How to Set Up Multi-Factor Authentication (MFA) for ClinicalConnect's Supporting Systems

Multi-Factor Authentication is required to access these supporting systems operated by the HITS eHealth Office:

1. The Access Governance System (AGS)
2. WellTracked Auditing & Surveillance System
3. ClinicalConnect-Related SharePoint Sites

What this means is that you will need to enter a Passcode, in addition to your existing username and password, every time you log into these system(s.) The Passcode is generated through an authenticator app you have, or will need to download, on your mobile device (smart phone or tablet), or from an extension for Chrome (if you don't have a mobile device to use), and the Passcode will change on your app at regular intervals. Because you need the randomly-generated Passcode each time you log into the system(s) above, it is important that you install the authenticator app and complete the steps below using a device you regularly have with you. To complete this one-time MFA set-up, please follow the instructions below.

Notes:

- This process is time-sensitive, so please do not delay.
- Using two devices is recommended where possible.
- It's also recommended you register more than one device for MFA if possible. You can add a second device later if you wish (see "Managing Your MFA Devices" later in this document).

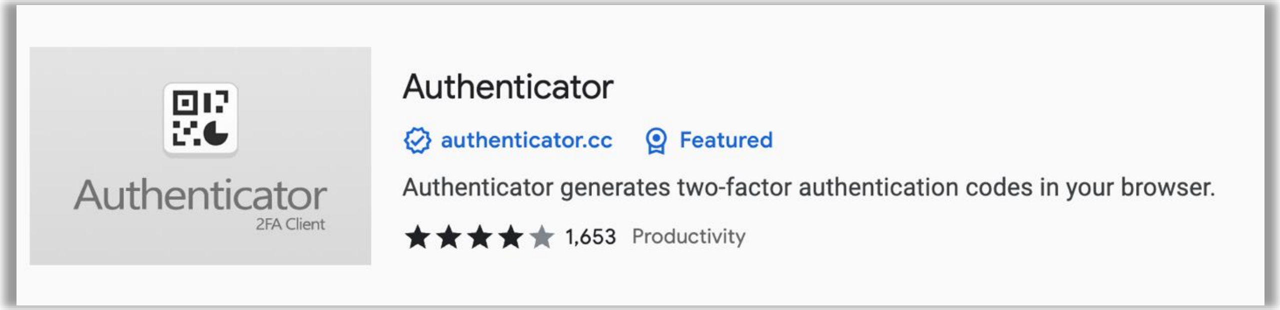
The first step is to install an Authenticator App – Option A as described below is preferred, but if you don't have a mobile device to use, see Option B.

How to Install an Authenticator App

Option A: Using a Mobile Device - On your mobile device, go to the App Store (Apple devices) or the Google Play Store (Android devices) and search for an authenticator to use. We recommend using the **"Google Authenticator"** as it is free to download and easy to use.

Note: If you already have an authenticator downloaded onto your mobile device for other purposes, such as Microsoft Authenticator, you can use it to complete the remaining steps.

Option B: Using One Desktop Device (less preferred) – Open the Chrome internet browser on your desktop computer, navigate to the **Chrome Web Store** at https://chrome.google.com/webstore/category/extensions, and search for **"Authenticator".**



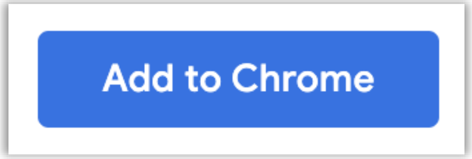
Authenticator

authenticator.cc Featured

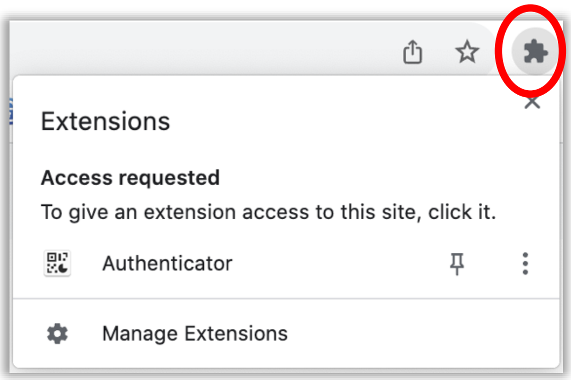
Authenticator generates two-factor authentication codes in your browser.

★★★★★ 1,653 Productivity

Open on the **Authenticator** option and click the **Add to Chrome** button to add Authenticator as an extension for Chrome.



After doing so, you can access the extension by clicking the Extensions icon (looks like a puzzle piece, per the instructions to the right) in your Chrome internet browser to enable the authenticator.


Extensions

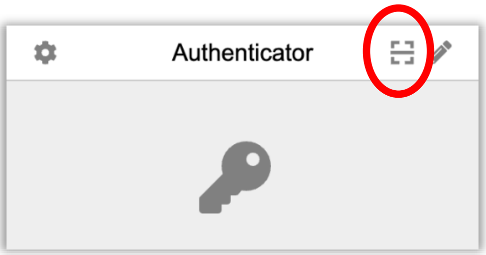
Access requested

To give an extension access to this site, click it.

Authenticator

Manage Extensions

Click "**Authenticator",** and you will see a 'scan' icon that looks like this: ⛶ . From here, go to the instructions that follow on the next page. When you see the QR code on screen (following the instructions below), you want to click that 'scan' icon and you'll be able to 'select' the QR code; this is in place of using a second device to do the scanning. Note this Authenticator Extension also gives you the ability to type in the set-up key that will also appear with the QR code in the steps that follow. If you prefer to type in the code manually, instead of clicking the 'scan' icon, click the pencil icon ✏ instead.

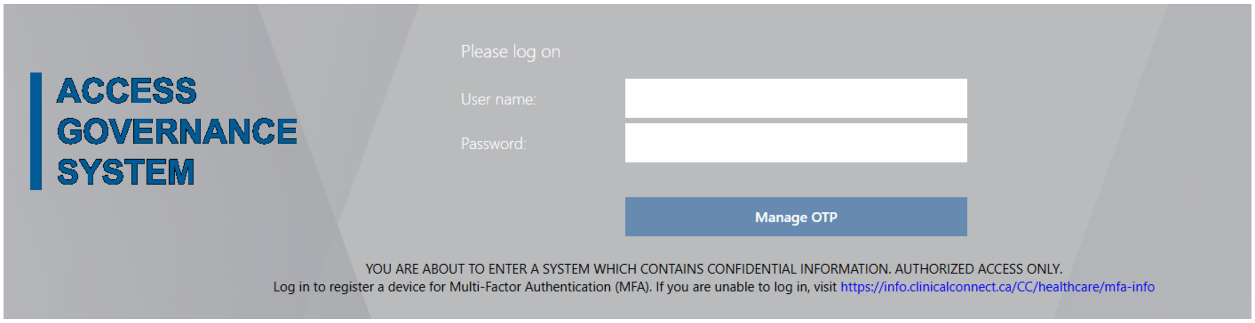


How to Register Your Device for MFA

From here, regardless if you're using a mobile device or Chrome Extension on your desktop device, the steps are the same:

1. Open the Authenticator app once it has finished installing.

2. Click **Begin Setup** (or equivalent, based on the authenticator app you're using), and it will ask you to either scan a barcode (QR code) or manually type in the entry. You can now leave your mobile device for a moment as you move onto the next step.

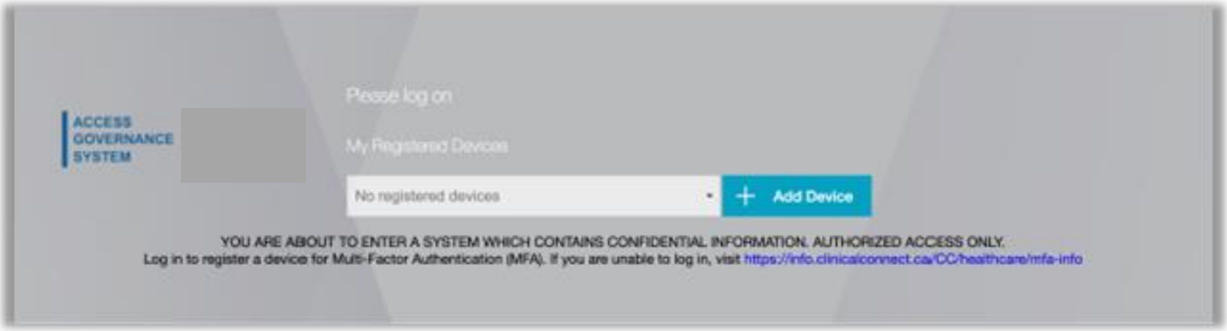


YOU ARE ABOUT TO ENTER A SYSTEM WHICH CONTAINS CONFIDENTIAL INFORMATION. AUTHORIZED ACCESS ONLY.

Log in to register a device for Multi-Factor Authentication (MFA). If you are unable to log in, visit https://info.clinicalconnect.ca/CC/healthcare/mfa-info

3. On your computer or tablet (but not the same tablet that has your authenticator app on it, if applicable, go to [https://registermfa.clinicalconnect.ca/.](https://registermfa.clinicalconnect.ca/)

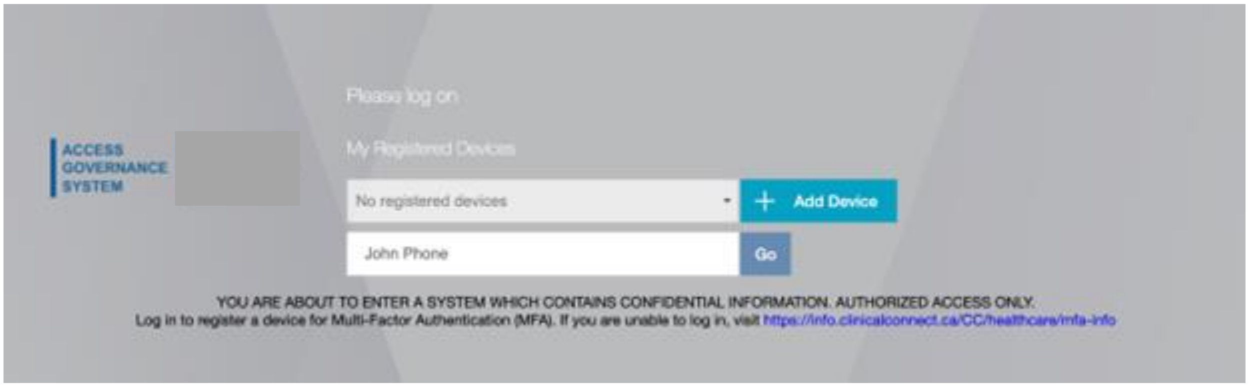
4. Enter your Username and Password normally used to access one or more of ClinicalConnect's supporting systems identified at the beginning of this document, then click **Manage OTP**.



YOU ARE ABOUT TO ENTER A SYSTEM WHICH CONTAINS CONFIDENTIAL INFORMATION. AUTHORIZED ACCESS ONLY.

Log in to register a device for Multi-Factor Authentication (MFA). If you are unable to log in, visit https://info.clinicalconnect.ca/CC/healthcare/mfa-info

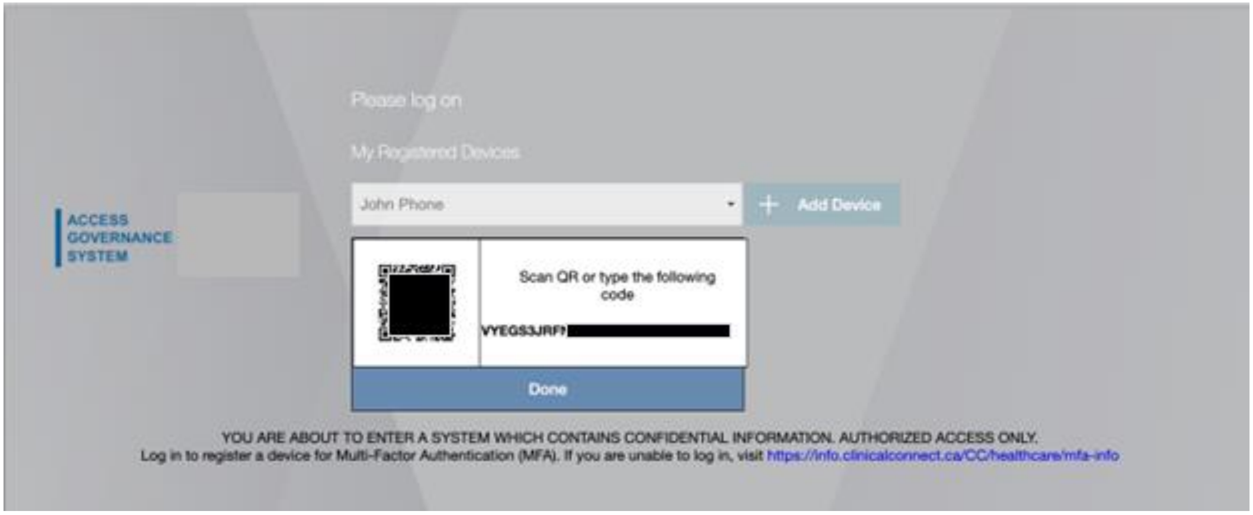
5. Since you are currently registering your first device, click **Add Device**.



YOU ARE ABOUT TO ENTER A SYSTEM WHICH CONTAINS CONFIDENTIAL INFORMATION. AUTHORIZED ACCESS ONLY.
Log in to register a device for Multi-Factor Authentication (MFA). If you are unable to log in, visit https://info.clinicalconnect.ca/CC/healthcare/mfa-info

6. Give your device a name in the field provided (i.e. a nickname), then click **Go**.

   Note: only use letters and numbers when naming your device; do not use special characters (!@#$%^&*”). A QR code and setup key (long series of letters and numbers) will appear.



Scan QR or type the following code

VYEGS3JRF [redacted]

YOU ARE ABOUT TO ENTER A SYSTEM WHICH CONTAINS CONFIDENTIAL INFORMATION. AUTHORIZED ACCESS ONLY.
Log in to register a device for Multi-Factor Authentication (MFA). If you are unable to log in, visit https://info.clinicalconnect.ca/CC/healthcare/mfa-info

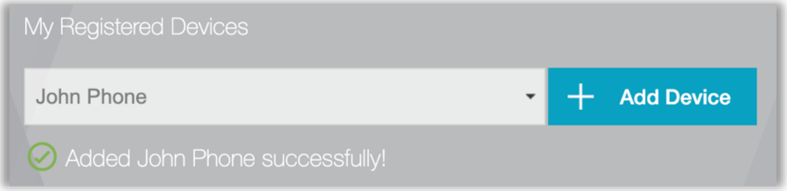
7. Open up the authenticator app that you had previously downloaded onto your mobile device, then select "Scan a QR" code in the app. You may need to "allow" access for the authenticator app to use the camera on your mobile device. Hold the mobile device up to your computer or tablet screen to scan the QR code. You will see a 6-digit code now displaying on your authenticator app, and right above the numbers, you'll see your 'account name' which is your username, followed by @registermfa.clinicalconnect.ca. ***Please do not delete this code/account as you'll need it each time you log into ClinicalConnect's ancillary systems.***

   Notes: If you are unable to scan the QR code, you can also set up your authenticator manually by typing in the setup key you see on your computer or tablet screen that accompanies the QR code.

   If you are only using one computer to complete this process, you can 'scan' the QR code using your Authenticator Extension in the Chrome browser (refer back to the bottom of page 2 of this Guide).

   Note: if scanning the QR code, be sure you're within your authenticator app; do not use your mobile device's built-in QR code scanner.

8. Click **Done**, and your device will be successfully registered.

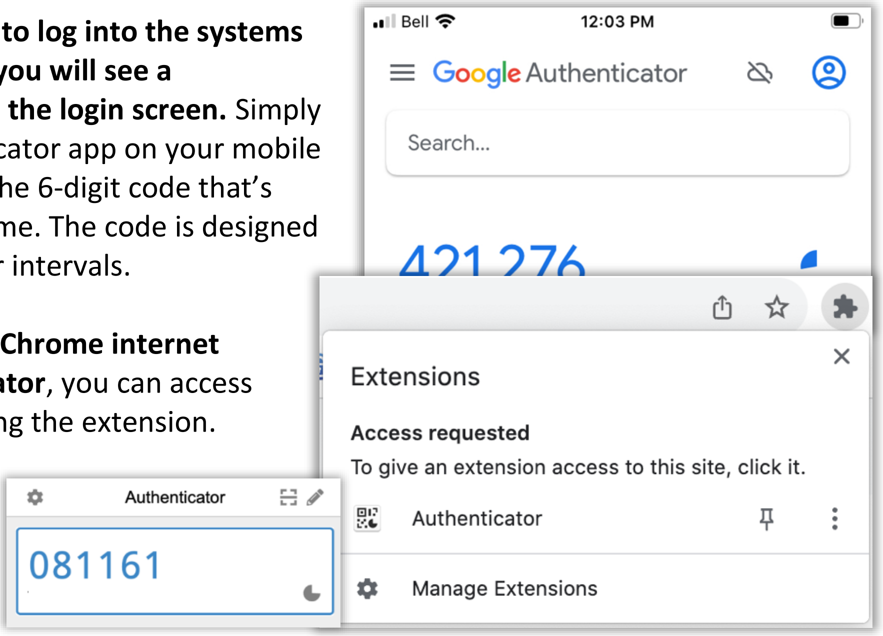


Added John Phone successfully!

9. Congratulations, your Multi-Factor Authentication set-up is now complete.

   When you attempt to log into the systems mentioned above, you will see a "Passcode" field on the login screen. Simply open your authenticator app on your mobile device and type in the 6-digit code that's displaying at that time. The code is designed to change at regular intervals.

   If you are using the **Chrome internet browser Authenticator**, you can access your code by opening the extension.



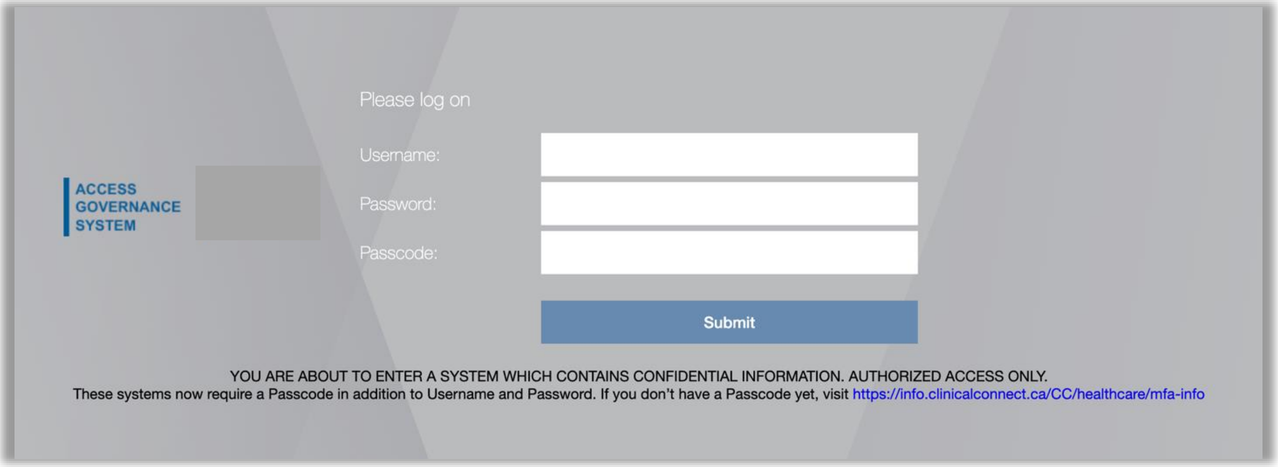
To give an extension access to this site, click it.

Managing the Devices You Registered for Multi-Factor Authentication

In the case where you want to add another device, or if you plan on replacing the device that your MFA is current set up on; you can manage this via the Manage MFA website: https://manageMFA.clinicalconnect.ca/.

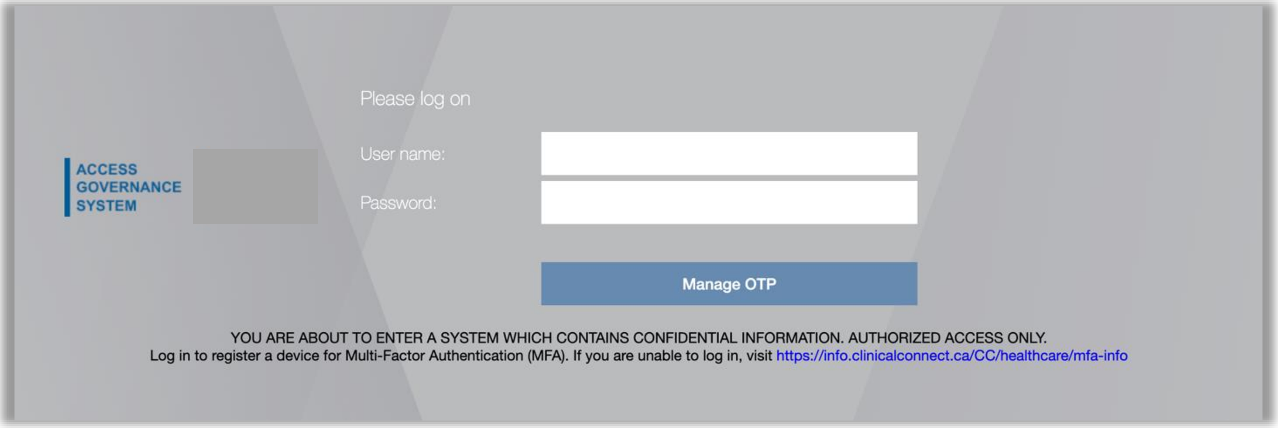
Note: you can only access this site with your existing Passcode in hand. In other words, if you lose access to the device you already registered, you will need to follow the steps outlined here https://info.clinicalconnect.ca/CC/healthcare/mfa-info in order to register a brand new device.

1. Go to https://manageMFA.clinicalconnect.ca/. Enter your User name, Password, and the Passcode from your authenticator in order to login, then click **Submit**.



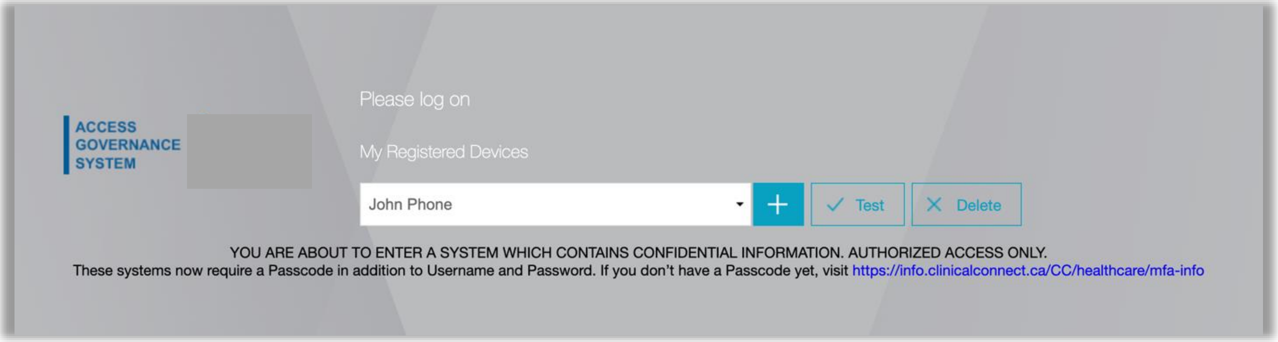
YOU ARE ABOUT TO ENTER A SYSTEM WHICH CONTAINS CONFIDENTIAL INFORMATION. AUTHORIZED ACCESS ONLY.
These systems now require a Passcode in addition to Username and Password. If you don't have a Passcode yet, visit https://info.clinicalconnect.ca/CC/healthcare/mfa-info

2. You will be prompted to log in again. Fill in your details and click **Manage OTP**.



YOU ARE ABOUT TO ENTER A SYSTEM WHICH CONTAINS CONFIDENTIAL INFORMATION. AUTHORIZED ACCESS ONLY.
Log in to register a device for Multi-Factor Authentication (MFA). If you are unable to log in, visit https://info.clinicalconnect.ca/CC/healthcare/mfa-info

3. When logged in you will be able to add a new device, test an authenticator that is already set up, or delete a registered device.



YOU ARE ABOUT TO ENTER A SYSTEM WHICH CONTAINS CONFIDENTIAL INFORMATION. AUTHORIZED ACCESS ONLY.
These systems now require a Passcode in addition to Username and Password. If you don't have a Passcode yet, visit https://info.clinicalconnect.ca/CC/healthcare/mfa-info