thinklogical®

A BELDEN BRAND

TLX Matrix Switch ADM

Web Based Administrative Interface

PRODUCT MANUAL

May 2023, Revision B

Thinklogical, A BELDEN BRAND • 100 Washington Street • Milford, Connecticut 06460 U.S.A.

Table of Contents

Copyright Notice

Initial release date: December 8, 2022

Subject: TLX Matrix Switch ADM Product Manual
Revision: A, December 2022
Revision: B, May 2023

thinklogical
A BELDEN BRAND

Certified to ISO 9001:2015

MADE IN USA

Website: https://www.thinklogical.com
Facebook: www.facebook.com/ThinklogicalUSA
LinkedIn: www.linkedin.com/company/thinklogical
YouTube: www.youtube.com/user/thinklogicalNA
Twitter: @thinklogical

Preface

About Thinklogical, A BELDEN BRAND

Thinklogical, a Belden Brand, is the leading manufacturer and provider of fiber-optic and CATx video, KVM, audio, and peripheral extension and switching solutions used in video-rich, big-data computing environments.

Thinklogical offers the only fiber-optic KVM Matrix Switches in the world that are accredited to the Common Criteria EAL4, TEMPEST SDIP 24 Level B, and NATO NIAPC Evaluation Scheme: GREEN and the U.S. DoD DISA JITC UCR 2013 APL information assurance standards. And Thinklogical Velocity products are the first system with both KVM and video matrix switching capabilities to be placed on the Unified Capabilities Approved Product List (UC APL) under the Video Distribution System (VDS) category.

Thinklogical products are designed and manufactured in the USA and are certified to the ISO 9001:2015 standard.

Thinklogical is headquartered in Milford, Connecticut and is owned by Belden, Inc., St. Louis, MO (http://www.belden.com). For more information about Thinklogical products and services, please visit https://www.thinklogical.com.

About This Manual

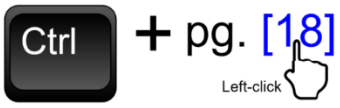
Active Links

This document contains active cross-reference links in the *Table of Contents* and for referenced pages throughout, shown in this format: [18], and for active hyperlinks, shown in this format: link.format.

For **.pdf**: *point/left click*

For **.doc**: *Ctrl/point/left click*

To **return to the front of the document:** *Ctrl/Home.*



Note and Warning Symbols

Throughout this manual you will notice certain symbols that bring your attention to essential information. These are **Notes** and **Warnings**. *Please read this information thoroughly*. Examples are shown below.

Note: A note is meant to call the reader's attention to helpful or valuable information at a point in the text that is relevant to the subject under discussion.

Warning! A warning is meant to call the reader's attention to critical information at a point in the text that is relevant to the subject under discussion.

Connection to the Product

Connections and installation hardware for our products use industry-standard devices and methods. All wiring connections to the customer equipment are designed to minimize proprietary or customized connectors and cabling. Power connections are made with regionally appropriate power cords and approved methods.

Introduction

The Thinklogical ADM is a web-based administrative interface utilized on the following Thinklogical systems: TLX Matrices, SMP systems. ADM efficiently enables both secure deployment and secure maintenance for the aforementioned Thinklogical systems. ADM is intended to provide both a significant reduction in the secure deployment effort and significant enhancements to the operations and maintenance of Thinklogical solutions.

This manual documents the ADM for Matrix switches.

ADM Features

The prominent features of ADM are:

Key operation and management features:

- User account management (web servers and Linux OS)
- IP addressing configuration
- System redundancy configuration / monitoring
- Troubleshooting / status reporting
- DATE/TIME services
- Server upgrade support

Key secure deployment features:

- Firewall configuration
- FIPS 140 (encryption) compliance
- Password complexity enforcement
- Remote logging, auditing
- Secure network topology guidance
- Supports full network encryption
  - Web-based services utilizes https (FIPS 140 compliant encryption)
  - SMP to/from Matrix comms utilizes MACsec (AES-GCM-256, TS compliant)

Warning! The secure deployment features should be configured by experienced Administrators. Improper configuration may result in the Matrix Switch being inaccessible.

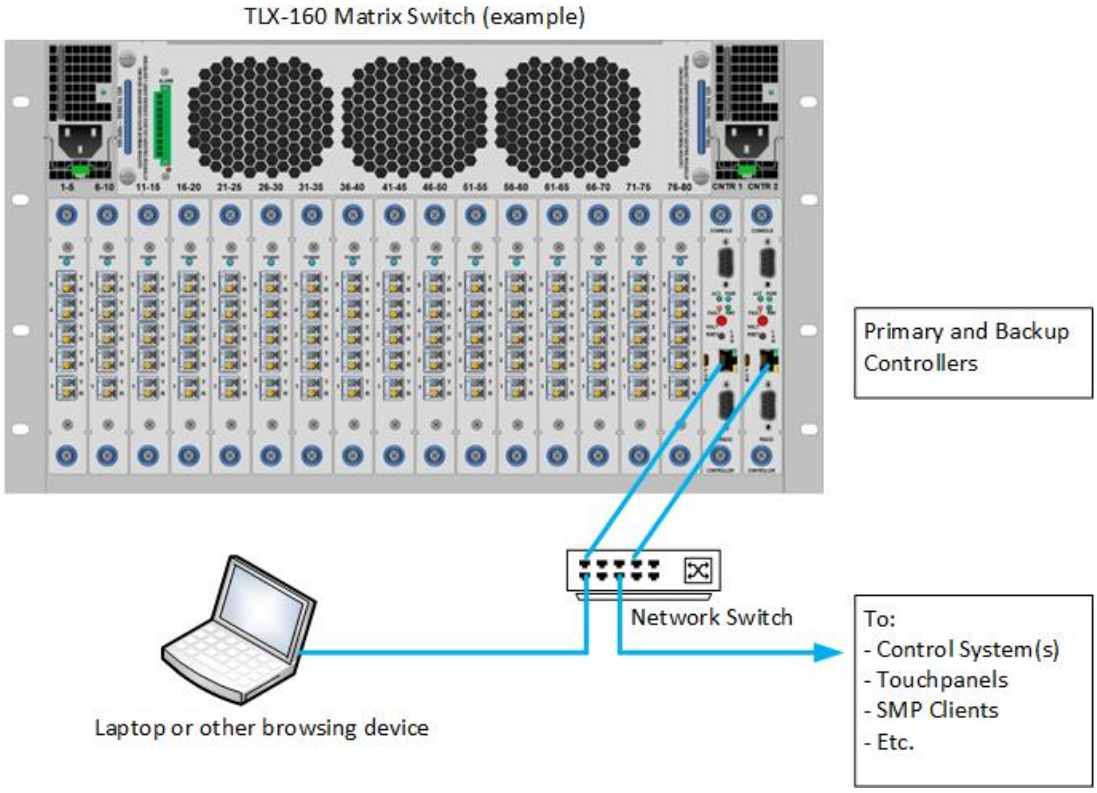
Setup

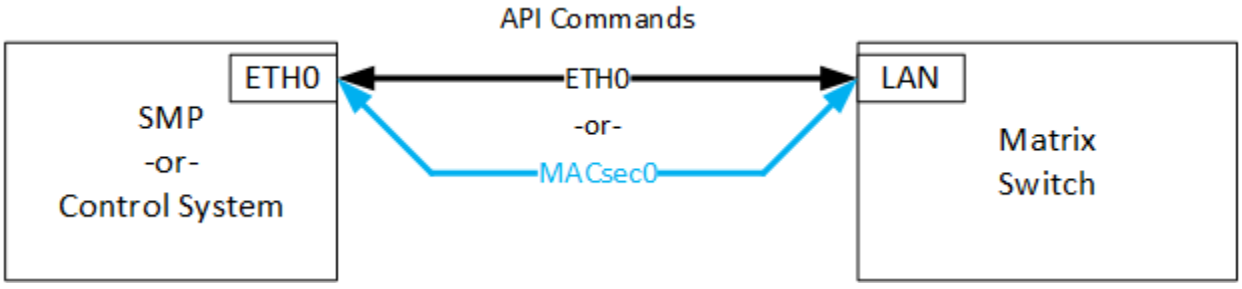
Pictured below is a typical system.

Note: The ***default*** IP addresses of the matrix are 192.168.13.115 and 192.169.13.16. Therefore, your browsing device (such as a laptop) must be configured for the 192.168.13.xxx subnet. For matrices with two controllers (Primary and Backup) the configuration must be done on both controllers individually. For the TLX-12 and TLX-24 matrices the default IP address is 192.169.13.15 (no Backup controller).

See also the Quick Start Guide in Appendix A.

Connection Diagram





Note: The API commands travel on the same physical interfaces when using eth0 or MACsec0 network devices.

Using ADM

Logging in

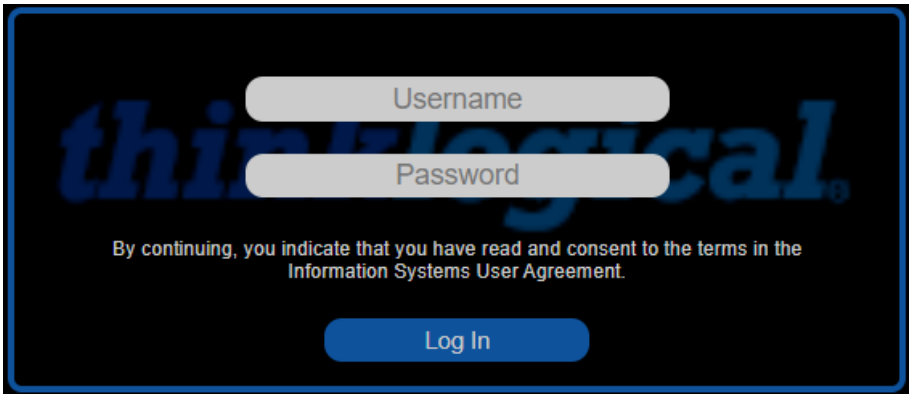
A typical Matrix Switch has three default IP addresses:

- 192.168.13.15 = Virtual – This address is assumed by the ACTIVE Controller card.
- 192.168.13.115 = Primary Controller Physical Address
- 192.168.13.16 = Backup Controller Physical Address

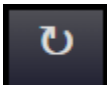
Therefore, to connect to the Primary Controllers ADM, browse to: https://192.168.13.115:60087

To connect to the Backup Controllers ADM, browse to: https://192.168.13.16:60087

You will then see the login page; ***default*** credentials are admin / admin.

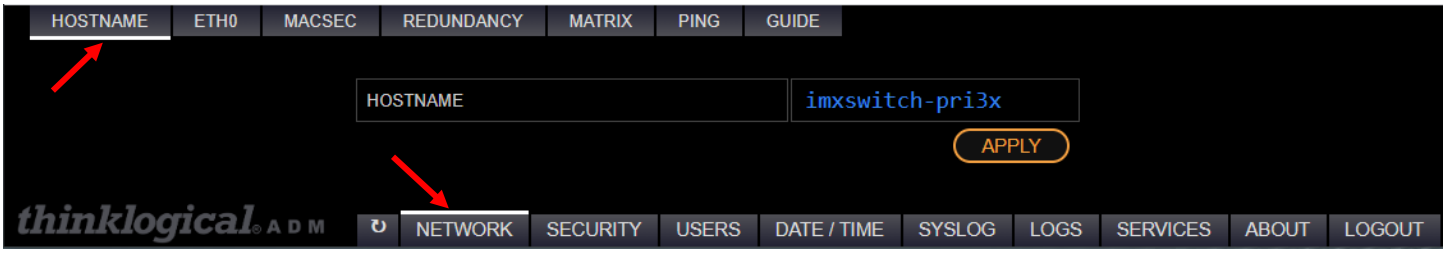


Note: After logging in you will notice a Page Refresh icon at the button of each page. Pressing Refresh will require a new login.



The NETWORK Tab

HOSTNAME

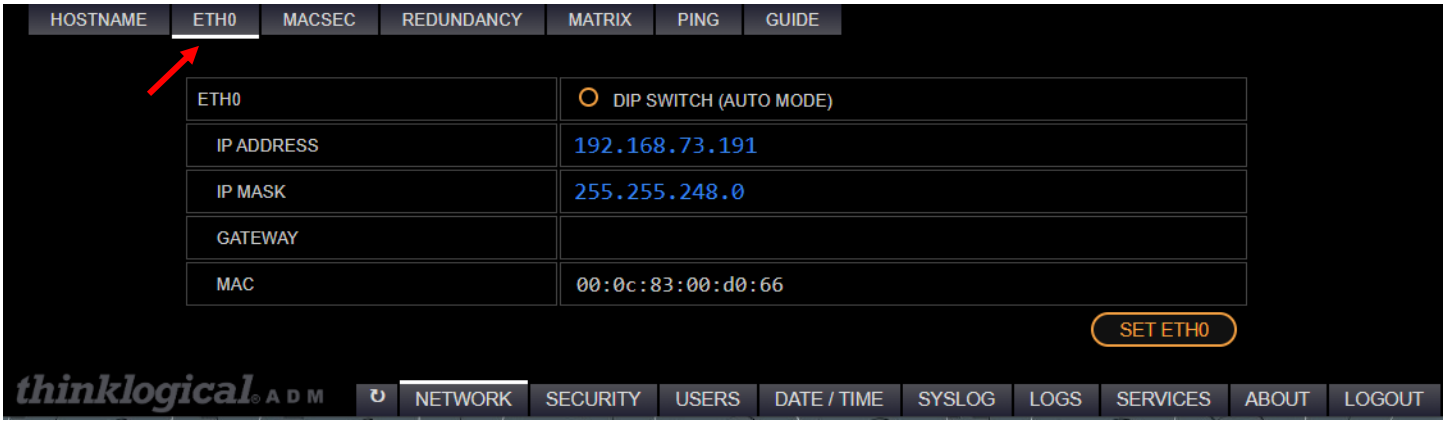


HOSTNAME - Defines the name of the Linux machine on the Matrix Switch. Hostname is mapped to an IP address via "hosts" file or a Domain Name System (DNS) server. This is especially useful for sites with multiple matrices.

[APPLY] - Modifies the /etc/hostname file.

ETH0

This is the Matrix Switch external ethernet interface.



DIP SWITCH (AUTO MODE) – Enabling this feature will cause the Matrix Switch to read the DIP switch value and configure itself automatically. See the appropriate Matrix Switch manual **(or click ABOUT)** for these values. The exception is the TLX-12 and TLX-24 which do not have DIP switches.

IP ADDRESS – The physical IP address of ETH0.

IP MASK – Utilized to define the size of the subnetwork (range of consecutive IP addresses).

GATEWAY – Forwarding host IP address (access point to another subnetwork).

MAC – Unique identifier assigned to a network interface, not changeable (Thinklogical = 00:0c:83:xx:xx:xx).

Warning! Enabling the DIP Switch feature (as in the case above) may result in loss of connectivity. You will need to reconfigure your laptop for the proper IP subnet and log in again.

Note: When configuring ETH0 for a subnet other than 192.168.xxx.xxx you must also hit APPLY in the MATRIX tab to configure the new broadcast address for the Matrix API.

MACSEC

MACsec = Message Authentication Code security (not MAC address)

MACsec (when enabled) is used to encrypt communications between the Matrix Switch API and an external control device.

MACSEC0 – Layer 2 ethernet cryptographic protocol that relies on GCM-AES-256 to offer network security.

Pre-requisite for MACsec membership:

- Same LAN.
- Support GCM-AES-256 cipher.
- Common CAK / CKN (manually pre-shared).

ENABLE – Enables MACsec using the configured settings.

MTX API – Configures MATRIX API communications over MACSEC0 device (vs. ETH0 device).

ADDRESS – Must be part of a unique IP subnet (i.e., not ETH0's IP subnet) dedicated to MACsec membership (32 maximum peers).

MASK – Subnet mask for the MACsec subnet.

MKA PRIORITY – Lowest value determines the Key Server of the MACsec group (a backup controller is the recommended key server). Displayed (in gray) are: Master key server, Backup key server, all others.

MAC – MAC address of the Matrix controller logged into.

CAK – Connectivity Association Key (16 bytes).

CKN – Connectivity Association Key Name (32 bytes), randomly generated keys.

[CREATE NEW CAC/CKN] – Provides random keys to be manually shared.

[CANCEL] – Reverts to prior CAK/CKN random key values.

[SET MACSEC] – Stores parameters: ADDRESS, MASK, MKA PRIORITY, CAK, CKN.

STATUS –

Cipher Suite GCM-AES-256 - Highest security level supported by MACsec.

Live peers – Number of active members in MACsec group.

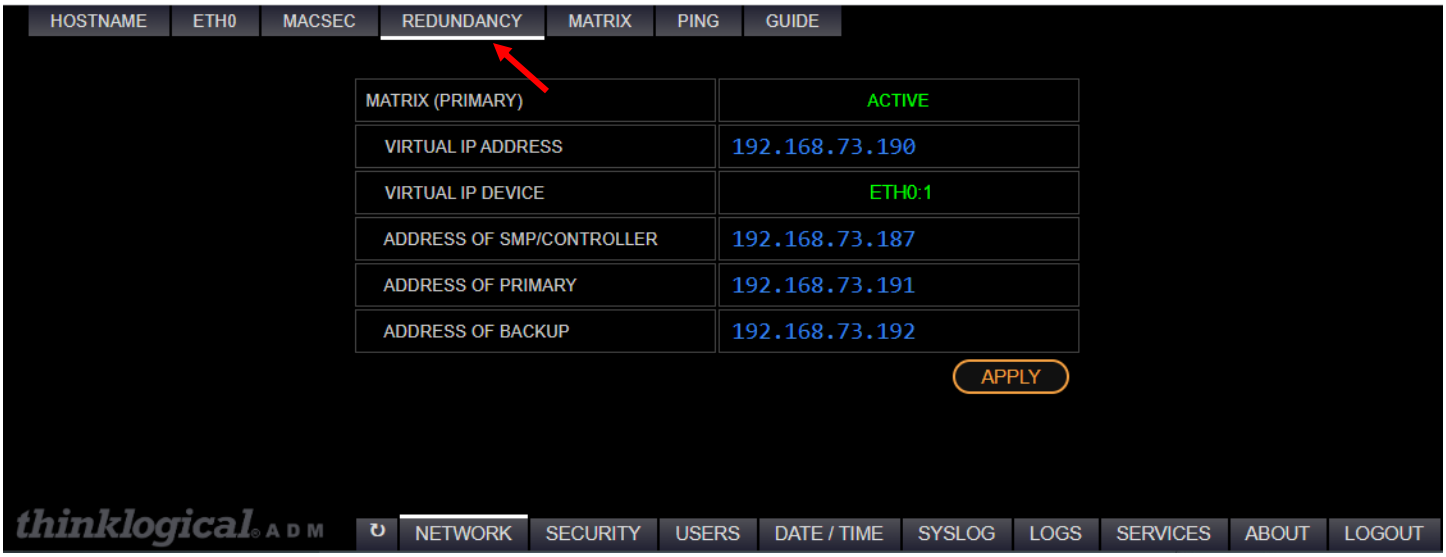
Key Server – Responsible for generating and distributing the Secure Association Keys (SAKs).

Displays other members of the MACsec subnet.

[REFRESH] - Provides current MACsec status.

Note: The configuration on this page applies to the MACsec IP address and the API commands to the Matrices. Normal operation of ETH0 is not affected.

REDUNDANCY



MATRIX - The status of the connected controller is displayed here as **ACTIVE** or **STANDBY**.
The title field will also indicate if it is the Primary or Backup controller.

MATRIX (PRIMARY) states:

ACTIVE – Normal state.

STANDBY – Failed state, primary faulted.

MATRIX (BACKUP) states:

STANDBY – Normal state.

ACTIVE – Failed state, primary faulted.

VIRTUAL IP ADDRESS – The address of the MATRIX ACTIVE controller card. This is the address where the MATRIX can be reached by the SMP/CONTROLLER (this gets transferred to the Backup controller during a failover operation.)

VIRTUAL IP DEVICE – Valid results are ETH0:1, MACSEC0:1, NONE.

ETH0:1 – ETH0 redundancy.

MACSEC0:1 – MACSEC redundancy.

NONE – Redundancy not configured.

ADDRESS OF SMP/CONTROLLER - Utilized by the MATRIX controller cards to support a network health check.

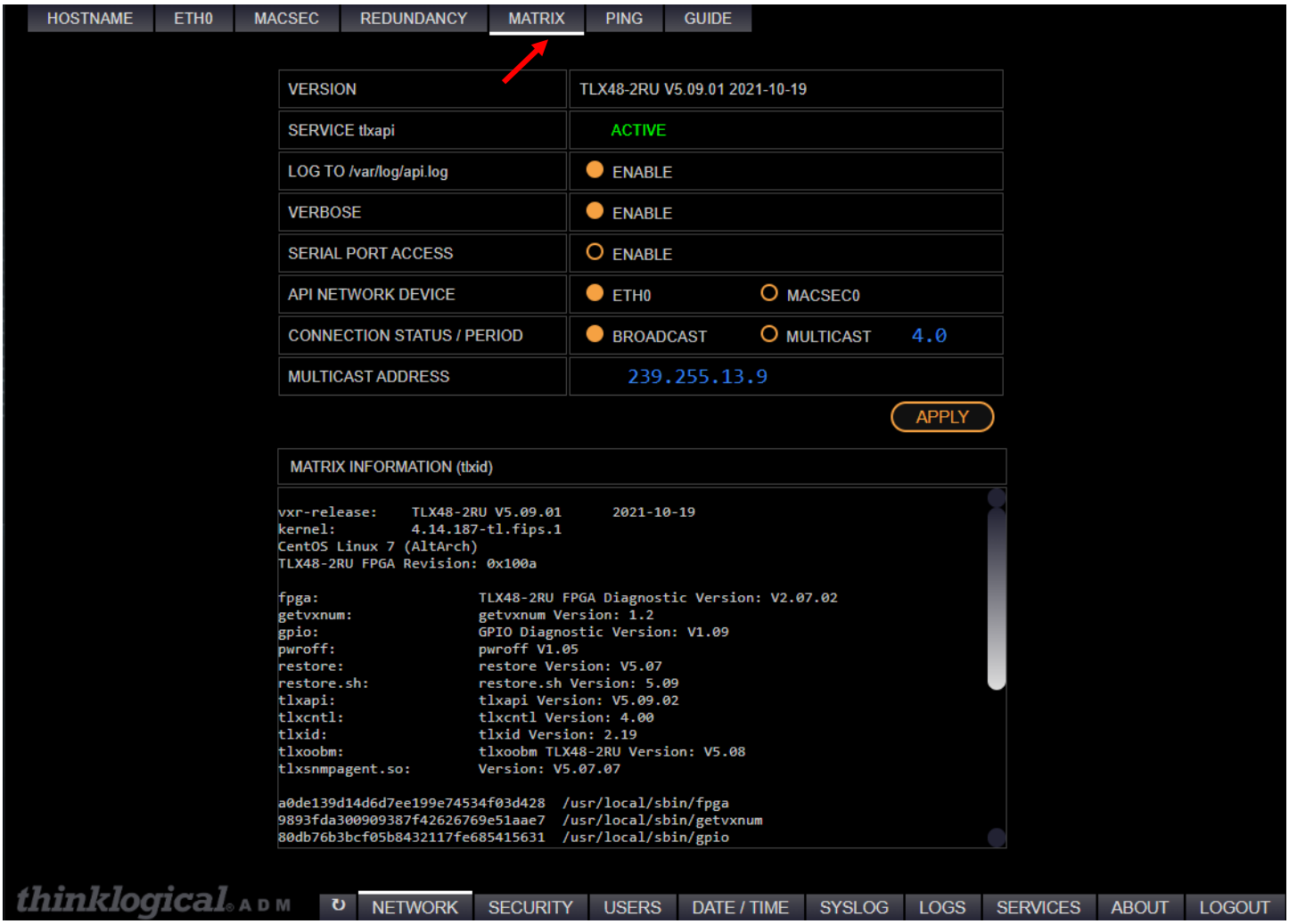
ADDRESS OF PRIMARY – The physical address of the MATRIX PRIMARY controller card.

ADDRESS OF BACKUP – The physical address of the MATRIX BACKUP controller card.

[APPLY] - Configures the 4 IP addresses.

Note: If MACsec is enabled, the VIRTUAL, PRIMARY, and BACKUP addresses should be part of the MACsec LAN group. If DIP SWITCH (reference NETWORK / ETH0 tab) is enabled, the VIRTUAL, PRIMARY and BACKUP shall be automatically assigned (per DIP SWITCH value).

MATRIX



VERSION – Matrix SD Card image version. (Example shows v.5.09.01)

SERVICE tlxapi – Provides operational status of MATRIX API (ACTIVE, STOPPED, FAILED).

LOG TO /var/log/api.log – Enable / disable API logging feature**.**

VERBOSE – Enable / disable extended logging details.

SERIAL PORT ACCESS – Enable / disable physical RS232 API port (9600 baud, 8 data bits, 1 stop bit, no parity, no flow control).

API NETWORK DEVICE – ETH0 selection (no encryption), MACSEC0 selection (GCM-AES-256 encryption), no selection (localhost only).

CONNECTION STATUS / PERIOD – Configure UDP broadcast or UDP multicast mode, and period (default 4.0 second).

MULTICAST ADDRESS – Configure UDP/IP multicast address (default 239.255.13.9).

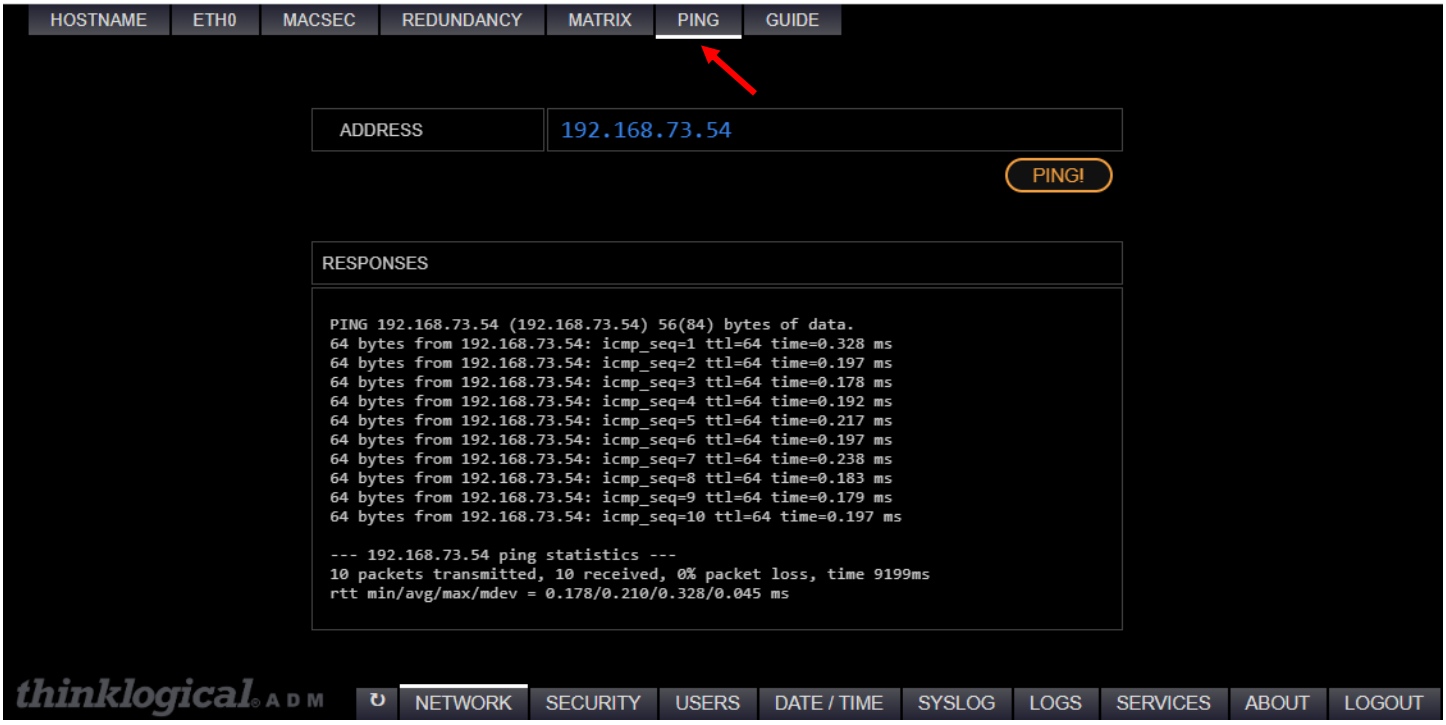
[APPLY] – Configures API parameters.

MATRIX INFORMATION (tlxid) – Provides the Matrix Controller Card's software release/version information. The most pertinent information here would be the "vxr-release" and "FPGA Revision" as well as if certain features are enabled as shown below:

```
partitioning file not found
restricted switching file not found
Point-to-Point file not found
restore connections on powerup disabled
```

Note: BROADCAST vs. MULTICAST - Broadcast mode copies UDP packets from Matrix port to all other ports on the network, multicast mode copies UDP packets from the Matrix port to a subset of ports on the network.

PING



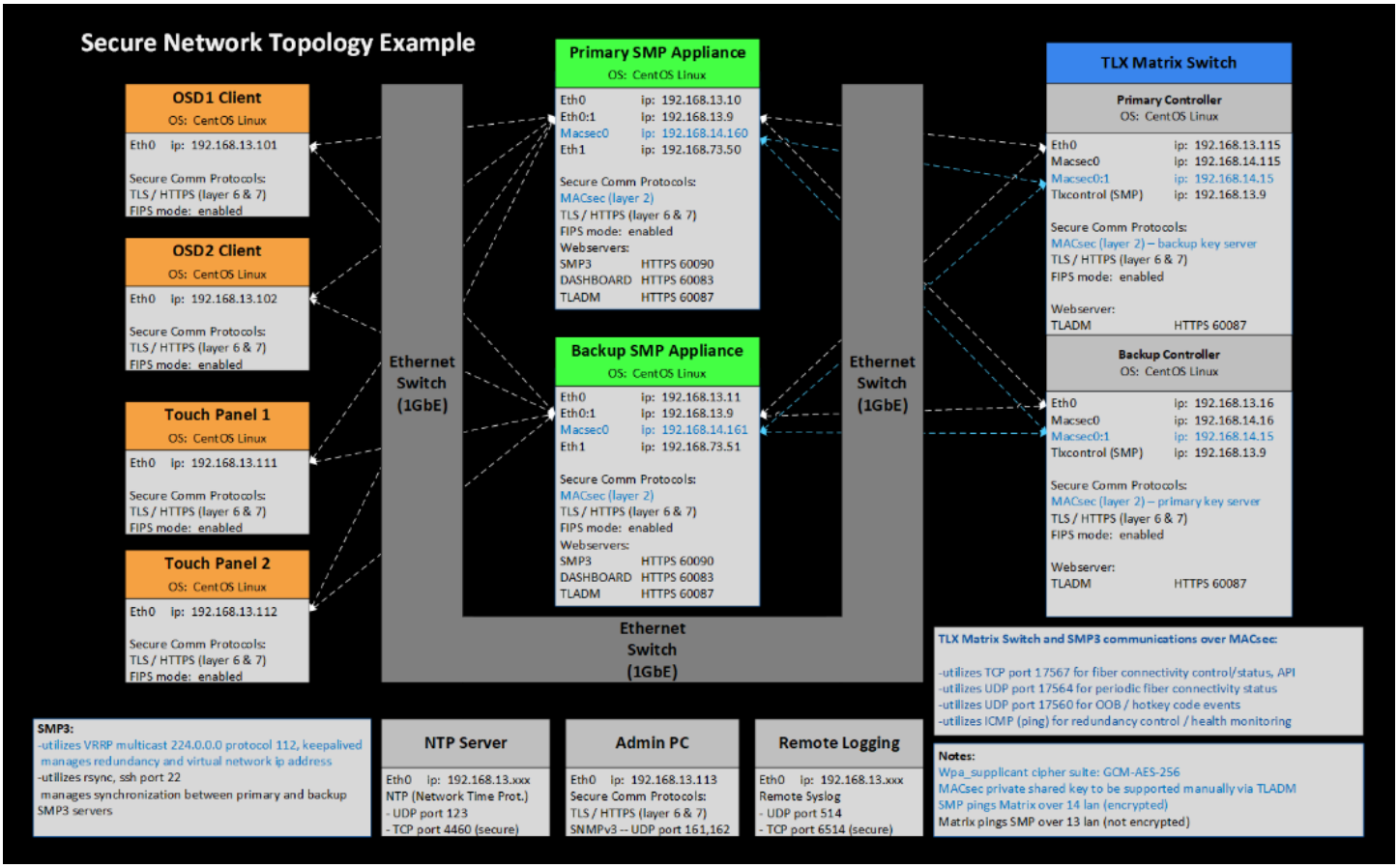
ADDRESS – Configurable remote IP address to be checked.

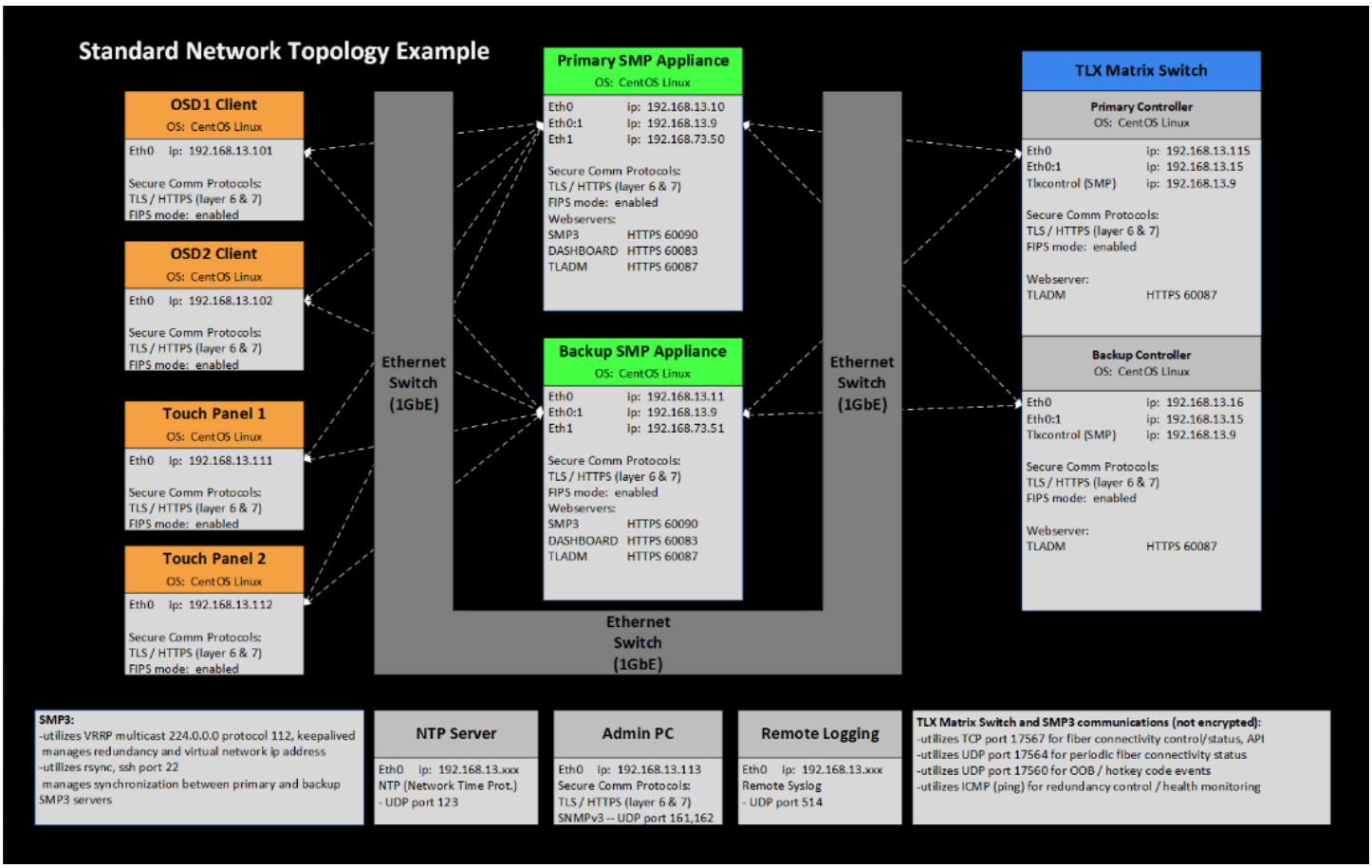
[PING!] - Sends 10 data packets to a configurable IP address to test network connectivity.

RESPONSES – Displays success/latency statistics of the IP connectivity to a remote machine.

GUIDE

Note: These are static diagrams of sample configurations. Clicking on one will zoom in for clarity.


Secure Network Topology Example
OSD1 Client
OS: CentOS Linux
Eth0 ip: 192.168.13.101
Secure Comm Protocols:
TLS / HTTPS (layer 6 & 7)
FIPS mode: enabled
OSD2 Client
OS: CentOS Linux
Eth0 ip: 192.168.13.102
Secure Comm Protocols:
TLS / HTTPS (layer 6 & 7)
FIPS mode: enabled
Touch Panel 1
OS: CentOS Linux
Eth0 ip: 192.168.13.111
Secure Comm Protocols:
TLS / HTTPS (layer 6 & 7)
FIPS mode: enabled
Touch Panel 2
OS: CentOS Linux
Eth0 ip: 192.168.13.112
Secure Comm Protocols:
TLS / HTTPS (layer 6 & 7)
FIPS mode: enabled
Ethernet Switch (1GbE)
Primary SMP Appliance
OS: CentOS Linux
Eth0 ip: 192.168.13.10
Eth0:1 ip: 192.168.13.9
Macsec0 ip: 192.168.14.160
Eth1 ip: 192.168.73.50
Secure Comm Protocols:
MACsec (layer 2)
TLS / HTTPS (layer 6 & 7)
FIPS mode: enabled
Webservers:
SMP3 HTTPS 60090
DASHBOARD HTTPS 60083
TLADM HTTPS 60087
Backup SMP Appliance
OS: CentOS Linux
Eth0 ip: 192.168.13.11
Eth0:1 ip: 192.168.13.9
Macsec0 ip: 192.168.14.161
Eth1 ip: 192.168.73.51
Secure Comm Protocols:
MACsec (layer 2)
TLS / HTTPS (layer 6 & 7)
FIPS mode: enabled
Webservers:
SMP3 HTTPS 60090
DASHBOARD HTTPS 60083
TLADM HTTPS 60087
Ethernet Switch (1GbE)
Ethernet Switch (1GbE)
TLX Matrix Switch
Primary Controller
OS: CentOS Linux
Eth0 ip: 192.168.13.115
Macsec0 ip: 192.168.14.115
Macsec0:1 ip: 192.168.14.15
Tlxcontrol (SMP) ip: 192.168.13.9
Secure Comm Protocols:
MACsec (layer 2) – backup key server
TLS / HTTPS (layer 6 & 7)
FIPS mode: enabled
Webserver:
TLADM HTTPS 60087
Backup Controller
OS: CentOS Linux
Eth0 ip: 192.168.13.16
Macsec0 ip: 192.168.14.16
Macsec0:1 ip: 192.168.14.15
Tlxcontrol (SMP) ip: 192.168.13.9
Secure Comm Protocols:
MACsec (layer 2) – primary key server
TLS / HTTPS (layer 6 & 7)
FIPS mode: enabled
Webserver:
TLADM HTTPS 60087
TLX Matrix Switch and SMP3 communications over MACsec:
-utilizes TCP port 17567 for fiber connectivity control/status, API
-utilizes UDP port 17564 for periodic fiber connectivity status
-utilizes UDP port 17560 for OOB / hotkey code events
-utilizes ICMP (ping) for redundancy control / health monitoring
SMP3:
-utilizes VRRP multicast 224.0.0.0 protocol 112, keepalived manages redundancy and virtual network ip address
-utilizes rsync, ssh port 22 manages synchronization between primary and backup SMP3 servers
NTP Server
Eth0 ip: 192.168.13.xxx
NTP (Network Time Prot.)
- UDP port 123
- TCP port 4460 (secure)
Admin PC
Eth0 ip: 192.168.13.113
Secure Comm Protocols:
TLS / HTTPS (layer 6 & 7)
SNMPv3 -- UDP port 161,162
Remote Logging
Eth0 ip: 192.168.13.xxx
Remote Syslog
- UDP port 514
- TCP port 6514 (secure)
Notes:
Wpa_supplicant cipher suite: GCM-AES-256
MACsec private shared key to be supported manually via TLADM
SMP pings Matrix over 14 lan (encrypted)
Matrix pings SMP over 13 lan (not encrypted)


Standard Network Topology Example
OSD1 Client
OS: CentOS Linux
Eth0 ip: 192.168.13.101
Secure Comm Protocols:
TLS / HTTPS (layer 6 & 7)
FIPS mode: enabled
OSD2 Client
OS: CentOS Linux
Eth0 ip: 192.168.13.102
Secure Comm Protocols:
TLS / HTTPS (layer 6 & 7)
FIPS mode: enabled
Touch Panel 1
OS: CentOS Linux
Eth0 ip: 192.168.13.111
Secure Comm Protocols:
TLS / HTTPS (layer 6 & 7)
FIPS mode: enabled
Touch Panel 2
OS: CentOS Linux
Eth0 ip: 192.168.13.112
Secure Comm Protocols:
TLS / HTTPS (layer 6 & 7)
FIPS mode: enabled
Ethernet Switch (1GbE)
Primary SMP Appliance
OS: CentOS Linux
Eth0 ip: 192.168.13.10
Eth0:1 ip: 192.168.13.9
Eth1 ip: 192.168.73.50
Secure Comm Protocols:
TLS / HTTPS (layer 6 & 7)
FIPS mode: enabled
Webservers:
SMP3 HTTPS 60090
DASHBOARD HTTPS 60083
TLADM HTTPS 60087
Backup SMP Appliance
OS: CentOS Linux
Eth0 ip: 192.168.13.11
Eth0:1 ip: 192.168.13.9
Eth1 ip: 192.168.73.51
Secure Comm Protocols:
TLS / HTTPS (layer 6 & 7)
FIPS mode: enabled
Webservers:
SMP3 HTTPS 60090
DASHBOARD HTTPS 60083
TLADM HTTPS 60087
Ethernet Switch (1GbE)
Ethernet Switch (1GbE)
TLX Matrix Switch
Primary Controller
OS: CentOS Linux
Eth0 ip: 192.168.13.115
Eth0:1 ip: 192.168.13.15
Tlxcontrol (SMP) ip: 192.168.13.9
Secure Comm Protocols:
TLS / HTTPS (layer 6 & 7)
FIPS mode: enabled
Webserver:
TLADM HTTPS 60087
Backup Controller
OS: CentOS Linux
Eth0 ip: 192.168.13.16
Eth0:1 ip: 192.168.13.15
Tlxcontrol (SMP) ip: 192.168.13.9
Secure Comm Protocols:
TLS / HTTPS (layer 6 & 7)
FIPS mode: enabled
Webserver:
TLADM HTTPS 60087
SMP3:
-utilizes VRRP multicast 224.0.0.0 protocol 112, keepalived manages redundancy and virtual network ip address
-utilizes rsync, ssh port 22 manages synchronization between primary and backup SMP3 servers
NTP Server
Eth0 ip: 192.168.13.xxx
NTP (Network Time Prot.)
- UDP port 123
Admin PC
Eth0 ip: 192.168.13.113
Secure Comm Protocols:
TLS / HTTPS (layer 6 & 7)
SNMPv3 -- UDP port 161,162
Remote Logging
Eth0 ip: 192.168.13.xxx
Remote Syslog
- UDP port 514
TLX Matrix Switch and SMP3 communications (not encrypted):
-utilizes TCP port 17567 for fiber connectivity control/status, API
-utilizes UDP port 17564 for periodic fiber connectivity status
-utilizes UDP port 17560 for OOB / hotkey code events
-utilizes ICMP (ping) for redundancy control / health monitoring

The SECURITY Tab

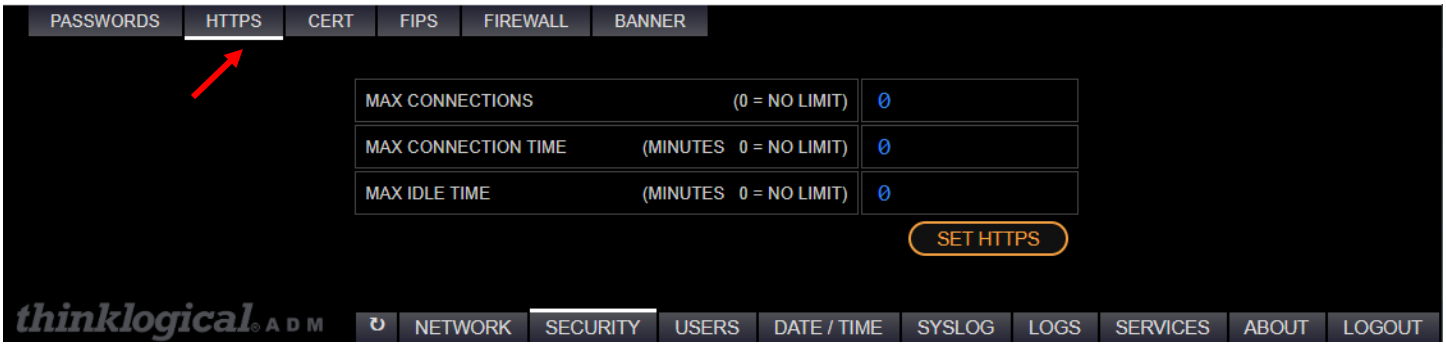
PASSWORDS

PASSWORD AUTHENTICATION MODULE – Enables PAM (Password Authentication Module). Password policy settings apply to both the Linux operating system and the ADM webserver.

[SUGGEST DEFAULTS] – Provides recommended password complexity for secure deployment.

[APPLY] – Saves the ENABLE state and numeric parameters to the configuration.

HTTPS



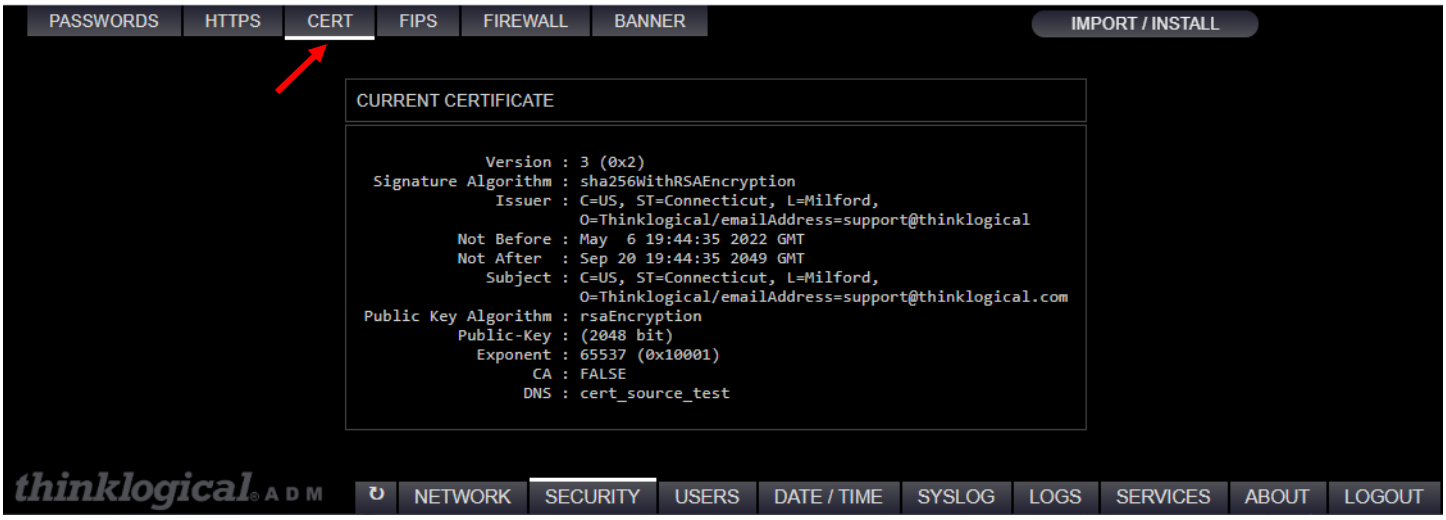
MAX CONNECTIONS – Sets the absolute maximum number of TCP connections to the ADM web server. (Note: It is common for web-browsers to open parallel TCP connections in order to load the different resources faster, e.g., Chrome browser supports 17 TCP connections).

MAX CONNECTION TIME – How long this connection can continue before requiring another login.

MAX IDLE TIME – Maximum time between commands before requiring another login.

[SET HTTPS] - Configures the three parameters.

CERT

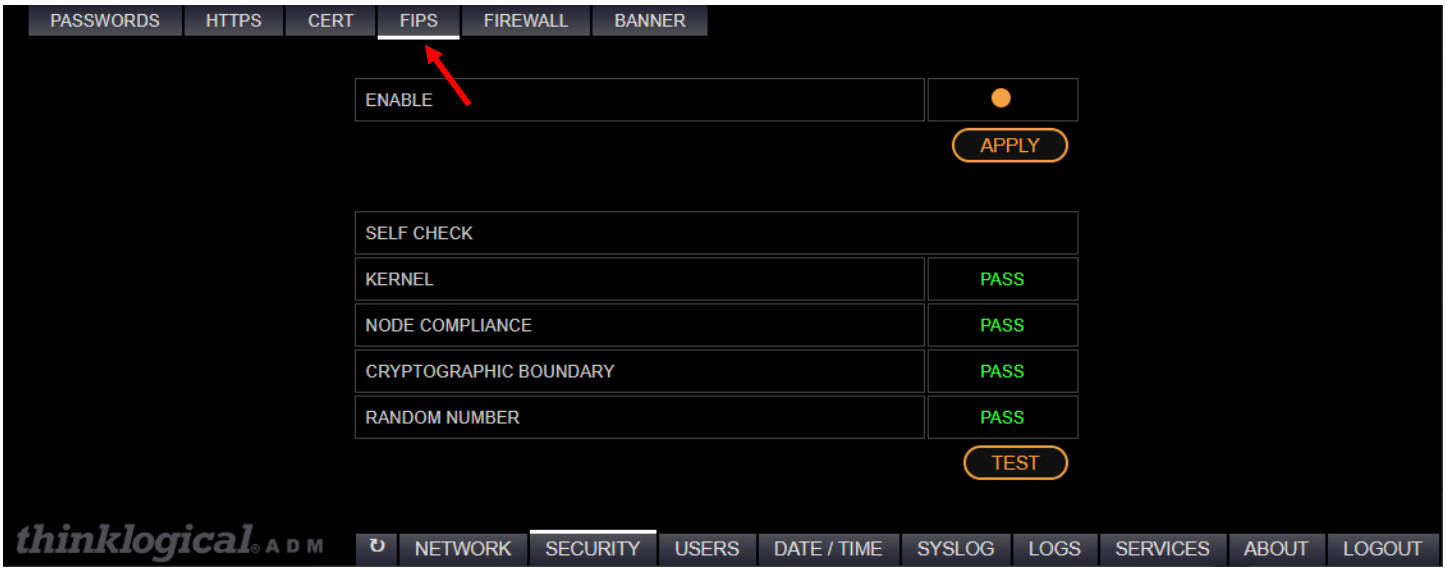


CURRENT CERTIFICATE - Provides details of the webserver(s) SSL certificate (encryption algorithm, issuer, expiration date, certificate authority, DNS name).

[IMPORT/INSTALL] - Enables importing locally stored SSL certificate files to the MATRIX. Naming convention must be “thinklogical.pem” and “thinklogical.crt”.

FIPS

FIPS - Federal Information Processing Standards



ENABLE – Enables FIPS (Federal Information Processing Standards).

[APPLY] - Enables / disables FIPS boot environment variable, requires reboot to change FIPS mode.

SELF CHECK – Displays the results of the TEST button.

KERNEL – Verifies the Linux kernel version supports fips (4.14.187-tl.fips.1) and that the boot environment variable for FIPS is set to '1' (enabled).

NODE COMPLIANCE – Verifies that the HTTPS web server only supports FIPS compliant algorithms via a known answer test.

CRYPTOGRAPHIC BOUNDARY – The integrity of the ARM32 hardware and the RHEL FIPS 140-2 object modules are validated by comparing a calculated HMAC's of the FIPS OPEN-SSL libraries with a stored HMAC file computed at build time.

RANDOM NUMBER – The random number generator test performs 1000 tests to ensure results are uniformly distributed, uncorrelated, and non-repeating.

[TEST] - Performs FIPS integrity checks and reports results.

Note: SELF CHECK is performed on power-up and on-demand. If FIPS is enabled and SELF CHECK fails during boot-up, the Linux kernel will halt.

FIREWALL

ENABLE FIREWALL – Please refer to the **Firewall (UFW) Settings** section of the **Thinklogical TLX Military Unique Deployment Guide** prior to enabling the default firewall policy.

ENABLE SSH – Enables / disables the ability to SSH into the Matrix Switch.

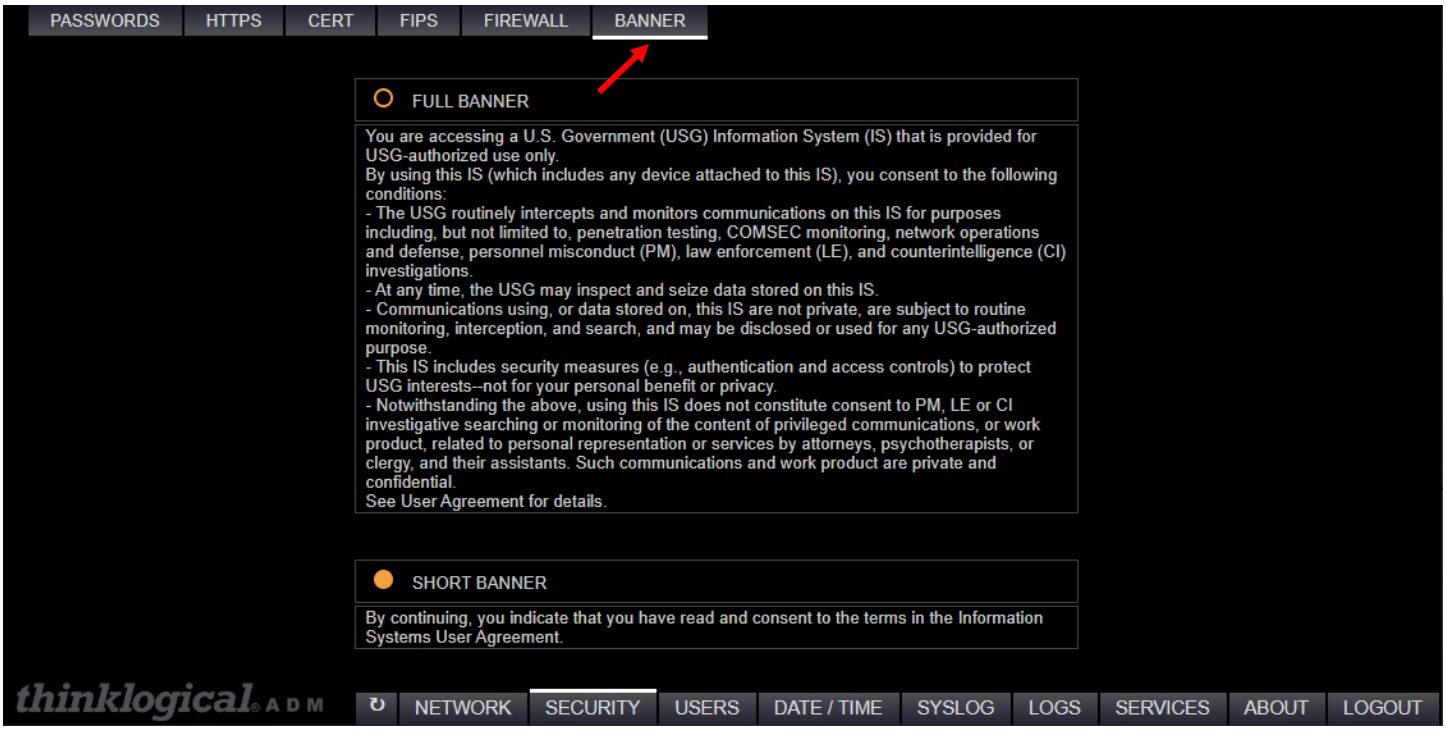
[APPLY] – Enables / disables the FIREWALL policy and management of the equipment via SSH protocol.

STATUS - Displays the current FIREWALL status/configuration.

[REFRESH] – Refreshes the current FIREWALL status/configuration.

Note: In order to disable SSH the Firewall must be enabled.

BANNER

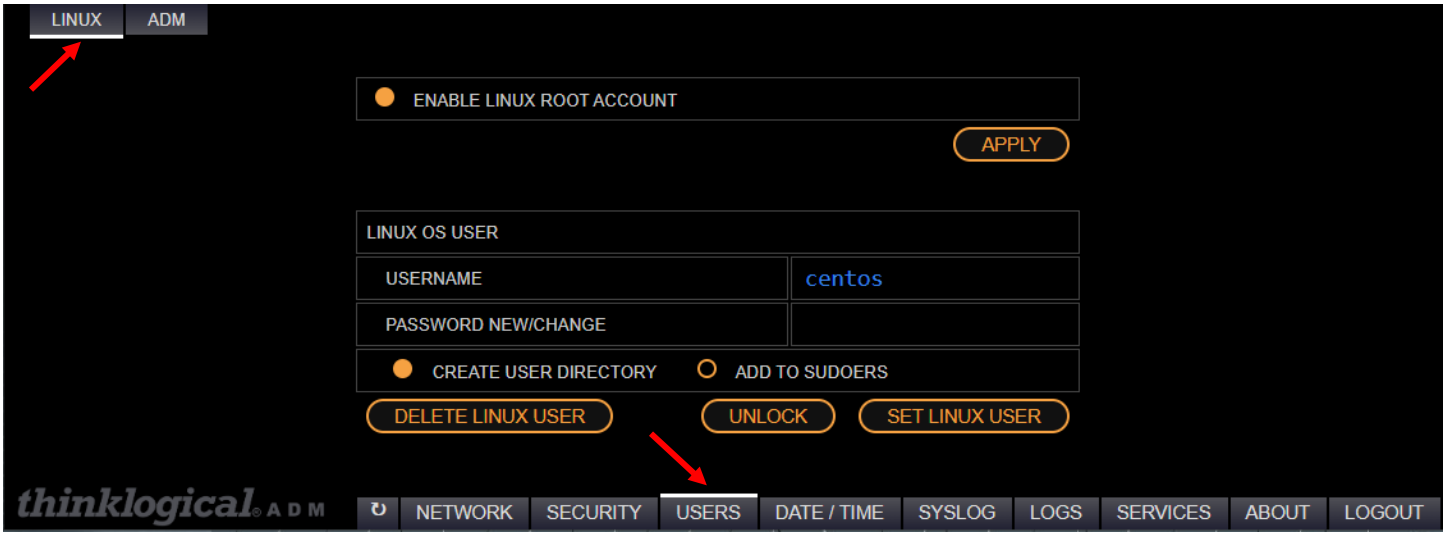


Selected banner will be shown in the splash page during browser login and in the terminal window during SSH login (if SSH login enabled)

The USERS Tab

LINUX

Linux user account information.



ENABLE LINUX ROOT ACCOUNT – Enables / disables ROOT access via SSH and Serial Console port.

USERNAME – Linux username being configured.

PASSWORD NEW/CHANGE – Enter new password here.

CREATE USER DIRECTORY – Adds a home directory for the specified user, /home/<username>.

ADD TO SUDOERS – Enables/disables superuser privileges.

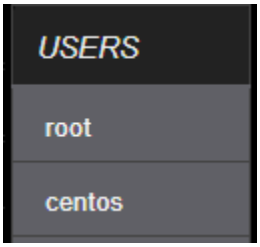
[DELETE LINUX USER] – Removes specified Linux user account.

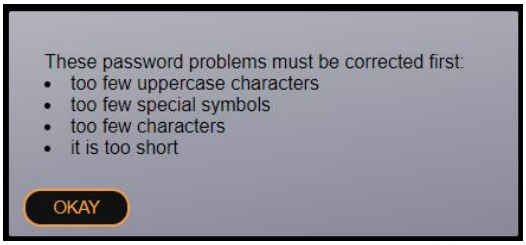
[UNLOCK] – Unlocks an account that has been disabled due to excessive failed password entry attempts.

[SET LINUX USER] - Applies USERNAME, PASSWORD, USER DIRECTORY, and SUDO membership.

Clicking in the **USERNAME** field will display a menu of currently configured Users, see example below.

If the password does not meet the requirements, a dialog box will appear.

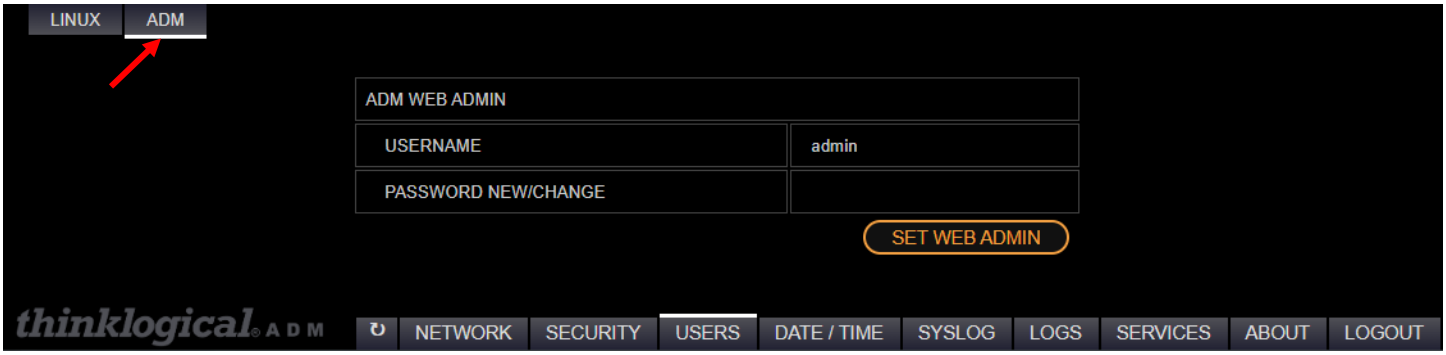




Note: The user "***root***" will not be able to be deleted.

ADM

ADM webserver password configuration

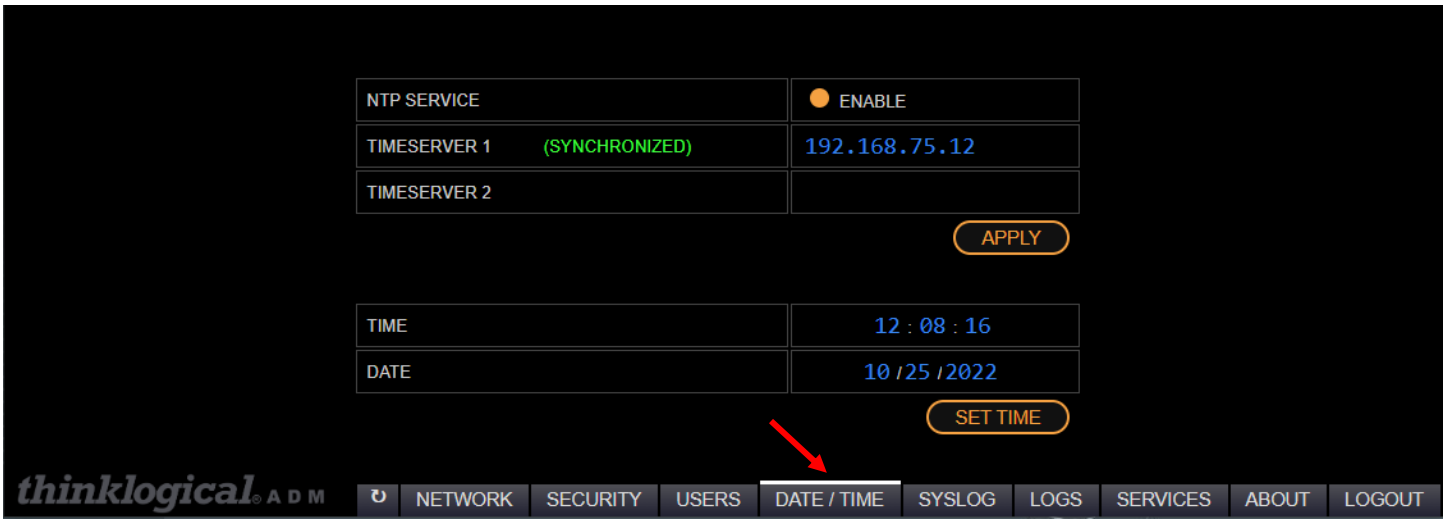


USERNAME – ADM web page login username.

PASSWORD NEW/CHANGE – Applies password changes.

[SET WEB ADMIN] - Sets new password for admin user.

The DATE / TIME Tab



NTP SERVICE – Enabled: Network Time Protocol client periodically requests timing information from a NTP server. The client synchronizes to the server every 64 seconds minimum, 1024 seconds maximum.

TIME SERVER 1 – IP address of primary NTP server.

TIME SERVER 2 – IP address of backup NTP server.

(SYNCHRONIZED) – Indicates which timeserver the unit is synchronized to.

[APPLY] - Configures NTP parameters.

TIME – Configurable system clock, synchronized to NTP server.

DATE – Configurable system date, synchronized to NTP server.

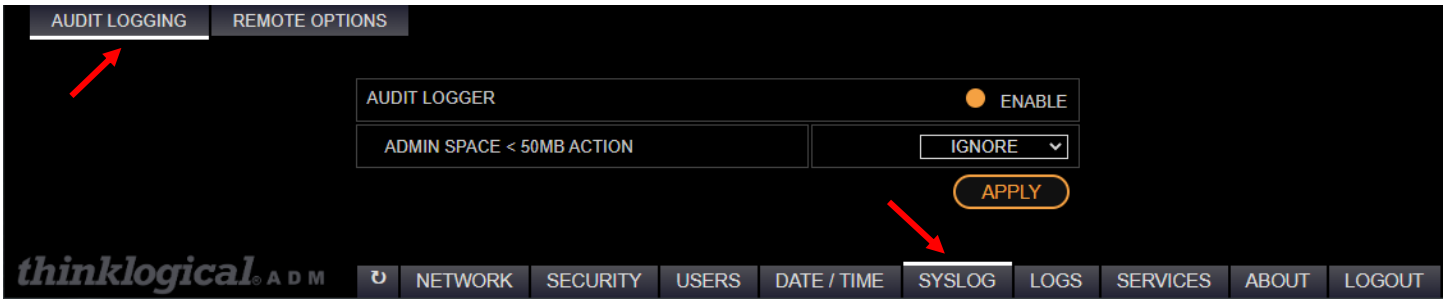
[SET TIME] - Configures system TIME & DATE when entered manually (no timeserver).

Note: When enabling the NTP Service it will not take effect immediately and will take some time to synchronize.

The SYSLOG Tab

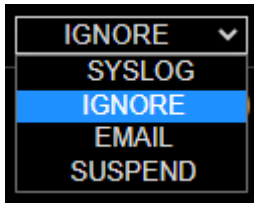
SYSLOG – standard message logging protocol, enabling the recording of security, analytical, debug, and informational messages.

AUDIT LOGGING



AUDIT LOGGER – A security relevant log providing documentary evidence of potentially suspicious events: authentication, changing file permissions, terminating a process, creating a network connection.

ADMIN SPACE < 50MB ACTION – Action to perform when hard drive partition is less than **50Mbytes.**



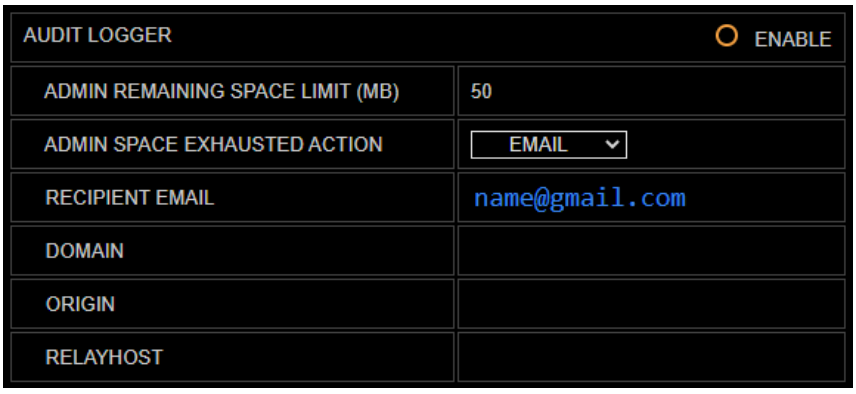
SYSLOG – Send warning to syslog.

IGNORE – No additional action, ignore warning.

EMAIL – Email warning to admin account.

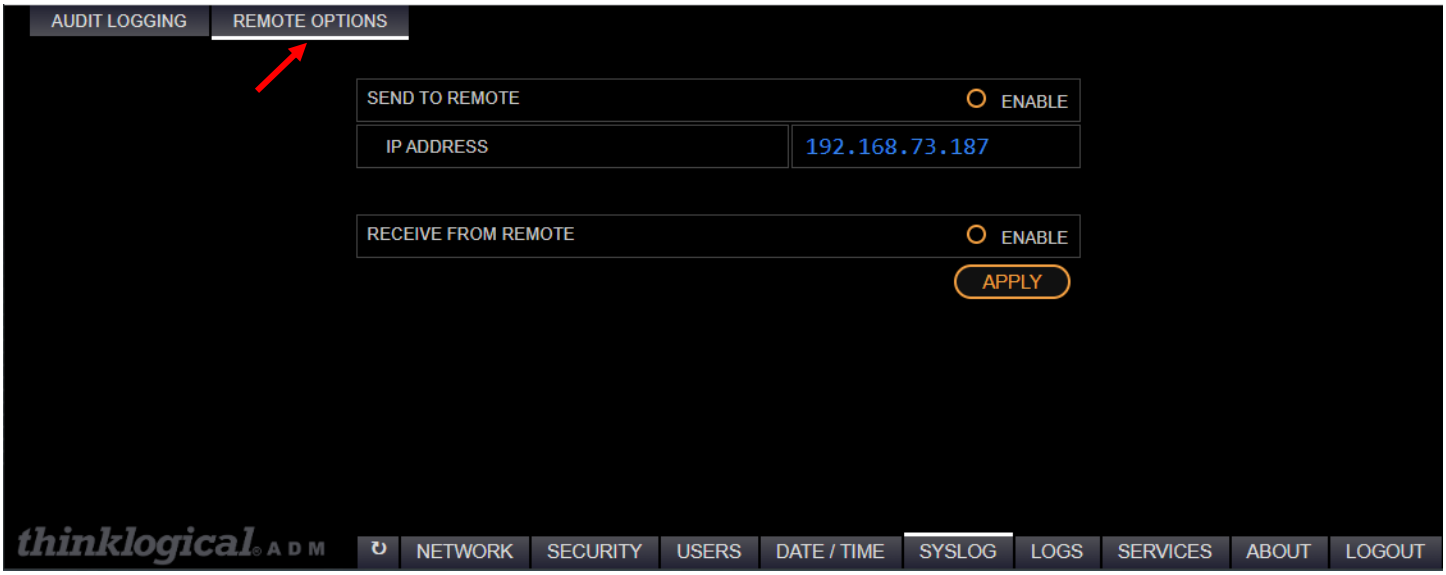
SUSPEND - Stop logging.

Note: Selecting EMAIL will provide further configuration options.



Note: Refer to **LOGS** tab for viewing / extracting SYSLOG and AUDIT log content.

REMOTE OPTIONS



SEND TO REMOTE – ENABLE: Sends SYSLOG messages to a centralized logging server located at <IP ADDRESS> utilizing UDP/IP port 514.

IP ADDRESS – Address of logging server utilizing UDP/IP port 514.

RECEIVE FROM REMOTE - ENABLE: Listens for SYSLOG messages (utilizing UDP/IP port 514) coming from network devices such as TL Matrix and SMP products, and stores data to the SYSLOG file.

Note: ADM prevents 'SEND TO REMOTE' and 'RECEIVE FROM REMOTE' from being enabled at the same time (prevents recursive logging event).

The LOGS Tab

The **LOGS** tab is used for viewing / extracting SYSLOG and AUDIT log content.

LOGS Window - This window contains the filenames of all the logs found in /var/log. They can be filtered by entering a string in the **Filter** field. Select the log(s) for download/inspection.

Filter - Allows filtering by line

Note: Log files are typically downloaded and then emailed to Thinklogical for analysis. Most of the log files shown are standard Linux logs.

Exceptions are the Thinklogical logs:

api – Log of the API (switch) commands received by the Matrix Switch.

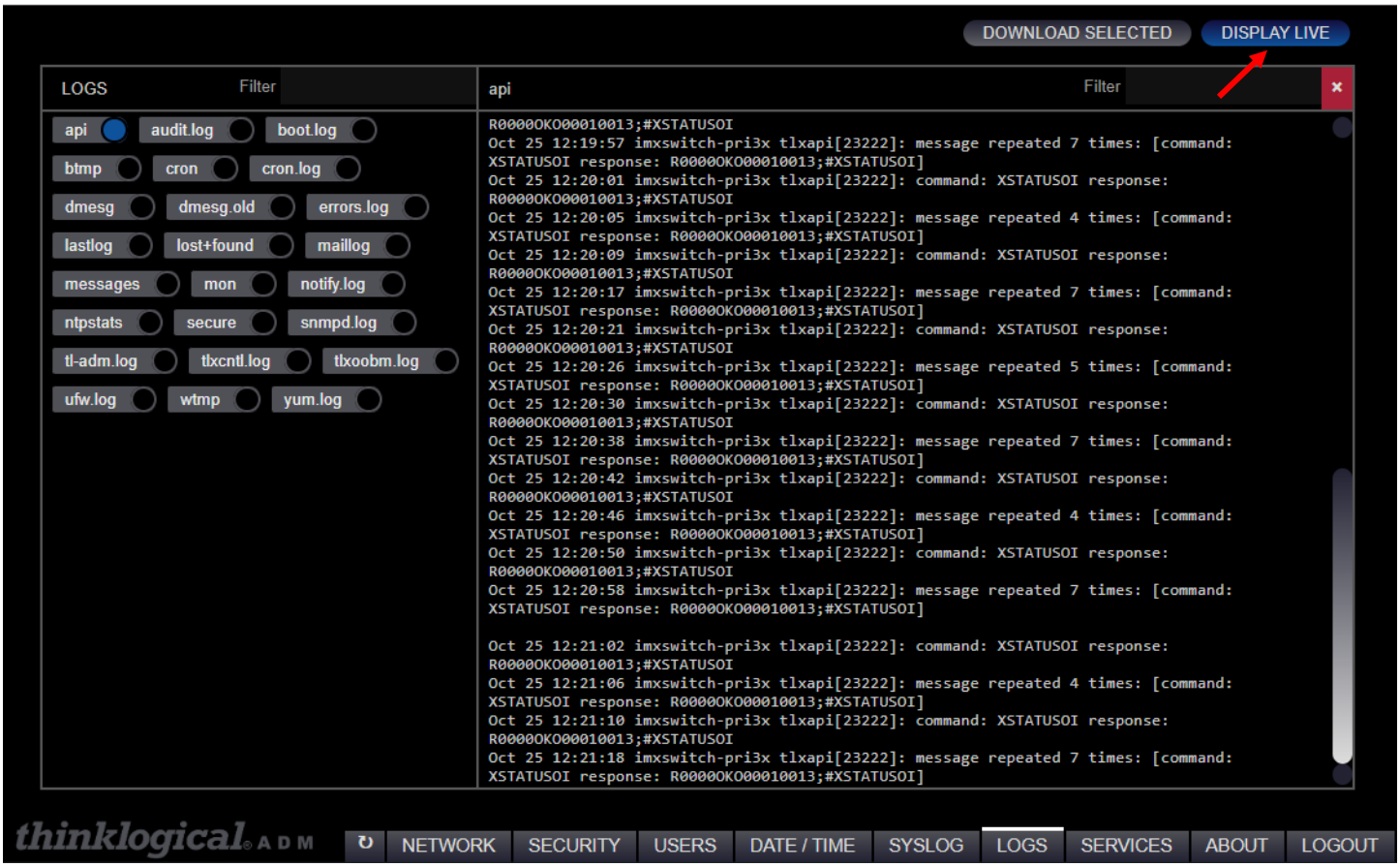
tlxcntl.log – Hardware related information.

tlxoobm.log – OOB (Out Of Band) Hotkey information.

DOWNLOAD SELECTED

This feature will compress the selected logs into a TGZ file and send it to your device, typically to the /Downloads directory.

DISPLAY LIVE



This is a Toggle - This option will display the selected log(s) in real time. If more than one log is selected, they will appear in their own frame. Deselect “DISPLAY LIVE” button to stop updating.

 - Closes the window for that log.

Note: In time, the logs will “roll over” to .GZ files. These are not viewable here but may be downloaded for analysis.

The SERVICES Tab

NTP – Network Time Protocol service

POSTFIX – Routes and delivers email to external accounts.

ADM – This program.

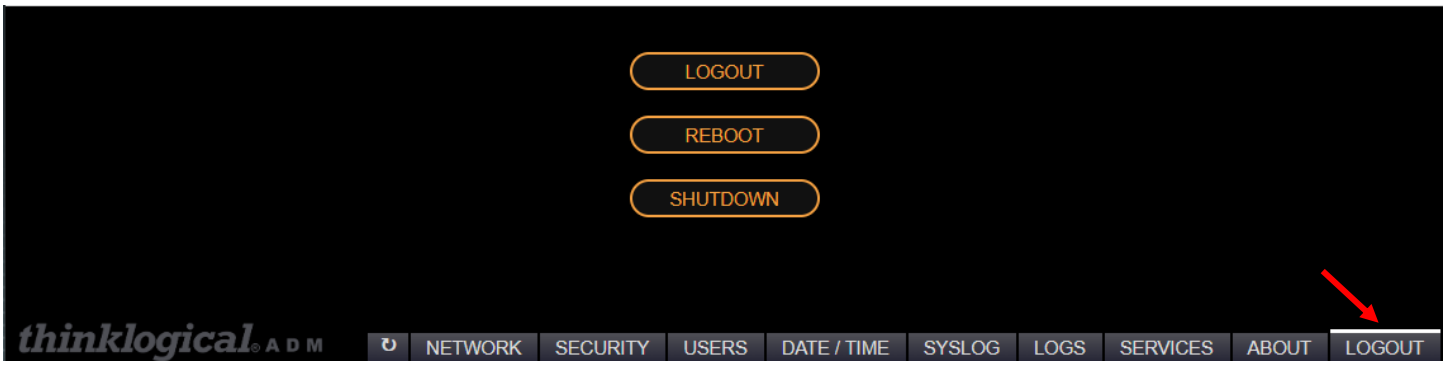
RSA SIGNATURE TEST REQUIRED – Enforces a secure verification method of the software files prior to installation (requires import of RSA INSTALLATION file)

[IMPORT / INSTALL] - Provides the ability to update to a new version of the ADM web server or import the RSA SIGNATURE file. Contact Thinklogical Support for ADM installation and RSA SIGNATURE files).

The ABOUT Tab

Clicking on the ABOUT tab on any of the pages will show the ADM version below and also add descriptive information about that page. For example: NETWORK / HOSTNAME is illustrated above.

The LOGOUT Tab



LOGOUT - Logs out of the TL ADM webserver.

REBOOT - Reboots the MATRIX controller card.

SHUTDOWN - Halts the MATRIX controller card processor (for removal).

Note: The SHUTDOWN operation is for the controller card you are logged into. If you wish to shutdown the entire Matrix, be sure to do both controllers, starting with the Backup Controller.

Thinklogical Support

Customer Support

Website: https://www.thinklogical.com

Check out our website for current products, support documents and useful information about all the products and services we offer, including:

- **Technical Specification Sheets**
- **Quick-Start Guides**
- **Product Manuals** (for viewing online or for download)
- **Chat live with a Technical Service Representative**

Email: mailto:support@thinklogical.com

For product support, technical issues or questions, product repairs and request for Return Merchandise Authorization.

Telephone: 1-203-647-8700

Please contact our expert sales staff in Milford, CT, USA, **Monday-Friday from 8:30am to 5:00pm**, Eastern Time Zone. If leaving a voice message, please provide a preferred time for us to call back.

Fax: 1-203-783-9949

Please indicate the nature of the communication on your cover sheet and provide contact information.

Product Support

Warranty

Thinklogical warrants this product against defects in materials and workmanship for a period of one year from the date of delivery, with longer terms available at the time of purchase on most products. Thinklogical and its suppliers disclaim all other warranties. Please refer to your product invoice for the Warranty Terms & Conditions.

Our Address

If you have any product issues or questions or need technical assistance with your Thinklogical system, please call us at **1-203-647-8700** and let us help. If you need to write us or return a product, please use the following address:

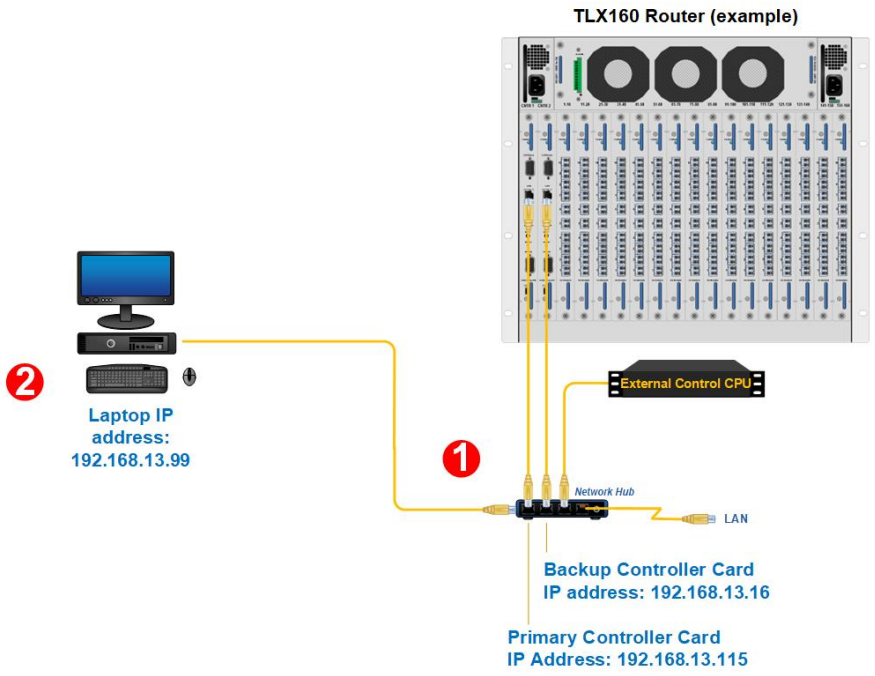
Please include the Return Merchandise Authorization number: **Thinklogical,** A **BELDEN** BRAND
100 Washington Street
Milford, CT 06460 USA
Attn: *RMA#*

QUICK-START GUIDE

ADM

MATRIX SWITCH ADMINISTRATIVE INTERFACE

Thinklogical's **ADM is a web based interface to our Matrix Switches. This provides a user-friendly method of configuring, monitoring and troubleshooting. The ADM also supports FIPS and MACsec.**



PROCEDURE:

STEP 1: Connect the laptop or other browsing device to the private LAN the Matrix Switch is a part of.

STEP 2: Configure the laptop to be part of the default subnet of 192.168.13.xxx. For example: 192.168.13.99.

STEP 3: Browse to the Primary controller at https://192.168.13.115:60087.

STEP 4: Login to the web page as admin/admin.

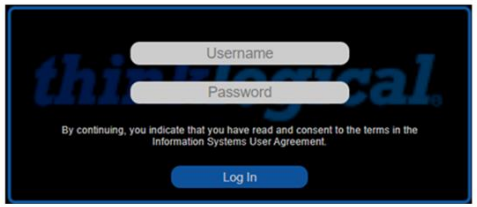
STEP 5: Configure the Primary Controller as per your requirements.

STEP 6: Browse to the Backup controller at https://192.168.13.16:60087.

STEP 7: Login to the web page as admin/admin.

STEP 8: Configure the Backup Controller as per your requirements.

STEP 9: Reboot the Matrix Switch to invoke the configuration changes.



3 4

thinklogical
A BELDEN BRAND
PHONE: 1-203-647-8700
WEBSITE: www.thinklogical.com
EMAIL: support@thinklogical.com

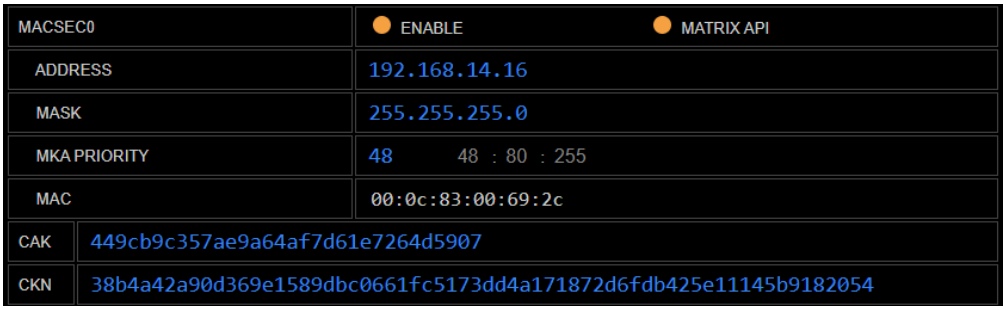
TLX Chassis & Modules

thinklogical®

Visit us online at www.thinklogical.com for more product information, firmware updates and the complete line of Thinklogical® products.

Appendix B: Example MACsec Configuration Procedure

1. First configure the Matrix Switch IP addresses per Appendix A and section NETWORK / ETH0.
2. Log into the Matrix Backup Controller card.
3. Navigate to NETWORK/MACSEC on the browser page.



4. Enable MACSEC and MATRIX API (top line).
5. Enter the IP address and subnet mask of this device on the **MACsec network.** This is separate from the eth0 network.
6. Set the MKA PRIORITY for the Backup Controller card to 48.
7. Click on [SET MACSEC], then [CREATE NEW CAK/CKN]. This will generate new keys.
8. Optional: You may also click on [REFRESH] to verify this is the key server and has a priority of 48, etc.
9. Check that the proper interface is selected under the NETWORK/MATRIX tab:

10. Copy these keys to Notepad or another editor for future use (see below).
11. Navigate to the NETWORK/REDUNDANCY tab and configure the MACsec IP addresses.

VIRTUAL IP ADDRESS	192.168.14.190
VIRTUAL IP DEVICE	MACSEC0:1
ADDRESS OF SMP/CONTROLLER	192.168.14.187
ADDRESS OF PRIMARY	192.168.14.191
ADDRESS OF BACKUP	192.168.14.192

12. Log into the Matrix Primary Controller card.
13. Navigate to NETWORK/MACSEC on the browser page.
14. Enable MACSEC and MATRIX API (top line).
15. Enter the IP address and subnet mask of this device on the MACsec network.
16. Set the MKA PRIORITY for the Primary Controller card to 80.
17. Copy the CAK and CKN keys here from the operation above.
18. Click on [SET MACSEC].
19. Check that the proper interface is selected under the NETWORK/MATRIX tab:

API NETWORK DEVICE	○ ETH0	● MACSEC0

20. Navigate to the NETWORK/REDUNDANCY tab and configure the MACsec IP addresses. See Step 11.
21. Optional: You may also click on [REFRESH] to verify this is not the key server and has a priority of 80, etc.
22. Reboot is recommended to fully invoke all changes.
23. Configure the SMP (or other control system) for MKA Priority, CAK, CKN, MACsec IP address.

Note: When configuring an SMP for MACsec, also enter the MACsec IP address under the SMP ADMIN/MTX tab.

Warning! After configuring the Matrix Switch for MACsec it will only be able to be controlled by a MACsec configured control system.

Appendix C: ETH0 and MACsec IP address worksheet

Interface	ETH0 / ETH1	MACsec
Matrix Primary Controller		
ETH0 tab		
Hostname		----------
IP address		----------
IP Mask		----------
Gateway		----------
MACsec tab		
Address (1)	----------	
Mask	----------	
MKA Priority	----------	
Redundancy tab		
Virtual IP Address		
Address of SMP/Controller		
Address of Primary (1)		
Address of Backup		
Matrix Backup Controller		
ETH0 tab		
Hostname		----------
IP address		----------
IP Mask		----------
Gateway		----------
MACsec tab		
Address (2)	----------	
Mask	----------	
MKA Priority	----------	
Redundancy tab		
Virtual IP Address		
Address of SMP/Controller		
Address of Primary		
Address of Backup (2)		
SMP or Controller		
ETH0 tab		
DHCP? Y/N		----------
IP Address		----------
IP Mask		----------
Gateway		----------
ETH1 tab		
DHCP? Y/N		----------
IP Address		----------
IP Mask		----------
MACsec tab		
Address	----------	
Mask	----------	
MKA Priority	----------	

Note (1), (2): When MACsec is configured, the MACsec address, and controller address should match.

NOTES: