



EOHHS-Information Technology

Executive Office of Health and Human Services

User Guide Library Series



Uninstalling Legacy VPN Client
and Installing New VPN Client



Summary	<p>The following instructions will explain how to uninstall the legacy VPN services issued to EOHHS staff before 3/17/20, allowing for the installation of new VPN services.</p> <p>Installing new VPN services will also require re-enrollment in multi-factor authentication (MFA).</p>
Content	<ul style="list-style-type: none">• Re-enroll in Multi-Factor Authentication (MFA)<ul style="list-style-type: none">○ Download the Authenticator Mobile App○ Setup MFA User-Account• Uninstall Legacy VPN Client<ul style="list-style-type: none">○ Confirm Legacy VPN Client○ Uninstall Legacy VPN Client• Install New VPN Client<ul style="list-style-type: none">○ Download New VPN Client○ Install New VPN Client• Configure New VPN Client<ul style="list-style-type: none">○ Initiating VPN Logon○ Verify VPN Connection• Disconnect from VPN Client



RE-ENROLL IN MULTI-FACTOR AUTHENTICATION (MFA)

Download the Authenticator Mobile App

Step 1 Install the **Microsoft Authenticator** mobile app.

- **Wait** to open and setup Microsoft Authenticator in a future step.
- If Microsoft Authenticator was already installed and being utilized, additional instructions will be provided in a future step.



**Microsoft
Authenticator**

Apple Devices
Apple App Store



Android Devices
Google Play



Setup MFA User-Account

Step 1 On a web browser, go to <https://EOTSS.My.Centrify.com>.

Step 2 If the following sign-in requests windows appear:

- Click **Cancel**.

Sign in
https://es-mm-cent-02.es.govt.state.ma.us:8443

Username

Password

Windows Security

iexplore.exe

Connecting to es-mm-cent-03.es.govt.state.ma.us.

User name

Password

Domain: EHS

☐ Remember my credentials

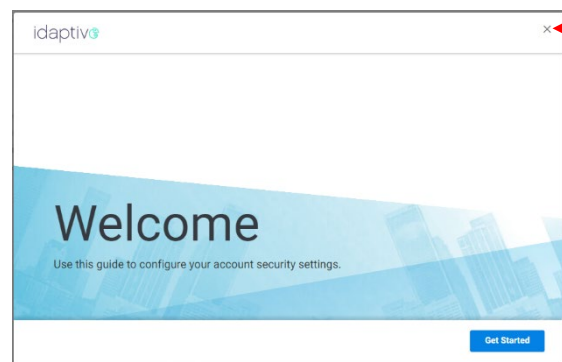
**Step 3** The correct sign-in window will appear.

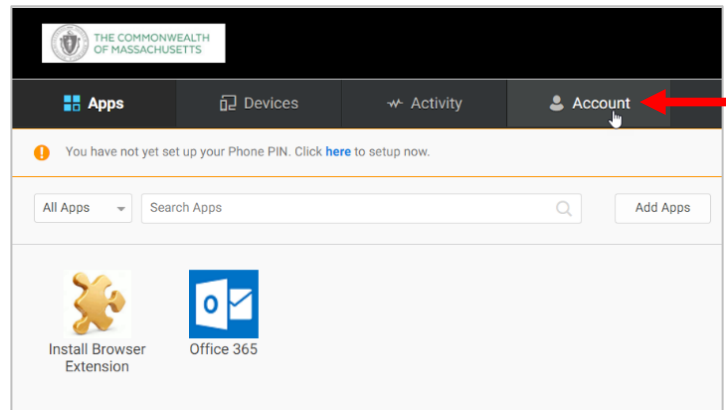
- In the **User Name** field, enter a user work email.
(Formats: @mass.gov or @massmail.state.ma.us)
- Click **Next**.

- Step 4**
- In the **Password** field, enter user Windows password.
 - Click **Next**.

NOTE: If an error message appears, call EOHHS-IT Service and Support Center (SSC): 617-994-5050.

NOTE: Anytime this “Welcome” message appears, close the window by clicking X located in the upper-right corner.



**Step 5** Click **Account**.

An **Authentication Factors** window will open.

Leave the screen open in the web browser to be used in a later step.

**Step 6****NOTE:**

- **If** Microsoft Authenticator was already installed and being utilized, **skip this step and go to [Step 7](#)**. If not, complete Step 6.
- **If** Microsoft Authenticator was opened prior to this step and the Data Privacy terms were accepted, **skip this step and go to [Step 8](#)**. If not, complete Step 6.

Data Privacy

We gather non-personally identifiable usage data to help us improve the app. You can turn this off in settings. Learn more in the FAQs available under the Help menu.

[OK](#)

Open the **Microsoft Authenticator** mobile app.

**Data Privacy**

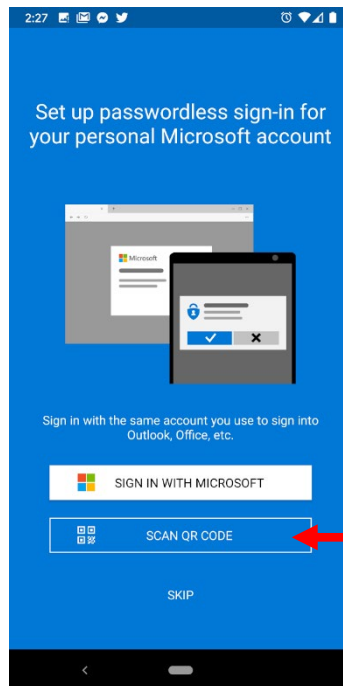
- Tap **OK**.

Data Privacy

We gather non-personally identifiable usage data to help us improve the app. You can turn this off in settings. Learn more in the FAQs available under the Help menu.

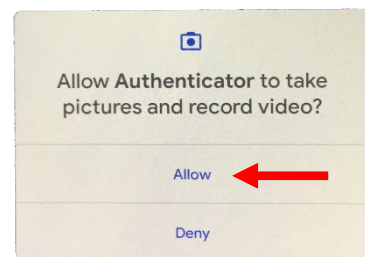
OK**Set up passwordless sign-in...**

- Tap **SCAN QR CODE**.

**Allow Authenticator to take pictures...**

- Tap **Allow**.
- A QR scanner window will open.

[Go to Step 10.](#)



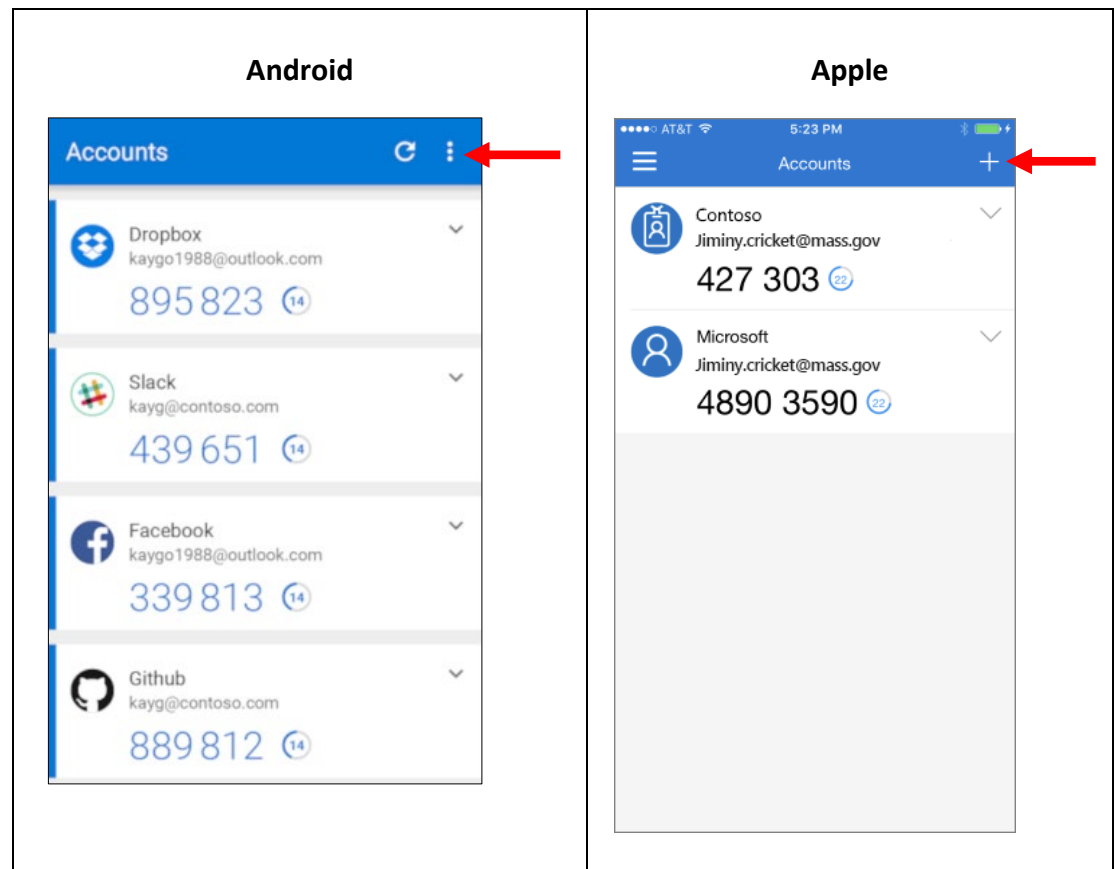
Step 7 Microsoft Authenticator was already installed and being utilized:

- Open **Microsoft Authenticator** mobile app.



- A screen will display listing all existing accounts.
 - Tap the symbol at the upper-right corner of the screen (images below).

Go to [Step 9](#).

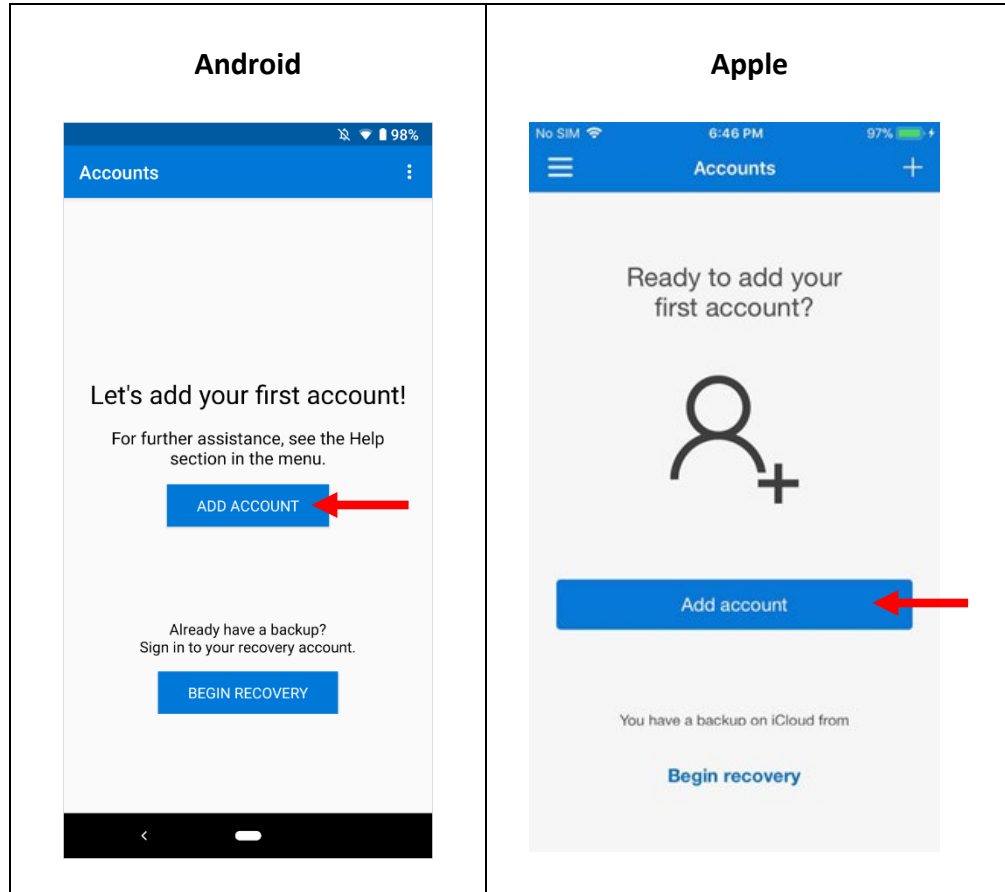


Step 8 After installing Microsoft Authenticator, the app was opened and the Data Privacy terms were accepted:

- Open the **Microsoft Authenticator** mobile app.

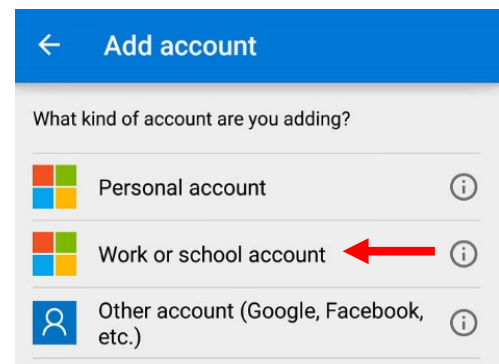


- Tap **Add Account**.



Step 9

- **What kind of account are you adding?**
 - Tap **Work or school account**.
- A QR scanner window will open.



Step 10

The QR scanner window in Microsoft Authenticator **should be open and ready to scan**.

- Go back to the MFA user-account window that was left open.
- Click on **Show QR Code**.



Authentication Factors

Passcodes

Personal Profile

Organization

Authentication Factors

[Learn more](#)

- ✓ Password
Last changed: May 14, 2020 Edit
- ! Phone PIN
You have not set a Phone PIN. Set
- ✓ OATH OTP Client
Configured successfully. Show QR Code

- A QR code will appear.

OATH OTP Client

1. Install your 3rd party authenticator app.
2. Launch your authenticator app and tap the "+" icon or the "Add Account" button to add a new account.
3. Select "Scan Barcode" or "Scan QR Code" and use your phone's camera to scan this code:
4. Once you have scanned the code, enter the 6-digit verification code generated by the authenticator app and click verify.

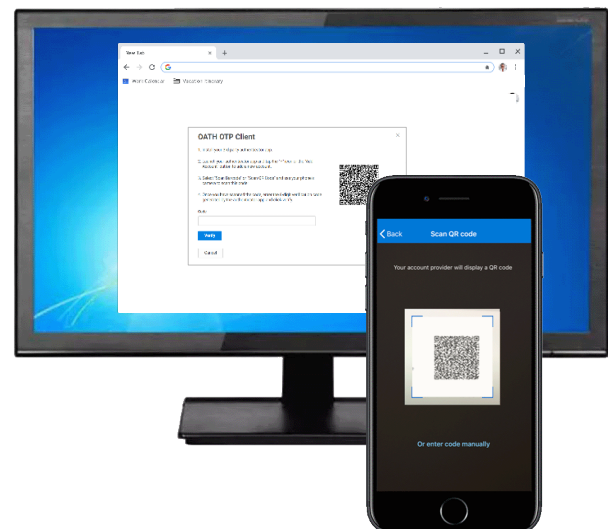
Code

Verify

Cancel

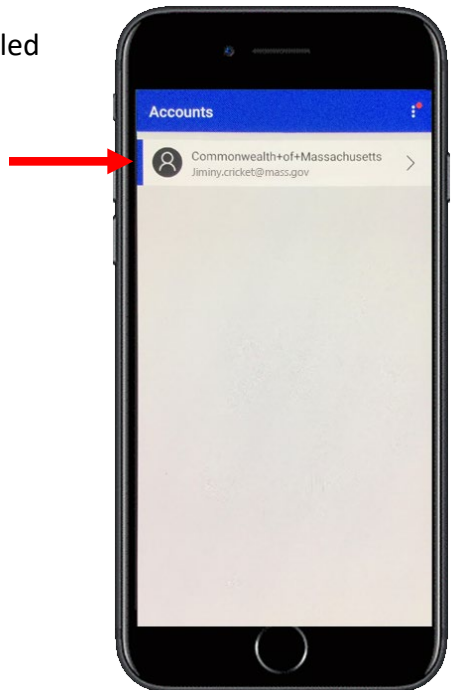
- Using the **Microsoft Authenticator** app, scan the QR code displayed in the web browser.

NOTE: Do not close the **OATH OTP Client** window after scanning.



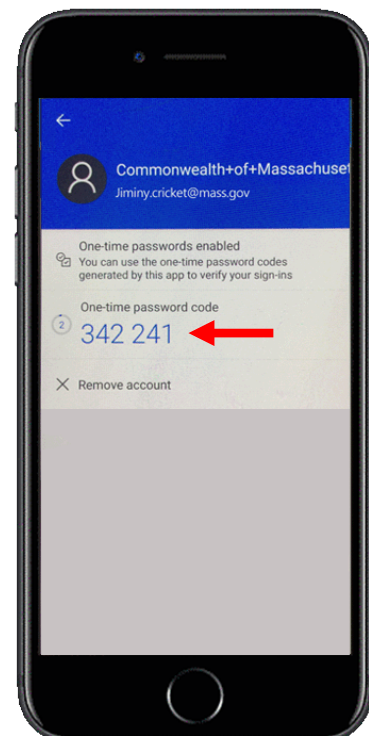


- A successful scan will add a new account called **Commonwealth+of+Massachusetts**.
- Tap on the account.



- A **one-time password code** is displayed and provided for authentication.

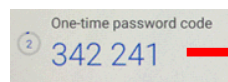
NOTE: The password will change every 30 seconds.



- Go back to the MFA user-account window and enter the **one-time password code** in the **Code** field.



- Click **Verify**.



OATH OTP Client

1. Install your 3rd party authenticator app.
2. Launch your authenticator app and tap the "+" icon or the "Add Account" button to add a new account.
3. Select "Scan Barcode" or "Scan QR Code" and use your phone's camera to scan this code:
4. Once you have scanned the code, enter the 6-digit verification code generated by the authenticator app and click verify.

Code

342 241

Verify

Cancel

- Successful verification will display **Oath OTP verified!**

- Click **Close**.

OATH OTP Client

1. Install your 3rd party authenticator app.
2. Launch your authenticator app and tap the "+" icon or the "Add Account" button to add a new account.
3. Select "Scan Barcode" or "Scan QR Code" and use your phone's camera to scan this code:
4. Once you have scanned the code, enter the 6-digit verification code generated by the authenticator app and click verify.

Code

515327

OATH OTP verified!

Close

Step 11

After re-enrollment in MFA, **reboot the computer.**



UNINSTALL LEGACY VPN CLIENT

Confirm Legacy VPN Client

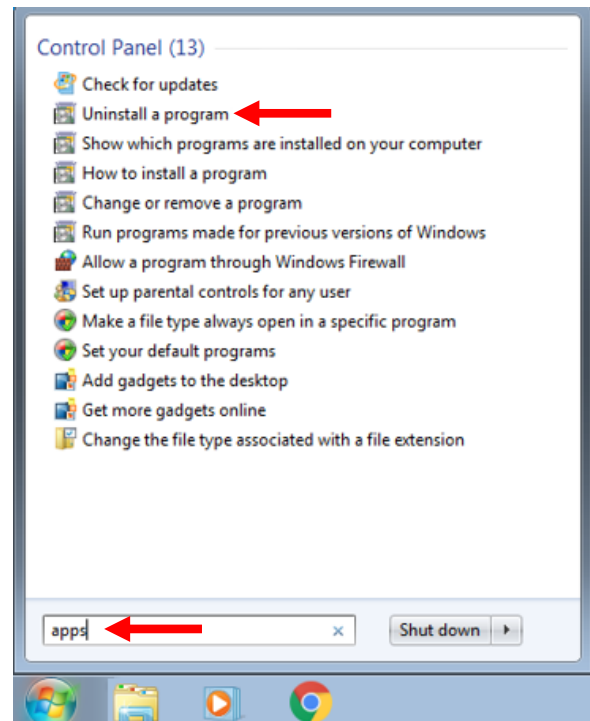
- Step 1** Confirm the legacy VPN program (**Pulse Secure**) is on the system.

Windows 7

- Click the **Windows Start** icon () on the taskbar.



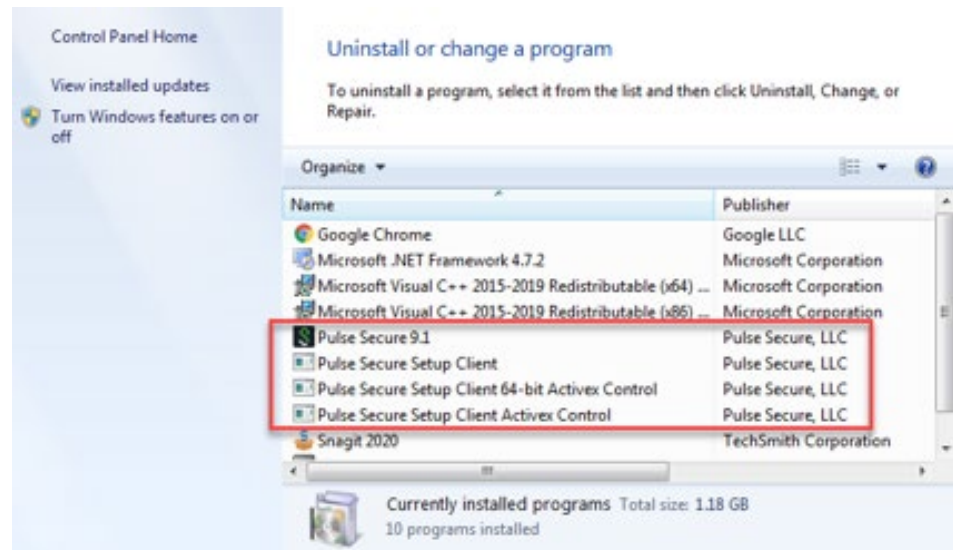
- In the search field, enter **apps**.
- When the search results appear, click **Uninstall a program**.



- The **Uninstall or change a program** window appears.



- Identify all items starting with the word **Pulse Secure** by scrolling through the list of programs.



- If Pulse items are not present, **skip the Uninstall Legacy VPN Program** section and go the the [Install New VPN section](#).

Windows 10

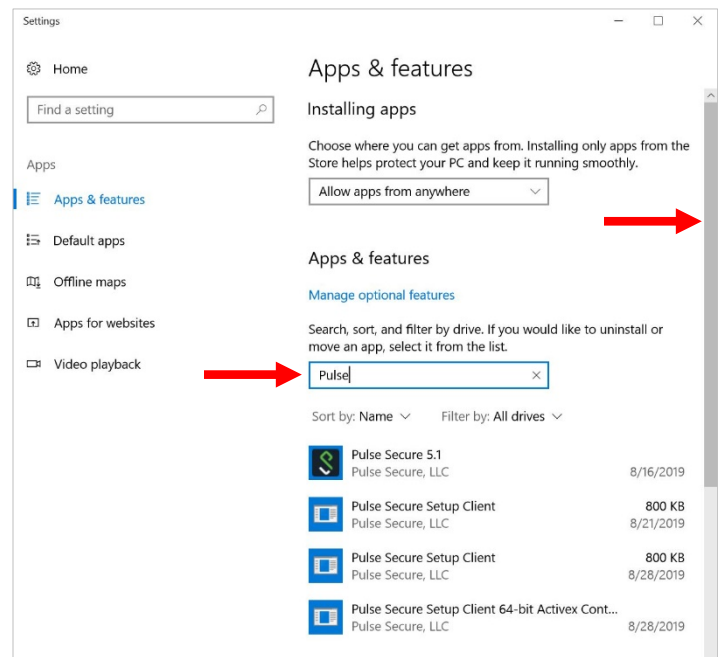
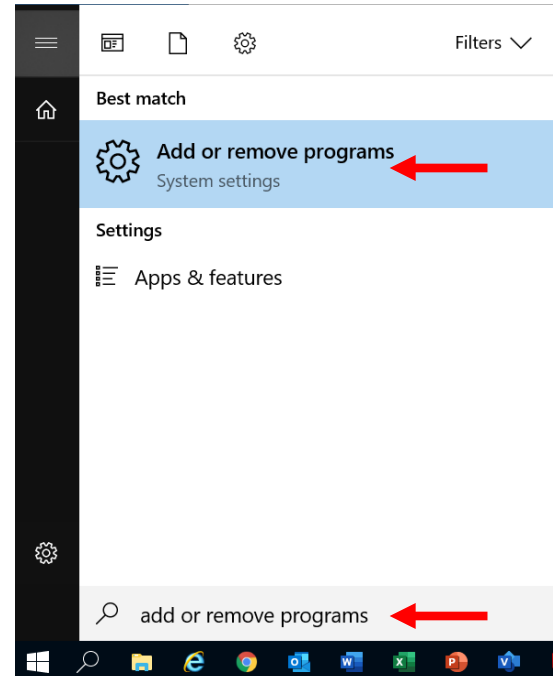
- Click the **Windows Start** icon () in the taskbar.



- Press the **Space bar** to reveal the search field.
- In the search field enter **add or remove programs**.



- When the search results appear, click **Add or remove programs**.
- The **Apps & features** window appears.
- Identify all items starting with the word **Pulse Secure** by scrolling through the list of programs or entering the word in the **Search this list** field.



- If Pulse Secure items are not present, **skip the Uninstall Legacy VPN Program section** and go the the [Install New VPN section](#).

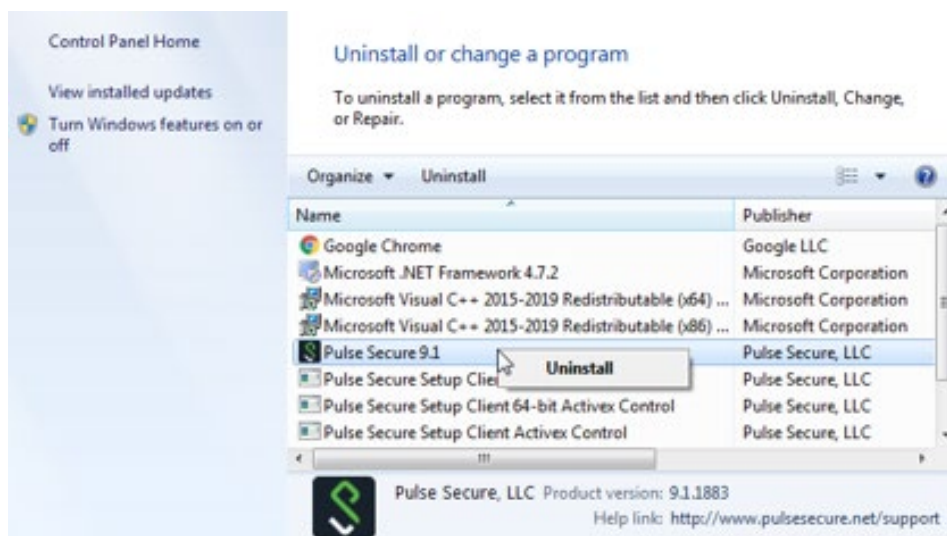


Step 1 If Pulse items are present, proceed with unistalling each item.

NOTE: Be diligent and avoid inadvertently uninstalling items that are not Pulse Secure related. Doing so may result in deleting or damaging work tools or causing issues with the computer system.

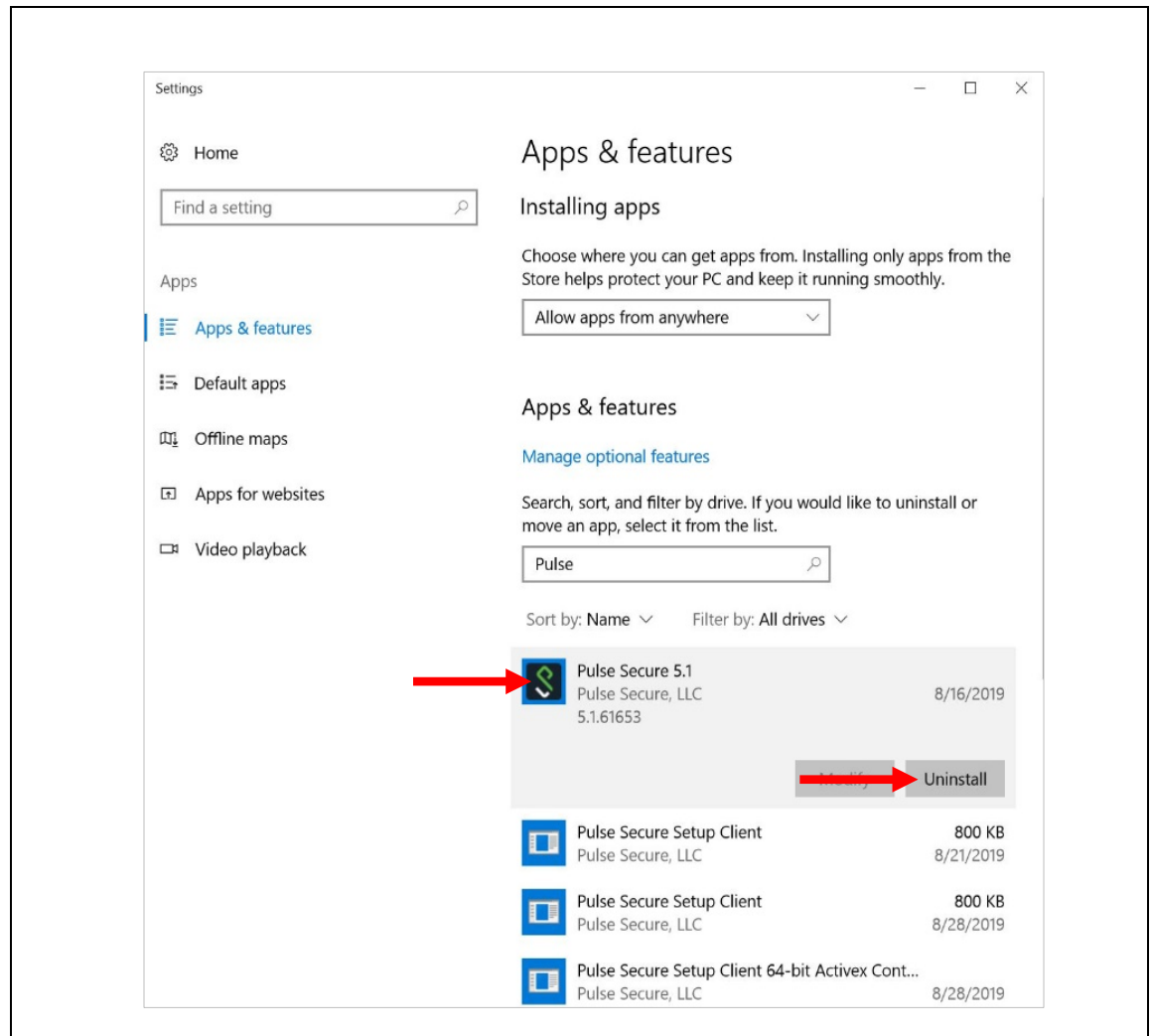
Windows 7

- Make sure that VPN is disconnected and not being used.
- Right click on each **Pulse Secure** item.
- Click **Uninstall** in the pop-up window.
- **Repeat the last two bullet-points** until all Pulse Secure items are removed.

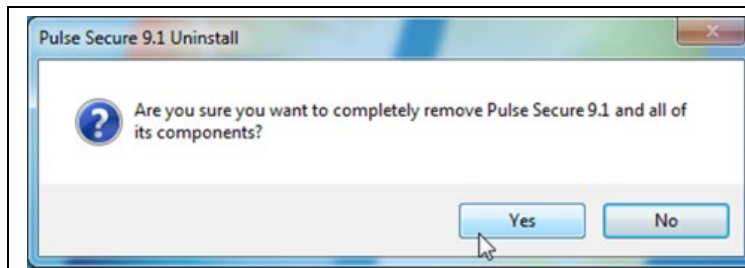


Windows 10

- Make sure that VPN is disconnected and not being used.
- Click on each **Pulse Secure** item.
- Click the **Uninstall** button that appears in the lower-right corner of the item description.
- **Repeat the last two bullet-points** until all Pulse Secure items are removed.

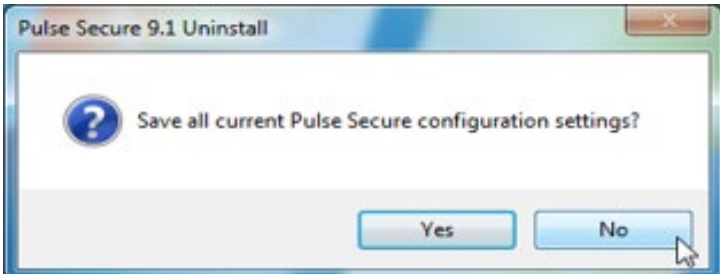
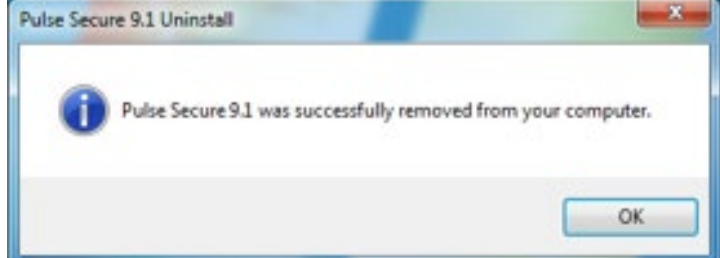
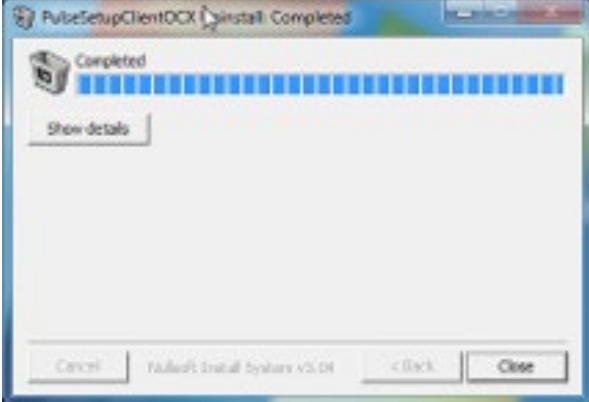


Step 2 During the unistall process, the followig messages may appear:



Click **Yes**.



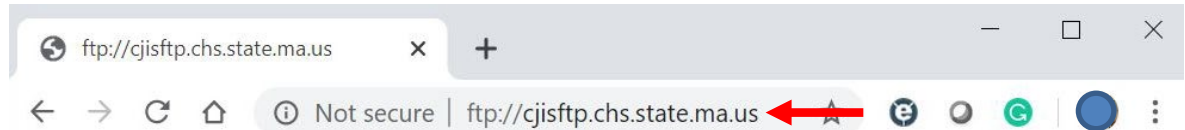
		Click No .
		Click OK .
		When this process is Completed , click Close .
Step 3	After uninstalling all Pulse Secure items, reboot the computer .	

INSTALL NEW VPN CLIENT

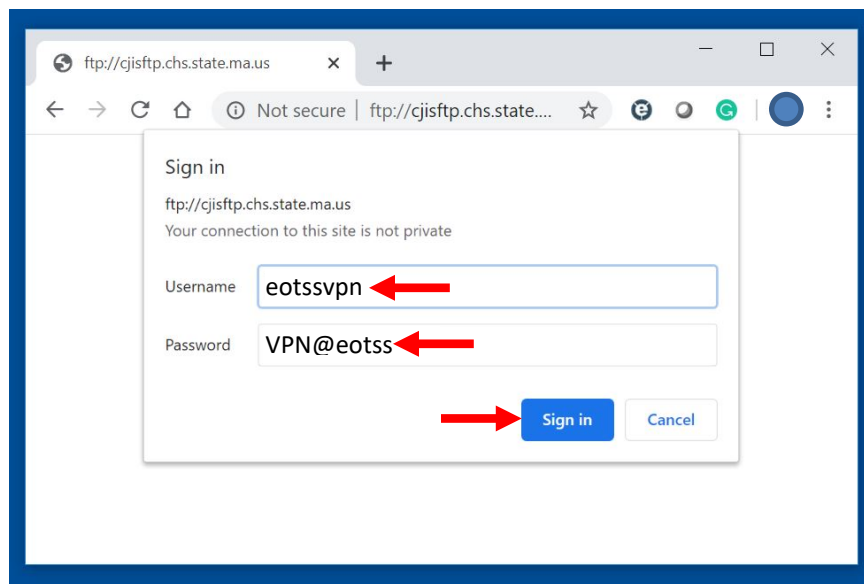
[Download New VPN Client](#)

**Step 1**

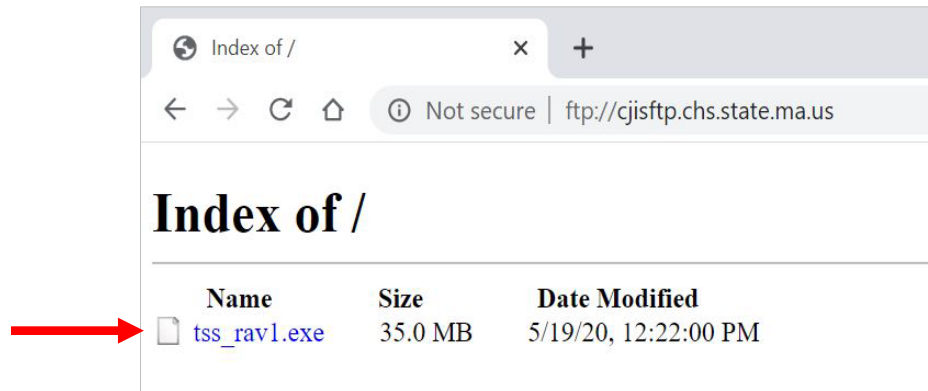
- On a web browser, go to the following webpage: **ftp://cjisftp.chs.state.ma.us**
 - The **URL must be copied and pasted** into a web browser's address bar.

**Step 2**

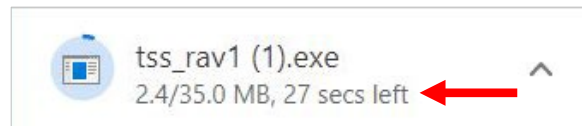
- A **Sign in** pop-up window will appear:
 - Enter this username: **eotssvpn**
 - Enter this password: **VPN@eotss** (case sensitive).
 - Click **Sign in**.

**Step 3**

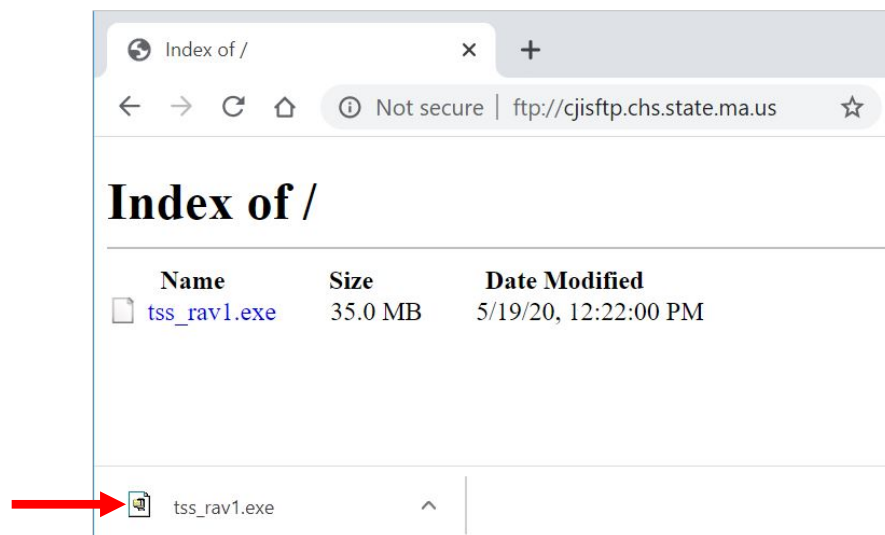
- Click **tss_rav1.exe** to download the VPN installation file to the computer.

**Step 4**

- **Wait** for the download to be completed.
 - The progress of the download can be monitored in the box located on the lower-left corner of the web browser.



- Once the download is complete, click the **tss_rav1.exe** box to open the installation file.



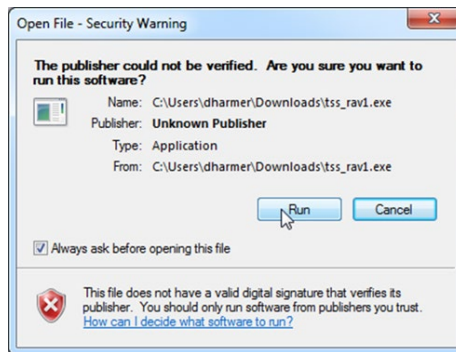
following messages will appear:

- The

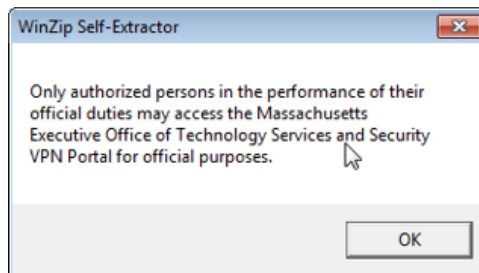


Windows 7

- Click **Run**.

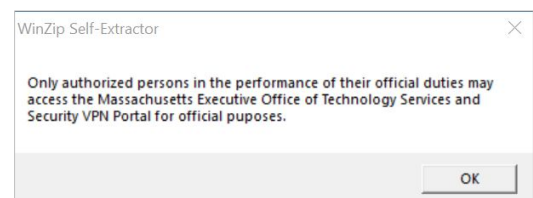


- Click **OK**.

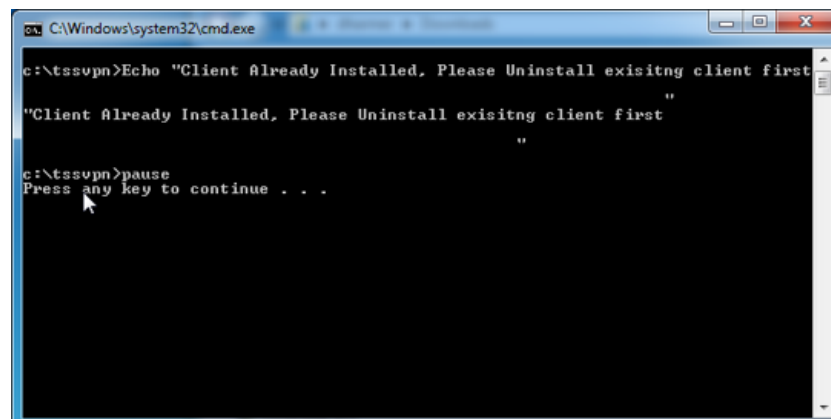


Windows 10

- Click **OK**.

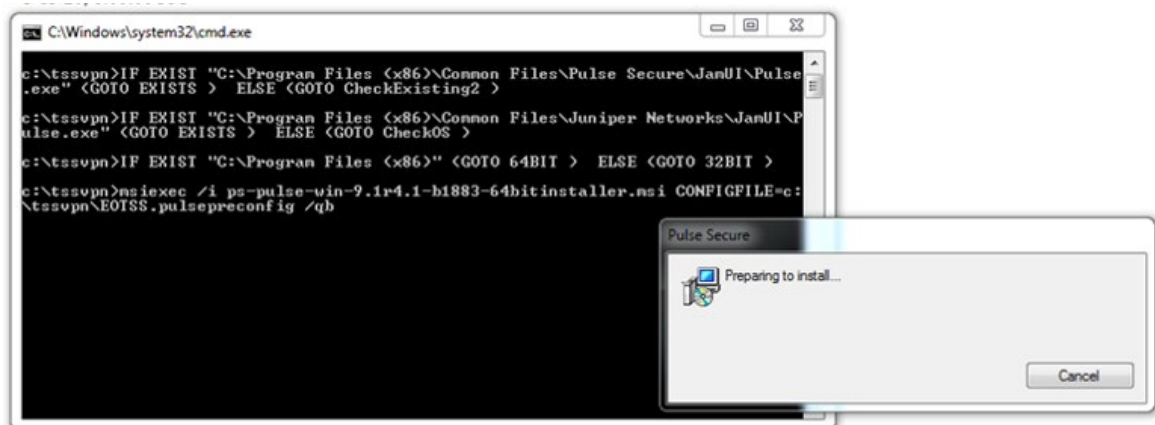


- If the below **warning message** appears, Pulse Secure items are still on the system.
 - Repeat all steps in the [UNINSTALL LEGACY VPN section](#).
 - Ensure all **Pulse Secure** items have been uninstalled.
 - Repeat the **INSTALL NEW VPN** section.



**Step 5**

- If there are no warning messages, Pulse Secure will proceed with the installation process.



- The following message will appear:

Windows 7 (no Windows 10 prompt)

- Click **Yes**

**Step 6**

The installation was successful when this image appears:



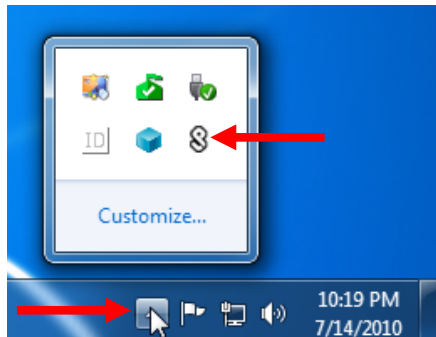


Initiating VPN Logon

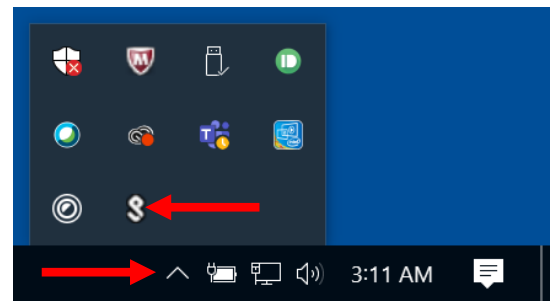
Step 1 Open Pulse Secure:


- At the end of the taskbar, click the **arrowhead symbol** to reveal a pop-up window holding **hidden icons**.

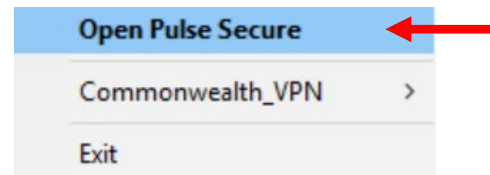
Windows 7



Windows 10

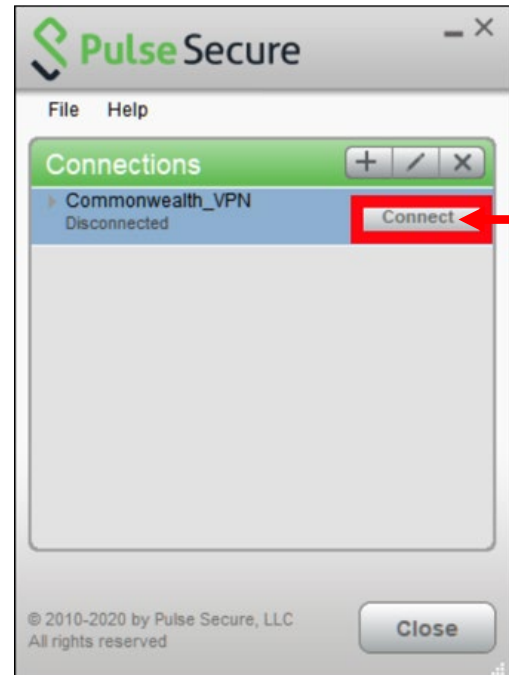
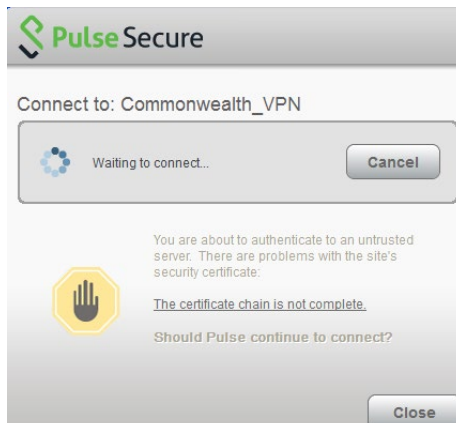


- Click on the Pulse Secure icon ().
- Click on **Open Pulse Secure**.

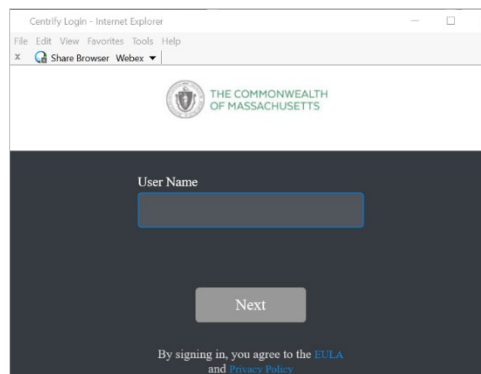


**Step 2** Initiate a VPN connection:

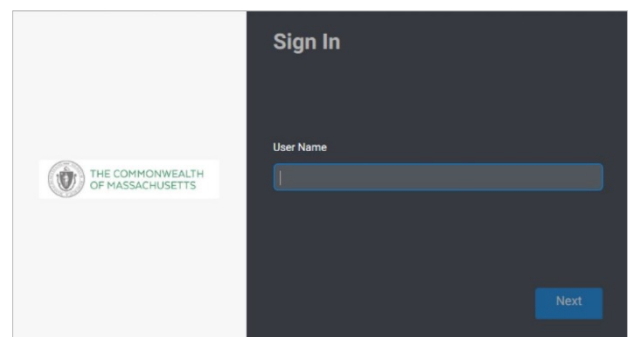
- Click **Connect**.
- If the following window appears, leave it to close on its own.

**Step 3** Login verification with a user name:

- In the **User Name** field, enter a user work email.
(Formats: @mass.gov or massmail.state.ma.us)
- Click **Next**.



OR



**Step 4** Login verification with password:

- In the **Password** field, enter user Windows password.
- Click **Next**.

The screenshot shows a web browser window titled 'Certify Login - Internet Explorer'. The address bar shows 'Share Browser - Webex'. The page header includes the Commonwealth of Massachusetts logo and name. The main content area has a dark background with a 'Password' label, a text input field, and a 'Next' button.

OR

The screenshot shows a dark-themed 'Authentication' window. It includes the Commonwealth of Massachusetts logo and name. The user email 'susan.cantrell@mass.gov' is displayed. There is a 'Password' field, an 'Authentication Method' dropdown menu set to 'OATH OTP Client', and a 'Next' button.

The screenshot shows the 'Authentication Method' dropdown menu with 'OATH OTP Client' selected. A blue 'Next' button is at the bottom.

- Click **Next**.

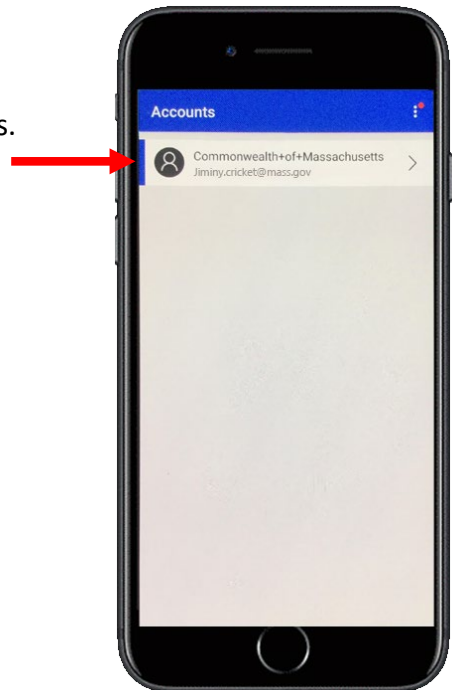
Step 5 Login verification with multi-factor authentication (MFA):

- The **Enter Verification Code** window requires an MFA, obtained in the next few bullet-points.

The screenshot shows a dark-themed 'Authentication (+)' window. It includes the Commonwealth of Massachusetts logo and name. The user email 'susan.cantrell@mass.gov' is displayed. There is an 'Enter Verification Code' label, a text input field, and a 'Next' button.



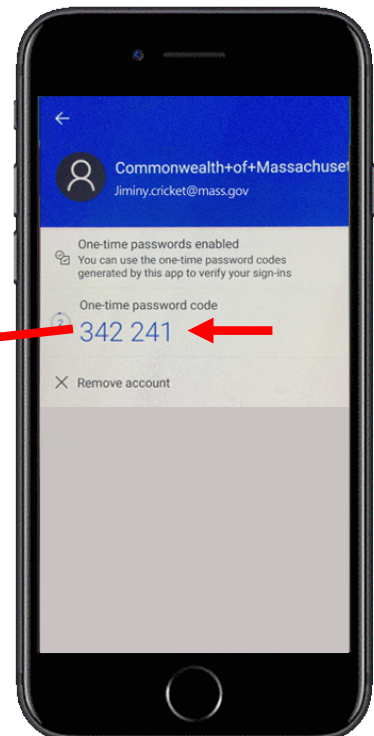
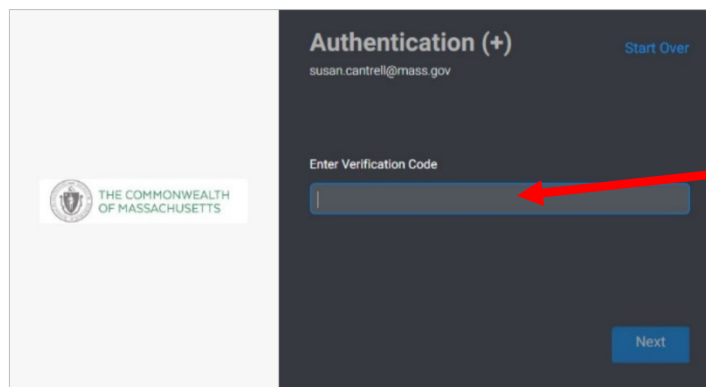
- Open **Microsoft Authenticator** mobile app.
- A screen will display listing all existing accounts.
 - Tap the account **Commonwealth+of+Massachusetts**.



- A **one-time password code** is displayed and provided for authentication.

NOTE: The password will change every 30 seconds.

- Enter the **one-time password code** into the **Enter Verification Code** field.

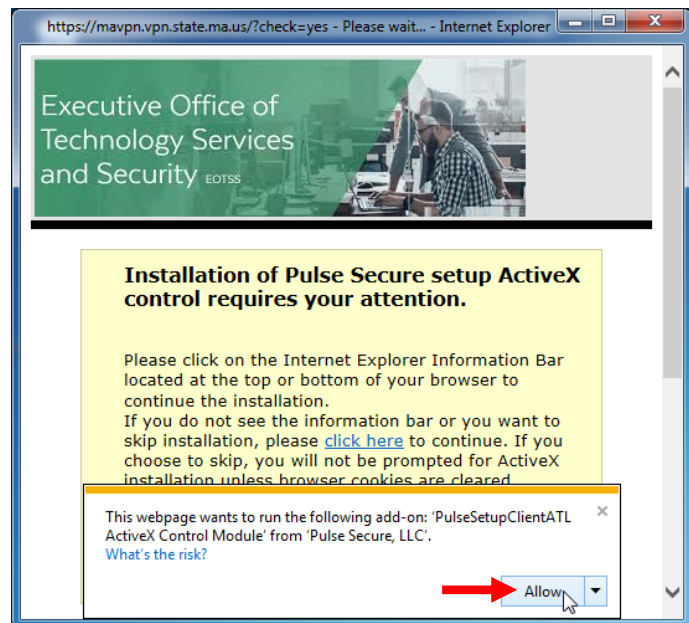


- Click **Next**.

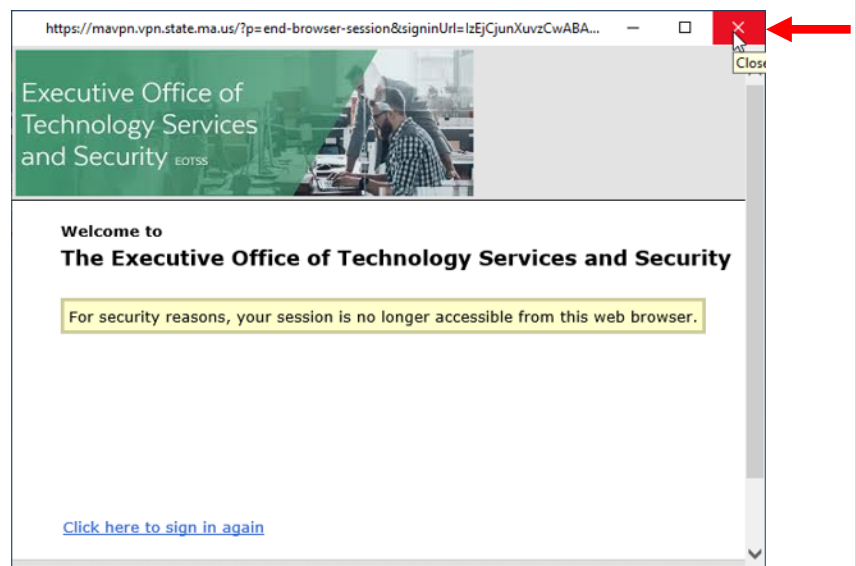
**Step 6**

- If an “ActiveX” message appears, click **Allow**.


NOTE: This is a one-time message seen in the first VPN logon session.

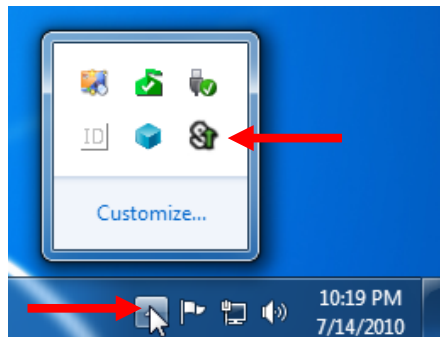
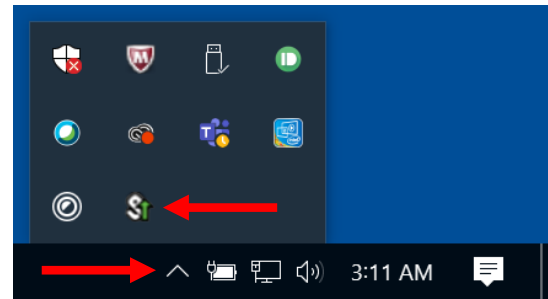
**Step 7**

- Upon completion of configuring VPN, the below message will appear.
- The window should close automatically.
- If the message does not close automatically, click the **X** located in the upper-right corner.



**Step 1** How to confirm VPN is connected:**OPTION 1:**

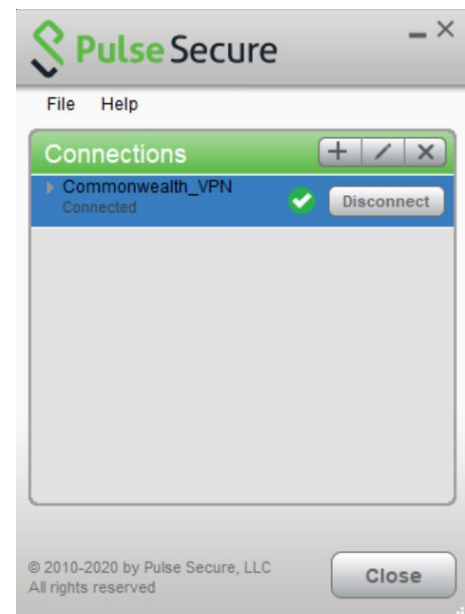
- At the end of the taskbar, click the **arrowhead symbol** to reveal a pop-up window holding **hidden icons**.
- VPN is connected if the **Secure Pulse icon** has an adjacent green arrow that points upward ().

Windows 7**Windows 10****OPTION 2:**

- The **Pulse Secure client interface** can offer indicators to confirm VPN is connected.

INDICATORS:

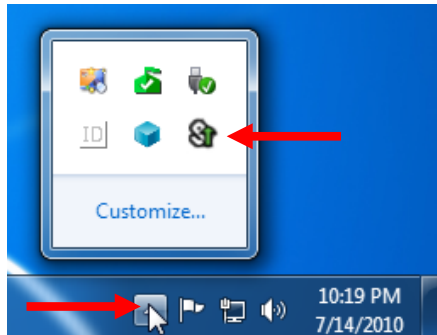
- The word **Connected**, located directly underneath the VPN account indicates VPN's current status.
- The green circle with the white checkmark only appears when VPN is connected.
- The **Disconnect** button indicates that the only action that can be taken is to disconnect from VPN.

**DISCONNECTING FROM VPN CLIENT**

**Step 1** Open Pulse Secure:


- At the end of the taskbar, click the **arrowhead symbol** to reveal a pop-up window holding **hidden icons**.

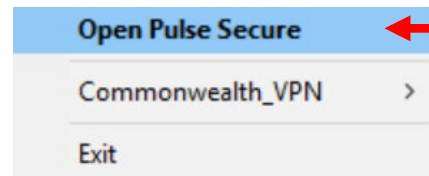
Windows 7



Windows 10



- Click on the Pulse Secure icon ().
- Click on **Open Pulse Secure**

**Step 2** The Pulse Secure client interface will appear:

- Click **Disconnect**.

