

Telework Set-Up



Configuring Devices for Remote Work



Overview:

Purpose: Allowing employees to access systems and functions from outside of the office spaces.

Equipment Needed:

- PC
- Cellphone
- VPN access approval

For the remainder of this document, you will be prompted to answer questions and instructed to move on to different sections. Please note, not all sections applies to everyone. Please use the next slide as the general guide. Each step functions separately but you will need to follow the steps in order.



What Do I Need to Get Started?

1. Laptop (Charged/Plugged-In)
2. State issued iPhone that has been setup
3. The phone number from your state issued iPhone
4. Secure Internet Connection
5. Google Chrome Installed on laptop
6. Your Remote Materials Checklist,
with your IP address and UPN email address



You are going to walk through the steps outlined in the next couple slides. These are your road map. You start with MFA, then set up VPN, and after that you log into your work computer.

Remember, Super Users are accessible if you need help! You aren't alone.

You can reach them by email at:

DTA.COVID-19Support@MassMail.State.MA.US

1. MFA (Multi-factor Authentication) Set Up

- a. Find your Remote Materials Checklist
- b. Set Up your myCentrify Profile
- c. Setup your SMS Authenticator

DTA issued iPhone

2. VPN (Virtual Private Network) Set UP

State Issued Laptop

Install Pulse Secure 2010-2020

3. Access

Log Into VPN through Pulse Secure (Step 2) and MFA authenticator (Step 1)

State Issued Laptop

*Remote Desktop into your
office PC*



➤ State Issued Laptops

1. Set up MFA
 - a. DTA Issued Phone: SMS Authentication
 - b. Personal Phone: SMS Authentication OR Microsoft Authenticator
2. Set up VPN
 - a. Install Pulse Secure 2010-2020
3. Log into VPN (Pulse Secure)
4. Remote Desktop Connection into your office PC
5. Begin work



MFA Set-Up

1

- a. Get your Remote Materials Checklist
- b. Set Up your myCentrify Profile
- c. Setup your Secondary Authenticator

DTA issued iPhone



Use SMS to receive your secondary authenticator



What is Multi-factor Authentication?

- Multi-factor authentication (MFA) refers to the pieces of information you need to provide to gain access to our employee-facing services outside the DTA network.
- Its an added layer of security making it harder for an account to be accessed by outside sources even if a password is compromised. This is essential in ensuring the safety and security of our clients Personally Identifiable Information.



Remote Materials Checklist

1

REMOTE MATERIALS CHECKLIST: **Must Be Completed Before You Leave!**

OVERVIEW

Due to COVID-19 the Department is working on deploying 815 state issued laptops and iPhones so staff can begin teleworking full-time. This is in addition to the 300 laptops and iPhones previously deployed to staff. Equipment may be set up from home, **but before you leave the TAO today, please make sure you have the following information from your TAO Desktop PC. Hold on to this information, you will need it to complete the installation process when you receive your state issued laptop on a later date.**

CHECKLIST ITEMS

Desktop PC Information: You will need the following information in order to set up Remote Desktop Connection. This will allow you to sign into your TAO's Desktop PC from home. This information can be found on the right-hand side of your screen. Before you leave for the day, sign out of your Desktop PC, but DO NOT shut it down.

- I have written down or taken a picture of my Desktop Computer's IP Address.

IP Address:

- I have written down or taken a picture of my Desktop Computer's Name.

Computer Name:

- I have written down or taken a picture of my UPN Email Address.

UPN email Address:

For the next couple of steps, you will need this information.

1a

If you have the Remote Materials Checklist from your office. Keep going moving through these slides, and start to set up your [my.centrify.account](https://my.centrify.com)

If the checklist isn't in your possession for whatever reason, contact the Super Users. Tell them that you do not have your Remote Materials Checklist.

1b

Logging in to Centrify



MFA Set Up: Logging into Centrifly

Type in the web address:
eotss.my.centrifly.com

Sign In

User Name
user@domain or user@suffix

Remember your UPN?

Steps to logging into Centrifly:

1. From an internet browser (ex. Chrome) type in:
eotss.my.centrifly.com

© 2004-2020 Centrifly Corporation. Terms of Use Privacy Policy Powered by Centrifly

MFA Set Up: Logging into Centrifly



Steps to logging into Centrifly (continued):

2. Enter your UPN address that you looked up earlier (or paste it if you copied it)
3. Click Next

© 20



MFA Set Up: Logging into Centrifly

User Portal

https://eotss.my.centrifly.com/my?customerId=AAQ0416

Authentication [Start Over](#)

Steven.Pavao@MassMail.State.MA.US

Password

Next

Enter the same password you use to log in to your computer at the beginning of the day

Pavao, Steven (DTA)

Terms of Use Privacy Policy Powered by Centrifly

Steps to logging into Centrifly (continued):

4. Enter the password you use to log in to your work computer
5. Click Next

MFA Set Up: Logging into Centrify

User Portal

https://eotss.my.centrify.com/my?customerId=AAQ0416#TXlBcHBz

Centrify

Welcome

Use this guide to configure your account security settings.

Steps to logging into Centrify (continued):

6. Click Get Started

[Get Started](#)

MFA Set Up: Logging into Centrify

Centrify

Authentication Factor Setup

Welcome to the User Portal. Before we get started, please choose and setup 1 factors required for Multifactor Authentication. We require Multifactor Authentication when you sign in to the user portal or an application from the user portal.

Text Message
Pending

Mobile Number *

Enter number of the mobile phone provided to you

Save

Steps to logging into Centrify (continued):

- 7) Enter the phone number of the mobile phone provided to you
- 8) Click Done

0 of 1 required mechanisms configured **Done**

MFA Set Up: Logging into Centrifly

The screenshot shows a web browser window with the URL <https://eotss.my.centrify.com/my?customerId=AAQ0416#TXlBcHBz>. The page title is "User Portal". The main content area displays the Centrifly logo and the heading "Authentication Factor Setup". Below the heading, there is a message: "Welcome to the User Portal. Before we get started, please choose and setup 1 factors required for Multifactor Authentication. We require Multifactor Authentication when you sign in to the user portal or an application from the user portal." A "Text Message" status is shown as "Pending". A modal window titled "Authentication Required" is overlaid on the page. It contains a "User Name" field with the value "Steven.Pavao@massmail.state.ma.us" and a "Password" field with a red asterisk and a red exclamation mark icon. Below the password field are "Proceed" and "Cancel" buttons. A yellow callout box with the text "Re-enter your password" and a red arrow pointing to the password field is positioned to the left of the modal. A white box with a black border contains the following text: "Steps to logging into Centrifly (continued): 9. Enter the password you use to login to your work computer once again. 10. Click Proceed".

Authentication Required

User Name
Steven.Pavao@massmail.state.ma.us

Password *

Proceed Cancel

Re-enter your password

Steps to logging into Centrifly (continued):

9. Enter the password you use to login to your work computer once again.
10. Click Proceed

MFA Set Up: Logging into Centrify

The screenshot shows a web browser window with the URL `https://eotss.my.centrify.com/my?customerId=AAQ0416#TXIBcHBz`. The page header includes the logo for THE COMMONWEALTH OF MASSACHUSETTS and the user name Pavao, Steven (DTA). The navigation menu contains 'Apps', 'Devices', 'Activity', and 'Account'. A notification banner states: 'You have not yet set up your Phone PIN. Click [here](#) to setup now.' Below the navigation, there is a search bar for apps and an 'Add Apps' button. On the left, there are two app tiles: 'Install Browser Extension' and 'Office 365'. A large green box in the center of the page contains the text: 'Congratulations! You're on your way to establishing your VPN connection!'.

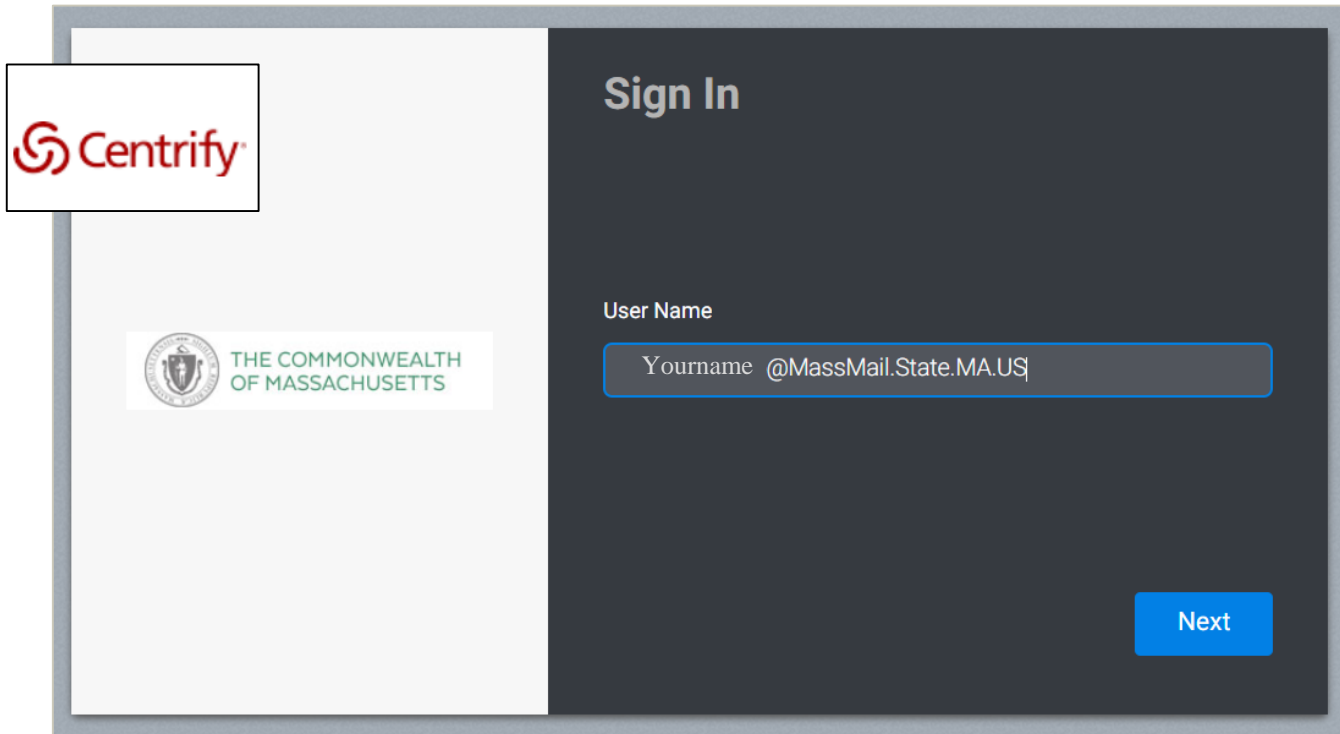
1c

Setting Up Multi-factor Authentication (MFA)



How Do I Set Up MFA?

Step 1: Log In to Centrify using your UPN and Password



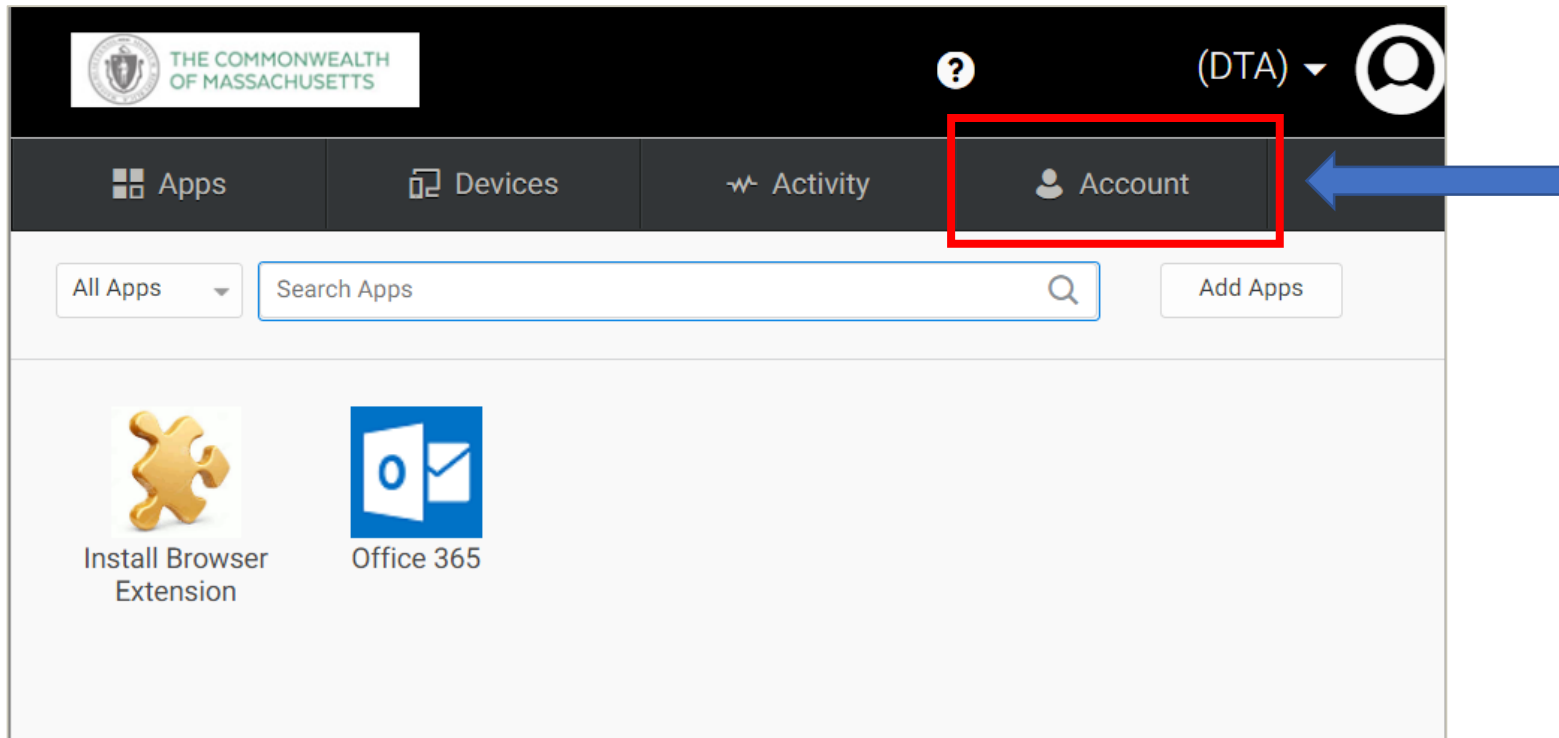
The screenshot displays the Centrify login interface. On the left, there is a white box with the Centrify logo and another white box with the Commonwealth of Massachusetts logo. The main area is dark grey with the text 'Sign In' at the top. Below this, the label 'User Name' is positioned above a text input field. The input field contains the text 'Yourname @MassMail.State.MA.US'. At the bottom right of the dark grey area, there is a blue button labeled 'Next'.

Quick Tip: Your password is the same password you use to log in to your work computer.

*For further assistance logging in to Centrify, refer to the “Finding your User Principal Name (UPN) and Logging into Centrify” guide.

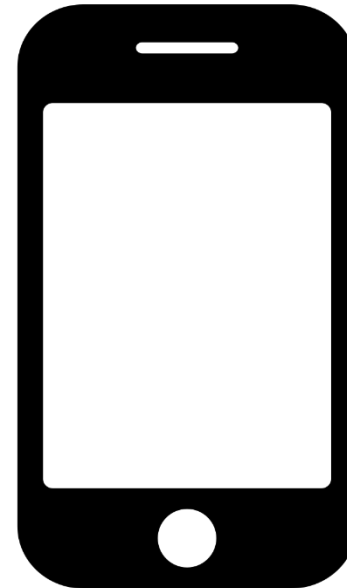
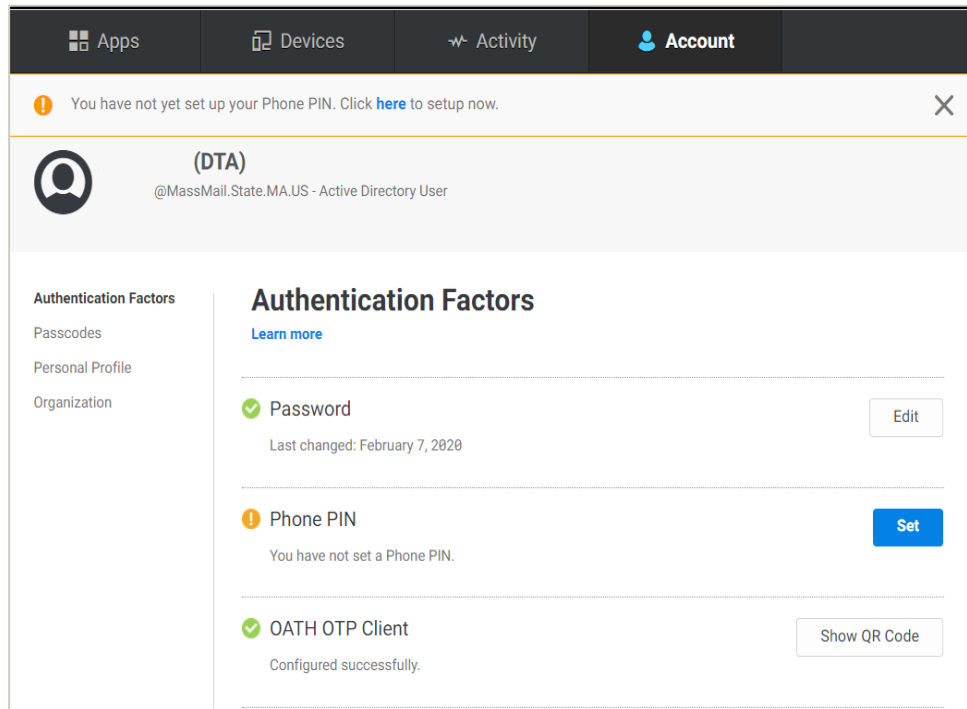
How Do I Set Up MFA?

Step 2 : Select Account.



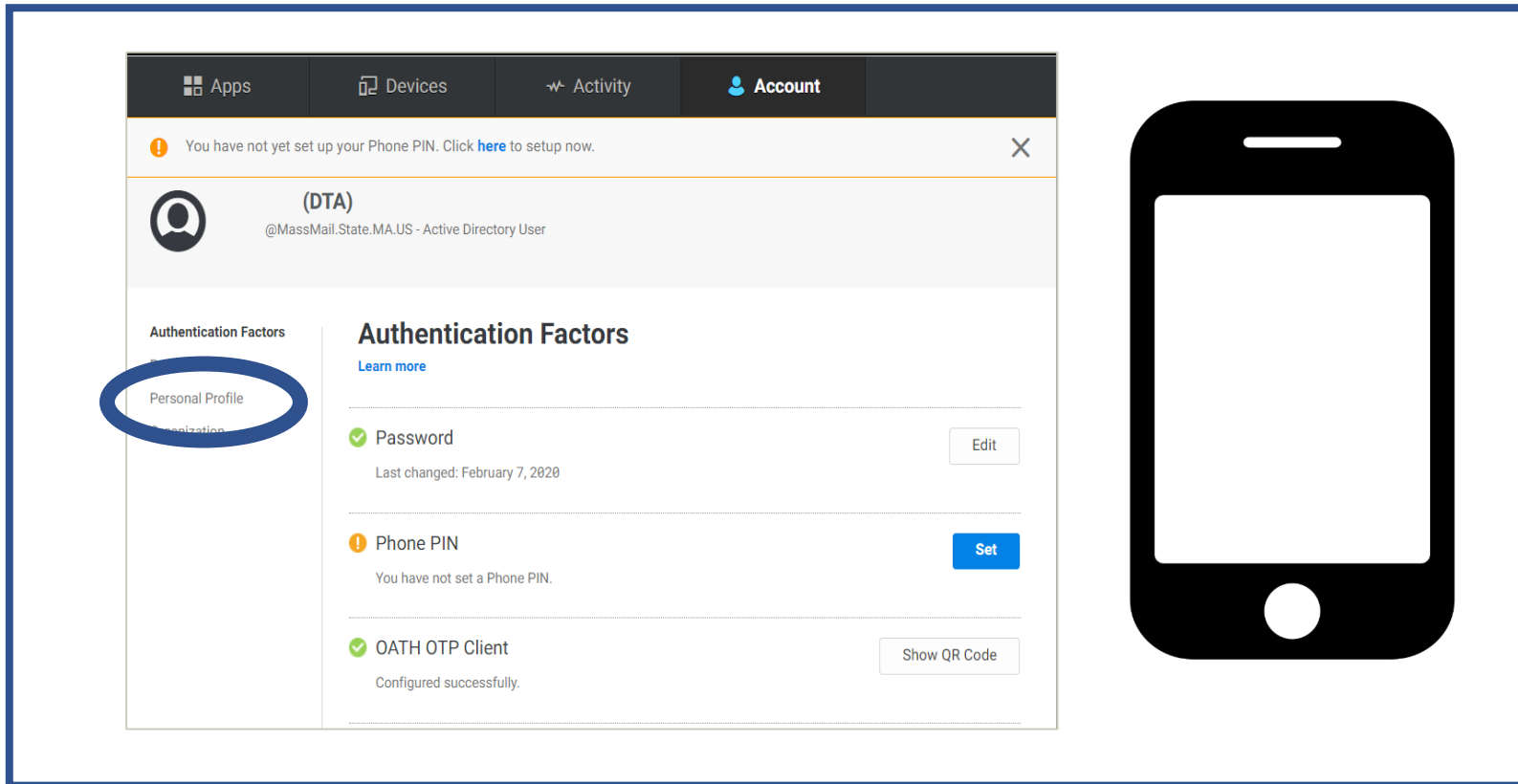
How Do I Set Up MFA?

Step 3: For this step, you will need the Centrify webpage open on your computer and you will need your smartphone readily available.



How Do I Set Up MFA?

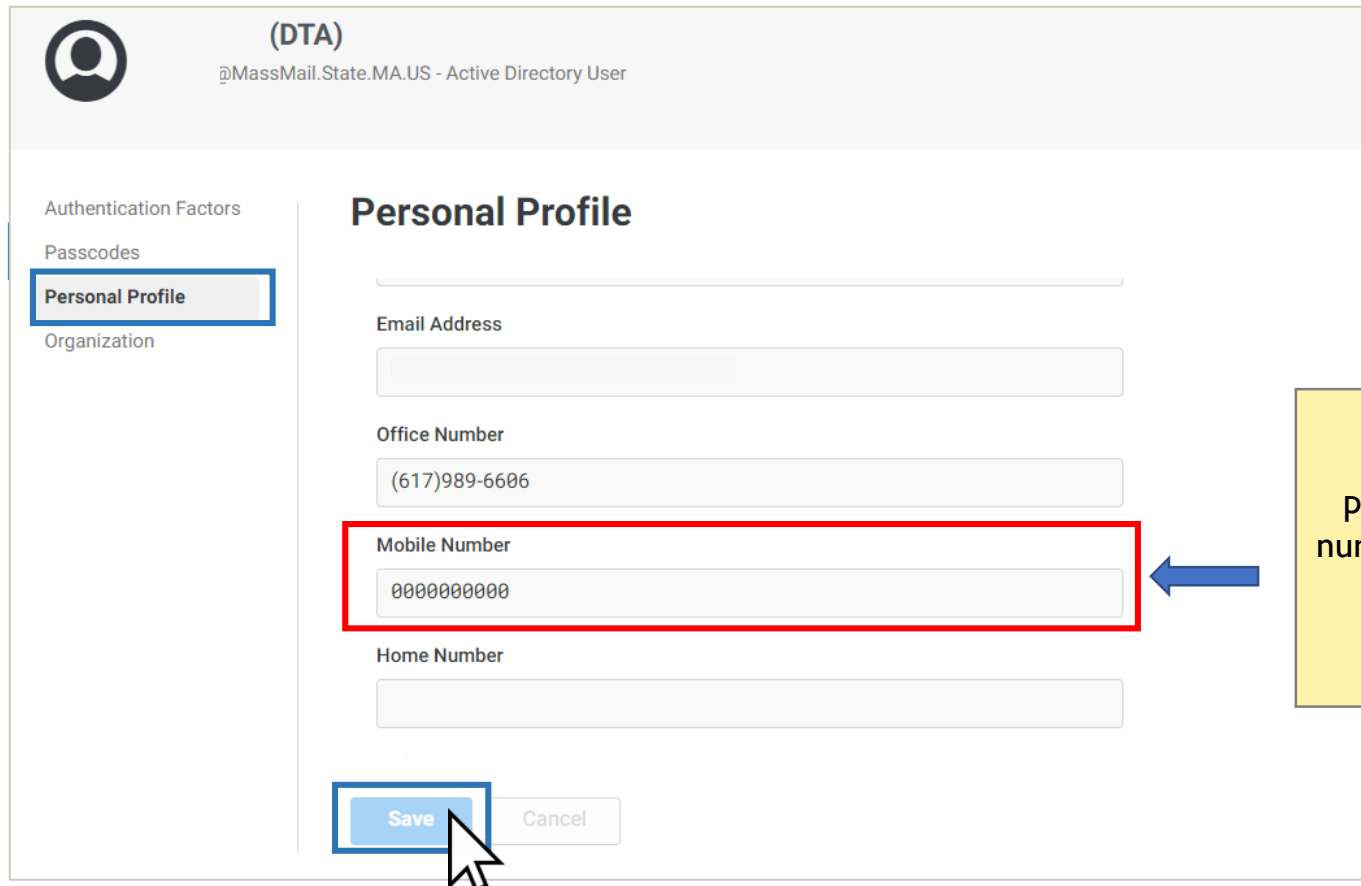
Step 4: Click Personal Profile on the left hand side. Denoted by the circle below



The screenshot shows the Microsoft account management interface. At the top, there are navigation tabs for 'Apps', 'Devices', 'Activity', and 'Account'. Below the tabs, a notification states: 'You have not yet set up your Phone PIN. Click [here](#) to setup now.' The main content area is titled '(DTA) @MassMail.State.MA.US - Active Directory User'. On the left sidebar, under 'Authentication Factors', the 'Personal Profile' option is circled in blue. The main content area lists three authentication factors: 'Password' (last changed February 7, 2020), 'Phone PIN' (not set), and 'OATH OTP Client' (configured successfully). A 'Set' button is visible next to the Phone PIN entry. To the right of the screenshot is a black silhouette of a smartphone.

How Do I Set Up MFA?

Step 5: Click the “Edit” button, scroll down and enter the DTA Issued mobile number here.



The screenshot shows the DTA (Data Transfer Agent) interface for a user named @MassMail.State.MA.US. The 'Personal Profile' section is active, showing fields for Email Address, Office Number, Mobile Number, and Home Number. The 'Mobile Number' field is highlighted with a red border and contains the placeholder '0000000000'. A blue arrow points from a yellow callout box to this field. The 'Save' button is highlighted with a blue border and a mouse cursor is over it.

(DTA)
@MassMail.State.MA.US - Active Directory User

Authentication Factors
Passcodes
Personal Profile
Organization

Personal Profile

Email Address

Office Number
(617)989-6606

Mobile Number
0000000000

Home Number

Save Cancel

For some, this may be prepopulated with the phone number entered when setting up the MFA.

VPN Set Up



State Issued Laptop

How do I install this VPN?

*Install Pulse Secure
2010-2020*

2

2

Installing Pulse Secure





Did you already install
Google Chrome on your
DTA issued laptop?

Yes I did.

Keep going to the
next slide.

No...

Go to your laptop set up
guide and complete those
steps before you continue.



Open Google Chrome

Follow the links below to get to the page to download the Pulse Secure application.



If you are reading this on a computer skip two slides and there is clickable link 😊



In Google Chrome:

- 1- In the middle of the screen, click inside of the search bar.
- 2 – Type “Mass.gov telework”
- 3 – Click on “Telework for Commonwealth Employees”
- 4 – Scroll down and click on “Find Technical Resources for Remote Access”
- 5 – Click on the “EOTSS Remove Access VPN (after 3/17/20)” option
- 6- Scroll down slightly and click on the “Download the EOTSS VPN client” option

Steps 5 and 6 will be visually represented on the next slide



Downloading Pulse Secure Software

The screenshot shows a web browser window with the URL `telework.digital.mass.gov/-M2eNTJtfqjnJw4lnYnq/?_ga=2.70493776.116395930.1587074890-707352183.1570638780`. The page title is "Guide to Teleworking for MA State Employees". The left sidebar contains a "VPN" section with a list of links. Two links are highlighted with blue boxes and numbered callouts: "EOTSS Remote Access VPN (after 3/17/20)" with callout 5, and "Download the EOTSS VPN client" with callout 6. The main content area has a heading "Guide to Teleworking for MA State Employees" and a paragraph: "Welcome to the Mass Telework Knowledge Base. From VPN to the Office productivity suite, you can find useful information about the technology and tools that can help you work remotely." Below this is a warning box with a red triangle icon and the text: "The Service Desk will not troubleshoot home wifi connectivity issues. If you are unable to connect to your home wifi, please contact your Internet Service Provider (ISP)."

Mass Telework Knowledge Base

Search...

VPN

Guidelines on VPN Use

EOTSS Remote Access VPN (after 3/17/20)

Getting started on the EOTSS VPN

Remove an old VPN client before installing a new one

Download the EOTSS VPN client

Unpack and install the EOTSS VPN client

Using the EOTSS VPN Client

Disconnecting from the VPN

Connect to your on-premise computer using Remote Desktop

5 Guide to Teleworking for MA State Employees

Welcome to the Mass Telework Knowledge Base. From VPN to the Office productivity suite, you can find useful information about the technology and tools that can help you work remotely.

6

⚠ The Service Desk will not troubleshoot home wifi connectivity issues. If you are unable to connect to your home wifi, please contact your Internet Service Provider (ISP).

Open Google Chrome

The website below will give you the link to download Pulse secure.

(Hold the ctrl button to the left of the space bar and click on the link below to open the page)

<https://telework.digital.mass.gov/-M2eNTjtfqjnJw4lnYnq/vpn/eotss-vpn-post-3-17-20/downloading-the-eotss-vpn-client>

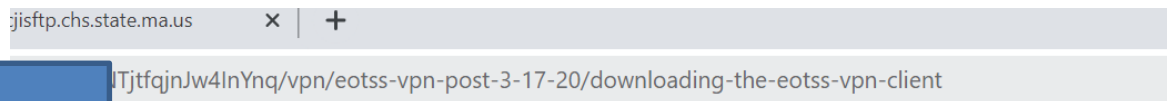


Going to that page will open this screen:

In your Google Chrome window click on the link that is circled on the slide.

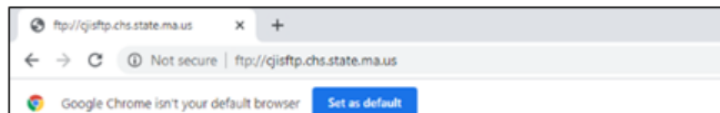
Doing this will open a new page in Google Chrome.

Go the next slide for next steps.

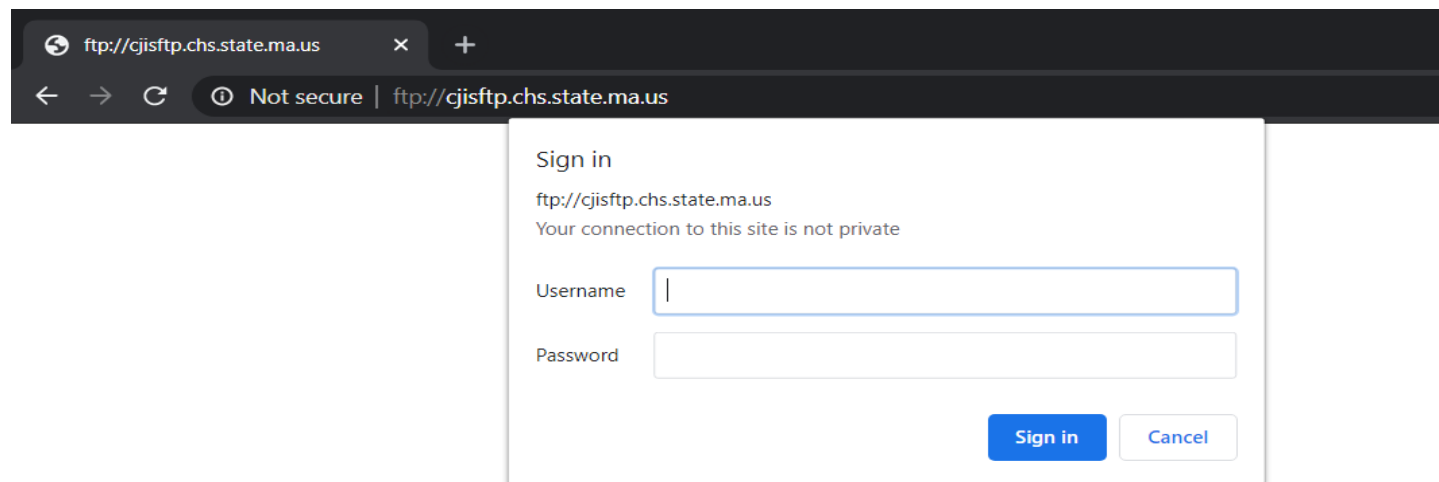


Start Google Chrome

Step 1: In the address/browser line enter <ftp://cjisftp.chs.state.ma.us> and press enter/return.



Going to that page will open this screen:



Username : eotssvpn

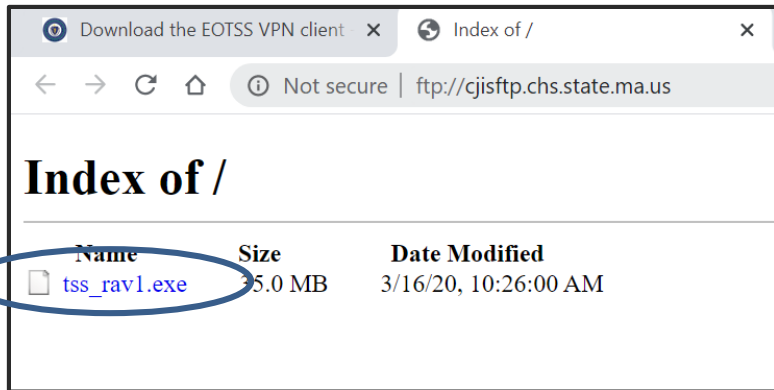
Password: VPN@eotss

The capitals are important please copy these exactly how they are written above.

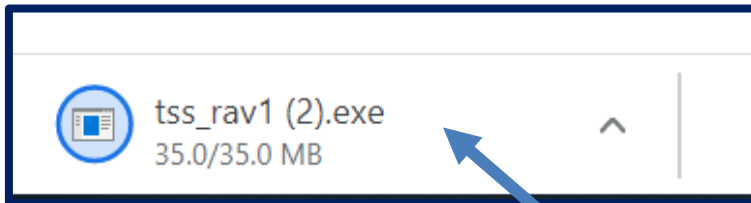
Once these are entered. Click “Sign In”



Signing in will start the download of Pulse Secure:



1 – Click on the tss_rav1.exe

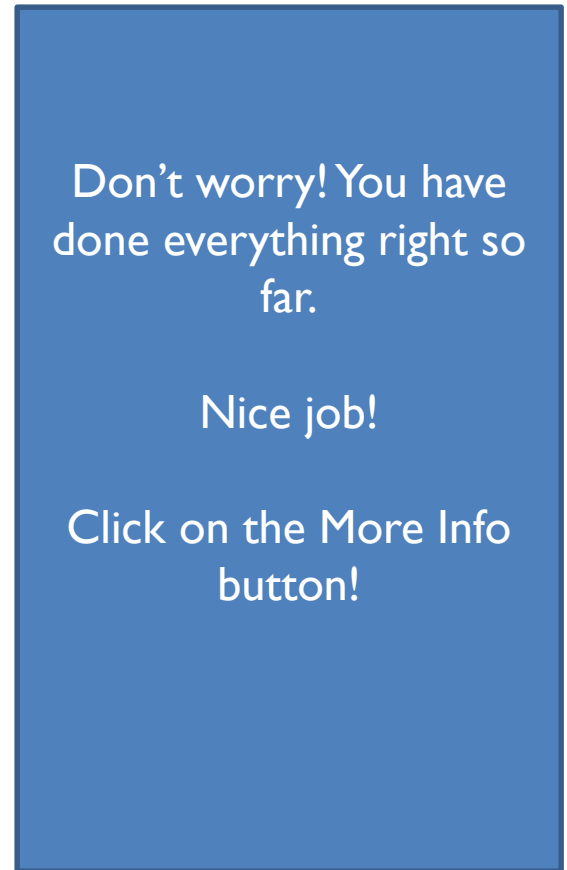
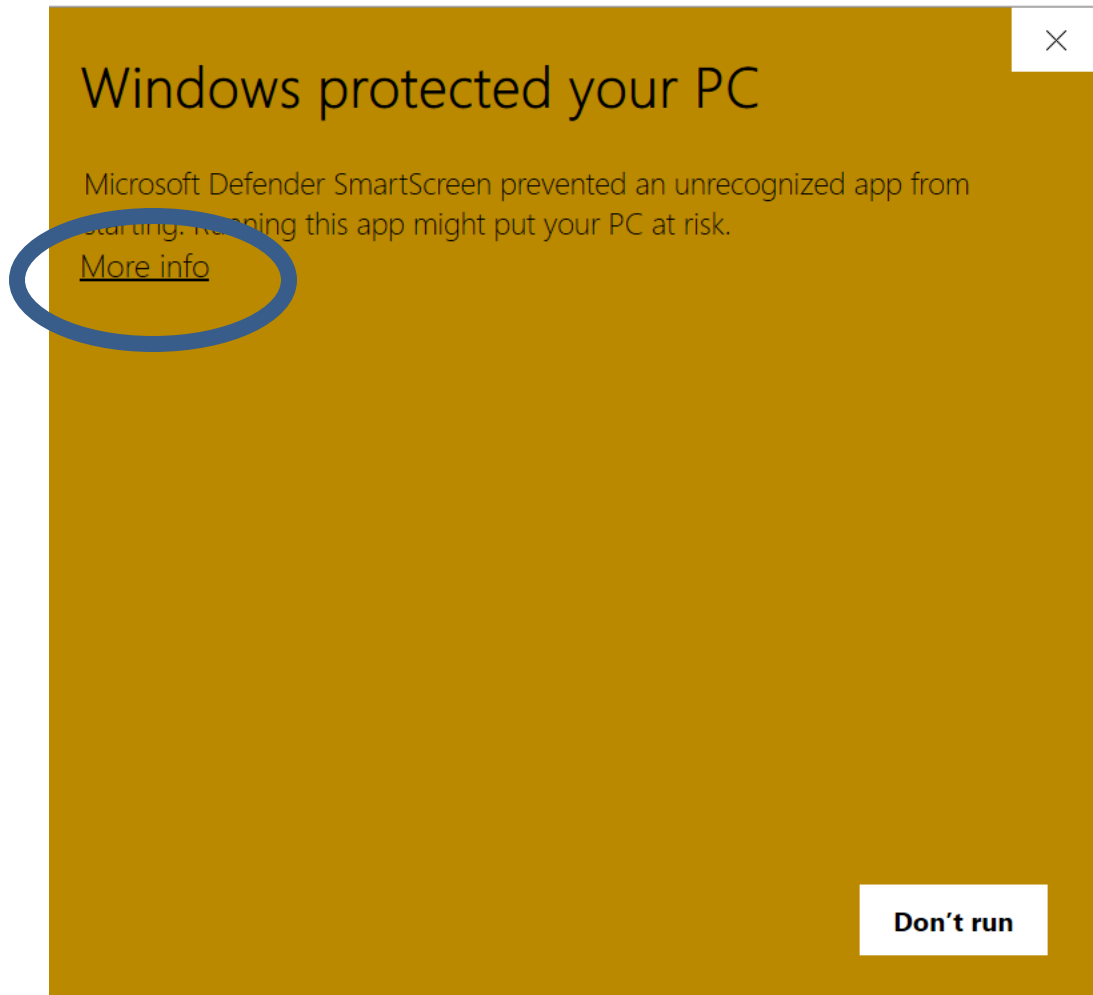


2 – This will start to download.
Located at the bottom of the window

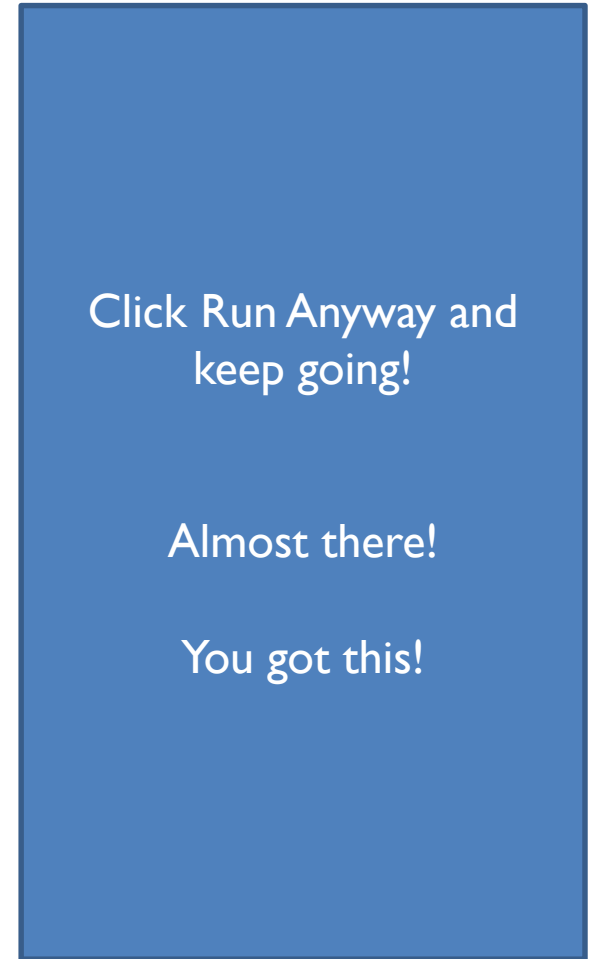
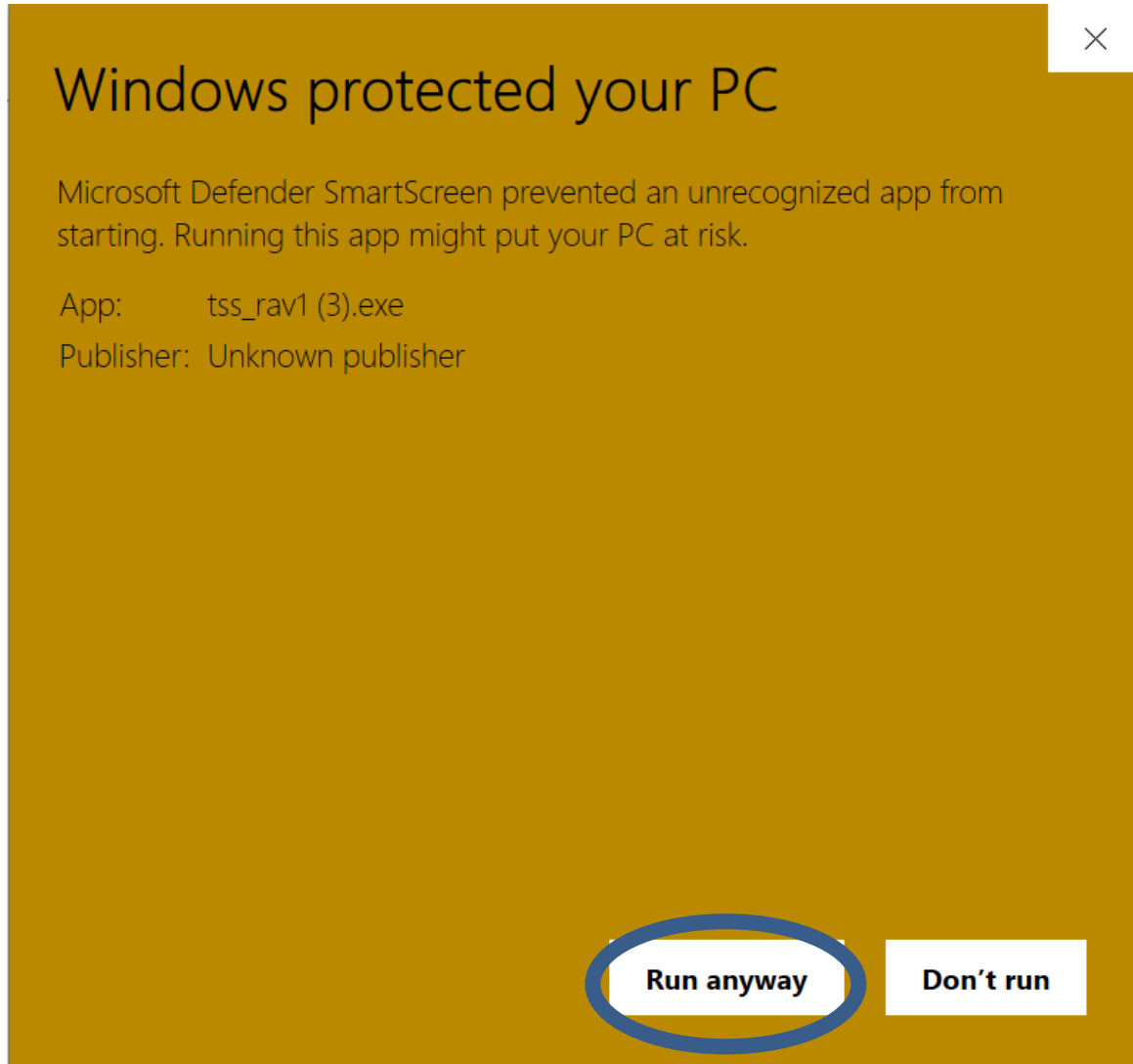
3 – Double click on the tss_rav1.exe
This will open a new window



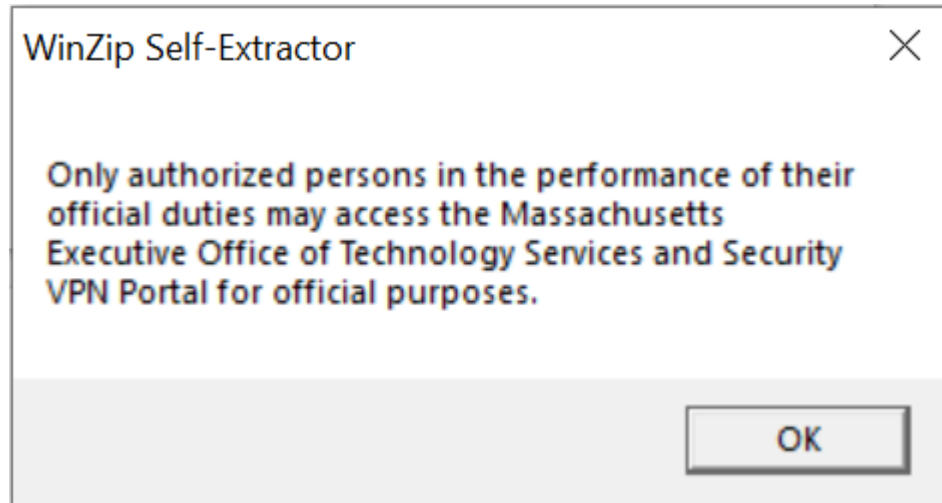
Scary Brown Box... It's okay!



Told you it was okay!



Doing great, almost there!



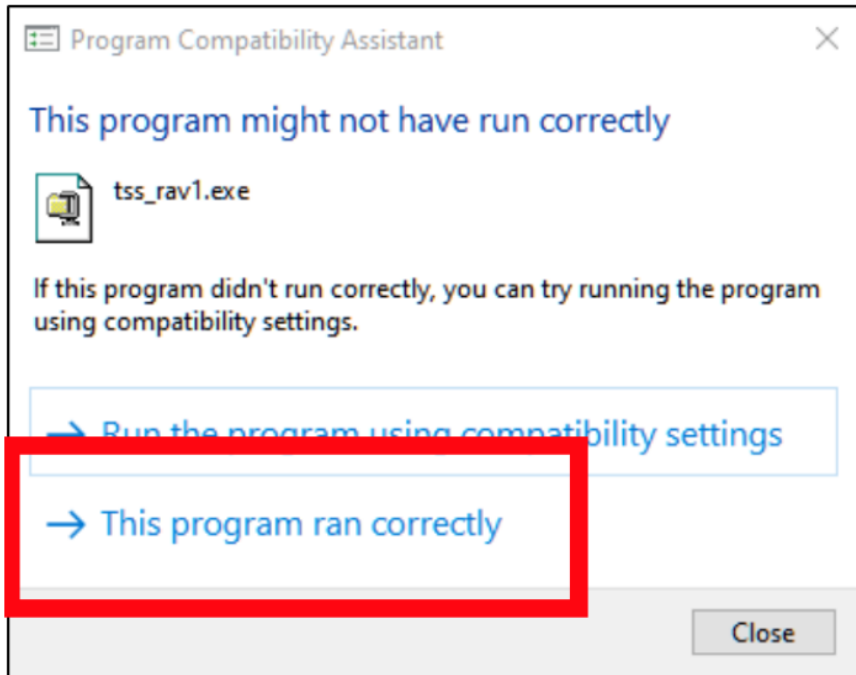
Click "Ok"

This will open some new windows. They are running permissions and installing your VPN.

Take your hands off the keyboard and let them run their course. You've earned a break!



You might see this. Might not.



If you see this screen:

Click “This program can run correctly”

If you don't see this screen:

Keep going!

You might see this. Might not.

```
C:\WINDOWS\system32\cmd.exe

c:\tssvpn>Echo "Client Already Installed, Please Uninstall existng client first
"Client Already Installed, Please Uninstall existng client first

c:\tssvpn>pause
Press any key to continue . . .
```

If you see this screen:
Press any key you want! If you're nervous, I'll choose for you. Press the Space bar.

If you don't see this screen:
Don't worry, just keep going!



At this Point...

YOU DID IT!!!

**Pulse Secure has been
installed!!!**

**Part 3 will show you how to
use it.**



Accessing Telework

3

State Issued Laptop



Log into VPN



Set up Remote
Desktop Connection to
your office PC



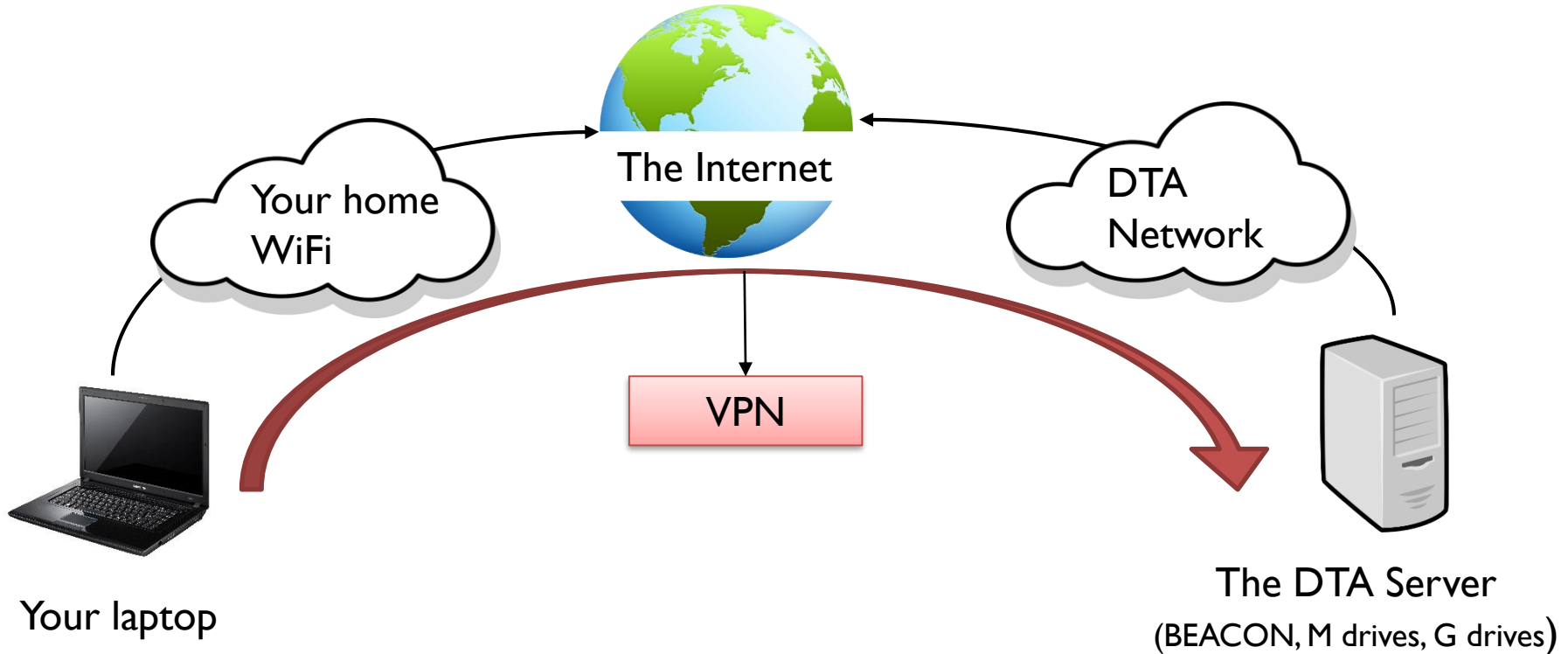
*Control your office PC from home, as
if you are in the office*

3

Logging Into VPN



What is VPN?



Virtual Private Network (VPN). It allows users to access a private network through a public network as if the device in use is directly connected to the private network.

To put of it simply, DTA employees, given VPN access, can use their laptops to log in to the DTA network and access BEACON and other programs.



Logging into VPN: Overview

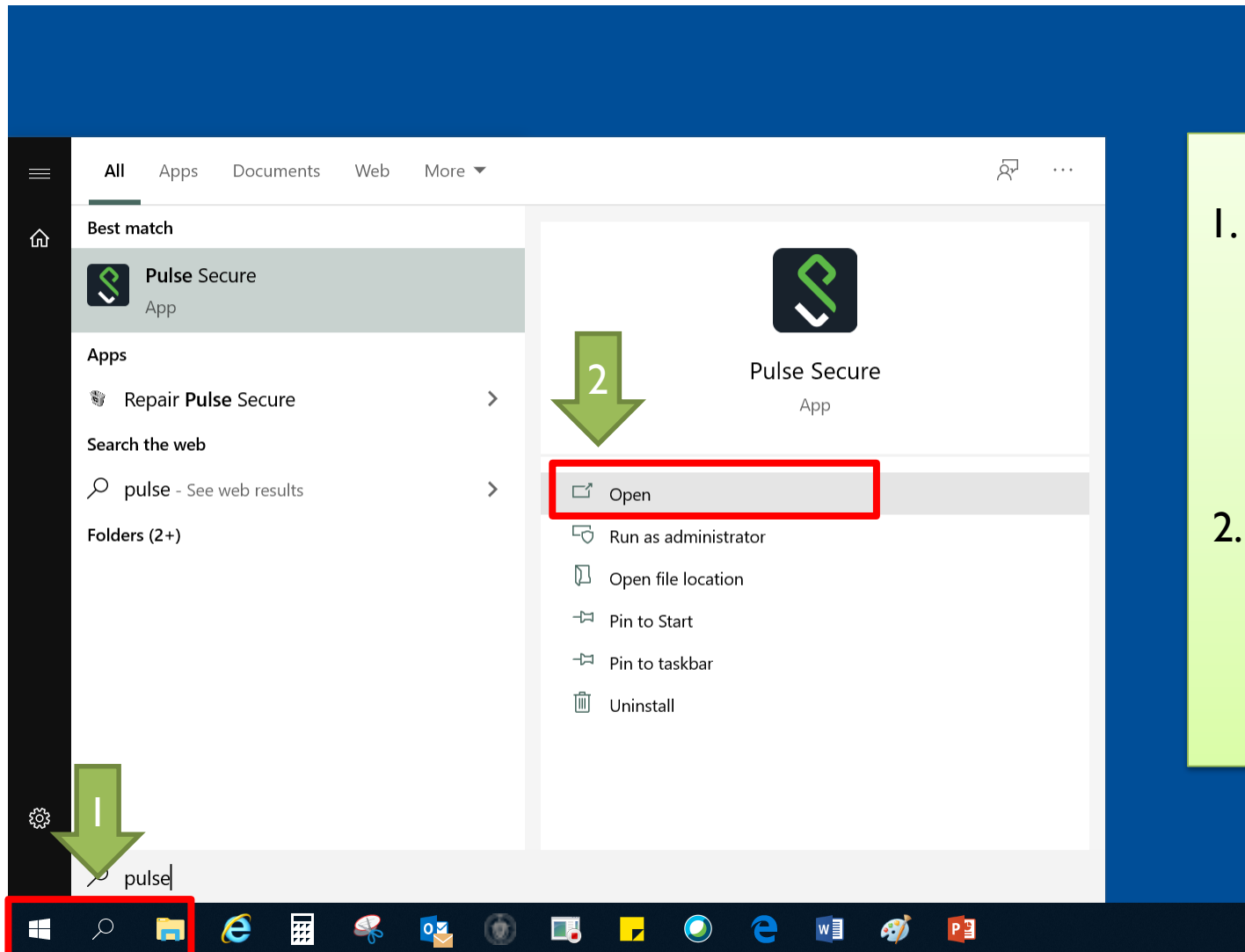
You will need:

- MFA Code
- Pulse Secure 2010-2020
- Your Network Login

1. Launch Pulse Secure
2. Connect to Commonwealth_VPN
3. Log in using your network login on Centrify
4. Enter your MFA code
5. Wait until Pulse Secure States “Connected”



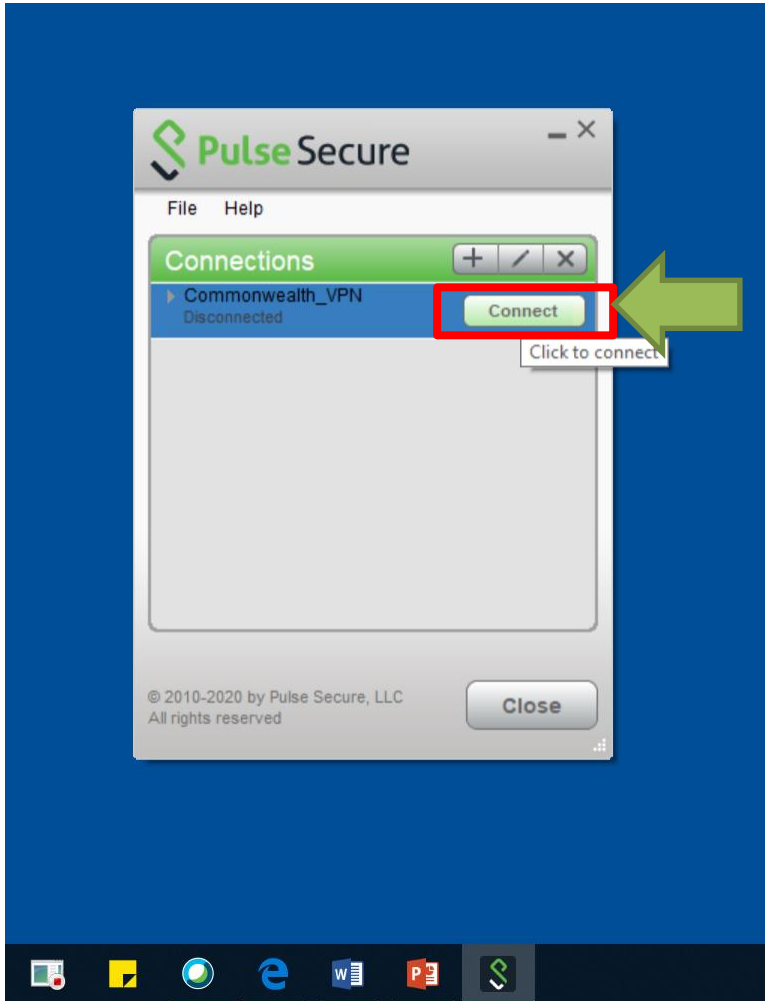
Logging into VPN



1. Select the search function at the bottom left hand corner and type ***“Pulse Secure.”***
2. Double click the icon or select ***“Open”*** to launch.



Logging into VPN



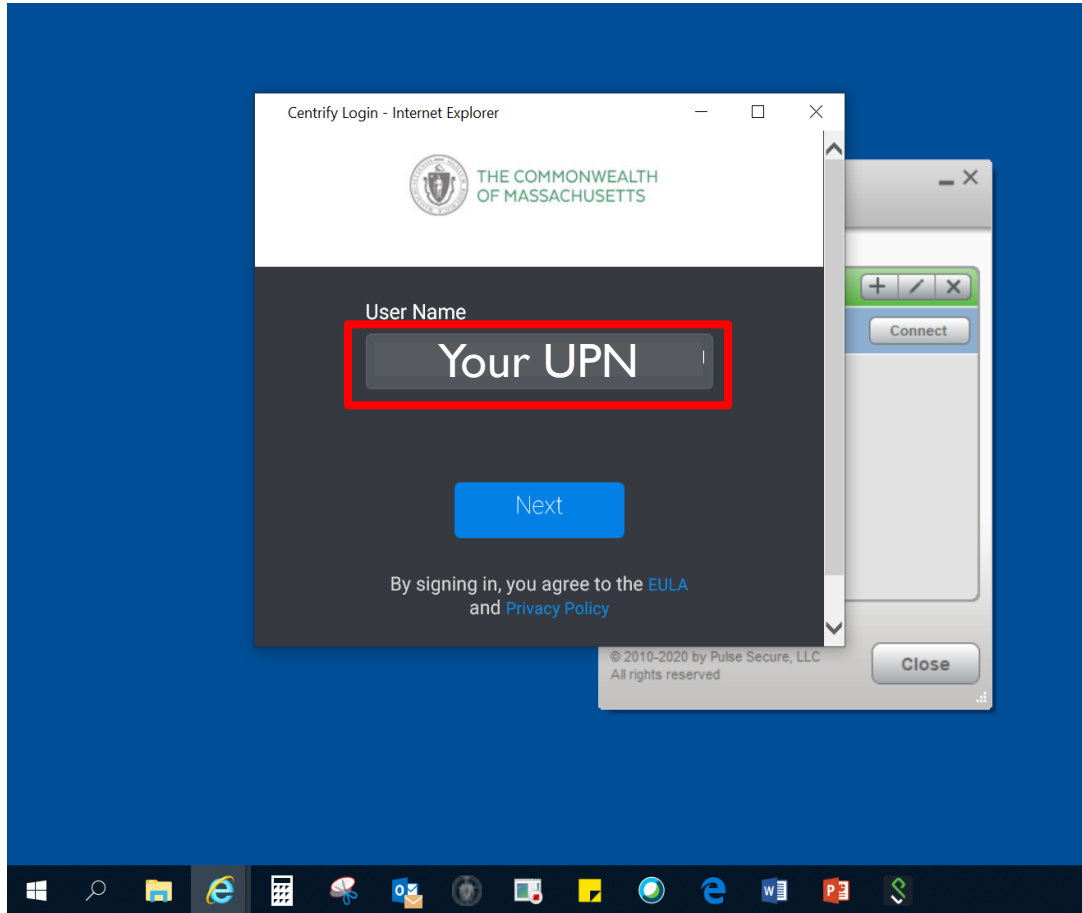
Before you select “Connect,”
make sure you:

- 1) Have your UPN and password ready
- 2) Have your MFA (DTA iPhone) device nearby

Note: if you start the connection and leave it idle, it will disconnect and you will need to start over.



Logging into VPN

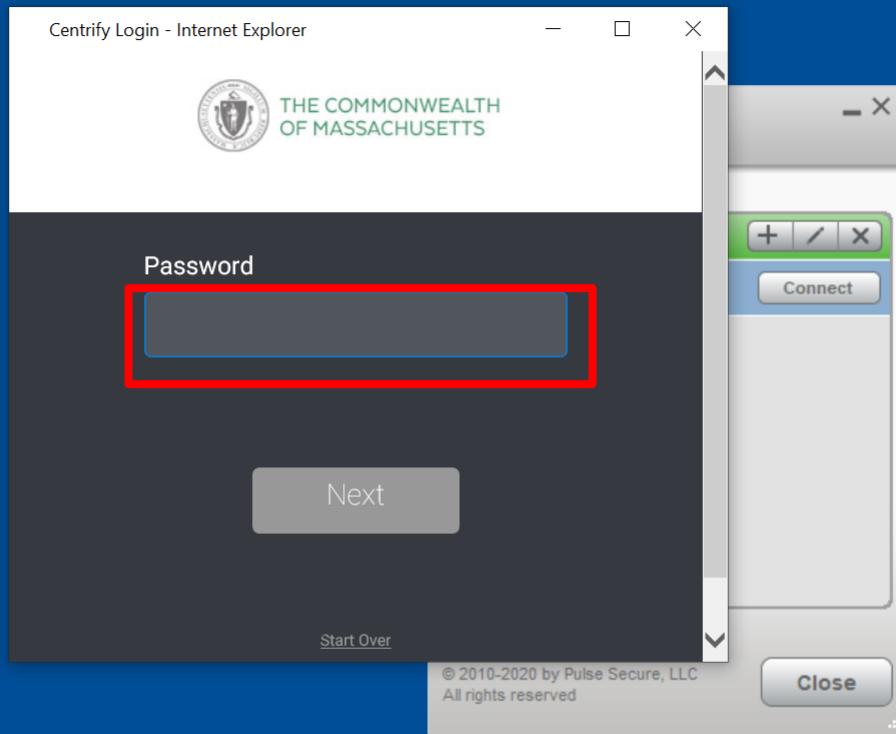


The Centrify pop up will automatically appear.

Log in using your UPN (Email Address)



Logging into VPN

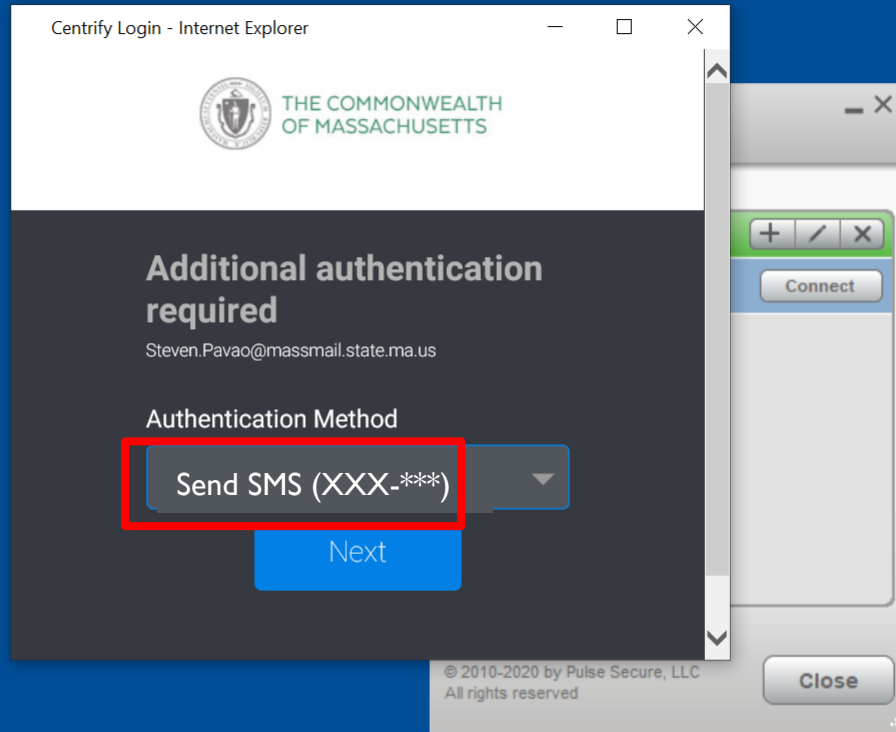


This is your network password.

When you log into your computer in the local office



Logging into VPN



MFA:

Make sure to have your phone ready. A text will be sent to your phone once you click next.



Logging into VPN

Centrifly Login - Internet Explorer

THE COMMONWEALTH OF MASSACHUSETTS

Additional authentication required

Steven.Pavao@massmail.state.ma.us

Enter Verification Code

Next

Connect

Close

© 2010-2020 by Pulse Secure, LLC
All rights reserved

T-Mobile Wi-Fi 4:47 PM

< 45 +1 (844) 204-8007 >

Text Message
Wednesday 12:28 PM

Commonwealth of Massachusetts - Account Verification
Code: 10551521

Wednesday 2:54 PM

Commonwealth of Massachusetts - Account Verification
Code: 13196799

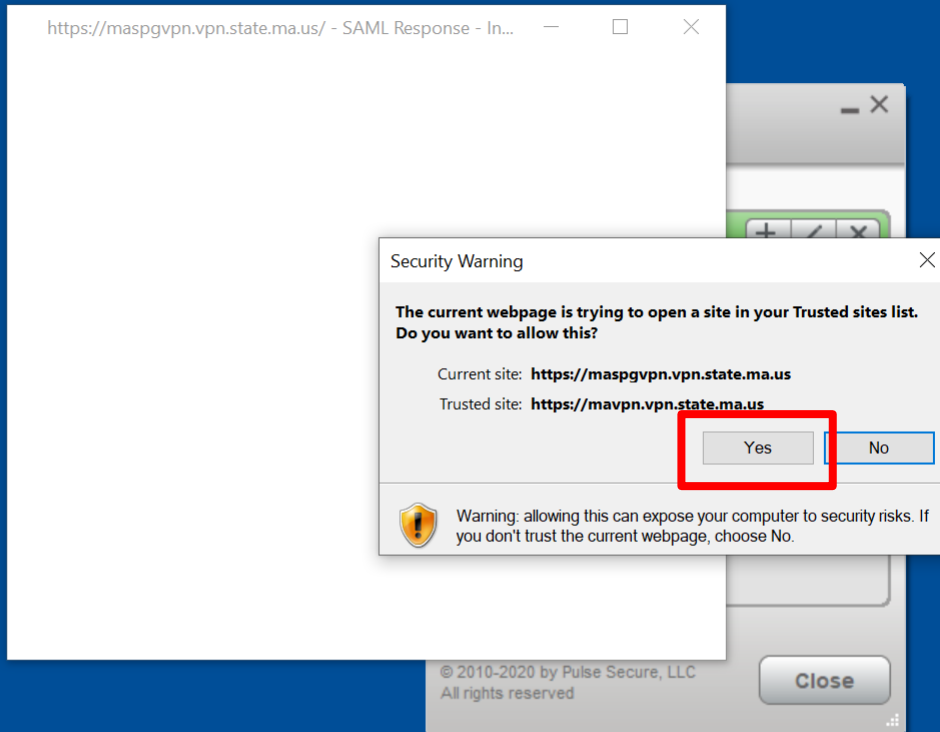
Camera App Store Text Message

Photos App Store Apple Pay Wallet Search Music

Sample SMS with code



Logging into VPN



A series of pop ups will begin to load after you select “yes.”

These pop up will automatically appear, load, and close, as each step continues.

Do not close out of any pop ups. They will automatically close after the steps are complete.

This may take a few moments.



Logging into VPN

EOHHS-IT
Service and Support Center
617-994-5050
Hours of Operation:
M-F, 6:00 am. - midnight
For 911 Emergencies
Dial "9+911"

DTA-BOS-M202D90

https://mavpn.vpn.state.ma.us/ - The Executive Office of Technology Services and Security - Home - Internet Explorer

File Edit View Favorites Tools Help

Pulse Secure

Logged-in as:
Helen.Xu@massmail.state.ma.us

Home Preferences Help Sign Out

Welcome to The Executive Office of Technology Services and Security,
helen.xu@massmail.state.ma.us.

Terminal Sessions

You don't have any terminal sessions.

Client Application Sessions

Pulse Secure Start

Note that launching Pulse Secure will terminate your browser session because of the security policy specified by your administrator.

Copyright © 2001-2020 Pulse Secure, LLC. All rights reserved.

EOHHS-IT
Service and Support Center
617-994-5050
Hours of Operation:
M-F, 6:00 am. - midnight
For 911 Emergencies
Dial "9+911"

10:31 AM
4/14/2020



Logging into VPN

The screenshot shows a Windows desktop environment. In the foreground, a Pulse Secure client window is open, displaying a 'Connections' list with 'Commonwealth_VPN' listed as 'Disconnected' and a 'Connect' button. Below this, it shows copyright information: '© 2010-2020 by Pulse Secure, LLC. All rights reserved.' and a 'Close' button.

Overlaid on the Pulse Secure window is an Internet Explorer browser window. The address bar shows the URL: `https://mavpn.vpn.state.ma.us/?launch_nc=1`. The page content includes a 'Please wait...' message: 'Launching Pulse Secure. This may take from a few seconds to a couple of minutes, depending on your bandwidth.' Below this, there is a troubleshooting section: 'If an error prevents the Pulse Secure from loading properly, you can:' followed by a list: '• Check browser compatibility' and '• Continue. Not all functionality may be available.'

The desktop background is a blue banner for 'EOHHS-IT Service and Support Center' with the phone number '617-994-5050' and hours of operation 'M-F, 6:00 am. - midnight'. It also includes the text 'For 911 Emergencies Dial "9+911"' and 'DTA-BOS-M202D90'.

The Windows taskbar at the bottom shows various application icons, including Internet Explorer, Chrome, and Pulse Secure. The system tray on the right indicates the time is 10:31 AM on 4/14/2020.



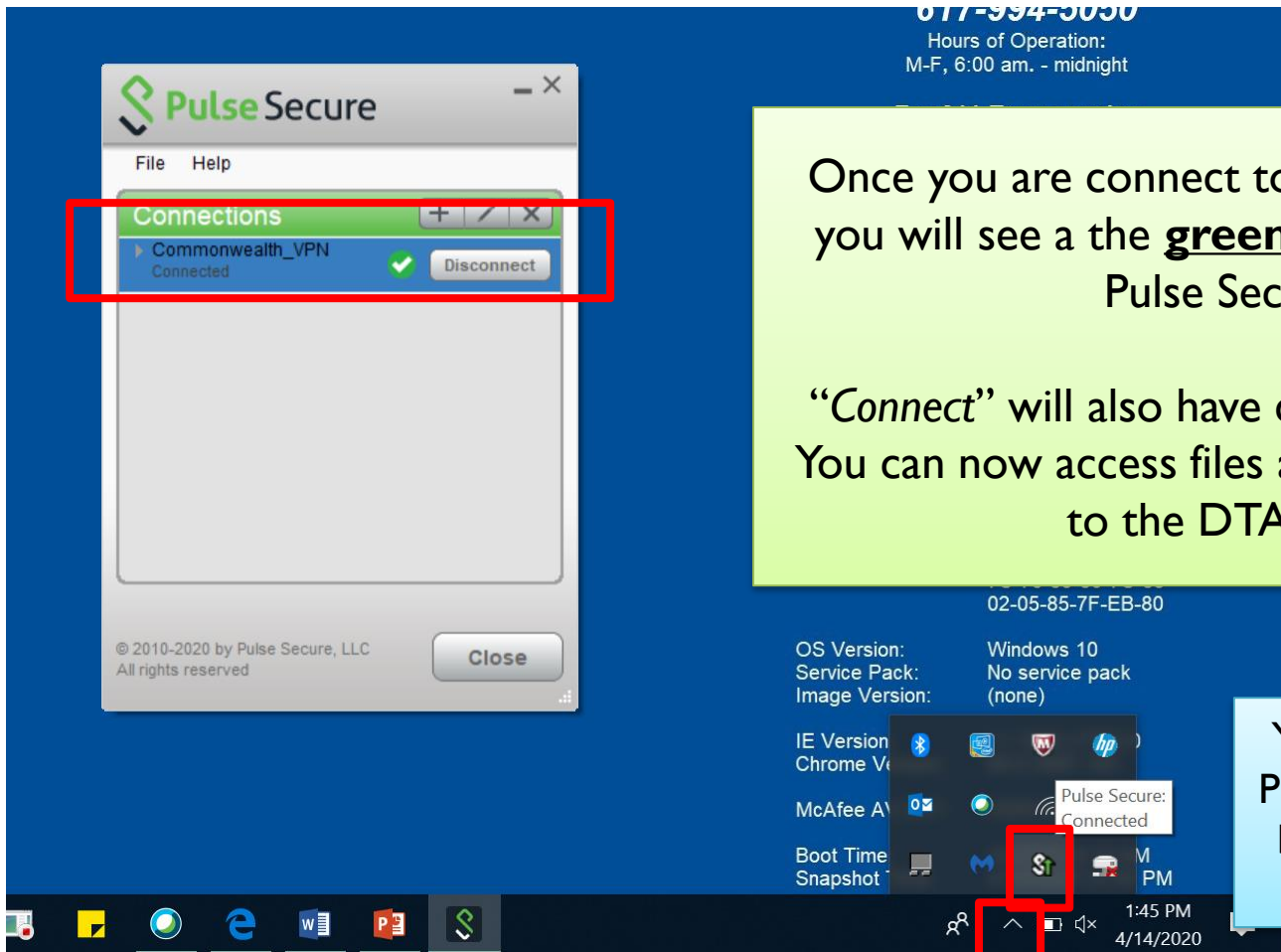
Logging into VPN

The screenshot shows a Windows desktop environment. In the background, there is a blue banner for EOHHS-IT Service and Support Center with the phone number 617-994-5050 and hours of operation (M-F, 6:00 am. - midnight). Below this, it says 'For 911 Emergencies Dial "9+911"'. The desktop also features a 'DTA-BOS-M202D90' label. A web browser window is open to the Executive Office of Technology Services and Security website. The page has a green header and a main heading 'Welcome to The Executive Office of Technology Services and Security'. A yellow box highlights a message: 'For security reasons, your session is no longer accessible from this web browser.' Below this, there is a link: 'Click here to sign in again'. A Pulse Secure window is open on the right side of the screen, showing a 'Connections' list with 'Commonwealth_VPN' and a 'Connecting' status. The Pulse Secure window has a 'Close' button at the bottom right. The taskbar at the bottom shows various application icons and the system tray with the date and time: 10:31 AM 4/14/2020.

Again, these will automatically close after they load.



Logging into VPN



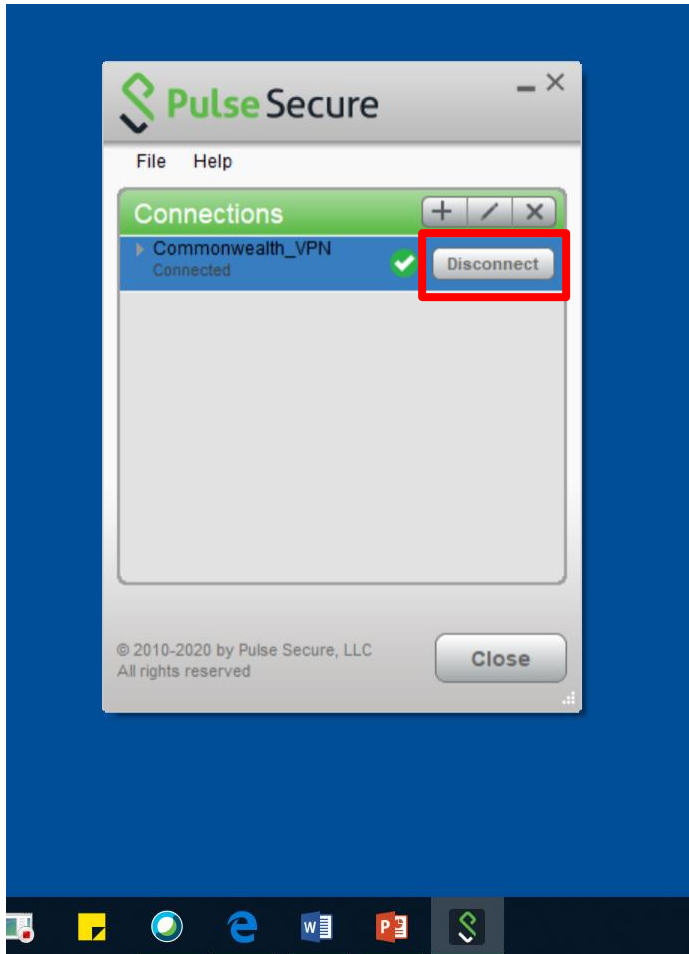
Once you are connect to Commonwealth_VPN you will see a the **green check mark** on your Pulse Secure App.

“Connect” will also have changed to “Disconnect.” You can now access files and functions connected to the DTA network.

You can also hover over the Pulse Secure Icon on the tool bar at the bottom to check your connection.



Logging into VPN



When you are done for the day, you can disconnect from the VPN by select the *Disconnect* button.

After, your laptop will no longer be able to access the DTA network until you log in again.

Shutting down the laptop will also disconnect you from the VPN.

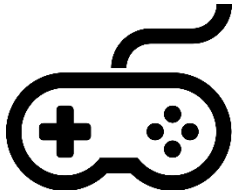


3b

Remote Desktop Connection



What is Remote Desktop Connection?



Your laptop
(Device B)



Your Office PC
(Device A)

Remote Desktop Connection is simply accessing your office PC with a different device. When you remote desktop, you are using Device B to control Device A. Both devices must be connected to a network and turned on.



Remote Desktop General Steps:

Some laptops are not configured with BEACON or other systems access. If that is the case, you will need to Remote Access into your office PC to begin work.

1. Set up MFA
2. Find your local office PC IP address
3. Connect to VPN through PULSE Secure
4. Connect through Remote Desktop

For the remainder of this guide, Device A will denote your office PC and Device B will denote your laptop you are using from home.



Important!

In order to Remote Desktop you must:

- Have VPN access
- Have a desktop to remote to, and a device to remote from
- The PC being accessed (Device A) must be ON



Accessing Remote Desktop



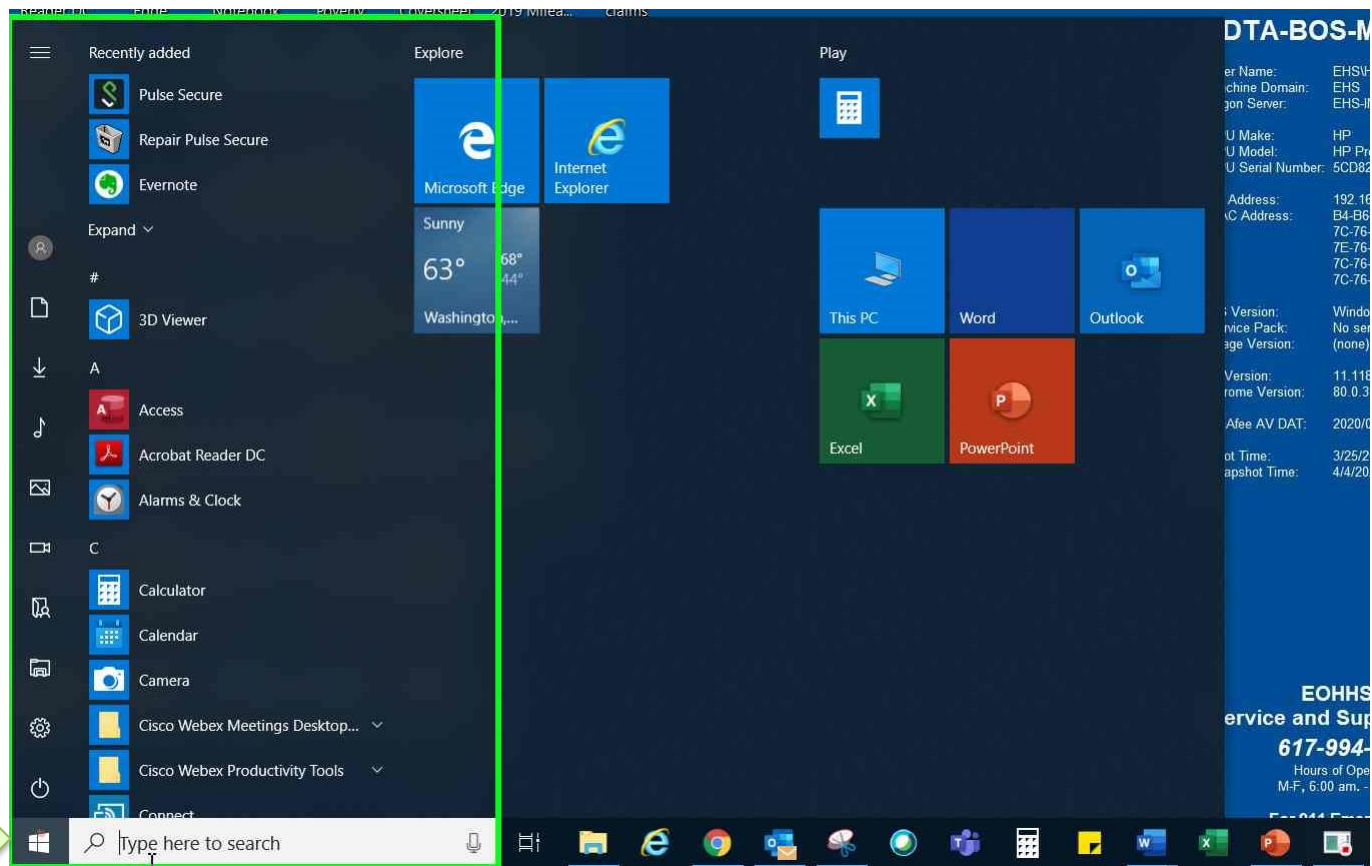
Remember, you MUST be connected to VPN before you do this!!



- 1) Are you connected to VPN?
- 2) Do you have Device A's IP address?
 - This is the one you wrote down before getting your iPhone and laptop in the office.

If yes to both, continue.

On Device B (laptop)



Select the Windows Icon on the bottom left corner to open up the Start Menu. Type **“Remote Desktop”** into the search.



On **Device B** (*laptop*)

The screenshot shows a Windows 10 desktop with a blue background. The Start menu is open, displaying search results for 'remote'. The 'Best match' section highlights the 'Remote Desktop Connection App'. A green arrow points to this app. The 'Recent' section shows the IP address '170.154.84.56'. The 'Apps' section lists 'Remote Desktop'. The search bar at the bottom contains the text 'remote Desktop Connection'. On the right side of the desktop, there is a blue panel with system information for 'DTA-BOS-M202D9G', including user name, machine domain, CPU details, IP address, and OS version. At the bottom right, there is contact information for 'EOHHS-IT Service and Support Center' with the phone number '617-994-5050'.

DTA-BOS-M202D9G	
User Name:	EHS\HeXu
Machine Domain:	EHS
Logon Server:	EHS-INF-WSH-121
CPU Make:	HP
CPU Model:	HP ProBook 440 G5
CPU Serial Number:	5CD8202D9G
IP Address:	192.168.1.7
MAC Address:	B4-B6-86-D3-86-39 7C-76-35-80-63-57 7E-76-35-80-63-53 7C-76-35-80-63-54 7C-76-35-80-63-53
OS Version:	Windows 10
Service Pack:	No service pack
Image Version:	(none)
IE Version:	11.1184.17134.0
Chrome Version:	80.0.3987.149
McAfee AV DAT:	2020/04/02
Boot Time:	3/25/2020 9:22 PM
Snapshot Time:	4/4/2020 9:54 PM

EOHHS-IT
Service and Support Center
617-994-5050
Hours of Operation:
M-F, 6:00 am, - midnight

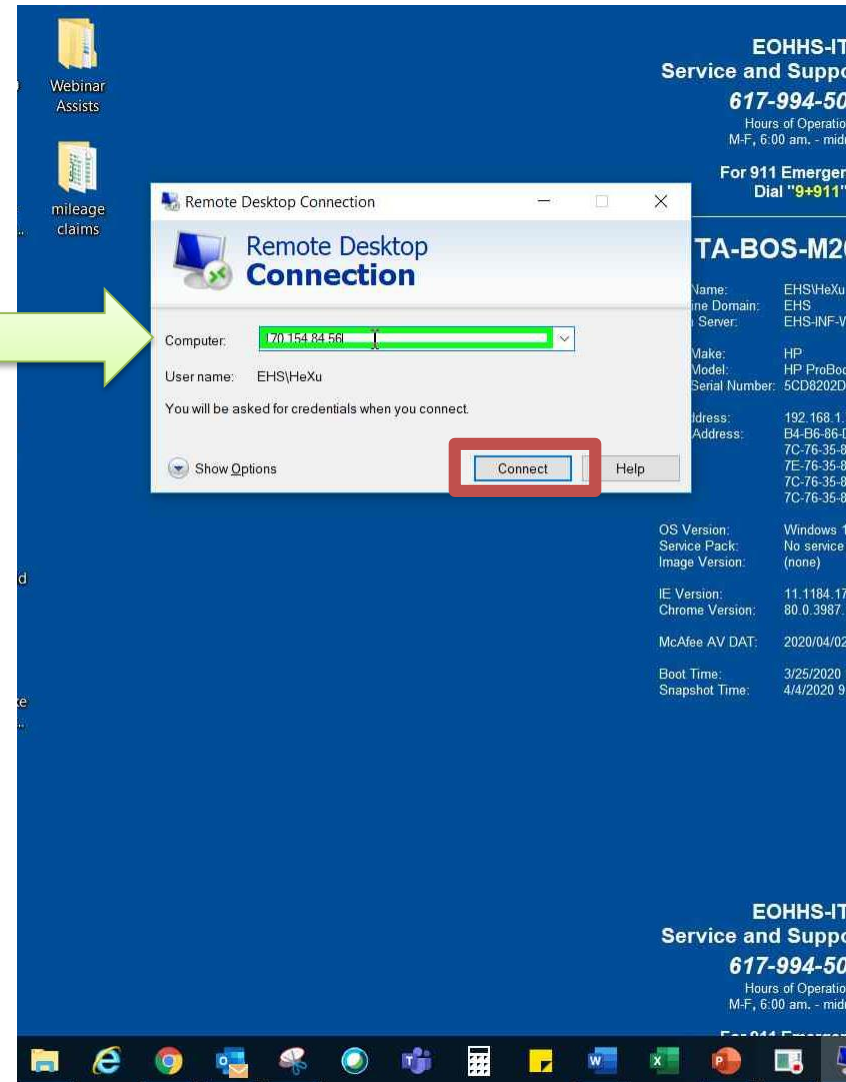
Select the **Remote Desktop Connection** App

On **Device B** (laptop)

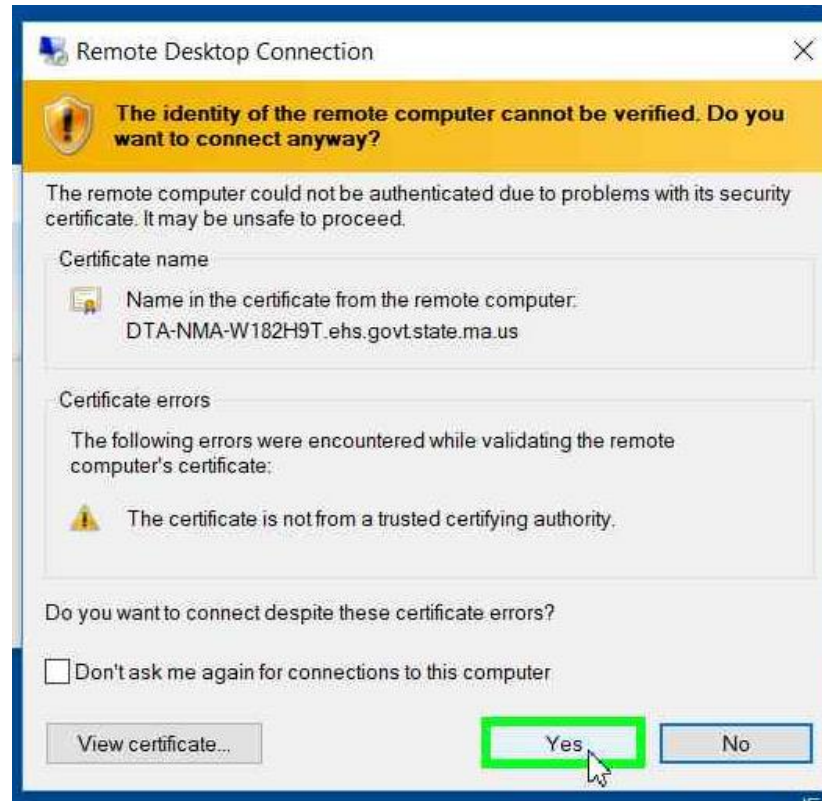
Type in **Device A's** IP address



Your user name is your EHS login credentials. In order to remote to a office PC (Device A), the device must be powered on.



On **Device B** (*laptop*)



If you see this pop up, select “YES” and your connection will be set up.



On **Device B** (laptop)

You can access your **Device A** desktop from **Device B** as if you are operating **Device A**. Any program selected on this screen will run on **Device A**.

EOHHS-IT
Service and Support Center
617-994-5050
Hours of Operation:
M-F, 6:00 am. - midnight
For 911 Emergencies
Dial "9+911"

DTA-NMA-W182H9T

User Name: EHS\Hexu
Machine Domain: EHS
Logon Server: EHS-INF-WSH-121

CPU Make: HP
CPU Model: HP ProDesk 400 G5 SFF
182H9T

170.154.84.56
09-17-51-60

ews 10
rice pack

7-17763.0
809-132

09/05

20 3:12 PM
20 4:15 PM

1:17 PM
4/9/2020

This is the desktop of **Device A**. Not the bar at the top. That is the indicator you are on **Device A**.



On **Device B** (laptop)

The screenshot displays a Windows desktop environment. The taskbar at the bottom shows the Start button, search icon, and several application icons including Cisco Jabber, BEACON3, and various files. A web browser window is open, showing a login page for 'https://bcn3-web-prod.dta.state.ma.us/beamon/logon/startup.html'. The login form contains two input fields labeled 'User name' and 'Password', and a 'Logon' button. Below the form is a link that says 'Add to Favorites...'. To the right of the browser window, there is a system information panel for 'EOHHS-IT Service and Support Center' with contact information and hardware details for 'DTA-NMA-W182H9T'.

EOHHS-IT Service and Support Center	
617-994-5050	
Hours of Operation:	M-F, 6:00 am - midnight
For 911 Emergencies	Dial "9+911"
DTA-NMA-W182H9T	
User Name:	EHS\Hexu
Machine Domain:	EHS
Logon Server:	EHS-INF-WSH-121
CPU Make:	HP
CPU Model:	HP ProDesk 400 G5 SFF
CPU Serial Number:	MXL9182H9T
IP Address:	170.154.84.56
MAC Address:	F4-39-09-17-51-60
OS Version:	Windows 10
Service Pack:	No service pack
Image Version:	(none)
IE Version:	11.557.17763.0
Chrome Version:	76.0.3809.132
McAfee AV DAT:	2019/09/05
Boot Time:	3/3/2020 3:12 PM
Snapshot Time:	4/6/2020 4:15 PM

If Remote Desktop is disconnected, the programs will continue to run on Device A, so make sure to close out of any program you are using before you end the Remote Access session.



On **Device B** (laptop)

Remote Desktop Connection

Your remote session will be disconnected

Programs on the remote computer will continue to run after you have disconnected. You can reconnect to this remote session later by logging on again.

Don't display this message again **OK** Cancel

Close X

McAfee AV DAT: 2019/09/05
Boot Time: 3/3/2020 3:12 PM
Snapshot Time: 4/6/2020 4:15 PM

1:18 PM
4/9/2020

Click “X” to Exit. You will receive a reminder. Click “ok” to end your session and you will be brought to your Device B desktop.

STOP

NOTE: DO NOT shut down Device A. If you shut down Device A, you will have to manually reboot the computer in the office.

t&d

➤ Reminders for Remote Desktop

1. Make sure you are connected to VPN before the accessing remote desktop.
2. Remote desktop connection is using your laptop from home to operate your desktop at the office. Both devices are necessary for a connection of be made.
3. Your Office PC IP address is the IP address listed on the desktop of your office PC. The IP addresses of the laptops are different than the desktops.
4. Make sure Device A reminds on. Again, you will have to manually turn the device back on at the office if you shut down the device.

