For products built on the Salesforce Platform

Admin Guide to Multi-Factor Authentication

Get ready for MFA from Salesforce and roll it out to your Salesforce users

Table of Contents

Version 2023.07

1 The Time for Multi-Factor Authentication is Now!

See how MFA is an effective way to safeguard access to Salesforce accounts

What Is MFA and Why Is It Important?

As the security landscape evolves and threats that compromise user credentials grow more common, it's important to implement strong security measures to protect your business and customers.

Usernames and passwords alone don't provide sufficient safeguards against unauthorized account access. **Multi-factor authentication (MFA)** adds an extra layer of protection against threats like phishing attacks, credential stuffing, and account takeovers.

Multi-factor authentication is one of the easiest, most effective ways to help prevent unauthorized account access and safeguard your Salesforce data.

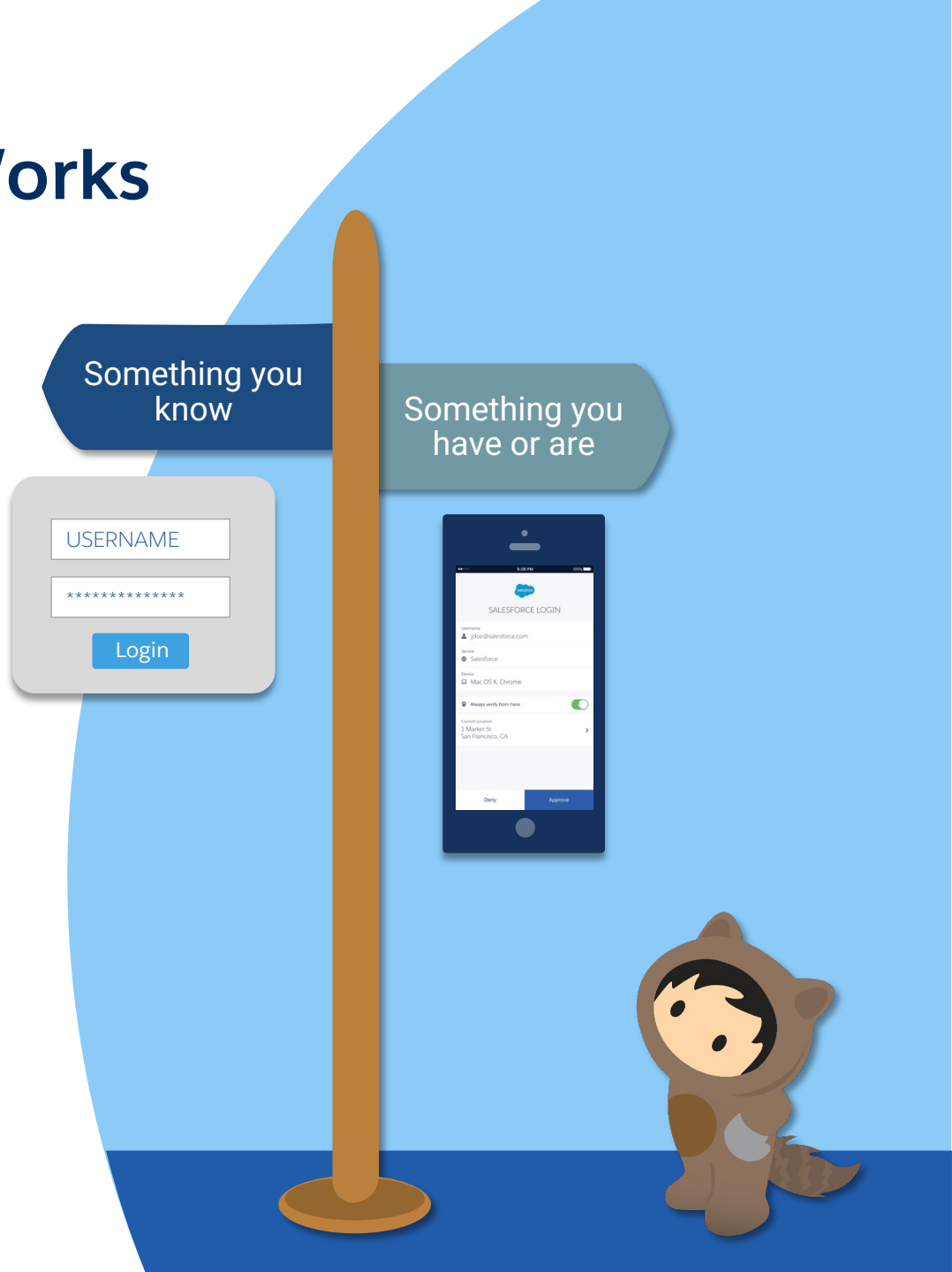
MFA from Salesforce is available at no extra cost!

How Multi-Factor Authentication Works

MFA requires users to prove they're who they say they are by providing two or more pieces 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 (such as an authenticator app or security key) or that the user is (such as biometrics).

By tying user access to multiple, different types of factors, it's much harder for a bad actor to gain entry to your Salesforce environment. Even if a user's password is stolen, the odds are very low that an attacker can guess or impersonate a factor that a user physically possesses.



MFA from Salesforce

Salesforce products include free, effective MFA services for direct logins to your Salesforce environments. MFA from Salesforce strikes a balance between strong security and user convenience.

Because your business requirements and users' needs are diverse, you can pick and choose between different types of verification methods, including mobile apps and hardware devices.

And to help manage your MFA implementation, we provide a variety of tools and resources, including:

- Reports and dashboards for monitoring usage
- Temporary verification codes that give users access if they've lost or forgotten their verification method

Use this guide to set up MFA for products built on the Salesforce Platform, including:

- Sales Cloud
- Service Cloud
- Analytics Cloud
- B2B Commerce
- Experience Cloud
- Industries products (Consumer Goods Cloud, Education Cloud, Financial Services Cloud, Government Cloud, Health Cloud, Manufacturing Cloud, Nonprofit Cloud, Philanthropy Cloud)
- Marketing Cloud Account Engagement
- Marketing Cloud Audience Studio
- Platform
- Salesforce Essentials
- Salesforce Field Service
- Partner solutions

MFA is available in Salesforce Classic and Lightning Experience

MFA is available in all Editions

MFA Verification Methods for Salesforce

MFA adds an extra authentication step to your Salesforce login process.

1. The user enters their username and password, as usual.
2. Then the user is prompted to provide a verification method.

Salesforce requires strong verification methods that provide high assurance users are who they say they are. You can allow any or all of these methods.

Email, SMS text messages, and phone calls aren't allowed as MFA verification methods because email credentials are more easily compromised, and text messages and phone calls can be intercepted.

It's a lot harder for bad actors to get control of an actual mobile device or physical security key than it is to infiltrate an email account or hack a cell phone number.

Salesforce Authenticator App

Fast, free authentication

Third-Party TOTP Authenticator Apps

Such as:
Google Authenticator
Microsoft Authenticator
Authy

Security Keys

Such as:
Yubico's YubiKey
Google's Titan Security Key

Built-In Authenticators

Desktop + mobile device biometrics, such as:
Windows Hello
Touch ID
Face ID

Salesforce Authenticator: Fast, Free, Frictionless MFA

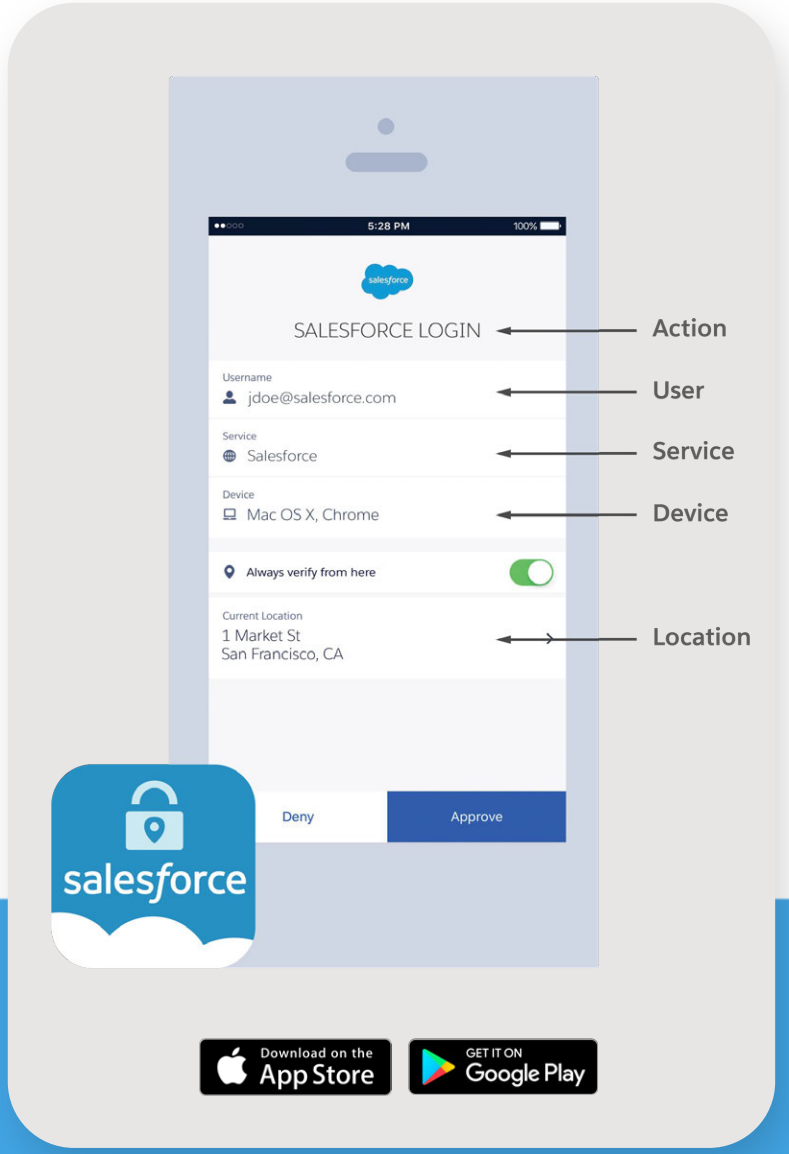
The Salesforce Authenticator mobile app makes MFA easy by integrating into your login process. It's simple for users to install and connect to their Salesforce accounts.

When a user logs in, they get a push notification on their mobile device. The user taps the notification to open Salesforce Authenticator and sees the following information:

- The **action** that needs to be approved
- Which **user** is requesting the action
- Which **service** is requesting the action
- What **device** the user is using
- The **location** from which the request is coming

With this information, the user can quickly and confidently approve or deny the authorization request. They can also automate the extra authentication step when working from a trusted location.

If the user's mobile device doesn't have connectivity, they can still log in using six-digit TOTP codes generated by Salesforce Authenticator.



Third-Party Authenticator Apps

Salesforce supports the use of third-party authenticator apps that generate temporary codes based on the OATH time-based one-time password (TOTP) algorithm (RFC 6238).

To log in using this type of verification method, the user gets a code from a TOTP authenticator app, then enters that code during the Salesforce login process.

Behind the Scenes

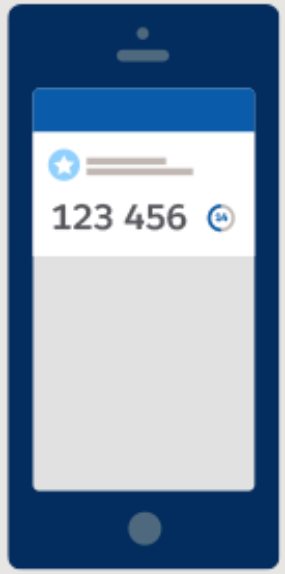
TOTP authenticator apps generate temporary codes on the basis of a secret key (known only to the user and the service, such as Salesforce) and the current time. A code is valid for 30 seconds and then a new one is generated.

TOTP authenticator apps can generate codes even if the user's phone doesn't have a data or internet connection.

➤ **TIP:** If users have already installed a TOTP app for personal or business use, they can set up the same app for Salesforce logins.

There are many apps available, including free versions. Options include:

- Google Authenticator
- Microsoft Authenticator
- Authy



Security Keys

Security keys are small physical devices that are easy to use because there's nothing to install and no codes to enter. This is a great option if users don't have a mobile device or if cell phones aren't allowed on the premises.

Security keys make MFA logins fast. A user simply:

1. Connects their key to the computer
2. Presses the key's button to verify their identity

Behind the Scenes

Salesforce supports security keys that are compatible with WebAuthn (FIDO2) and FIDO U2F. These standards use strong public-key cryptography to protect users from man-in-the-middle attacks and malware. To learn more about what's happening behind the scenes with security keys, check out the WebAuthn or FIDO U2F sites.

Security keys require a supported browser to act as an intermediary between the key and Salesforce.

Security key options include Yubico's YubiKey and Google's Titan Security Key

Supported form factors:

USB-A, USB-C, Lightning

Supported browsers for WebAuthn keys:

Chrome, Edge Chromium, Firefox, Safari

Supported browsers for U2F keys:

Chrome, version 41 or later; Edge Chromium

Built-In Authenticators

Built-in authenticators verify a user's identity using a device's biometric reader, such as a fingerprint, iris, or facial recognition scanner. Or in some cases, built-in authenticators confirm a user via a PIN or password that the user sets up with their device's operating system.

Logging in with this type of method is easy. A user:

1. Enters their username and password.
2. Uses their built-in authenticator to provide a pre-configured biometric identifier, PIN, or password.

Important: This type of method is tied to a user's device. If a user logs in from multiple computers, they need to register a built-in authenticator on each system, or also register an alternate verification method.

Behind the Scenes

Built-in authenticator support is based on the FIDO2 and WebAuthn specifications. Registering a built-in authenticator creates a pair of private and public keys that are unique to the user's account.

Built-in authenticators include:

- Windows Hello
- Face ID
- Touch ID

Requirements:

- User's device, OS, and browser must support the FIDO2 WebAuthn standard.
- The built-in authenticator service must be enabled and set up ahead of time to verify a user's identity.
- For biometric authentication, the user's device must include a supported fingerprint, iris, or facial scanner.
- Works only for logins to the device where the built-in authenticator exists.
- Not supported for MFA verification in the Salesforce Mobile app.

Choose Verification Methods for Your Implementation

	Salesforce Authenticator	Third-Party Authenticator Apps	Security Keys	Built-In Authenticators (*Beta*)
Description	A smart and simple mobile app that users can easily connect to their Salesforce accounts.	Apps generate unique, temporary verification codes based on the OATH TOTP algorithm.	Physical devices that use public-key cryptography.	Verify identity with fingerprint, iris, or facial recognition scan, or a PIN or password.
Form Factor	Mobile app for iOS and Android	Apps available for multiple operating systems	USB and Lightning devices that support the WebAuthn (FIDO 2) or U2F (FIDO) standards	Available via a device's built-in authenticator service (Windows Hello, Touch ID, Face ID, and so forth)
User Experience	• Delivers push notifications to users' phones for fast access • See real-time details to confirm request validity • Deny fraudulent requests with a tap • Automates authentication from trusted locations • Generates TOTP codes if connectivity isn't available	• Wide variety of apps to choose from • Connectivity isn't required	• Fast and easy to use • Recognizes and denies fraudulent requests • Connectivity isn't required • No batteries needed	• Fast and easy to use • No apps required • Strong public-key cryptography that's unique to the user's account
Considerations	• Requires a mobile device	• Requires a mobile device • Typing errors possible when manually entering codes • Invalid codes possible if mobile device clock gets out of sync with Salesforce	• Requires browser support • Key may be left unattended or plugged in all the time • Operational overhead for purchasing, stocking, and distributing devices to users	• Device, OS, and browser must support FIDO2 WebAuthn standard • Built-in authenticator service must be enabled and set up • Tied to the user's device • Supported scanner required for biometric identification
Cost	Free	Free and paid options	Starts around $20	$25 and up for biometric peripherals, if needed

2 The Salesforce MFA Requirement

Understand how the Salesforce initiative requiring MFA affects you

What is the Salesforce MFA Requirement?

It's a **contractual requirement** that's covered in the Notice and License Information (or NLI) section of the **Salesforce Trust and Compliance Documentation**.

For full details about the MFA requirement and how to satisfy it, see the **Salesforce MFA FAQ**.

The number of cyberattacks targeting businesses, including Salesforce customers, is on the rise. To protect against these types of threats, we believe it's important to adopt MFA as soon as possible. That's why...

Effective February 1, 2022, Salesforce requires all customers to use MFA when accessing Salesforce products

How Salesforce is Enforcing the MFA Requirement

To help customers satisfy the contractual requirement to use MFA, Salesforce will:

Auto-Enable MFA for Direct Logins

What to expect:

- Salesforce turns on MFA on a customer's behalf.
- Users must use MFA to log in (after a 30-day grace period).
- Login process prompts users to register for MFA.
- Users already using MFA aren't affected.
- If auto-enablement occurs before a product's enforcement date, admins can disable MFA.

Enforce MFA for Direct Logins

What to expect:

- MFA becomes a permanent part of the login experience – users must verify their identity each time they log in.
- Non-MFA users are auto-enabled for direct logins.
- Users already using MFA aren't affected.
- Customer admins and users can't disable MFA.

Check out the **MFA Enforcement Roadmap** to keep track of the auto-enablement and enforcement schedule for your Salesforce orgs.

Using SSO? Salesforce won't take action to enable MFA for your SSO identity provider. But the contractual requirement applies when accessing Salesforce products via SSO.

3 Implement MFA from Salesforce

Get ready for MFA, then roll it out to your users

The Recommended Path to MFA

Get Ready

Evaluate which verification methods meet your business and user requirements.

Inventory users, roles, and permissions to identify your privileged users (they're your top priority) and to determine the level of effort for your project.

Plan rollout, change management, implementation, testing, and user support strategies.

Roll Out

Kick off change management activities to engage and prepare users for MFA.

Work with your support team to establish an access recovery process and train them to handle MFA issues.

Distribute verification methods to users.

Waive MFA for valid exempt use cases.

Enable MFA for user interface logins.

Help users register and log in with a verification method.

Manage

Collect feedback and monitor usage metrics to ensure users are adopting MFA.

Support ongoing operations and assist users with authentication issues.

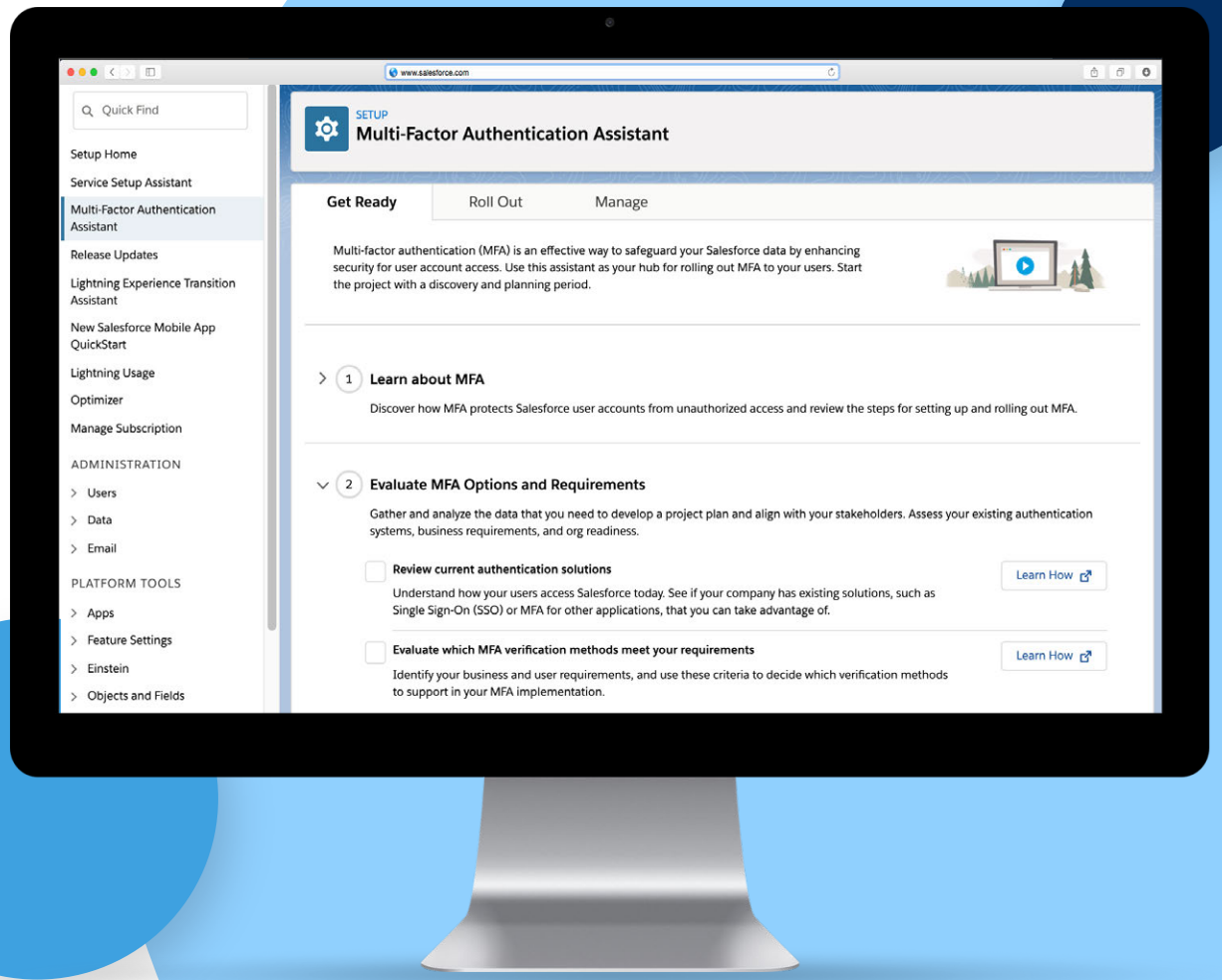
Optimize your overall security strategy.

Get It Done with the Multi-Factor Authentication Assistant

The Multi-Factor Authentication Assistant is your one-stop shop for delivering MFA to your users. It walks you through the recommended path for rolling out MFA.

- Get step-by-step guidance, with tools and resources to help you take action.
- Steps are presented in checklists so you can track completed tasks and overall progress.

Access the Assistant from Setup in Lightning Experience by selecting **Multi-Factor Authentication Assistant**.



Plan Your Rollout

To ensure a successful rollout, cover these criteria in your project plan.

Rollout Strategy

- Decide if you'll roll out MFA to everyone at the same time or go live in phases to different groups over time.
- If you do a phased rollout, admins and other privileged users are your top priority.

➤ **TIP**: We recommend starting with a pilot group to test the rollout process and fine-tune things.

Change Management

- Communicate upcoming changes to users.
- Build awareness and get user buy-in with campaigns and promotional materials.
- Train users on MFA concepts and how to obtain, register, and use verification methods to log in with MFA.
- Create registration and troubleshooting materials for your launch day.

Support Team

- Establish policies and processes for ongoing operations, including helping users with lost or forgotten verification methods.
- Train your support team on setup, troubleshooting, and access recovery steps.
- Update your employee onboarding procedures so new hires get MFA from the start.

Make Your Rollout a Success with Change Management

To help jump-start your multi-factor authentication (MFA) project, we provide a Rollout Pack that's brimming with change management guidance and customizable templates. Use the pack to plan your MFA implementation and prepare your users.

Download the Rollout Pack

What's in the Rollout Pack

Stakeholder presentation: make the case and get aligned.

User inventory templates: audit users' permissions to see who should get MFA first.

Change management guidance and templates: develop a strategy to prepare your users.

Sample drip email campaign: let users know MFA is coming.

User training deck: demo how MFA works and how it affects the login process.

User onboarding templates: create resources that help users register and log in with MFA.

Also: resources for planning your rollout, including a checklist to keep you on track, a project schedule template, and a simple test plan template.

When You’re Ready to Go Live

When you turn on MFA, each user is responsible for setting up their own verification methods. Here’s the recommended approach for your launch.

Admin

Kick things off by distributing verification methods to users, along with instructions for the registration process. Encourage users to register at least one method ahead of time so they avoid delays logging in after MFA is live.

Then turn on MFA for user interface logins.

Users

Each user must register a verification method to connect it to their Salesforce account. Users are automatically invited to do so the next time they log in (unless they registered a method before MFA was enabled).

For all subsequent logins, users are required to supply the method in addition to their username and password.

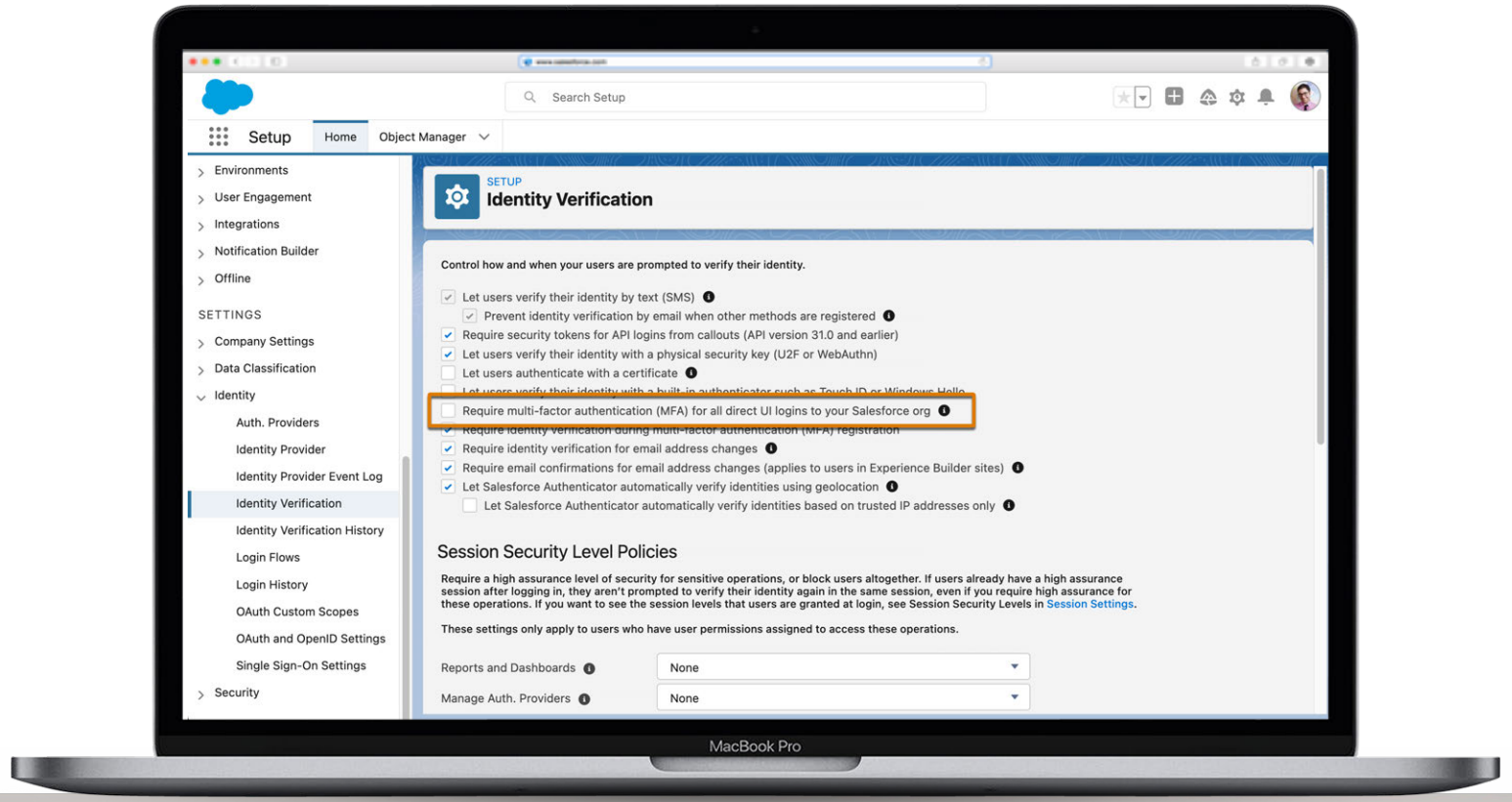
Enable MFA

1. Enable security keys or built-in authenticators if you want to allow the use of these types of verification methods.
2. Waive MFA for exempt user types. See Exclude Exempt Users from MFA in Salesforce Help for guidance.
3. Decide how you want to enable MFA.
    - **Turn it on for all users in your org**: See the next page for the steps.
    - **Roll it out to groups of users in phases**: Assign the **Multi-Factor Authentication for User Interface Logins** user permission. See Enable MFA for Specific Users in Salesforce Help for more information.

Turn on MFA for Your Entire Org

Quickly enable MFA for all your users at the same time.

1. From Setup, enter `Identity` in the Quick Find box, then select **Identity Verification**.
2. Select **Require multi-factor authentication (MFA) for all direct UI logins to your Salesforce org**, and then select **Save**.



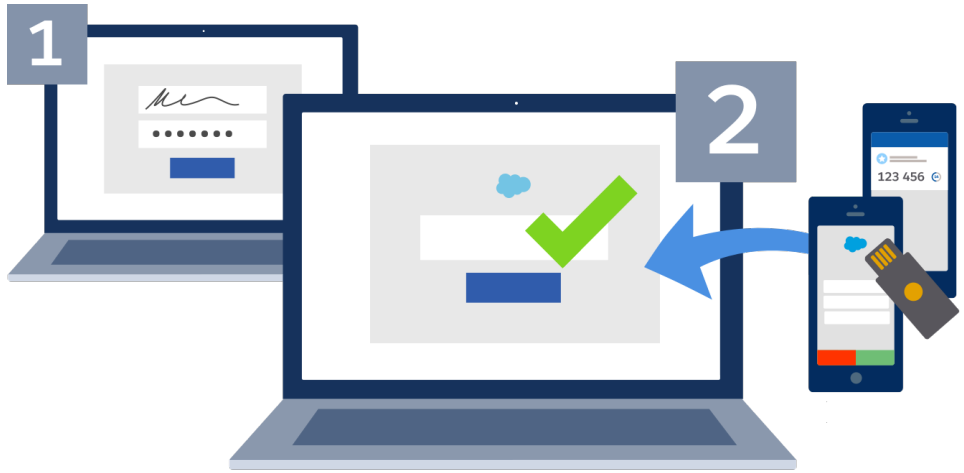
Considerations:

- This step requires the "Customize Application" user permission.
- If you have user types that are excluded from the MFA requirement, there may be an extra step to complete before turning on MFA. See Exclude Exempt Users from MFA in Salesforce Help for guidance.

The User Experience When MFA is Live

When MFA is enabled for user interface logins, each user must have at least one registered verification method before they can log in to Salesforce. The registration process connects a method to the user's Salesforce account.

Users can register methods at any time. If a user doesn't have a method ready by the time MFA is enabled, they're automatically prompted to register one the next time they log in. On-screen prompts guide users through the process.



Registration and login steps vary a little for each verification method. Let's take a closer look.

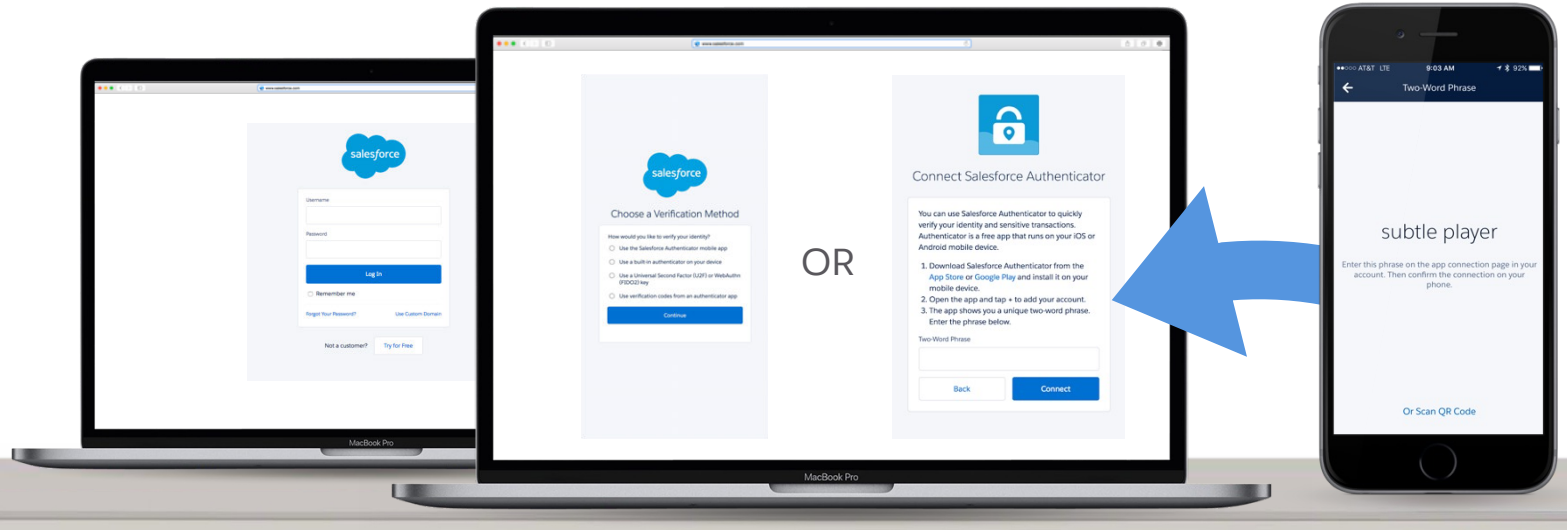
- Salesforce Authenticator
- Third-Party Authenticator Apps
- Security Keys
- Built-In Authenticators

Salesforce Authenticator: How Users Register and Log In

To register and connect the app:

1. On a mobile device, download and install the app from the Apple Store or Google Play.
2. On your Salesforce product's login screen, enter a username and password.
3. Select the Salesforce Authenticator option from the list. If you see the Salesforce Authenticator screen by default, skip to step 4.
4. Open Salesforce Authenticator and tap **Add an Account**. The app displays a two-word phrase.
5. On the Connect Salesforce Authenticator screen, enter the phrase in the **Two-Word phrase** field, then click **Connect**.
6. In Salesforce Authenticator, verify that the request details are correct, then tap **Connect**.

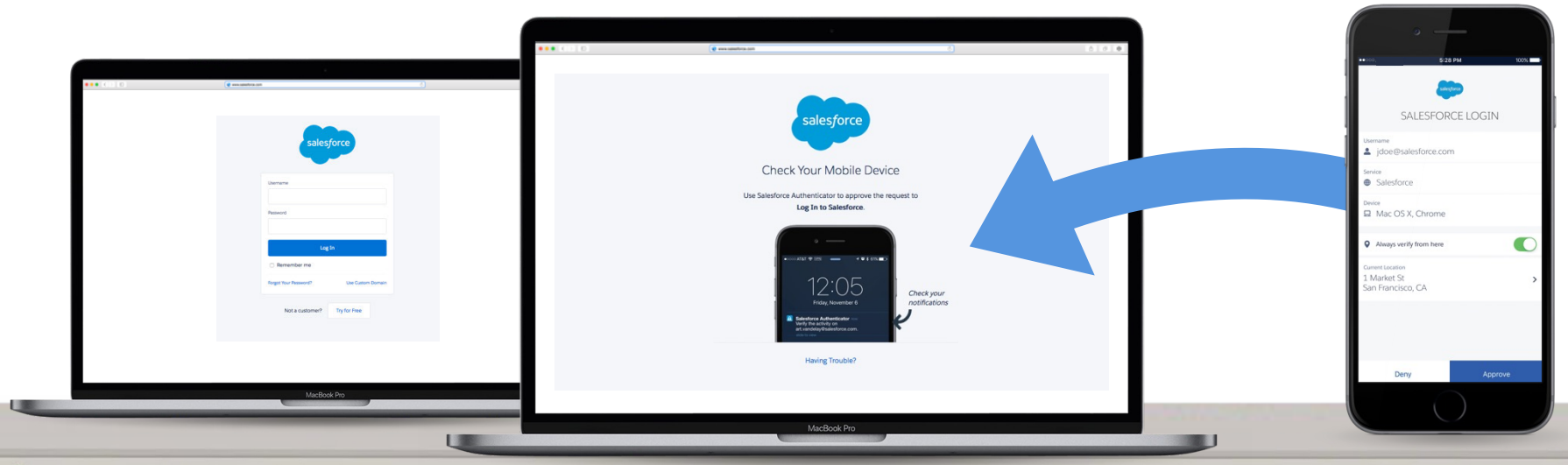
➤ **TIP**: Alternatively, users can get a head start by registering Salesforce Authenticator directly from their profile. See Connect Your Salesforce Account to Salesforce Authenticator in Salesforce Help.



Salesforce Authenticator: How Users Register and Log In *continued*

To log in using the app:

1. On the Salesforce login screen, enter a username and password, as usual.
2. On the mobile device, respond to the push notification to open Salesforce Authenticator.
3. In Salesforce Authenticator, verify that the request details are correct, then tap **Approve** to finish logging in to Salesforce.



Third-Party Authenticator Apps: How Users Register and Log In

To register and connect a TOTP authenticator app:

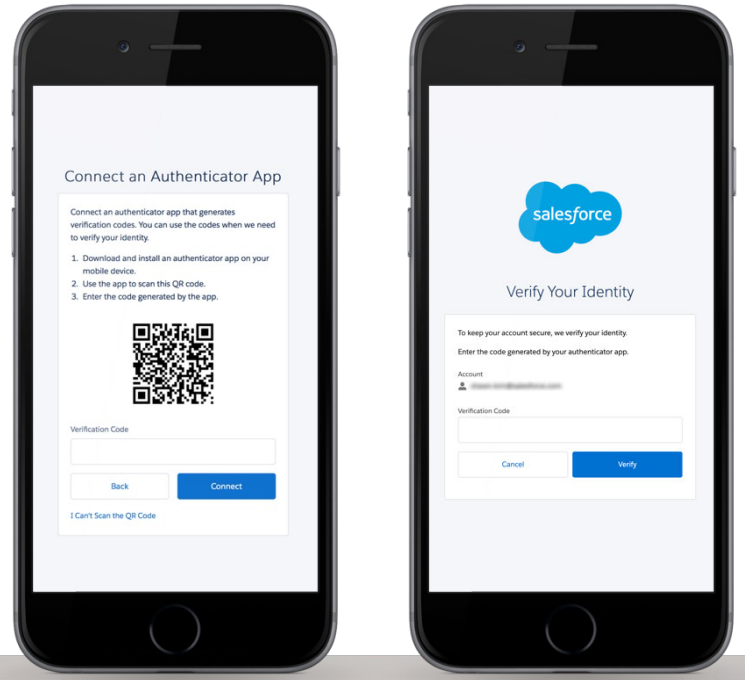
1. On a mobile device, download and install an authenticator app.
2. On the Salesforce login screen, enter a username and password.
3. In the list of verification methods, select **Use verification codes from an authenticator app**. If you see the Connect Salesforce Authenticator screen by default, first select **Choose Another Verification Method** in the bottom left corner of the screen.
4. Open the authenticator app and follow any in-app instructions for adding a new account.
5. Use the authenticator app to scan the QR barcode that's displayed on the Connect an Authenticator App screen.

   If scanning the QR barcode isn't an option, select to manually generate your security key. Then enter it in the TOTP app.
6. On the Connect an Authenticator App screen, enter the code generated by the authenticator app in the **Verification Code** field, then click **Connect** to log in.

➤ **TIP**: Alternatively, users can get a head start by registering an authenticator app directly from their profile. See Verify Your Identity with a TOTP Authenticator App in Salesforce Help.

To log in using a TOTP authenticator app:

1. On the Salesforce login screen, enter a username and password, as usual.
2. Open the authenticator app.
3. On the Verify Your Identity screen, enter the code generated by the authenticator app in the **Verification Code** field, then click **Verify** to finish logging in to Salesforce.



Security Keys: How Users Register and Log In

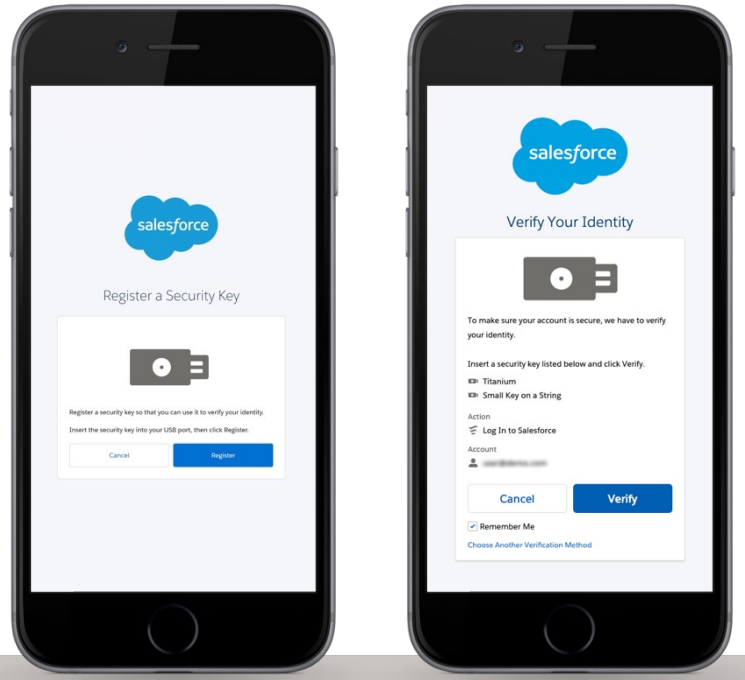
To register and connect a security key:

1. In a supported browser, go to the Salesforce login screen and enter a username and password.
2. In the list of verification methods, select **Use a Universal Second Factor (U2F) or WebAuthn (FIDO2) key**. If you see the Connect Salesforce Authenticator screen by default, first select **Choose Another Verification Method** in the bottom left corner of the screen.
3. Connect the security key to the computer, then click **Register**.
4. When prompted by the browser, press the button on the security key to finish logging in.

➤ **TIP**: Alternatively, users can get a head start by registering an authenticator app directly from their profile. See Register a U2F or WebAuthn Security Key for Identity Verification in Salesforce Help.

To log in using an app:

1. In a supported browser, go to the Salesforce login screen and enter a username and password, as usual.
2. When the Verify Your Identity screen displays, connect the security key, then click **Verify**.
3. When prompted by the browser, press the button on the security key to finish logging in.



* An admin must enable security keys before users can select this option for MFA.

Built-In Authenticators: How Users Register and Log In

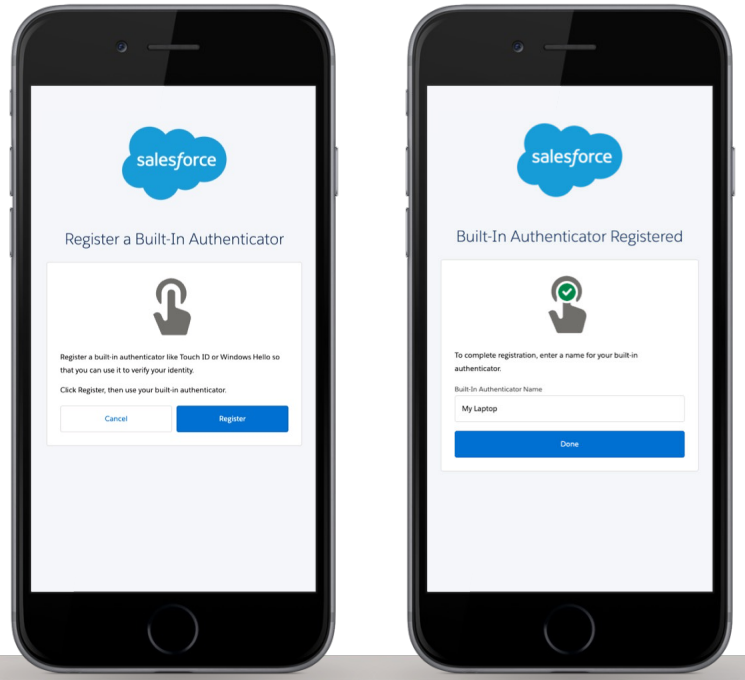
To register and connect a built-in authenticator:

1. In a supported browser, go to your Salesforce product's login screen and enter a username and password.
2. In the list of verification methods, select **Use a built-in authenticator on your device**. If you see the Connect Salesforce Authenticator screen by default, first select **Choose Another Verification Method** in the bottom left corner of the screen.
3. Click **Register**.
4. When prompted, enter the identifier for the built-in authenticator, such as a fingerprint, facial scan, or PIN, to finish logging in.

➤ **TIP**: Alternatively, users can get a head start by registering an authenticator app directly from their profile. See Register a Built-In Authenticator for Identity Verification in Salesforce Help.

To log in using a built-in authenticator:

1. In a supported browser, go to your Salesforce product's login screen and enter a username and password, as usual.
2. On the identity verification screen, click **Verify**.
3. When prompted enter the identifier for the built-in authenticator, such as a fingerprint, facial scan, or PIN, to finish logging in.



* An admin must enable built-in authenticators before users can select this option for MFA.

4 Ensure Successful Adoption of MFA

Manage your users' experience with MFA

Measure the Success of Your Rollout

Don’t just set it and forget it! Keep an eye on things to ensure your users are adopting MFA and getting the support they need. Salesforce has built-in tools to help.

Collect and evaluate user feedback

- Check in with users periodically to understand how they feel about the new MFA login requirement and see if there are any pain points that you can address.
- To gather feedback, you can conduct polls in Slack or Chatter, use a survey app, or schedule focus group sessions.

Monitor MFA usage

- Review help desk tickets and logs to see if there are recurring problems with registering verification methods or logging in.
- Track adoption over time and analyze usage patterns, including changes to the volume of daily or monthly Salesforce logins and who’s using which methods.
- Use these tools to get usage data and insights:
  - Login Metrics tab in the Lightning Usage App
  - MFA Dashboard app from AppExchange
  - Identity Verification Methods report or custom list views

Support Users and Ongoing Operations

Work with your support team to handle operational issues and the day-to-day needs of your users.

- Troubleshoot and resolve login and authentication problems, including account lockouts.
- Help users recover access if they've lost or forgotten their verification methods.
- Enable MFA for new employees as part of your new hire onboarding process.
- Stock and distribute security keys, if you're supporting this type of verification method.

Arm Your Support Team to Help with MFA Issues

Assign the **Manage Multi-Factor Authentication in User Interface** permission to your support team. With this permission, support staff can assist users with tasks such as generating temporary verification codes, disconnecting verification methods, and monitoring and reporting on identity verification activity. See Delegate Multi-Factor Authentication Management Tasks in Salesforce Help for more details.

Recover Access With Temporary Verification Codes

Generate temporary codes for users who don't have their usual MFA verification methods. You set when the code expires, from 1 to 24 hours after you generate it. The code can be used multiple times until it expires. See Generate a Temporary Verification Code in Salesforce Help.

5 Learn More

Be an MFA Trailblazer – Check out these additional resources

Additional Resources

Get More Info About the MFA Requirement

- How MFA Works to Protect Account Access (*video*)
- Everything You Need to Know About MFA Auto-Enablement and Enforcement
- Salesforce MFA FAQ
- MFA Enforcement Roadmap
- MFA Requirement Checker

Get More Help Implementing MFA

- Launch Multi-Factor Authentication (*video*)
- Get Ready for MFA Blog Series: prepare users and user access recovery tips
- Introduction to Salesforce Authenticator (*video*)
- Multi-Factor Authentication (*help*)
- MFA Glossary of Terms

Learn About MFA with Trailhead


Quick Start: Turn On MFA


User Authentication


Identity Basics

Expert Coaching

Getting Started: Platform: Multi-Factor Authentication

Get Even More Good Stuff

- Salesforce MFA Customer Site – the latest information and all MFA resources
- MFA Rollout Pack – change management guidance and templates
- How to Roll Out Multi-Factor Authentication (help) – detailed guidance and best practices

Join the MFA discussion in the MFA – Getting Started Trailblazer Community!