

MCC Multifactor Authentication Setup & Management Guide

Purpose:

This document is intended to provide end users of the Colorado Department of Health Care Policy & Financing, Member Contact Center Salesforce hosted database (MCC) guidance on the initial set up of multifactor authentication (MFA) for accessing MCC, as well as ongoing management. This guide only addresses setup and management of the Salesforce Authenticator application, which is the preferred MFA option for MCC.

What is MFA & Why Is It Important?

As the security landscape evolves & threats that compromise user credentials grow more common, it's important to implement strong security measures to protect client data.

Username & passwords alone don't provide sufficient safeguards against unauthorized account access. MFA adds an extra layer of protection against threats like phishing attacks, credential stuffing, & account takeovers.

MFA requires users to prove they're who they say they are by providing two or more pieces of evidence - or *factors* - when they log in.

One factor is something the user knows, such as their username & password combination. Other factors are verification methods that the user has, such as an authenticator application or security key.

By tying user access to multiple, different types of factors, it's much harder for a bad actor to gain entry to MCC. Even if a user's password is stolen, the odds are very low that an attacker can guess or impersonate a factor that a user physically possesses.

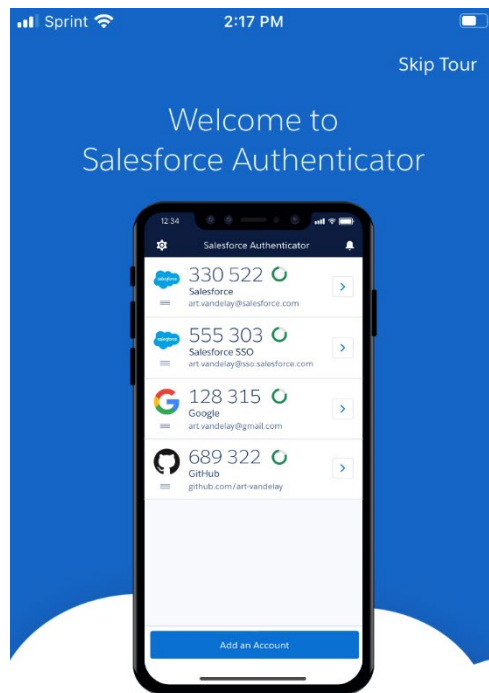
Approved Multifactor Authentication Applications

The Salesforce Authenticator application is the preferred MFA option for MCC as it provides a very seamless user experience.

However, Salesforce is compatible with any authenticator app that generates temporary codes based on the OATH time-based one-time password (TOTP) algorithm. Popular MFA options include Google Authenticator, Microsoft Authenticator, & Authy. If you, or your organization already have a preferred MFA app you may use that option to meet the MCC MFA requirement.

Initial Setup of Salesforce Authenticator Application

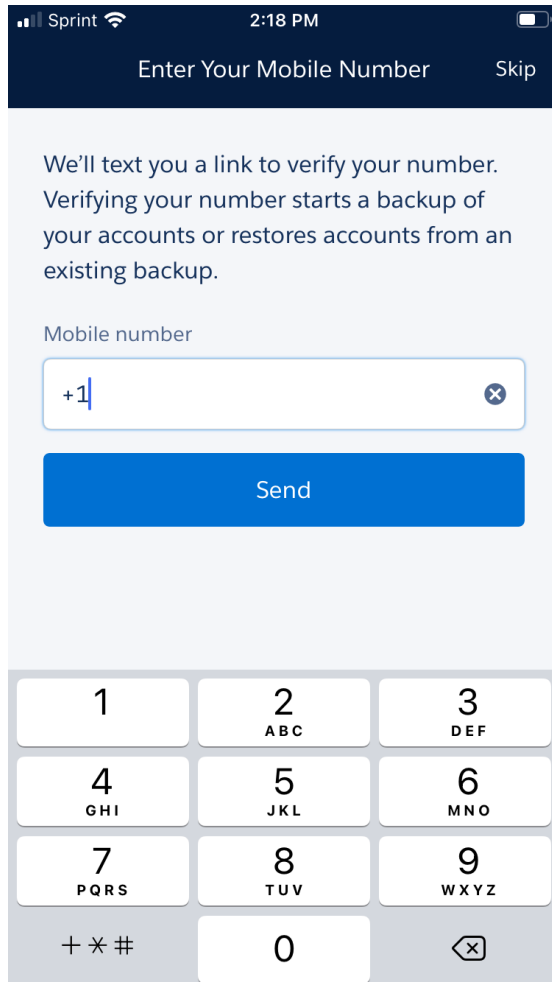
1. Download the Salesforce Authenticator application to your smartphone. The application is compatible with both [iOS](#) & [Android](#) operating systems.
 - a. If you do not have a device that you can install this, or any other MFA application on please notify your supervisor so arrangements may be made to find an alternative solution.
2. Complete the basic setup of Salesforce Authenticator on your device.
 - a. Complete brief overview tour of the application



Now it's even easier to keep your online accounts secure.

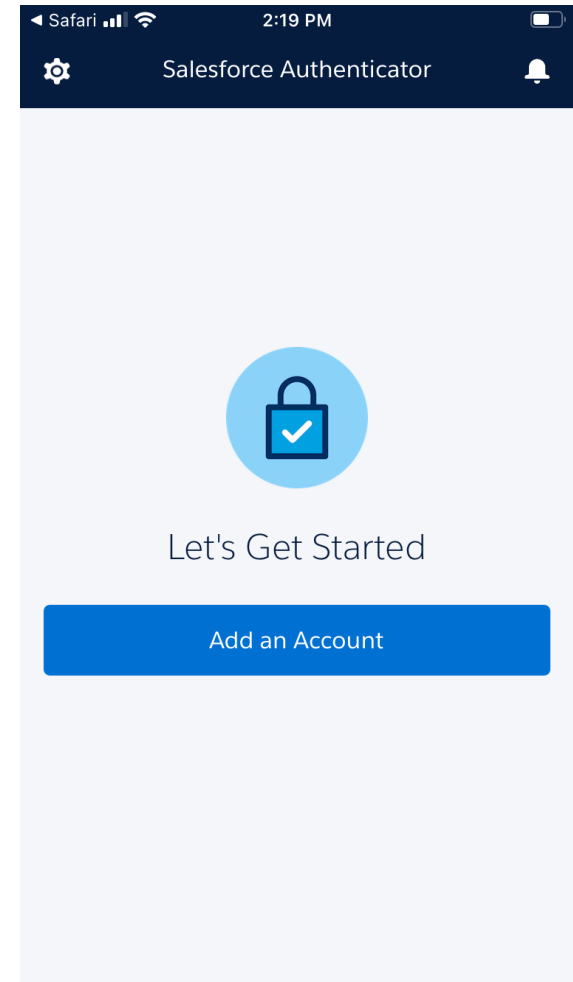


- b. Enter your phone number for the application to send a verification link to. This will be used to allow for backing up your Salesforce accounts & restoring them later if needed.



The screenshot shows the 'Enter Your Mobile Number' screen of the Salesforce Authenticator app. The status bar at the top indicates 'Sprint' and '2:18 PM'. The header has 'Enter Your Mobile Number' and a 'Skip' link. The main text says: 'We'll text you a link to verify your number. Verifying your number starts a backup of your accounts or restores accounts from an existing backup.' Below this is a 'Mobile number' label and a text input field containing '+1'. A blue 'Send' button is positioned below the input field. At the bottom is a numeric keypad with letters for numbers 2-9, and symbols for '+ * #', '0', and a backspace icon.

- c. You'll then receive a text message with the verification code, which you'll enter on a prompt screen on the application. Once that step is complete you'll see a confirmation page.



The screenshot shows the 'Let's Get Started' screen of the Salesforce Authenticator app. The status bar at the top indicates 'Safari' and '2:19 PM'. The header has a settings icon, 'Salesforce Authenticator', and a notification icon. The main content features a blue circular icon with a white padlock and checkmark. Below the icon is the text 'Let's Get Started' and a large blue button labeled 'Add an Account'.

3. Navigate to <https://hcpfccc.my.salesforce.com/> on a computer & enter your username & password to login into MCC at <https://hcpfccc.my.salesforce.com/>
4. You'll be presented with a prompt to enter two verification words.



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.

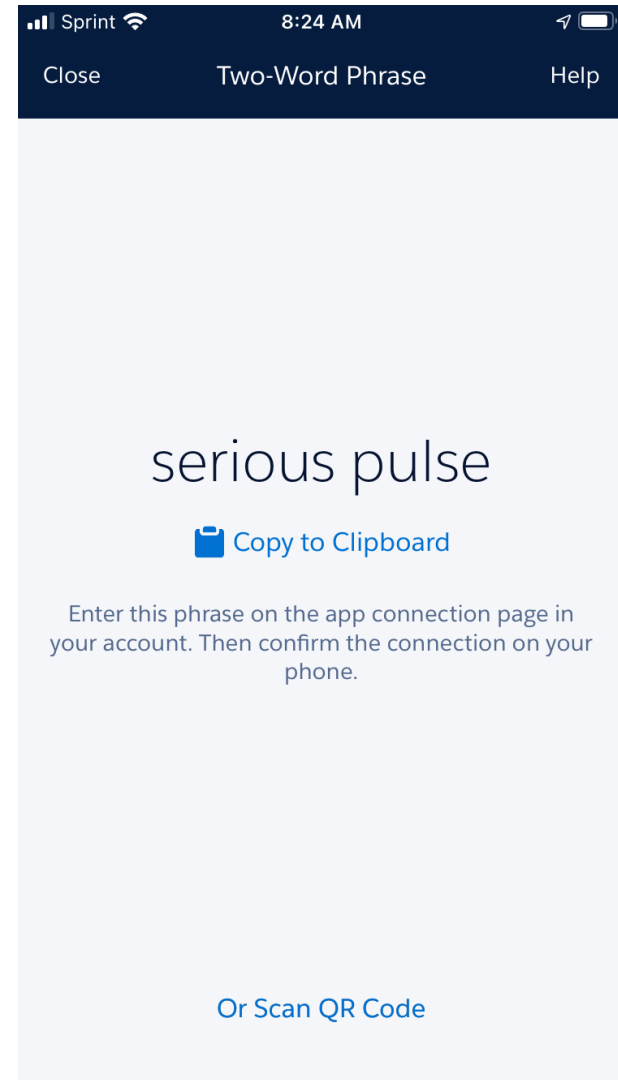
1. Download Salesforce Authenticator from the [App Store](#) or [Google Play](#) and install it on your mobile device.
2. Open the app and tap to add your account.
3. The app shows you a unique two-word phrase. Enter the phrase below.

Two-Word Phrase

[Back](#) [Connect](#)

[Choose Another Verification Method](#)

5. Go back to your application & click “Add Account” which will then provide you with two words to enter in your web browser.



Sprint 8:24 AM

Close Two-Word Phrase Help

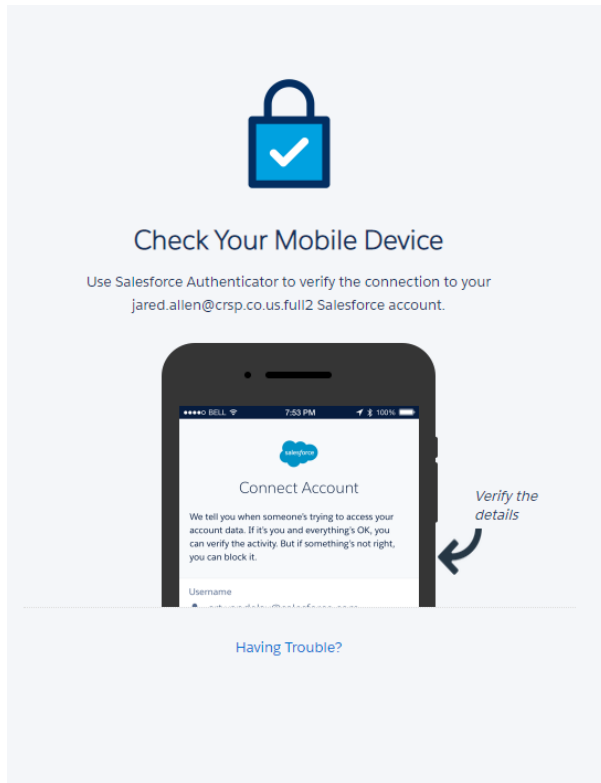
serious pulse

 [Copy to Clipboard](#)

Enter this phrase on the app connection page in your account. Then confirm the connection on your phone.

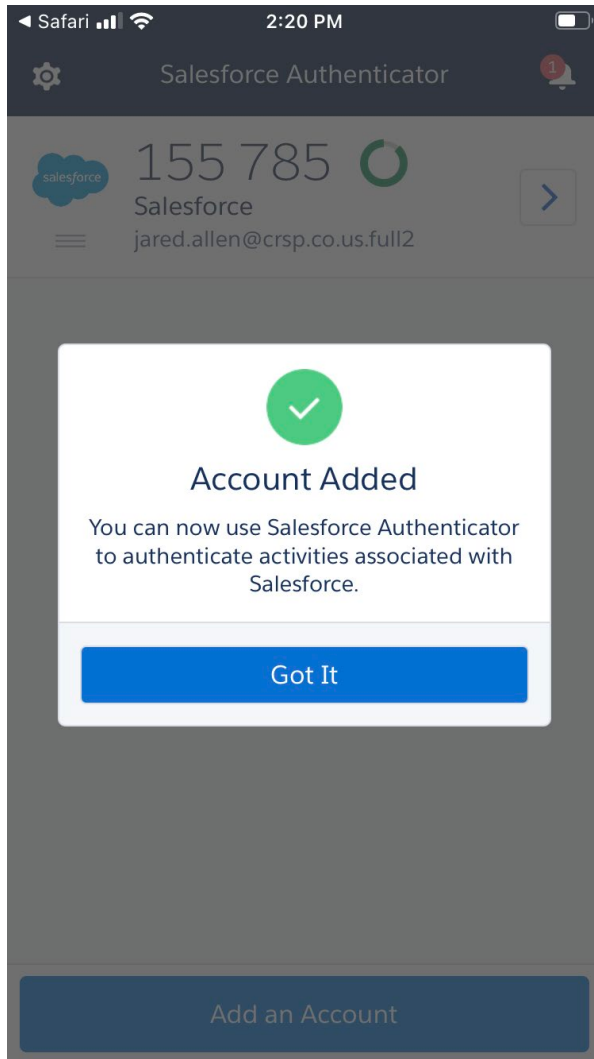
[Or Scan QR Code](#)

6. Follow the prompts in the app to confirm adding the MCC account.

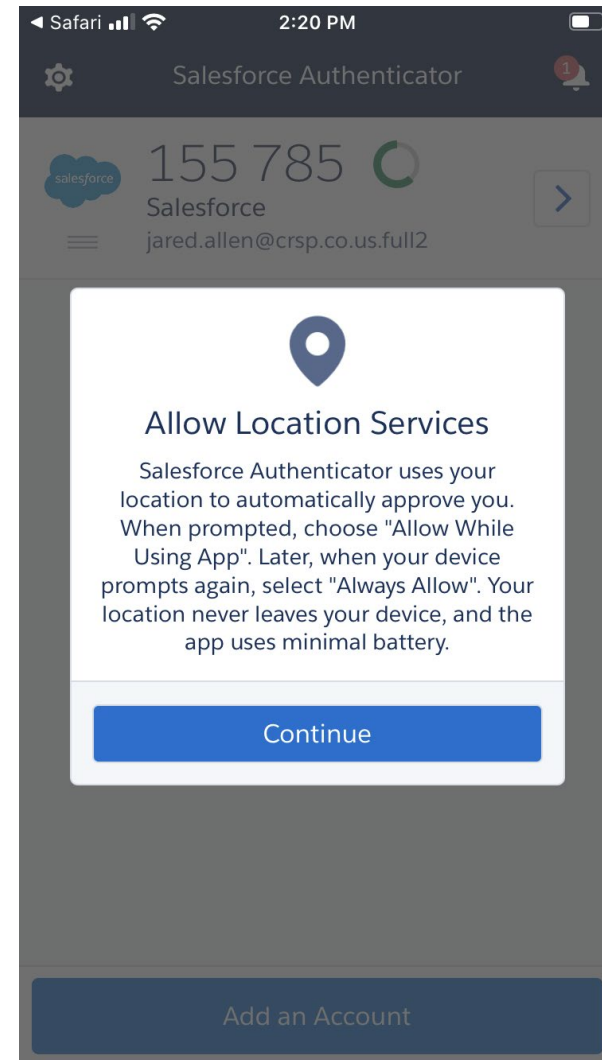


The screenshot shows the 'Connect Account' screen in the Salesforce Authenticator app. At the top is the Salesforce logo. Below it is the title 'Connect Account'. The text reads: 'We tell you when someone's trying to access your account data. If it's you and everything's OK, you can verify the activity. But if something's not right, you can block it.' Below this is a form with two fields: 'Username' with the value 'jared.allen@crsp.co.us.full2' and 'Service' with the value 'Salesforce'. At the bottom are two buttons: 'Cancel' and 'Connect'.

7. Your MCC account is now linked to the Authenticator application & is ready to use.



You can also enable location settings on your device so the application will recognize an approved location on future logins. After account creation you'll be prompted to setup this feature



8. When you login for the first time you will get an email from Salesforce 'A new verification method was added to your Salesforce account. You do not need to do anything.