Admin Guide to Multi-Factor Authentication

Get ready for MFA and rolling it out to Salesforce users
# Table of Contents

## Chapter 1
**The Time for Multi-Factor Authentication is Now!**

4 What Is MFA and Why Is It Important?

5 How Multi-Factor Authentication Works

6 MFA for Salesforce

7 MFA Verification Methods for Salesforce

8 ➢ Salesforce Authenticator

9 ➢ Third-Party Authenticator Apps

10 ➢ Security Keys

11 Choose Verification Methods for Your Implementation

## Chapter 2
**Implement MFA for Salesforce**

13 The Recommended Path to MFA

14 Get It Done with the Multi-Factor Authentication Assistant

15 Plan Your Rollout

16 When You’re Ready to Go Live

17 ➢ Enable MFA for Your Users

18 ➢ Create an MFA Permission Set

19 ➢ Assign the Permission Set to Users

20 The User Experience When MFA is Live

21 ➢ Salesforce Authenticator: How Users Register and Log In

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

24 ➢ Security Keys: How Users Register and Log In

## Chapter 3
**Ensure Successful Adoption of MFA**

26 Measure the Success of Your Rollout

27 Support Users and Ongoing Operations

## Chapter 4
**Learn More**

29 Additional Resources
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 for 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.

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 for Salesforce

Salesforce offers simple, innovative MFA solutions that provide 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, Financial Services Cloud, Government Cloud, Health Cloud, Manufacturing Cloud, Philanthropy Cloud)
• Marketing Cloud – Audience Studio
• Marketing Cloud – Pardot
• Platform
• Salesforce Essentials
• Salesforce Field Service

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 users to provide a verification method that’s in their possession. You can allow any or all of these methods.

- **Salesforce Authenticator App**
  - Fast, free authentication

- **Third-Party TOTP Authenticator App**
  - Such as: Google Authenticator, Microsoft Authenticator, Authy

- **U2F Security Key**
  - Such as: Yubico’s YubiKey, Google’s Titan Security Key

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: 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 FIDO U2F. This standard uses 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 FIDO U2F site.

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 U2F keys:
Chrome, version 41 or later
Chose Verification Methods for Your Implementation

<table>
<thead>
<tr>
<th>Salesforce Authenticator</th>
<th>Third-Party Authenticator Apps</th>
<th>Security Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apps generate unique, temporary verification codes based on the OATH TOTP algorithm.</td>
<td>Physical device that uses public-key cryptography.</td>
<td></td>
</tr>
<tr>
<td>Mobile app for iOS and Android</td>
<td>Apps available for multiple operating systems</td>
<td>USB and Lightning devices that support the FIDO U2F standard</td>
</tr>
<tr>
<td>• Delivers push notifications to users’ phones for fast access</td>
<td>• Wide variety of apps to choose from</td>
<td>• Fast and easy to use</td>
</tr>
<tr>
<td>• See real-time details to confirm request validity</td>
<td>• Connectivity isn’t required</td>
<td>• Recognizes and denies fraudulent requests</td>
</tr>
<tr>
<td>• Automate authentication from trusted locations</td>
<td>• Generates TOTP codes if connectivity isn’t available</td>
<td>• Connectivity isn’t required</td>
</tr>
<tr>
<td>• Deny fraudulent requests with a tap</td>
<td>• No batteries needed</td>
<td>• Requires browser support</td>
</tr>
<tr>
<td>• Generates TOTP codes if connectivity isn’t available</td>
<td></td>
<td>• Users could leave key unattended or plugged in all the time</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Considerations</th>
<th>Considerations</th>
<th>Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Requires a mobile device</td>
<td>• Requires a mobile device</td>
<td>• Requires browser support</td>
</tr>
<tr>
<td>• Typing errors possible when manually entering codes</td>
<td>• Typing errors possible when manually entering codes</td>
<td>• Users could leave key unattended or plugged in all the time</td>
</tr>
<tr>
<td>• Invalid codes possible if mobile device clock gets out of sync with Salesforce</td>
<td>• Invalid codes possible if mobile device clock gets out of sync with Salesforce</td>
<td>• Operational overhead for purchasing, stocking, and distributing devices to users</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cost</th>
<th>Cost</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free</td>
<td>Free and paid options</td>
<td>Starts around $20</td>
</tr>
</tbody>
</table>
2 Implement MFA for 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.

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
Your one-stop shop for delivering MFA to your users

The Assistant walks you through the recommended path to 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:
• Click Multi-Factor Authentication Assistant in the Setup menu.
Plan Your Rollout

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

**Rollout Strategy**
- Determine who is required to use MFA. Admins and other privileged users are your top priority.
- Decide if you’ll roll out MFA to everyone at the same time, or go live in phases to different groups over time.

➤ **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.
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.

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 by enabling it for everyone or just the desired 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 for Your Users

Turning on MFA for user interface logins is a simple process.

1. If you’re using security keys, enable this option for your org.

2. Assign the Multi-Factor Authentication for User Interface Logins user permission via a permission set or directly in custom profiles.

Let’s take a closer look at how to use a permission set to enable MFA for specific people.

➤ TIP: We recommend distributing verification methods before you enable MFA so users can get a head start registering a method.

Required user permissions:
- Customize Application
- Manage Profiles
- Manage Users
- Permission Sets
Create an MFA Permission Set

To create the permission set:

1. From Setup, enter Permission Sets in the Quick Find box, then select Permission Sets.
2. Click New.
3. Enter the required information for your MFA permission set.
4. Select a permission set license to define the types of users who will use the permission set.
5. Click Save.
6. Click the System Permissions link, then click Edit.
7. Scroll to Multi-Factor Authentication for User Interface Logins, then select the checkbox for the permission.
8. Click Save, then confirm your selection.
Assign the Permission Set to Users

To assign the permission set:

1. From Setup > Permission Sets, click the MFA permission set.
2. Click Manage Assignments.
3. Click Add Assignments.
4. Select the users to whom you want to assign the permission set.
5. Click Assign.
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
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 the Salesforce login screen, enter a username and password. The Connect Salesforce Authenticator screen displays.

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.
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.
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. Click the Choose Another Verification Method link in the bottom left corner of the Connect Salesforce Authenticator screen, then select One-Time Password Generator.
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.

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. Click the Choose Another Verification Method link in the bottom left corner of the Connect Salesforce Authenticator screen, then select Security Key.
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.

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.
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 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 any 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:
  o [Identity Verification Methods report or custom list views](#)
  o Monitor metrics with the [MFA Dashboard app from AppExchange](#).
Support Users and Ongoing Operations

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

- Troubleshooting and resolving login and authentication problems, including account lockouts.
- Helping users recover access if they’ve lost or forgotten their verification methods.
- Enabling MFA for new employees as part of your new hire onboarding process.
- Stocking and distributing 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. For more details, see Delegate Multi-Factor Authentication Management Tasks in Salesforce Help.

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. For more details, see Generate a Temporary Verification Code in Salesforce Help.
Learn More

Be an MFA Trailblazer – Check out these additional resources
Additional Resources

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

Get More Information About MFA
• Salesforce MFA FAQ
• Introduction to Salesforce Authenticator (video)
• Secure Account Access With MFA (webinar)

See More Details About Implementing MFA
• Launch Multi-Factor Authentication (video)
• How to Roll Out Multi-Factor Authentication (help)
• Multi-Factor Authentication (help)

Learn About MFA Using Trailhead
• User Authentication
• Identity Basics
• Security Basics

Get More Information on Security
• Security Health Check
• Salesforce Shield
• Salesforce Security Guide
• Security – Salesforce Trust Site