Tusna & data

T-MFA Secure Login

Enterprise-Grade Multi-Factor Authentication & Access Control Server

EXECUTIVE OVERVIEW

In the modern threat landscape, compromised credentials remain the primary vector for enterprise data breaches. T&d's T-MFA Secure Login delivers a robust, highly scalable, and flexible multi-factor authentication (MFA) solution designed to defend critical network infrastructures, corporate networks, and sensitive endpoints against identity-based attacks.

Engineered to blend seamlessly into complex legacy environments and cutting-edge zero-trust frameworks, T-MFA Secure Login enables organizations to implement strict access validation without operational friction. By providing extensive AAA capabilities over standard protocols and an array of versatile token choices, the platform guarantees that every access attempt is contextually verified and authorized.

> ***Key Benefit:*** *T-MFA Secure Login seamlessly transitions businesses from traditional, weak static password paradigms to high-assurance authentication baselines, lowering data breach risks by up to 99%.*

PRODUCT HIGHLIGHTS & CAPABILITIES

Flexible RADIUS Integration

Native compliance with standard corporate gateways, firewalls, and network access tools via production-tested RADIUS engines.

Diverse Token Framework

Support different OTP types and out-of-band delivery channels ensuring access compliance under any operational condition.

Granular User Management

Dynamic user lifecycle tools combined with precise, structured tier licensing matching organization growth vectors.

Granular Safety Profiles

Support for distinct non-2FA groups alongside fortified standard token configurations for total environment adaptation.

T & d
Tusna & data

CORE ARCHITECTURE & PROTOCOL SUPPORT

At its core, T-MFA Secure Login operates on an enterprise-hardened AAA framework built to maintain continuous operations within high-availability environments. The integration layer ensures reliable validation sequences with downstream firewalls, VPN concentrators, switches, and edge infrastructure.

RADIUS Implementation Specifications

The platform boasts exhaustive support for Remote Authentication Dial-In User Service (RADIUS), ensuring plug-and-play capability with industry-standard network security appliances. Supported authentication protocols include:

- **PAP (Password Authentication Protocol):** Supported for legacy application interoperability and basic routing verification mechanisms.
- **CHAP (Challenge Handshake Authentication Protocol):** Delivers enhanced cryptographic password protection utilizing a point-to-point 3-way challenge sequence.
- **MS-CHAP (Microsoft CHAP):** Full integration compatibility for legacy Microsoft-centric domain structures and architectural layers.
- **MS-CHAPv2 (Microsoft CHAP Version 2):** Premium, high-assurance authentication standard offering robust mutual cryptographic verification sequences, eliminating split-session interception threats.

Flexible Software Token Infrastructure

Organizations can easily match user requirements with an assortment of delivery models and mathematical validation algorithms:

- **TOTP (Time-Based One-Time Password):** Standardized cryptographic hashes utilizing highly accurate internal system intervals. Fully compliant with modern mobile authenticator apps (FreeOTP, Google Authenticator, Microsoft Authenticator, ...).
- **HOTP (HMAC-Based One-Time Password):** Event-counter-driven token codes ideal for scenarios where strict temporal synchronization is unfeasible.
- **Email OTP:** Highly efficient out-of-band delivery channel utilizing secure SMTP infrastructure, reducing the burden of device provisioning for third-party contractors and external auditors.
- **Without2FA (Excluded Profiles):** Dedicated rule-set enabling network administrators to route specific service accounts, automated APIs, or legacy operational equipment through distinct standard security layers without multi-factor prompts.

DEPLOYMENT TOPOLOGY

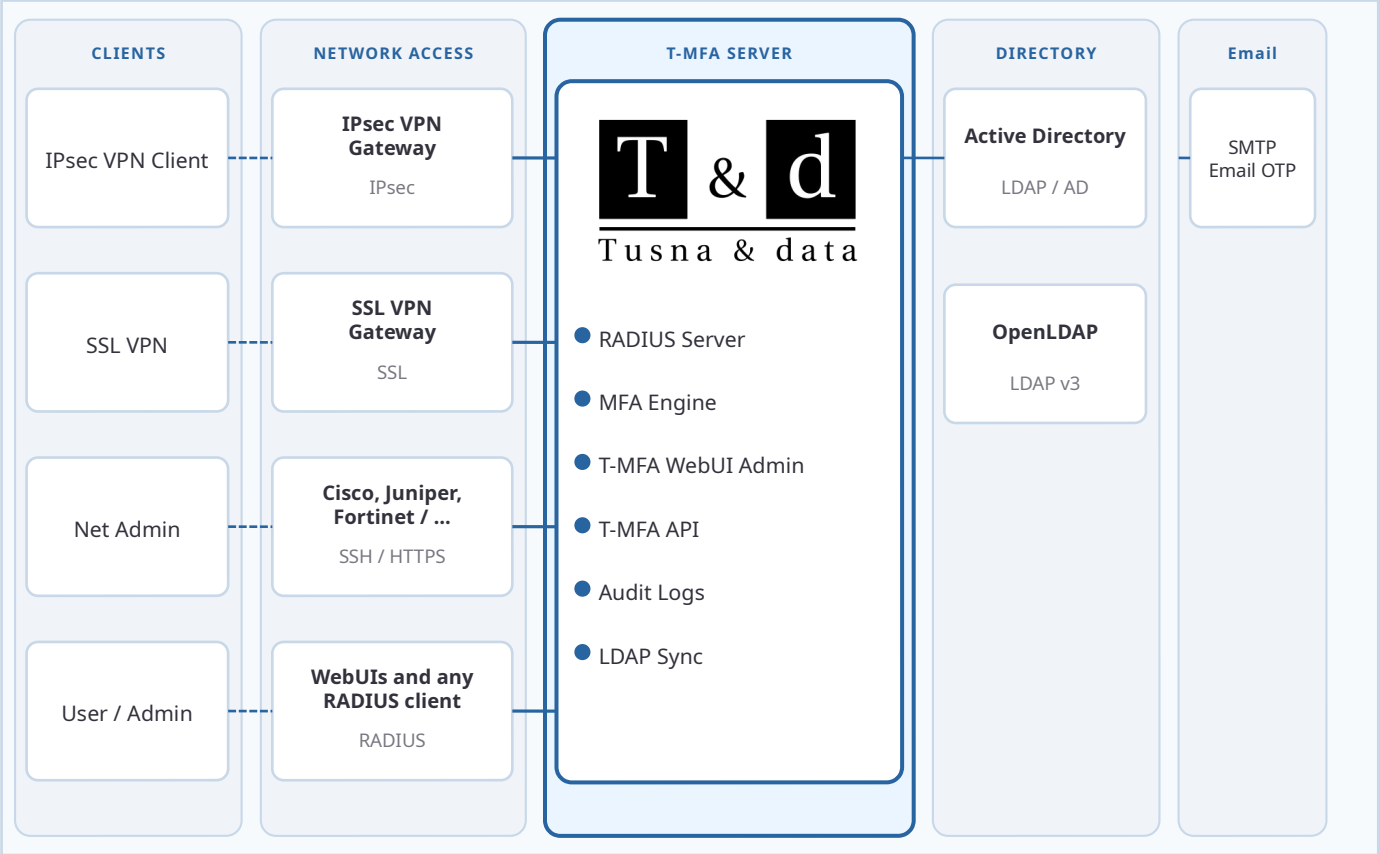


FIGURE 1: TECHNICAL INTEGRATION AND AUTHENTICATION FLOW TOPOLOGY

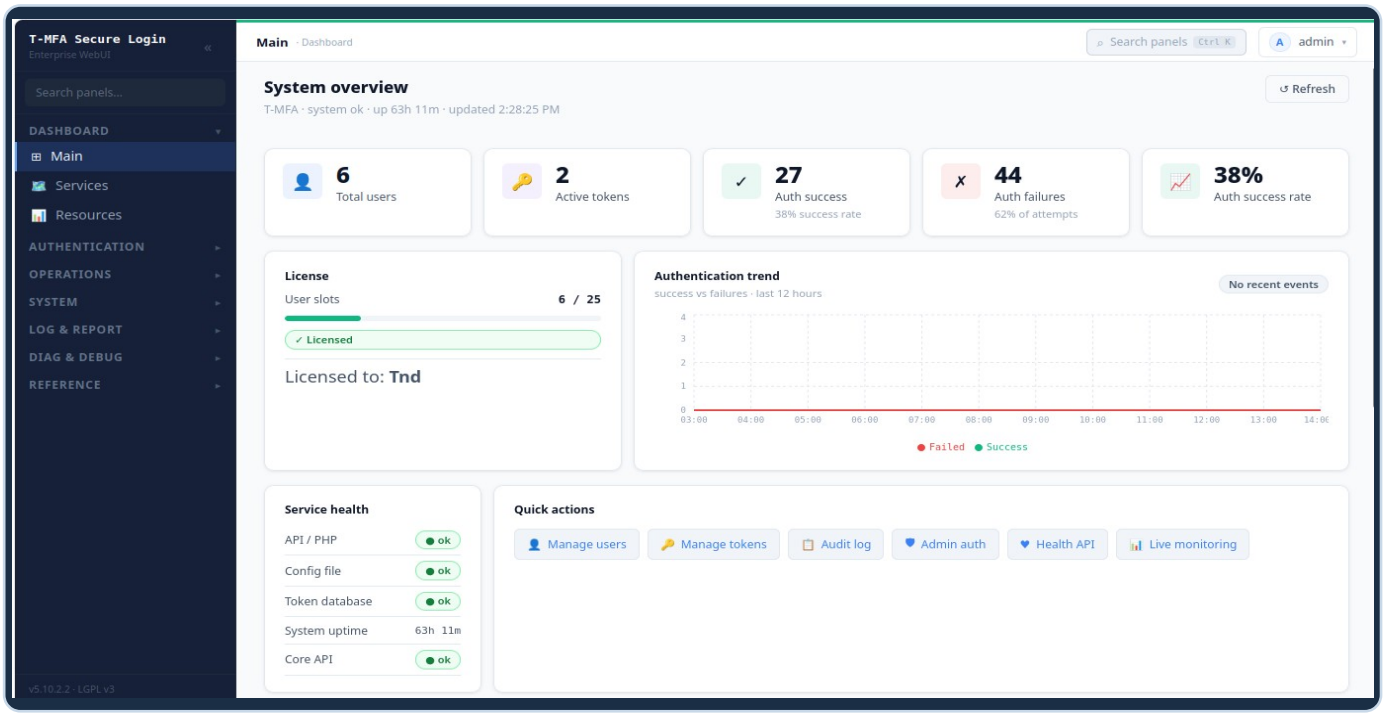
TECHNICAL SPECIFICATIONS

System & Operational Specifications	
Protocol Layer	**Supported Parameters / Standards**
RADIUS Authentication	PAP, CHAP, MS-CHAP, MS-CHAPv2
Multi-Factor Mechanisms	TOTP (RFC 6238), HOTP (RFC 4226), Out-of-band SMTP Email OTP
Exemptions Engine	Native "Without2FA" policy filters for dedicated API / Service identities
Directory Synchronisations	Active Directory, OpenLDAP, Local SQL Cryptographic Store
Deployment Modes	Virtual Appliance (OVA) — VMware vSphere, KVM / QEMU

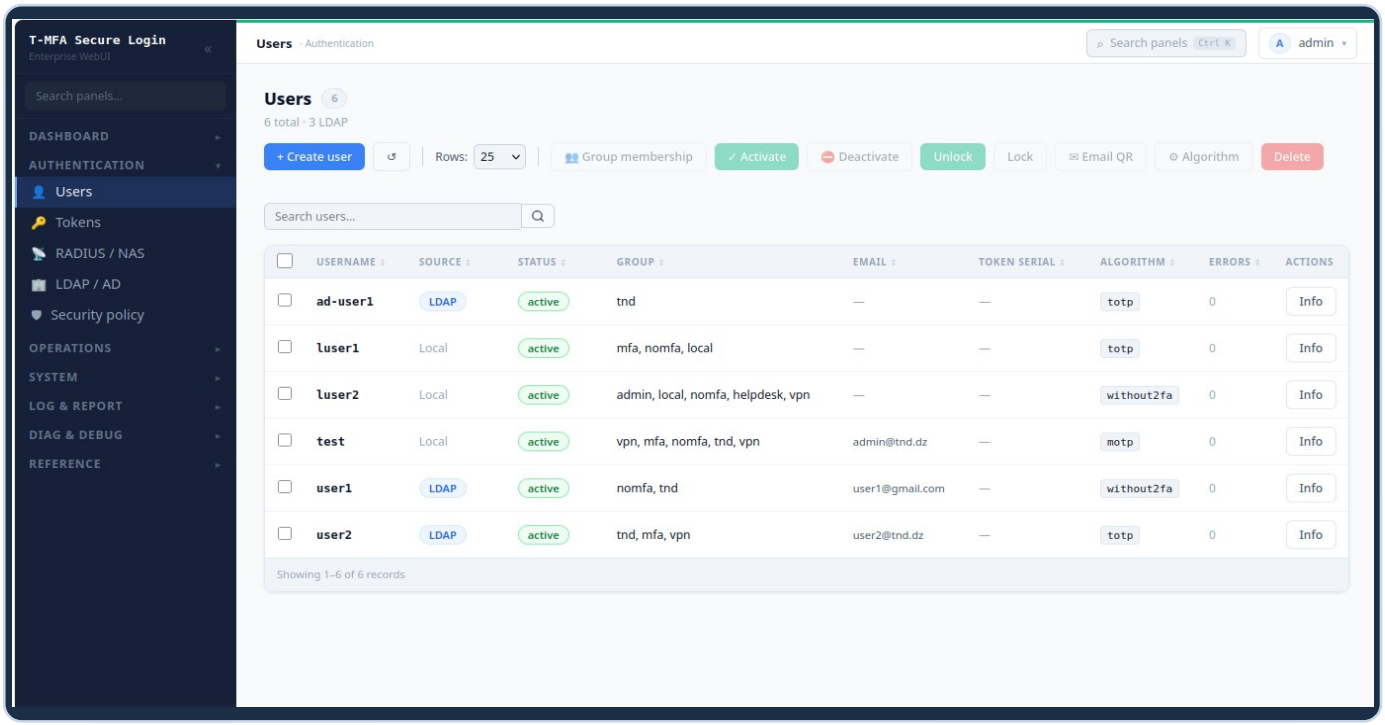
ADMINISTRATION INTERFACE

T-MFA Secure Login features a sophisticated, highly intuitive administration console designed to simplify enterprise-grade access control.

Dashboard — System Overview



Users Panel — Lifecycle Management



LICENSING & COMMERCIAL OPTIONS

The T-MFA Secure Login commercial framework is built around a predictable, User-Based seat model. Organizations face no hidden overhead costs per token, authentication server instance or communication gateway. All tiers offer the exact same full enterprise feature set, including all supported validation protocols and soft token vectors.

Product SKU	User Capacity Seat	Included Token Packages
TMFA-SL-005	Up to 5 Users	Unlimited TOTP / HOTP / Email OTP
TMFA-SL-010	Up to 10 Users	Unlimited TOTP / HOTP / Email OTP
TMFA-SL-025	Up to 25 Users	Unlimited TOTP / HOTP / Email OTP
TMFA-SL-050	Up to 50 Users	Unlimited TOTP / HOTP / Email OTP
TMFA-SL-100	Up to 100 Users	Unlimited TOTP / HOTP / Email OTP
TMFA-SL-200	Up to 200 Users	Unlimited TOTP / HOTP / Email OTP
TMFA-SL-500	Up to 500 Users	Unlimited TOTP / HOTP / Email OTP
TMFA-SL-1000	Up to 1000 Users	Unlimited TOTP / HOTP / Email OTP

SUPPORT SUBSCRIPTION

Type	Size	Description
Annual support	Per user	Includes technical support and updates

Tusna & data