Salesforce Admin-Sicherheit

Phishing-resistente MFA-Installationsanleitung

Wirksamkeitsdatum: Produktionsumgebungen ab dem 1. Juli 2026 | Sandboxes ab dem 22. Juni 2026. Lesen Sie auch **: Vorbereitung phishing-resistentes MFA (Administratoren):** help.salesforce.com/s/articleView?id=005321563.

1. Was ist erforderlich?

Ab dem 1. Juli 2026 müssen sich alle privilegierten Salesforce-Nutzer mit einer phishing-resistenten MFA-Methode anmelden. Privilegierte Nutzer sind Nutzer mit:

- das Systemadministrator- oder Systemadministrator-Mysolution-Profil
- Systeempermissie alle Daten ändern, alle Daten ansehen, Anwendung des Autoren-Apex anpassen

Standard-Authenticator-Apps (wie Google Authenticator, Microsoft Authenticator oder Authy), die sechsstellige TOTP-Codes generieren, erfüllen die neue Anforderung nicht. Nutzer, die eine geeignete Methode nicht registriert haben, werden vom Anmeldebildschirm ausgeschlossen.

Qualifizierte Methoden sind:

- Ingebouwde Authenticators: Touch ID, Face ID (Mac/iPhone), Windows Hello (Windows 10/11)
- Physische Sicherheitsschlüssel: YubiKey, Google Titan Key oder ein anderer WebAuthn/FIDO2/U2F-Schlüssel
- Synchronisierte Passkeys, die in einem Passwortmanager gespeichert sind (Apple iCloud Keychain, 1Password, Bitwarden usw.).

> ℹ Salesforce empfiehlt, mindestens zwei qualifizierte Methoden pro Administrator als Backup zu registrieren, falls ein Gerät verloren geht oder nicht verfügbar ist.

2. Überblick über die Szenarien

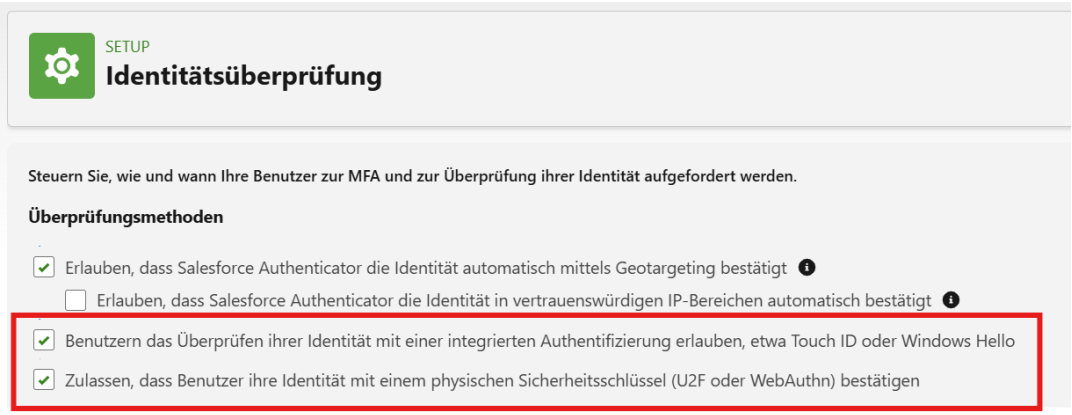
Die folgende Tabelle fasst die häufigsten Konfigurationen und die zugehörige Anmeldeerfahrung nach der Einrichtung zusammen.

Plattform	Methode	Login-Erfahrung nach der Einrichtung	Qualifiziert?
Windows	Physischer Sicherheitsschlüssel (YubiKey usw.)	Tasteninsert/Tipp + Touch-Taste	☑ Qualifiziert
Windows	Windows Hello (PIN / Gesicht / Fingerabdruck)	Windows Hello-Fenster – nahezu nahtlos	☑ Qualifiziert
Windows	Externe passkey (1Password, Bitwarden)	Erweiterungs-Popup, bestätigen Sie in der App	☑ Qualifiziert
Mac	Apple Passkey (iCloud-Schlüsselbund)	Naadloos – Touch ID von Mac-loginvenster	☑ Qualifiziert
Mac	Externe passkey (1Password, Bitwarden)	Erweiterungs-Popup, bestätigen Sie in der App	☑ Qualifiziert
Mac	Physischer Sicherheitsschlüssel (YubiKey usw.)	Tasteninsert/Tipp + Touch-Taste	☑ Qualifiziert

Plattform	Methode	Login-Erfahrung nach der Einrichtung	Qualifiziert?
Alle	TOTP-app (Google/Microsoft Authenticator)	Blockiert – ERFÜLLT die Voraussetzung NICHT	❌ Nicht qualifiziert

3. Aktivierung des Sicherheitsschlüssels

Wie bereits erwähnt, wird diese Methode ab dem 1. Juli 2026 bei Salesforce verpflichtend sein. Vor diesem Datum können Sie dies für Benutzer mit einem Systemadministrator-Profil aktivieren. Dazu gehen Sie zu Einrichten, Identitätsverifizierung und aktivieren Sie die entsprechenden Optionen gemäß den Richtlinien Ihrer Organisation:



Registrieren Sie Ihren Passkey für Ihr Konto in der Produktionsumgebung und wiederholen Sie diese Schritte für alle Sandbox-Benutzerkonten. Wählen Sie eine der Installationsmethoden unter Windows oder Mac.

> ⚠ Registrieren Sie immer einen Backup-Schlüssel als Backup. Wenn du den einzigen Schlüssel verlierst, wirst du ausgesperrt und musst den Salesforce-Support kontaktieren, um den Zugriff wiederherzustellen.

3. Installationsanleitung

Szenario A: Passkey auf iPhone, iPad oder Android-Telefon (Windows)

Empfohlen für: Windows 10/11-Nutzer mit einem Telefon, das biometrische Anmeldung unterstützt.

1. Melden Sie sich bei Salesforce an und klicken Sie oben rechts auf Ihren Avatar. Wähle Einstellungen, erweiterte Benutzerdaten.
2. Im Bereich App-Registrierung: Sicherheitsschlüssel und integrierte Authentifikatoren klicken Sie auf Registrieren.
3. Kontoverifizierung per E-Mail folgt. Geben Sie den Verifizierungscode ein, den Sie per E-Mail erhalten.
4. Im nächsten Bildschirm wählen Sie die Registrierung des Sicherheitsschlüssels.
5. Der Browser zeigt ein Windows-Sicherheitsfenster an, um den Passkey zu speichern. Wählen Sie die Option 'Ändern' auf dem Bildschirm, um den Schlüssel auf einem anderen Gerät als einem USB-Schlüssel/Sicherheitsschlüssel zu speichern.
6. Auf dem nächsten Bildschirm wählen Sie die Option iPhone, iPad oder Android-Gerät.
7. Scannen Sie den QR-Code und schließen Sie die Registrierung des Passkeys im Passwortmanager Ihres Handys durch.
8. Gib dem Passkey einen Namen, um ihn für deine Umgebung zu erkennen.

Szenario B: Apple Passkey (iCloud Keychain op Mac)

Empfohlen für: Mac-Nutzer, die sich mit iCloud wohlfühlen und das reibungsloseste Erlebnis wünschen.

1. Melden Sie sich bei Salesforce an und klicken Sie oben rechts auf Ihren Avatar. Wähle Einstellungen, erweiterte Benutzerdaten.
2. Im Bereich App-Registrierung: Sicherheitsschlüssel und integrierte Authentifikatoren klicken Sie auf Registrieren.
3. Scannen Sie den QR-Code mit Ihrem iPhone und bestätigen Sie die Erstellung auf Ihrem Handy.
4. Der Passkey wird im iCloud-Schlüsselbund gespeichert und mit anderen Apple-Geräten synchronisiert, die mit derselben Apple-ID angemeldet sind.

Szenario C: Physischer Sicherheitsschlüssel als YubiKey oder Google Titan (Windows und Mac)

Empfohlen für: Organisationen mit strengen Sicherheitsrichtlinien, gemeinsam genutzte Arbeitsplätze oder Nutzer, die einen rein hardwarebasierten Ansatz bevorzugen.

Gleiches Verfahren wie bei Szenario A. Die Schritte sind identisch – Schlüssel einfügen, Browser-Eingabe folgen. Du speicherst den Passkey jetzt in einem speziellen USB-Stick von zum Beispiel YubiKey.

Szenario D: Windows Hello (Windows)

Empfohlen für: Windows 10/11-Nutzer mit einem Gerät, das PIN, Gesichtserkennung oder Fingerabdruckentsperrung unterstützt.

1. Stelle sicher, dass Windows Hello auf deinem Gerät eingerichtet ist (Einstellungen, Konten, Anmeldeoptionen).
2. Melden Sie sich bei Salesforce an und klicken Sie oben rechts auf Ihren Avatar. Wähle Einstellungen, erweiterte Benutzerdaten.
3. Im Bereich App-Registrierung: Sicherheitsschlüssel und integrierte Authentifikatoren klicken Sie auf Registrieren.
4. Der Browser zeigt ein Windows-Sicherheitsfenster an. Authentifiziere dich mit deiner Windows-Hello-Methode (PIN, Gesicht oder Fingerabdruck).
5. Die Registrierung ist abgeschlossen. Der Schlüssel wird im Trusted Platform Module (TPM) des Geräts gespeichert.

> ℹ Windows Hello-Schlüssel sind gerätegebunden – sie werden nicht mit anderen Geräten synchronisiert. Registrieren Sie Windows Hello separat auf jedem Windows-Gerät, auf dem Sie Salesforce verwenden.

Szenario E: Remote Passwortmanager aktiviert (Windows und Mac)

Empfohlen für: Nutzer, die eine plattformübergreifende Lösung wünschen oder bereits 1Password, Bitwarden usw. verwenden.

1. Stelle sicher, dass die Browsererweiterung deines Passwortmanagers in Chrome oder Edge installiert und aktiv ist.
2. Melden Sie sich bei Salesforce an und klicken Sie oben rechts auf Ihren Avatar. Wähle Einstellungen, erweiterte Benutzerdaten.
3. Im Bereich App-Registrierung: Sicherheitsschlüssel und integrierte Authentifikatoren klicken Sie auf Registrieren.
4. Wenn der Passschlüssel-Dialog erscheint, wähle den Passwortmanager aus den Optionen aus.
5. Bestätigen Sie in der Passwortmanager-Erweiterung mit Ihrem Hauptpasswort oder Biometrie.
6. Der Passkey wird in Ihrem Tresor gespeichert und ist auf jedem Gerät verfügbar, auf dem der Passwortmanager installiert ist.

5. SSO-Nutzer

Wenn Ihre Organisation Single Sign-On verwendet (z. B. Azure AD, Okta, Ping), muss die phishing-resistente MFA-Anforderung auf Ebene des Identitätsanbieters (IdP) erfüllt werden, nicht direkt in Salesforce.

- Ihr IdP sollte ACR/AMR-Signale (RFC 8176) weiterleiten, die bestätigen, dass eine phishing-resistente Methode verwendet wurde.
- Wenn diese Signale fehlen, fordert Salesforce den Nutzer auf, eine qualifizierte Methode direkt zu registrieren.