Salesforce Admin Security

Phishing-resistant MFA installation guide

Effective Date: Production environments starting July 1, 2026 | Sandboxes from June 22, 2026. Also read: **Preparation phishing-resistant MFA (administrators):** help.salesforce.com/s/articleView?id=005321563.

1. What is required?

Starting July 1, 2026, all privileged Salesforce users will be required to log in using a phishing-resistant MFA method. Privileged users are users with:

- the System Administrator or System Administrator Mysolution profile
- System Permission Modify All Data, View All Data, Customize Application of Author Apex

Standard authenticator apps (such as Google Authenticator, Microsoft Authenticator, or Authy) that generate 6-digit TOTP codes don't meet the new requirement. Users who have not registered an appropriate method will be blocked from the login screen.

Qualified methods are:

- Build-in authenticators: Touch ID, Face ID (Mac/iPhone), Windows Hello (Windows 10/11)
- Physical security keys: YubiKey, Google Titan Key, or another WebAuthn/FIDO2/U2F key
- Synced passkeys stored in a password manager (Apple iCloud Keychain, 1Password, Bitwarden, etc.)

> ℹ Salesforce recommends registering at least two qualified methods per administrator as a backup, in case a device is lost or unavailable.

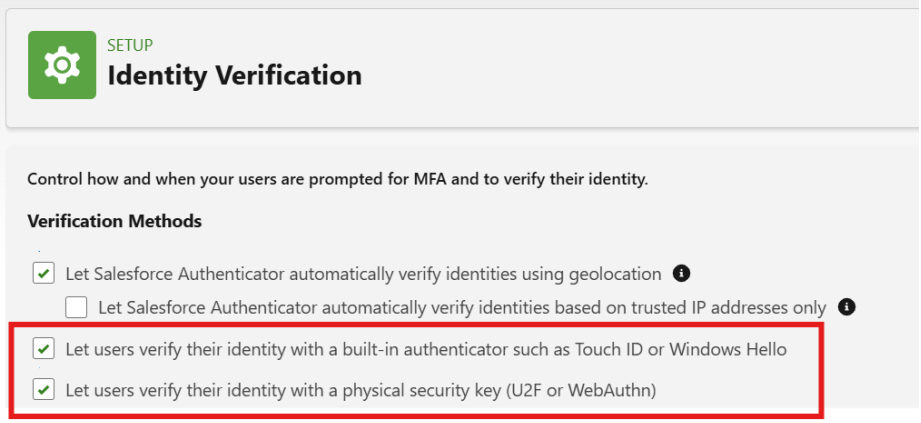
2. Overview of scenarios

The table below summarizes the most common configurations and the associated post-setup sign-in experience.

Platform	Method	Post-setup login experience	Qualified?
Windows	Physical security key (YubiKey etc.)	Key insert/tap + touch button	☑ Qualified
Windows	Windows Hello (PIN / Face / Fingerprint)	Windows Hello window – virtually seamless	☑ Qualified
Windows	External passkey (1Password, Bitwarden)	Extension pop-up, confirm in app	☑ Qualified
Mac	Apple Passkey (iCloud Keychain)	Seamless – Touch ID or Mac-login screen	☑ Qualified
Mac	Externe passkey (1Password, Bitwarden)	Extension pop-up, confirm in app	☑ Qualified
Mac	Physical security key (YubiKey etc.)	Key insert/tap + touch button	☑ Qualified
All	TOTP-app (Google/Microsoft Authenticator)	Blocked – DOES NOT meet the requirement	✗ Not qualified

3. Activation of the security key

As indicated, this method will become mandatory from Salesforce from July 1, 2026. Before this date, you can activate this for users with a system administrator profile. To do this, go to Setup, Identity Verification and activate the corresponding options, according to your organization's policy:



Register your passkey for your account in the production environment and repeat these steps for any Sandbox user accounts. Choose from one of the installation methods in Windows or Mac.

> ⚠ Always register a backup key as a backup. If you lose the only key, you will be locked out and will need to contact Salesforce Support to restore access.

4. Installation Instructions

Scenario A: Windows Hello (Windows)

Recommended for: Windows 10/11 users with a device that supports PIN, facial recognition, or fingerprint unlock.

1. Make sure that Windows Hello is set up on your device (Settings, Accounts, Sign-in options).
2. Log in to Salesforce and click on your avatar in the top right. Choose Settings, Advanced User Data.
3. In the App registration: Security keys and built-in authenticators section, click Register.
4. The browser shows a Windows security window. Authenticate with your Windows Hello method (PIN, face, or fingerprint).
5. The registration is complete. The key is stored in the device's Trusted Platform Module (TPM).

> ℹ Windows Hello keys are device-bound — they are not synced to other devices. Register Windows Hello separately on each Windows device that you use Salesforce on.

Scenario B: Passkey on iPhone, iPad, or Android phone (Windows)

Recommended for: Windows 10/11 users with a phone that supports biometric sign-in.

1. Log in to Salesforce and click on your avatar in the top right. Choose Settings, Advanced User Data.
2. In the App registration: Security keys and built-in authenticators section, click Register.
3. Account verification via email follows. Enter the verification code that you will receive via email.
4. In the next screen, choose to register the Security Key.
5. The browser will show a Windows security window to store the passkey. Choose the 'Change' option on the screen to save the key to a device other than a USB key/Security key.
6. On the next screen, choose the iPhone, iPad, or Android device option.

7. Scan the QR code and complete the registration of the passkey in your phone's password manager.
8. Give the Passkey a name to recognize it for your environment.

Scenario C: Apple Passkey (iCloud Keychain op Mac)

Recommended for: Mac users who are comfortable with iCloud and want the most seamless experience.

1. Log in to Salesforce and click on your avatar in the top right. Choose Settings, Advanced User Data.
2. In the App registration: Security keys and built-in authenticators section, click Register.
3. Scan the QR code with your iPhone and confirm the creation on your phone.
4. The passkey is stored in iCloud Keychain and synced to other Apple devices signed in to the same Apple ID.

Scenario D: Physical security key as YubiKey or Google Titan (Windows and Mac)

Recommended for: Organizations with strict security policies, shared workstations, or users who prefer a purely hardware-based approach.

Same procedure as Scenario A. The steps are identical — insert key, follow browser prompt. You now store the passkey in a special USB key from, for example, YubiKey.

Scenario E: Remote password manager on (Windows and Mac)

Recommended for: Users who want a cross-platform solution or are already using 1Password, Bitwarden, etc.

1. Make sure your password manager's browser extension is installed and active in Chrome or Edge.
2. Log in to Salesforce and click on your avatar in the top right. Choose Settings, Advanced User Data.
3. In the App registration: Security keys and built-in authenticators section, click Register.
4. When the passkey dialog appears, select the password manager from the options.
5. In the password manager extension, confirm with your master password or biometrics.
6. The passkey is stored in your vault and is available on any device where the password manager is installed.

5. SSO Users

If your organization uses Single Sign-On (e.g., Azure AD, Okta, Ping), the phishing-resistant MFA requirement must be met at the identity provider (IdP) level, not directly in Salesforce.

- Your IdP should pass ACR/AMR signals (RFC 8176) that confirm that a phishing-resistant method was used.
- If those signals are missing, Salesforce prompts the user to register a qualified method directly.