MFA Onboarding Template: Register and Log in with a Third-Party TOTP Authenticator App

How to use this template:

* This template provides onboarding instructions for users who want to use a third-party authenticator app as an MFA verification method.
  + Salesforce supports the use of authenticator apps that generate temporary codes based on the OATH time-based one-time password (TOTP) algorithm ([RFC 6238](http://tools.ietf.org/html/rfc6238)). There are a variety of TOTP authenticator apps available, including many free options. Widely used apps include Google Authenticator, Microsoft Authenticator, and Authy.
* This template assumes you’re turning on MFA for direct logins to your customer’s org. If you're using an SSO identity provider's MFA service instead, modify the content and screenshots to align with the details of that implementation (including the verification methods that the identity provider supports).
* Customize this template to match the customer’s MFA implementation.
  + As of the Summer ’23 Salesforce release, [the MFA registration experience can begin with either a list of all supported verification methods or with the Connect Salesforce Authenticator screen](https://help.salesforce.com/s/articleView?id=sf.security_optimize_verification_method_registration.htm). Pick the version of the template that’s appropriate for your customer’s org.
  + Review the comments for tips and guidance.
  + Edit any placeholders, which are noted with [brackets and red text], to include your customer’s details.
  + Include your MFA rollout resources and instructions on how users can ask questions or get assistance.
* Decide how you want to distribute onboarding instructions to users. Options include saving this template as a PDF file and emailing it to users, hosting a PDF on an internal site, or generating an HTML page for online access.

Delete this text before sharing with users.

How to Register and Use a Third-Party Authenticator App for Multi-Factor Authentication (MFA) Logins

**Register a third-party authenticator app**

To use a third-party authenticator app as a verification method for MFA logins, register the app to connect it to your account. You can register an app at any time, even before MFA is turned on.

To register a third-party authenticator app the first time you log in after MFA is turned on, follow these onscreen instructions.

|  |  |  |  |
| --- | --- | --- | --- |
| **1**  Graphical user interface, text  Description automatically generated  A picture containing graphical user interface  Description automatically generated | **2**  Graphical user interface, application  Description automatically generated | **3** | **4**  Qr code  Description automatically generated |
| Install a third-party authenticator app on your mobile device. Apps are available from the Apple App Store or Google Play. | On your computer, log in to your account. You may be prompted to verify your identity with a one-time passcode via email or text message. | Select **Use verification codes from an authenticator app**. | The Connect an Authenticator app screen displays. |

|  |  |  |  |
| --- | --- | --- | --- |
| **5**  Graphical user interface, application  Description automatically generated | **6**  Qr code  Description automatically generated | **7**  Graphical user interface, text, application, chat or text message  Description automatically generated | **8**  Qr code  Description automatically generated |
| On your mobile device, open your authenticator app and select to add a new account. | Use the authenticator app to scan the QR barcode that’s displayed on your computer. | The authenticator app is connected to your account. The app automatically starts generating time-based one-time passcodes. | On your computer, enter a one-time code generated by the authenticator app in the Verification Code field, then click **Connect**. |

|  |  |  |  |
| --- | --- | --- | --- |
| **9**  A picture containing text, monitor, electronics, computer  Description automatically generated |  |  |  |
| And that’s it! You’ve successfully connected your third-party authenticator app to your account, and you finish logging in. |  |  |  |

To register a third-party authenticator app from personal settings in your account:

1. Download and install the authenticator app on your mobile device. The app is available from the Apple Store or Google Play.
2. Log in to your account, then go to your personal settings.
3. Enter Advanced User Details in the Quick Find box, then select **Advanced User Details**.
4. In the App Registration: One-Time Password Authenticator field, click **Connect**.
5. For security purposes, you may be prompted to log in to your account or verify your identity by receiving a one-time passcode via email or test message.
6. Complete steps 4 through 9 in the above table.

**Log in with a third-party authenticator app**

To use a third-party authenticator app to verify your identity for MFA logins:

|  |  |  |  |
| --- | --- | --- | --- |
| **1**  Graphical user interface, application  Description automatically generated | **2**  Graphical user interface, application, Teams  Description automatically generated | **3**  Graphical user interface, text, application, chat or text message  Description automatically generated | **4**  A picture containing text, monitor, electronics, computer  Description automatically generatedGraphical user interface, application, Teams  Description automatically generated |
| On the login screen, enter your username and password, as usual. | You’re prompted to enter a code from your authenticator app to verify your identity. | On your mobile device, open your authenticator app to get a time-based one-time passcode. | On your computer, enter the code generated by the authenticator app, then click **Verify**. You’re successfully logged in to your account. |

**How to get help**

* [Add links to your company’s MFA rollout resources.]
* [Add contact information where users can ask questions and get help.]

How to Register and Use a Third-Party Authenticator App for Multi-Factor Authentication (MFA) Logins

**Register a third-party authenticator app**

To use a third-party authenticator app as a verification method for MFA logins, register the app to connect it to your account. You can register an app at any time, even before MFA is turned on.

To register a third-party authenticator app the first time you log in after MFA is turned on, follow these onscreen instructions.

|  |  |  |  |
| --- | --- | --- | --- |
| **1**  Graphical user interface, text  Description automatically generated  A picture containing graphical user interface  Description automatically generated | **2**  Graphical user interface, application  Description automatically generated | **3**  Graphical user interface, text  Description automatically generated | **4** |
| Install a third-party authenticator app on your mobile device. Apps are available from the Apple App Store or Google Play. | On your computer, log in to your account. You may be prompted to verify your identity with a one-time passcode via email or text message. | The Connect Salesforce Authenticator screen displays by default. Click **Choose Another Verification Method**. | Select **Use verification codes from an authenticator app**. |

|  |  |  |  |
| --- | --- | --- | --- |
| **5**  Qr code  Description automatically generated | **6**  Graphical user interface, application  Description automatically generated | **7**  Qr code  Description automatically generated | **8**  Graphical user interface, text, application, chat or text message  Description automatically generated |
| The Connect an Authenticator app screen displays. | On your mobile device, open your authenticator app and select to add a new account. | Use the authenticator app to scan the QR barcode that’s displayed on your computer. | The authenticator app is connected to your account. The app automatically starts generating time-based one-time passcodes. |

|  |  |  |  |
| --- | --- | --- | --- |
| **9**  Qr code  Description automatically generated | **10**  A picture containing text, monitor, electronics, computer  Description automatically generated |  |  |
| On your computer, enter a one-time code generated by the authenticator app in the Verification Code field, then click **Connect**. | And that’s it! You’ve successfully connected your third-party authenticator app to your account, and you finish logging in. |  |  |

To register a third-party authenticator app from personal settings in your account:

1. Download and install the authenticator app on your mobile device. The app is available from the Apple Store or Google Play.
2. Log in to your account, then go to your personal settings.
3. Enter Advanced User Details in the Quick Find box, then select **Advanced User Details**.
4. In the App Registration: One-Time Password Authenticator field, click **Connect**.
5. For security purposes, you may be prompted to log in to your account or verify your identity by receiving a one-time passcode via email or test message.
6. Complete steps 5 through 10 in the above table.

**Log in with a third-party authenticator app**

To use a third-party authenticator app to verify your identity for MFA logins:

|  |  |  |  |
| --- | --- | --- | --- |
| **1**  Graphical user interface, application  Description automatically generated | **2**  Graphical user interface, application, Teams  Description automatically generated | **3**  Graphical user interface, text, application, chat or text message  Description automatically generated | **4**  A picture containing text, monitor, electronics, computer  Description automatically generatedGraphical user interface, application, Teams  Description automatically generated |
| On the login screen, enter your username and password, as usual. | You’re prompted to enter a code from your authenticator app to verify your identity. | On your mobile device, open your authenticator app to get a time-based one-time passcode. | On your computer, enter the code generated by the authenticator app, then click **Verify**. You’re successfully logged in to your account. |

**How to get help**

* [Add links to your company’s MFA rollout resources.]
* [Add contact information where users can ask questions and get help.]