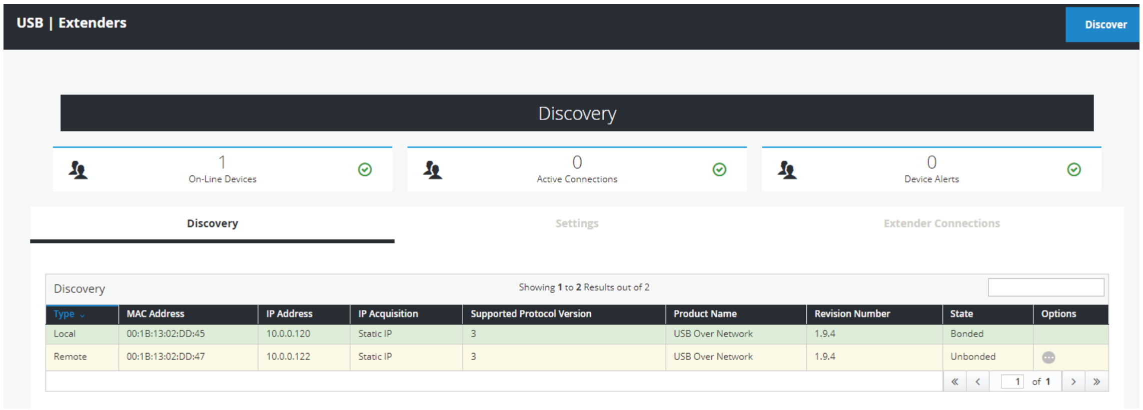
FIGURE 9-1. DISCOVERY TAB



Type	MAC Address	IP Address	IP Acquisition	Supported Protocol Version	Product Name	Revision Number	State	Options
Remote	00:1B:13:02:DD:46	10.8.100.46	DHCP	3	USB Over Network	1.9.4	Unbonded	⋯
Remote	00:1B:13:02:DD:47	10.8.100.45	DHCP	3	USB Over Network	1.9.4	Unbonded	⋯
Local	00:1B:13:02:DD:45	10.8.100.47	DHCP	3	USB Over Network	1.9.4	Unbonded	⋯

FIGURE 9-2. DISCOVERY SUCCESS

Once discovered, the DHCP IP address will need to change to Static by using the “Edit Network” option, so be sure to configure the devices with Static IP addresses that are part of the same subnet as the Emerald technology.

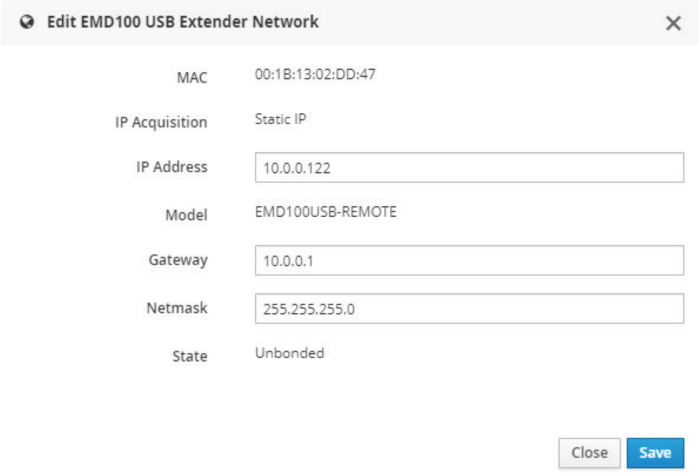


Discovery

Showing **1** to **2** Results out of 2

Type	MAC Address	IP Address	IP Acquisition	Supported Protocol Version	Product Name	Revision Number	State	Options
Local	00:1B:13:02:DD:45	10.0.0.120	Static IP	3	USB Over Network	1.9.4	Bonded	
Remote	00:1B:13:02:DD:47	10.0.0.122	Static IP	3	USB Over Network	1.9.4	Unbonded	●

FIGURE 9-3. EDIT NETWORK OPTION

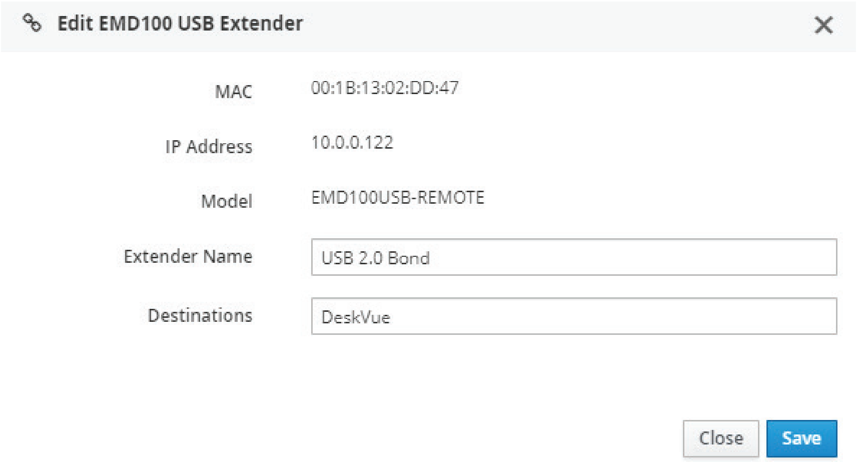

Edit EMD100 USB Extender Network

MAC	00:1B:13:02:DD:47
IP Acquisition	Static IP
IP Address	10.0.0.122
Model	EMD100USB-REMOTE
Gateway	10.0.0.1
Netmask	255.255.255.0
State	Unbonded

FIGURE 9-4. EDIT USB EXTENDER NETWORK SCREEN

NOTE: The automatic discovery of EMD100USB devices assumes a DHCP server is operational on the target network. If a DHCP server is not present on the target network each EMDUSB100 extender is initially configured with the 169.254 static subnet direct from the factory, with its detailed IP address under the subnet remaining hidden. If you do not have a DHCP server on the network that can assign an IP address to the device, Black Box can provide the needed steps to configure them using a command prompt.

You can now Bond the USB 2.0 Transmitters and Receivers to the Emerald Transmitters and Receivers by choosing “Edit Bonding” and giving the device a name and selecting which Emerald device it is bonded with.



Edit EMD100 USB Extender

MAC 00:1B:13:02:DD:47

IP Address 10.0.0.122

Model EMD100USB-REMOTE

Extender Name USB 2.0 Bond

Destinations DeskVue

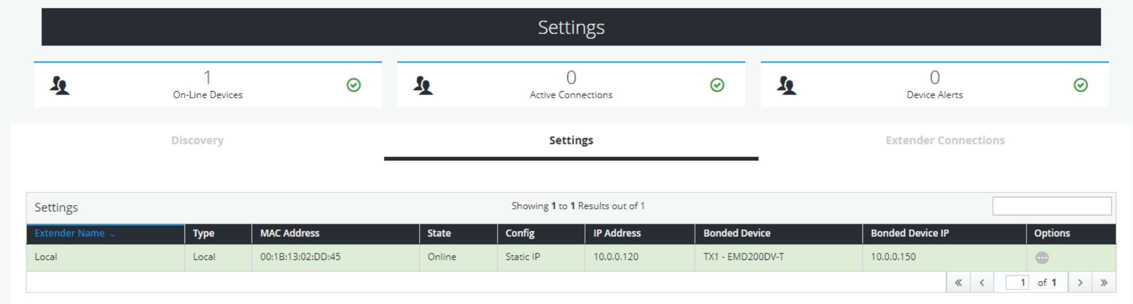
FIGURE 9-5. BONDING CONFIGURATION

Repeat the bonding for additional extenders.

Once the USB 2.0 Transmitters and Receivers are bonded with Emerald hardware, they can be used during the connection. When establishing a new connection or breaking a connection, the USB 2.0 Transmitters and Receivers will switch with their respective bonded Emerald connection.

9.2 PERIPHERALS - SETTINGS TAB

Additional functions can be used with the USB 2.0 Transmitter and Receivers hubs by navigating to Peripherals>>Settings.



Settings

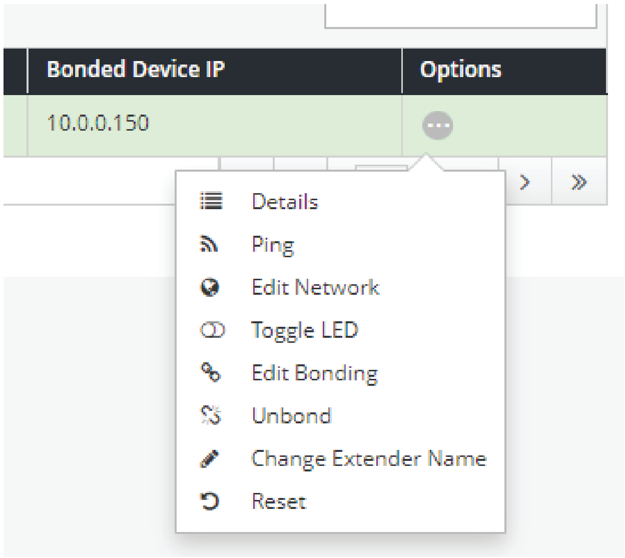
Showing **1** to **1** Results out of 1

Extender Name ⌄	Type	MAC Address	State	Config	IP Address	Bonded Device	Bonded Device IP	Options
Local	Local	00:1B:13:02:DD:45	Online	Static IP	10.0.0.120	TX1 - EMD200DV-T	10.0.0.150	⋯

« ‹ 1 of **1** › »

FIGURE 9-6. PERIPHERALS>>SETTINGS TAB

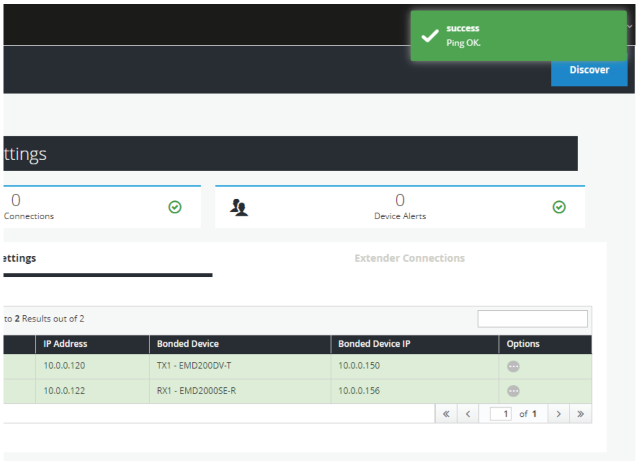
Additional functions and features can be found by clicking on the ellipsis "..." next to any device.



Bonded Device IP	Options
10.0.0.150	⋯

FIGURE 9-7. ADDITIONAL FUNCTIONS AND FEATURES

- Pinging devices



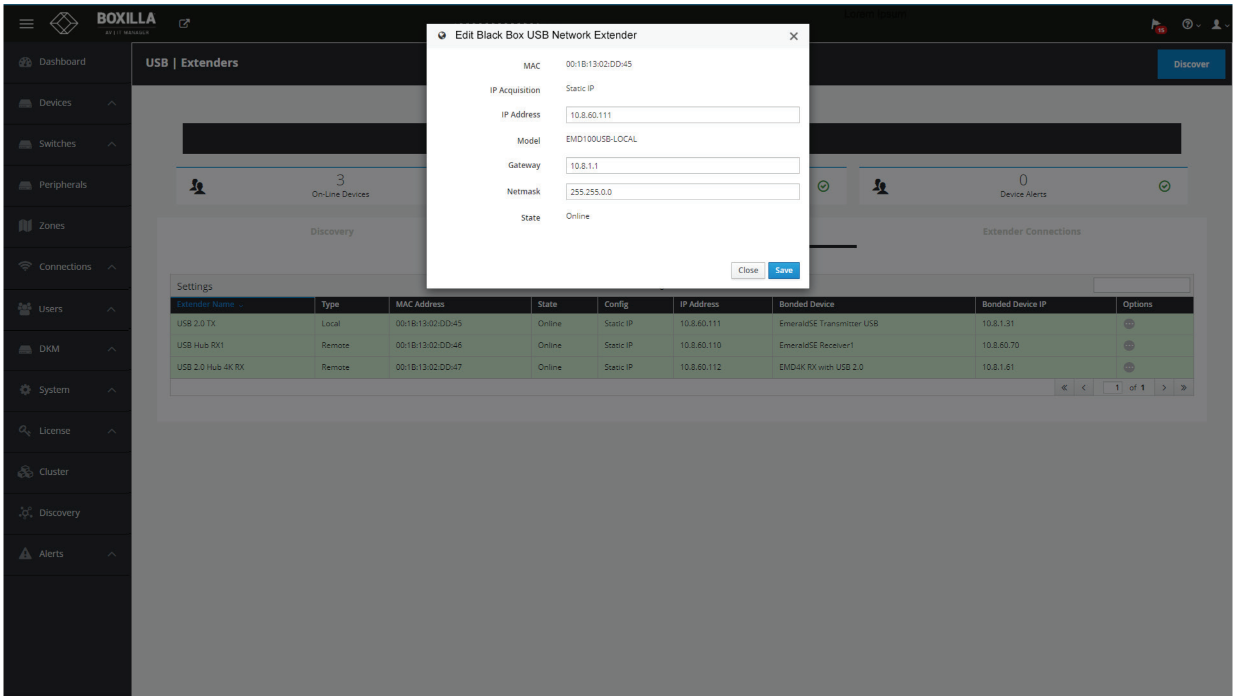
success
Ping OK.

to 2 Results out of 2

	IP Address	Bonded Device	Bonded Device IP	Options
	10.0.0.120	TX1 - EMD200DV-T	10.0.0.150	⋯
	10.0.0.122	RX1 - EMD2000SE-R	10.0.0.156	⋯

FIGURE 9-8. PINGING DEVICES TO CONFIRM AVAILABILITY

- Edit Network Settings



Edit Black Box USB Network Extender

MAC: 00:1B:13:02:DD:45

IP Acquisition: Static IP

IP Address: 10.8.60.111

Model: EMD100USB-LOCAL

Gateway: 10.8.1.1

Netmask: 255.255.0.0

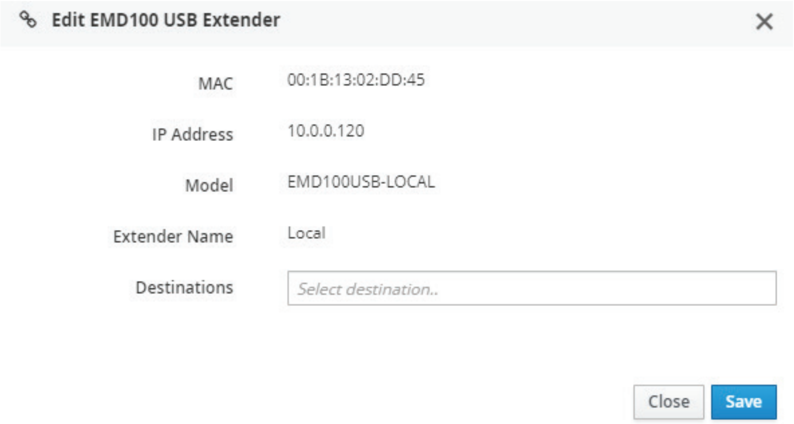
State: Online

Extender Name	Type	MAC Address	State	Config	IP Address	Bonded Device	Bonded Device IP	Options
USB 2.0 TX	Local	00:1B:13:02:DD:45	Online	Static IP	10.8.60.111	EmeraldSE Transmitter USB	10.8.1.31	⋯
USB Hub RX1	Remote	00:1B:13:02:DD:46	Online	Static IP	10.8.60.110	EmeraldSE Receiver1	10.8.60.70	⋯
USB 2.0 Hub 4K RX	Remote	00:1B:13:02:DD:47	Online	Static IP	10.8.60.112	EMD4K RX with USB 2.0	10.8.1.61	⋯

FIGURE 9-9. EDIT NETWORK SETTINGS SCREEN

- Toggle LED for identification

- Edit Bonding Settings



Edit EMD100 USB Extender

MAC 00:1B:13:02:DD:45

IP Address 10.0.0.120

Model EMD100USB-LOCAL

Extender Name Local

Destinations Select destination..

FIGURE 9-10. EDIT BONDING SETTINGS SCREEN

- Unbond the USB hub
- Change extender name
- Reset the unit

9.3 PERIPHERALS - EXTENDER CONNECTIONS TAB

Additionally, you can see the active connections under Peripherals>>Extender Connections.

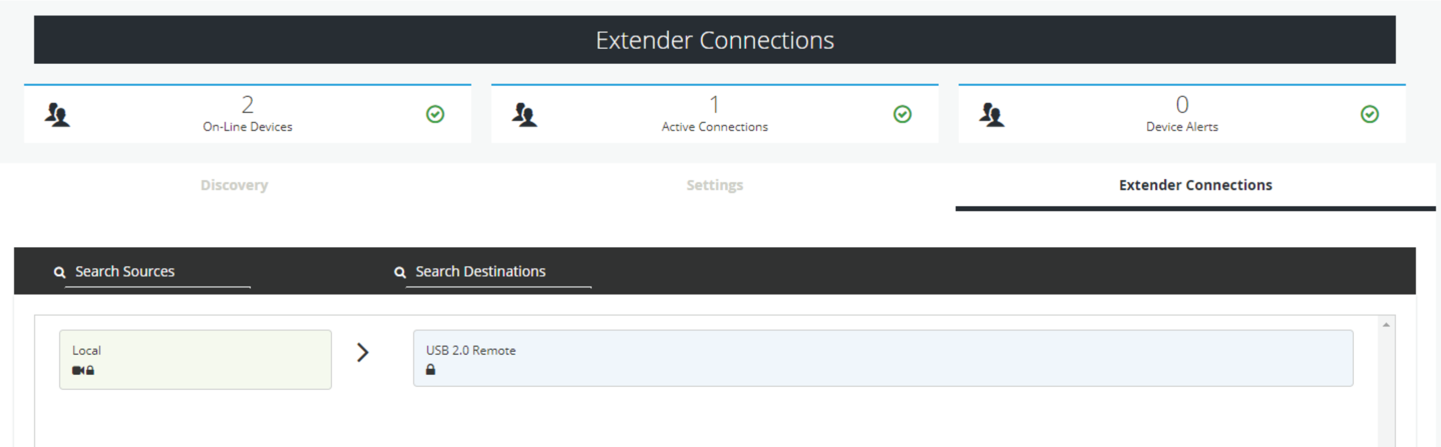


FIGURE 9-11. EXTENDER CONNECTIONS TAB

CHAPTER 10: ZONES

10.1 EMERALD ZONING FEATURE

Background:

Emerald users can have access to Emerald devices from multiple locations. These locations can be on different rooms, floors, buildings, or even cities. The concept is that users in different locations are required to use their login, but may have different security access depending on locations or simply different access requirements based on location.

Zoning in Emerald is used to associate each Physical Receiver and each connection (physical or virtual) with a zone; the zone is typically a location.

Feature Description/Use Case:

The System can set up each Receiver and each connection to be in a zone. The user will receive Targets on their OSD list that are dependent on the Location/zone they currently working in. For Example in Room A, which is classed as secure, the user can access relevant secure targets. When the same user moves out to his office desk, he will not be allowed to even see the secure targets on his OSD list even though he logged in with exactly the same user name and password.

You can find Zones in the left menu bar of the Boxilla® interface, between Peripherals and Connections.

CHAPTER 10: ZONES

When you click on Zones, the following screen appears.

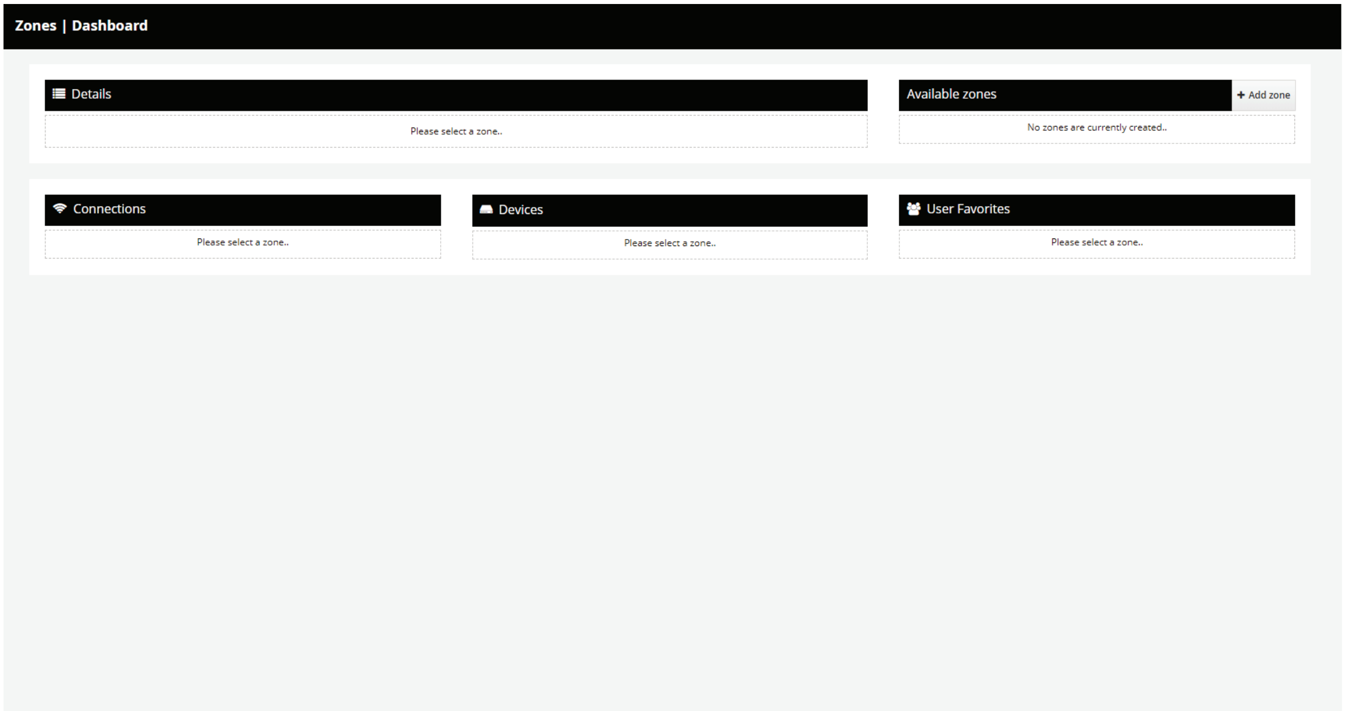
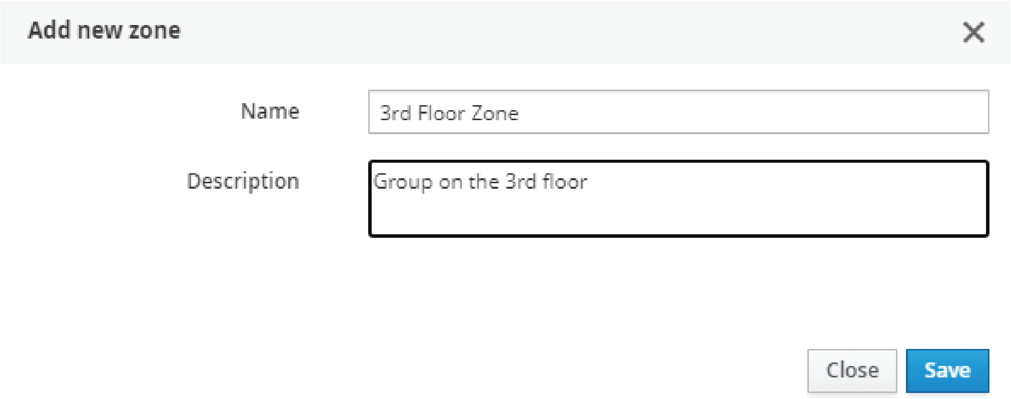


FIGURE 10-1. ZONES UNPOPULATED

To get started with setting up Zones, go to the top right hand corner of the page and click on “Add Zone.” Once you add a zone, give it a name and description.

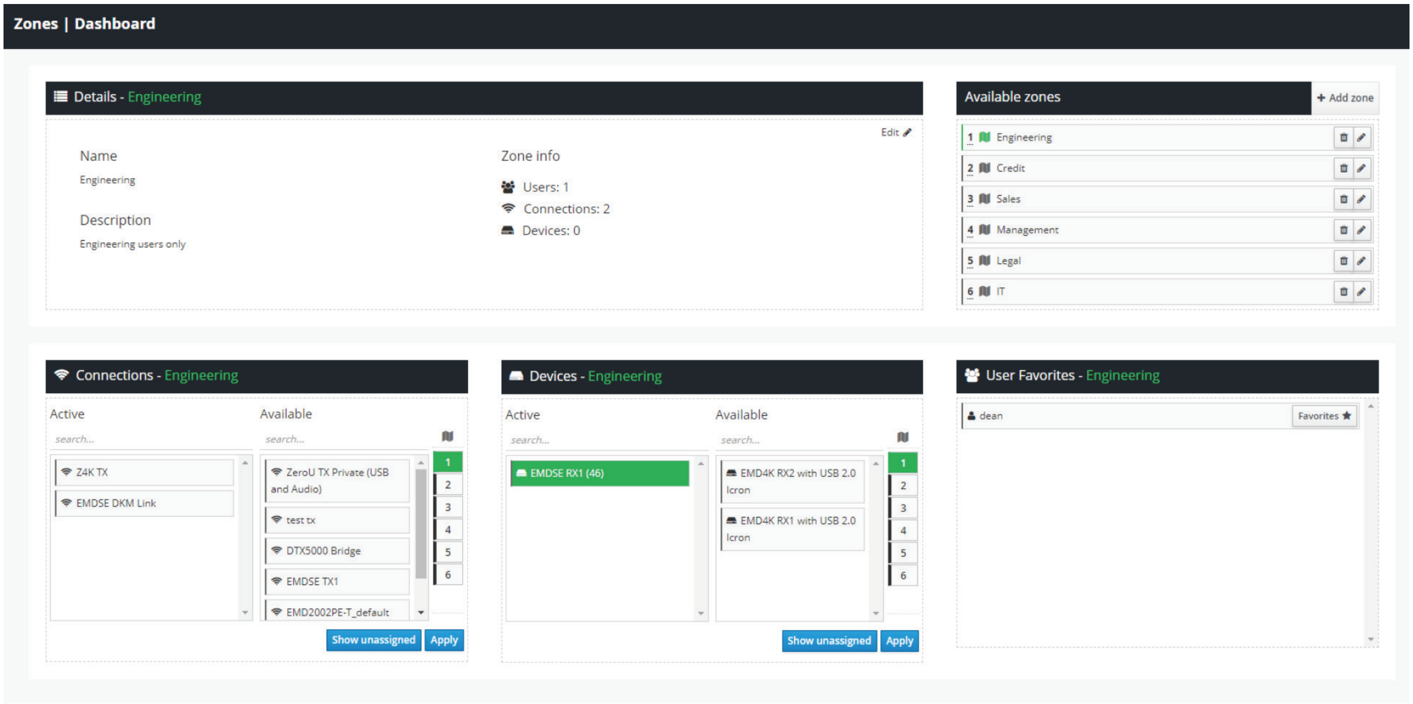


Name: 3rd Floor Zone

Description: Group on the 3rd floor

FIGURE 10-2. ADD NEW ZONE

When the zone is created, you can now click on it under "Available Zones" to begin configuring the zone details.



Zones | Dashboard

Details - Engineering

Name: Engineering

Description: Engineering users only

Zone info
- Users: 1
- Connections: 2
- Devices: 0

Available zones
1 Engineering
2 Credit
3 Sales
4 Management
5 Legal
6 IT

Connections - Engineering
- Active: Z4K TX; EMDSE DKM Link
- Available: ZeroU TX Private (USB and Audio); test tx; DTX5000 Bridge; EMDSE TX1; EMD2002PE-T_default

Devices - Engineering
- Active: EMDSE RX1 (46)
- Available: EMD4K RX2 with USB 2.0 Icron; EMD4K RX1 with USB 2.0 Icron

User Favorites - Engineering
- dean

FIGURE 10-3. ZONES DASHBOARD

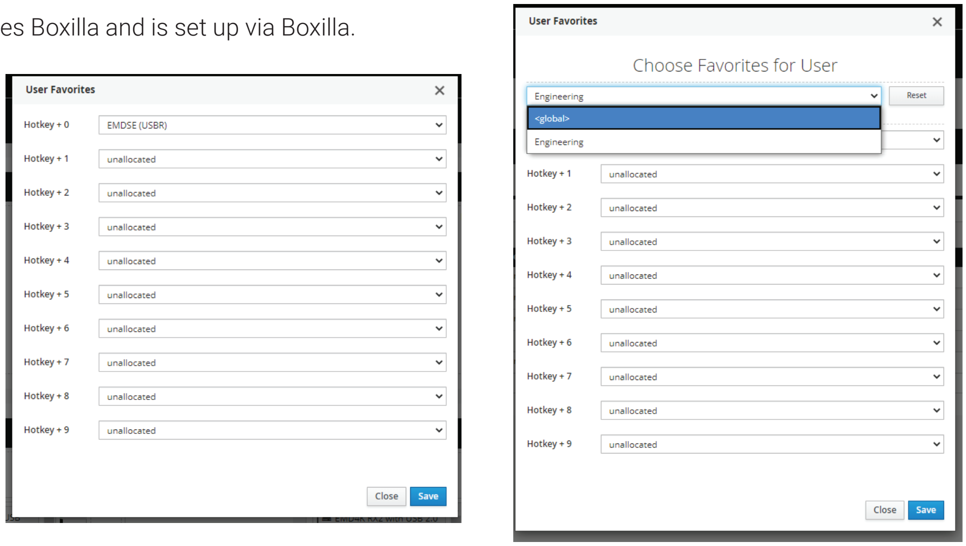
When the zone is selected, the administrator can place connections and devices within that zone. Once the device/connection is assigned to a zone, it cannot be used in any other zone. If you need to modify the connections/devices for a zone, you can easily do so by clicking on the assigned device and it will move it back to available. Once all changes are made, you can use the "Apply" button to save your changes. You can only delete a Zone if there are no Connections and Devices assigned to the Zone. When the "Show unassigned" button is selected, it shows the Connections OR Devices that are not assigned to any Zone.

When a zone is established, you can now assign new devices/connections to the zone. Boxilla® supports up to 10 zones maximum.

You can also link any user's favorites to the zone to help adding shortcut keys to specific systems for that zone.

Additional Information:

- The user can also have a different set of Favorites when they login from different zones.
- This feature requires Boxilla and is set up via Boxilla.



User Favorites

Hotkey + 0	EMDSE (USBR)
Hotkey + 1	unallocated
Hotkey + 2	unallocated
Hotkey + 3	unallocated
Hotkey + 4	unallocated
Hotkey + 5	unallocated
Hotkey + 6	unallocated
Hotkey + 7	unallocated
Hotkey + 8	unallocated
Hotkey + 9	unallocated

User Favorites

Choose Favorites for User

Engineering
<global>
Engineering

Hotkey + 1	unallocated
Hotkey + 2	unallocated
Hotkey + 3	unallocated
Hotkey + 4	unallocated
Hotkey + 5	unallocated
Hotkey + 6	unallocated
Hotkey + 7	unallocated
Hotkey + 8	unallocated
Hotkey + 9	unallocated

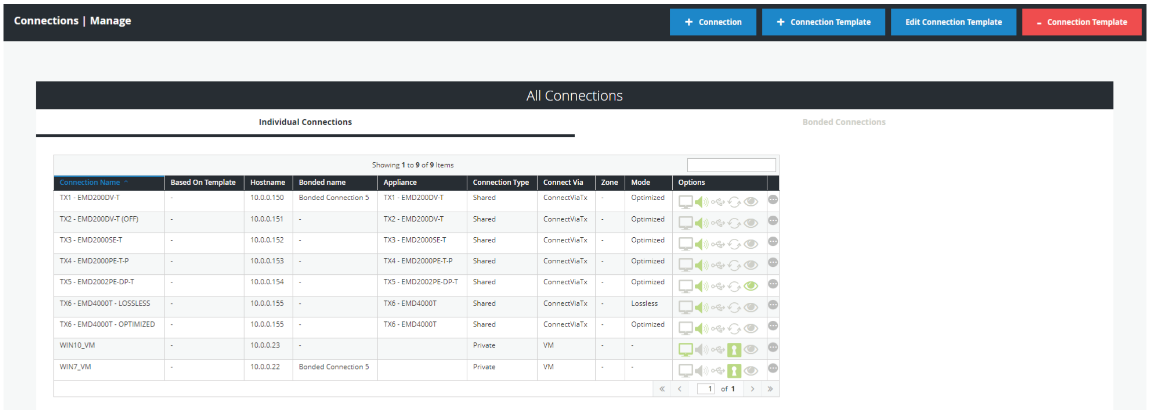
FIGURE 10-4. USER FAVORITES AND USER FAVORITES WITH ZONES

CHAPTER 11: CONNECTIONS

Connections define the properties for the flow of keyboard, mouse, video, audio and USB traffic between a receiver appliance and transmitter appliance, or a receiver appliance and a virtual machine. Connections are created and then allocated to Users to provide them access to Transmitters or Virtual Machines. A connection is a definition and can be allocated to multiple users. When a user logs into a receiver appliance, they are presented with their allocated connections on the Connections Tab of the OSD on that Receiver.

11.1 CONNECTIONS—MANAGE

The Connections — Manage page lists the currently defined connections and allows them to be edited, deleted or new connections to be added. The connections are listed shown in Figure 11-1.



Connection Name	Based On Template	Hostname	Bonded name	Appliance	Connection Type	Connect Via	Zone	Mode	Options
TX1 - EMD200DV-T	-	10.0.0.150	Bonded Connection 5	TX1 - EMD200DV-T	Shared	ConnectViaTx	-	Optimized	
TX2 - EMD200DV-T (OFF)	-	10.0.0.151	-	TX2 - EMD200DV-T	Shared	ConnectViaTx	-	Optimized	
TX3 - EMD2000SE-T	-	10.0.0.152	-	TX3 - EMD2000SE-T	Shared	ConnectViaTx	-	Optimized	
TX4 - EMD2000PE-T-P	-	10.0.0.153	-	TX4 - EMD2000PE-T-P	Shared	ConnectViaTx	-	Optimized	
TX5 - EMD2002PE-DP-T	-	10.0.0.154	-	TX5 - EMD2002PE-DP-T	Shared	ConnectViaTx	-	Optimized	
TX6 - EMD4000T - LOSSLESS	-	10.0.0.155	-	TX6 - EMD4000T	Shared	ConnectViaTx	-	Lossless	
TX6 - EMD4000T - OPTIMIZED	-	10.0.0.155	-	TX6 - EMD4000T	Shared	ConnectViaTx	-	Optimized	
WIN10_VM	-	10.0.0.23	-		Private	VM	-	-	
WIN7_VM	-	10.0.0.22	Bonded Connection 5		Private	VM	-	-	

FIGURE 11-1. CONNECTIONS MANAGE SCREEN

The table shows the connection name, whether the connection is linked to a connection template, connection type (private or shared), what/how the connection is made (via Tx, Direct to VM, via VM Pool or via Connection Broker or TX pair, what Zone the connection is in, and the connection options. The options for connections are the parameters that can be defined for the connection. The icons represent the parameters—when enabled the icon is Green and when disabled it is Grey. Hovering over the icon provides details of the parameter status. The icon definitions are:

Extend desktop: On a dual-video head Emerald, when set it enables the secondary video interface (by default it is disabled). This setting has no effect on a single-video head Emerald.

Audio: When set, this enables analog audio to be supplied to the remote audio connectors.

View only: When enabled, users can only view connections with no keyboard and mouse controls during the connection.

USB Redirection: When set, this enables non-keyboard and non-mice devices to be redirected for this connection.

Persistent Connection: When turned on, Persistent Connection will constantly try to connect to the Transmitter until successful. This is useful when using Emerald for digital signage or applications with no keyboard/mouse that need to stay connected to a defined source.

🔓 NLA: When set, this enables Network Level Authentication, requiring that the user be authenticated to the RD Session Host server before the session is created. This setting needs to match the NLA setting on the target VM for a successful connection.

Emerald has NLA set to "disabled" by default and doesn't have option to change. On VM, the NLA setting has to be set to "disabled". If the connection has NLA enabled, the VM must also have NLA enabled.

The administrator can edit the connections parameters or delete the connection using the ellipsis "•••" icon on the specific connection row. The parameters for a connection are defined in more detail in section 9.1.1.

When you left-click on a connection name, a popup box appears that tells you details about the connection and gives you the option to disconnect.

NLA Note: If connecting to a Windows 10VM and you encounter NLA issues, you can use the steps below to fix it.

1. Open RegEdit

2. Navigate to this Key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp

3. Change "SecurityLayer" to a zero

4. Reboot and done!

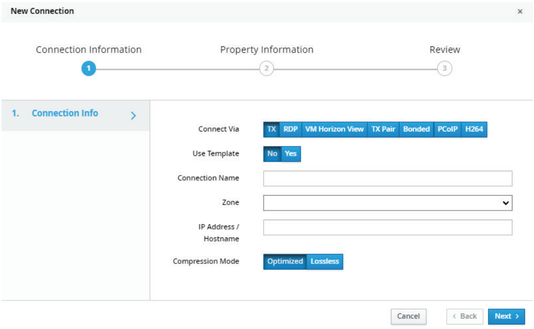
11.1.1 CONNECTIONS—ADD CONNECTION

To allow a receiver appliance to connect to a target transmitter appliance or Virtual Machine, an administrator must create a connection. This is done on the Connections — Manage page from the main menu as shown in Figure 11-1.

Clicking on the +Connection button launches a wizard that takes the Administrator step-by-step through the creation of a new connection.

On the first screen of the wizard the Administrator selects the type of connection. This can be one of four types (as set by Connect Via parameter):

- Tx — connect to an Emerald or ZeroU Transmitter;
- RDP VM — connect directly to a virtual machine using its IP address or hostname;
- VM Horizon View (EMD4000R Only) — connect to a VM Horizon server; The target of the connection must have the appropriate Horizon Agent installed;
- TX Pair — for paired connections (i.e. two paired single head transmitters connecting to any dual-head receiver).
- Bonded — A Bonded Connection is a group of 2 to 8 connections which have been added to form a "bonded connection." The bonded connection is treated just like any other connection, where users must be assigned access to this connection. Each connection in a group is assigned a number in order 1 to 8 and these will be matched with the receiver with the bonded receiver group. See Section 7.2, Devices — Groups.
- PCoIP — (DESKVUE only) — connect to a PCoIP target; There are two types of Windows and Linux PCoIP hosts (Graphics Agent and Standard Agent). The PCoIP Graphics Agent is installed on a GPU powered virtual machine whereas the Standard Agent is installed on a non GPU powered virtual machine. PCoIP Ultra is supported if the target is properly configured and is powered by the CPU/ GPU. Otherwise the connection will use the standard PCoIP quality. Before setting this up with Emerald, be sure that the PCoIP standard client can connect to the target to verify the configuration is setup properly.
- H.264 —(DESKVUE only) —add a H.264 streaming connection to the DESKVUE receiver.



Connect Via: [✓ TX] RDP VM Horizon View TX Pair Bonded PCoIP H264

Use Template: [✓ No] Yes

Connection Name:

Zone:

IP Address / Hostname:

Compression Mode: [✓ Optimized] Lossless

FIGURE 11-2. ADD CONNECTION—TX

The other parameters on this screen are:

- Use Template: option to use predefined connection template or a unique connection
- Connection Name: this is a unique name for the new connection. The name can be between 1 and 32 characters. The name can be composed of any Alphanumeric characters and special characters except for “ ”/ \ [ ] : ; | = , + * ? < > `’.
- Zone: allows the Zone setting to be changed. Zones enable the administrator to setup unique zones (or groups) of Connections, Physical Receivers, and Users so that a large system can be more easily managed.
- IP Address/Hostname: the IP address of the Emerald Transmitter or the Virtual Desktop in IPv4 format.
- For RDP, VM Horizon View, and PCoIP Connections, the password field now supports the * and + characters
- Compression Mode (only for TX connections):

Optimized: Use this option if a 2K receiver is connecting to this target. The connection could be for a 2K or 4K target. (i.e. 2K RX connecting to 2K TX or 2K RX connecting to a 4K TX)

Lossless: Use this option if a 4K receiver is connecting to a 4K transmitter.

To allow users to connect from a 2K Receiver to a 4K Transmitter, a dual-channel can be used meaning that one connection would be set for Lossless (for any 4K receivers) and a secondary connection set for Optimized (for any 2K receivers), and both connections can be active at the same time. If the 4K Transmitter is using a resolution above 1920x1080, the 2K receiver and RemoteApp will scale it down to fit the window, and the image may appear to be skewed. Go to Connections and create a new connection (or Edit an existing connection). Enter all of the connection details (or confirm they are correct) and a new option can be selected for Compression Mode. Use this information to set the right compression mode:

4K RX to 4K TX: Compression Mode = Lossless

4K RX to 2K TX: Compression Mode = Optimized

2K RX to 2K TX: Compression Mode = Optimized

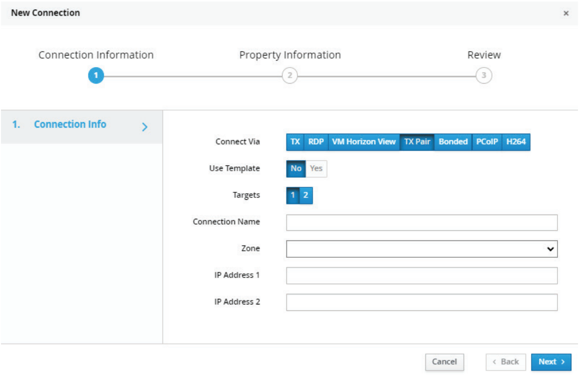
2K RX to 4K TX: Compression Mode = Optimized (Firmware 6.3.10 or later)

TX Pair allows any dual-head receiver to connect to two separate single-head transmitters that channelize the video from the transmit side into one of the video heads on the receiver. This connection type can be used for a dual-head receiver that needs to connect to two single-head computers, giving the user on the dual-head receiver access to each system that supports video, keyboard, and mouse. The user can switch between both single-head computers by moving the mouse between the screens on the dual-head receiver. When using this connection method with two separate computers, each transmitter must be configured for an Absolute HID Configuration in order for the mouse to track properly.

TX Pair also can work with a single computer but use two separate single-head transmitters. This would typically be used with a single computer with dual-head video that may use video dithering. Single-head Emerald transmitters have dithering controls whereas the dual-head does not, so utilizing this connection type in that application would not always require the use of Absolute HID configuration.

The TX Pair offers the option to place the video side by side, or on top of each other which will determine how the users switches between them (left <> right) or (up <> down).

If the TX Pair is set, you can set how many targets will be used in the connection.



Connect Via: TX | RDP | VM Horizon View | TX Pair | Bonded | PCoIP | H264

Use Template: No | Yes

Targets: 1 | 2

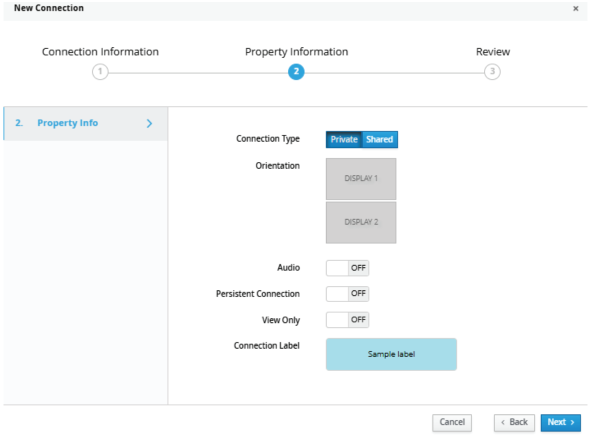
Connection Name

Zone

IP Address 1

IP Address 2

FIGURE 11-3. ADD CONNECTION—TX PAIR



Connection Type: Private | Shared

Orientation

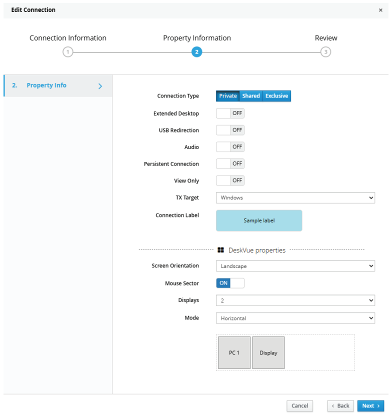
Audio: OFF

Persistent Connection: OFF

View Only: OFF

Connection Label: Sample label

FIGURE 11-4. TX PAIR SETTINGS SCREEN



Connection Type: Private | Shared | Exclusive

Extended Desktop: OFF

USB Redirection: OFF

Audio: OFF

Persistent Connection: OFF

View Only: OFF

TX Target: Windows

Connection Label: Sample label

DeskVue properties

Screen Orientation: Landscape

Mouse Sector: ON

Displays: 2

Mode: Horizontal

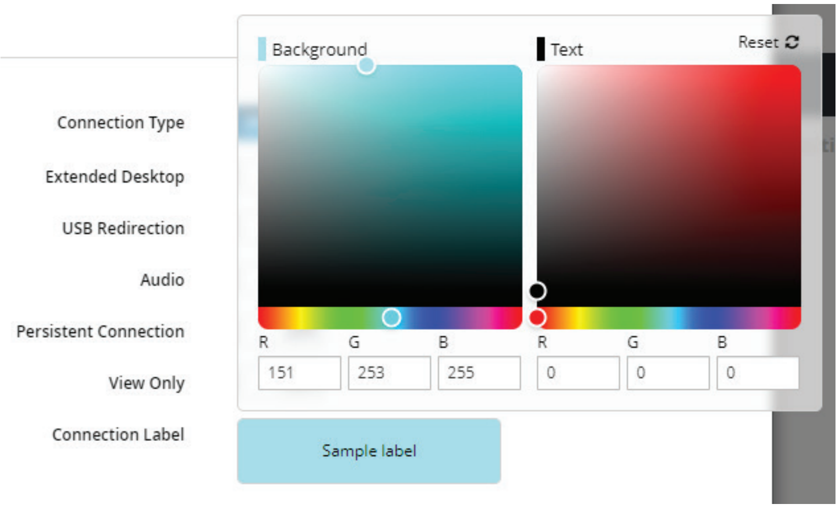
FIGURE 11-5. ADD CONNECTIONS—PROPERTIES

The second page of the New Connection Wizard outlines additional connection parameters that are related to the type of connection. These connections parameters are as follows:

Connection Type: This defines the connection as being private to this user when the connection is made or is open to be shared with other users. A shared connection allows the keyboard, video and mouse to be shared to all users that join the connection. Audio and USB redirection disabled on shared connections.

- Extended Desktop: On a dual-video head Emerald, this enables the second video head to operate if connected to a source that supports dual-head operation (e.g. Dual-head Emerald Transmitter). This setting has no effect on a single-video head Emerald. This extended desktop parameter also applies to RDP connections if the Group Policies do not restrict a second video head.
- USB Redirection (Private Connections only): When set, this enables non-keyboard and non-mice devices to be redirected for this connection. USB Redirection is not supported on the EMD200DV-T or the EMD200DP-T. The ZeroU Transmitters do not support this parameter and only support Keyboard and Mouse.
- Audio: When set, this enables analog audio to be supplied to the remote audio connectors.
- Persistent Connection: When turned on, Persistent Connection will constantly try to connect to the Receiver until successful. This is useful when using Emerald or DESKVUE for digital signage or an application with no keyboard/mouse that needs to stay connected to a defined source.
- View Only mode: The View Only parameter for a connection allows user to monitor what is been transmitted from a source without being able to interact with the source. This feature allows a user or administrator to monitor the actions on the network without accidentally interacting with other users. View only connection is available in both private and shared mode connections with or without analog audio.
- TX Target: Used to specify what OS the target machine is running. This setting enables improved mouse movement within DESKVUE workspaces for Windows machines that have extended desktops across multiple tiles. Setting to OSX or Linux ensures the mouse buttons operate as intended within those environments also.

Connection Label: The connection label that is displayed when establishing a connection can be modified to allow customized background and text colors.



Background: R 151, G 253, B 255

Text: R 0, G 0, B 0

Sample label

FIGURE 11-6. CONNECTION LABEL

When Connect Via is set to VM (i.e. connect directly to a VM), there is an extra parameter to define:

- NLA (RDP Connections only): When set, this enables Network Level Authentication, requiring that the user be authenticated to the RD Session Host server before the session is created. This setting needs to match the NLA setting on the target VM for a successful connection. If you are having issues connecting to a Windows 10 VM, read section 11.1 about NLA for Windows 10.

When Connection Type is Private, the following parameters are shown in the New Connection screen: Connection Type (Private), Connection Name, Host IP address, Extended Desktop, USB Redirection, Audio, and Persistent Connection. When using the shared connection, the USB Redirection will not be available to support transparent USB devices that require USB Redirection.

DESKVUE Settings:

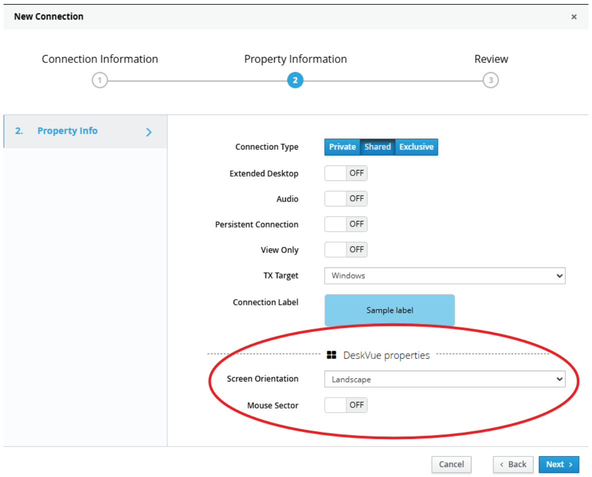
Screen Orientation: If making a connection for the DESKVUE, the connection parameter for screen orientation can be set for Portrait or Landscape mode. This setting simply uses either the typical Landscape view on the output or will turn it 90 degrees in Portrait mode.

Mouse Sectors:

This section shows how to use the Mouse Sector configuration interface within connections to allow DeskVue to control target machines that have an extended desktop of 2, 3 or 4 displays. Mouse sectors are not required for target machines which will have only a single monitor.

Connection DESKVUE Properties:

When creating a new connection for any Emerald transmitter type you will notice on the second page of the process that there is a DESKVUE properties section for applying attributes relevant to when the connection is launched from a DESKVUE receiver.



Connection Type: Private | Shared | Exclusive

Extended Desktop: OFF

Audio: OFF

Persistent Connection: OFF

View Only: OFF

TX Target: Windows

Connection Label: Sample label

DeskVue properties

Screen Orientation: Landscape

Mouse Sector: OFF

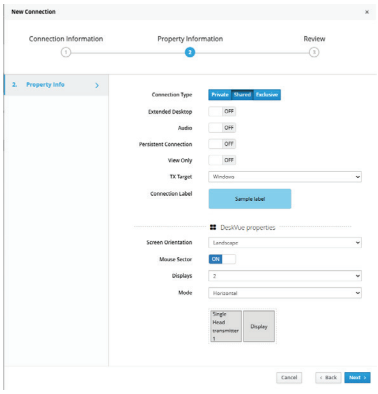
FIGURE 11-7. DESKVUE PROPERTIES

Flipping the switch for the Mouse Sector property to the "ON" position will reveal extra configuration options for this particular connection, allowing you select the total number of displays the machine believes it has in its extended desktop, either 2, 3 or 4. If those outputs are orientated in a portrait or landscape fashion, then the basic arrangement of those screens in regards to how the target OS believes the screens have been arranged according to the display settings on that target machines OS.

Horizontal: All screens are in a row.

Vertical: All screens are in a column.

Matrix: Screens are perhaps arranged in a "quad" or 2x2 arrangement.



Connection Type: Private | Shared | Exclusive

Extended Desktop: OFF

Audio: OFF

Persistent Connection: OFF

View Only: OFF

TX Target: Windows

Connection Label: Sample label

Screen Orientation: Landscape

Mouse Sector: ON

Displays: 2

Mode: Horizontal

Single Head transmitter 1 | Display

FIGURE 11-8. MOUSE SECTOR SETTINGS

The next thing you see is a visual representation of the target machines screens via the grey boxes at the bottom of that configuration page. Depending on if you selected 2, 3 or 4 Displays there will be as many grey boxes denoting the display arrangement and only one of the boxes will have the name of the connection that you are configuring.

Drag-and-drop the grey box with the name of the connection, placing the the connection name into the correct position that reflects what video output of the target PC this transmitter/connection is connected to.

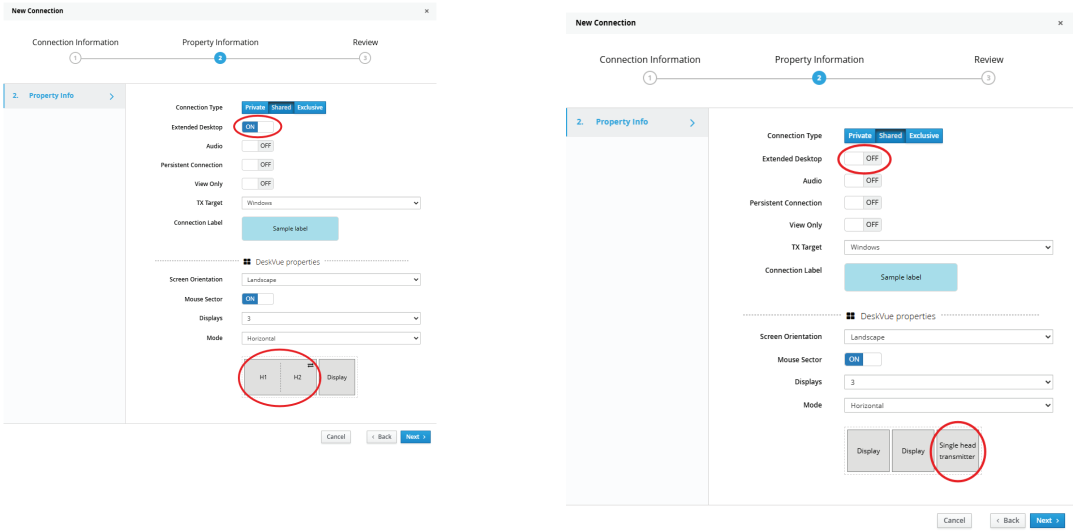
Best practice is to connect one transmitter at a time to a multihead machine, setting the mouse sector for each transmitter/connection as you add them so you can easily be certain to have the correct sector.

If you are using single head transmitters, for example for a dual head machine this will mean of course that you will have two transmitters, two connection names and each connection will need to be configured to tell it what position it relates to in the screen arrangement.

Dual-Head Transmitters:

In Boxilla 5.1.5 Mouse Sectors to support dual-head Emerald transmitters has also been added. When creating a connection with a dual-head transmitter and enabling the “Extended Desktop” option, you will notice that when configuring the positioning for the dual-head transmitter connection, it will incorporate both heads of that one dual-head transmitter in regards to the box positioning within the mouse sector mapping.

These dual-head transmitters can also be mixed with single-head transmitters to create triple monitor setups, for example, showing the two separate connections to configure the triple-head setup by combining a dual transmitter and a single-head transmitter.



New Connection

Connection Information — Property Information — Review

2. Property Info

Connection Type: Private | Shared | Exclusive
Extended Desktop: ON
Audio: OFF
Persistent Connection: OFF
View Only: OFF
TX Target: Windows
Connection Label: Sample label

DeskVue properties

Screen Orientation: Landscape
Mouse Sector: ON
Displays: 3
Mode: Horizontal

New Connection

Connection Information — Property Information — Review

2. Property Info

Connection Type: Private | Shared | Exclusive
Extended Desktop: OFF
Audio: OFF
Persistent Connection: OFF
View Only: OFF
TX Target: Windows
Connection Label: Sample label

DeskVue properties

Screen Orientation: Landscape
Mouse Sector: ON
Displays: 3
Mode: Horizontal

FIGURE 11-9. TRIPLE-HEAD SETUP

Absolute Mouse and Extended Desktop:

When using Emerald transmitters with multi-head machines additional mouse drivers can be required to reach the full extent of the desktop with the mouse cursor depending on the OS like Windows for example and in some cases other OSes may not support absolute coodrinate mouse drivers for extended desktop and will only allow mouse movement on the primary monitor.

There may be alternative configuration solutions to this depending on the OS environment. Contact your local support for guidance if needed.

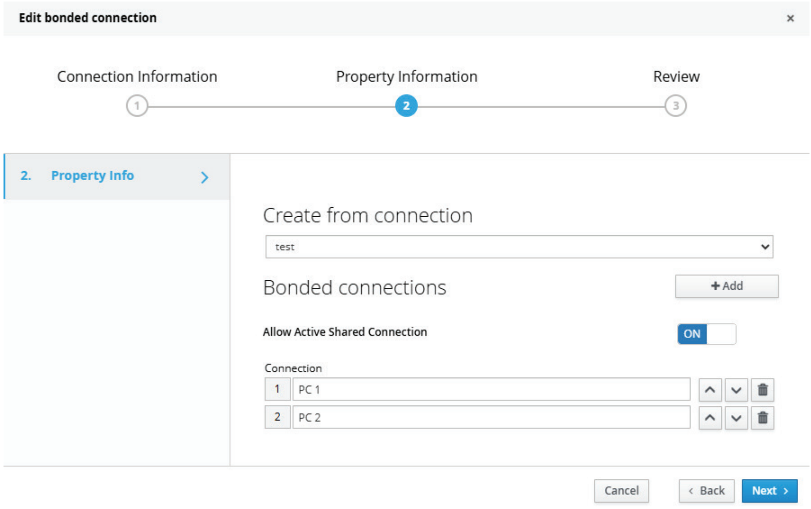
11.1.2 CONNECTIONS—BONDED CONNECTIONS

The purpose of the bonding feature is to switch multiple receivers to multiple connections quickly and simply from one user station with one button click. A typical example is where a user has a dual-head 4K system; the user will have two 4K monitors and 4K receivers on their desk but only one keyboard and mouse. The user will select the “bonded connection” from their OSD and both receivers will switch to their pre-configured 4K transmitters. Typically this will be set up in extended desktop and the user can move mouse and keyboard activity between both screens. We described 2 head setup above but the same applies for up to 8 connections.

Setup will be done via Boxilla® only. Create a bonded group of Receivers (see Section 7.2)– Can be up to 8 receivers in a bonded group numbered 1 to 8. Create a “bonded connection” – Again up to 8 connections within the bonded connection.

NOTE: All connections within a bonded connection group and the bonded connection group itself must be in the same zone.

If Bonded Connection is set, you will see the following Connection Information.



Edit bonded connection ×

Create from connection: test

Bonded connections

Allow Active Shared Connection: ON

Connection

1 PC 1

2 PC 2

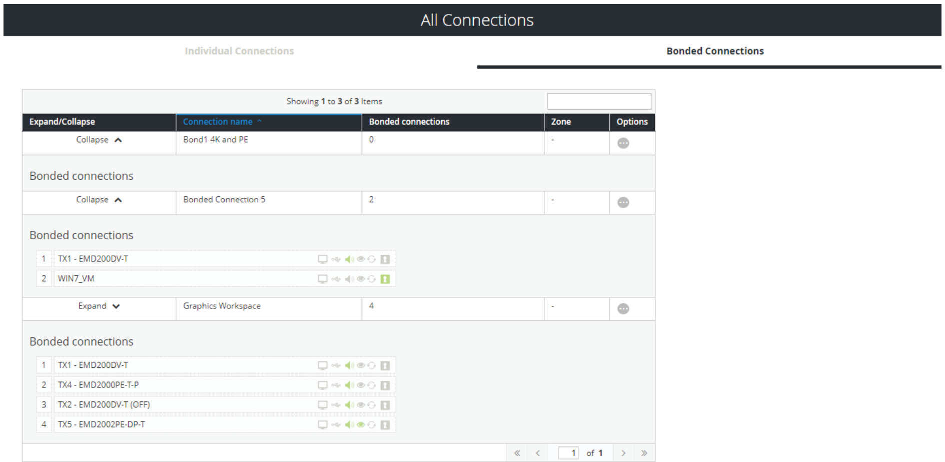
FIGURE 11-10. ADD YOUR CONNECTIONS

Connections can be added to a Bonded Connection in one of two ways:

1. Select connections from an existing Bonded Connection using the "Create from connection."

2. Allow active shared connection: This allows a bonded connection to launch even if shared connections within that bonded connection are already in use. If this is not enabled, the bonded connection will not launch if one of the shared connections is already in use.

The list of available connections is determined by the selected Zone option from Step 1. If no Zone is selected, the UI will only display connections that are not assigned to any Zone.



All Connections

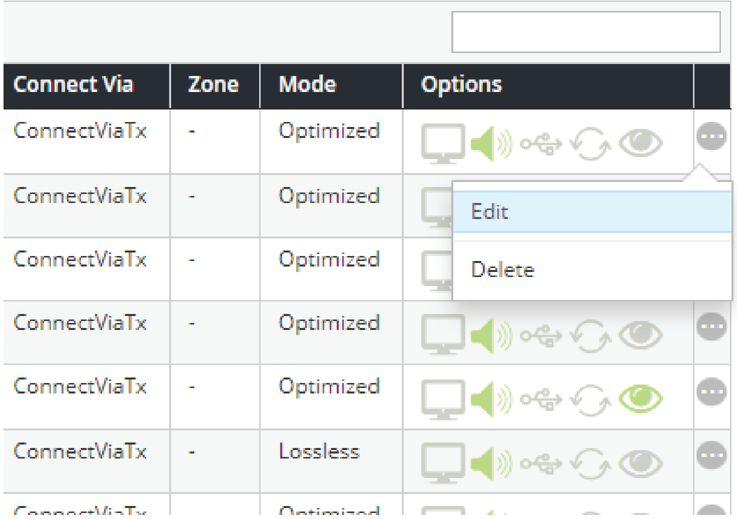
Showing 1 to 3 of 3 Items

Expand/Collapse	Connection name ^	Bonded connections	Zone	Options
Collapse ^	Bond1 4K and PE	0	-	⋯
Bonded connections				
Collapse ^	Bonded Connection 5	2	-	⋯
Bonded connections 1 TX1 - EMD200DV-T 2 WIN7_VM				
Expand ⌄	Graphics Workspace	4	-	⋯
Bonded connections 1 TX1 - EMD200DV-T 2 TX4 - EMD2000PE-T-P 3 TX2 - EMD200DV-T (OFF) 4 TX5 - EMD2002PE-DP-T				

FIGURE 11-11. ADDED BONDED CONNECTION SUCCESSFUL

11.1.3 CONNECTIONS—EDIT CONNECTIONS

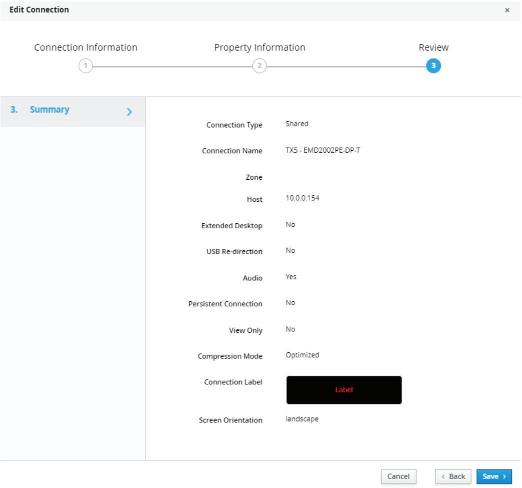
To edit connections, click on the Edit Connections button.



Connect Via	Zone	Mode	Options
ConnectViaTx	-	Optimized	
ConnectViaTx	-	Optimized	
ConnectViaTx	-	Optimized	
ConnectViaTx	-	Optimized	
ConnectViaTx	-	Optimized	
ConnectViaTx	-	Lossless	
ConnectViaTx		Optimized	

FIGURE 11-12. EDIT CONNECTIONS

After configuring or editing any connection, you will be able to review the final connection parameters to make sure it is properly configured.



Edit Connection

Connection Information — Property Information — Review

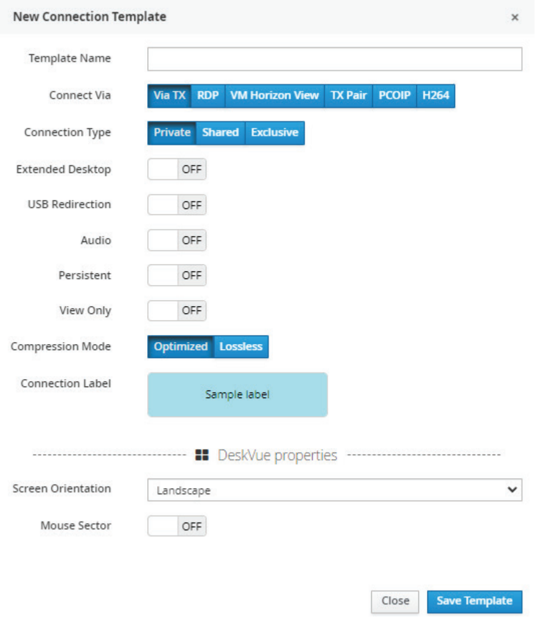
3. Summary

Connection Type: Shared
Connection Name: TX5 - EMD2002PE-DP-T
Zone:
Host: 10.0.0.154
Extended Desktop: No
USB Re-direction: No
Audio: Yes
Persistent Connection: No
View Only: No
Compression Mode: Optimized
Connection Label: Label
Screen Orientation: landscape

FIGURE 11-13. CONNECTION REVIEW

11.1.4 CONNECTIONS—ADD CONNECTION TEMPLATE

Connection Templates are used to aid in the creation of connections. Templates define a set of properties as shown in Figure 11-14. The template can be used when creating a connection to ensure that the same properties are attached to a group of the connection. Clicking on +Connection Template launches the screen to set these properties.



New Connection Template ×

Template Name:

Connect Via: Via TX | RDP | VM Horizon View | TX Pair | PCOIP | H264

Connection Type: Private | Shared | Exclusive

Extended Desktop: OFF

USB Redirection: OFF

Audio: OFF

Persistent: OFF

View Only: OFF

Compression Mode: Optimized | Lossless

Connection Label: Sample label

DeskVue properties

Screen Orientation: Landscape

Mouse Sector: OFF

FIGURE 11-14. ADD CONNECTION TEMPLATE

11.1.5 CONNECTIONS—DELETE CONNECTION TEMPLATE

To delete a connection template, click -Connection Template and this launches a screen that shows a list of connection templates. Select the template(s) to be deleted and click on delete.

Boxilla® will only display the list of connection templates that are not currently assigned to connections. If you wish to delete a template that is associated with a connection, you will first need to remove the template from the connection.

11.2 CONNECTIONS—GROUPS

Boxilla supports the creation of a connection group to make it easier to allocate a common set of resources to user.
If a connection group gets changed, it will be reflected on all users allocated to this Connection Group.

Connections option can be found on left side pane of the Boxilla user interface.

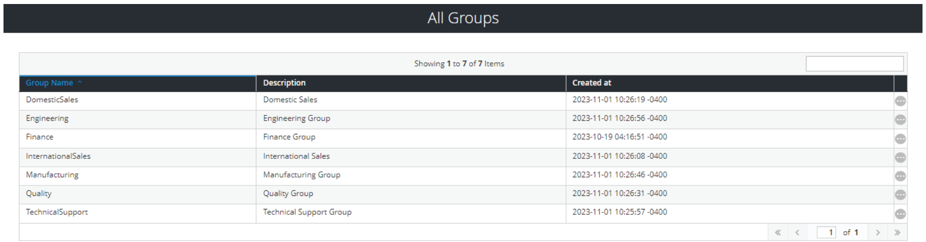
There are two new Connection Groups for the Active Directory feature updates:

1) OU Not Found.

2) OU Undefined.

These 2 Connection Groups are created by default on upgrade to Boxilla 3.6.0.

NOTE: These groups can be removed in the future as they do not add any value. In older versions of Boxilla, if these groups are removed, they will reappear after a reboot of the Boxilla manager.



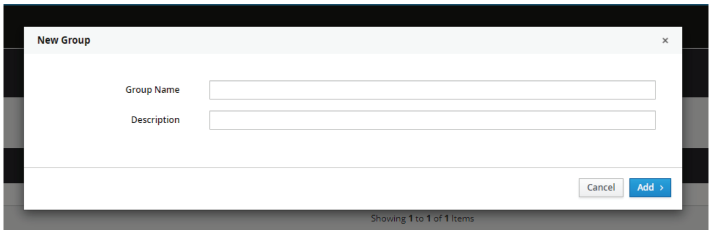
All Groups

Showing 1 to 7 of 7 Items

Group Name ^	Description	Created at
DomesticSales	Domestic Sales	2023-11-01 10:26:19 -0400
Engineering	Engineering Group	2023-11-01 10:26:56 -0400
Finance	Finance Group	2023-10-19 04:16:51 -0400
InternationalSales	International Sales	2023-11-01 10:26:08 -0400
Manufacturing	Manufacturing Group	2023-11-01 10:26:46 -0400
Quality	Quality Group	2023-11-01 10:26:31 -0400
TechnicalSupport	Technical Support Group	2023-11-01 10:25:57 -0400

FIGURE 11-15. CONNECTIONS OPTION

To add a connection group, click the +Group button in the top right hand corner of the screen:



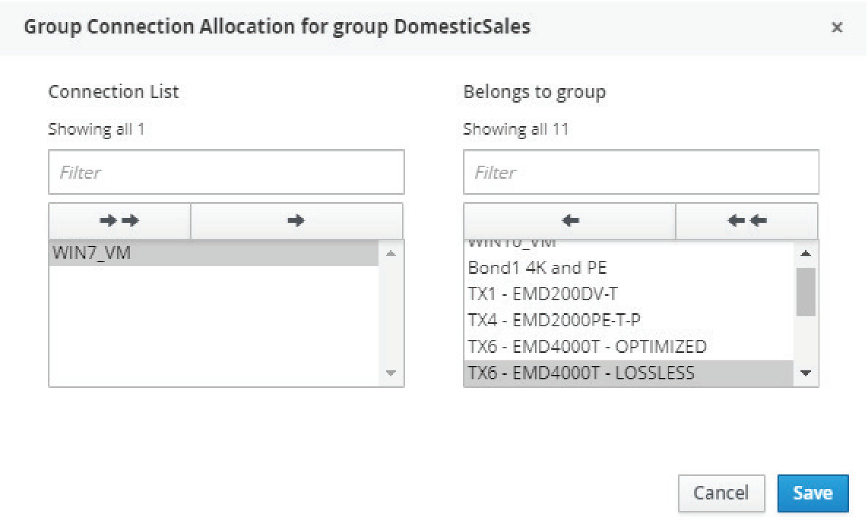
New Group

Group Name

Description

FIGURE 11-16. ADD CONNECTION GROUP SCREEN

You can manage the Connection Group by adding or removing connections to or from the connections group. To configure the connection group, click the ellipsis "..." next to the Connection group and select "Manage Connections."



Group Connection Allocation for group DomesticSales

Connection List

Showing all 1

WIN7_VM

Belongs to group

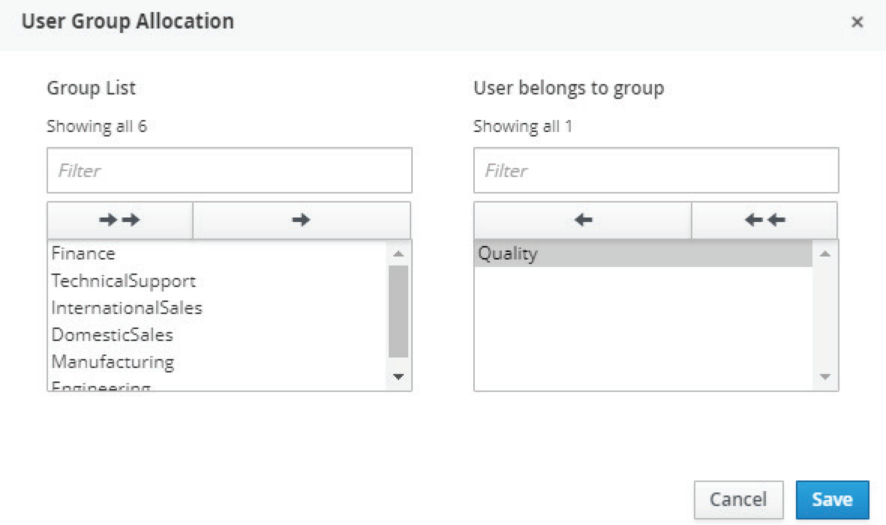
Showing all 11

WIN10_VM
Bond1 4K and PE
TX1 - EMD200DV-T
TX4 - EMD2000PE-T-P
TX6 - EMD4000T - OPTIMIZED
TX6 - EMD4000T - LOSSLESS

FIGURE 11-17. MANAGE CONNECTIONS SCREEN

CHAPTER 11: CONNECTIONS

You can add / manage groups from individual Users under Users -> Manage. Once a user logs in at the appliance GUI, all the assigned connections (both individual and group connections) with be visible to the user. To assign a user to a Connection Group, click on the ellipsis "..." icon next to the user account and select "Manage Group" under the Users -> Manage page.



User Group Allocation ×

Group List

Showing all 6

Filter

Finance
TechnicalSupport
InternationalSales
DomesticSales
Manufacturing
Engineering

User belongs to group

Showing all 1

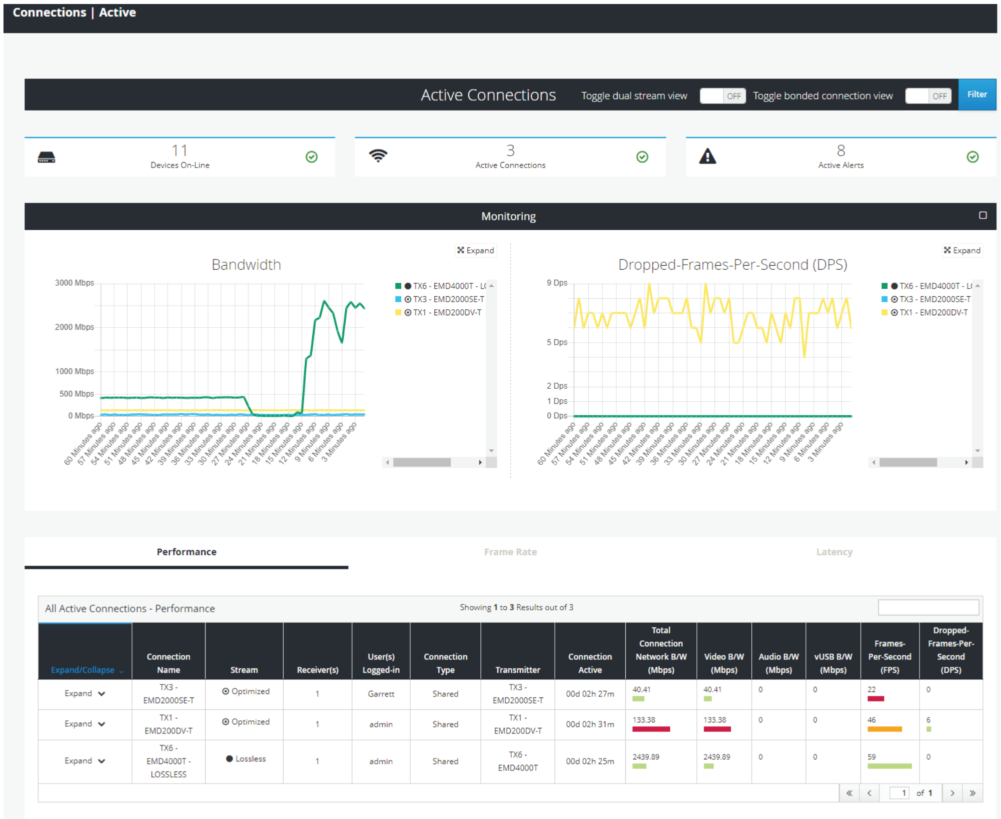
Filter

Quality

Cancel | Save

FIGURE 11-18. MANAGE CONNECTION GROUPS FOR A USER ACCOUNT

Active connections will be listed under Connections -> Active. The toggle bonded connection view option can be enabled to view an individual connection within a bonded connection.



Connections | Active

Active Connections | Toggle dual stream view: OFF | Toggle bonded connection view: OFF | Filter

11 Devices On-Line | 3 Active Connections | 8 Active Alerts

Monitoring

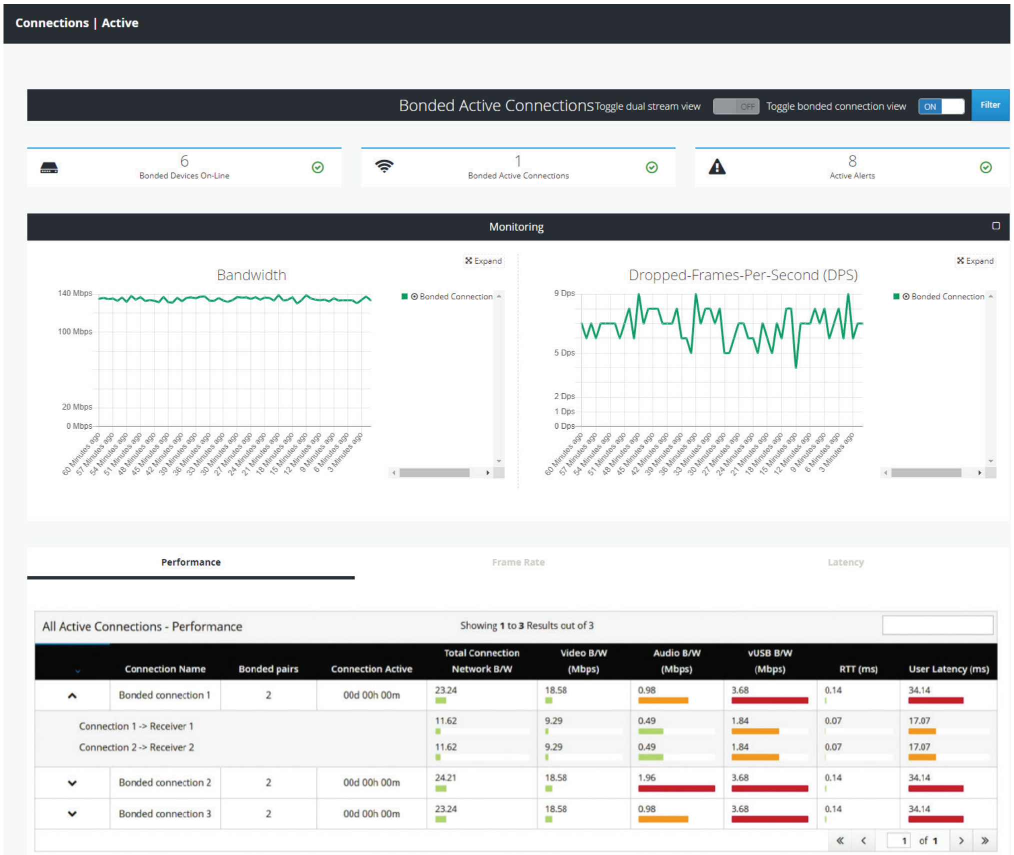
All Active Connections - Performance

Showing 1 to 3 Results out of 3

Expand/Collapse	Connection Name	Stream	Receiver(s)	User(s) Logged-in	Connection Type	Transmitter	Connection Active	Total Connection Network B/W (Mbps)	Video B/W (Mbps)	Audio B/W (Mbps)	vUSB B/W (Mbps)	Frames-Per-Second (FPS)	Dropped-Frames-Per-Second (DPS)
Expand	TX3 - EMD2000SE-T	⦿ Optimized	1	Garrett	Shared	TX3 - EMD2000SE-T	00d 02h 27m	40.41	40.41	0	0	22	0
Expand	TX1 - EMD200DV-T	⦿ Optimized	1	admin	Shared	TX1 - EMD200DV-T	00d 02h 31m	133.38	133.38	0	0	46	6
Expand	TX6 - EMD4000T - LOSSLESS	● Lossless	1	admin	Shared	TX6 - EMD4000T	00d 02h 25m	2439.89	2439.89	0	0	59	0

« ‹ 1 of 1 › »

FIGURE 11-19. ACTIVE CONNECTIONS SCREEN



All Active Connections - Performance

Showing **1** to **3** Results out of 3

	Connection Name	Bonded pairs	Connection Active	Total Connection Network B/W	Video B/W (Mbps)	Audio B/W (Mbps)	vUSB B/W (Mbps)	RTT (ms)	User Latency (ms)
^	Bonded connection 1	2	00d 00h 00m	23.24	18.58	0.98	3.68	0.14	34.14
Connection 1 -> Receiver 1				11.62	9.29	0.49	1.84	0.07	17.07
Connection 2 -> Receiver 2				11.62	9.29	0.49	1.84	0.07	17.07
v	Bonded connection 2	2	00d 00h 00m	24.21	18.58	1.96	3.68	0.14	34.14
v	Bonded connection 3	2	00d 00h 00m	23.24	18.58	0.98	3.68	0.14	34.14

« ‹ 1 of 1 › »

FIGURE 11-20. ACTIVE BONDED CONNECTIONS SCREEN

To delete (dissolve) a Connection Group, click on the ellipsis "..." next to the Connection Group and then select "Dissolve."

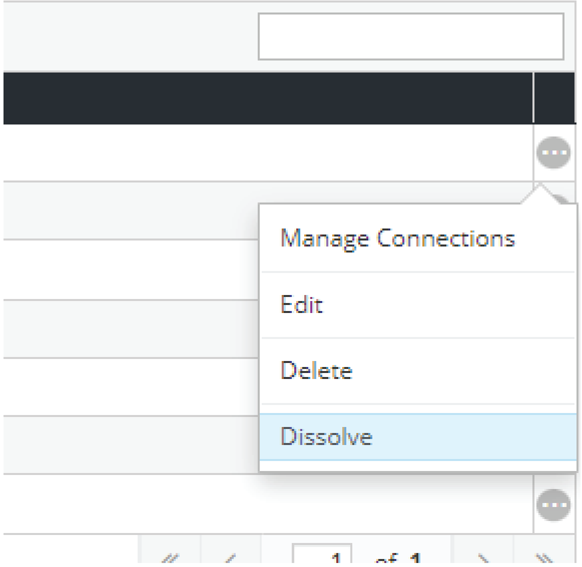


FIGURE 11-21. DISSOLVE CONNECTION GROUP SCREEN

By dissolving a group, the group no longer appears under Connections-Groups but the active connections are retained with the users logged in.

Unlike Delete groups, Dissolve Groups doesn’t leave any impact on connections.

After dissolving a Connection Group, all Connections from the Connection Group are moved to the list of Managed Connections for each User that was assigned to the Connection Group.

Delete Connection Group: Delete the Connection Group everywhere it is used.

The maximum number of connection groups is 100 and once it is reached, the add group button gets disabled.

NOTE: Boxilla® restricts the total number of User Connections across the system to 22500 unique User Connections. Boxilla supports:

- 150 users, each supporting a maximum of 150 unique connections
- 150 users, each supporting a maximum of 10 Connection Groups each group supporting a maximum of 15 unique connections
- 200 users, each supporting a maximum of 112 unique connections
- 200 users, each supporting a maximum of 10 Connection Groups each group supporting a maximum of 11 unique connections
- 250 users, each supporting a maximum of 90 unique connections
- 250 users each supporting a maximum of 10 Connection Groups each group supporting a maximum of 9 unique connections

11.3 CONNECTIONS—ACTIVE

The Connections—Active page lists the currently active connections—a live connection between a Receiver and a Transmitter. There are three tabs on this page: Performance, Frame-Rate and Configuration. These pages provide information on all active connections for the past 60 minutes: the name of the connection, the Receiver in the connection, the user who is logged into the Receiver, the type of connection (e.g. private or shared), the Transmitter in the connection and then statistics on the connection. The statistics include:

- On the Performance tab:

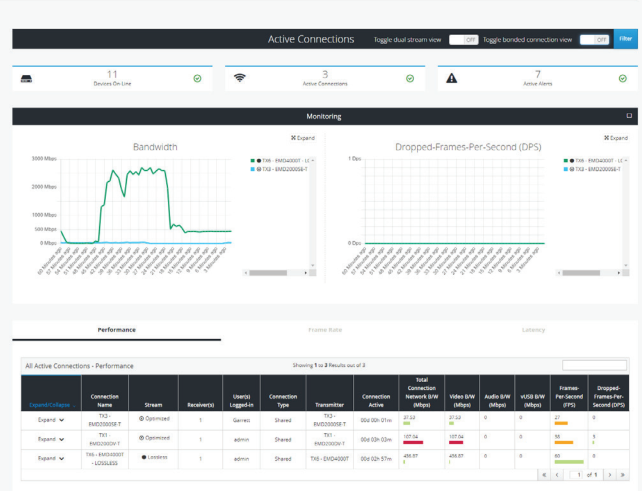
- Connection Active: the total time the connection has been established
- Connection Bandwidth: network traffic generated on the connection during the last polling interval
- Video/Audio/vUSB Bandwidth: a breakdown of connection bandwidth into its individual components of video, audio and vUSB
- Round-trip time: the round-trip latency between Receiver and Transmitter on the network during last polling interval
- User Latency: the latency a user experiences on video/mouse during the last polling interval

- On the Frame-Rate tab:

- Frame-per-Second: active frames sent from Transmitter to Receiver (typically will be 60 fps)
- Dropped-Frames-per-Second : number of frames dropped on the Transmitter. Normally this should be 0. Frames can be dropped for reasons such as network congestion.

- On the Connection tab:

- Shows the properties active on the connection: USB and Audio (i.e., is USB and Audio enabled or disabled on the connection)
- If a statistic exceeds a threshold, the color changes from green to amber to red.



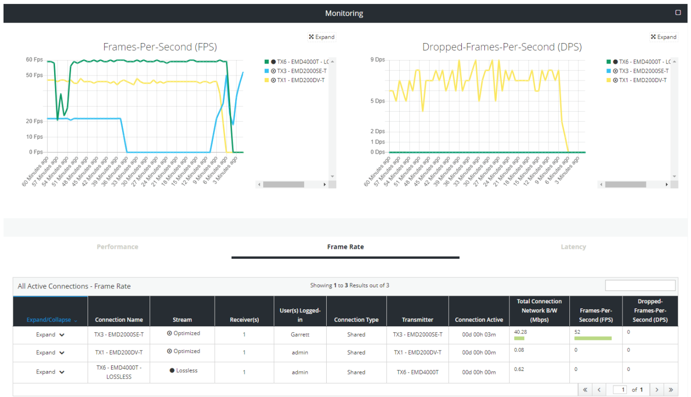
All Active Connections - Performance

Showing **1** to **3** Results out of 3

Expand/Collapse	Connection Name	Stream	Receiver(s)	User(s) Logged-in	Connection Type	Transmitter	Connection Active	Total Connection Network B/W (Mbps)	Video B/W (Mbps)	Audio B/W (Mbps)	vUSB B/W (Mbps)	Frames-Per-Second (FPS)	Dropped-Frames-Per-Second (DPS)
Expand	TX3 - EMD2000SE-T	⊙ Optimized	1	Garrett	Shared	TX3 - EMD2000SE-T	00d 00h 01m	37.53	37.53	0	0	27	0
Expand	TX1 - EMD200DV-T	⊙ Optimized	1	admin	Shared	TX1 - EMD200DV-T	00d 03h 03m	107.04	107.04	0	0	38	3
Expand	TX6 - EMD4000T - LOSSLESS	● Lossless	1	admin	Shared	TX6 - EMD4000T	00d 02h 57m	436.87	436.87	0	0	60	0

« ‹ 1 of 1 › »

FIGURE 11-22. ACTIVE CONNECTIONS



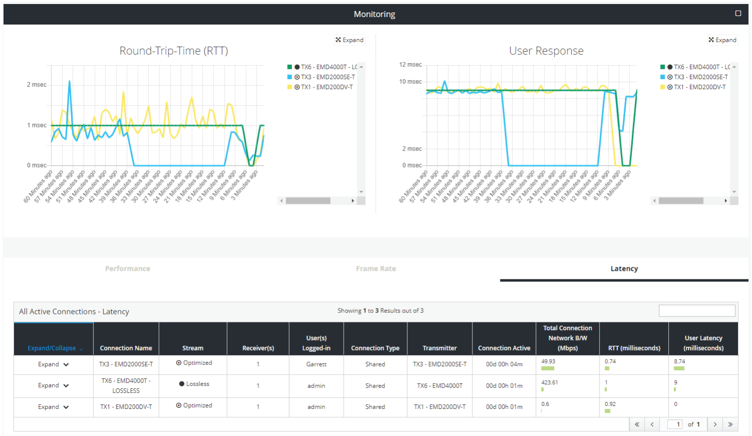
All Active Connections - Frame Rate

Showing **1** to **3** Results out of 3

Expand/Collapse	Connection Name	Stream	Receiver(s)	User(s) Logged-in	Connection Type	Transmitter	Connection Active	Total Connection Network B/W (Mbps)	Frames-Per-Second (FPS)	Dropped-Frames-Per-Second (DPS)
Expand	TX3 - EMD2000SE-T	⊙ Optimized	1	Garrett	Shared	TX3 - EMD2000SE-T	00d 00h 03m	40.28	52	0
Expand	TX1 - EMD200DV-T	⊙ Optimized	1	admin	Shared	TX1 - EMD200DV-T	00d 00h 00m	0.08	0	0
Expand	TX6 - EMD4000T - LOSSLESS	● Lossless	1	admin	Shared	TX6 - EMD4000T	00d 00h 00m	0.62	0	0

« ‹ 1 of 1 › »

FIGURE 11-23. ACTIVE CONNECTIONS FRAME RATE



All Active Connections - Latency

Showing **1** to **3** Results out of 3

Expand/Collapse	Connection Name	Stream	Receiver(s)	User(s) Logged-in	Connection Type	Transmitter	Connection Active	Total Connection Network B/W (Mbps)	RTT (milliseconds)	User Latency (milliseconds)
Expand	TX3 - EMD2000SE-T	⊙ Optimized	1	Garrett	Shared	TX3 - EMD2000SE-T	00d 00h 04m	49.93	0.74	8.74
Expand	TX6 - EMD4000T - LOSSLESS	● Lossless	1	admin	Shared	TX6 - EMD4000T	00d 00h 01m	423.61	1	9
Expand	TX1 - EMD200DV-T	⊙ Optimized	1	admin	Shared	TX1 - EMD200DV-T	00d 00h 01m	0.6	0.92	0

« ‹ 1 of 1 › »

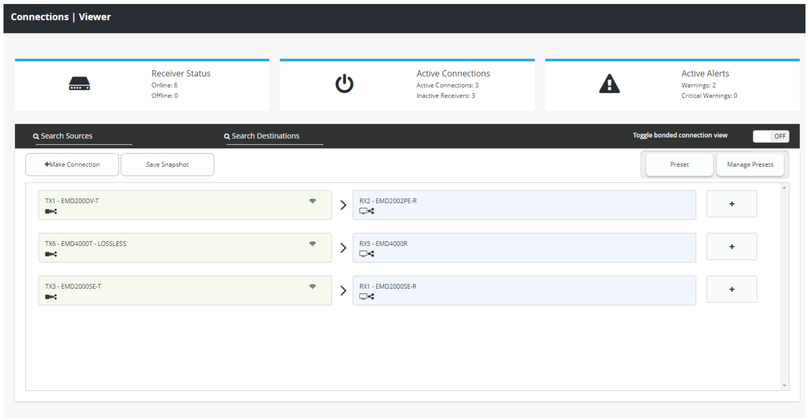
FIGURE 11-24. ACTIVE CONNECTIONS LATENCY

CHAPTER 11: CONNECTIONS

11.4 CONNECTIONS—VIEWER

On the Connections drop-down menu, click on Viewer. The appliance matrix screen appears.

NOTE: The toggle bonded connection view option can be enabled to view an individual connection within a bonded connection.



Receiver Status
Online: 6
Offline: 0

Active Connections
Active Connections: 3
Inactive Receivers: 3

Active Alerts
Warnings: 2
Critical Warnings: 0

Toggle bonded connection view OFF

TX1 - EMD200DV-T > RX2 - EMD2002PE-R

TX6 - EMD4000T - LOSSLESS > RX5 - EMD4000R

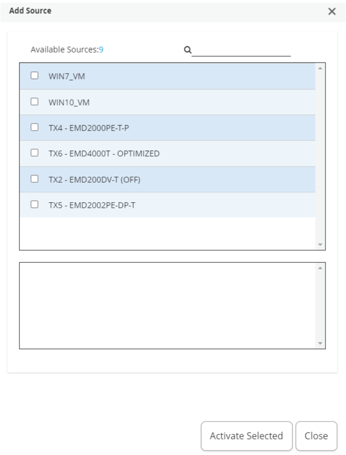
TX3 - EMD2000SE-T > RX1 - EMD2000SE-R

FIGURE 11-25. CONNECTIONS—VIEWER SCREEN

11.4.1 MAKE CONNECTIONS

Click on the Make Connections button, and the Add Source screen pops up.

NOTE: It is only possible to connect Emerald Receivers to Emerald Transmitters. For instructions on how to bond two Emerald ZeroU Transmitters to one Dual-Head Emerald SE Receiver, refer to the Emerald SE manual.



Available Sources:9

- ☐ WIN7_VM
- ☐ WIN10_VM
- ☐ TX4 - EMD2000PE-T-P
- ☐ TX6 - EMD4000T - OPTIMIZED
- ☐ TX2 - EMD200DV-T (OFF)
- ☐ TX5 - EMD2002PE-DP-T

FIGURE 11-26. ADD SOURCE BUTTON

Select a source from the list and press Activate Selected. Once the source connection is added successfully, add a destination (RX) from the available destinations to the selected source and activate by clicking the “Add Destination” button. To detach a destination, click on “X.”

Once you have a connection established, you will see the Connection Viewer page reflect this by displaying the connection name alongside all the attached receivers. To detach one of the receivers, move your mouse over that receiver tile and you will see an ‘X’ appear on the button. Clicking this X detaches only that receiver from the connection and leaves the rest of them intact.

By moving your mouse over the connection name tile you will also see an X appear. Clicking this will break all connections from any receiver connected with this connection name.

To revert, select Delete from the dropdown list to delete the source entry. This should show the “X” button, which is the Delete button.

If you click to ‘add destination’ to a private connection, you will only have the option to select one receiver. This is the receiver that is then used in the connection. If you wish to establish to the same connection from another receiver you will have to break this connection and establish the new one.

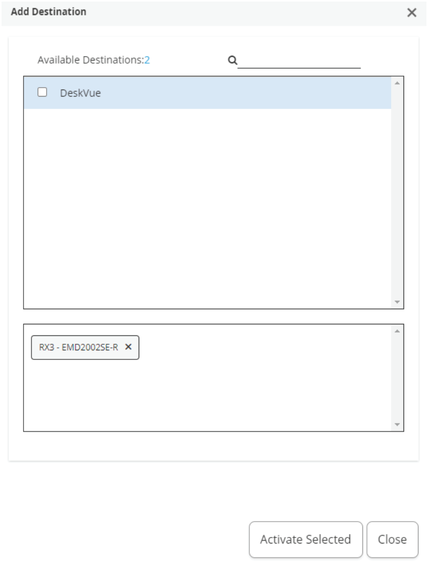


FIGURE 11-27. CONNECTIONS—ADD DESTINATION TO A PRIVATE CONNECTION

11.4.2 MANAGE PRESETS

Click on the Manage Presets button, and the Manage Presets screen pops up. Under this page all the existing presets will be listed. In the Manage Presets screen, you can rearrange the preset priority to change what presets display on th main Viewer screen. Essentially, you can pick your top three presets.

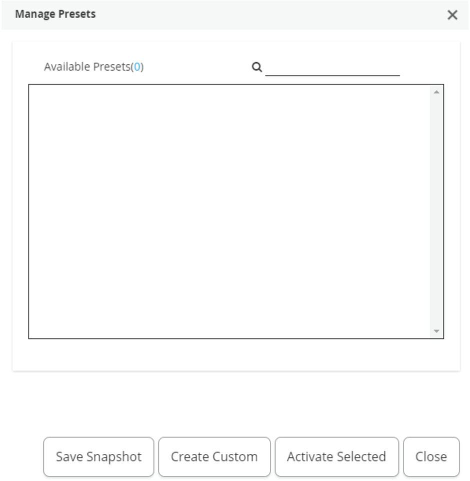
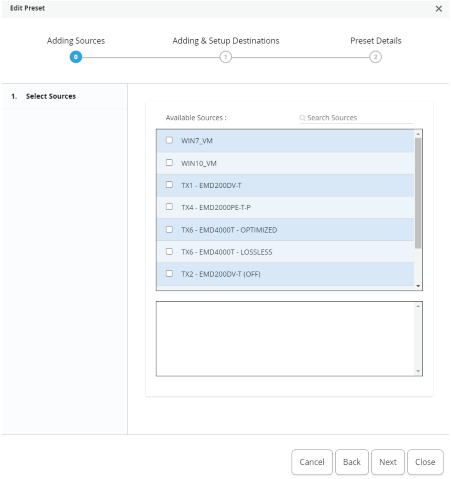


FIGURE 11-28. MANAGE PRESETS SCREEN

To create a new / custom template , click on " Create Custom" and select the required sources from the available list.



Edit Preset ✕

Adding Sources (0) — Adding & Setup Destinations (1) — Preset Details (2)

1. Select Sources

Available Sources : Search Sources

- □ WIN7_VM
- □ WIN10_VM
- □ TX1 - EMD200DV-T
- □ TX4 - EMD2000PE-T-P
- □ TX6 - EMD4000T - OPTIMIZED
- □ TX6 - EMD4000T - LOSSLESS
- □ TX2 - EMD200DV-T (OFF)

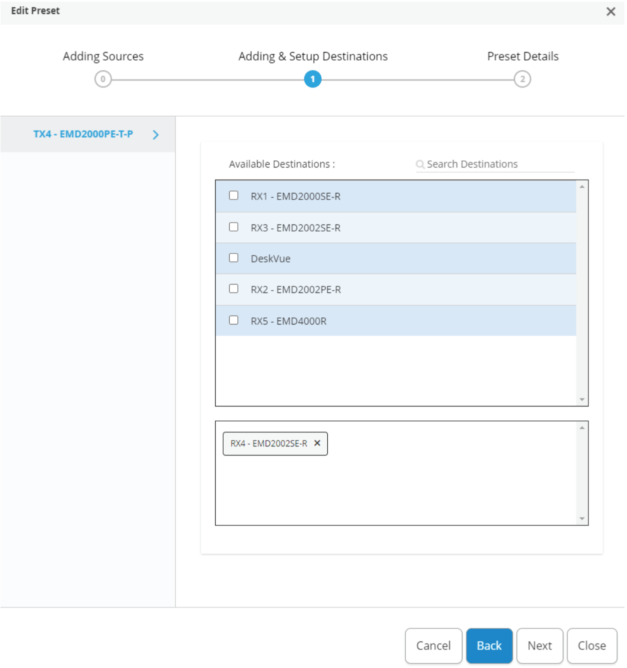
FIGURE 11-29. SELECT SOURCES SCREEN

Click next and select the destinations per source. Save the preset with a name and type (Partial or Full). Both preset types will forcibly take any source and destinations required to establish their configuration. For example, if those TX/VM and RX are already in active connections, then these connections will be broken.

The partial type applies only to the specific TX/VM and RX that are selected in this preset type.

The full type is applied to all of the TX/VM and RX. Any TX/VM and RX not selected in this preset type will become inactive when this preset is launched.

The icons on the sources screen are:



Edit Preset ✕

Adding Sources (0) — Adding & Setup Destinations (1) — Preset Details (2)

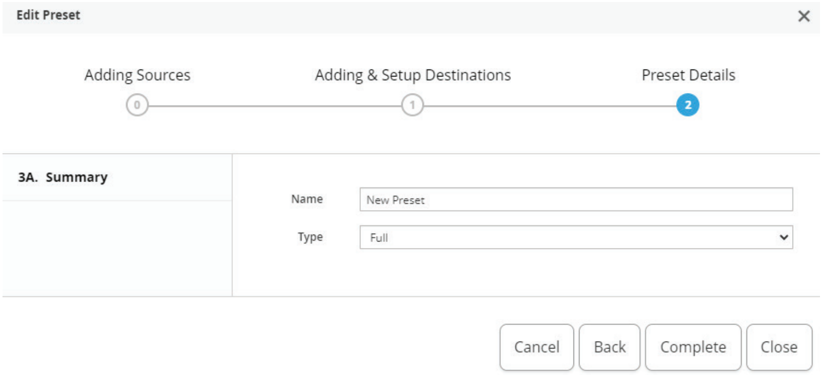
TX4 - EMD2000PE-T-P >

Available Destinations : Search Destinations

- □ RX1 - EMD2000SE-R
- □ RX3 - EMD2002SE-R
- □ DeskVue
- □ RX2 - EMD2002PE-R
- □ RX5 - EMD4000R

RX4 - EMD2002SE-R ✕

FIGURE 11-30. ADDING AND SETUP DESTINATIONS



Name: New Preset

Type: Full

FIGURE 11-31. PRESET DETAILS EDIT SCREEN

Click “Complete” to save the preset.

The following methods are available to activate presets:

1. Direct preset activation in the Viewer: The first three presets (ordered by creation) are presented directly in the Viewer and can be activated with a direct click.
2. Activation via Manage Presets: All presets can be activated with the “Activate Selected” option in “Manage Presets.” This is mandatory for any preset that is the fourth or later one created, as there is no other method to activate these presets from within Boxilla®.

Under manage presets, we have a snapshot option, which will automatically save the current active connections as a “ Preset”.

11.4.3 WORKSPACES

Workspaces can be used to configure the screen layout for DESKVUE only. The DESKVUE can support up to 16 active connections across multiple monitors. The DESKVUE user manual covers configuration details and should be referenced for more information about Workspaces.

Refer to Appendix B for more information about Workspaces for DESKVUE.

11.5 CONNECTIONS — FOLDERS

A separate menu is listed in the navigation menu to support the “Connection Folder” feature.

It is listed as a separate menu item as it is capable of containing all the Connection & Workspace elements within the Boxilla and gives a way to organize how they are presented to the KVM user which is independent of Users and Receiver settings. The hierarchy created under this section will be displayed the same across all Emerald Receivers and for all the users depending on their access right to those connections and workspaces contained.

11.5.1 ROOT DIRECTORY

Initially, when there is no hierarchy created yet and there are no Connection or Workspace elements added from the Boxilla yet, the connection folders page will be empty as shown in the following figure.

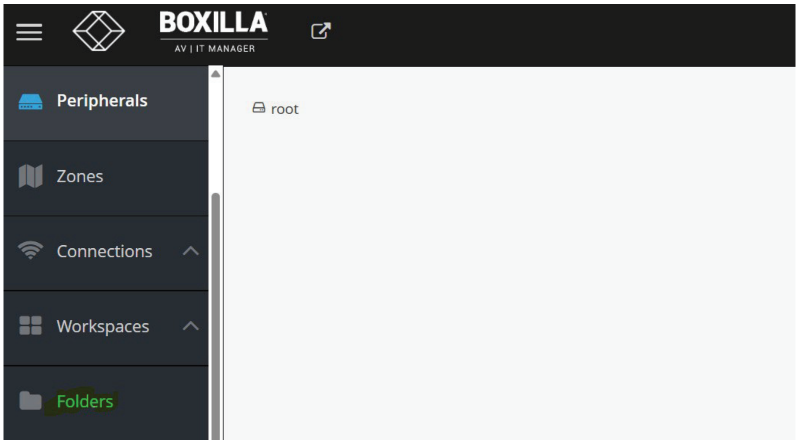


FIGURE 11-32. ROOT FOLDER

This is the default folder named as root. The root folder is not allowed to be deleted or edited. The custom hierarchy will be created under this root folder.

11.5.2 MENU ITEMS

When right-click is pressed on the root folder, it will display the “Add Folder” option as shown in the following figure.

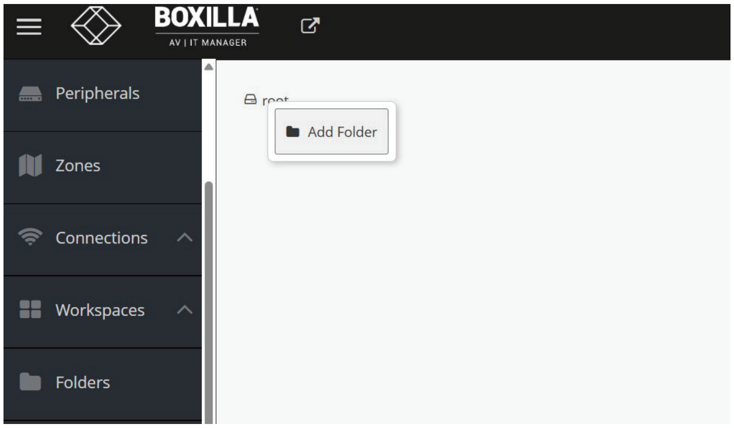


FIGURE 11-33. ADD NEW FOLDER

11.5.3 CREATE CONNECTION FOLDER HIERARCHY

Selecting the “Add new Folder” will create a new folder under the root directory providing a text input box to enter your desired name for the first folder. The name can contain text characters and spaces but does not support special characters. Complete the name entry with a press of the Enter key.

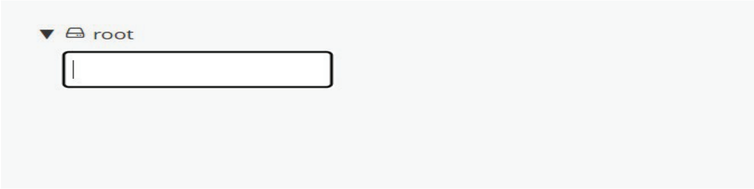


FIGURE 11-34. CREATE NEW FOLDER

By default, the hierarchy will display folders first and then any other elements after if on the same level. Once the name is saved it will appear as below:

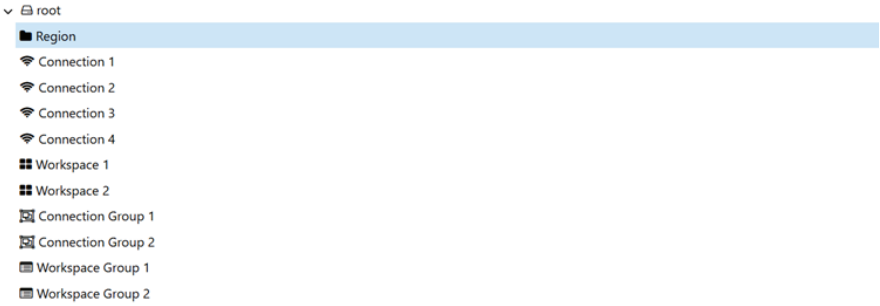


FIGURE 11-35. FOLDER ARRANGEMENTS

It is evident from the Figure, that all the elements and the Folders under the root are aligned in the same hierarchy level.

It is possible to create sub-folders for up three levels, With the ability to expand to the sub-folder on each level as below:

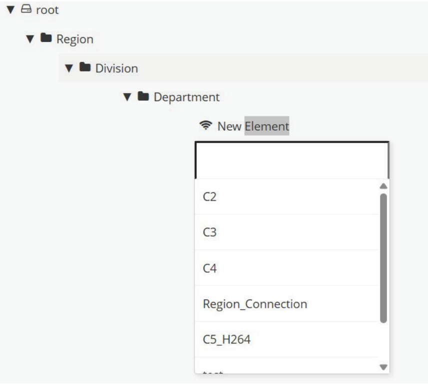


FIGURE 11-36. HIERARCHY EXAMPLE

11.5.4 UPDATE HIERARCHY WITH ELEMENTS

There are multiple ways to insert an element into the Folders.

Elements like Connections and Workspaces as well as groups of these can be inserted into the Folders by pressing right-click on the Folder. The Options are as below:

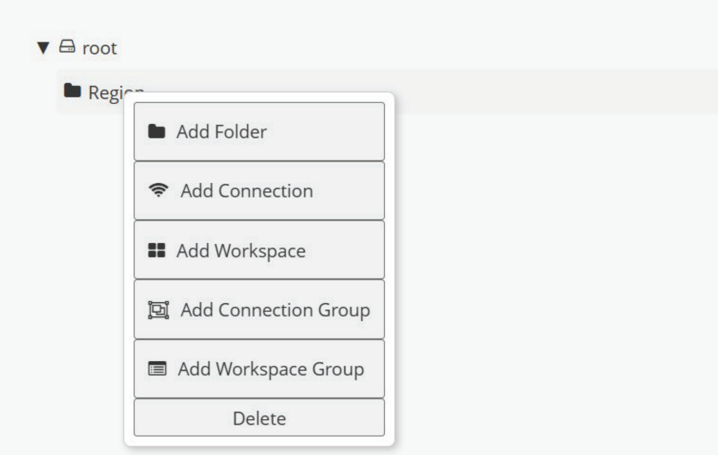
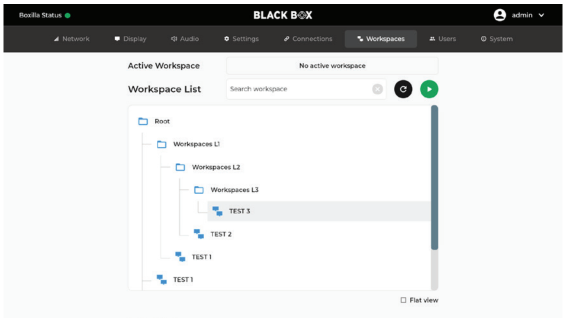


FIGURE 11-37. UPDATE HIERARCHY

Selecting the “Add New Connection” will now provide an option when double clicked upon to select from the list of all the connection elements present in the Boxilla. It will provide a dropdown to search/select the Connections.

This dropdown will also allow you to search the connections from the Boxilla by typing into the text entry field at the top of the dropdown menu, once the desired connection is found, a left click on its name will assign it to the Folder. Similarly, it will work with other elements like Workspace, Connection Group, and Workspace Group.



Active Workspace: No active workspace

Workspace List

FIGURE 11-38. ADD WORKSPACE

11.5.5 EDITING AN ELEMENT

Double-clicking on any element will give the dropdown menu if you need to re-assign a different Connection name or Workspace name.

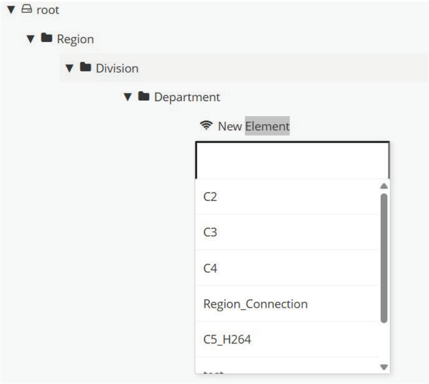
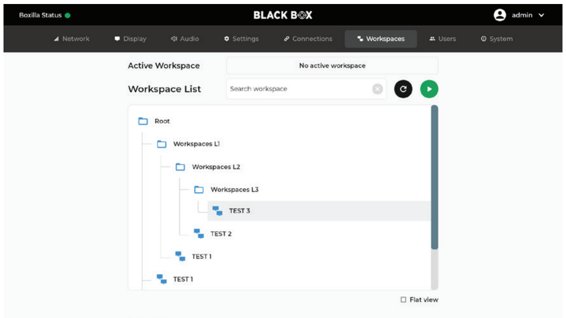


FIGURE 11-39. EDIT ELEMENT

Double-clicking on a folder will also allow you to re-name a folder if needed. With any element or folder if you need to remove it, you can do so with a right-click and you will have a delete option presented. Deleting a folder will remove all subfolders and elements within them.

Once configuration is complete, the following figure is an example of how the connection folders are presented to the KVM user at their receiver. This shows DESKVUE with three layers of folder hierarchy with one Workspace name placed within each layer.



Active Workspace: No active workspace

Workspace List

FIGURE 11-40. CONFIGURATION COMPLETE

This shows Emerald PE receiver also with three layers of folder hierarchy with one connection name placed within each layer.

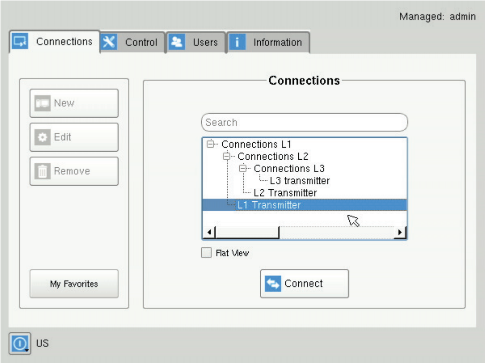


FIGURE 11-41. PE HIERARCHY

CHAPTER 12: USERS

Users are defined in the Boxilla® system to provide rights to manage the system, rights to connect to different target devices and rights to set parameters for connections.

12.1 USER TYPES

There are three types of users that can be created in the system:

1. Administrator: Users of this class have full rights to configure the system. They can create/modify/delete users and connections, change network settings, etc.
2. Power User: Users of this class can modify resolution for connections to virtual desktops and change his/her local password.
3. Standard Users: Users of this class can only select from a list of pre-defined connections to access and view system information. They cannot change any configuration settings.

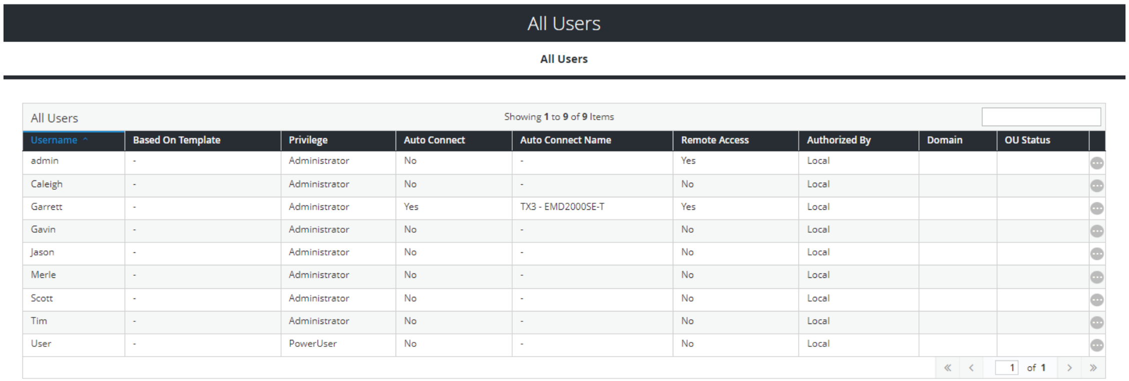
The Boxilla has one default user — admin, which is a member of the administrator group. This user is defined by default and cannot be deleted. Boxilla currently supports up to 1,000 individual users.

NOTE: The Boxilla user cannot be an Active Directory user; the user must be local to the Boxilla system.

To manage users, an administrator selects the Users button on the main menu.

12.2 USER—MANAGE

The User—Manage screen is used to create, edit and delete users as shown in Figure 12-1. It provides a list of the currently created users.



All Users

All Users

All Users — Showing **1** to **9** of **9** Items

Username ^	Based On Template	Privilege	Auto Connect	Auto Connect Name	Remote Access	Authorized By	Domain	OU Status
admin	-	Administrator	No	-	Yes	Local		
Caleigh	-	Administrator	No	-	No	Local		
Garrett	-	Administrator	Yes	TX3 - EMD2000SE-T	Yes	Local		
Gavin	-	Administrator	No	-	No	Local		
Jason	-	Administrator	No	-	No	Local		
Merle	-	Administrator	No	-	No	Local		
Scott	-	Administrator	No	-	No	Local		
Tim	-	Administrator	No	-	No	Local		
User	-	PowerUser	No	-	No	Local		

FIGURE 12-1. USERS—MANAGE

12.2.1 ADD USER

To create a user, click on the +User button at the top of the page and this opens up the new user wizard. The initial page of this wizard is shown in Figure 12-2.

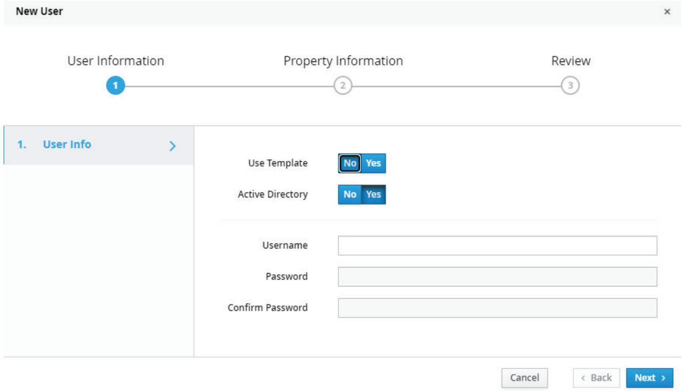


FIGURE 12-2. NEW USER WIZARD

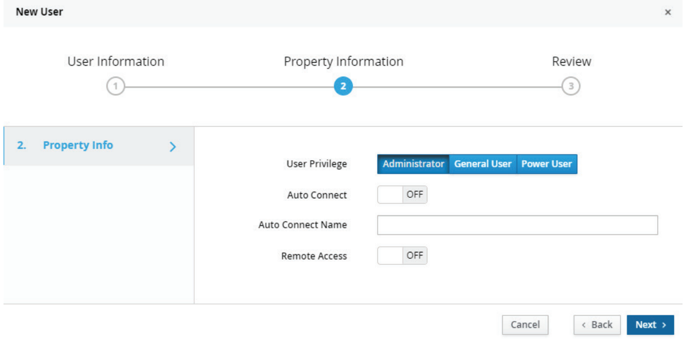
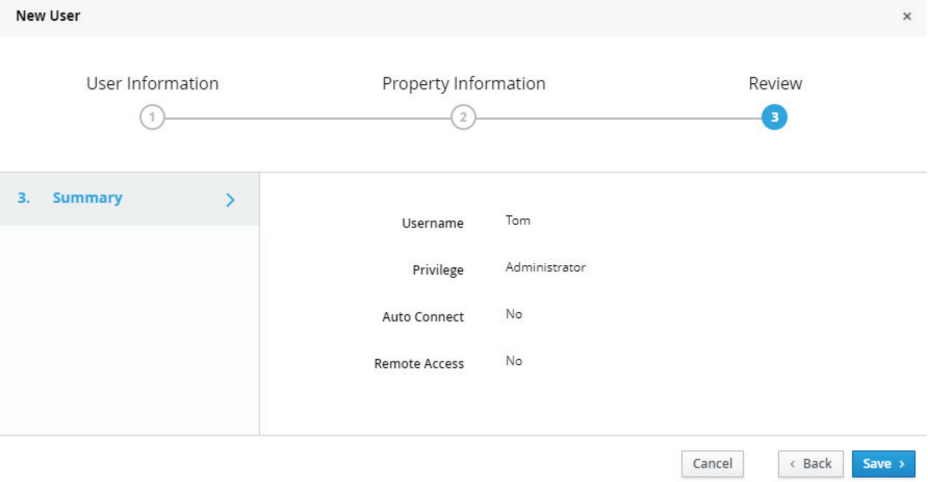


FIGURE 12-3. NEW USER PROPERTY INFORMATION SCREEN

The administrator can use a template to follow a common set of properties for a user as described in the next section. The definitions of the properties of a user are:

- User Name: This is a unique name that uses 1–32 characters. The username can be any valid username for a Microsoft O/S. This means the username cannot contain " "/ \ [] ; | = + * ? < > `.
- Active Directory: Select "Yes" if the user belongs to Active Directory that is enabled on Boxilla®.
- Password: This field can be a minimum of 0 characters (i.e. blank) and a maximum of 32 characters. The password can be any valid password for a Microsoft O/S. The user password MAY contain the following special characters , ~ : ! @ # $ % ^ & ' { } which means the password cannot contain " "/ \ [] : ; | = , + * ? < > `'
- User Privilege: This field defines the type of user the new user will be: Administrator, General User or Power User.
- Auto-Connect: This enable/disable whether the attempts to connect immediately to the selected connection after a logon by this user. This automatic connection only occurs after a logon. If a user exits the connection, the connection tab is displayed to the user for selection of a connection.
- Auto Connect Name: Select the connection the user will auto connect to after logging in.
- Remote Access: Enable Remote Access for users who need to log in and use the RemoteApp software. If this is turned off, the user cannot log into the RemoteApp software. When in the On state, one RemoteApp license will be used, and when turned off, the license will go back to the general pool for other users to use.



Username Tom

Privilege Administrator

Auto Connect No

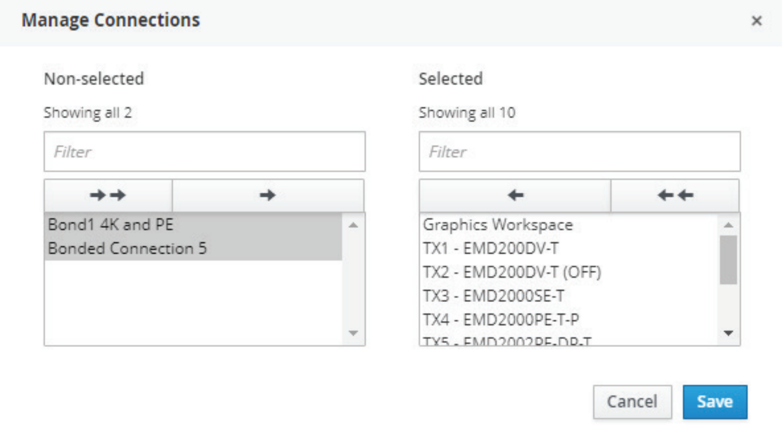
Remote Access No

FIGURE 12-4. NEW USER SCREEN

Once the new user fields have been filled out, you must click the Save button to create the new user. Clicking the Save button causes the validation of the new username, checking that it is unique and that the two password entries match. If this validation fails, a pop-up window displays the reason for the failure, and the new user is not created. After dismissing the pop-up window, the user can fix the error and click Save again.

12.2.2 MANAGE USER CONNECTIONS

The new user must be allocated Connections that he/she can access. This is done by clicking on "Manage Connection" option on the ellipsis "•••" icon in the required user row. The required connections are selected from the available Connections—click on the connection in the Non-Selected List and then click the "->" button). This causes the selected connections to be "added" to a user's selected connection window as shown in Figure 12-3. This will also include the set of configured bonded connections. Click Save to complete the selection. It is a similar process to edit an existing users list of connections. To remove a connection from a user, select the specific connection in the Selected list (i.e. current connections allocated to the user) and click on the "<-" button. Click Save to complete the task.



Bond1 4K and PE
Bonded Connection 5

Graphics Workspace
TX1 - EMD200DV-T
TX2 - EMD200DV-T (OFF)
TX3 - EMD2000SE-T
TX4 - EMD2000PE-T-P
TX5 - EMD2002PE-DP-T

FIGURE 12-5. MANAGE USER CONNECTIONS

12.2.3 ACTIVE DIRECTORY USER MANAGEMENT

When you create a new user and save it as an Active Directory user, you will see the ”OU Status” change to a loading spinner. This means Boxilla® is attempting to retrieve the DN string for the user that contains the OU and CN information. If the retrieve was successful, the spinner will change to a “tick” or check mark and we will store the new OU tree information in our database. If the retrieve was not successful, then the spinner will change to an X. If the Boxilla administrator wishes to manually specify an OU for this user, then they can manually “edit” the user and they will then be presented with the text fields to enter the OU information manually. As of Boxilla 3.6.0, the administrator no longer needs to configure AD users in Boxilla.

ACTIVE DIRECTORY USER LOGGING INTO RECEIVER

When a user logs onto the receiver as an AD user, Boxilla® queries Active Directory server for authentication. When the Active Directory returns a successful response, the local user is allowed to log into the device.

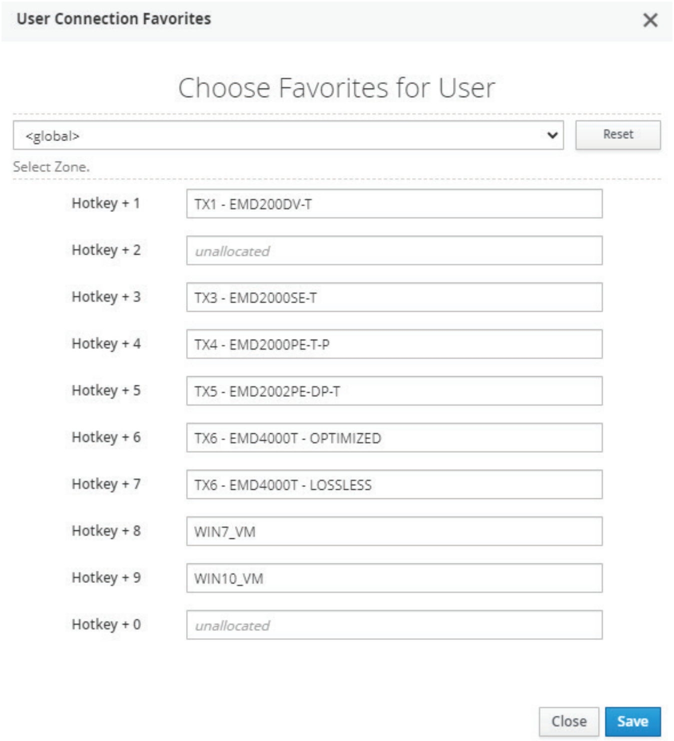
12.2.4 CONNECTION FAVORITES

Connection favorites provide a quick convenient mechanism for users to switch between their pre-defined connections. Favorites are configured by the administrator where a maximum of 10 favorites can be assigned to users using a combination of hotkey and [0-9].

Assigning Connection Favorites

A pre-requisite is that the user exists and has connections assigned.

The following screenshot demonstrates the administrator assigning connections for the user to the available hotkeys. Favorites do not need to be allocated sequentially and hotkeys can be skipped. Favorites can now be also assigned to bonded connections.



Choose Favorites for User

<global>

Select Zone.

Hotkey + 1	TX1 - EMD200DV-T
Hotkey + 2	unallocated
Hotkey + 3	TX3 - EMD2000SE-T
Hotkey + 4	TX4 - EMD2000PE-T-P
Hotkey + 5	TX5 - EMD2002PE-DP-T
Hotkey + 6	TX6 - EMD4000T - OPTIMIZED
Hotkey + 7	TX6 - EMD4000T - LOSSLESS
Hotkey + 8	WIN7_VM
Hotkey + 9	WIN10_VM
Hotkey + 0	unallocated

FIGURE 12-6. CONNECTION FAVORITES SCREEN

Listing Connection Favorites:

When a user logs in they can view their assigned favorites by clicking on the “My Favorites” button on the Receiver GUI under “Connections.”

12.2.5 MANAGE WORKSPACES

Similar to Manage Connections, Workspaces can be assigned to users so that they can access the layout in the DESKVUE GUI. This configuration only applies to users who log into the DESKVUE Receiver.

12.2.6 MANAGE WORKSPACE GROUPS

This option allows for the configuration of the specific user in the Workspace Group. A Workspace Group can contain a collection of individual workspaces, and assigning a user to a workspace group is more efficient in some applications.

12.2.7 MANAGE WORKSPACE FAVORITES

Similar to Manage Connection Favorites, the Manage Workspace Favorites allows users to quickly access different workspaces by using the hotkeys and buypassing the GUI.

12.2.8 MANAGE PRESETS FOR NBR

This feature manages the the presets designed for the Northbound Rest API.

12.2.9 DELETE USER

This option allows the administrator to permanently delete the user from the Boxilla database.

12.3 MANAGE GROUPS

Once a user is registered in Boxilla®, the administrator can assign the user to a User Group by using the Manage Groups option. Once the group profile is assigned to a user, that user will be able to make a connection to the targets found in that group. Connection Groups can be assigned to a user via the Manage Groups option. There are two default Connection Groups:

1) OU Undefined.

2) OU Not Found.

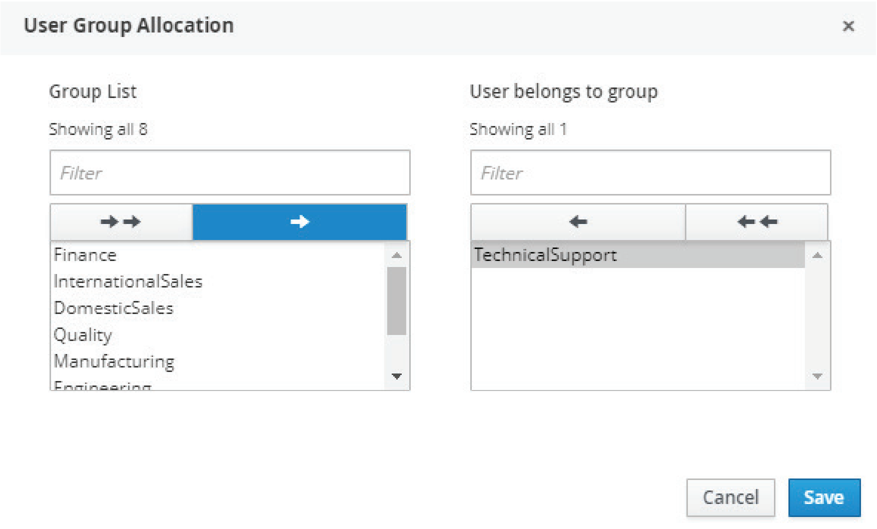
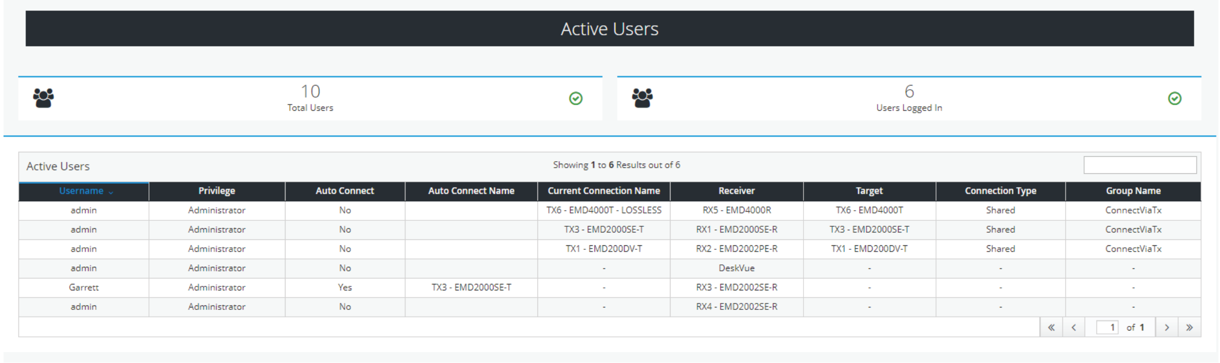


FIGURE 12-7. MANAGE GROUPS

12.4 USER—ACTIVE

The User—Active page shows a list of all the users logged in to a Receiver. The page provides information on what Receiver the user is logged in on and details on any active connection as shown in Figure 12-8.



Active Users

10
Total Users

6
Users Logged In

Active Users

Showing **1** to **6** Results out of 6

Username	Privilege	Auto Connect	Auto Connect Name	Current Connection Name	Receiver	Target	Connection Type	Group Name
admin	Administrator	No		TX6 - EMD4000T - LOSSLESS	RX5 - EMD4000R	TX6 - EMD4000T	Shared	ConnectViaTx
admin	Administrator	No		TX3 - EMD2000SE-T	RX1 - EMD2000SE-R	TX3 - EMD2000SE-T	Shared	ConnectViaTx
admin	Administrator	No		TX1 - EMD200DV-T	RX2 - EMD2002PE-R	TX1 - EMD200DV-T	Shared	ConnectViaTx
admin	Administrator	No		-	DeskVue	-	-	-
Garrett	Administrator	Yes	TX3 - EMD2000SE-T	-	RX3 - EMD2002SE-R	-	-	-
admin	Administrator	No		-	RX4 - EMD2002SE-R	-	-	-

FIGURE 12-8. ACTIVE USERS

CHAPTER 13: DKM INTEGRATION

13.1 INTRODUCTION

This chapter considers integration aspects of Boxilla®. The chapter is divided into two main sections, which include activities on the DKM end and on the Boxilla side. The chapter describes the configuration elements for Boxilla and DKM.

Boxilla manages DKM connections towards Emerald appliances by means of Virtual CPUs. The VirtualCPU name must match the Emerald Connection name. When the DKM Connection (vCPU to CON) is established, the DKM switch will echo this operation onto the network. This will be picked up by Boxilla and it will initiate the desired connections between the Receiver and the Transmitter/VM.

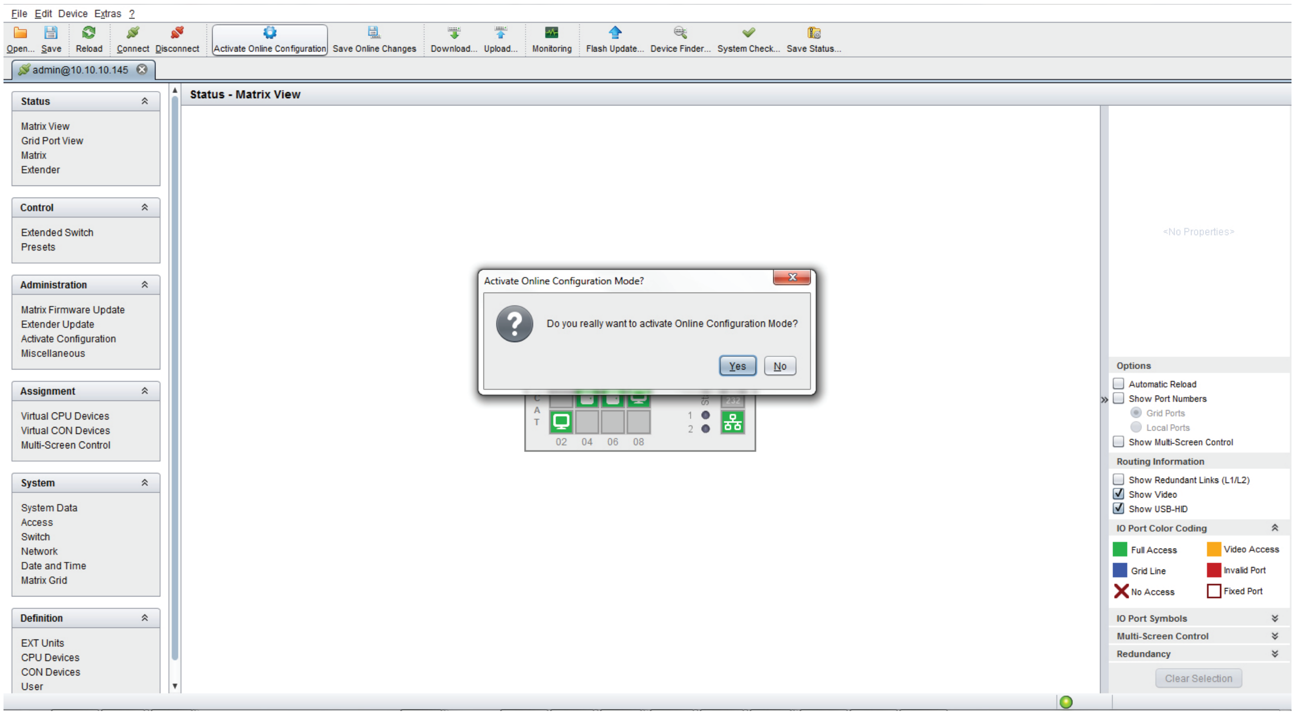
Follow these steps:

1. Create desired Emerald Connection.
2. Add a DKM Switch under Boxilla -> DKM -> Switches.
3. Create a Virtual CPU using the DKM Configuration Utility (named the same name as the Emerald Connection). Physically attach this to the Emerald Receiver. When the DKM CON is then connected to the VirtualCPU, the connection name will be picked up and the Emerald leg of the connection will be set up.

13.2 STEPS TO CREATE AND MANAGE VCPU CONNECTIONS ON THE UTILITY

Assumed: You have the desired Emerald connection setup.

Open the Java Tool and select "Activate Online Configuration," which is found in the toolbar of the DKM FX Tool. Select Yes when you are asked to confirm. NOTE: The screen you see depends on the version of the DKM Java Tool used.



Activate Online Configuration Mode?

Do you really want to activate Online Configuration Mode?

Yes No

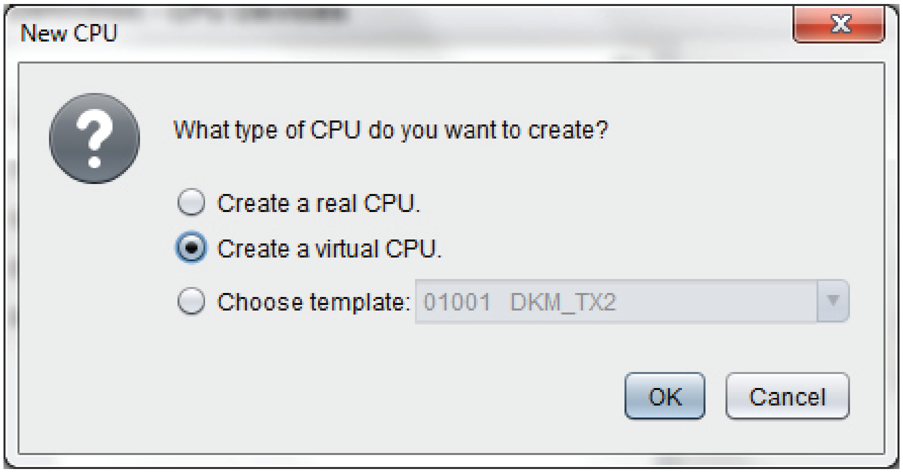
☐ Automatic Reload
☐ Show Port Numbers
○ Grid Ports
○ Local Ports
☐ Show Multi-Screen Control

☐ Show Redundant Links (L1/L2)
☑ Show Video
☑ Show USB-HID

🟩 Full Access 🟧 Video Access
🟦 Grid Line 🟥 Invalid Port
✗ No Access □ Fixed Port

FIGURE 13-1. DKM CONFIGURATION UTILITY SCREEN

Click "CPU Devices," which is a menu item under "Definition" on the lower left side. Next, select the "New Device" button on the lower right side of the screen. Select "Create a virtual CPU."



New CPU

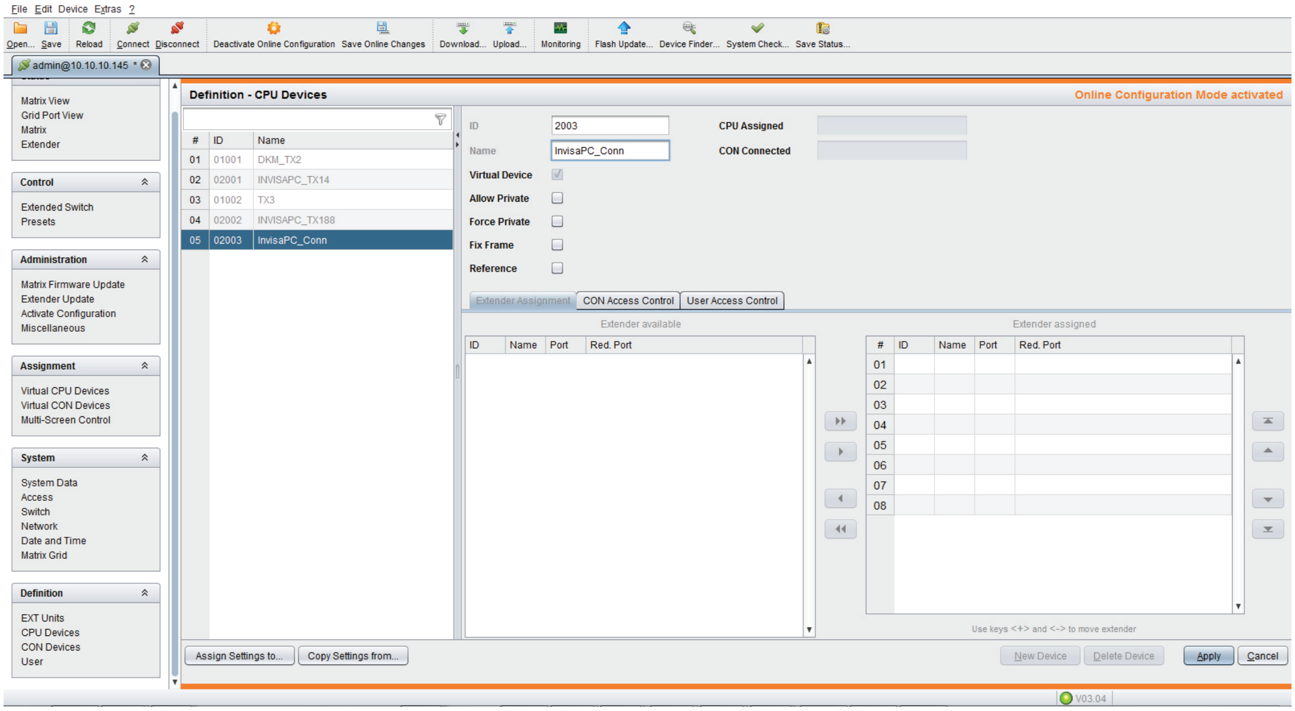
What type of CPU do you want to create?

- ○ Create a real CPU.
- ● Create a virtual CPU.
- ○ Choose template: 01001 DKM_TX2

FIGURE 13-2. CREATE A VIRTUAL CPU OPTION

You will then have the option to name your Virtual CPU.

IMPORTANT: This name must be the same as the Emerald Connection name that you want it to be associated with.



Definition - CPU Devices

Online Configuration Mode activated

#	ID	Name
01	01001	DKM_TX2
02	02001	INVISAPC_TX14
03	01002	TX3
04	02002	INVISAPC_TX188
05	02003	InvisaPC_Conn

ID: 2003

Name: InvisaPC_Conn

CPU Assigned:

CON Connected:

Virtual Device ☑

Allow Private □

Force Private □

Fix Frame □

Reference □

Extender available

ID	Name	Port	Red. Port

Extender assigned

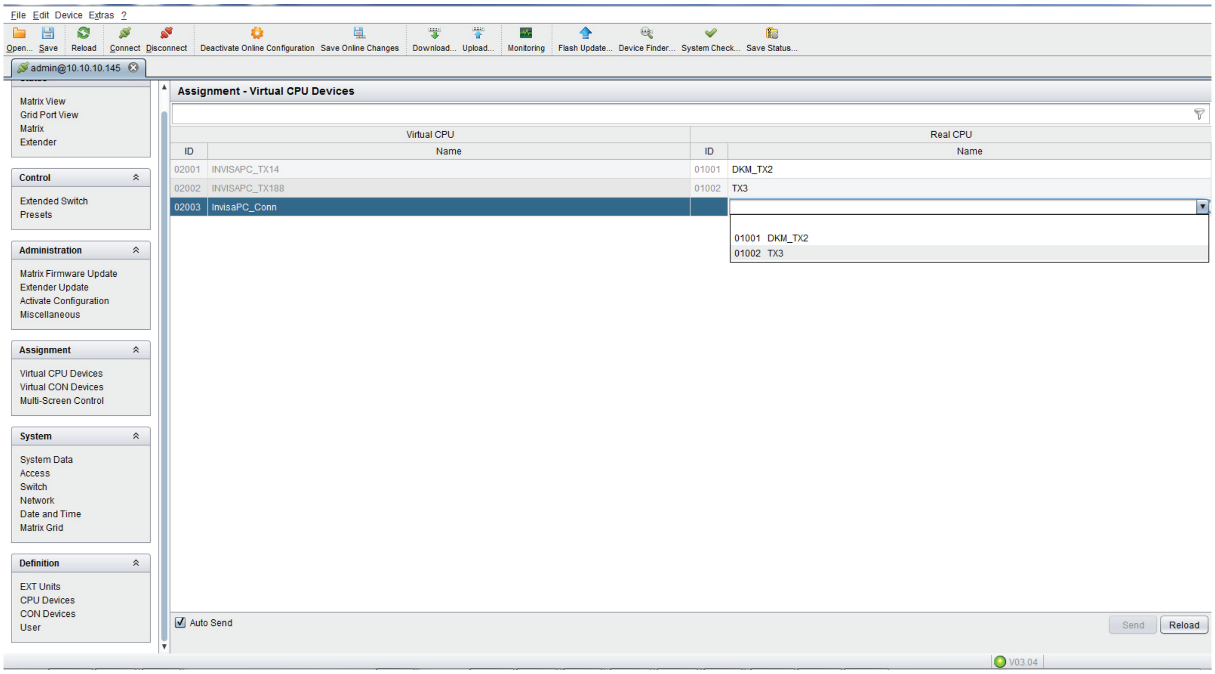
#	ID	Name	Port	Red. Port
01				
02				
03				
04				
05				
06				
07				
08				

Use keys <+> and <-> to move extender

FIGURE 13-3. NAME VIRTUAL CPU SCREEN

Press “Apply.”

Next, navigate to "Virtual CPU Devices," which appears under the "Assignment" tab on the main menu on the left side of the application window. Here you can assign your new Virtual CPU to the real CPU that's physically connected into your Emerald receiver. This is done by clicking the empty space in the "Name" column and seeing the drop down of available Real CPUs.



Assignment - Virtual CPU Devices

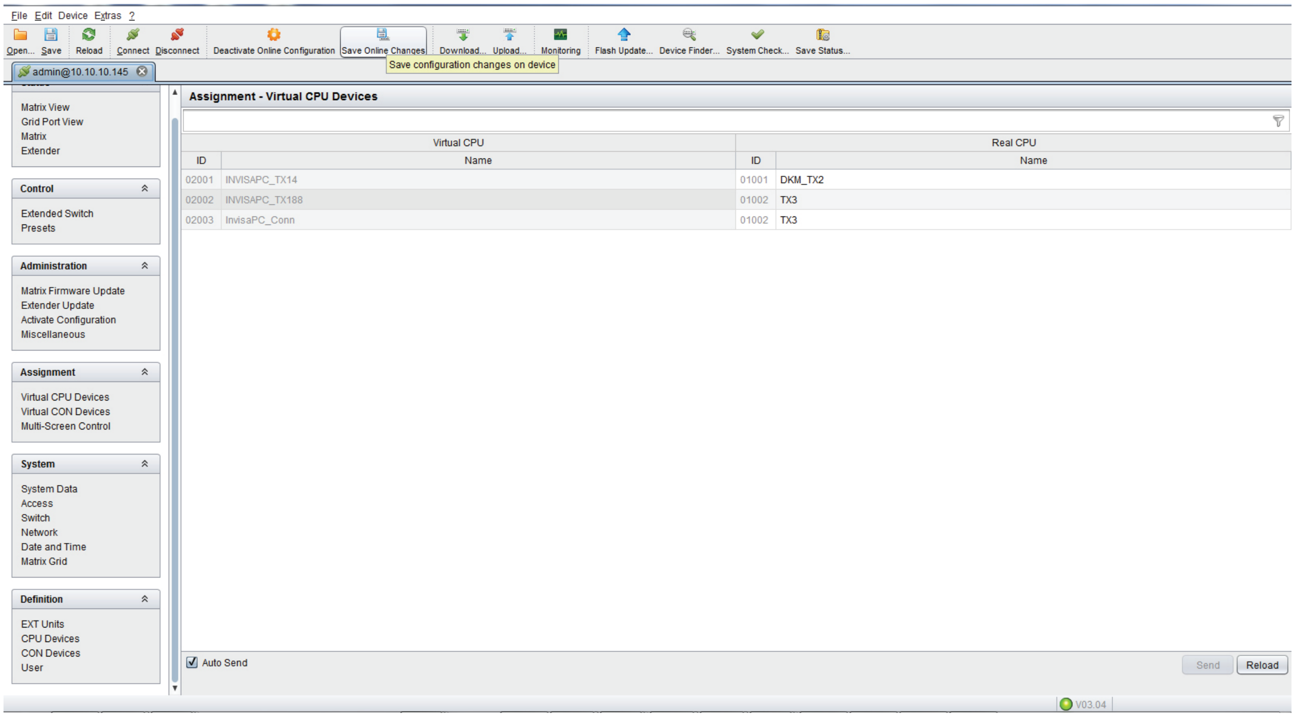
Virtual CPU		Real CPU	
ID	Name	ID	Name
02001	INVISAPC_TX14	01001	DKM_TX2
02002	INVISAPC_TX188	01002	TX3
02003	InvisaPC_Conn		

01001 DKM_TX2
01002 TX3

☑ Auto Send

FIGURE 13-4. DROP DOWN LIST OF AVAILABLE REAL CPUS

Next, click “Save Online Changes.” This pushes the changes down to the DKM switch so even if it reboots it will hold onto the new settings.



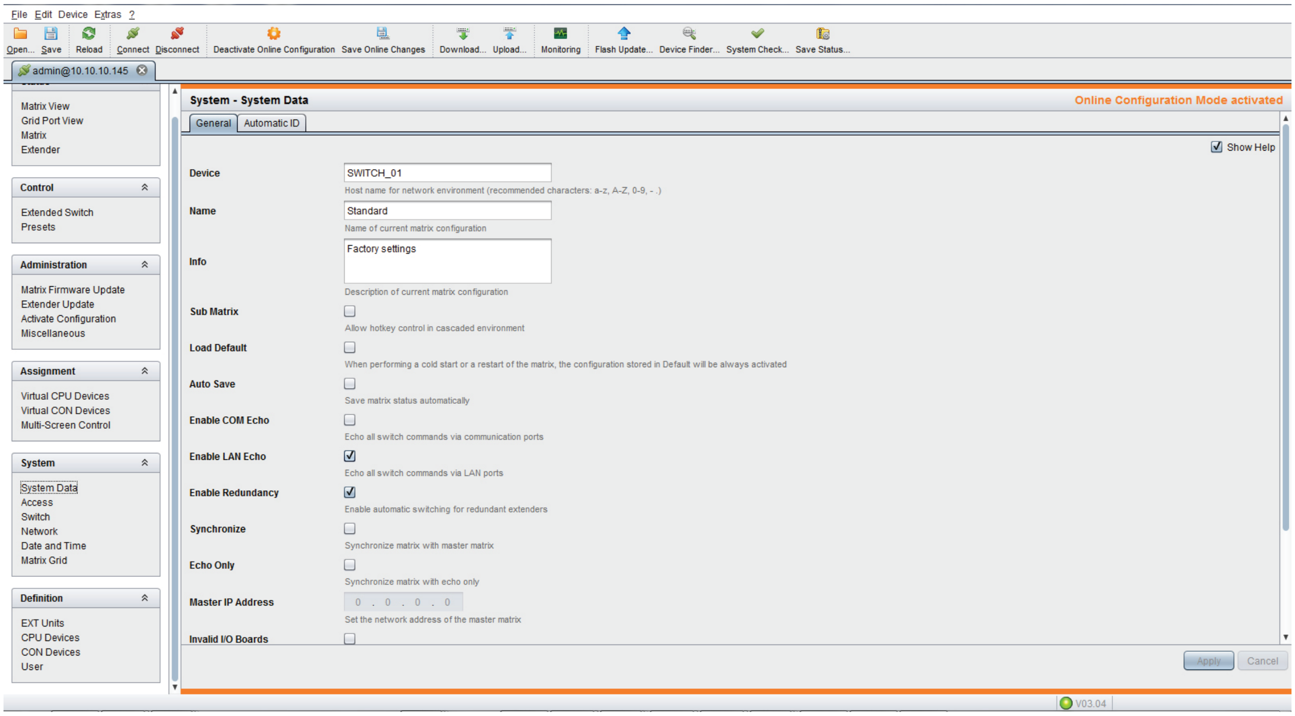
Assignment - Virtual CPU Devices

Virtual CPU		Real CPU	
ID	Name	ID	Name
02001	INVISAPC_TX14	01001	DKM_TX2
02002	INVISAPC_TX188	01002	TX3
02003	InvisaPC_Conn	01002	TX3

FIGURE 13-5. SAVED CHANGES

HOW TO ENABLE LAN ECHO

Next, you must Enable LAN Echo. This will enable the switch to echo the results of the connection initiations to the network, where Boxilla® can put them up and set up the corresponding Emerald Connections.



System - System Data

Online Configuration Mode activated

☑ Show Help

Device: SWITCH_01
Host name for network environment (recommended characters: a-z, A-Z, 0-9, - .)

Name: Standard
Name of current matrix configuration

Info: Factory settings
Description of current matrix configuration

Sub Matrix ☐
Allow hotkey control in cascaded environment

Load Default ☐
When performing a cold start or a restart of the matrix, the configuration stored in Default will be always activated

Auto Save ☐
Save matrix status automatically

Enable COM Echo ☐
Echo all switch commands via communication ports

Enable LAN Echo ☑
Echo all switch commands via LAN ports

Enable Redundancy ☑
Enable automatic switching for redundant extenders

Synchronize ☐
Synchronize matrix with master matrix

Echo Only ☐
Synchronize matrix with echo only

Master IP Address: 0 . 0 . 0 . 0
Set the network address of the master matrix

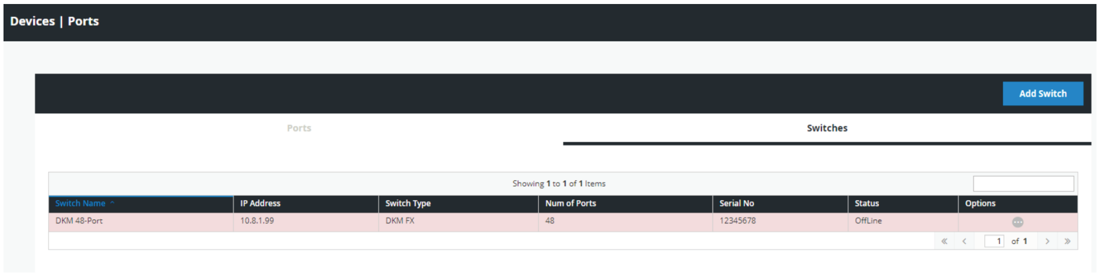
Invalid I/O Boards ☐

FIGURE 13-6. ENABLE LAN ECHO

If you encounter issues with the configuration not staying in place, you will need to save the DKM DTC file on a local computer, then, using the DKM Configuration Utility, go to File>>Upload and activate the configuration which also requires a DKM switch reboot.

13.3 STEPS TO ADD SWITCHES

Under Boxilla®, to add the DKM switch, navigate to DKM —Switches and click the blue “Add Switch” button on the top right of the screen.



Showing 1 to 1 of 1 Items

Switch Name ^	IP Address	Switch Type	Num of Ports	Serial No	Status	Options
DKM 48-Port	10.8.1.99	DKM FX	48	12345678	OffLine	⋯

FIGURE 13-7. ADD SWITCH SCREEN

The Add new switch box will appear on the page. The only critical detail here is the IP address. Fill in the details and press Save.

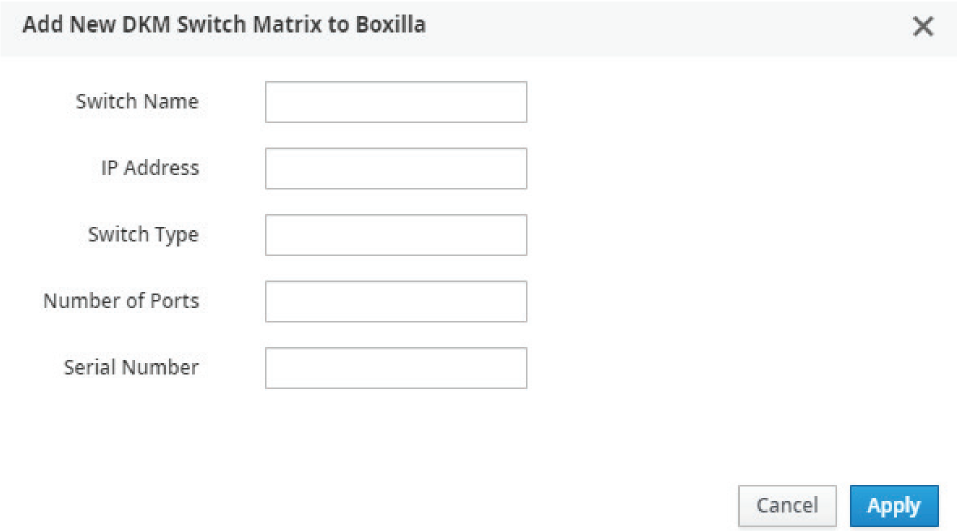
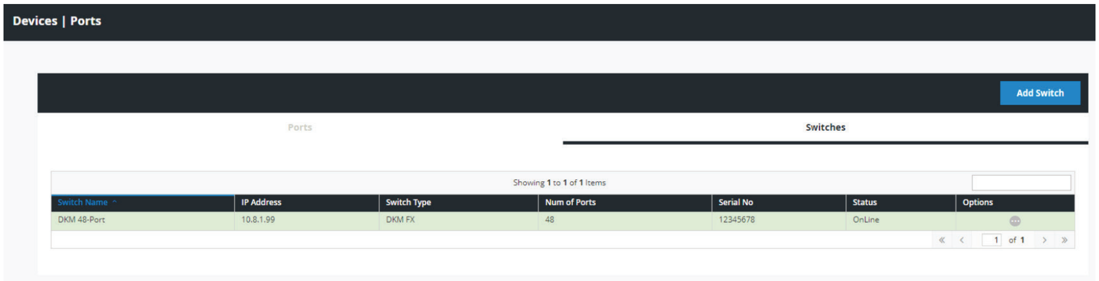


FIGURE 13-8. ADD NEW DKM SWITCH

Once the switch is added successfully, it gets listed with an online status.



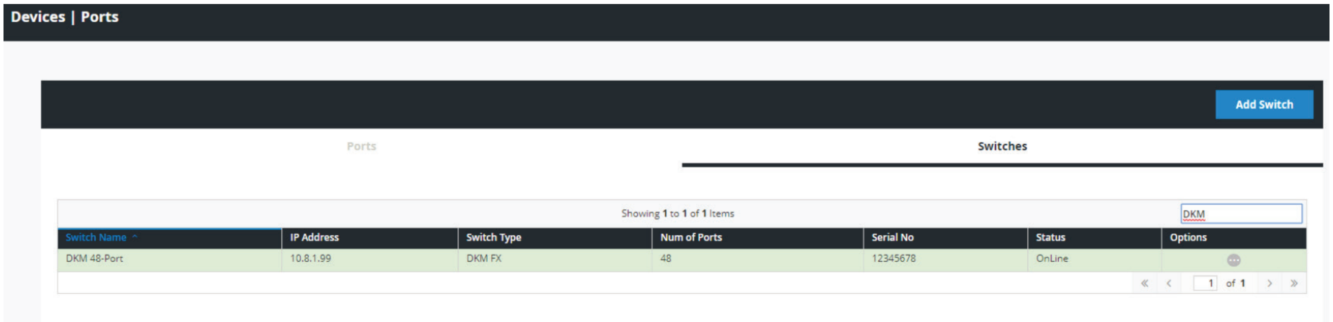
Showing 1 to 1 of 1 Items

Switch Name ^	IP Address	Switch Type	Num of Ports	Serial No	Status	Options
DKM 48-Port	10.8.1.99	DKM FX	48	12345678	OnLine	⋯

FIGURE 13-9. ONLINE STATUS OF SWITCH

If you wish to remove/delete the DKM Switch from the Boxilla® system, click on the ellipsis "..." button next to the DKM switch that you would like to remove. Then select the "Delete" option.

If using multiple DKM switches, you can search for a switch by entering the switch name into quick search box at the right corner.



Showing 1 to 1 of 1 Items

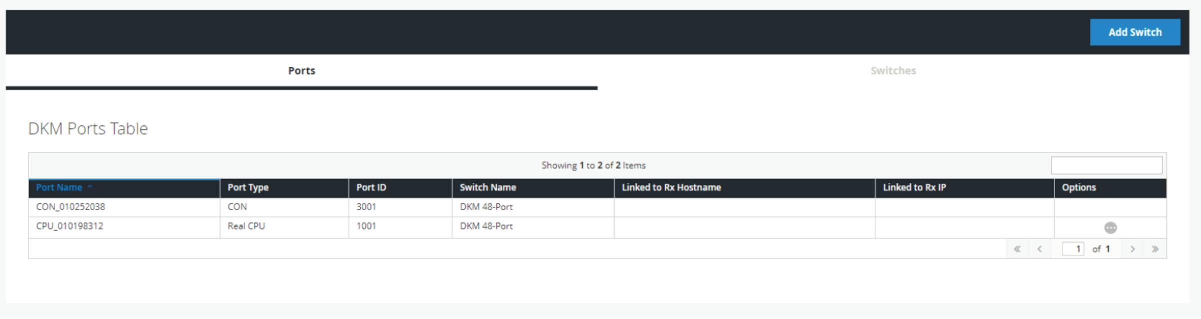
DKM

Switch Name ^	IP Address	Switch Type	Num of Ports	Serial No	Status	Options
DKM 48-Port	10.8.1.99	DKM FX	48	12345678	OnLine	⋯

FIGURE 13-10. SEARCH FOR A SWITCH

Once the switch is added successfully, all DKM CONs and DKM CPUs (physical) connected will be listed in Boxilla® under the "Ports" tab. Also any Virtual CPUs configured on the DKM switch will be listed. Boxilla will automatically update with any new DKM CONs, DKM CPUs and Virtual CPUs that may be added in the future. Follow the next steps to create a new connection.

The DKM Ports Table displays ports based on the DKM switch that has been added.



DKM Ports Table

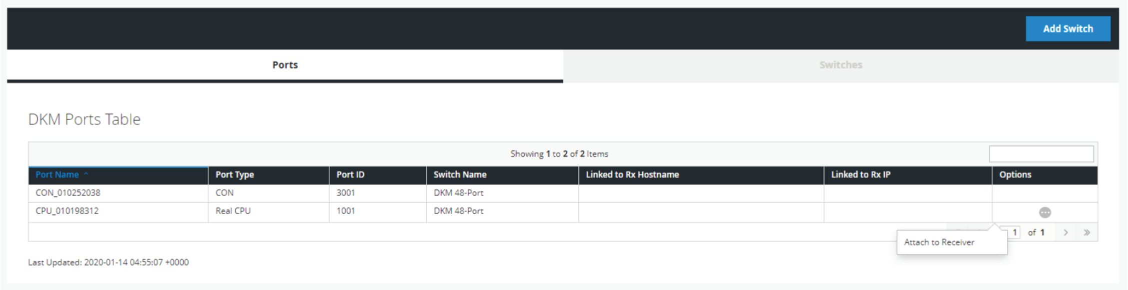
Showing 1 to 2 of 2 Items

Port Name ^	Port Type	Port ID	Switch Name	Linked to Rx Hostname	Linked to Rx IP	Options
CON_010252038	CON	3001	DKM 48-Port			
CPU_010198312	Real CPU	1001	DKM 48-Port			⋯

FIGURE 13-11. DKM PORTS TABLE

The "Last Updated" text at the bottom of the screen is the last time Boxilla® audited the DKM switch.

Find the Virtual CPU in the "Ports" list on the DKM-Switches page. Click the options button on the right hand side to "Attach to Receiver."



DKM Ports Table

Showing 1 to 2 of 2 Items

Port Name ^	Port Type	Port ID	Switch Name	Linked to Rx Hostname	Linked to Rx IP	Options
CON_010252038	CON	3001	DKM 48-Port			
CPU_010198312	Real CPU	1001	DKM 48-Port			⋯

Last Updated: 2020-01-14 04:55:07 +0000

FIGURE 13-12. ATTACH TO RECEIVER

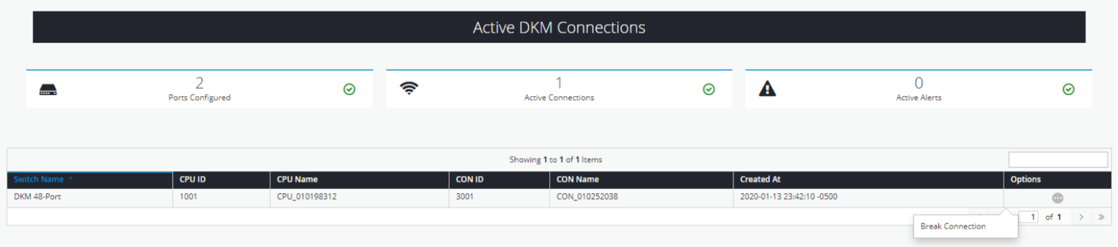
If you wish to search for a specific port, enter the Port ID at the search box within ports table.

To start a connection you have two options:

1. Manual connections using "Add custom Source," which lasts until the connection is broken.

2. Saving connection configurations as "Presets," which can be activated on demand.

To detach a connection, left-click on the connection name. You will see a popup box that gives you the option to disconnect.



Showing 1 to 1 of 1 Items

Switch Name ^	CPU ID	CPU Name	CON ID	CON Name	Created At	Options
DKM 48-Port	1001	CPU_010198312	3001	CON_010252038	2020-01-13 23:42:10 -0500	⋯

FIGURE 13-13. DETACH CONNECTION SCREEN

13.4 ADD CUSTOM SOURCE

Under Viewer, click “Make a Connection” and select one or multiple sources from the list of available sources to activate, which will create connections with the selected sources.

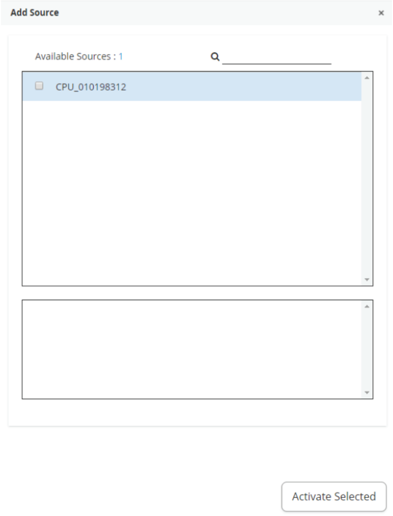


FIGURE 13-14. ADD CUSTOM SOURCE SCREEN

Once these connections are listed, each connection needs at least one destination added to form a functional connection.

Connections have the following options:

1. Detach Source: Break the connection by detaching the source.
2. Detach Destination: Break the connection by detaching the destination.
3. Add Destination: Add additional destinations to the source, e.g. if you wish to share the source.

You also have the option of saving the current connections in the Viewer as a preset via “Save Snapshot.” Save Snapshot is located under “Manage Presets.”

Active connections are listed under the Connections link. Each connection has the option of remotely disconnecting it.

13.5 PRESETS

Under Viewer, click “Manage Presets,” then click “Create Custom” and select one or more available sources.

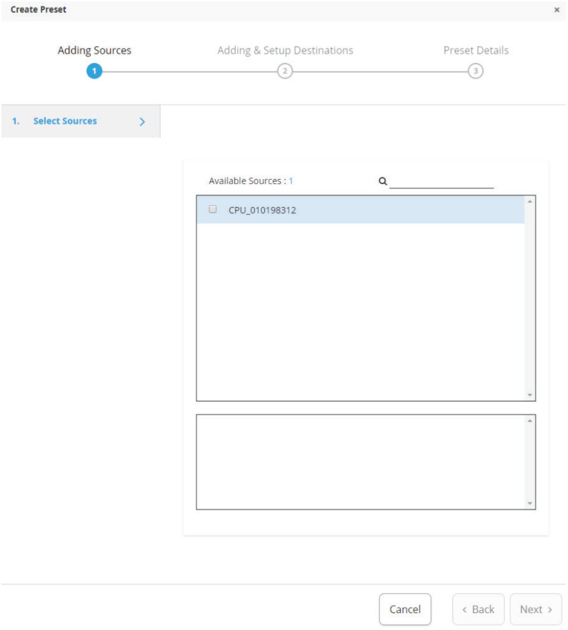


FIGURE 13-15. CREATE CUSTOM PRESETS

Next, select one or more destinations from the list of available destinations.

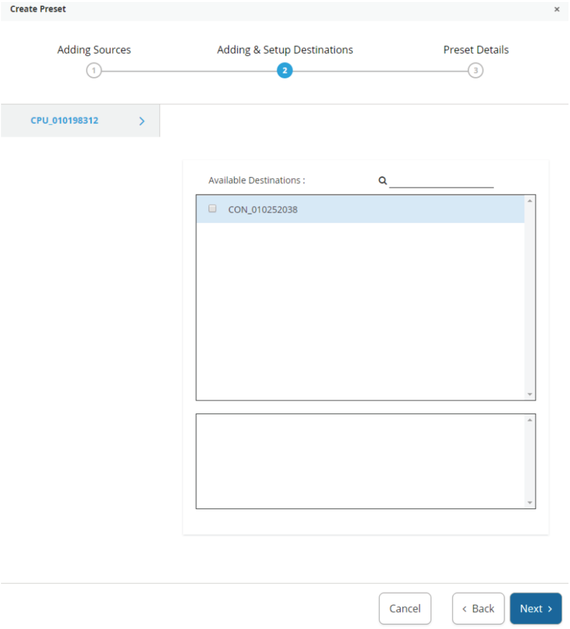


FIGURE 13-16. SELECT DESTINATIONS

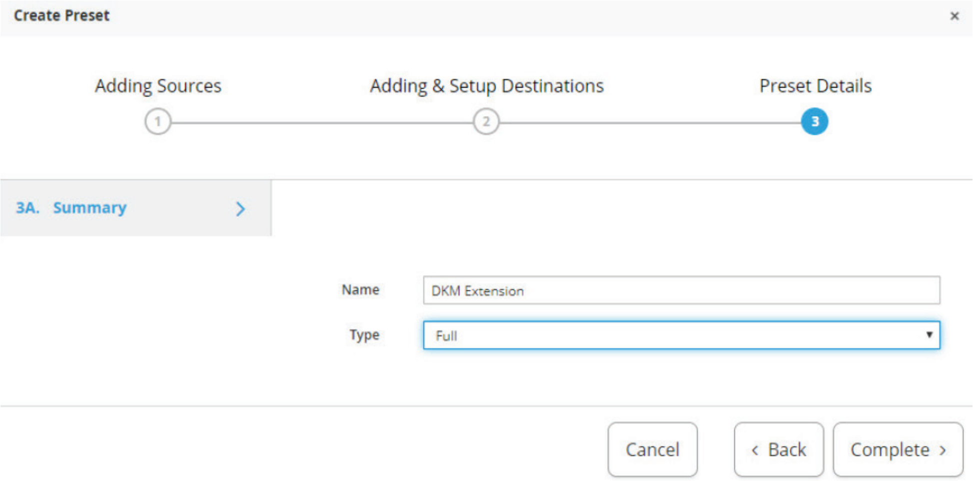
Now enter the name for the preset and choose the type of preset you want.

Both preset types will forcibly take any CONs and CPUs required to establish their configuration, i.e., if those CONs and CPUs are already in active connections then these connections will be broken.

The partial type applies only to the specific CONs and CPUs that are selected in this preset type.

The full type is applied to all the CONS and CPUS. Any CONs and CPUs not selected in this preset type will become inactive when this preset is launched.

Click “Complete” to save the preset.



Name: DKM Extension

Type: Full

FIGURE 13-17. PRESETS SCREEN

The following methods are available to activate presets:

1. Direct preset activation in the Viewer: The first three presets (ordered by creation) are presented directly in the Viewer and can be activated with a direct click.

2. Activation via Manage Presets: All presets can be activated with the “Activate Selected” option in “Manage Presets.” This is mandatory for any preset that is the fourth or later one created, as there is no other method to activate these presets from within Boxilla®.

Connections started via Presets will be displayed in the work area with the following options:

1. Detach Source: Break the connection by detaching the source.

2. Detach Destination: Break the connection by detaching the destination.

3. Add Destination: Add additional destinations to the source, e.g., if you wish to share the source.

Deselect a source/destination

To disconnect a connection while active status , click on ‘x’ on either destination / source (in case of one to one only). The “x” only is visible when you move your mouse over the source or destination.

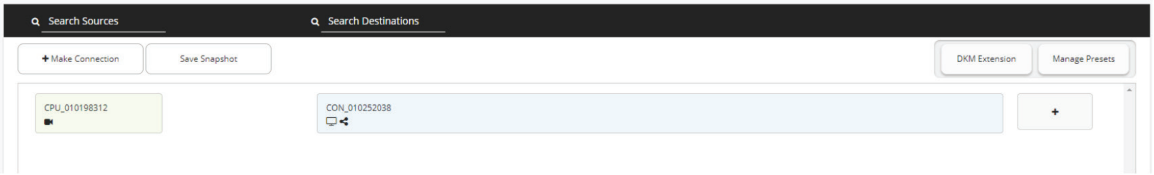
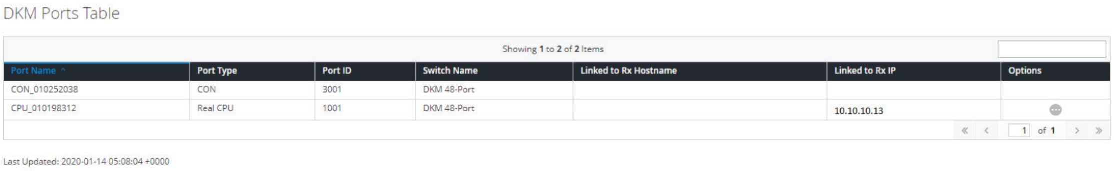


FIGURE 13-18. DESELECT A SOURCE/DESTINATION

13.6 ATTACHING VIRTUAL CPUS TO AN EMERALD RX

Virtual CPU based connections from a DKM switch can be connected directly to a managed Emerald RX on Boxilla® by attaching them.



DKM Ports Table

Showing 1 to 2 of 2 Items

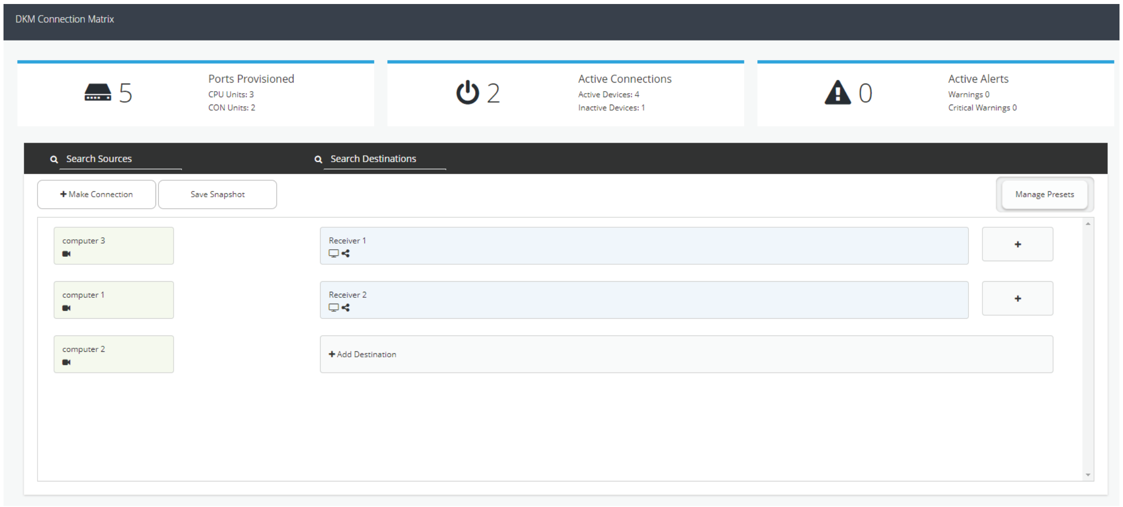
Port Name ^	Port Type	Port ID	Switch Name	Linked to Rx Hostname	Linked to Rx IP	Options
CON_010252038	CON	3001	DKM 48-Port			
CPU_010198312	Real CPU	1001	DKM 48-Port		10.10.10.13	⋯

« ‹ 1 of 1 › »

Last Updated: 2020-01-14 05:08:04 +0000

FIGURE 13-19. VIRTUAL CPUS CONNECTED TO EMERALD SCREEN

In the DKM Viewer within the Boxilla manager web interface, the administrator can view, create, and break DKM and Emerald connections.



DKM Connection Matrix

5 Ports Provisioned
CPU Units: 3
CON Units: 2

2 Active Connections
Active Devices: 4
Inactive Devices: 1

0 Active Alerts
Warnings 0
Critical Warnings 0

FIGURE 13-20. CONNECTIONS SCREEN

To make a new connection, click on the “Make Connection” button.

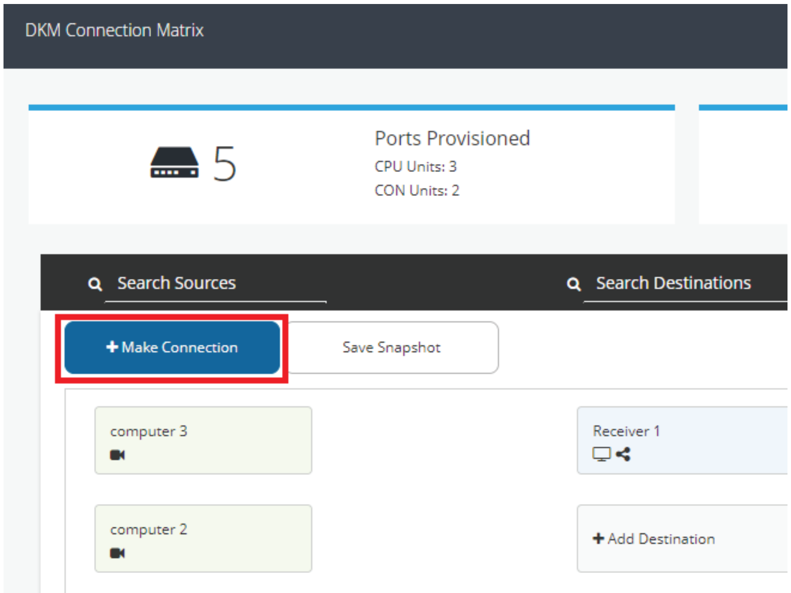


FIGURE 13-21. MAKE CONNECTION BUTTON

Select the DKM Transmitter that you want to connect with on the first page.

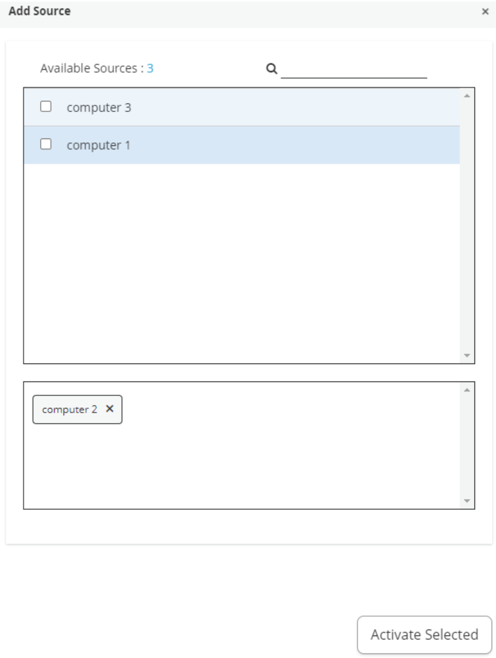


FIGURE 13-22. ADD SOURCE SCREEN

A new connection template will be created as seen in the next image:

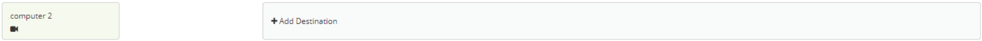


FIGURE 13-23. NEW CONNECTION TEMPLATE

Now click on the “Add Destination” button to connect an Emerald Receiver with the DKM target.

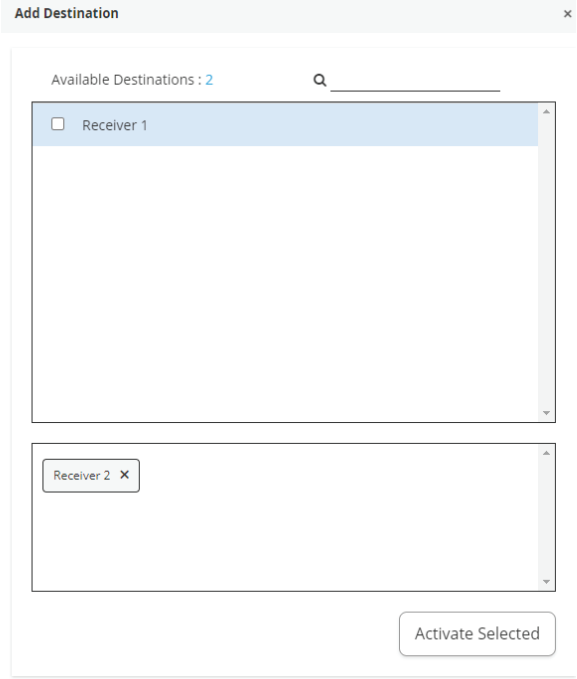


FIGURE 13-24. ADD DESTINATION SCREEN

Once the connection is made, the DKM Viewer page will be updated to show the new connection that was made.

To break any DKM connections, move the mouse over the Destination box and click on the “X” icon.

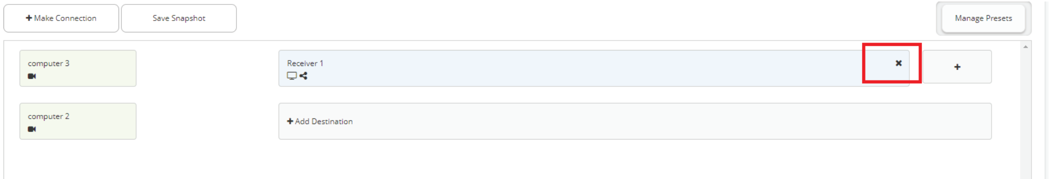


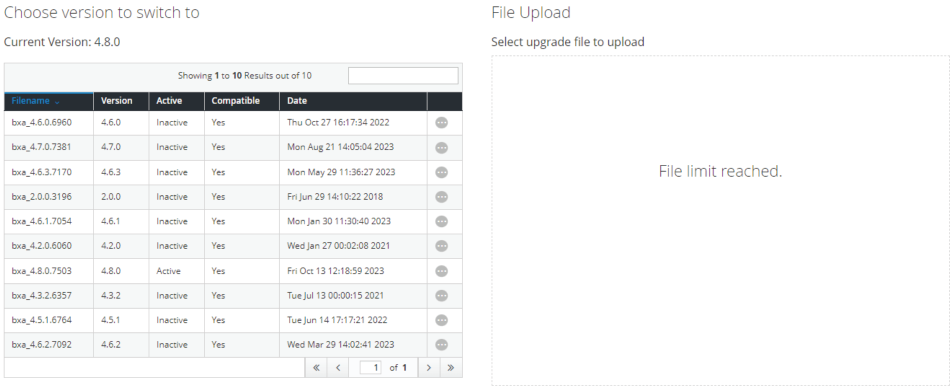
FIGURE 13-25. X ICON

CHAPTER 14: SYSTEM

14.1 SYSTEM —> ADMINISTRATION

The System button in the main menu brings up Administration and Setting pages. These pages allow the Boxilla® Administrator to configure and manage the Boxilla system. The following settings can be configured under System:

- Upgrade the Boxilla firmware:



Choose version to switch to

Current Version: 4.8.0

Showing **1** to **10** Results out of 10

Filename	Version	Active	Compatible	Date
bxa_4.6.0.6960	4.6.0	Inactive	Yes	Thu Oct 27 16:17:34 2022
bxa_4.7.0.7381	4.7.0	Inactive	Yes	Mon Aug 21 14:05:04 2023
bxa_4.6.3.7170	4.6.3	Inactive	Yes	Mon May 29 11:36:27 2023
bxa_2.0.0.3196	2.0.0	Inactive	Yes	Fri Jun 29 14:10:22 2018
bxa_4.6.1.7054	4.6.1	Inactive	Yes	Mon Jan 30 11:30:40 2023
bxa_4.2.0.6060	4.2.0	Inactive	Yes	Wed Jan 27 00:02:08 2021
bxa_4.8.0.7503	4.8.0	Active	Yes	Fri Oct 13 12:18:59 2023
bxa_4.3.2.6357	4.3.2	Inactive	Yes	Tue Jul 13 00:00:15 2021
bxa_4.5.1.6764	4.5.1	Inactive	Yes	Tue Jun 14 17:17:21 2022
bxa_4.6.2.7092	4.6.2	Inactive	Yes	Wed Mar 29 14:02:41 2023

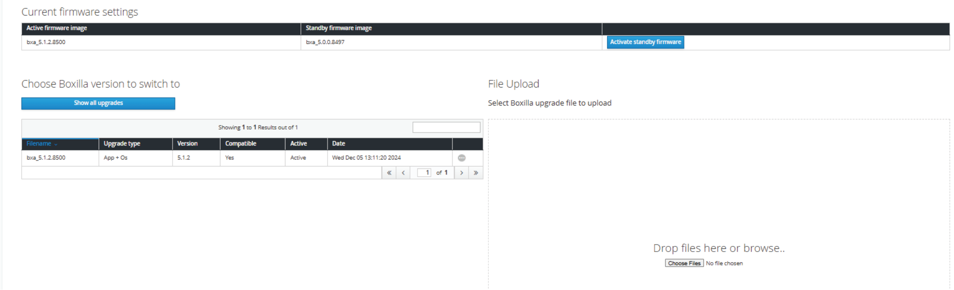
1 of 1

File Upload

Select upgrade file to upload

File limit reached.

FIGURE 14-1. UPGRADE FIRMWARE SCREEN (FIRMWARE EARLIER THAN 5.1.2)



Current firmware settings

Active firmware image	Standby firmware image	
bxa_5.1.2.8500	bxa_5.0.0.8497	Activate standby firmware

Choose Boxilla version to switch to

Showing **1** to **1** Results out of 1

Filename	Upgrade type	Version	Compatible	Active	Date
bxa_5.1.2.8500	App + Os	5.1.2	Yes	Active	Wed Dec 05 13:11:20 2024

1 of 1

File Upload

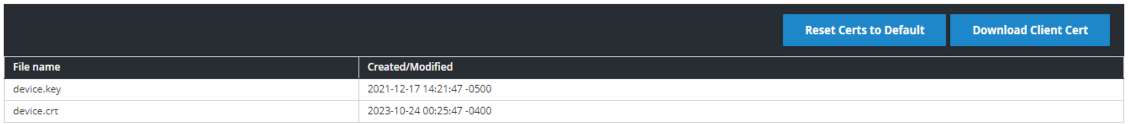
Select Boxilla upgrade file to upload

Drop files here or browse..

No file chosen

FIGURE 14-2. UPGRADE FIRMWARE SCREEN (FIRMWARE 5.1.2)

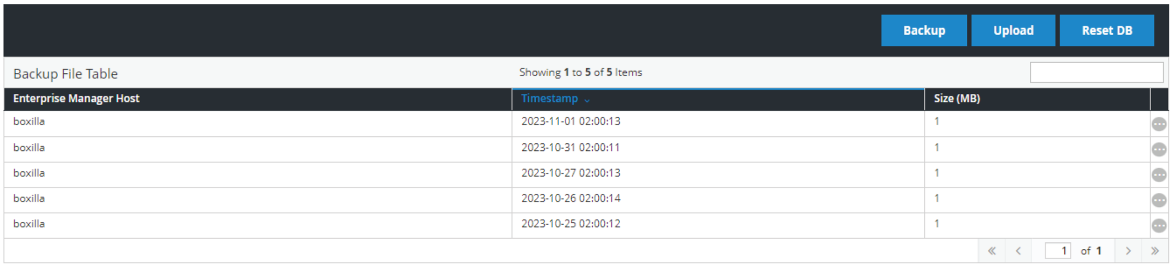
- Reset or Download the Boxilla Certificate:



File name	Created/Modified
device.key	2021-12-17 14:21:47 -0500
device.crt	2023-10-24 00:25:47 -0400

FIGURE 14-3. CERTIFICATE SCREEN

- Back up/Restore the Boxilla® database:



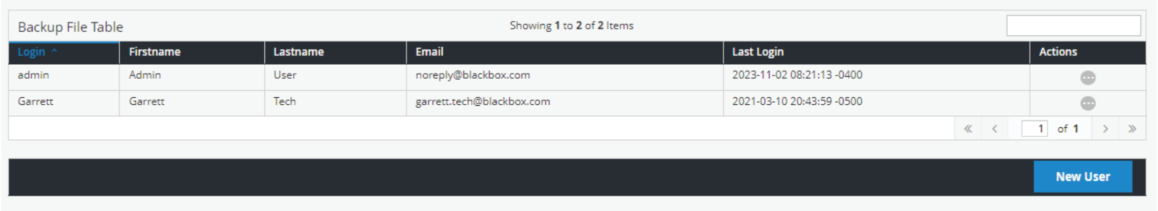
Backup File Table — Showing 1 to 5 of 5 Items

Enterprise Manager Host	Timestamp	Size (MB)
boxilla	2023-11-01 02:00:13	1
boxilla	2023-10-31 02:00:11	1
boxilla	2023-10-27 02:00:13	1
boxilla	2023-10-26 02:00:14	1
boxilla	2023-10-25 02:00:12	1

1 of 1

FIGURE 14-4. BACKUP/RESTORE DATABASE SCREEN

- Manage Boxilla Administrators by adding, editing, or removing them:



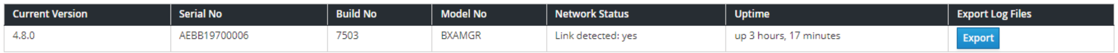
Backup File Table — Showing 1 to 2 of 2 Items

Login	Firstname	Lastname	Email	Last Login	Actions
admin	Admin	User	noreply@blackbox.com	2023-11-02 08:21:13 -0400	
Garrett	Garrett	Tech	garrett.tech@blackbox.com	2021-03-10 20:43:59 -0500	

1 of 1

FIGURE 14-5: BOXILLA USER SCREEN

- Check system information, such as firmware version, serial number, build number, model number, network status, and uptime, and also export Boxilla logs:

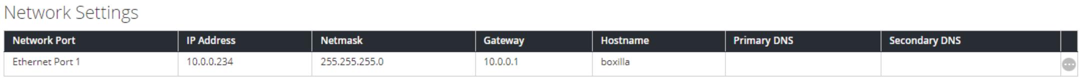


Current Version	Serial No	Build No	Model No	Network Status	Uptime	Export Log Files
4.8.0	AEBB19700006	7503	BXAMGR	Link detected: yes	up 3 hours, 17 minutes	Export

FIGURE 14-6. CHECK SYSTEM INFORMATION SCREEN

14.2 SYSTEM —> SETTINGS

- Configure or change the Boxilla network settings:

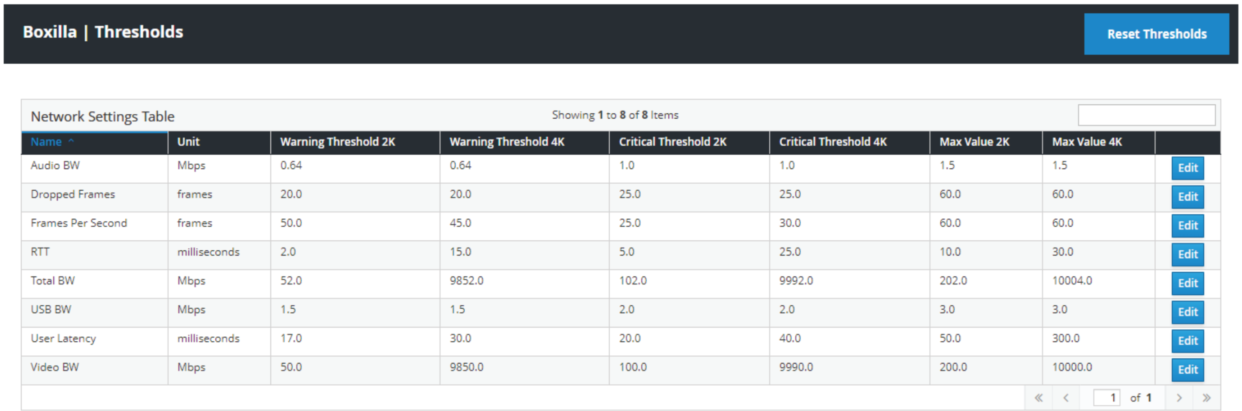


Network Settings

Network Port	IP Address	Netmask	Gateway	Hostname	Primary DNS	Secondary DNS
Ethernet Port 1	10.0.0.234	255.255.255.0	10.0.0.1	boxilla		

FIGURE 14-7: NETWORK SCREEN

- Set and configure thresholds.



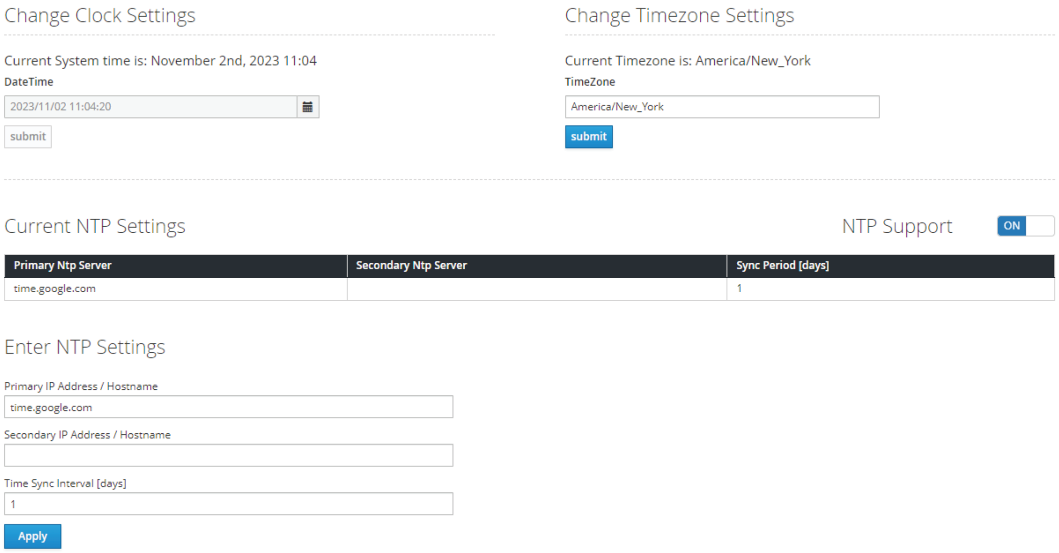
Network Settings Table

Showing **1** to **8** of **8** Items

Name ^	Unit	Warning Threshold 2K	Warning Threshold 4K	Critical Threshold 2K	Critical Threshold 4K	Max Value 2K	Max Value 4K	
Audio BW	Mbps	0.64	0.64	1.0	1.0	1.5	1.5	Edit
Dropped Frames	frames	20.0	20.0	25.0	25.0	60.0	60.0	Edit
Frames Per Second	frames	50.0	45.0	25.0	30.0	60.0	60.0	Edit
RTT	milliseconds	2.0	15.0	5.0	25.0	10.0	30.0	Edit
Total BW	Mbps	52.0	9852.0	102.0	9992.0	202.0	10004.0	Edit
USB BW	Mbps	1.5	1.5	2.0	2.0	3.0	3.0	Edit
User Latency	milliseconds	17.0	30.0	20.0	40.0	50.0	300.0	Edit
Video BW	Mbps	50.0	9850.0	100.0	9990.0	200.0	10000.0	Edit

FIGURE 14-8. SET THRESHOLDS FOR ACTIVE ALERTS SCREEN

- Clock



Change Clock Settings

Current System time is: November 2nd, 2023 11:04

DateTime: 2023/11/02 11:04:20

Change Timezone Settings

Current Timezone is: America/New_York

TimeZone: America/New_York

Current NTP Settings

NTP Support: ON

Primary Ntp Server	Secondary Ntp Server	Sync Period [days]
time.google.com		1

Enter NTP Settings

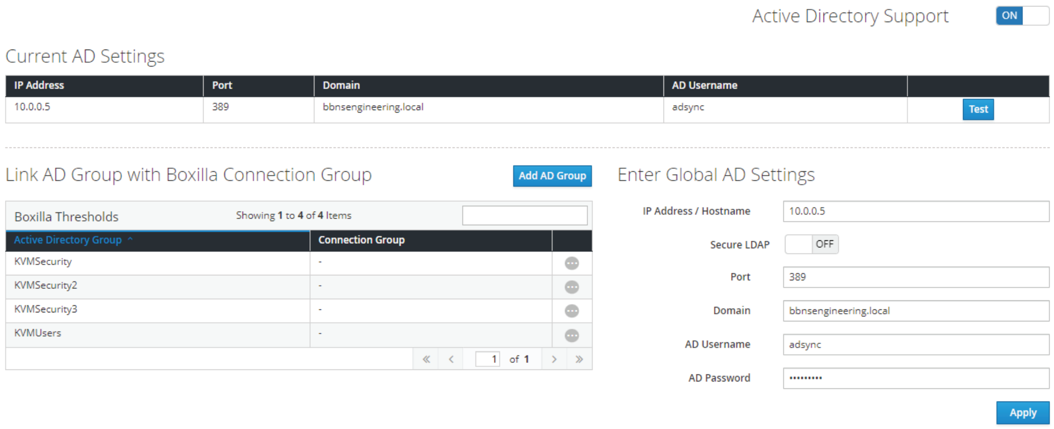
Primary IP Address / Hostname: time.google.com

Secondary IP Address / Hostname:

Time Sync Interval [days]: 1

FIGURE 14-9. CLOCK

- Active Directory allows for the configuration of an AD server using LDAP or LDAPS



Active Directory Support ON

Current AD Settings

IP Address	Port	Domain	AD Username	
10.0.0.5	389	bbnsengineering.local	adsync	Test

Link AD Group with Boxilla Connection Group

Add AD Group

Boxilla Thresholds — Showing 1 to 4 of 4 Items

Active Directory Group ^	Connection Group	
KVMSecurity	-	⋯
KVMSecurity2	-	⋯
KVMSecurity3	-	⋯
KVMUsers	-	⋯

« ‹ 1 of 1 › »

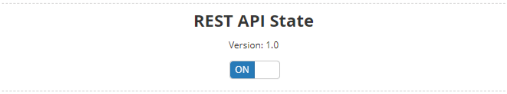
Enter Global AD Settings

IP Address / Hostname	10.0.0.5
Secure LDAP	OFF
Port	389
Domain	bbnsengineering.local
AD Username	adsync
AD Password	•••••••••

Apply

FIGURE 14-10. ACTIVE DIRECTORY

- RESTapi



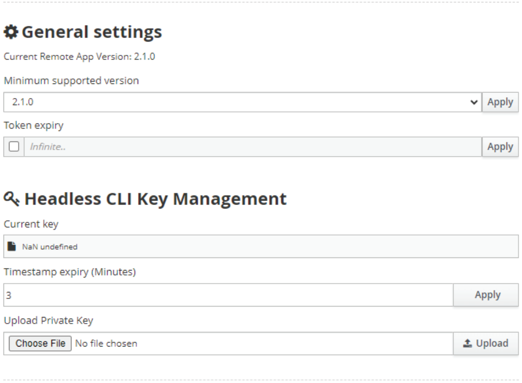
REST API State

Version: 1.0

ON

FIGURE: 14-11. REST API

- Minimum Support for RemoteApp allows for the configuration of the RA version to be used with the system along with a timeout option. Headless CLI key management is also available for configuration.



General settings

Current Remote App Version: 2.1.0

Minimum supported version

2.1.0 — Apply

Token expiry

□ Infinite.. — Apply

Headless CLI Key Management

Current key

NaN undefined

Timestamp expiry (Minutes)

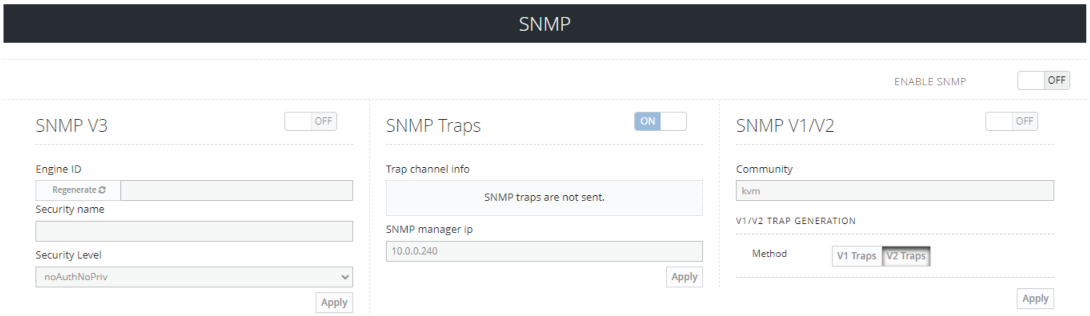
3 — Apply

Upload Private Key

Choose File No file chosen — Upload

FIGURE 14-12. REMOTE APP

- SNMP



SNMP

ENABLE SNMP OFF

SNMP V3 OFF

Engine ID: Regenerate

Security name:

Security Level: noAuthNoPriv

Apply

SNMP Traps ON

Trap channel info: SNMP traps are not sent.

SNMP manager ip: 10.0.0.240

Apply

SNMP V1/V2 OFF

Community: kvm

V1/V2 TRAP GENERATION

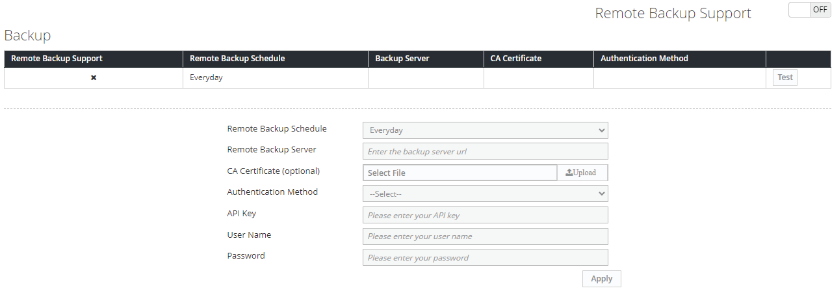
Method: V1 Traps [✓ V2 Traps]

Apply

FIGURE 14-13. SNMP

- Remote Backup Support

Remote Backup Support can be configured to support remote backups for the Boxilla® system, which allows the backup file to be sent to a remote server instead of being stored locally on the Boxilla.



Remote Backup Support OFF

Backup

Remote Backup Support	Remote Backup Schedule	Backup Server	CA Certificate	Authentication Method	
✖	Everyday				Test

Remote Backup Schedule: Everyday

Remote Backup Server: Enter the backup server url

CA Certificate (optional): Select File | Upload

Authentication Method: --Select--

API Key: Please enter your API key

User Name: Please enter your user name

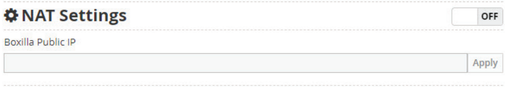
Password: Please enter your password

Apply

FIGURE 14-14. REMOTE BACKUP SUPPORT

- NAT

If Boxilla will communicate with endpoints on different networks over a NAT, this parameter can be enabled and configured using the external IP address assigned to Boxilla so that it can communicate with appliances not on the same network.



NAT Settings OFF

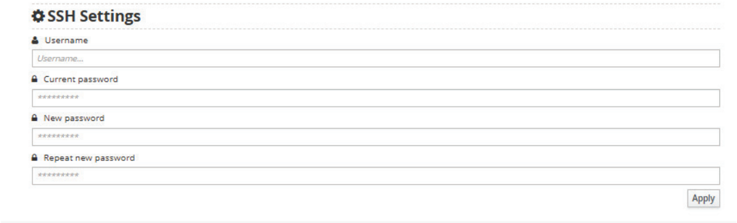
Boxilla Public IP:

Apply

FIGURE 14-15. SYSTEM SCREEN—NAT SETTINGS

- SSH

Change the default SSH settings for security scanning. If the default credentials are needed in order to change the default SSH password, contact Black Box technical support.



SSH Settings

Username

Username...

Current password

****

New password

****

Repeat new password

****

FIGURE 14-16. SSH SETTINGS

- Reboot

The administrator can reboot the Boxilla® unit by clicking on the Reboot button on the top right of the System —> Administration screen.

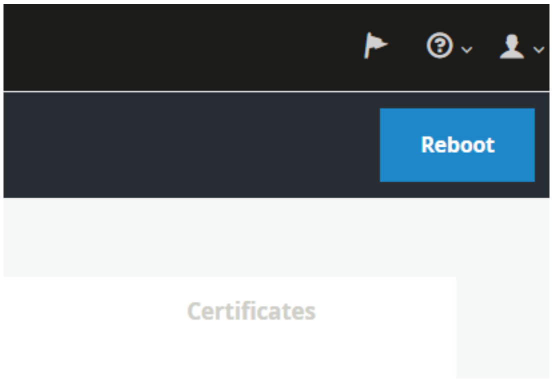


FIGURE 14-17. SYSTEM SCREEN—UPGRADE

14.3 SYSTEM—UPGRADING BOXILLA UNIT FIRMWARE

To upgrade the firmware on the Boxilla unit, choose the file to be used to upgrade and click on submit and follow the instructions provided. This will cause the new firmware to be added to the Backup Image table (i.e., the firmware file is copied onto the Boxilla unit). To initiate the upgrade of the the Boxilla unit, click on Activate on ellipsis "•••" icon options on the row of the firmware to be used to upgrade the unit.

NOTE: Boxilla supports the uploading and storage of a maximum of 10 Boxilla upgrade images.

The upgrade will not change the contents of the database. If you are upgrading to Boxilla 1.2 from a Boxilla 1.0, 1.0.1, or 1.1 unit, you will need to reboot the Boxilla unit when the upgrade is completed.

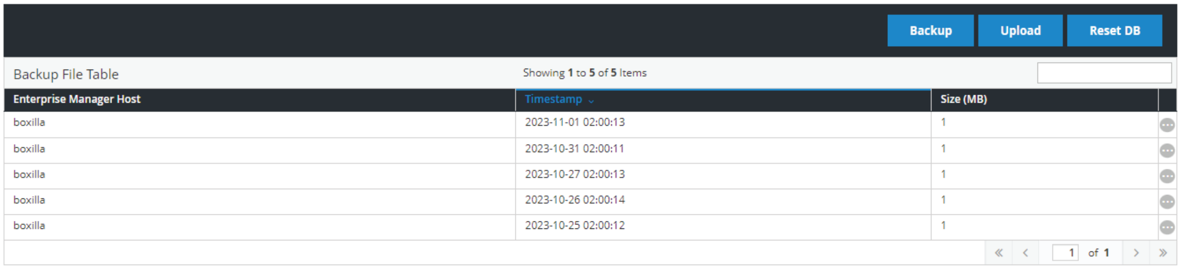
VERY IMPORTANT: Ensure the Boxilla unit stays powered-up during the upgrade. Losing power during an upgrade may cause the unit to cease functioning.

14.4 SYSTEM—BACKUP/RESTORE

The Administrator can backup and restore the database of the Boxilla unit on the Backup/Restore tab on the System screen.

When the Backup button is clicked, a complete backup of the Boxilla unit is created and added to the Backup table with a timestamp. This file is still on the Boxilla® unit. To save this backup file to your local system, click on Download using the ellipsis "•••" icon found next to the specific backup.

The Boxilla will automatically back up the database nightly, and the files are stored locally on the unit for up to 8 days. Additionally, the Boxilla 4.6.1 and later adds an option for Remote Backup Support located at System -> Settings -> Backup. The administrator can also push the Boxilla backup out to an external server using RESTapi commands.



Backup File Table

Showing 1 to 5 of 5 Items

Enterprise Manager Host	Timestamp ⌄	Size (MB)	
boxilla	2023-11-01 02:00:13	1	•••
boxilla	2023-10-31 02:00:11	1	•••
boxilla	2023-10-27 02:00:13	1	•••
boxilla	2023-10-26 02:00:14	1	•••
boxilla	2023-10-25 02:00:12	1	•••

« ‹ 1 of 1 › »

FIGURE 14-18. SYSTEM BACKUP/RESTORE TAB

There is a two-step process to restore a Boxilla unit from an external backup file. First the file must be uploaded to the Backup table and then the backup file in the table must be imported into the Boxilla unit.

When the Upload button is clicked, the administrator is prompted for the filename to upload into the Backup Table. Once the upload has been completed, the administrator clicks on Import using the ellipsis "•••" icon found next to the specific backup.

Clicking on ResetDB purges the database on the Boxilla unit and restores it to a default state. The IP address will not be changed when using the ResetDB option.

The Enterprise Manager Host column refers to the name of the host machine where the backup was generated. Currently, this will always be this Boxilla unit.

14.5 SYSTEM —SYSTEM INFO

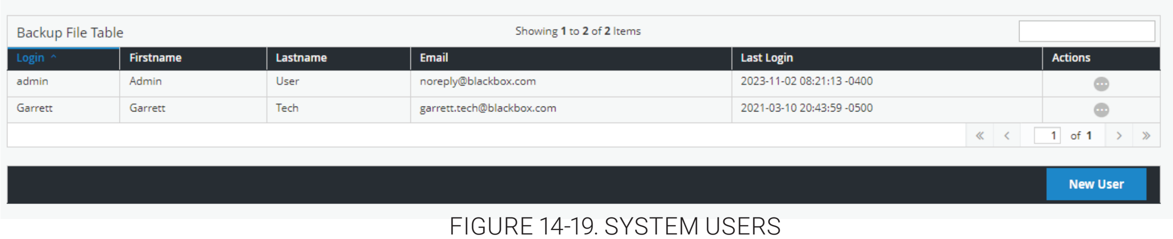
The System Info tab provides summary information on the Boxilla unit. This information is:

- Current Version: Version of firmware currently running on the Boxilla Unit.
- Serial No: The serial number of the Boxilla unit.
- Build No: The software build number (internal Black Box number to software control of firmware on the Boxilla unit).
- Model No: The model number of the Boxilla unit (internal Black Box number to indicate hardware version on Boxilla unit).
- Network Status: Whether Boxilla is active on the network.
- Uptime: Length of time that the Boxilla unit has been powered up.
- Export Log files: allows the administrator to export log files from the Boxilla unit.

14.6 SYSTEM — ADMINISTRATION — BOXILLA USERS

The System —> Administration — Boxilla Users tab shows a table of users for the Boxilla unit (not the same as users for the managed domain) as shown below, System Users. The users here should be considered Adminstrative users.

NOTE: Users can not be imported from Active Directory here, and only internal Boxilla users can be created and used.

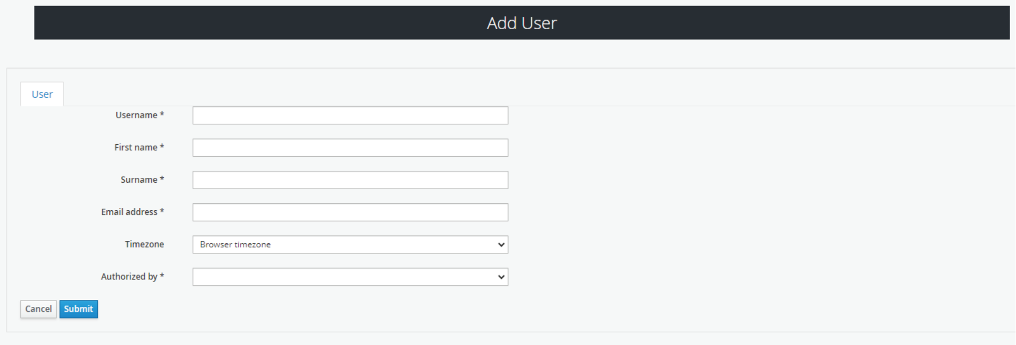


Backup File Table

Showing **1** to **2** of **2** Items

Login ^	Firstname	Lastname	Email	Last Login	Actions
admin	Admin	User	noreply@blackbox.com	2023-11-02 08:21:13 -0400	⋯
Garrett	Garrett	Tech	garrett.tech@blackbox.com	2021-03-10 20:43:59 -0500	⋯

FIGURE 14-19. SYSTEM USERS



Add User

User

Username *	
First name *	
Surname *	
Email address *	
Timezone	Browser timezone
Authorized by *	

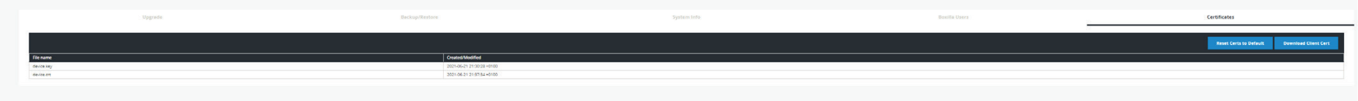
FIGURE 14-20. NEW SYSTEM USER

Enter Username, First name, Surname, Email address, Language, Time zone, and Authorized by. Then click Submit to save your changes or Cancel to cancel your entries.

14.7 CERTIFICATES

14.7.1 DOWNLOAD THE CLIENT CERTIFICATE

The Boxilla® administrator can download the Client Certificate so it can be imported into a web browser to support a secure connection (i.e. green security lock). When the Download Client Cert is clicked on, Boxilla will automatically generate the .pem file for the user and download the file to the local Downloads folder. In a cluster environment, the .pem file will support the configured Virtual IP address together with the IP addresses of the Active & Standby Boxilla units.



File name	Created/Modified
device.key	2021-06-21 21:30:28 +0100
device.crt	2021-06-21 21:37:34 +0100

FIGURE 14-21. CERTIFICATES BUTTONS

Method for Importing CA Certificate (PEM format) to Client Windows PC (Recommended)

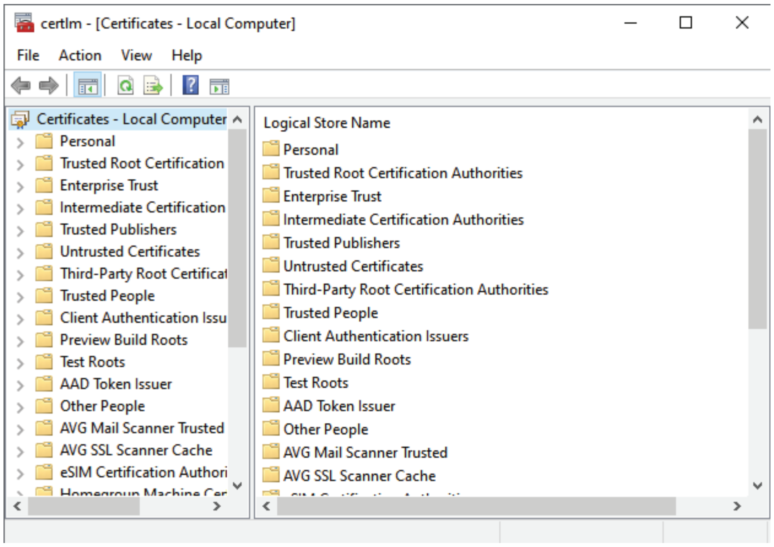
After the CA certificate is properly re-generated, users need to import it to the Trusted Root CA Certificate Store of the client PC so that any SSL connection from the client PC (via browser, Emerald remote app, etc.) to Boxilla would be secured.

For Windows platforms, the Trusted Root CA Certificate Store is configured by the Certificate Manager of Windows under both the “Current User” and the “Current Local Machine” User Access Control levels. When the CA certificate is imported into Chrome and IE/Edge browsers, the certificate is configured within the “Current User” Trusted Root CA Certificate Store that works for the current Windows user logged in only. If an alternate Windows user logs onto the PC, the CA certificate would NOT be present within the associated Trusted Root CA Certificate Store, and the SSL connections to Boxilla in this case would NOT be secured.

For this reason, we recommend that users import the CA certificate PEM file to the "Current Local Machine" Trusted Root CA Certificate Store, so that all Windows users of the PC are able to have the CA certificate configured in their own Trusted Root CA Certificate Stores.

The steps to import the CA certificate to "Current Local Machine" Trusted Root CA Certificate Store are as follows:

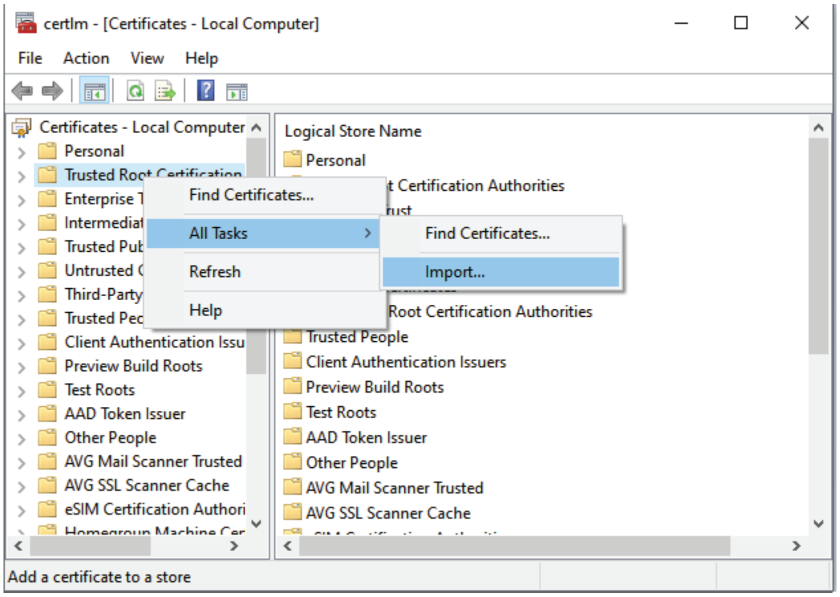
Step 1. In the client Windows PC, click the search button on the task bar and type in "Manage computer certificates", and then click the matching option within the menu and open the "Current Local Machine" Trusted RootCA Certificate Store in control panel. (In comparison, the option "Manage user certificates" is for the "Current User" Certificate Store):



Logical Store Name
Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Client Authentication Issuers
Preview Build Roots
Test Roots
AAD Token Issuer
Other People
AVG Mail Scanner Trusted
AVG SSL Scanner Cache

FIGURE 14-22. STEP 1

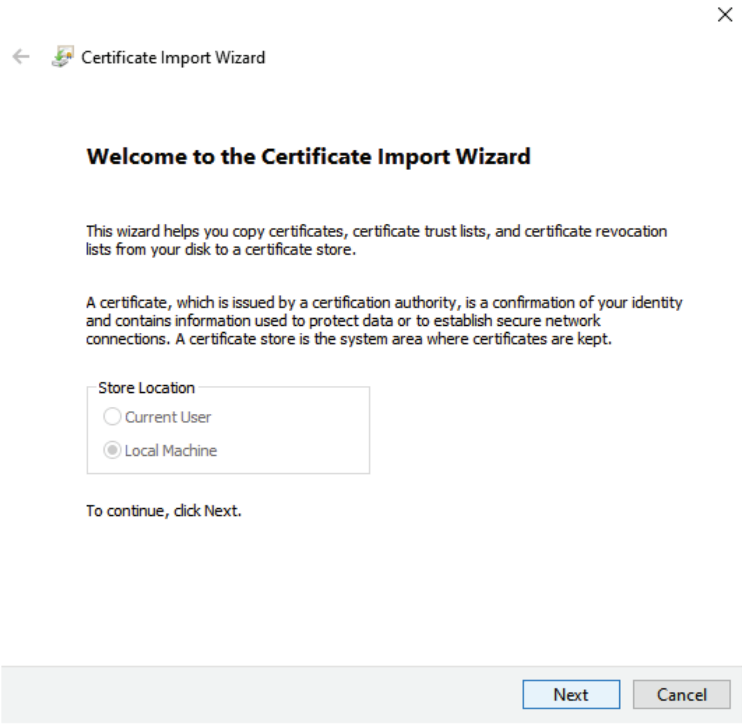
Step 2. In the certificate store, right click "Trusted Root Certification Authorities" -> "Certificates" and select "All Tasks" -> "Import"



Logical Store Name
Personal
t Certification Authorities
rust
Root Certification Authorities
Trusted People
Client Authentication Issuers
Preview Build Roots
Test Roots
AAD Token Issuer
Other People
AVG Mail Scanner Trusted
AVG SSL Scanner Cache

Add a certificate to a store

FIGURE 14-23. STEP 2



Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location

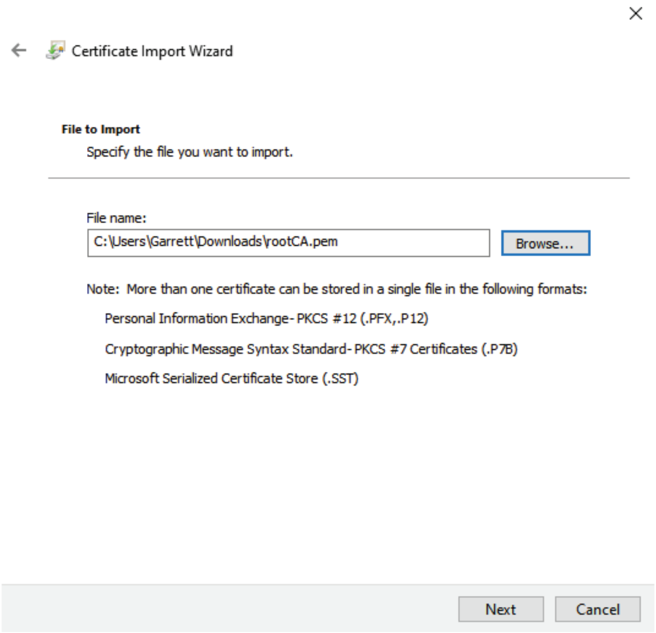
○ Current User

● Local Machine

To continue, click Next.

FIGURE 14-24. STEP 3

Step 3. In the wizard window, click “Next” and then select the re-generated CA certificate PEM file from local path:



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name: C:\Users\Garrett\Downloads\rootCA.pem

Note: More than one certificate can be stored in a single file in the following formats:

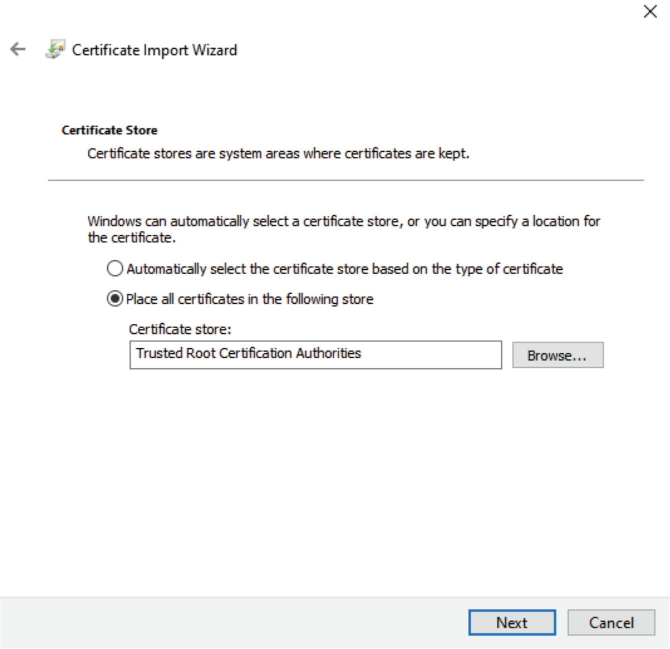
Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

FIGURE 14-25. STEP 3

Step 4. Click "Next" and in the next wizard window, making sure that the specified certificate store is "Trusted Root Certification Authorities" instead of letting Windows automatically select the certificate store based on the certificate type, before going forward:



Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

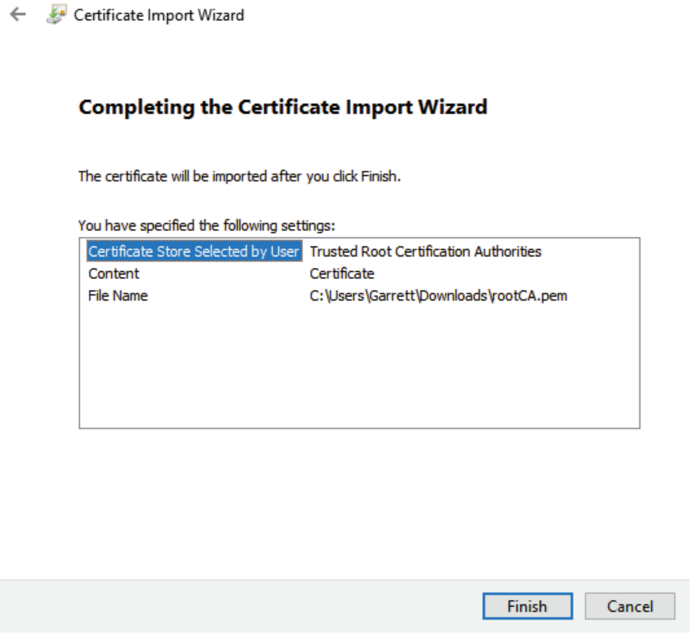
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

FIGURE 14-26. STEP 4

Step 5. Click "Next" to redirect to the completing wizard window, and then click "Finish"



Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate
File Name	C:\Users\Garrett\Downloads\rootCA.pem

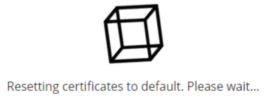
FIGURE 14-27. STEP 5

The re-generated CA certificate should be successfully imported to the certificate store for "Current Local Machine" now, and SSL connections from the client Windows PC should be secured for any Windows users.

The browser session to Boxilla should be secured without the additional need for importing the CA certificate to the browsers anymore, as described in the last section.

14.7.2 RESET CERTIFICATES TO DEFAULT

The Boxilla® Administrator can also select the Reset the Certificate to Default option if they believe the certificates within Boxilla are not correct.



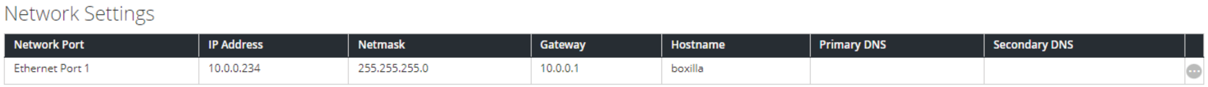
Resetting certificates to default. Please wait...

FIGURE 14-28. RESETTING CERTIFICATES TO DEFAULT

14.8 SYSTEM—SETTINGS—NETWORK

The System —> Settings —> Network tab shows the IP settings for the Boxilla unit and enables the Administrator to change the IP settings for the Boxilla unit (enter IP address, Net Mask, Gateway, and DNS in IPv4 format and click Apply). The second Ethernet port is disabled by default. Also note when setting up a Primay / Backup Boxilla that if the Primary Ethernet 2 is enabled, it must also be enabled on the Backup, otherwise they will fail to link together.

NOTE: Ethernet Port 2 is disabled by default.



Network Settings

Network Port	IP Address	Netmask	Gateway	Hostname	Primary DNS	Secondary DNS	
Ethernet Port 1	10.0.0.234	255.255.255.0	10.0.0.1	boxilla			⋯

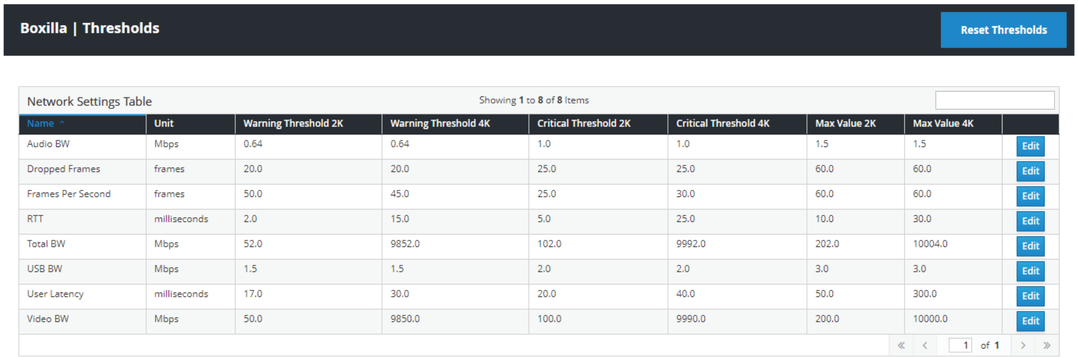
FIGURE 14-29 SYSTEM —> SETTINGS —> NETWORK SCREEN

IMPORTANT: If enabling the secondary network port of Boxilla, you must not use the 192.168.1.x/24 range even if the primary interface does not use it.

NOTE: Ethernet Port 2 does not support KVM traffic. All KVM traffic is routed through Ethernet Port 1.

14.9 SYSTEM — SETTINGS —THRESHOLDS

The System —> Settings—> Threshold tab shows the level used to define an alert for various measurements recorded on a connection and enables the Administrator to change them.



Network Settings Table

Showing 1 to 8 of 8 Items

Name ^	Unit	Warning Threshold 2K	Warning Threshold 4K	Critical Threshold 2K	Critical Threshold 4K	Max Value 2K	Max Value 4K	
Audio BW	Mbps	0.64	0.64	1.0	1.0	1.5	1.5	Edit
Dropped Frames	frames	20.0	20.0	25.0	25.0	60.0	60.0	Edit
Frames Per Second	frames	50.0	45.0	25.0	30.0	60.0	60.0	Edit
RTT	milliseconds	2.0	15.0	5.0	25.0	10.0	30.0	Edit
Total BW	Mbps	52.0	9852.0	102.0	9992.0	202.0	10004.0	Edit
USB BW	Mbps	1.5	1.5	2.0	2.0	3.0	3.0	Edit
User Latency	milliseconds	17.0	30.0	20.0	40.0	50.0	300.0	Edit
Video BW	Mbps	50.0	9850.0	100.0	9990.0	200.0	10000.0	Edit

FIGURE 14-30. ALERT THRESHOLDS

The Warning Threshold sets the level above which a measurement must be below to be classified as normal or at "info" level. Measurements above the Warning Threshold and below Critical Threshold are classified as at "Warning" level. Measurements at or above the Critical Threshold are classified as "Critical" level. The following alert settings show the default configuration but can be adjusted by a system administrator.

- 2K AUDIO BANDWIDTH: WARNING: 0.64; CRITICAL: 1.0; MAX: 1.5
- 4K AUDIO BANDWIDTH: WARNING: 0.64; CRITICAL: 1.0; MAX: 1.5

- 2K DROPPED FRAMES: WARNING: 20; CRITICAL: 25; MAX: 60
- 4K DROPPED FRAMES: WARNING: 20; CRITICAL 25; MAX: 60

- 2K FRAMES PER SECOND: WARNING: 50; CRITICAL 25; MAX: 60
- 4K FRAMES PER SECOND: WARNING: 45; CRITICAL: 30; MAX 60

- 2K RTT: WARNING: 2; CRITICAL: 5; MAX: 10
- 4K RTT: WARNING: 15; CRITICAL: 25; MAX: 30

- 2K TOTAL BANDWIDTH: WARNING: 52; CRITICAL: 102; MAX: 202
- 4K TOTAL BANDWIDTH: WARNING: 9852; CRITICAL: 9992.0; MAX:10004

- 2K USB BANDWIDTH: WARNING: 1.5; CRITICAL: 2.0; MAX: 3.0
- 4K USB BANDWIDTH: WARNING: 1.5; CRITICAL: 2.0; MAX: 3.0

- 2K USER LATENCY: WARNING: 17; CRITICAL: 20; MAX: 50
- 4K USER LATENCY: WARNING: 30; CRITICAL: 40; MAX: 300

- 2K VIDEO BANDWIDTH: WARNING: 50; CRITICAL: 100; MAX: 200
- 4K VIDEO BANDWIDTH: WARNING: 9850; CRITICAL: 9990; MAX: 10000

In an existing deployment, these values are updated via the 'Reset Threshold's' button.

Clarification on Frames Per Second (FPS) Alert:

A Critical FPS Alert is generated when the Frames Per Second value drops below the critical value AND the Dropped Frames value goes above the critical value a FPS critical alert is generated.

A Warning FPS Alert is generated when the Frames Per Second value drops below the warning value AND the Dropped Frames value goes above the warning value a FPS warning alert is generated.

The color coding on graphs and tables for measurements (such as Bandwidth) follow these rules:

- Info Level (or normal level): color set as Green
- Warning Level: color set as Amber
- Critical Level : color set as Red

14.10 SYSTEM — SETTINGS — CLOCK

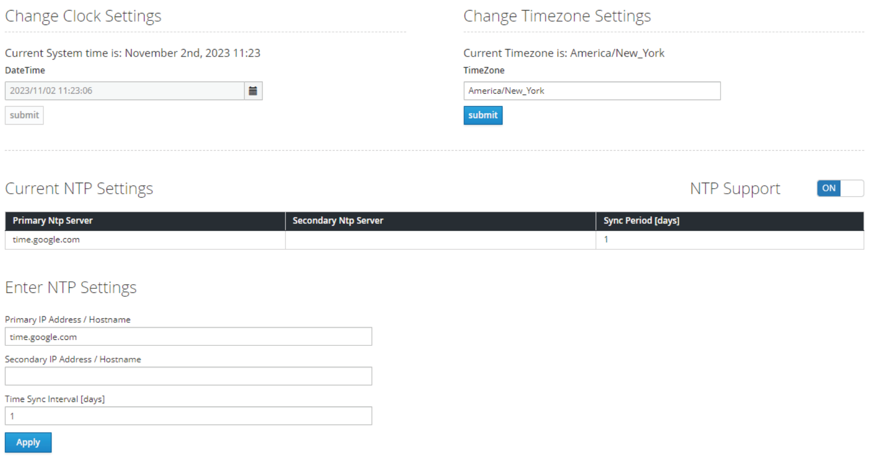
The System —> Settings —> Clock tab enables the Administrator to see the current system time and to change it.

There are two options for the Clock.

1. Manually configure time, time is not maintained.

2. Use NTP Server to set and maintain time.

Time Zone setting can be applied to both options above.



Change Clock Settings

Current System time is: November 2nd, 2023 11:23

DateTime: 2023/11/02 11:23:06

Change Timezone Settings

Current Timezone is: America/New_York

TimeZone: America/New_York

Current NTP Settings

NTP Support: ON

Primary Ntp Server	Secondary Ntp Server	Sync Period [days]
time.google.com		1

Enter NTP Settings

Primary IP Address / Hostname: time.google.com

Secondary IP Address / Hostname:

Time Sync Interval [days]: 1

FIGURE 14-31. CLOCK (OR TIME) SETTINGS

14.11 SYSTEM — SETTINGS— ACTIVE DIRECTORY

Active Directory is a Directory Services implementation that allows for user/group authentication, group policies etc. LDAP (lightweight Directory Access Protocol) is a cross platform protocol used for such directory services authentication. The Boxilla® also supports Secure LDAP which can allow the LDAPS protocol or StartTLS to be used if using a Boxilla at firmware 4.6 or later.

14.11.1 ADMIN USER ENABLING ACTIVE DIRECTORY ON BOXILLA

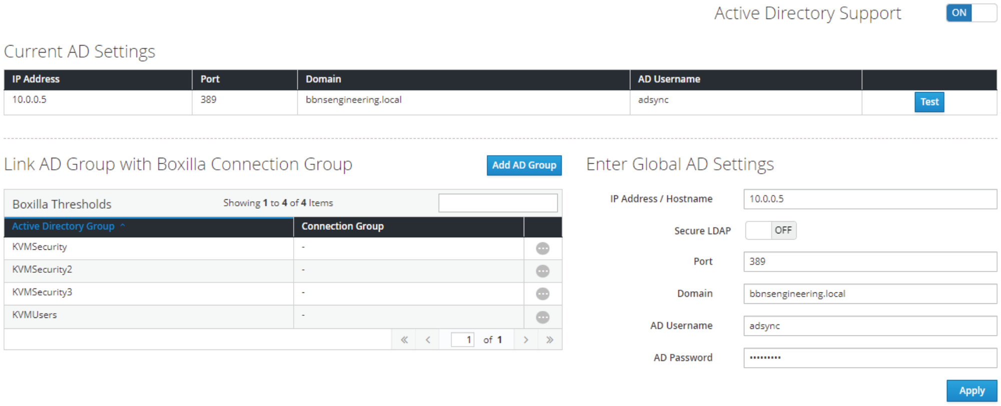
The Boxilla administrator can enable Active Directory for the KVM Network by enabling Active Directory authentication by switching the option ON/OFF under System -> Settings -> Active Directory tab

Boxilla can support the Active Directory Organizational Units/Security Groups as active group types. They need to be manually added and use the same naming convention that is on the server hosting Active Directory.

To enable Active Directory support on Boxilla:

1. In System -> Settings -> Active Directory tab, you will see the ON/OFF switch, which needs to be ON to globally enable Active Directory support.
2. You then need to enter the Active Directory server details. Secure LDAP setting (if required), IP, Port (by default this is 389), the domain of the active directory server, and the AD Username and AD Password, which are any administrator account on Active Directory. This account is not used for authentication and is used to retrieve OU information for the users in Boxilla.

3. You then save your settings and Boxilla is set up for Active Directory support.
4. The Boxilla should automatically import all AD Groups into the table on the same page for easy access of management.



Active Directory Support ON

Current AD Settings

IP Address	Port	Domain	AD Username	
10.0.0.5	389	bbnsengineering.local	adsync	Test

Link AD Group with Boxilla Connection Group — Add AD Group

Boxilla Thresholds — Showing 1 to 4 of 4 Items

Active Directory Group ^	Connection Group
KVMSecurity	-
KVMSecurity2	-
KVMSecurity3	-
KVMUsers	-

Enter Global AD Settings

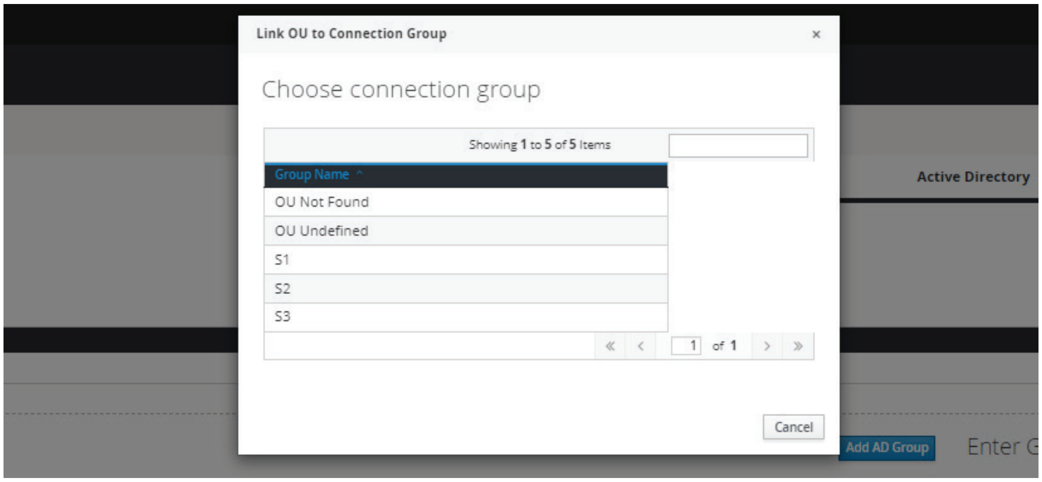
IP Address / Hostname: 10.0.0.5
Secure LDAP: OFF
Port: 389
Domain: bbnsengineering.local
AD Username: adsync
AD Password: ••••••••
Apply

FIGURE 14-32. ACTIVE DIRECTORY DETAILS—SYSTEM CONFIGURATION

Boxilla® supports Secure LDAP (LDAPS) via STARTTLS in version 4.6 and later , and it is considered the "LDAP over SSL". It will use port 636 by default and can be setup with or without server side certificate validation. STARTTLS will use port 389 by default. The Boxilla also supports Azure Active Directory with or without a certificate. Boxilla supports LDAPS / STARTTLS which uses a CA certificate that can be uploaded by the administrator. The Certificate SAN field is mandatory, and the value to be entered is the contents of the SAN field for the Active Directory Server Certificate. This feature also supports Certificate SAN which is typically the domain name (This can cause issues if it doesn't match the certificate).

14.11.2 LINKING AN ACTIVE DIRECTORY OU TO A BOXILLA CONNECTION GROUP

The Boxilla admin user will have the option to specify what Active Directory OU or Security Group is linked to a Connection Group. Once Active Directory is successfully connected, Boxilla may automatically retrieve a few OUs and store them in its database (not all), but not Security Groups. The Boxilla administrator has the option to associate the Active Directory user with connections by adding them to the Users List (as an AD user), or they can assign the connection group to the entire OU or Security Group. Connections are automatically assigned to the users once configured and the receiver is logged out and back in.



Link OU to Connection Group ×

Choose connection group

Showing 1 to 5 of 5 Items

Group Name ^
OU Not Found
OU Undefined
S1
S2
S3

1 of 1

Cancel

FIGURE 14-33. CONNECTING OU TO CONNECTION GROUP

14.11.3 USING ACTIVE DIRECTORY WITH ORGANIZATIONAL UNITS (OUS)

When configuring the Active Directory credentials within Boxilla®, you have the option to enter the details of the AD server and then test the connection to make sure it is successful. Once connected to the AD, the OU list (Organization Unit) may update with available OU groups found within the AD server automatically, however most of the time the OU will need to be added manually, or will become visible once a user/member of that OU is manually added to Users as an AD user. The administrator may now Link an OU with a Connection Group (which is configured under Connections). Only those users will have access to the connection list, thus limiting the number of connections for that OU group. If any user needs more unique connections, the administrator can add that AD user to the Users list and manually configure available connections. The user will see a composite access control list from the OU Group and Custom Configuration. Any AD user can now login to the receiver even though their username may not be found under the Users profile, as long as they are part of the AD group they can login. If an AD user profile is still under the Users menu, it is because they were added prior to the firmware update or they require more unique connection options that may not fit other users within the same OU. If for any reason the user(s) within the OU shouldn't have access to any KVM hardware, you can Delete the OU and the users in that OU won't have access to the system, or you can configure certain users for Groups that are empty. This in turn will not allow those users to access the system.

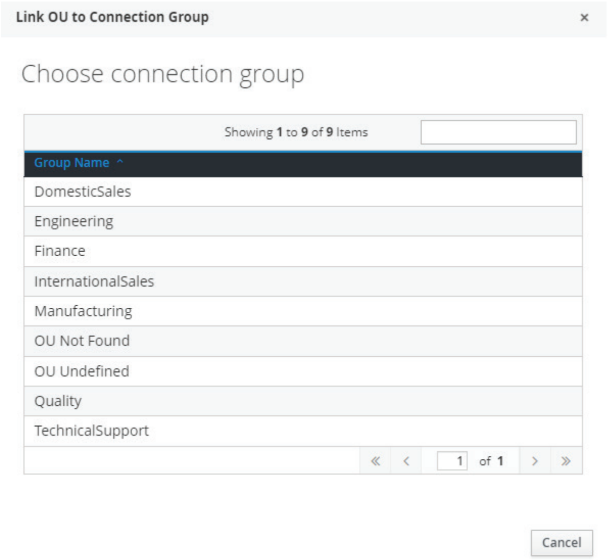
OU Setup

The Admin will be able to add OUs and assign these OUs to Connection groups. See Section 11.2, Connections — Groups.

When the user above is authenticated as described above and the OU matches one added by the admin they will get access to the assigned connection groups.

If the OU cannot be matched, the user can define a connection group: "OU undefined."

If the OU cannot be found or there is no OU, the user can define another connection group: "No OU found."



Link OU to Connection Group

Choose connection group

Showing 1 to 9 of 9 Items

Group Name ^
DomesticSales
Engineering
Finance
InternationalSales
Manufacturing
OU Not Found
OU Undefined
Quality
TechnicalSupport

FIGURE 14-34. OU GROUPING

14.11.4 USING ACTIVE DIRECTORY WITH SECURITY GROUPS

Security Groups may also be used within Boxilla® by manually entering the Security Group Name (name from AD server must match Boxilla). The administrator may now Link a Security Group with a Connection Group (which is configured under Connections). Only those users will have access to the connection list, thus limiting the number of connections for that Security Group. If any user needs more unique connections, the administrator can add that AD user to the Users list and manually configure available connections. The user will see a composite access control list from the OU Group and Custom Configuration. Any AD user can now login to the receiver even though their username may not be found under the Users profile, as long as they are part of the AD group they can login.If for any reason the user(s) within the Security Group shouldn't have access to any KVM hardware, you can Delete the Security Group and the users in that group won't have access to the system, or you can configure certain users for Groups that are empty. This in turn will not allow those users to access the system.

14.12 SYSTEM — SETTINGS — REST API

This will enable REST API support on the Boxilla so other 3rd-party devices can communicate with the manager to perform additional functions.

REST API State

Version: 1.0

ON

FIGURE 14-35. API ON

14.13 SYSTEM — SETTINGS — REMOTE APP

Minimum Supported Remote App Version: The recommended minimum revision of Remote App will be set by Boxilla® and automatically be set following an upgrade of the system.

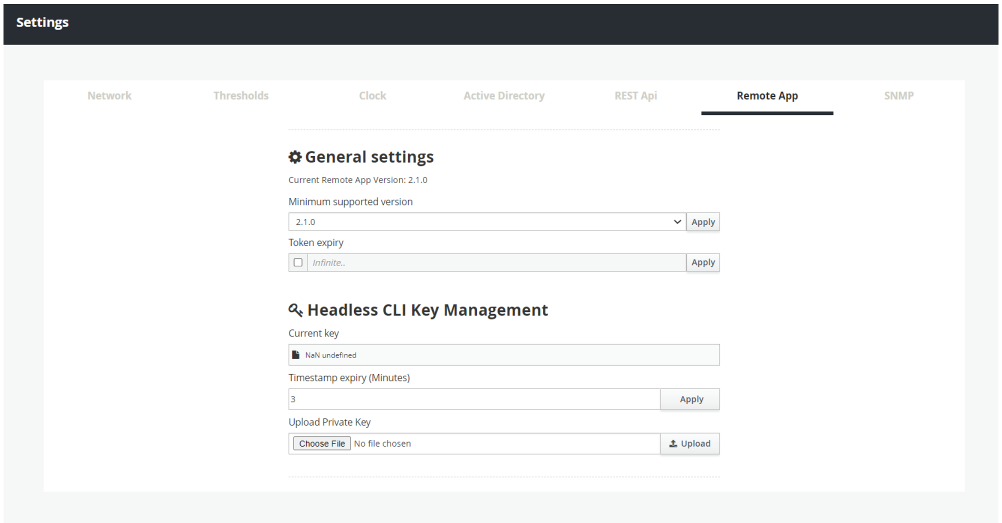
However, the Boxilla user can decide to set another minimum version. Versions to choose from will automatically be added to the list following a failed login attempt from a Remote App user at a lower revision.

The Boxilla administrator will be notified of a failed attempt. A minimum supported Remote App version will create a Boxilla alert.

The Boxilla administrator can decide to advise the app user to upgrade or in an exception could change the setting in Boxilla to match the lower revision. The Boxilla Administrator should only change this Minimum supported version if advised by the Black Box support team.

Remote App error message:

The Remote App will check on login if the Remote App is at a compatible version of Boxilla.



General settings

Current Remote App Version: 2.1.0

Minimum supported version: 2.1.0

Token expiry: □ Infinite..

Headless CLI Key Management

Current key: NaN undefined

Timestamp expiry (Minutes): 3

Upload Private Key: No file chosen

FIGURE 14-36. REMOTE APP

Boxilla 4.6 allows the administrator to not only set the RemoteApp compatibility / version, but it also allows configuration of a Headless CLI key management feature. Boxilla 4.3.2 together with Remote App 2.4.0 extends Remote App User Authentication by supporting the configuration of a validity period for each User's Authentication.

The Token Expiry option allows for configuration of a timeout for the RemoteApp when not in use. This period is configured via the 'Token expiry' field. When a Remote App User's Authentication period expires, any existing connections will be terminated, the user will be automatically logged out from the Remote App. If the User wishes to continue using the Remote App, the User needs to re-authenticate by logging back into the Remote App.

To configure the 'Token expiry' field, select the field by clicking on the tick box, then click on the field to enter the relevant token value (Days & Hours).

Note: Each token expires following a successful User Logout.

The valid ranges for these field include:

- Days 0-999.
- Hours 1-99.

14.14 SYSTEM — SETTINGS — SNMP

The Boxilla® SNMP features improves the system reliability by allowing notifications to be sent out. The SNMP feature supports MIB files that contain pre-defined definitions of commands that can be used which include:

- Node IP Address
- Node State
- Cluster Replicating Alert and Latency
- Status of Active / Primary Boxilla devices
- Information on all devices
- Description context of Boxilla alerts
- Information on device IP, Mac Address, and Display Settings
- Information on all network switches such as switch name, IP address, Mac Address, and Switching Information
- Device Status (Device Offline, Device Online)

The followed data can be retreived via the SNMP Get requests:

*DeviceInfo: Name, Mac, IP, Model, State

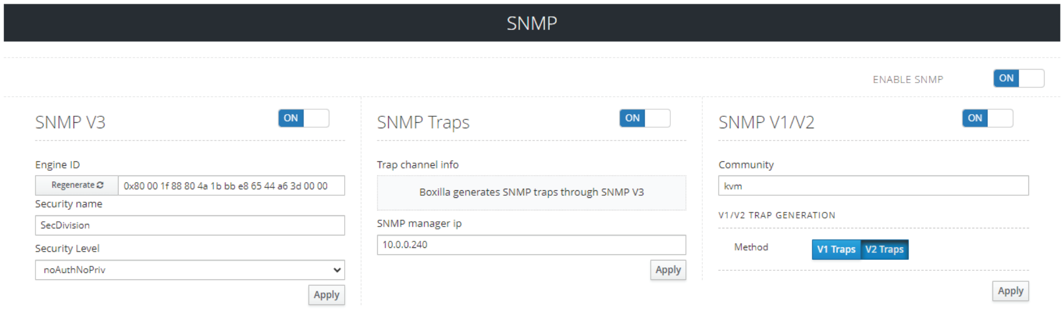
*SwitchInfo: Name, Mac, IP, Model, State

*ClusterNodeInfo: ID, Name, IP, State, ReplicationLag

The Boxilla administrator can also configure SNMP traps using SNMP V1, V2, and V3 and a community string can be declared.

A EngineID (application ID) can be used if an external SNMP manager is having connection issues. A Security Name can be used like a user name configuration for privacy. Security levels can be adjusted and will use different encryption methods. These methods include "no AuthNoPriv" which is the weakest. The "authNoPriv" can be used as a medium encryption option, while the "authPriv" is the strongest method.

An Authentication Protocol can be set using MD5 or SHA. The Authentication Key is like a password for the Security Name, and it can use a Privacy Protocol like DES and a Privacy Key.



SNMP

ENABLE SNMP: ON

SNMP V3: ON

Engine ID: 0x80 00 1f 88 80 4a 1b bb e8 65 44 a6 3d 00 00

Security name: SecDivision

Security Level: noAuthNoPriv

SNMP Traps: ON

Trap channel info: Boxilla generates SNMP traps through SNMP V3

SNMP manager ip: 10.0.0.240

SNMP V1/V2: ON

Community: kvm

V1/V2 TRAP GENERATION

Method: V1 Traps / V2 Traps

FIGURE 14-37 SNMP

14.15 SYSTEM — SETTINGS — BACKUP (REMOTE BACKUP SUPPORT)

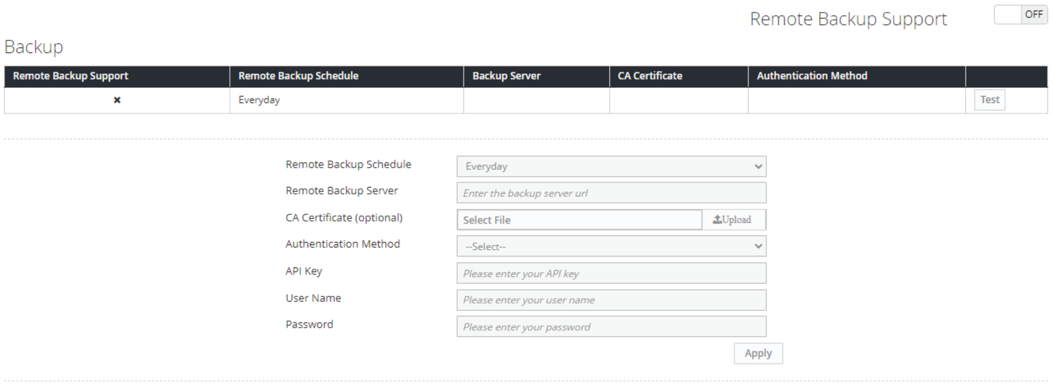
Boxilla® supports the automatic exporting of the Boxilla nightly backup file to an external HTTPS Backup Server.

The Boxilla backups can be exported daily or weekly. Backups are exported at 2AM on the specified day.

The CA Certificate field is an optional field. This field is used to upload the root CA certificate for the HTTPS Backup Server.

Boxilla supports 2 Authentication methods when accessing the HTTPS Backup Server: Basic Authentication and API Key.

1. Basic Authentication: Username and Password are required.
2. API Key: API Key for the HTTPS Backup Server.



Remote Backup Support OFF

Backup

Remote Backup Support	Remote Backup Schedule	Backup Server	CA Certificate	Authentication Method	
×	Everyday				Test

Remote Backup Schedule	Everyday
Remote Backup Server	Enter the backup server url
CA Certificate (optional)	Select File Upload
Authentication Method	--Select--
API Key	Please enter your API key
User Name	Please enter your user name
Password	Please enter your password

FIGURE 14-38. SYSTEM SCREEN—REMOTE BACKUP SUPPORT

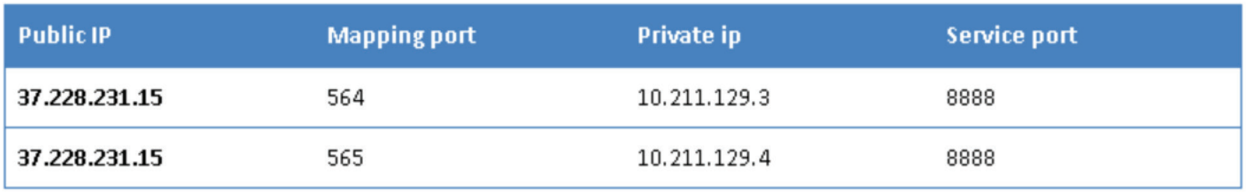
14.16 SYSTEM — SETTINGS — NAT

14.16.1 PORT ADDRESS TRANSLATION

In cases where the appliance is physically located behind a NAT, its private IP is hidden from the Boxilla® Manager. The Boxilla device is capable of communicating with multiple appliances behind a NAT. Typically, port forwarding can be used to address this, but, when you have multiple devices behind a NAT, this could cause problems.

Boxilla uses Port Address Translation (PAT), which is a technique to allow mapping of local ports and private IP addresses to a public mapping port. A mapping port acts as a unique identifier which allows identification of traffic designated for a particular recipient behind a NAT and rerouting the traffic to a private IP and Service Port.

An example of two devices behind a NAT that are both listening to the same port is shown in Figure 14-39 below:



Public IP	Mapping port	Private ip	Service port
37.228.231.15	564	10.211.129.3	8888
37.228.231.15	565	10.211.129.4	8888

FIGURE 14-39 EXAMPLE OF TWO DEVICES BEHIND NAT WITH BOTH LISTENING TO SAME PORT

When the request comes in to 37.228.231.15:564, shown in the first line of Figure 14-36 above, all traffic is redirected to the private IP and service port 10.211.129.3:8888, which is also shown in the same line of Figure 14-36. Similarly, if a request comes in to 37.228.231.15:565, shown in the second line of Figure 14-36 above, it is rerouted to 10.211.129.4:8888, as also shown in the second line of Figure 14-36. This method allows requests to a particular device hidden behind a public IP even when multiple devices are listening to the same port.

The Boxilla unit can access multiple appliances behind a NAT, but it will no longer be able to access appliances using known ports and will have to keep track of the unique set of ports for those appliances, which increases device management difficulty. The more devices behind a NAT, the more configuration that is needed. For example, if there are 20 devices behind a NAT, 60 mapping ports in total will need to be set up. The configuration is also dependent on a specific hardware supporting PAT, such as SonicWall firewall or PAT capable routers.

14.16.2 ONE TO ONE NAT

A one to one NAT allows the mapping of a set of Private IP addresses to unique Public IP addresses, which effectively makes it possible to access a device behind a NAT using a unique Public IP mapped to a Private destination.

This configuration is easier to configure compared to PAT. It doesn't require the user to enter any additional information when managing an appliance using its public IP. The drawback to this method is that the user is still required to set up an IP mapping rule for each appliance. This requires specific hardware, such as Cisco RV320.

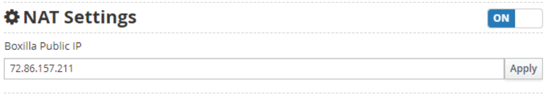
14.16.3 SITE TO SITE VPN (IPSEC)

Site to site VPN allows connections from a local network to a remote network. This method allows the devices to talk to each other using their Private IP addresses as if they were on the same LAN. This eliminates all issues associated with single Public IP addresses and shared ports.

With IPsec, the admin doesn't need to configure any mapping rules per device. IPsec protocol provides an additional security layer since it encrypts IP traffic before the packets are transferred from the source to the destination and decrypts the traffic when it arrives. However, it requires hardware that supports VPN tunneling. There is also a risk of overlapping local IP addresses if the networks were not designed in parallel.

14.16.4 BOXILLA STATIC NAT

This setting only applies to the Boxilla® and not to the endpoints/appliances. If the Boxilla is not on the same local network as the appliances, Boxilla requires this information to be configured in order to communicate with the appliances. A popup hint will be presented as a reminder for anyone following this type of configuration.



NAT Settings ON

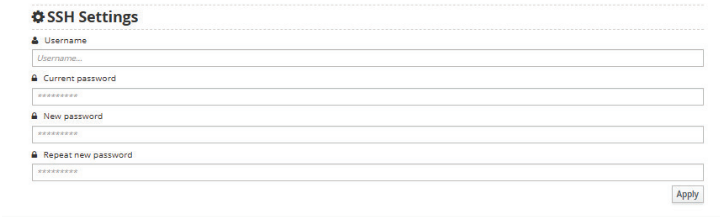
Boxilla Public IP: 72.86.157.211 [Apply]

FIGURE 14-40 STATIC NAT ENABLED

Apart from enabling NAT Settings for the Boxilla and entering the Boxilla Public IP address, there are no other differences between managing NAT and local Appliances.

14.16.5 SSH

Boxilla will offer a way to configure the default SSH settings in cases where end users need to perform security scans within port 22. There is no way to completely disable the SSH port on Boxilla, but this setting can be used to change the default SSH password. Once you gain access to the SSH interface, it is restricted and all options are secured, but end users could gain access to it in order to perform security scans that may be required. To receive the default login credentials, contact Black Box technical support.



SSH Settings

Username: Username...

Current password: *********

New password: *********

Repeat new password: *********

[Apply]

FIGURE 14-41 SSH

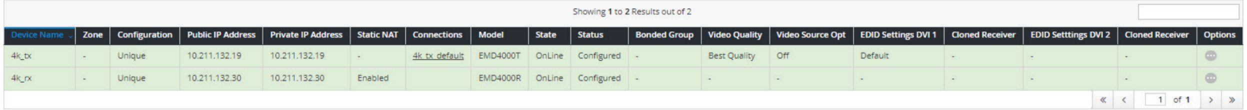
Warning: If the SSH password is lost, there is no way to reset or recover it. Black Box does not have any way to reset it. If the password is changed, keep the password in a safe place that won't get lost.

14.16.6 DEVICE SETTINGS

A table on the Devices >> Settings page displays columns which include:

1. Private IP Address: Displays appliance Private IP, which is retrieved by an audit
2. Public IP Address: Displays appliance Public IP
3. Static NAT: Displays current NAT state per appliance

The device information table is shown in Figure 14-42 below:



Showing **1** to **2** Results out of 2

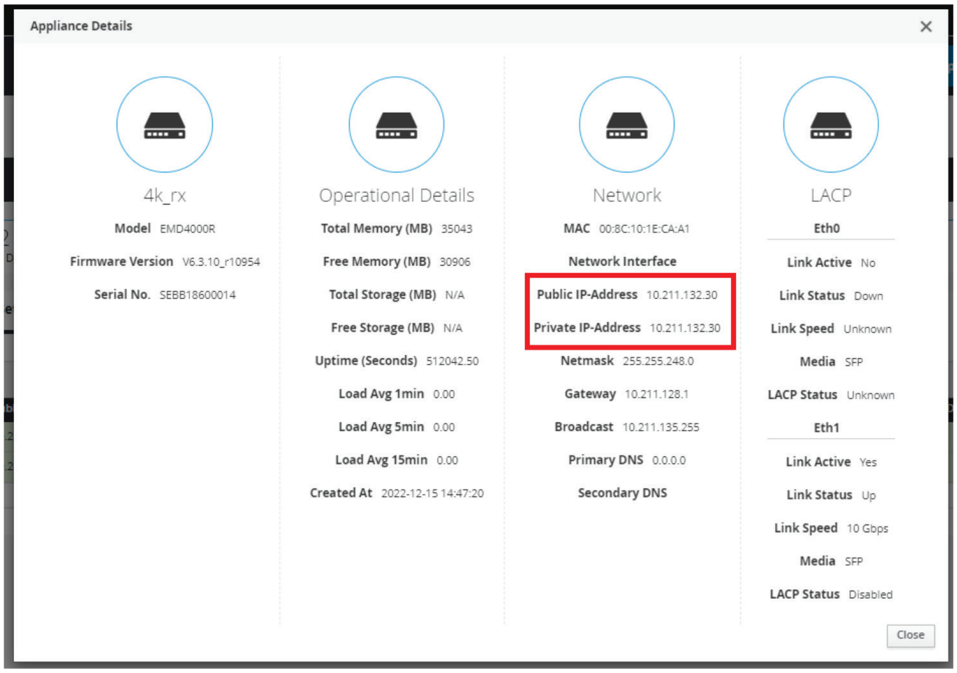
Device Name	Zone	Configuration	Public IP Address	Private IP Address	Static NAT	Connections	Model	State	Status	Bonded Group	Video Quality	Video Source Opt	EDID Settings DVI 1	Cloned Receiver	EDID Setttings DVI 2	Cloned Receiver	Options
4k_tx	-	Unique	10.211.132.19	10.211.132.19	-	4k_tx_default	EMD4000T	OnLine	Configured	-	Best Quality	Off	Default	-	-	-	⋯
4k_rx	-	Unique	10.211.132.30	10.211.132.30	Enabled		EMD4000R	OnLine	Configured	-	-	-	-	-	-	-	⋯

FIGURE 14-42 DEVICE INFORMATION TABLE

14.16.7 APPLIANCE DETAILS

The appliance details information window includes both the Private and Public IP addresses for a user to reference.

Figure 14-43 provides an example of appliance details with the Public and Private IP addresses highlighted.



Appliance Details

4k_rx

Model EMD4000R

Firmware Version V6.3.10_r10954

Serial No. SEBB18600014

Operational Details

Total Memory (MB) 35043

Free Memory (MB) 30906

Total Storage (MB) N/A

Free Storage (MB) N/A

Uptime (Seconds) 512042.50

Load Avg 1min 0.00

Load Avg 5min 0.00

Load Avg 15min 0.00

Created At 2022-12-15 14:47:20

Network

MAC 00:8C:10:1E:CA:A1

Network Interface

Public IP-Address 10.211.132.30

Private IP-Address 10.211.132.30

Netmask 255.255.248.0

Gateway 10.211.128.1

Broadcast 10.211.135.255

Primary DNS 0.0.0.0

Secondary DNS

LACP

Eth0

Link Active No

Link Status Down

Link Speed Unknown

Media SFP

LACP Status Unknown

Eth1

Link Active Yes

Link Status Up

Link Speed 10 Gbps

Media SFP

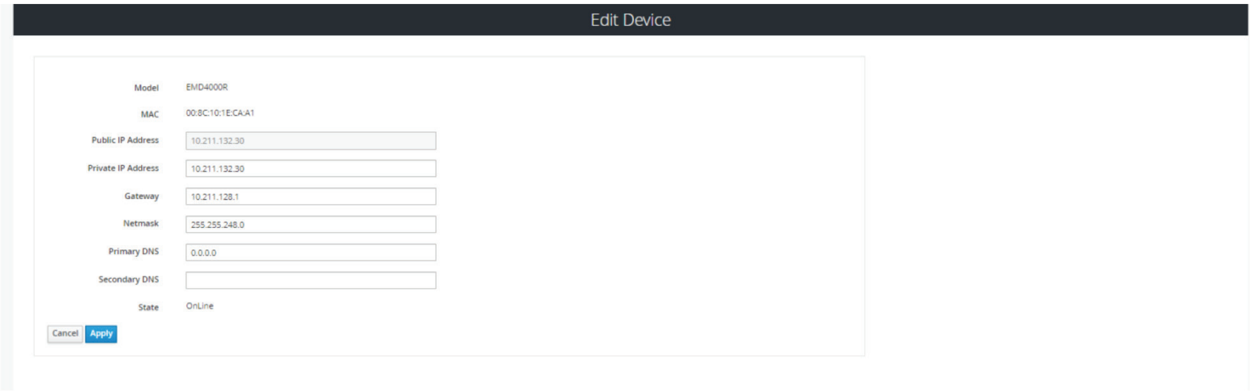
LACP Status Disabled

FIGURE 14-43 APPLIANCE DETAILS

14.16.8 EDIT NETWORK

When editing an appliances network, an IP address field within the “Edit Network” form is renamed to “Private IP Address.” The form also includes the Public IP Address field, which is disabled by default and is present for user reference only.

The “Edit Device” screen is shown in Figure 14-44 below:



Model	EMD4000R
MAC	00:8C:10:1E:CA:A1
Public IP Address	10.211.132.30
Private IP Address	10.211.132.30
Gateway	10.211.128.1
Netmask	255.255.248.0
Primary DNS	0.0.0.0
Secondary DNS	
State	OnLine

FIGURE 14-44 EDIT DEVICE SCREEN

CHAPTER 15: LICENSE

15.1 LICENSE PAGE — BOXILLA LICENSING

Boxilla® licensing allows for customization of the system. It gives the ability to add licenses to Boxilla to define number of Users, Connections, and Devices to be supported in a Managed Domain. Release 2.0 default licensing model will be 25 Devices, 25 Connections, and 25 Users (BXAMGR-R2).

The system supports the addition of:

- BXAMGR-R2-LIC-25 (25 more devices/users/connections)
- BXAMGR-R2-LIC-50 (50 more devices/users/connections)
- BXAMGR-R2-LIC-100 (100 more devices/users/connections)
- BXAMGR-R2-LIC-200 (200 more devices/users/connections)
- BXAMGR-R2-LIC-300 (300 more devices/users/connections)
- BXAMGR-R2-LIC-ULT (unlimited devices/users/connections)
- BXAMGR-R2-LICBAK-25 (Boxilla KVM Manager 25 Device License for Active and Standby Boxilla)
- BXAMGR-R2-LICBAK-100 (Boxilla KVM Manager 100 Device License for Active and Standby Boxilla)
- BXAMGR-R2-LICBAK-200 (Boxilla KVM Manager 200 Device License for Active and Standby Boxilla)
- BXAMGR-R2-LICBAK-300 (Boxilla KVM Manager 300 Device License for Active and Standby Boxilla)
- BXAMGR-R2-LICBAK-ULT (Boxilla KVM Manager Unlimited Device License for Active and Standby Boxilla)

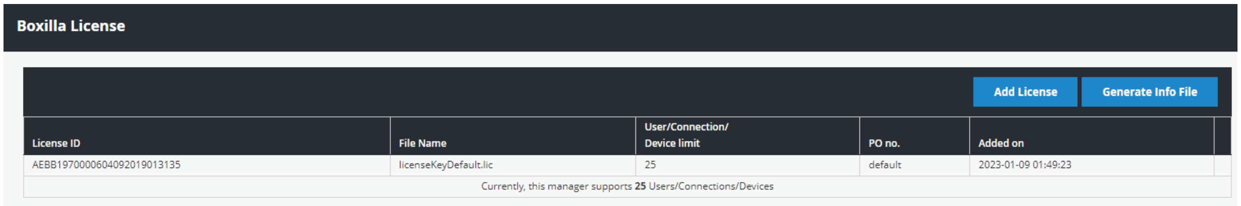
Licenses can be added under the System -> License Page.

To find the current license, click on the License button and you will be able to verify the Boxilla licenses.

CHAPTER 15: LICENSE

15.1.1 HOW TO REQUEST A LICENSE

To procure a new license file, generate the info file from your current system using Generate Info File option at the top of the License page. The info file will be downloaded onto the local machine. Provide the info file to Black Box at the time of ordering new licenses so that they can be generated.



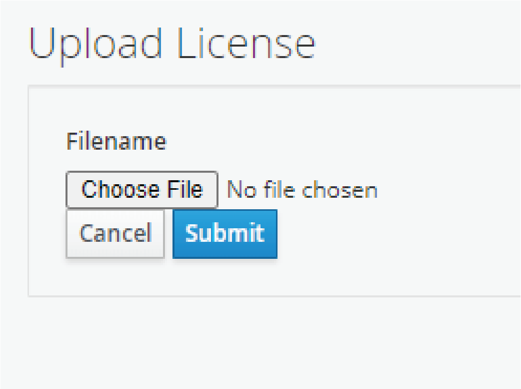
License ID	File Name	User/Connection/ Device limit	PO no.	Added on
AEBB1970000604092019013135	licenseKeyDefault.lic	25	default	2023-01-09 01:49:23

Currently, this manager supports **25** Users/Connections/Devices

FIGURE 15-1. ADD LICENSE SCREEN

15.1.2 HOW TO UPLOAD A LICENSE FILE

Once you receive the license file, upload the new license.



Upload License

Filename: No file chosen

FIGURE 15-2. UPLOAD LICENSE SCREEN

CHAPTER 16: CLUSTER

16.1 INTRODUCTION

The Boxilla® system can support a Primary/Standby manager that allows the standby to take over if the Primary is not online. This ensures a smooth operating environment for users and administrators.

16.2 BEFORE YOU BEGIN/PREREQUISITES

Before you begin configuring the Boxilla managers for Primary / Standby mode, verify the following prerequisites have been met first; otherwise, the Primary / Standby mode will not work.

- Boxilla managers must have firmware 3.0 or higher
- Boxilla managers must be on the same firmware version
- Boxilla managers must be using the same endpoint/RemoteApp licenses
- Boxilla managers must be on the same subnet and connected to the network so they can be seen
- Both the Primary / Standby must have matching Ethernet Port Configurations (i.e. if Primary has Ethernet 2 enabled, so does the standby, if it is disabled on the Primary, then the Standby must also be disabled).
- DNS settings must match, and the DNS server must be accessible from the Boxilla.

16.3 OVERVIEW OF OPERATION

When the system is configured for Primary / Standby, you will use a Virtual IP address to access the managers (*you won't use the actual Boxilla IP address unless you are initially creating the cluster, updating the managers, or breaking the clusters*), and all activity will be managed via the Virtual IP address. The Virtual IP address is assigned during the configuration of the Primary Boxilla.

If the Primary Boxilla goes offline and the Virtual IP is no longer accessible, it will take approximately 4 minutes between the time the Primary goes offline and when you can access the Virtual IP again. This timeout occurs to make sure the Primary is truly offline before the Standby takes over. Once this time has elapsed, you can access the Virtual IP again to manage the system.

In certain situations, when the Primary Boxilla goes offline and the Standby takes over, you will be required to login into the Virtual IP interface to make sure both Boxilla managers are operating in their proper roles after bringing the Primary back online, and in some instances when the Primary comes back online, you may need to swap the roles (Primary / Standby). In this situation, where the roles must be swapped, it is because both managers think they are Primary, but they do not have valid Standby configurations. To swap the roles, simply select the ellipsis "•••" icon and select "Make Standby" for the old Primary.

An example of this situation is when the Primary Boxilla gets disconnected from the network and comes back eventually. If you log into the Virtual IP address and see that the Primary is still offline (but you can physically ping it and access it on its own IP), click the ellipsis "•••" icon of the old Primary Boxilla, and click on "Make Standby". This will address the roles for all managers' part of that cluster.

When configuring the Primary / Standby system, keep in mind the following functions and what they really do:

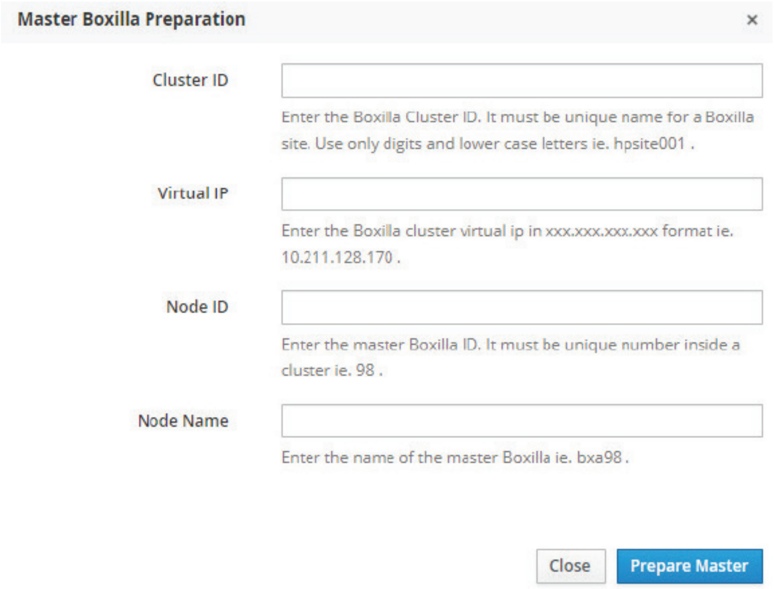
- Make Standalone – This will factory restore the Boxilla and clear the users, connections, and endpoints, but keep the existing network configuration, endpoint licenses, and firmware.
- Detach – This will disconnect the Boxilla from the cluster, but will keep all of its configuration parameters including users, connections, and endpoints. Detaching a Boxilla from a cluster will enable its webpage so it can be accessible, and it is the first step before properly dissolving a cluster.
- Switchover to Acitve – This will force the standby Boxilla to change roles and be the acting primary. This change over can take 4 minutes to complete.

16.4 CREATING THE CLUSTER

To create a Boxilla® Primary / Standby system, first make sure you have met all of the prerequisites as stated above. The next step is to make a backup of the existing Boxilla configuration in case it is needed to be uploaded to restore the system endpoints, connections, users, and settings.

PREPARING THE PRIMARY

1. Within the Boxilla Primary manager, login and navigate to "Cluster" in the menu.
2. Click the "Prepare Master" button and enter the configuration information. Use the help windows throughout this process. The Virtual IP will be used as a single point of access to the Primary / Standby cluster.



Master Boxilla Preparation

Cluster ID

Enter the Boxilla Cluster ID. It must be unique name for a Boxilla site. Use only digits and lower case letters ie. hpsite001 .

Virtual IP

Enter the Boxilla cluster virtual ip in xxx.xxx.xxx.xxx format ie. 10.211.128.170 .

Node ID

Enter the master Boxilla ID. It must be unique number inside a cluster ie. 98 .

Node Name

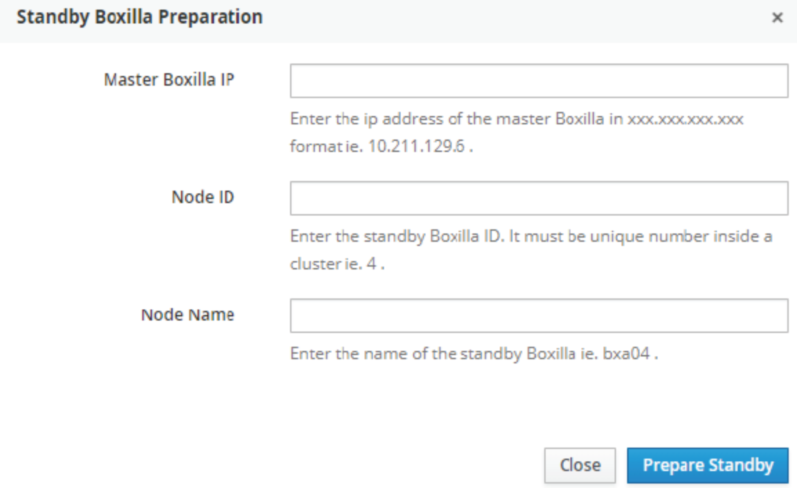
Enter the name of the master Boxilla ie. bxa98 .

FIGURE 16-1. SETUP NEW MASTER SCREEN

PREPARING THE STANDBY

This will take the active configuration of the designated Primary and overwrite the configuration in the Standby Boxilla® manager.

1. Within the Boxilla Standby manager, login and navigate to “Cluster” in the menu.
2. Click the “Prepare Standby” button and enter the configuration information. Use the help windows throughout this process.



Standby Boxilla Preparation

Master Boxilla IP

Enter the ip address of the master Boxilla in xxx.xxx.xxx.xxx format ie. 10.211.129.6 .

Node ID

Enter the standby Boxilla ID. It must be unique number inside a cluster ie. 4 .

Node Name

Enter the name of the standby Boxilla ie. bxa04 .

FIGURE 16-2. STANDBY BOXILLA PREPARATION

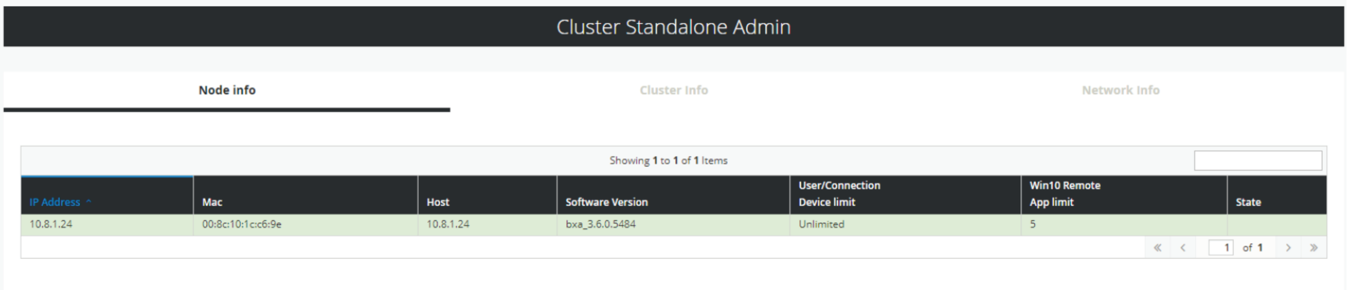
At this time, you should only be able to access the Boxilla Primary web interface and Virtual IP web interface. The Standby manager can be pinged, but the Standby web interface will be disabled on purpose.

NOTE 1: You will only use the Virtual IP address unless you are dissolving a cluster (i.e. to perform an update as an example).

NOTE 2: The Standby Boxilla will disable its web interface once part of the system. The only way the webpage will become accessible is if the Boxilla is Detached.

You now have a Primary / Standby system configured.

The configured cluster shows up in the Node Info tab on the screen.



Cluster Standalone Admin

Showing 1 to 1 of 1 Items

IP Address ^	Mac	Host	Software Version	User/Connection Device limit	Win10 Remote App limit	State
10.8.1.24	00:8c:10:1c:c6:9e	10.8.1.24	bxa_3.6.0.5484	Unlimited	5	

FIGURE 16-3. CONFIGURED CLUSTER PRIMARY VIEW

16.5 CLUSTER SWITCHOVER

Boxilla® firmware version 4.3 and later includes the option to switch over a Standby BXA to an Active BXA. This operation is available as an option on the Standby BXA in the Cluster Admin page.

16.6 FAILOVER

When a Primary / Standby system is configured and the acting Primary is disconnected or goes offline, it will take about 4 minutes before the Standby will take over and begin responding as the new Primary. There will be a small window where the Virtual IP web interface cannot be accessed.

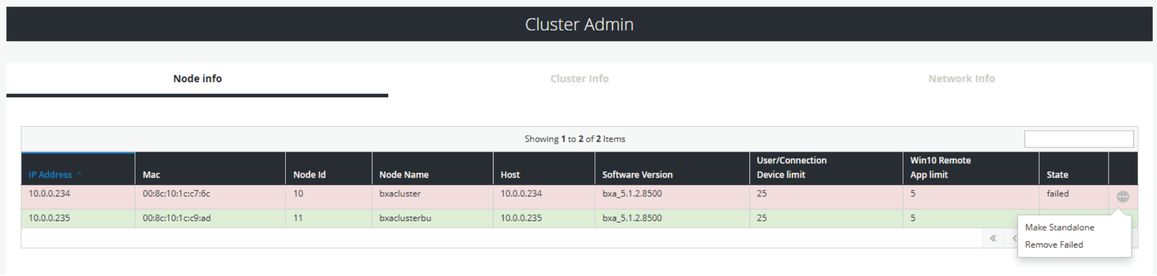
Once the system has been identified as having performed a failover, it is important as a system admin to go into the Virtual IP web interface and make sure your Primary / Standby are operating in their correct roles. Depending on the circumstances and firmware version of the Boxilla, the system may be restored naturally without any user intervention, but it is always good practice to make sure.

In Boxilla 4.3, a failed unit is automatically recovered back into the cluster once the failure condition has been resolved. There is now no need to perform the Prepare Standby action.

NOTE: An extensive list of Cluster alerts has been added in Boxilla 4.3 and later. There alerts provide status information on Cluster failover and recovery operations.

In the case of the active Boxilla going offline or failing for any reason, the cluster will automatically fail over within 4 minutes. In a failed state, you will see the failed Boxilla highlighted in red with the option to make standalone or remove failed. In most cases the Boxilla is just turned off or the network connection was interrupted, and, once that is resolved, the system will automatically come back.

In software versions before 4.3, if you navigate to this page and see that the “old Primary” is in a “failed” state, you can simply click the ellipsis “•••” icon near the failed controller and click “Prepare Standby”. This will in turn flip the Primary / Standby roles (IP addresses of the Boxilla managers will remain the same) and initialize the cluster again so you still have a Primary / Standby configuration.



Cluster Admin

Showing **1** to **2** of **2** Items

IP Address	Mac	Node Id	Node Name	Host	Software Version	User/Connection Device limit	Win10 Remote App limit	State	
10.0.0.234	00:8c:10:1c:c7:6c	10	bxacluster	10.0.0.234	bxa_5.1.2.8500	25	5	failed	⋯
10.0.0.235	00:8c:10:1c:c9:ad	11	bxaclusterbu	10.0.0.235	bxa_5.1.2.8500	25	5		

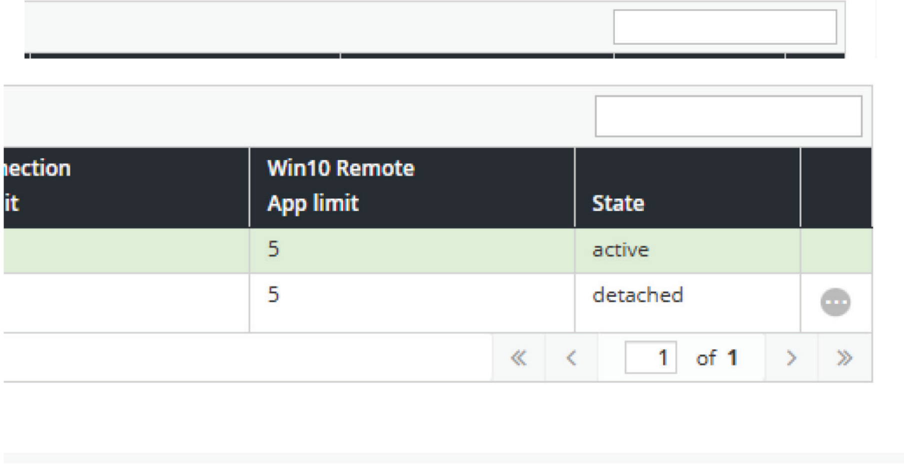
FIGURE 16-4. OPTIONS FOR FAILED VIEW BACKUP DROP-DOWN BOX

16.7 PRIMARY/STANDBY FIRMWARE UPDATES

In order to upgrade Boxilla® units in a clustered state, the cluster must be dissolved completely. This section describes the sequence of steps that are needed in order to perform the upgrades. The method of breaking down a cluster is similar to the next section and is referenced here for convenience.

- Before you begin, verify that you have the latest Backup of the Boxilla system saved to a computer.
- Throughout these steps there should be no requirement to perform a manual Boxilla reboot. Reboots will automatically take place during certain transitions, and you will be notified in the pop-up windows

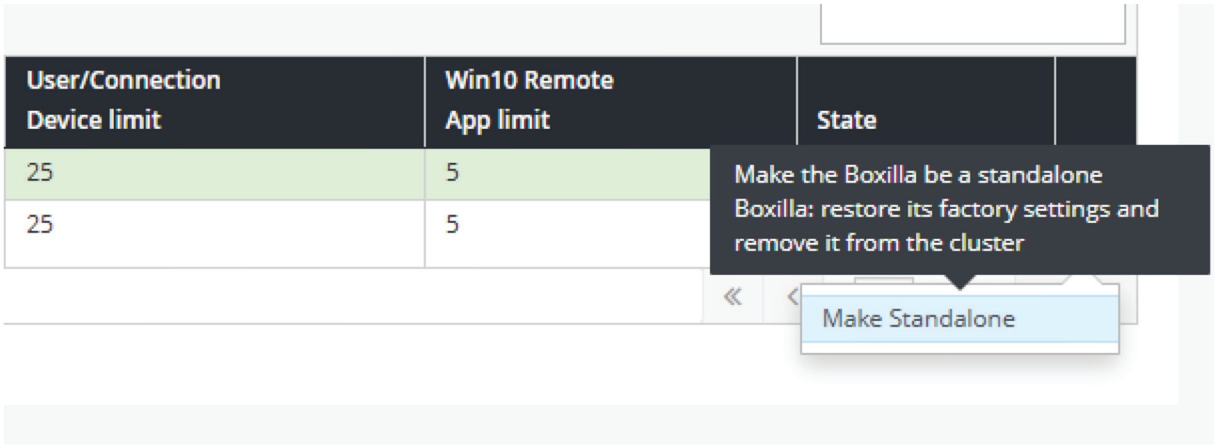
1. (Virtual IP) Go to the Virtual IP of the cluster and navigate to Cluster. Verify that the original Primary Boxilla has the “Active” state and the original Backup Boxilla has the “Standby” state. If they are reversed or in any other state, this must be addressed first. You should always put the Boxillas back in order before starting the dissolving process. If the roles are reversed, you can click on the ellipsis “…” next to the current Standby Boxilla and click on “Switchover to Active” to swap them. If in a failed state, determine the root issue (i.e., Boxilla turned off, network cable unplugged, network switch turned off) and restore it. If it is truly failed, contact our technical support team for next steps.
2. (Virtual IP) Click on the ellipsis “…” next to the Standby Boxilla. Then click on the “Detach” button. Then click on “OK” in the prompt to let the process finish.



ection it	Win10 Remote App limit	State	
	5	active	
	5	detached	⋯

FIGURE 16-6 STATE SHOWING ACTIVE AND DETACHED

3. (Virtual IP) Under the Cluster page, click on the ellipsis "…" again. Then click on "Make Standalone." Then click on the "OK" button, and let it finish.



User/Connection Device limit	Win10 Remote App limit	State
25	5	
25	5	

Make the Boxilla be a standalone Boxilla: restore its factory settings and remove it from the cluster

FIGURE 16-7 MAKE STANDALONE OPTION

4. (Virtual IP) Under the Cluster page, click on the "Dissolve Cluster" button. Then click on the "OK" button, and let the process finish.

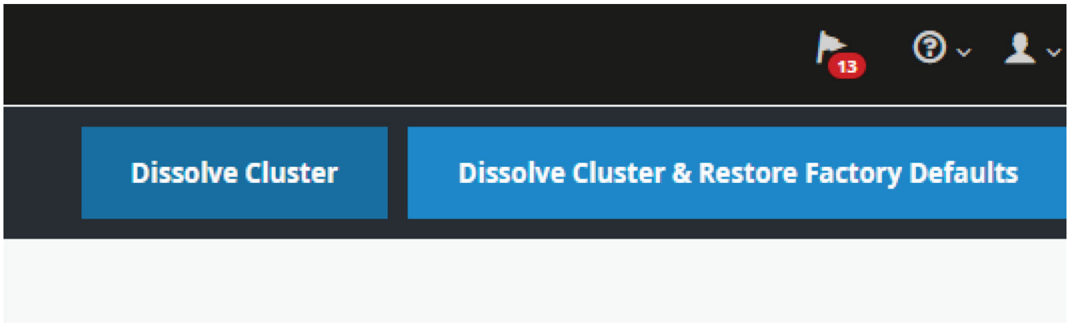


FIGURE 16-8 DISSOLVE CLUSTER OPTION

5. Give the system a few minutes to process. Then open two new tabs and type the IP addresses in for the original controllers to gain access to them. You can now Upgrade, apply licenses, or change network settings on the Boxilla® systems.

When these steps are completed, you can choose to build the cluster back up.

16.8 DISSOLVE CLUSTER

In certain situations or environments, you may need to dissolve the Boxilla Primary / Standby Cluster. Some of these reasons include:

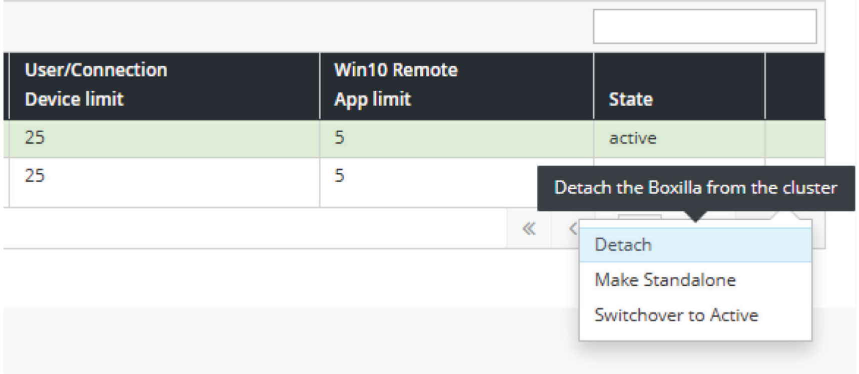
- Upgrading firmware
- Applying or changing licensing
- Changing network settings
- Replacing / Swapping in new Boxilla hardware

- Wanting to only have a single Boxilla manager without a Standby manager
- Technical reasons that include synchronization problems

To Dissolve a Cluster:

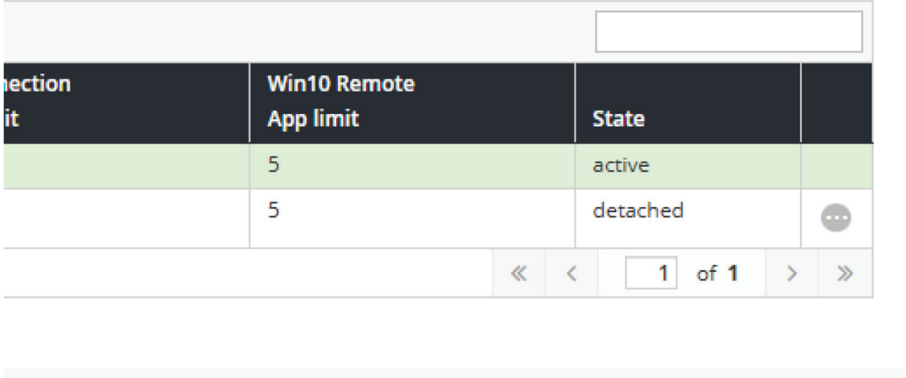
1. (Virtual IP) Go to the Virtual IP of the cluster and navigate to Cluster. Verify that the original Primary Boxilla has the “Active” state and the original Backup Boxilla has the “Standby” state. If they are reversed or in any other state, this must be addressed first. You should always put the Boxillas back in order before starting the dissolving process. If the roles are reversed, you can click on the ellipsis “…” next to the current Standby Boxilla and click on “Switchover to Active” to swap them. If in a failed state, determine the root issue (i.e., Boxilla turned off, network cable unplugged, network switch turned off) and restore it. If it is truly failed, contact our technical support team for next steps.

2. (Virtual IP) Click on the ellipsis “…” next to the Standby Boxilla. Then click on the “Detach” button. Then click on the “OK” button in the prompt to proceed and let the process finish.



User/Connection Device limit	Win10 Remote App limit	State	
25	5	active	
25	5		

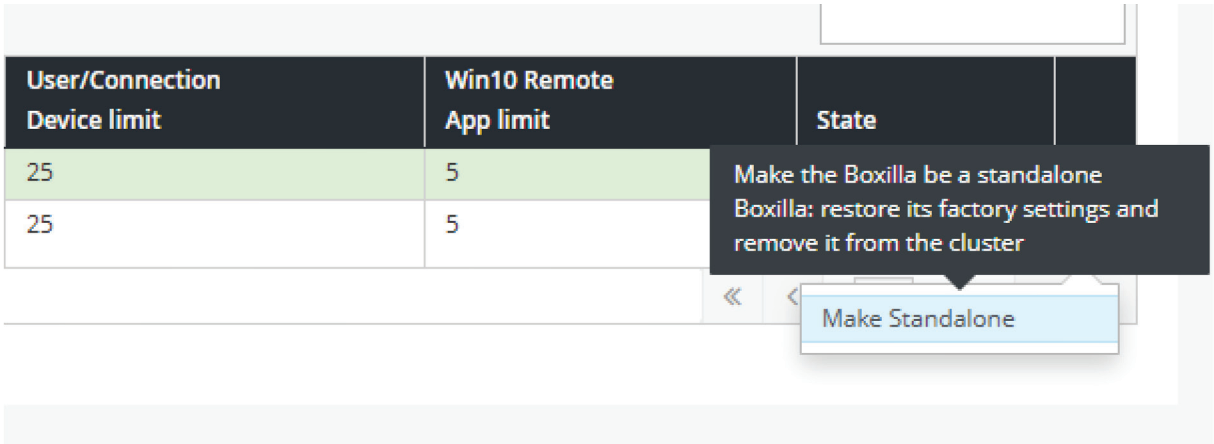
FIGURE 16-9 DROP-DOWN MENU SHOWING DETACH OPTION



ection it	Win10 Remote App limit	State	
	5	active	
	5	detached	

FIGURE 16-10 STATE SHOWING ACTIVE AND DETACHED

3. (Virtual IP) Under the Cluster page, click on the ellipsis "..." again. Then click on "Make Standalone." Then click on the "OK" button, and let it finish.



User/Connection Device limit	Win10 Remote App limit	State
25	5	
25	5	

Make the Boxilla be a standalone Boxilla: restore its factory settings and remove it from the cluster

FIGURE 16-11 MAKE STANDALONE OPTION

4. (Virtual IP) Under the Cluster page, click the "Dissolve Cluster" button. Then click on the "OK" button, and let the process finish.

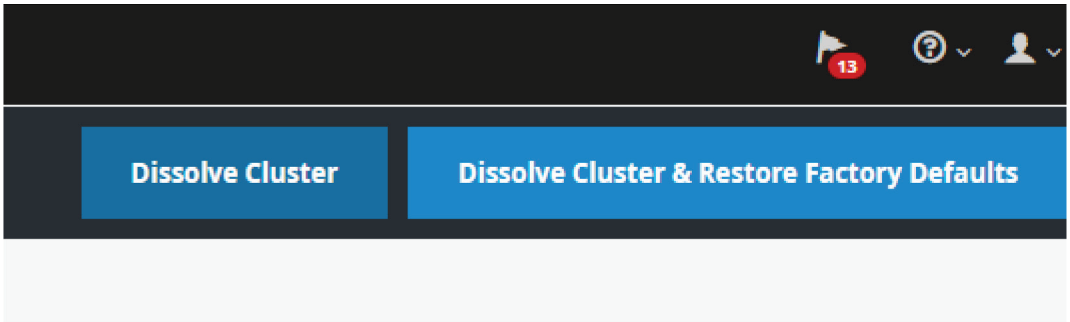


FIGURE 16-12 DISSOLVE CLUSTER OPTION

5. Give the system a few minutes to process. Then open two new tabs and type the IP addresses in for the original controllers to gain access to them.

Now that the Boxilla® Primary / Standby are dissolved. The Virtual IP will no longer work, and you must navigate to the original Boxilla IP addresses to gain access to the web interface.

CHAPTER 17: ALERTS

Alerts in Boxilla® log significant events within the Boxilla and its managed domain. Alerts can be normal events such as users logging in, a user making a connection, a user disconnecting or logging out.

Alerts are classified as Info, Warning or Critical. Normal events are Info Alerts. Events that may be indicate an unusual activity level is classified as a Warning Alert. Events that indicate a potential serious negative impact on the system is classified as a Critical event.

Events that are classified as Critical are:

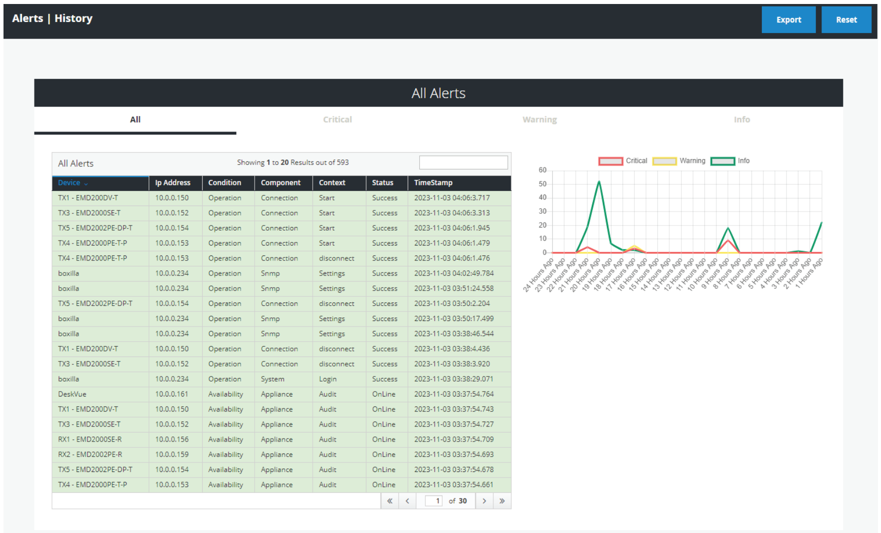
- Failure to update the IP Address of a managed appliance.
- Failure to retrieve appliance details.
- Failure to UnManage a managed appliance.
- Failure to reboot a managed appliance.
- Failure to Upgrade a managed appliance.
- When a managed appliance goes Off-Line

Events that are classified as Warnings are:

- When a user fails to login.
- Firmware on a device mismatches domain's active firmware version
- When a device transitions to Out of Service during an upgrade.
- System threshold is exceeded
- Forced connection fails to establish

17.1 ALERTS— HISTORY

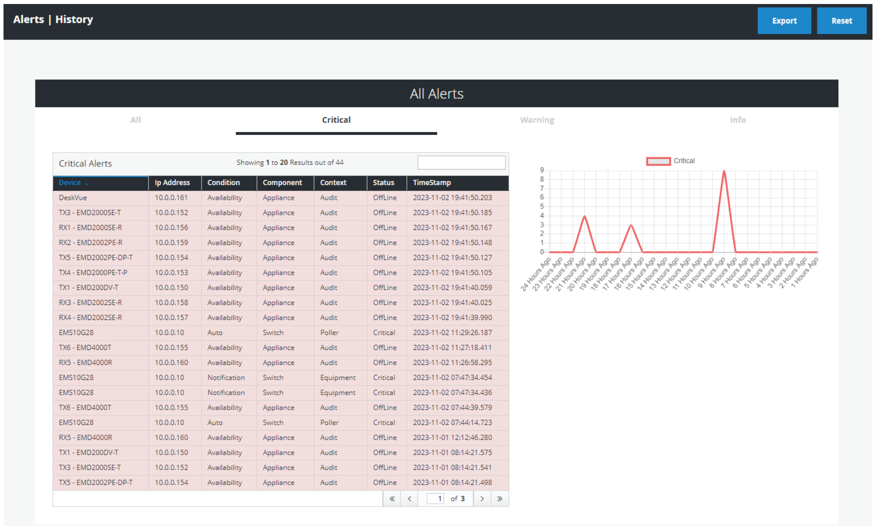
Alert history is a time-stamped log of events across the system. This history can be examined by either looking at all Alerts, or filtering them down to just Critical, Warning or Info by selecting the appropriate tab on the Alerts—History screen as shown in Figure 17-1. The Boxilla will retain up to 10,000 alerts per category for a maximum of 8 days.



Device	Ip Address	Condition	Component	Context	Status	TimeStamp
TX1 - EMD200DV-T	10.0.0.150	Operation	Connection	Start	Success	2023-11-03 04:06:3.717
TX3 - EMD2000SE-T	10.0.0.152	Operation	Connection	Start	Success	2023-11-03 04:06:3.313
TX5 - EMD2002PE-DP-T	10.0.0.154	Operation	Connection	Start	Success	2023-11-03 04:06:1.945
TX4 - EMD2000PE-T-P	10.0.0.153	Operation	Connection	Start	Success	2023-11-03 04:06:1.479
TX4 - EMD2000PE-T-P	10.0.0.153	Operation	Connection	disconnect	Success	2023-11-03 04:06:1.476
boxilla	10.0.0.234	Operation	Snmp	Settings	Success	2023-11-03 04:02:49.784
boxilla	10.0.0.234	Operation	Snmp	Settings	Success	2023-11-03 03:51:24.558
TX5 - EMD2002PE-DP-T	10.0.0.154	Operation	Connection	disconnect	Success	2023-11-03 03:50:2.204
boxilla	10.0.0.234	Operation	Snmp	Settings	Success	2023-11-03 03:50:17.499
boxilla	10.0.0.234	Operation	Snmp	Settings	Success	2023-11-03 03:38:46.544
TX1 - EMD200DV-T	10.0.0.150	Operation	Connection	disconnect	Success	2023-11-03 03:38:4.436
TX3 - EMD2000SE-T	10.0.0.152	Operation	Connection	disconnect	Success	2023-11-03 03:38:3.920
boxilla	10.0.0.234	Operation	System	Login	Success	2023-11-03 03:38:29.071
DeskVue	10.0.0.161	Availability	Appliance	Audit	OnLine	2023-11-03 03:37:54.764
TX1 - EMD200DV-T	10.0.0.150	Availability	Appliance	Audit	OnLine	2023-11-03 03:37:54.743
TX3 - EMD2000SE-T	10.0.0.152	Availability	Appliance	Audit	OnLine	2023-11-03 03:37:54.727
RX1 - EMD2000SE-R	10.0.0.156	Availability	Appliance	Audit	OnLine	2023-11-03 03:37:54.709
RX2 - EMD2002PE-R	10.0.0.159	Availability	Appliance	Audit	OnLine	2023-11-03 03:37:54.693
TX5 - EMD2002PE-DP-T	10.0.0.154	Availability	Appliance	Audit	OnLine	2023-11-03 03:37:54.678
TX4 - EMD2000PE-T-P	10.0.0.153	Availability	Appliance	Audit	OnLine	2023-11-03 03:37:54.661

FIGURE 17-1. ALERTS HISTORY

Critical logs are shown below.



Critical Alerts

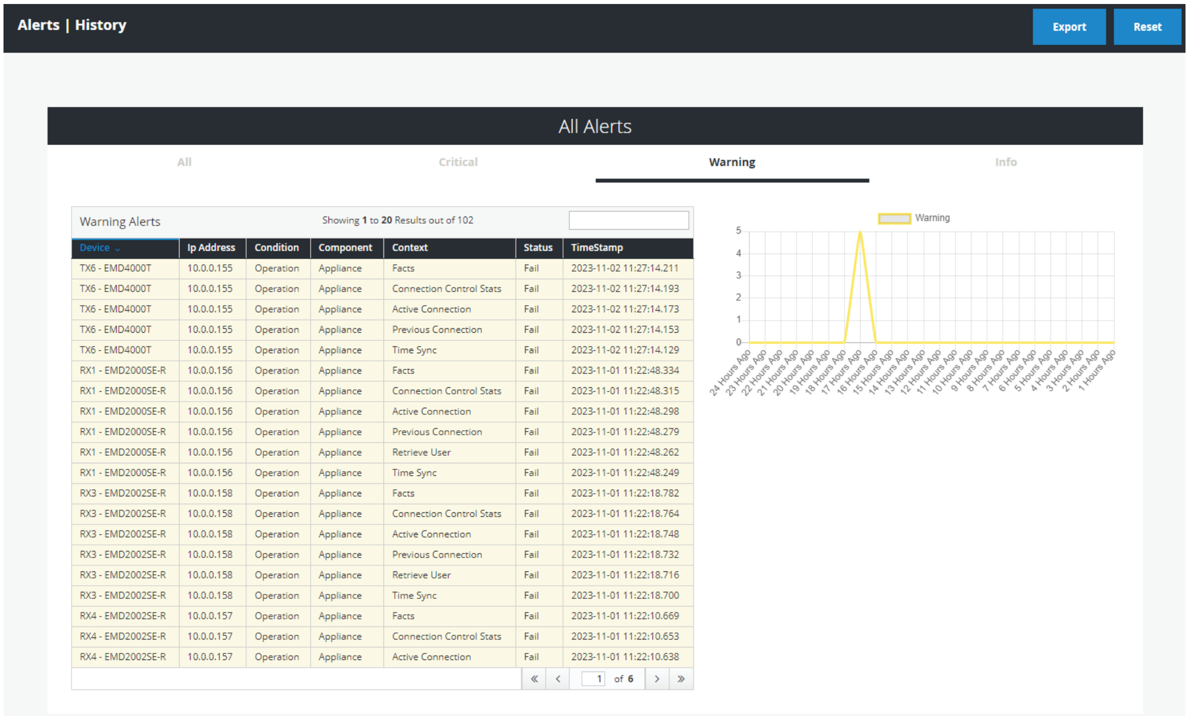
Showing **1** to **20** Results out of 44

Device ⌄	Ip Address	Condition	Component	Context	Status	TimeStamp
DeskVue	10.0.0.161	Availability	Appliance	Audit	OffLine	2023-11-02 19:41:50.203
TX3 - EMD2000SE-T	10.0.0.152	Availability	Appliance	Audit	OffLine	2023-11-02 19:41:50.185
RX1 - EMD2000SE-R	10.0.0.156	Availability	Appliance	Audit	OffLine	2023-11-02 19:41:50.167
RX2 - EMD2002PE-R	10.0.0.159	Availability	Appliance	Audit	OffLine	2023-11-02 19:41:50.148
TX5 - EMD2002PE-DP-T	10.0.0.154	Availability	Appliance	Audit	OffLine	2023-11-02 19:41:50.127
TX4 - EMD2000PE-T-P	10.0.0.153	Availability	Appliance	Audit	OffLine	2023-11-02 19:41:50.105
TX1 - EMD200DV-T	10.0.0.150	Availability	Appliance	Audit	OffLine	2023-11-02 19:41:40.059
RX3 - EMD2002SE-R	10.0.0.158	Availability	Appliance	Audit	OffLine	2023-11-02 19:41:40.025
RX4 - EMD2002SE-R	10.0.0.157	Availability	Appliance	Audit	OffLine	2023-11-02 19:41:39.990
EMS10G28	10.0.0.10	Auto	Switch	Poller	Critical	2023-11-02 11:29:26.187
TX6 - EMD4000T	10.0.0.155	Availability	Appliance	Audit	OffLine	2023-11-02 11:27:18.411
RX5 - EMD4000R	10.0.0.160	Availability	Appliance	Audit	OffLine	2023-11-02 11:26:58.295
EMS10G28	10.0.0.10	Notification	Switch	Equipment	Critical	2023-11-02 07:47:34.454
EMS10G28	10.0.0.10	Notification	Switch	Equipment	Critical	2023-11-02 07:47:34.436
TX6 - EMD4000T	10.0.0.155	Availability	Appliance	Audit	OffLine	2023-11-02 07:44:39.579
EMS10G28	10.0.0.10	Auto	Switch	Poller	Critical	2023-11-02 07:44:14.723
RX5 - EMD4000R	10.0.0.160	Availability	Appliance	Audit	OffLine	2023-11-01 12:12:46.280
TX1 - EMD200DV-T	10.0.0.150	Availability	Appliance	Audit	OffLine	2023-11-01 08:14:21.575
TX3 - EMD2000SE-T	10.0.0.152	Availability	Appliance	Audit	OffLine	2023-11-01 08:14:21.541
TX5 - EMD2002PE-DP-T	10.0.0.154	Availability	Appliance	Audit	OffLine	2023-11-01 08:14:21.498

« ‹ 1 of **3** › »

FIGURE 17-2. CRITICAL

Warning logs are shown next.



Warning Alerts

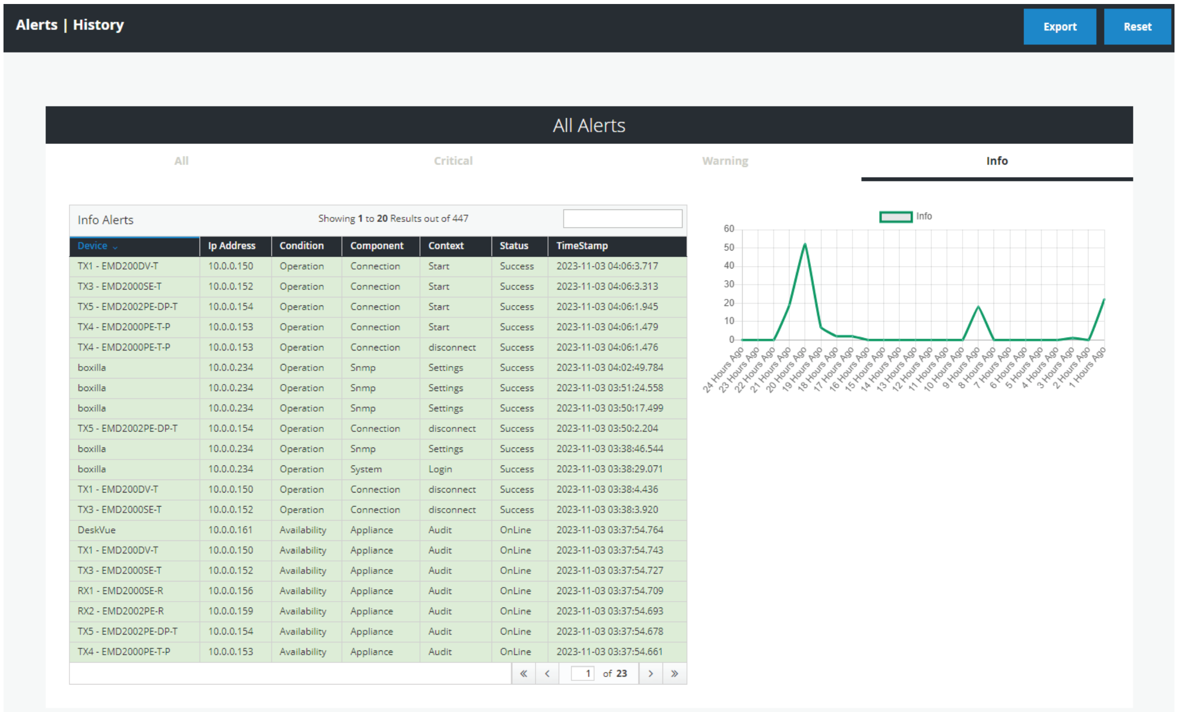
Showing **1** to **20** Results out of 102

Device ⌄	Ip Address	Condition	Component	Context	Status	TimeStamp
TX6 - EMD4000T	10.0.0.155	Operation	Appliance	Facts	Fail	2023-11-02 11:27:14.211
TX6 - EMD4000T	10.0.0.155	Operation	Appliance	Connection Control Stats	Fail	2023-11-02 11:27:14.193
TX6 - EMD4000T	10.0.0.155	Operation	Appliance	Active Connection	Fail	2023-11-02 11:27:14.173
TX6 - EMD4000T	10.0.0.155	Operation	Appliance	Previous Connection	Fail	2023-11-02 11:27:14.153
TX6 - EMD4000T	10.0.0.155	Operation	Appliance	Time Sync	Fail	2023-11-02 11:27:14.129
RX1 - EMD2000SE-R	10.0.0.156	Operation	Appliance	Facts	Fail	2023-11-01 11:22:48.334
RX1 - EMD2000SE-R	10.0.0.156	Operation	Appliance	Connection Control Stats	Fail	2023-11-01 11:22:48.315
RX1 - EMD2000SE-R	10.0.0.156	Operation	Appliance	Active Connection	Fail	2023-11-01 11:22:48.298
RX1 - EMD2000SE-R	10.0.0.156	Operation	Appliance	Previous Connection	Fail	2023-11-01 11:22:48.279
RX1 - EMD2000SE-R	10.0.0.156	Operation	Appliance	Retrieve User	Fail	2023-11-01 11:22:48.262
RX1 - EMD2000SE-R	10.0.0.156	Operation	Appliance	Time Sync	Fail	2023-11-01 11:22:48.249
RX3 - EMD2002SE-R	10.0.0.158	Operation	Appliance	Facts	Fail	2023-11-01 11:22:18.782
RX3 - EMD2002SE-R	10.0.0.158	Operation	Appliance	Connection Control Stats	Fail	2023-11-01 11:22:18.764
RX3 - EMD2002SE-R	10.0.0.158	Operation	Appliance	Active Connection	Fail	2023-11-01 11:22:18.748
RX3 - EMD2002SE-R	10.0.0.158	Operation	Appliance	Previous Connection	Fail	2023-11-01 11:22:18.732
RX3 - EMD2002SE-R	10.0.0.158	Operation	Appliance	Retrieve User	Fail	2023-11-01 11:22:18.716
RX3 - EMD2002SE-R	10.0.0.158	Operation	Appliance	Time Sync	Fail	2023-11-01 11:22:18.700
RX4 - EMD2002SE-R	10.0.0.157	Operation	Appliance	Facts	Fail	2023-11-01 11:22:10.669
RX4 - EMD2002SE-R	10.0.0.157	Operation	Appliance	Connection Control Stats	Fail	2023-11-01 11:22:10.653
RX4 - EMD2002SE-R	10.0.0.157	Operation	Appliance	Active Connection	Fail	2023-11-01 11:22:10.638

« ‹ 1 of **6** › »

FIGURE 17-3. WARNING

Info alerts can also be viewed.



Info Alerts

Showing **1** to **20** Results out of 447

Device ⌄	Ip Address	Condition	Component	Context	Status	TimeStamp
TX1 - EMD200DV-T	10.0.0.150	Operation	Connection	Start	Success	2023-11-03 04:06:3.717
TX3 - EMD2000SE-T	10.0.0.152	Operation	Connection	Start	Success	2023-11-03 04:06:3.313
TX5 - EMD2002PE-DP-T	10.0.0.154	Operation	Connection	Start	Success	2023-11-03 04:06:1.945
TX4 - EMD2000PE-T-P	10.0.0.153	Operation	Connection	Start	Success	2023-11-03 04:06:1.479
TX4 - EMD2000PE-T-P	10.0.0.153	Operation	Connection	disconnect	Success	2023-11-03 04:06:1.476
boxilla	10.0.0.234	Operation	Snmp	Settings	Success	2023-11-03 04:02:49.784
boxilla	10.0.0.234	Operation	Snmp	Settings	Success	2023-11-03 03:51:24.558
boxilla	10.0.0.234	Operation	Snmp	Settings	Success	2023-11-03 03:50:17.499
TX5 - EMD2002PE-DP-T	10.0.0.154	Operation	Connection	disconnect	Success	2023-11-03 03:50:2.204
boxilla	10.0.0.234	Operation	Snmp	Settings	Success	2023-11-03 03:38:46.544
boxilla	10.0.0.234	Operation	System	Login	Success	2023-11-03 03:38:29.071
TX1 - EMD200DV-T	10.0.0.150	Operation	Connection	disconnect	Success	2023-11-03 03:38:4.436
TX3 - EMD2000SE-T	10.0.0.152	Operation	Connection	disconnect	Success	2023-11-03 03:38:3.920
DeskVue	10.0.0.161	Availability	Appliance	Audit	OnLine	2023-11-03 03:37:54.764
TX1 - EMD200DV-T	10.0.0.150	Availability	Appliance	Audit	OnLine	2023-11-03 03:37:54.743
TX3 - EMD2000SE-T	10.0.0.152	Availability	Appliance	Audit	OnLine	2023-11-03 03:37:54.727
RX1 - EMD2000SE-R	10.0.0.156	Availability	Appliance	Audit	OnLine	2023-11-03 03:37:54.709
RX2 - EMD2002PE-R	10.0.0.159	Availability	Appliance	Audit	OnLine	2023-11-03 03:37:54.693
TX5 - EMD2002PE-DP-T	10.0.0.154	Availability	Appliance	Audit	OnLine	2023-11-03 03:37:54.678
TX4 - EMD2000PE-T-P	10.0.0.153	Availability	Appliance	Audit	OnLine	2023-11-03 03:37:54.661

FIGURE 17-4. INFO

17.2 ALERTS—ACTIVE

Active Alerts are alerts that are currently active, e.g. devices that are offline, thresholds that are exceeded, and devices with mis-matched software versions.

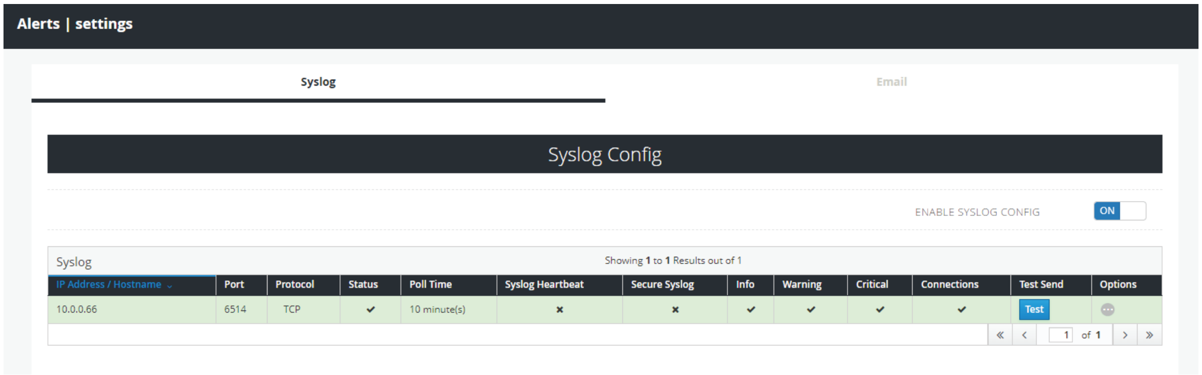
These active alerts are cleared when the devices are back online, device metrics return to below threshold levels, and devices are upgraded to the domain's active firmware version.

17.3 SYSLOG

Syslog supports the configurable generation of Alert History event and Active Connection statistics to an external Syslog Server.

The administrator can use an external SYSLOG server to capture all of the alert details. During the configuration of the SYSLOG server, you can select which alerts you would like to capture on the remote SYLOG server (Info, Warning, Critical, Connections. Secure SYSLOG is also supported.

The Secure SYSLOG uses port 6514 by default, and, when enabled, the CA Certificate and Authentication Mode options become available.



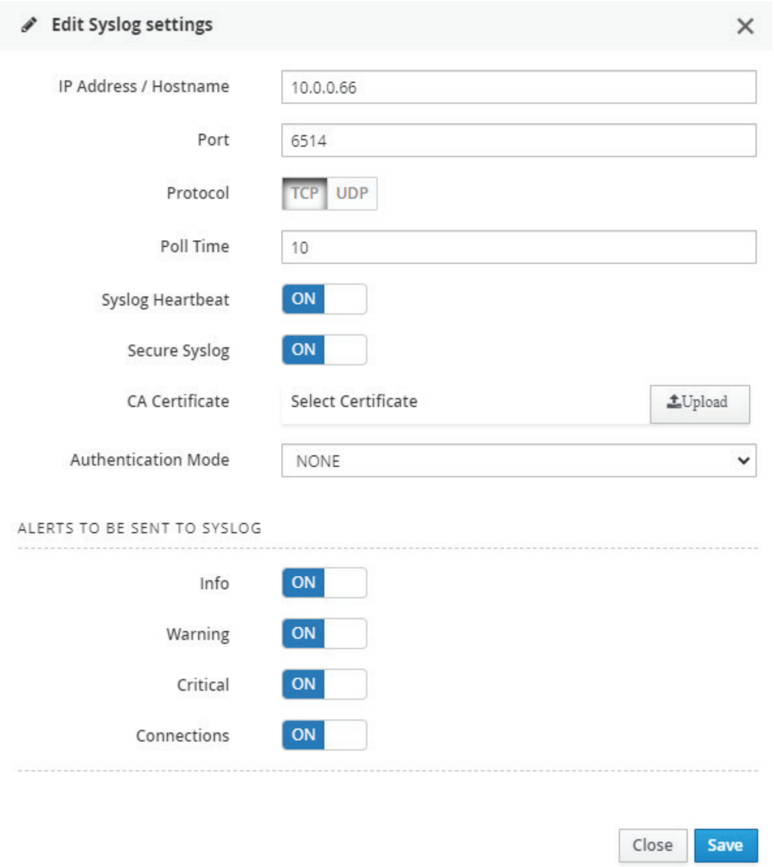
Syslog Config

ENABLE SYSLOG CONFIG: ON

Syslog — Showing **1** to **1** Results out of 1

IP Address / Hostname	Port	Protocol	Status	Poll Time	Syslog Heartbeat	Secure Syslog	Info	Warning	Critical	Connections	Test Send	Options
10.0.0.66	6514	TCP	✓	10 minute(s)	✗	✗	✓	✓	✓	✓	Test	⋯

FIGURE 17-5. SYSLOG



Edit Syslog settings

IP Address / Hostname	10.0.0.66
Port	6514
Protocol	TCP UDP
Poll Time	10
Syslog Heartbeat	ON
Secure Syslog	ON
CA Certificate	Select Certificate
Authentication Mode	NONE

ALERTS TO BE SENT TO SYSLOG

Info	ON
Warning	ON
Critical	ON
Connections	ON

FIGURE 17-6. ADD SYSLOG SERVER

- IP Address/Hostname – This is the IP address or hostname of the server where the external syslog server is running.
- Port – The port the syslog server is listening on.
- Protocol – Select TCP or UDP depending on the SYSLOG configuration.
- Poll time – Poll time sets how often (in minutes) active connections will send connection stats to the syslog server.
- Syslog Heartbeat –A heartbeat that works in conjunction with the Poll time can be enabled. It allows Boxilla® to send out a heartbeat SYSLOG notification to let other systems know that it is still online.
- Secure Syslog – Turning this on allows additional configuration.
- CA Certificate – This generated by the user, so it can be imported.
- Authentication Mode – Set None, Validity, or Name based upon the configuration of the SYSLOG server.
- Alerts to be sent to syslog — You can limit what type of alerts are sent to the syslog server by turning these options on/off.

NOTE: Black Box can provide a technical document with detailed steps on how to configure Secure SYSLOG. If you need this, contact our tech support team.

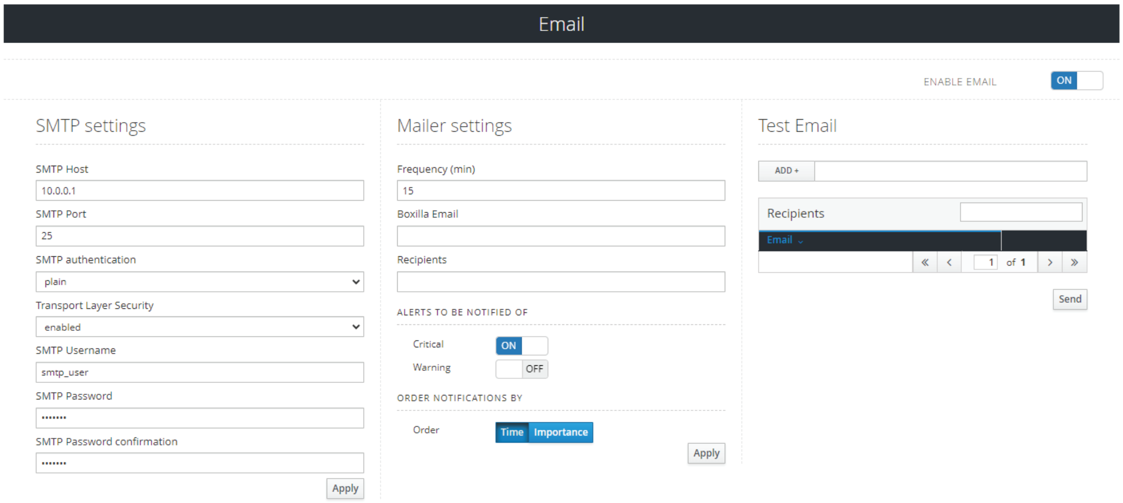
17.4 ALERTS — SETTINGS — EMAIL

An administrator can configure an SMTP server that is a mail system for logging. This page also offers additional settings to send the Boxilla® admin emails on system info/alerts.

1) SMTP stands for Simple Mail Transfer Protocol. The Boxilla offers the SMTP configuration to allow a user to enter their mail server information so that the Boxilla can properly communicate with the server using the protocol. The information required here is used to find and authenticate against the mail server so that a communication link can be made.

2) Mailer Settings allows the Boxilla administrator to configure who the email is from and who it is going to, and how often to check. You may also configure what alerts (critical and/or information) are in the message.

3) Test Email allows the Boxilla administrator to perform a quick verification of the SMTP setting to make sure the emails are getting through properly without having to wait for an actual alert to be sent. This Test Email feature is typically used at the time of configuration and during troubleshooting.



Email

ENABLE EMAIL: ON

SMTP settings

SMTP Host: 10.0.0.1
SMTP Port: 25
SMTP authentication: plain
Transport Layer Security: enabled
SMTP Username: smtp_user
SMTP Password: •••••••
SMTP Password confirmation: •••••••

Mailer settings

Frequency (min): 15
Boxilla Email:
Recipients:

ALERTS TO BE NOTIFIED OF
Critical: ON
Warning: OFF

ORDER NOTIFICATIONS BY
Order: Time Importance

Test Email

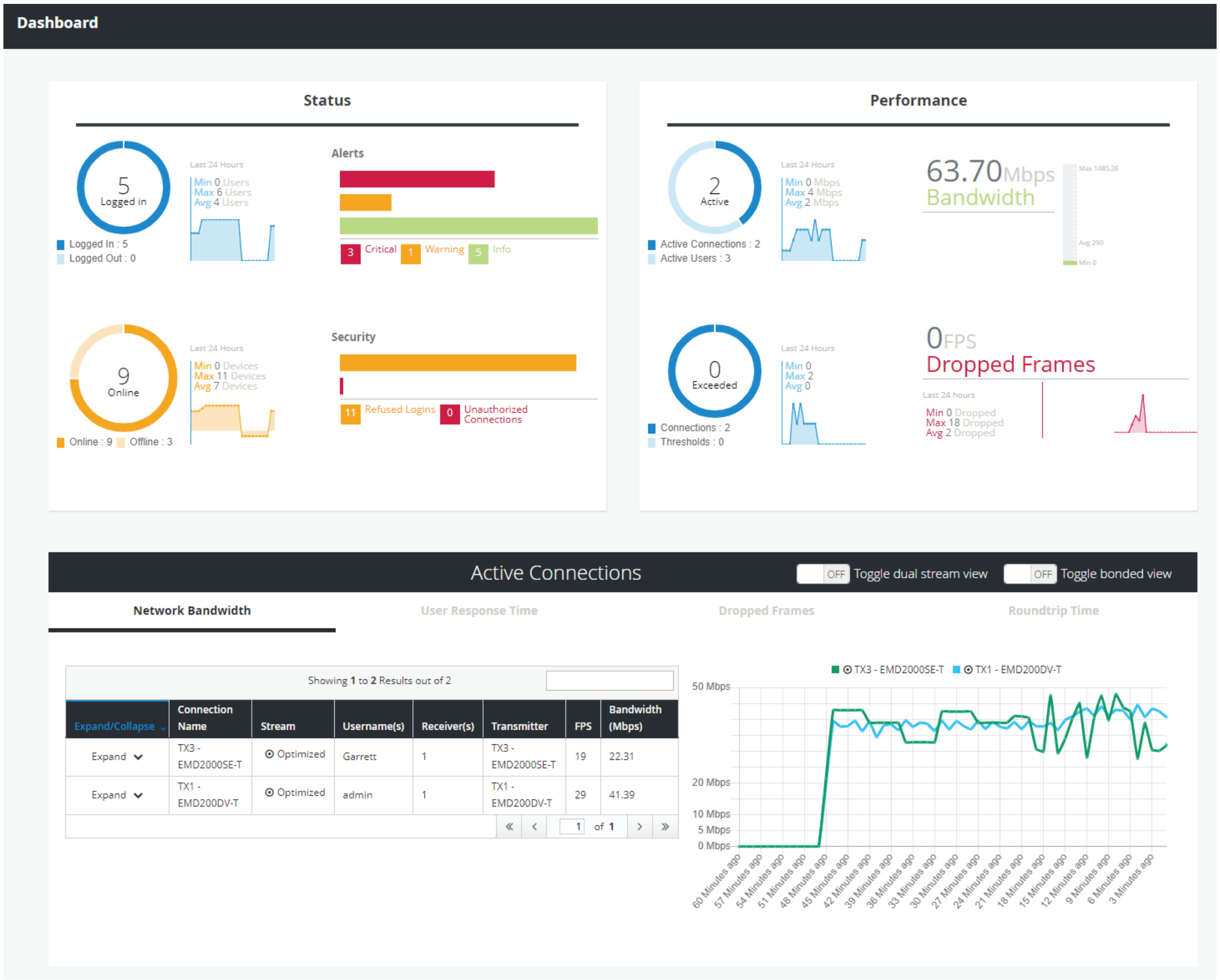
Recipients
Email
1 of 1

FIGURE 17-7. ALERTS — SETTINGS — EMAIL

CHAPTER 18: DASHBOARD

The dashboard is divided into three main areas: Status & Performance Indicators, Active Connections and Active Logins.

18.1 STATUS AND PERFORMANCE INDICATORS



Showing **1** to **2** Results out of 2

Expand/Collapse	Connection Name	Stream	Username(s)	Receiver(s)	Transmitter	FPS	Bandwidth (Mbps)
Expand	TX3 - EMD2000SE-T	⦿ Optimized	Garrett	1	TX3 - EMD2000SE-T	19	22.31
Expand	TX1 - EMD200DV-T	⦿ Optimized	admin	1	TX1 - EMD200DV-T	29	41.39

« ‹ 1 of **1** › »

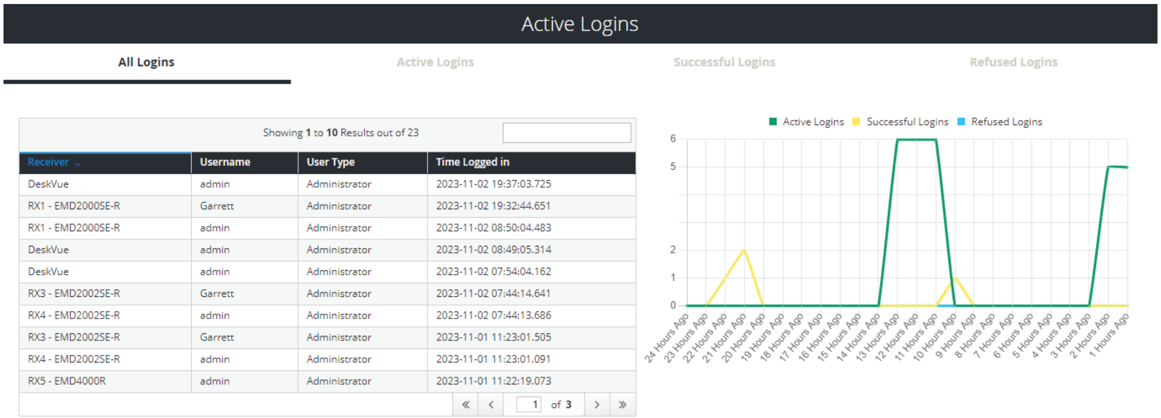
FIGURE 18-1. DASHBOARD TOP

The Status and Performance Indicators are defined as:

Status:

1. Logged-In—number of users currently logged-in is displayed in the center of ring. The Ring shows the number of users logged-in on Receivers and the number of Receiver units with no one logged-in (i.e. shows % of Receiver units that have a user logged in).

The graph portion of the Logged-In indicator shows the minimum, maximum and average number of users logged-in over the last 24 hours and a graph of number logged-in over the last 24-hours.



Showing **1** to **10** Results out of 23

Receiver ⌄	Username	User Type	Time Logged in
DeskVue	admin	Administrator	2023-11-02 19:37:03.725
RX1 - EMD2000SE-R	Garrett	Administrator	2023-11-02 19:32:44.651
RX1 - EMD2000SE-R	admin	Administrator	2023-11-02 08:50:04.483
DeskVue	admin	Administrator	2023-11-02 08:49:05.314
DeskVue	admin	Administrator	2023-11-02 07:54:04.162
RX3 - EMD2002SE-R	Garrett	Administrator	2023-11-02 07:44:14.641
RX4 - EMD2002SE-R	admin	Administrator	2023-11-02 07:44:13.686
RX3 - EMD2002SE-R	Garrett	Administrator	2023-11-01 11:23:01.505
RX4 - EMD2002SE-R	admin	Administrator	2023-11-01 11:23:01.091
RX5 - EMD4000R	admin	Administrator	2023-11-01 11:22:19.073

« ‹ 1 of **3** › »

FIGURE 18-2. ACTIVE LOGINS

2. Devices Online—the number of devices (Receivers and Transmitter units) in the managed domain at this time that are online is displayed in the center of the ring. The Ring shows the number of devices in the managed domain that are online and offline. A device is considered online if Boxilla® can contact it over the network—and offline if not contactable.

The graph portion of the Devices Online indicator shows the minimum, maximum and average number of devices online over the last 24 hours and a graph of number devices online over the last 24-hours.

3. Alerts—the number of alerts in each category of Critical, Warning and Info (see section 11 for definition of the different categories).

4. Security—the number of Refused Logins and the number of Unauthorized Connections. Refused Logins are counted on each Receiver when a user fails a login attempt. Unauthorized Connections are counted on Receivers and Transmitters when they detected something has attempted to connect to them in an unauthorized manner—such as devices not part of our managed domain trying to connect to a managed device or an attempt to access a service using a network protocol not authorized on a device (SSH, SNMP, etc.) as may occur during a port-scan attack.

Performance:

1. Active Connections—number of currently Active connections is displayed in center of Ring. The Ring shows the number of Active connections on Receiver units with Active Users (i.e. logged in) and the number of Receivers with no connection that have users logged in. If using Dual-Stream (4K receiver and 2K receiver connected to a 4K target), the Dashboard will show the two connections which can then be expanded to see more information.

The graph portion of the Active Connections indicator shows the minimum, maximum and average number of Active Connections over the last 24 hours and a graph of Active Connections over the last 24 hours.

2. Threshold Exceeded —the number of connections with a threshold exceeded is shown in the center of the Ring. The thresholds are defined in section 11.4. The Ring shows the number of active connections that have a threshold exceeded and the number of connections with no threshold exceeded.

The graph portion of the Threshold Exceeded indicator shows the minimum, maximum and average number of connections with a threshold exceeded over the last 24 hours and a graph of number connections with a threshold exceeded over the last 24 hours.

3. Bandwidth— the current total network bandwidth generated by the devices in the domain (i.e., the sum of the network bandwidth of all the active connections) is displayed as a number on the indicator.

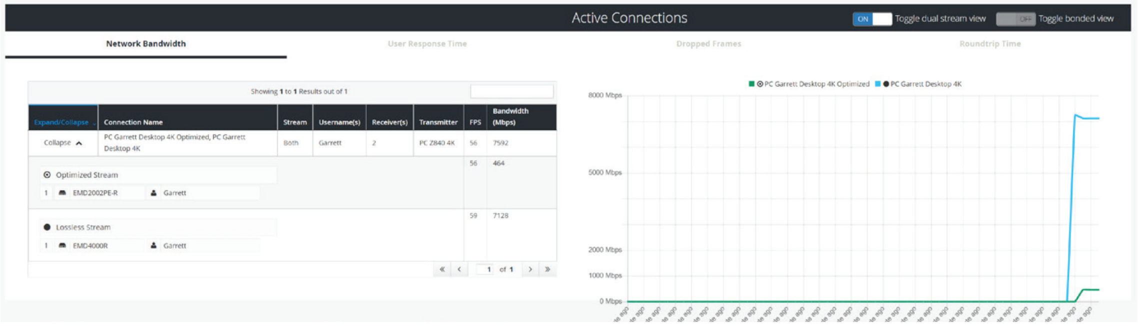
The graph portion of the Bandwidth indicator shows the minimum, maximum and average total bandwidth last 24 hours.

4. Dropped Frames— the current number of dropped frames summed across all active connections in frames-per-seconds.

The graph portion of the Dropped Frames indicator shows the minimum, maximum and average number of Dropped Frames across all active connection over the last 24 hours and a graph of Dropped Frames across all active connection over the last 24 hours.

18.2 ACTIVE CONNECTIONS

The Active Connections section of the dashboard displays the 10 most active connections based upon bandwidth usage in the managed domain. The table portion provides a sortable list of the active connections. Each column can be used to sort the table—in ascending or descending order—just click on a column header to sort and click again to invert sort order. The filter box at the top right of the table will filter the table based on the filter box contents.



Showing 1 to 1 Results out of 1

Expand/Collapse	Connection Name	Stream	Username(s)	Receiver(s)	Transmitter	FPS	Bandwidth (Mbps)
Collapse ^	PC Garrett Desktop 4K Optimized, PC Garrett Desktop 4K	Both	Garrett	2	PC Z840 4K	56	7592
⦿ Optimized Stream 1 EMD2002PE-R Garrett						56	464
● Lossless Stream 1 EMD4000R Garrett						59	7128

« ‹ 1 of 1 › »

FIGURE 18-3. ACTIVE CONNECTION VIEW

The Active Connection view in this example shows an active Dual-Stream connection where a 4K and 2K receiver are accessing a 4K Connection

The first five columns of the table are fixed for all the tabs that can be selected (Network Bandwidth, User Response, Dropped Frames or Roundtrip Time). The columns are defined as:

- Connection Name—the name of the active connection
- User Name—the user name logged into the Receiver that has initiated the active connection
- Receiver—the name of the Receiver on the active connection
- Transmitter—the name of the Transmitter on the active connection
- FPS—the current frames per second being encoded/transferred on the connection

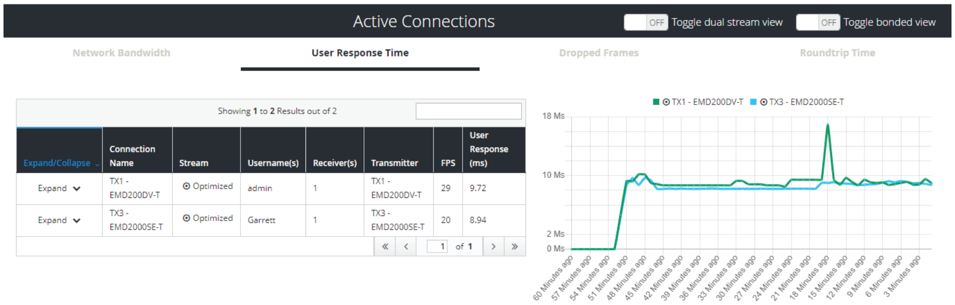
The contents of the last column in the table will vary depending on the tab selected—Network Bandwidth, User Response, Dropped Frames or Roundtrip Time.

The last column displays when the selected tab is:

- Network Bandwidth—the total network bandwidth that this connection is generating (in Mbps). Typically, 0 Mbps for a static screen and up to 250 Mbps when playing a 1080p video.

  NOTE: 4K connections can consume up to 9.5Gbps.

- User-Response Time—the time it takes for an event on the server to be displayed on the Monitor attached to the receiver. This includes video encode time in the Transmitter, network latency and video decode time in the Receiver as part of its calculation (in milliseconds). Typically 8–16 ms but can grow to 20–30 ms on congested networks due to dropped frames.

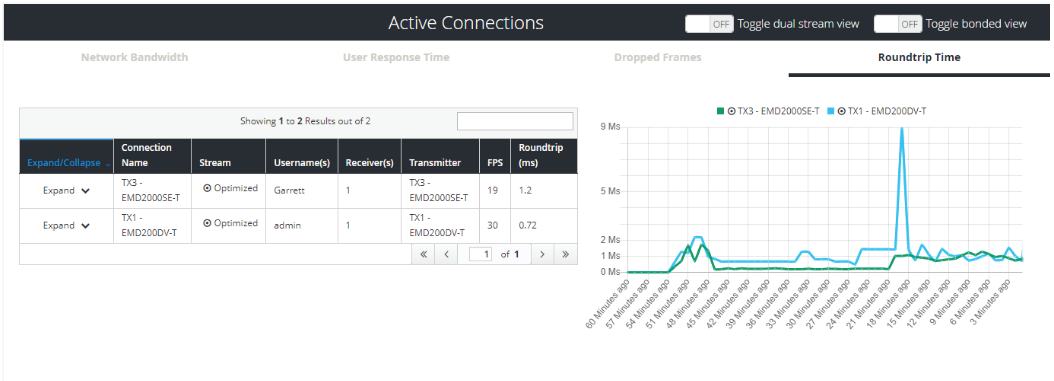


Showing **1** to **2** Results out of 2

Expand/Collapse	Connection Name	Stream	Username(s)	Receiver(s)	Transmitter	FPS	User Response (ms)
Expand	TX1 - EMD200DV-T	⊙ Optimized	admin	1	TX1 - EMD200DV-T	29	9.72
Expand	TX3 - EMD2000SE-T	⊙ Optimized	Garrett	1	TX3 - EMD2000SE-T	20	8.94

FIGURE 18-4. USER RESPONSE TIME

- Dropped Frames—the number of dropped frames in the Transmitter that is part of this connection. Dropped frames usually result from network congestion (in frames-per-second). Typically will be 0 fps.
- Round-trip time—measures the network round-trip time experienced at an IP packet level for the active connection (in milliseconds). Typically this will be 0 ms on a gigabit network with low congestion.



Showing **1** to **2** Results out of 2

Expand/Collapse	Connection Name	Stream	Username(s)	Receiver(s)	Transmitter	FPS	Roundtrip (ms)
Expand	TX3 - EMD2000SE-T	⊙ Optimized	Garrett	1	TX3 - EMD2000SE-T	19	1.2
Expand	TX1 - EMD200DV-T	⊙ Optimized	admin	1	TX1 - EMD200DV-T	30	0.72

FIGURE 18-5. ROUNDTRIP TIME

The graph part of the Active Connections dashboard displays a graph of the last column over time, so it can be network bandwidth, user-response time, dropped frames per second or roundtrip time.

18.3 ACTIVE LOGINS

The Active Logins section of the dashboard displays the current active logins in the managed domain. The table portion provides a sortable list of the active connections. Each column can be used to sort the table— in ascending or descending order—just click on column header to sort and click again to invest sort order. The filter box at the top right of the table will filter the table based on the filter box contents.

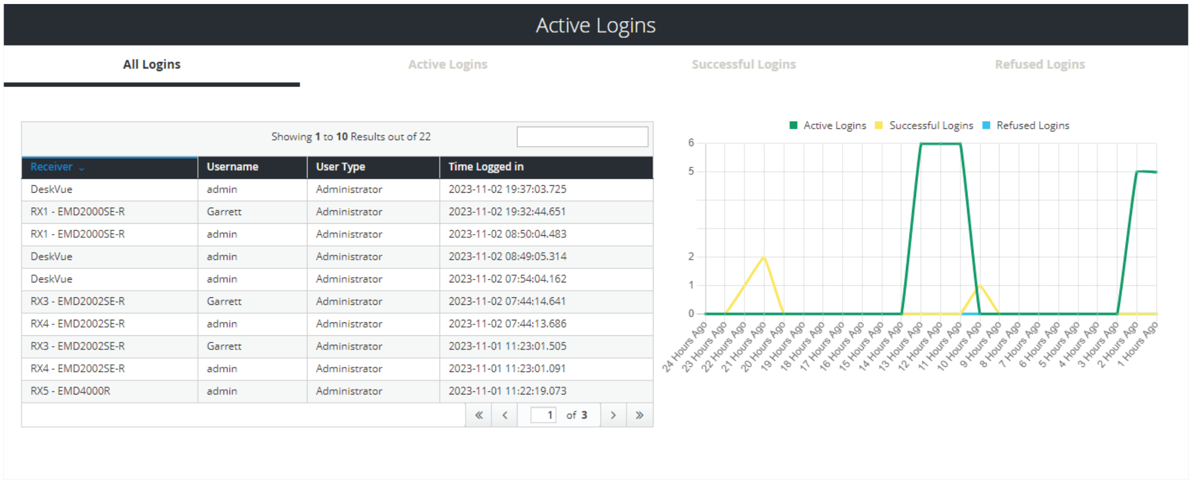
The table portion has the following columns:

- Receiver— the receiver name that has been logged into

- Username—the user name that has logged into the Receiver
- User-Type—the type of user that has logged in: administrator, Power User, User (see section 9.1 for definitions of user types)
- Time Logged In —when the user logged-in
- Duration—how long the user has been logged-in

There are four tabs in the Active Logins section:

- All Logins—all logins and attempts

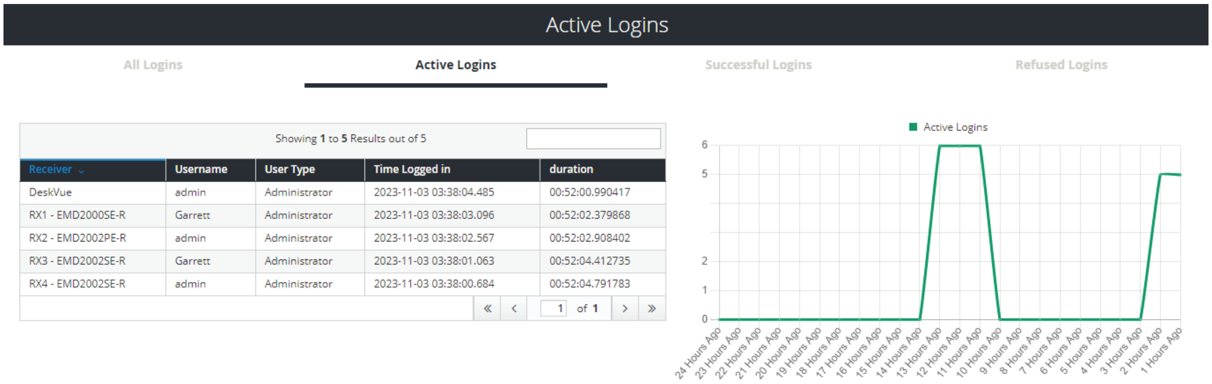


Showing **1** to **10** Results out of 22

Receiver ⌄	Username	User Type	Time Logged in
DeskVue	admin	Administrator	2023-11-02 19:37:03.725
RX1 - EMD2000SE-R	Garrett	Administrator	2023-11-02 19:32:44.651
RX1 - EMD2000SE-R	admin	Administrator	2023-11-02 08:50:04.483
DeskVue	admin	Administrator	2023-11-02 08:49:05.314
DeskVue	admin	Administrator	2023-11-02 07:54:04.162
RX3 - EMD2002SE-R	Garrett	Administrator	2023-11-02 07:44:14.641
RX4 - EMD2002SE-R	admin	Administrator	2023-11-02 07:44:13.686
RX3 - EMD2002SE-R	Garrett	Administrator	2023-11-01 11:23:01.505
RX4 - EMD2002SE-R	admin	Administrator	2023-11-01 11:23:01.091
RX5 - EMD4000R	admin	Administrator	2023-11-01 11:22:19.073

FIGURE 18-6. DASHBOARD BOTTOM

- Active Logins—all current active logins

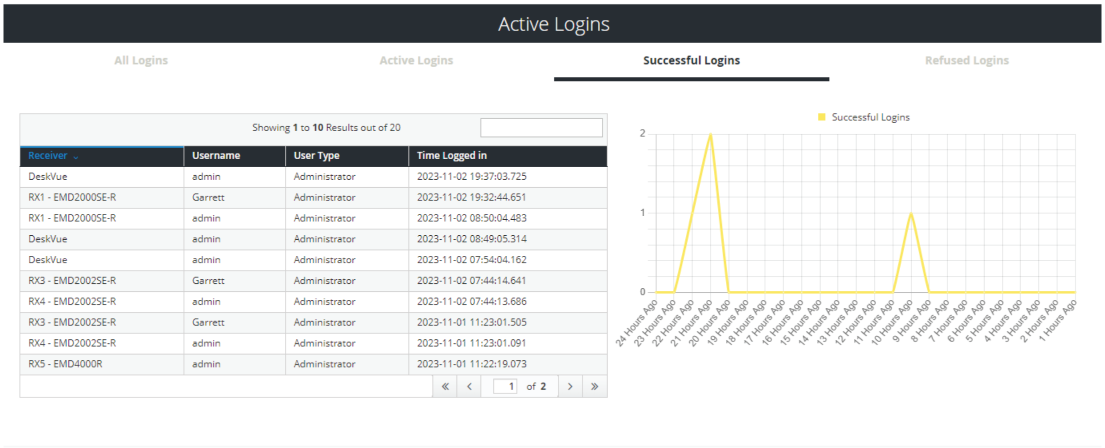


Showing **1** to **5** Results out of 5

Receiver ⌄	Username	User Type	Time Logged in	duration
DeskVue	admin	Administrator	2023-11-03 03:38:04.485	00:52:00.990417
RX1 - EMD2000SE-R	Garrett	Administrator	2023-11-03 03:38:03.096	00:52:02.379868
RX2 - EMD2002PE-R	admin	Administrator	2023-11-03 03:38:02.567	00:52:02.908402
RX3 - EMD2002SE-R	Garrett	Administrator	2023-11-03 03:38:01.063	00:52:04.412735
RX4 - EMD2002SE-R	admin	Administrator	2023-11-03 03:38:00.684	00:52:04.791783

FIGURE 18-7. ACTIVE LOGINS

- Successful Logins—all Successful logins, both currently active logins and previous ones



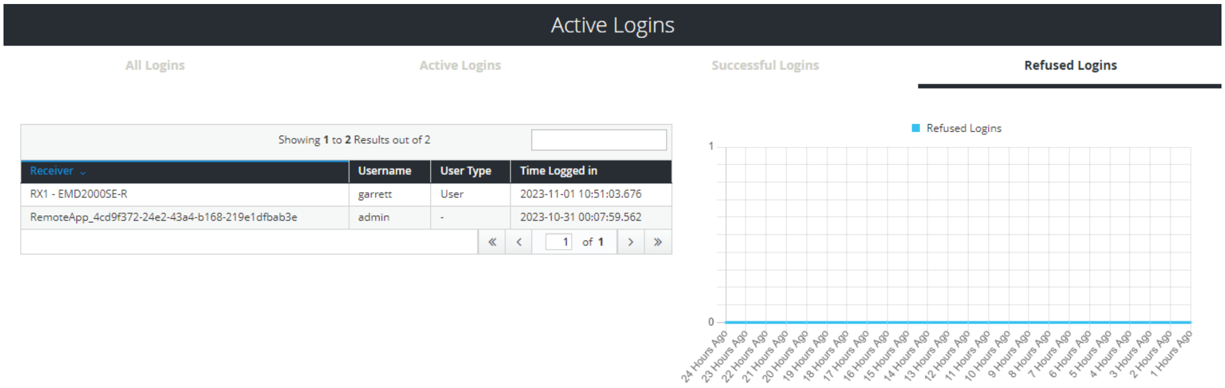
Showing **1** to **10** Results out of 20

Receiver	Username	User Type	Time Logged in
DeskVue	admin	Administrator	2023-11-02 19:37:03.725
RX1 - EMD2000SE-R	Garrett	Administrator	2023-11-02 19:32:44.651
RX1 - EMD2000SE-R	admin	Administrator	2023-11-02 08:50:04.483
DeskVue	admin	Administrator	2023-11-02 08:49:05.314
DeskVue	admin	Administrator	2023-11-02 07:54:04.162
RX3 - EMD2002SE-R	Garrett	Administrator	2023-11-02 07:44:14.641
RX4 - EMD2002SE-R	admin	Administrator	2023-11-02 07:44:13.686
RX3 - EMD2002SE-R	Garrett	Administrator	2023-11-01 11:23:01.505
RX4 - EMD2002SE-R	admin	Administrator	2023-11-01 11:23:01.091
RX5 - EMD4000R	admin	Administrator	2023-11-01 11:22:19.073

« ‹ 1 of **2** › »

FIGURE 18-8. SUCCESSFUL LOGINS

- Refused Logins—all refused logins



Showing **1** to **2** Results out of 2

Receiver	Username	User Type	Time Logged in
RX1 - EMD2000SE-R	garrett	User	2023-11-01 10:51:03.676
RemoteApp_4cd9f372-24e2-43a4-b168-219e1dfbab3e	admin	-	2023-10-31 00:07:59.562

« ‹ 1 of **1** › »

FIGURE 18-9. REFUSED LOGINS

The graph part of the Active Logins dashboard displays a graph of the selected tab information over time.

CHAPTER 19: REPLACING YOUR BOXILLA

This section defines what an Administrator should do to ensure the Boxilla® unit can be replaced and the system restored with its previous settings.

A key maintenance task is for the Administrator to backup the system so the system can be restored to a known state. See section 14.4.

1. Remove the original Boxilla from the network. Connect the new Boxilla in its place and power up.
2. Before connecting the new Boxilla unit to the main network, connect the Boxilla unit to a network switch that is isolated from the main network.
3. Use a computer connected to the same switch to login to the new Boxilla Unit.
4. Set the IP address of the Boxilla unit to match that of the original unit. (Ideally, you have all this done in advance of failure.)
5. Add Licenses to the new Boxilla unit, if required.
6. Restore a backup file of the original Boxilla database to the new device.
7. Navigate to Devices | Settings page, and all devices should appear as OnLine after 10 seconds.
8. The replacement Boxilla unit is now operational.

NOTES

THIS PAGE IS INTENTIONALLY LEFT BLANK

APPENDIX A: BOXILLA DISCOVERY

A.1 BOXILLA DISCOVERY

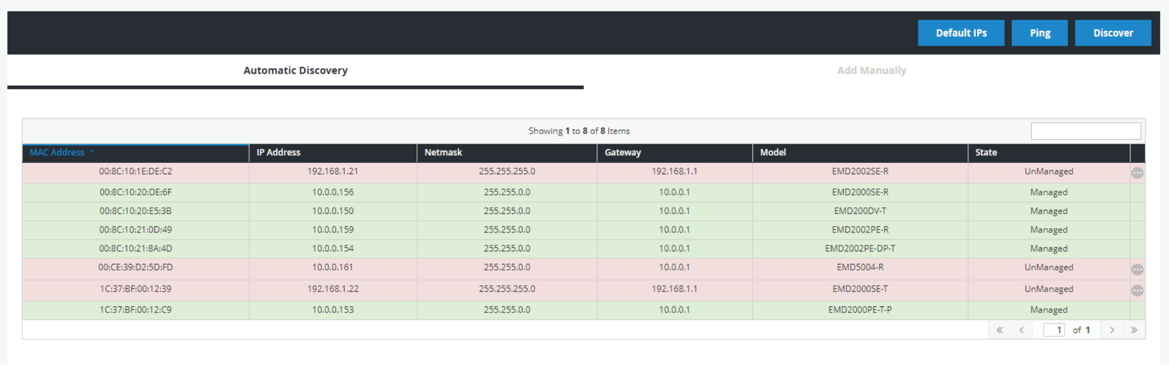
The Emerald® DESKVUE unit can be discovered and managed by the Boxilla® manager as long as it is using the DESKVUE firmware version 1.1.0.r94 or later **and** the Boxilla unit is using firmware version 4.7.0 or later. Older firmware versions do not support integrating DESKVUE and Boxilla.

NOTE: If the DESKVUE unit is managed by another Boxilla Manager, it will need to be factory reset prior to performing the Boxilla Discovery process.

A.1.1 DISCOVERING AND MANAGING THE DESKVUE UNIT

To discover and manage the DESKVUE unit through the Boxilla Manager:

1. Verify that the DESKVUE unit is turned on.
2. Verify that the the DESKVUE unit is connected to the network so that Boxilla can detect it.
3. Verify that the IP Address (192.168.1.1) is not in use. Otherwise, the Boxilla discovery process will not work.
4. In the Boxilla administrative interface, go to Discovery and press the "Discovery" button. The DESKVUE unit should then be discovered and show as Unmanaged under model EMD5004-R, as shown in Figure A-1 below:



Showing **1** to **8** of **8** Items

MAC Address ^	IP Address	Netmask	Gateway	Model	State
00:8C:10:1E:DE:C2	192.168.1.21	255.255.255.0	192.168.1.1	EMD2002SE-R	UnManaged
00:8C:10:20:DE:6F	10.0.0.156	255.255.0.0	10.0.0.1	EMD2000SE-R	Managed
00:8C:10:20:E5:3B	10.0.0.150	255.255.0.0	10.0.0.1	EMD200DV-T	Managed
00:8C:10:21:0D:49	10.0.0.159	255.255.0.0	10.0.0.1	EMD2002PE-R	Managed
00:8C:10:21:8A:4D	10.0.0.154	255.255.0.0	10.0.0.1	EMD2002PE-DP-T	Managed
00:CE:39:D2:5D:FD	10.0.0.161	255.255.0.0	10.0.0.1	EMD5004-R	UnManaged
1C:37:BF:00:12:39	192.168.1.22	255.255.255.0	192.168.1.1	EMD2000SE-T	UnManaged
1C:37:BF:00:12:C9	10.0.0.153	255.255.0.0	10.0.0.1	EMD2000PE-T-P	Managed

1 of 1

FIGURE A-1: DETECTED DESKVUE UNIT SHOWING AS UNMANAGED

5. Change the Emerald® DESKVUE network settings, if necessary, through the Boxilla® web interface by selecting “Edit” from the drop-down menu shown in Figure A-2 below:

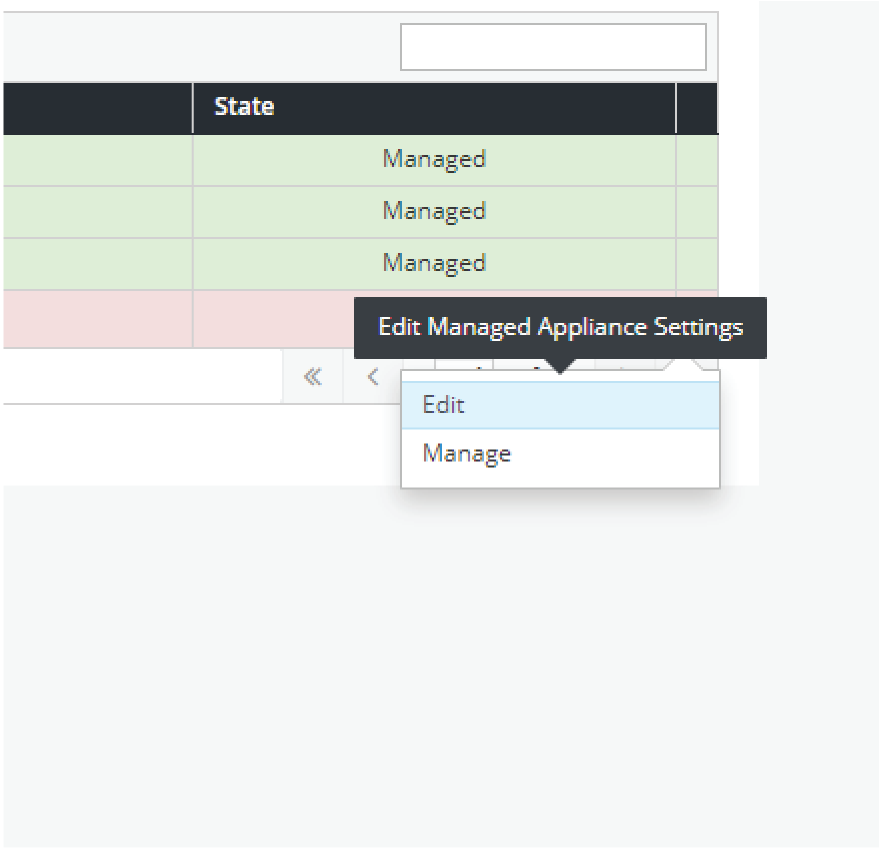
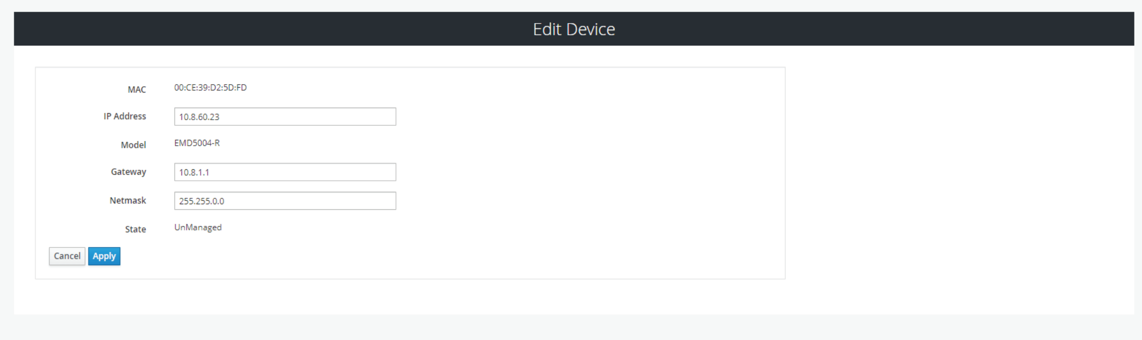


FIGURE A-2: EDIT OPTION

6. Configure the network settings for the Emerald® DESKVUE unit using the "Edit Device" screen, shown in Figure A-3 below:



MAC 00:CE:39:D2:5D:FD

IP Address 10.8.60.23

Model EMD5004-R

Gateway 10.8.1.1

Netmask 255.255.0.0

State UnManaged

FIGURE A-3: EDIT DEVICE SCREEN

NOTE: Use network settings that allow the DESKVUE unit and Boxilla® Manager to be on the same subnet/network.

7. Click on the "Apply" button to accept your changes.

8. After the system returns to the Discovery page in the Boxilla® Manager, manage the Emerald® DESKVUE unit by using the "Manage" option in the drop-down menu, as shown in Figure A-4 below:

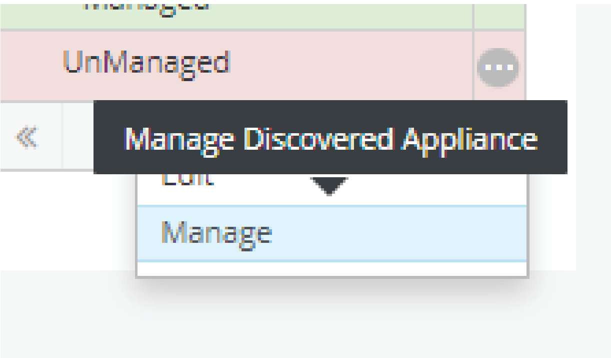
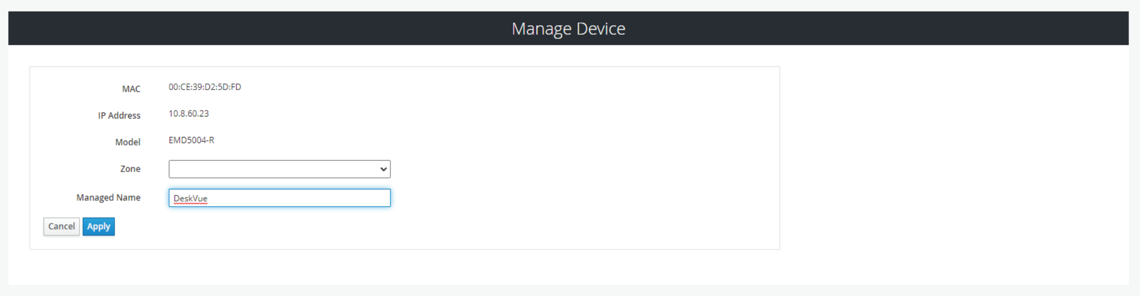


FIGURE A-4: EDIT AND MANAGE OPTIONS ON DROP-DOWN MENU

Before the DESKVUE can be managed, a managed name must be assigned to it so it can be referenced. This name is visible in the Boxilla interface only, and it is not the name of the connection. Optionally, the zone can be configured if the application requires it. Once done configuring the zone and managed name, click on the "Apply" button, as shown in Figure A-5 below:

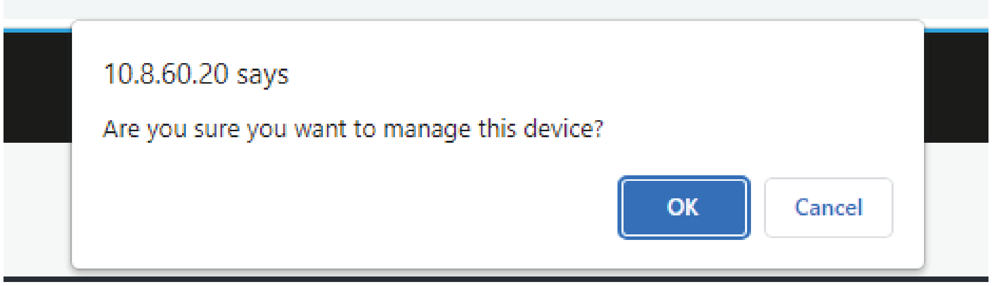


Manage Device

MAC	00:CE:39:D2:5D:FD
IP Address	10.8.60.23
Model	EMD5004-R
Zone	
Managed Name	DeskVue

FIGURE A-5: APPLY BUTTON

After you click on the "Apply" button, the system may display a confirmation message, as shown in Figure A-6 below:

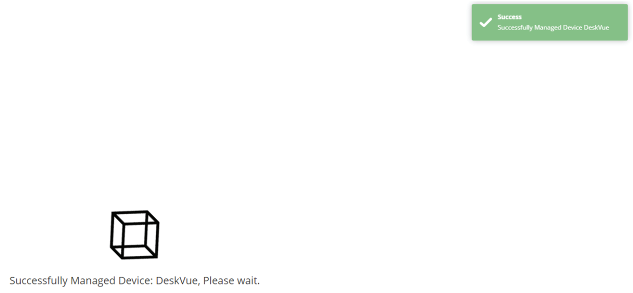


10.8.60.20 says

Are you sure you want to manage this device?

FIGURE A-6: DEVICE MANAGEMENT CONFIRMATION MESSAGE

9. Click on the “OK” button shown in Figure A-6 above to enable Boxilla® to manage the Emerald® DESKVUE unit. The system should display a confirmation message stating that the operation was successful, as shown in Figure A-7 below:



Success
Successfully Managed Device DeskVue

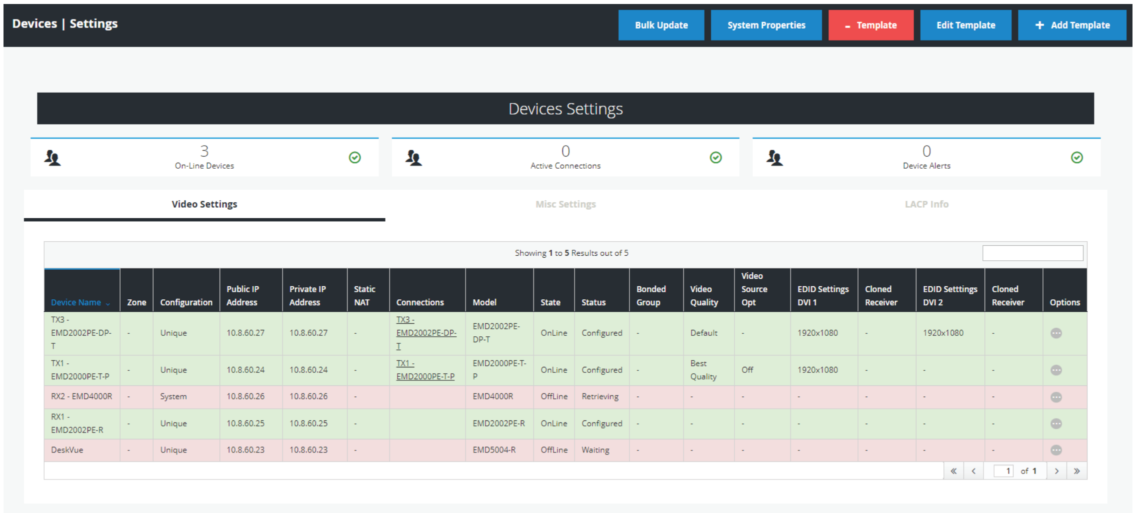
Successfully Managed Device: DeskVue, Please wait.

FIGURE A-7: OPERATION SUCCESSFUL CONFIRMATION MESSAGE

NOTE: When the DESKVUE unit is on the same network/subnet as the Boxilla Manager, the operation should be successful. If the operation fails, verify that the DESKVUE unit and the Boxilla Manager are on the same network/subnet and that supported firmware is being used, per information specified in “A1: Boxilla Discovery.”

APPENDIX A: BOXILLA DISCOVERY

The Emerald® DESKVUE unit may initially show up in the device list as “Offline” with a “Waiting” status, as shown in Figure A-8 below;



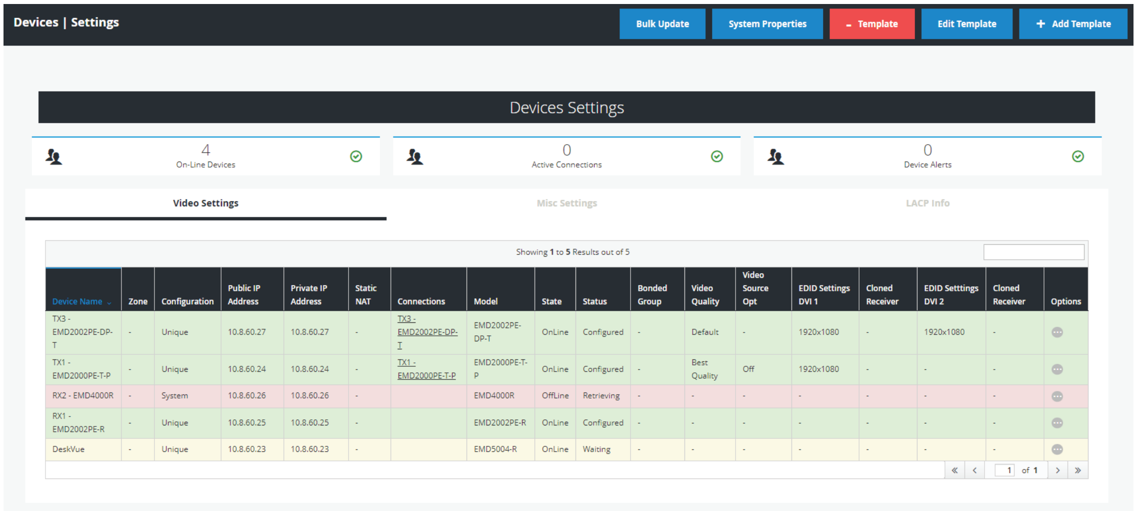
Showing **1** to **5** Results out of 5

Device Name	Zone	Configuration	Public IP Address	Private IP Address	Static NAT	Connections	Model	State	Status	Bonded Group	Video Quality	Video Source Opt	EDID Settings DVI 1	Cloned Receiver	EDID Setttings DVI 2	Cloned Receiver	Options
TX3 - EMD2002PE-DP-T	-	Unique	10.8.60.27	10.8.60.27	-	TX3 - EMD2002PE-DP-T	EMD2002PE-DP-T	OnLine	Configured	-	Default	-	1920x1080	-	1920x1080	-	⋯
TX1 - EMD2000PE-T-P	-	Unique	10.8.60.24	10.8.60.24	-	TX1 - EMD2000PE-T-P	EMD2000PE-T-P	OnLine	Configured	-	Best Quality	Off	1920x1080	-	-	-	⋯
RX2 - EMD4000R	-	System	10.8.60.26	10.8.60.26	-		EMD4000R	OffLine	Retrieving	-	-	-	-	-	-	-	⋯
RX1 - EMD2002PE-R	-	Unique	10.8.60.25	10.8.60.25	-		EMD2002PE-R	OnLine	Configured	-	-	-	-	-	-	-	⋯
DeskVue	-	Unique	10.8.60.23	10.8.60.23	-		EMD5004-R	OffLine	Waiting	-	-	-	-	-	-	-	⋯

« ‹ 1 of **1** › »

FIGURE A-8: DESKVUE UNIT SHOWN AS OFFLINE WITH WAITING STATUS

The operation will finish in a few minutes, and the system will update the status to “Online” as shown in Figure A-9 below:



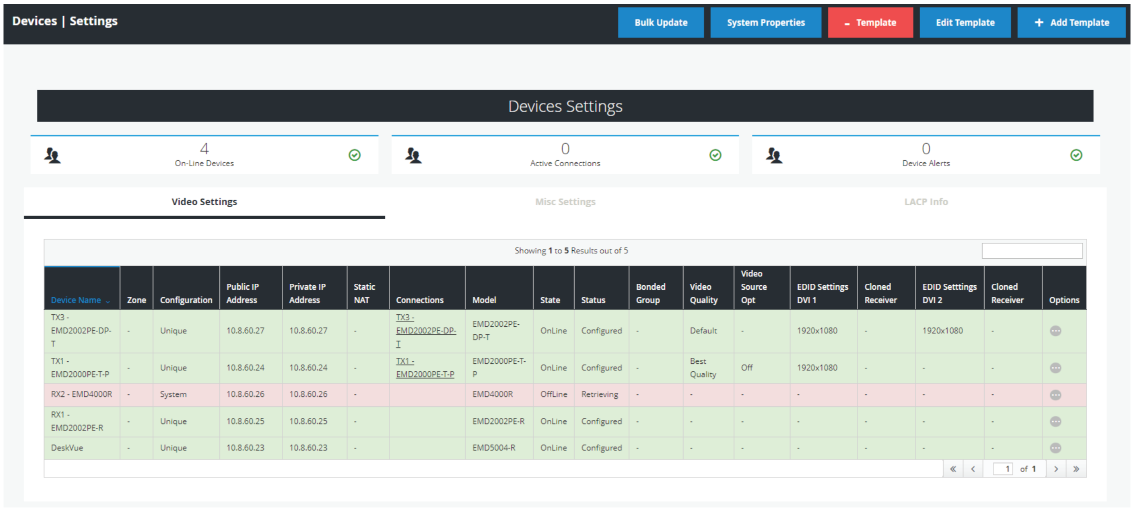
Showing **1** to **5** Results out of 5

Device Name	Zone	Configuration	Public IP Address	Private IP Address	Static NAT	Connections	Model	State	Status	Bonded Group	Video Quality	Video Source Opt	EDID Settings DVI 1	Cloned Receiver	EDID Setttings DVI 2	Cloned Receiver	Options
TX3 - EMD2002PE-DP-T	-	Unique	10.8.60.27	10.8.60.27	-	TX3 - EMD2002PE-DP-T	EMD2002PE-DP-T	OnLine	Configured	-	Default	-	1920x1080	-	1920x1080	-	⋯
TX1 - EMD2000PE-T-P	-	Unique	10.8.60.24	10.8.60.24	-	TX1 - EMD2000PE-T-P	EMD2000PE-T-P	OnLine	Configured	-	Best Quality	Off	1920x1080	-	-	-	⋯
RX2 - EMD4000R	-	System	10.8.60.26	10.8.60.26	-		EMD4000R	OffLine	Retrieving	-	-	-	-	-	-	-	⋯
RX1 - EMD2002PE-R	-	Unique	10.8.60.25	10.8.60.25	-		EMD2002PE-R	OnLine	Configured	-	-	-	-	-	-	-	⋯
DeskVue	-	Unique	10.8.60.23	10.8.60.23	-		EMD5004-R	OnLine	Waiting	-	-	-	-	-	-	-	⋯

« ‹ 1 of **1** › »

FIGURE A-9: STATUS CHANGED TO ONLINE

Although the status is updated to online, the system is still updating. Once the operation is complete, the unit's status will be updated to "Online" and "Configured," as shown in Figure A-10 below:



Showing **1** to **5** Results out of 5

Device Name	Zone	Configuration	Public IP Address	Private IP Address	Static NAT	Connections	Model	State	Status	Bonded Group	Video Quality	Video Source Opt	EDID Settings DVI 1	Cloned Receiver	EDID Setttings DVI 2	Cloned Receiver	Options
TX3 - EMD2002PE-DP-T	-	Unique	10.8.60.27	10.8.60.27	-	TX3 - EMD2002PE-DP-T	EMD2002PE-DP-T	OnLine	Configured	-	Default	-	1920x1080	-	1920x1080	-	⋯
TX1 - EMD2000PE-T-P	-	Unique	10.8.60.24	10.8.60.24	-	TX1 - EMD2000PE-T-P	EMD2000PE-T-P	OnLine	Configured	-	Best Quality	Off	1920x1080	-	-	-	⋯
RX2 - EMD4000R	-	System	10.8.60.26	10.8.60.26	-		EMD4000R	OffLine	Retrieving	-	-	-	-	-	-	-	⋯
RX1 - EMD2002PE-R	-	Unique	10.8.60.25	10.8.60.25	-		EMD2002PE-R	OnLine	Configured	-	-	-	-	-	-	-	⋯
DeskVue	-	Unique	10.8.60.23	10.8.60.23	-		EMD5004-R	OnLine	Configured	-	-	-	-	-	-	-	⋯

« ‹ 1 of **1** › »

FIGURE A-10: STATUS UPDATED TO ONLINE AND CONFIGURED

APPENDIX B: WORKSPACE CONFIGURATION

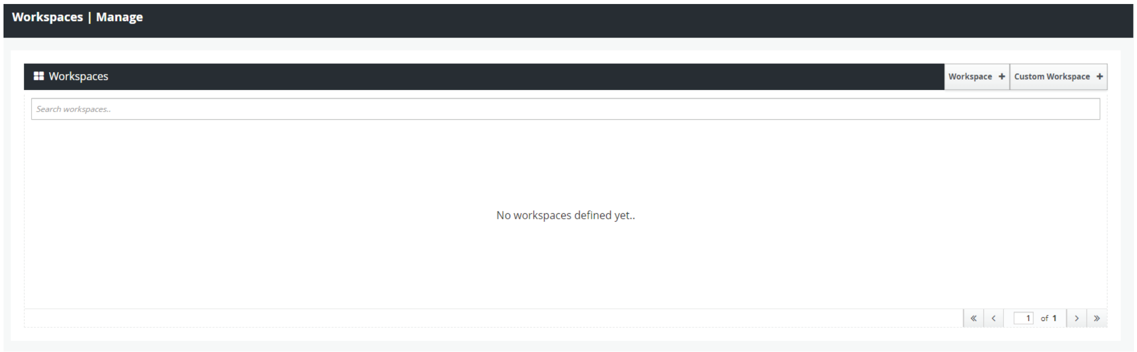
B.1 WORKSPACE CREATION/ASSIGNMENT

When the Emerald® DESKVUE unit is managed by a Boxilla® Manager, a workspace can be created and assigned to one or multiple users.

B.1.1 CREATING A WORKSPACE

To create a workspace:

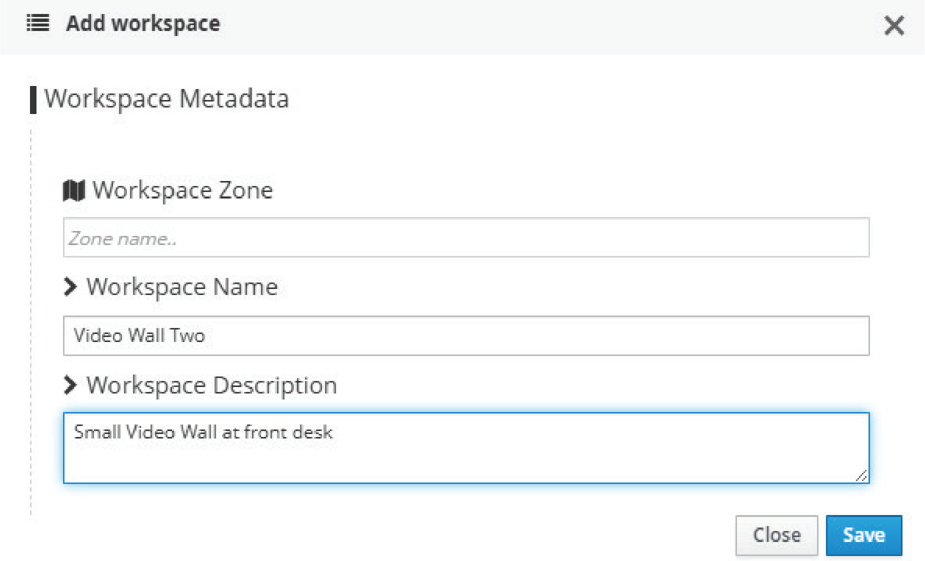
1. In the Boxilla web interface, navigate to Workspaces --> Manage. The workspace screen is shown in Figure B-1 below:



No workspaces defined yet..

FIGURE B-1: WORKSPACE SCREEN

2. Click on the “Add Workspace +” button to create a new workspace. Then enter both a name and description for the workspace in the appropriate fields shown in Figure B-2. If zoning is required and already set up, the DESKVUE can also be assigned into a zone.



Workspace Metadata

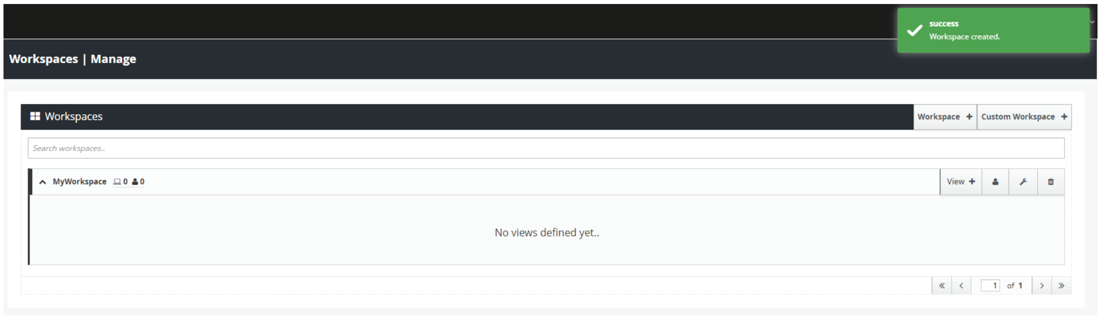
Workspace Zone: Zone name..

Workspace Name: Video Wall Two

Workspace Description: Small Video Wall at front desk

FIGURE B-2: ADD WORKSPACE SCREEN

3. Click on the “Save” button shown in Figure B-2 above.
   If the workspace was configured properly, the system will display a success notification in the top right corner of the screen, as shown in Figure B-3 below:



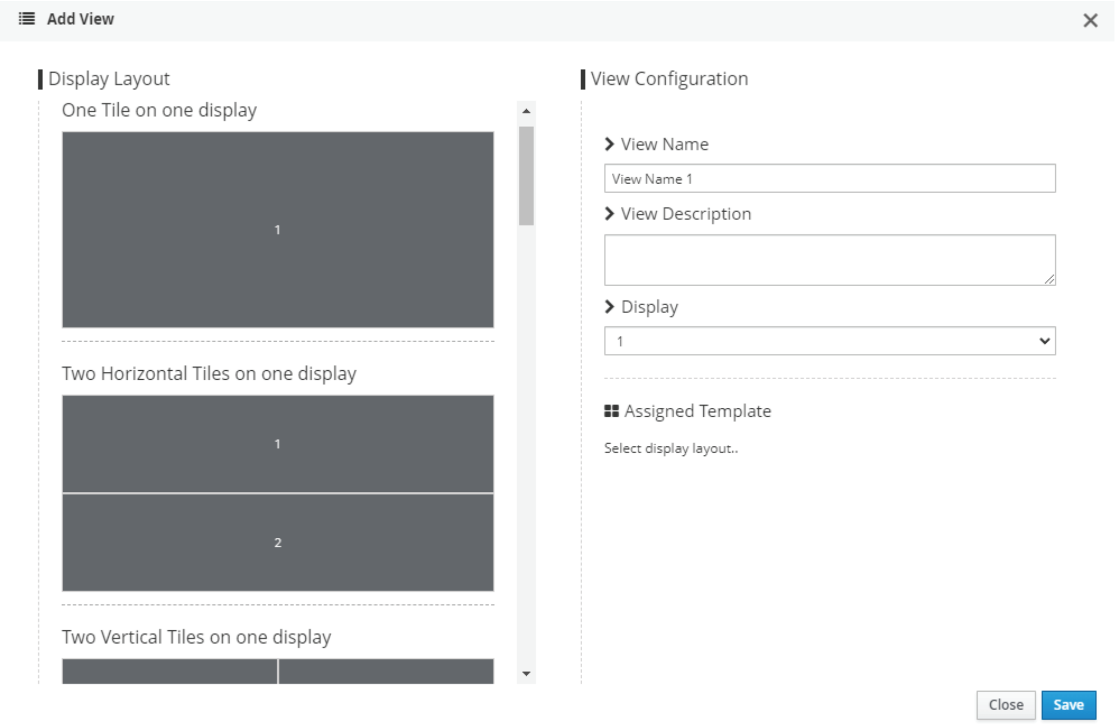
success
Workspace created.

No views defined yet..

FIGURE B-3: SUCCESS MESSAGE

NOTE: If an error occurs, review the error message for information about the problem.

4. Add a View by clicking on the “View +” button next to the workspace that was just created. The “Add View” screen will appear, as shown in Figure B-4 below:

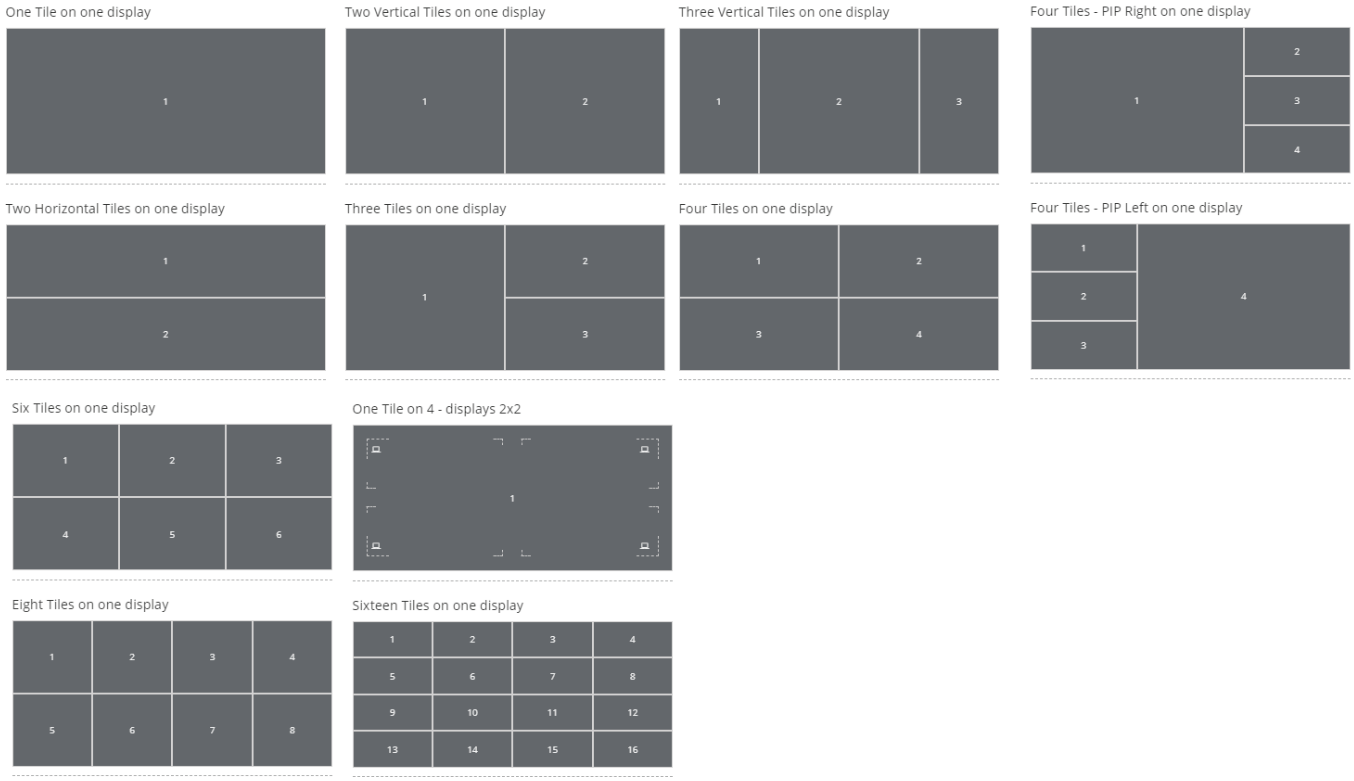


View Name: View Name 1
View Description:
Display: 1
Select display layout..

FIGURE B-4: ADD VIEW SCREEN

5. Select a Display Layout Format. Choose from these options:
   - One Tile on one display
   - Two Horizontal Tiles on one display
   - Two Vertical Tiles on one display
   - Three Tiles on one display
   - Three Vertical Tiles on one display
   - Four Tiles on one display
   - Four Tiles - PIP Right on one display
   - Four Tiles - PIP Left on one display
   - Six Tiles on one display
   - Eight Tiles on one display
   - One Tile on 4 - displays 2x2 (This template can be used for 2x2 video walls.)
   - Sixteen Tiles on one display

   Figure B-5 shows available display layout options:



One Tile on one display

Two Vertical Tiles on one display

Three Vertical Tiles on one display

Four Tiles - PIP Right on one display

Two Horizontal Tiles on one display

Three Tiles on one display

Four Tiles on one display

Four Tiles - PIP Left on one display

Six Tiles on one display

One Tile on 4 - displays 2x2

Eight Tiles on one display

Sixteen Tiles on one display

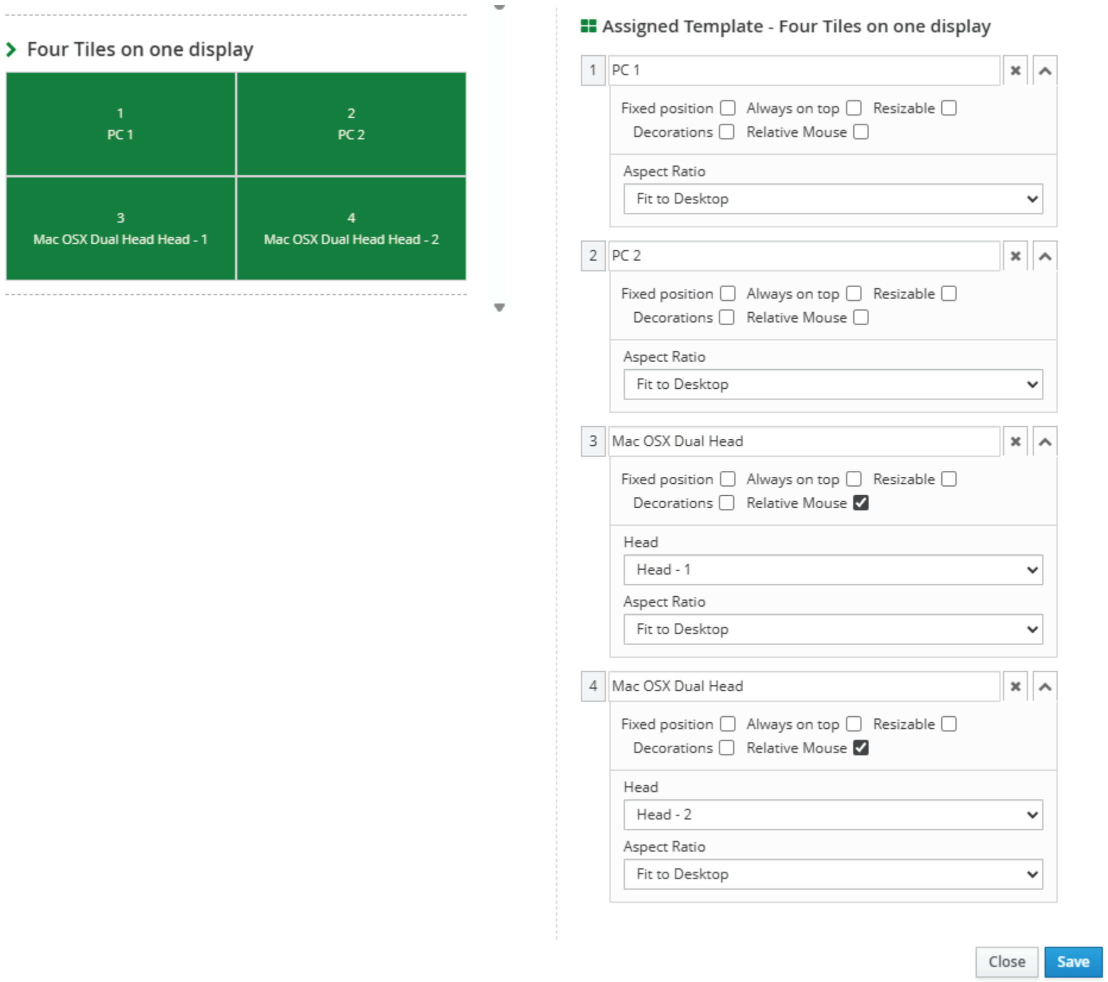
FIGURE B-5: DISPLAY LAYOUT OPTIONS

NOTE: The 32-tile layout is only available on unmanaged DESKVUE receivers; It is not available when managed by the Boxilla® manager.

APPENDIX B: WORKSPACE CONFIGURATION

6. Enter a Name for the View in the appropriate field.
7. Enter a Description for the View in the appropriate field.
8. Select which display should be used.

An example using "Four Tiles on One Display" with completed fields appears in Figure B-6 below:



Four Tiles on one display

1 PC 1	2 PC 2
3 Mac OSX Dual Head Head - 1	4 Mac OSX Dual Head Head - 2

Assigned Template - Four Tiles on one display

1 PC 1
Fixed position □ Always on top □ Resizable □
Decorations □ Relative Mouse □
Aspect Ratio: Fit to Desktop

2 PC 2
Fixed position □ Always on top □ Resizable □
Decorations □ Relative Mouse □
Aspect Ratio: Fit to Desktop

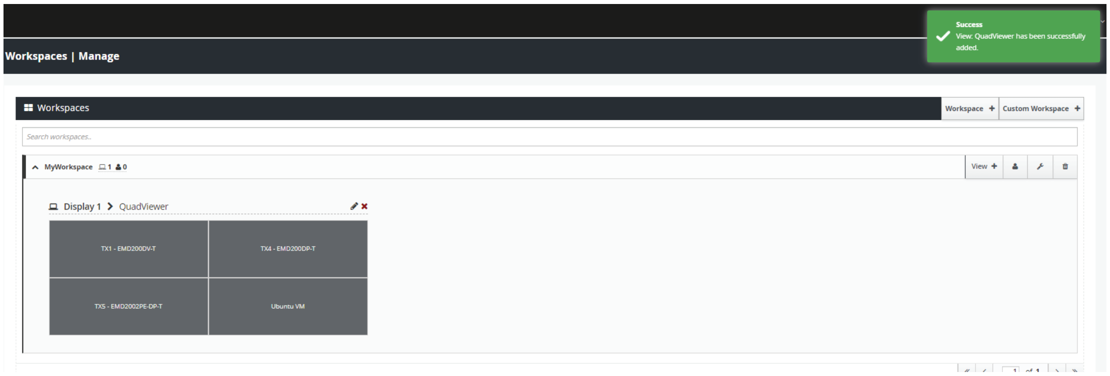
3 Mac OSX Dual Head
Fixed position □ Always on top □ Resizable □
Decorations □ Relative Mouse ☑
Head: Head - 1
Aspect Ratio: Fit to Desktop

4 Mac OSX Dual Head
Fixed position □ Always on top □ Resizable □
Decorations □ Relative Mouse ☑
Head: Head - 2
Aspect Ratio: Fit to Desktop

FIGURE B-6: RELATIVE MOUSE WORKSPACE

9. Click on the "Save" button.

If the workspace and view were configured properly without any errors, the system will display a success notification in the top right corner of the screen, as shown in Figure B-7 below:

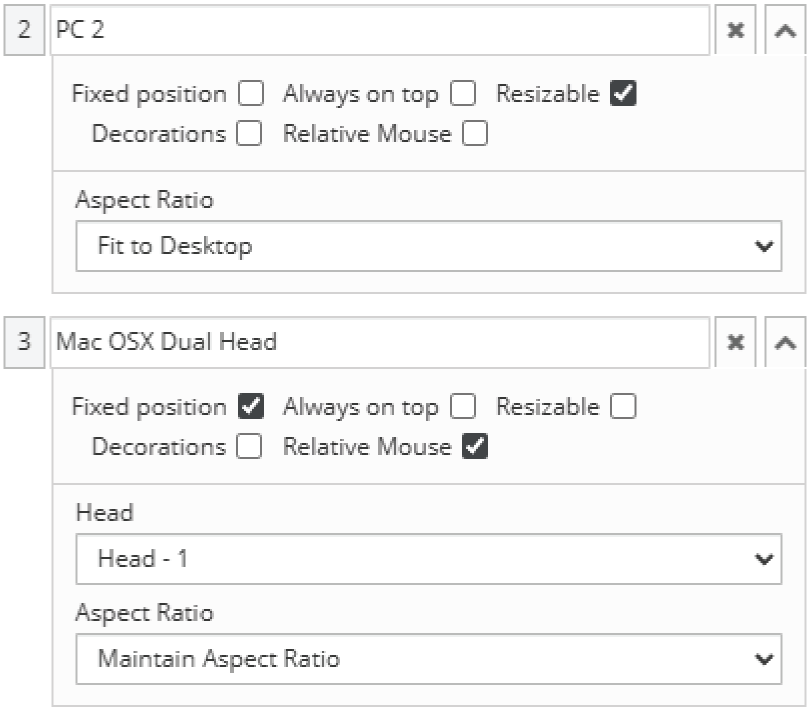


Success
View: QuadViewer has been successfully added.

FIGURE B-7: SUCCESS MESSAGE

NOTE: If there was an error, such as a missing view name, it will be displayed in the top right corner of the screen.

Each target in the workspace will have additional parameters to configure as seen in Figure B-8 below.



2 PC 2

Fixed position □ Always on top □ Resizable ☑
Decorations □ Relative Mouse □

Aspect Ratio: Fit to Desktop

3 Mac OSX Dual Head

Fixed position ☑ Always on top □ Resizable □
Decorations □ Relative Mouse ☑

Head: Head - 1

Aspect Ratio: Maintain Aspect Ratio

FIGURE B-8: CONFIGURATION SCREEN

APPENDIX B: WORKSPACE CONFIGURATION

Every connection under Workspace will have additional options to manipulate the video signal, as shown in Table B-1 below.

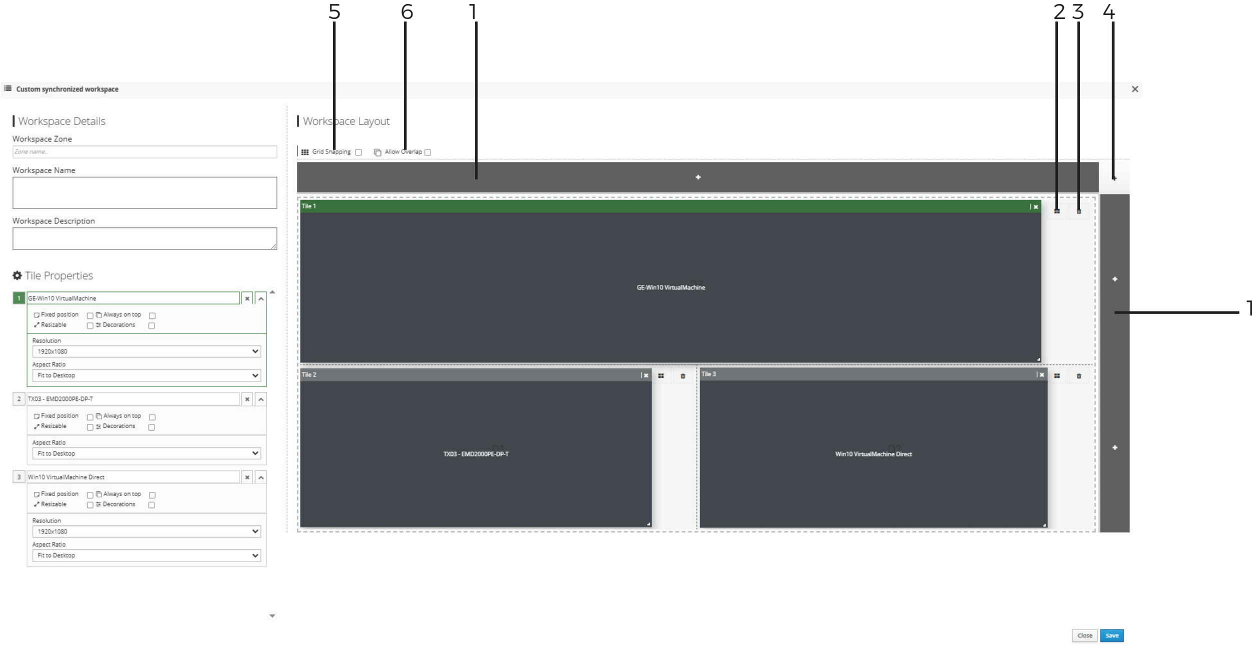
TABLE B-1. TARGET PROPERTIES

ITEM	DESCRIPTION
Resolution (RDP and PCoiP options)	Choose the resolution that the target should use.
Decoration	Options are "Ticked" or "Unticked." If set to "Ticked," the tile's title bar will be displayed displayed. If set to "Unticked," the tile's title bar will not be visible.
Fixed Position	Options are "Ticked" or "Unticked." If set to "Ticked," the tile cannot be moved or resized,. If set to "Unticked," the tile can be freely moved around and scaled.
Always on Top	Options are "Ticked" or "Unticked." If set to "Ticked," the connection window will always appear on top. If set to "Unticked," the connection window will not always appear on top.
Aspect Ratio	Options are "Fit" or "Maintain." If set to "Fit," the input is stretched to fit the viewable tile. If set to "Maintain," the original aspect ratio is maintained, which may cause blank borders.
Resizable	Options are "Ticked" or "Unticked." If set to "Ticked," the tile can be scaled and resized. If set to "Unticked," the viewable window cannot be scaled and resized.
Relative Mouse	Options are "Ticked" or "Unticked." If set to "Ticked", this will cause KVM control of this tile to be locked into the target machine until using the hotkey sequence: CTRL CTRL E If set to "Unticked" keyboard and mouse control over the tiles will glide and switch between tiles automatically which have this option unticked not requiring any hotkey.

If DESKVUE has more than one monitor, simply simply click on the "View +" button. Then configure another Layout and select another monitor. Do this for each additional display until each one has been configured.

B.2 CUSTOM WORKSPACE

Custom workspaces can be configured by clicking on the “Custom Workspace” button located on the workspaces main page, as shown in Figure B-9 below. Custom workspaces are user generated templates that can be configured. Since most of the options for custom templates are explained in the previous steps, only the additional buttons are described in this section.



Custom synchronized workspace

Workspace Details

Workspace Zone: Zone name..

Workspace Name:

Workspace Description:

Tile Properties

1 GE-Win10 VirtualMachine
□ Fixed position □ Always on top □
Resizable □ Decorations □
Resolution: 1920x1080
Aspect Ratio: Fit to Desktop

2 TX03 - EMD2000PE-DP-T
□ Fixed position □ Always on top □
Resizable □ Decorations □
Aspect Ratio: Fit to Desktop

3 Win10 VirtualMachine Direct
□ Fixed position □ Always on top □
Resizable □ Decorations □
Resolution: 1920x1080
Aspect Ratio: Fit to Desktop

Workspace Layout

Grid Snapping □ Allow Overlap □

Tile 1: GE-Win10 VirtualMachine

Tile 2: TX03 - EMD2000PE-DP-T

Tile 3: Win10 VirtualMachine Direct

FIGURE B-9: CUSTOM WORKSPACE SCREEN

TABLE B-2. CUSTOM WORKSPACE SCREEN COMPONENTS

NUMBER IN FIGURE B-8	COMPONENT	DESCRIPTION
1	Add new monitor	Use this option to add an additional display to the vertical or horizontal viewing plane.
2	Start with template	Use this option to create a custom workspaced based upon an existing template. When you click on this button, use the additional options displayed to select the desired template.
3	Delete current workspace	Use the trash can icon to delete the current display layout. NOTE: When you only have one display layout, it cannot be deleted.
4	Add New Title/View	Use this option to create a new window in which to view a target. When adding a new tile, it can be moved or resized, as needed.

TABLE B-2. CUSTOM WORKSPACE SCREEN COMPONENTS (CONTINUED)

NUMBER IN FIGURE B-8	COMPONENT	DESCRIPTION
5	Grid snapping	The grid system utilizes a dynamic snapping mechanism designed to accommodate tiles of varying sizes. Unlike fixed-grid snapping, this system analyzes the positions of existing tiles to ensure consistent and proportional tile alignment during drag and resize operations. Dynamic Alignment: When grid snapping is enabled, tiles snap to intervals relative to the positions of other tiles, preventing overlaps and undesirable gaps. Resize Constraints: When resizing tiles to the left, the system highlights the minimum allowable size increase. This constraint prevents resizing that would violate grid spacing and alignment rules.
6	Allow overlap	The Allow Overlap checkbox provides flexible tile placement within the grid by disabling the automatic vertical compaction and displacement of tiles. When enabled: Tiles can be positioned to overlap existing tiles. Automatic vertical alignment of tiles is deactivated. NOTE: While overlap is permitted, grid snapping functionality remains active, ensuring tile positioning and resizing are still proportional to the grid layout. This allows for precise, yet overlapping, tile arrangement.

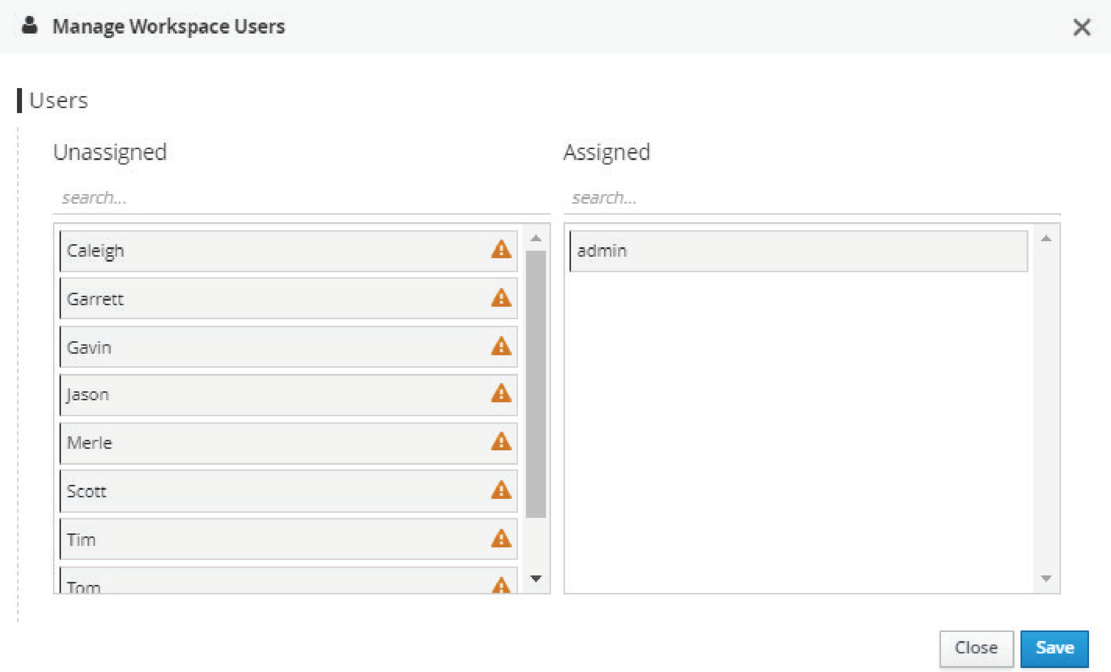
B.2.1 ASSIGNING A USER TO A WORKSPACE

After the workspace and views are configured, a user must be assigned so that the user can access the workspace and views when logging into the Emerald® DESKVUE unit.

To assign users to a workspace:

1. Click on the user icon.

2. Assign which users have access to the workspace using the “Manage Workspace Users” screen, as shown in Figure B-10 below:



Manage Workspace Users

Users

Unassigned

search...

Caleigh ⚠
Garrett ⚠
Gavin ⚠
Jason ⚠
Merle ⚠
Scott ⚠
Tim ⚠
Tom ⚠

Assigned

search...

admin

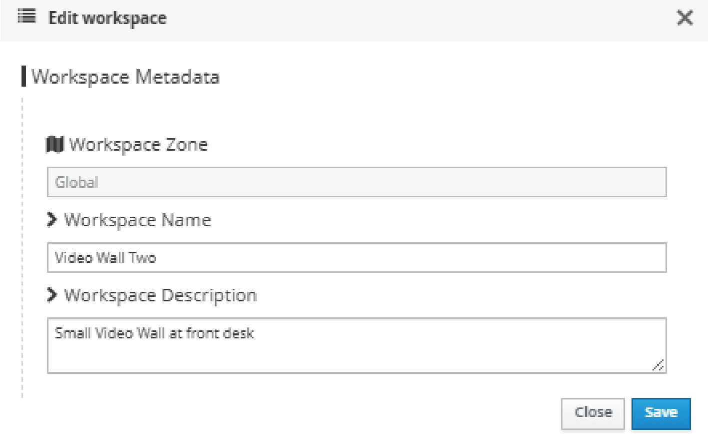
FIGURE B-10: MANAGE WORKSPACE USERS SCREEN

NOTE: Unassigned and assigned targets that have the warning icon next to them confirms what connections are not yet assigned to a user account. In order for a workspace to work properly, the user must have access to all connections that are part of that workspace.

3. Click on the “Save” button to save the assignments.

B.2.2 EDITING A WORKSPACE

Once the workspace is created, the Boxilla® administrator can edit it at any time by using the edit (wrench) icon. The “Edit Workspace” screen is shown in Figure B-11 below:



Edit workspace

Workspace Metadata

Workspace Zone: Global

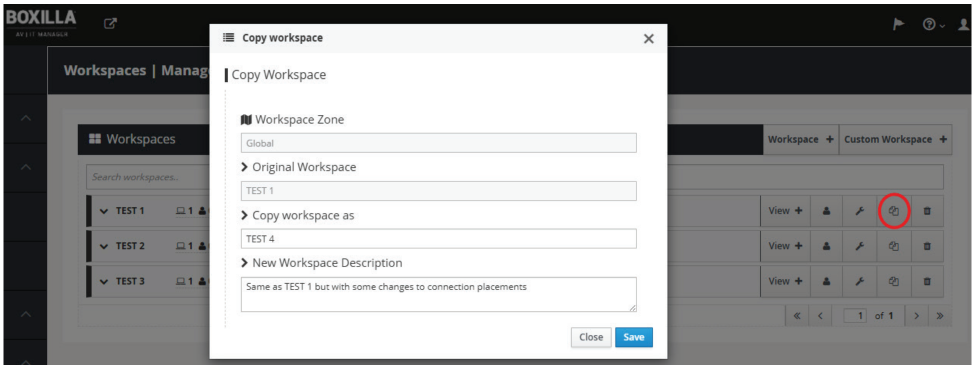
Workspace Name: Video Wall Two

Workspace Description: Small Video Wall at front desk

FIGURE B-11: EDIT WORKSPACE SCREEN

B.2.3 COPYING A WORKSPACE

New in Boxilla version 5.1.5, once a workspace is created, you can copy that workspace as a new workspace with a new name and description. This saves time time, enabling you to create multiple variants of a workspace based on an original that you use as a template.



Copy workspace

Copy Workspace

Workspace Zone: Global

Original Workspace: TEST 1

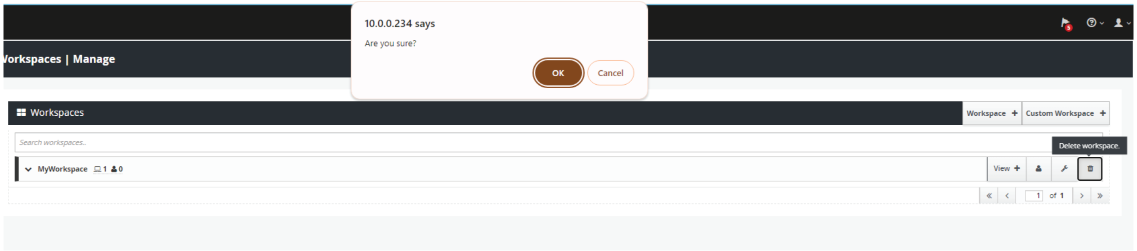
Copy workspace as: TEST 4

New Workspace Description: Same as TEST 1 but with some changes to connection placements

FIGURE B-12. COPYING A WORKSPACE

B.2.4 DELETING A WORKSPACE

To delete a workspace, click on the delete workspace icon (trash can), as shown in Figure B-13 below:



10.0.0.234 says

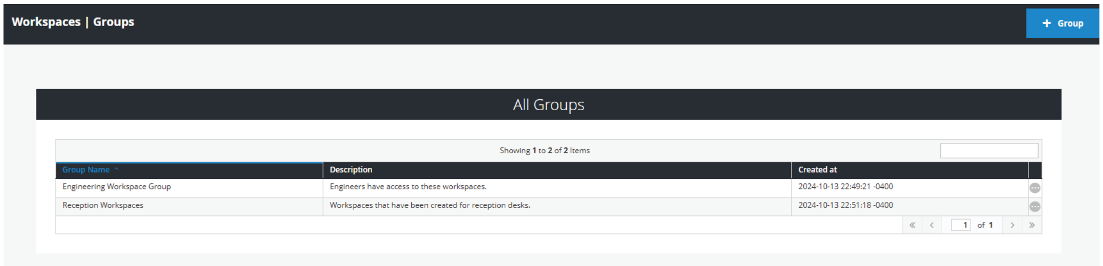
Are you sure?

FIGURE B-13: WORKSPACE SHOWING DELETE WORKSPACE

B.2.5 WORKSPACE GROUPS

To make workspace access easier, a Workspace group can be configured to add multiple workspaces to a group which then could be assigned to a user. The alternative is managing the individual Workspaces for each user.

The Workspaces Groups page will show a summary of all groups that have been configured as referenced in Figure B14 below:

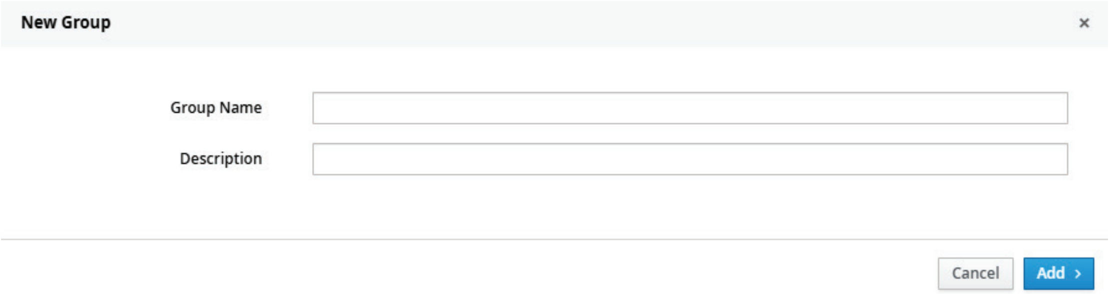


Showing 1 to 2 of 2 Items

Group Name	Description	Created at
Engineering Workspace Group	Engineers have access to these workspaces.	2024-10-13 22:49:21 -0400
Reception Workspaces	Workspaces that have been created for reception desks.	2024-10-13 22:51:18 -0400

FIGURE B-14: WORKSPACES GROUP PAGE

When you create a new group by clicking on the "+ Group" button in the top right hand corner of the page, the New Group screen appears, as shown in Figure B-15 below:



New Group ×

Group Name

Description

FIGURE B-15: NEW GROUP SCREEN

Enter the Group Name and Description. Then click on the "Add" button. Clicking on the "Cancel" button will not create the Workspace group and return back to the Workspaces Groups home page.

Once a group has been created, additional options can be accessed using the ellipsis "..." icon next to the workspace group, as shown in Figure B-16 below:

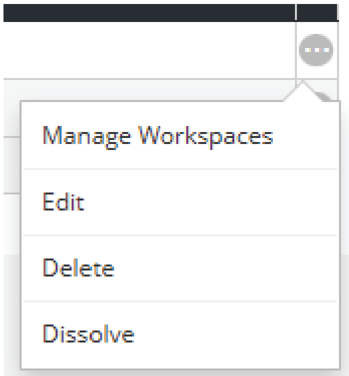
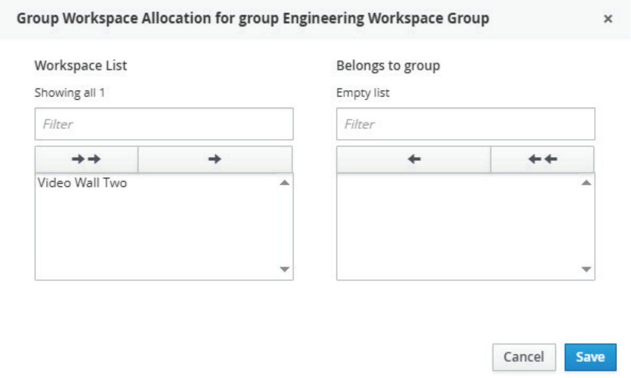


FIGURE B-16: ADDITIONAL OPTIONS

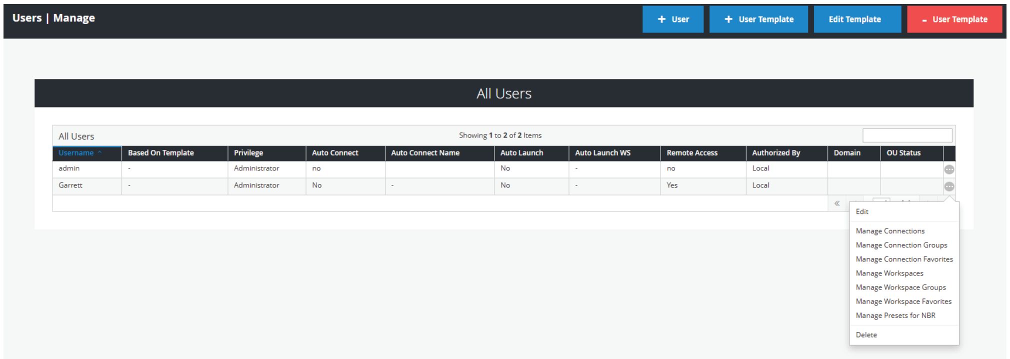
Table B-3 explains the options available thorugh the drop-down menu.

TABLE B-3. ADDITIONAL OPTIONS

ITEM	DESCRIPTION
Manage Workspaces	Allows the assignment of any existing workspaces to be assigned to the group, as shown in Figure B-17 below:  Group Workspace Allocation for group Engineering Workspace Group × Workspace List Showing all 1 Filter Video Wall Two Belongs to group Empty list Filter Cancel Save FIGURE B-17: ASSIGNING WORKSPACES TO A GROUP
Edit	Use this option to edit the Group Name and Description.
Delete	Use this option to delete the workspace group from the system and from all active connections for users that are currently logged in.
Dissolve	Use this option to dissolve a workspace group. Dissolving a workspace group will remove the group from the web configuration options. The workspace groups will be retained with users who are currently logged in, however.

B.2.6 ADDITIONAL CONFIGURATION OPTIONS

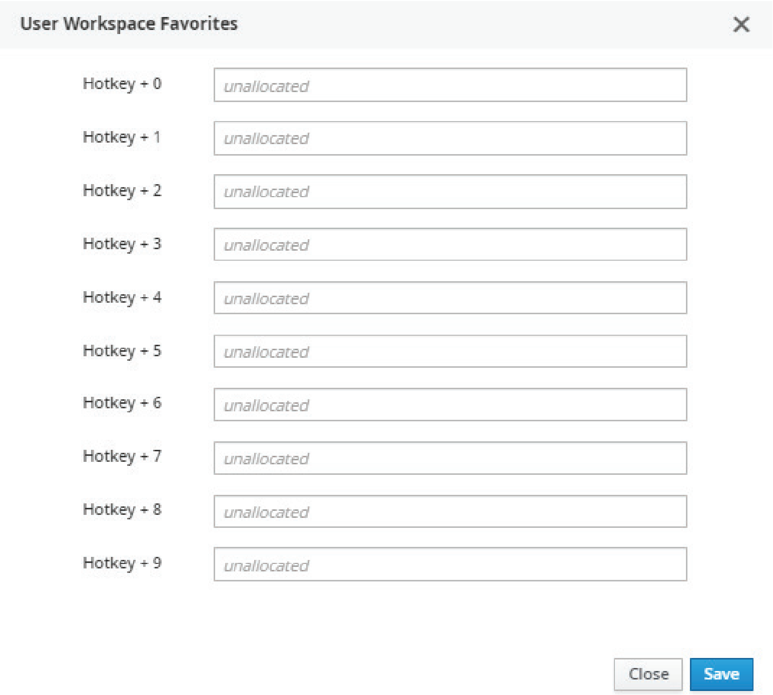
Within the Boxilla® web interface in the "Users" section, additional parameters can be configured for each user. "Manage Workspaces," "Manage Workspace Groups," and "Manage Workspace Favorites" are available through the ellipsis icon next to a user name, and these options can be used to adjust user configurations. Configuration options can be accessed through the resulting drop-down menu shown in Figure B-18 below:



Username	Based On Template	Privilege	Auto Connect	Auto Connect Name	Auto Launch	Auto Launch WS	Remote Access	Authorized By	Domain	OU Status
admin	-	Administrator	no		No	-	no	Local		
Garrett	-	Administrator	No	-	No	-	Yes	Local		

FIGURE B-18: DROP-DOWN MENU LIST

To change Workspace favorites, click in the empty text box for a hotkey that needs to be configured and link the workspace to the corresponding hotkey using the screen shown in Figure B-19 below:



User Workspace Favorites

Hotkey + 0: unallocated

Hotkey + 1: unallocated

Hotkey + 2: unallocated

Hotkey + 3: unallocated

Hotkey + 4: unallocated

Hotkey + 5: unallocated

Hotkey + 6: unallocated

Hotkey + 7: unallocated

Hotkey + 8: unallocated

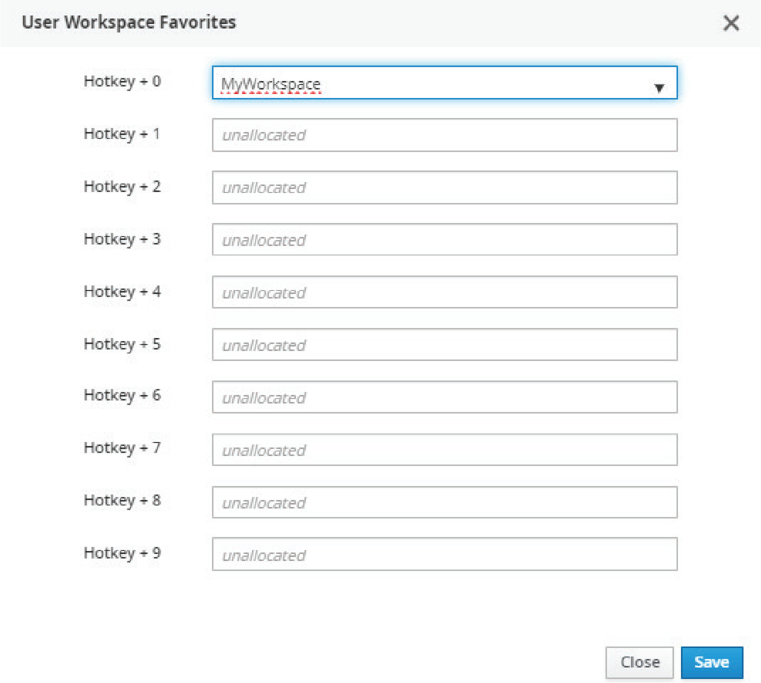
Hotkey + 9: unallocated

FIGURE B-19: HOTKEY CONFIGURATION SCREEN

TIP: When configuring user workspace favorites, use the “User Manage Workspaces” option to verify that the user has access to the workspace.

Click on the “Save” button when finished.

An example of assigning the first hotkey to a workspace appears in Figure B-20 below:



User Workspace Favorites

Hotkey + 0	MyWorkspace
Hotkey + 1	unallocated
Hotkey + 2	unallocated
Hotkey + 3	unallocated
Hotkey + 4	unallocated
Hotkey + 5	unallocated
Hotkey + 6	unallocated
Hotkey + 7	unallocated
Hotkey + 8	unallocated
Hotkey + 9	unallocated

FIGURE B-20: EXAMPLE OF HOTKEY ASSIGNMENT

B.2.7 CONFIGURATING USER ACCESS THROUGH BOXILLA

User access to a Workspace can also be configured under the Boxilla® Users Management page by selecting "Manage Workspaces" from the drop-down list. The Boxilla "Manage Workspaces" screen appears in Figure B-21 below:

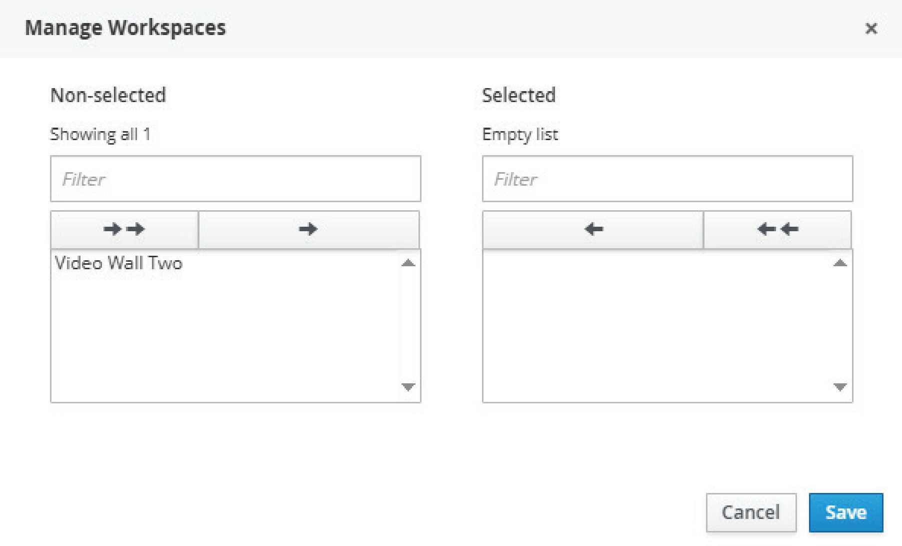


FIGURE B-21: BOXILLA MANAGE WORKSPACES SCREEN

The user may be assigned to a group in order to access the individual workspaces found within that group. This option allows the user to be assigned to these groups to gain access to them.

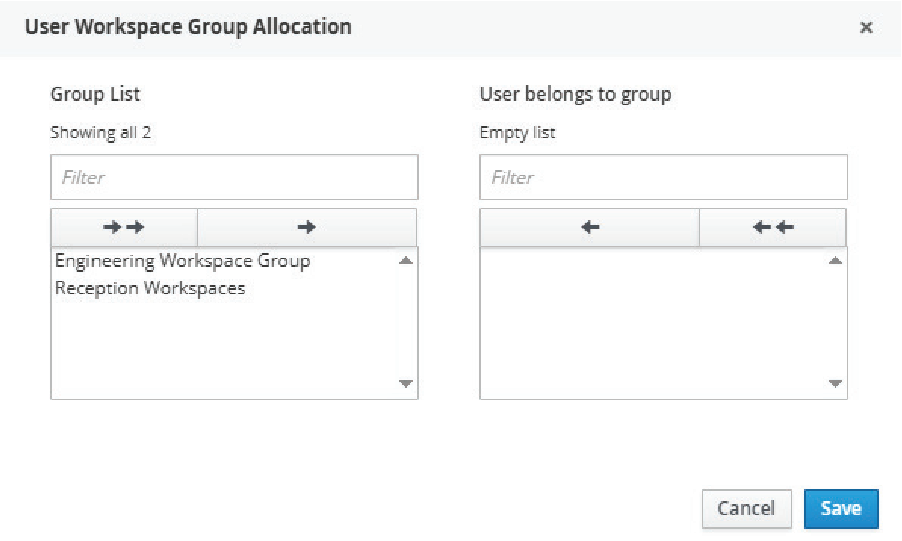


FIGURE B-22: MANAGE WORKSPACES GROUP UNDER USERS SCREEN

APPENDIX C: PROTOCOLS

OVERVIEW

Emerald and DESKVUE use standard IP protocols for communication between Receivers and Transmitters.

TABLE C-1. PORT USAGE PER APPLIANCE

COMPONENT	APPLICATION	PORT	EMERALD 4K	EMERALD PE/ZU
Appliance	Appliance REST HTTP	TCP: 7778	Yes	Yes
	Appliance REST HTTPS	TCP: 8888	Yes	Yes
	Communications	TCP: 22	Yes	Yes
	Manager Discovery (to Appliance): Multicast 224.0.1.249. Appliance listens on UDP Port	UDP: 39150	Yes	Yes
	(4K Only) Default Slave Multicast IP Port (IP: 239.0.0.1)	UDP: 8000	Yes	No
	(4K only) Default Master Multicast IP Port (IP: 239.0.0.1)	UDP: 8001	Yes	No
	Audio (Private/Multi Unicast)	TCP: 9000	Yes (1.2 onwards)	Yes (5.0x onwards)
	Video EMDSE & 4K	TCP: 16384	Yes	Yes (5.3x onwards)
	Video, 2nd channel, (Paired only)	TCP: 16385	No	Yes (5.4x only)
	Reserved – Future	TCP: 16387	—	—
	Reserved – Future	TCP: 16388	—	—
	Multicast 225.0.0.37 (Appliance – recovery)	UDP: 12345	Yes	Yes
	RDP VM & RDP Broker	TCP: 3389 (default)	Yes (Default)	Yes (Default)
	TX connections	TCP: 3389	Yes	Yes
Boxilla®	Boxilla REST HTTPS	TCP: 443	—	—
	Communications	TCP: 22	—	—
	Discovery: Multicast 224.0.1.249 (Send)	UDP: 39150	—	—

NOTE: Firewalls on the WAN may cause audio to fail due to a protocol issue that prevents it traversing some firewalls. The audio channel does not perform the SYN/SYNACK sequence which leads to some of these streams being blocked.

APPENDIX D: SNMP SUMMARY

D.1 SNMP SUMMARY

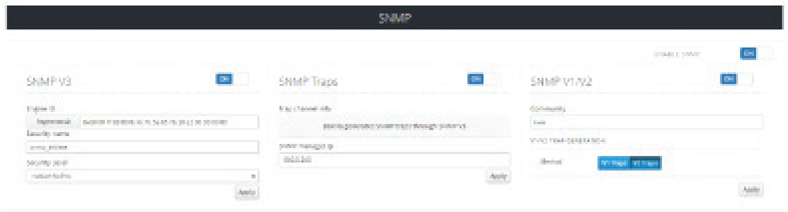


FIGURE D-1: SNMP OPTIONS

SNMP V3: This option can be enabled, and it supports options for the EngineID, Security Name, and Security Level.

Options, including for security level, are shown in Table D-1:.

TABLE D-1. SNMP OPTIONS

OPTION	DESCRIPTION
noAuthNoPriv	authNoPriv: Requires Authentication Protocol using MD5 or SHA, and an Authentication key authPriv: Requires everything the authNoPriv has, but includes Privacy Protocol options for DES or AES. This option also requires the Privacy Key.
SNMP Traps	When enabled, this option will generate the SNMP Traps and send it to an SNMP manager using SNMP V2. Enter the IP address of the SNMP manager IP to complete the configuration.

SNMP V1/V2: When enabled, this allows the Boxilla® administrator to configure the Community string which by default is “kvm”. The options are available to use V1 or V2 Traps.

TABLE D-2. SNMP DEFINITIONS

```
Table:
-- Organization (BlackBox) root OID definition by enterprise number
BLACKBOX-ENTITY-MIB DEFINITIONS ::= BEGIN
  IMPORTS
    MODULE-IDENTITY, NOTIFICATION-TYPE,
OBJECT-TYPE, -- GW for SMIv2 compliance and consistency
enterprises, INTEGER, Gauge32, IpAddress
  FROM SNMPv2-SMI
TEXTUAL-CONVENTION,
DisplayString, DateAndTime, TruthValue, MacAddress
 FROM SNMPv2-TC
  MODULE-COMPLIANCE,
  NOTIFICATION-GROUP,
  OBJECT-GROUP
 FROM SNMPv2-CONF;

blackbox MODULE-IDENTITY
LAST-UPDATED “202208250000Z”
ORGANIZATION “Black Box Corp.”
CONTACT-INFO
“1000 Park Drive Lawrence,
PA 15055 United States of America
E-mail: support@blackbox.com”
DESCRIPTION
  “The MIB module representing BlackBox Devices’
  implementation of enterprise specific MIBs
  for Boxilla, Emerald and peripherial products.”
  REVISION  “202201310000Z”
  DESCRIPTION “Initial”

::= { enterprises 6878 }

blackboxEntity OBJECT IDENTIFIER ::= { blackbox 100 }
blackboxEntityNotifications OBJECT IDENTIFIER ::= { blackboxEntity 0 }
blackboxEntityGet OBJECT IDENTIFIER ::= { blackboxEntity 1 }

DeviceState ::= TEXTUAL-CONVENTION
STATUS current
DESCRIPTION
“State of Emerald device.”
SYNTAX INTEGER { online(1), offline(2) }

SwitchState ::= TEXTUAL-CONVENTION
STATUS current
DESCRIPTION
“State of BlackBox network switch.”
SYNTAX INTEGER { online(1), offline(2) }
```

```
ClusterInfoAvailability ::= TEXTUAL-CONVENTION
STATUS current
DESCRIPTION
“Availability of Boxilla cluster info.”
SYNTAX INTEGER { unavailable(0), available(1) }

ClusterReplicationLagLev ::= TEXTUAL-CONVENTION
STATUS current
DESCRIPTION
“Boxilla cluster replication lag level.”
SYNTAX INTEGER { unknown(0), normal(1), warning(2), critical(3) }

ClusterNodeState ::= TEXTUAL-CONVENTION
STATUS current
DESCRIPTION
“State of Boxilla cluster node.”
SYNTAX INTEGER { active(1), standby(2), detached(3), failed(4), failedstandby(5) }

__****************************************************************************************
-- Data objects
__****************************************************************************************

alertDescription OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
“Description context of Boxilla alert.”
::= { blackboxEntity 2 }

__****************************************************************************************
-- SNMP GETs
__****************************************************************************************

deviceInfoTable OBJECT-TYPE
SYNTAX SEQUENCE OF DeviceInfoEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
```

```
"Information of all Emerald devices."
::= { blackboxEntityGet 1 }

deviceInfoEntry OBJECT-TYPE
  SYNTAX DeviceInfoEntry
  MAX-ACCESS not-accessible
  STATUS current
  DESCRIPTION
"Information entry of each Emerald device."
  INDEX { deviceName }
  ::= { deviceInfoTable 1 }

DeviceInfoEntry ::= SEQUENCE {
deviceName   DisplayString,
deviceIp    IpAddress,
deviceMac    MacAddress,
deviceModel    DisplayString,
deviceState DeviceState
}

deviceName OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
  DESCRIPTION
"Device name with this deviceInfoEntry."
  ::= { deviceInfoEntry 1 }

deviceIp OBJECT-TYPE
SYNTAX IpAddress
MAX-ACCESS read-only
STATUS current
  DESCRIPTION
"Device IP address with this deviceInfoEntry."
  ::= { deviceInfoEntry 2 }

deviceMac OBJECT-TYPE
SYNTAX MacAddress
MAX-ACCESS read-only
```

```
STATUS current
  DESCRIPTION
"Device MAC address with this deviceInfoEntry."
  ::= { deviceInfoEntry 3 }

deviceModel OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
  DESCRIPTION
"Device model with this deviceInfoEntry."
  ::= { deviceInfoEntry 4 }

deviceState OBJECT-TYPE
SYNTAX DeviceState
MAX-ACCESS read-only
STATUS current
  DESCRIPTION
"Device state with this deviceInfoEntry."
  ::= { deviceInfoEntry 5 }

switchInfoTable OBJECT-TYPE
SYNTAX SEQUENCE OF SwitchInfoEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
"Information of all network switches."
::= { blackboxEntityGet 2 }

switchInfoEntry OBJECT-TYPE
  SYNTAX SwitchInfoEntry
  MAX-ACCESS not-accessible
  STATUS current
  DESCRIPTION
"Information entry of each network switch."
  INDEX { switchName }
  ::= { switchInfoTable 1 }
```

```
SwitchInfoEntry ::= SEQUENCE {
switchName DisplayString,
switchIp IpAddress,
switchMac MacAddress,
switchModel DisplayString,
switchState SwitchState
}

switchName OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
  DESCRIPTION
“Switch name with this switchInfoEntry.”
  ::= { switchInfoEntry 1 }
switchIp OBJECT-TYPE
SYNTAX IpAddress
MAX-ACCESS read-only
STATUS current
  DESCRIPTION
“Switch IP address with this switchInfoEntry.”
  ::= { switchInfoEntry 2 }

switchMac OBJECT-TYPE
SYNTAX MacAddress
MAX-ACCESS read-only
STATUS current
  DESCRIPTION
“Switch MAC address with this switchInfoEntry.”
  ::= { switchInfoEntry 3 }

switchModel OBJECT-TYPE
SYNTAX DisplayString
```

```
MAX-ACCESS read-only
STATUS current
  DESCRIPTION
"Switch model with this switchInfoEntry."
  ::= { switchInfoEntry 4 }

switchState OBJECT-TYPE
SYNTAX SwitchState
MAX-ACCESS read-only
STATUS current
  DESCRIPTION
"Switch state with this switchInfoEntry."
  ::= { switchInfoEntry 5 }

-- cluster info section
clusterInfoAvailability OBJECT-TYPE
SYNTAX ClusterInfoAvailability
MAX-ACCESS read-only
STATUS current
  DESCRIPTION
"Availability status of the clusterInfo."
  ::= { blackboxEntityGet 3 }

clusterInfoTable OBJECT-TYPE
SYNTAX SEQUENCE OF ClusterInfoEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
"Information of Boxilla clusters."
::= { blackboxEntityGet 4 }

clusterInfoEntry OBJECT-TYPE
  SYNTAX ClusterInfoEntry
  MAX-ACCESS not-accessible
  STATUS current
  DESCRIPTION
"Information entry for a Boxilla cluster."
  INDEX { clusterId }
  ::= { clusterInfoTable 1 }
```

```
ClusterInfoEntry ::= SEQUENCE {
clusterId DisplayString,
clusterVirtualIp IpAddress,
clusterReplicationLagLev   ClusterReplicationLagLev,
clusterNodeInfoTableSize INTEGER
}

clusterId OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
  DESCRIPTION
"Boxilla Cluster ID."
  ::= { clusterInfoEntry 1 }
clusterVirtualIp OBJECT-TYPE
SYNTAX IpAddress
MAX-ACCESS read-only
STATUS current
  DESCRIPTION
"Boxilla Cluster Virtual IP address."
  ::= { clusterInfoEntry 2 }

clusterReplicationLagLev OBJECT-TYPE
SYNTAX ClusterReplicationLagLev
MAX-ACCESS read-only
STATUS current
  DESCRIPTION
"Boxilla Cluster Replication lag level."
  ::= { clusterInfoEntry 3 }

 clusterNodeInfoTableSize OBJECT-TYPE
  SYNTAX   INTEGER
  MAX-ACCESS read-only
  STATUS   current
  DESCRIPTION
    "Size of the clusterNodeInfoTable."
  ::= { clusterInfoEntry 4 }
```

```
clusterNodeInfoTable OBJECT-TYPE
SYNTAX SEQUENCE OF ClusterNodeInfoEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
“Information entry for the Boxilla cluster nodes.”
::= { blackboxEntityGet 5 }

clusterNodeInfoEntry OBJECT-TYPE
  SYNTAX ClusterNodeInfoEntry
  MAX-ACCESS not-accessible
  STATUS current
  DESCRIPTION
“Information entry for a Boxilla cluster node.”
  INDEX { clusterNodeId }
  ::= { clusterNodeInfoTable 1 }

ClusterNodeInfoEntry ::= SEQUENCE {
clusterNodeId INTEGER,
clusterNodeName DisplayString,
clusterNodeIp IpAddress,
clusterNodeState ClusterNodeState
}

clusterNodeId OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
  DESCRIPTION
“Node id in clusterNodeInfoEntry.”
  ::= { clusterNodeInfoEntry 1 }

clusterNodeName OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
  DESCRIPTION
“Node name in clusterNodeInfoEntry.”
```

```
  ::= { clusterNodeInfoEntry 2 }

clusterNodeIp OBJECT-TYPE
SYNTAX IpAddress
MAX-ACCESS read-only
STATUS current
  DESCRIPTION
"Node IP address in clusterNodeInfoEntry."
  ::= { clusterNodeInfoEntry 3 }

clusterNodeState OBJECT-TYPE
SYNTAX ClusterNodeState
MAX-ACCESS read-only
STATUS current
  DESCRIPTION
"Node state in clusterNodeInfoEntry."
  ::= { clusterNodeInfoEntry 4 }

--******************************************************************************
-- Traps
--******************************************************************************

deviceOffLine NOTIFICATION-TYPE
  OBJECTS {
deviceName,
deviceIp,
deviceMac,
deviceModel
  }
  STATUS current
  DESCRIPTION
"Emerald device is offline"
  ::= { blackboxEntityNotifications 1 }

switchOffLine NOTIFICATION-TYPE
  OBJECTS {
switchName,
switchIp,
switchMac,
switchModel
 }
 STATUS current
 DESCRIPTION
"Switch is offline"
 ::= { blackboxEntityNotifications 2 }

clusterReplicationAlert NOTIFICATION-TYPE
 OBJECTS {
clusterId,
alertDescription
 }
 STATUS current
 DESCRIPTION
"Cluster replication failure"
 ::= { blackboxEntityNotifications 3 }

-- *
-- * SNMPv2 Conformance Information *******************************************
-- *

bbMibConformance  OBJECT IDENTIFIER ::= { blackboxEntity 3 }
bbMibGroups    OBJECT IDENTIFIER ::= { bbMibConformance 1 }

bbMibBasicGroup  OBJECT-GROUP
 OBJECTS {
alertDescription
}
STATUS current
 DESCRIPTION
"Objects used in the traps."
 ::= { bbMibGroups 1 }

bbMibTrapGroup NOTIFICATION-GROUP
 NOTIFICATIONS {
deviceOffLine,
switchOffLine,
clusterReplicationAlert
 }
```

```
  STATUS current
  DESCRIPTION
"BlackBox SNMP traps."
  ::= { bbMibGroups 2 }

bbMibGetGroup OBJECT-GROUP
  OBJECTS {
deviceName,
deviceIp,
deviceMac,
deviceModel,
deviceState,
switchName,
switchIp,
switchMac,
switchModel,
switchState,
clusterInfoAvailability,
clusterId,
clusterVirtualIp,
clusterReplicationLagLev,
clusterNodeInfoTableSize,
clusterNodeId,
clusterNodeName,
clusterNodeIp,
clusterNodeState
  }
  STATUS current
  DESCRIPTION
"BlackBox retrievable objects"
  ::= { bbMibGroups 3 }

END
```

APPENDIX E: REGULATORY INFORMATION

E.1 FCC AND IC STATEMENTS

Federal Communications Commission and Industry Canada Radio Frequency Interference Statements

This equipment generates, uses, and can radiate radio-frequency energy, and if not installed and used properly, that is, in strict accordance with the manufacturer's instructions, may cause interference- to radio communication. It has been tested and found to comply with the limits for a Class A computing device in accordance with the specifications in Subpart B of Part 15 of FCC rules, which are designed to provide reasonable protection against such interference when the equipment is operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user at his own expense will be required to take whatever measures may be necessary to correct the interference.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This digital apparatus does not exceed the Class A limits for radio noise emission- from digital apparatus set out in the Radio Interference Regulation of Industry Canada.

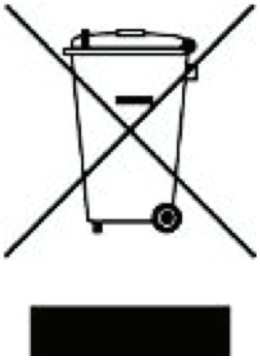
Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Règlement sur le brouillage radioélectrique publié par Industrie Canada.

E.2 SAFETY AND EMC APPROVALS AND MARKINGS/PATENT INFORMATION

E.2.1 SAFETY AND EMC APPROVALS AND MARKINGS

FCC and CE Safety certifications and EMC certifications for this product are obtained under one or more of the following designations: CMN (Certification Model Number), MPN (Manufacturer's Part Number) or Sales Level Model designation. The designation that is referenced in the EMC and/or safety reports and certificates are printed on the label applied to this product.

European Union Notification Warning: This is a class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.



E.2.2 PATENT INFORMATION

This product contains patented designs and is protected by U.S. and international patents and patents pending.

APPENDIX F: TECH SUPPORT/DISCLAIMERS/TRADEMARKS

F.1 TECH SUPPORT/CONTACT INFORMATION

Visit blackbox.com/discover-bb/global-presence for regional technical support and contact information.

F.2 DISCLAIMERS

Black Box Corporation shall not be liable for damages of any kind, including, but not limited to, punitive, consequential or cost of cover damages, resulting from any errors in the product information or specifications set forth in this document and Black Box Corporation may revise this document at any time without notice.

Images contained in this document are included solely to illustrate how to use the product. Since the product can be customized and/or undergo periodic updates, images in this manual will be representative of, although not necessary identical to, the ones displayed on your screen.

F.3 TRADEMARKS USED IN THIS MANUAL

Black Box and the Black Box logo type and mark are registered trademarks of Black Box Corporation.

Any other trademarks mentioned in this manual are acknowledged to be the property of the trademark owners.