Silverfort | THALES

Silverfort and Thales SafeNet Trusted Access (STA) integration

Extend single sign-on (SSO), multi-factor authentication (MFA), and access management to your on-prem and legacy resources with the Silverfort and Thales STA integration

Global, cloud-first organizations face the challenge of extending secure, continuous access to the growing number of applications and services your teams rely on every day. With the increased adoption of SaaS and the integrated nature of these applications, one weak access point can lead to a lot of downstream risks for the business at large.

Passwords have become the weakest security parameter due to employees having to remember hundreds of credentials, self-service password resets being exploited, and attackers leveraging the helpdesk to impersonate privileged users. These aspects have motivated organizations to go passwordless, and remove an area of growing risk and a ton of user friction.

The biggest barrier for passwordless adoption has been because of disparate on-prem and legacy resources scattered across the organization, which can't be replicated in the cloud. By design these apps use passwords for authentication, and while protecting them with MFA is often a mandatory requirement, replacing them or redesigning them will not be a business priority.

Bridging legacy resources with Silverfort and Thales STA

To help organizations with a smooth passwordless migration, Silverfort and Thales have come together to deliver an authentication and access management solution that extends from cloud-based applications to legacy resources seamlessly.

With the Silverfort's Thales STA bridge, you can:

- **Go passwordless**: For mobile, SaaS, modern web applications, and managed windows PC
- **MFA and SSO for legacy resources**: Non-SAML web applications, desktop applications, file shares, databases, command line access tools, and other on-prem resources.

Thales SafeNet Trusted Access (STA)

SafeNet Trusted Access (STA) is a single sign-on (SSO), multi-factor authentication (MFA), and access management solution for both cloud and on-premises applications. With STA you can:

- Improve MFA adoption with a wide range of authentication tokens, including software and hardware tokens, such as FIDO, based on user action, data access, and more
- Automate workflows tailored to the specific needs, behaviors, and characteristics of different users
- Never compromise on user experience while maintaining a high standard of security

Unlike basic authentication and access management tools, STA enables organizations to secure access to their cloud and on premises applications by protecting against unauthorized access, without sacrificing user experience. As a modern authentication solution, STA helps increase MFA adoption for any type of workforce user.

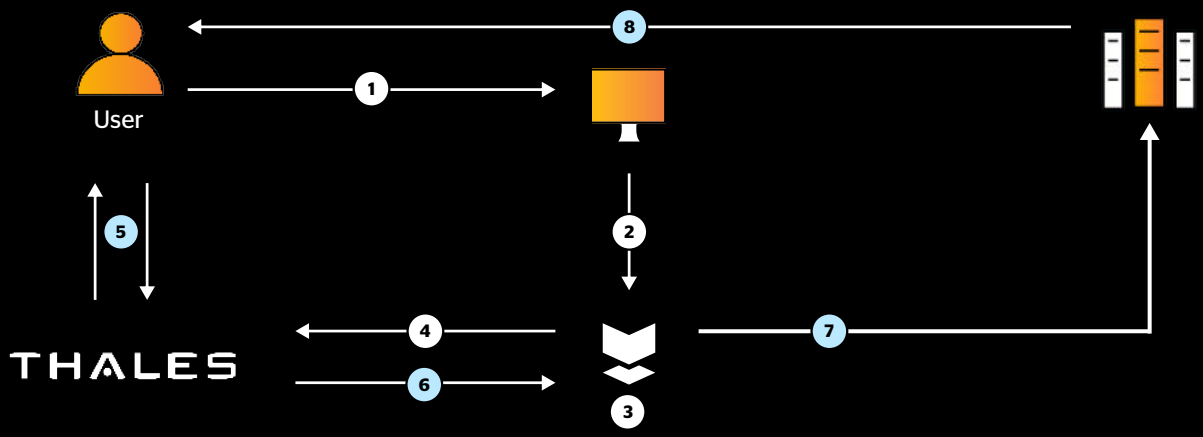
Silverfort Identity Security Platform

Silverfort seamlessly bridges any type of authentication (legacy apps, command-line tools, and more) into Thales STA as if it were a modern web application. With Silverfort's Thales STA bridge, customers can create SAML apps for on-prem resources, allowing them to leverage any Thales STA authentication flow. By applying a policy to each bridged on-prem resource, organizations can unify hybrid resource management. Once authentication and access policies are set, Silverfort forwards all access attempts through the bridged application to Thales STA, where they are managed, monitored, and secured.

How Silverfort and Thales STA work

Silverfort acts as a SAML Service Provider (SP) and seamlessly integrates legacy authentication protocols like Kerberos, NTLM, and LDAPS into Thales STA, allowing them to be treated like a modern web application. Users can define access policies for these bridged applications, leveraging Thales STA security controls and MFA capabilities. By applying policies to each bridged on-prem resource, organizations can unify hybrid resource management. Once authentication and access policies have been configured, Silverfort forwards all access attempts to Thales STA, where they are managed, monitored, and secured.

Enabling Silverfort's Thales STA bridge



1. User initiates an authentication to on-prem resources (to Active Directory) and sends Active Directory (AD) a request to access the resource.
2. AD forwards the request to Silverfort.
3. Silverfort evaluates the authentication and decides whether to allow, trigger MFA, or block.
4. If Silverfort triggers MFA, Silverfort sends the access request to Thales STA.
5. Thales STA evaluates the authentication based on set policy and sends the MFA request to the user.
6. After user's identity verification, Thales STA forwards the verdict to Silverfort.
7. Silverfort accepts the verdict and forwards it to AD.
8. AD sends the response to the user to either allow the authentication or block it.

Key benefits

Organization-wide passwordless authentication

Provide your employees with seamless passwordless experience, enabling secure, frictionless access to critical resources without the risks of traditional usernames and passwords.

Broad range of phishing-resistant authenticators

Extend Thales STA MFA, phishing-resistant authentication such as FIDO, SSO, and access policies to any resource, including on-prem servers, desktop and legacy web apps, IT infrastructure, and command-line tools.

Consistent user experience

Provide users with a consistent and familiar experience when accessing any resource, both on-prem and in the cloud.

Hybrid attack protection

Detect and prevent advanced lateral movement attacks that connect between the on-prem and cloud environments.

About Silverfort

Silverfort secures every dimension of identity. We are the first to deliver an end-to-end identity security platform that is easy to deploy and won't disrupt business operations, resulting in better security outcomes with less work. Discover every identity across every environment, analyze exposures to reduce your attack surfaces, and enforce security controls inline to stop lateral movement, ransomware, and other identity threats.

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.