How to Setup VPN Entrust Certificate with Soft Token Device for Non-Bank (Personal) iOS (11.4 +) or Android (8 +) Mobile Device

Windows PC – New User

NOTE: You will need your One Time Verification Code (OTVC password) in order to log into Virtual Private Network (VPN). OTVC, Entrust Password & Self Serv documentation will be sent by: VPN.Administration@Scotiabank.com to your personal email address via Scotia Banks Secure Email Website

Pre-Requisite:

- **You must** have already logged into your Windows PC with your Scotia ID (Sxxxxxxx) and Temporary password
- **You must** be connected to your Home WIFI

IMPORTANT: Connecting to Scotiabank's VPN system first requires access to the Internet. How you connect to the Internet is just as important as using VPN to connect to the Bank. You should only use trusted and known internet connections at home or from your Bank-provided mobile device. Once connected to a trusted internet connection, VPN must be used to then connect to Scotiabank's network.

Guide Content:

PART A: SETUP & LOG INTO ENTRUST DIGITAL ID

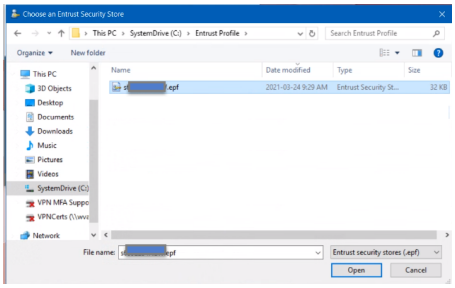
1. Right Click on the Entrust Digital ID icon (located on your task bar, bottom right corner near your date and time). The icon will either have a Lock or an Orange X on it, and choose Log In…

2. Under the Name Field you should see your Scotia ID or, your First Initial_Lastname. Enter your Password and **choose OK**. **NOTE:** If you do not see your Scotia ID in the Name Field , please proceed **to step number 4 (Page 2)**

3. If password entry is successful, Entrust window will disappear, you will see a **Yellow Key** on the Entrust Digital ID icon. Please proceed to: **PART B. LOG INTO CISCO ANYCONNECT SECURE MOBILITY CLIENT(VPN) (Page 3)**

4. If name Field is blank choose **Browse option**

5. Double Click on your **Scotia ID** or, **Choose Open**

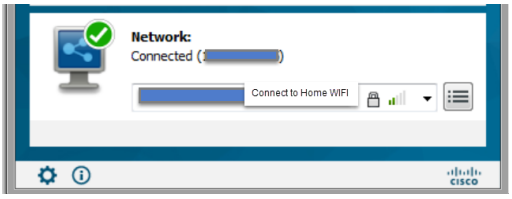


6. Entrust Security Window will appear & you will notice your Scotia ID populated in the “Name” field. **Enter your password & Click OK.** Expected result is Window to disappear if entry is correct

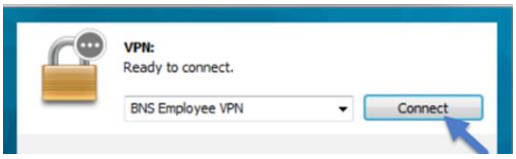
PART B. LOG INTO CISCO ANY CONNECT SECURE MOBILITY CLIENT (VPN)

1. From your Task Bar launch (Double Click) on your **CISCO Any Connect Secure Mobility Client icon**

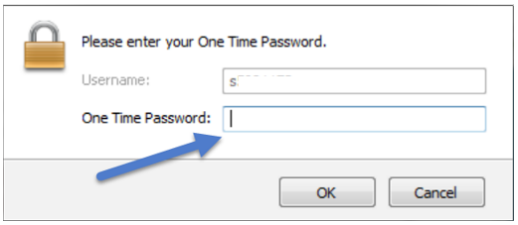
2. Ensure you are connected to your **Home WIFI**



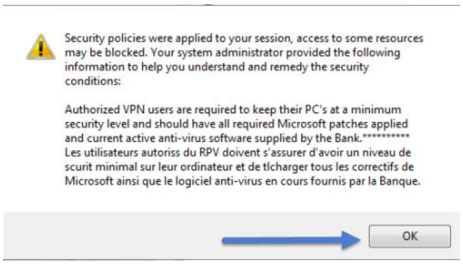
3. Click **Connect**



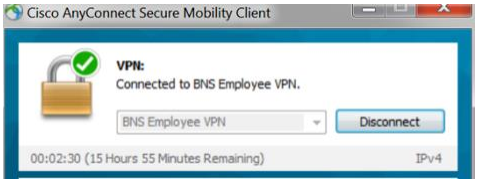
4. Enter your **One Time Verification Code Password**



5. Click **Accept** & **OK**



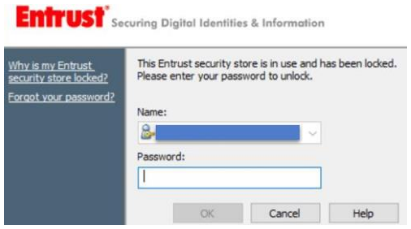
6. You are now **successfully connected** to **Scotiabank's Virtual Private Network**.



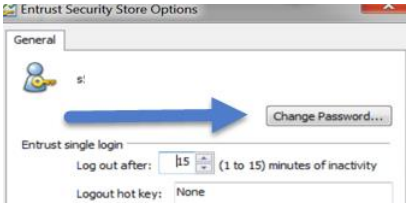
PART C. Changing Your Entrust Password

1. Right Click on the **Entrust icon** and choose **Options…**

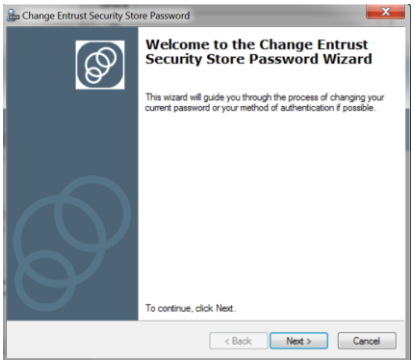
2. **PLEASE NOTE:** By Default, Entrust will log you out after 15 minutes of inactivity, please ensure you Sign back on with your current password in order to successfully set a new password



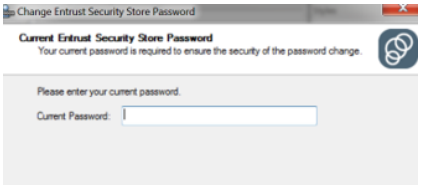
3. Choose **Change Password**



4. Choose **Next**

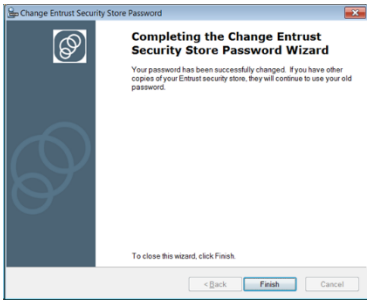


5. Enter **Current Password** and Click **Next**



6. Enter your **New Password** in the "Password" field and the **"Confirm Password"** field and Click **Next**

7. Click **Finish**



NOTE: Make a **mental note of your new password**. If you forget your password, you will need to open a Service Now Ticket: VPN MFA IS&C Form **choose "Recovery" Tab** as a new certificate will be required. This will take 24\48 hours to complete.

PART D: REGISTERING YOUR SOFT TOKEN

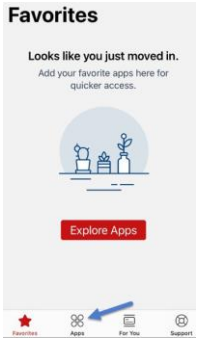
Pre-Requisite:

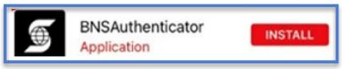
- **You must** change your **temporary Windows password**: Change your Windows Password and **register for your Security Questions**
- Please ensure your iOS device is 11.4 or higher.
- **You must** have successfully enrolled your Workspace ONE (AirWatch) Profile prior to completing the next steps
- **You must** have received your OTRC (One Time Registration code) from the VPN Administration Team

If you have not received your QR code or require assistance with Workspace ONE (AirWatch), please reach out to: IT.Servicedesk@scotiabank.com, or call 416 863 7001- choose Option 1 or Tollfree: 1866 572 6842 - choose Option 1

1. Tap the Hub App to launch the application on your Phone

2. Tap on the Apps icon to open the App catalogue, find **BNS Authenticator** and **Tunnel App** and tap to install both.

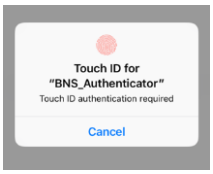




NOTE: The Apps generally install in a few seconds. If the status of your installation says "Processing", please ignore this message and navigate out of the Hub App and find the BNS Authenticator App.

3. Tap and launch the **BNS Authenticator App**

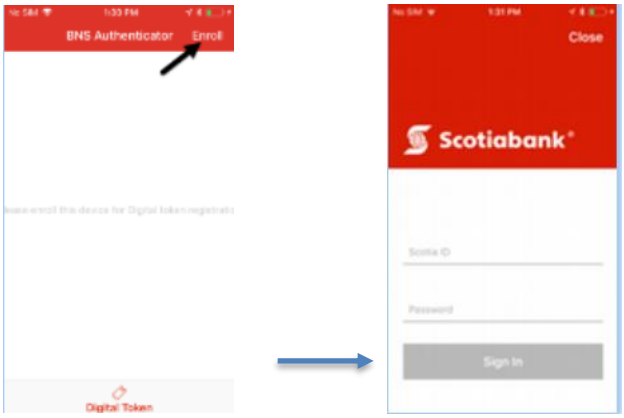
4. For Non-bank iOS devices, Use Touch ID for Authentication. **NOTE:** For assistance with Touch ID setup please contact: https://support.apple.com/en-ca/HT201371



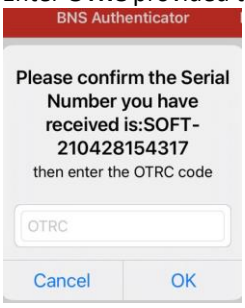
5. Depending on your Android Operating version, most devices require you to enter your phone password prior to setting up your **fingerprint scanner**. Refer to your mobile device for instructions or see a few examples provided.

Workspace settings	**Work profile settings**
Workspace Folder located within all your appl>Tap more options (3 dots) in right corner>Workspace settings>Select Fingerprint Scanner>Enter Phone password>Follow steps to add your fingerprints	Phone settings>Scroll down to Work profile>Select Fingerprints>Click continue>Create a work profile password, if you haven't set up one already>Follow the steps to add your fingerprint
Security settings	**Lock Screen and Security Settings**
Phone settings>Scroll down and select Security>Work profile security>Fingerprints>Follow the steps to add your fingerprint	Phone settings>Scroll down and select Work profile fingerprints>You maybe prompted to enter your phone password>Follow the steps to add your fingerprint

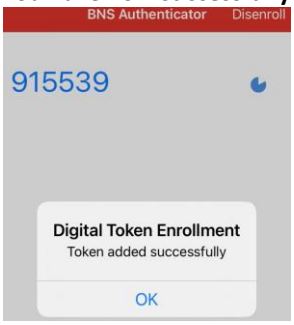
6. Click **Enroll** and enter **your Scotia ID (Sxxxxxx)** and **Windows Password** and **Click Sign In**



7. Enter **OTRC** provided to you and **click OK**



8. You have now **successfully registered** your Soft token

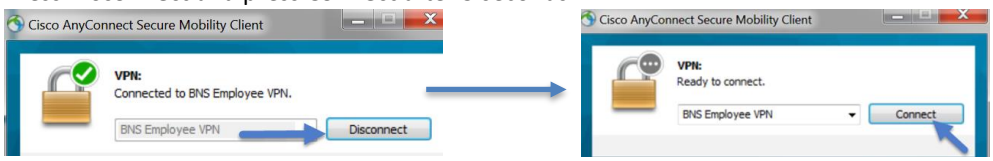


NOTE: Your OTP (One Time Password) changes every 30 seconds. Close the application to exit BNS Authenticator and please **DO NOT click on Disenroll**, as it will prompt you to enter your scotia ID and windows password before **deleting** your Soft Token. If you've accidentally clicked on disenroll and have deleted your Soft Token, please open a Service Now ticket: VPN MFA IS&C Form and choose **"Token Only, OR Replace lost, stolen or damaged token"**.

PART E: TESTING YOUR SOFT TOKEN AFTER YOU'VE SUCCESSFULLY REGISTERED

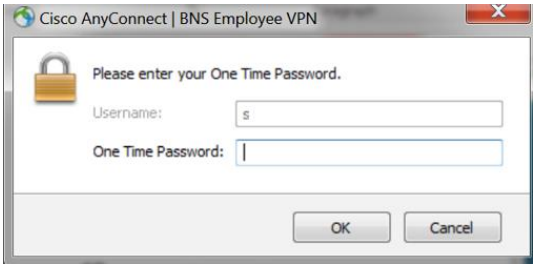
1. **Launch** (Double Click) on Cisco AnyConnect Secure Mobility Client

2. Press **Disconnect** and press **Connect** after 5 seconds

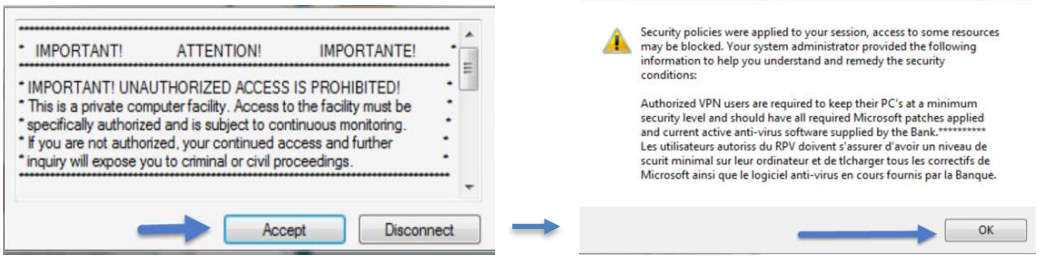


3. Open **BNS Authenticator App** with your Touch ID

4. Enter numbers displayed from your **BNS Authenticator App** "One Time Password and Click **OK**.



5. Click **Accept** & **OK**



NOTE: You are now on Scotiabank's Network using your Soft Token from your personal mobile device. If there are any issues with your Soft Token or your BNS Authenticator application, please reach out to VPN.Administration@scotiabank.com

Troubleshooting TIPS: "CONNECTION TIMED OUT" Error - when Enrolling your Soft Token

1. Reboot device
2. Switch Off WIFI, ensure that you're using phone data
3. Launch Tunnel, let the app run for 5-10 seconds
4. Launch Web, let the app run for 5-10 seconds
5. Launch BNS Authenticator – retry enrolling using the OTRC code provided