

Salesforce MFA Guide

Multi-Factor Authentication (MFA) is used by many companies for security purposes, requiring users to supply an extra layer of proof when accessing an online account. In addition to a Username and password, MFA allows individuals to prove their identity using something they have in their possession. Authenticator apps are used for this purpose, eliminating the possibility of security threats targeting user credentials. While MFA is enabled, users supply something they know (password), as well as something they have (authenticator app code) prior to gaining access to an account.

Salesforce customers are now contractually obligated to use MFA when logging onto the platform. This additional layer of security reinforces the safety of company information and helps to prevent unauthorized access to user accounts. Logging onto the Salesforce platform remains quick and easy with MFA. Here's how it works...

- 1) Download an authenticator app from your store of choice (Google, Apple, etc.), or use an existing authenticator app if you have one. Salesforce has its own authenticator app, but there are other options as well.



Salesforce Authenticator 4+

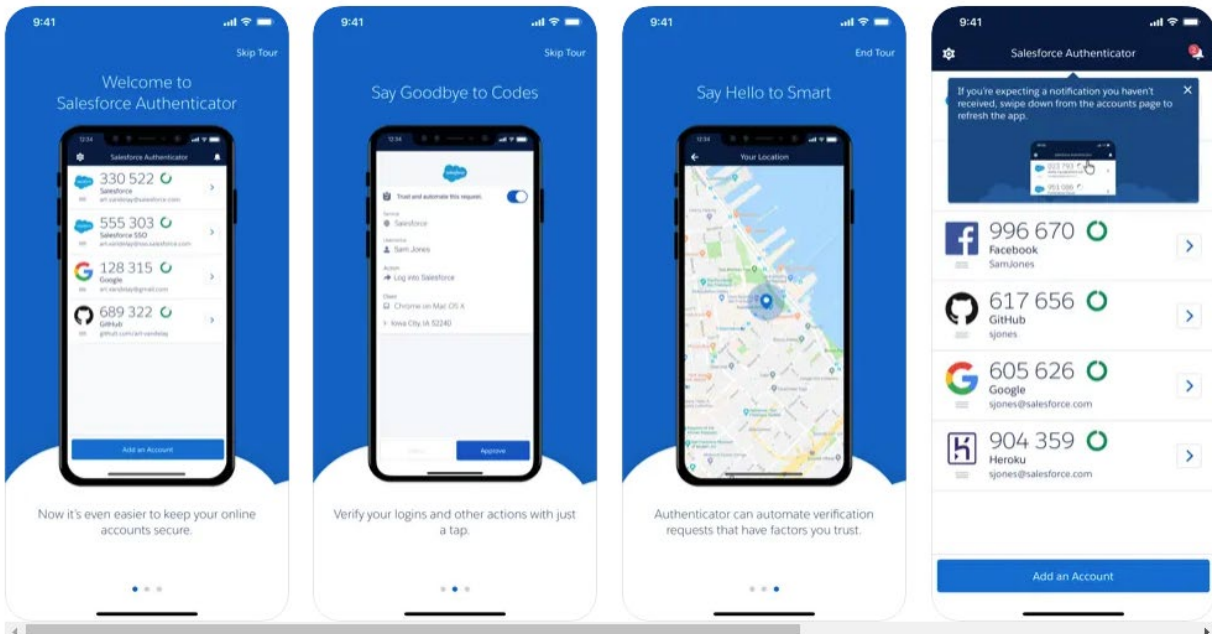
salesforce.com

#99 in Business

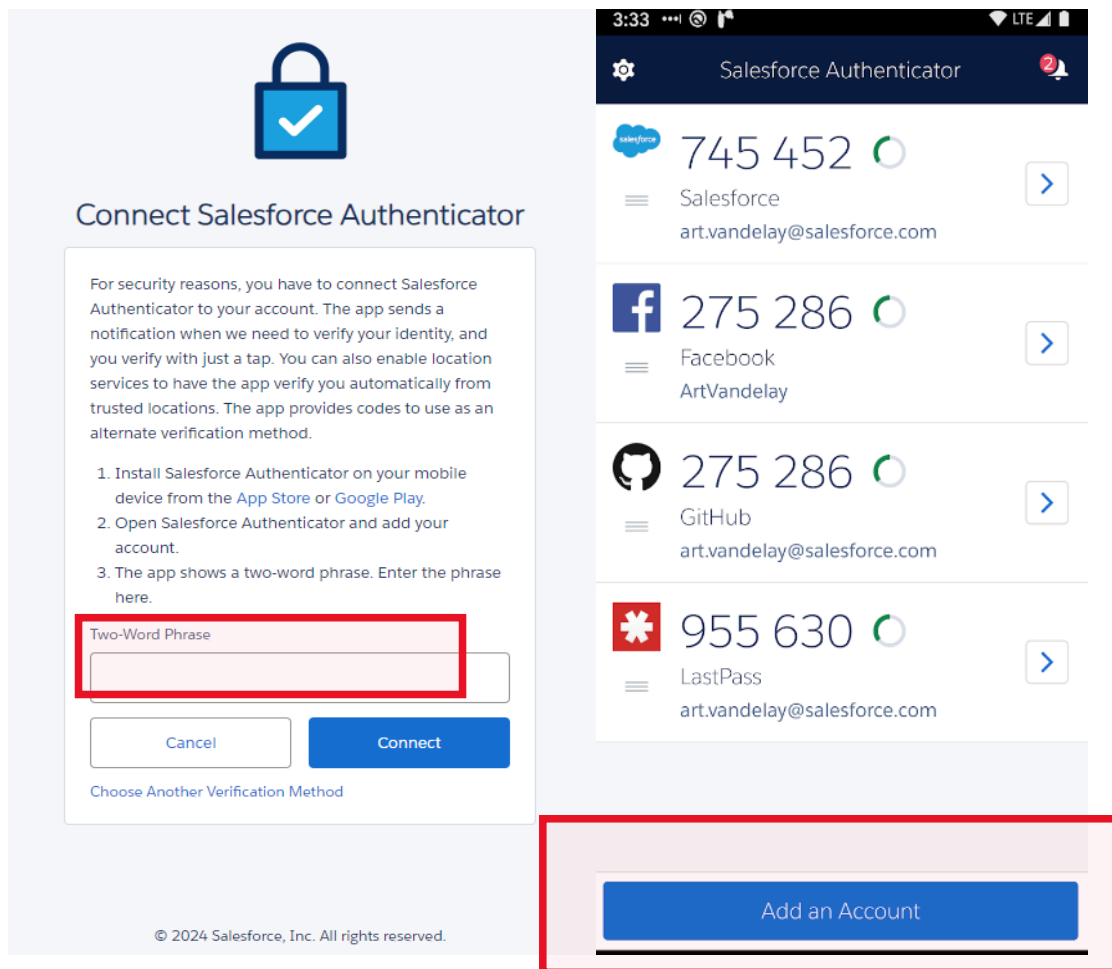
★★★★★ 4.6 • 3.4K Ratings

Free

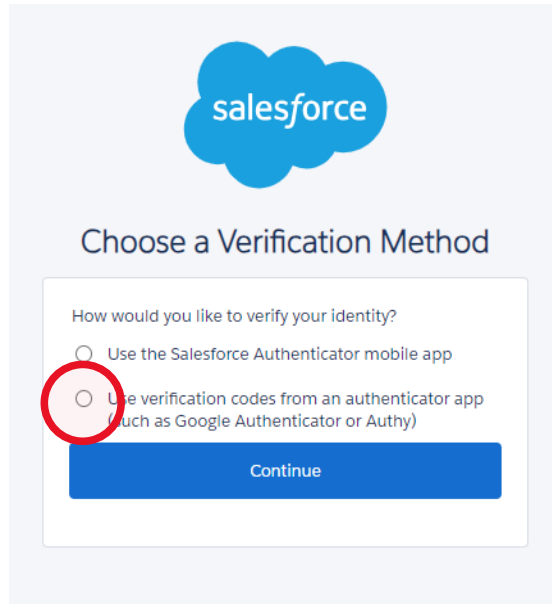
Screenshots iPhone Apple Watch



- 2) Navigate to the Salesforce login page where you enter your Username and password. After entering your user credentials, you will see a page asking for a “Two-Word Phrase” from the Salesforce Authenticator App.

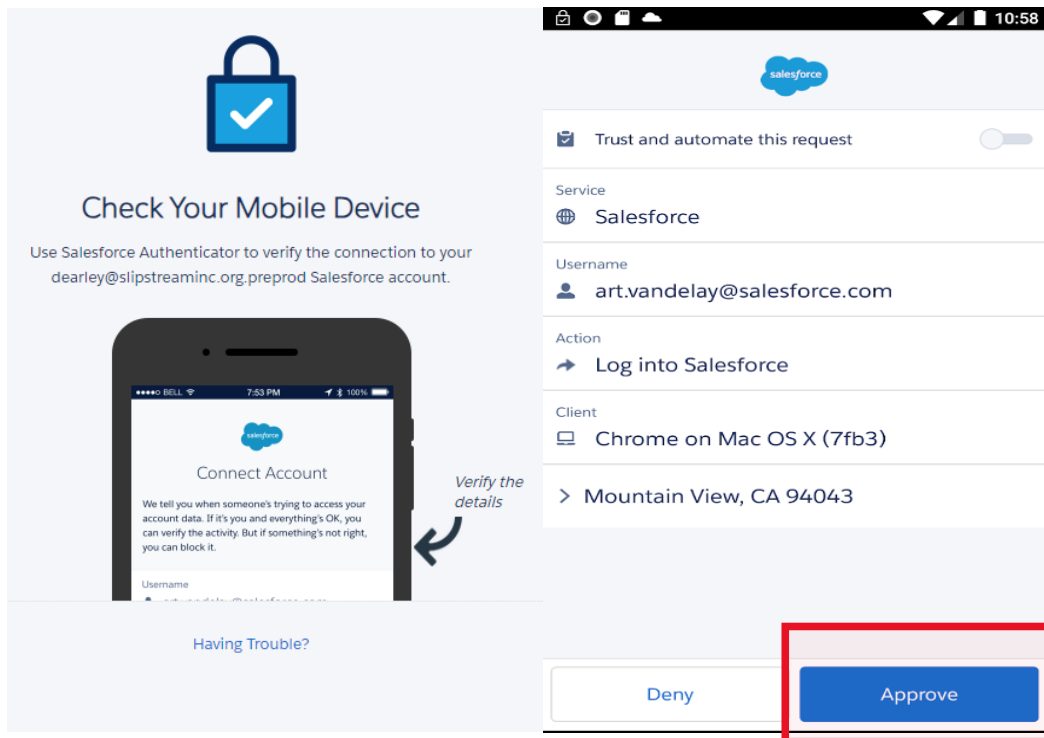


- 3a) Click “Add an Account” on your mobile device and enter the phrase provided in the Salesforce Authenticator App (continue to step 4) or select “Choose Another Verification Method” at the bottom of the screen (continue to step 3b).

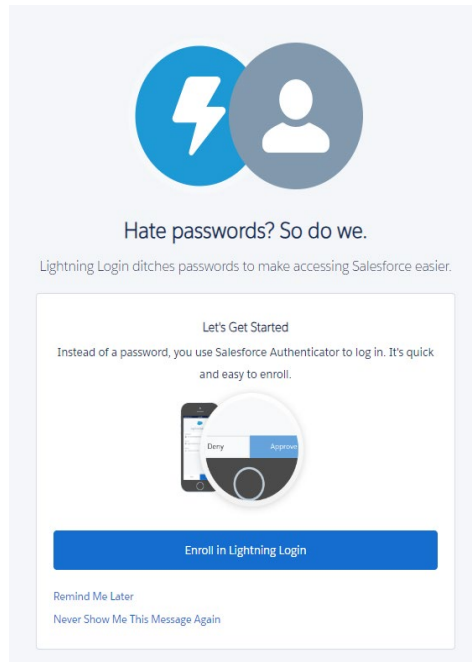


3b) After selecting an alternative, a QR code can be used on a mobile device to supply the necessary verification code and gain access to your account.

4) Using the Salesforce Authenticator App, click “Add an Account” and enter the phrase which appears on your mobile device to connect, then click the “Approve” button to continue. If you do not see the “Approve” button, click “Add an Account” a second time. You will have 90 seconds to log in using MFA, after 90 seconds the process will start over.



- 5) You should now be logged into your Salesforce account. Next time you log in, you can simply press the “Approve” button which appears in the Salesforce Authenticator App to access your account. Next, enable Lightning Login (optional) to access your account quicker.



- 6) Click “Approve” once again from your mobile device to verify Lightning Login and receive a success message. Click “Got It” on your computer to access your account. Next time you log into your account you can gain access with two clicks: once on your Username, and another on your mobile device. Remember, some users may need to click “Add an Account” to access the button for approval.

Security Tip: If you receive a request on your mobile device when not logging into Salesforce, someone else may be trying to access your account using your user credentials. MFA prevents other individuals from accessing your account by sending a notification to your mobile device through the authenticator app. Go to “Settings” in Salesforce and change your password if you believe someone else is trying to access your account.

Troubleshooting Tips

Please view the [Common MFA Authentication Troubleshooting](#) article provided by Salesforce if you are having trouble accessing your account. This article addresses the following known issues pertaining to using the Salesforce Authenticator App:

- 1) In Salesforce Authenticator the message, "This service is temporarily unavailable, please try again later." is displayed.

- 2) When logging in with MFA, a message, "The Salesforce account could not be found in Salesforce Authenticator application. If the account is deleted from the application on a mobile device, you can reconnect the account in the user settings." is displayed.
- 3) Salesforce Authenticator automatic approval (approval through trusted locations) does not function correctly.
- 4) A pop-up containing [Approve] and [Deny] is not displayed in Salesforce Authenticator, and I cannot login.
- 5) I cannot login to Data Loader using MFA.
- 6) A message, "Error: The verification code is inactive or expired. Please enter the code again," is displayed.
- 7) A message, "Error: Allowed number of retries is exceeded," is displayed and I cannot login.
- 8) There is a profile that cannot be checked in "User interface login multi-factor authentication."
- 9) How to change the Salesforce Authenticator configuration terminal.
- 10) Precautions for "changing domain" at an organization that uses "a security key" and "the built-in Authenticator."
- 11) Difference between two methods to enable MFA: configuration with "user interface login multi-factor element" permission and setting "the profile session security level to [High Assurance]", and which to be used.
- 12) I want to use a security key to login to the mobile app, but the security key is not recognized, and authentication fails.

Contact your Salesforce system administrator for the following reasons:

- 1) You are unable to disconnect MFA from a device.
- 2) You reviewed the troubleshooting documentation and are not able to log into your Salesforce account using MFA.