BXAMGR

BOXILLA KVM & AV/IT MANAGER

BLACK BOX

TABLE OF CONTENTS

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

TABLE OF CONTENTS

NEED HELP?
LEAVE THE TECH TO US

LIVE 24/7
TECHNICAL
SUPPORT

1.877.877.2269

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

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.

NEED HELP?
LEAVE THE TECH TO US
**LIVE 24/7
TECHNICAL
SUPPORT**
1.877.877.2269

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	CE, FCC
Connectors	10/100/1000 Ethernet (RJ-45) , Serial (DB9), (4) USB 2.0, DVI
Power	AC input: 120–240 V, 50–60 Hz
Power Dissipation	<75 W (PSU rated for 250 W)
Dimensions	System: 1.73"H x 17.3"W x 10.6"D (4.4 x 44 x 26.8 cm); Shipping box: 7.2"H x 22.4"W x 15.4"D (18.5 x 57 x 39 cm)
Weight	System: 10.96 lb. (4.98 kg); Shipping: 14.92 lb. (6.78 kg)
Compatibility	Works with Emerald Unified KVM (EMD4000T, EMD4000R, EMD2002T, EMD2002R, EMD2000T, EMD2000R), InvisaPC (DTX1002-R, DTX1002-T, DTX1000-R, DTX1000-T) and DKM (multiple part numbers)
Serial Port Configuration	112.5 kbaud, 1 Stop bit, No Parity, No Handshake
Default IP Address	192.168.1.24
Default Username	admin
Default Password	admin

1.877.877.2269 BLACKBOX.COM

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

Boxilla is a state-of-the-art KVM and AV/IT 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,

◆ 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 Unified KVM or InvisaPC system and Modular and Compact DKM KVM Matrix Switches. The Emerald or InvisaPC 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.

Emerald or InvisaPC enables 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 Emerald or InvisaPC system provides its users with Receivers that communicate with target compute nodes (whether physical PC or virtual desktop) over a standard TCP/IP network. Physical PCs/Workstations/Servers have an Emerald or InvisaPC Transmitter unit physically connected to provide communication over the TCP/IP network. The performance of Emerald or InvisaPC 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 Emerald or InvisaPC system.

NOTE: References to the Emerald or InvisaPC system or Modular or Compact DKM KVM Switch systems in this document refer to both Receivers and Transmitters.

An Emerald or InvisaPC system can be composed of just Receivers and Transmitters. In these types of systems—called unmanaged— there is no central management. Each device needs to be configured individually 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.

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 Emerald or InvisaPC Receivers and Transmitters 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.
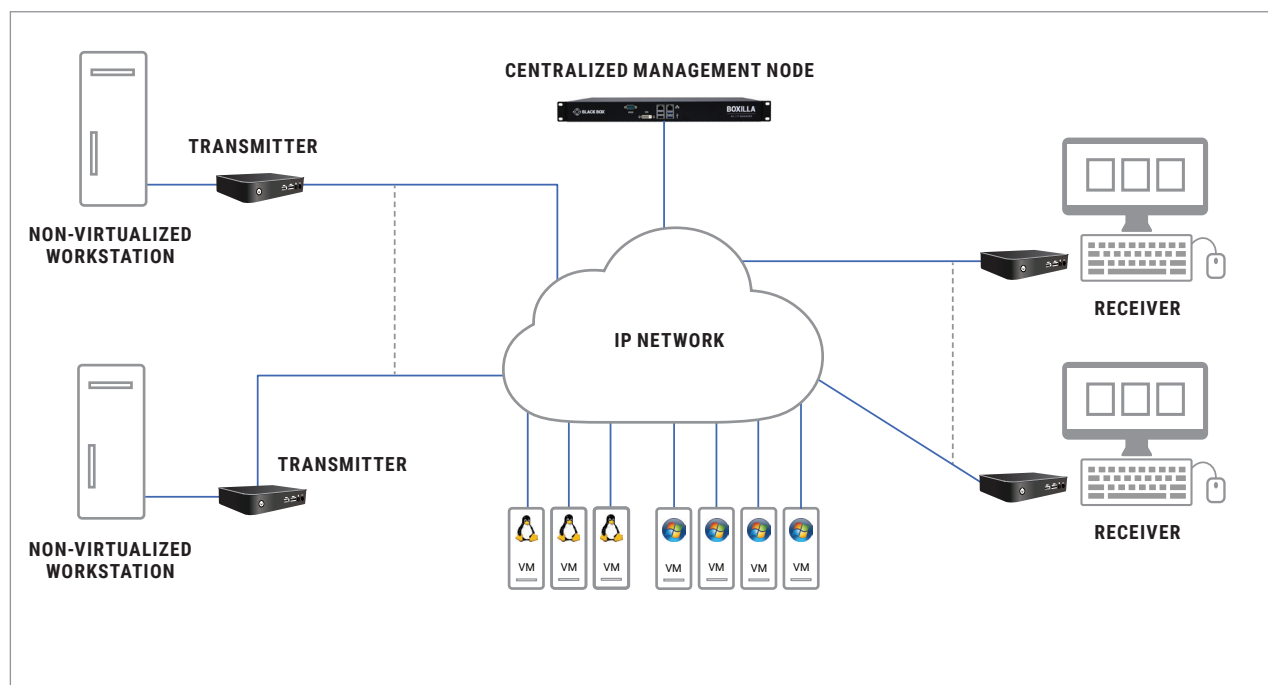
FIGURE 1. EMERALD OR INVISAPC SYSTEM EXAMPLE—INCLUDING PHYSICAL AND VIRTUAL DESKTOPS

2.1 OVERVIEW OF BOXILLA CONCEPTS

The Emerald family is composed of Receivers, Transmitters and Switches. The Emerald or InvisaPC family is composed of Receivers, Transmitters and Managers. Boxilla is the Enterprise class Manager for Emerald or InvisaPC and Modular and Compact DKM KVM Matrix Switches. The core design of the Emerald or InvisaPC architecture is that there is no single point of failure. This means that even if Boxilla goes off-line, the Emerald or InvisaPC system 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.

NEED HELP?
LEAVE THE TECH TO US
**LIVE 24/7
TECHNICAL
SUPPORT**
1.877.877.2269

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;

◆ Devices—KVM and AV appliances that can communicate with each other. In the current release, Emerald or InvisaPC devices and DKM KVM Matrix Switches devices 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 re-direction 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. From the dashboard the administrator can drill down for more detail on activity, errors and individual devices.
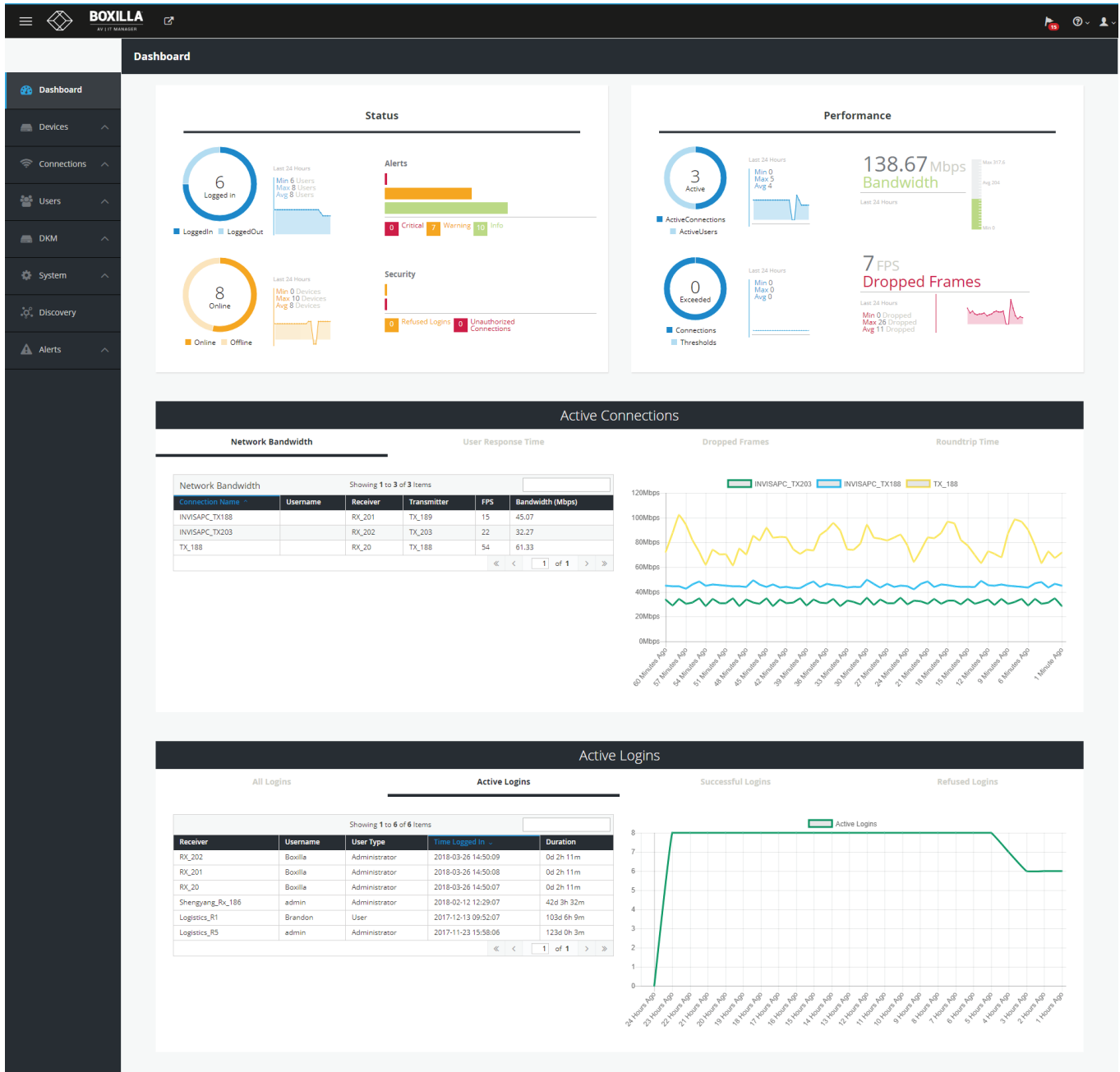
FIGURE 2. BOXILLA DASHBOARD EXAMPLE

CHAPTER 2: PRODUCT OVERVIEW

NEED HELP?
LEAVE THE TECH TO US

LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

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 Emerald or InvisaPC system— 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.

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 3. The Main Menu provides access to:

- Dashboard
- Devices
- Connections
- Users
- DKM
- System
- Discovery
- Alerts

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

FIGURE 3. SCREEN LAYOUT

CHAPTER 2: PRODUCT OVERVIEW

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

A common feature of tables in Boxilla is that they can be sorted by each column (alphabetically either ascending or descending). Clic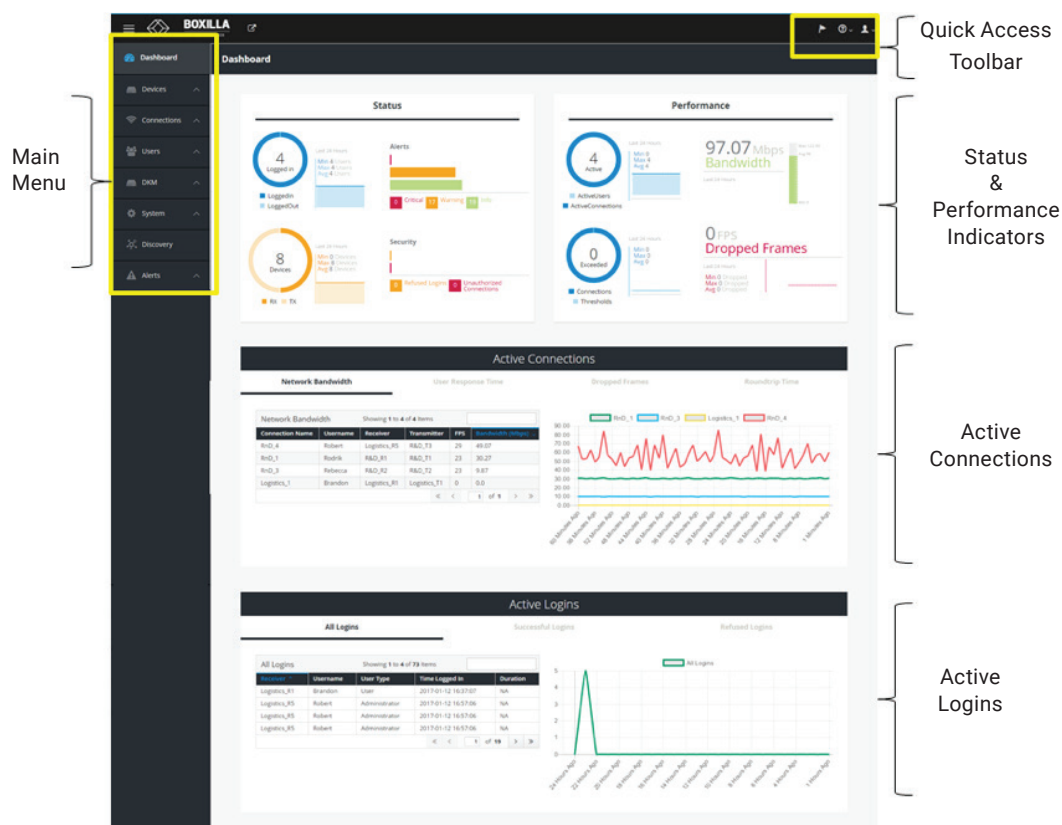k on the column's label (e.g. Connection Name) and the table will be sorted by that column in ascending order. Click on the same column label again and the order will be reversed. Also, a filter can be applied to the values in the column to pick out a subset of rows in the table. For example, typing in RnD into the filter box in the Network Bandwidth table in Active Connection section of the Dashboard in Figure 3 would result in three instead of four rows being displayed as shown in Figure 4.

FIGURE 4. FILTERING TABLE

2.4 MODES OF OPERATION

The Emerald or InvisaPC system has various modes of operation, such as Auto-Login, Auto-Connect, Private Connection and Shared Connection Modes. The Emerald or InvisaPC devices 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 Emerald or InvisaPC devices or that you use DHCP addresses with "infinite time-outs."

2.4.1 AUTO LOGIN

In Auto-Login Mode, turning on the Emerald or InvisaPC Receiver 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 Emerald or InvisaPC Receiver, 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 (INVISAPC ONLY)

In Shared Connection Mode on InvisaPC, 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.

CHAPTER 3: APPLICATIONS

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

The Emerald or InvisaPC system is architected to be flexible so that it 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. Emerald or InvisaPC provides the 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 Emerald or InvisaPC's intuitive On-Screen-Display (OSD). Figure 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 Emerald or InvisaPC products.

NEED HELP?
LEAVE THE TECH TO US

LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

4.1 HARDWARE DESCRIPTION

A Boxilla manager is supplied with the items shown in Table 4-1.

TABLE 4-1. WHAT'S INCLUDED

ITEM
Boxilla Unit
IEC power cord
(4) rubber feet for tabletop deployments
(1) ESD screw
Quick Start Guide

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 browser.
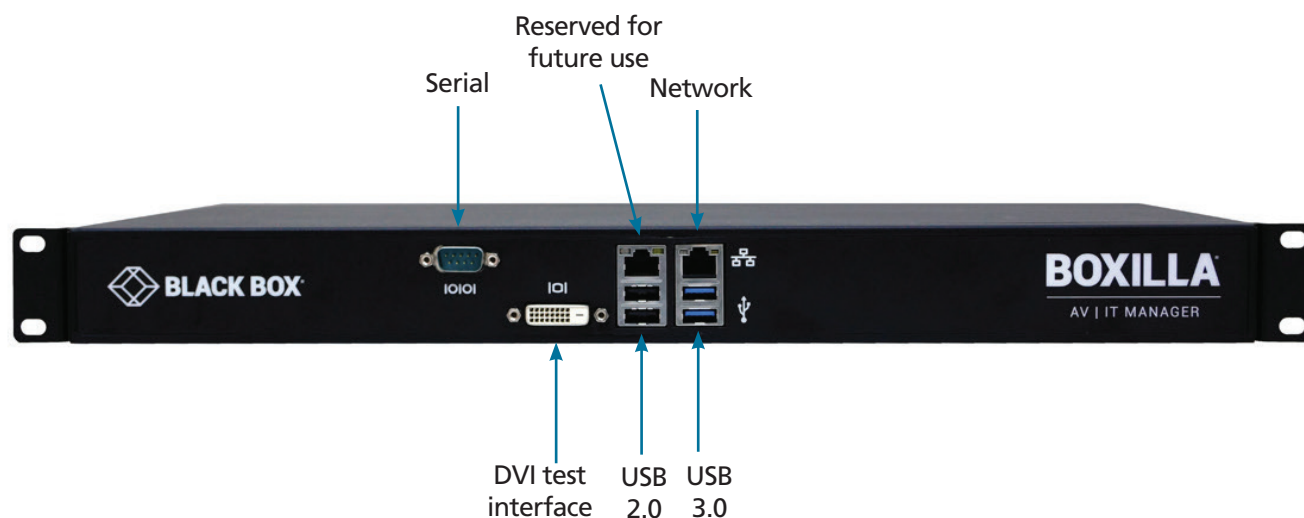

FIGURE 6. BOXILLA FRONT PANEL

NOTE: Only the Network port pointed to in the above diagram (on the right-hand side when you look at the Boxilla unit from the front) is currently operational. The other port is reserved for a future feature.

CONNECTORS NEEDED FOR INSTALLATION

• Serial Port

• Network Port

• Power connector

Power ON/OFF switch

Power supply connector

FIGURE 7. BOXILLA REAR PANEL

TABLE 4-2. PANEL COMPONENTS

COMPONENT	DESCRIPTION
Serial port	DB9 male console
DVI port	Test interface
RJ-45 port	Reserved for future use
Network port	1G Ethernet RJ-45 connector
(2) USB Type A ports	USB 2.0, used for exporting log files
(2) USB Type A ports	USB 3.0, used for exporting log files
Power switch	ON/OFF switch
3-prong outlet	100–240 VAC, 50-60 Hz

CONNECT THE POWER

1. Locate the AC line cord.

2. Attach the AC line 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

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

4.3 INSTALLATION SAFETY

To avoid 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.

4.4 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. 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: 112.5 kBaud

◆ 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.
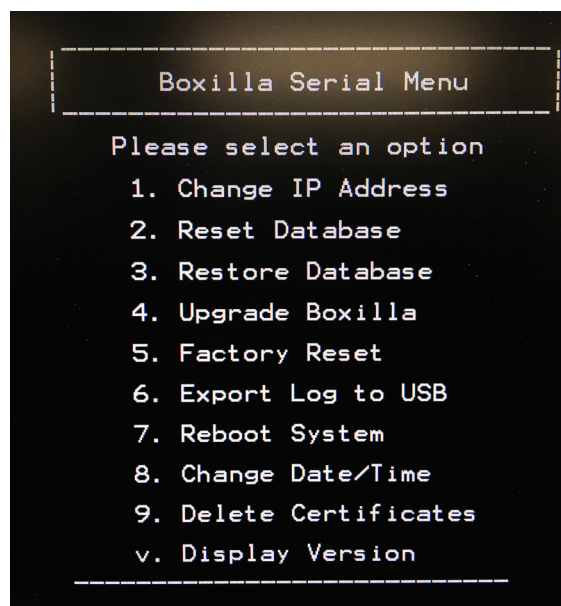

FIGURE 8. BOXILLA SERIAL MENU

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

4.5 BROWSER 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. 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 Network port (RJ-45) as shown in Figure 6, open a web-browser and enter the default IP address for the Boxilla AV/IT Manager: 192.168.1.24. This should bring up the Boxilla login screen shown below in Figure 9.
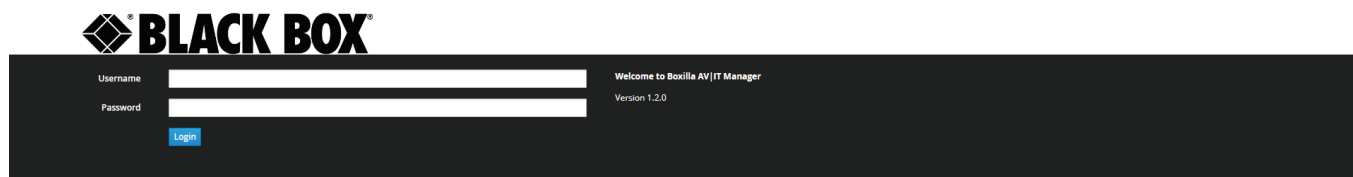

FIGURE 9. BOXILLA LOGIN SCREEN

NOTE: Only the Network port pointed to in Figure 6 (on the right-hand side one when you look at the Boxilla unit from the front) is currently operational. The other port is reserved for a future feature.

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 10), 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.
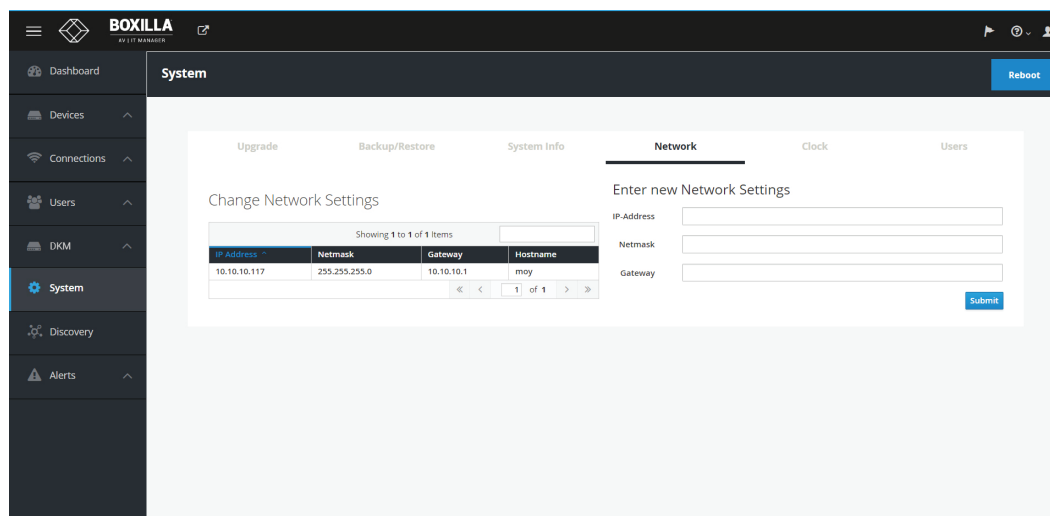

FIGURE 10. SYSTEM —> SETTINGS —> NETWORK SCREEN

NEED HELP?
LEAVE THE TECH TO US
**LIVE 24/7
TECHNICAL
SUPPORT**
1.877.877.2269

4.6 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. Slide the Boxilla unit into the vacant 1U space within the rack.

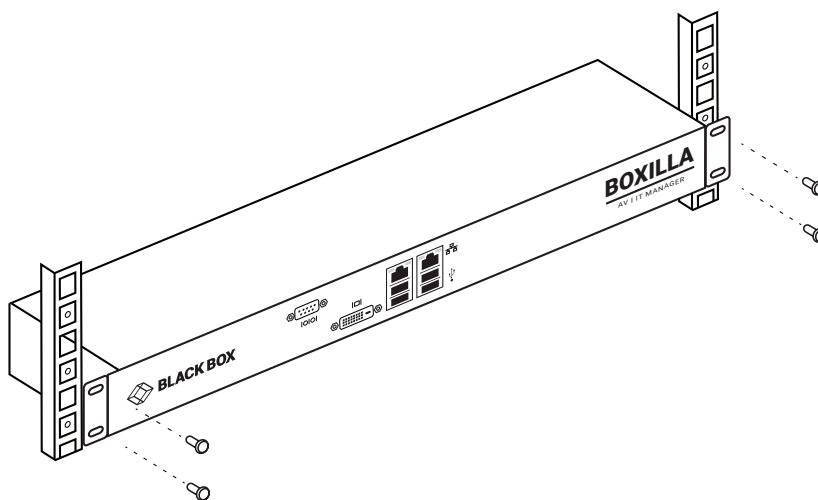2. Secure each bracket to the rack using two screws per side as shown below.

FIGURE 11. MOUNTING BOXILLA IN A RACK

To protect the unit, please use the ground point on the Boxilla unit on the rear of the Boxilla unit shown in Figure 12 (using the provided screw) for connecting to the ground point of the rack or cabinet.

4.6.1 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).

NEED HELP?
LEAVE THE TECH TO US

**LIVE 24/7
TECHNICAL
SUPPORT**

1.877.877.2269

FIGURE 12. ESD CONNECTION

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

CHAPTER 5: BOXILLA CONFIGURATION

This section covers the configuration of Boxilla for administrators.

5.1 SUPPORTED BROWSERS

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

◆ Google Chrome

◆ Internet Explorer

◆ Firefox

◆ Safari

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

5.2 LOGIN

Ensure the Boxilla unit is powered up. Wait two minutes after applying power before attempting to access to allow the system to boot up.

Using a computer located anywhere within the network, open a web browser (see supported browsers list above) and enter the default IP address for the Boxilla server: 192.168.1.24 .

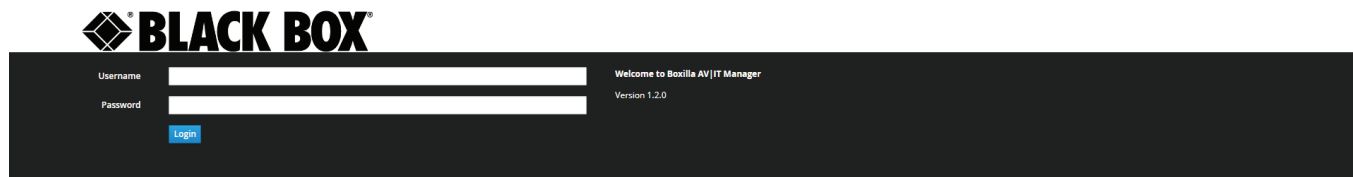The Login screen will be displayed as shown in Figure 13.

FIGURE 13. BOXILLA LOGIN SCREEN

Enter your Username and Password and click the Login button.

Default username: admin
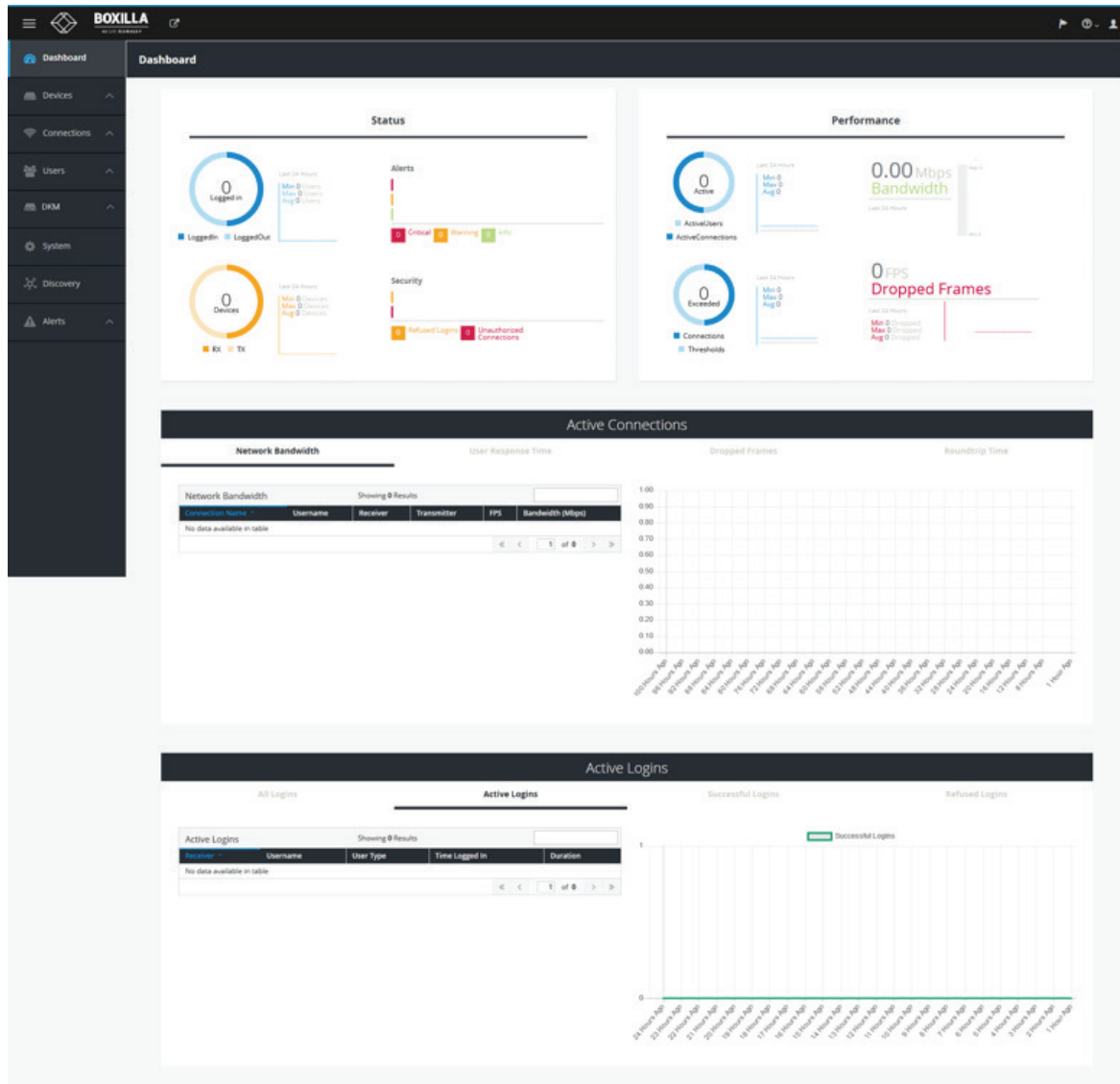
Default password: admin

FIGURE 14. BOXILLA INITIAL SCREEN ON LOGIN

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

CHAPTER 5: BOXILLA CONFIGURATION

You are strongly recommended 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 15.

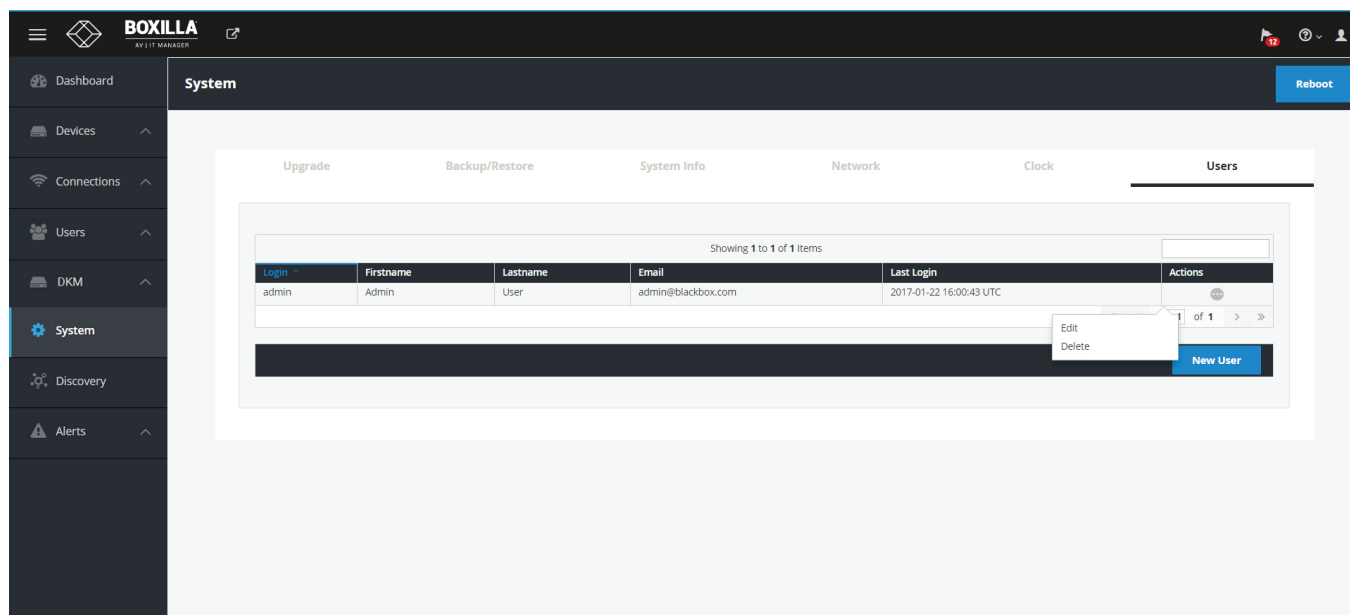◆ Click the "…" icon on the Admin row and click on the edit option.

FIGURE 15. CHANGING ADMIN USER PASSWORD

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

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
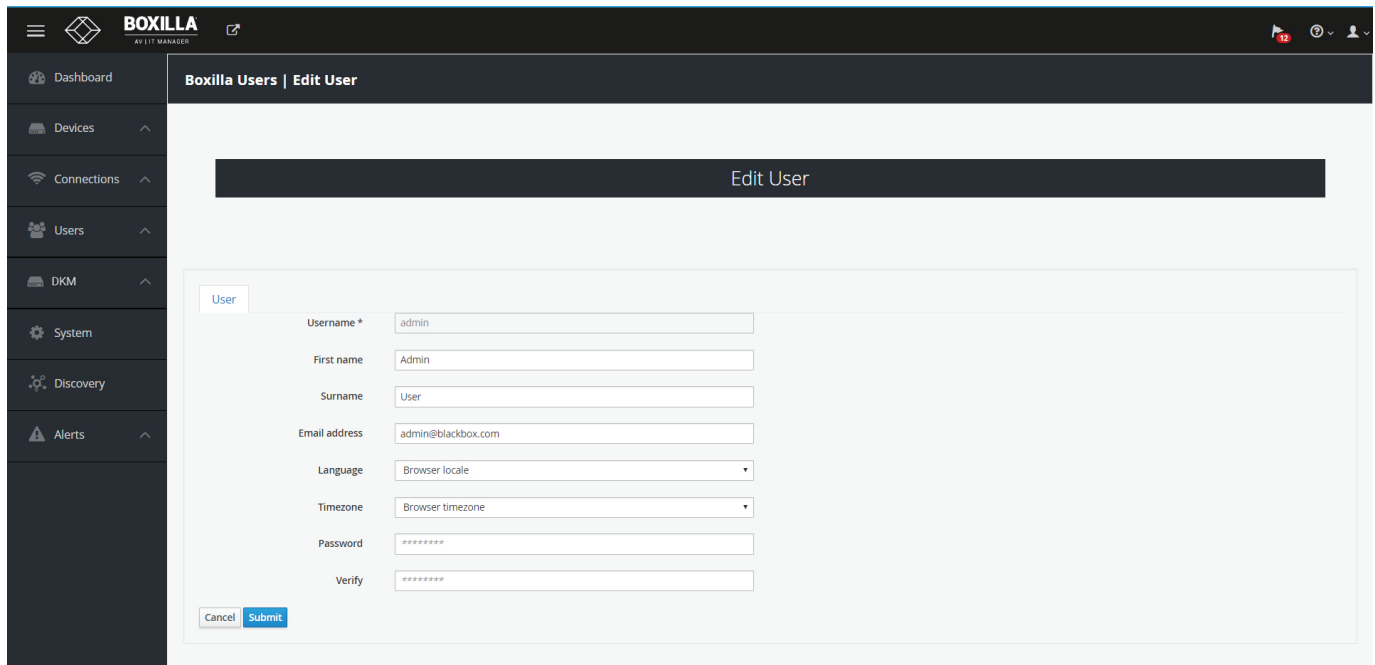1.877.877.2269

CHAPTER 5: BOXILLA CONFIGURATION

FIGURE 16. EDIT ADMIN USER

5.3 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).

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: Swapping Out a Boxilla Server.

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 Black Box's discovery protocol to automatically find devices to be managed on the network. This discovery protocol can span across subnets. To allow Black Box's Emerald or InvisaPC automatic discovery protocol to operate across subnets, multicast routing should be enabled in the routers in the network. Black Box's discovery protocol is not required for Emerald or InvisaPC systems to operate but it is recommended to enable Boxilla to search for devices across multiple subnets. If the Emerald or InvisaPC discovery protocol is not enabled, 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 17. The example page already has some devices "discovered." The devices are listed in a table as shown in Figure 17.
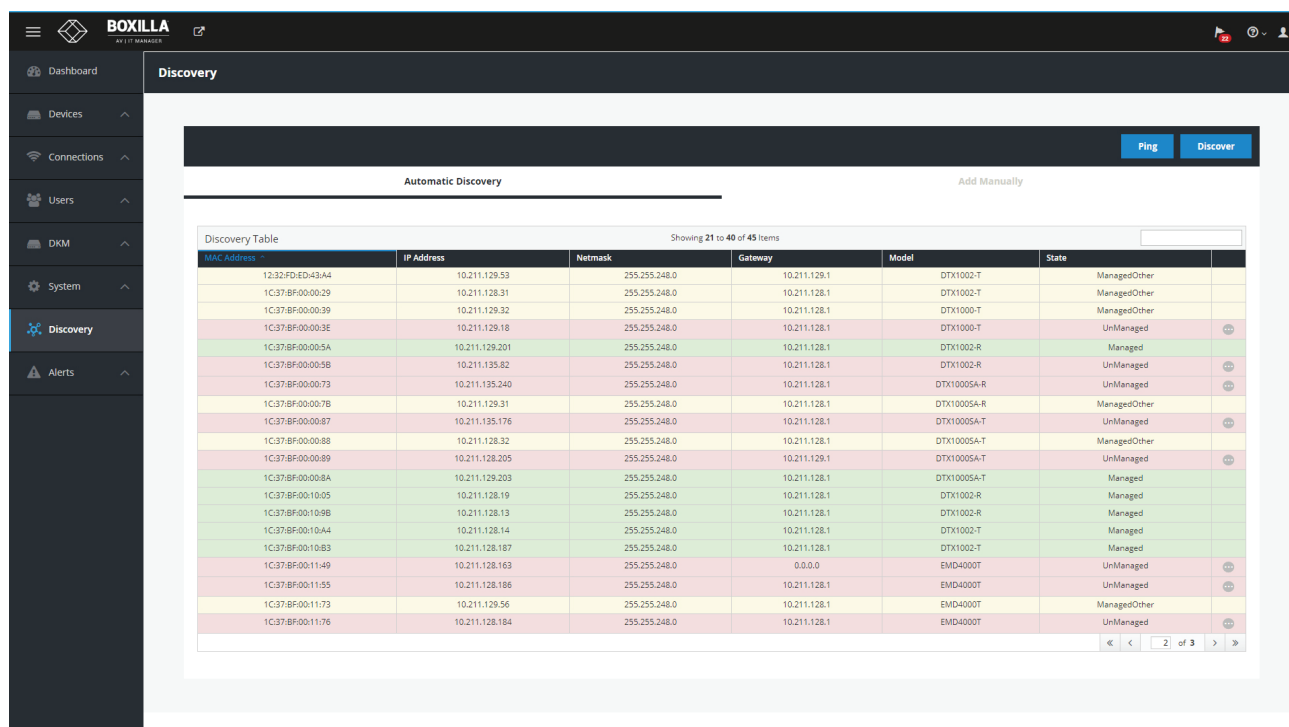

FIGURE 17. DISCOVERY PAGE

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 B: Overview of Boxilla and Emerald or InvisaPC Network Protocols for more details on the actual protocol sequence.
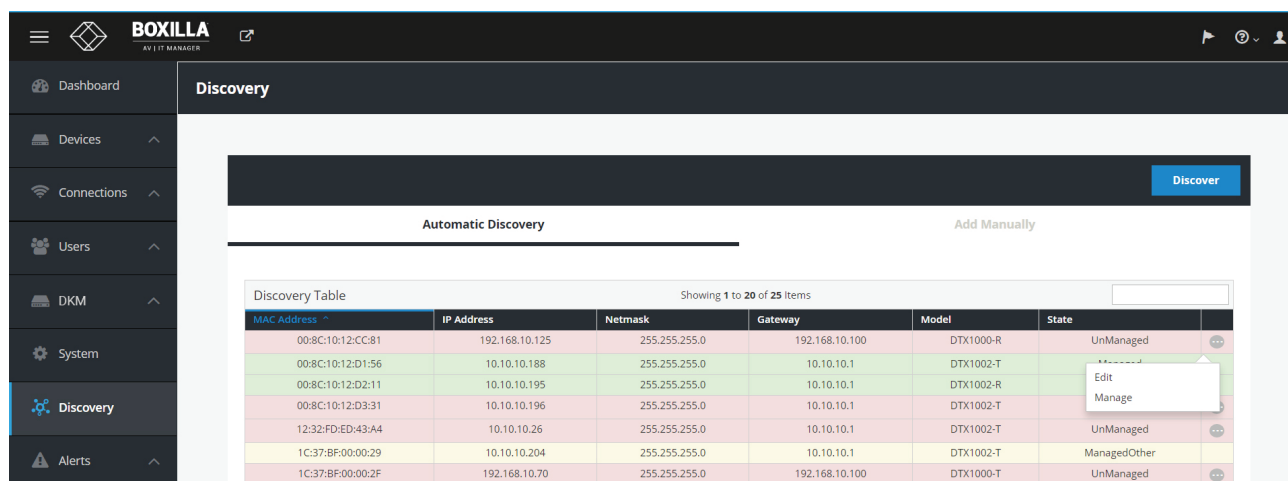
NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

CHAPTER 6: DISCOVERY—ADDING DEVICES

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

◆ Managed—this device is part of the domain managed by this Boxilla manager

◆ 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 as shown in Figure 18 and select the Edit option. This allow Network configuration of a device to be changed as shown in Figure 19. Typically, this is used to change a device from its default IP address to a unique address.

FIGURE 18. DISCOVERY—EDIT DEVICE

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 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 20. 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 Emerald or InvisaPC device)
the system will return a message of "device not reachable."
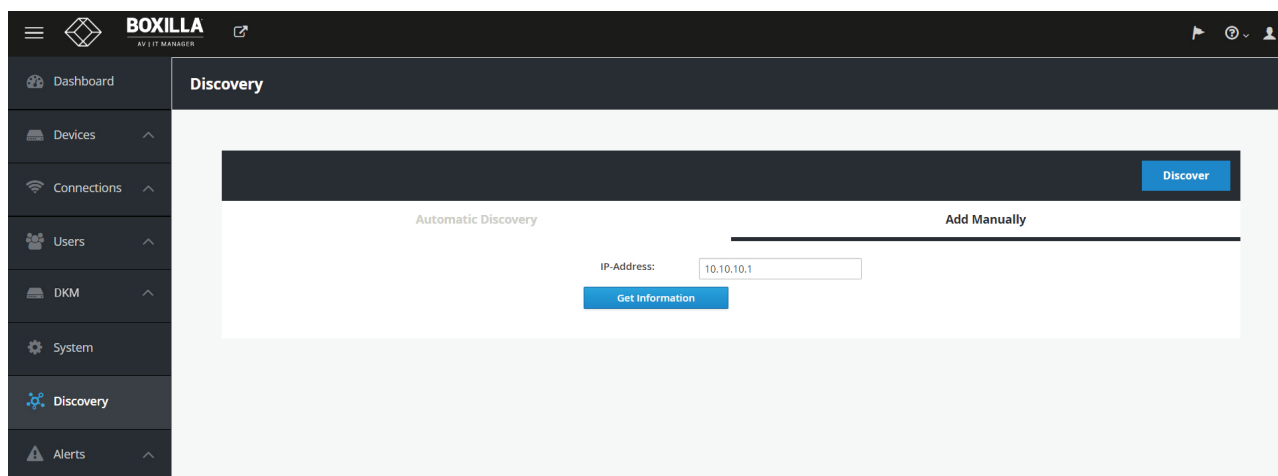

FIGURE 20. DISCOVERY—MANUAL ADD

The administrator can give the device a name and check that the device's details are correct if required to ensure it is the correct device (IP address, Serial Number and Model type). To manage this device, click on "Manage Device" button as shown in Figure 21.
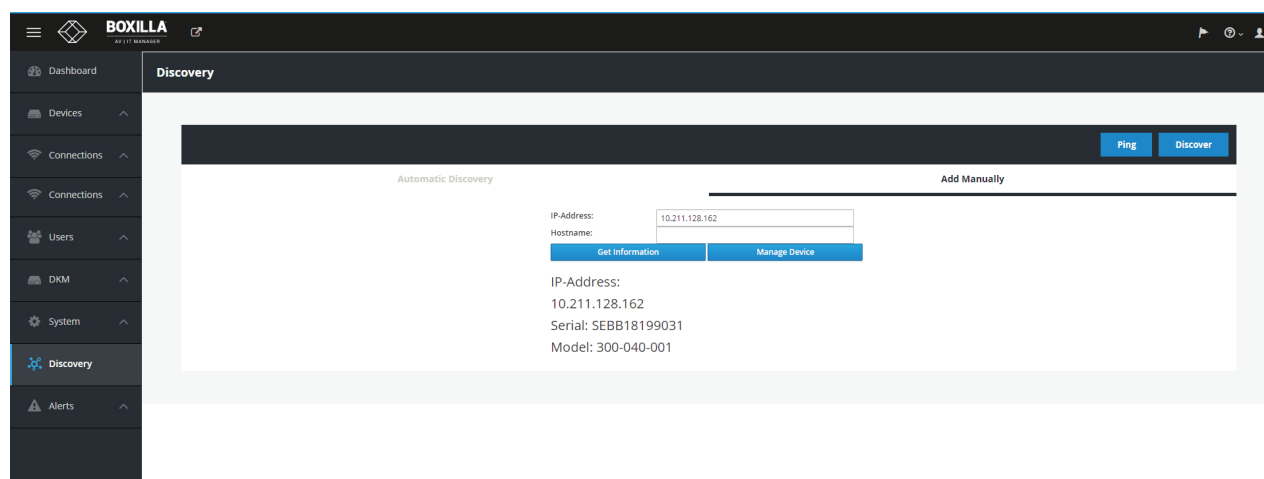

FIGURE 21. DISCOVERY MANUAL ADD & MANAGE DEVICE

CHAPTER 6: DISCOVERY—ADDING DEVICES

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

6.3 DISCOVERY—WHAT HAPPENS TO A DEVICE WHEN MANAGED

Emerald or InvisaPC units 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 logins on 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 or InvisaPC Receiver powers up automatically when power is applied or needs the power button to be pressed;

◆ Auto-Login—whether an Emerald or InvisaPC 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 InvisaPC 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.

NEED HELP?
LEAVE THE TECH TO US

LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

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 22 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 four options: Settings, Upgrades, Global and Statistics. These options are described in the following sections. Click on Settings and the following screen appears.

FIGURE 22. DEVICES SETTINGS SCREEN

Click on Video Settings in the middle of this screen to see the Device Name, Configuration, IP Address, Model, State, Status, Video Quality, Video Source Opt, EDID Settings DVI 1, Cloned Receiver, EDID Settings DVI 2, Cloned Receiver and Options for each TX or RX unit.

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.

NOTE:

a) It's not possible to configure the TX settings of an Emerald TX device.

b) A user can configure the HTTP_Enable attribute for Emerald RX deivces but it not possible to configure the Power Mode setting for Emerald RX devices.

7.1 DEVICES—SETTINGS

With Boxilla 2.0, 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

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

CHAPTER 7: DEVICES

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 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.

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 results in the device rebooting.

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.
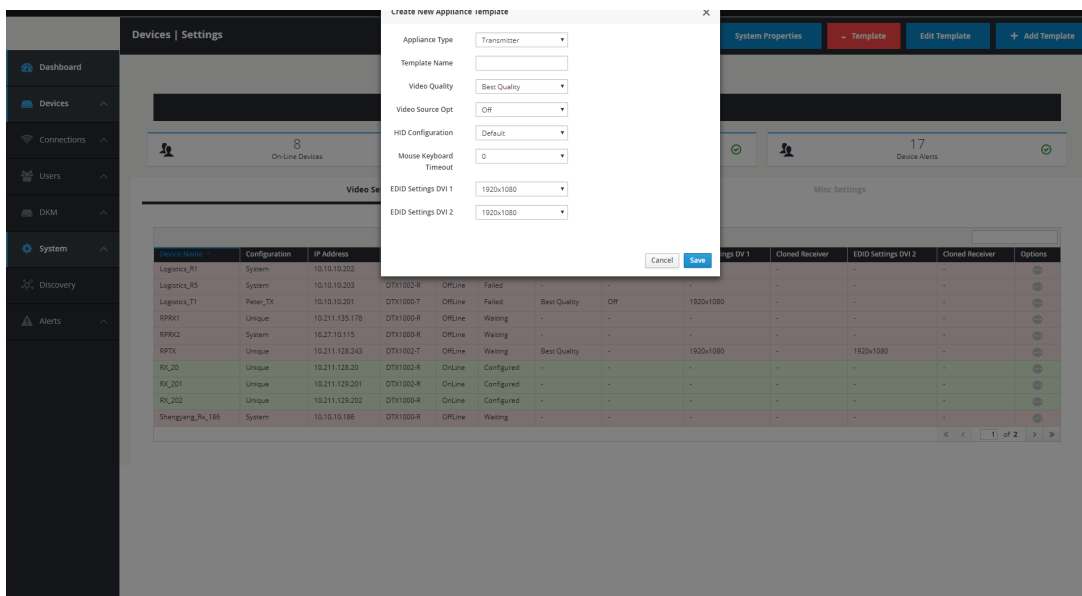

FIGURE 23. CREATE NEW DEVICE TEMPLATES SCREEN

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.

CHAPTER 7: DEVICES

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

- 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, or MAC.

- 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, or 1024 x 768.

- EDID Settings DVI 2: Choose from 1920 x 1080, 1920 x 1200, 1680 x 1050, 1280 x 1024, or 1024 x 768.

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.

FIGURE 24. EDIT TEMPLATE SCREEN
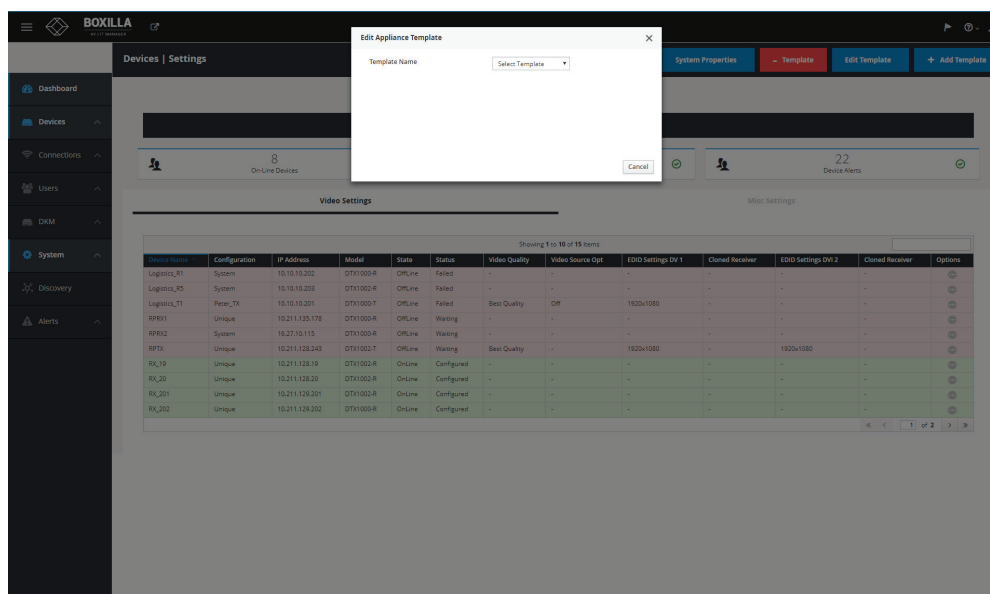
To delete a device template, click on the red -Template button at the top of the Devices —> Settings screen. The Delete Appliance Template screen pops up. Select the template you want to delete from the drop-down menu, then click the Delete button to delete the template, or click the Cancel button to cancel the deletion.

NOTE: You can only delete a template that is currently not in use.

CHAPTER 7: DEVICES

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
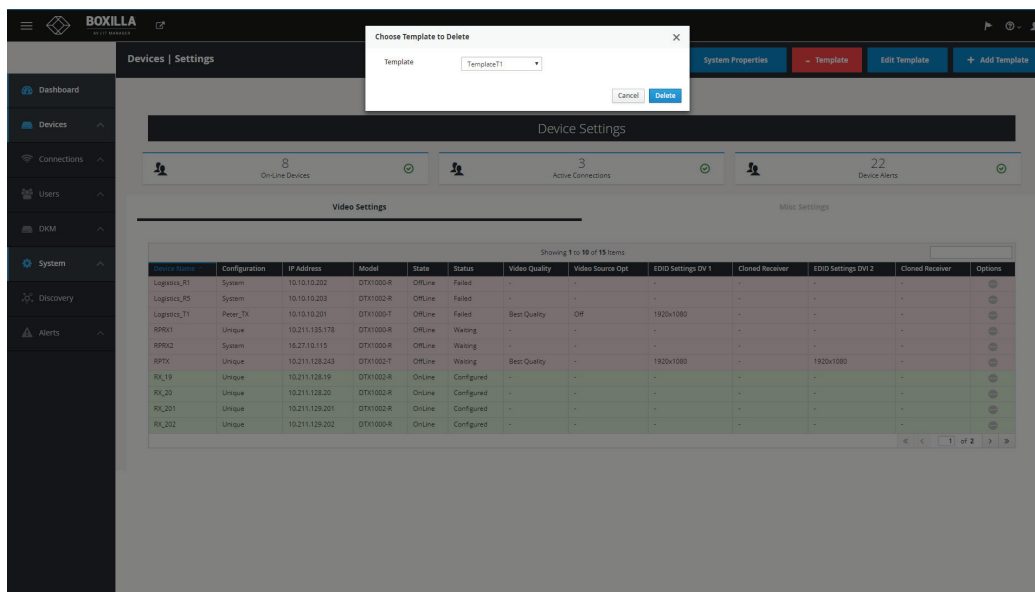**TECHNICAL**
SUPPORT
1.877.877.2269

FIGURE 25. DELETE TEMPLATE 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.
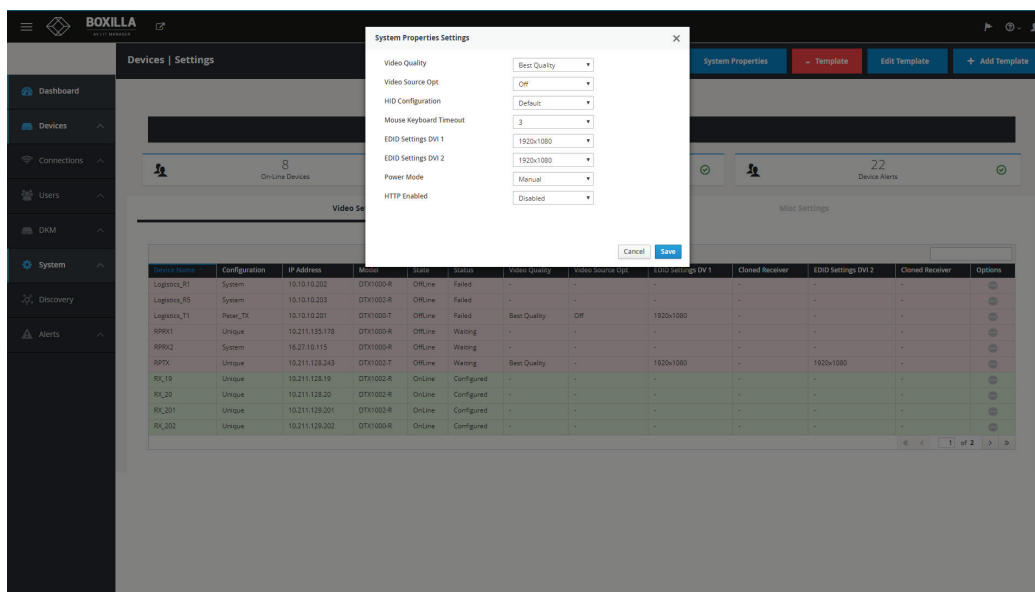

FIGURE 26. EDIT SYSTEM PROPERTIES SCREEN

- ◆ 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, or MAC.
- 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, or 1024 x 768.
- EDID Settings DVI 2: Choose from 1920 x 1080, 1920 x 1200, 1680 x 1050, 1280 x 1024, or 1024 x 768.
- 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 —> Network 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 and EDID Settings DVI 2. Click Save, or click Cancel to cancel the changes without saving.
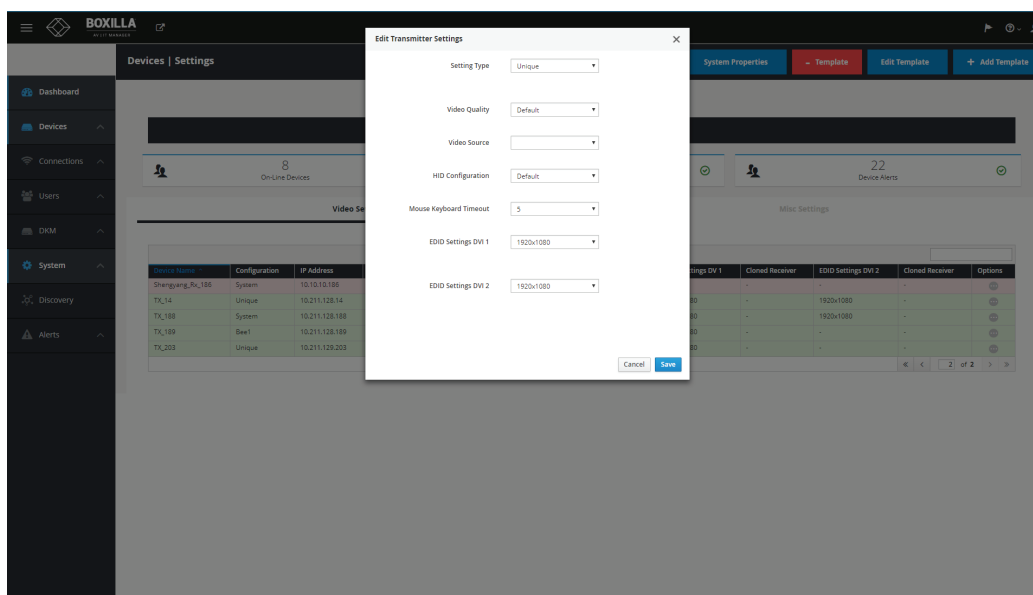

FIGURE 27. EDIT INDIVIDUAL DEVICE SETTINGS SCREEN

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 28. 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)
- UnManage— removes the device from the managed domain and restores the device back to factory defaults
- Change Device Name — allows the network settings to be changed
- Reboot—power cycles the device

CHAPTER 7: DEVICES

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
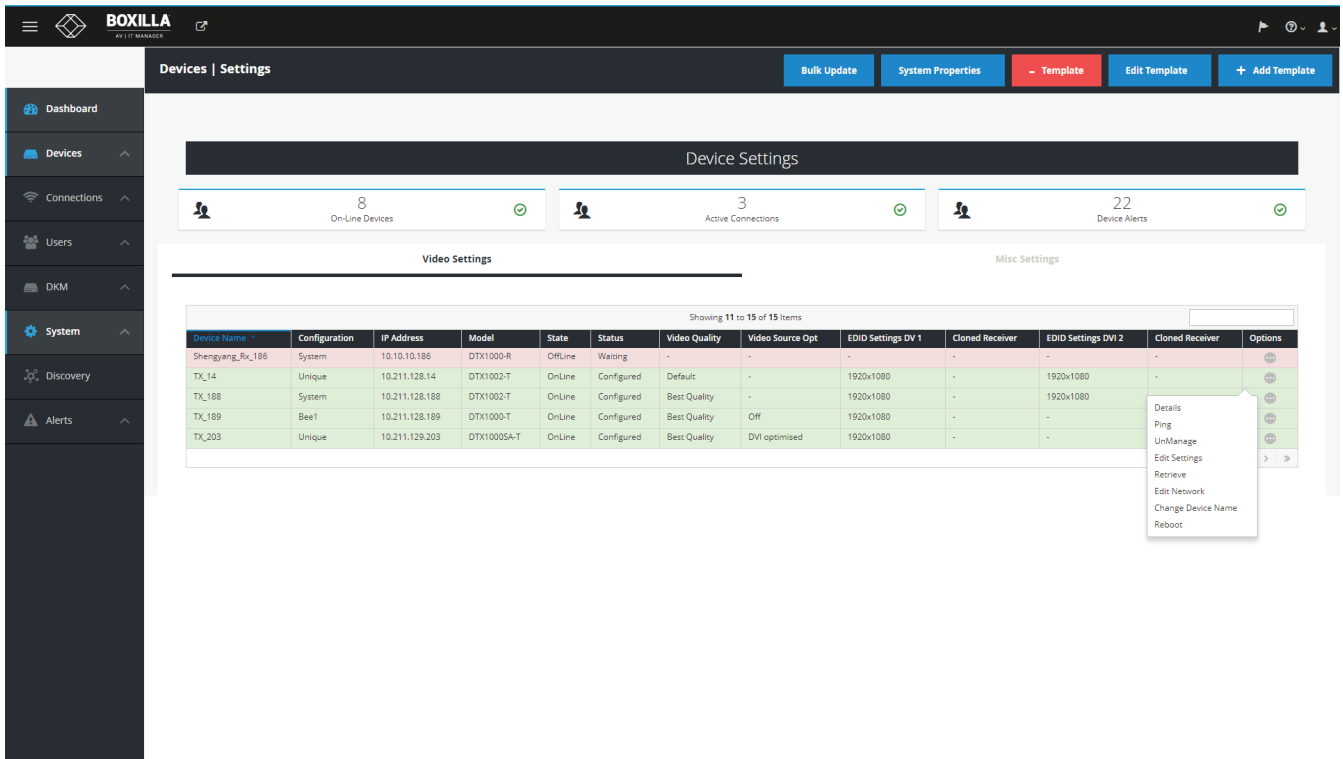**TECHNICAL**
SUPPORT
1.877.877.2269

FIGURE 28. DEVICE OPTIONS

The Ping button on the page allows any IP device (not just Emerald or InvisaPC devices) to be pinged to check its reachability.

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.
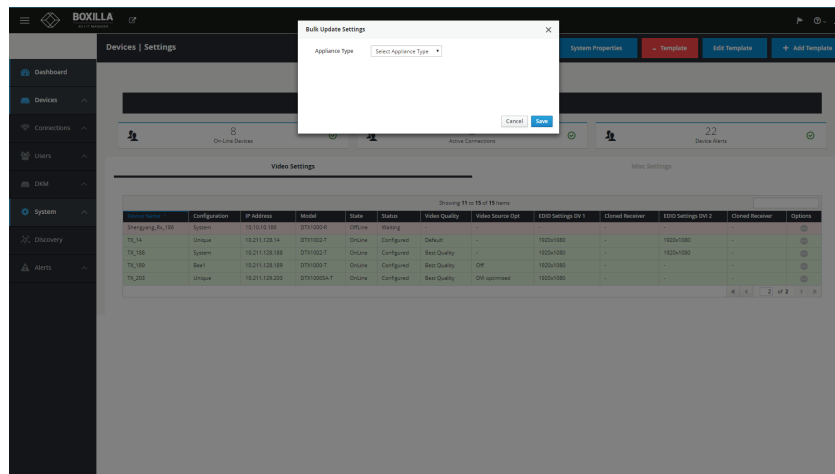

FIGURE 29. BULK UPDATE SETTINGS SCREEN

7.2 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 30.

7.2.1 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). For Emerald or InvisaPC, this needs to be done for both Receivers (DTX-R or EMD4K-R) and Transmitters (DTX-T or EMD4K-T).

FIGURE 30. DEVICE UPGRADE PAGE

The Administrator loads a new version of firmware by clicking on the "Upload" button on the page and choosing the file 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.). This new firmware version will be added to appropriate Device list (i.e. Receiver or Transmitter list).

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

CHAPTER 7: DEVICES

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

7.2.2 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.
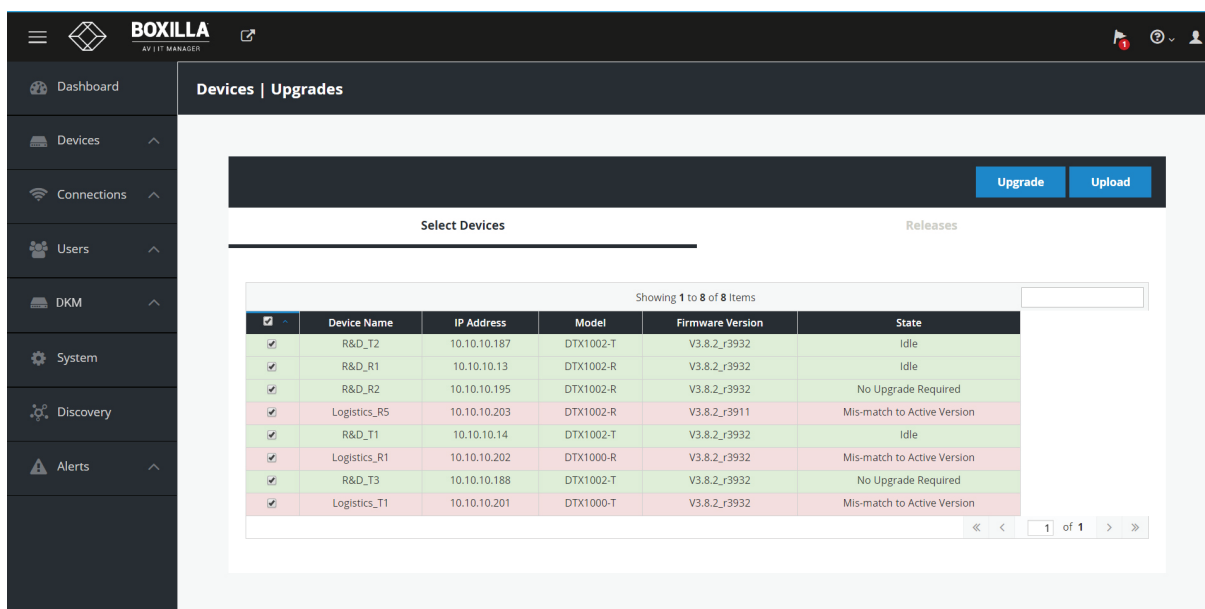

FIGURE 31. DEVICE UPGRADE SELECTION

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.

CHAPTER 7: DEVICES

NEED HELP?
LEAVE THE TECH TO US

LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

7.3 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—Settings page as shown in Figure 32. 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 Emerald or InvisaPC devices 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.

FIGURE 32. DEVICE SETTINGS—CONFIGURATION SETTINGS

7.3.1 HOTKEY

The hotkey is used with the "o" key to terminate the current connection and bring up the OSD on an Emerald or InvisaPC 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.

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

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 or InvisaPC Receiver. 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.

7.3.2 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).

NEED HELP?
LEAVE THE TECH TO US
**LIVE 24/7
TECHNICAL
SUPPORT**
1.877.877.2269

7.3.3 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 or InvisaPC 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 Emerald or InvisaPC.

NOTE: Inactivity occurs when the mouse or keyboard is not pressed or moved for a set period of time.

7.3.4 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 Emerald or InvisaPC Receiver.

NOTE: We currently do not cater for 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.

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.

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

CHAPTER 7: DEVICES

On the Emerald or InvisaPC Receiver, 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 Emerald or InvisaPC Receiver 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.

7.4 DEVICES—STATISTICS

The Device Statistics page provides an overview of the operation of the managed domain as shown in Figure 33. 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.
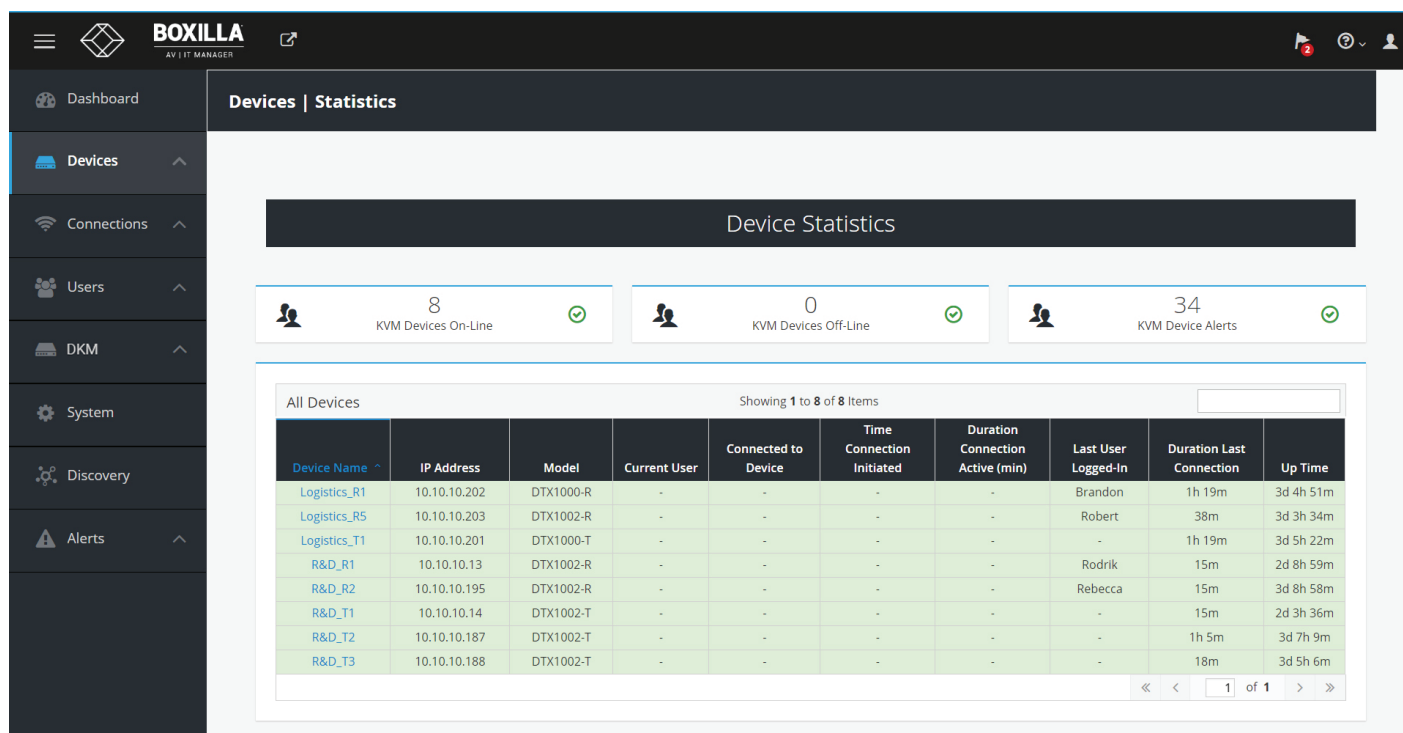

FIGURE 33. DEVICE STATISTICS

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

CHAPTER 8: CONNECTIONS

Connections define the properties for the flow of keyboard, mouse, video, audio and USB traffic between an Emerald or InvisaPC Receiver and an Emerald or InvisaPC Transmitter or 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 an Emerald or InvisaPC Receiver, they are presented with their allocated connections on the Connections Tab of the OSD on that Receiver.

8.1 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 34.

FIGURE 34. CONNECTIONS MANAGE SCREEN

The table shows the connection name, whether the connection is linked to a connection template (see section 8.1.2), connection type (private or shared), what/how the connection is made (via Tx, Direct to VM, via VM Pool or via Connection Broker) 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 or InvisaPC, when set it enables both video heads to operate if connected to a source that supports dual-head operation (e.g. Dual-head Emerald or InvisaPC Transmitter). This setting has no effect on a single-video head Emerald or InvisaPC.

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

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 Receiver until successful. This is useful when using Emerald or InvisaPC 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 1.0 has NLA set to "disabled" by default and user doesnt have option to change. On VM, the NLA setting has to be set to "disabled".

The administrator can edit the connections parameters or delete the connection using the "•••" icon on the specific connection row. The parameters for a connection are defined in more detail in section 8.1.1.

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.

8.1.1 CONNECTIONS—ADD CONNECTION

To allow an Emerald or InvisaPC Receiver to connect to a target Emerald or InvisaPC Transmitter 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 34.

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, as shown in Figure 35, 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 InvisaPC Transmitter;

◆ Direct to VM—connect directly to a virtual machine using its IP address or hostname;

◆ Broker—connect to a virtual machine via a connection broker (i.e., indirect connection);

◆ VM Pool—connect to a virtual desktop that is hosted in VM Pools. The IP address for this Pool is defined in the global settings (see section 7.3.5).
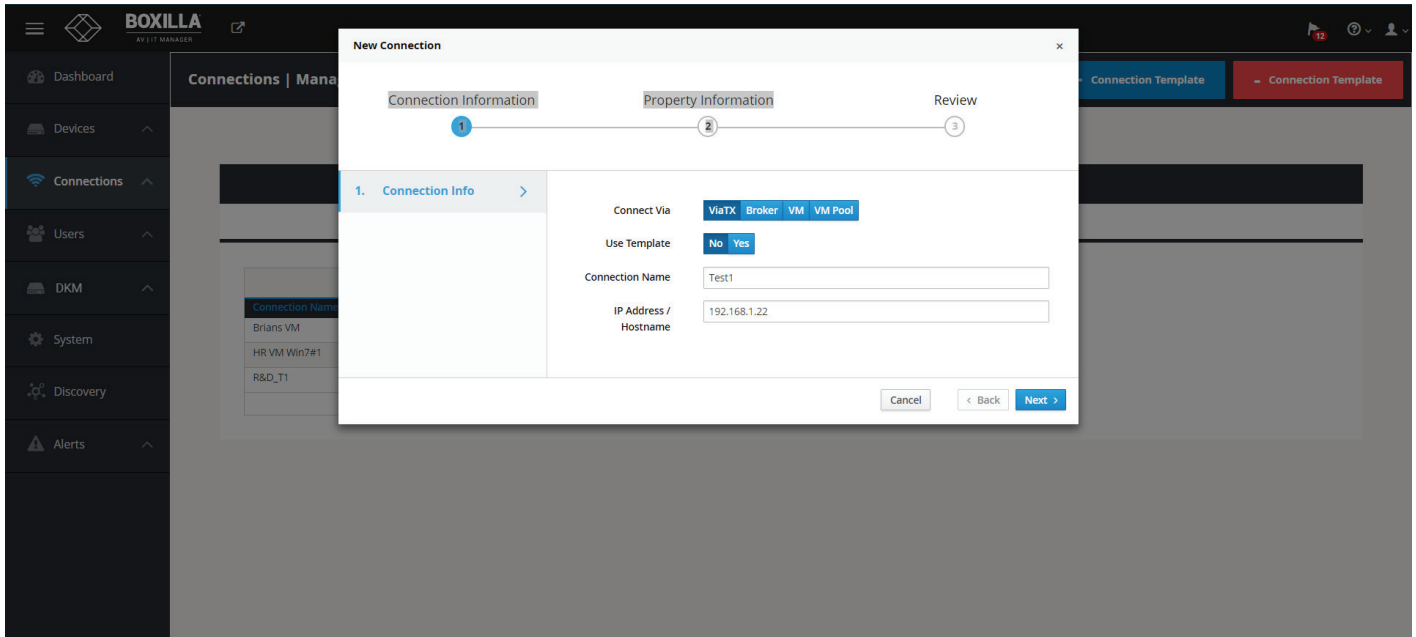
FIGURE 35. ADD CONNECTION—TX

The other parameters on this screen are:

- 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 " "/ \ [ ] : ; | = , + * ? < > `'.

- IP Address/Hostname: the IP address of the Emerald or InvisaPC Transmitter or the Virtual Desktop in IP v4 format.

If the Connect Via is set as "Broker" as shown in the figure below, extra parameters can be defined.
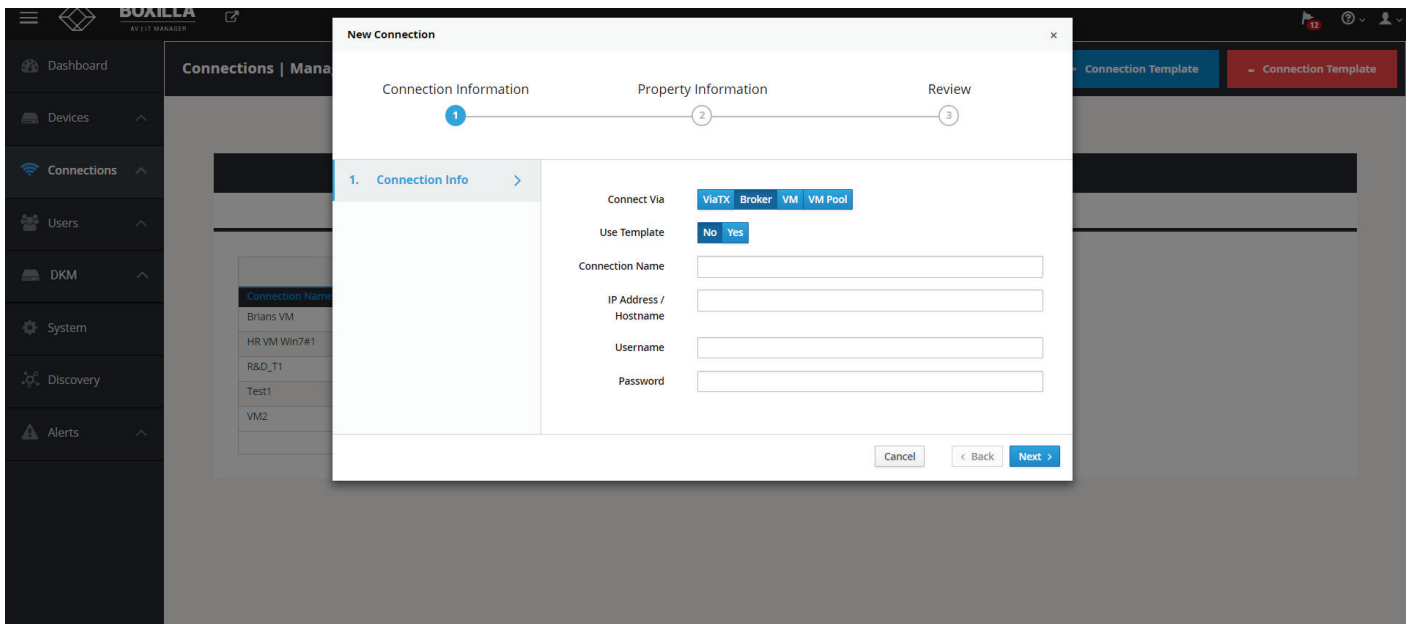
FIGURE 36. ADD CONNECTION—BROKER OR VM

NEED HELP?
LEAVE THE TECH TO US
**LIVE 24/7
TECHNICAL
SUPPORT**
1.877.877.2269
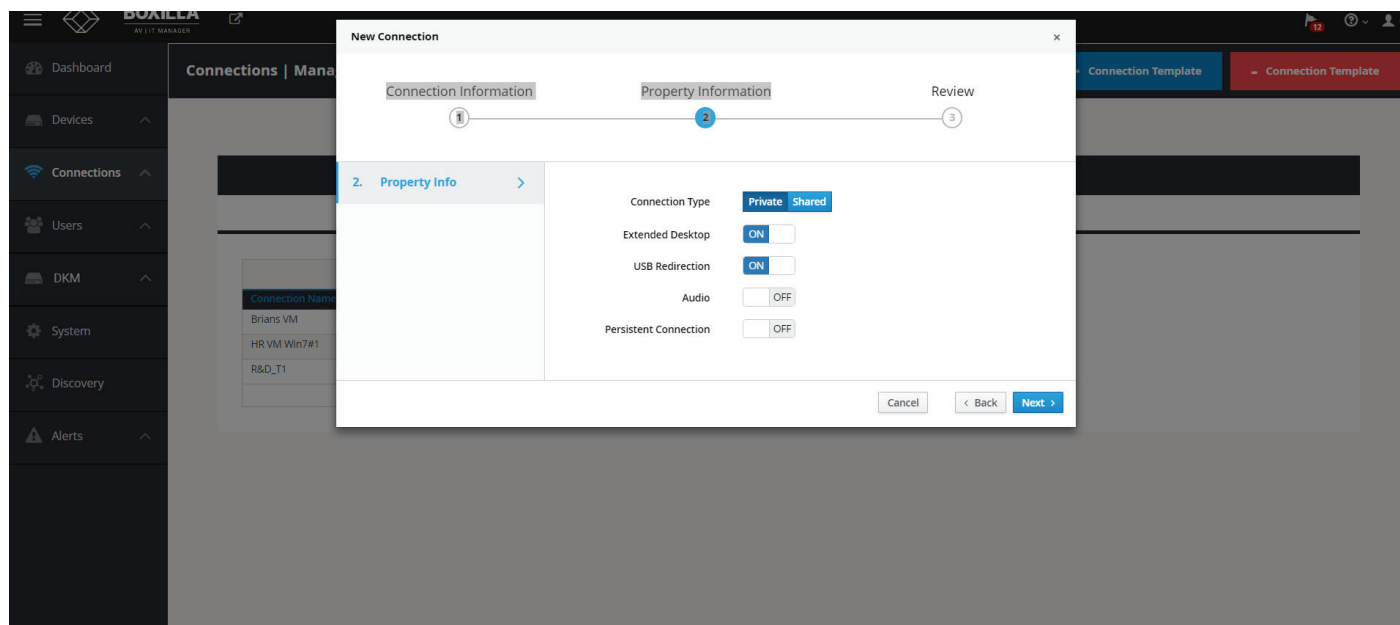
FIGURE 37. ADD CONNECTIONS—PROPERTIES

The extra parameters that can be defined are:

◆ 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 re-direction disabled on shared connections.

◆ Extended Desktop: On a dual-video head Emerald or InvisaPC, this enables both video heads to operate if connected to a source that supports dual-head operation (e.g. Dual-head Emerald or InvisaPC Transmitter). This setting has no effect on a single-video head Emerald or InvisaPC.

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

◆ Audio: When set, this enables 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 InvisaPC for digital signage or an application with no keyboard/mouse that needs to stay connected to a defined source.

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

◆ 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.

.

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

CHAPTER 8: CONNECTIONS

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.
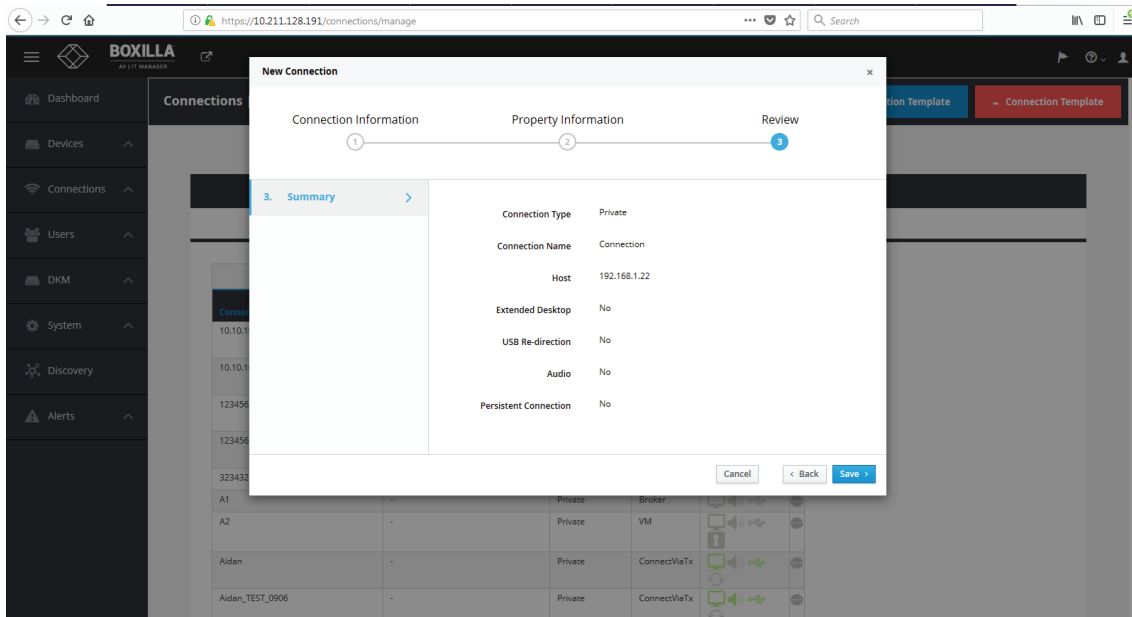

FIGURE 38. CONNECTION TYPE — PRIVATE

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

CHAPTER 8: CONNECTIONS

8.1.2 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 39. 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.
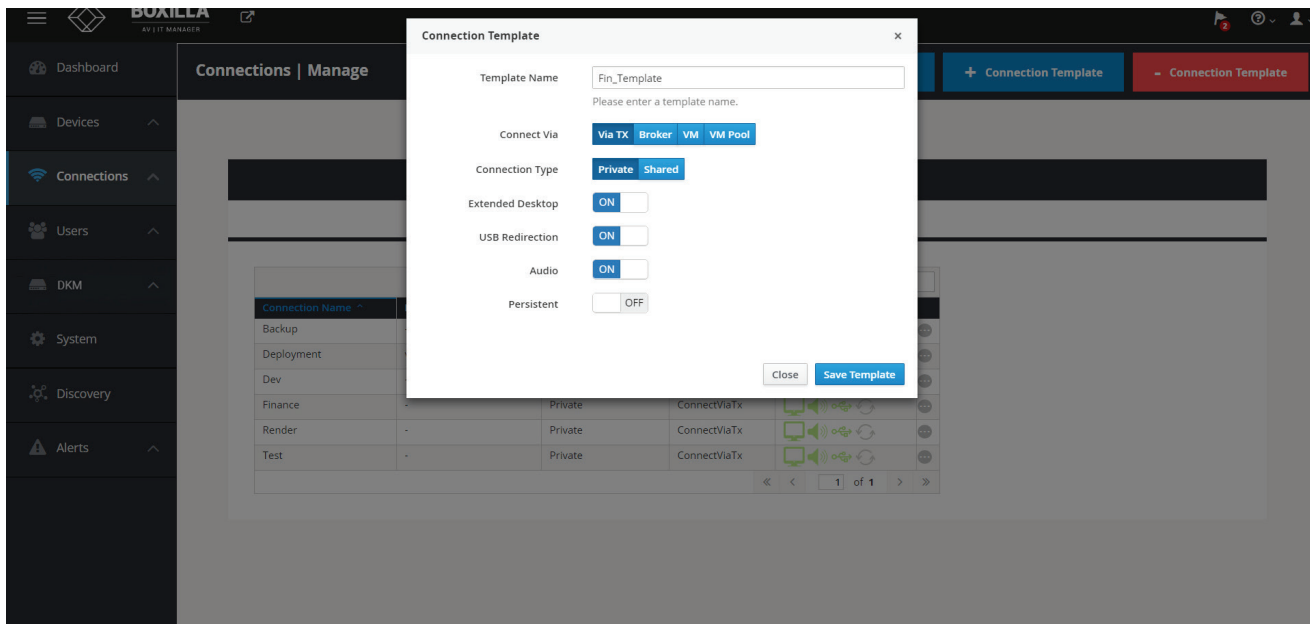
FIGURE 39. ADD CONNECTION TEMPLATE

8.1.3 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.

8.2 CONNECTIONS—GROUPS

Boxilla 1.1 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.

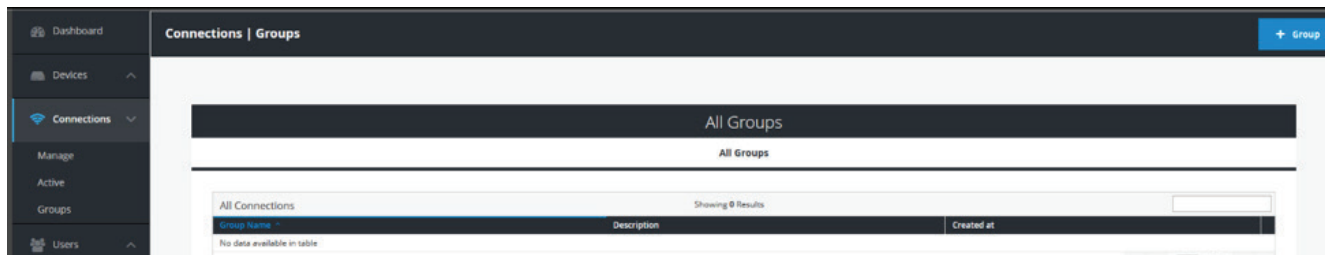Connections option can be found on left side pane of Boxilla user interface.

FIGURE 40. CONNECTIONS OPTION

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

CHAPTER 8: CONNECTIONS
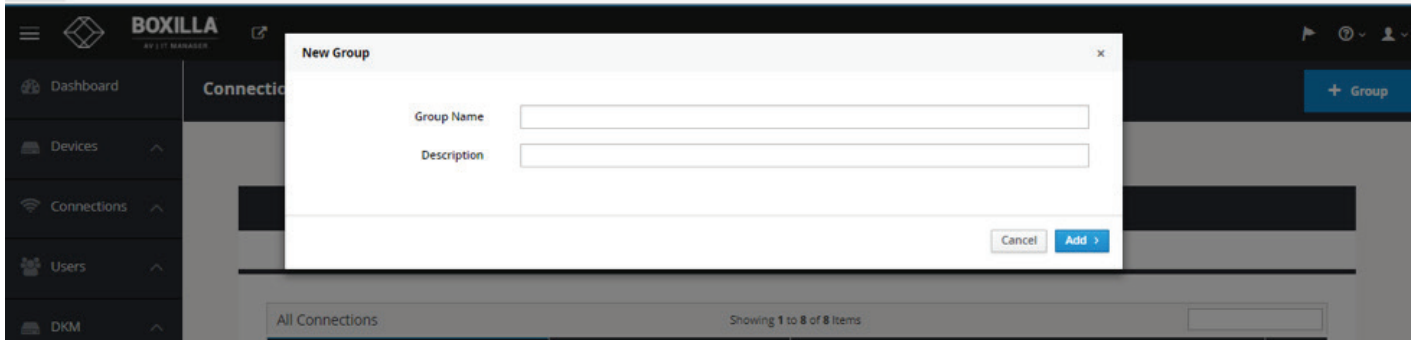
To add a connection group:

FIGURE 41. ADD CONNECTION GROUP SCREEN

Once a connection group has been added, you will see the following screen.
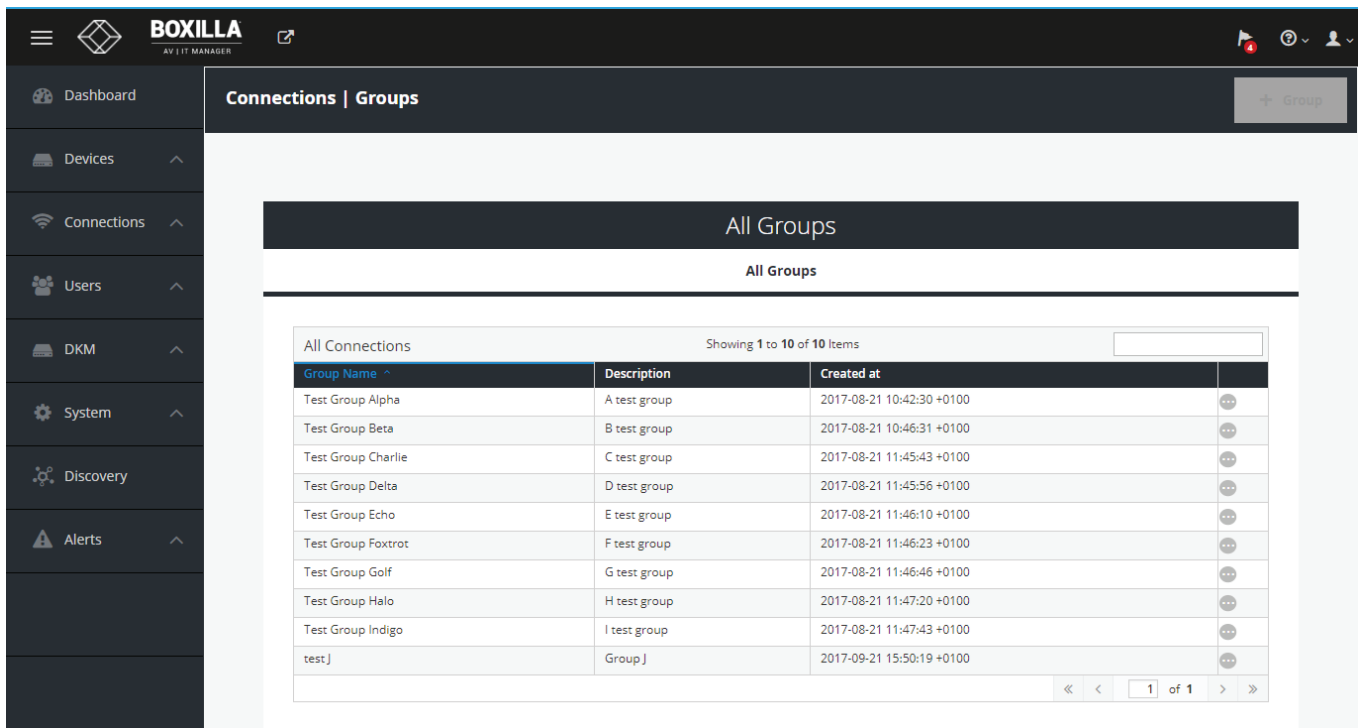

FIGURE 42. UPDATED CONNECTION GROUP SCREEN

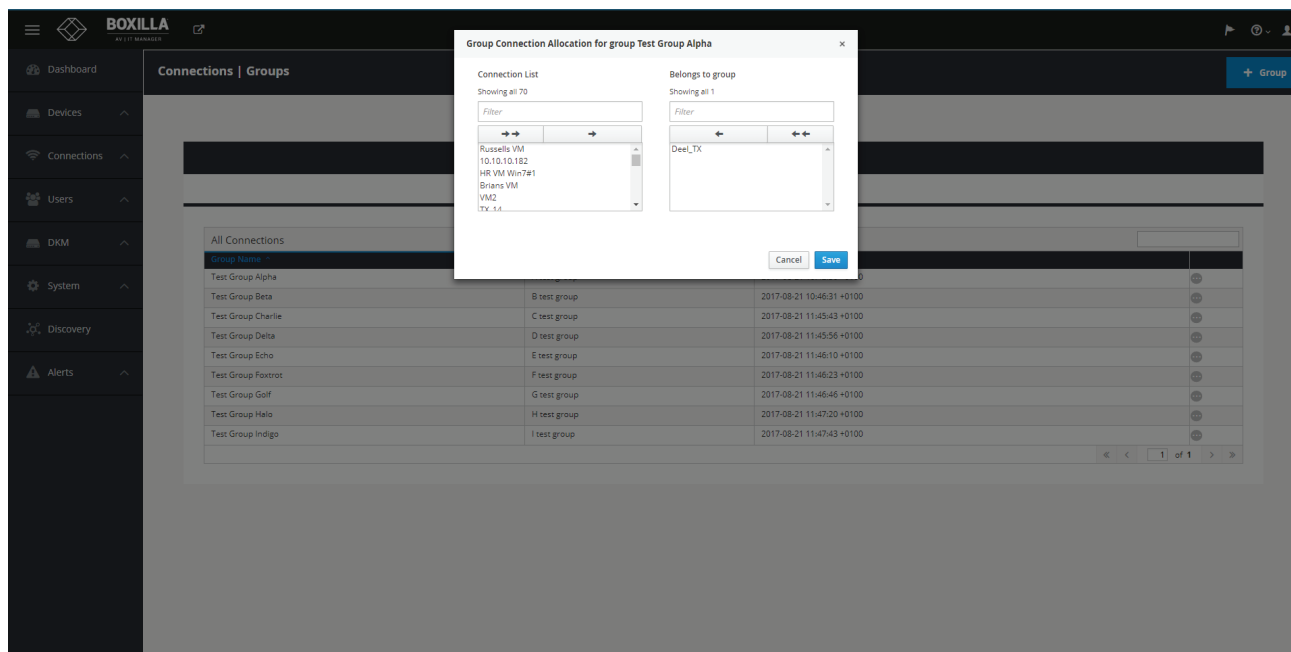You can manage connections by adding or removing connections to or from the connections group.

FIGURE 43. MANAGE CONNECTIONS SCREEN

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.
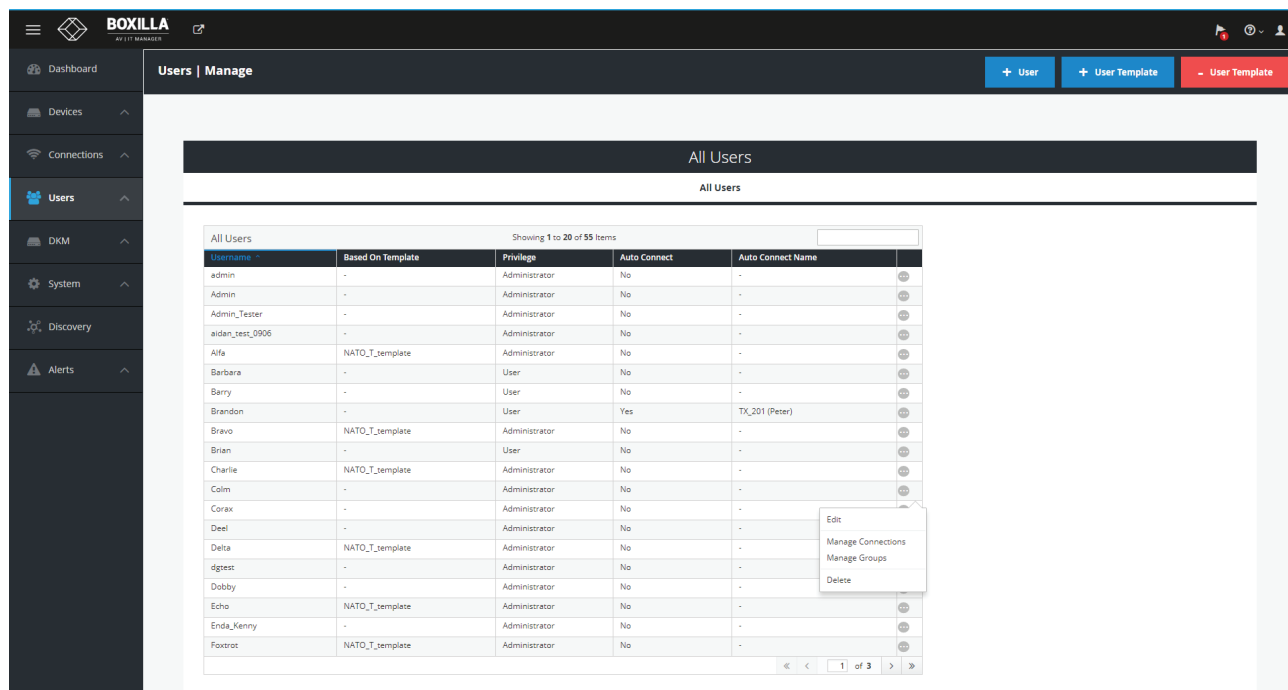
FIGURE 44. MANAGE USERS SCREEN

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

CHAPTER 8: CONNECTIONS

Active connections will be listed under Connections -> Active.
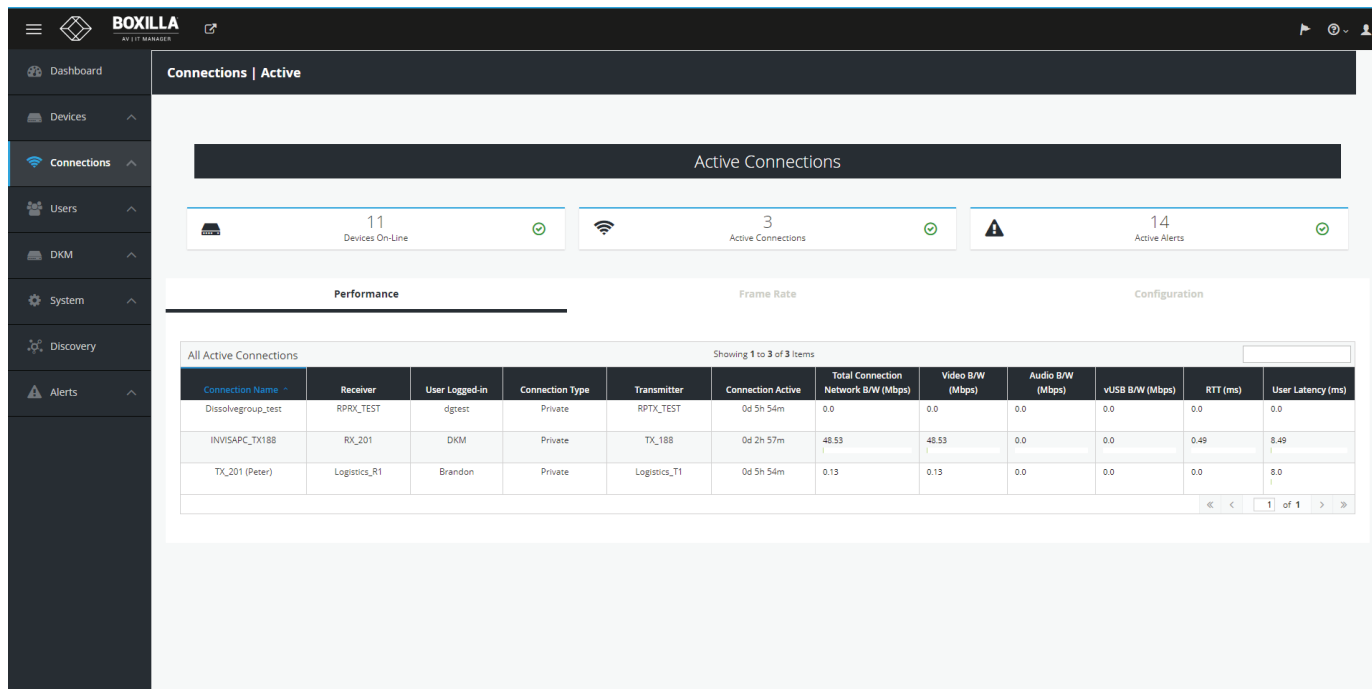
FIGURE 45. ACTIVE CONNECTIONS SCREEN

To dissolve a connection group (Map Connections from Connection Group to Individual Connections):
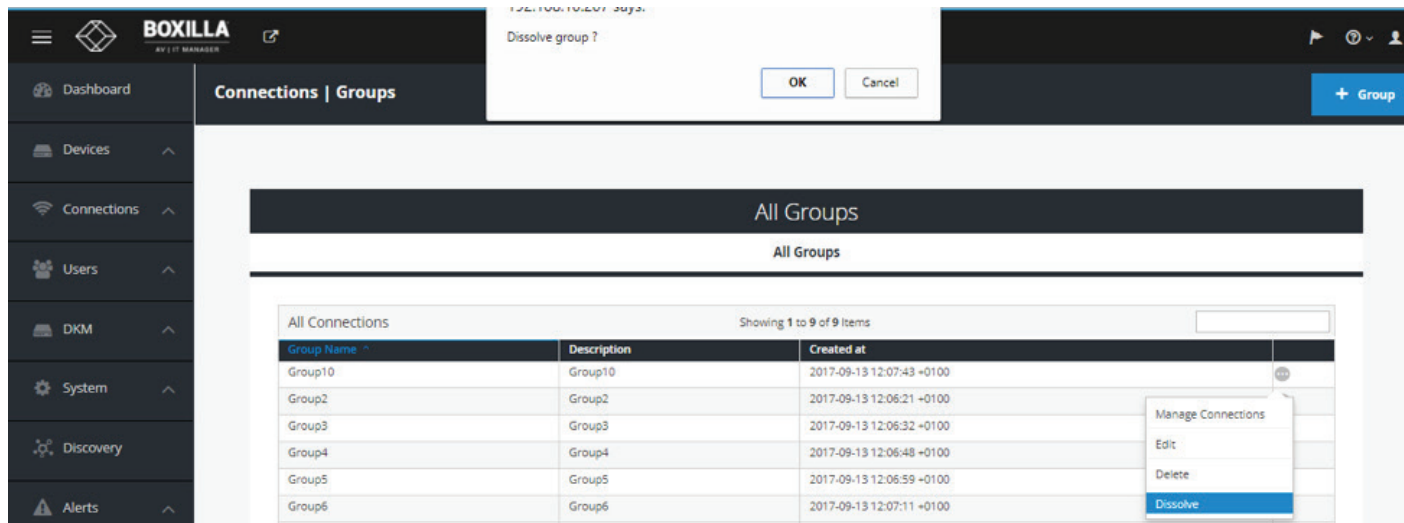

FIGURE 46. DISSOLVE CONNECTION GROUP SCREEN

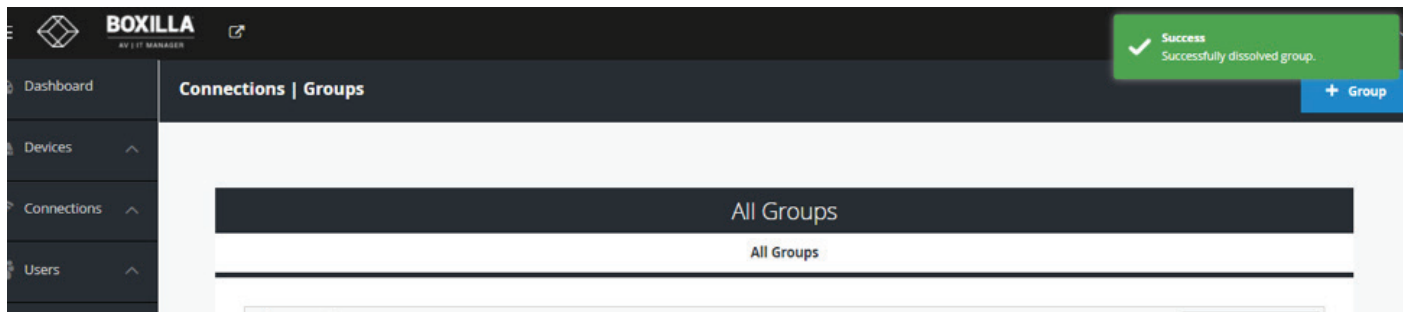Once you confirm with OK, a success message will be prompted.

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

CHAPTER 8: CONNECTIONS

FIGURE 47. SUCCESS MESSAGE

By dissolving a group, the group no longer appear 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.

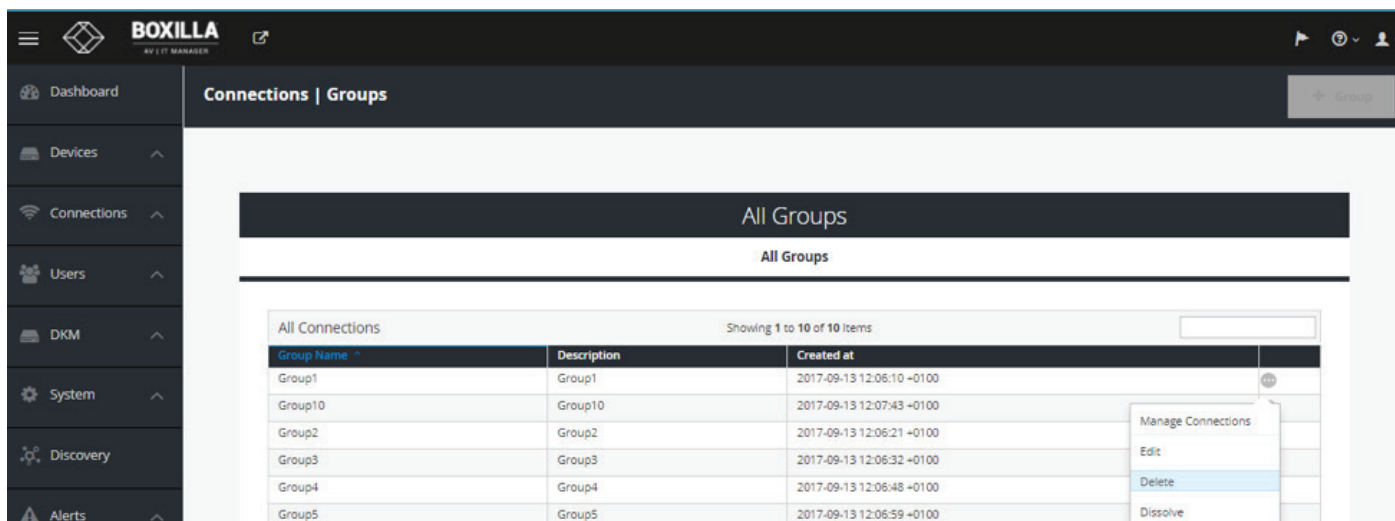Delete Connection Group: Delete the Connection Group and everywhere it is used.

FIGURE 48. DELETE THE CONNECTION GROUP

Confirm with OK and a confirmation message about deletion is displayed.

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269
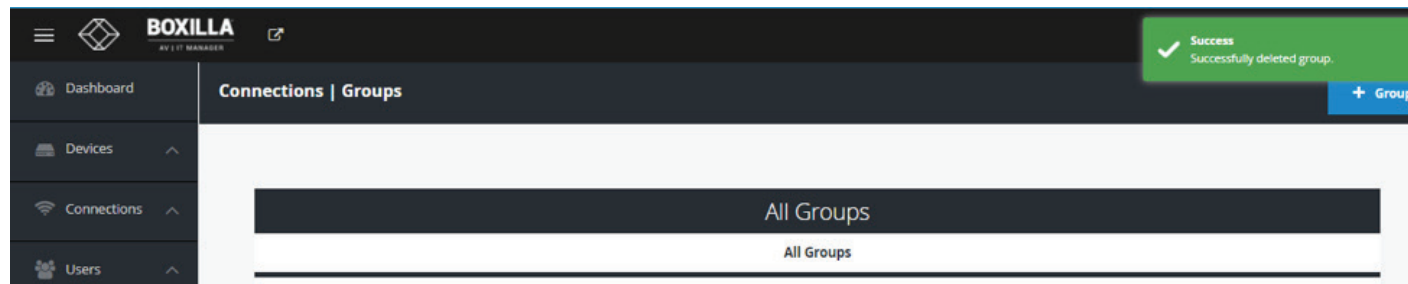
CHAPTER 8: CONNECTIONS

FIGURE 49. CONFIRM DELETION

The maximum number of connection groups is 10 and once it is reached, the add group button gets disabled.
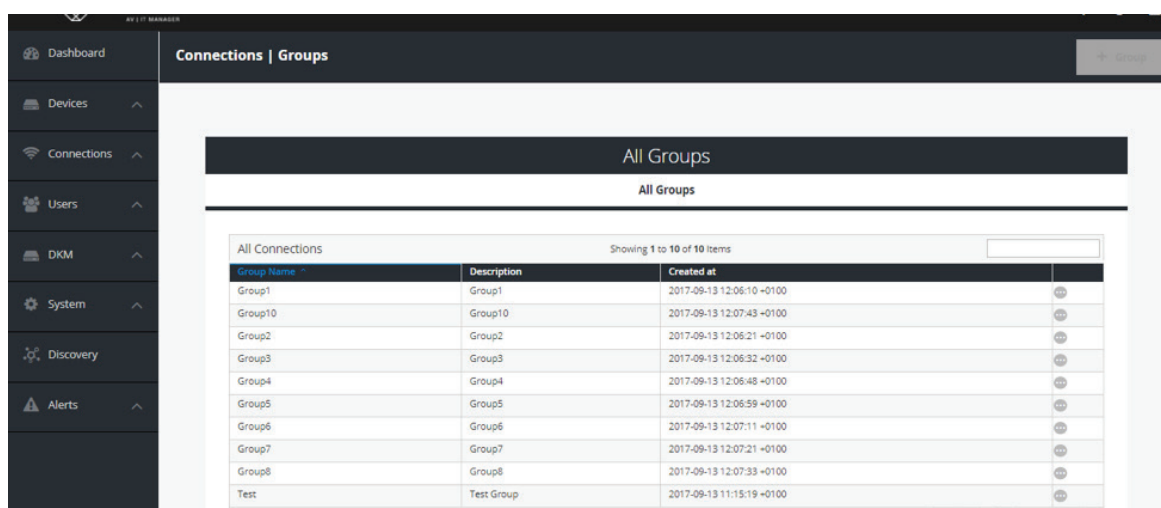

FIGURE 50. MAXIMUM NUMBER OF CONNECTION GROUPS

IMPORTANT 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

CHAPTER 8: CONNECTIONS

8.3 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: 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 time the connection has been made

- 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 as shown in Figure 51.
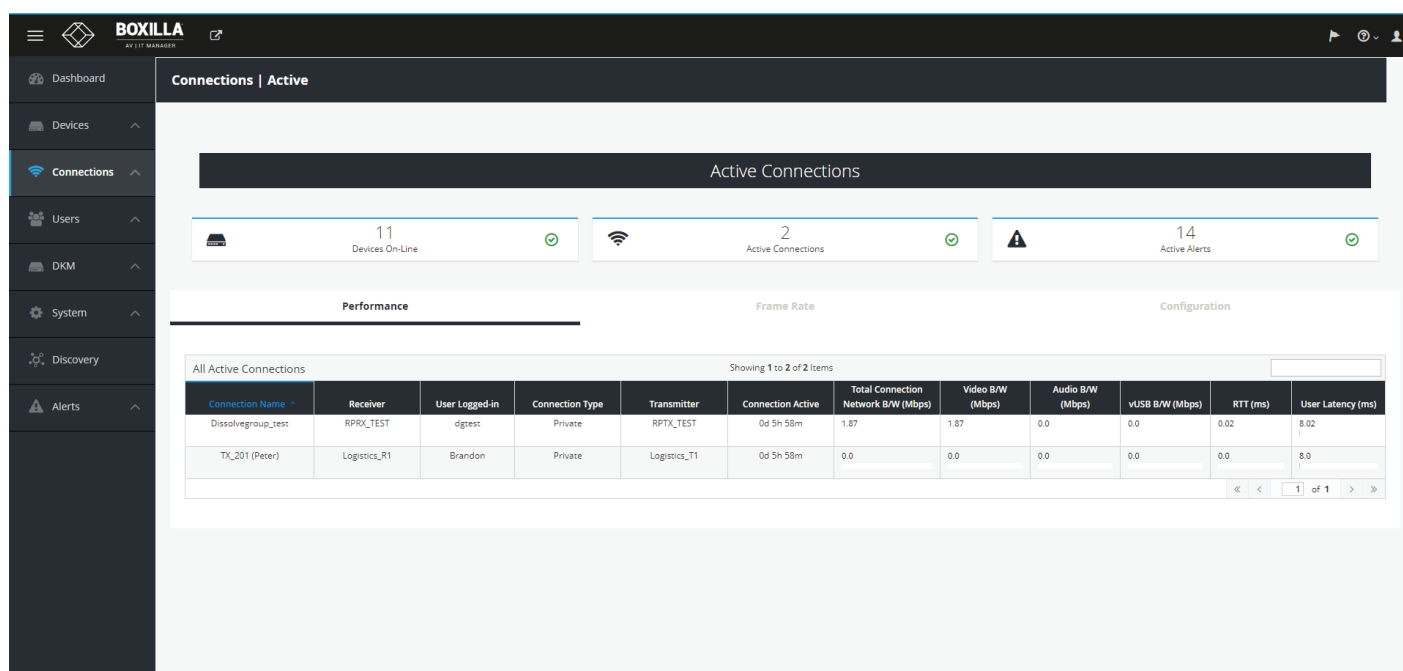

FIGURE 51. ACTIVE CONNECTIONS

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

CHAPTER 8: CONNECTIONS

8.4 CONNECTIONS—VIEWER

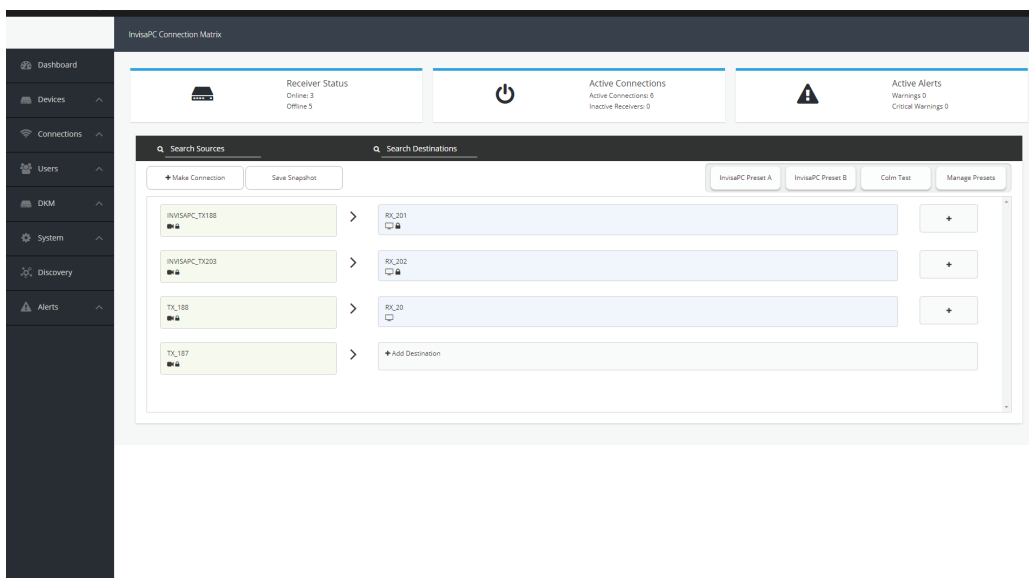On the Connections drop-down menu, click on Viewer. The Emerald or InvisaPC Connection Matrix screen appears.

FIGURE 52. CONNECTIONS—VIEWER SCREEN

8.4.1 MAKE CONNECTIONS

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

NOTE: It is only possible to connect InvisaPC Receivers to InvisaPC Transmitters and Emerald Receivers to Emerald Transmitters. Boxilla does not support connection interoperablity between Emerald and InvisaPC devices.
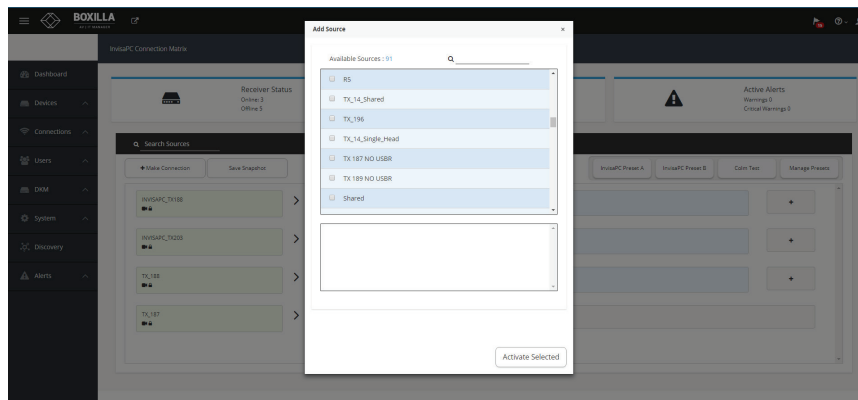

FIGURE 53. ADD SOURCE BUTTON

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."

CHAPTER 8: CONNECTIONS

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

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 54. CONNECTIONS—ADD DESTINATION TO A PRIVATE CONNECTION

8.4.2 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 Emerald or InvisaPC Viewer — Preset Manage, you can rearrange the preset priority to change what presets display on th main Viewer screen. Essentially, you can pick your top three presets.
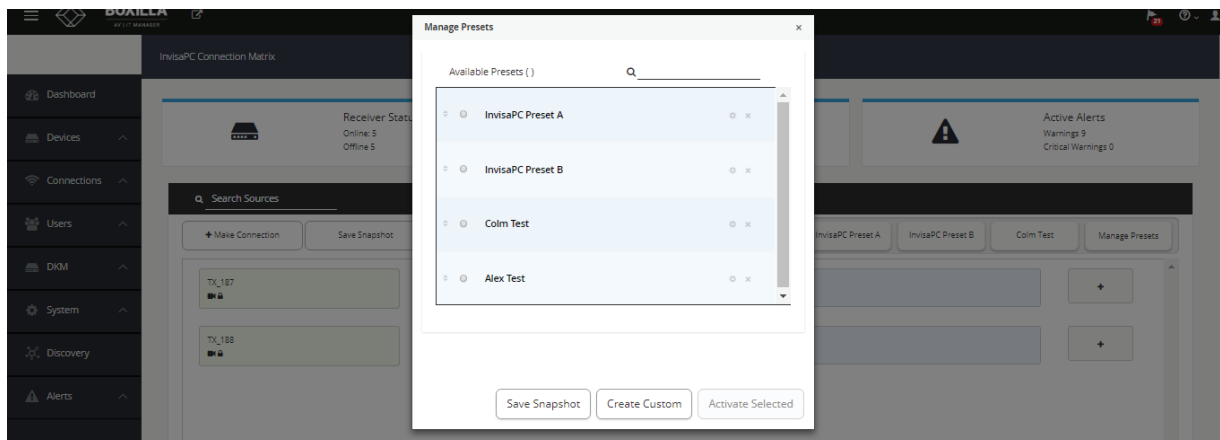

FIGURE 55. MANAGE PRESETS SCREEN

CHAPTER 8: CONNECTIONS

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

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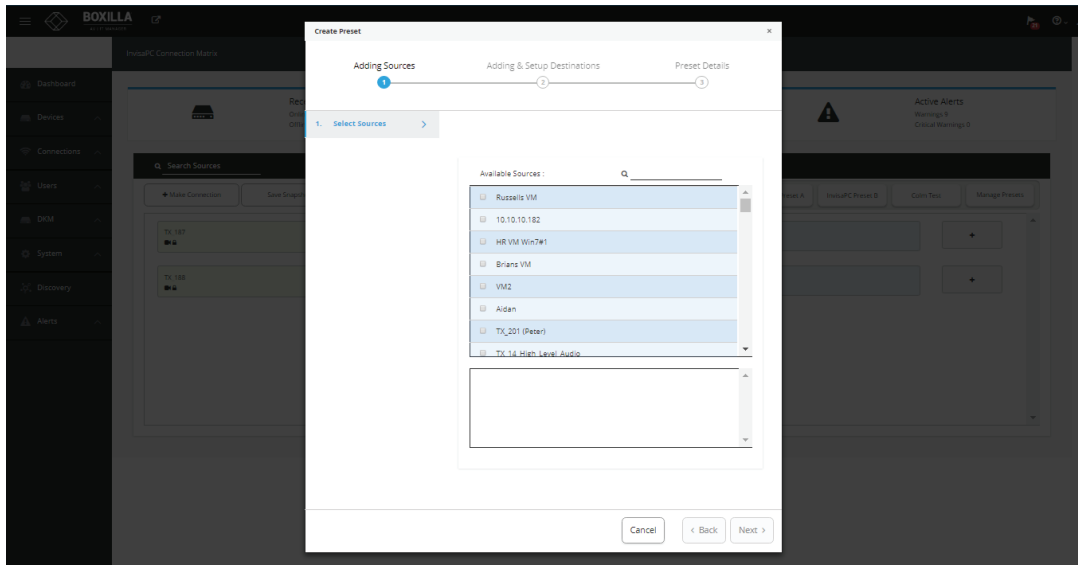

FIGURE 56. SELECT SOURCES SCREEN

Click next and select the destinations per source. Save the preset with a name and type (Partial or Full).

The icons on the sources screen are:

Icon	Meaning
	Source
	Destination
	View Only
	Shared Mode
	Private Mode

FIGURE 57. ICONS ON THE SOURCES SCREEN

CHAPTER 8: CONNECTIONS

NEED HELP?
LEAVE THE TECH TO US
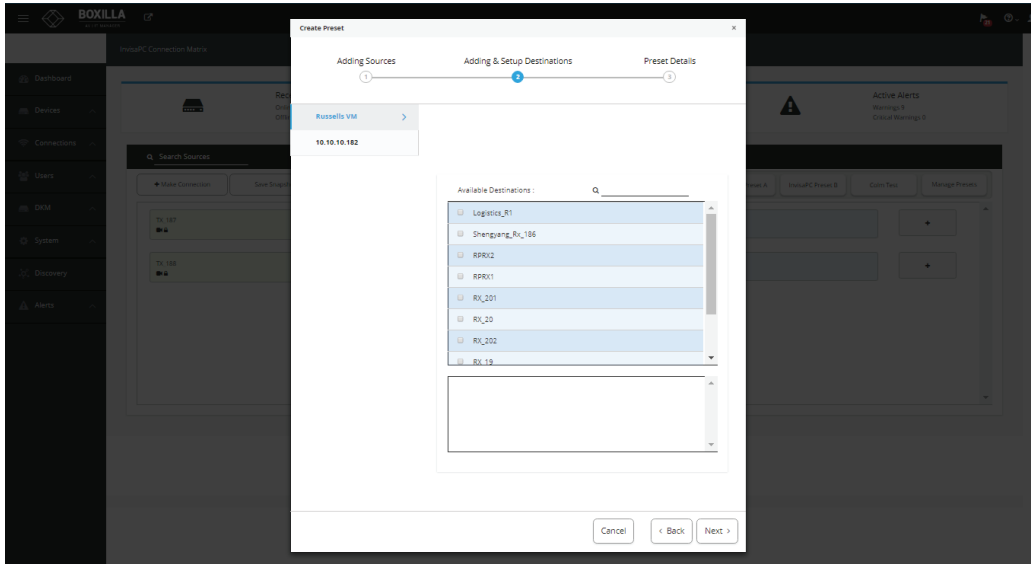
**LIVE 24/7
TECHNICAL
SUPPORT**
1.877.877.2269

FIGURE 58. SELECT DESTINATIONS SCREEN

The icons on the destination screen are:

Icon	Meaning
📹	Source
🖥	Destination
👁	View Only
⤳	Shared Mode
🔒	Private Mode

FIGURE 59. ICONS ON THE DESTINATIONS SCREEN

1.877.877.2269   BLACKBOX.COM

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

CHAPTER 8: CONNECTIONS

Both preset types will forcibly take any source and destinations required to establish their configuration, i.e., 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 the Tx/Vm and RX. Any Tx/Vm and RX not selected in this preset type will become inactive when this preset is launched.
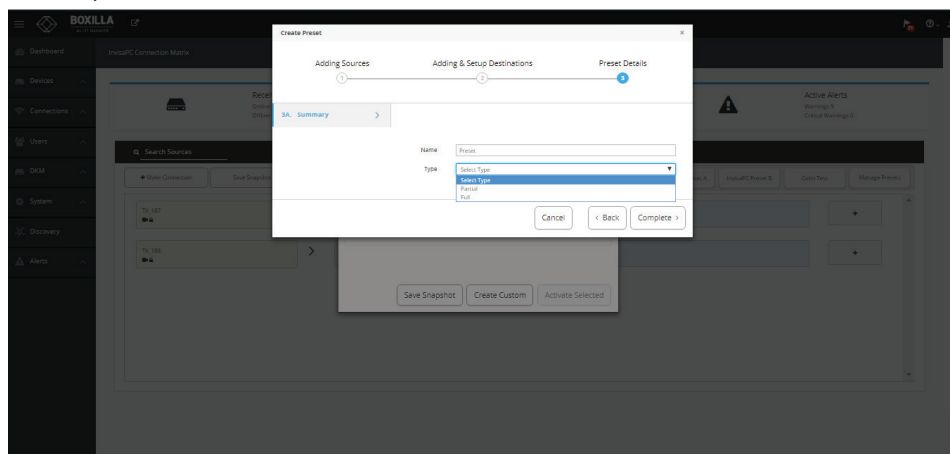
Click "Complete" to save the preset.

FIGURE 60. SAVE PRESET 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.

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

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

CHAPTER 9: USERS

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

9.1 USER TYPES

There are three types of users that can be created in an Emerald or InvisaPC system:

1. Administrator: Users of this class have full rights to configure the system. They can create/modify/delete users and connection, 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.

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

9.2 USER—MANAGE

The User—Manage screen is used to create, edit and delete users as shown in Figure 61. It provides a list of the currently created users.
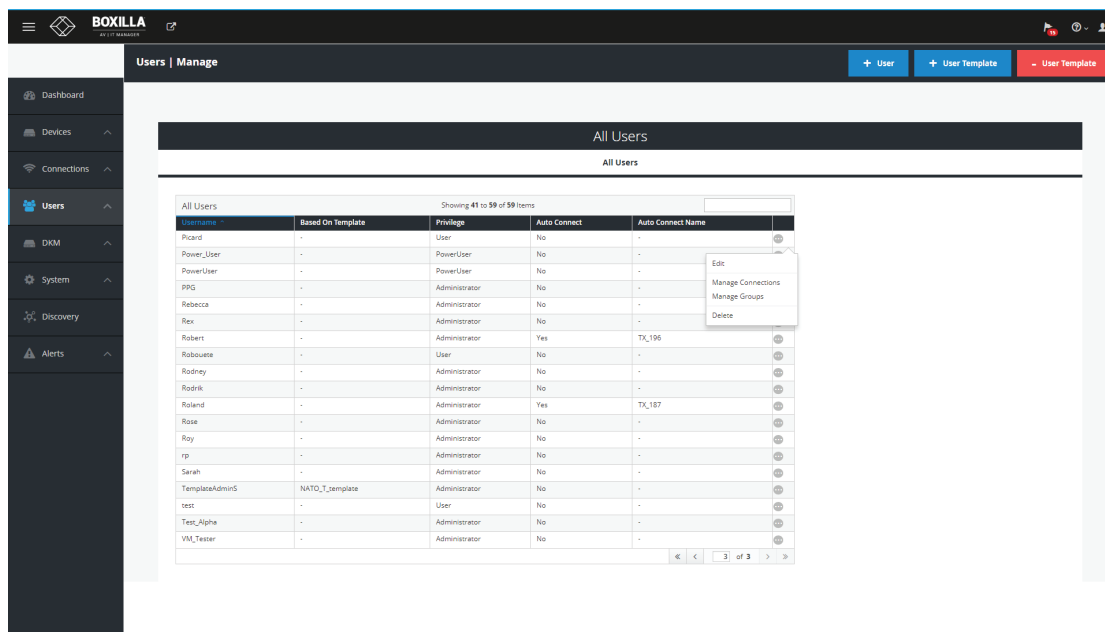

FIGURE 61. USERS—MANAGE

9.2.1 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 62.
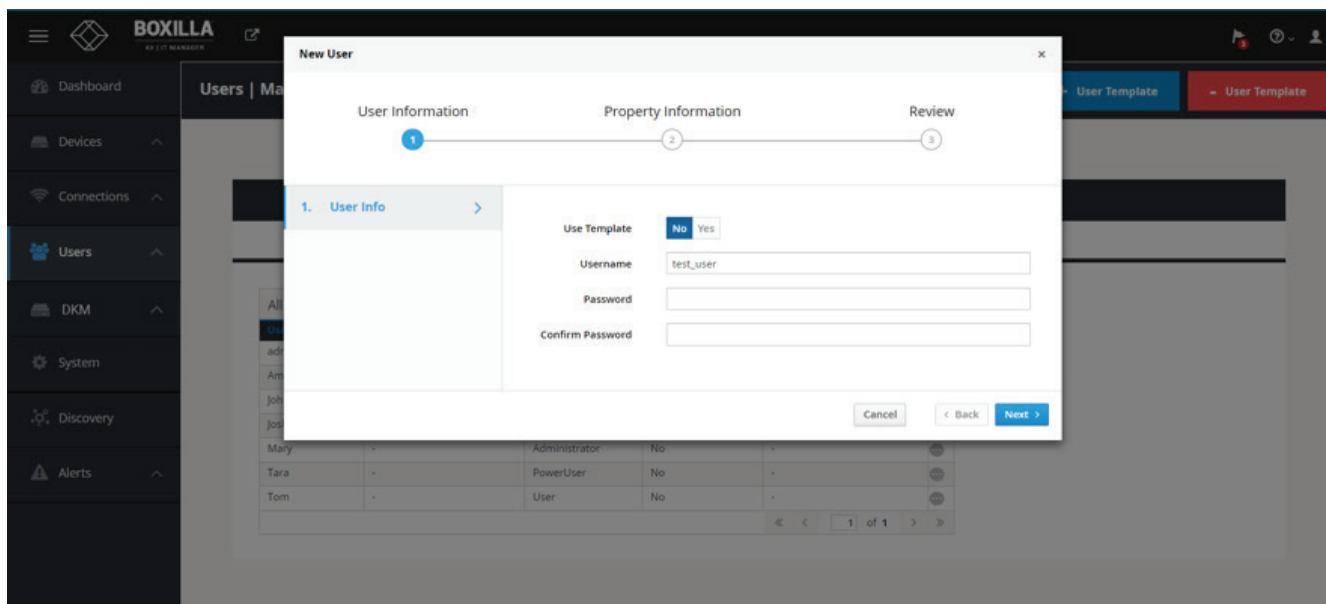

FIGURE 62. NEW USER WIZARD

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 " "/ \ [ ] : ; | = , + * ? < > `'.

* 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. This 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 Emerald or InvisaPC Receiver 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.

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.

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

9.2.2 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 "•••" 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 63. 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.
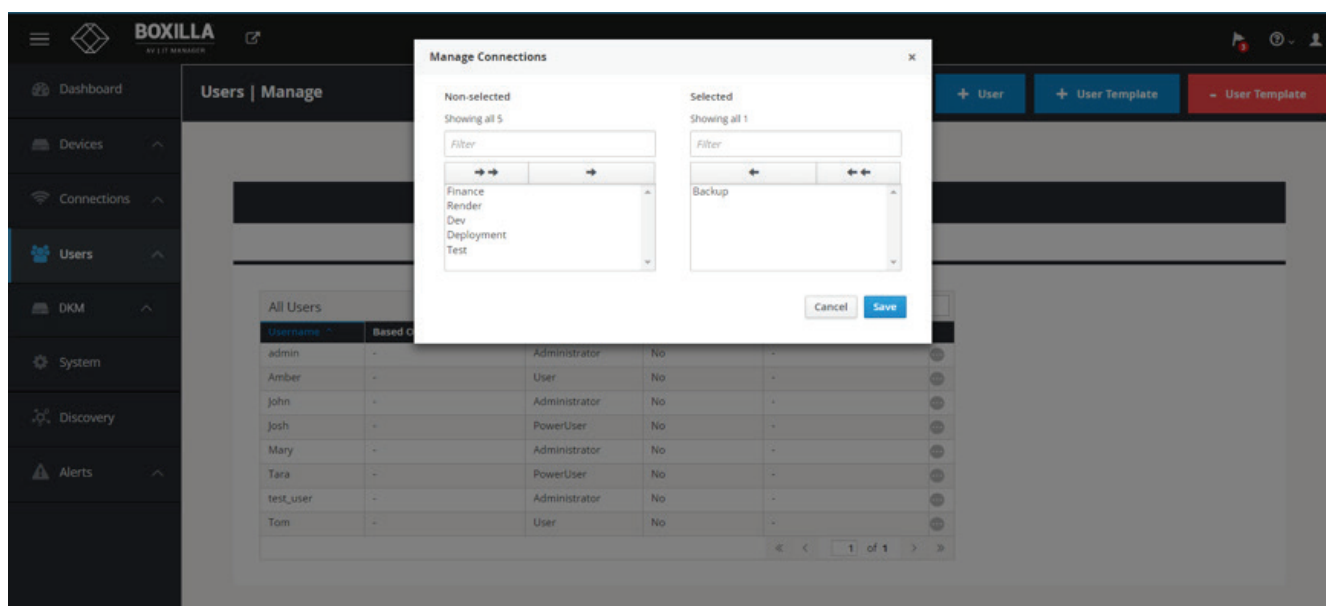

FIGURE 63. MANAGE USER CONNECTIONS

9.2.3 DELETE USER

To remove a user from the system, click on the "•••" icon on the row of the user to be deleted and click on the delete option.

9.3 USER—ACTIVE

The User—Active page shows a list of all the users logged in to an Emerald or InvisaPC Receiver. The page provides information on what Receiver the user is logged in on and details on any connective connection as shown in Figure 64.
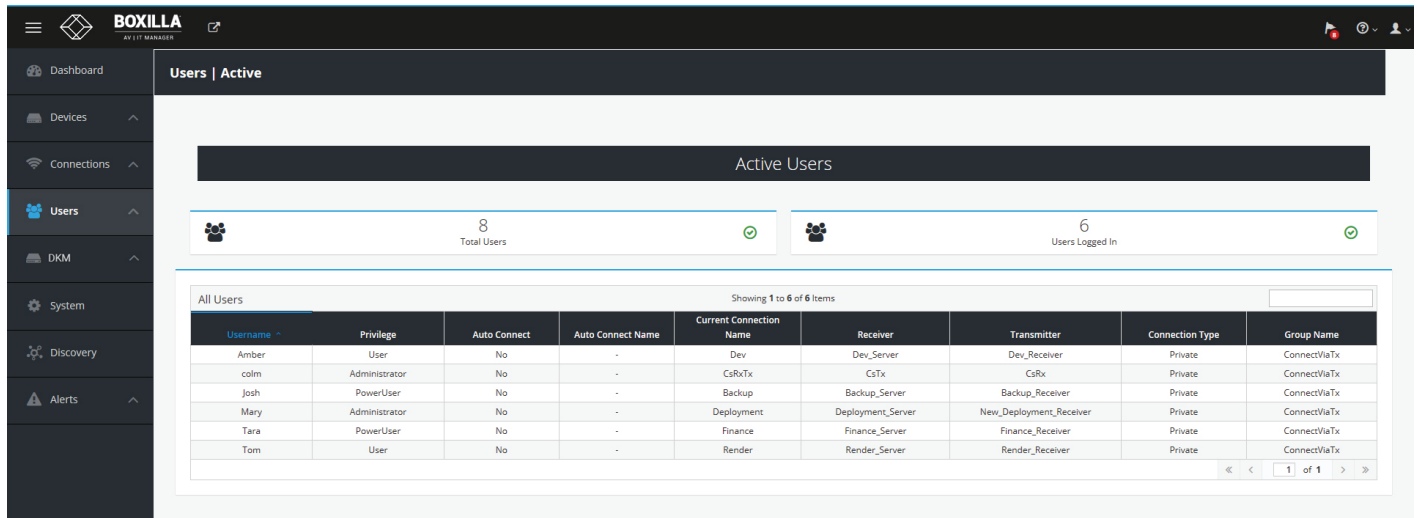

FIGURE 64. ACTIVE USERS

NEED HELP?
LEAVE THE TECH TO US
**LIVE 24/7
TECHNICAL
SUPPORT**
1.877.877.2269

CHAPTER 9: USERS

9.4 MANAGE GROUPS

You can add/manage groups from individual Users under Users -> Manage. Once the users are mapped under a group, all the connections and users associated to the group will get listed at the appliance's GUI. See the screens below and on the next page.

FIGURE 65. MANAGE GROUPS

FIGURE 66. USER GROUP ALLOCATION SCREEN

NEED HELP?
LEAVE THE TECH TO US

LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

CHAPTER 10: DKM INTEGRATION

10.1 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 InvisaPC appliances by means of Virtual CPUs. The VirtualCPU name must match the InvisaPC 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 Boxilla will initiate the desired connections between the InvisaPC Receiver and the InvisaPC Transmitter/VM.

Follow these steps:

1. Create desired InvisaPC Connection.

2. Add a DKM Switch under Boxilla -> DKM -> Switches.

3. Create a Virtual CPU on the DKM JavaTool (named the same name as the InvisaPC Connection). Physically attach this to the InvisaPC Receiver. When the DKM CON is then connected to the VirtualCPU, the connection name will be picked up and the InvisaPC leg of the connection will be set up.

10.2 STEPS TO CREATE AND MANAGE VCPU CONNECTIONS ON THE UTILITY

Assumed: You have the desired InvisaPC connection setup.

Open the Java Tool and select "Activate Online Configuration," which is the 6th button in from the left in DKM FX Tool 3.4.3.0.81. Select Yes when you are asked to confirm. NOTE: The screen you see depends on the version of the DKM Java Tool used.
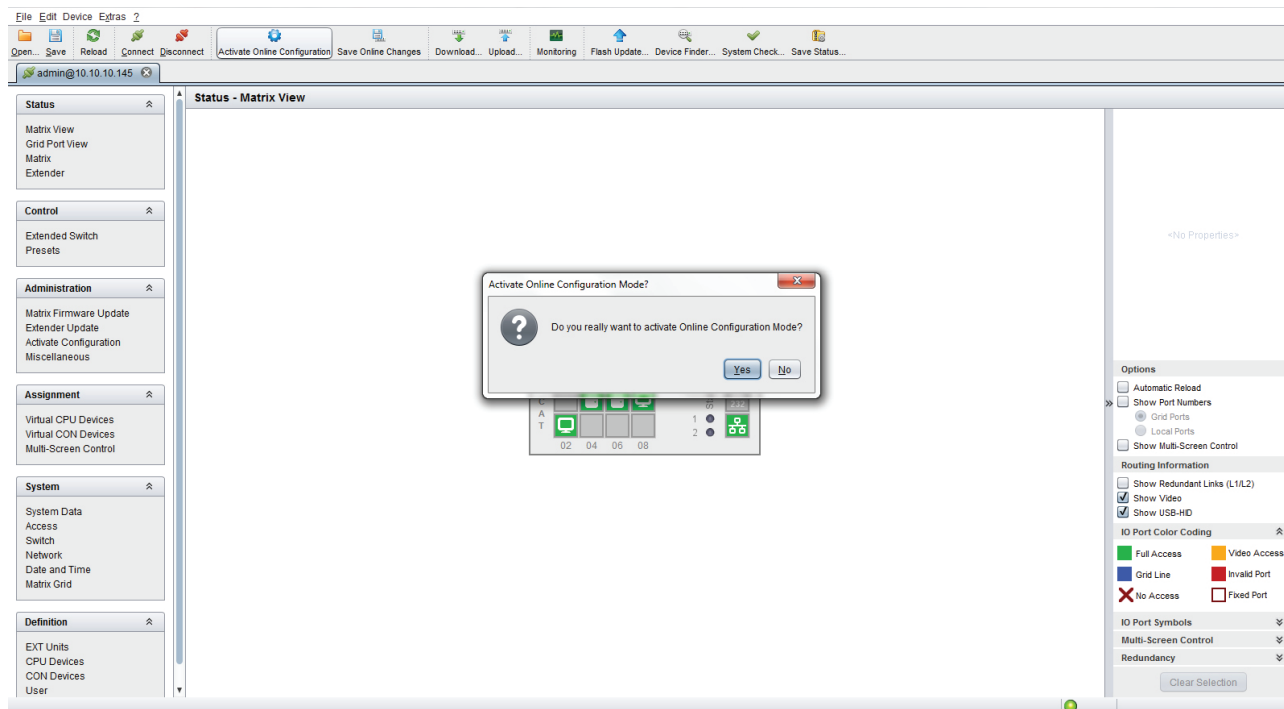
FIGURE 67. JAVA TOOL SCREEN

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."

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

CHAPTER 10: DKM INTEGRATION

FIGURE 68. 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 InvisaPC Connection name that you want it to be associated with.
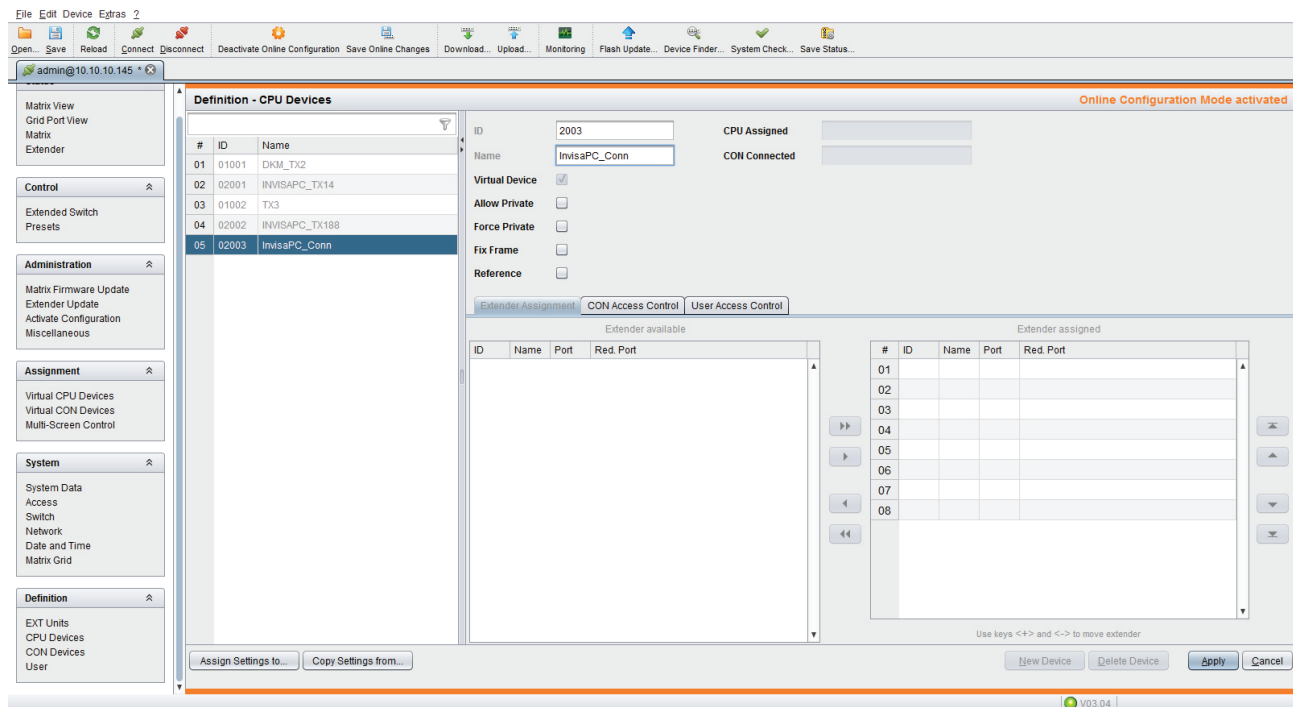
FIGURE 69. NAME VIRTUAL CPU SCREEN

Press "Apply."

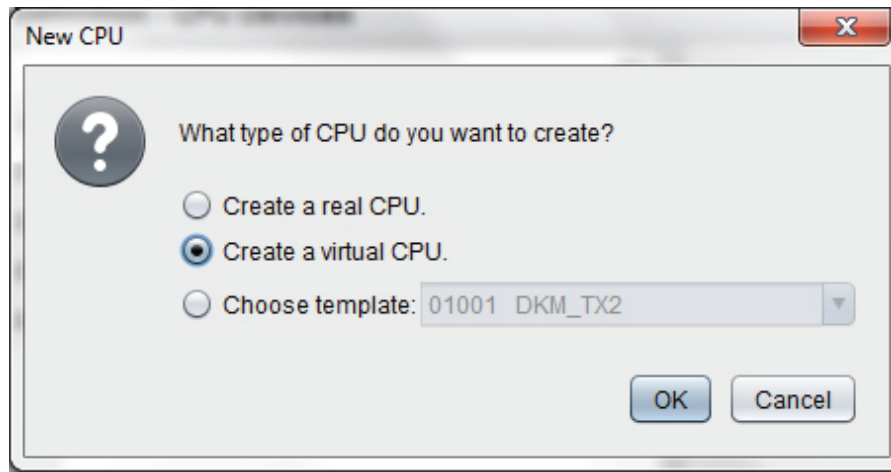Next, navigate to "Virtual CPU Devices," which appears under the "Assignment" tab on the main menu on the left side of the application window. Here you can assign your new Virtual CPU to the real CPU that's physically connected into your InvisaPC receiver. This is done by clicking the empty space in the "Name" column and seeing the drop down of available Real CPUs.
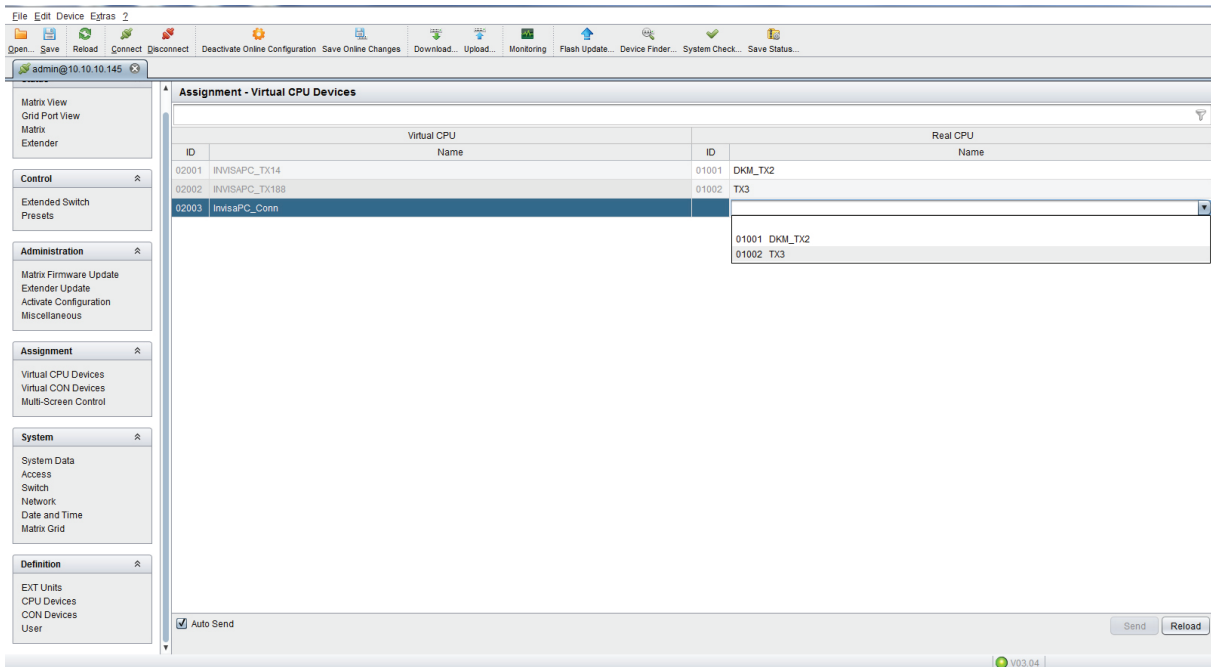
FIGURE 70. DROP DOWN LIST OF AVAILABLE REAL CPUS

CHAPTER 10: DKM INTEGRATION

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

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.

FIGURE 71. SAVED CHANGES

NEED HELP?
LEAVE THE TECH TO US

LIVE 24/7
TECHNICAL
SUPPORT

1.877.877.2269
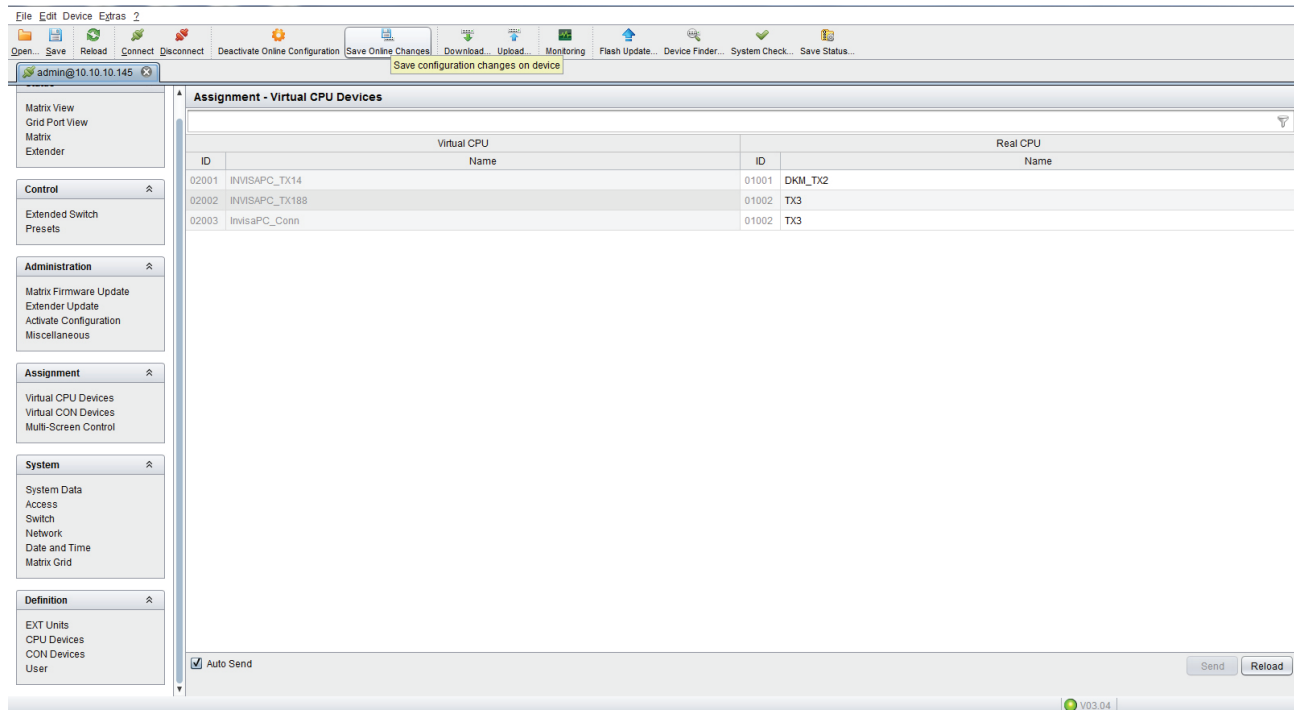
HOW TO ENABLE LAN ECHO

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 InvisaPC Connections.

FIGURE 72. ENABLE LAN ECHO

10.3 STEPS TO ADD SWITCHES

Under Boxilla, to add the DKM switch, navigate to DKM —Switches and click the "Add Switch" blue button on the top right of the screen.
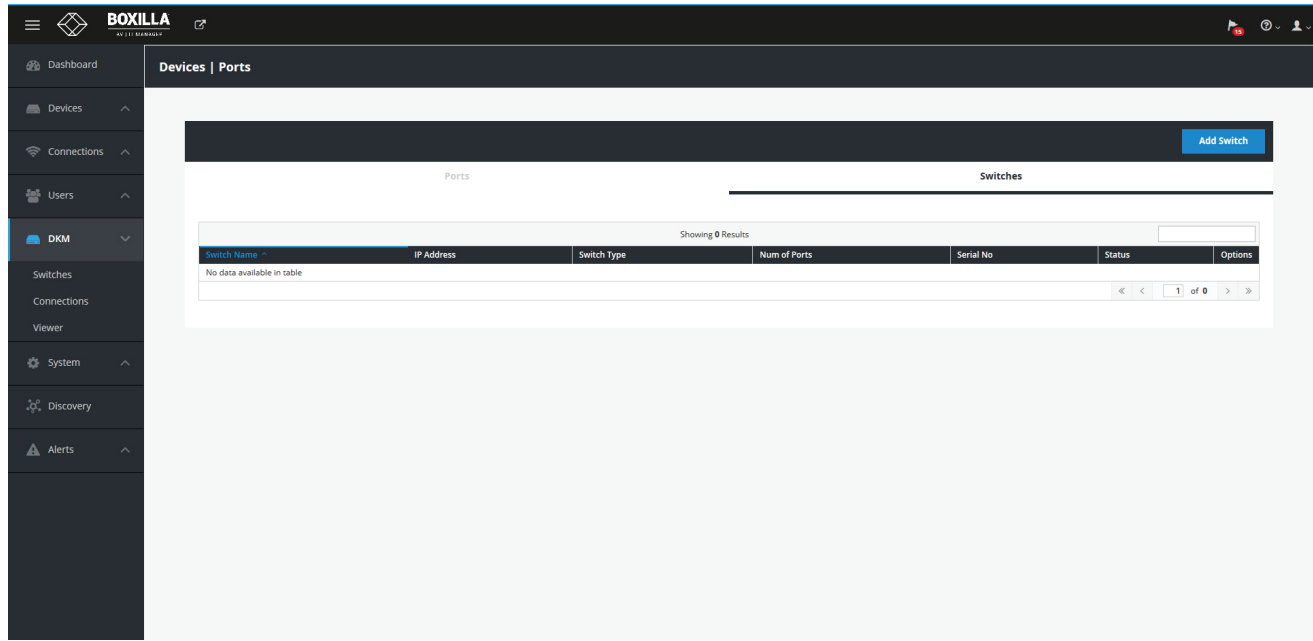
FIGURE 73. ADD SWITCH SCREEN

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 74. ADD NEW SWITCH BOX

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269
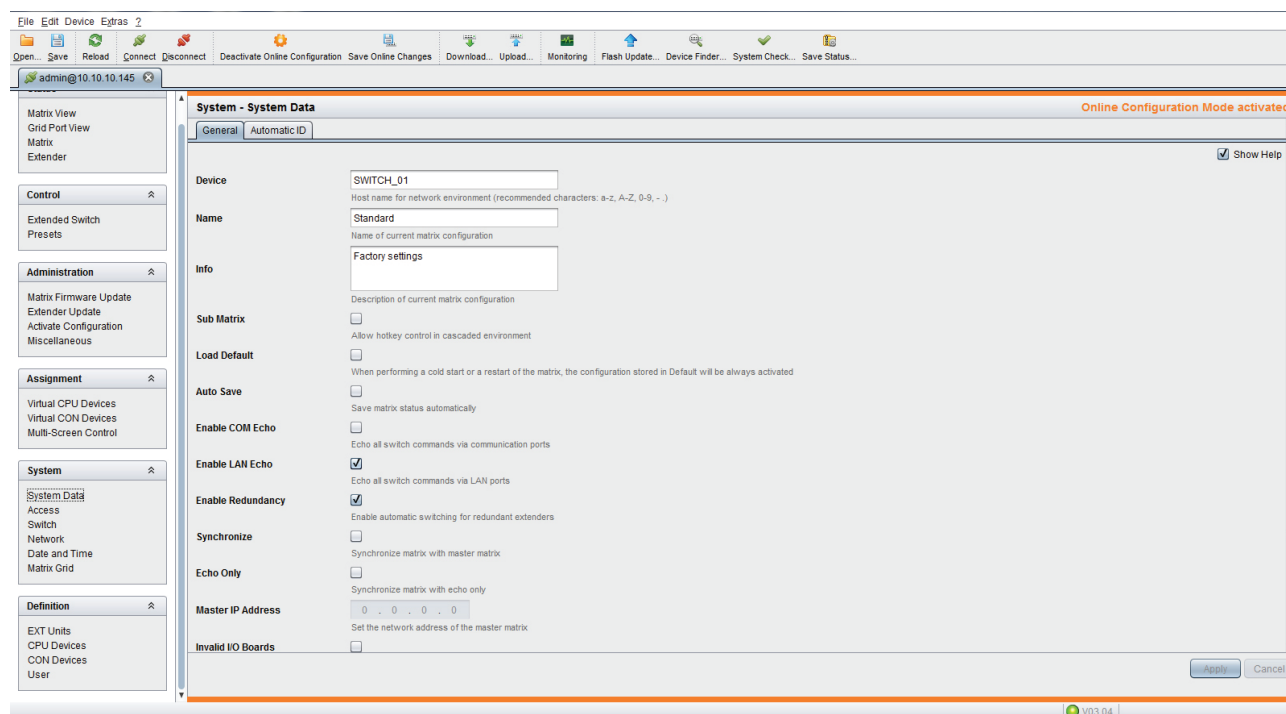
CHAPTER 10: DKM INTEGRATION

Once the switch is added successfully, it gets listed with an online status.
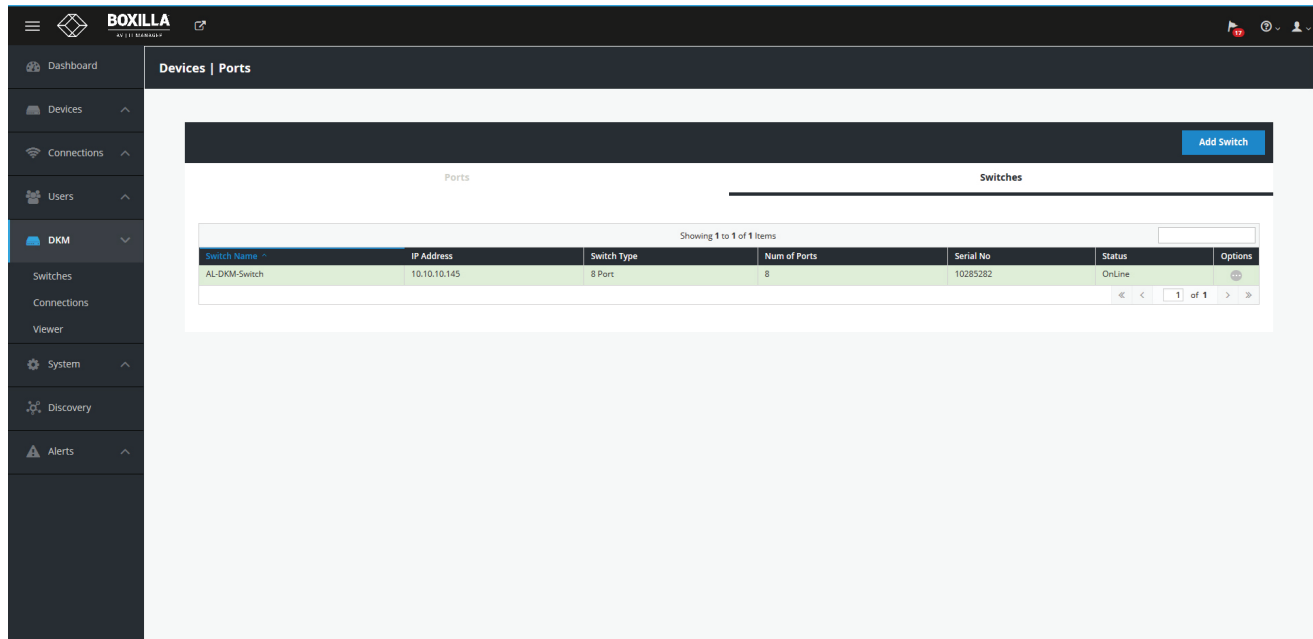
FIGURE 75. ONLINE STATUS OF SWITCH

If you wish to revert, select Delete from the dropdown list within options to delete the switch entry.
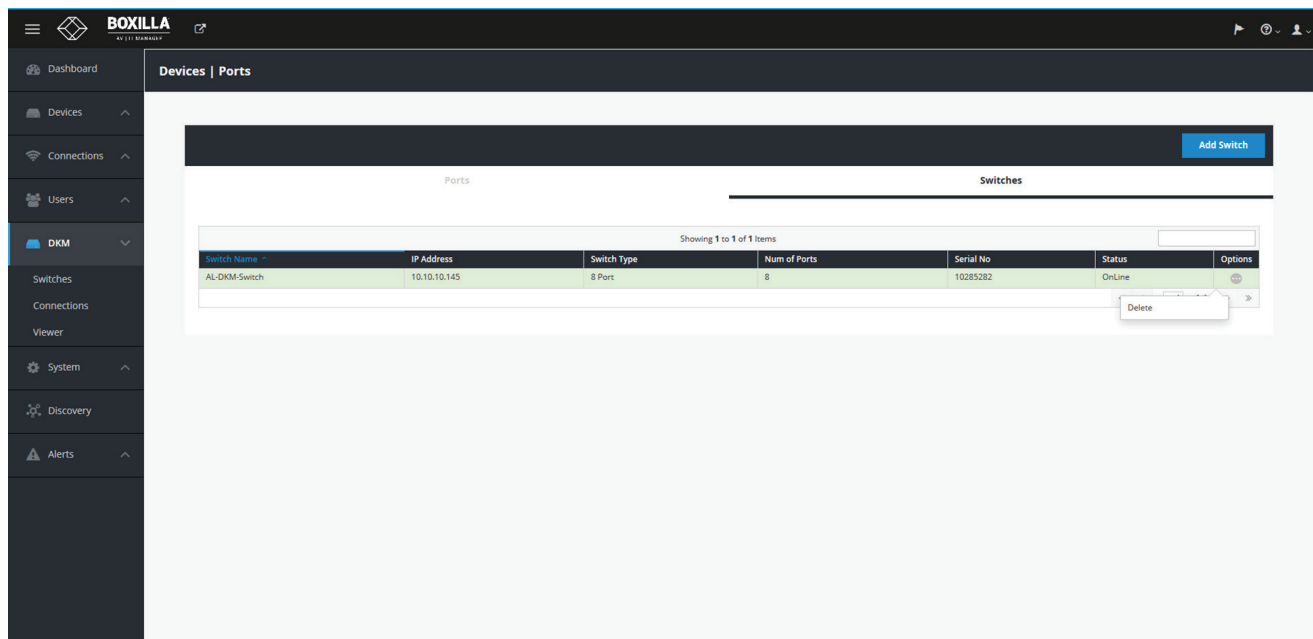
FIGURE 76. DELETE THE SWITCH ENTRY

You can search for a switch by entering the switch name into quick search box at the right corner.

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

CHAPTER 10: DKM INTEGRATION
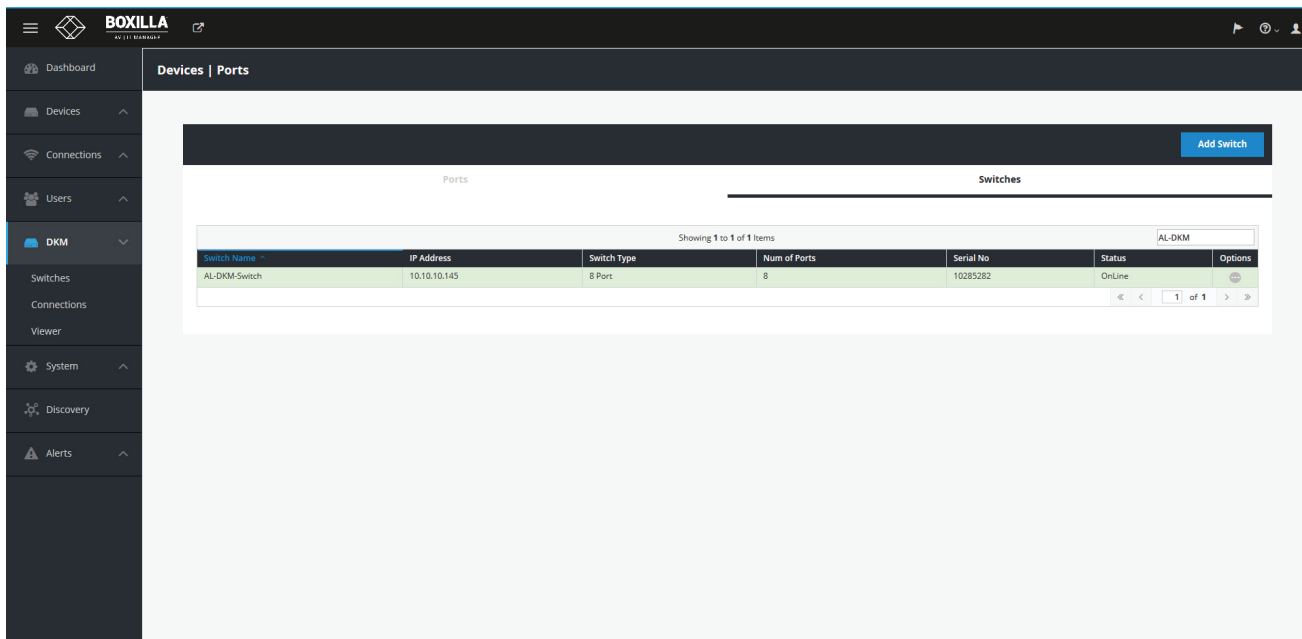
FIGURE 77. SEARCH FOR A SWITCH

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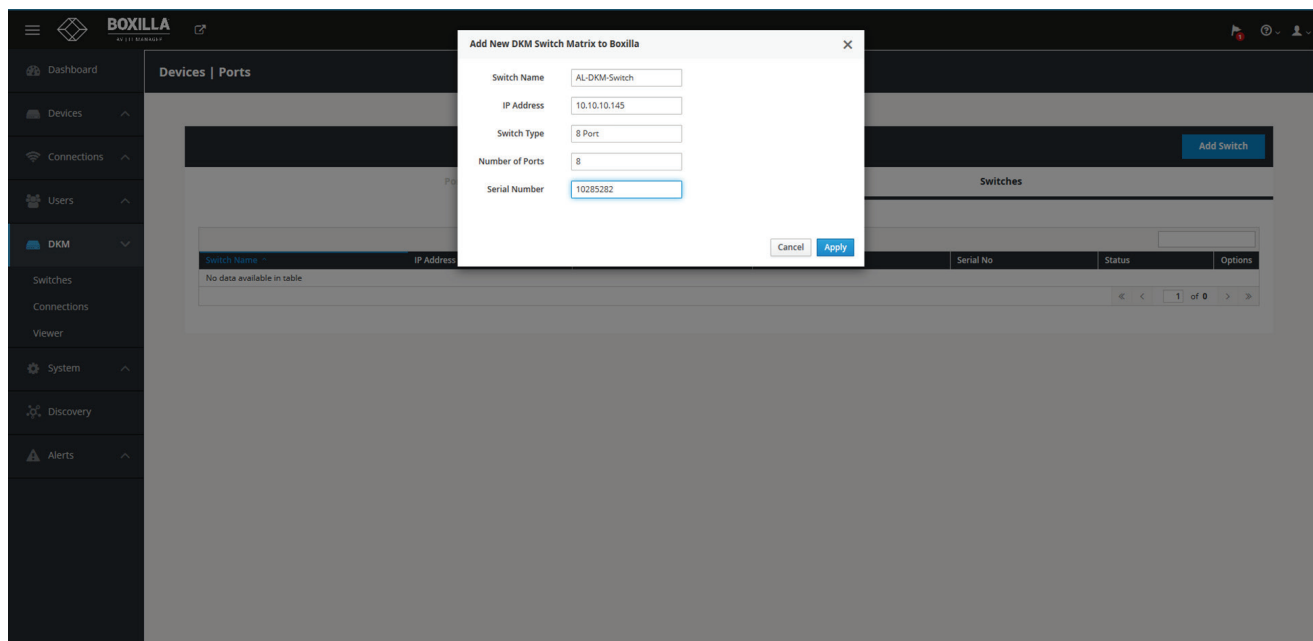ed on the DKM switch will be listed. Boxilla will automatically update with any new DKM CONs, DKM CPUs and Virtual CPUs that may be added in the future. Follow the next steps to create a new connection.

The DKM Ports Table displays ports based on the DKM switch that has been added.
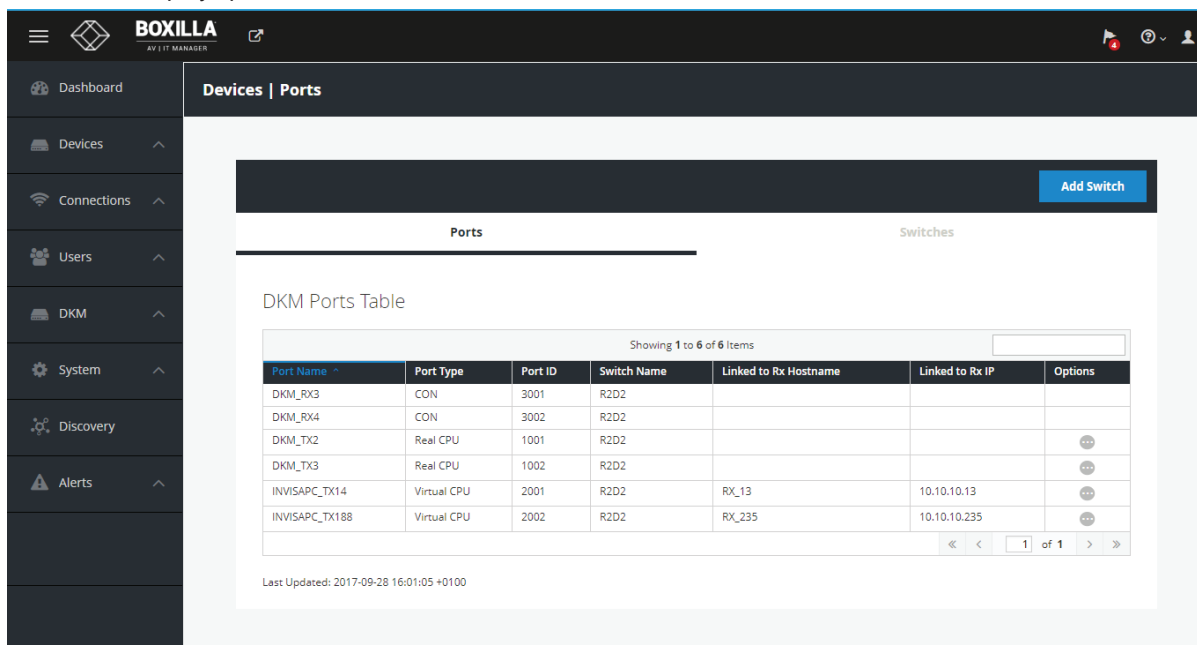
FIGURE 78. DKM PORTS TABLE

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

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

CHAPTER 10: DKM INTEGRATION

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 InvisaPC Connection."

NOTE: It is not possible to attach to an Emerald connection.
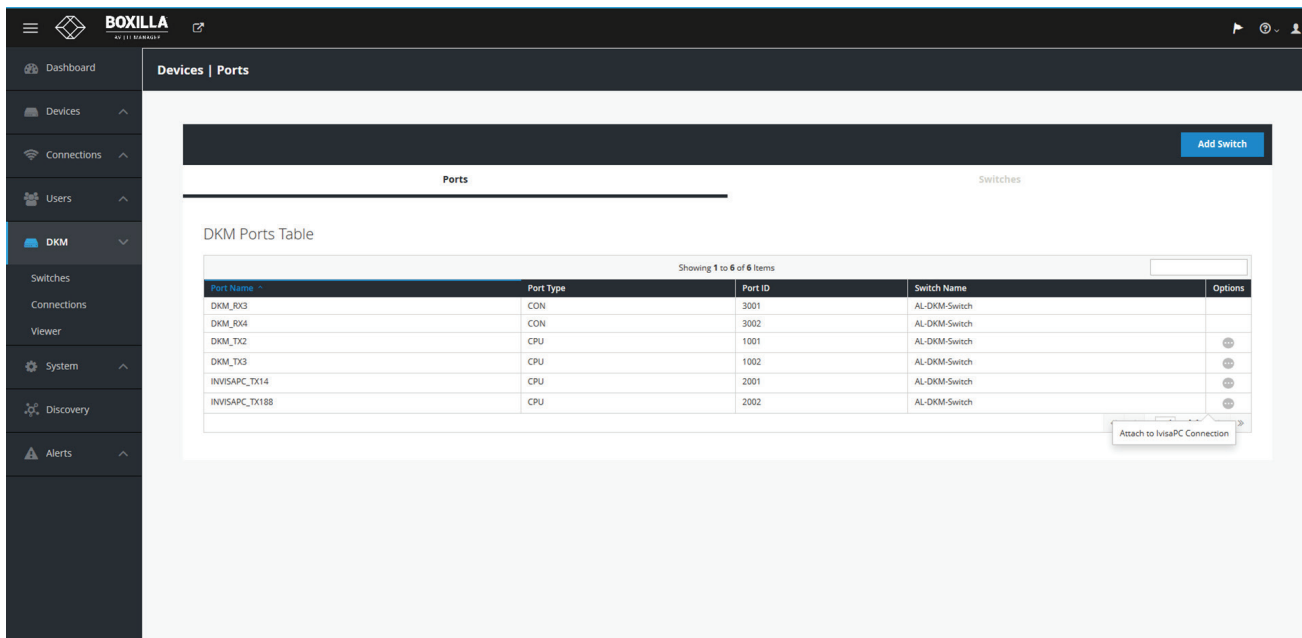
FIGURE 79. ATTACH TO INVISAPC CONNECTION

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

FIGURE 80. PORT ID SCREEN

CHAPTER 10: DKM INTEGRATION

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

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.
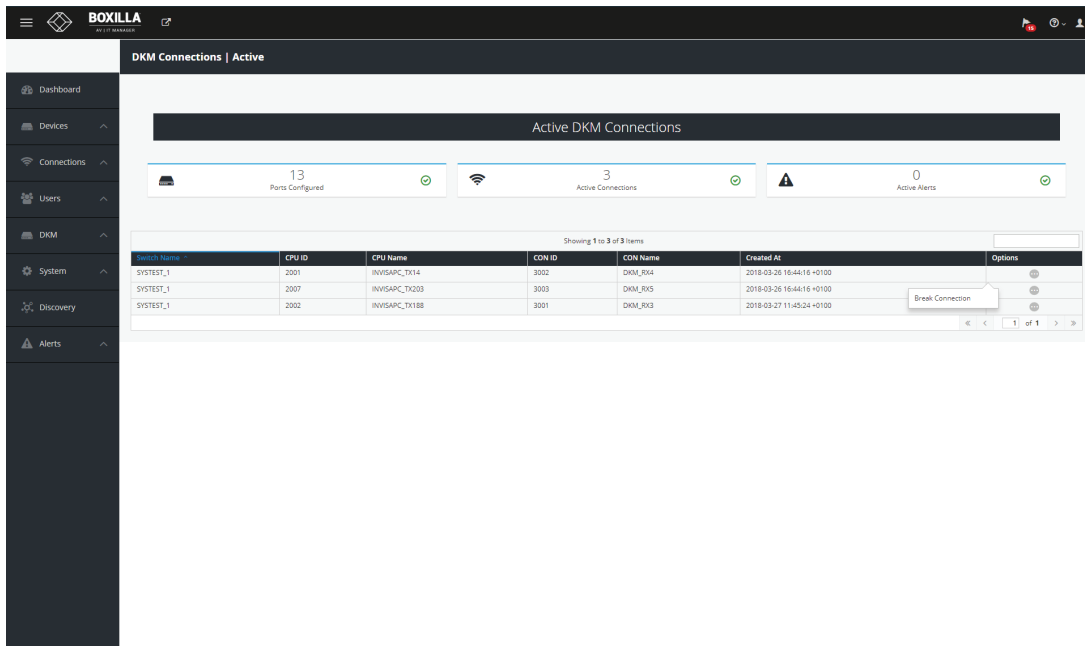
FIGURE 81. DETACH CONNECTION SCREEN

NEED HELP?
LEAVE THE TECH TO US

LIVE 24/7
TECHNICAL
SUPPORT

1.877.877.2269

10.4 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.
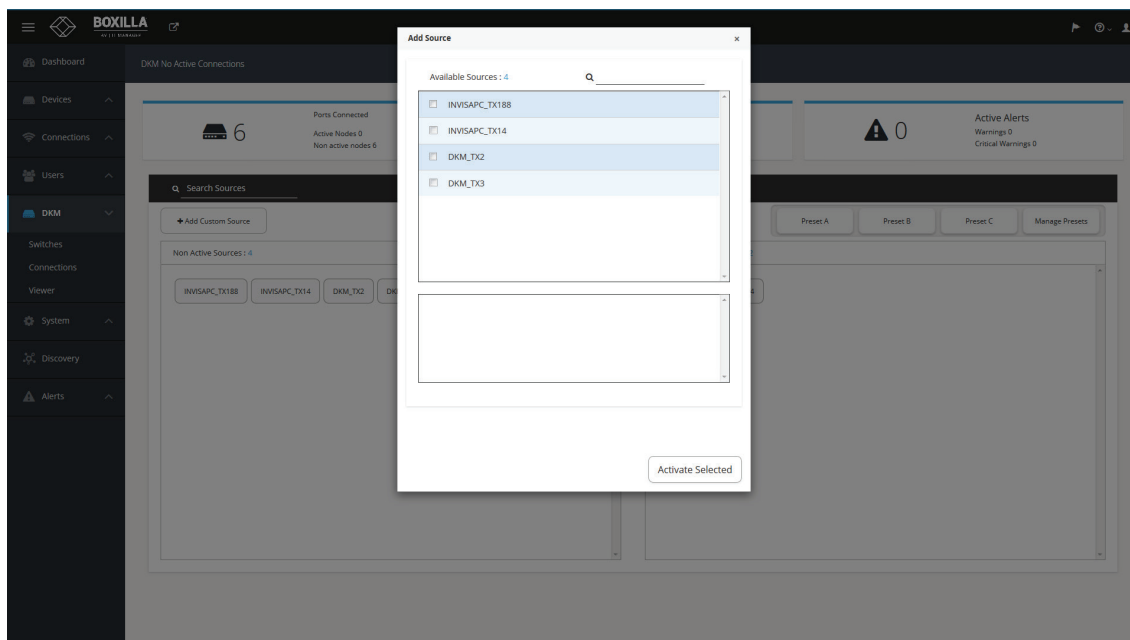
FIGURE 82. ADD CUSTOM SOURCE SCREEN

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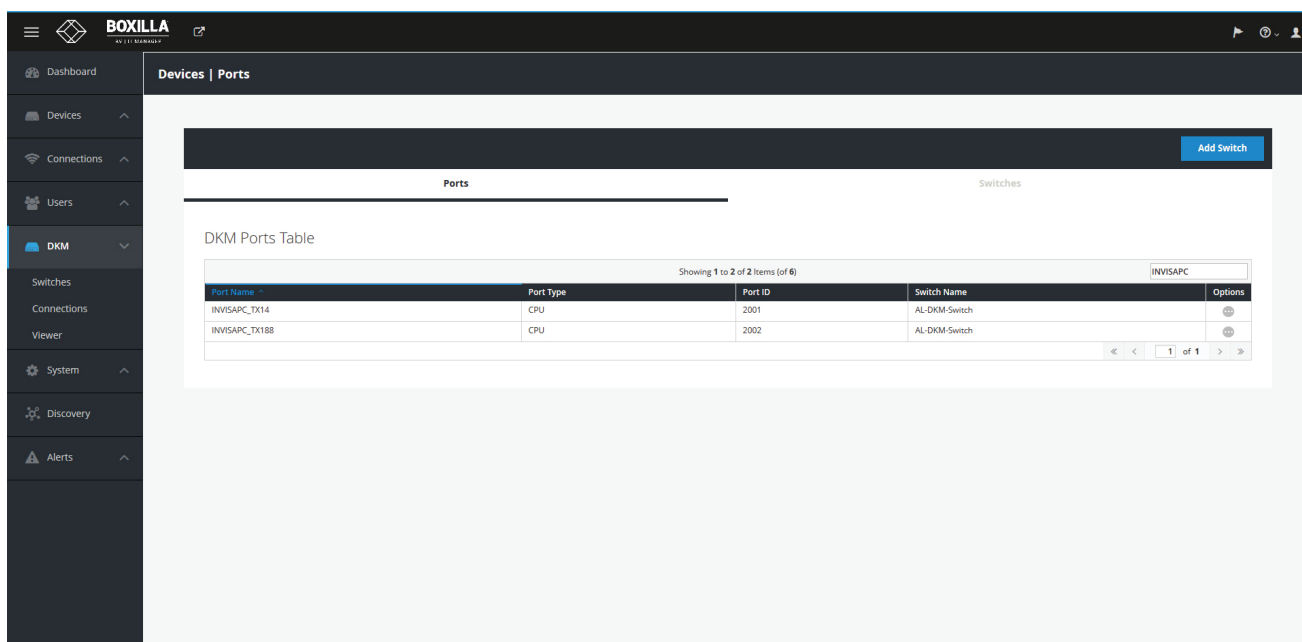
2. Detach Destination: Break the connection by detaching the destination.

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."

CHAPTER 10: DKM INTEGRATION

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269
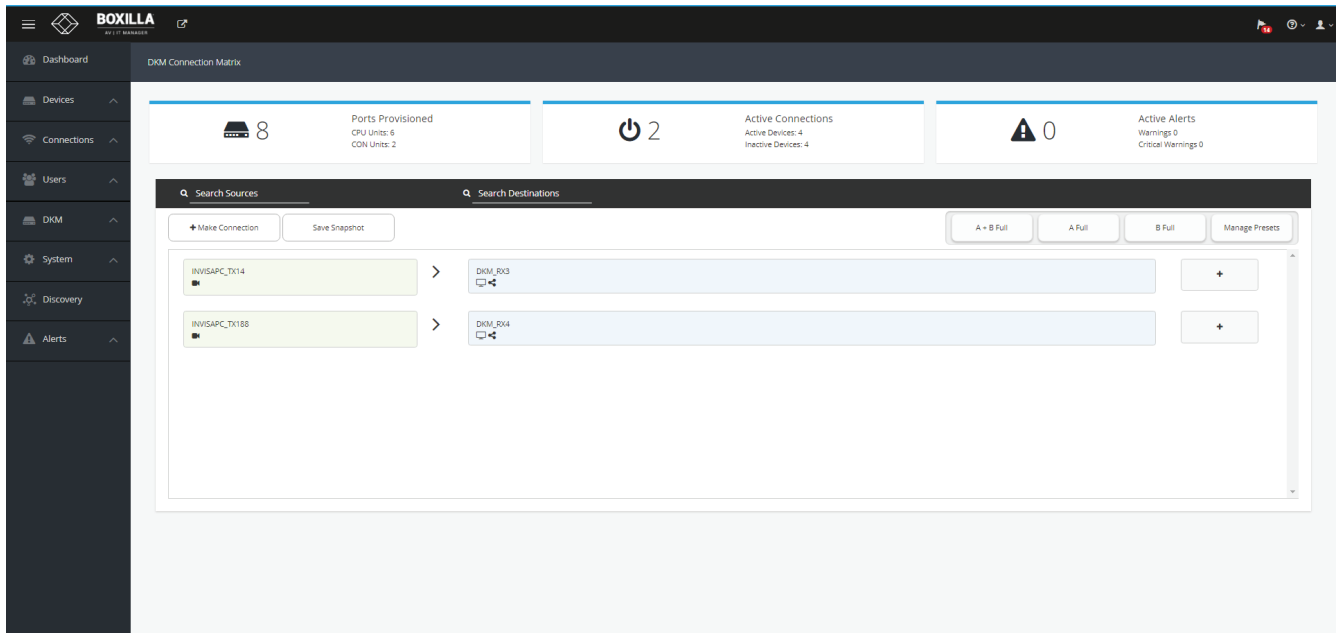
FIGURE 83. MANAGE PRESETS BUTTON

Search of available destinations can be completed within the "Add Destinations" popup box.
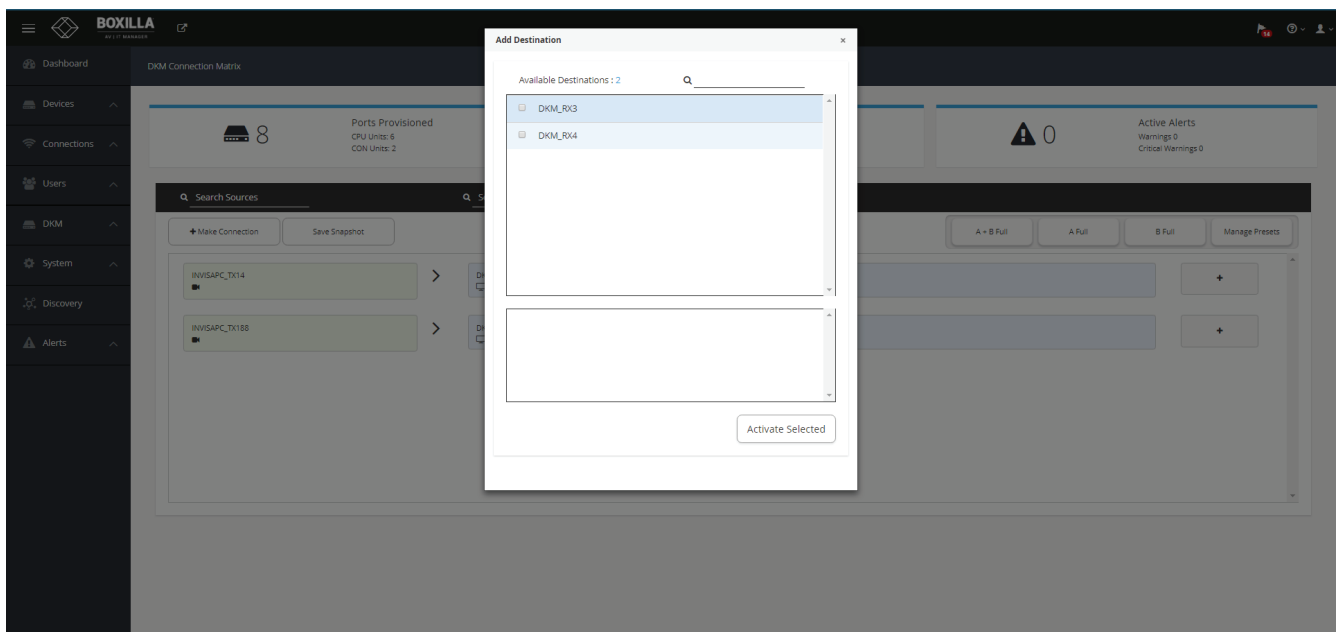
FIGURE 84. ADD DESTINATION POPUP BOX

CHAPTER 10: DKM INTEGRATION

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269
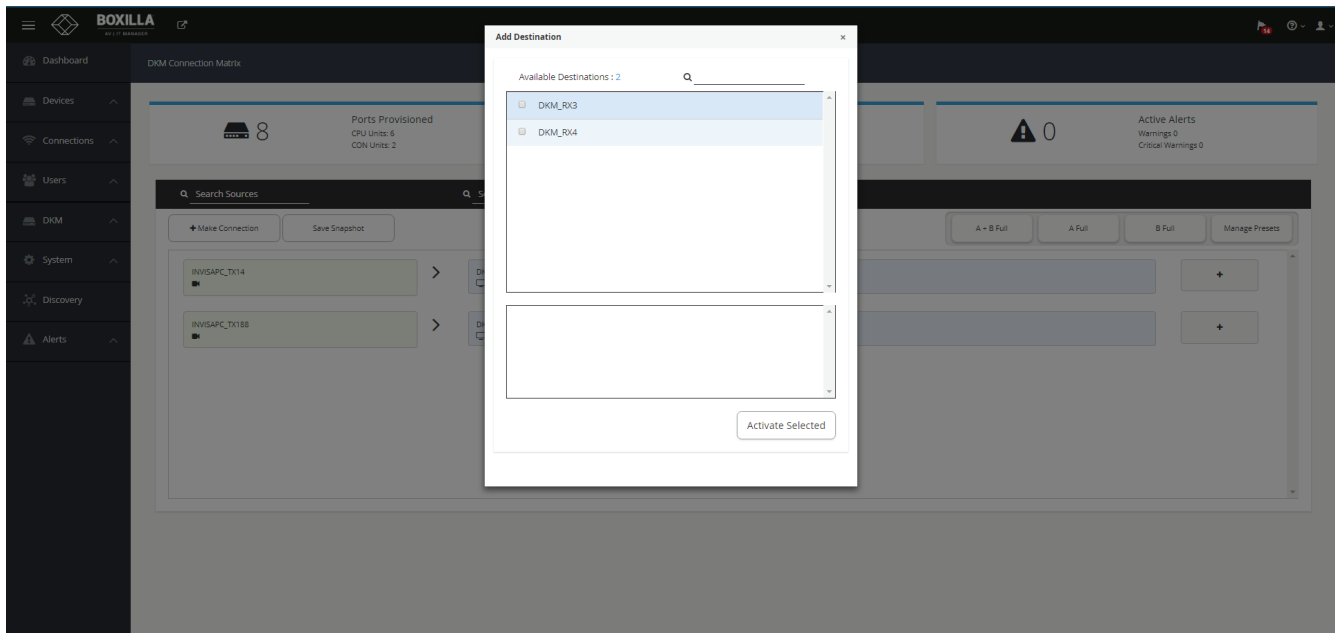
FIGURE 85. ADD DESTINATION POPUP BOX, ACTIVATE SELECTED BUTTON

Select the Destinations from the available destinations and click next
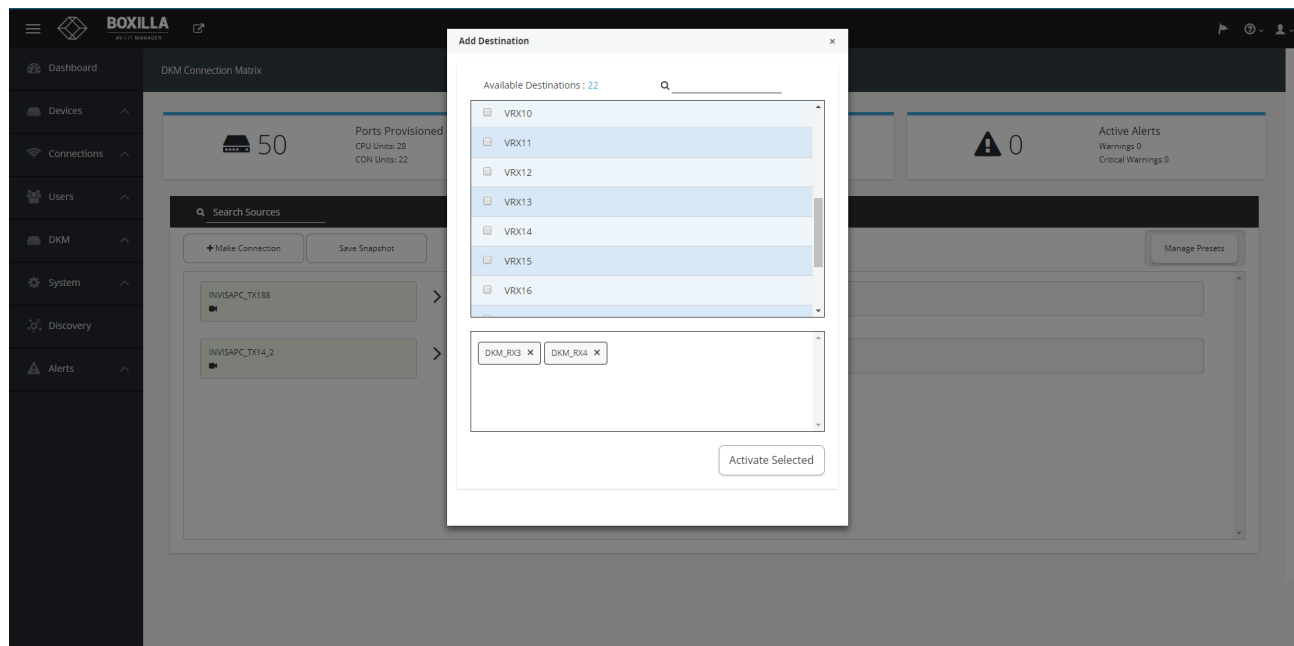
FIGURE 86. ADD DESTINATION RESULTING CONNECTION SCREEN

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

CHAPTER 10: DKM INTEGRATION

Once Activated, connections get listed under the Viewer screen.
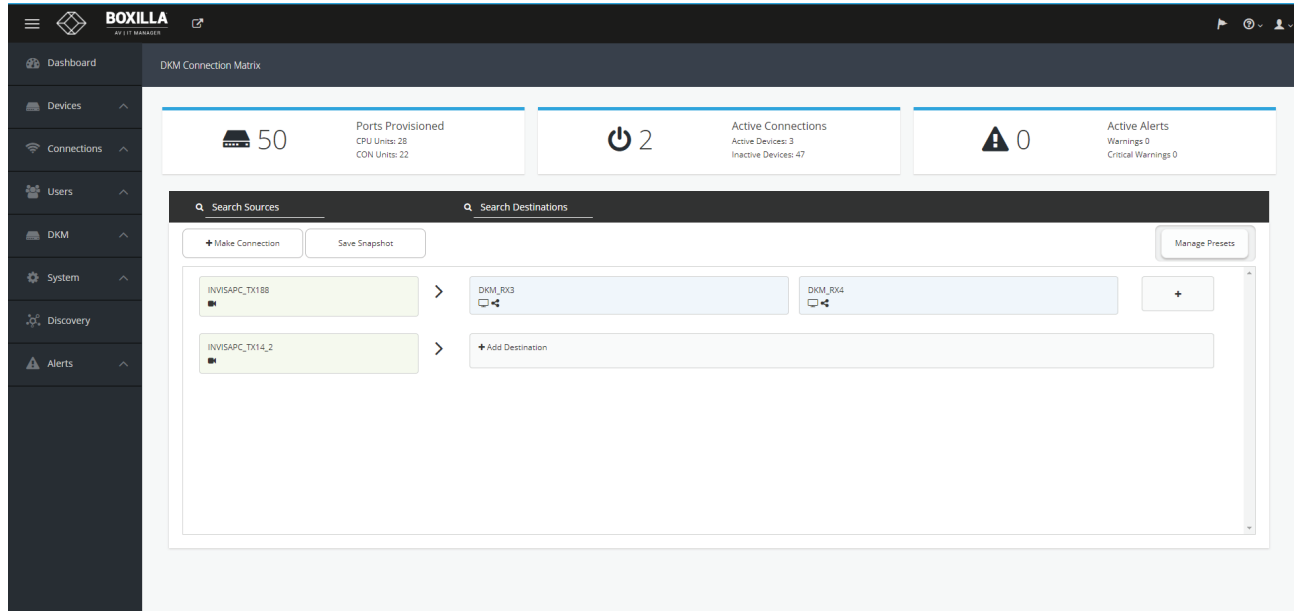
FIGURE 87. VIEWER SCREEN

Active connections are listed under the Connections link. Each connection has the option of remotely breaking it.
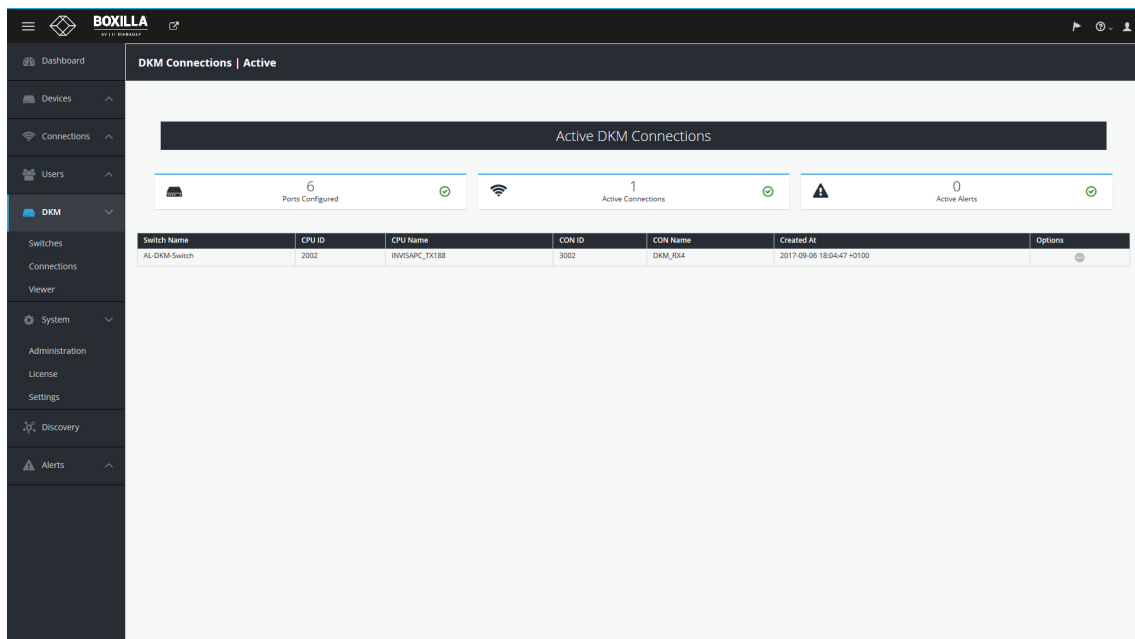
FIGURE 88. ACTIVE DKM CONNECTIONS

NEED HELP?
LEAVE THE TECH TO US
**LIVE 24/7
TECHNICAL
SUPPORT**
1.877.877.2269

CHAPTER 10: DKM INTEGRATION

10.5 PRESETS

Under Viewer, click "Manage Presets," then click "Create Custom" and select one or more available sources.
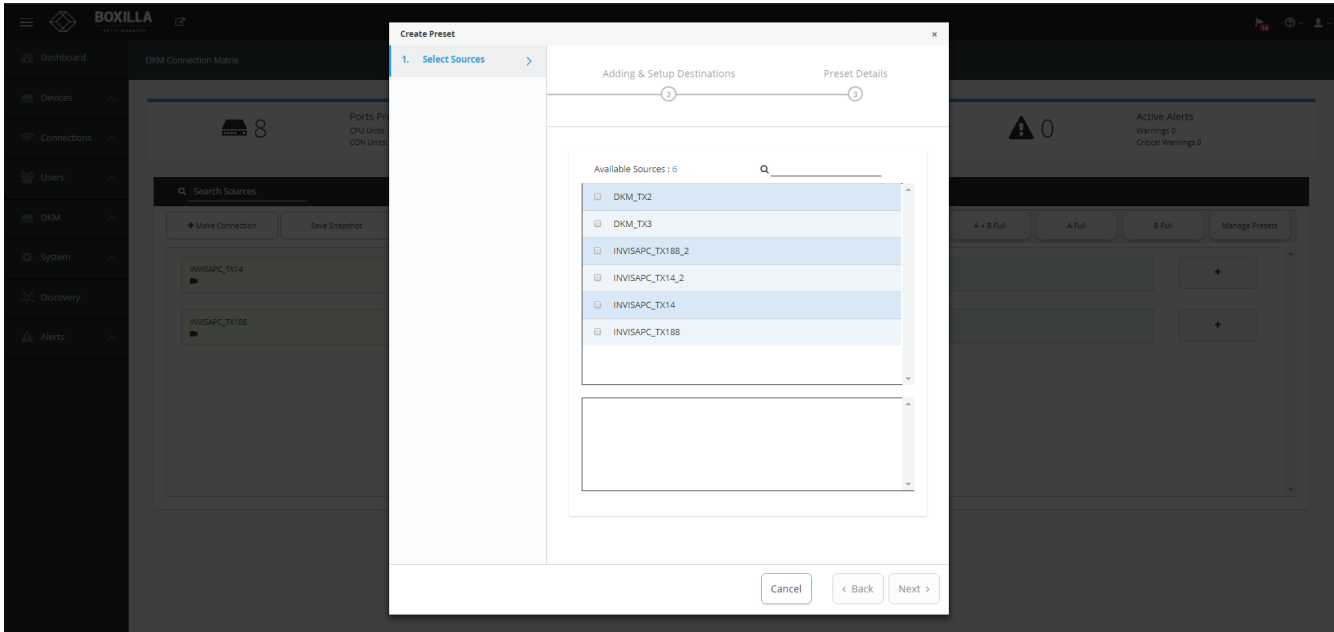
FIGURE 89. CREATE CUSTOM PRESETS

Next, select one or more destinations from the list of available destinations.
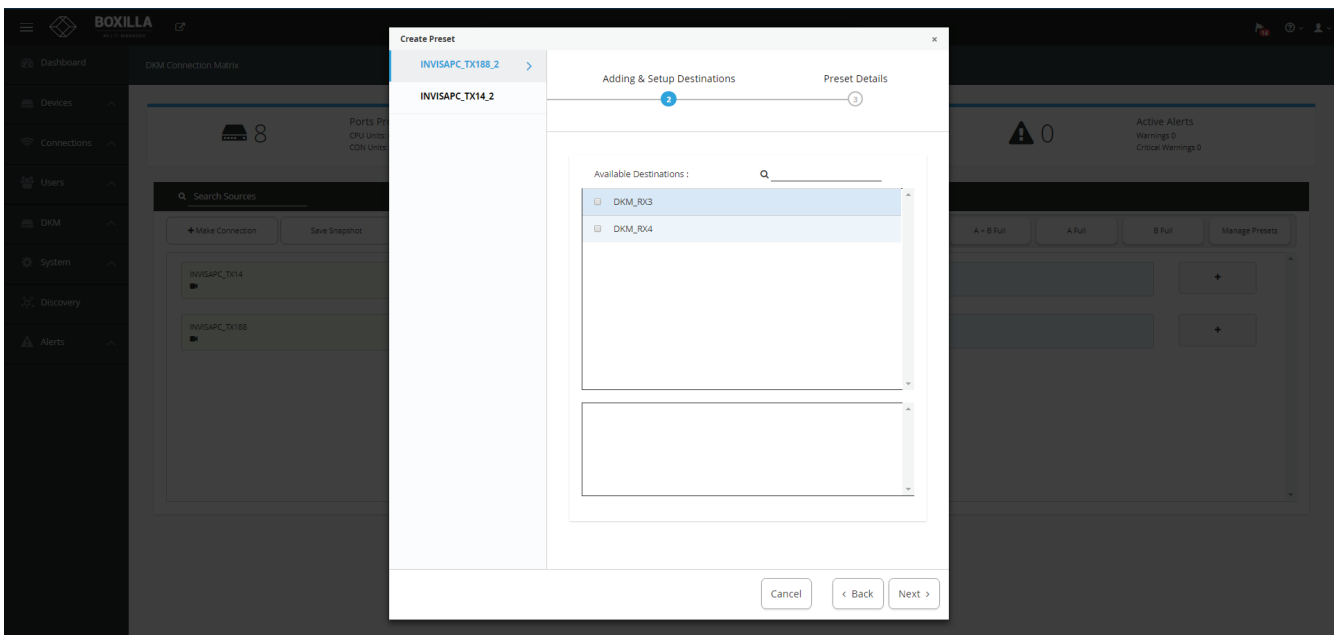
FIGURE 90. SELECT DESTINATIONS

NEED HELP?
LEAVE THE TECH TO US
**LIVE 24/7
TECHNICAL
SUPPORT**
1.877.877.2269

CHAPTER 10: DKM INTEGRATION

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.
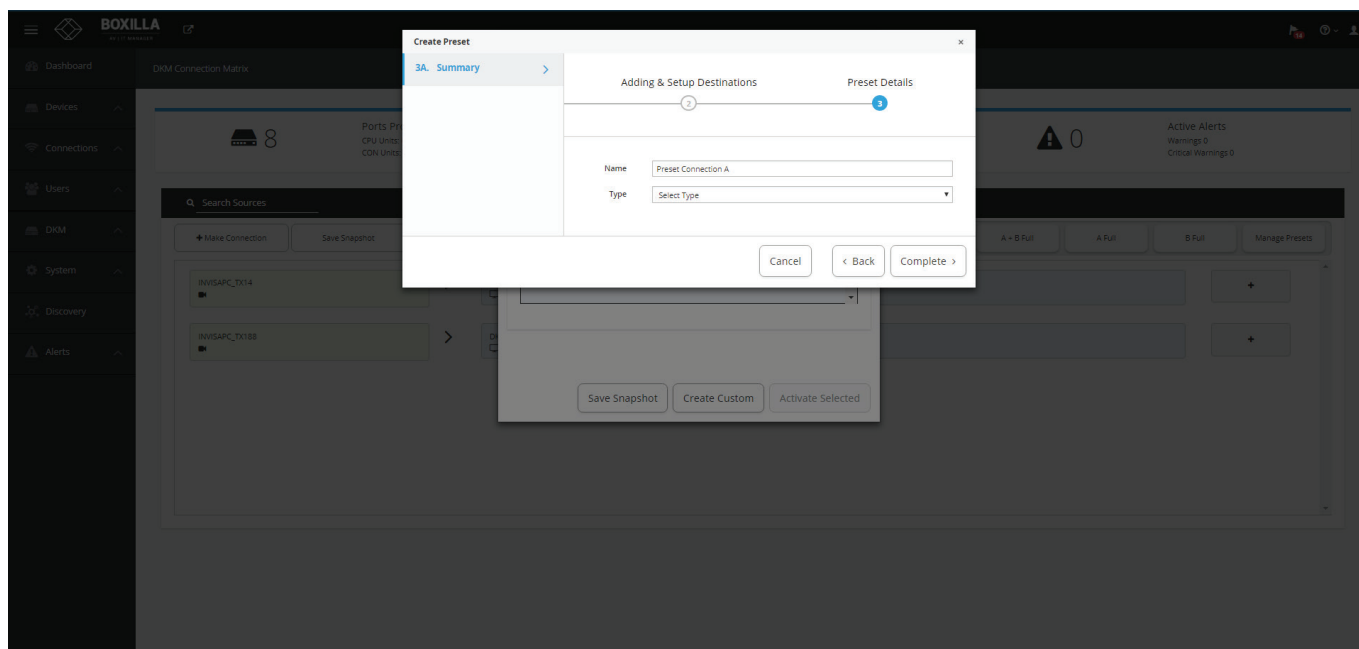
FIGURE 91. PRESETS SCREEN

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.
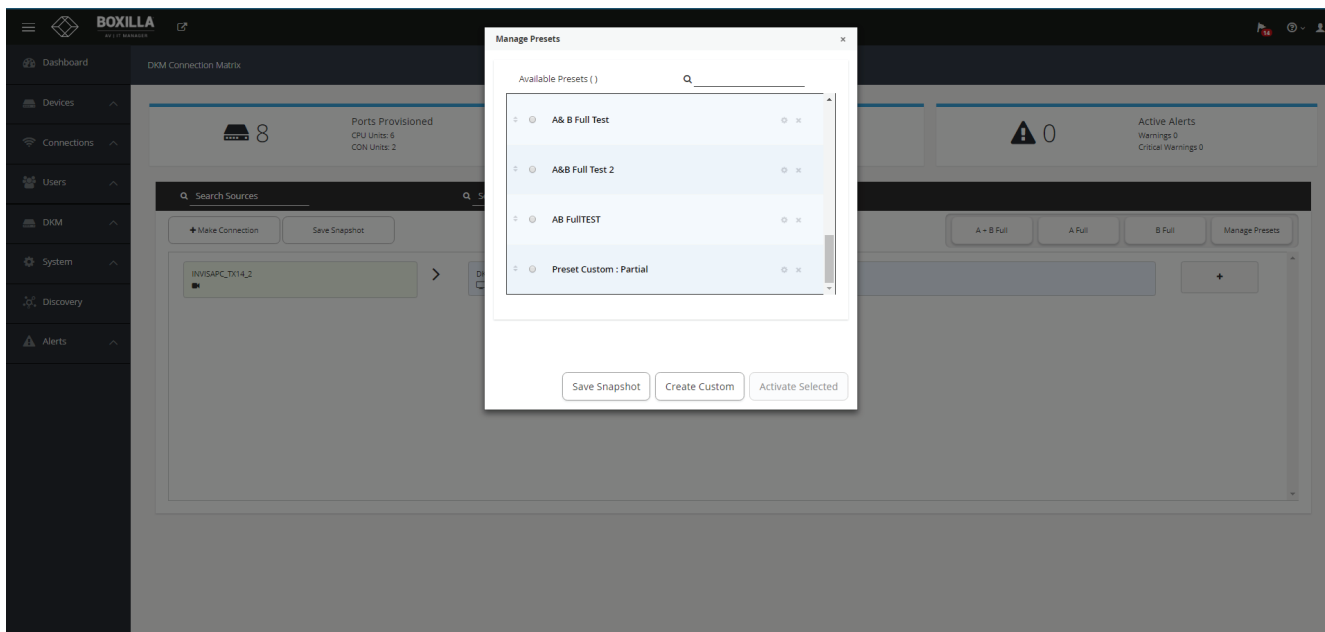
FIGURE 92. CREATE CUSTOM PRESETS COMPLETED SCREEN

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.
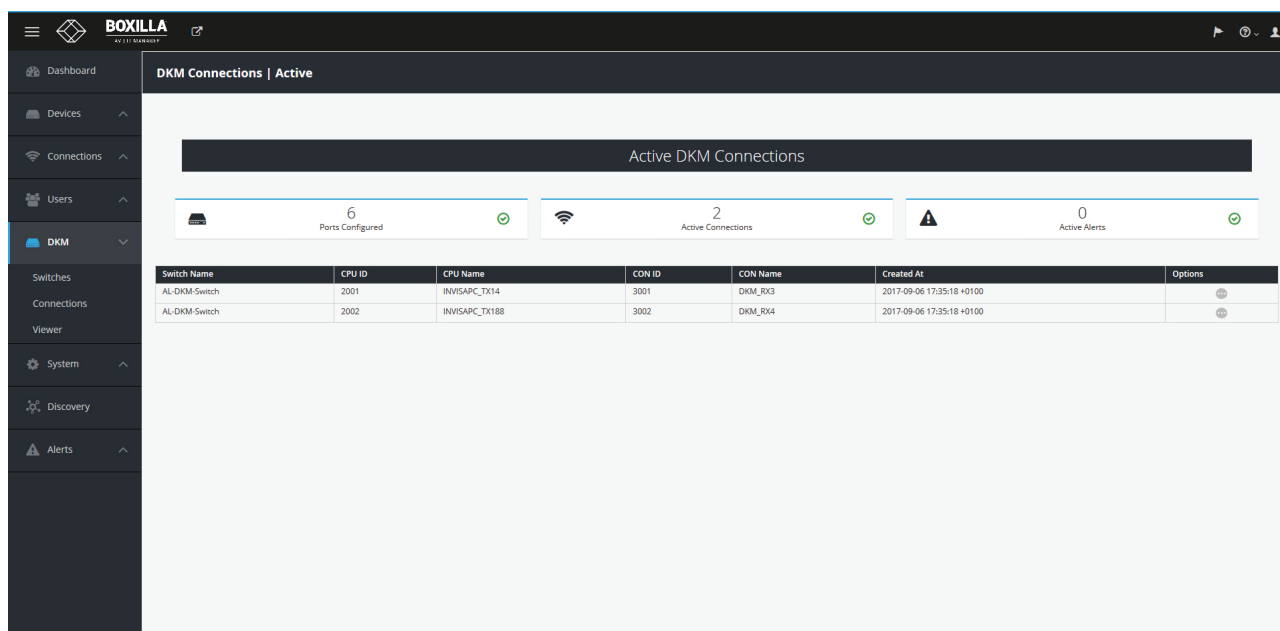
FIGURE 93. ACTIVE DESTINATIONS SCREEN

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)
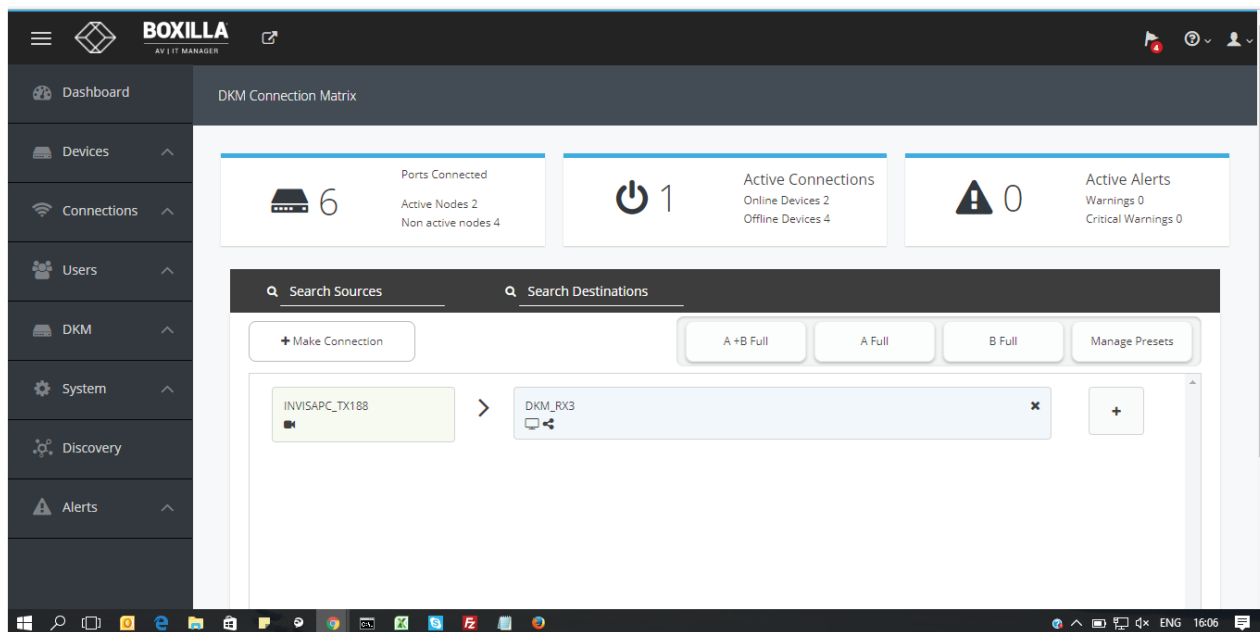
FIGURE 94. DESELECT A SOURCE/DESTINATION

10.6 ATTACHING VIRTUAL CPUS TO INVISAPC RX

Virtual CPU based connections from a DKM switch can be connected to a directly managed InvisaPC RX on Boxilla by attaching them.
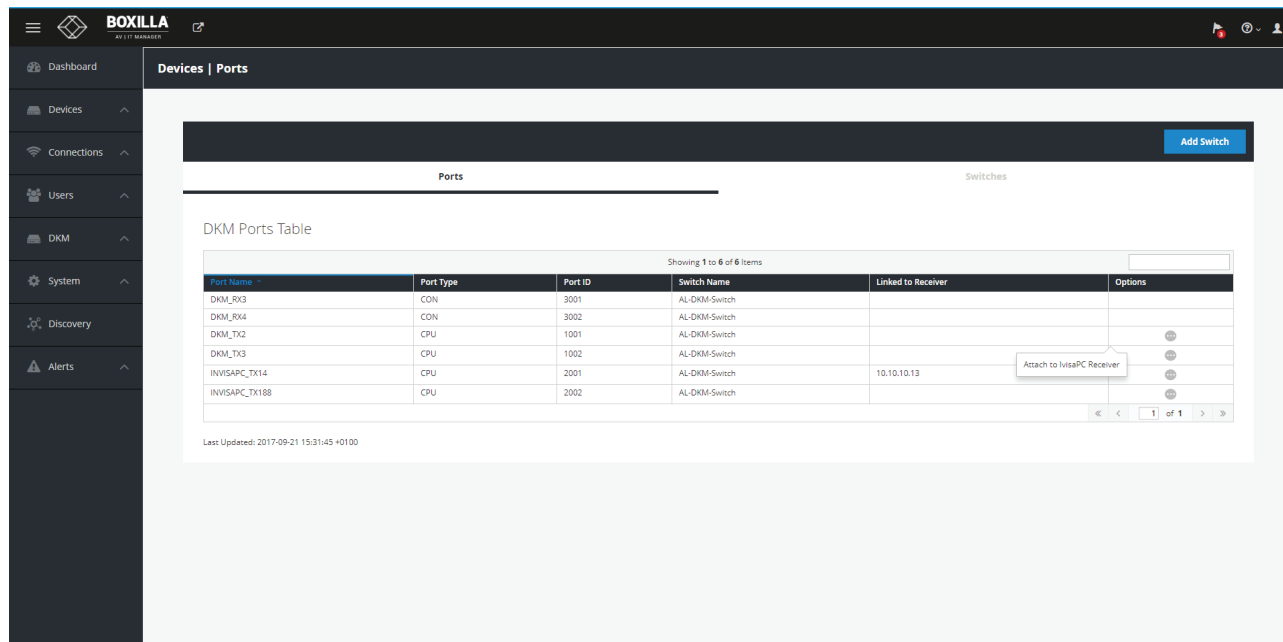
FIGURE 95. VIRTUAL CPUS CONNECTED TO INVISAPC SCREEN

NEED HELP?
LEAVE THE TECH TO US

LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

CHAPTER 11: SYSTEM

The System button in the main menu brings up the System —> Administration —> Upgrade screen shown next. This screen allows the Boxilla unit itself to be managed:

◆ upgrade the firmware;
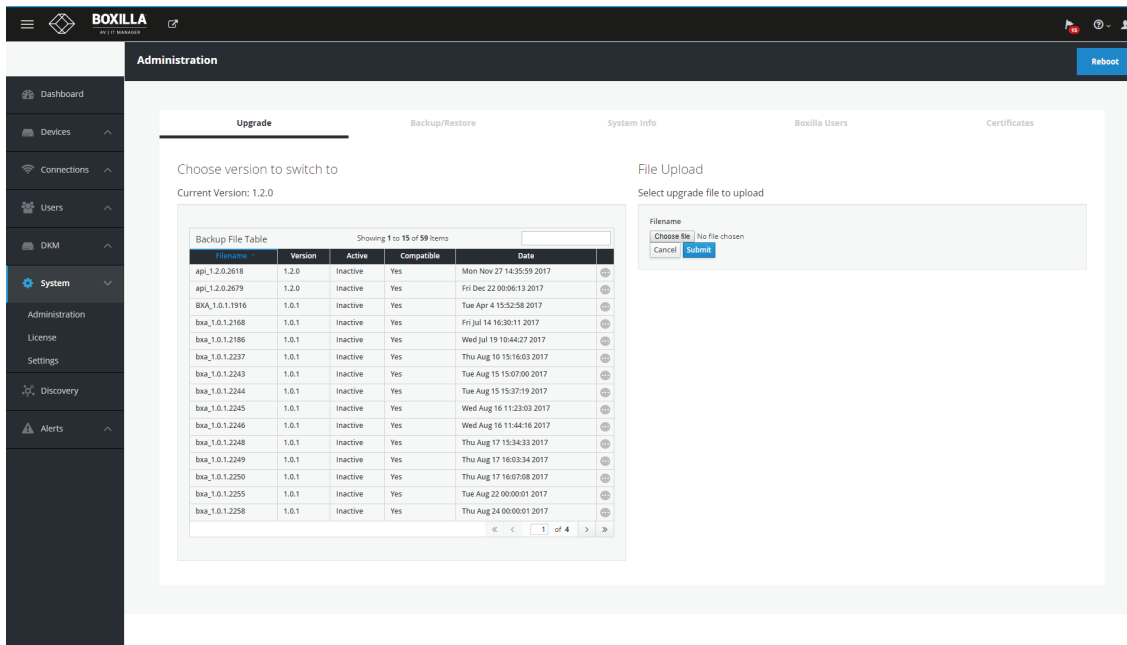
FIGURE 96. UPGRADE FIRMWARE SCREEN

◆ procure a new license file (go to System —> License page);
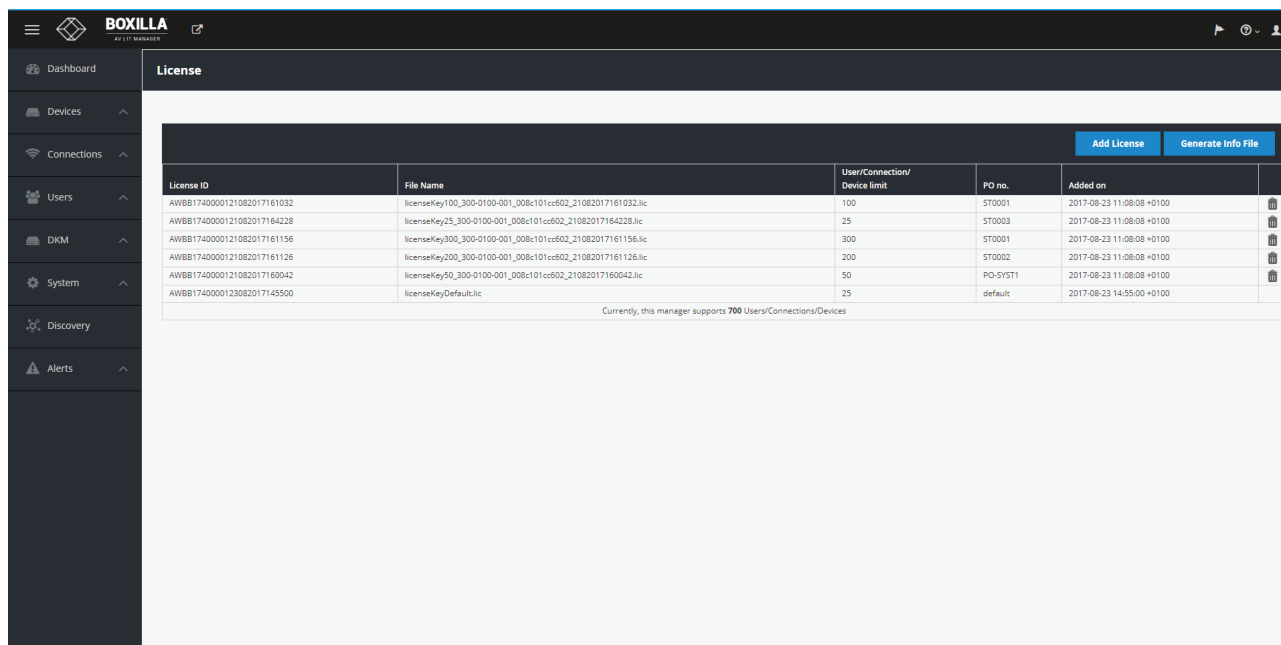
FIGURE 97. LICENSE SCREEN

NEED HELP?
LEAVE THE TECH TO US

LIVE 24/7
TECHNICAL
SUPPORT

1.877.877.2269

CHAPTER 11: SYSTEM

◆ generate your own self-signed certificate;

◆ backup/restore the database (go to System —> Adminstration —> Backup/Restore);
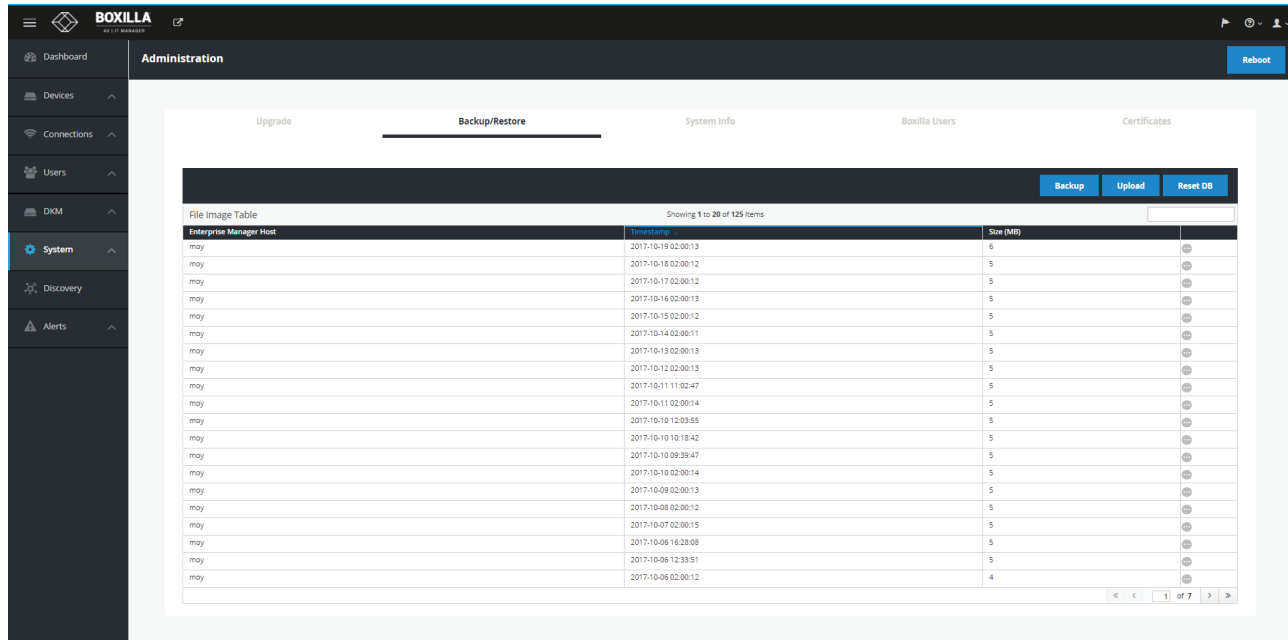
FIGURE 98. BACKUP/RESTORE DATABASE SCREEN

◆ check system information (go to System —> Administration —> System Info page):
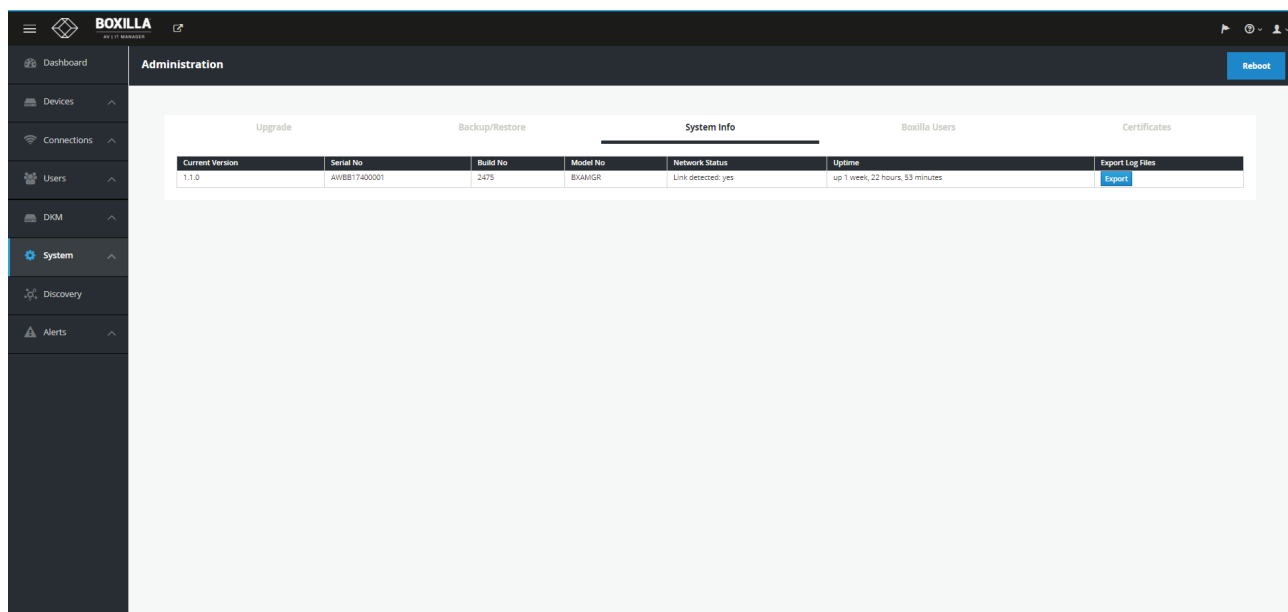
FIGURE 99. CHECK SYSTEM INFORMATION SCREEN

NEED HELP?
LEAVE THE TECH TO US

LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

◆ set thresholds for alerts (go to System —> Settings —> Thresholds page):
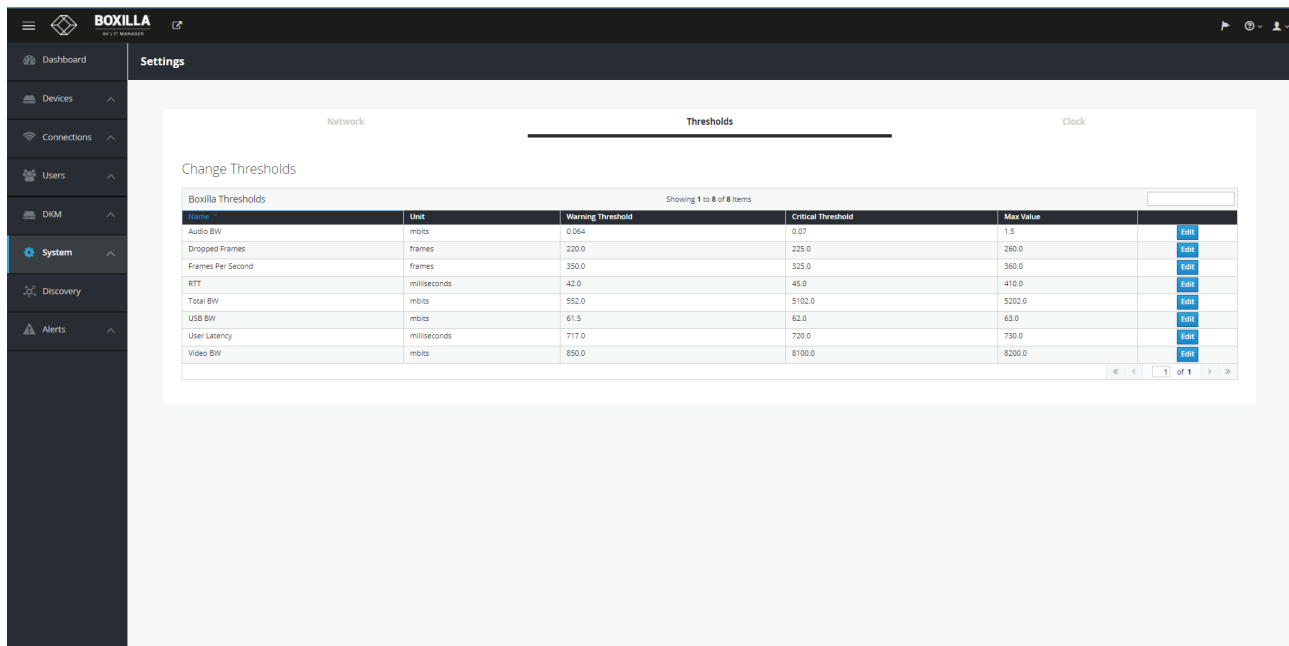
FIGURE 100. SET THRESHOLDS FOR ACTIVE ALERTS SCREEN

◆ change network settings (go to System —> Settings —> Network page):
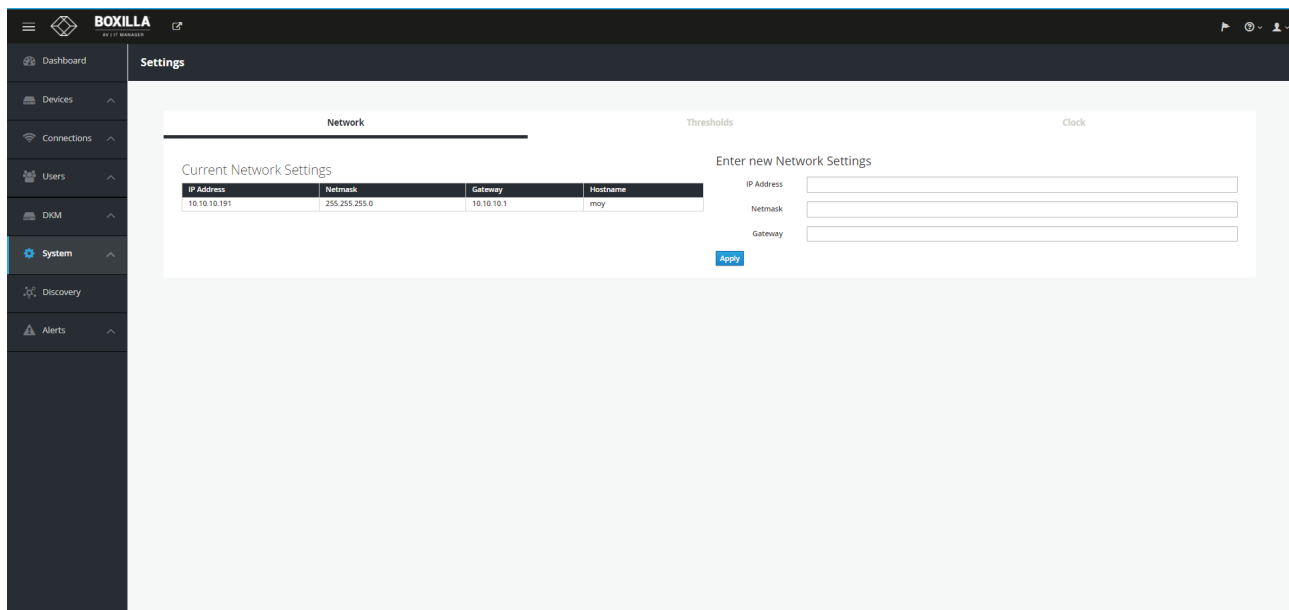
FIGURE 101. NETWORK SETTINGS SCREEN

◆ set system time (or Clock) (go to System —> Settings —> Clock page):
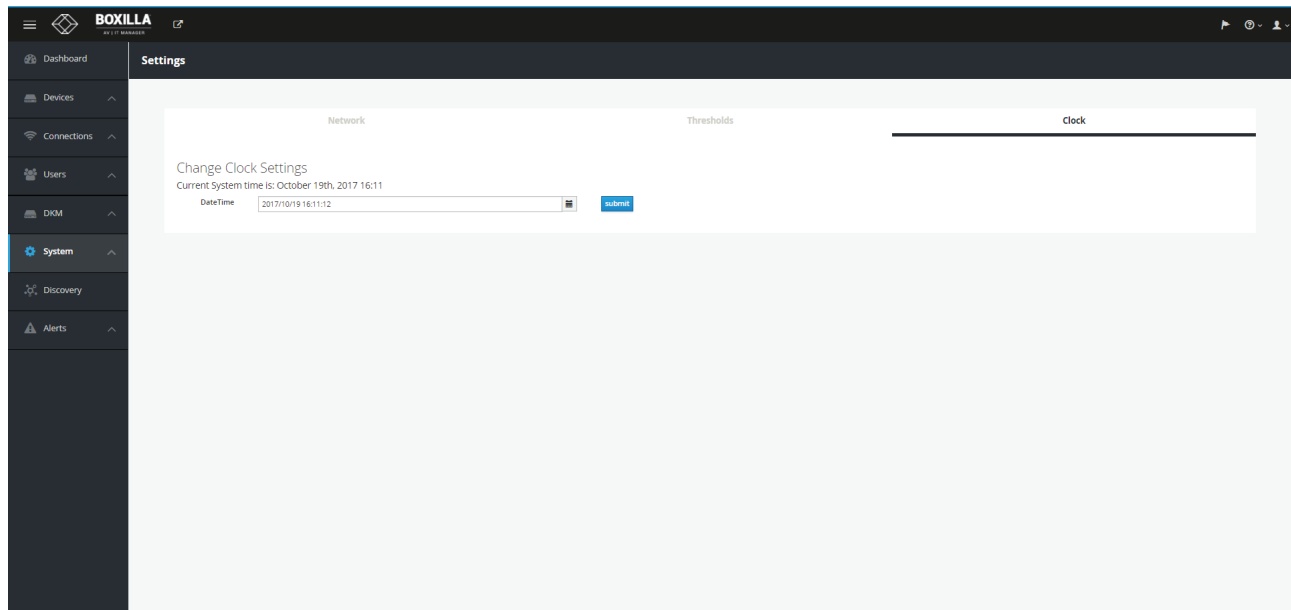
FIGURE 102. SYSTEM CLOCK SCREEN

◆ create/edit Boxilla users (go to System —> Administration —> Boxilla Users page):
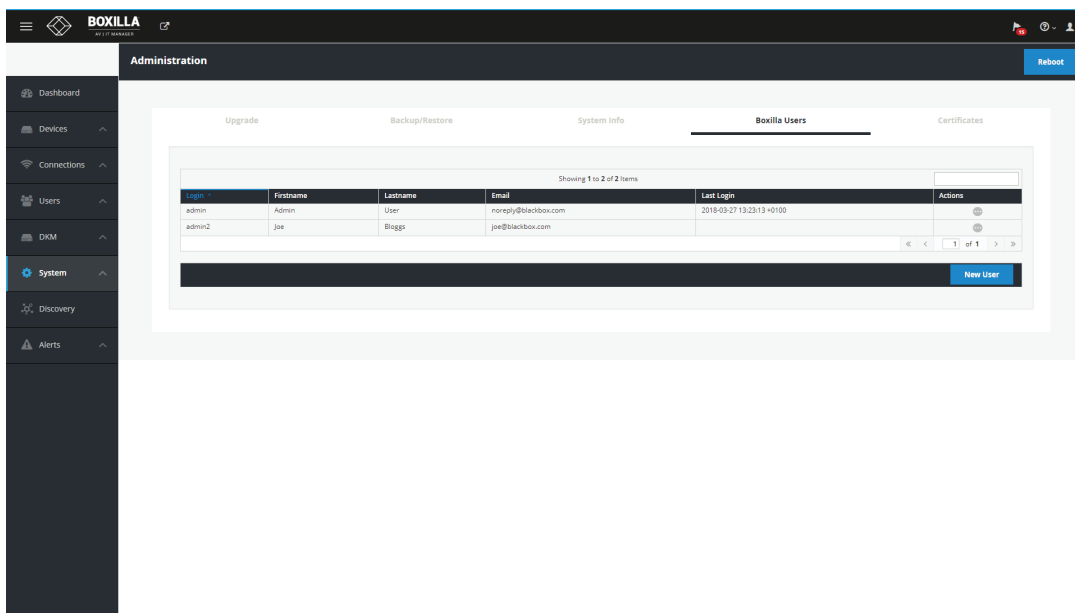
FIGURE 103. CREATE/EDIT BOXILLA USERS SCREEN

The administrator can reboot the Boxilla unit by clicking on the Reboot button on the top right of the System —> Administration screen.
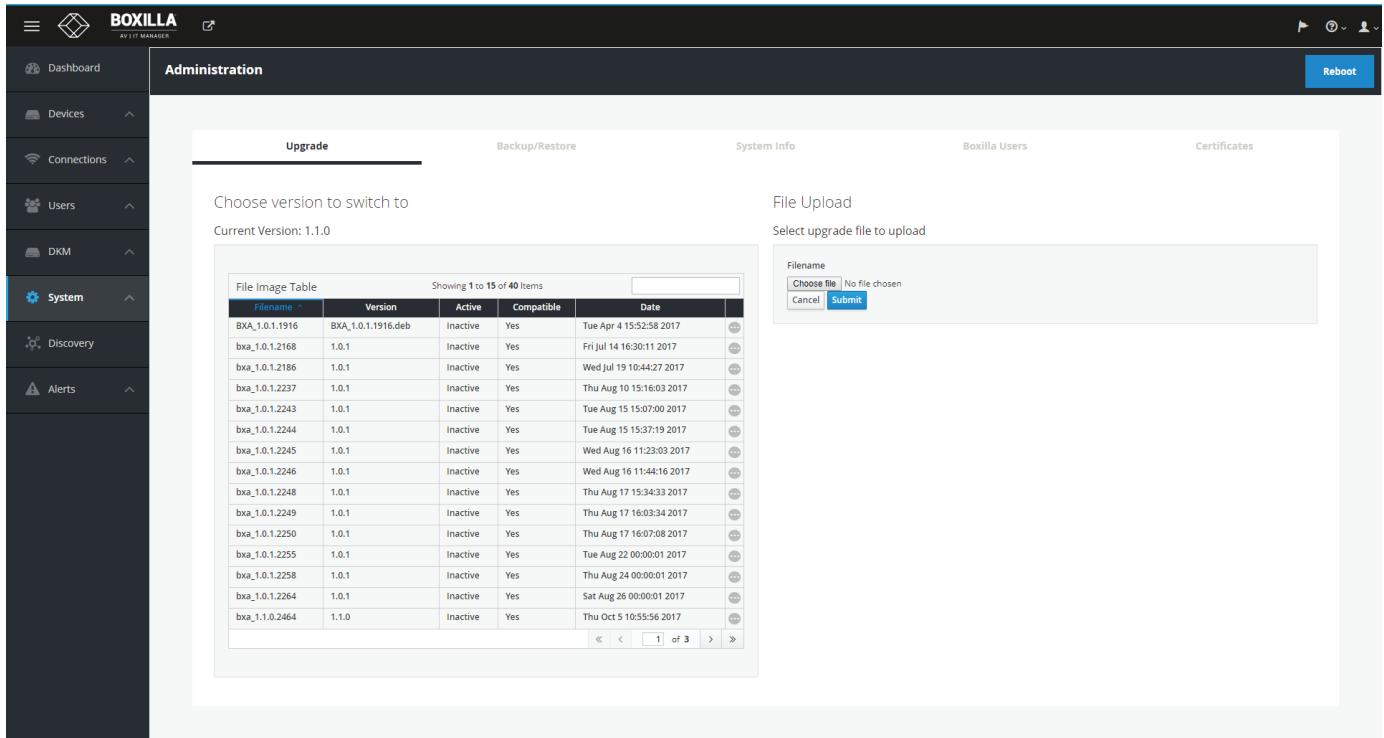
FIGURE 104. SYSTEM SCREEN—UPGRADE

CHAPTER 11: SYSTEM

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

11.1 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 "•••" icon options on the row of the firmware to be used to upgrade the unit.

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.

11.2 SYSTEM — LICENSE PAGE — BOXILLA LICENSING

Boxilla licensing allows the customer to customize the size of the domain to be supported. 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).

The system supports the addition of:

- BXAMGR-LIC25 (25 more devices/users/connections)
- BXAMGR-LIC50 (50 more devices/users/connections)
- BXAMGR-LIC100 (100 more devices/users/connections)
- BXAMGR-LIC200 (200 more devices/users/connections)
- BXAMGR-LIC300 (300 more devices/users/connections)
- BXAMGR-LIC-ULT (unlimited more devices/users/connections)

Licenses can be added under System -> License Page. Alternatively, it can be found under Admin page—admin item.

To find the current license, select License Information.

CHAPTER 11: SYSTEM

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269
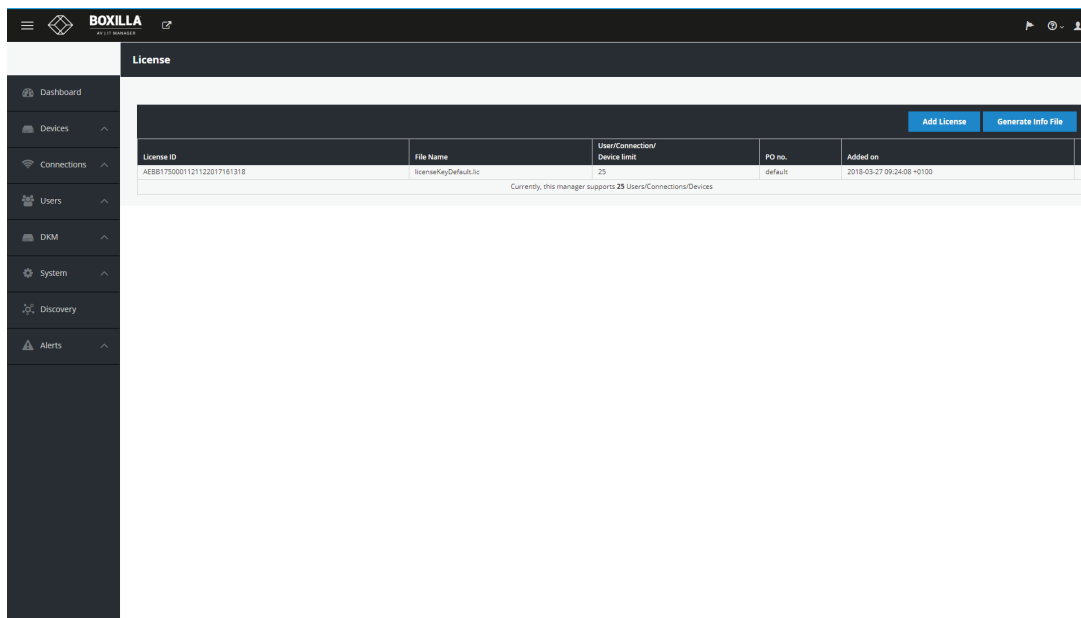
FIGURE 105. SYSTEM —> LICENSE SCREEN

11.2.1 HOW TO REQUEST A LICENSE

To procure a new license file, generate the info file from your current system using Generate Info File option within License link. The info file will be downloaded onto the local machine. Provide the info file to Black Box Technical Support (contact us at 877-877-2269 or info@blackbox.com) to generate the license file for you.
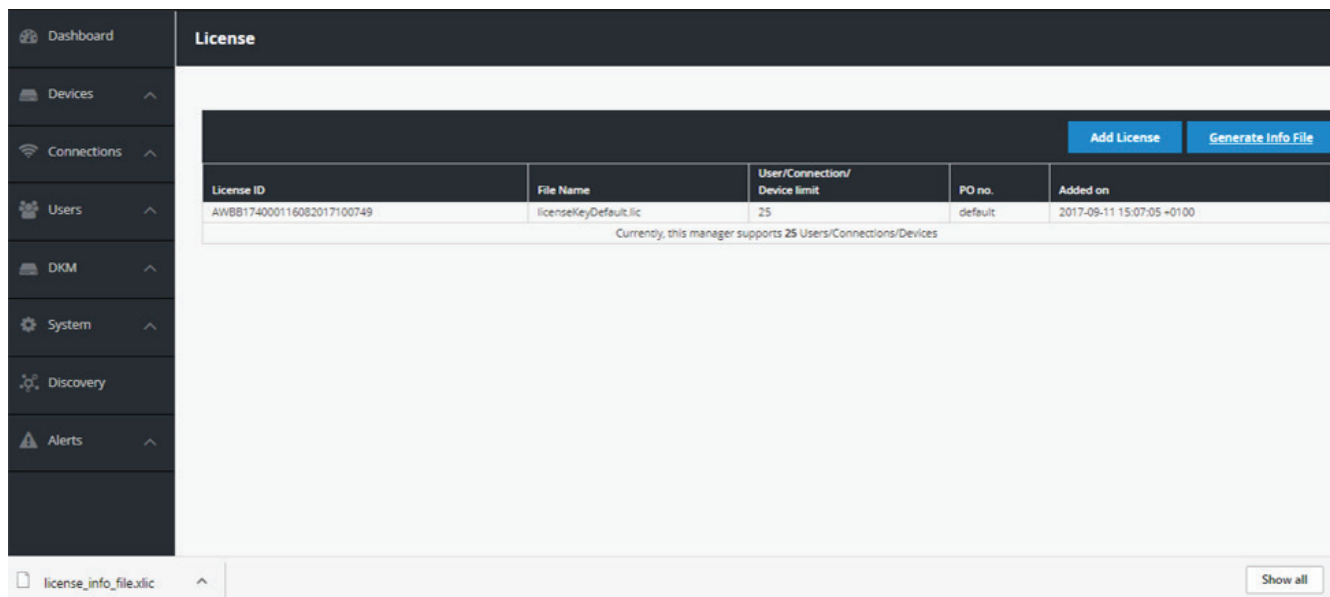
FIGURE 106. ADD LICENSE SCREEN

CHAPTER 11: SYSTEM

NEED HELP?
LEAVE THE TECH TO US
**LIVE 24/7
TECHNICAL
SUPPORT**
1.877.877.2269

11.2.2 HOW TO UPLOAD A LICENSE FILE

Once you receive the license file, upload the new license.
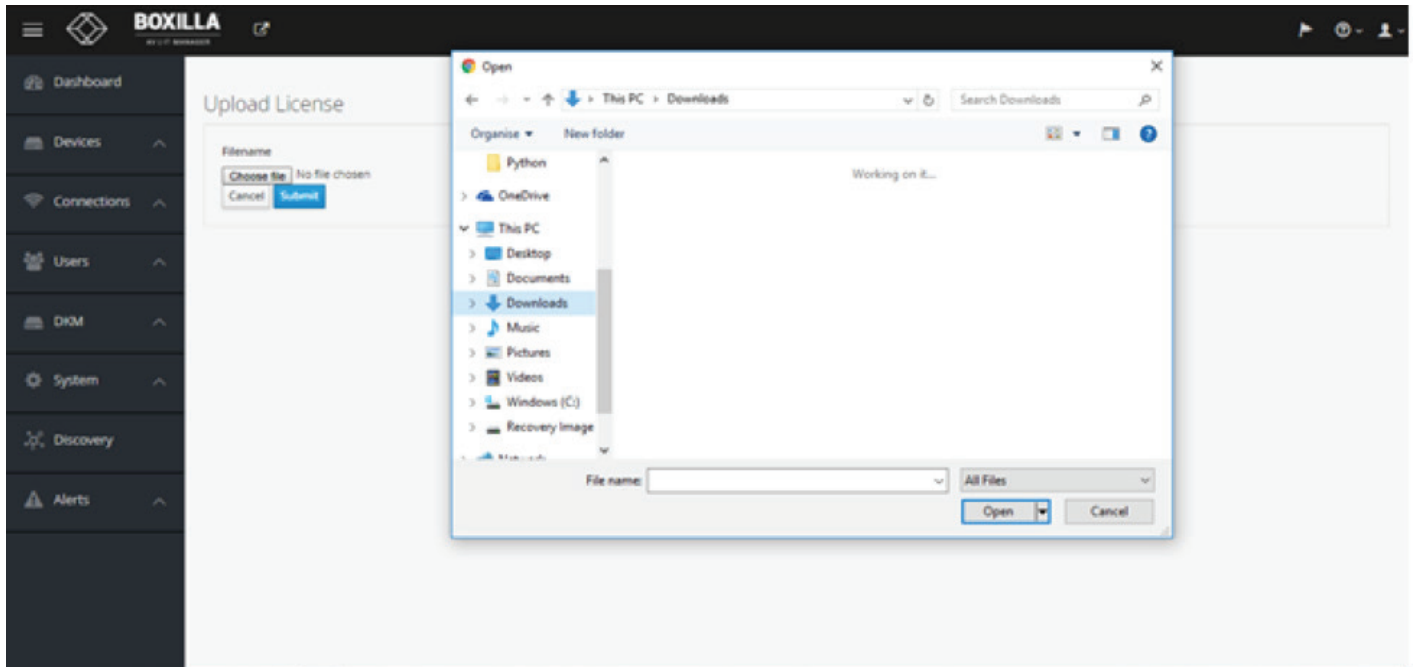
FIGURE 107. UPLOAD LICENSE SCREEN

CHAPTER 11: SYSTEM

NEED HELP?
LEAVE THE TECH TO US
**LIVE 24/7
TECHNICAL
SUPPORT**
1.877.877.2269

11.3 SYSTEM—ADMINISTRATION — CERTIFICATES UPLOAD

Users who wish to remove the "This connection is insecure" need to have the ability to generate their own self signed certificates with their own company information or certificates generated form a registered Certificate Authority (CA). The new system allows the users to upload these files into Boxilla so they can upload the other key into their browser. This will then act as an authenticated certificate and the user will no longer get the security warning.

Under the System —> Administration page, go to the Certificates tab to add and manage certificates.
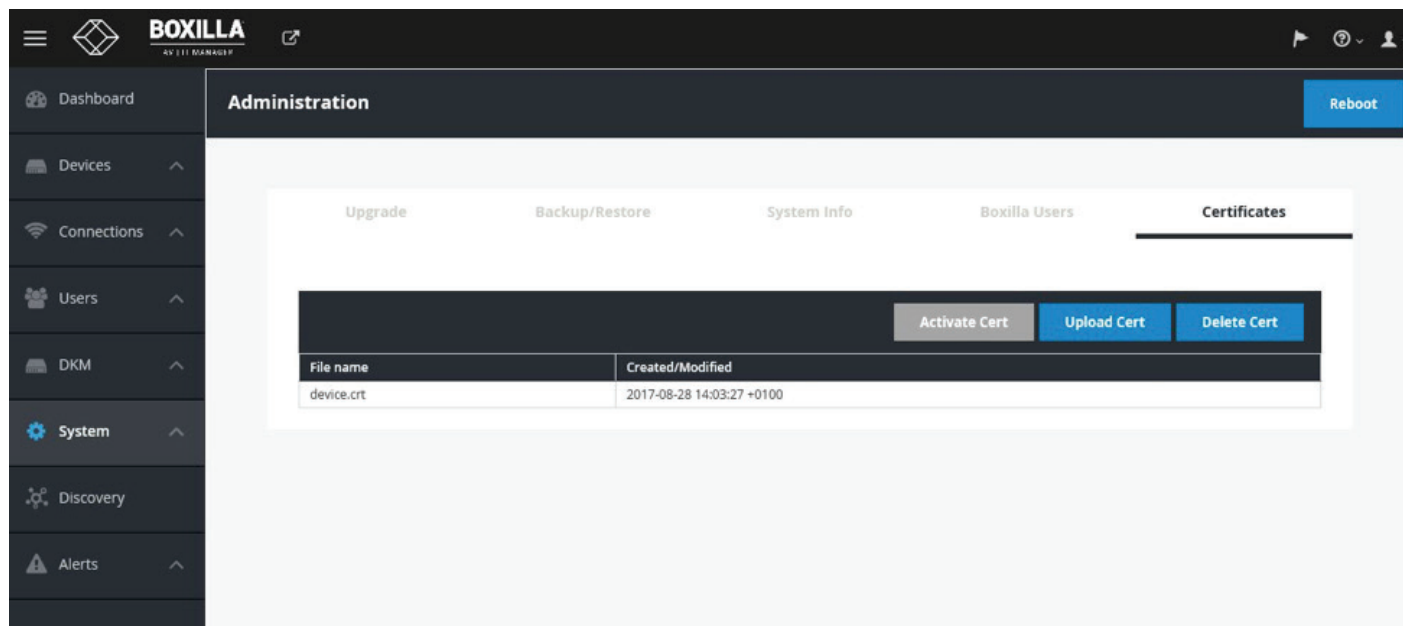
FIGURE 108. CERTIFICATES TAB

To upload a certificate, click on the Upload certificate file button under the Certificates tab. Browse the local machine folder to upload the certificate.

CHAPTER 11: SYSTEM

NEED HELP?
LEAVE THE TECH TO US

LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269
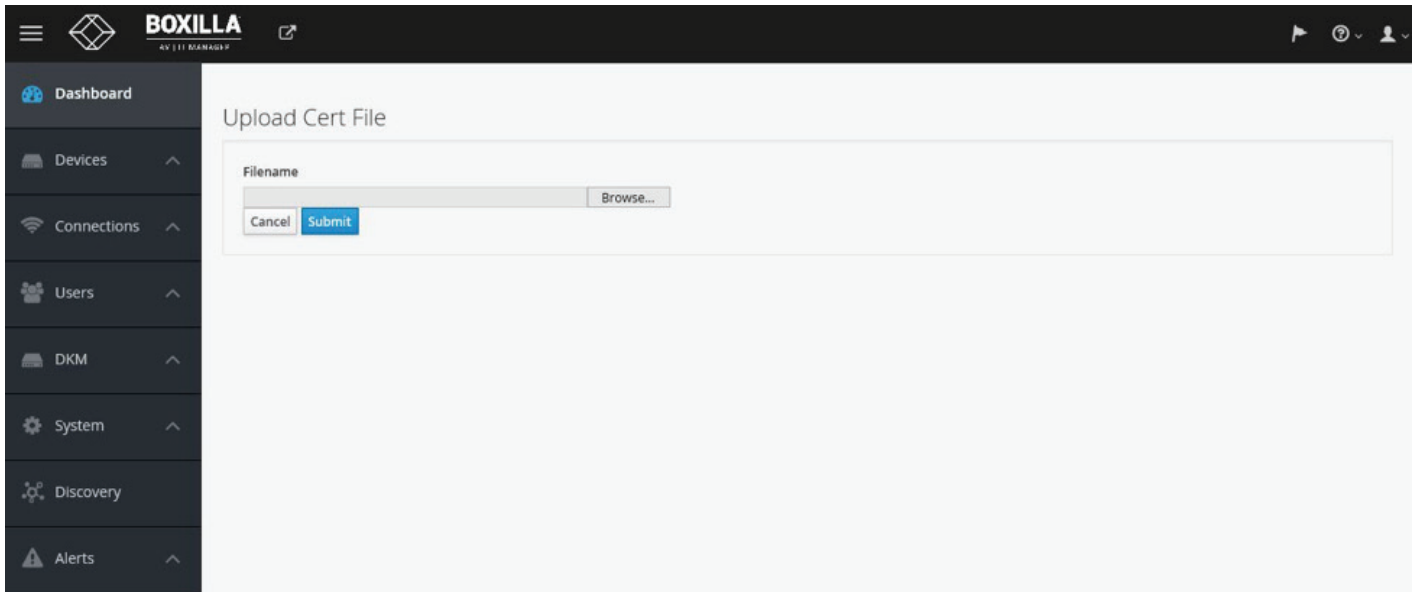
FIGURE 109. UPLOAD CERTIFICATE BUTTON
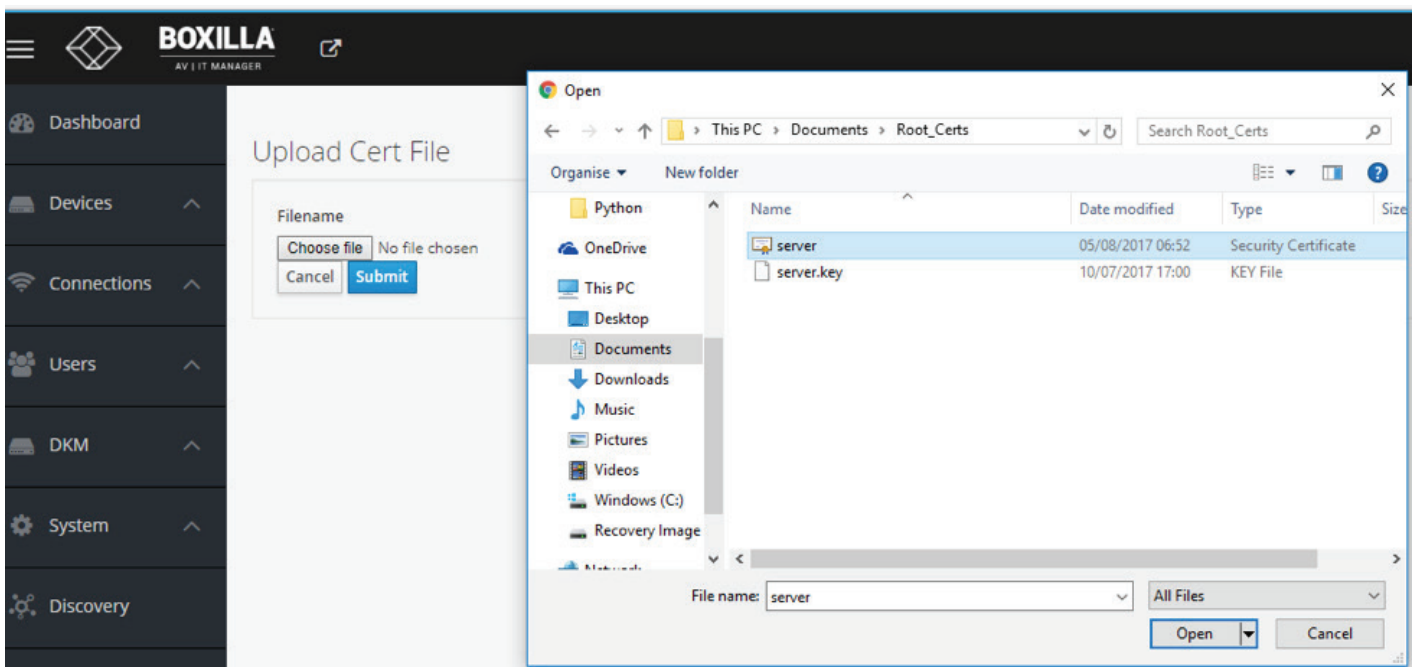
FIGURE 110. SELECT THE CERTIFICATE FILE

A green alert on the page indicates that the certifcate is uploaded.
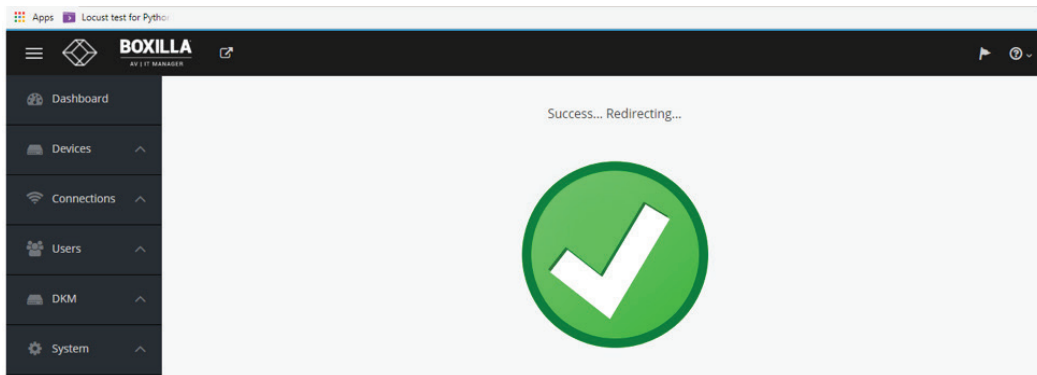
FIGURE 111. GREEN ALERT

To delete any existing certificates, click on the delete cert button under certificates tab.
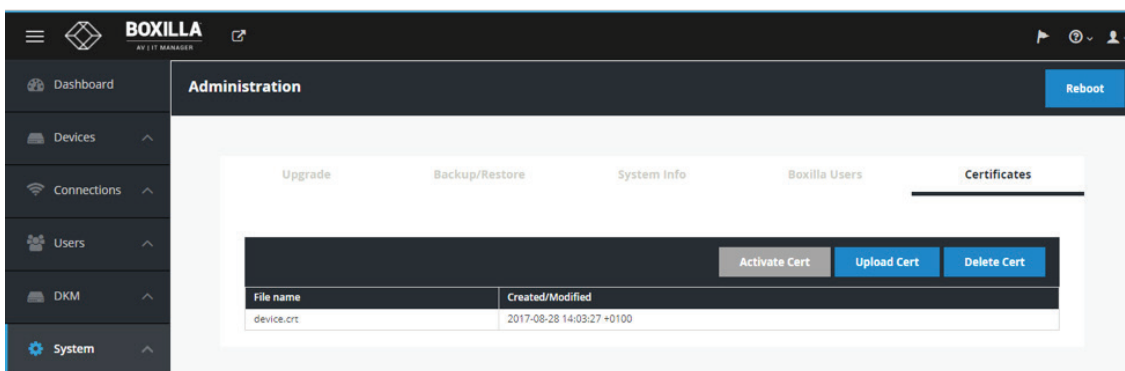
FIGURE 112. DELETE BUTTON

A popup message will be displayed once the certificate is deleted.
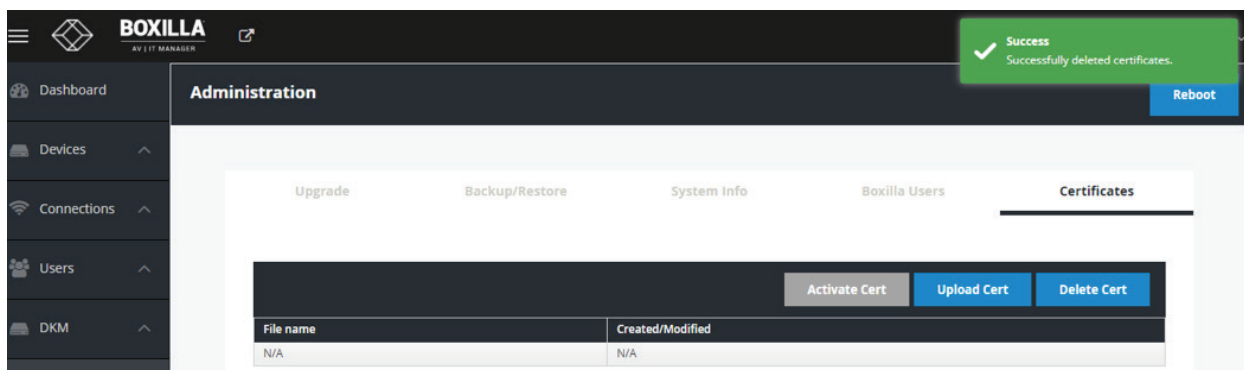
FIGURE 113. DELETE SUCCESSFUL

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

CHAPTER 11: SYSTEM

11.4 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 external to unit, click on Download on the "•••" icon options on the row on the Backup table to be downloaded.
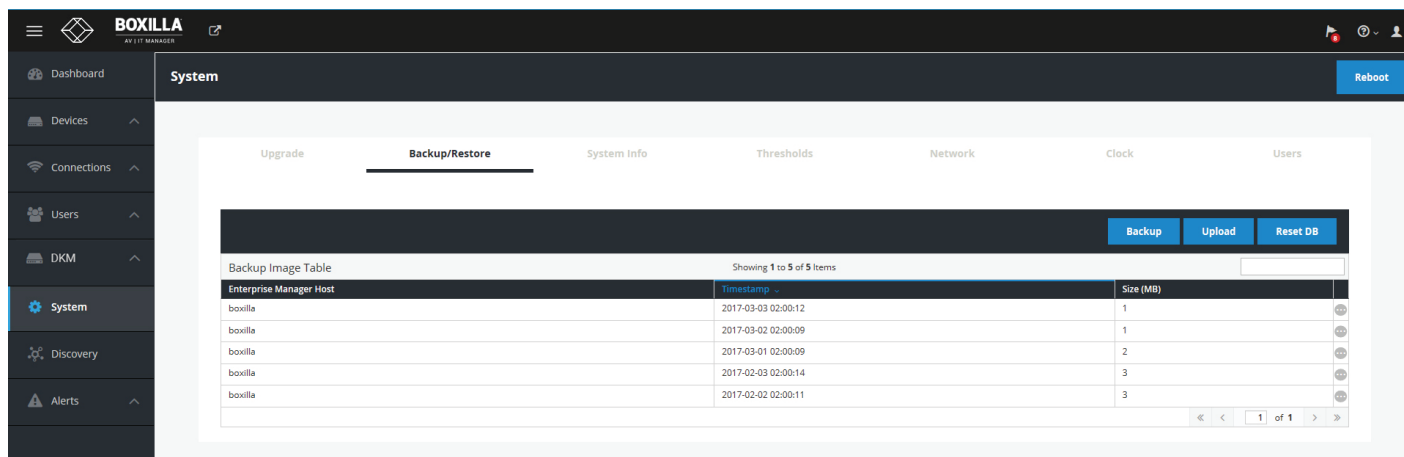
FIGURE 114. SYSTEM BACKUP/RESTORE TAB

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 on the "•••" icon options on the row on the Backup table to be used to restore the Boxilla unit settings.

Clicking on ResetDB purges the database on the Boxilla unit and restores it to a default state.

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.

11.5 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.

11.6 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.

FIGURE 115. 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 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

NEED HELP?
LEAVE THE TECH TO US

LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

CHAPTER 11: SYSTEM

11.7 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 and Gateway in IPv4 format and click Apply).
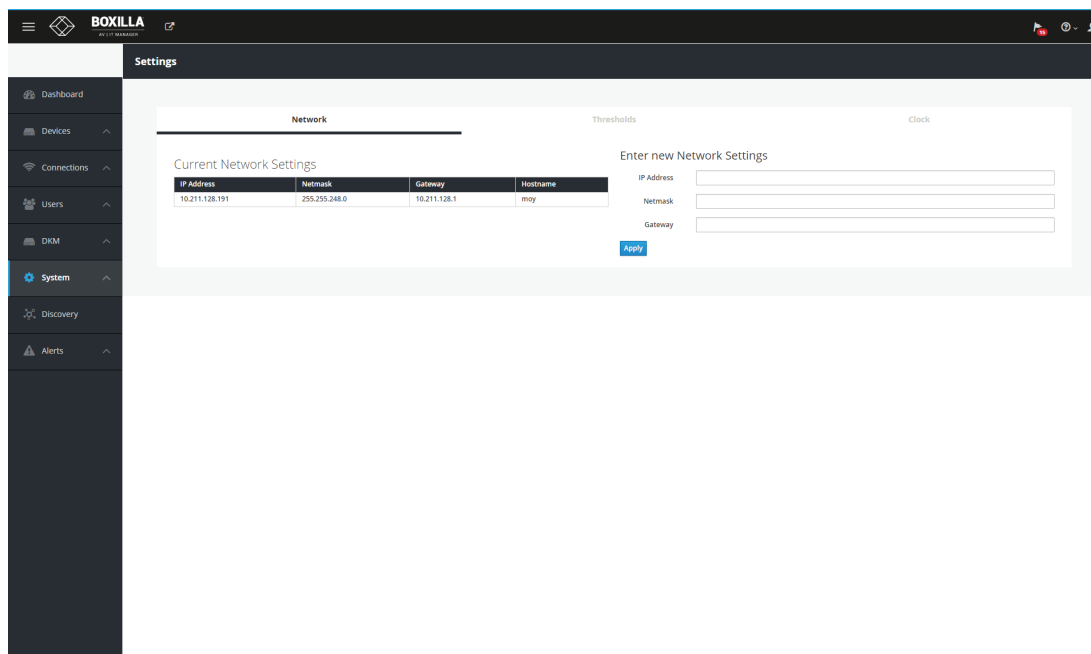
FIGURE 116. SYSTEM —> SETTINGS —> NETWORK SCREEN

11.8 SYSTEM — SETTINGS — CLOCK

The System —> Settings —> Clock tab enables the Administrator to see the current system time and to change it.
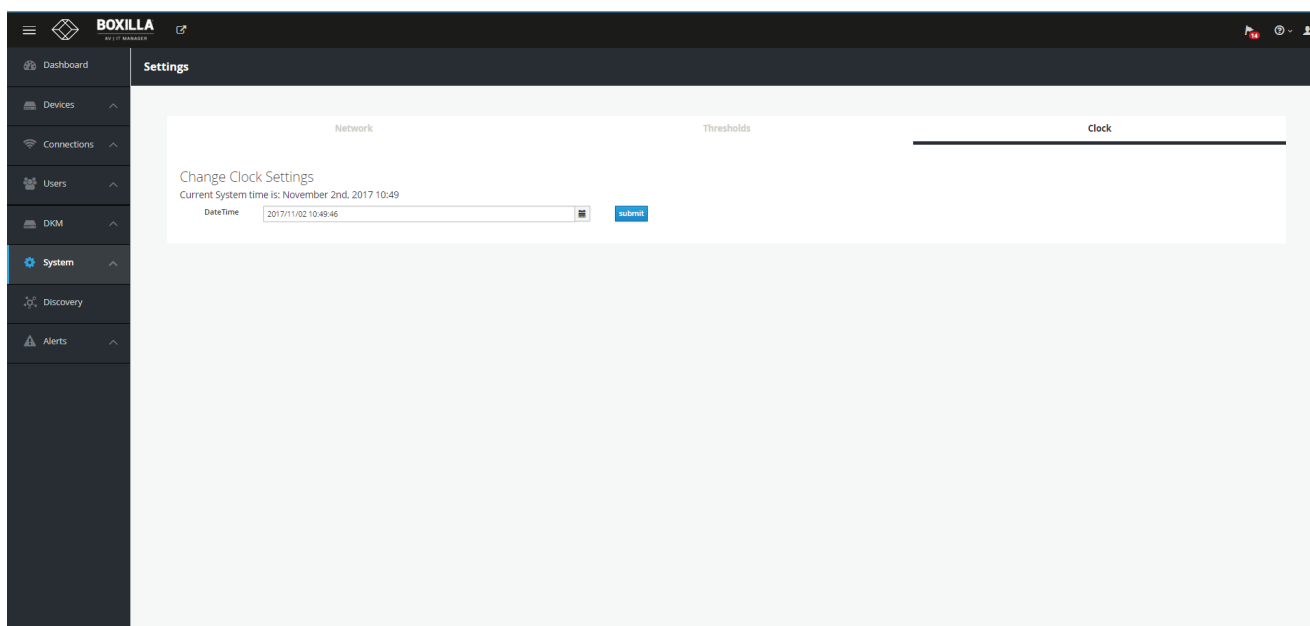
FIGURE 117. CLOCK (OR TIME) SETTINGS

CHAPTER 11: SYSTEM

11.9 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.
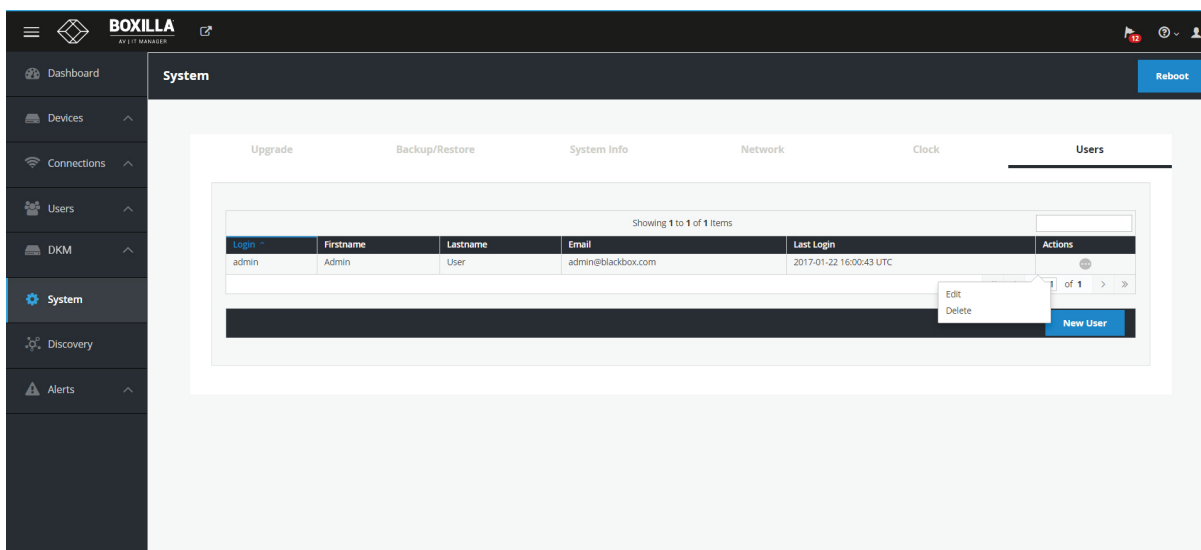
FIGURE 118. SYSTEM USERS
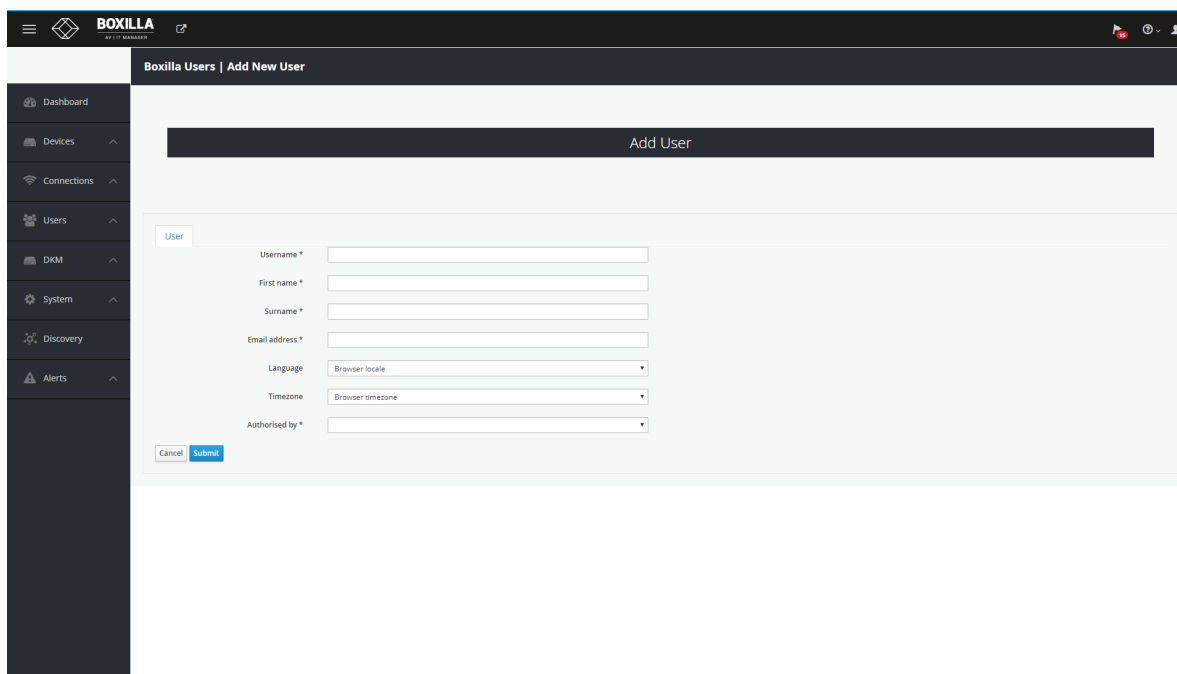
FIGURE 119. NEW SYSTEM USER

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.

NEED HELP?
LEAVE THE TECH TO US
**LIVE 24/7
TECHNICAL
SUPPORT**
1.877.877.2269

CHAPTER 12: 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

NEED HELP?
LEAVE THE TECH TO US
**LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269**

CHAPTER 12: ALERTS

12.1 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 120.
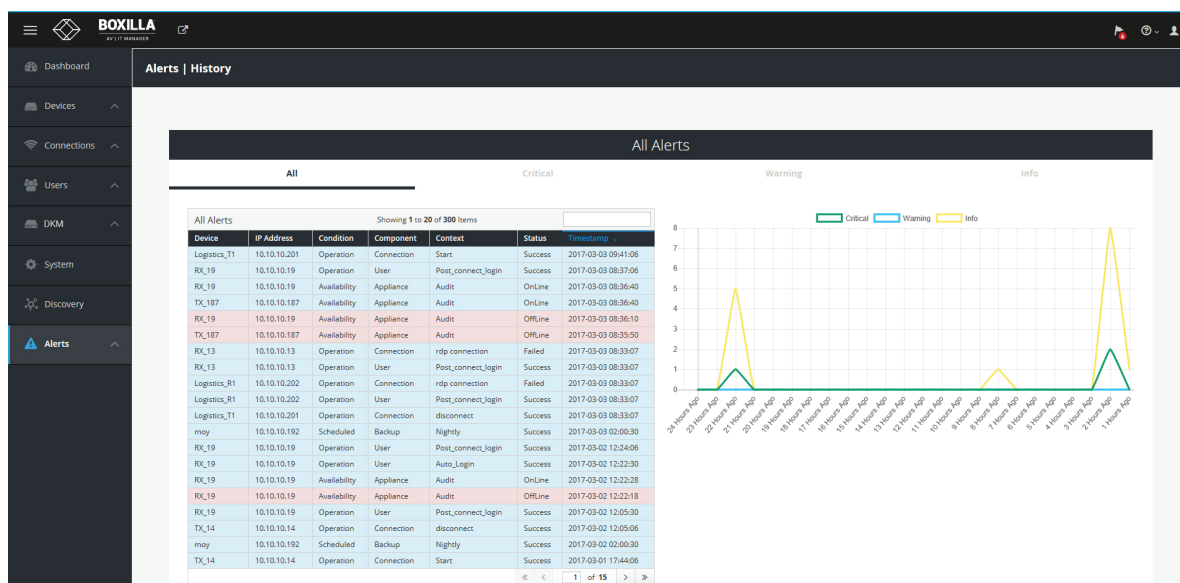
FIGURE 120. ALERTS HISTORY

12.2 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.

CHAPTER 13: DASHBOARD

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

The dashboard is divided into three main areas: Status & Performance Indicators, Active Connections and Active Logins.

13.1 STATUS AND PERFORMANCE INDICATORS

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.

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.

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 10.4. 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.

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

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.

13.2 ACTIVE CONNECTIONS

The Active Connections section of the dashboard displays the currently active connections 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 invest sort order. The filter box at the top right of the table will filter the table based on the filter box contents.

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 <35 Mbps when playing a 1080p video.
- 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.
- 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.

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.

NEED HELP?
LEAVE THE TECH TO US

LIVE 24/7
TECHNICAL
SUPPORT

1.877.877.2269

13.3 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
- Active Logins—all current active logins
- Successful Logins—all Successful logins, both currently active logins and previous ones
- Refused Logins—all refused logins

The graph part of the Active Logins dashboard displays a graph of the selected tab information over time.

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

APPENDIX A: 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 11.4.

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. Upload and Activate Certificates to the new Boxilla unit, if required.

7. Restore a backup file of the original Boxilla database to the new device.

8. Navigate to Devices | Settings page, and all devices should appear as OnLine after 10 seconds.

9. The replacement Boxilla unit is now operational.

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

APPENDIX B: BOXILLA AND TX/RX PROTOCOLS

OVERVIEW

Emerald or InvisaPC uses standard IP protocols for communication between Receivers and Transmitters. Port 3389 is used for unicast communications.

For management purposes, some other ports are used. The Black Box Discovery protocol uses UDP Multicast Group 224.0.1.249 (port 39150). This is sent by the Manager to discover Emerald or InvisaPC devices in the network. The router must allow UDP Multicast forwarding to allow devices on a subnet different than where the Manager is located to be discovered.

Emerald or InvisaPC devices respond to the discovery multicast by sending a UDP unicast back to the Manager IP address on the same port (Port 39150).

Once an Emerald or InvisaPC device is part of the managed domain, the Manager periodically "audits" the device to determine information such as is the device on-line, who is logged into device, device statistics, etc. These audit requests and responses are unicast UDP to specific IP addresses (responses are sent back to Manager's IP address) on port 39150.

On power-up, a Transmitter sends out a "here I am" multicast message on multicast group 225.0.0.37 on port 12345.

Boxilla periodically retrieves device statistics using Port 8888.

Also port 22 and port 443 are used for some manager to appliances communications.

Port 8000 is also used for communications.

NEED HELP?
LEAVE THE TECH TO US
**LIVE 24/7
TECHNICAL
SUPPORT**
1.877.877.2269

APPENDIX C: REGULATORY INFORMATION

C.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.

C.2 SAFETY AND EMC APPROVALS AND MARKINGS/PATENT INFORMATION

C.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.

C.2.2 PATENT INFORMATION

This product contains patented designs and is protected by U.S. and international patents and patents pending.

1.877.877.2269   BLACKBOX.COM

NEED HELP?
LEAVE THE TECH TO US

**LIVE 24/7
TECHNICAL
SUPPORT**

1.877.877.2269

APPENDIX D: DISCLAIMER/TRADEMARKS

D.1 DISCLAIMER

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.

D.2 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.

NEED HELP?
LEAVE THE TECH TO US

LIVE 24/7
TECHNICAL
SUPPORT

1.877.877.2269

NEED HELP?
LEAVE THE TECH TO US
LIVE 24/7
TECHNICAL
SUPPORT
1.877.877.2269

NEED HELP?
LEAVE THE TECH TO US

**LIVE 24/7
TECHNICAL
SUPPORT**

1.877.877.2269

NOTES

NEED HELP?
LEAVE THE TECH TO US
**LIVE 24/7
TECHNICAL
SUPPORT**
1.877.877.2269