# Frequently asked questions

## Scope and timing

### 1. Who is affected by the phishing-resistant MFA requirement?

The requirement applies to users with the System Administrator profile or any of these elevated permissions: Modify All Data, View All Data, Customize Application or Author Apex. Check custom profiles, permission sets and permission set groups, not only users named System Administrators.

### 2. Are standard team members or HR users automatically affected?

No. A user is in scope because of the elevated permissions assigned to them, not simply because they are an HR user or use Sage People. A standard user without the listed permission remains subject to the normal MFA requirements rather than the privileged-user phishing-resistant requirement.

### 3. Does enforcement apply to both production and sandbox?

The enforcement date is 1 October 2026 for both production and sandbox organisations. You should complete testing before that date.

### 4. What happens if an affected user has not set up a compliant method?

An affected user will generally be prompted to create a passkey at their next login. However, device or organisational policies may prevent successful enrolment, so users should not rely on the enforcement prompt and should configure and test access in advance.

### 5. Why are some users already being prompted to create a passkey?

Salesforce have transitioned to a Phishing resistant first approach. When standard users are required to setup an MFA method, they will be prompted to create a passkey but have the option to choose another method at the bottom. A sandbox refresh can also bring forward the enforcement. If a user is prompted to setup a passkey and has no option to select another method prior to October 1st please raise a case with the user's details.

## SSO and High Assurance

### 6. We use SSO. Does that mean we are already compliant?

Not automatically. For affected users, confirm that the identity provider uses a phishing-resistant authentication method and sends a recognised phishing-resistant AMR or ACR signal to Salesforce. The applicable SSO authentication method must also appear under High Assurance in Session Security Levels.

### 7. Azure SSO and Multi-Factor Authentication are already under High Assurance. Are we ready?

If Azure SSO is the method currently used by affected users, and the login sends a recognised phishing-resistant signal, the configuration is correct.

## 8. I cannot see an item called “SSO” in Session Security Levels. What should I move?

The item may use the configured provider or connection name, such as Azure, Microsoft, Entra, Google or a custom SAML name. In Setup, review Single Sign-On Settings to confirm the name, then locate that authentication method in Session Settings and move it to High Assurance if needed.

## 9. What changes when we set our SSO method to High Assurance?

It allows Salesforce to recognise a successful session using that authentication method as High Assurance. It does not give users extra permissions. Review any sensitive actions your organisation has configured in the identity verification page in setup to require High Assurance and test the full login and action journey in sandbox.

## 10. Do both AMR and ACR need to contain a value?

No. A recognised phishing-resistant signal in either AMR or ACR can be sufficient. In Login History, the value may appear as a long URI; the final part of the value is usually the signal to compare with Salesforce guidance.

## 11. Is x509 a phishing-resistant signal?

Yes, a value of x509 shown in AMR can be treated as a recognised phishing-resistant signal. Do not rely on the fact that you use x509 though, ensure you have checked the correct signal are being sent.

## 12. What if AMR and ACR are blank or our provider does not send a recognised signal?

Work with your IT or identity-provider team to confirm the authentication method and update the SAML or OpenID Connect claims sent to Salesforce. If Salesforce cannot recognise a phishing-resistant signal, the affected user may be required to register a Salesforce passkey to complete login.

## Direct login and passkeys

## 13. Do non-System Administrator users need Setup access to add a passkey?

No. A user can add a passkey from their own personal settings: Profile > Settings > Advanced User Details > Built-in Authenticators > Add. They do not need administrator access to Setup for this user-level action.

## 14. If a user already added Windows Hello for Step-Up Authentication, will it also work for login?

A registered built-in authenticator can be used as a phishing-resistant method. The user should sign out and test the full login journey to confirm that the expected authenticator is offered for their account and device.

## 15. Do we need to disconnect Salesforce Authenticator before adding a passkey?

A Salesforce Authenticator can remain registered after a built-in authenticator is added. Salesforce Authenticator does not satisfy the privileged-user phishing-resistant requirement, but it does not need to be removed simply to register a passkey.

### 16. Which method should an administrator choose if they use both a work computer and a personal mobile device?

Choose an organisation-approved method that is available across every device the administrator needs to use. Device-bound passkeys may not be shared between devices. We would recommend an SSO configured with phishing-resistant MFA for cross-device access or a third-party passkey management solution, subject to your IT and security policies.

## API users, integrations and Data Loader

### 17. Does the requirement apply to API or integration users?

This requirement applies to only UI based logins, API logins are exempt. However, do not decide based only on the account name or licence. Confirm how the account actually authenticates and whether it also signs in through the browser UI.

### 18. How do we confirm whether an integration account is an API user?

Review the account's real login route and Login History, not only its profile name. In the same login history where you can check AMR and ACR signals you can also see the details of each login and if it is completed via API or UI.

### 19. Will Salesforce Data Loader using OAuth be affected?

Yes, there are a number of methods of login for salesforce data loader however if you are signing in via your username and password you will be prompted to setup / confirm your phishing resistant MFA method.

### 20. Do DocuSign, Power BI or other integrations need a passkey?

It depends on whether the account uses an API/integration flow or signs in interactively through the Salesforce UI. Confirm the login type for each integration account. If an account uses both API and browser access, review the browser access separately.

## Reporting, mobile and resources

### 21. Is there a standard report showing every affected user?

There is no built-in report for this. Review profiles, permission sets and permission set groups. For larger audits, consider SOQL or Salesforce's User Access and Permissions Assistant.

### 22. What should mobile users do?

Affected administrators should use the latest supported Sage People mobile app V2.4 and test their actual mobile login route before 1 October. If the selected passkey is device-bound, check whether it is available on the mobile device. Browser-based mobile access and SSO may have different behaviour, so test the route users will genuinely use.

## 23. Where can users find step-by-step instructions?

Use the Sage People Help Centre article on phishing-resistant MFA for privileged users and administrators. It covers identifying affected users, direct login, SSO checks, AMR/ACR, High Assurance, passkey registration and testing. Our webinar also covers this information in detail.