MFA Onboarding Template: Register and Log in with a Built-In Authenticator

How to use this template:

* This template provides onboarding instructions for users who want to use a built-in authenticator, such as Windows Hello, Touch ID or Face ID, as an MFA verification method.
* 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 Built-In Authenticator for Multi-Factor Authentication (MFA) Logins

|  |  |
| --- | --- |
| **Confirm that you meet the requirements to use a built-in authenticator** | * Your computer/mobile device, operating system, and browser support the Web Authentication ([FIDO2 WebAuthn](https://fidoalliance.org/fido2/fido2-web-authentication-webauthn/)) standard. |
| * Your built-in authenticator service, such as Windows Hello, Touch ID, or Face ID, is enabled and configured to verify your identity via a biometric like a fingerprint or facial recognition scan, or a PIN. |

**Register a built-in authenticator**

To use a built-in authenticator as a verification method for MFA logins, go through the registration process to connect it to your account.

**Tip**: A built-in authenticator is tied to your device. If you log in from multiple computers (for example, a desktop workstation and a laptop), you either need to register a built-in authenticator on each device or register a second type of verification method that you can use on devices where you don’t have a built-in authenticator.

When you log in for the first time after MFA has been turned on, follow these onscreen instructions.

|  |  |  |  |
| --- | --- | --- | --- |
| **1**  Graphical user interface, application  Description automatically generated | **2** | **3**  Graphical user interface, text, application, chat or text message, website  Description automatically generated | **4**  Graphical user interface, application, Teams  Description automatically generated |
| In a supported browser, 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 a built-in authenticator on your device** from the list of verification methods. | Click **Register**. | When prompted by your browser, provide the identifier that you previously set up with your built-in authenticator, such as your fingerprint, facial scan, PIN, or password. |

|  |  |  |  |
| --- | --- | --- | --- |
| **5**  Graphical user interface, application, Teams  Description automatically generated | **6**  A picture containing text, monitor, electronics, computer  Description automatically generated |  |  |
| Assign a name to your built-in authenticator so it’s easy to recognize, then click **Done**. | And that’s it! You’ve successfully connected your built-in authenticator to your account, and you finish logging in to your account. |  |  |

To register a built-in authenticator from personal settings in your account:

1. In a supported browser, log in to your account, then go to your personal settings.
2. Enter Advanced User Details in the Quick Find box, then select **Advanced User Details**.
3. In the Built-in Authenticators section, click **Add**.
4. 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.
5. Complete steps 3 through 6 in the above table.

**Log in with a built-in authenticator**

To use a built-in authenticator to verify your identity for MFA logins:

|  |  |  |  |
| --- | --- | --- | --- |
| **1**  Graphical user interface, application  Description automatically generated | **2**  Graphical user interface, text, application  Description automatically generated | **3**  Graphical user interface, text, application  Description automatically generated | **4**  A picture containing text, monitor, electronics, computer  Description automatically generated |
| In a supported browser, on the login screen, enter your username and password, as usual. | When you see the Verify Your Identity screen, click **Verify**. | When prompted by your browser, provide the identifier that you previously set up with your built-in authenticator, such as your fingerprint, facial scan, PIN, or password. | 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 Built-In Authenticator for Multi-Factor Authentication (MFA) Logins

|  |  |
| --- | --- |
| **Confirm that you meet the requirements to use a built-in authenticator** | * Your computer/mobile device, operating system, and browser support the Web Authentication ([FIDO2 WebAuthn](https://fidoalliance.org/fido2/fido2-web-authentication-webauthn/)) standard. |
| * Your built-in authenticator service, such as Windows Hello, Touch ID, or Face ID, is enabled and configured to verify your identity via a biometric like a fingerprint or facial recognition scan, or a PIN. |

**Register a built-in authenticator**

To use a built-in authenticator as a verification method for MFA logins, go through the registration process to connect it to your account.

**Tip**: A built-in authenticator is tied to your device. If you log in from multiple computers (for example, a desktop workstation and a laptop), you either need to register a built-in authenticator on each device or register a second type of verification method that you can use on devices where you don’t have a built-in authenticator.

When you log in for the first time after MFA has been turned on, follow these onscreen instructions.

|  |  |  |  |
| --- | --- | --- | --- |
| **1**  Graphical user interface, application  Description automatically generated | **2**  Graphical user interface, text  Description automatically generated | **3** | **4**  Graphical user interface, text, application, chat or text message, website  Description automatically generated |
| In a supported browser, 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 a built-in authenticator on your device** from the list of verification methods. | Click **Register**. |

|  |  |  |  |
| --- | --- | --- | --- |
| **5**  Graphical user interface, application, Teams  Description automatically generated | **6**  Graphical user interface, application, Teams  Description automatically generated | **7**  A picture containing text, monitor, electronics, computer  Description automatically generated |  |
| When prompted by your browser, provide the identifier that you previously set up with your built-in authenticator, such as your fingerprint, facial scan, PIN, or password. | Assign a name to your built-in authenticator so it’s easy to recognize, then click **Done**. | And that’s it! You’ve successfully connected your built-in authenticator to your account, and you finish logging in to your account. |  |

To register a built-in authenticator from personal settings in your account:

1. In a supported browser, log in to your account, then go to your personal settings.
2. Enter Advanced User Details in the Quick Find box, then select **Advanced User Details**.
3. In the Built-in Authenticators section, click **Add**.
4. 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.
5. Complete steps 4 through 7 in the above table.

**Log in with a built-in authenticator**

To use a built-in authenticator to verify your identity for MFA logins:

|  |  |  |  |
| --- | --- | --- | --- |
| **1**  Graphical user interface, application  Description automatically generated | **2**  Graphical user interface, text, application  Description automatically generated | **3**  Graphical user interface, text, application  Description automatically generated | **4**  A picture containing text, monitor, electronics, computer  Description automatically generated |
| In a supported browser, on the login screen, enter your username and password, as usual. | When you see the Verify Your Identity screen, click **Verify**. | When prompted by your browser, provide the identifier that you previously set up with your built-in authenticator, such as your fingerprint, facial scan, PIN, or password. | 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.]