NETWORK TECHNOLOGIES INCORPORATED
1275 Danner Dr Tel:330-562-7070
Aurora, OH 44202 Fax:330-562-1999
www.networktechinc.com

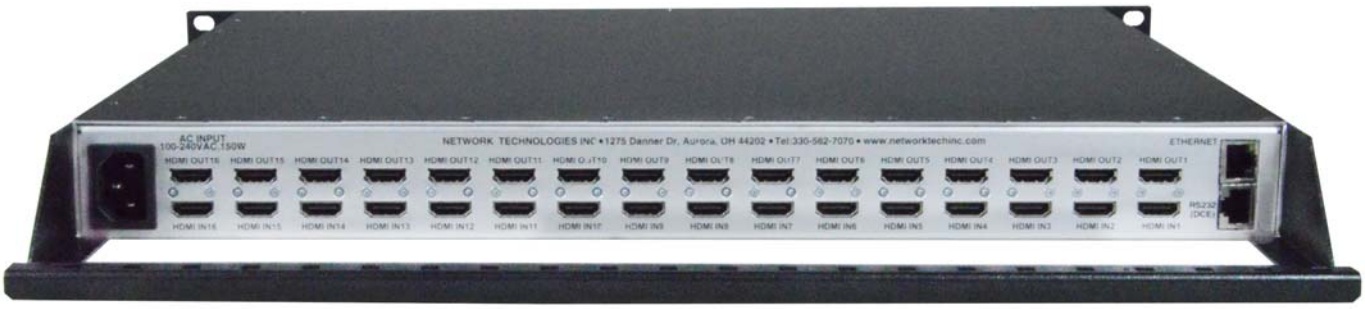
VEEMUX® Series

SM-16X16-HD4K

HDMI 4K Video Matrix Switch

Installation and Operation Manual

Front and Rear View of SM-16X16-HD4K



Rear View of SM-16X16-HD4K with cable tray installed

TRADEMARK

COPYRIGHT

CHANGES

The material in this guide is for information only and is subject to change without notice. Network Technologies Inc reserves the right to make changes in the product design without reservation and without notification to its users.

FIRMWARE VERSION

Current Firmware version 1.5

TABLE OF CONTENTS

TABLE OF FIGURES

INTRODUCTION

The VEEMUX HDMI 4K Video Matrix switch (VEEMUX) provides non-blocking access to 16 4k x 2k video sources from 16 displays. Locate computers up to 20 feet away from 4K @ 60Hz displays or 50 feet from 1080p @ 60Hz displays, enabling easy access to multiple servers in various locations. Cables longer than 50 feet can be used for 1080p displays provided they have the built-in digital video equalizer (also known as an "active HDMI cable").

Application Note: Greater distances can be achieved using an ST-C64K-300 Video Extender supporting up to 4K@30hz. The ST-C64K-300 does not support HDMI2.0 and HDCP2.2. Be sure the video source connected is providing a 4K@30Hz signal for the ST-C64K-300 extender to work.

Features:

- Configure and control the switch through serial port, front panel buttons, web interface, or optional infrared control.
- Supports HDMI interface for crisp and clear video quality on flat panel displays.
- Supports HDMI operation up to 18 Gb/second
- Resolutions to 3840x2160 (UHD), and 4096x2160 (4K) @ 60Hz / RGB/YCBCR 4:4:4.
    - Supports up to 12 bits deep color.
    - Supports 4:4:4, 4:2:2 and 4:2:0 pixel encoding.
- EDID learning for the support of any HDMI display device.
- Built in default EDID configuration tables for 1080p and 4K resolution.
- Each output provides one video signal.
- Each input can be independently connected to any or all outputs.
- Up to 16 users (including “root”) can be configured to control the VEEMUX from the Web Interface
- HDMI 1.4 and 2.0 compatible.
- HDCP 1.4 and 2.2 support.
- Passes embedded audio.

Supported Web Browsers

Most modern web browsers should be supported. The following browsers have been tested:

- Microsoft Internet Explorer 6.0 or higher
- Microsoft Edge 86 or higher
- Netscape 7.0 or higher
- Mozilla FireFox 40 or higher
- Google Chrome 9.0.5 or higher
- Apple Safari 5.0.3 or higher
- Opera 11.0 or higher

Set your browser to always check if there is a newer version of the page than the version stored in cache. This action will ensure that it will display the most up-to-date information.

MATERIALS

Materials supplied with this kit:

- NTI SM-16X16-HD4K HDMI 4K Video Matrix Switch
- Power Cord- country specific
- CT6182 DB9 Female-to-RJ45 Female adapter
- CB4352- 5 foot CAT5 patch cable
- 4pcs #10-32 x 3/4" pan head screws and #10-32 cage nuts (server cabinet mounting hardware)
- 36 pcs zip ties

Materials *Not* supplied but *REQUIRED:*

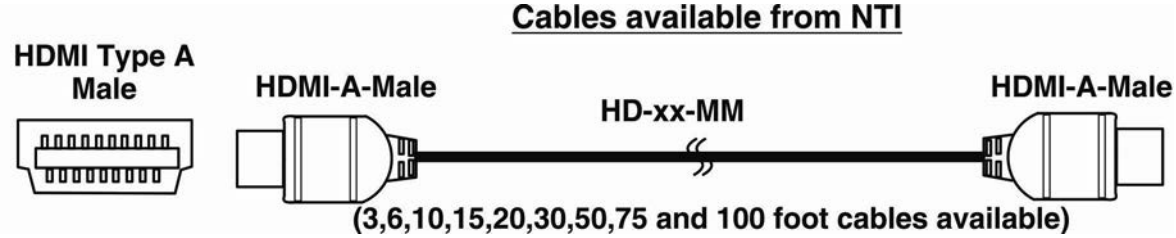
- HD-xx-MM cable for each 4K monitor being connected to the switch and for each PC being connected- available in 3, 6,10, 15,20,30,50,75 and 100 foot lengths

where:

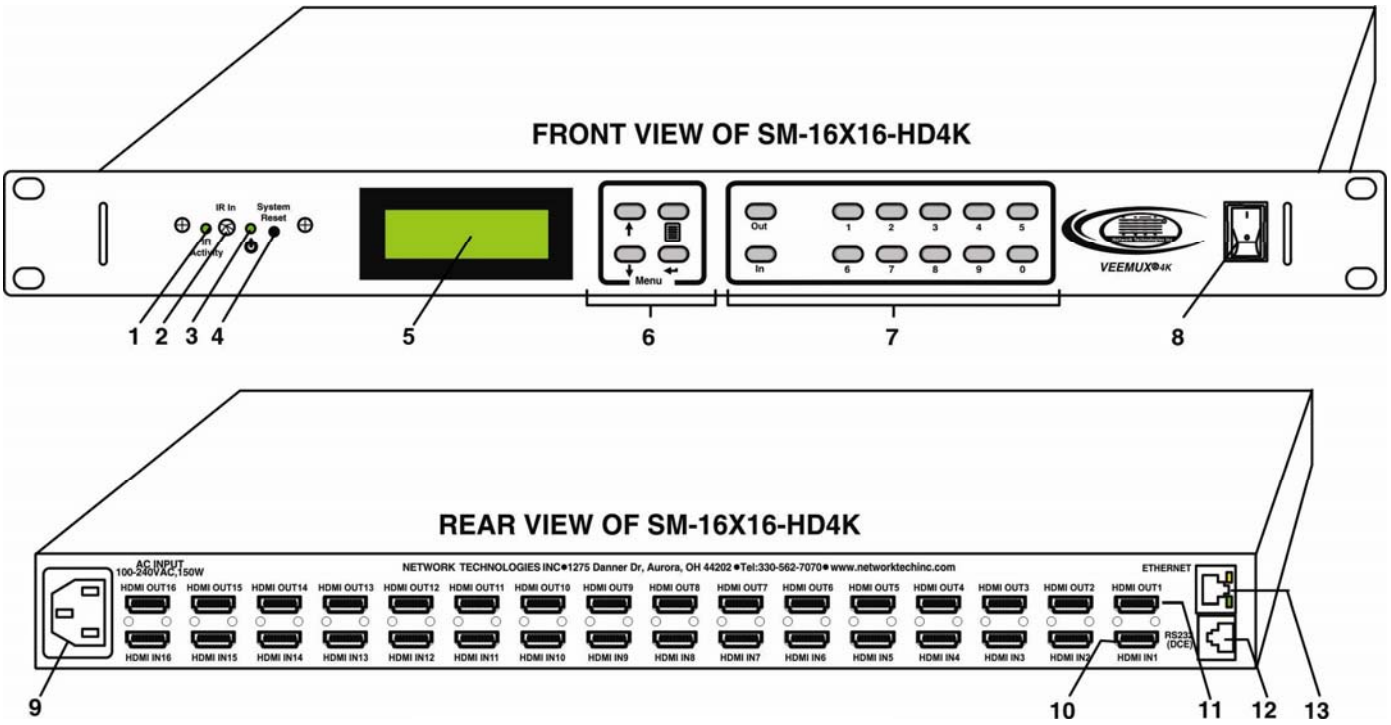
xx is the length of the cable in feet
MM indicates male-to-male connector

Note:

- HD-3/6/10/15/20-MM supports resolutions to 4Kx2K.
- HD-30/50/75/100-MM supports resolutions to 1080p.
    - HD-75/100-MM have a built-in digital video equalizer for extending HD signals up to 1080p at 60Hz. These cables are directional, with one plug end marked for the display.



FEATURES AND FUNCTIONS



(Rear view shown without cable tray)

Item	Type	Description
1	**IR LED**	For indicating when an infrared signal is being received from the IR remote control
2	**IR Receiver**	this receives the IR signal from the infrared remote control (IRT-UNV sold separately)
3	**Power/Standby LED**	Indicates when the VEEMUX is either ready for user interface (green) or in standby mode (red)
4	**System Reset button**	press this button to cycle the VEEMUX processor and reboot the system
5	**LCD Display**	indicates what inputs (video sources) are connected to the labeled output (display device
6	**Menu buttons**	Used to control LCD menu navigation
7	**Out and In buttons**	Used to select which outputs (display devices) to connect to which inputs (video sources) when pressed
8	**Power Switch**	To control the ON/OFF function of the switch
9	**IEC Connector**	For attachment of country-specific power cord
10	**HDMI Female**	For connecting to HDMI video sources
11	**HDMI Female**	For connection of HDMI display devices
12	**RJ45 Female**	RS232 (DCE) connection for attachment of RS232 control cable
13	**RJ45 Female**	For connection of CATx cable to Local Area Network (LAN) for WEB interface

INSTALLATION

This NTI switch was designed to be mounted to a rack. It includes rack mount flanges to make attachment to a rack easy and a cable tray to easily secure attached cables to prevent disconnection.

To Mount to a Rack

1. Install 4 cage nuts (supplied) to the rack in locations that line up with the holes in the mounting flanges on the NTI switch.

2. Secure the NTI switch to the rack using four #10-32X3/4" screws (supplied). Each screw should be of sufficient length to go completely through the NTI mounting flange, rack frame and fully engage all threads in the cage nut. Be sure to tighten all mounting screws securely.

3. Attach all cables securely to the switch and where necessary supply adequate means of strain relief for cables.

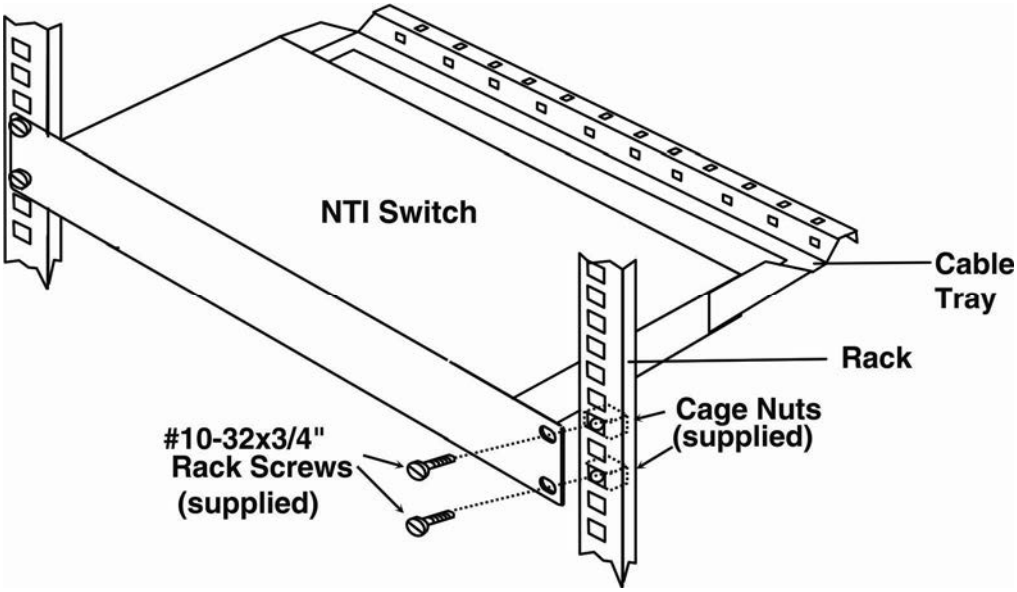


Figure 1- Secure switch to a rack

Make All Connections

1. Connect a HDMI male cable between each video source and an “HDMI INx” connector on the rear of the VEEMUX.

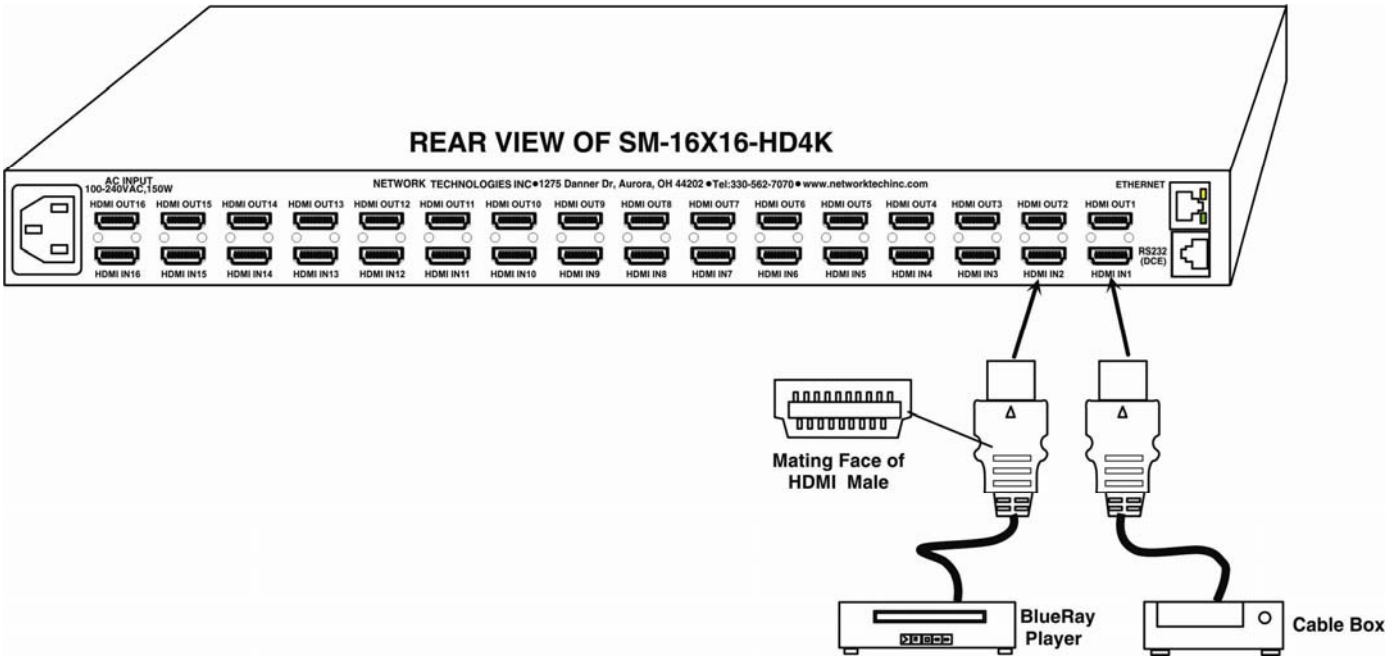


Figure 2- Connect video sources to VEEMUX

2. Connect a HDMI male cable between each display device and an “HDMI OUTx” connector on the rear of the VEEMUX.

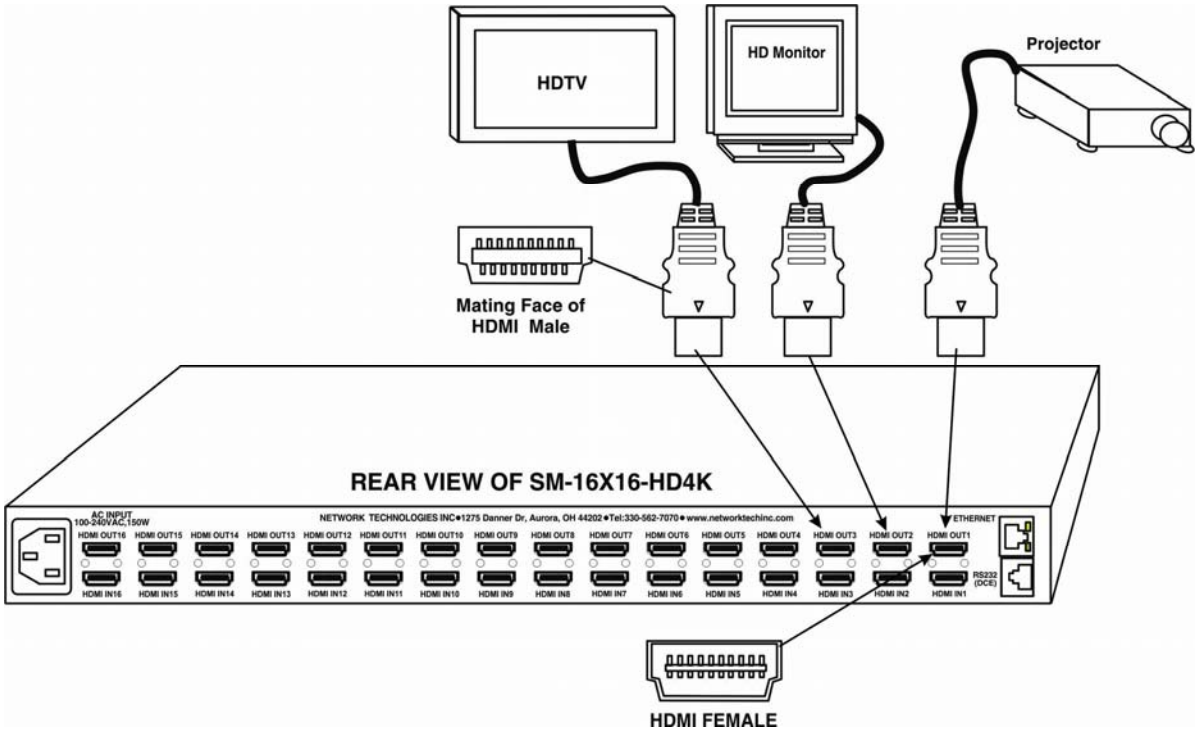


Figure 3- Connect display devices to VEEMUX

3. If the VEEMUX will be controlled using RS232, then make a connection between the “RS232” port on the VEEMUX and a serial port on a PC. A DB9M-to-RJ45F adapter and 5 foot CAT5 patch cable have been provided to help with this connection if needed.

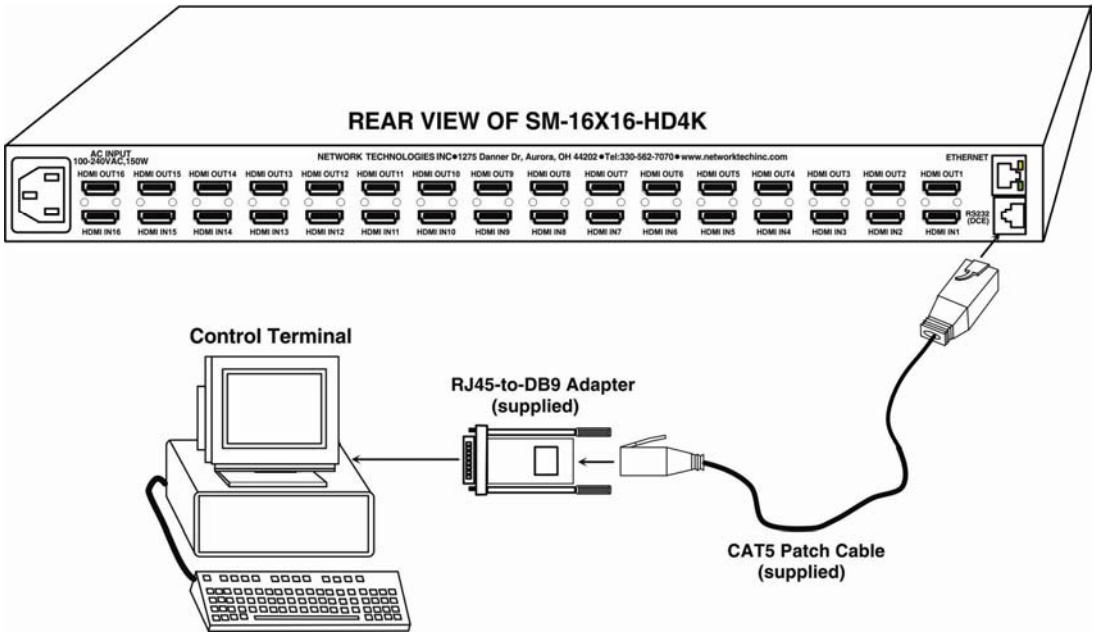


Figure 4- Connect RS232 control terminal to VEEMUX

4. To make a remote connection, over the Ethernet, from anywhere on the local area network, connect a CAT5/5e/6 Ethernet cable with RJ45 male connectors on the ends, wired straight through (pin 1 to pin 1, pin 2 to pin 2, etc.).

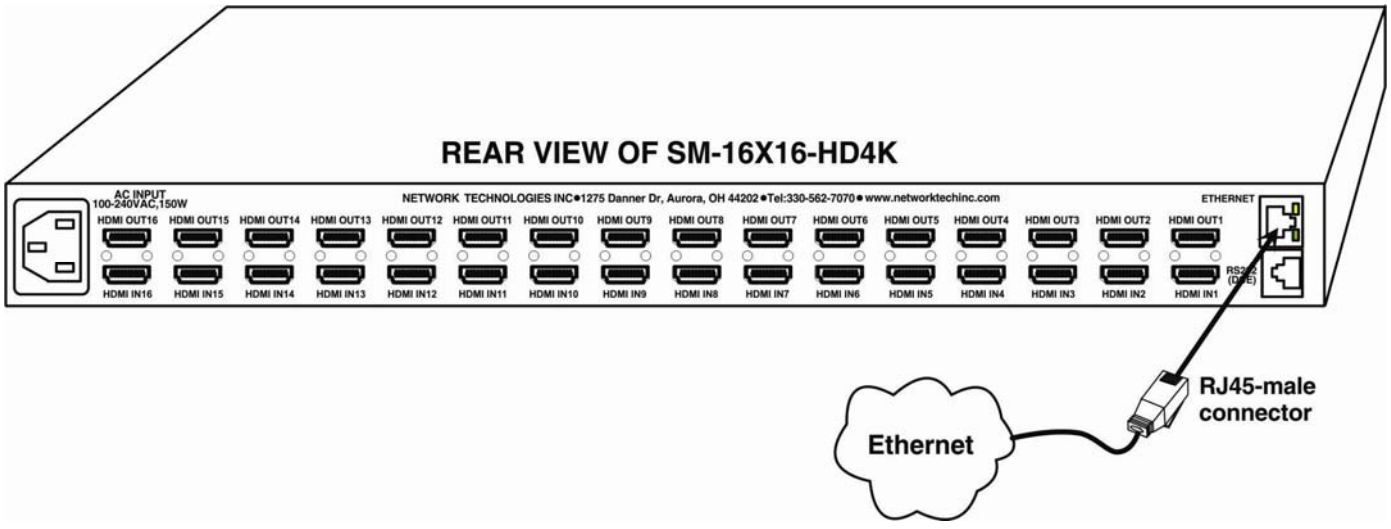


Figure 5- Connect VEEMUX to local area network

5. Connect the powercord to the VEEMUX and plug it in.

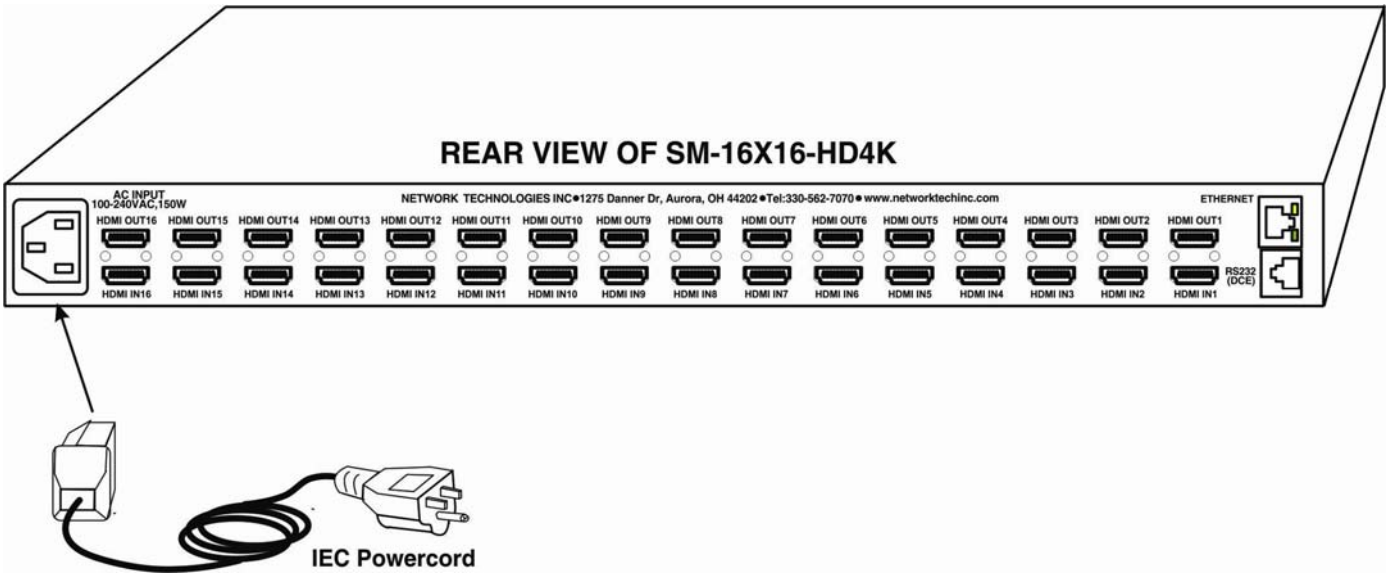


Figure 6- Attach AC power cord to VEEMUX

6. Power ON all components. (In any order, which ones are first and which are last does not matter.)

OPERATING THE VEEMUX

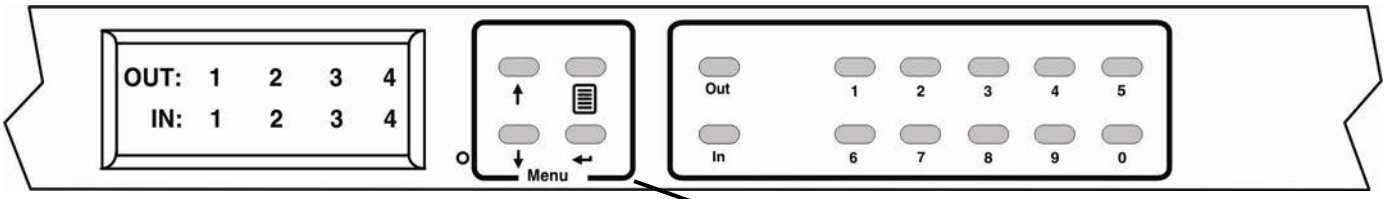
The VEEMUX video matrix switch has four methods of control:

- Front Panel LCD with Keypad
- Directly via an RS232 Interface
- Remotely via Ethernet
- Infrared Remote

Every unit comes standard with all control methods built-in. An IRT-UNV-IR Remote Control is required to use the Infrared option. No software is involved (see Infrared Control on page 41). With the RS232 option, there are no external devices to be purchased. NTI provides software commands as well as a test program to ensure the RS232 functions properly (see page 11 – RS232 Control).

Front Panel LCD with Keypad Control

The front panel LCD and keypad allow the user to monitor switch status and route any user to any video source on the switch. When the unit is first powered-up, each monitor is automatically connected to the video source of its equal number (i.e. monitor 1 to source 1, monitor 2 to source 2, monitor 3 to source 3, etc.). (After configurations have been saved (page 24), upon power-up the VEEMUX will load the configuration saved into memory location 0.) Along with the routing of the inputs (video sources) to the outputs (monitors) the keypad and LCD allow the users to configure the RS232 control interface. The keypad buttons perform the following functions:



Key Functions:

Up Arrow- Scroll up the menu

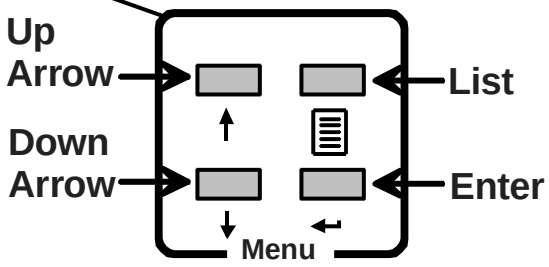
Down Arrow- Scroll down the menu

Left Arrow (Enter Key)- Select the menu item

List - Open the menu, or exit the menu (also used to back out of the menu, one step at a time)

Out-1- through 16 Used in command sequence to select which output (display device) to connect

In-1-though 16 Used in command sequence to select which input (video source) to connect



To quickly change a connection, simply press the associated port number and then the "In" or "Out" button to designate the video source or the display (respectively). Alternatively, the "In" or "Out" button can be pressed, then the port number, followed by the "Enter" button.

Multiple displays can be connected to a single video source using one command sequence:
<**In**> xx<**Out**>xx<**Out**>xx<**Out**>xx<**Out**>xx<**Enter**> or
<**Out**>xx<**Out**>xx<**Out**>xx<**Out**>xx <**In**> xx <**Enter**> (where xx is the port number)

To configure the VEEMUX, use the Menu keys.

Press the **List** button to list your main menu options:

1- Serial
2- Ethernet
3- DDC
4- Standby
5- Save Config
6- Load Config

Use the **Up** and **Down Arrow** keys to scroll through this list.
Use the **Enter** Key to select a menu item.
Press the **List** button again to exit the menu.

If, while in a menu, you pause for more than 5 seconds, you will automatically exit the menu.

LCD Menus

Serial Menu

Under the "Serial" menu are two parameters:

1- Baud rate
2- Address

These parameters are used when the VEEMUX is controlled through an RS232 connection (page 11). If you select Baud rate, use the arrow keys to toggle through the available baud rates. The baud rate can be set to 115200, 57600, 38400, 19200, 9600, 4800, 2400, or 1200.

If you select Address, use the arrow keys to toggle through the address options (01-15). This is also the switch address used in conjunction with the IR Remote operation (page 45).

Ethernet Menu

Under "Ethernet" menu are several parameters:

1- Mode
2- IP Address
3- Mask
4- Gateway
5- Pref. DNS
6- Alt. DNS

The Mode parameter will let you select between a manual IP setting, a DHCP assigned dynamic IP address setting, or disabling the Ethernet port. An asterisk indicates which mode is configured, an arrow shows which mode is being selected. To change the configured setting and move the asterisk, select the desired mode and press the **Enter** button.

If you choose a manual IP setting, the IP parameter provides the fields for entering a valid IP address. Use the up and down arrows to advance the numbers, and the **Enter** button to move from field to field. Press **List** to exit this screen.

Selections 3, 4 are necessary to apply valid values for your Subnet Mask and Gateway. Navigate these settings as described for setting the IP address.

Selections 5 and 6 are not used at this time and are therefore unnecessary.

DDC Menu

DDC enables the video source to get EDID information from the display device. This enables the video source to automatically select the optimal resolution for the display by receiving, at power up, information from the display device concerning its resolution specifications.

Under the "DDC" menu are five parameters:

1- Chose Input (Choose Input)
2- All Inputs
3-FacDefault1
4-UsrDefault1
5-ReloadOptn

1) Choose Input- select the EDID information source for each input individually, or
2) All Inputs- select EDID information source for all inputs at once.
Within these sections you will need to select between:
default 1- the inputs will get EDID information from a predefined table in the VEEMUX supporting 1080p resolution
default 2- the inputs will get EDID information from a predefined table in the VEEMUX supporting UHD resolutions
From Out (?)- select which Output port the Input will get EDID information from regardless of which output it is connected to
DDC Mix(?)- select which Input will receive EDID information that is common to the Outputs selected on the "DDC Mix" page (page 36) for that input

3) FacDefault1- Select this to use the factory default EDID data for DDC "Default 1" configuration
4) UsrDefault1- Select this to replace the EDID information stored in the VEEMUX for "Default 1" with the EDID data from the monitor presently connected to Output 1.
5) ReloadOptn- Select this and choose to **enable** or **disable** this feature. When enabled, the switch will refresh DDC data stored in the VEEMUX each time the VEEMUX is power-cycled. The DDC data will be based on the current DDC configuration settings.

Standby

The fourth option in the main menu is "Standby". When Standby is selected, the VEEMUX switch will immediately go into a power saver mode and the LCD display will go blank. It will remain in this state until

1) any button is pressed on the front panel,
2) the Standby button is pressed on the optional IR Remote Control (page 42), or
3) the "Disable Standby" button is pressed in the web interface (page 38)

Save and Load (Recall) Config

The SM-16X16-HD4K includes the ability to save and recall up to 100 switch configurations using the LCD menu. The switch configurations define the current port connections, volume control settings, and video blank status.

Note: The IRT-UNV IR Remote (page 41) can also be used to access these configurations by using the "SAVE" and "RECALL" buttons.

To save a configuration, select "Save Config" from the main menu followed by a numeric button(s) (0-99) corresponding to the memory slot the configuration is to be saved in. Press **Enter** after your selection to force the current configuration to immediately be saved to the selected memory slot.

Configurations can be loaded (recalled) in much the same manner. To recall, select "Load Config" from the main menu followed by the numeric button(s) (0-99) corresponding to the memory slot from which the configuration is to be recalled. Press **Enter** after your selection to immediately force the switch to change the current switch configuration to match that of the configuration recalled.

RS232 CONTROL

RS232 enables the VEEMUX to be remotely controlled via RS232. To control the VEEMUX via RS232 the user has four options:

- write a program that runs on a PC using the Command Protocol (page 12)
- use the Matrix Switcher's Control Program (page 13)
- use the SerTest program (page 14)
- Remote Connection

The RS232 Interface is designed to meet the RS232C standard and can be controlled from any CPU or other controller with an RS232 communications port. The pin-out for the RJ45 connector on the unit is as follows:

RS232 (RJ45) CONNECTOR

PIN	SIGNAL	FUNCTION
1	-	No connection
2	-	No connection
3	RX+	Receive data (TXD at host)
4	GND	Ground
5	-	No connection
6	TX+	Transmit data (RXD at host)
7	-	No connection
8	-	No connection

A 5 foot patch cable and adapter, RJ45-to-DB9, have been provided for connection to most CPUs (see page 6).

Baud Rate

The baud rate can be changed by selecting MENU on the front panel keypad, using the OSD menu, using Telnet commands (page 16) or from the RS232 commands (page 12). The baud rate can be set to 115200, 57600, 38400, 19200, 9600, 4800, 2400, or 1200. A data protocol of 8 data bits, no parity, and 1 stop bit is used for communications. The default baud rate setting is 9600.

Command Protocol

CPU controller commands supported by the unit are defined below. All commands must be terminated with a <CR> (carriage return). When a command is sent, the entire string is echoed back along with a response from the addressed unit as shown in the Command Definitions table (below). All characters in the command string are case sensitive (see Command Definitions table), and all numbers below 10 must have a leading 0 (ex: 1 = 01).

Legend:

(All numbers must be two digits)

SW	:	Switch (01-15)	MM	:	Save Into Memory Bank (00-99)
BR	:	Baud Rate Code	LL	:	Load From Memory Bank (00-99)
OP	:	Output Port (01-MAXOUTPUTS)	<CR>	:	Carriage Return (Hex 0xD)
IP	:	Input Port (01-MAXINPUTS)	ip	:	IP address

Command Definitions

Command String	Good Response	Description
CS *SW,IP,OP*	*<CR>	VIDEO Connect One Output/User Port To Input/CPU Port
CA *SW,IP*	*<CR>	VIDEO Connect All Output/User Ports To Input/CPU Port
RO *SW,OP*	*<CR>*IP*<CR>	VIDEO Read Connection For Output/User Port
VB *SW,OP*,01	*<CR>	Blank the video for specific Output/User Port
VB *SW,OP*,00	*<CR>	Unblank the video for specific Output/User Port
CC *SW,MM*	*<CR>*MM*<CR>	Save Matrix Connections Into Memory Bank xx Xx=00-99
RC *SW,LL*	*<CR>LL<CR>	Restore Matrix Connections From Memory Bank
CB 00,*BR*	None	Change baud rate of serial line, BR=11(5200),57(600),38(400),19(200)96(00),48(00),24(00),12(00) Factory default is 9600
RS *SW*	*<CR>	Reboot Unit
RV *SW*,00	*<CR>string\0<CR>	Read NTI Version String
RU *SW*	*<CR>*IP,OP*<CR>	Read Unit Size
EA *SW,ip*	*<CR>	Set the IP address, ip is in xxx.xxx.xxx.xxx format, number of digits is minimum 1 and maximum 3 for each field Leading zeroes are accepted
EM *SW,ip*	*<CR>	Set the Subnet mask, ip is in xxx.xxx.xxx.xxx format, number of digits is minimum 1 and maximum 3 for each field. Leading zeroes are accepted
EG *SW,ip*	*<CR>	Set the default gateway, ip is in xxx.xxx.xxx.xxx format, number of digits is minimum 1 and maximum 3 for each field Leading zeroes are accepted
ET *SW*,timeout	*<CR>	Set the website timeout; timeout = numeric string of timeout in seconds. Values: 60, 300, 600, 900, 1800, 3600, 7200, 18000, 28800
RA *SW* *	<CR>*ip*<CR>	Read the IP address, ip is in xxx.xxx.xxx.xxx format, number of digits is minimum 1 and maximum 3 for each field Leading zeroes are accepted
RM *SW* *	<CR>*ip*<CR>	Read the Subnet mask, ip is in xxx.xxx.xxx.xxx format, number of digits is minimum 1 and maximum 3 for each field Leading zeroes are accepted
RG *SW* *	<CR>*ip*<CR>	Read the default gateway, ip is in xxx.xxx.xxx.xxx format, number of digits is minimum 1 and maximum 3 for each field Leading zeroes are accepted
RT *SW* *	<CR>timeout<CR>	Read the website timeout; timeout = numeric string of timeout in seconds. Values: 60, 300, 600, 900, 1800, 3600, 7200, 18000, 28800
SS *SW*,00	*<CR>	Disable Autostatus feature (see below)
SS *SW*,01	*<CR>	Enable Autostatus feature (see below)
GO *SW*,OP	*<CR>go *SW,OP:IP*<CR>	Read connection of a Video Output Port to Video Input Port
GM *SW*,00	*<CR>go *SW,OP:IP* (all ports)<CR>	Read connection matrix of all Video Output ports

If the first field is not a known command (as listed above) or SW field is different from the serial address programmed in the switch memory, the command will be ignored. If the SW field corresponds to the unit address, but the syntax is wrong after this field, the switch will answer with a bad response ?<CR>.

Autostatus

When Autostatus is enabled, any output-to-input connection change in the VEEMUX will cause an Autostatus message to be sent via RS232 to the administrator. The format of the message would be "pc SW,OP:IP<CR>"

Example of an Autostatus message:

pc 01,01:04<CR>

which means "At the switch with unit address 01, the output (01) has changed connection to input 04."

Notes: Message to the administrator will be delayed by any RS232 traffic being received by the switch from the administrator.
Autostatus must be disabled before using SerTest or the Matrix Switcher's Control Program (page 13).

By default, Autostatus is disabled and must be manually enabled. Autostatus is also disabled any time the power to the VEEMUX is interrupted.

NTI Switch Control Program For Windows 9X, NT, 2000, XP, Vista, 7, 8,10 and 11

The NTI Switch Control Program is an easy and powerful graphical program that controls NTI matrix switches through an RS232 interface. The NTI Switch Control Program is downloaded from http://www.networktechinc.com/download/d-vmtx-dvi.html.

To install the Program after downloading

1. Locate the ***Setup.exe*** in the directory the program was downloaded to and double-click on it
2. Follow the instructions on the screen

The NTI Switch Control Program performs best on monitors set to a screen resolution of at least 800 X 600. Instruction for using the NTI Switch Control Program is available by opening "MSCP Help" in the "NTI" program group once the program has been installed and is open on the screen.

To open "MSCP Help" from the Windows desktop

1. Click on **START**
2. Click on **PROGRAMS**
3. Click on **NTI**
4. Click on **MSCP Help**

Note: While in Scan Mode, the video radio buttons shown on the Switch page of the NTI Switch Control Program may not be in sync with the connection changes within the VEEMUX. Connections will change without updating the image on the screen.

SerTest- RS232 Interface Test Program

This software allows a user to test the functions of an NTI server switch, matrix switch or Multi-user/Multi-platform switch RS232 interface. The SerTest program is automatically loaded when installing the NTI Switch Control Program as described above. The SerTest program, located in the NTI program group, generates a main menu with the 4 selections described below:

Main Options

- Matrix Operations - send commands to the matrix unit.
- Ethernet Operations - set Ethernet connection variables
- Setup Options - set COM port, baud rate, and unit address
- About SerTest - display the program version

Matrix Operations

Key	Selection	Description
1)	Connect Video Output/User to an Input/CPU	- connect an output to an input
2)	Connect All Video Outputs/Users to an Input/CPU	- connect all outputs to an input
3)	Connect Audio Output/User to an Input/CPU	- connect an output to an input (audio ports only)
4)	Connect All Audio Outputs/Users to an Input	- connect all outputs to an input (audio ports only)
5)	Change Mute Status for Audio Output/User	- mute or un-mute the Audio port output
6)	Change Volume for Audio Output/User	- change Audio port output volume
7)	Read Connection for Video Output/User	-read the connection of a specific video output
8)	Read Connection for Audio Output/User	-read the connection of a specific audio output
9)	Read Mute and Volume for Audio Output/User	- read the volume and the mute status of the specified output (audio ports only)
a)	Save I/O Connections into Unit Memory	-save the connections into switch memory bank
b)	Restore I/O Connections from Unit Memory	-restore the connections from switch memory bank
c)	Change All Units Baud Rate (9600/COM1:)	-change RS-232 Baud rate of all switches -the current baud rate and serial port are displayed in parentheses
d)	Reset Unit	- send a reset (reboot) command to the switch - the current unit address is displayed in parentheses
e)	Reset All Units	- send an internal reset command to all switches
f)	Read Unit Size	- read the switch size (number of inputs and outputs)
g)	Read Unit Version/Revision String	-read a string containing the switch version, type, and size
h)	Save All Units I/O Connections into Units Memory	-save the connections into switch memory bank, command for all switches
i)	Restore All Units I/O Connections from Units Memory	-restore the connections from switch memory bank, command for all switches

Grayed keys are not applicable to this product

Ethernet Operations

Key	Selection	Description
1)	Set Unit IP Address	- enter the desired IP address in xxx.xxx.xxx.xxx format - number of digits is minimum 1 and maximum 3 for each field. Leading zeroes are accepted
2)	Set Unit Subnet Mask	- enter the desired IP address in xxx.xxx.xxx.xxx format - number of digits is minimum 1 and maximum 3 for each field. Leading zeroes are accepted
3)	Set Unit Default Gateway	- enter the desired default gateway - number of digits is minimum 1 and maximum 3 for each field. Leading zeroes are accepted
4)	Set Unit Website Timeout	- set the website timeout; timeout = numeric string of timeout in seconds - Values: 60, 300, 600, 900, 1800, 3600, 7200, 18000, 28800 0 = no timeout
5)	Read Unit IP Address	- read the unit IP address in xxx.xxx.xxx.xxx format
6)	Read Unit Subnet Mask	- read the unit subnet mask in xxx.xxx.xxx.xxx format
7)	Read Unit Default Gateway	- read the unit default gateway in xxx.xxx.xxx.xxx format
8)	Read Unit Website Timeout	- read the current website timeout period in seconds - Values: 60, 300, 600, 900, 1800, 3600, 7200, 18000, 28800 0 = no timeout

Setup Options

Key	Selection	Description
1)	select Com port current: (COM1:)	- select PC serial port - the current PC serial port is displayed in parentheses
2)	select Baud rate current: (9600)	- select PC serial port baud rate - the current baud rate is displayed in parentheses
3)	set unit Address current: (1)	- select the unit address - the current address is displayed in parentheses
4)	set read timeout (5)	- select the time period (in seconds) the SerTest will wait for an answer to a command - the current time period is displayed in parentheses

For any selection that requires user input, the user is prompted. When commands are sent to the matrix unit, the command string and matrix unit responses are echoed to the screen. All commands generated by the program are formatted according to the information provided in sections above. If any transmission problems are detected, an error message is displayed.

Press <**Esc**> or <**Enter**> to back out to the main menu and press again to exit.

ETHERNET CONTROL

Telnet Interface-Port 2000

The Telnet Interface enables the user to control the switch using telnet client through an Ethernet connection. The telnet server (telnet must be enabled- see page 26) listens on ports 2000 and 2005. Port 2000 is for an operator telnet session while port 2005 is intended for a software control type session (see page 18 for more on Port 2005 control). For operator telnet control using the telnet interface and the current IP address, type the following in a command shell:

telnet 192.168.1.30 2000 (for Port 2005 control, substitute "2005" for "2000" in this command)

The VEEMUX will prompt the user for a password. The user must enter the password followed by <Enter>.

The factory default password is **"nti".**

Since Port 2005 control is initiated via software from a controller, rather than manually, the password requirement is not part of the command sequence.

With a proper password sent the VEEMUX will respond with:

Password Successful
Connection Established

The commands below are now available.

Telnet Interface- Port 2000 Commands

Command	Reply	Description
H(elp) or h(elp)	Displays the list of commands	Help
CS nn,mm	*<CR>	Connect One input nn To output mm
CA nn	*<CR>	Connect All Outputs To Input nn
RO mm	*<CR>nn<CR>	Read Connection For Output. Returns the number of the input nn connected to output mm
CC nn	*<CR>nn<CR>	Save Matrix Connections Into Memory Bank nn nn should be between 00 and 99
RC nn	*<CR>nn<CR>	Restore Matrix Connections From Memory Bank nn nn should be between 00 and 99
CB nn	*<CR>	Change baud rate of serial line, nn=12(00),24(00),48(00),96(00) Factory default is 9600.
RV 00	*<CR>string<CR>	Read NTI Version String
RU	*<CR>nn,mm<CR>	Read Unit Size Returns the number of inputs nn and the number of outputs mm
RS	*<CR>	Reboot Unit
Ss nn,dwt	*<CR>	Set value of Scan Mode dwell time (see page 9) for specific Output (nn) dwt = 000-255 (seconds) 000= disable Scan Mode

Command	Reply	Description
Gs nn	*<CR> dwt<CR>	Read set Scanning Sequence dwell time value (dwt) for specific Output (nn) in seconds (see also "Scanning Sequences" on page 31)
Sa nn,mm	*<CR>	Set scan list of individual output nn to all inputs mm
Sc nn	*<CR>	Clear scan list of individual output nn
S+ nn,mm	*<CR>	Add input mm to Scan List of output nn
S- nn,mm	*<CR>	Remove input mm from Scan List of output nn
Sx nn	*<CR>oooxoxxxooooxxx<CR>	Display the Scan List of output nn (o=skip x=don't skip)
CP	User is prompted to introduce the password twice	Change password- five (5) characters minimum
<Ctrl>-<X> (see note 4 below)	Good Bye. Connection to host lost.	Quit telnet session
H(elp) or h(elp)	Displays the list of commands	Help

Notes:

1. ***The commands must be typed exactly as shown in the chart. The commands are case sensitive.***
2. ***If a mistake is made, the user must backspace to the beginning and completely retype the command.***
3. ***If a command is sent that the VEEMUX does not recognize or exceeds the configuration of the switch, the reply "?" may be received. Check the command syntax and try again.***
4. ***To quit the telnet session, press the keyboard keys <Ctrl><X> + <Enter>.***

Telnet Interface-Port 2005

For a software control type of telnet interface session (versus operator telnet control through port 2000 as described on page 16), connect to the VEEMUX through the current IP address at port 2005. Use the command set below to control and acquire information from the VEEMUX.

Note: After establishing the connection, the unit will answer with a blinking prompt on the next line. If the connection fails it will answer with ?<CR>

Note: When using some controllers (Crestron for example), a slight delay may necessary to be added at the end of each command string.

Legend: (All numbers must be two digits)

OP : Output Port (01-MAXOUTPUTS)
IP : Input Port (01-MAXINPUTS)
<CR> : Carriage Return (Hex 0xD)

Command Summary

Command String	Good Response	Description
RU<CR>	ru IP,OP<CR>	Read unit size
RO OP<CR>	pc OP,IP<CR>	Read connection for OP
CS IP,OP<CR>	*<CR>	Connect OP to IP
CA IP<CR>	*<CR>	Connect all outputs to IP
SS 01<CR>	*<CR>	Enable auto-status mode
SS 00<CR>	*<CR>	Disable auto-status mode
SX<CR>	See details	Examine connections
XX<CR>	*<CR>	Close connection

A <CR> (carriage return, 0x0D) is considered to be the end of the command string. If a string exceeds 16 characters, an end of string will be inserted automatically to avoid buffer overflow. An eventual <LF> (line feed, new line, 0x0A) after a <CR> will be ignored. A bad string will always be responded to with the ASCII character '?' followed by a <CR>.

Note: Always be sure to terminate your telnet session with the <X> - <X> - <Enter> command string.

Command Detail

RU-Read Unit Size

Command:

Byte 1	Byte2	Byte3
'R' (0x52)	'U' (0x55)	<CR> (0x0D)

Response:

Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7	Byte 8	Byte 9
'r' (0x72)	'u' (0x75)	Space (0x20)	Input – 1st digit (0x30…0x32)	Input – 2nd digit (0x30…0x39)	',' (0x2C)	Output – 1st digit (0x30…0x32)	Output-2nd digit (0x30…0x39)	<CR> (0x0D)

This command will read the size of the unit. The response returns the number of inputs and the number of outputs in two-digit, ASCII code format. If the numbers are smaller than 10, the 1st digit is '0'.

RO-Read Connection for Output Port

Command:

Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6
'R' (0x52)	'O' (0x4F)	Space (0x20)	Output – 1st digit (0x30…0x32)	Output – 2nd digit (0x30…0x39)	<CR> (0x0D)

Response:

Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7	Byte 8	Byte 9
'p' (0x70)	'c' (0x63)	Space (0x20)	Output – 1st digit (0x30…0x32)	Output-2nd digit (0x30…0x39)	',' (0x2C)	Input – 1st digit (0x30…0x32)	Input – 2nd digit (0x30…0x39)	<CR> (0x0D)

This command will read the connection of an output port. The response returns the output port that is connected to the input port.

CS- Connect Output Port to Input Port

Command:

Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7	Byte 8	Byte 9
'C' (0x43)	'S' (0x53)	Space (0x20)	Input –1st digit (0x30…0x32)	Input –2nd digit (0x30…0x39)	',' (0x2C)	Output – 1st digit (0x30…0x32)	Output – 2nd digit (0x30…0x39)	<CR> (0x0D)

Response:

Byte 1	Byte 2
'*' (0x2A)	<CR> (0x0D)

This command connects the specified input port to the specified output port.

CA- Connect All Output Ports to Input Port

Command:

Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6
'C' (0x43)	'A' (0x41)	Space (0x20)	Input – 1st digit (0x30…0x32)	Input - 2nd digit (0x30…0x39)	<CR> (0x0D)

Response:

Byte 1	Byte 2
'*' (0x2A)	<CR> (0x0D)

This command connects all output ports to the specified input port.

SS_01- Enable Auto Status Mode

Command:

Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6
'S' (0x53)	'S' (0x53)	Space (0x20)	'0' (0x30)	'1' (0x31)	<CR> (0x0D)

Response:

Byte 1	Byte 2
'*' (0x2A)	<CR> (0x0D)

Auto status mode is disabled by default whenever the connection is established, and this command must be entered to enable it. When auto status mode is enabled, a message will be sent whenever an input/output connection changes from any source. The format of this message is given in the table below. The first two numeric digits are the output port number and the two after the colon are the number of the input port that is now connected to it.

Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7	Byte 8	Byte 9
'p' (0x70)	'c' (0x63)	Space (0x20)	Output – 1st digit (0x30…0x32)	Output – 2nd digit (0x30…0x39)	':' (0x3A)	Input – 1st digit (0x30…0x32)	Input – 2nd digit (0x30…0x39)	<CR> (0x0D)

SS_00- Disable Auto Status Mode

Command:

Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6
'S' (0x53)	'S' (0x53)	Space (0x20)	'0' (0x30)	'0' (0x30)	<CR> (0x0D)

Response:

Byte 1	Byte 2
'*' (0x2A)	<CR> (0x0D)

This command disables auto status mode.

SX- Examine connections

Command:

Byte 1	Byte 2	Byte 3
'S' (0x53)	'X' (0x58)	<CR> (0x0D)

Response:
Multiple lines, one line for each output:

Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7	Byte 8	Byte 9
'p' (0x70)	'c' (0x63)	Space (0x20)	Output – 1st digit (0x30…0x32)	Output – 2nd digit (0x30…0x39)	':' (0x3A)	Input – 1st digit (0x30…0x32)	Input – 2nd digit (0x30…0x39)	<CR> (0x0D)

Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7	Byte 8	Byte 9
'p' (0x70)	'c' (0x63)	Space (0x20)	Output – 1st digit (0x30…0x32)	Output – 2nd digit (0x30…0x39)	':' (0x3A)	Input – 1st digit (0x30…0x32)	Input – 2nd digit (0x30…0x39)	<CR> (0x0D)

Last line:

Byte 1	Byte 2
'*' (0x2A)	<CR> (0x0D)

Terminate telnet session

Command:

Byte 1	Byte 2	Byte 3
'X' (0x58)	'X' (0x58)	<CR> (0x0D)

Response:

Byte 1	Byte 2
'*' (0x2A)	<CR> (0x0D)

The unit will respond with '*'<CR> and close the connection, terminating the telnet session. The unit is then available for future connections.

Web Interface

A user may control the connections of the VEEMUX using a Web Interface via any web browser (see page 1 for supported web browsers). With the VEEMUX connected to a LAN through an Ethernet cable, a user can access the web interface controls inside the VEEMUX.

FYI: To quickly locate a VEEMUX on the LAN and edit the IP address settings, use the Device Discovery Tool (page 40).

To access the web interface, type the current IP address into the address bar of the web browser.
Address http://192.168.1.30

To open a SSL-encrypted connection, type:
Address https://192.168.1.30

You will be prompted to accept a certificate. Accept the NTI certificate.

A "Login Page" will appear.

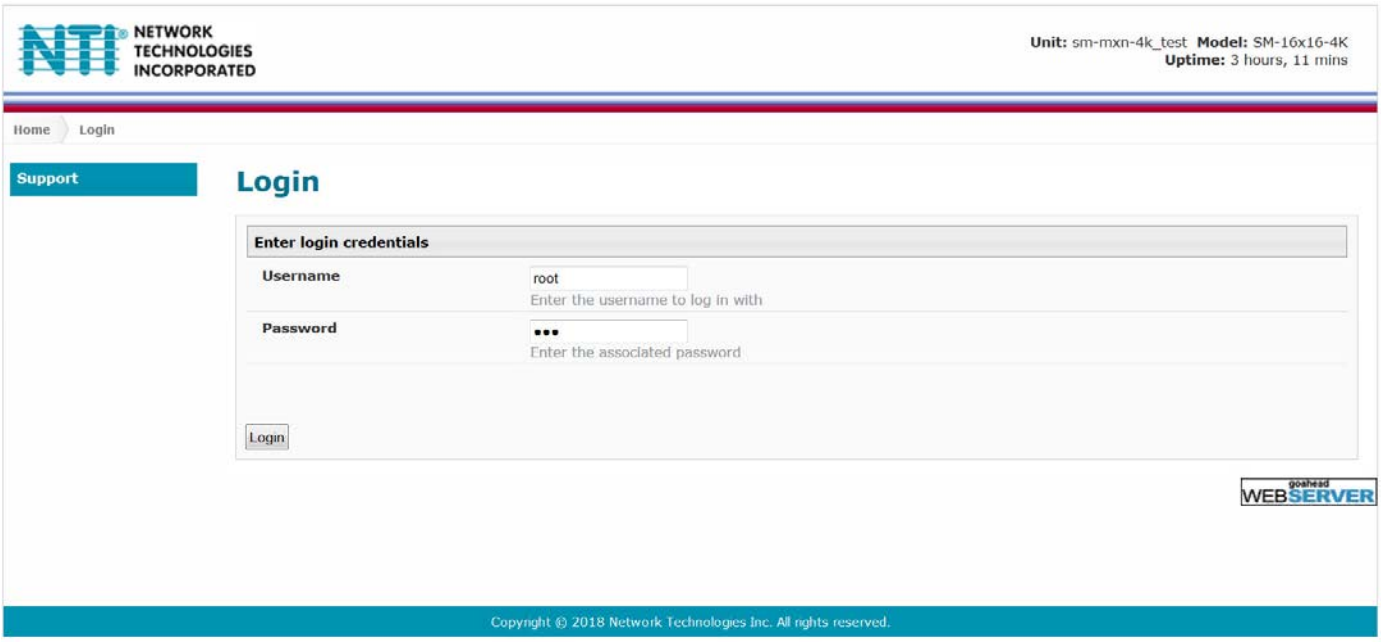


Figure 7- Web interface Login page

Enter the Password

The cursor will be flashing inside the username box. Enter the administrative username (this cannot be changed), then enter the default password:

User Name = root (lower case letters only)
Password = nti (lower case letters only)

To change the password, see page 33.

If you are not the “root” user, access to the VEEMUX may be limited. Contact the VEEMUX administrator for your individual username and password.

For information on setting up as many as 15 additional users, see page 33.

Note: The browser must be configured to accept cookies in order for the user to successfully make use of the web interface.

With a successful login, the main menu and Video Switch page will appear.

Main Menu

The VEEMUX main menu provides control over all functions of the switch. The administrative menu includes options not available to other users with limited privileges.

When logged in a user without administrative privileges, only the SWITCH, LOGOUT, and SUPPORT menu options will be available.

For more on user management, see page 33.

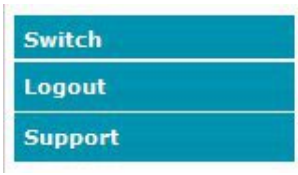


Figure 8- Administrator Menu

(User Main Menu)

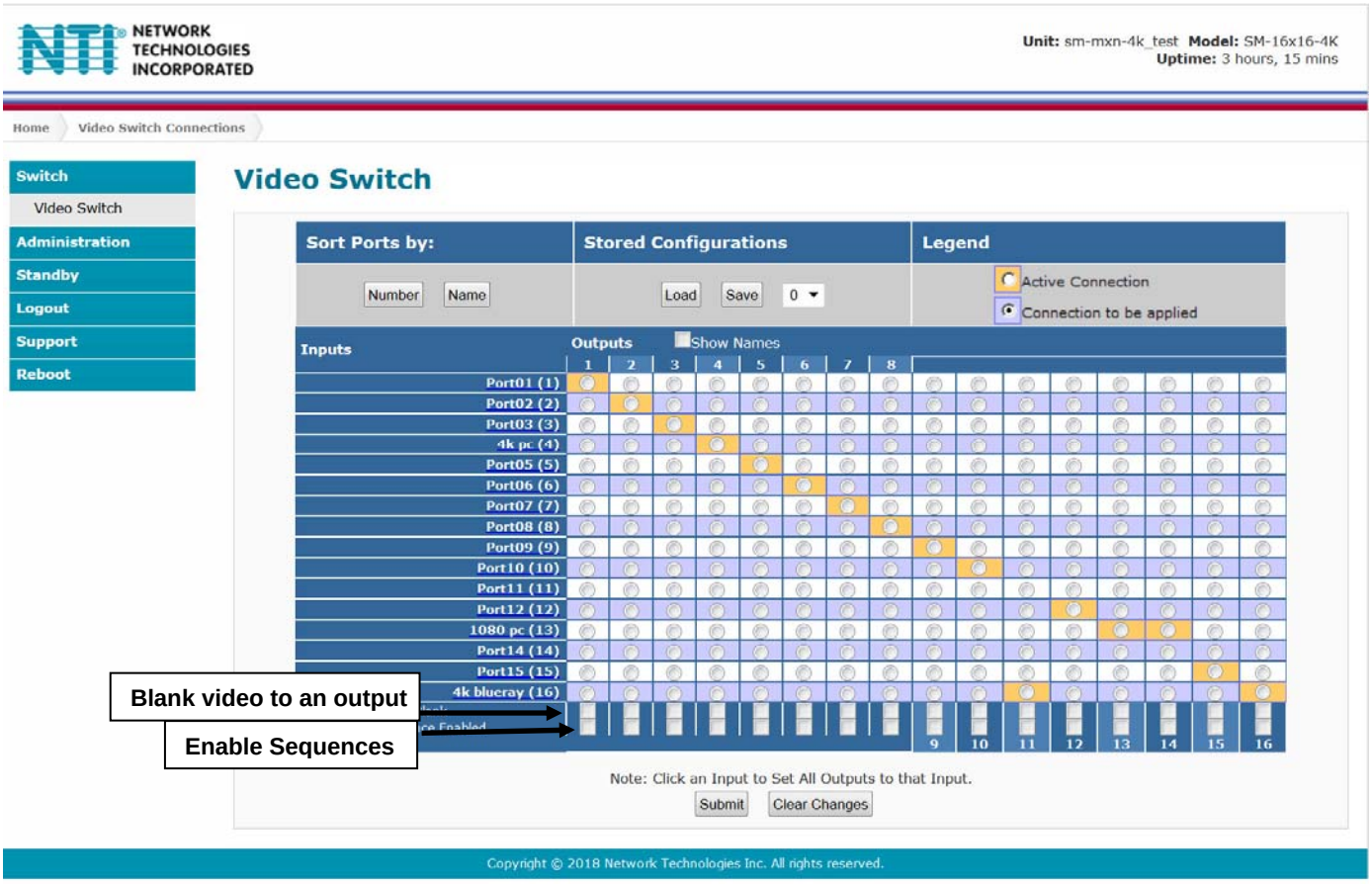


Figure 9- Main menu and Video Switch page

From the menu the administrative user can choose from several links to either view the status of the switch or change the configuration of it. As described on the following pages, each link will enable different areas of control.

Video Switch Page

The Video Switch page (Figure 9) displays the active connections (shown in orange) and enables the user to control the video connections of the VEEMUX. Up to 100 different connection configurations can be saved and later recalled by any connection method. Scanning Sequences (page 31) for each output can also be enabled.

Note: Changes made using the keypad (page 8) or by another user through the web interface will be updated automatically to your browser every 10 seconds.

Note: Configuration 0 will be automatically loaded when the VEEMUX is powered-up.

To change a connection, click on the radio button (square image with circle in the center) that intersects the input and output columns. A black dot will be placed in the circle to indicate the selection. Then press the **Submit** button. The display will be reloaded with the selections changed to orange to indicate they are now active. Multiple connections can be changed simultaneously.

To quickly clear the selected radio buttons press the **Clear Changes** button. This will only work if the **Submit** button has not already been pressed with the selections made.

To quickly connect all outputs to a single input, click on the desired input.

FYI: See page 32 for an example of using the Outputs Scanning Sequences feature.

To save a configuraton, from the **Stored Configurations** user interface, use the drop-down list to select the desired slot (numbers 0-99) to save the active configuration into and press the **Save** button.

Note: This will save the currently active configuration on the VEEMUX and the DDC configuration (page 34). If changes have been made in the web interface without first pressing the Submit button, those changes will not yet be part of the active configuration.

Note: If changes to the active configuration have been made by another user prior to saving the current connection selections, the changes made by the other user will be saved as the configuration.

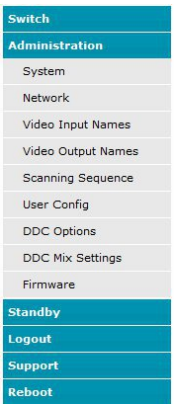
The webpage configuration that loads after a **Save** is the configuration that was actually saved.

To load a saved configuration, from the **Stored Configurations** user interface, use the drop-down list to select the desired configuration. Then press the **Load** button. The VEEMUX will make the connections and the screen will refresh to show the connections associated with that configuration selection. This also loads the saved DDC configuration (page 34).

To blank the video to a specific output, click the box to the right of "Blank" that corresponds with the desired output to place a checkmark in it. The video going to that output will be disabled.

To enable the scanning sequence configured for an output, configure the automatic scanning sequence of inputs that should be viewed at the output (see page 31) and then click the box to the right of "Sequence Enabled" that corresponds with the desired output to place a checkmark in it. The video viewed from that output will switch from input to input according to the configured sequence.

Administration



The Administration section provides links to pages for all configuration options in the VEEMUX switch. Only the user ROOT and users with administrative privileges have access to this section. The administration section is broken up into 10 topics:

System	Assign the switch name and serial port communication settings
Network	Assign all network settings for connection to LAN
Video Input Names	Assign port names to each cable connection from video sources for easy reference
Video Output Names	Assign port names to each cable connection from display devices for easy reference
Scanning Sequence	Assign dwell times for each input as it is assigned to each output's scanning sequence
User Config	Add, edit, and delete users and control user privileges
DDC Options	Configure how each input will receive EDID information
DDC Mix Settings	Select outputs/displays to be used for EDID mixing for each input
Firmware	Update the firmware as new versions become available

System Configuration

On the System Configuration page, under Administration, fields are provided to assign a unique name to the VEEMUX, set the baud rate for serial communications, and the serial address to be used in RS232 commands.

After applying the desired settings, press "**Save**" to finish.

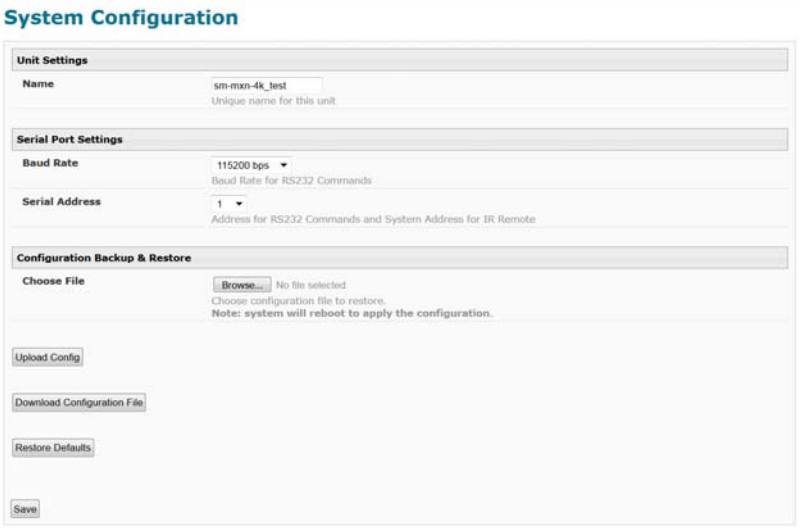


Figure 10- System Configuration page

Download Configuration File - To save VEEMUX configuration and DDC settings for a future reload or to save time in configuring multiple VEEMUX switches, the configuration file for the VEEMUX can be downloaded to your PC using "**Configuration Backup & Restore**". Click on "**Download Configuration File**" to save the VEEMUX configuration to your PC.

From your PC the downloaded configuration file can be edited using any text editor or html editor. Using an editor you can change settings, change IP address, etc. and then upload the result into an additional VEEMUX switch to save time.

Upload Config- Click on the **Browse** button to browse to the file, click on "**Upload Config**", and restore the VEEMUX to the configuration stored in the uploaded file.

Restore Defaults- Click on "**Restore Defaults**" to remove all user-configured settings and restore the VEEMUX to a factory default configuration.

Note: Before restoring defaults, we recommend you download the existing configuration file to your PC.

After applying the desired settings, press "**Save**" to finish.

Network Configuration

ON the Network Configuration page, under Administration, the administrative user can configure the VEEMUX web interface connection. This will provide access to control of the VEEMUX from any web-accessible computer.

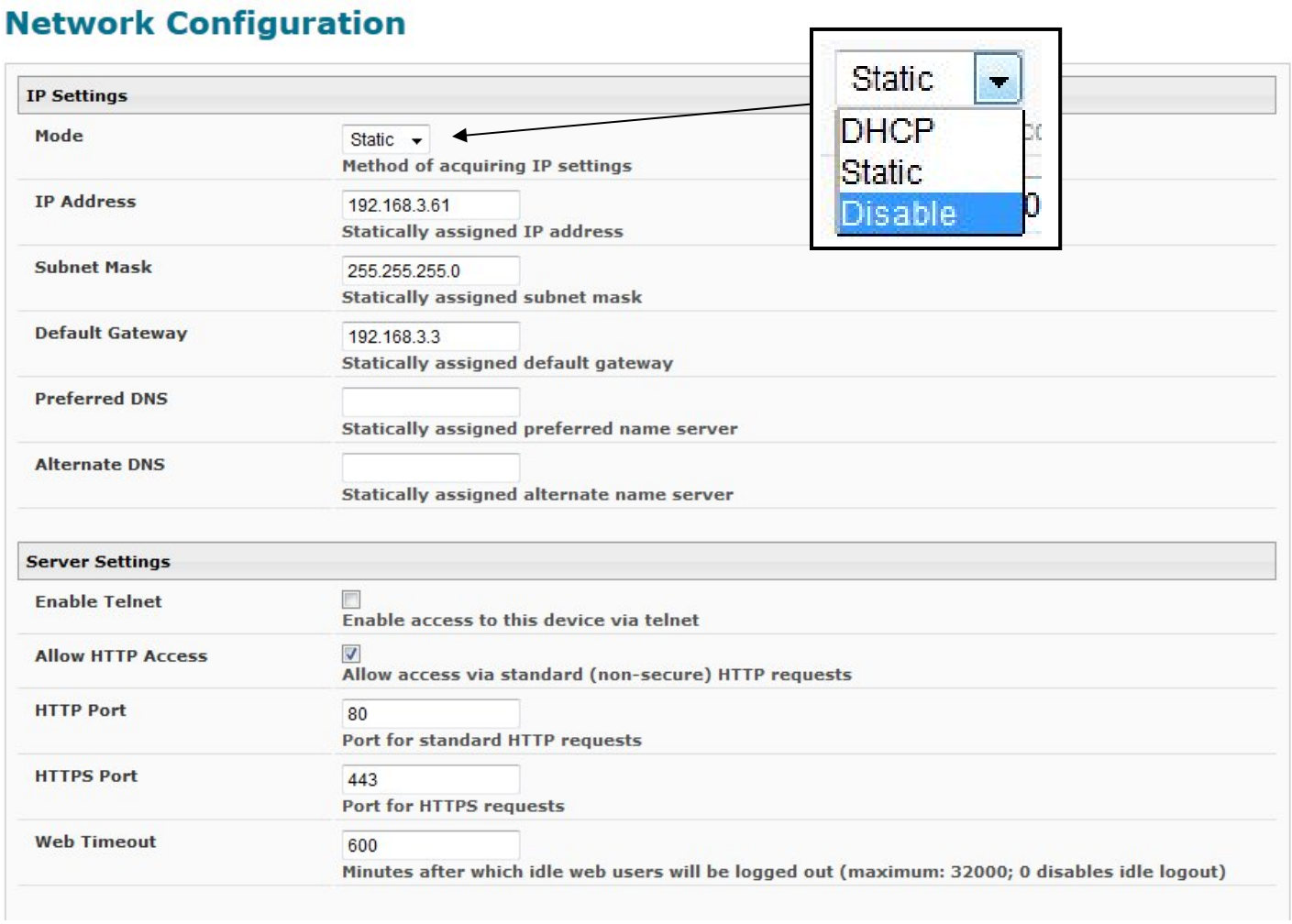


Figure 11- Network Configuration page

Mode – Choose between Static IP assignment, DHCP (dynamic IP assignment) or Disable the Ethernet port entirely.

IP Address- If using Static IP assignment, enter a valid IP address to use

Subnet Mask- Enter a valid subnet mask value

Default Gateway- Enter a valid gateway address

Preferred DNS- Enter a valid Domain Name Server address (not required)

Alternate DNS- Enter a valid alternate Domain Name Server address if desired (not required)

This change will take a few seconds and automatically redirect the user to the IP address specified.

If telnet is going to be used to control the VEEMUX, place a checkmark in the “Enable Telnet” block.

If you wish to disable non-secure web access to the VEEMUX, remove the checkmark from “Allow HTTP Access”. With this box empty, only secure shell web access will be allowed.

A standard port number can be assigned for the HTTP (non-secure) and HTTPS (secure) ports, numbers ranging from 0-65535. Default HTTP port is 80, and default HTTPS port is 443.

The Website Timeout option controls how long an inactive web connection will stay logged in. The range is 0-3200 minutes (0 disables it). Any change to the Website Timeout configuration takes effect immediately.

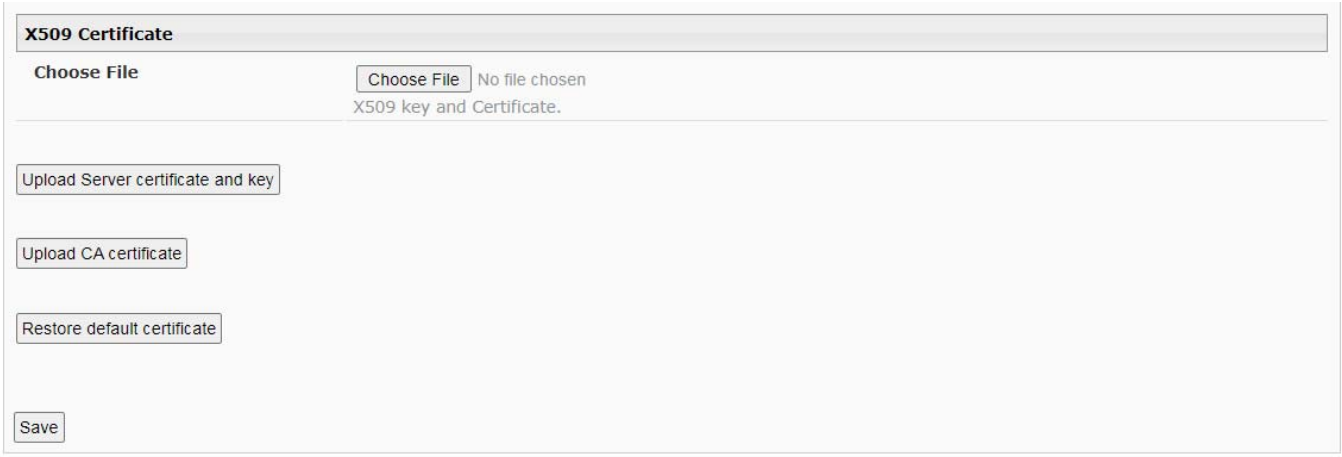


Figure 12- Network Configuration Page (continued)

X509 Certificate

The VEEMUX is designed to be configurable with secure access to the web interface controls. The VEEMUX is pre-loaded with a generic X509 Server Certificate. If you wish to provide your own X509 Server certificate, the Server certificate must be uploaded to the VEEMUX. The Server certificate and key must be combined into a single file (“PEM” format). For instruction to create your own certificate, see page 47 for more information.

.

Browse to the Server certificate file and select it. Then load using the button “**Upload Server Certificate and key**”.

Note: The key used should not be password protected.

X509 Certificate Authority

A Certificate Authority (CA) needs to be used to sign the server certificate describe above. This Certificate Authority can be created as a self-signed certificate in "CRT" format. It can also be given to you by an external Certificate Authority in "CRT" or "PEM" format.

For https to work properly, you must load the certificate of your CA onto the VEEMUX. Use the "**Choose File"** button to browse to the file containing the CA certificate (which may also contain an intermediate certificate) and select it. Then click on the "**Upload CA certificate**" button. Please see page 47 for more information.

The “**Restore default certificate**” button will restore the unit’s default self-signed certificates if needed.

Note: HTTP access can be enabled/disabled from web page under Administration -> Network -> Server Settings -> Allow HTTP Access (page 26). Do not disable http access until you verify certificate verification works properly for https connection. HTTP connection will allow you to change any settings if a wrong certificate is uploaded. Once HTTPS client certificate validation is verified to be working properly, disable HTTP access for security.

After loading your own Server Certificate, **reboot the VEEMUX for this certificate to take effect.**

Press the "**Save**" button to save any changes made.

Video Input Names

From the Administration menu, the Video Input Names page can be displayed. This page enables the administrative user to change the name of the input ports displayed on the Video Switch page.

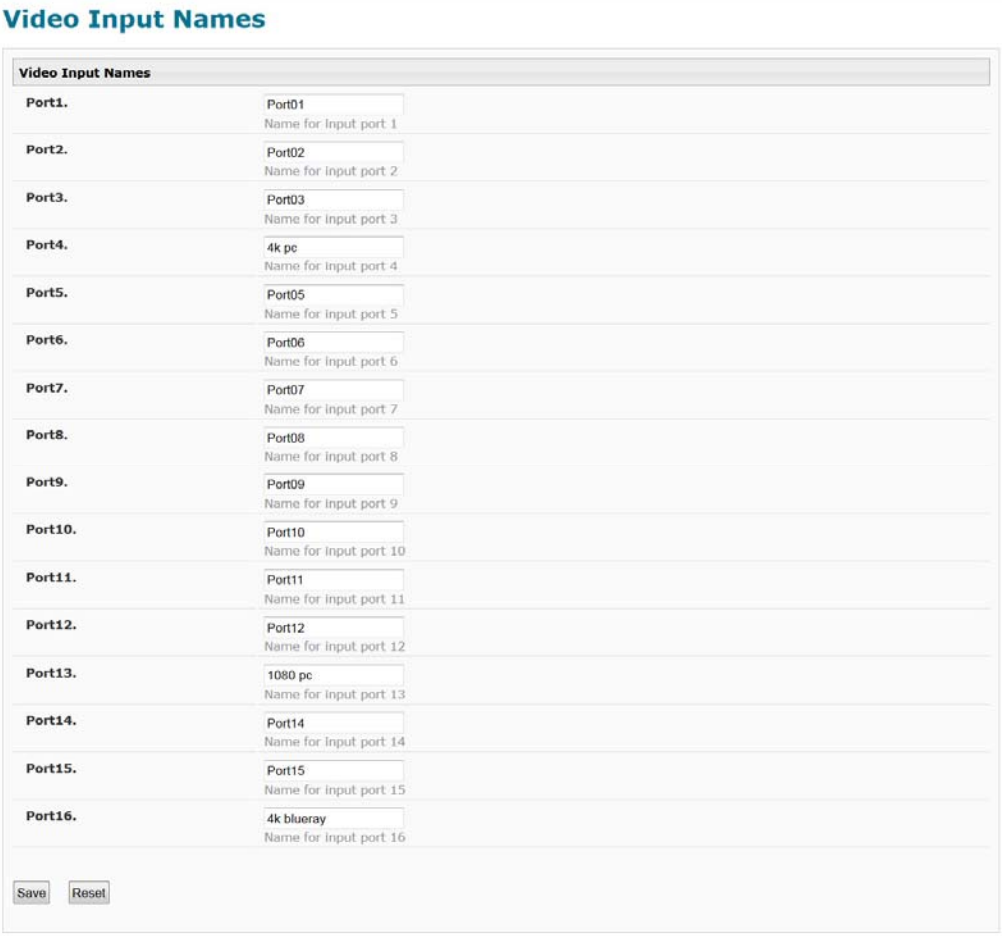


Figure 13- Video Input Names page

To change an Input Name, enter the name of the port for the desired input port number, and press "**Save**".

If you make changes and change your mind and want to return the names back to what they were before changing them, press "**Reset**". This must be done before pressing the "**Save**" button, or changes will not be able to be reversed.

Video Output Names

From the Administration menu, the Output Names page can be displayed. This page enables the Administrator to change the names of the output ports displayed on the Switch page.

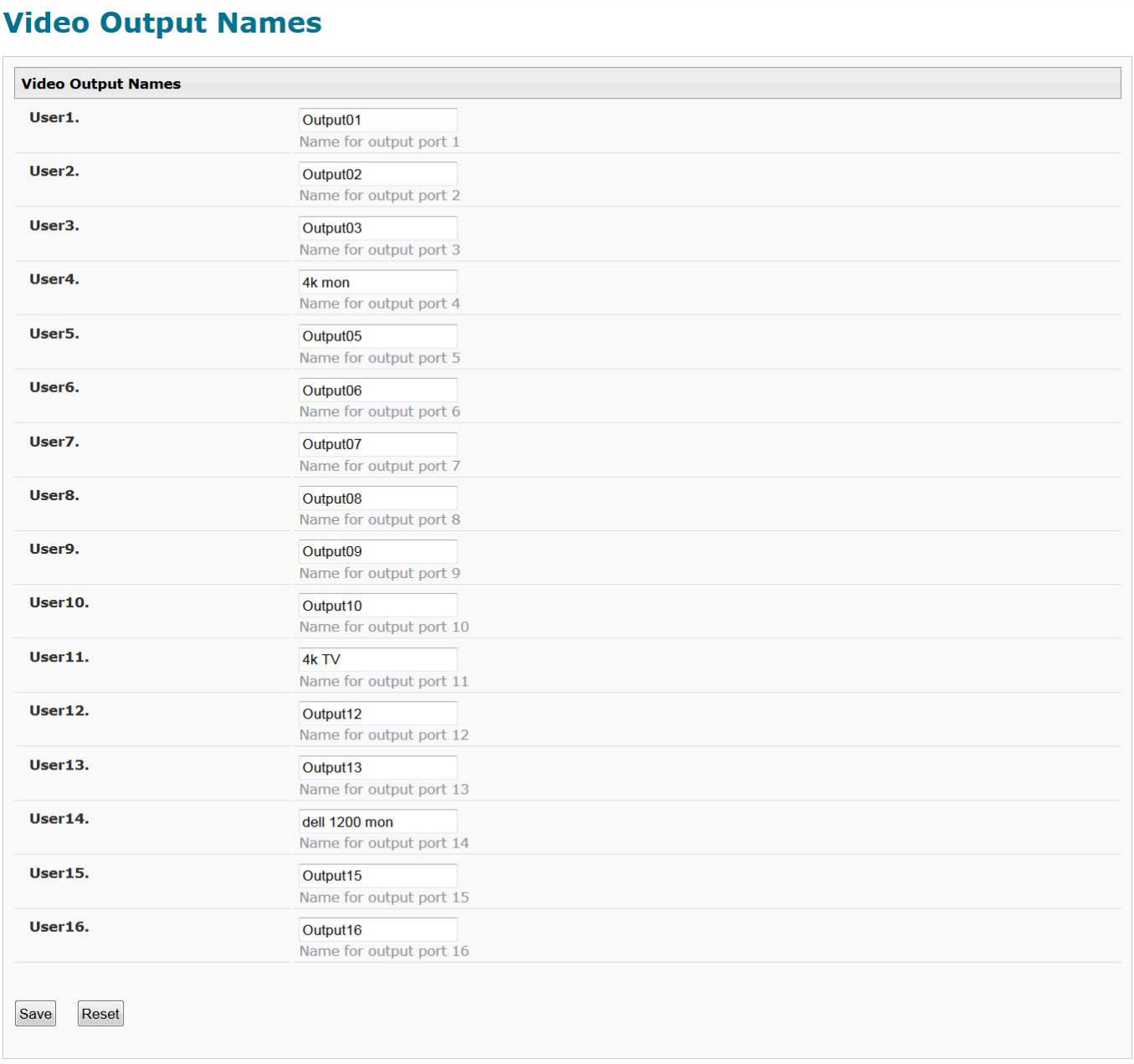


Figure 14- Video Output Names page

To change an Output Name, enter the name of the port for the desired output port number, and press "**Save**".

If you make changes and change your mind and want to return the names back to what they were before changing them, press "**Reset**". This must be done before pressing the "**Save**" button, or changes will not be able to be reversed.

Scanning Sequences

From the Administration menu, the Scanning Sequence page can be displayed. The Scanning Sequence page displays the configuration of an automatic switching sequence from input (video source) to input for each output (monitor).

The page displays:

- output number being configured
- the Scanning Sequence function status for that output
- the length of time in seconds (dwell time) that each input will be viewed when connected- the dwell time value ranges from 0-255 seconds

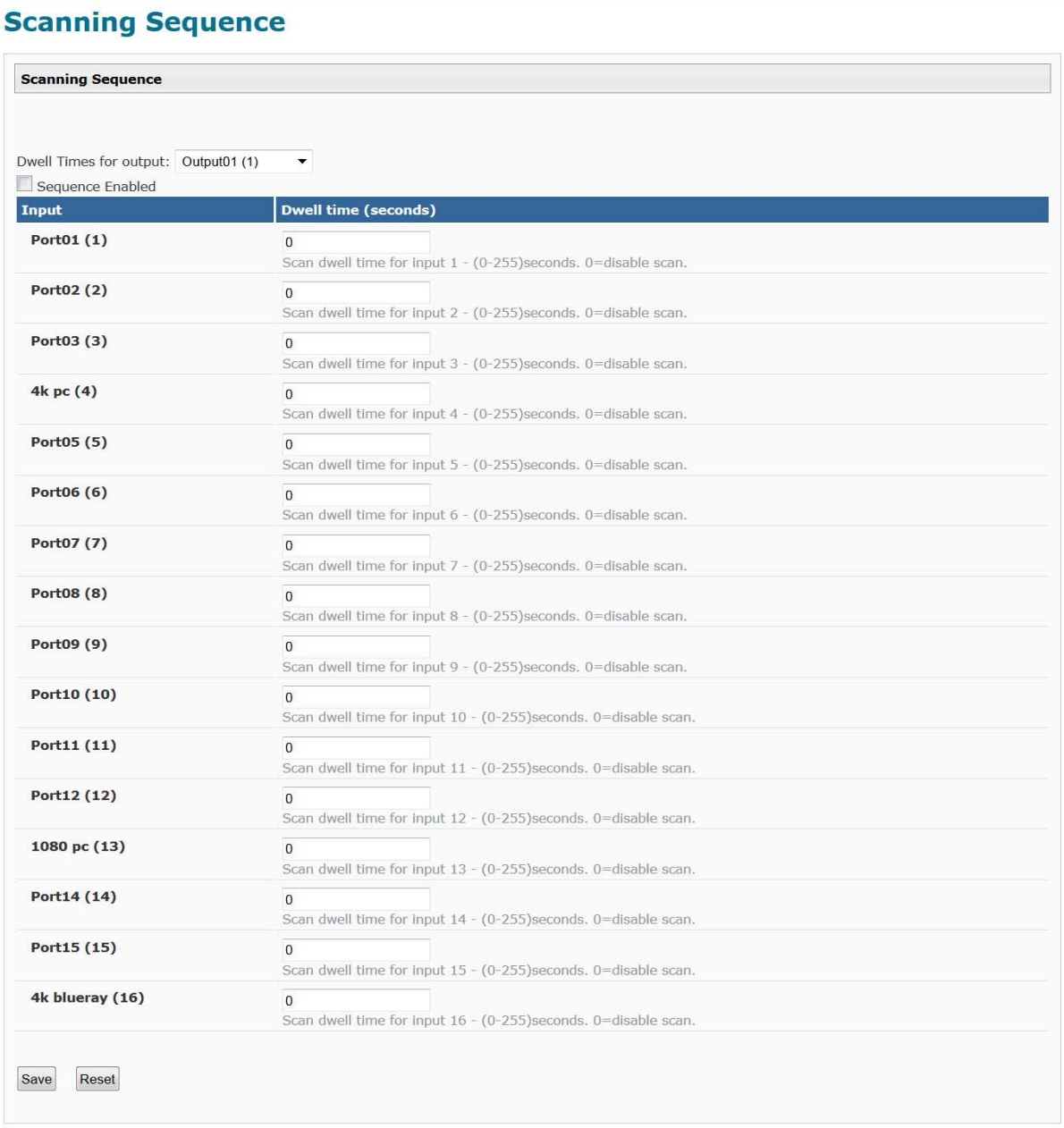


Figure 15- Scanning Sequence page

The output selection at the top of the page can be changed to any output to display the Scan Sequence Input dwell time values for that output.

The inputs and the amount of time that each will be viewed (0-255 seconds) can be set to cycle sequentially for each connected output. If an input is set to 0 seconds, that input will not be viewed and will be skipped from the scanning sequence. To include an input in the sequence, enter a dwell time period from 1-255 seconds, and press "**Save"**.

If you make changes and change your mind and want to return the values back to what they were before changing them, press "**Reset**". This must be done before pressing the "**Save**" button, or changes will not be able to be reversed.

To enable the scanning sequence for the output shown, place a checkmark in the "**Sequence Enabled**" block.

Tip: To quickly enable the scan sequence for multiple outputs, use the "Sequence Enable" blocks found on the Switch Page (page 18).

Note: If only one input has a dwell time value entered, then the output connection to that input will not end when the Scanning Sequence is enabled.

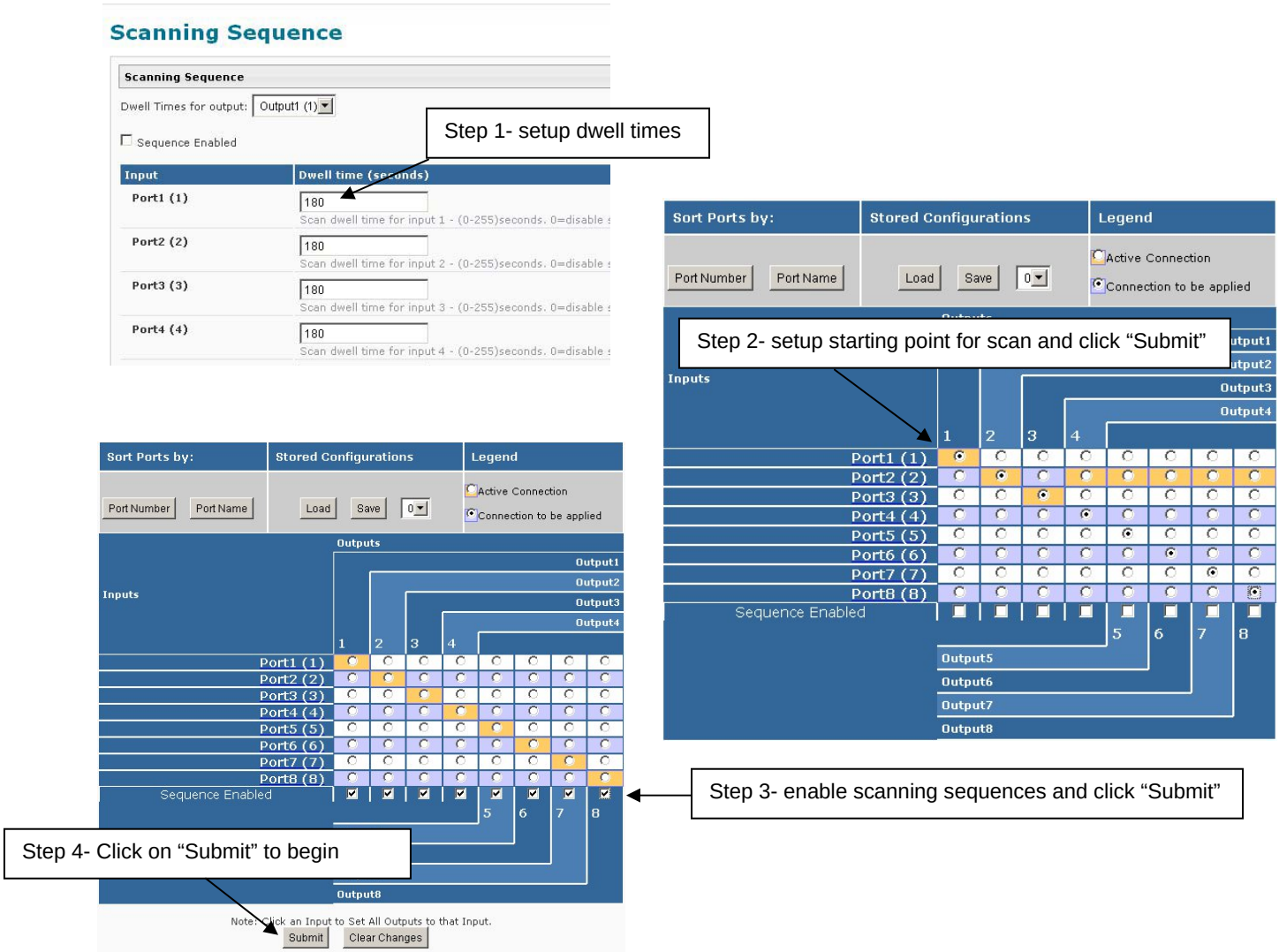
Example of using Outputs Scanning Sequences

Problem: A synchronous scan is desired for all outputs with a dwell time of 3 minutes per input, and no two outputs should be looking at the same input at any given time.

Solution:

1. Set the dwell time for all inputs listed in each output at 180 seconds (3 minutes). Press "**Save**" each time changes are made to the selected output. .
2. Go to the Video Switch page (page 18) and set each output to an input of the same number (1 to 1, 2 to 2, 3 to 3, etc..). Click on "**Submit**" at the bottom of the Video Switch Page to submit selections and establish a connection and starting point for the scanning sequence. (Blocks shown in yellow in the third image indicate connections made.)
3. Click on the "**Sequence Enabled**" box for each output (from the Video Switch Page).
4. Click on "**Submit**" again to begin the scanning sequence for each output.

From the moment the configuration is submitted, a synchronous scan will begin on all outputs. Each output will connect to its respective input for 3 minutes. After 3 minutes, the outputs will each switch to the next consecutive input and remain connected for 3 minutes. This cycle will continue indefinitely until sequencing is disabled.



User Config

From the Administration menu, select the User Config to display a list of the users that have been configured on the VEEMUX.

- To add a user, select “Add New User”.
- To change the configuration of a user, select the Username, or “Edit”.
- To delete a user, select “Delete” for that user.

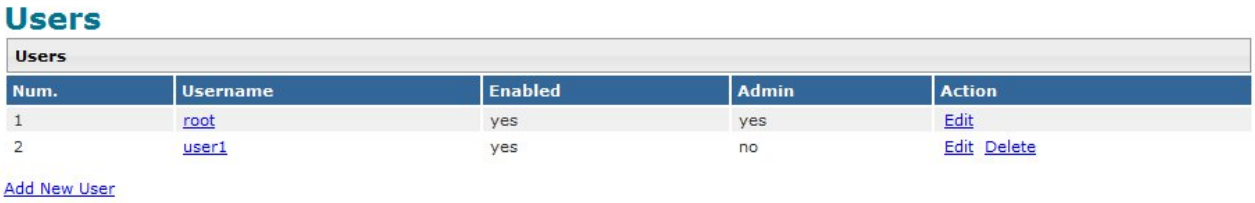


Figure 16- Users page

Whether you add a user, or edit a user, the “Configure User” page will open. If this is a new user being added, enter a user name, decide if the user should have administrative privileges or not, enable their access to the VEEMUX (or not), and assign a password.

- Usernames and passwords are case sensitive.
- Usernames can be from 1 to 16 characters in length and can be alphabetical or numeric.
- Passwords can be from 5 to 16 characters in length and can be alphabetical or numeric.

Note: A password must be entered for the user to be enabled, even if the “Enable” block is checked and the user is saved without a valid password being entered.

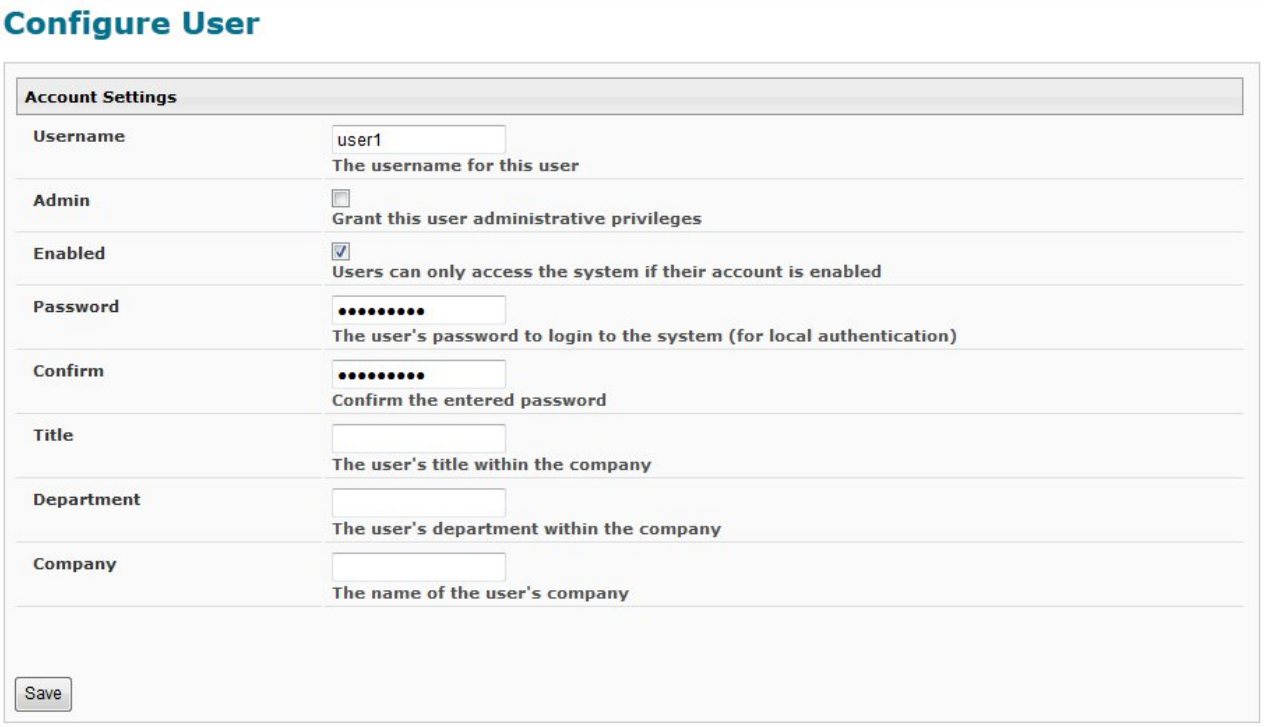


Figure 17- User configuration page

After making any changes, be sure to click “Save”.

DDC Options

From the Administration menu, the DDC Options page can be displayed. DDC enables the video source to get EDID information from the display device. This enables the video source to automatically select the optimal resolution for the display by receiving, at power up, information from the display device concerning its resolution specifications.

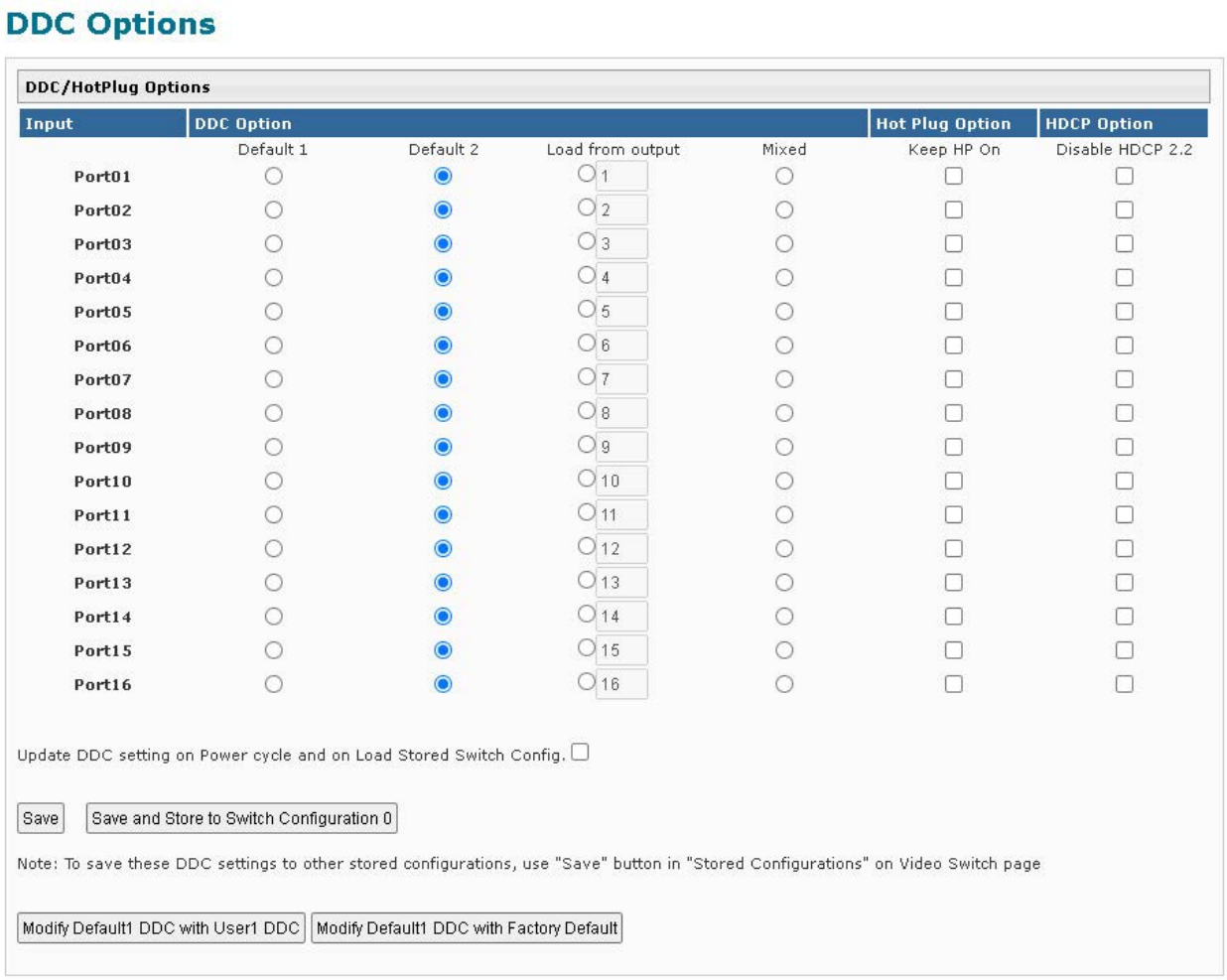


Figure 18- DDC Options page

EDID information can be provided to the video source by the VEEMUX as follows:

Default1- The video source on the input port will receive EDID information from the VEEMUX through an onboard table of values. The values for Default 1 support computer monitors. The factory default value is 1920x1080@60Hz(1080p).

Default2- The video source on the input port will receive EDID information from the VEEMUX. The value for Default 2 is 3840x2160@60Hz(UHD)

Load from Output- select the radio button for this option and enter the output number associated with the monitor that the CPU should get its EDID information from.

Mixed- The video source on the input port will receive EDID information that is common to the outputs selected on the "DDC Mix" page (page 36) for that input.

Update DDC setting on Power cycle and on Load Stored Switch Config- place a checkmark in the box to refresh DDC data stored in the VEEMUX each time the VEEMUX is power-cycled or when a stored configuration (page 24) that includes this DDC configuration is loaded. The DDC data will be updated based on the configuration on this page.

Save and Store to Switch Configuration 0- press to save the DDC Configuration settings to Switch Configuration 0 so that when the VEEMUX is power cycled and the "Update DDC setting on Power Cycle…." (above) is checked, the DDC Configuration will be loaded as configured above.

Modify Default1 DDC with User1 DDC- click this button to load the EDID information to "Default1" from the video display connected to Output 1.

Modify Default1 DDC with Factory Default- click this button to restore "Default1" with factory supplied EDID information

Once any changes are made, press "**Save**" to have them take effect.

Note: In order for the video sources to correctly receive the EDID information from the switch at boot-up, the switch must be powered-up before all attached video sources.

Hot Plug Options

Enabling "Keep HP On" (see Figure 18) ensures that PC does not re-read EDID from the VEEMUX when the input video port connection is changed to a different output video port regardless of whether the output port has a monitor connected. This applies when manually reconfiguring the video connection or when the device is in Scan Mode. Physically disconnecting the output cable will still send a hot plug signal to the connected input port.

Disable HDCP 2.2
Place a checkmark in the **Disable HDCP 2.2** box if you wish to disable the port's compatibility with HDCPv2.2.

Normally, if a video source senses that the VEEMUX is compliant, it will provide HDCP 2.2 compliant video. Then, provided the connected monitor is also HDCP 2.2 compliant, a picture will be displayed. If the monitor connected to a port is not compliant with HDCP 2.2 (i.e. only compliant with HDCP 1.4), then no picture would be displayed. To display a picture on a non-HDCP 2.2 compliant monitor, place a checkmark here to disable the feature for the source supplying video to that output port.

Application Note:

To save and reuse the EDID information of any monitor please use the procedure below. This procedure will reuse the stored EDID even if a different monitor is connected or the matrix switch is rebooted.

1 Connect desired monitor to Output 1
2. Click "Modify Default 1 DDC with User1 DDC" in DDC Options menu
3. Now any Inputs with DDC Options set to "Default 1" will see this monitor's EDID going forward.

Optionally you can save this to a Stored Configuration (page 32) to send these saved DDC settings to the Inputs selected on the DDC Options page. Once the Stored Configuration is saved, it can be recalled at any time.

DDC Mix

From the Administration menu, the DDC Mix page can be displayed. DDC Mix provides a means to decide which outputs (displays) will be used to provide EDID information to the selected input. The VEEMUX will compare EDID information from all selected outputs and provide EDID information that is common to those displays to the video source. If the "Mixed" option is desired for an input on the "DDC Options" page (page 34), settings of the DDC Mix for that input (below) should be selected and saved first.

If the DDC Mix configuration for an input is not configured and the "Mixed" option for the input is selected on the DDC Options page, a minimal default collection of EDID information will be provided to the video source.

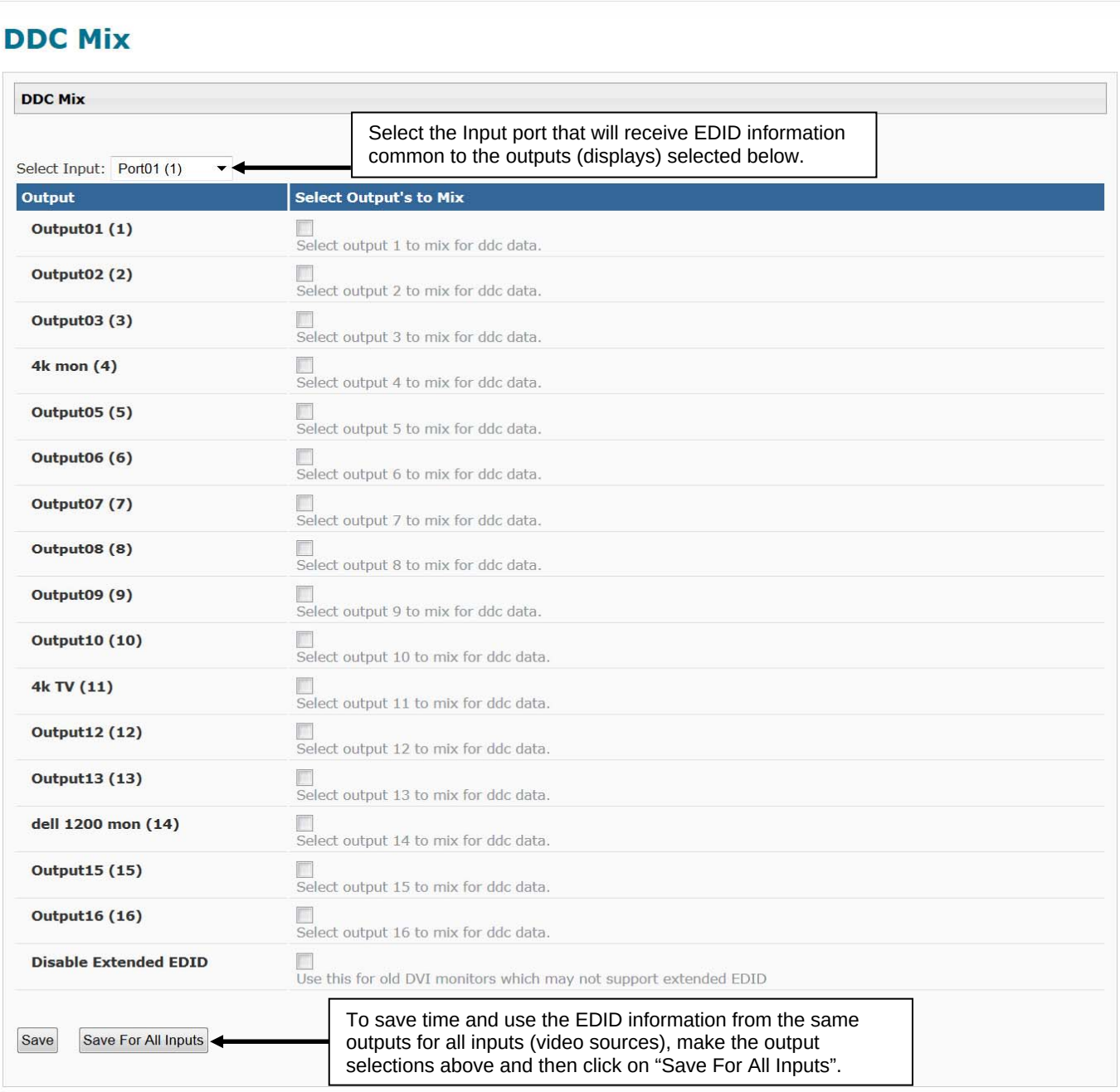


Figure 19- DDC Mix page

Update Firmware

From the Administration menu, the Update Firmware page can be displayed. The Update Firmware page shows the current version of the firmware and enables the Administrator to update the firmware to the latest version available.

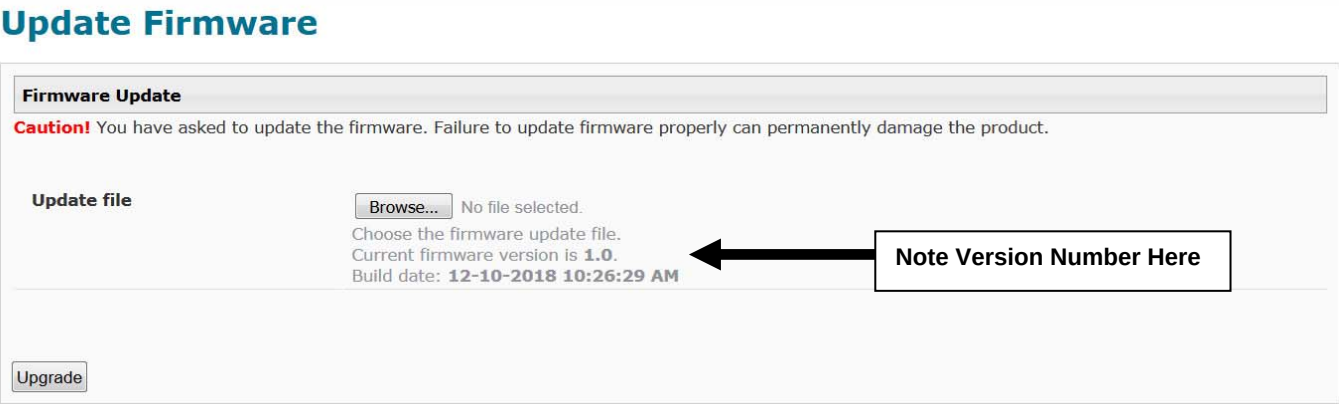


Figure 20- Update Firmware page

WARNING: Failure to carefully follow these directions can permanently damage the VEEMUX. Please read these directions in full before continuing. Do not, under any circumstances, reset or power-down the VEEMUX while the firmware is being updated. Do not attempt to update the firmware if a power-failure is likely.

Note: The Firmware can only be updated from the non-secure (http) website. If you attempt to access this page from the secure (https) website, you will be automatically redirected to the non-secure site.

To update the firmware:

1. Contact NTI for the latest firmware file name **`veemux-hd4k-vx-x.bin`** (where x.x is the version number) and copy it to your computer.
2. On the Update Firmware page, in the "Update File" block, browse to the firmware file.
3. Press **Upgrade**.

Note: If an update is attempted using the wrong firmware for the section an error message will be received. No update will occur.

4. The VEEMUX will upload the firmware and then restart itself (this may take up to 4 minutes), logging out all connections. After the restart, approximately 4 more minutes, the VEEMUX will be ready to resume operation.

If a message appears stating that the Upload has failed, or that a non-fatal error has occurred:

1. Ensure that the file being uploaded is the NTI firmware file.
2. Repeat the process from step 2 above.

Note: The following message does not indicate that damage to the product has occurred.

If a message appears stating that there has been a fatal error:

1. **DO NOT RESET OR POWER-DOWN THE VEEMUX**.
2. Repeat the update process from the first step 2 above.
3. If you get another Fatal Error message, call NTI tech-support at 1-800-742-8324 or 330-562-7070.

FYI: The VEEMUX should continue to run normally unless it is reset. However, damage may have occurred to the web server firmware that will prevent the product from starting up correctly.

Standby Mode

From the menu, the user can quickly place the VEEMUX in Standby Mode. When in Standby, the VEEMUX will still be powered-ON but all functions will stop. The VEEMUX will be in a power-saving ready-to-use state.

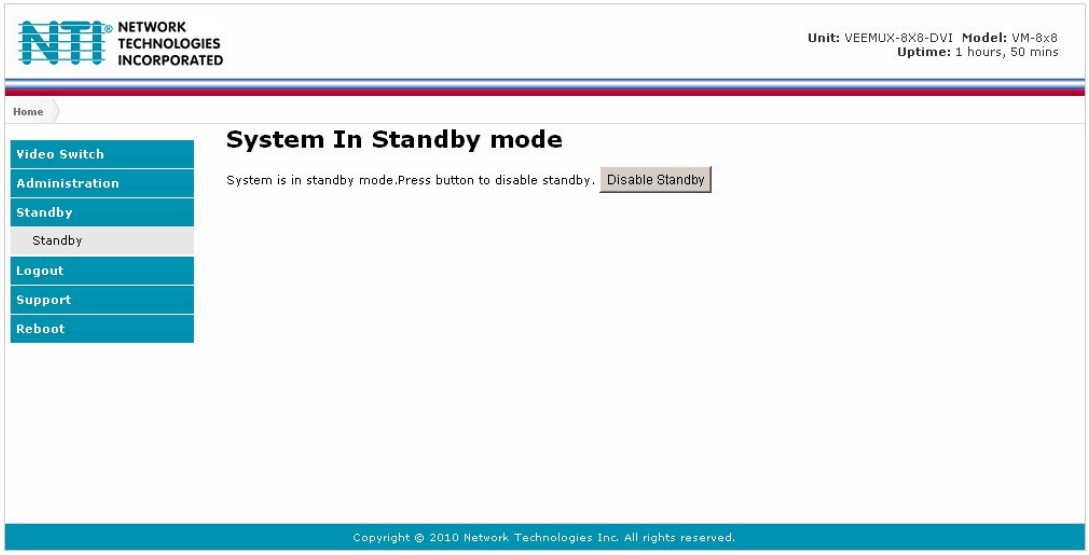


Figure 21- VEEMUX in Standby Mode

By simply selecting “Standby” from the side menu, the VEEMUX is placed in Standby Mode. When in Standby Mode, the VEEMUX will not provide video to any displays and cannot be manipulated further until standby is disabled.

Standby Mode can be disabled either

by pressing “Disable Standby” through the web interface (above),
by pressing any button on the front panel keypad
by using the IR Remote control (optional)

Logout

To quickly logout of the web interface, select “Logout” from the menu. You will immediately be logged out and presented with a login screen.

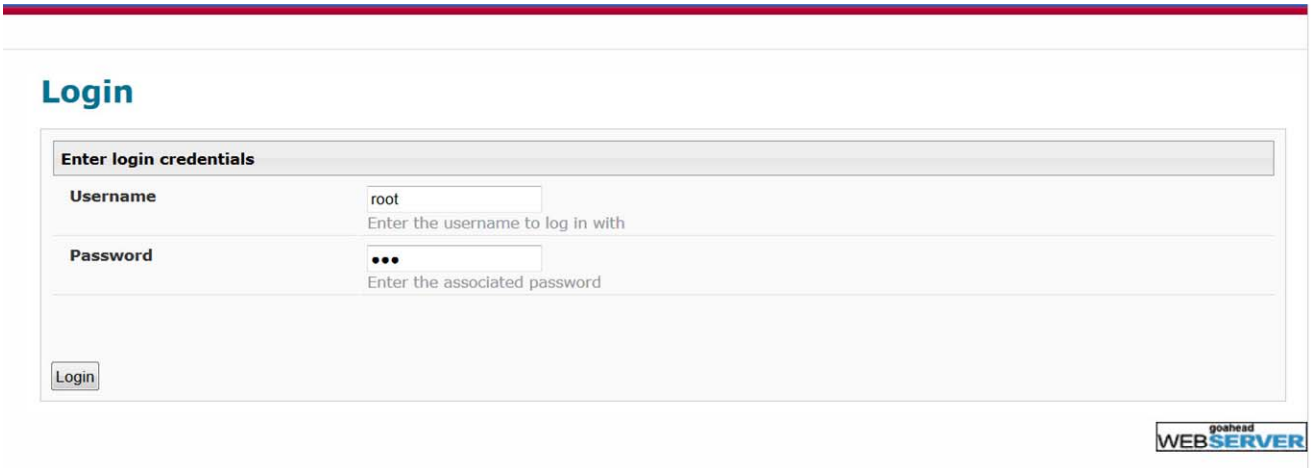


Figure 22- Logout of the VEEMUX web interface

Support

The Support link on the menu drops down to two choices, **Manua**l and **Downloads**.

The **Manual** link will open the pdf manual for the VEEMUX.

The **Downloads** link (http://www.networktechinc.com/download/d-4k-hdmi-matrix-switch.html) will open the firmware downloads page for the SM-16X16-HD4K Video Matrix Switch at NTI. From there you can see what versions of firmware are available and determine if the version in your VEEMUX is current or in need of an upgrade (page 37).

Figure 23- Support Tab

Reboot

To quickly reboot the VEEMUX, select “Reboot” from the side menu. This will force the VEEMUX to power cycle its processor. A reboot will take approximately 45 seconds to occur. Refresh your browser and log back in to the VEEMUX as desired.

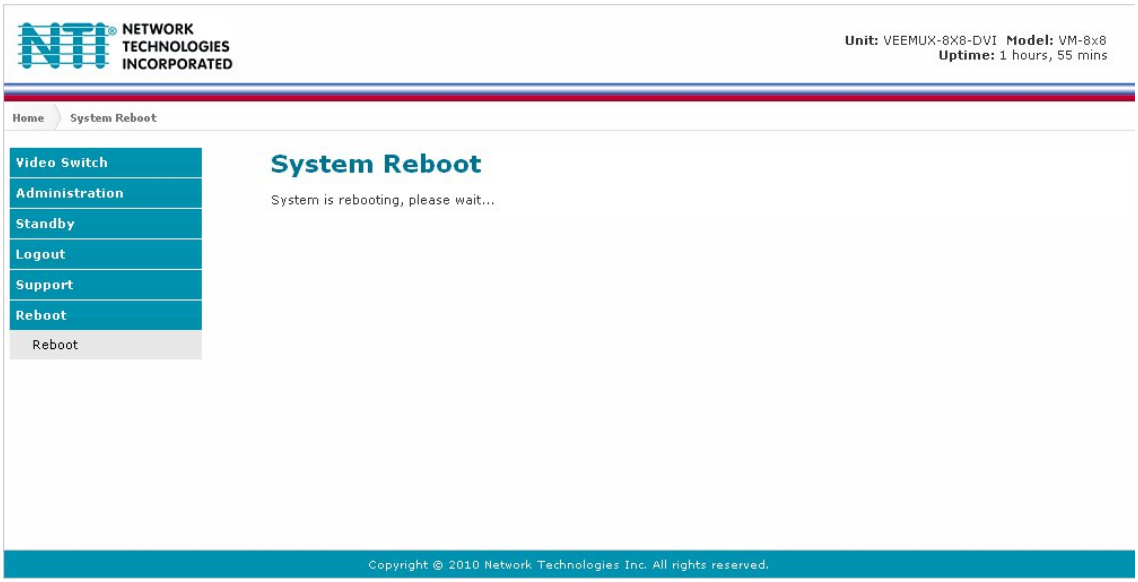


Figure 24- System Reboot

DEVICE DISCOVERY TOOL

In order to easily locate the VEEMUX on a network, or to change network settings, the NTI Device Discovery Tool may be used. The Discovery Tool can be found at **http://www.networktechinc.com/download/d-4k-hdmi-matrix-switch.html .**

Unzip and save to a location on your PC. To open it just double-click on the file **`NTIdiscover.jar.`** This will open your browser and display the Device Discovery Tool page.

Note: The Device Discovery Tool requires the Java Runtime Environment (version 6 or later) to operate. Here is a link to the web page from which it can be downloaded.

Note: The computer using the Discovery Tool and the VEEMUX must be connected to the same physical network in order for the Device Discovery Tool to work.

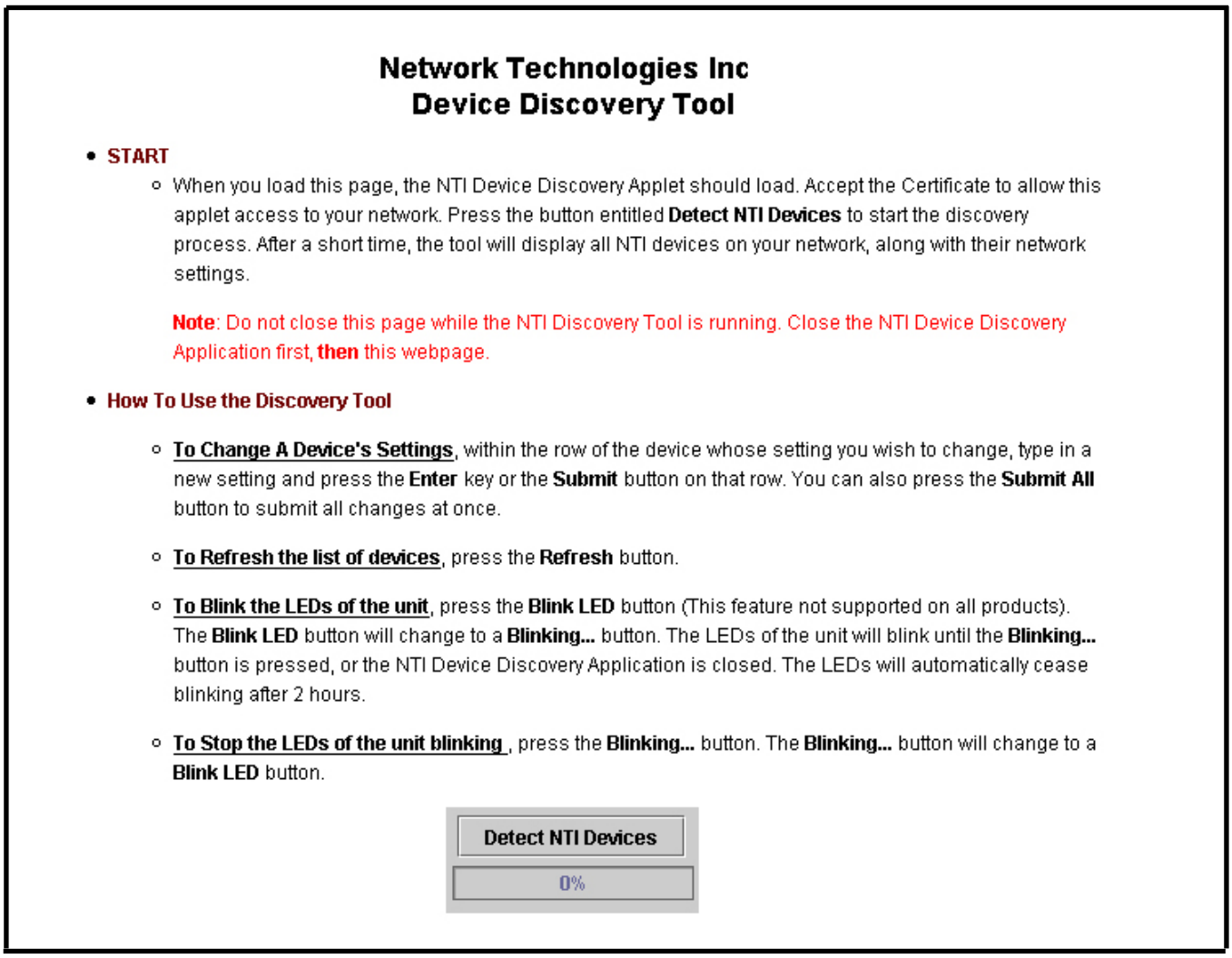


Figure 25- Device Discovery Tool page

Use the Device Discovery Tool to display all NTI VEEMUXs on your network, along with their network settings. Follow the instructions on the Device Discovery Tool page to use the tool and to change the device settings if so desired.

The "Blink LED" button is not supported on this product.

INFRARED REMOTE CONTROL

The IRT-UNV Infrared Remote Control (**optional- sold separately**) allows the user to remotely and intuitively control up to 15 NTI SM-16X16-HD4K video matrix switches, providing the ability to route connections, save and recall switch configurations, and put the switch into Standby.

Features:

- Routing of video signals
- Ability to switch one input to all outputs
- Scroll through inputs for a single output by using the Input +/- keys (similar to changing channels)
- Automatically scan through all channels for a single output
- Save or Recall up to 10 matrix switch preset configurations
- Control up to 15 NTI switches (systems) with a single remote
- Put the switch in Standby

Materials

Materials supplied with the IRT-UNV:

- NTI IRT-UNV Infrared Remote Control
- 2- AAA Batteries (installed)

Buttons

The IRT-UNV Infrared Remote Control user interface consists of a keypad with 29 buttons. The buttons have the following functions:

- **Numerical Values (0-9)**
  - Selects port numbers (for IN, OUT)
  - Selects memory locations (for saved configurations)

- *** (Asterisk)**
  - Pressed to select all outputs

- **OUT**
  - Pressed to indicate an output port selection

- **IN**
  - Pressed to indicate an input port selection

- **IN + / -**
  - Cycles through input ports (up or down), connecting to each one (similar to changing channels)

  Note: This affects only the selected output port

- **SAVE**
  - Pressed to save the current switch configuration (port connections and volume settings)
  - Up to 10 configurations can be saved (0-9)

- **RECALL**
  - Pressed to recall a switch configuration (port connections and volume settings)
  - Up to 10 configuration can be recalled (0-9)

- **SYS**
  - Pressed to select the desired NTI system to be controlled
  - Only used when controlling multiple systems
  - Must be followed by a system number: 1-15

- **ENTER**
  - Pressed to immediately accept the command (normal delay is approx. 5 seconds).

- **ESC**
  - Pressed to cancel the current command

  Note: If the command has not yet been accepted, all button presses in the command sequence will be cleared

- **Standby** 
  Pressed to put the unit into or out of standby mode

- **VIDEO**  **THIS BUTTON IS NOT USED FOR THIS PRODUCT**

- **BLANK Video** 
  - Turns OFF Video for the selected output
  - Can be used with *(Asterisk button) to turn OFF video for all outputs
  - Video will be turned ON by pressing the Blank Video button again, or by switching ports

  Note: Blank and Un-Blank commands are applied only to the selected output

- **AUDIO** **THIS BUTTON IS NOT USED FOR THIS PRODUCT**
- **VOL + / -** **THIS BUTTON IS NOT USED FOR THIS PRODUCT**
- **MUTE Audio** **THIS BUTTON IS NOT USED FOR THIS PRODUCT**
- **SCAN**
  - Pressed to toggle the scan enable/disable feature for the selected port
  - Must be preceded by an output port number (1 or 2 digits), or the * (Asterisk) button to toggle all ports

  Note: If the dwell time for a port is set for 0 seconds, it will not be scanned (page 31)

- **PREV -THIS BUTTON IS NOT USED FOR THIS PRODUCT**

Operation

Operation of the IRT-UNV is intuitive. The number of button presses required to complete any operation is kept to a minimum. This is accomplished using intelligent software within the NTI Matrix Switch. Additionally, the Matrix Switch allows for multiple ways for the user to complete the same operation – ensuring that the Remote will work as expected, regardless of who uses it.

Changing Ports

The first, and most important operational use of the IR Remote is changing ports of the switch. This requires the selection of both input and output ports. There are several methods of control.

Channel Surfing

The “IN +/-“ and “SCAN” buttons can be used to surf through input port connections. However, since there are multiple outputs/users, the question becomes “which output connection is being changed?” As a result, it is required that an output be selected prior to using the “IN +/-“ buttons.

The output port can be selected in two ways:

- by pressing the “OUT” button before selecting the output port number
- by pressing the “OUT” button after selecting the output port number

In both cases, the user must enter the output port number using the Numeric Keys (0-9). However, when the “OUT” button is pressed prior to selecting the port number, there will be a two (2) second delay after the last digit of the output port is entered that must expire before the output port is accepted. To avoid this delay, press the “ENTER” button to immediately accept the port number.

Once the output port has been accepted, there will be a five (5) second timeout, during which the user must press another button (“IN +,” IN -,” or “SCAN”). Each subsequent press of “IN+” or “IN-“ will renew the timeout, waiting for you to press it again (to advance or go back by one more Input channel). If no new command is sent to the switch before the timeout expires, the switch will forget the selected output, and pressing the “IN +/-“ buttons will have no effect.

All output channels can surf inputs at once by pressing the “ * “ button prior to pressing the “IN +/-“ buttons.

Examples:

Change connection of Output 1 from Input 1 to Input 3:

<**OUT**> + <**1**> + wait 2 seconds + <**IN+**> + <**IN+**>
<**OUT**> + <**1**> + <**ENTER**> + <**IN+**> + <**IN+**> (must press <**IN+**> within 5 seconds of pressing <**ENTER**>)
<**1**> + <**OUT**> + <**IN+**> + <**IN+**> (must press <**IN+**> within 5 seconds of pressing <**OUT**>)

Jump To Input

With the output port selected, a user knowing the desired input port number can enter it using the Numeric keys (0-9). Just as with using the "OUT" button, pressing the "IN" button after the number will force the command immediately. If the "IN" button is pressed prior to the port number, the "ENTER" button must be pressed to avoid a two (2) second delay before the input port is accepted.

Examples:

Quick method to change Output 1 from Input x (any) to Input 8:

<**1**> + <**OUT**> + <**8**> + <**IN**>

Quick method to change Output 12 from Input x (any) to Input 20:

<**1**> + <2> + <**OUT**> + <2> + <0> + <**IN**>

Jump To Output

Users can also change ports by specifying the input port number first. Similar to selecting the output port first, the "IN" button can be pressed either before or after entering the port number. Once the input port has been selected, the output port can be selected, following the same format as "Jump to Input…"

Expiration of a five (5) second timeout will force the switch to forget the entered input port number.

Example:

Quick method to change Input 1 from Output x (any) to Output 8:

<**1**> + <**IN**> + <**8**> + <**OUT**> (must enter the <x> + <**OUT**> command within 5 seconds of pressing <**IN>**)

Connect All

It may be desirable to broadcast the video signals from one input to all of the outputs. In this situation, the user can quickly make all of these connections by using the " * " (asterisk) button which selects all outputs. With the input port selected, pressing the " * " button will immediately force the command to connect all output ports to the selected input.

Example :

Connect all users to Input 2:

<**2**> + <**IN**> + <*****>

The " * " button can also be pressed prior to selecting the input port. In this case, the command will take effect once the input port has been selected.

<*****> + <**2**> + <**IN**>

If no command is received before the five (5) second timeout expires, the switch will forget the " * " key-press.

Save and Recall

This video matrix switch provides the ability to save and recall up to 100 switch configurations. The switch configurations define the current port connections, volume control settings, and video blank status. The IRT-UNV IR Remote can be used to access these configurations by using the “SAVE” and “RECALL” buttons.

To save a configuration, press the “SAVE” button followed by Numeric key(s) 0-99 corresponding to the memory slot the configuration is to be saved in. After the numeric key(s) press the “Enter” button. If the “Enter” button is not pressed, after two seconds the function will timeout and the number entered will be saved as that configuration.

Configurations can be recalled in much the same manner. To recall, press the “RECALL” button followed by the numeric key (s) corresponding to the memory slot from which the configuration is to be recalled. After the numeric key(s) press the “Enter” button. If the “Enter” button is not pressed, after two seconds the function will timeout and the number entered will be recalled to the current configuration.

Multiple Switch Control

All compatible NTI matrix switches will work with the same IRT-UNV IR Remote control. As a result, a user with multiple NTI matrix switches may find that, if the switches are installed too close together, both switches may respond to an IR command intended only for one switch. Or, the user may want to control multiple switches with a single remote, instead of having one remote per switch. To accommodate this situation, the IRT-UNV IR Remote provides the “SYS” button, which can be used to select the NTI switch to be controlled.

All switches will have the capability to allow the user to set the switch address (0-15). Each switch to be separately controlled must be set to a different address prior to using the Remote Control. With the addresses set, press the “SYS” button on the IRT-UNV, followed by a two digit number corresponding to the address of the matrix switch to be controlled.

Upon accepting the “SYS” command, the switch with the corresponding address will illuminate the “IR” LED and respond to all IR Remote commands and will blink the “IR” LED on the front of the switch for visual indication. All other switches will ignore any further commands, until the “SYS” button is pressed again. To select a new NTI switch to control, press the “SYS” button again and repeat the process.

Canceling a Command

Considering the number of key presses required for some of the commands, it’s possible that the user may inadvertently press an incorrect button. Should this happen, the user can press the “ESC” button to cancel a command. Provided the command has not been accepted by the system, pressing the “ESC” button will cause the switch to “forget” or “erase” all button commands from the current command sequence. Once the command sequence has been cancelled, the user can begin entering the command again.

Technical Specifications For IRT-UNV

Number of Controllable Systems	Max: 15
Pushbutton Control	29 keys
Power supply	2x AAA Battery
Chassis material	Plastic
Approvals	RoHS

Troubleshooting the IRT-UNV

PROBLEM	SOLUTION
IRT-UNV is not selecting outputs or inputs	• Check battery • The IRT-UNV may be configured to control the wrong switch- see “Multiple Switch Control” above.

Troubleshooting the VEEMUX

PROBLEM	SOLUTION
VEEMUX will not boot up	1. Make an RS232 connection to the VEEMUX as described on page 6. 2. Set the terminal program to communicate at 115200bps. 3. Power ON the VEEMUX and, as it is powering up, press and hold the **<Tab>** key until a boot prompt appears (**VEEMUX>**) in the terminal program. 4. At the boot prompt type the following: **VEEMUX>nand erase config** and press the **<Enter>** key. 5. Power-cycle the VEEMUX. It should bootup and resume normal operation with all factory default settings restored. **Any customized settings previously entered will be erased and will need to be re-entered.**

CREATION OF CUSTOM X509 CERTIFICATES

The VEEMUX SM-16X16-HD4K (and other sizes) is designed to be configurable with security to limit access to their web interface controls. The VEEMUX includes a default x.509 certificate. However, this procedure will help you create your own custom x.509 certificate to use with this feature. This procedure was created using CentOS and OpenSSL.

Note: Do not disable access to the VEEMUX web interface using http before you verify that the https client authentication works properly (see last page).

I. Using Self-Signed Certificates for VEEMUX Series Products

We can use self-signed certificates to access VEEMUX products with HTTPS with a self-signed root certificate authority. In this procedure, our root certificate authority needs to be explicitly added to every PC as trusted authority, to access the product page.

1. Creating a Self-Signed Certificate Authority using OpenSSL

An example SSL configuration file to use can be found here: http://www.networktechinc.com/download/openssl.cnf
When using this document, make a copy of the current default openssl configuration file and replace it with the file above.

a. Creating the Certificate Management Files and Directories

The following directories are made for organizing the files being used and generated. These directories are also used for other procedures in the document.
1. Create directory "ntiCA" in /usr/local/ssl for ntiCA certificate management and change to that directory. If you prefer, this directory name can be set to any other name like MyCompanyCA. Make sure the **`openssl.cnf`** file is edited to match the changes to the folder name. The **`openssl.cnf`** file can usually be found in /usr/local/openssl/openssl.cnf on local installations of OpenSSL.

```
# mkdir /usr/local/ssl/ntiCA
# cd /usr/local/ssl/ntiCA
```

Create the following directories in the ntiCA directory: **(The number sign (#) is the command prompt, not part of the command.)**

```
# mkdir CA
# mkdir server
# mkdir server/certificates
# mkdir server/requests
# mkdir server/keys
# mkdir user
# mkdir user/certificates
# mkdir user/requests
# mkdir user/keys
```

Perform the following commands in the ntiCA directory:

```
# cd /usr/local/ssl/ntiCA
# touch index.txt
# echo "01" > serial
```

b. Creating the CA Key and Certificate

The general process for creating a certificate includes:

1. Creating a private CA key
2. Creating a certificate request
3. Creating and signing a certificate from the certificate request

1. Create the private CA key:

```
# cd /usr/local/ssl/ntiCA
# openssl genrsa -out ./CA/ntiCA.key 2048
Generating RSA private key, 2048 bit long modulus
.....++++++
......++++++
e is 65537 (0x10001)
```

2. Create the CA certificate signing request:

```
# openssl req -sha512 -new -key ./CA/ntiCA.key -out ./CA/ntiCA.csr
```

```
You are about to be asked to enter information that will be incorporated into your certificate
request.
    What you are about to enter is what is called a Distinguished Name or a DN.
    There are quite a few fields but you can leave some blank
    For some fields there will be a default value,(indicated by the characters "[ ]")
    If you enter '.', the field will be left blank.
  -----
    Country Name (2 letter code) [US]:US
    State or Province Name (full name) [OH]:OH
    Locality Name (eg, city) []:
    Organization Name (eg, company) [NTI]:NTI
    Organizational Unit Name (eg, section) []:
    Common Name (eg, YOUR name) [NTI CA]:NTI CA
    Email Address [sales@ntigo.com]:sales@ntigo.com

    Please enter the following 'extra' attributes
    to be sent with your certificate request
    . []:
    . []:
```

3. Self-sign the CA certificate:

```
# openssl x509 -req -sha512 -days 3650 -in ./CA/ntiCA.csr -out ./CA/ntiCA.crt
-signkey ./CA/ntiCA.key
Signature ok
subject=C = US, ST = OH, O = NTI, CN = NTI CA, emailAddress = sales@ntigo.com
Getting Private key
```

c. Verifying the CA certificate contents

At this point we have our self-signed CA certificate and our CA key, which will be used to sign the VEEMUX certificates that we create. To verify the certificate contents, use the following command:

```
# openssl x509 -in ./CA/ntiCA.crt -text
```

The output should look similar to this:

```
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number:
            b2:ce:14:9d:bf:52:f5:1f
    Signature Algorithm: sha512WithRSAEncryption
        Issuer: C = US, ST = OH, O = NTI, CN = NTI CA, emailAddress = sales@ntigo.com
        Validity
            Not Before: Dec  4 20:00:24 2018 GMT
            Not After : Dec  1 20:00:24 2028 GMT
        Subject: C = US, ST = OH, O = NTI, CN = NTI CA, emailAddress = sales@ntigo.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
```

```
                        00:b0:43:2b:de:93:7b:ac:1f:24:96:9d:e9:98:26:
                        44:bc:cb:7e:04:ec:c2:64:da:60:59:a1:c8:b7:42:
                        52:04:b7:b2:91:b1:10:db:ea:04:25:52:14:8b:52:
                        a4:7f:5a:fc:08:65:c6:77:44:8b:48:27:71:68:00:
                        c2:09:a2:b4:4a:3d:f9:3c:f8:d0:69:24:e8:44:b8:
                        07:57:e1:57:2d:0e:9b:2f:3e:df:4c:71:00:45:bb:
                        ff:2d:a6:7f:11:2d:34:ca:f2:07:f5:79:f0:4f:9b:
                        d8:d3:ad:04:3b:3c:56:07:25:c1:be:fe:09:03:8a:
                        6e:4d:72:82:ad:67:22:2c:54:1b:d5:69:5b:2b:67:
                        1f:12:f5:98:ef:a4:10:1d:56:83:13:ca:8d:d7:2f:
                        c5:0a:da:d5:3b:30:25:9a:2c:6f:8c:94:c1:69:35:
                        e2:38:9b:1b:37:53:ff:d6:2d:3e:d9:1c:7a:03:b3:
                        71:a6:76:16:f4:eb:35:2a:f2:86:6f:40:d9:cc:6e:
                        59:31:ef:94:11:cf:cc:52:9d:eb:8e:06:69:67:ee:
                        86:98:b0:54:11:61:71:aa:ae:19:2a:f3:77:ce:95:
                        2c:a5:87:0d:10:16:b9:5e:88:c8:03:da:d9:6d:90:
                        3b:ca:4c:32:15:0c:ba:05:64:79:c7:4b:b0:7a:f5:
                        26:5d
                    Exponent: 65537 (0x10001)
            Signature Algorithm: sha512WithRSAEncryption
                 9f:d2:50:61:36:f3:d9:b9:cb:39:5e:31:d6:2a:a8:e4:03:f0:
                 e0:65:4d:37:e0:60:cd:71:f5:5a:6d:7d:87:53:6e:2e:8b:3a:
                 f2:fb:73:fc:21:51:63:79:8a:2d:5d:a9:c2:a9:47:a1:b3:17:
                 9a:2e:5b:8a:7f:29:ab:08:cb:2f:52:70:26:2c:76:2d:2d:07:
                 81:cc:84:6f:59:db:f3:be:fe:77:dc:67:6b:5d:ff:b3:17:24:
                 bd:f3:c0:cc:83:10:d0:17:67:2d:e5:5b:4b:59:aa:80:fb:ec:
                 53:ed:e4:c5:0d:a1:0d:13:b3:0b:ee:a4:c2:f0:d2:a0:29:ef:
                 11:f5:6a:29:8b:46:ed:1a:64:2b:93:02:af:0d:7f:83:28:2c:
                 a2:11:2e:e6:fc:af:61:d2:df:eb:e2:c0:e2:46:6e:ef:51:6e:
                 e1:db:4f:d4:24:2b:6d:63:21:d0:3c:f2:02:6e:d0:63:10:bf:
                 1c:9c:bf:31:c8:74:cd:88:51:7b:cc:a6:8d:6d:c1:fb:5c:63:
                 8a:dc:74:de:5f:04:d2:2d:b0:5b:c7:65:06:37:c0:42:8d:87:
                 22:2e:2d:59:dc:89:6c:e4:32:fe:2f:88:da:42:50:6e:67:3e:
                 6c:7c:86:9b:f4:20:60:6b:26:c2:cd:0b:97:d8:e1:f5:f9:c1:
                 4c:32:6c:ab
        -----BEGIN CERTIFICATE-----
        MIIDLjCCAhYCCQCyzhSdv1L1HzANBgkqhkiG9w0BAQ0FADBZMQswCQYDVQQGEwJV
        UzELMAkGA1UECBMCT0gxDDAKBgNVBAoTA05USTEPMA0GA1UEAxMGTlRJIENBMR4w
        HAYJKoZIhvcNAQkBFg9zYWxlc0BudGlnby5jb20wHhcNMTgxMjA0MjAwMDI0WhcN
        MjgxMjAxMjAwMDI0WjBZMQswCQYDVQQGEwJVUzELMAkGA1UECBMCT0gxDDAKBgNV
        BAoTA05USTEPMA0GA1UEAxMGTlRJIENBMR4wHAYJKoZIhvcNAQkBFg9zYWxlc0Bu
        dGlnby5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCwQyvek3us
        HySWnemYJkS8y34E7MJk2mBZoci3QlIEt7KRsRDb6gQlUhSLUqR/WvwIZcZ3RItI
        J3FoAMIJorRKPfk8+NBpJOhEuAdX4VctDpsvPt9McQBFu/8tpn8RLTTK8gf1efBP
        m9jTrQQ7PFYHJcG+/gkDim5NcoKtZyIsVBvVaVsrZx8S9ZjvpBAdVoMTyo3XL8UK
        2tU7MCWaLG+MlMFpNeI4mxs3U//WLT7ZHHoDs3Gmdhb06zUq8oZvQNnMblkx75QR
        z8xSneuOBmln7oaYsFQRYXGqrhkq83fOlSylhw0QFrleiMgD2tltkDvKTDIVDLoF
        ZHnHS7B69SZdAgMBAAEwDQYJKoZIhvcNAQENBQADggEBAJ/SUGE289m5yzleMdYq
        qOQD8OBlTTfgYM1x9VptfYdTbi6LOvL7c/whUWN5ii1dqcKpR6GzF5ouW4p/KasI
        yy9ScCYsdi0tB4HMhG9Z2/O+/nfcZ2td/7MXJL3zwMyDENAXZy3lW0tZqoD77FPt
        5MUNoQ0TswvupMLw0qAp7xH1aimLRu0aZCuTAq8Nf4MoLKIRLub8r2HS3+viwOJG
        bu9RbuHbT9QkK21jIdA88gJu0GMQvxycvzHIdM2IUXvMpo1twftcY4rcdN5fBNIt
        sFvHZQY3wEKNhyIuLVnciWzkMv4viNpCUG5nPmx8hpv0IGBrJsLNC5fY4fX5wUwy
        bKs=
-----END CERTIFICATE-----
```

2. Creating a CA-Signed VEEMUX server Certificate (This will need to be done for each VEEMUX device.)

The procedure for creating a CA-Signed web server certificate is similar to that for creating the CA certificate except that the device certificate will be signed using the CA key rather than self-signing with a server-specific key.

a. Create the web server private key using a fully qualified DNS name (or IP address).

```
# cd /usr/local/ssl/ntiCA
# openssl genrsa -out ./server/keys/your_device_fqdn_or_ipaddress.key 2048
Generating RSA private key, 2048 bit long modulus
.......++++++
.++++++
e is 65537 (0x10001)
```

b. Create the web server certificate signing request using the same fully qualified DNS name (or IP address) you used for the private key. **It is vitally important** that you set the Common Name value to the fully qualified DNS name of your web server because that's the value that a browser client will verify when it receives the web server's certificate.

```
# openssl req -sha512 -new -key ./server/keys/your_device_fqdn_or_ipaddress.key -
out ./server/requests/your_device_fqdn_or_ipaddress.csr
```

```
You are about to be asked to enter information that will be incorporated into your
certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value, (indicated by the characters "[ ]")
If you enter '.', the field will be left blank.
-----
Country Name [US]:US
State or Province Name [OH]:OH
Locality Name []:Aurora
Organization Name [NTI]:NTI
Organizational Unit Name []:
Common Name [NTI CA]:192.168.3.144
Email Address [sales@ntigo.com]:your_name@example.com

Please enter the following 'extra' attributes
to be sent with your certificate request
. []:
. []:
```

c. Create a file defining the Subject Alternative Name. This extension file extensions.ext can be made with any text editor, and should be added to the /usr/local/ssl/ntiCA directory. This needs to be defined to know for what domains or IP addresses the certificate will be valid. Add the following lines to the **`extensions.ext`** file:

basicConstraints=CA:FALSE
subjectAltName=IP:**<ip_address>**

Replace "**<ip_address>**" with the IP address you plan to use to access the device. Other options are available for specifying this. Below is an example using a DNS:

subjectAltName = DNS:server.example.com

d. Sign the web server certificate with the CA key:

```
# openssl x509 -req –in server/requests/your_device_fqdn_or_ipaddress.csr -CA
CA/ntiCA.crt -CAkey CA/ntiCA.key –CAcreateserial -out your_device_fqdn_or_ipaddress.pem -
days 1024 -extfile extensions.ext
```

```
Signature ok
subject=C = US, ST = OH, L = Aurora, O = NTI, CN = 192.168.3.144, emailAddress =
sales@ntigo.com
Getting CA Private Key
```

To verify the web server certificate contents, use the following command:

```
# openssl x509 -in your_device_fqdn_or_ipaddress.pem -text
```

Key values to look for are:

```
Subject CN=192.168.3.144
Issuer CN=NTI CA
```

3. Uploading a Self-Signed Certificate Authority to a VEEMUX Device

You should import the "ntiCA.crt" file located in the /usr/local/ssl/ntiCA/CA directory that is generated using this procedure into the VEEMUX. To import this file into the VEEMUX, you must log into its web interface.

On the VEEMUX Web Interface menu Under "Administration" select "Network". In X509 certificates, select "Choose File", select the CA certificate file ntiCA.crt, and click **"Upload CA certificate**".

4. Uploading Server Certificate to a VEEMUX Device

The NTI VEEMUX web server expects the certificate and key as a single file in "PEM" format.

Use the following command to combine certificate and key file to a single file with extension “pem”.

```
cat ./server/keys/your_device_fqdn_or_ipaddress.key your_device_fqdn_or_ipaddress.pem > server.pem
```

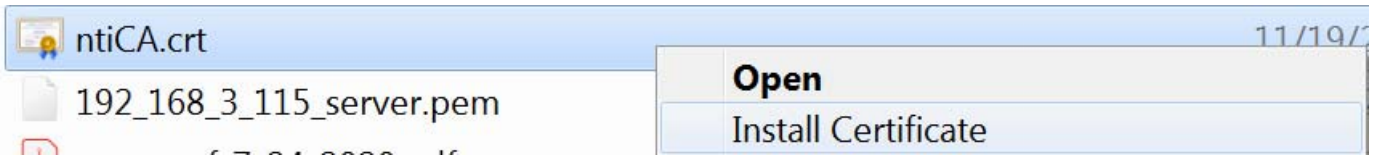
On the VEEMUX Web Interface menu Under “Administration” select “Network”. In X509 certificates, select “Choose File”, select the server certificate and key file, and click “Upload **Server certificate and key"**.
The following is an example of what the **`server.pem`** file should look like:

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAxKmpFfvWbJymSP2Pos/+NIDQvmoIU4xv2FBZBuOrc+uRKf1D
y2VeFKlMufp2JXMTxSHXCOjyZgVvEH9jb1VORU6WRz2/6vG5hYDqFa8dptC9YJ2S
yRUa6ST0bwSZCCHMfE6Qxk/1ren59rtckYpygz7/VdcNAhgcoLoIHRoJFTLw0NMF
MTt1kW1cNXTSBT//s5jTYOfba7qck1HpSRTPdWOHwajnoyH9t/I/JnFdtJJu3IQN
qnA9G3pQdoi/J3Nug2CNKrSLJutBtTAmLQsJjUlmwg4MvcxpWURATNOwnnGAhuX1
t694QVI8owZ+bycidUjGSmdr3GUQ4i6/97sdeQIDAQABAoIBAEHVle/xDVfwnM3k
bBgRzsRetwJ3VnA5nBtqOlK6RIiavE61JOPK/FKoVjIQAUsKGfOtFeI6sSKr+Ez8
iBn2Eayr4SzaJAuEOznQ7QvzQlbcm/ji5wd/lDGmGFmtzVjmj6CxYE+y5siggfgx
woxKL4l2Jl3jDsy7q6G2hQ7Q72dzvtlEFRBaZvBdQ5LjPCrnZxzQBZGXCMUS/ro9
IWwlXzpKUceOIDG27WqpSFa7DSzwouq8gSkIGNxe643pBGFJYLoz4+O0DyFiaete
izqNh9ulhgrwu6AVwO/Mtl5icSdPZgtgQ6Az1/tcT5y89zKyaNHEtXho5jiOvlPi
+iYCyuOCgYEA5jJXHAxcdMzDBsjUln8D1nYr87CSac7DEG4Oo2S1fBL93rUe62Cu
cPuyy8goFFKtmbxdl1dZtxmQww+VMWxZ8jBsH81VexqgkiYgTy1dde/Ih6v94CcU
nFiouwU92BRWt7zf3y6AhrR2bLfUCBrNqscdPCS7QuYKkPlwiCjzUNsCgYEA2rUK
w8u3dOpFEsJYttxv1BHSLVlBN7wsACo2RC9qkevEPAcjMmSCzJpgiA6JpwMlZa9b
AfU1zACtkHkW7gd8Xb7HOJkCpH4FN+YO9SxEWuE/XetznrV4vobPJbzzHHDG7cUb
jvaYcDM6UUQSLPXlUp5RWuwnMAc6FdVJqKT14TsCgYEA1LuO3v/ZbaNRVHLCa7ZD
wKOCnzj9hcSrZgKfioZmZZxTer4dLd7yNr2UlViLGYTyo9F9GICEC38X1fwPn1YH
pZb0RUuIBLUt0QJk92bwKS6IPkFG5CCZnoccngCe75KUNUbaCTG7W0Fo873KuBa1
HG7YaJ11ZTScbS/nvB1EBuMCgYAXddAUpLebbjYwmw5VHzRHtVmsT6S1S9QUeHK1
wbhWysmT/tgBsdJuDClKrvSJG8dJLxQ+E4wfynrTwol5IwhuLebE5XTpHDOHGYCF
QChc70iS1IzkfBlkpqVV0PzrEhXkr34TSdR0RKp+ySSB+iaNRDpJ3IcfmcbbTLPI
CVnuvQKBgCpS6uxdhXJMd6Wgeutq9gQOQ8Og+VtMWHmIuEXvW9oth+jCKTRmuz3W
S7MgNuljPctusLig+exnUG8fxy467lCk7nAgslDrozGjPpix2BZF5AhuoCwCklwc
3LWF4AnRW4VgcUSTBSzEIOsDai/4oqbz65Ry2ZpXYzn5jpQfQQsc
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIID4TCCAsmgAwIBAgIJAJMjatDg7g/aMA0GCSqGSIb3DQEBCwUAMIGcMQswCQYD
VQQGEwJVUzELMAkGA1UECBMCT0gxDzANBgNVBAcTBkF1cm9yYTEhMB8GA1UEChMY
TmV0d29yayBUZWNobm9sb2dpZXMgSW5jMRQwEgYDVQQLEwtFbmdpbmVlcmluZzEP
MA0GA1UEAxMGTlRJIENBMSUwIwYJKoZIhvcNAQkBFhZqdXN0aW4uZmVycmlAbnRp
Z28uY29tMB4XDTE4MTIwMzE4MzkzNloXDTIxMDkyMjE4MzkzNlowgaIxCzAJBgNV
BAYTAlVTMQswCQYDVQQIEwJPSDEPMA0GA1UEBxMGQXVyb3JhMSEwHwYDVQQKExho
ZXR3b3JrIFRlY2hub2xvZ2llcyBJbmMxFDASBgNVBAsTC0VuZ2luZWVyaW5nMRUw
EwYDVQQDEwwxOTIuMTY4LjMuNzExJTAjBgkqhkiG9w0BCQEWFmp1c3Rpbi5mZXJy
aUBudGlnby5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDEqakV
+9ZsnKZI/Y+iz/4OgNC+aghTjG/YUFkG7Stz65Ep/UPLZV4UqUy5+nYlcxPFIdcI
6PJmBVUQf2NvVU5FTpZHPb/pUbmFgOoVrx2m0L1gnZLJFRrpJPRvBJkIIcx8TpDG
T/Wt6fn2u1yRinKDPv9V1w0CGByguggdGgkVMvDQOwUxO3WRbVw1dNIFP/9LmNNg
59trupyTUe1JFM91Y4fBqOejIf238j8mcV2Okm7chA2qcDObelB2iL8nc26DYIOq
tIsm6OG1MCYtCwmNSWbCDgy9zGlZREBMO5aecYCG5fW3r3hBUjyjBn5vJyJ1SMZK
Z2vcZRDiLr/3ux15AgMBAAGjHjAcMAkGA1UdEwQCMAAwDwYDVR0RBAgwBocEwKgD
RzANBgkqhkiG9w0BAQsFAAOCAQEAFM6WKCwdU1ARIKc8tM4bI9GmA7VEC+69CgCo
GkiZ4WBEYfibc265uH7Lz+/z88rdflXW9B5Xc2B2GCzCxPYIwLcHfZpxbf6C7kp2
bs2OHzvCTGluVwm+r51bjmqQZzUQVH5vMZP8ct7HbOZbhtc6KwFRFIW5CZSu1qhn
tfxBEFiQGaR7wNTuEk9B4LJ3ghSNBYC+gPXOCDQSK3taXq1uA5fx08/6QBULQgbA
FzosbstNc7INpqtK9OZUOtwO3HAnr+gZJb3i4XQK5BReUlCLhlKy6X36Px4hf1rh
rf6da7kDfkC0g3x6B1EJzR/Cmazfmutd/AKKpvFT25YKE78jMQ==
-----END CERTIFICATE-----
```

5. Accepting a Self-Signed Certificate Authority as Trustworthy

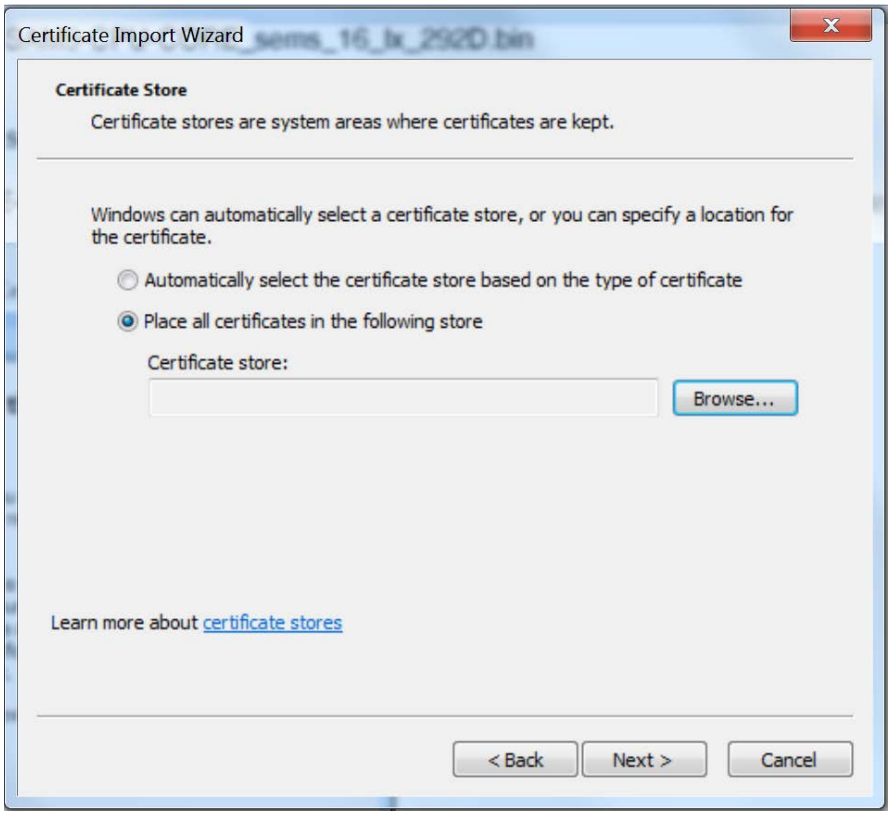
How to add a Self-Signed Certificate Authority as a Trusted Root Certification Authority on Windows

The browsers must recognize and trust the Certificate Authority created. The following are directions for trusting the newly created CA.

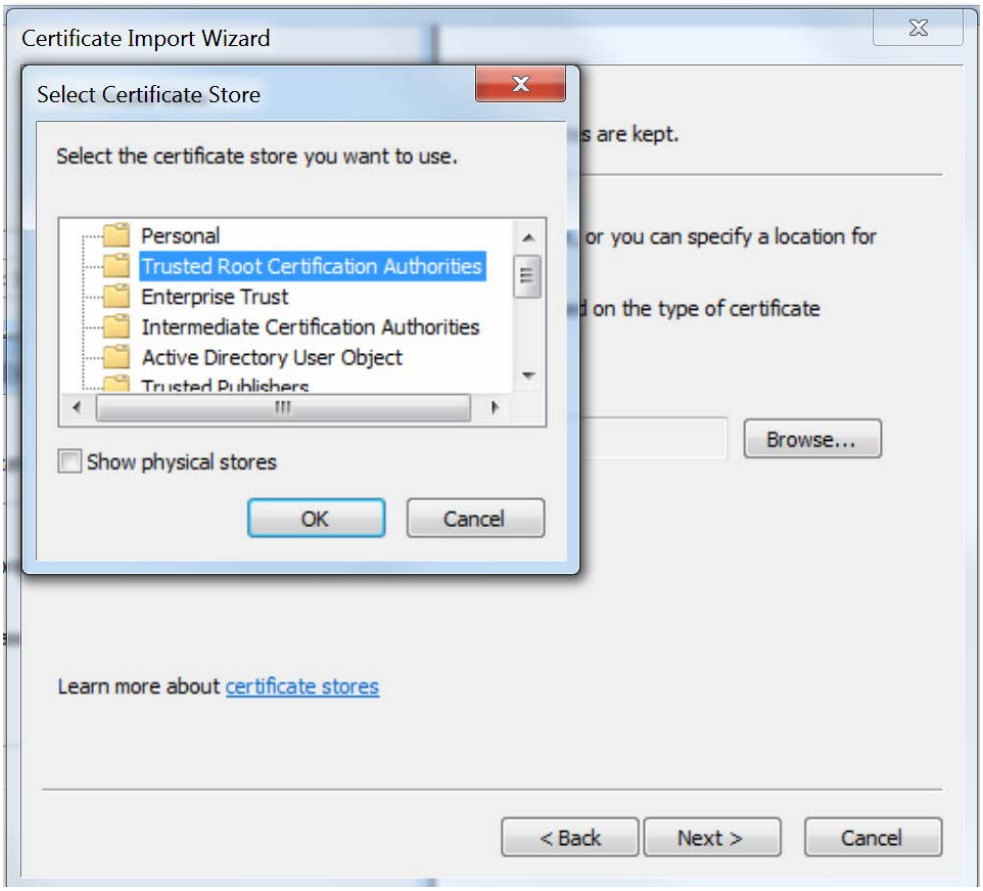


1.Right click on **"ntiCA.crt"** on the PC. Choose "**Install Certificate**".

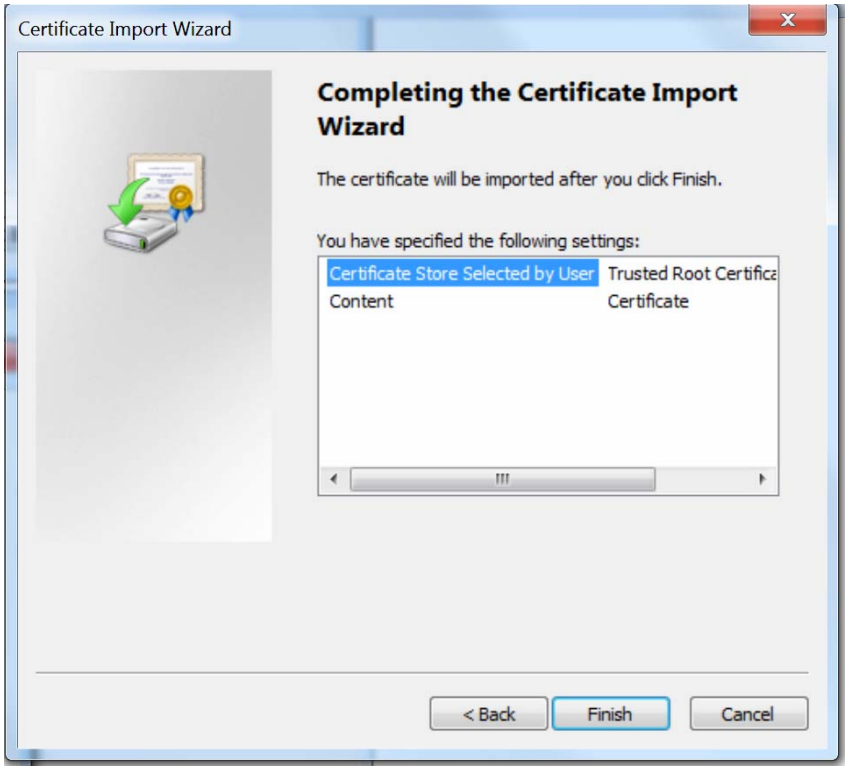
2. There will be a wizard to guide you through the next steps. Click "**Next**".



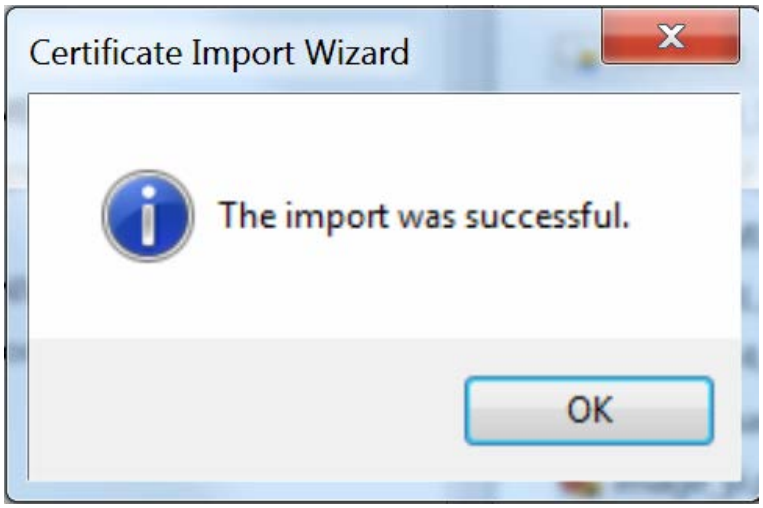
3. Click **"Browse"** and then.....



.....select **"Trusted Root Certification Authorities"**



4. Click **"Finish"** to complete.



5. You are done! Restart the preferred browser.

How to add a Self-Signed Certificate Authority as a Trusted Root Certification Authority on Mozilla Firefox

Mozilla Firefox does not use Window's Certificate Authorities. For the Firefox browser to recognize your CA, do the following:

1. Open the Mozilla Firefox browser.
2. Type "about:preferences#privacy" in the URL field of the browser.
3. Under "Security" in the "Certificates" section, press the "View Certificates" button.
4. Navigate to the "Authorities" tab.
5. Select "Import"
6. Find your self-made CA and press "Open"
7. Select "Trust this CA to identify websites" and click "OK".
8. Restart the Firefox browser.

Note that some of these directions may be slightly different for older versions of Firefox.

II. Using External CA Signed Certificates for VEEMUX Series Products

1. Creating a certificate signing request for External Certificate Authority

A Certificate Signing Request must be provided to an external Certificate Authority like DigiCert, Verisign, or Comodo.

The Certificate Signing Request should be made using the following command:

```
# mkdir thirdparty
# mkdir thirdparty/certificates
# mkdir thirdparty/keys
# openssl genrsa -out ./thirdparty/keys/server.key 2048
# openssl req -sha512 -new -key ./thirdparty/keys/server.key -out
./thirdparty/certificates/server.csr
```

Below is an example of a valid certificate signing request:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDGzCCAgMCAQAwgawxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJPSDEPMA0GA1UE
BxMGQXVyb3JhMSEwHwYDVQQKExhOZXR3b3JrIFRlY2hub2xvZ2llcyBJbmMxFDAS
BgNVBAsTC0VuZ2luZWVyaW5nMR8wHQYDVQQDExZ3d3cubmV0d29ya3RlY2hpbmMu
Y29tMSUwIwYJKoZIhvcNAQkBFhZqdXN0aW4uZmVycmlAbnRpZ28uY29tMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzc1BU6EbJL4hNYj9UfM2EO2qzTHr
c/OUL8kaoZZyExpnK3ekrlGWSTciV3hP4ZY+AlxuYOP5pzWWnIGXzBHgw0XybIgM
/IraRiEzrh8jw+kKUCjcBhP1DQXES7EhX1MDoNyTVEaIXF5Ya8RWJMxisrd4VTfc
eCm3zgUq1HN4rmY4Uj4EN7fsDrT2QppClPKvFiFaFdwAsi7GXA8q2Gffx5mfhPiw
yb5qAPPx78f6wTYk/MeasUDVDC5DHl0L87MfYkMLhc+1tLIOxUSKu0NJYczuC/g0
OAuk+khgkH5gau9t83lCThEI6OkHswNR8P9eHSHTOo0U9XfuOywmpL6ByQIDAQAB
oCkwJwYJKoZIhvcNAQkOMRowGDAJBgNVHRMEAjAAMAsGA1UdDwQEAwIF4DANBgkq
hkiG9w0BAQ0FAAOCAQEAqQ2Es1PHsBrPIDwCLZ/9+4hTCcgTyIXBb6A7TmvLmnzF
JcyC7/78np+jGbhSMbM9Pgh6DJpcTuIgSSDlwzP9JJLGq+5jKn3Lm6tScGCz7YYT
cf6VFtPyCP5GkNVqfZfTApKESj40tIqM/gVyByQzD1CFL4FIGhRrYXpbbGpoBpj/
C9S1FZT5XjuS/ixbKm/O6GwzO6H6US8PAFMtViSHaOg6i9nhIBWUg7OeOjwBdnTb
JaQpAIF3OrTbQ/iKgXzYb4L9bowExyvP/DldOx7vG9egbi4WJjjIhuOssxFb7Q1J
ODh+Cc7uALD5PhLaUgglhi8a1IgtlIuiPlB1UztZcg==
-----END CERTIFICATE REQUEST-----
```

Upload your CSR to your Certificate Authority to get the certificate.

2. Uploading Server Certificate to a VEEMUX Device

The NTI VEEMUX device expects the certificate and key as a single file in "PEM" format.

The server certificate file with extension “pem” should be received by your external CA after submitting a certificate request. Get your server certificate in a .pem or .cer format. Copy your server certificate into another file and add the device key as shown below.

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAyQ1pnlRkr3r4wlCJiOjYrFW2+bXqv6WrotMyGfIRZaZkLo5J
1whYb/uFcX2Unc/H5X7wDa3gawr6iJki/dVf8X16gpHicrWR+WFAiRs/D7z+B/ew
iaM5vqDMTw5mvAmnNaOsZ3gsOnSEFgiZMewkimJYyyfHjHv2kpW51HekWraa8dVJ
dunAhzeTTcDghxhT2p2hsKxARB5m4DOvjv2aEcxnRixxvDA/2uggxfXJil8SCpAk
qxiJzeqPv+xRvp/jTpI1wlGPmuemJILGs95iFOv8WpUFM3xDR3o8GCuOl8eokEEA
lpWNgiRuQcjjh464Z8rbr8lO+FJP0AhEJ7XufwIDAQABAoIBABStQHN8Em7JotO5
HKwqBb4rgonj36SeESzJs5lff9KIbjOrfQSUYyQBJhQp6iLgv5oml+GQREg99M4f
ka2xSBC56uOKxVMuwTh4e/6dwrqHoUiIfKtrEgE84EYxIPettniZwJ1Tipjoar0p
XTf5JTjmLGOYT7lu9kjVBSuIsmpxtn8xNu1po5l1zY/Soy3p38qTKwNJ1n9CnJXo
q9LTnfiGvq7JfRhjHFx4AYKJsZMNE4ZI4WEr4B72wxifpINr0llk0ezrKn5UB+Ug
8nXONonxAlotv7McIM+u4cjv8ww3yTb7Mw5isAS9zeS9eN5ticLLh5yFFJyYKai6
e2HgpEECgYEA7XY94+z2Xy48z5ogQErgHCwFv7wWP6kUObJGkITCygPON5jqKSuo
pprtpr4gpvH8V78krPA5sdXrmm3UyVmrK5z89T0SQMnSls6HX+vfVsHVxmKW3Wa6
BChtA2+YsHPtpFeAYK/rUxh/3rRblFOpTfpiHpmYEWNOwyXT2Jg2HPcCgYEA2L+D
t6HvFnscOdcr1KE2VGEmLgD6ll2eUBp3/6+MrAqgdVqaaBgxuv57sWNS7Ys4Fv7V
EioI/CwDcB4uIIK4mbenW39uu2OZAGceNXOmdOsg97Vxs7GR76tyC9irei6u0HX2
ySpb5L8cB1PevTP058GHVjqhKmSrzQx/URx9ALkCgYEAyhZc6YKa0bnp6svCMrUG
MTON2O9S5O6h1dBQmWFC3OWsizxJ26vaJZ+oLMWVyD4cgRicv8i4QDxL++sIsirr
r3w1EwhcZmLcI5e0Qf/c3Fqt8d2pgtaP7EXzMH9itJiUX85P5PkSDm/FMuTPI1Zn
uYMiyePxNKsNNqsUtToko1UCgYAsRWHX/iFhjB/FyKdRNORt87Hir5x/XfvaDK35
8ZdgBIOltK3ZGSf/M798CfeEQW1hdQd8QE25hBvnqKJvTYP7EcIDNFIfwEYeCPHo
pQiY1PXU4qCovVo7g981gDn2KNbYCWAw0pAWdtp4vK7AIn6hX6wO9sa4a/uTVDwl
CxaVMQKBgFhJvBHD9cKY41kMTYHvNPaXmJAtWlEBMyVkFWAtz+e4C+ojzyLuI34e
TPkk8ivxeZO0c8X241dIBZKbwCLnV3TprvA2UeMui5LjyU0H4AEnzan1H4S2G+Rz
gWWEFZmTlg0R7f7H9uBPpoNjnJzhsAMkBAVgwPJvY6PyoPP0tglR
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIDazCCAlogAwIBAgIJAMib9H5kqNSpMA0GCSqGSIb3DQEBCwUAMFkxCzAJBgNV
BAYTAlVTMQswCQYDVQQIEwJPSDEMMAoGA1UEChMDTlRJMQ8wDQYDVQQDEwZOVEkg
Q0ExHjAcBgkqhkiG9w0BCQEWD3NhbGVzQG50aWdvLmNvbTAeFw0xODEyMDQyMDA1
MzhaFw0yMTA5MjMyMDA1MzhaMHExCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJPSDEP
MA0GA1UEBxMGQXVyb3JhMQwwCgYDVQQKEwNOVEkxFjAUBgNVBAMTDTE5Mi4xNjgu
My4xNDQxHjAcBgkqhkiG9w0BCQEWD3NhbGVzQG50aWdvLmNvbTCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAMkNaZ5UZK96+MJQiYtI2KxVtvm16r+lq6LT
MhnyEWWmZC6OSdcIWG/7hXF9lJ3Px+V+8A2t4GsK+oiZIv3VX/F9eoKR4nK1kflh
QIkbPw+8/gf3sImjOb6gzE8OZrwJpzwjrGd4LDp0hBYImTHsJIpiWmsnx4x79pKV
udR3pFq2mvHVSXbpwIc3kO3A4IcYU9qdobCsQEQeZuA9L479mhHMZOYscbwwP9ro
IMX1yYpfEgqQJKsYic3qj7/sUb6f406SNcJRj5rnpiSCxrPeYhdL/FqVBTN8Q0d6
PBgrtJfHqJBBAJaVjYIkbkHI44eOuGfK26/JdPhST9AIRCe17n8CAwEAAaMeMBww
CQYDVR0TBAIwADAPBgNVHREECDAGhwTAqAOQMA0GCSqGSIb3DQEBCwUAA4IBAQBd
CNA7H/4DeYR70j13yOmN9ajgRU5XbzETNA1Cr+3W+2YuaJ4cAOdo/e9TLwhTC1pH
E1HKrkFyjag5JEE32PT/Pn+gb++/2U94jw7qatqrcwiboy7ytJcZgEKYOEPjVfUJ
fS1saVbgWmQMGAOLuRr2NLLU9vCYlTpeeTGyC/ve5k3rjOYFAcQL5rKa9D7Vgn6r
IWTU13uwvDxP7QzvkgjKuEJkWlg2DlMS3bw2ejAOc9HAl8RCROxm55Z7maRqeLzJ
GLbf3587pCZMQIu21YU9DJ/7ORSN1xdyKQG4KNfOxMHkmuAafqIFp+d8D+3xtVSw
h94zxQI77VarHxLswk3e
-----END CERTIFICATE-----
```


On the VEEMUX Web Interface menu Under “Administration” select “Network”. In X509 certificates, select “Choose File”, select the combined server certificate /key file, click **"Upload Server certificate and key"**.

3. Uploading External CA Certificate to VEEMUX Device:


```
-----BEGIN CERTIFICATE-----
MIIDtjCCAp4CCQDy25JKAce+dDANBgkqhkiG9w0BAQ0FADCBnDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAk9IMQ8wDQYDVQQHEwZBdXJvcmExITAfBgNVBAoTGE5ldHdv
cmsgVGVjaG5vbG9naWVzIEluYzEUMBIGA1UECxMLRW5naW5lZXJpbmcxDzANBgNV
BAMTBk5USSBDQTElMCMGCSqGSIb3DQEJARYWanVzdGluLmZlcnJpQG50aWdvLmNv
bTAeFw0xODEyMDMxODE1NDZaFw0xOTExMjgxODE1NDZaMIGcMQswCQYDVQQGEwJV
UzELMAkGA1UECBMCT0gxDzANBgNVBAcTBkF1cm9yYTEhMB8GA1UEChMYTmV0d29y
ayBUZWNobm9sb2dpZXMgSW5jMRQwEgYDVQQLEwtFbmdpbmVlcmluZzEPMA0GA1UE
AxMGTlRJIENBMSUwIwYJKoZIhvcNAQkBFhZqdXN0aW4uZmVycmlAbnRpZ28uY29t
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtUVXiaF44xtBRQ6if1Ch
evpmQJfxHyQL8KtnGXgAuWk1KNp+3S1culYzlHgMSJU//W/srqnoPh6DmkokhB/r
qYt4KbdeC7t8w4oNX4ltdJz0+7chBBqvoN7DYLS45/OIrTLpaHnbBJPhxsFEREWU
hW1iX14SqTw40X49EfPJdGshORMAEsqwk37JddX440ALrjLcEI82Rv4Mb8EV9oJ8
JyulpWHqfuRVMCn3X/yzHiEP7Dql7nrFjAM8OhmlOJxHizAZQRdqfqHGO09zgrct
qJOQVLMW8amWFn2l3DAzSQdJOrFl1zOx7D2zlBkTYm7gr1E7mzR12uAOfl5owqEL
2wIDAQABMA0GCSqGSIb3DQEBDQUAA4IBAQBxkTZ3oR7eRLv+Q5u2a4iNj6l/UkW9
loHhu9YtMOpijt/CUeD4q3Cu56i6JNyru4of7Q4ZUSU+jTXxWhh2QCb0+eF+LMEC
NnF/J26pfXQNh30mq1KRLq6EpZ5DedSbrRTB/lEO5zm/ChOyY7bOizp/B8+AY4Id
/AU63BULTN2tRL4doNcbEcCtS37YRdRZTJF85es9qlfTKVA4mBYjE5p9bgDzHCdQ
Xliuv5fiELp3O7y7NNLtO9nVRrbzS9YHHmmJORP4j7SPaAxveyFfz93LuQn8kKlw
0dzroXCmGuMVPDilq1Z2ORZVDNw9+AZvk7/lH++EguB5p7y5aP7zpEfN
-----END CERTIFICATE-----
```


Get the certificate of your CA in a *.cer or *.pem format which should be as shown above. Optionally this file may include an intermediate certificate, which would be different from the above root Certificate, in the same file. On the VEEMUX Web Interface menu Under “Administration” select “Network”. In X509 certificates, click “Choose File”, select this CA certificate file, and click **"Upload CA certificate"**.

GENERAL TECHNICAL SPECIFICATIONS

Video	
Video Bandwidth	18 GB/s
Max. Resolution supported	3840x2160 (UHD), and 4096x2160 (4K) @ 60Hz / RGB/YCBCR 4:4:4.
HDMI Compatibility	HDMI 1.4 and 2.0
HDCP Support	v1.4 and v2.2
Color Depth	Up to 12 bits per color
Pixel Encoding	4:4:4,4:2:2, 4:2:0
Control	
Serial	RS232, RJ45 female connector
Ethernet	RJ45 female connector
Infrared	IR Receiver (works with remote control transmitter)
Power	IEC connector for 100-240VAC power connection
General	
Operating temperature	32 to 104°F (0 to 40°C)
Storage temperature	-20 to 140°F (-30 to 60°C)
Operating and Storage Relative Humidity	5 to 90% non-condensing RH
Dimensions (WxDxH)	19x13.75x1.75

Switching Latency

Switching latency is the delay time from the moment a switching command is issued to the moment that the new picture is stably displayed on the monitor. The length of this delay depends on many factors, including but not limited to:

- How much difference there is between the two channels to be switched to or from. Resolution, frequency, color depth, color mode etc.
- Whether or not HDCP encryption is involved
- The monitor's characteristic response time

For example, the switching latency using a Sony XBR-55X850D TV was recorded as follows:

- When switching from a 1080p channel to another 1080p channel, it takes about 3 to 4 seconds to show the new channel on the monitor
- When switching from a 1080p channel to a 4k channel, it takes about 5 to 6 seconds to show the new channel.

INDEX

WARRANTY INFORMATION

The warranty period on this product (parts and labor) is two (2) years from the date of purchase. Please contact Network Technologies Inc at **(800) 742-8324** (800-RGB-TECH) or **(330) 562-7070** or visit our website at http://www.networktechinc.com for information regarding repairs and/or returns. A return authorization number is required for all repairs/returns.

MAN319 Rev.5/10/23