PRODUCT BRIEF

SafeNet Authentication Manager

Empower your organization's authentication infrastructure with a flexible, extensible, and scalable management platform.

Support for your Evolving Authentication Needs

SafeNet Authentication Manager is a comprehensive authentication server that allows organizations to implement a future-ready strong authentication strategy for securing local and remote access to numerous corporate resources using a single authentication back-end.

Offering OTP, certificate-based and software authentication solutions as well as context-based and step-up authentication, SafeNet Authentication Manager enables organizations to address their current and evolving secure access needs.

Context-based Authentication for Optimal Convenience

SafeNet Authentication Manager's context-based authentication capabilities allow organizations to achieve convenient, cost-effective secure remote access with unobtrusive strong authentication, while maintaining the flexibility and agility to add protection with stronger methods of security when required.

With its "step-up" authentication capabilities, SafeNet Authentication Manager makes it easier for users by requiring an additional authentication factor only if they don't meet pre-defined policy rules determined by IT administrators.

Extend Strong Authentication to Cloud Computing

As enterprises migrate to cloud computing environments and SaaS applications, they face the challenge of ensuring secure and convenient access to core applications and highly confidential resources that no longer reside within the corporate network.

SafeNet Authentication Manager addresses this challenge by providing a seamless, consistent strong authentication and federated login experience for enterprise users who need to securely access SaaS applications, such as GoogleApps and SalesForce.com (SFDC).

Benefits

- **Extend secure access to cloud environments:** Secure access, federated login and automatic user provisioning for SaaS applications.
- **Extend secure access to mobile endpoints:** Credential provisioning and authentication management for iOS devices ensures that only employees with trusted devices can access corporate resources.
- **Achieve granular control with context-based authentication:** Configurable policy rules to offer granular control over the level of authentication required each time a user logs on to an online resource.
- **Address different risk levels:** Support for a broad range of authentication methods allows organizations to address numerous risk profiles.
- **Flexibility to grow:** Evolve your authentication infrastructure to include OTP and CBA solutions, as well as advanced security applications.
- **Reduce support costs:** Automated processes, over-the air activation and installation for software tokens, and intuitive self-service tools ensure extensive support for end users and lower helpdesk costs.
- **Maintain compliancy:** Comprehensive auditing and reporting features enable compliance with privacy regulations.

Combined Physical and Logical Access in One Credential

Many organizations have the need to protect physical locations, including doors, parking facilities and secure zones. Adding a converged badge solution has clear benefits for the office user who only needs to carry one credential and remember a single PIN code or a short password to use in conjunction with their badge.

SafeNet Authentication Manager is a comprehensive authentication and credential management server for securing physical controls in addition to logical and remote access.

Features

Multiple authentication methods and form factors

- Native support for context-based authentication
- Support for step-up authentication
- Support for certificate-based, OTP, software, and OOB authentication
- Available form factors include key fob tokens, USB tokens, smart cards, software tokens, phone tokens

Secure access to multiple resources

- Cloud (SaaS) applications via support for SAML 2.0, e.g. SalesForce
- VPNs
- OWA, SharePoint and other Web-based portals
- Virtual Desktop Environments, e.g. Citrix, VMware and AWS
- Local network logon (supported in online and offline mode)

Support for secure mobility

- Secure access using any authentication method from any endpoint
- Credential provisioning and management for iOS devices

Native identity federation

- Embedded support for federated login using SAML 2.0
- Automatic user account registration and provisioning to select SaaS applications

Comprehensive management capabilities

Reporting and compliance

- Single audit trail for entire authentication ecosystem
- Separation of duties and role-based authorization
- Reporting and audit tracking

Complete lifecycle administration

- Self-service portals that allow user self-enrollment and token management
- Certificate lifecycle management
- Authenticator assignment, enrollment, and update based on predefined policies
- Authenticator revocation, temporary disablement, and replacement
- Temporary token provisioning

Flexibility to scale

- Cross-domain management
- Multi-forest Active Directory support

Supported SafeNet Authenticators

- IDPrime MD 830-FIPS smart card
- IDPrime MD 830-ICP smart card
- IDPrime MD 3810 smart card
- IDPrime MD 3811 smart card
- IDPrime MD 3810 MIFARE 1K smart card
- SafeNet eToken 5110, 5110 HID
- SafeNet eToken 7300

Supported Operating Systems

- Windows Server 2008 SP2 (32-bit, 64-bit) and 2008 R2 SP1(32-bit, 64-bit)
- Windows Server 2012 and 2012 R2 (64-bit)
- Windows Server 2016
- Windows 7 SP1 (32-bit, 64-bit)
- Windows 8 (32-bit, 64-bit)
- Windows 8.1 (32-bit, 64-bit)
- Windows 10 (32-bit, 64-bit)
- Mobile Clients: iOS

User repositories:

- Microsoft Active Directory
- AD LDS
- Microsoft SQL Server
- Open LDAP
- Novell eDirectory

Contact Us: For all office locations and contact information, please visit safenet.gemalto.com

Follow Us: blog.gemalto.com/security

GEMALTO.COM

gemalto
security to be free