Two-factor authentication (2FA) FAQ

Two-factor authentication (2FA) is a simple security measure built to prevent unauthorized access to user accounts. In order to keep your business running and your data safe, it is important that each of your users' credentials are used only by those authorized users. Implementing two-factor authentication is one of simplest and most effective actions your company can take to improve security of your Salesforce deployment.

What is two-factor authentication (2FA)?
Two-factor authentication is a type of multi-factor authentication that requires two forms of validation to access an account. These two factors include something you know (e.g., a password) and something you have (e.g., a mobile device). Adding the second factor to the current password login process (which is single factor authentication) significantly reduces your vulnerability to security attacks and someone signing in to your account. Even if your password is compromised, your account is still protected. Two-factor authentication can be enabled to protect your Salesforce org(s).

What is Salesforce Authenticator and what is it used for?
Salesforce Authenticator is a mobile app, developed by Salesforce and used to provide secure two-factor authentication. You can use Salesforce Authenticator to log in to your Salesforce org, whether you log in on your desktop or mobile device.

Besides Salesforce Authenticator, how else may I enable 2FA?
While Salesforce Authenticator is the flagship 2FA solution for protecting your Salesforce org, other solutions exist as well. Salesforce supports OATH-protocol, time-based, one-time passcodes (aka TOTP) tokens, U2F protocol tokens, and temporary token generation. To learn more about 2FA at Salesforce, visit https://www.salesforce.com/2fa/

What is Verification History?
Verification history allows an admin to audit individual login requests to validate which policy
triggered the authentication process, which method was used, and the status of that request.

**What is 2FA Dashboard?**
2FA Dashboard allows admins to track the adoption of 2FA in their org. The Dashboard helps admins monitor verification challenges and Identity Confirmation events as well. Admins can install the 2FA Dashboard from [this package](#).

**What is 2FA Delegation?**
2FA Delegation allows admins to delegate 2FA administrative rights to non-admin users. This functionality enables admins to delegate specific privileges to non-admins, including the ability to generate temporary tokens for users locked out of their accounts.

**How can I increase 2FA adoption in my org?**
With 2FA Campaign, admins can use the mass email tool to invite users to adopt 2FA for their org.

**What is the difference between two-factor authentication and Identity Confirmation (IC)?**
Two-factor authentication differs from Identity Confirmation (IC) insofar as 2FA challenges users across two forms of authentication, whereas IC challenges users when logins are unfamiliar. To ensure the highest levels of trust, Salesforce strives to ensure that valid users have access to their data. As such, during the authentication process, 2FA will ask a user to authenticate their identity in two different ways (see above). However, if Salesforce does not recognize elements of the login process (e.g., your browser), then IC will ask a user to confirm their identity in an alternate channel, such as a code provided via SMS or email. If a user is enrolled in 2FA, then IC will not be required.

**What is new with the latest release of Salesforce Authenticator?**
Salesforce Authenticator has a new look and a new push notification feature to allow you to authenticate your Salesforce login with one tap. Once you set up your device with the new version, the app will send you a push notification when you log in to your org. You can approve the authentication request with one tap. You can also deny any request you don’t recognize to
keep your data safe. Using this new feature, it’s now even faster and easier to log in to Salesforce securely.

Additionally, Salesforce Authenticator now features actionable notifications. Actionable notifications allow a user to approve or deny a request without launching the mobile app. With actionable notifications, users may even respond to notifications from the lock screen of their mobile devices. Further, Salesforce Authenticator adds even more security and convenience with the added ability to approve or deny requests from your Apple Watch or Android Wear devices.

For details on the latest release, please see the release notes.

How do I install and setup the new Salesforce Authenticator version?
Start by updating or downloading the app from the App Store or Google Play Store. Next, follow the Quick Pairing Video to complete the new registration.

**Note:** If you currently use Salesforce Authenticator, just update the app on your phone. Do not delete the old app and do not delete the current “connection” of your registered account.

Can I still log into Salesforce using a token generated by Salesforce Authenticator, YubiKey, or other authenticator app?
Yes. You can still log into Salesforce using your token code generated by the Salesforce Authenticator app or your YubiKey. However, using the new Salesforce Authenticator doesn’t require any added typing on your part. Just wait for the push notification and tap Approve!

Can I use Salesforce Authenticator on any mobile device?
Salesforce Authenticator is supported on iOS and Android devices and can be installed on your mobile devices.

Can I set up Salesforce Authenticator on multiple devices?
You can register Salesforce Authenticator on multiple devices. However, please note that the push notification feature will only work on one device at a time.
Is there a Salesforce Authenticator app for desktop?
No. Salesforce Authenticator is strictly a mobile application, which provides the second factor in two-factor authentication. That means that you’ll need to have your mobile device when logging into Salesforce. If you don’t have your phone on-hand, you can still use a Yubikey as your two-factor authentication backup.

Is 2FA hard to set up?
No, 2FA at Salesforce is easy to setup, regardless if you’re an admin or a user.

From an admin’s perspective, enabling 2FA throughout the org takes a couple of minutes by creating a 2FA permission set and assigning that permission set to users, whether as groups or as individuals.

From a user’s perspective, setting up 2FA is very quick and easy. Simply follow this Quick Pairing Video to onboard. Once enabled, 2FA at Salesforce adds minimal overhead, especially if trusted locations are enabled. With trusted locations, a user may opt to automate known responses from the mobile device, if the request is the same action, from the same service, from the same user, from the same terminal, from the same trusted location (defined by mobile device).

Does traveling “break” my logins with 2FA?
Absolutely not. In fact, traveling from trusted locations reinforces the trust and flexibility of 2FA at Salesforce. If you log in from a new location, Salesforce Authenticator will prompt you to approve or deny the request as the request will be treated as an unknown location. Additionally, if you’re traveling and do not have reliable connectivity for your mobile device, simply open the Salesforce Authenticator app and use the one-time passcode associated with your account. Salesforce Authenticator has you covered even when you’re remote.

What happens if I lose my mobile device?
As always, if you lose your company-issued mobile device, contact your admin or IT service and follow company policy. However, losing, breaking, or dropping your mobile device into the toilet doesn’t spell the end of trusted access for Salesforce. With Salesforce 2FA,
admins can generate temporary tokens to enable users specific and one-time access to their accounts. Additionally, with Salesforce Authenticator v2.6 and later, users may enable the Backup and Restore feature to recover their connections on a new device from a previously enrolled device.

I have questions about two-factor authentication, where can I go to ask?
Please visit us at: https://beta.trust.salesforce.com/en/security/2fa/