

Strong Authentication for Secure Remote (VPN) Access



The Move to Ubiquitous Remote Access

To accommodate flexible work arrangements, support traveling employees, retain expertise following office relocation, and keep pace with international work hours, organizations are coming under increased pressure to offer a secure VPN access strategy that allows users to access the enterprise network anytime, anywhere.

Hurdles to Ubiquitous Access

Organizations implementing a secure network access strategy are confronted with several key challenges, namely:

- **Mobility** - With users connecting from multiple devices, organizations require a device-agnostic authentication strategy.
- **Security** - Passwords provide an insufficient form of protection for remote network access, as they are vulnerable to theft, social engineering, phishing, and hacking, and leave organizations vulnerable to unauthorized access and data breaches.
- **Cost** - Secure remote access for all employees is still perceived to be a high-cost endeavor.
- **Compliance** - A fragmented authentication strategy makes it difficult to satisfy security-audit requirements, as there is no unified visibility into the entire chain of access events, throughout the IT environment.

Frictionless Remote Access

SafeNet Access Management and Authentication solutions offer frictionless remote access:

- From any device
- Using the broadest range of multi factor authentication methods, including software tokens, phone-as-a-token, and tokenless methods such as context-based authentication and PKI certificate based methods including virtual smart cards, hardware and tokens
- With over a dozen seamless VPN integrations from leading vendors such as F-5, Palo Alto, Cisco, Check Point, Citrix, Fortinet, IBM, Oracle, Microsoft, and others
- Delivered on-premises or as-a-service from the cloud, offering platform flexibility

Key benefits

- Strong, multi-factor authentication with the broadest range of methods, including soft tokens and passwordless authentication
- Secure access from any device
- Automated workflows yielding reduced IT management overhead
- Simplified compliance

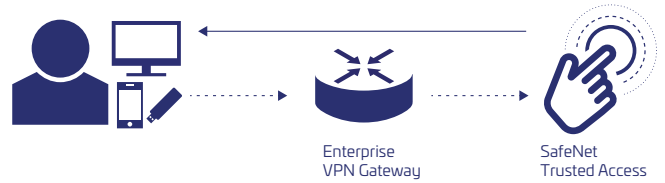
Wide-ranging VPN Support

- Any VPN application supporting RADIUS or SAML
- Native support for SSL VPNs
- Prevalidated integrations with leading VPN solutions

Frictionless Management Strategy

SafeNet Access Management and Authentication Solutions reduce IT management overhead and simplify compliance through:

- Fully automated workflows, including:
 - Token and user lifecycle management, including policy-based provisioning, revocation, and administration
 - Real time threshold-and event-based alerts
 - Extensive user self-service via fully customizable portals, allowing users to manage their own passwords and tokens, driving down help desk calls
- A single point of management for defining and enforcing access control throughout your organization's IT ecosystem, including all on-premises, virtual, and cloud-based resources, producing a single audit trail. Integration for complementary use cases is offered out-of-the-box for leading network logon, VDI, web portal, and cloud (SaaS) solutions.
- Native support for identity federation, allowing you to secure SaaS applications with the same authentication solution used to secure the corporate VPN.



About SafeNet Access Management and Authentication Solutions

Thales's industry-leading Access Management and Authentication solutions let enterprises centrally manage and secure access to enterprise IT, web and cloud-based applications. Utilizing policy-based SSO and universal authentication methods, enterprises can effectively prevent breaches, migrate to the cloud securely and simplify regulatory compliance.

To learn more about access management from Thales, visit <https://safenet.gemalto.com/access-management/> or join a livedemo webinar at <https://www.brighttalk.com/webcast/2037/334449>

Easily extend MFA to cloud apps

SafeNet Trusted Access: Access Management AND multi factor authentication in One

With SafeNet Trusted Access, businesses get the best of both worlds — a broad range of authentication methods combined with intuitive cloud-based access management and single sign on.

SafeNet Trusted Access easily lets you apply the multi-factor authentication methods deployed for VPNs to cloud and web-based applications. By federating your cloud apps via SAML or OIDC and applying the same authentication methods to both VPNs and cloud apps, organizations are able to achieve consistent access security across their IT ecosystem.



Supported Authentication Methods

- OTP Push
- OTP App
- OTP Hardware
- Pattern-based authentication
- Out-of-band via email and SMS text messages
- Password
- Kerberos
- PKI credentials
- Google Authenticator
- Passwordless authentication
- Biometric
- Voice
- 3rd party

Management Platform

- SafeNet Trusted Access