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.

Usernames & 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.

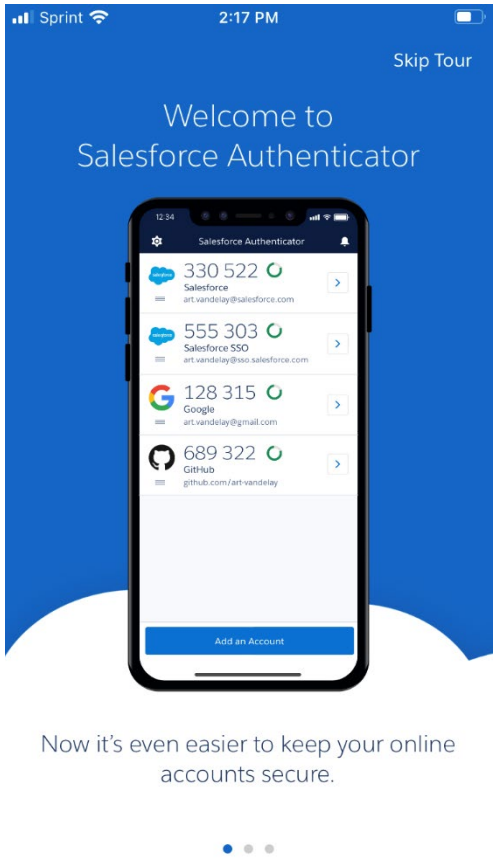
Approved Multifactor Authentication Applications

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

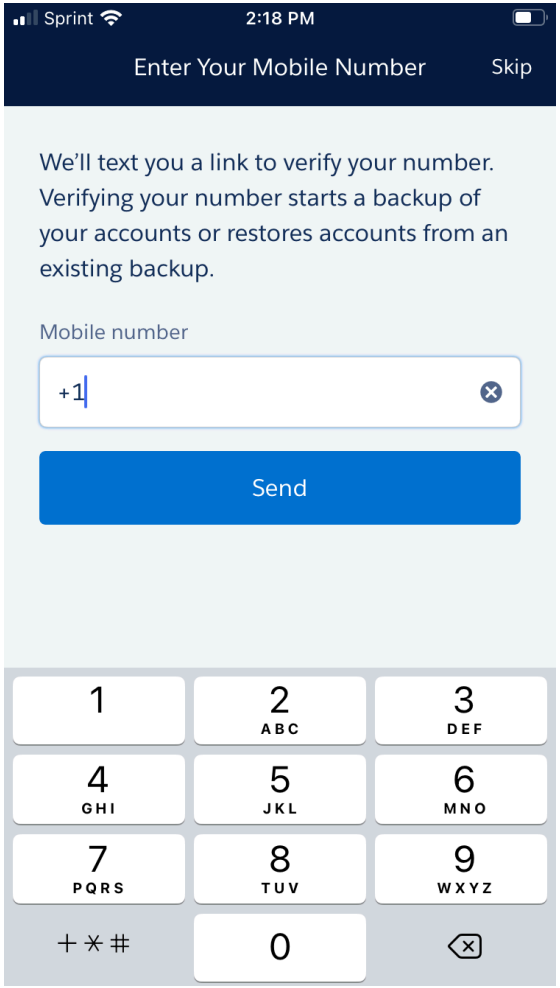
However, Salesforce is compatible with any authenticator app that generates temporary codes based on the OATH time-based one-time password (TOTP) algorithm. Popular MFA options include Google Authenticator, Microsoft Authenticator, & Authy. If you, or your organization already have a preferred MFA app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

Initial Setup of Salesforce Authenticator Application

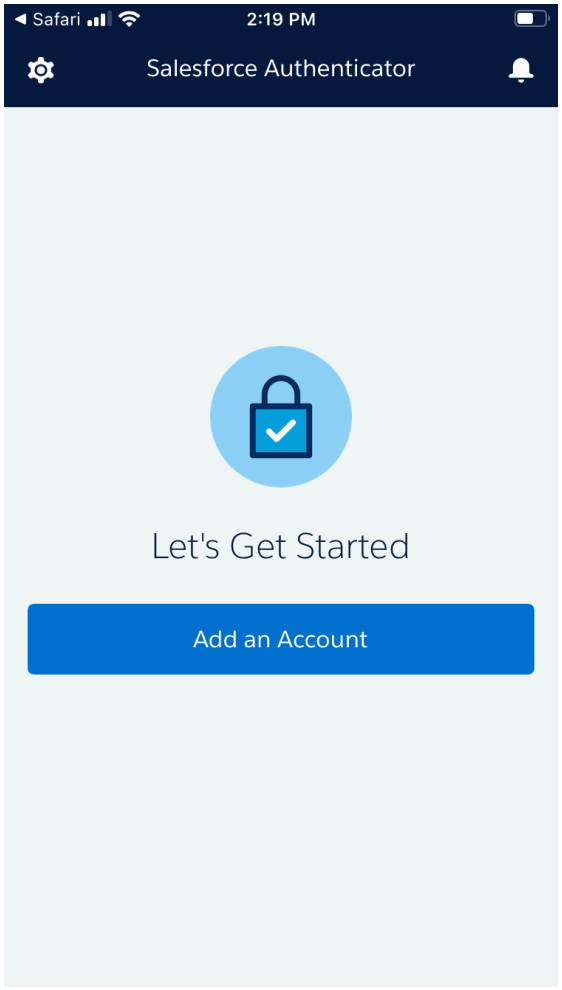
1. Download the Salesforce Authenticator application to your smartphone. The application is compatible with both iOS & Android operating systems.
    a. If you do not have a device that you can install this, or any other MFA application on please notify your supervisor so arrangements may be made to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



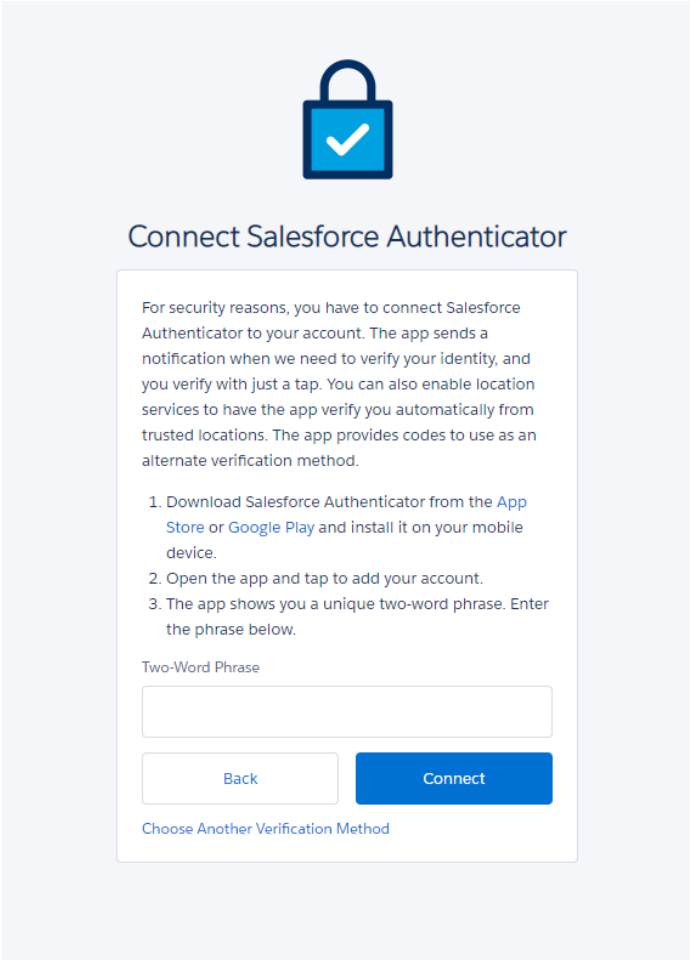
b. Enter your phone number for the application to send a verification link to. This will be used to allow for backing up your Salesforce accounts & restoring them later if needed.



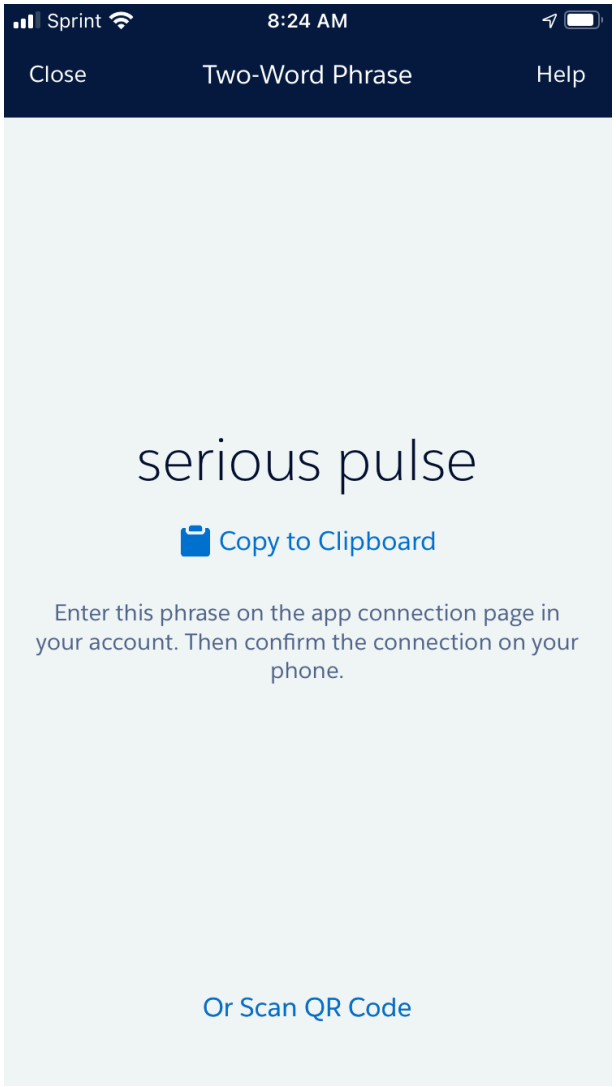
c. You'll then receive a text message with the verification code, which you'll enter on a prompt screen on the application. Once that step is complete you'll see a confirmation page.



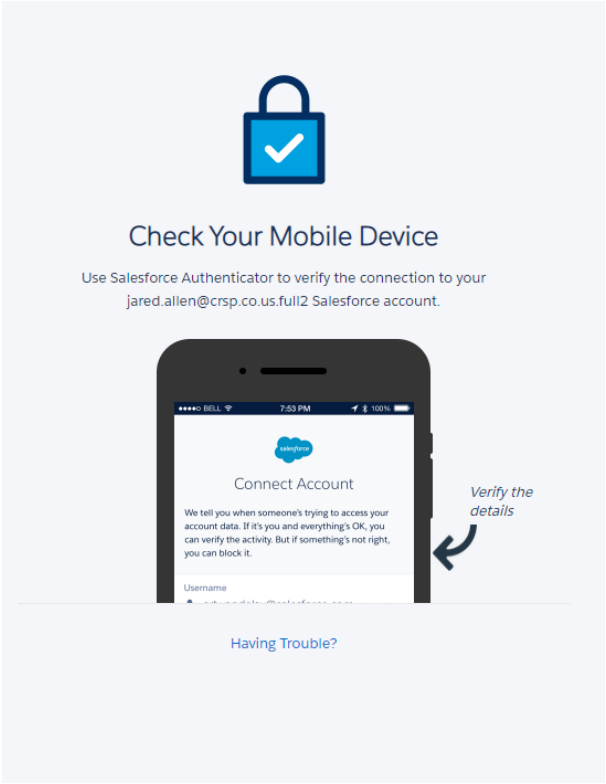
3. Navigate to https://hcpfccc.my.salesforce.com/ on a computer & enter your username & password to login into MCC at https://hcpfccc.my.salesforce.com/
4. You'll be presented with a prompt to enter two verification words.

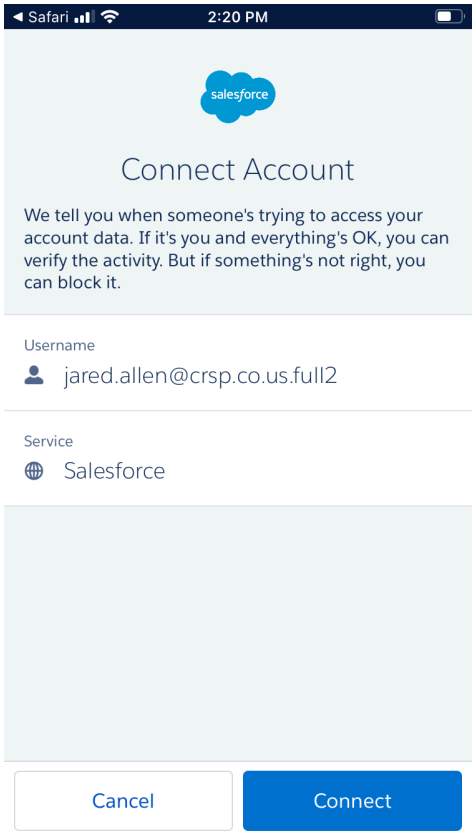


5. Go back to your application & click "Add Account" which will then provide you with two words to enter in your web browser.

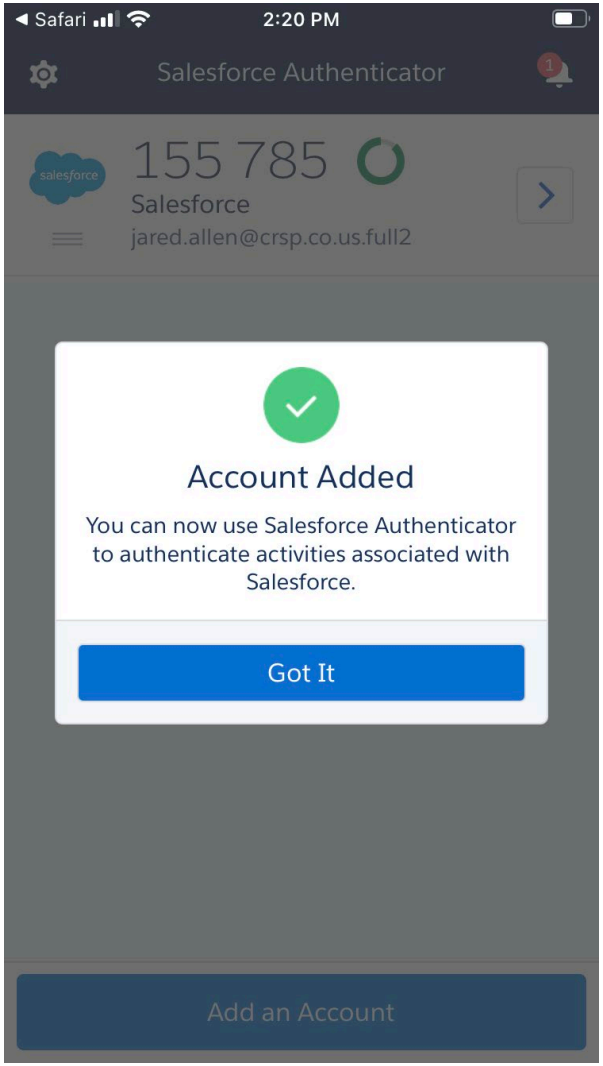


6. Follow the prompts in the app to confirm adding the MCC account.

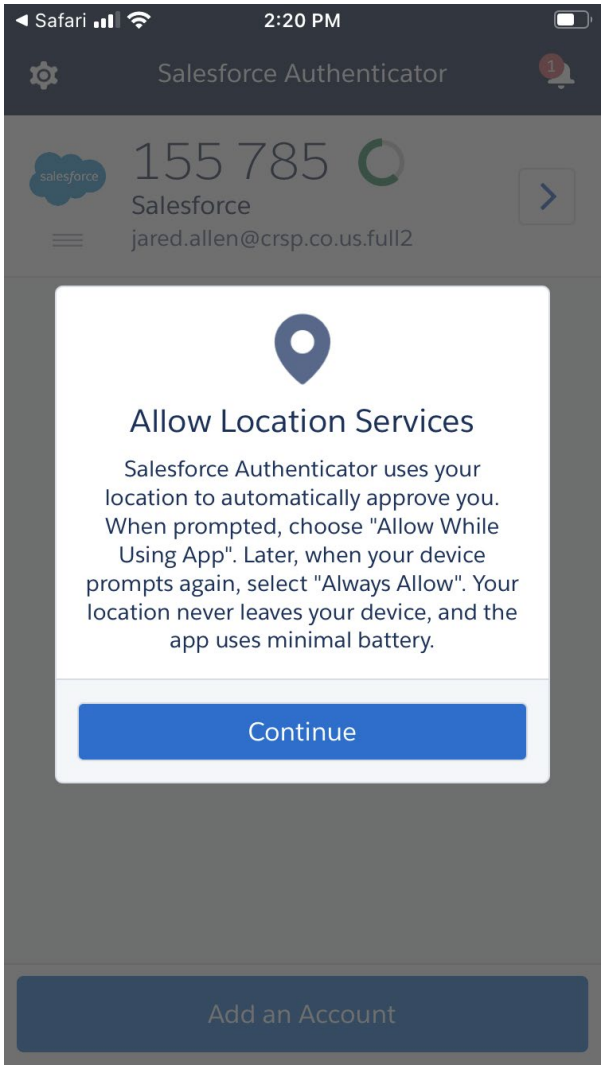




7. Your MCC account is now linked to the Authenticator application & is ready to use.



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.