cpl.thalesgroup.com

THALES
Building a future we can all trust

10 Things to Know

Are you ready for the SFDC MFA requirements?

1. What is the new Salesforce (SFDC) MFA requirement?

All internal users (anyone who has employee privileges, whether or not they are an employee) who log into SFDC products through the user interface, from mobile or desktop devices, must use MFA.

2. Deadline to comply

SFDC requirements for MFA are in effect starting February 1, 2022.

3. What happens if you don't comply?

Customers who don't enable appropriate MFA by February 1, 2022 will be out of compliance with their contractual obligations. SFDC recommends that customers consult with their legal team to understand the implications.

4. What methods are not accepted as MFA?

SFDC aligns with NIST and the general consensus in the security industry – weaker authentication methods are discouraged or disallowed. SFDC does not accept the following methods for MFA:

- Email
- SMS text messages
- Phone calls

5. What options does an organization have to meet the SFDC MFA requirement?

a. Use a third-party authentication and SSO provider, such as Thales SafeNet Trusted Access.

b. Use the SFDC authentication service.

6. What considerations should I take into account when deciding which approach to take?

Given that 90% of hacks start with compromised credentials, you may be in one of the many organizations looking for ways to deploy MFA across your entire SaaS estate – not only for SFDC apps.

In today's enterprise reality, users have diverse authentication needs. Some users will have inconsistent mobile coverage. Many will use multiple devices. All will need to securely access dozens of apps.

To maintain optimal security and ensure a convenient login experience, IT leaders should look for a solution that can:

- Meet users' expectations about being able to log into SFDC and other apps, whatever the context, on any device, with an MFA experience that suits them
- Address the needs of IT teams who have to support and onboard thousands of users remotely and securely with minimal involvement
- Support multiple business units across the globe and offer a local language experience
- Deliver an audit trail of all access and authentication events and remain compliant

7. How can Thales help my organization meet the SFDC requirement?

With its wizard-based template for SFDC and hundreds of other enterprise apps, Thales's SafeNet Trusted Access lets you enable a policy in a couple of minutes — we make it easy and fast to meet the SFDC Feb 2022 deadline.

SafeNet Trusted Access enables organizations to protect enterprise applications and scale securely in the cloud with a broad range of authentication capabilities, while ensuring security with Smart SSO and policy-driven access controls.

> "Enable a policy in a couple of minutes"

Thales SafeNet Trusted Access

Universal authentication methods

OTP Push
FIDO
Biometric
Hardware
Pattern Based
PKI
Passwordless
3rd Party
Google Authenticator
Password
Voice
eMail
SMS

- Deploy secure access quickly & efficiently
- Avoid vendor lock-in & keep control of your access security
- Prevent breaches and avoid financial liability and penalties
- Meet budget and business goals

a. In addition to expanding the MFA options, SafeNet Trusted Access simplifies implementation, management, and governance.

For SFDC products, other cloud services, and on-prem apps, SafeNet Trusted Access provides Smart Single-Sign On (Smart SSO, also known as "Secure SSO") – the ability to seamlessly evaluate each access attempt and enforce the right authentication method for your user.

Smart SSO offers the optimal balance of convenience and security, and helps organizations achieve Zero Trust security by evaluating access security continuously and stepping up authentication measures when the access attempt does not match what you have configured as acceptable. Unlike regular SSO, Smart SSO eliminates the scenario in which a user's credentials can become a single point of failure.

b. Thales can support all of your users' diverse authentication needs and help you achieve "authentication everywhere" by offering the largest selection of authentication methods with different form factors and certifications to support a spectrum of users and work environments. Our focus is:

1. **Risk-appropriate authentication**
2. **End-to-end security**
3. **Low-friction and superior user experience**
4. **Minimum number of authentication methods/user**
5. **Audit trail and certifications to meet compliance regulations**

8. How does Thales meet NIST security categorizations?

SFDC typically contains GDPR-sensitive information, Personally Identifiable Information (PII), and key company and competitive information – compelling reasons to select higher-assurance authentication.

Thales offers authentication methods for every NIST Assurance Level, with software and hardware solutions including: OTP + PIN + Password, mobile push + biometrics, FIDO devices, and a pattern-based option. This means you can deploy multiple authentication methods to your users – or deploy different authentication methods to groups of users – and enforce the right method depending on their needs, security constraints and the login context.

9. Overview of Thales Authentication

Thales's SafeNet Trusted Access provides authentication and access management, including Smart SSO for SFDC products, other cloud services and on-prem apps. SafeNet Trusted Access simplifies implementation, management and governance, allowing you to meet the diverse authentication needs of your users and ensure optimal access security for all apps. Smart SSO improves security and user experience, increases productivity and decreases help desk costs.

Authentication

Offering the broadest range of authentication methods and form factors, SafeNet Trusted Access authentication solutions allow customers to address numerous use cases, assurance levels, and threat vectors with unified, centrally-managed policies—managed from one authentication backend delivered in the cloud or on-premises.

Supported authentication methods include context-based authentication combined with step-up capabilities, One Time Password (OTP), FIDO, X.509 certificate-based solutions, and OOB. All authentication methods are available in numerous form factors, including mobile authenticator app and pattern-based software authenticators, and smart card, USB security key/token hardware authenticators.

Physical Access

Thales offers a range of FIDO devices and smart cards with dual physical and logical access capabilities, including contact cards with a wide choice of card body options and contactless technologies, and interface cards compatible with NFC. Use case examples include: Building access, printing, computer log in, email encryption, and document signing. This allows users to have a single authentication device for logging into SFDC and other cloud services, and accessing physical premises and devices.

Strong Authentication for Privileged Access

SafeNet Trusted Access supports policy-based access with the ability to apply and enforce different methods of authentication and session management rules depending on the role of the user and the sensitivity of the resource. SFDC admins could be forced to use stronger authentication more frequently than a general SFDC end user.

10. Why Thales?

Thales offers the only complete portfolio of Authentication and Access Management solutions, including Cloud Access Management, FIDO, PKI, Certificate-Based Authentication (CBA), One-Time Password (OTP) authentication, identity federation, complete lifecycle management and auditing tools.

Thales also has data protection and encryption solutions that work together with our Authentication and Access Management solutions to provide persistent protection and management of sensitive data.