## Table of Contents

### CHAPTER 1

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Time for Multi-Factor Authentication is Now!</td>
<td></td>
</tr>
<tr>
<td>What Is MFA and Why Is It Important?</td>
<td>4</td>
</tr>
<tr>
<td>How Multi-Factor Authentication Works</td>
<td>5</td>
</tr>
<tr>
<td>MFA for Salesforce</td>
<td>6</td>
</tr>
<tr>
<td>MFA Verification Methods for Salesforce</td>
<td>7</td>
</tr>
<tr>
<td>Choose Verification Methods for Your Implementation</td>
<td>11</td>
</tr>
</tbody>
</table>

### CHAPTER 2

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implement MFA for Salesforce</td>
<td></td>
</tr>
<tr>
<td>The Recommended Path to MFA</td>
<td>13</td>
</tr>
<tr>
<td>Plan Your Rollout</td>
<td>14</td>
</tr>
<tr>
<td>When You’re Ready to Go Live</td>
<td>15</td>
</tr>
<tr>
<td>Enable MFA for Your Users</td>
<td>16</td>
</tr>
<tr>
<td>The User Experience When MFA is Live</td>
<td>17</td>
</tr>
<tr>
<td>Salesforce Authenticator: How Users Register and Log In</td>
<td>18</td>
</tr>
<tr>
<td>Third-Party Authenticator Apps: How Users Register and Log In</td>
<td>20</td>
</tr>
<tr>
<td>Security Keys: How Users Register and Log In</td>
<td>21</td>
</tr>
</tbody>
</table>

### CHAPTER 3

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure Successful Adoption of MFA</td>
<td></td>
</tr>
<tr>
<td>Measure the Success of Your Rollout</td>
<td>23</td>
</tr>
<tr>
<td>Support Users and Ongoing Operations</td>
<td>24</td>
</tr>
</tbody>
</table>

### CHAPTER 4

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learn More</td>
<td></td>
</tr>
<tr>
<td>Additional Resources</td>
<td>26</td>
</tr>
</tbody>
</table>

---

Version 2020.10
© Copyright 2000-2020 salesforce.com, inc. All rights reserved. Salesforce is a registered trademark of salesforce.com, inc., as are other names and marks. Other marks appearing herein may be trademarks of their respective owners.
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 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

MFA is currently available for these Salesforce products.

- Products built on the Salesforce Platform:
  - B2C Commerce Cloud
  - Marketing Cloud–Datorama
  - Marketing Cloud–Email Studio, Mobile Studio, and Journey Builder

Our goal is to deliver MFA support for all Salesforce products by mid-2021.
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. Depending on your Salesforce product, 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 or WebAuthn 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.*

* Marketing Cloud-Datorama customers: Push notifications aren’t supported yet. You can use Salesforce Authenticator as a TOTP generator only.
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.

All Salesforce products support the use of TOTP authenticator apps as an MFA verification method.

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
Depending on your Salesforce product, we support security keys that are compatible with FIDO U2F and FIDO2 WebAuthn. Both 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 FIDO U2F site or the WebAuthn Guide.

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, NFC*

Supported browsers for WebAuthn keys:
Chrome, Edge, Firefox, Safari

Supported browsers for U2F keys:
Chrome, version 41 or later

Products that support security keys:
• Products built on the Salesforce Platform*
• B2C Commerce Cloud*
• Marketing Cloud—Email, Mobile, & Journeys

* NFC devices aren’t supported in products built on the Salesforce Platform.
** WebAuthn isn’t supported in products built on the Salesforce Platform.
*** WebAuthn-compatible keys aren’t supported in non-Chromium versions of the Edge browser.
# Choose 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>A smart and simple mobile app that users can easily connect to their Salesforce accounts.</td>
<td>Apps generate unique, temporary verification codes based on the OATH TOTP algorithm.</td>
<td>Physical device that uses public-key cryptography.</td>
</tr>
<tr>
<td><strong>Form Factor:</strong> Mobile app for iOS and Android</td>
<td><strong>Form Factor:</strong> Apps available for multiple operating systems</td>
<td><strong>Form Factor:</strong> USB, Lightning, and NFC* devices that support the U2F or WebAuthn** standards</td>
</tr>
</tbody>
</table>
| **User Experience:**  
• Delivers push notifications to users’ phones for fast access  
• See real-time details to confirm request validity  
• Automate authentication from trusted locations  
• Deny fraudulent requests with a tap  
• Generates TOTP codes if connectivity isn’t available | **User Experience:**  
• Wide variety of apps to choose from  
• Connectivity isn’t required | **User Experience:**  
• Fast and easy to use  
• Recognizes and denies fraudulent requests  
• Connectivity isn’t required  
• No batteries needed |
| **Considerations:**  
• Requires a mobile device | **Considerations:**  
• Requires a mobile device  
• Typing errors possible when manually entering codes  
• Invalid codes possible if mobile device clock gets out of sync with Salesforce | **Considerations:**  
• Requires browser support (limited for U2F)  
• Users could leave key unattended or plugged in all the time  
• Operational overhead for purchasing, stocking, and distributing devices to users |
| **Cost:** Free | **Cost:** Free and paid options | **Cost:** Starts around $20 |

---

* NFC devices aren’t supported in products built on the Salesforce Platform.
** WebAuthn isn’t supported in products built on the Salesforce Platform. WebAuthn-compatible keys aren’t supported in non-Chromium versions of the Edge browser.
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.
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.

**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 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.

**Users**
Enable MFA for Your Users

The way you enable MFA is determined by your Salesforce product. Here’s an overview for each product that currently supports MFA.

### B2C Commerce Cloud

1. Make sure you’ve migrated Business Manager users to Account Manager via Unified Authentication.
2. Verify that the desired set of verification methods are enabled.
3. Open Account Manager’s Organization settings.
4. In the MFA Settings section, select **MFA enabled for all users in the organization**. Or select specific roles to roll out in phases.

See [Enabling MFA for Business Manager Users](#) for full details.

### Marketing Cloud—Datorama

In August 2020, MFA was enabled for all Datorama customers. If you disabled MFA for your account, it’s easy to turn it back on.

1. In Account Settings, select **Require Multi-Factor Authentication**.
2. Click **Save**.

See [Multi-Factor Authentication (MFA)](#) in the Datorama Success Center for full details.

### Marketing Cloud—Email, Mobile, & Journeys

1. Verify that the desired set of verification methods are enabled for your account.
2. In Setup > Security > Multi-Factor Authentication, select **Enable Multi-Factor Authentication**.

See [Transition Your Tenant from IDV to MFA in Marketing Cloud](#) in Salesforce Help for full details.

### Products Built on the Salesforce Platform

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.

See [Set Multi-Factor Authentication Login Requirements](#) in Salesforce Help for full details.
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 your Salesforce product’s login screen, enter a username and password.

3. **For products built on the Salesforce Platform**: The Salesforce Authenticator screen displays by default.

   **For B2C Commerce Cloud OR Marketing Cloud–Email, Mobile, & Journeys**: Select Salesforce Authenticator from the list of verification methods.

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**: To use Salesforce Authenticator with Marketing Cloud–Datorama, follow the steps for registering a third-party authenticator app.
Salesforce Authenticator: How Users Register and Log In  

To log in using the app:

1. On your Salesforce product’s 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 your Salesforce product’s login screen, enter a username and password.
3. For products built on the Salesforce Platform: Click Choose Another Verification Method in the bottom left corner of the Connect Salesforce Authenticator screen, then select One-Time Password Generator.
   For B2C Commerce Cloud OR Marketing Cloud–Email, Mobile, & Journeys: Select One-Time Password Generator.
   For Marketing Cloud–Datorama: The authenticator app registration screen displays automatically.
4. Open the authenticator app and select to add a new account.
5. Use the authenticator app to scan the QR barcode that’s displayed on the app connection screen.
   If scanning the QR barcode isn’t an option, manually generate your security key. Then enter it in the authenticator app.
6. On the app connection screen, enter the code generated by the authenticator app, then click the button to connect and log in.

To log in using a TOTP authenticator app:

1. On your Salesforce product's login screen, enter a username and password, as usual.
2. Open the authenticator app.
3. On the identity verification screen, enter the code generated by the authenticator app in the designated field, then click the button to verify and 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 your Salesforce product’s login screen and enter a username and password.

2. **For products built on the Salesforce Platform**: Click **Choose Another Verification Method** in the bottom left corner of the Connect Salesforce Authenticator screen, then select **Security Key**.
   
   For **B2C Commerce Cloud OR Marketing Cloud—Email, Mobile, & Journeys**: Select **Security Key** from the list of verification methods.

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 your Salesforce product’s 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.

---

*Marketing Cloud–Datorama customers: Security keys aren’t supported at this time.*
3 Ensure Successful Adoption of MFA

Manage your users’ experience with MFA
Measure the Success of Your Rollout

Ensure your users are adopting MFA and getting the support they need.

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, conduct online polls, 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.
• Analyze usage patterns, including any changes to the volume of daily or monthly Salesforce logins and who’s using which methods.
• Look for spikes and trends related to issuing temporary verification codes.
• Depending on your Salesforce product, take advantage of built-in tools to help monitor MFA adoption.
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.

Recover Access With Temporary Verification Codes

Generate temporary codes for users who can’t access their usual MFA verification methods. A code can be used multiple times until it expires.

➤ NOTE: Temporary codes aren’t available yet for B2C Commerce Cloud or Marketing Cloud–Datorama.
Learn More

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

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

More Information about MFA
• Salesforce MFA FAQ
• How to Roll Out Multi-Factor Authentication (help)
• Introduction to Salesforce Authenticator (video)

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

For Products built on the Salesforce Platform
• Launch Multi-Factor Authentication (video)
• Set Up Multi-Factor Authentication (help)
• Salesforce Security Guide

For B2C Commerce Cloud
• B2C Commerce MFA and Unified Authentication for Business Manager (video)
• Enabling MFA for Business Manager Users: A Step-By-Step Guide

For Marketing Cloud–Datorama
• MFA Knowledge Article
• MFA FAQ

For Marketing Cloud–Email, Mobile, & Journeys
• MFA for Marketing Cloud (help)
• MFA for Marketing Cloud FAQ