cpl.thalesgroup.com

THALES
Building a future we can all trust

10 cosas que hay que saber
¿Está preparado para los requisitos de SFDC MFA?

1. ¿Cuál es el nuevo requisito de Salesforce (SFDC) de MFA?

Todos los usuarios internos (cualquiera que tenga privilegios de empleado, sea o no empleado) que inicien sesión en los productos de SFDC a través de la interfaz de usuario, desde dispositivos móviles o de escritorio, deben utilizar un MFA.

2. Fecha límite para cumplir

Los requisitos de SFDC para MFA entran en vigor a partir del 1 de febrero de 2022.

3. ¿Qué ocurre si no se cumple?

Los clientes que no habiliten la MFA adecuada antes del 1 de febrero 2022 no cumplirán con sus obligaciones contractuales. SFDC recomienda que los clientes consulten con su equipo legal para entender las implicaciones.

4. ¿Qué métodos no se aceptan como MFA?

SFDC se alinea con el NIST y el consenso general en la industria de la seguridad seguridad: los métodos de autenticación más débiles no se recomiendan o o no están permitidos. SFDC no acepta los siguientes métodos para MFA:

- Correo electrónico
- Mensajes de texto SMS
- Llamadas telefónicas

5. ¿Qué opciones tiene una organización para cumplir el requisito de habilitación de MFA en SFDC?

a. Utilizar un proveedor de autenticación y SSO de terceros, como Thales SafeNet Trusted Access.

b. Utilizar el servicio de autenticación de SFDC.

6. ¿Qué debo considerar a la hora de decidir qué enfoque adoptar?

Dado que el 90% de los de seguridad comienzan con credenciales comprometidas, es posible que usted pueda ser una de las muchas organizaciones que buscan formas de implementar un MFA en todo su entorno de SaaS, no sólo para las aplicaciones de SFDC.

En el mundo empresarial actual, los usuarios tienen diversas necesidades de autenticación. Algunos usuarios tendrán una cobertura móvil inconsistente. Muchos utilizarán múltiples dispositivos. Todos necesitarán acceder de forma segura a docenas de aplicaciones.

Para mantener una seguridad óptima y garantizar una experiencia de inicio de sesión cómoda, los responsables de TI deben buscar una solución que pueda

- Cumplir las expectativas de los usuarios de poder iniciar sesión en SFDC y otras aplicaciones, sea cual sea el contexto, en cualquier dispositivo, con una experiencia MFA que se adapte a ellos
- Responder a las necesidades de los equipos de TI que tienen que dar soporte a miles de usuarios de forma remota y segura con una con una participación mínima.
- Dar soporte a múltiples unidades de negocio en todo el mundo y ofrecer una experiencia en el idioma local
- Ofrecer una pista de auditoría de todos los eventos de acceso y autenticación y seguir cumpliendo con las regulaciones.

7. ¿Cómo puede Thales ayudar a mi organización a cumplir los requisitos de SFDC?

Con su plantilla basada en un asistente para SFDC y cientos de otras aplicaciones empresariales, SafeNet Trusted Access de Thales le permite habilitar una política en un par de minutos: hacemos que sea fácil y rápido cumplir con el plazo de SFDC de febrero de 2022.

SafeNet Trusted Access permite a las organizaciones proteger las aplicaciones empresariales y escalar de forma segura en la nube con una amplia gama de capacidades de autenticación, al mismo tiempo que garantiza la seguridad con Smart SSO y controles de acceso basados en políticas.

"Habilitar una política en un par de minutos"

Thales SafeNet Trusted Access

Métodos de autenticación universal

- Implemente el acceso seguro de forma rápida y eficaz
- Evite la dependencia de un proveedor y mantenga el control de su seguridad de acceso
- Prevenga las multas y evite la responsabilidad financiera y las sanciones
- Cumplir con el presupuesto y los objetivos empresariales

a. Además de ampliar las opciones de MFA, SafeNet Trusted Access simplifica la implementación, la gestión y el gobierno.

Para los productos de SFDC, otros servicios en la nube y aplicaciones on-prem, SafeNet Trusted Access proporciona Smart Single-Sign On (Smart SSO, también conocido como "Secure SSO") - la capacidad de evaluar sin problemas cada intento de acceso y aplicar el método de autenticación adecuada para su usuario.

Smart SSO ofrece el equilibrio óptimo entre comodidad y seguridad, y ayuda a las organizaciones a lograr la confianza cero.evaluando continuamente la seguridad de los accesos e intensificando medidas de autenticación cuando el intento de acceso no coincide con lo que usted ha configurado como aceptable. A diferencia del SSO, Smart SSO elimina el escenario en el que las credenciales de un usuario pueden convertirse en un único punto de fallo.

b. Thales puede soportar todas las diversas necesidades de autenticación de sus usuarios y ayudarle a conseguir la "autenticación en todas partes" ofreciendo la mayor selección de métodos de autenticación con diferentes mecanismos y certificaciones para soportar un espectro de usuarios y entornos de trabajo. entornos de trabajo. Nuestro enfoque es:

1. La autenticación adecuada al riesgo

2. Seguridad de extremo a extremo

3. Baja fricción y experiencia superior

4. Número mínimo de métodos de autenticación/usuario

5. Registro de auditoría y certificaciones para cumplir con las regulaciones

8. ¿Cómo cumple Thales con las clasificaciones de seguridad del NIST de seguridad del NIST?

SFDC suele contener información sensible al GDPR, Información de identificación personal Identificable (PII), e información clave de la empresa y de la competencia, razones de peso para seleccionar una autenticación de mayor seguridad.

Thales ofrece métodos de autenticación para cada Nivel de aseguramiento del NIST con soluciones de software y hardware que incluyen OTP + PIN + contraseña, push móvil + biometría, dispositivos FIDO y una opción basada en patrones. Esto significa que puede desplegar múltiples métodos de autenticación para sus usuarios - o desplegar diferentes métodos de autenticación para grupos de usuarios, y aplicar el método adecuado para sus necesidades, las restricciones de seguridad y el contexto de inicio de sesión.

9. Visión general de la autenticación de Thales

SafeNet Trusted Access de Thales proporciona autenticación y gestión de acceso , incluido Smart SSO para productos SFDC, otros servicios en la nube y aplicaciones on-prem. SafeNet Trusted Access simplifica la implementación, la gestión y el gobierno,

permitiéndole satisfacer las diversas necesidades de autenticación de sus usuarios y garantizar una seguridad de acceso óptima para todas las aplicaciones. Smart SSO mejora la seguridad y la experiencia del usuario, aumenta la productividad y reduce los costos de mesa de ayuda.

Autenticación

Al ofrecer la más amplia gama de métodos de autenticación y mecanismos, las soluciones de autenticación de SafeNet Trusted Access permiten a los clientes abordar numerosos casos de uso, niveles de seguridad y vectores de amenaza con políticas unificadas y gestionadas de forma centralizada. gestionadas desde un backend de autenticación suministrado en la nube o en las instalaciones

Los métodos de autenticación soportados incluyen la autenticación basada en el contexto combinada con capacidades reforzadas, One Time Password (OTP), FIDO, soluciones basadas en certificados X.509 y (OTP), FIDO, soluciones basadas en certificados X.509 y OOB. Todos los métodos de autenticación están disponibles en numerosos mecanismos estándar, incluyendo autenticadores de software basados en patrones y aplicaciones, autenticadores de hardware de tarjeta inteligente, llave de seguridad USB y token. autenticadores de hardware.

Acceso físico

Thales ofrece una gama de dispositivos FIDO y tarjetas inteligentes con doble capacidad de acceso físico y lógico, incluyendo de contacto con una amplia gama de opciones de cuerpo de tarjeta y tecnologías sin contacto, y tarjetas de interfaz compatibles con NFC. Los casos de uso ejemplos de uso incluyen: Acceso a edificios, impresión, inicio de sesión en ordenadores, cifrado

y firma de documentos. Esto permite a los usuarios tener un único dispositivo de autenticación para iniciar sesión en SFDC y otros servicios y otros servicios en la nube, y para acceder a las instalaciones y dispositivos físicos.

Autenticación sólida para el acceso privilegiado

SafeNet Trusted Access admite el acceso basado en políticas con la capacidad de aplicar e imponer diferentes métodos de autenticación y reglas de gestión de sesiones de acuerdo a la función y la sensitividad del recurso. Los administradores de SFDC podrían verse obligados a utilizar una autenticación más fuerte con más frecuencia que un usuario final general de SFDC.

10. ¿Por qué Thales?

Thales ofrece un portafolio completo de soluciones de autenticación y gestión de acceso, incluyendo la gestión de Gestión de Acceso a la Nube, FIDO, PKI, Autenticación Basada en Certificados (CBA), autenticación por contraseña de un solo uso (OTP), federación de identidades, gestión del ciclo de vida completo y herramientas de auditoría. Thales también dispone de soluciones de protección de datos y cifrado que funcionan junto con nuestras soluciones de autenticación y gestión de acceso para proporcionar una protección y gestión persistentes de los datos sensitivos.