Arcon

Arcon

Multi-Factor Authentication

ARCON | MFA

Enforcing access security across the entire user journey—before, during, and after user authentication.

DOCUMENT	CAPABILITIES	COMPLIANCE	WEB
Comprehensive Feature Guide	20 Features . 4 Monitoring Types	PCI-DSS . HIPAA . SOZ . ISO 27001 . GDPR	www.arconnet.com

PREDICT • PROTECT • PREVENT

00 Strengthening Access Beyond Login Security

ABOUT THE GUIDE

This document introduces ARCON | Multi-Factor Authentication (MFA), an enterprise-grade authentication framework designed to secure access beyond passwords. It highlights how ARCON | MFA protects users, applications, endpoints, infrastructure, and privileged operations through adaptive, risk-based, and contextual authentication.

The brochure covers key capabilities such as TOTP, FIDO2/WebAuthn, biometric authentication, role-based access control, geolocation and IP-based MFA, SAML/API integrations, audit reporting, and endpoint-level MFA through EPM integration. It also explains how ARCON | MFA supports Zero Trust security, reduces credential compromise risks, strengthens compliance, and extends protection before, during, and after user authentication.

01 Beyond Passwords, Stronger Access Control Security

In current IT threat landscape, relying on passwords alone is no longer sufficient to secure enterprise access. Organizations face increasing risks from credential theft, phishing attacks, and unauthorized access across applications, endpoints, and infrastructure.

ARCON | MFA delivers a comprehensive, enterprise-grade authentication framework that goes beyond traditional login security. It ensures secure access through multi-layered authentication, adaptive risk-based controls, and deep integration with enterprise systems such as PAM and EPM.

Unlike conventional MFA solutions that focus only on login, ARCON MFA enforces security across the entire user journey—before, during, and after authentication.

ARCON | MFA helps organizations to:

- Strengthens enterprise security with multi-layered authentication
- Enables Zero Trust access control across users and systems
- Reduces risk of credential compromise and phishing attacks
- Provides adaptive, context-aware authentication decisions
- Enhances compliance with regulatory and audit requirements
- Extends security beyond login to post-authentication user actions

AT A GLANCE

Built for scale, tuned for the SOC.

20
Capabilities that authenticate, secure and monitor

8
Advanced capabilities integrated with EPM

7
Compliance frameworks supported with audit-ready reporting

2
Flagship solution workflows integrated with MFA

1 Predict → 2 Protect → 3 Prevent

02 Comprehensive Feature List with Validated Use Cases

Identity & Access Control

01 Application Onboarding

Seamlessly onboard enterprise applications to enforce MFA across web and business-critical systems.

Use case:

Enterprises can onboard HRMS, ERP, CRM, ticketing, and cloud portals to enforce MFA, prevent unauthorized access, reduce credential-theft risk, and maintain audit-ready visibility across business-critical applications.

02 Role-Based Access Control (RBAC)

Define granular administrative roles and permissions for MFA configuration and governance.

Use case:

Enterprises can assign MFA admins, auditors, and helpdesk teams granular permissions, ensuring only authorized roles manage policies, user resets, reports, and governance workflows.

03 User & Group Management

Manage users, create MFA groups, and enforce policies consistently across users and applications.

Use case:

IT firms can create separate MFA groups for developers, admins, and vendors, applying consistent access policies across HRMS, DevOps, CRM, and cloud applications.

04 Disable Self-Registration

Prevent unauthorized MFA enrollment by restricting user registration to admin-approved workflows.

Use case:

IT firms can restrict MFA enrollment to admin-approved employees, contractors, and vendors, preventing rogue accounts from self-registering and accessing sensitive business applications.

Authentication Methods

01 Time-Based One-Time Password (TOTP)

Standards-based OTP authentication for secure and reliable access.

Use case:

Employees use TOTP codes from an authenticator app to securely access VPN, admin consoles, and business applications, ensuring reliable MFA even when SMS or email delivery is unavailable.

02 Token-Based Authentication

Support for hardware and software tokens.

Use case:

IT teams can secure VPN, admin portals, and critical applications by requiring hardware or software token OTPs, reducing credential misuse even when passwords are compromised.

03 FIDO2 / WebAuthn

Passwordless, phishing-resistant authentication using security keys and biometrics.

Use case:

Privileged IT admins use FIDO2 security keys or biometrics to access critical systems passwordless, preventing phishing-led credential compromise and strengthening enterprise access security.

04 Biometric Authentication

Secure login using fingerprint and device-based biometrics.

Use case:

Employees can securely access HRMS, payroll, and admin portals using fingerprint or device biometrics, reducing password misuse and strengthening identity verification.

02 Comprehensive Feature List with Validated Use Cases

05 Email-Based Push Authentication

Interactive email-based MFA approvals for enhanced user convenience.

Use case:
Employees can approve MFA requests through interactive email prompts when accessing HRMS, ERP, or cloud portals, ensuring convenient, secure access without relying on mobile apps.

06 Fallback Authentication Mechanisms

Define granular administrative roles and permissions for MFA configuration and governance.

Use case:
Enterprises can assign MFA admins, auditors, and helpdesk teams granular permissions, ensuring only authorized roles manage policies, user resets, reports, and governance workflows.

Adaptive & Contextual Security

01 Risk-Based Adaptive Authentication

Dynamically enforces MFA based on user behavior, device context, and risk signals.

Use case:
If an employee logs into VPN from an unmanaged device or unusual location, ARCON MFA triggers step-up authentication before granting access

02 Geolocation-Based MFA

Apply MFA policies based on user location and detect anomalies.

Use case:
If a developer logs in from an unusual country, ARCON MFA triggers additional verification or blocks access, preventing unauthorized entry to source-code repositories and cloud consoles.

03 IP-Based Conditional MFA

Trigger MFA when access originates outside trusted networks.

Use case:
When employees access ERP or cloud consoles from outside office IPs, ARCON MFA triggers additional verification before allowing login, reducing unauthorized access risk.

Integration & Deployment

01 API-Based Integration

Easily integrate MFA with enterprise applications and third-party systems.

Use case:
An IT helpdesk integrates ARCON MFA APIs with its ticketing portal to verify technicians before approving password resets or privileged support actions.

02 SAML-Based Integration

Support for SAML-based authentication for seamless SSO environments.

Use case:
A company integrates ARCON MFA with its SAML SSO to secure ERP and HRMS access, enabling users to authenticate once while enforcing MFA for sensitive business applications

02 Comprehensive Feature List with Validated Use Cases

05 Cisco Duo Integration

Enable hybrid MFA with Duo as an external factor with failover capabilities.

Use case:
IT teams can use Duo push as an external MFA factor for VPN or admin portal access, with ARCON failover ensuring secure login continuity during Duo outages.

06 SaaS & On-Prem Deployment

Flexible deployment options to suit enterprise infrastructure requirements.

Use case:
Any regulated bank deploys ARCON MFA on-prem for core banking while using SaaS for remote workforce access, aligning security with infrastructure and compliance needs.

Monitoring, Reporting & Compliance

01 Authentication Reports & Auditing

Detailed visibility into login attempts, failures, and authentication patterns.

Use case:
IT teams can review failed ERP login attempts and unusual access patterns to detect credential misuse, support audits, and strengthen MFA policies.

02 Exportable Audit Logs

Export logs in CSV/Excel formats for compliance and audit requirements.

Use case:
During quarterly audits, IT teams export MFA login failures, factor usage, and user activity to Excel, helping compliance teams validate access controls and investigate anomalies

03 Real-Time Activity Tracking

Monitor user authentication behavior and detect anomalies.

Use case:
An IT company tracks repeated failed MFA attempts and unusual login locations in real time, helping security teams detect account compromise and block suspicious access quickly.

Advanced Capabilities (MFA + EPM Integration)

01 Endpoint MFA (Windows & Linux)

Enforce MFA for endpoint login and critical operations.

Use case:
IT teams can enforce MFA on Windows/Linux admin workstations before login or privilege elevation, preventing unauthorized endpoint access and securing critical operations.

02 Process-Level MFA

Trigger MFA for execution of sensitive desktop applications.

Use case:
When administrators launch sensitive desktop tools like database consoles, PowerShell, or server management utilities, ARCON MFA triggers verification to prevent unauthorized execution and privileged misuse.

02 Comprehensive Feature List with Validated Use Cases

05 Privilege Elevation MFA

Require MFA before granting elevated privileges.

Use case:
A server administrator verifies with ARCON MFA before receiving temporary admin rights to install patches, modify configurations, or troubleshoot production systems.

06 Service Account MFA

Secure machine and service-level access.

Use case:
DevOps teams can enforce MFA for service accounts running scripts, jobs, or integrations, preventing unauthorized machine-level access to servers, databases, and business-critical systems.

Monitoring, Reporting & Compliance

01 Lateral Movement Protection

Prevent unauthorized access across systems within the network.

Use case:
A compromised developer account is blocked from accessing production servers or admin consoles from another endpoint unless MFA validates the user, preventing lateral movement.

02 Agentless MFA for AD Users

Enforce MFA without requiring endpoint agents.

Use case:
An IT firm can enforce MFA for Active Directory logins across shared admin servers without installing endpoint agents, reducing rollout effort while securing privileged access.

Why ARCON MFA?

ARCON | MFA is a deep security enforcement platform

While traditional MFA solutions focus only on verifying identity at login, ARCON MFA ensures end-to-end access security in modern enterprise environments.

PCI-DSS | HIPAA | SOX | GDPR | DORA | ISO 27001 | SOC 2

Control over what users can do after login

Enforces MFA beyond initial authentication, validating sensitive actions like process launches, privilege elevation, and command execution before access is allowed.

Protection at endpoint, application, and infrastructure levels

Secures access across endpoints, business applications, and infrastructure assets, reducing credential misuse, unauthorized operations, lateral movement, and enterprise-wide exposure risks.

Integration with privileged access and operational security layers

Integrates MFA with PAM and EPM workflows, enforcing step-up authentication for privileged sessions, endpoint actions, and enterprise operational security controls

SUPPORT & CONTACT

04 Talk to us. Then deploy with confidence.

ARCON|MFA is developed and maintained by ARCON Tech Solutions Private Limited. Remote support is available 24 × 7, 365 days per year.

SALES & DEMO

Book a working session with our solutions team.

For pricing, product demonstrations, or enquiries — reach the ARCON sales team directly, or leave your contact details on the website and we'll respond promptly.

sales@arconnet.com →

VISIT

arconnet.com

ARCON SUPPORT CENTRE (ASC)

arcon.my.site.com/login

Sign in with your registered account. Access is exclusive to registered users with a valid, active support package.

CENTRAL SUPPORT

arcos.support@arconnet.com

Remote support is available 24 × 7, 365 days per year.

GLOBAL HOTLINES

GLOBAL	+91 8080 005 577	UAE	+971 800 035 703 628
USA	1 800 350 1093	EUROPE	+49 32 212 249 836

For ARCON Support, press 3 on all hotlines.

Arcon

Securing every identity. Protecting every file. Across the entire enterprise estate.

— ARCON TECH SOLUTIONS PRIVATE LIMITED