



SMP ADM

SMP ADMINISTRATIVE INTERFACE

SECURE CONFIGURATION & SYSTEM CONTROL

The Thinklogical ADM (Administration Module) is a secure, browser-based interface used across TLX Matrices, SMP products, and Touch Panels. It centralizes administration, diagnostics, and security settings into a single platform and reducing setup time and simplifying ongoing system administration.

ADM enables administrators to provision, secure, and maintain devices within a consistent, policy-driven environment.

CORE OPERATIONAL ELEMENTS

NETWORK CONFIGURATION

Configure IP addressing, gateways, and routing. Integrated diagnostic tools verify connectivity and support reliable communication.

SECURITY MANAGEMENT

Apply and manage security policies including firewall settings, certificate management, FIPS 140 compliance, and MACsec encryption to protect system communications.

USER ACCOUNT ADMINISTRATION

Create, modify, and remove users, assign roles, and support controlled system access.

AUDITING AND LOGGING

Monitor system activity, configuration changes, and user actions. Logs can be reviewed, filtered, and exported for traceability and compliance.

ADMINISTRATIVE FEATURES

SECURITY DEPLOYMENT TOOLS

Integrated security deployment controls for system hardening, including password enforcement, firewall configuration, security policy management, and controlled administrative access.

SECURE DEPLOYMENT		UPDATE
+ SERIAL CONSOLE	✓	
+ DeD BANNER	✓	
+ PASSWORD AND ACCOUNT SECURITY SETTINGS	✓	
+ SSH SECURITY SETTINGS	✓	
+ FIREWALL (UFW) SETTINGS	×	
+ NTP (NETWORK TIME PROTOCOL) SETTINGS	×	
+ SYSCTL UTILITY	✓	
+ SYSTEM LOGGING AND AUDIT SETTINGS	×	
+ FIPS MODE	×	
+ SYSTEMD - IGNORE CTRL-ALT-DEL KEY SEQUENCE	✓	
+ SMART CARD AUTHENTICATION	×	
+ GRUB PASSWORD PROTECTION (7 PRODUCTS)	✓	
+ LUKS DRIVE ENCRYPTION	✓	

PASSWORD POLICY ENFORCEMENT

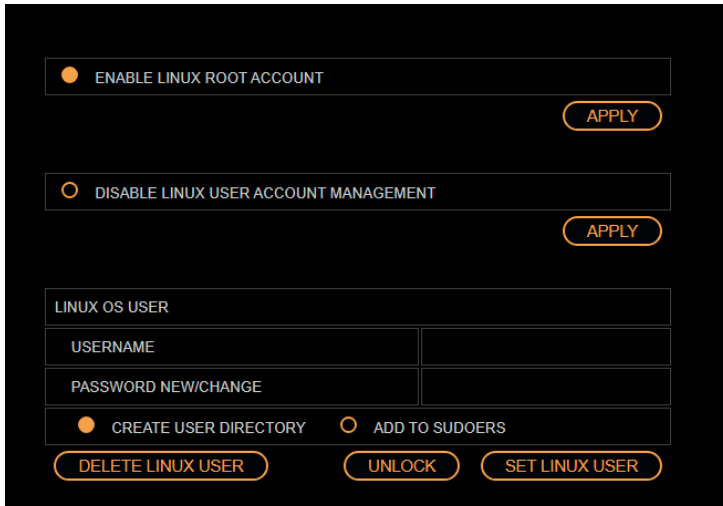
Define and enforce password complexity requirements to support security standards and controlled administrative access.

PASSWORD AUTHENTICATION MODULE	● ENABLE
MINIMUM PASSWORD LENGTH	15
MINIMUM LOWER CASE	1
MINIMUM UPPER CASE	1
MINIMUM NUMERIC	1
MINIMUM SPECIAL CHARS	1
MAXIMUM REPEATED CHARS	3
MINIMUM CHANGES NEW / OLD	4
LOGIN FAILURES BEFORE LOCKOUT	3
LOGIN FAILURES INTERVAL (SECONDS)	900
LOCKOUT TIMEOUT (MINUTES)	0
INACTIVITY TIMEOUT (MINUTES)	10
NEW PASSWORD (DAYS)	60

SUGGEST DEFAULTS APPLY

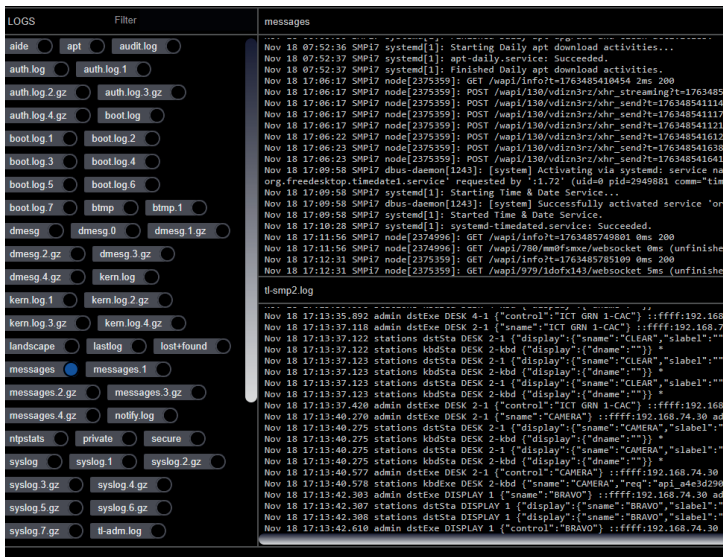
USER MANAGEMENT TOOLS

Efficiently manage user accounts, permissions, and credentials from a through a browser-based console.



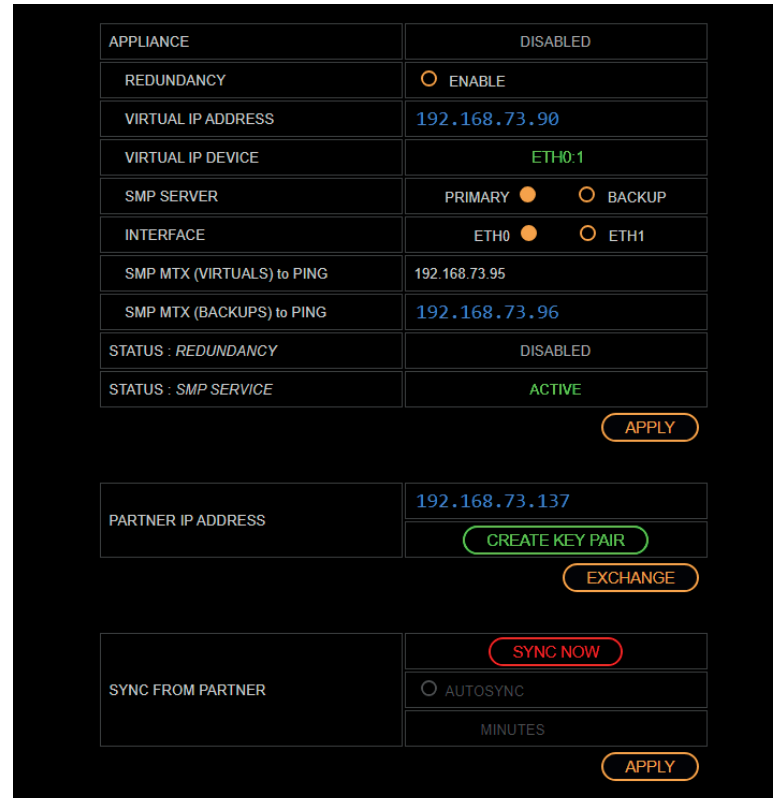
AUDITING AND LOGGING

Provides consolidated event tracking for system activity, configuration modifications, user actions, and security-related events to support compliance and operational transparency.



REDUNDANCY MANAGEMENT

Supports active/standby configurations with failover coordination to improve system reliability



SYSTEM ADVANTAGES (TECHNICAL/PLATFORM CAPABILITIES)

- Centralized access to system controls and security settings
- Consistent, policy-driven device management
- Strong security support including MACsec, HTTPS, and firewall controls
- Enhanced visibility into system activity and events
- Improved uptime through redundancy and diagnostic tools
- Supports enterprise and defense-level environments
- Reduces command-line complexity with a graphical interface

OPERATIONAL BENEFITS

- Simplifies platform configuration and administration
- Faster system setup through an intuitive browser-based interface
- Strengthens security across connected devices
- Enables traceable and auditable system changes
- Reduces operational complexity for administrators
- Supports standardized configuration across deployed systems