

Salesforce Multi-Factor Authentication for nBS

What is it?

Multi factor authentication is a way of protecting user accounts against threats with the intent of stealing the account and have unauthorized access to a Salesforce environment. This protection consists of using multiple factors as a way of identifying the true owner of the user account, this includes a user+password combination with the addition of presenting a code from an authenticator app. Email, SMS and phone calls are not a form of MFA authorized by Salesforce.

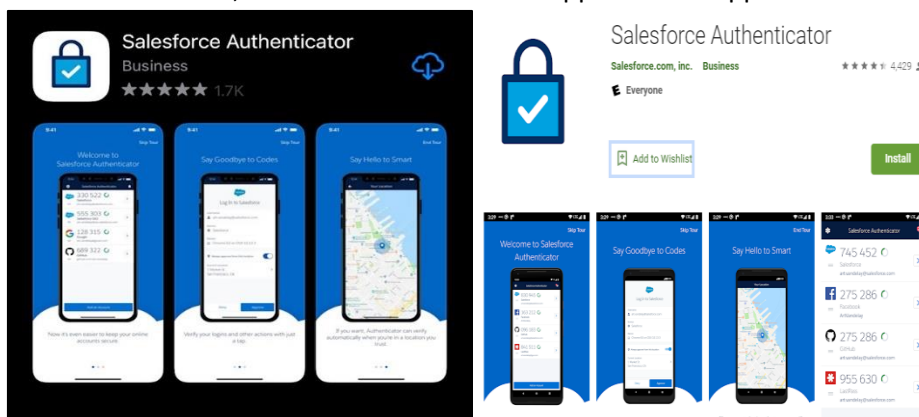
How to implement (User view)?

To ease the setup process below there are instructions on how to setup and login into salesforce after the MFA requirement has been enabled for the user. Please follow the instructions for the [official salesforce authenticator](#) below.

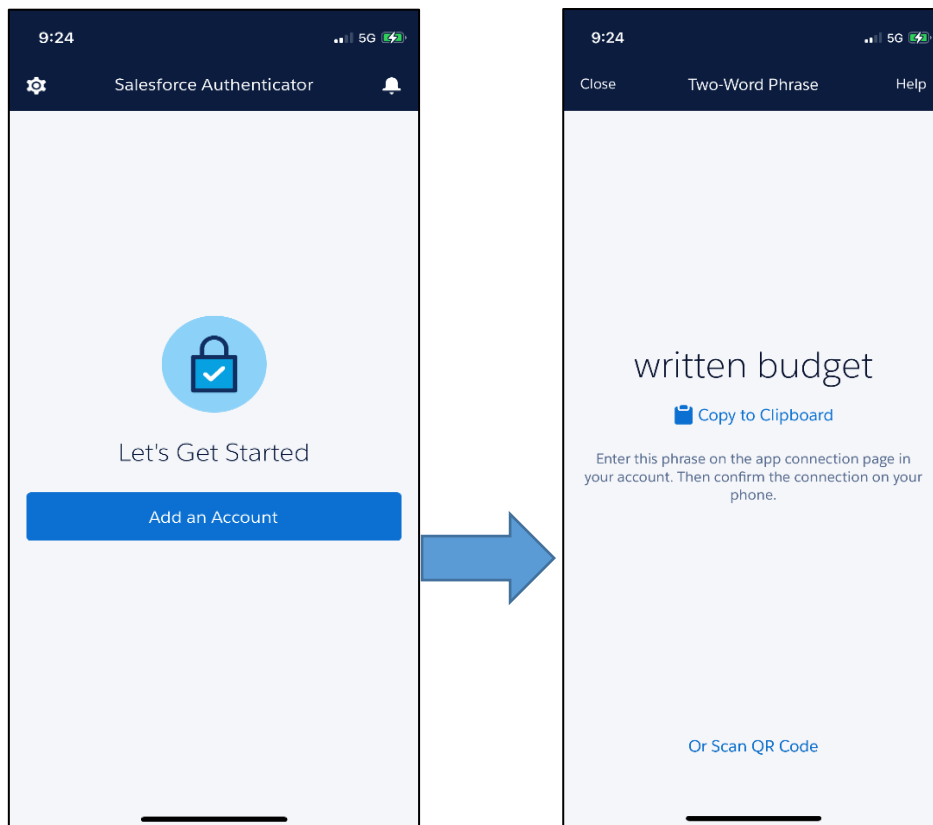
Official Salesforce Authenticator

Setup

1. On your Salesforce Instance, from your personal settings, in the Quick Find box, enter Advanced User Details, then select **Advanced User Details**. No results? In the Quick Find box, enter Personal Information, then select **Personal Information**.
2. Find **App Registration: Salesforce Authenticator**, and click **Connect**.
 - a. For security purposes, you're sometimes prompted to either log in to your account again or enter a passcode sent via email or text message.
3. On a mobile device, download and install the app from the Apple Store or Google Play.



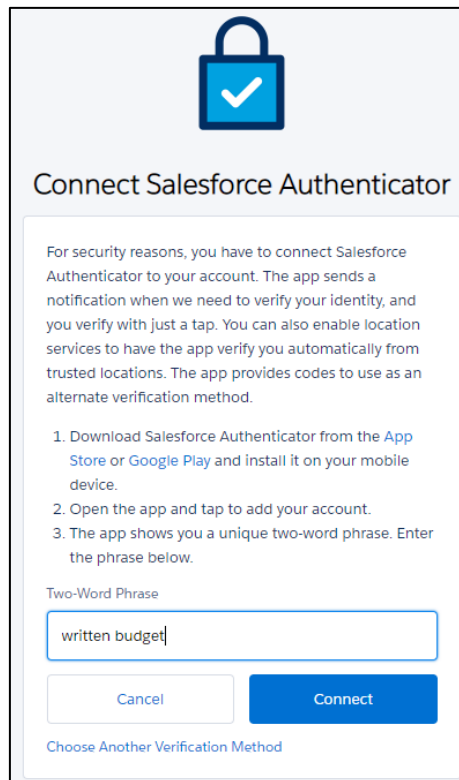
4. On your Salesforce product's login screen, enter a username and password.
5. The Salesforce Authenticator screen displays by default.
6. Open Salesforce Authenticator and tap Add an Account. The app displays a two-word phrase.



7. On the Salesforce instance, it will ask you to verify your identity by entering a code sent to your email.

The image shows a web page for Salesforce identity verification. At the top is the Salesforce logo. Below it is the heading 'Verify Your Identity'. The main content area contains a message: 'You're trying to Connect Salesforce Authenticator. To make sure your Salesforce account is secure, we have to verify your identity.' Below this message is a prompt: 'Enter the verification code we emailed to jo*****@*gi.com.' followed by a text input field labeled 'Verification Code'. At the bottom of the form are two buttons: 'Back' and 'Verify'. Below the buttons is a link that says 'Resend Code'.

8. Enter the Authenticator's phrase in the Two-Word phrase field, then click Connect.



The image shows a dialog box titled "Connect Salesforce Authenticator". At the top is a blue padlock icon with a white checkmark. Below the title, there is a paragraph explaining the security requirements for connecting the authenticator. This is followed by a numbered list of three steps: downloading the app, opening it to add an account, and entering the two-word phrase. Below the list is a text input field labeled "Two-Word Phrase" containing the text "written budget". At the bottom of the dialog are two buttons: "Cancel" and "Connect". A link "Choose Another Verification Method" is located at the very bottom.

Connect Salesforce Authenticator

For security reasons, you have to connect Salesforce Authenticator to your account. The app sends a notification when we need to verify your identity, and you verify with just a tap. You can also enable location services to have the app verify you automatically from trusted locations. The app provides codes to use as an alternate verification method.

1. Download Salesforce Authenticator from the [App Store](#) or [Google Play](#) and install it on your mobile device.
2. Open the app and tap to add your account.
3. The app shows you a unique two-word phrase. Enter the phrase below.

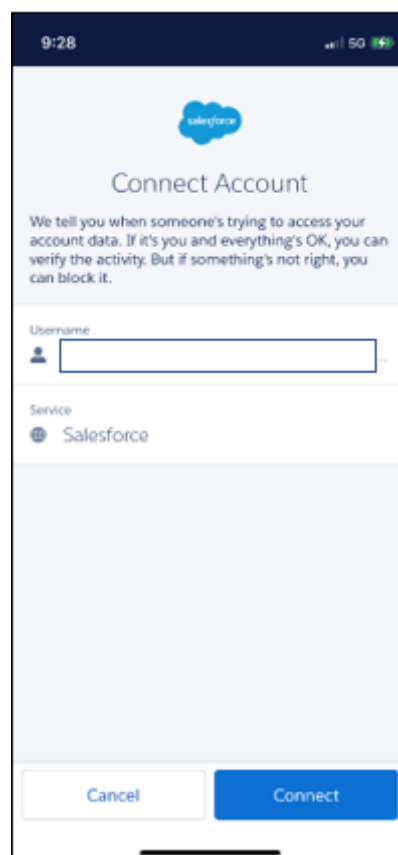
Two-Word Phrase

written budget

[Cancel](#) [Connect](#)

[Choose Another Verification Method](#)

9. On Salesforce Authenticator, verify that the request details are correct, then tap Connect.



The image shows a mobile app screen titled "Connect Account" with the Salesforce logo at the top. Below the title is a paragraph explaining the account connection process. There are two input fields: "Username" with a person icon and "Service" with a globe icon and the text "Salesforce". At the bottom are two buttons: "Cancel" and "Connect". The status bar at the top shows the time as 9:28 and 5G connectivity.

Connect Account

We tell you when someone's trying to access your account data. If it's you and everything's OK, you can verify the activity. But if something's not right, you can block it.

Username

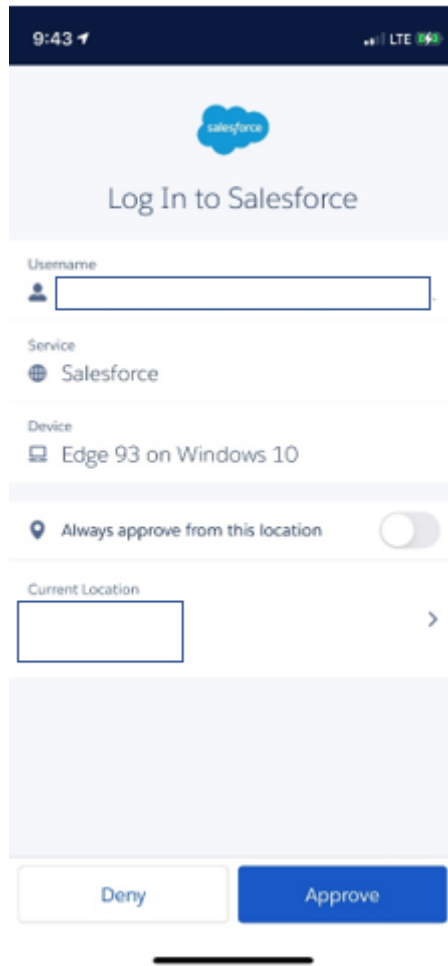
Service

Salesforce

[Cancel](#) [Connect](#)

Login

1. On your Salesforce product's login screen, enter a username and password, as usual.
2. On the mobile device, respond to the **push notification** to open Salesforce Authenticator.
3. In Salesforce Authenticator, verify that the request details are correct, then tap Approve to finish logging in to Salesforce.



After setup and logging in

After the authenticator app setup has been completed and the Log in process was confirmed to be working, from now on every time a user tries to log in to Salesforce they will be asked to approve the login or provide a one time use code after logging in with their username and password. This will only add a few seconds to the user log in experience but it will allow a stronger security for all NPower Salesforce orgs.