Remote Work Self Help Guide

Solution Guidelines to Work from Home (Updated: 04/14/2020)

Overview

The purpose of this document is to provide a 'How-to' walk through on systems that can be used while away from the office. Click the links for quick jumps to each section or needed website.

Awareness

1. Many issues experienced offsite can be resolved with a reboot.
2. VPN will disconnect every 10 hours, and will disconnect after 1 hour of inactivity. (ITD Policy)
3. Workstations at ITD that are powered off, will have to be manually powered on.
4. Be mindful of the personal devices that are plugged into ITD computers.
5. Be mindful of the sites accessed while you are on ITD – VPN, Especially on personal equipment.
6. Be mindful of Personally Identifying Information (PII) and ITD Sensitive information. Please do not use personal devices to print or store any ITD proprietary information.
7. For Additional Resources here and visit the Technology Hub!

Hardware

When working from remotely, be sure you have what is need to operate your equipment. In addition, Sign into the workstation you will be using before taking the ITD equipment off site.

1. Workstation – Desktop PC, Laptop, Tablets
2. Cables – Power cables, Display Cables (Display port, HDMI, DVI, VGA), Network cables (LAN), Printer cables, charging cables
3. Monitors – Displays and stands
4. Docking stations – Power supplies, Docking station, Adapters, Surge protectors or Battery backups
5. Printers – Desktop Printers, Label makers
6. Headsets

Software

1. *Cisco AnyConnect Client* – Application can be installed on non-ITD computers and should be available on all ITD workstations. See directions for VPN here
2. *Remote Desktop (RDP)* – Application is available on all windows based computers, no install required. Access is provided by the Service Center. Follow the process here
3. *Microsoft TEAMS* - Available to install from office.com after signing in. Follow the process here

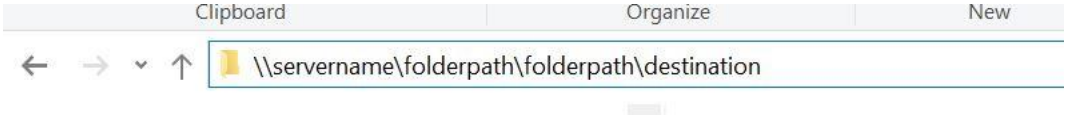
Access

1. *WebEx* - Information can be found here (SharePoint link)

2. *Conference Now* – Directions can be found here
3. *Office.com* – Log in to Office.com to gain access to quick online applications in the application dashboard. Including installing TEAMS, resetting your ITD password and updating MFA security options.
4. *Outlook Desktop application (MFA)* – Due to security policies set in place, MFA users will be prompted to key in their Outlook (MFA) password when accessing the desktop application. Follow the process here
5. *Resetting ITD password* – Follow the process here
6. *OneDrive for Business* – Directions can be found here

Mapped Folder Work-Around

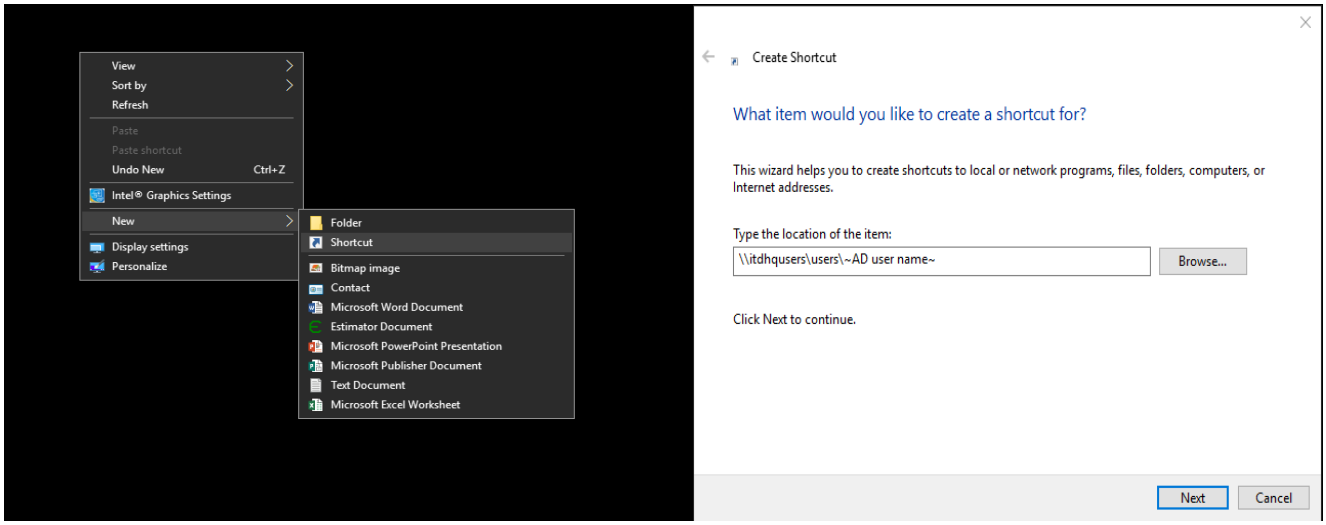
1. Network drives that are mapped will have to be navigated to manually, Automatic mapping does not work remotely.
   a. To manually navigate to the directory needed key in: Example



   b. Alternatively, Use SharePoint!

Accessing Personal ITD U: Drive

1. Create New Desktop shortcut, by 'right clicking' desktop, selecting 'New' and then select 'Shortcut'



2. Type in the path: \\itdhqusers\users\USERNAME (username is your ITD sign in name)
3. Save the name for your Shortcut as 'U Drive'
4. To access the U: drive open the newly created shortcut on the desktop

Conference Now

Can be initiated onsite/offsite at anytime

HOST (person creating the conference call)

Dial (208)334-8142

1. Enter Conference Number (This is your 5 digit desk phone extension) example- 78175
2. Enter PIN Number: 1234

Participants (People joining your calls)

1. Dial (208) 334-8142
2. Enter Conference Number: (The 5 digit desk phone extension # of Host)

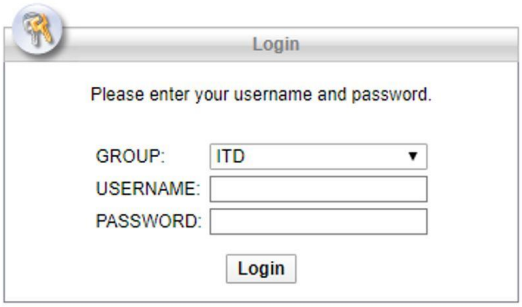
You'll need to send (208) 334-8142 and your desk extension # (conference number) to your participants.

Your desk extension# or conference number is only an ID to route people to your conference call.

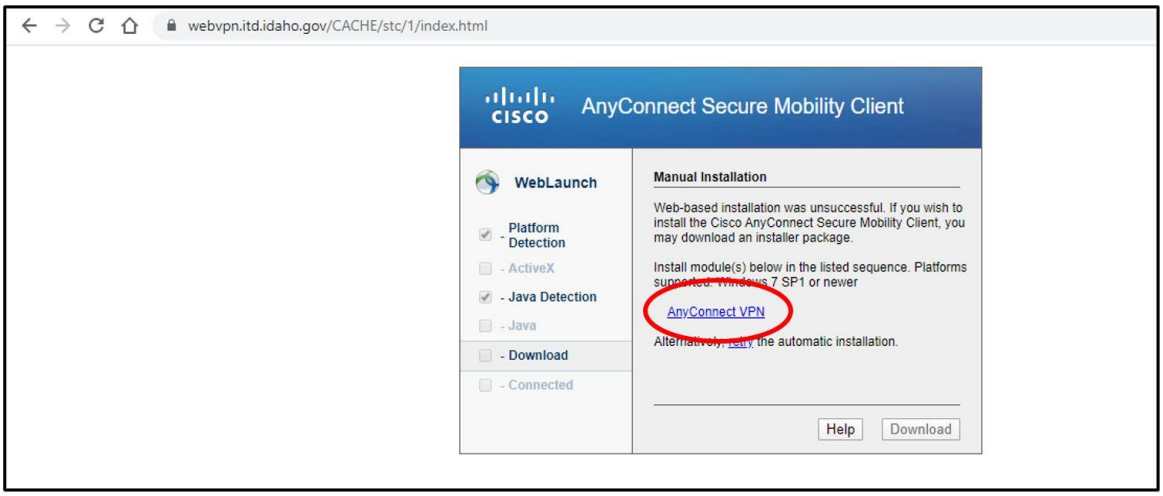
How-to install Cisco AnyConnect VPN on your PERSONAL Computer

NOTE: You cannot be connected to ITD's VPN while at ITD. You must be connected to a different network (i.e. your home network).

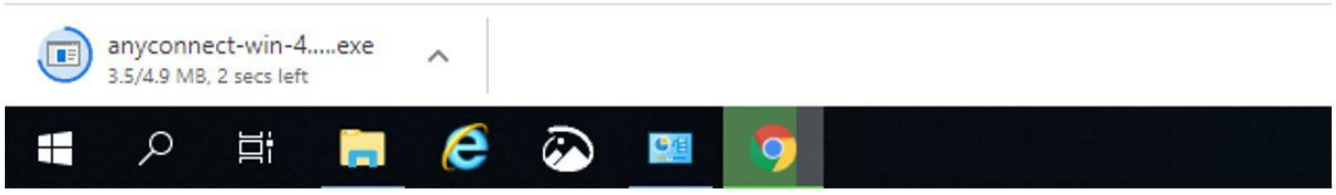
1. Navigate to https://webvpn.itd.idaho.gov in your internet browser (We recommend **Google Chrome**)
2. Select the appropriate Group assignment for your company, ITD employees will select 'ITD'
3. Enter your ITD Credentials and select 'Login'



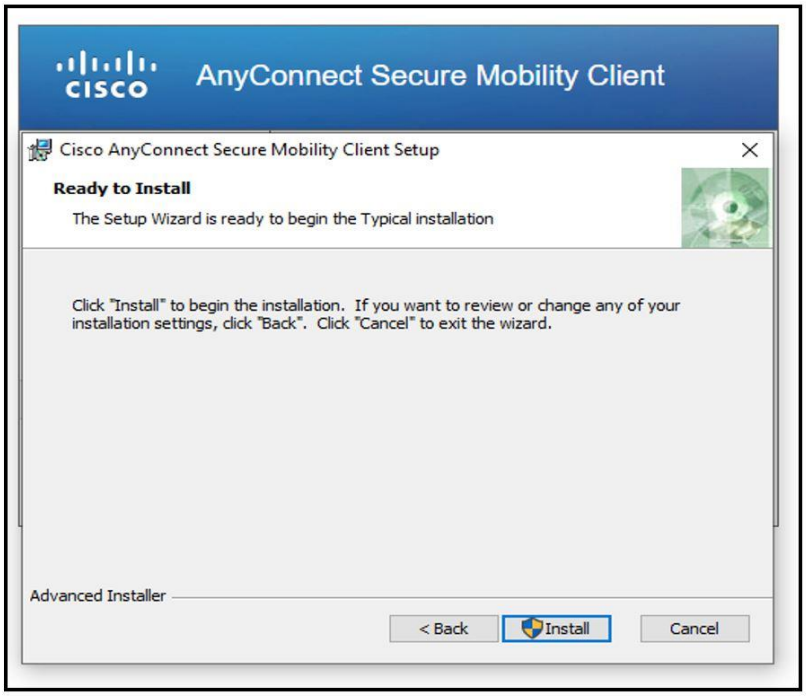
4. As shown in the image below click on the AnyConnect VPN button



5. Click on the 'AnyConnect VPN' link to download

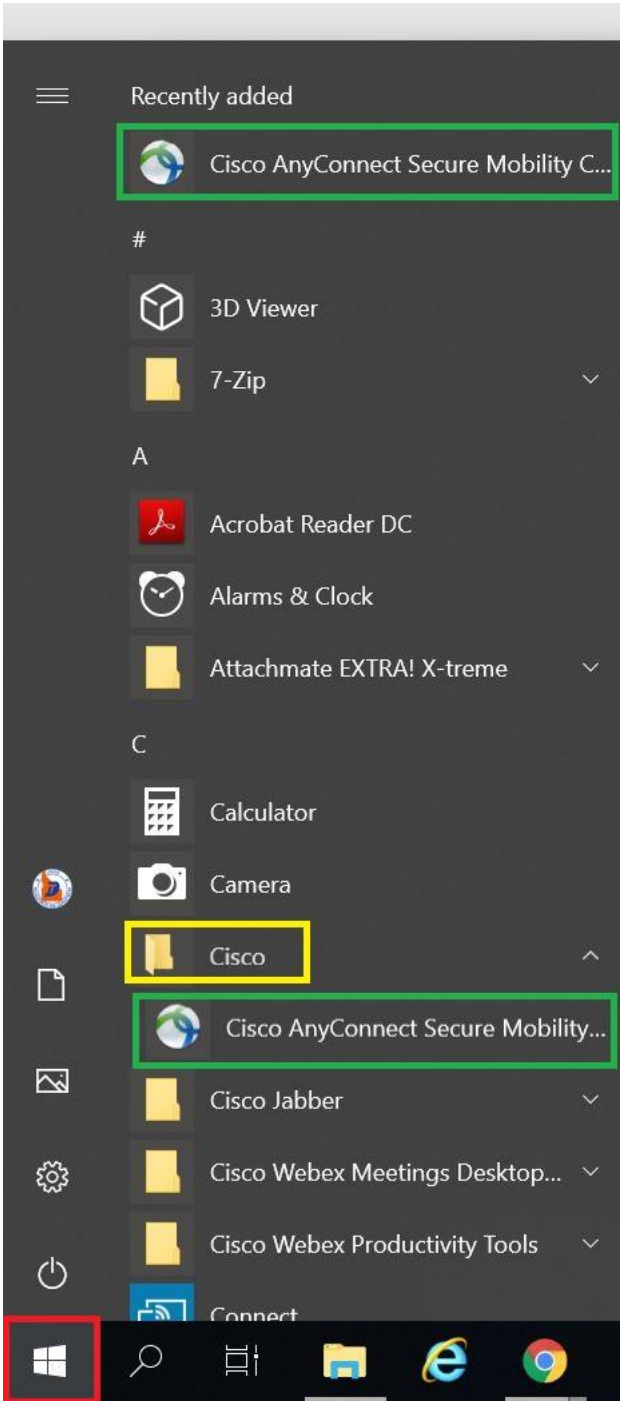


6. Proceed through the install, click the ‘Install’ button

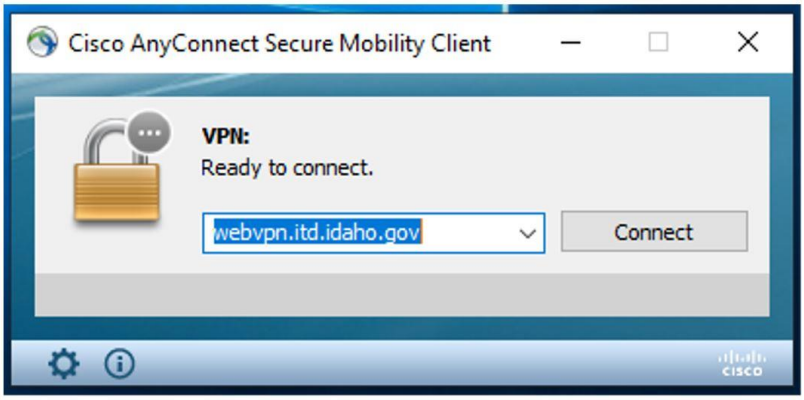


7. Click ‘Finish’ to complete and close the install window

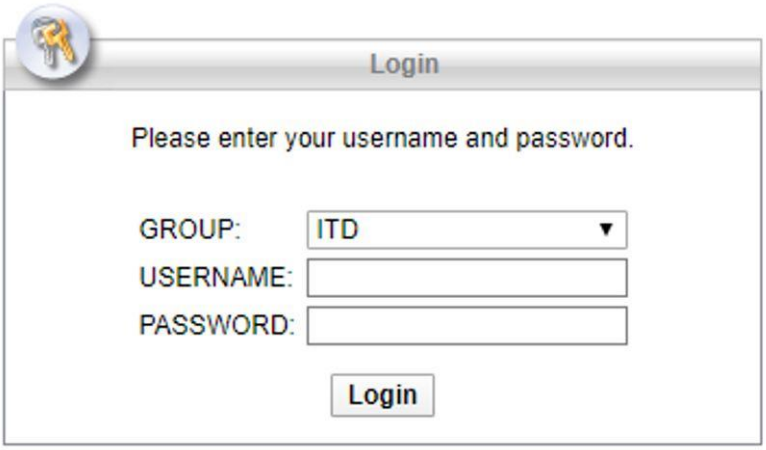
8. Open the start menu (as shown below) Cisco AnyConnect Secure Mobility client should be in your "recently installed" applications. OR open the start menu and type in "Cisco AnyConnect" and click the application icon.
    a. It can also be found under the Cisco folder in the Start Menu.



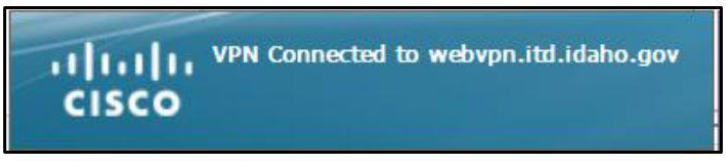
9. Type in **webvpn.itd.idaho.gov** into the box (as shown below) and click connect.



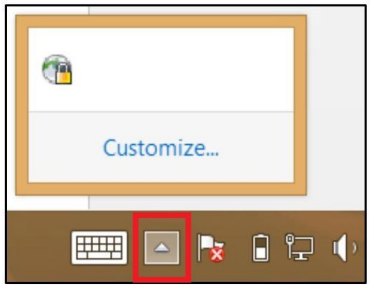
10. Select the appropriate company group from the drop down, ITD employees will select "ITD" group.
11. Proceed with your ITD username and password.



12. You should receive a notification that you are now connected.



13. You may also verify your connection in the System Tray.



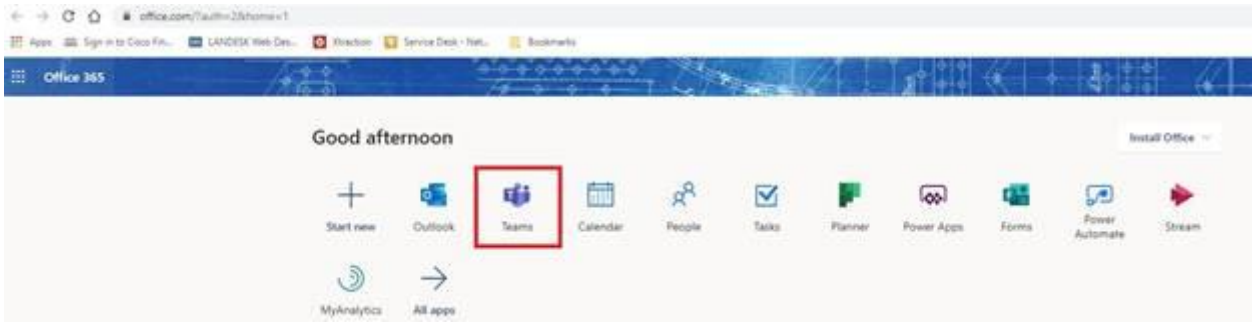
14. To **disconnect** from the ITD network, click the Cisco AnyConnect icon in the system tray, OR click on the Cisco AnyConnect icon from the Start menu, then click 'Disconnect'.

Microsoft TEAMS

How to install and connect to Microsoft TEAMS

1. Open Web Browser, Any browser will work
2. Browse to https://www.office.com/
    a. outlook.office.com or office365.com will also work, process is slightly different
3. Click Sign in (Top right corner)
    a. If prompted, Click on Work or School account

4. Type ITD email address and password
5. Office 365 Dashboard will load
6. Located at the top is the applications list, Select Teams icon to start the install

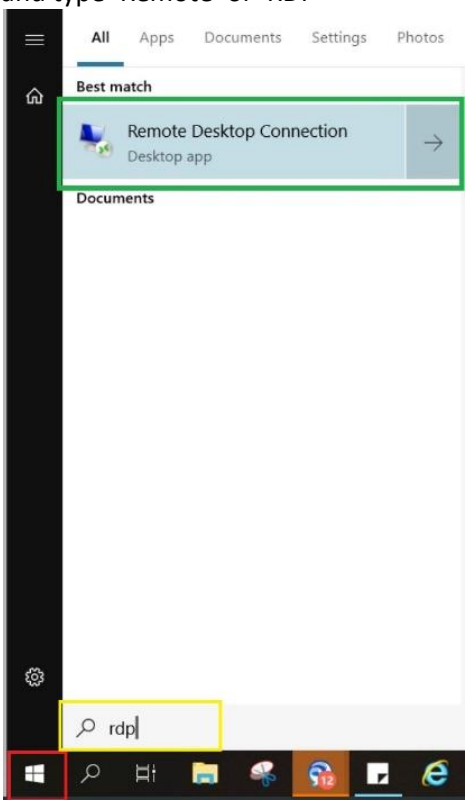


7. An icon will install on the desktop and Teams will automatically launch once the install completes.
8. TEAMS will automatically sign in you in, if not reach out the service center.

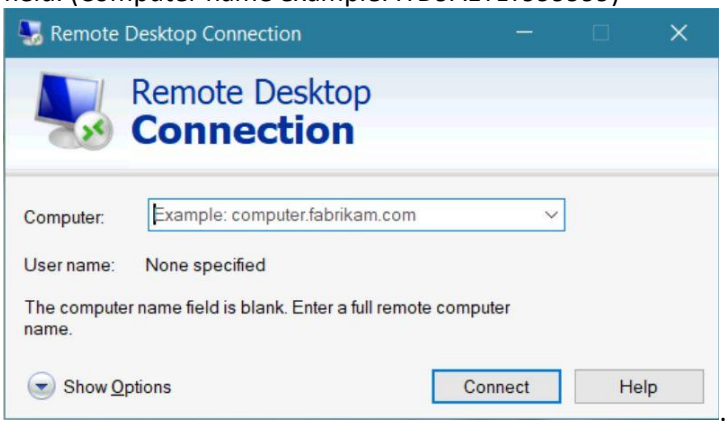
How to use Remote Desktop (RDP)

For remote desktop access to be enabled on the system remaining at your office, call or email the Service Center. Once enabled follow the directions below.

1. After logging into Cisco AnyConnect and establishing ITD VPN connection
2. Select the Start menu button and type 'Remote' or 'RDP'



3. Click 'Remote Desktop Connection'
4. When the remote Desktop Connection Client opens type in the FULL 15 character ITD computer name into the computer field. (Computer name example: ITD9AETLT999999)



5. Click ‘Connect’
6. You will be prompted to Sign in. In the user name Field type ITD\username and verify the domain has updated to show ITD.

7. Type in your ITD password and click ‘OK’
8. The ITD lock screen should load of the workstation you entered. To access the workstation, key in your ITD credentials as normal.

How to update your ITD password through Remote Desktop

Before resetting your password, ensure you are connected to the ITD network. In order to access the ‘crtl+alt+del’ screen you have two options.

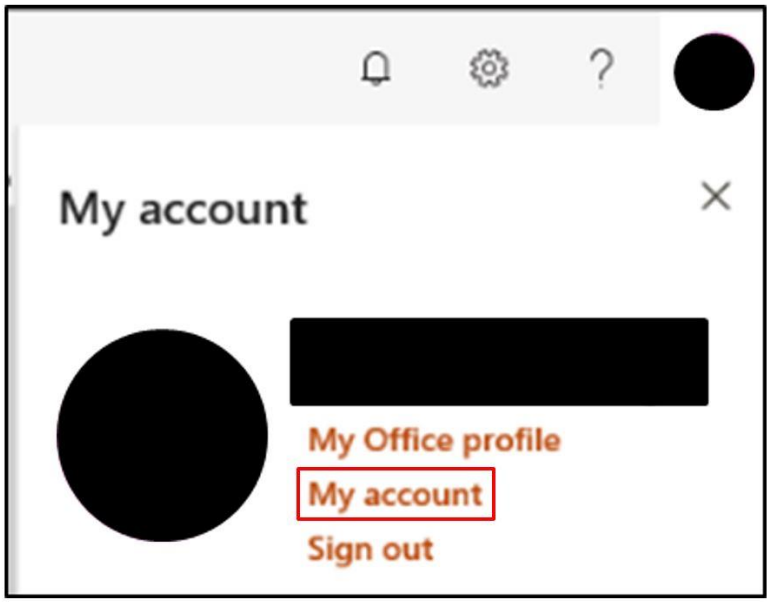
1. After remoting to your ITD workstation, press ‘crtl+alt+end’ to load the task screen and reset the password.
2. You can use the on screen keyboard (type ‘osk’ in start menu to open) and press ‘crtl+alt+del’ to access the task screen and reset the password.
3. Once completed lock your ITD workstation and log back in with your new ITD credentials. Do not disconnect from VPN
4. If the password has expired please contact the service center for assistance.

Multi-factor Authentication (MFA)

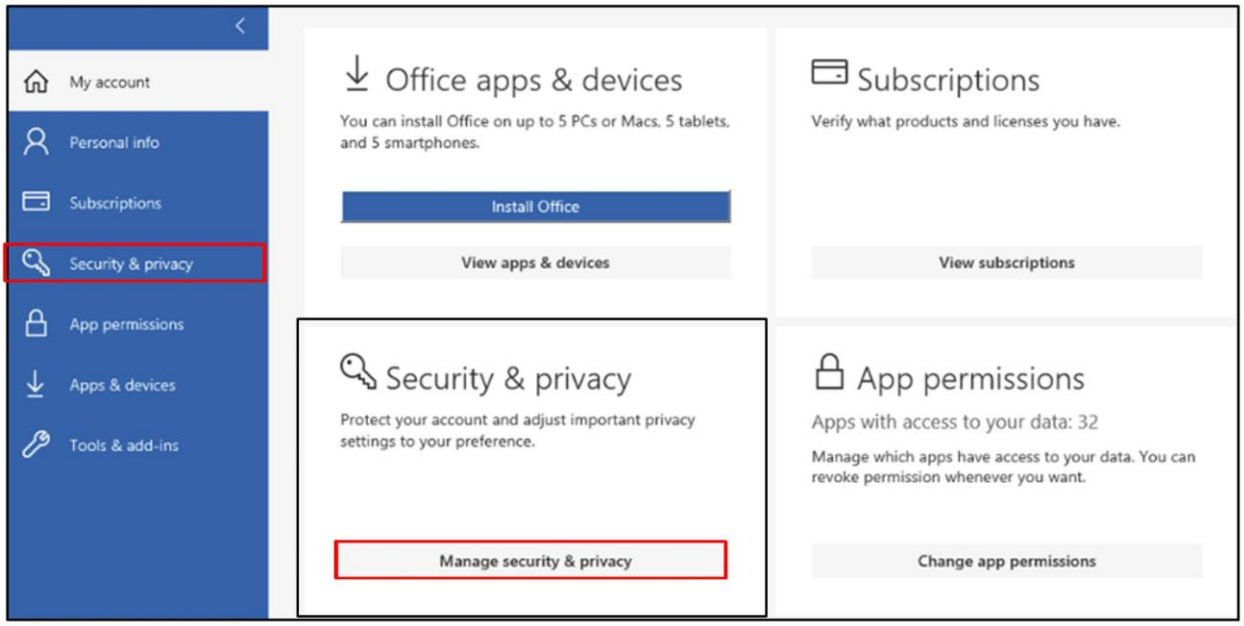
How to update Multi-factor settings and re-assign an application (Outlook Desktop) password.

1. Log into https://www.office.com and select your 'profile icon' in the top right

2. Then select 'My Account'

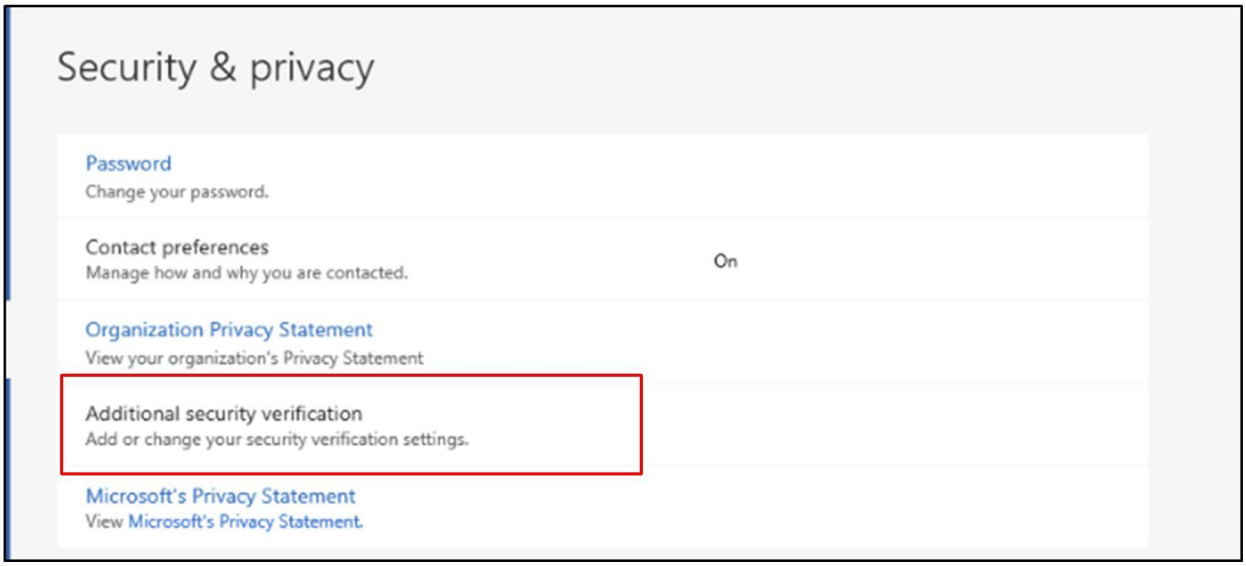


3. Select 'Manage Security and Privacy' you may need to select 'Security and Privacy' from the menu on the left.

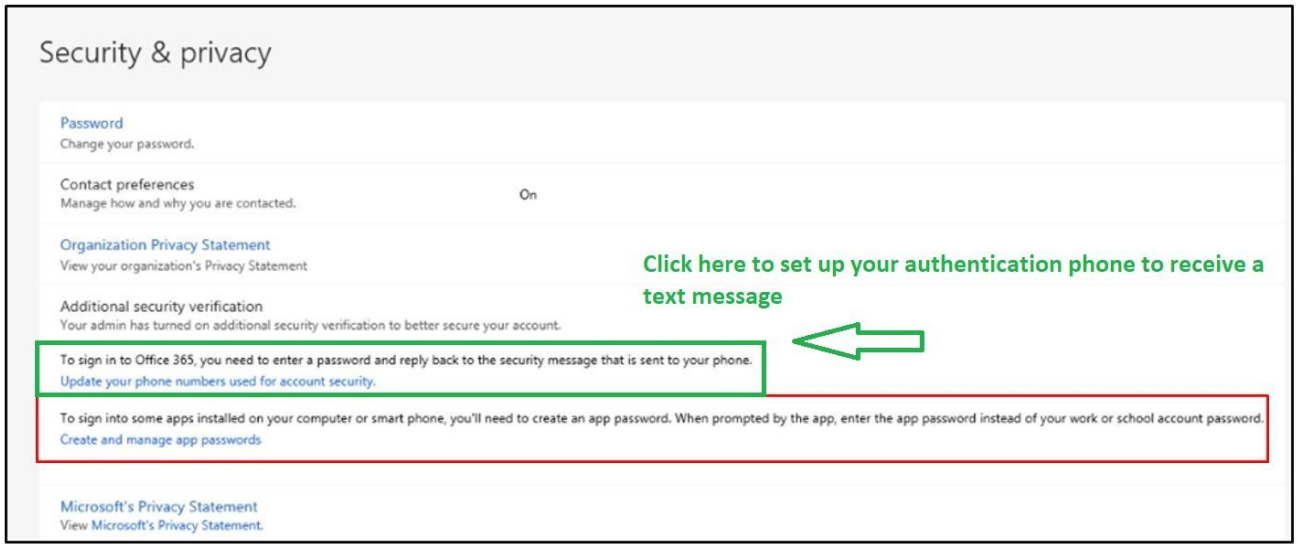


Note: Logging into https://portal.office.com/account/ will also load the above screen.

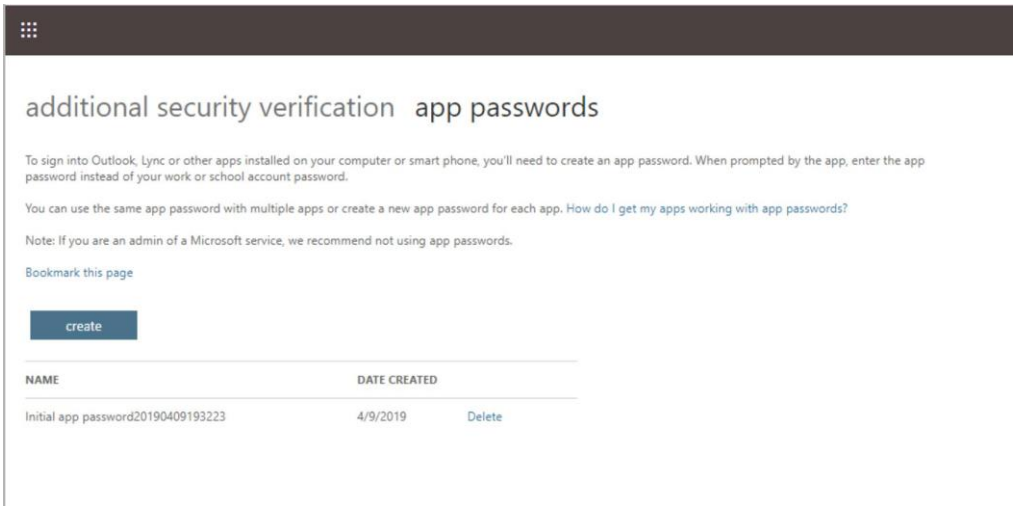
4. Click on 'Additional Security Verification'



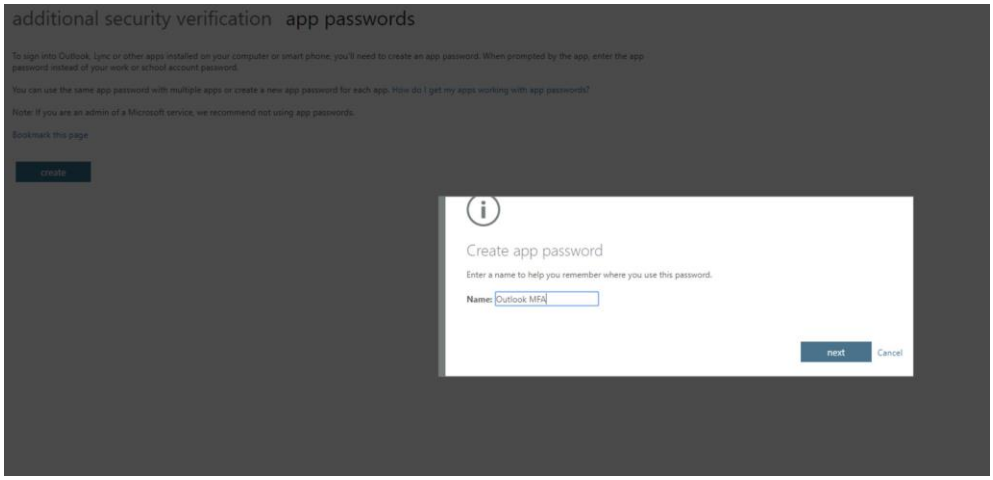
5. This will open up a few more options and you will select 'Create and manage app passwords'



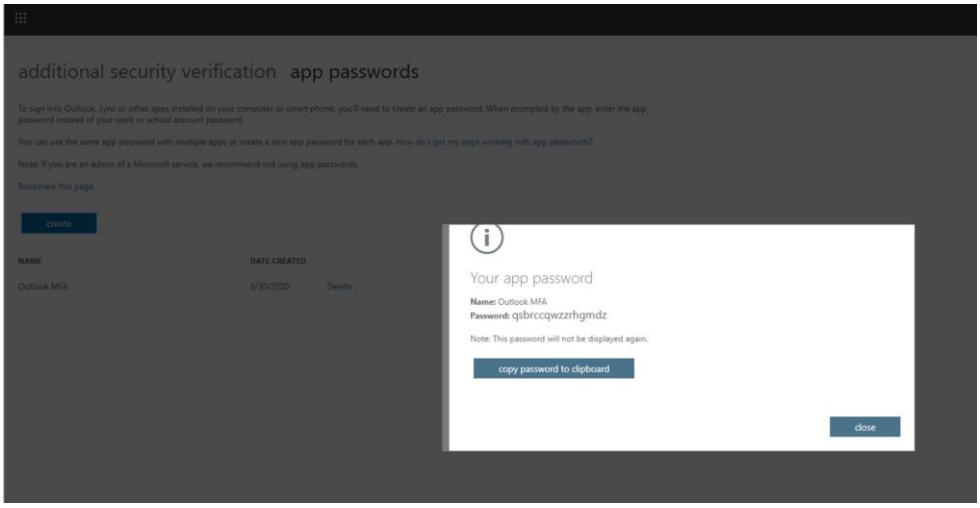
6. You should then see your old App password which you will select 'Delete'.



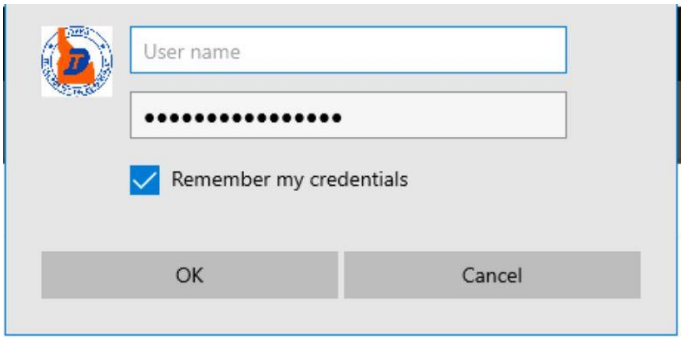
7. Then after it is deleted go ahead and press 'Create App Password'.
8. It will prompt for a name to call it, we suggest "Outlook MFA", and then select 'Next'.



9. This will generate a new app password.



10. Save it to a secure location so you can get to it at a later date.
11. Paste the password into Outlook and then log in.

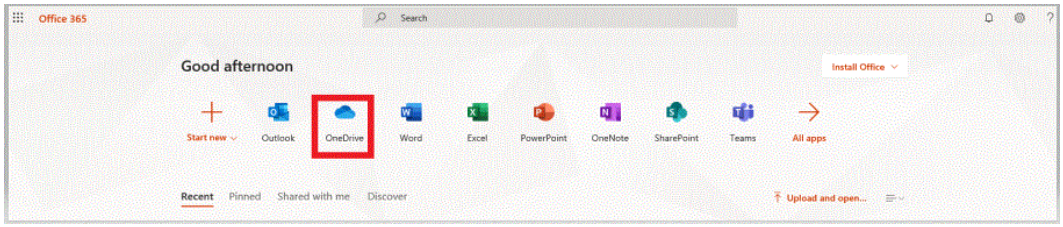


OneDrive Setup Instructions

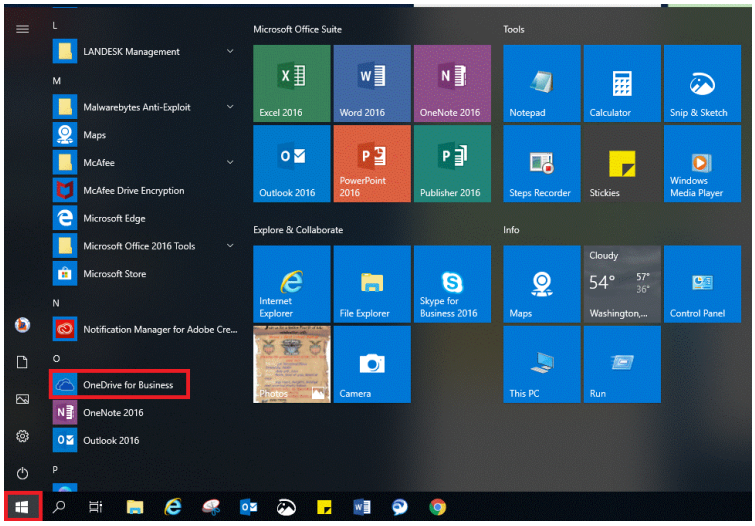
There are different ways to open OneDrive for Business.

The following information illustrates the options available to start OneDrive for Business.

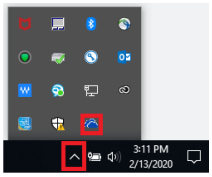
- Method 1: Go online and log into your Office 365 Microsoft account using your ITD credentials.
  Once logged in, navigate to the Apps section.
  Select the OneDrive app.



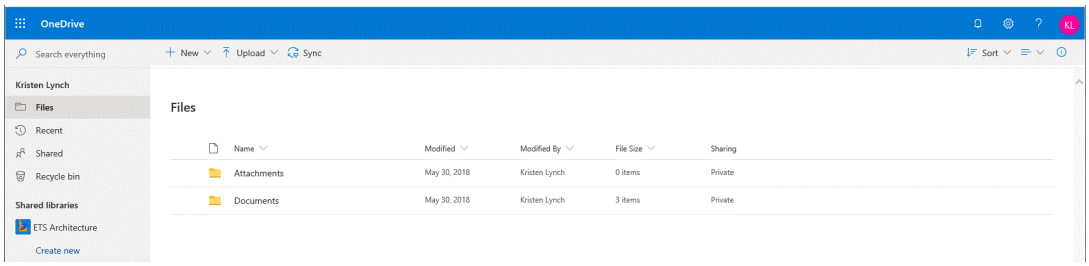
- Method 2: Access your OneDrive folder directly from your desktop.
  Click on the Windows Start icon, and then double-click on the OneDrive for Business icon.
  Note: In order to use this method you will need to first email Service Center for permissions.



- Method 3: On the lower right corner of your computer screen, click the up arrow to access hidden icons, and then double-click on the OneDrive icon.



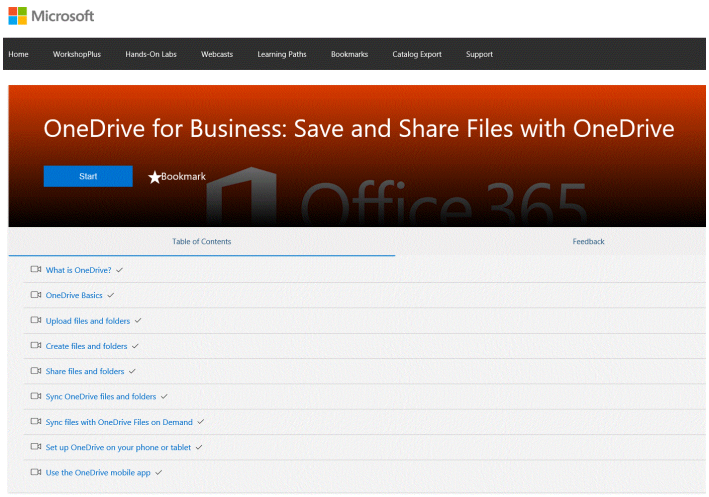
After accessing OneDrive, the file navigation page opens.



Quick tips for getting started

Once in the OneDrive page, you can upload files, share files, sync files, and collaborate in real time.

Additional learning tools and training can be accessed on the Microsoft support pages.



Note: As a reminder, OneDrive for Business creates opportunities for sharing and storing files. ITD follows the ITA governing policies for employee personal computer use. OneDrive for Business should only be used for ITD business-related content.

Please see guidelines here: https://ita.idaho.gov/resources/

Additional Resources

Visit the ITD Collaboration Tools site which includes instructional Videos for Office 365, OneDrive and Microsoft TEAMS.

Additional Support

The Service Center is staffed Monday through Friday (excluding state holidays) operation hours are 7:00 A.M. to 6:00 P.M. (Mountain Time). Additional support can be reached as follows:

Service Center *Phone*: 208-334-8175

- Email: Service.Center@itd.idaho.gov

DMV Helpdesk *phone*: 1-800-634-7790

- Email: ITDDMVHelpDesk@itd.idaho.gov

Advantage *Phone*: 208-332-2020

- Email: AdvantagePasswordResets@itd.idaho.gov