

A man and a woman are in a server room. The man, on the left, is smiling and looking at a tablet held by the woman. The woman, on the right, is looking down at the tablet. They are both wearing white shirts and dark ties. The background shows server racks with yellow and blue cables.

Product Brief

Protect Critical Systems & Simplify Access with SafeNet Authentication Service

cpl.thalesgroup.com

THALES
Building a future we can all trust

While moving to the cloud is a trend for the majority of businesses founded in the 21st-century, many well-established companies have made the conscious and strategic decision to maintain their on-premises systems due to security and compliance requirements, downtime and data sovereignty concerns, or simply because their mainframes or custom-built legacy applications cannot be supported in the cloud.

Security vendors are pushing for widespread cloud-based identity and access management (IAM) solutions, but these often don't work for businesses that are still largely running on-prem. These organizations need an authentication management solution that meets them where they are, uniquely tailored to their environment.

Cloud-based IAM Falls Short for Security-First Organizations

Fragmented and Hybrid IT environments make authentication more complex

Many organizations relinquish control in pursuit of flexibility from a cloud-based IAM, but this often doesn't align with their security and resiliency priorities.

One-Size-Fits-All MFA Leaves Significant Gaps

With different application sensitivity, user roles, compliance requirements, and more, simple SMS-based 2FA methods or otherwise just aren't cutting it. Other solutions are often overly complex for some users or not secure enough in other situations.

Increased Scrutiny from Compliance Regulators and Sovereignty Laws

Standards like PCI DSS, NIS 2, ISO 27001 require least privilege principles and enabling MFA policies for accessing any PII and other forms of protected data, which outdated solutions fail to do effectively, leading to avoidable fines.

Password-based Logins Are Highly Targeted

Attackers still use their tried-and-true methods of stealing login credentials. Gaining access to just one credential leads to hefty downstream effects as they traverse the system to access a goldmine of valuable data.

SafeNet Authentication Service Private Cloud Edition: For Enterprises That Can't Go Cloud-Only

SafeNet Authentication Service Public Cloud Edition (SAS PCE) is a single sign-on (SSO) and multi-factor authentication (MFA) identity provider (IdP) for on-premises and SaaS applications. With SAS PCE you can:



Improve MFA adoption with a wide range of authentication tokens you can apply based on user action, data access, and more



Remove unnecessary reauthentication for access requests coming from the same user and browser to reduce excessive user friction



Never compromise on user experience while maintaining a high standard of security

Unlike cloud-based authentication and access management tools, SAS PCE is a uniquely equipped solution that seamlessly integrates with existing infrastructure and applications, minimizing disruptions and ensuring smooth operations.



What You Get: The Thales Advantage

Seamless Single Sign-On (SSO) for Your Whole Application Environment

Eliminate the hassle and frustration of managing multiple logins. With SSO, users can authenticate once and seamlessly access multiple applications—no more password fatigue or constant interruptions. Plus, while SAS PCE acts as an on-prem IdP, you can enable a unified authentication experience by integrating another IdP of choice.

Passwordless Authentication

Using advanced, phishing-resistant authentication methods such as FIDO, Windows Hello, PKI, and many others, your organization no longer has to rely on traditional, highly vulnerable passwords.

Extensive Suite of Modern MFA Methods

- Push OTP
- MobilePASS+ (Authenticator app)
- OTP
- Hardware token
- SMS/Email
- GrIDSure (pattern-based)
- Certificate-based authentication
- FIDO

Conditional Access Policies

Powerful policy configuration ensures you enforce the right access policies for the right apps and users to maintain the integrity of all authentications.

Fast Time-to-Value and User-Initiated Self-Enrollment

Upon integrating with existing directories, SAS PCE deployment is user-led—speeding up organization-wide adoption and reducing IT toil. Once SAS PCE is deployed, users receive a step-by-step guide for registering their MFA factors and enabling SSO.

Data-Driven Insights and Seamless Workflow Integration

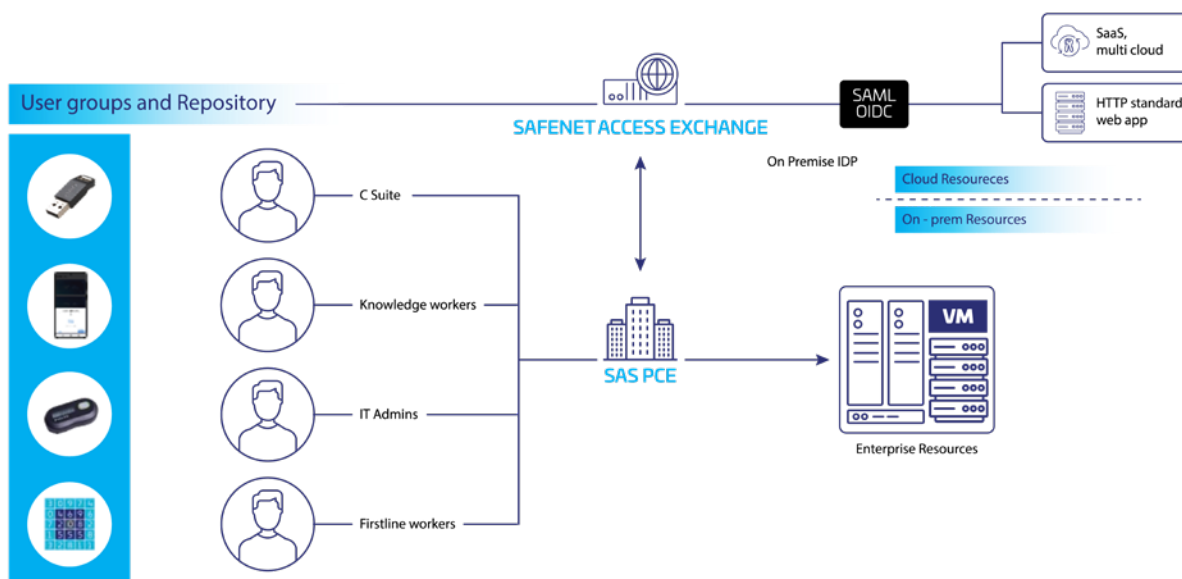
With up to 30-days of detailed event logs automatically exported to your SIEM, you can get deeper context into failed access attempts, informing future authentication policies.

Support for Broad Range of Protocols

- SAML
- OIDC
- WS-Fed
- RADIUS
- Agents
- REST and SCIM APIs
- Application gateways
- Legacy applications

Fallback Support for Cloud-Based IdPs


SAS PCE acts as a fallback mechanism for other cloud-based IdPs like Okta, Ping, and EntraID in the event of an outage to maintain access for your employees.



About Thales

As a global leader in cybersecurity, Thales safeguards sensitive data, identities, applications, and software for the most trusted brands in the world. Through advanced encryption, identity access management,

application security, and software entitlement, Thales secures cloud environments, defends against cyber threats, ensures compliance, and enables trusted digital experiences



Take SafeNet Authentication Service Private Cloud Edition for a spin by requesting your exclusive demo here.