What is Multi-Factor Authentication and why is it important?

Traditionally Sunnybrook have relied on username & password pair as the primary method of authentication into various IT systems. Though this has served well in the past, proliferation in credential phishing and crafted hacking activities have starting to put access to various IT systems at greater risk. To mitigate this risk -- Sunnybrook Information services will be implementing Multi-factor authentication (MFA) to various IT systems & assets, starting with ones that are readily accessible from the Internet – namely VPN and VDI.

What’s changing and how will it affect me?

Prior to March 1st, 2021:

- Attempt to access VPN or VDI from Internet
- Only one Authentication Factor required: Sunnybrook network username/password
- Access granted to VPN or VDI from Internet

After March 1st, 2021:

- Attempt to access VPN or VDI from Internet
- 1st Authentication Factor required: Sunnybrook network username/password

2nd Authentication Factor required:
- Verification code sent via **SMS Text** OR
- Verification code announced during **voice call** OR
- Verification sent to your cell phone as an **app “notification”**

- Access granted to VPN or VDI from Internet
What do I need to do?

PRIOR to March 1st, 2021, make sure you follow the enrollment instruction in the following pages.

Those not enrolled by specified date will not be able to access VPN / VDI from the Internet.
Type of authentication factors

1. Open a browser and visit [https://sunnybrook.okta.com](https://sunnybrook.okta.com). You can perform this task from work computer or from home without VPN connection.
2. Sign-in with your Sunnybrook network username & password.
3. After clicking on “Sign In”, you will see the following screen allowing you to choose the authentication factor you prefer to use. Here is a quick summary of each authentication factor and how it may be the suitable factor for you. **Note you can setup multiple authentication factors if you wish.**

How it works

1. On your mobile device, download the “Okta Verify” App from Google Play Store (Android devices) or App Store (Apple iOS devices)
2. During enrollment you scan a 3D/QR barcode to associate your mobile device with your Okta account.
3. To authenticate, all you have to do is “acknowledge” the notification that is pushed to your mobile device.

Ideal For:
- Users who prefer a streamlined authentication experience and do not mind installing a 3rd party App (Okta Verify) on their mobile device.

How it works

1. During enrollment you associate your cellphone number with your Okta account.
2. To authenticate and gain access to VPN/VDI, you type in the code received as a SMS text message on your cellphone.

Ideal For:
- Users who prefer not to install a 3rd party application (Okta Verify) on their mobile phone.
- Users who don’t mind having to key-in verification code each time when prompted.

How it works

1. During enrollment you associate a phone number with your Okta account.
2. To authenticate and gain access to VPN/VDI, you type in the code announced to you during a voice call to you.

Ideal For:
- Users who do not have a cellphone but have access to a landline or voice mail.
4. When you click on “Setup”, you’ll see steps that are **intuitive to follow for most users**. However, if you need further details to guide you through setting-up/enrolling each of these authentication factors, it can be found in the following pages.
How to setup/enroll “Okta Verify” as an authentication factor

1. If you have an Apple iPhone device:
   
   From Your phone -- visit the App Store and download “Okta Verify”

   If you have an Android device:
   
   From Your phone -- visit the Google Play and download “Okta Verify”

2. From your phone -- Launch the Okta Verify App you’ve just downloaded. Click on the “+” sign. If you get prompted for camera access, please allow it.

   Leave your phone on this screen – you will need it on a later step.
3. Using separate device (computer or laptop), go to https://sunnybrook.okta.com
Sign-in with your Sunnybrook network username & password.
Click on Setup under “Okta Verify”.
4. Select the your mobile device type and click on Next:

- iPhone
- Android

Download Okta Verify from the App Store onto your mobile device.
5. The following should be displayed within your web browser:

![Setup Okta Verify](image-url)

- **Scan barcode**
  - Launch Okta Verify application on your mobile device and select Add an account.
  - Can't scan?

- **Back to factor list**
6. **From your phone**, make sure you’re still in the **Okta Verify App** (as instructed in step 2).
Pickup your phone and use its camera to scan the 3D/QR bar code displayed in the web browser on your computer/laptop.

Tips for a successful scan:
- Ensure your camera lens is clean and free of debris.
- Make sure the 3D/QR bar code is inside the square brackets.
- Try to keep your hand/phone steady to allow it to properly focus.
- If it still won’t scan, try to vary the distance slightly, then hold steady.
7. Once the enrollment is successful and your phone is now associated with your Okta account, you’ll see the following screen. Click on Finish to complete enrolling Okta Verify, or you can choose to setup/enroll additional factors (i.e. SMS Text or Voice Call authentication).
8. If you clicked on “Finish”, you’ll see the following screen asking you to pick a security image. Be sure to click on “Create My Account” to complete the enrollment process.
9. Once your account is created, you can enroll additional authentication factors by **clicking on your name at the top-right corner, then select settings**:
10. Scroll down until you see the **Extra Verification** section. Here you can setup additional authentication factors such as SMS or Voice Call Authentication.
Setup/Enroll “SMS” as an authentication factor

1. Go to [https://sunnybrook.okta.com](https://sunnybrook.okta.com) and sign-in with your Sunnybrook network username & password. Click on Setup. (Reference Page 13 and 14 of this guide if you don’t see setup)
2. Enter your cellular number that you would like to enroll. This number must be capable of receiving SMS text messages. Click on “Send code”. Enter the verification code you received on your phone as SMS text message, then click on Verify.

3. Your phone number is now enrolled for SMS authentication.
Setup/Enroll “Voice Call” as an authentication factor

1. Go to https://sunnybrook.okta.com and sign-in with your Sunnybrook network username & password.
2. Click on Setup. (Reference Page 13 and 14 of this guide if you don’t see setup)
3. Enter the phone number where you would like to receive voice call authentication, then click on Call. You'll receive a phone call. Enter the code announced during the voice call, then click on Verify.

4. Your phone number is now enrolled for voice call authentication.
I have completed enrolling my authentication factors. What’s next?

On March 1st, 2021, Information Services will make multi-factor authentication mandatory when accessing VPN or VDI externally from the Internet.

As of March 1st, 2021 you will notice that the VPN and external VDI login screen look different. You will be presented with additional prompts (challenge/response), where you will have to input your MFA passcode received via one of the following methods:

1) Call
   If you enrolled in “Voice Call” as your authentication factor, and selected 1 as your challenge

2) Push
   If you enrolled in “Okta Verify” as your authentication factor, and selected 2 as your challenge

3) SMS
   If you enrolled in “SMS” as your authentication factor, and selected 3 as your challenge
**What my experience will look like?**

Below are some examples of the login screens and authentication prompts that you will receive:

- If you enrolled for “Okta Verify”, you will see the following prompts:
• If you enrolled for “SMS” (in this example user is using PulseSecure to connect to the VPN), you will see the following prompts/login screen:
• If you enrolled for “SMS” (in this example user is using VMware Horizon to connect to external VDI), you will see the following prompts/login screen:
For detailed documentation on how to access VPN and VDI externally and anticipated prompts, please visit:

VPN -- https://sunnynet.ca//Default.aspx?cid=103659&lang=1