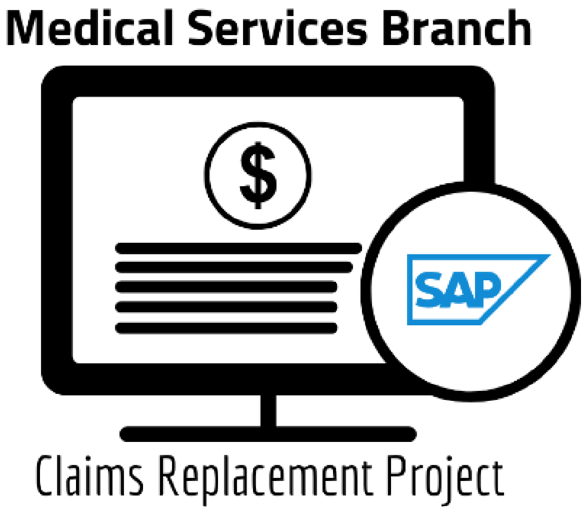
Signing into Customer Portal with Multi-Factor Authentication (MFA)

User Manual



saskatchewan.ca

Saskatchewan

Table of Contents

Module ONE: Overview

Learning Objectives

Upon completion, learners will have an understanding of:

- What MFA is?
- Why is it required?
- How to use MFA?

Getting Started

Authorized users of Customer Portal include all users who will access Customer Portal over the internet. To ensure only authorized users gain access to Customer Portal, eHealth Saskatchewan Security requires Multi-Factor Authentication (MFA).

Logging In to Customer Portal

Once fully registered in the Physician Registry (this includes having your direct email address registered with your profile), a welcome email and password reset email will be sent to you. Follow the prompts to reset your password to login to Customer Portal. Your userid will be your registered email address. The password you personally set must conform to eHealth Saskatchewan password complexity policy to be accepted.

Multi-Factor Authentication (MFA)

Logging onto the Customer Portal for the first time will also trigger the **Multi-Factor Authentication (MFA**) process.

What is MFA?

Multi-factor authentication (MFA) is **a multi-step account login process that requires users to confirm their identity beyond simply a valid and active userid and password.** The second step triggers an authentication through a mobile device associated with the user account.

Module ONE: Overview

Why use MFA?

Traditionally, logging into applications required only a username and password to access an application. In the case where someone who has not been granted credentials to log in to an application obtains the credentials of an authorized user, there is a risk of unauthorized individuals being able to access the application. To reduce the risk of unauthorized persons accessing a system, multi-factor authentication is being implemented. This requires a second ‘layer’ of authentication to occur, using a mobile device of the authorized user. The two-step process to authenticate and log in has been developed to ensure you are who you say you are. This is similar to the log in process at most financial institutions, government agencies and many web-based applications.

MFA provides robust protection by adding an additional layer of security beyond passwords. It is designed to safeguard you, the user, the company, and the integrity of the system by mitigating risks of credential theft and attacks from hackers and unwanted persons. MFA is a generally recognized and (now) widely implemented cyber security method of securing internet-accessed applications.

How does it work?

On your first login to Customer Portal, you will be prompted to enter a second, unique code that is generated either by an **Authentication App** or by requesting a one-time passcode (OTP) through **SMS** on a mobile device. On the initial log-in, you will also specify a mobile device phone number with your account, which cannot be changed by another person (securing your mobile device to your account).

Do I have to go through the MFA process each time I login?

No, you will not have to go through the MFA process each time you log in.

MFA will trigger when:

- The user logs in from a different device (this includes a different device within the office, at home or when a new laptop or desktop computer is purchased) .
- The user logs in from a different location.
- The login location differs from the previous login location and the system determines there was ‘impossible travel time’ (i.e., given the time/date of the last login location, is it feasible the same user could be logging in again at a different location).
- The login is from a known untrusted IP Address.

The MFA challenge is only invoked when there are changes to previous logins detected.
If you are logging in from a previously authenticated location/device (laptop),
the additional step of an MFA challenge is not triggered.

Module TWO: Getting Started

Learning Objectives

Upon completion, learners will have an understanding of:

- Logging into Customer Portal,
- Activating MFA,
- Resetting Passwords

Overview

All users are required to set up the MFA Authenticator on the very first login to Customer Portal. After the initial set up:

- **External Users** (i.e., Physicians, Billing Clerks, etc.) will receive the MFA Challenge when the adaptive MFA detects a sign in from a different laptop/desktop.
- **Internal Users** will not be presented with the MFA Challenge after the initial setup as they will access Customer Portal through the firewall.

How do I receive my MFA passcode?

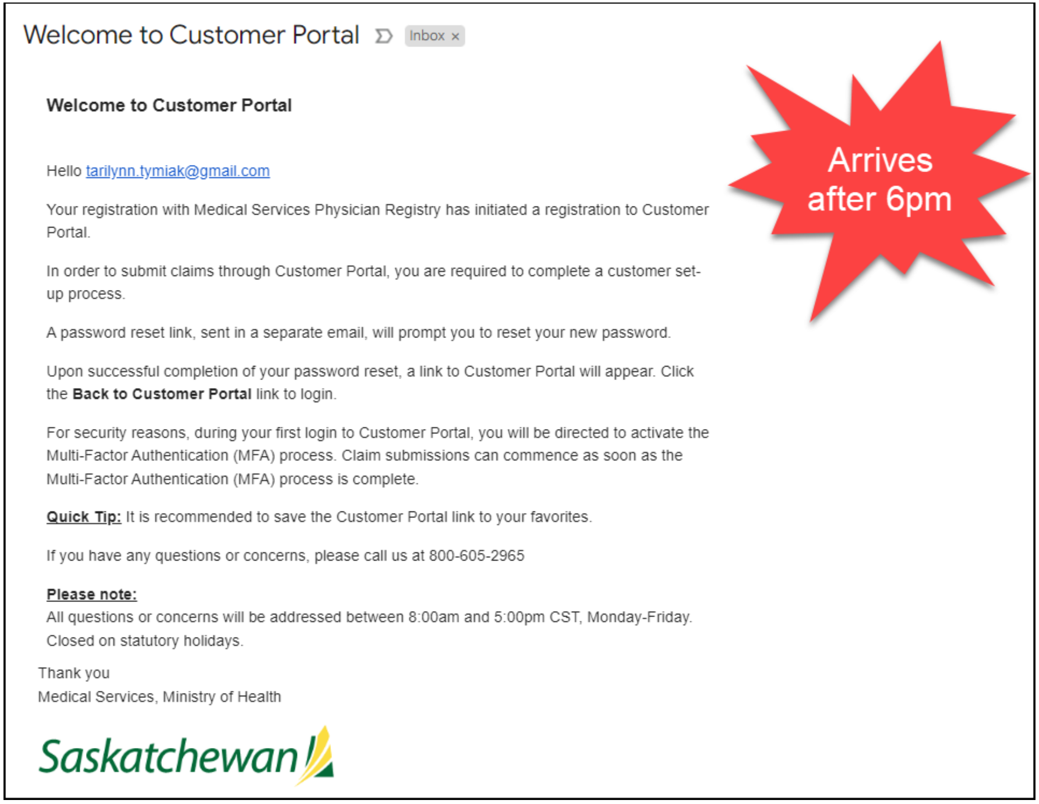
You can receive your MFA passcode in one of two ways:

- Unique code generated by authenticator app (Google or Microsoft)
- SMS (text message) sent to mobile number associated with the USERID.

The MFA Authenticator method chosen on the initial login cannot be changed later.
In other words, if the Authenticator App is first selected, the user cannot
change to SMS for future logins or visa-versa.

Welcome Email and Password Reset Email

Two emails will be sent to the email address registered in the Physician Registry. The first is a welcome email and arrives AFTER 6pm on the day your account is activated. This email often lands in the spam folder.



Welcome to Customer Portal Inbox ×

Welcome to Customer Portal

Hello tarilynn.tymiak@gmail.com

Your registration with Medical Services Physician Registry has initiated a registration to Customer Portal.

In order to submit claims through Customer Portal, you are required to complete a customer set-up process.

A password reset link, sent in a separate email, will prompt you to reset your new password.

Upon successful completion of your password reset, a link to Customer Portal will appear. Click the **Back to Customer Portal** link to login.

For security reasons, during your first login to Customer Portal, you will be directed to activate the Multi-Factor Authentication (MFA) process. Claim submissions can commence as soon as the Multi-Factor Authentication (MFA) process is complete.

Quick Tip: It is recommended to save the Customer Portal link to your favorites.

If you have any questions or concerns, please call us at 800-605-2965

Please note:
All questions or concerns will be addressed between 8:00am and 5:00pm CST, Monday-Friday. Closed on statutory holidays.

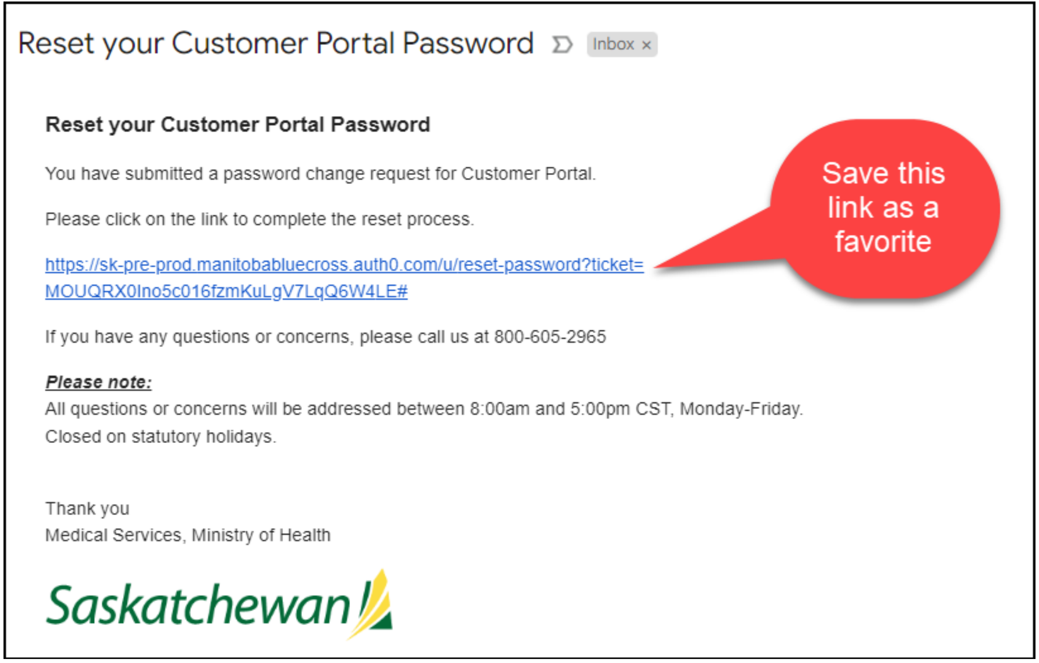
Thank you
Medical Services, Ministry of Health

Saskatchewan

Arrives after 6pm

The welcome email and password reset email may appear in your Spam/Junk folder.

The second email includes a link to reset your password. Click the link and follow the prompts to reset your password.



Reset your Customer Portal Password Inbox ×

Reset your Customer Portal Password

You have submitted a password change request for Customer Portal.

Please click on the link to complete the reset process.

https://sk-pre-prod.manitobabluecross.auth0.com/u/reset-password?ticket=MOUQRX0Ino5c016fzmKuLgV7LqQ6W4LE#

If you have any questions or concerns, please call us at 800-605-2965

Please note:
All questions or concerns will be addressed between 8:00am and 5:00pm CST, Monday-Friday.
Closed on statutory holidays.

Thank you
Medical Services, Ministry of Health

Saskatchewan

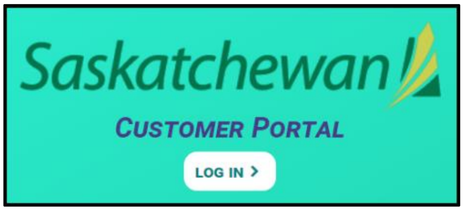
Save this link as a favorite

Login to Customer Portal

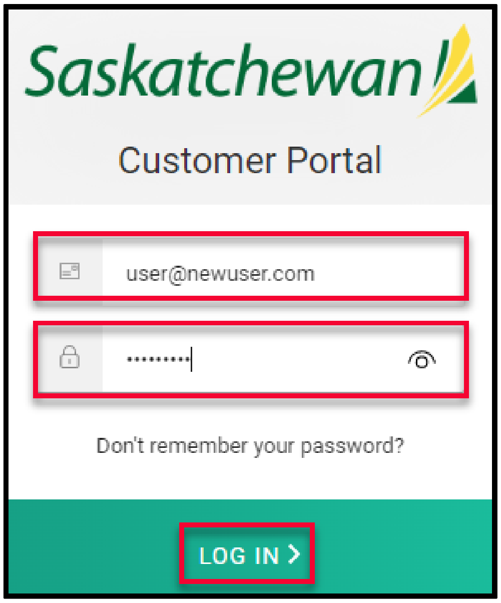
Regardless of the option you choose to use for MFA, you will first have to log into Customer Portal.

1. Open the **Customer Portal** application.

2. Click on **Log in.**



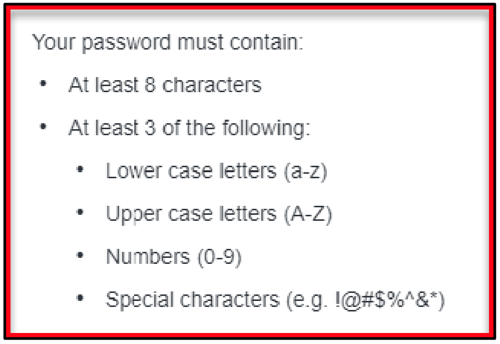
3. Enter your **Username** (your email address registered on your profile).



user@newuser.com

••••••••••

4. Enter a new **Password**, then click **Login.** Your new password must follow the below guidelines.



Your password must contain:

- At least 8 characters
- At least 3 of the following:
  - Lower case letters (a-z)
  - Upper case letters (A-Z)
  - Numbers (0-9)
  - Special characters (e.g. !@#$%^&*)

Module TWO: Getting Started

What is an Authenticator App

The authenticator app is a powerful tool that enhances the security of your accounts by providing an additional layer of protection during the authentication process.

An authenticator app is a mobile application designed to generate one-time passwords (OTPs) or codes that are used for the second factor of authentication. It generates these unique codes based on a secret key that is shared between the app and the service you are trying to access. These codes are time-sensitive and typically refreshed every 30 seconds, ensuring a high level of security.

Benefits of Using an Authenticator App

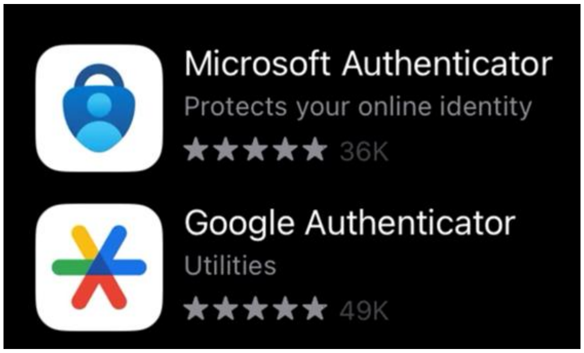
By utilizing an authenticator app as your second factor of authentication, you enjoy the following benefits:

1. **Enhanced Security**: The authenticator app adds an extra layer of security by requiring a unique OTP in addition to your password. This makes it significantly harder for unauthorized individuals to gain access to your accounts.
2. **Offline Access:** Since the authenticator app generates OTPs locally on your device, you can use it even when you don't have an internet connection. This ensures uninterrupted access to your accounts.
3. **Convenience:** The app is typically installed on your smartphone, making it easily accessible whenever you need it. You won't have to carry any physical tokens or worry about losing them.

To Begin Using the Authenticator App

To begin using an authenticator app, follow these steps:

1. **Download and Install** an **Authenticator App** on your mobile device. These apps can be found in your device's app store (e.g., Google Play Store, Apple App Store). Some popular options include Google Authenticator and Microsoft Authenticator. **Download and install** the app that suits your preference.



Microsoft Authenticator
Protects your online identity
★★★★★ 36K

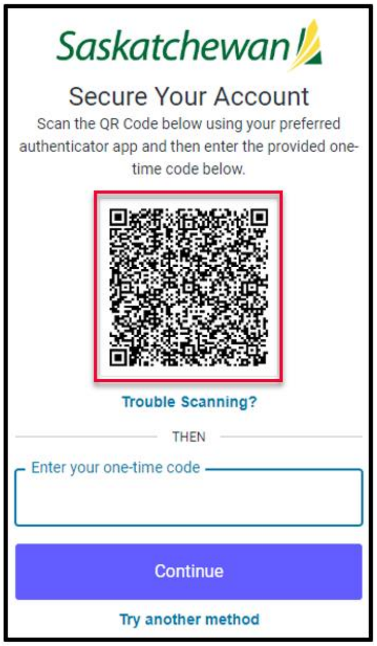
Google Authenticator
Utilities
★★★★★ 49K

Once the app has downloaded, follow the on-screen instructions to set up your personal account.

Some authenticator apps offer the option to back up your accounts. This allows you to restore them if you change devices or accidentally lose access to the app.

Follow the instructions within the app to enable the backup feature, if available.

2. **Launch** the authenticator app on your mobile device and **scan the QR code** using the camera on your mobile device.



Saskatchewan

Secure Your Account

Scan the QR Code below using your preferred authenticator app and then enter the provided one-time code below.

Trouble Scanning?

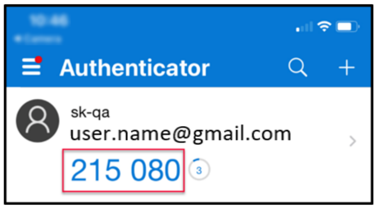
THEN

Enter your one-time code

Continue

Try another method

3. The app will generate a time-based one-time passcode (OTP) for that specific account.

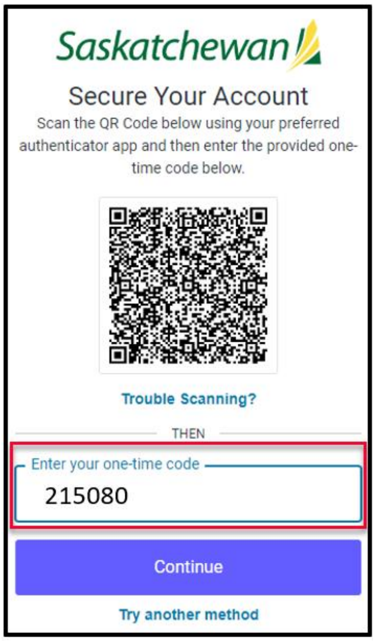


sk-qa

user.name@gmail.com

215 080

4. Enter this **One-time Passcode (OTP)** to verify the setup. This confirms that the authenticator app is correctly synchronized with the service.



Saskatchewan

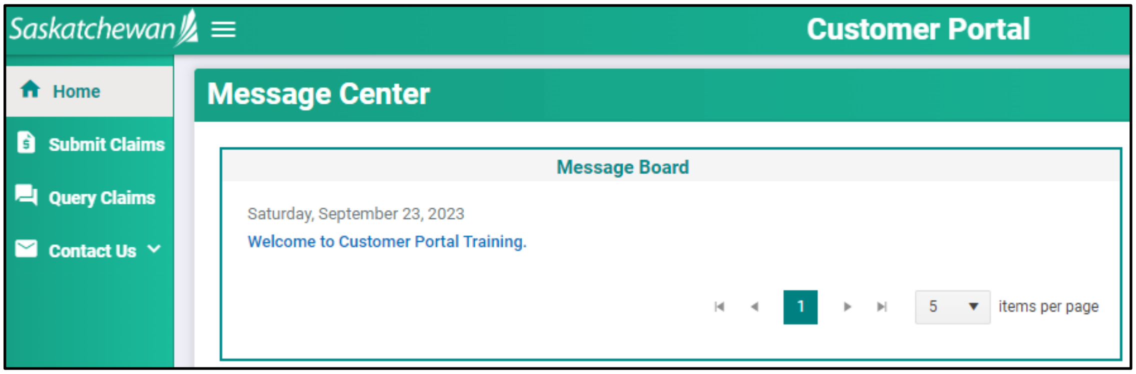
Secure Your Account

Scan the QR Code below using your preferred authenticator app and then enter the provided one-time code below.

Enter your one-time code
215080

5. Click **Continue.**

6. Arrive at the homepage of **Customer Portal.**



Message Center

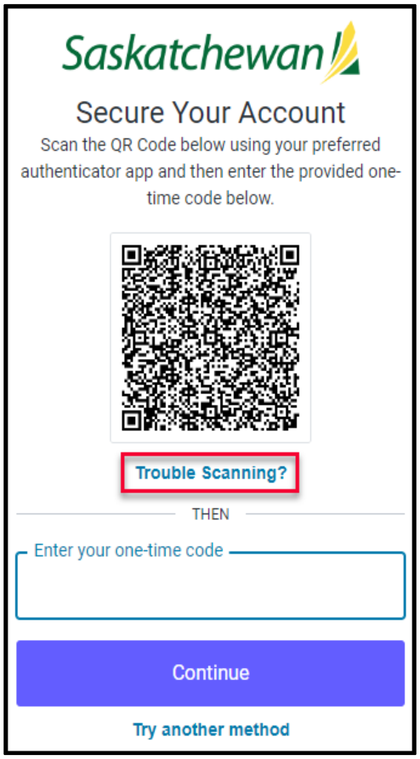
Message Board

Saturday, September 23, 2023
Welcome to Customer Portal Training.

Trouble Scanning the QR Code

If you encounter issues with scanning the QR code, a manual option can be activated.

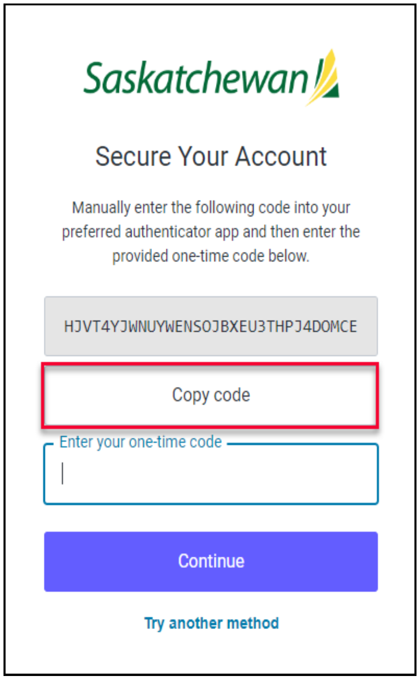
1. Click on **Trouble Scanning.**



Secure Your Account

Scan the QR Code below using your preferred authenticator app and then enter the provided one-time code below.

2. Click on **Copy Code.**

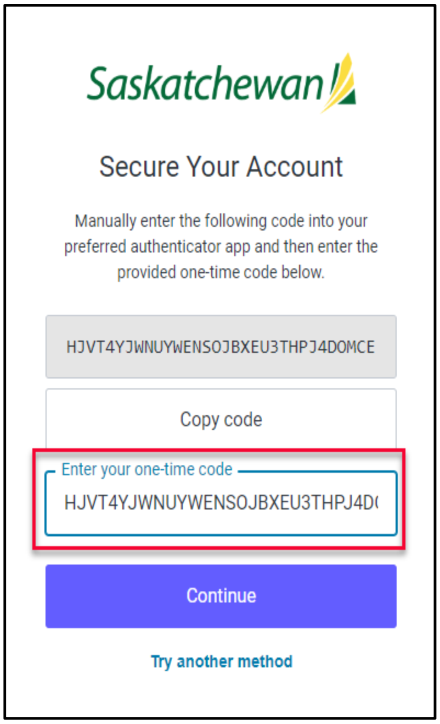


Secure Your Account

Manually enter the following code into your preferred authenticator app and then enter the provided one-time code below.

HJVT4YJWNUYWENSOJBXEU3THPJ4DOMCE

3. Paste the code into the **One-time Code Field.** **Note:** Right click + Paste is the most efficient way to paste the data.



Secure Your Account

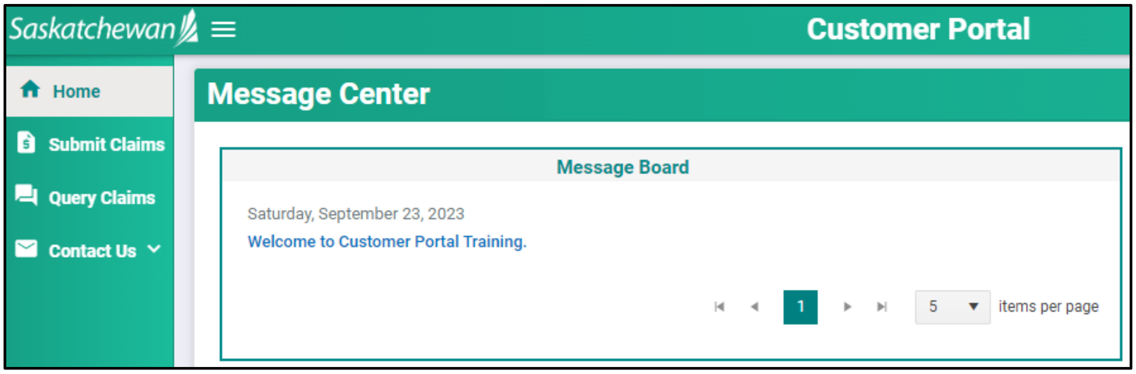
Manually enter the following code into your preferred authenticator app and then enter the provided one-time code below.

HJVT4YJWNUYWENSOJBXEU3THPJ4DOMCE

Enter your one-time code: HJVT4YJWNUYWENSOJBXEU3THPJ4D(

4. Click **Continue.**

5. Arrive at the homepage of **Customer Portal.**



Message Center

Message Board

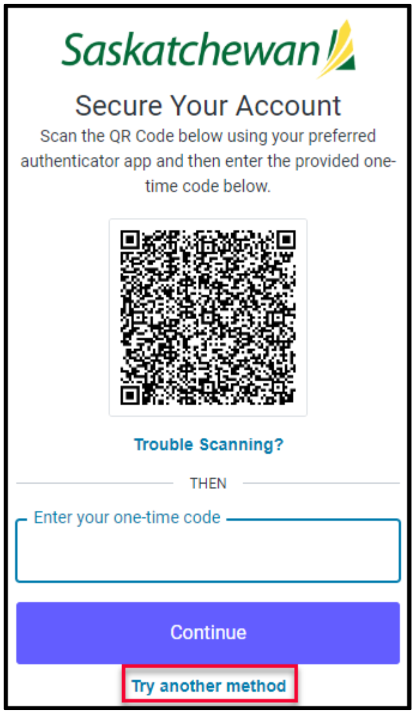
Saturday, September 23, 2023
Welcome to Customer Portal Training.

SMS (Text Message)

If you choose to have the passcode sent to you via SMS (text message), follow these steps:

The mobile number entered during the initial enrolment cannot be changed. Be sure to select a mobile number that is always available to you. If extenuating circumstances arise and the mobile number must be changed, a service desk ticket is required.

1. Select **Try another method.**

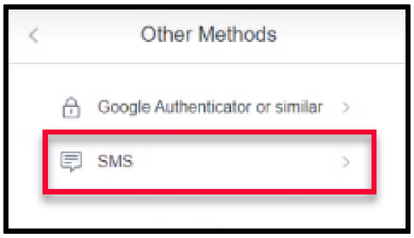


Saskatchewan

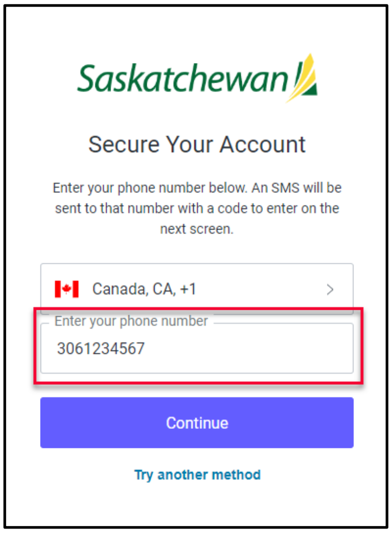
Secure Your Account

Scan the QR Code below using your preferred authenticator app and then enter the provided one-time code below.

2. Select **SMS.**



3. Enter your **10-digit mobile number (**i.e., 3062223333). **NOTE:** As this is the first time signing in, you are associating your userid with your mobile number. Once set, the only way to change your mobile number is to log a support ticket.



Secure Your Account

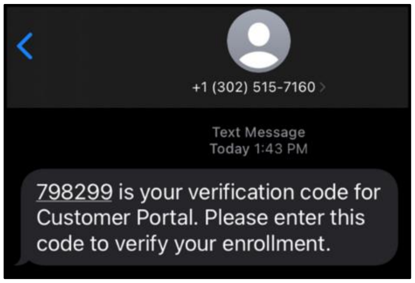
Enter your phone number below. An SMS will be sent to that number with a code to enter on the next screen.

Canada, CA, +1

Enter your phone number: 3061234567

4. Click **Continue.**

5. The 6-digit code will be sent to your mobile device as a text message.

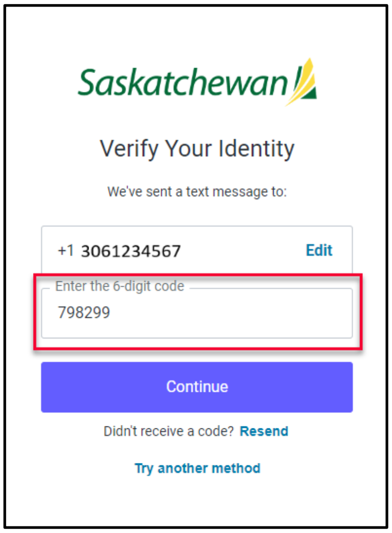


+1 (302) 515-7160

Text Message
Today 1:43 PM

798299 is your verification code for Customer Portal. Please enter this code to verify your enrollment.

6. Enter the **6-digit code** on the screen.



Verify Your Identity

We've sent a text message to:

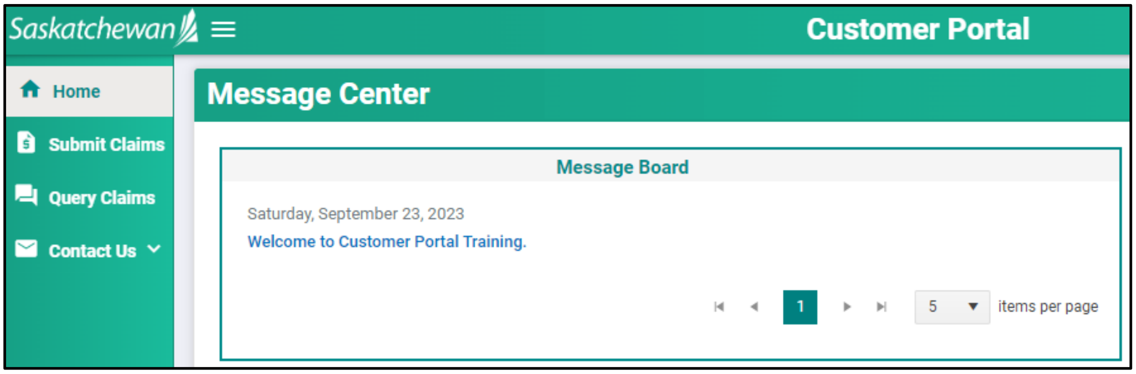
+1 3061234567

Enter the 6-digit code: 798299

Didn't receive a code? Resend

7. Click **Continue.**

8. Arrive at the homepage of **Customer Portal.**



Saturday, September 23, 2023
Welcome to Customer Portal Training.

Service Bureau

When a Service Bureau uses an Application Programming Interface (API) to upload their batch files, the MFA will not be triggered. At go-live Acurro, Perspect and CBA are using API's.

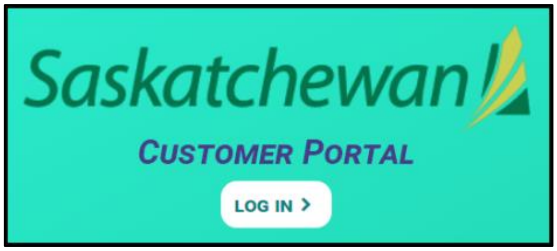
If an individual at a Service Bureau logs into Customer Portal, using their personal userid, MFA will trigger. The process for this individual is the same as listed above.

Resetting Password

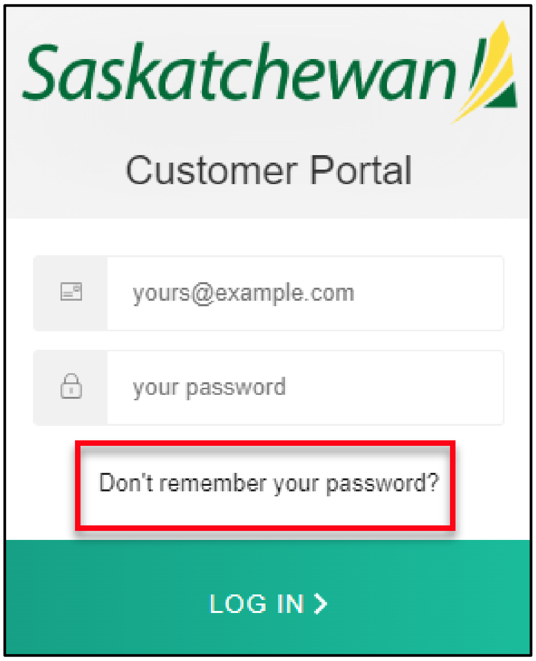
Resetting your password is a self-serve option within Customer Portal. If you require your password to be reset, follow these steps.

1. Open the **Customer Portal** application.

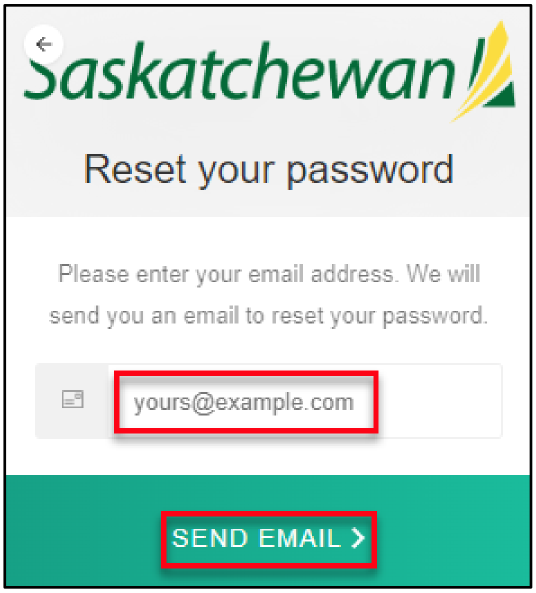
2. Click on **Log in.**



3. Click **Don't remember your password?**



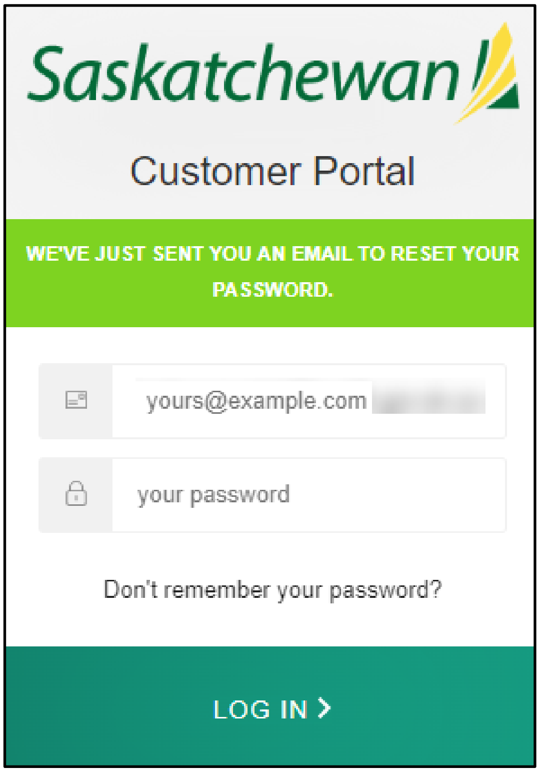
4. Enter your username which is your email registered to your Physician Registry profile and then click **Send Email.**



Reset your password

Please enter your email address. We will send you an email to reset your password.

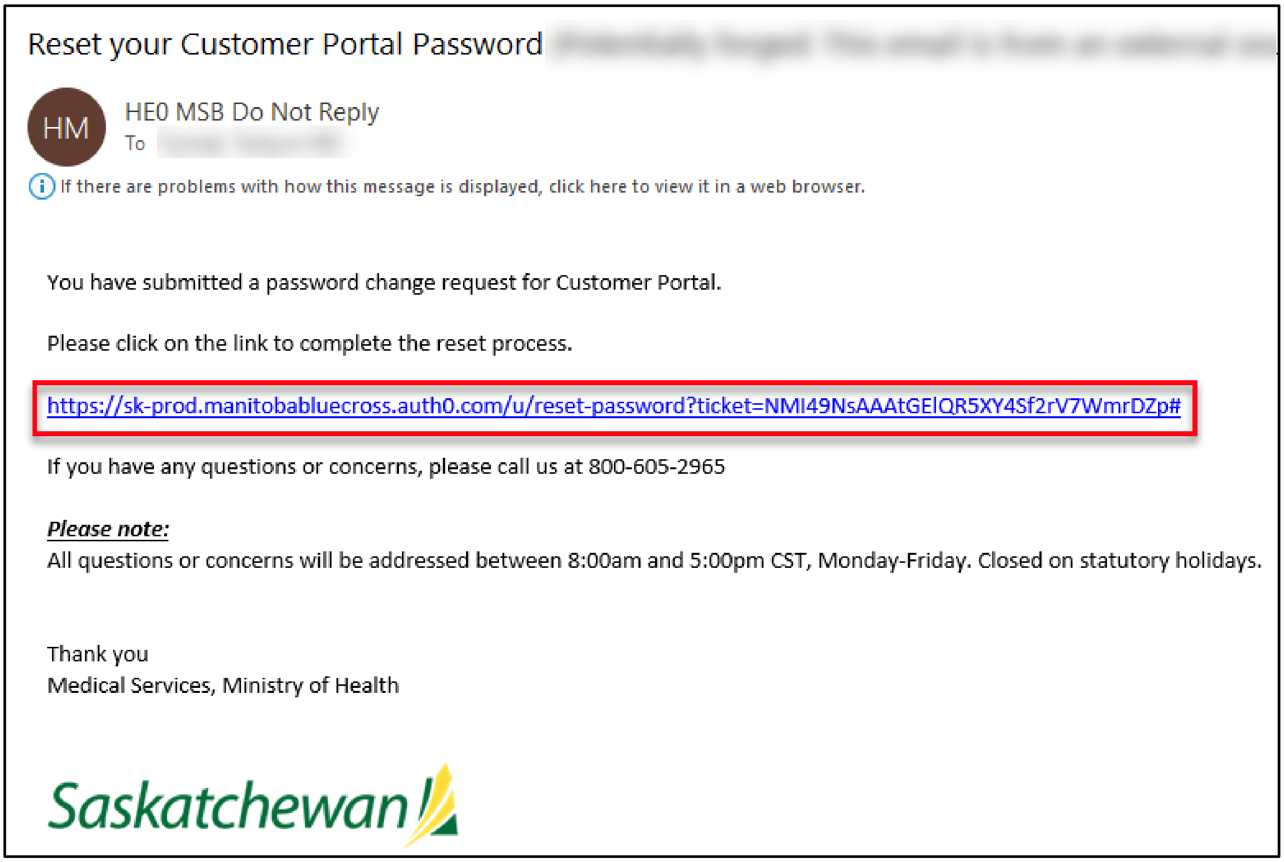
5. Confirmation pop-up is received.



Customer Portal

WE'VE JUST SENT YOU AN EMAIL TO RESET YOUR PASSWORD.

6. Click on the link within the email.



Reset your Customer Portal Password [redacted]

HEO MSB Do Not Reply
To [redacted]

If there are problems with how this message is displayed, click here to view it in a web browser.

You have submitted a password change request for Customer Portal.

Please click on the link to complete the reset process.

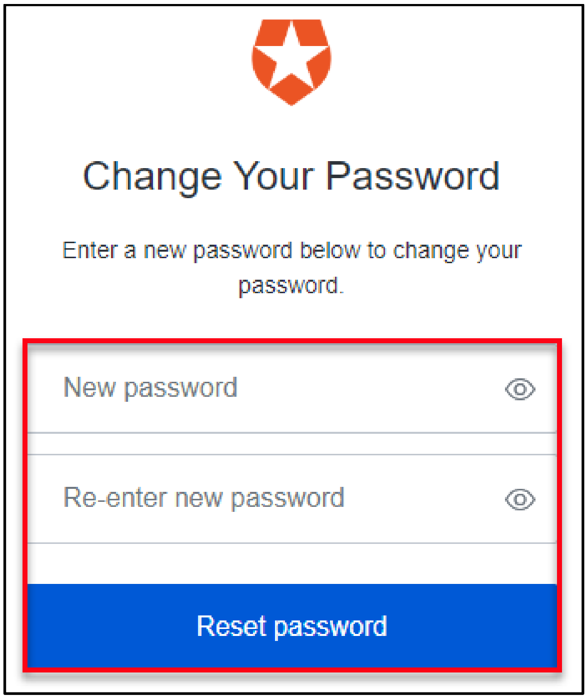
https://sk-prod.manitobabluecross.auth0.com/u/reset-password?ticket=NMI49NsAAAtGElQR5XY4Sf2rV7WmrDZp#

If you have any questions or concerns, please call us at 800-605-2965

Please note:
All questions or concerns will be addressed between 8:00am and 5:00pm CST, Monday-Friday. Closed on statutory holidays.

Thank you
Medical Services, Ministry of Health

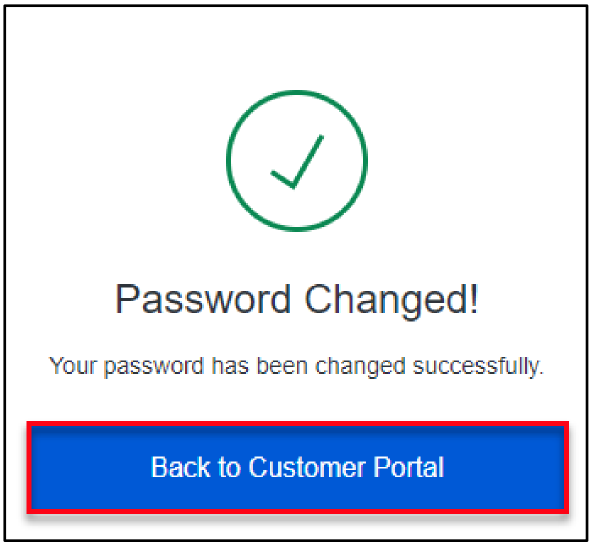
7. Enter your new password twice and then click **Reset Password.**



Change Your Password

Enter a new password below to change your password.

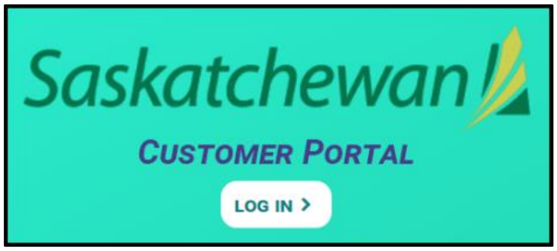
8. Click **Back to Customer Portal** on the confirmation pop-up window.



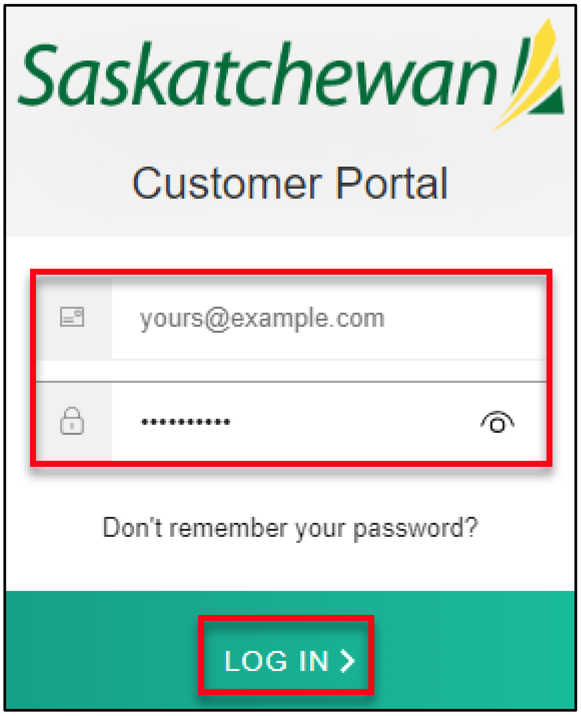
Password Changed!

Your password has been changed successfully.

9. Click on **Log in.**



10. Enter your username and your new password, then click **Log In.**



Saskatchewan
Customer Portal
yours@example.com
•••••••••••
Don't remember your password?
LOG IN >