Introducing Multi-Factor Authentication (MFA) to the CAFT System

FAQs

November 24, 2023

What is MFA and why is it important?

Multi-factor Authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to an application or an online account. MFA provides strong identity and access management to help protect your online accounts and information. MFA requires one or more verification factors in addition to a user ID and password which decreases the likelihood of a successful cyber attack.

How will MFA change my CAFT login experience?

The introduction of MFA will change how you log into CAFT and is an important step for enhancing the cybersecurity of your account. The CAFT system itself is not changing.

Using MFA is common and quite simple. In essence, it is like having to login twice.

Once MFA is in place, CAFT users will still use the same URL (web address) to navigate to the system. However, you will first see a dialogue box entitled “Welcome to CAFT’s new authentication process.” ALWAYS check that the URL you are at is correct. Login with your usual user ID and password. The system will then ask you to input a code provided by the MFA app that you will have installed on your mobile phone.

What MFA tool should I use?

Servus cannot advise on which tool is right for you or your organization. Microsoft Authenticator or Google Authenticator are just two examples of products that are widely available on the Google and Apple app stores have support directly from the provider. However, the CAFT system will work with any MFA. The MFA will work with iOS or android smartphones or tablets. The apps are free and secure.

What support will be available to help me start with MFA?

A support package for CAFT users will be shared in advance of the MFA roll out.

We have a shared user ID for CAFT, what do we do?

Under the new CAFT multifactor authentication (MFA) login process, shared user IDs will no longer be possible, as each user must login by providing an authentication code from an app installed on their device. We will create unique, individual user IDs for each staff member. Please summarize the following information for you organization:

- How many new user IDs are required, and the type of user IDs required
- The 'parent' (or current) user ID, and who the user ID is assigned to
- The first and last name of each new user

Send the information to BusinessServices@Servus.ca

If you have no shared IDs, please email so we know there is no need to follow up with your credit union on this issue. We will provide the new user IDs and access credentials for your staff as quickly as possible upon receiving this information.

There will be no cost associated with creating these additional user IDs.

When will MFA be implemented for all CAFT users?

The pilot testing program is expected to run with several organizations before the end of November. The final timing of the launch for all CAFT users will depend on the results of the pilot. We will keep you informed of the progress and timing as this information becomes available. Please note we expect this to transpire quickly and urge you to prepare by setting up MFA for all users in your organization now.

Where can I get more information?

Resources are available and will continue to be updated on the Servus website. The URL has been obscured to make it difficult for threat actors to find: https://servus.ca/business/caft-system-security-update

For support, contact your advisor or BusinessServices@servus.ca