Multi-Factor Authentication (MFA)

Contents

Overview

Multi-Factor Authentication ("MFA") requires a user to validate their identity with two or more forms of evidence — or factors — when they log in. One factor is something the user knows, such as their username and password combination. Other factors are verification methods that the user has in their possession. While there's a risk that a password may be compromised, it's highly unlikely that a bad actor can also gain access to a strong verification method like a security key or authentication app.

See also: https://salesforce.vidyard.com/watch/Zs9r7CyxF6Wu9rfNmMnmFf

MFA Requirements

Use the **MFA Requirement Checker** to see if your current or planned implementation satisfies the MFA requirement. The general requirements are below.

If your users access Salesforce products by logging in directly

Your users must log into Salesforce by entering a username and password, and then must receive an MFA challenge, for which they must verify their identity with a supported verification method. Your users must receive an MFA challenge upon every login.

> - If a supported verification method is required only when users log in from new browsers or devices, you're using **Device Activation** or **Identity Verification** instead of MFA. That's good, but it doesn't satisfy the MFA requirement. You need to turn on MFA for your Salesforce products.
> - If users are never prompted for a verification method after they enter their username and password, you need to turn on MFA for your Salesforce products.

If your users access Salesforce products by logging into an SSO site

Your users must receive an MFA challenge when they log into your SSO site and they must verify their identity with a strong verification method.

> One-time passcodes via email, text messages, and voice calls aren't acceptable. To satisfy the MFA requirement, consider these options:
>
> - Talk to your SSO provider about using their MFA service.
> - Integrate a Continuous Adaptive Risk and Trust Assessment (CARTA) or risk-based authentication system with your SSO solution.
> - For products built on the Salesforce Platform, you can use the free MFA functionality provided in Salesforce instead of enabling MFA at the SSO level. See Use Salesforce MFA for SSO Logins in Salesforce Help for details.

Enforcement Timeline

Effective 01 Feb 2022, per the Salesforce Trust and Compliance Documentation, all Salesforce customers are contractually required to use MFA to access Salesforce products. To help customers who haven't satisfied the requirement, MFA will be **automatically enabled** for users who log in directly to Salesforce products. Administrators will still have the option to disable MFA if their users aren't ready yet. In addition, MFA will be gradually **enforced** by making it a permanent part of the direct login process and removing controls for administrators to disable it. Auto-enablement and enforcement dates vary by product.

For each of your Salesforce products, you'll receive notice before auto-enablement goes into effect -- with a minimum of six months notice before MFA is enforced. Notices will be published in standard release notification channels.

Dates in this table apply to all users unless otherwise noted. Confirmed dates are bold and underlined. This table is accurate as of 12 Jan 2023.

Product	Projected MFA Auto-Enablement Date	Projected MFA Enforcement Date	Notifications and Details
Products built on the Salesforce Platform	Between January and June 2023	September 2023	Article Release Note Email Notification
B2C Commerce Cloud	Enforcement is in effect (as of May, 2022)		Email Notification Release Note
ClickSoftware— Field Service Edge (FSE)	Enforcement is in effect (as of June, 2022)		Email Notification
ClickSoftware— Service Optimization V8 Cloud	Enforcement is in effect (as of June, 2022)		Email Notification
Heroku	Both will occur at the same time **between January 9 - 31, 2023**		Email Notification
Marketing Cloud Engagement (powered by Email, Messaging, and Journeys)	Enforcement is in effect (as of June, 2022)		Email Notification Release Note
Marketing Cloud Intelligence (powered by Datorama)	Enforcement is in effect (as of October, 2022)		Email Notification
Marketing Cloud Social	Privileged Users: **Between May 9 - 13, 2022** All Users: **August 9, 2022**	All Users: **November 30, 2022**	Email Notification Release Note
MuleSoft Anypoint Platform	New Users: **July 23, 2022** All Users: **October 29, 2022**	Second half of 2023	Email Notification Article
Quip products	Enforcement is in effect (as of May 1, 2022)		Email Notification
Tableau Online	Both will occur at the same time. Privileged Users: **Between March 13 - 17, 2023** All Users: **Between April 17 - 21, 2023**		Email Notification

See also: Multi-Factor Authentication (MFA) Enforcement Roadmap

Verification Methods for Direct Logins

Salesforce offers simple, innovative MFA solutions that provide a balance between strong security and user convenience. Salesforce products support several types of strong verification methods to satisfy your business and user requirements.

- **Salesforce Authenticator Mobile App:** A fast, frictionless solution that makes MFA verification easy via simple push notifications that integrate into your Salesforce login process. Use this app in your MFA implementation to increase security while driving a better user experience.
- **Third-Party Authenticator Apps:** Authenticate with apps that generate temporary codes based on the OATH time-based one-time password (TOTP) algorithm. There are many apps available, including Google Authenticator[TM], Microsoft Authenticator[TM], and Authy[TM].
- **Security Keys:** These small physical devices are easy to use because there's nothing to install and no codes to enter. Security keys are a great solution if mobile devices aren't an option for your users. Salesforce supports USB, Lightning, and NFC keys that support the WebAuthn or U2F standards, including Yubico's YubiKey[TM] and Google's Titan[TM] Security Key.
- **Built-In Authenticators:** Easy MFA verification using a desktop or mobile device's built-in authenticator service, such as Windows Hello[TM], Touch ID[R], or Face ID[R].

See also: Verification Methods for Multi-Factor Authentication

MFA for Single Sign-On (SSO)

On its own, a single sign-on (SSO) solution doesn't satisfy the MFA requirement. If your Salesforce products are integrated with SSO, make sure MFA is enabled for all your Salesforce users. For help, check out these answers to common questions about SSO and the MFA requirement. For full details about the requirement, see the complete MFA FAQ.

See also: SSO and the MFA Requirement

Enable MFA

Follow the steps in [Enable MFA for Users](#) to enable MFA for your users.

> The steps for enabling MFA are determined by your Salesforce product.

When MFA is turned on for a user, they must have a registered verification method to access Salesforce. If a user didn't self-register a method before your launch day, on-screen prompts guide them through the process the next time they log in. For all subsequent logins, users are required to supply the method in addition to their username and password.

See also:

- [Connect Your Salesforce Account to Salesforce Authenticator](#). *Salesforce Help.*
- [Set up a YubiKey for Salesforce Logins](#). *Yubico.*

See also

- [API Login with Multi-Factor Authentication](#)

- [https://security.salesforce.com/mfa](#). *Salesforce Security Documentation.*
- [Admin Guide to Multi-Factor Authentication](#). *Salesforce Documentation.*
- [Salesforce Multi-Factor Authentication FAQ](#). *Salesforce Help.*