



SafeNet Authentication Solutions: A Single Strong Authentication Platform for Cloud and On-Premises Applications

SECURITY GUIDE

Benefits

- **Seamlessly extend secure access to the cloud:** Protect resources residing in the cloud from a single authentication platform, offering validated integrations with dozens of leading SaaS apps
- **Increased user convenience:** Federated login allows users to log on to the corporate network, on-prem and cloud applications—all with the same enterprise logon credentials
- **Central management of entire IT ecosystem security:** Define and deploy policies for network, web- and cloud-based apps from a single backend, optimizing visibility and facilitating compliance
- **Deploys without changing existing architecture:** Support for a wide range of authentication methods lets organizations implement strong authentication without sacrificing existing investments, with SafeNet solutions available from the cloud or on-premises
- **Automate provisioning of SaaS user accounts:** Automatic provisioning to SaaS applications significantly reduces administration overhead by enabling IT teams to centrally configure access controls to all applications from within SafeNet Authentication Manager

Easily Secure Access to Cloud Applications by Federating Identities with SafeNet

The Security and Business Implications of the Cloud

The move to the cloud has been both widespread and fast. However, for the enterprise security teams tasked with protecting access to sensitive data and systems, this evolution has been presenting significant challenges:

- **Diffusion of access control boundaries:** As enterprises transition to the cloud, they are essentially shifting their focus from controlling security with physical boundaries, to that of a virtual infrastructure. When security is physically contained, information is protected in the data center using methods such as encryption, strong authentication, access controls and application permissions. But when data and applications move to the cloud, user access—by default—takes place remotely, with weak, static passwords serving as the only security mechanism to protect against unauthorized access. Organizations therefore have to contend with a blurred IT perimeter, necessitating access controls for applications both in the cloud and those within the confines of the data center.
- **Identity proliferation:** The deployment of numerous cloud applications that are not part of an enterprise identity scheme, results in numerous additional credentials that users need to memorize. This translates into heightened security risks, greater overhead for helpdesk personnel and inconvenience for users. Users now have an even greater number of identities and permissions that are not necessarily issued by the organization.

The trends described above have direct security and administrative ramifications on how organizations maintain control and manage user access to applications in the cloud, how they cope with the proliferation of user identities, and how they cope with supporting a comprehensive secure mobility policy.

Strong Authentication and Identity Federation to Cloud-based SaaS Applications

To contend with the complexity of these security and management challenges, SafeNet's authentication platforms allow organizations to extend users' on-premises identities to cloud applications. By so doing, organizations are able to centrally manage and control their strong authentication environments, automatically provision users with SaaS application accounts, and provide a complete web federated login experience, sparing users the time and effort required to maintain—and log on with—separate SaaS account credentials.

Supported authentication methods

- One-time passwords (OTP)
- Certificate-based authentication
- Context-based authentication
- Out-of-band via SMS and email
- Pattern-based authentication

Available form factors

- Hardware tokens
- Software tokens
- Smartcards
- USB tokens
- Phone-as-a-token

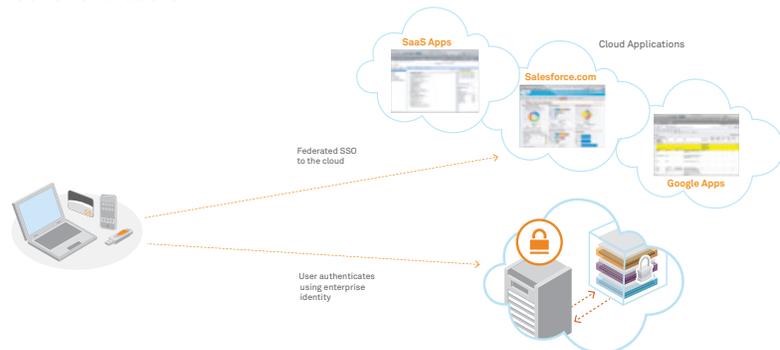


SafeNet's authentication platforms provide a seamless, consistent strong authentication and federated login experience for users who want to access cloud applications such as Microsoft Office 365, Google Apps and Salesforce.com. By federating an enterprise user's identity via the Security Assertion Markup Language (SAML), SafeNet authentication platforms leverage an organization's existing authentication infrastructure so that users can use the same logon credentials for both on-premises and cloud-based applications.

SafeNet Authentication Solutions: Your Trusted Authentication Provider

SafeNet's authentication management platforms in essence act as the trusted identity provider, giving authorized users permission to access SaaS applications. The SaaS service, in turn, is configured to allow access only to those users given permission by SafeNet's authentication platform.

This unified approach, combined with support for a broad range of authentication methods and form factors, allows organizations to transition to the cloud without compromising their security perimeter. Moreover, since access control settings, provisioning and federated login are handled from one platform, organizations achieve significant cost efficiencies that are reflected in reduced IT infrastructure costs, lower IT maintenance and better productivity and convenience for end users.



Move to the Cloud without Relinquishing Security Controls

Strong authentication and federated login to SaaS applications is available with SafeNet Authentication Service and SafeNet Authentication Manager.

With either platform, the enterprise security team retains complete control over the configuration, deployment, and administration of the authentication infrastructure, which remains in the enterprise's IT domain.

Organizations can deploy either platform in their network's DMZ, so users can authenticate directly to cloud-based applications and services, rather than having to go through the corporate VPN. As a result, users have a faster, more seamless experience accessing on-premises and cloud-based applications, while enterprises enjoy optimized security.

The SafeNet Family of Authentication Solutions

SafeNet offers Next Generation Authentication solutions that protect identities and ensure that individuals are who they claim to be. With automated administration and user & token management, SafeNet's solutions support the broadest range of authentication methods and extend identities beyond the enterprise with federated login.

SafeNet's solutions streamline authentication across an organization's IT ecosystem with unified, centrally managed access policies—managed from one authentication back end, delivered in the cloud or on premises.

To learn more about SafeNet's complete portfolio of authentication solutions, please visit our website at www.safenet-inc.com/multi-factor-authentication/.

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

Follow Us: www.safenet-inc.com/news-media/

©2014 SafeNet, Inc. All rights reserved. SafeNet and SafeNet logo are registered trademarks of SafeNet. All other product names are trademarks of their respective owners. WP (EN)-11.17.14

