Cisco AnyConnect User Guide

For MacOS Devices

/ Connecting to the UHN VPN with Multi-Factor Authentication (MFA)

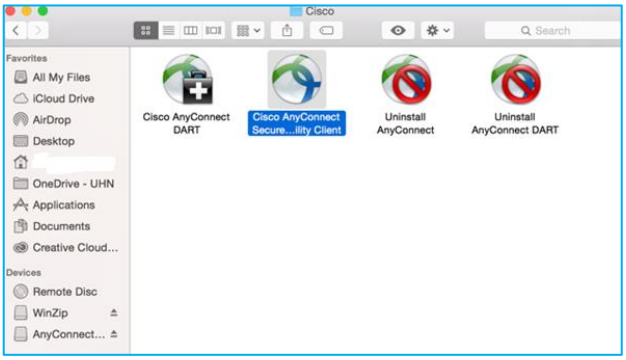
If you have been set up for VPN access with MFA, use the instructions below.
Otherwise, please contact the Help Desk to request VPN access through MFA.

Before you begin, please set up your MFA settings using the MFA Portal https://mfa.uhn.ca.
Further instructions are available on the MFA Portal homepage.

How does Multi-Factor Authentication (MFA) work?
MFA verifies your identity when connecting to the UHN network from offsite using one of these methods: a text message code, phone call or through a Microsoft Authenticator app.

---

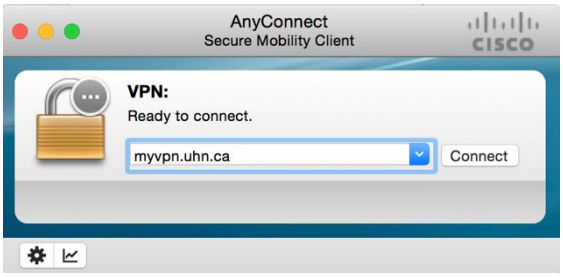
1. From your Applications folder, open the Cisco folder, then click the **Cisco AnyConnect Secure Mobility Client**.



2. The AnyConnect application window will appear. The **UHN VPN Service** option should automatically appear.

   If the field appears blank, type in **myvpn.uhn.ca**.

   Click **Connect**.

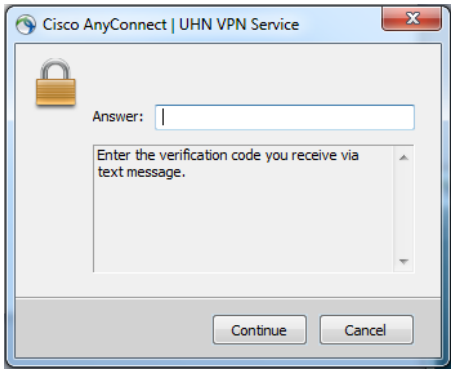


3. Enter your T-ID and network password. This should be the same password you use to log into your computer at UHN.

   a. If your MFA default option is **Text Message**, a new window will appear prompting you to "Enter the verification code you receive via text message".

      Enter the 6-digit code then click **Continue**.

   b. If your MFA default option is **Phone Call**, you will receive an automated call and you will need to press # to complete verification.



c. If your MFA delivery option is **Mobile App**, then a notification will be sent to your phone's Authenticator app. Tap **Approve** on your phone to complete verification.

4. You will see a welcome message once you successfully connect. The message will vary slightly for RMP and TC-LHIN employees.

   Click **Accept.**