DCMA Teleworker's Reference Guide

7APR2020, Rev. 1

Contents

1. Quick Tips for Teleworkers

1.1 Connecting to a Wi-Fi network

1.1.1 The first time you attempt to connect your computer to a wireless network, you will see the following icon in the system tray located in the lower right of your screen.

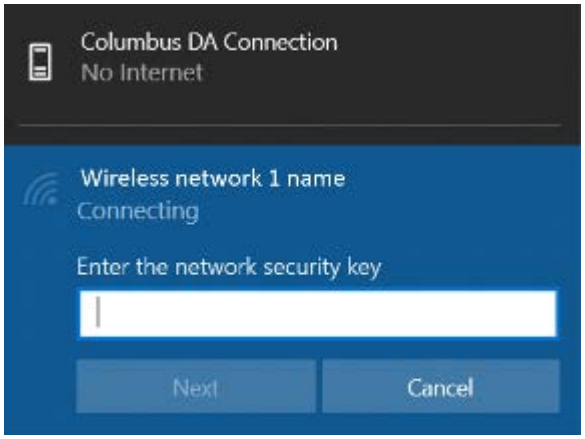
1.1.2 Left-click on this icon to reveal the available wireless networks as shown to the right.

1.1.3 Left click on the desired wireless network name and click the **Connect automatically** option.

1.1.4 This action will cause an automatic reconnection when joining a Wi-Fi network. It will also join automatically upon a reboot to receive computer policies.

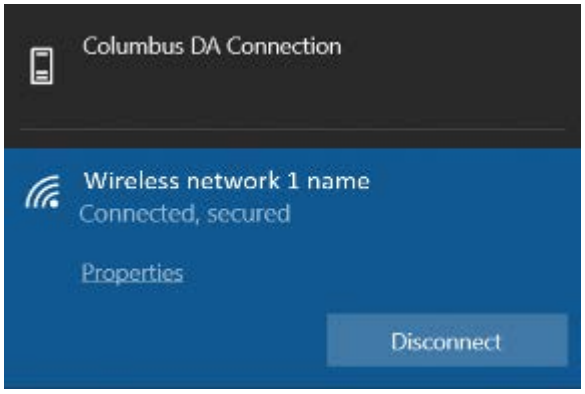
1.1.5 Click the **Connect** button. When prompted, enter the network password.

*****NOTE: If the network does not have a password, switch to a password protected wireless network. The word "Secured" under the wireless network name indicates an encrypted connection and use of a password. *****



1.1.6 Click the Next button.

1.1.7 A successful connection looks similar to the below image.



1.2 While in a telework status use Outlook Web Access (OWA)

1.2.1 With the increase in telework, remote access solutions are more important than ever. Using Outlook over DA may cause an increase in experienced slowness or errors.

1.2.2 To help alleviate some of the traffic through DA, please use web mail to access your email rather than the full Outlook client. OWA works even if DA is down. This also preserves bandwidth for other critical applications.

1.2.3 Refer to Section 3 on OWA access in this document.

1.3 Accessing Personal Storage Table (PST) files

1.3.1 PST files are not accessible when using OWA. If this need arises, open the Outlook client only for the time necessary to access the required information. Close the Outlook client and return to using OWA.

1.3.2 Although this may seem trivial, several thousand instances of this action will degrade bandwidth performance for everyone within DCMA.

1.4 Do not leave websites open that are not actively in use

1.4.1 With each website open (eTools, DCMA360, DCPDS, etc., data is continually attempting to be refreshed.

1.4.2 Although this may seem trivial, several thousand instances of this action will degrade bandwidth performance for everyone within DCMA.

1.5 Leave your computer powered on and connected

1.5.1 Even in a telework state, it is important to keep the computer powered on and connected. Required updates and patches download and install overnight when the computer is not is use due to their high bandwidth usage. Computers not allowed to receive their updates and patches are denied access to the DCMA network.

2. What is DirectAccess (DA)?

DirectAccess (DA) allows remote users secure access to internal network file shares, websites, and applications. A DA-enabled computer connects to the Internet, even before the user logs on. Users never have to think about connecting to the internal network. Once again, when a computer is off the DCMA network, the following will apply.

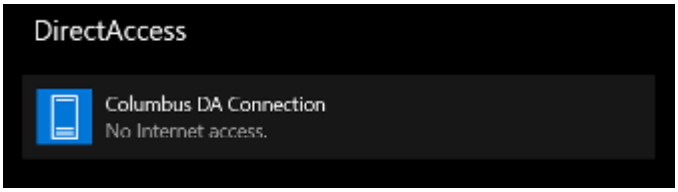
2.1 How do I receive DA?

2.1.1 All DCMA laptops have DA installed. Do not install DA personal home computers for connection to a DCMA network.

2.2 What to look for after logging into my computer

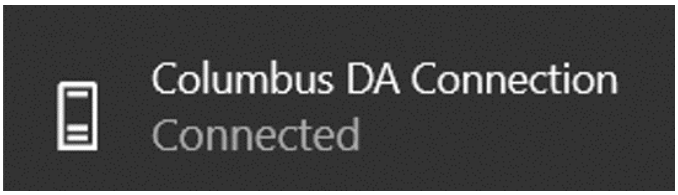
2.2.1 *Wired Network Connection* *Wireless Network Connection*

2.2.2 The image to the right shows the Columbus DA Connection in the disconnected state. Most DCMA websites are not accessible. This state can exist in both a wired and wireless connection.

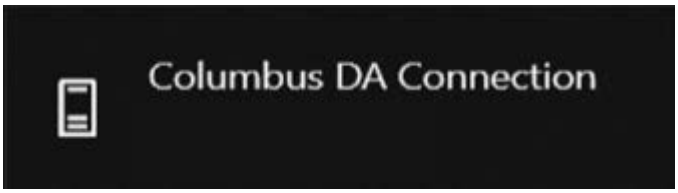


2.2.3 The image to the right shows the Columbus DA Connection in the Connecting state. Most DCMA websites are not accessible. This may take a few minutes depending on network bandwidth.

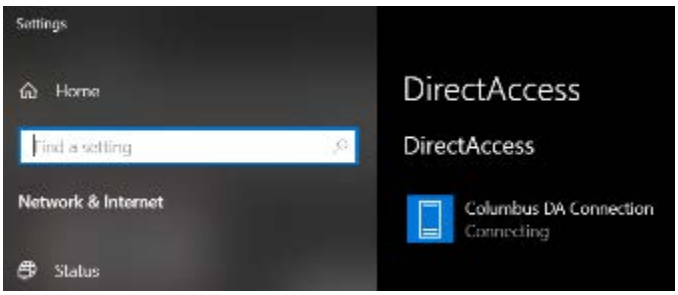
2.2.4 Below, the word “Connected” displays when the connection is established.



2.2.5 On occasion, the DA status may not show.



2.2.6 This is resolved by clicking on the **Columbus DA Connection**. This opens the settings and displays the status of the DA connection.



2.3 DA on the DCMA network

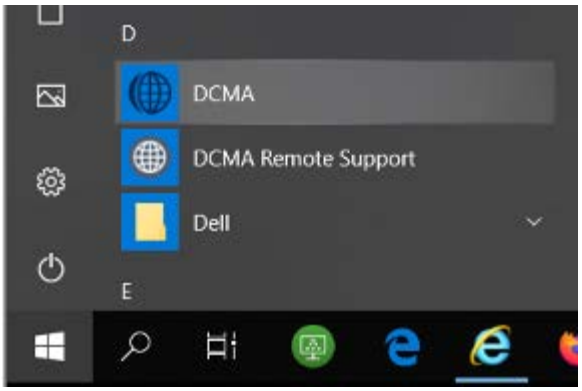
2.3.1 DA recognizes when it is on and off the DCMA network, whether it is a wired or wireless connection. When on the DCMA network, DA is turn off.

2.4 DA off the DCMA network

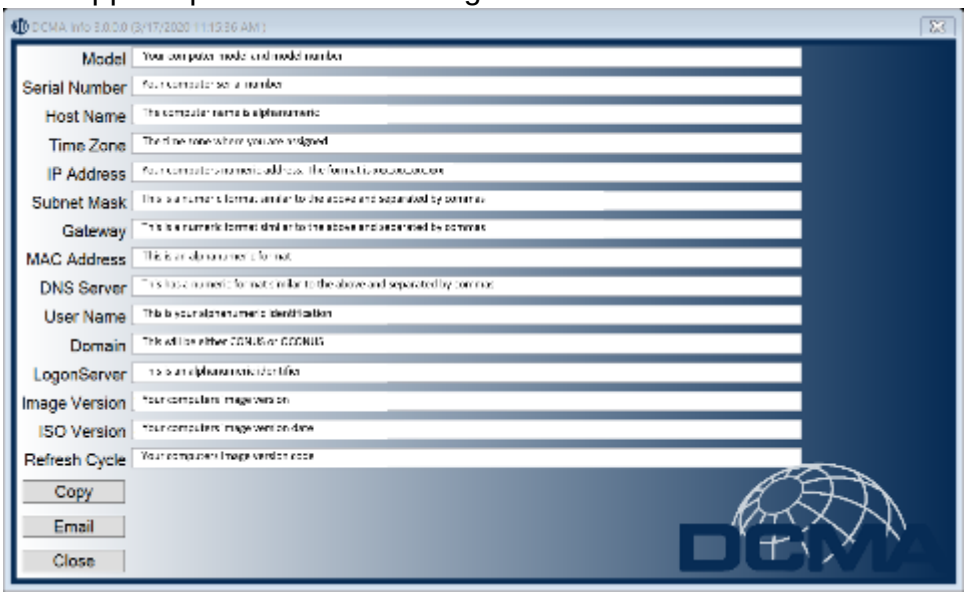
2.4.1 If the **Columbus DA Connection** remains in a *Connecting* state, call the Global Service Center (888.576.3262) or utilize the Service Catalog Portal, (https://servicecenter.dcma.mil/CGWeb/MainUI/ServiceCatalog/ServiceCatalog.aspx) to create an Incident Record to receive technical assistance.

2.5 What else can I provide?

2.5.1 Contained within each DCMA system image is a program that will provide basic information about your computer. This information is found by click the Windows Start button and scrolling through the list of apps.



2.5.2 This app will provide the following information



3. Outlook Web Access (OWA)

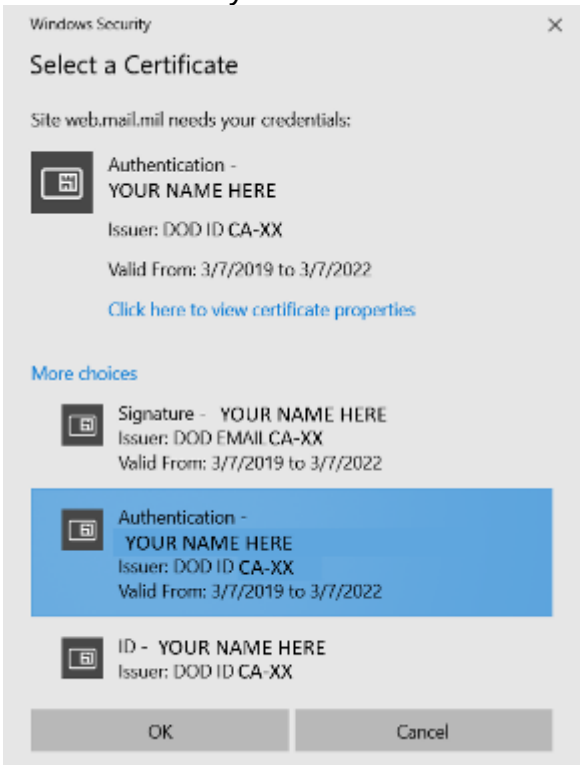
Outlook Web Access (OWA) is a web-based email client. With OWA, customers can access their mailboxes from any Internet connection without the use of DirectAccess.

3.1 Connecting for the first time

***** NOTE: Do not use personal computers. Only use the issued DCMA to conduct work business. *****

3.1.1 From Internet Explorer, enter https://web.mail.mil.

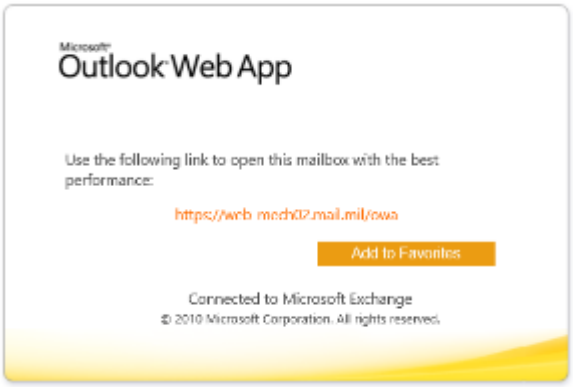
3.1.2 Select your **Authentication / PIV** certificate. If it is not immediately available, click **More choices** to reveal your additional certificates.



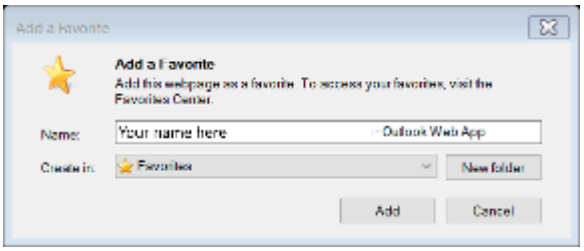
3.1.3 Click the **OK** button.

3.1.4 Click the **OK** button on **USG Warning and Consent Banner.**

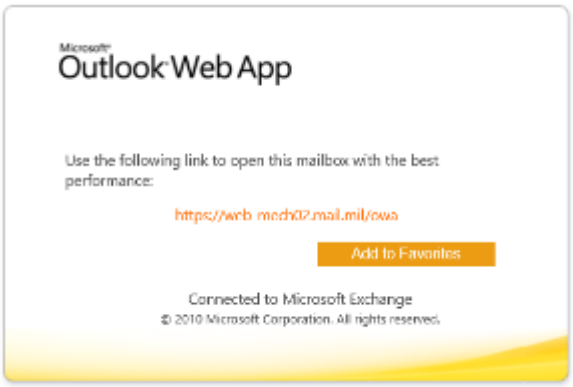
3.1.5 Click the **Add to Favorites** button.



3.1.6 Click the **Add** button.



3.1.7 Click on the link shown above the **Add to Favorites** button.



3.1.8 Ensure to select your **Authentication / PIV** certificate as demonstrated in Section 3.1.2.

3.1.9 Click the **OK** button on the Windows Security popup.

3.1.10 Once again, click the **OK** button on **USG Warning and Consent Banner.** *****NOTE: If you have not accessed OWA previously, the remaining steps display to assist in initial configuration. *****

3.1.11 **Use the blind and low vision experience** is unchecked.

3.1.12 Language is **English (United States).**

3.1.13 Correct time zone is set.

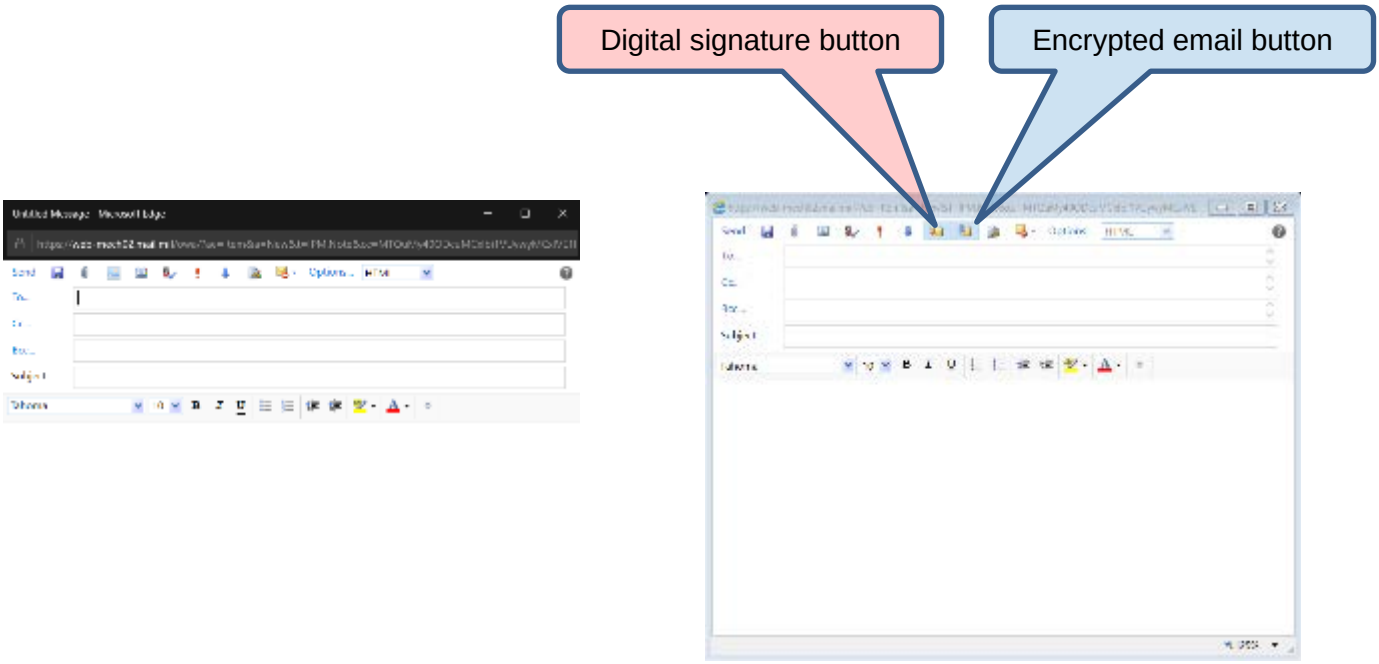
3.1.14 Click the **OK** button.

3.2 Reading encrypted email

***** NOTE: S/MIME is exclusive to the 32-bit version of Internet Explorer. Firefox, Safari, Google Chrome, the 64-bit version of Internet Explorer and Microsoft Edge will not digitally encrypt [or decrypt] email. *****

3.2.1 Customers do not have the permission level to install the S/MIME software on DCMA computers. Call the DCMA Service Center to request this installation.

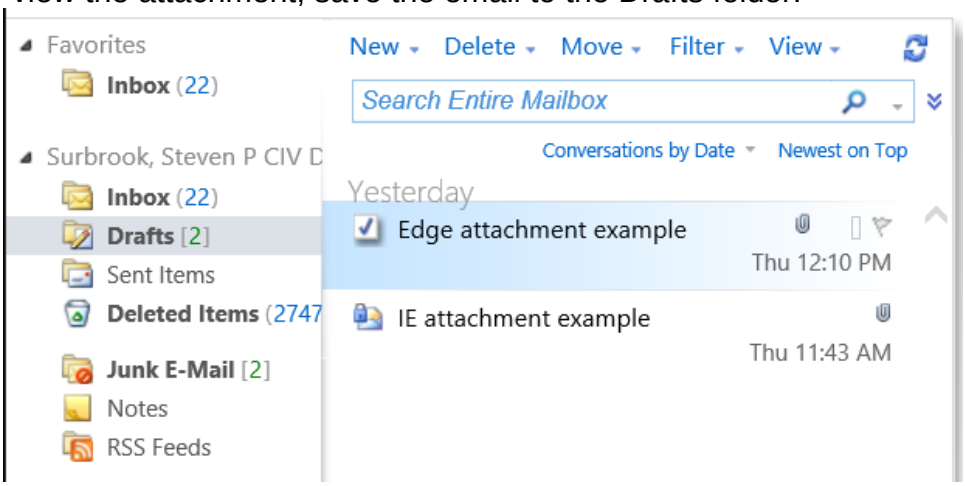
3.2.2 Below is an example of the uniqueness with S/MIME installed and functioning using the 32-bit version of Internet Explorer. The Digital Signature and Encrypted email buttons are available. No other browser will provide this capability.



3.3 Adding email attachments

3.3.1 Internet Explorer will not show the email attachment immediately, giving the perception there is no attachment associated with the email.

3.3.2 To view the attachment, save the email to the Drafts folder.

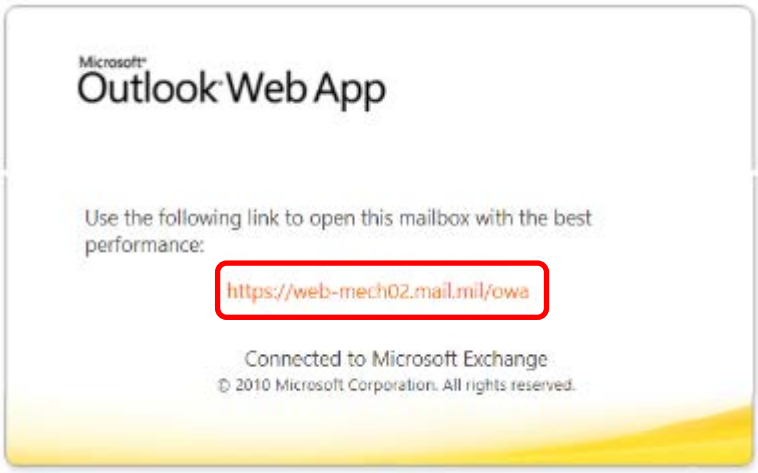


3.3.3 Click on the Drafts folder. This shows the draft email with an attachment and if encrypted is applied.

3.4 Accessing Delegator's calendar and Inbox

3.4.1 If you were able to access another person's calendar and/or Inbox under Outlook, that access is available through OWA.

3.4.2 The Delegator will need to provide their DEE mail pod information from the OWA screen.



3.4.3 The Delegator's full DEE email is required.

3.4.4 In Internet Explorer, click **File>New Session.**

3.4.5 Copy and paste the example URL shown below into Internet Explorer, substituting the information from Steps 3.4.2 and 3.4.3.

Calendar access:

https://web-mech02.mail.mil/owa/first.mi.last.civ@mail.mil/?cmd=contents&module=calendar

Inbox access:

https://web-mech02.mail.mil/owa/first.mi.last.civ@mail.mil/?cmd=contents&module=inbox

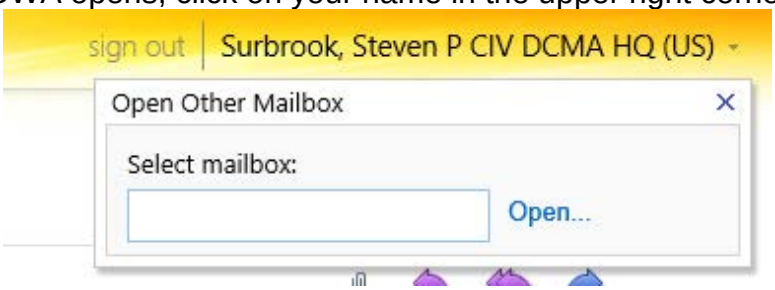
3.4.6 Continue to use your **Authentication / PIV** certificate when prompted.

3.5 Accessing additional mailboxes

3.5.1 Some employees may normally engage in interacting with shared or Non-Person Entity (NPE) mailboxes in the Defense Enterprise Email (DEE) system. Interaction with NPE mailboxes can occur in OWA, although through a slightly different process.

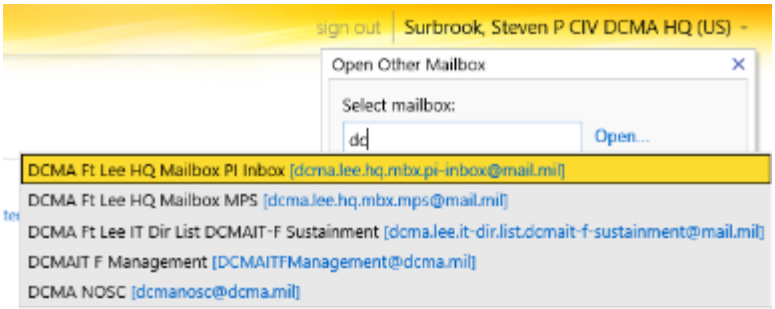
3.5.2 From Internet Explorer, enter https://web.mail.mil as demonstrated in Section 3.1.

3.5.3 After OWA opens, click on your name in the upper right corner.



3.5.4 In the Select Mailbox field, begin typing the friendly name of the shared mailbox. You do not need to enter the mailboxes email address.

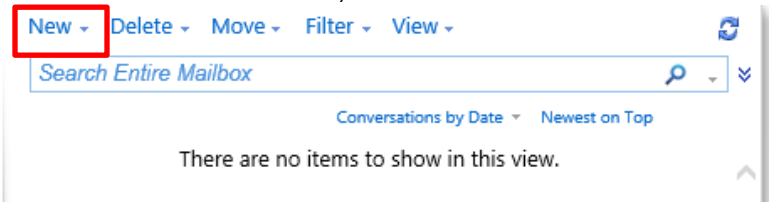
***** NOTE: After you enter the mailbox successfully the first time, an autocomplete list builds. *****



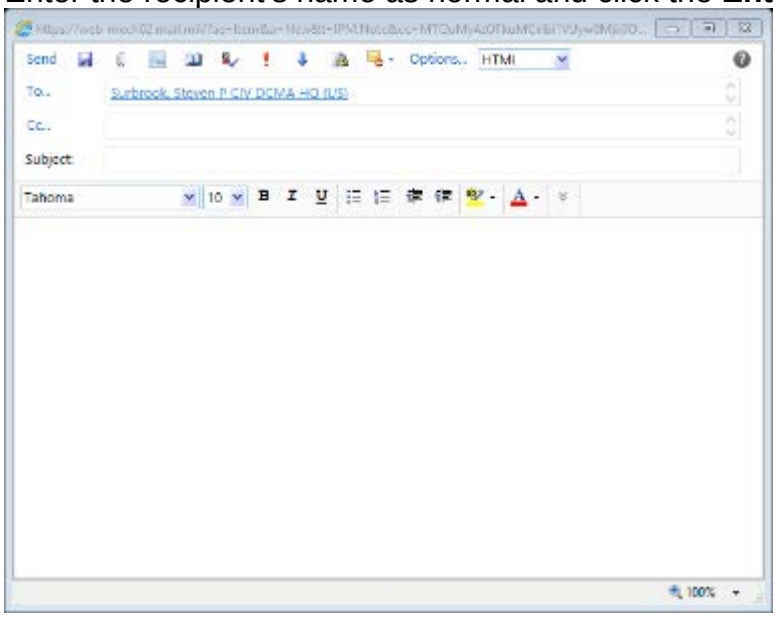
3.5.5 Click the **Open…** button.

3.5.6 Once the mailbox has opened, you may wish to click the **Add to Favorites bar** button to save this mailbox for easy access and use later.

3.5.7 To send an email, click the New button.



3.5.8 Enter the recipient's name as normal and click the **Enter** or **Send** button.



3.5.9 Click on the shared mailbox name.

3.5.10 To return to your mailbox, follow the same process.

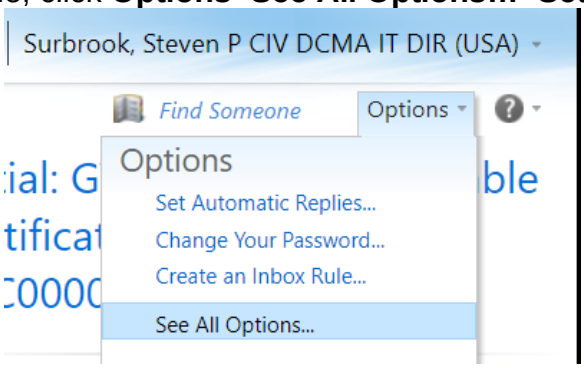
3.6 Time zone setting

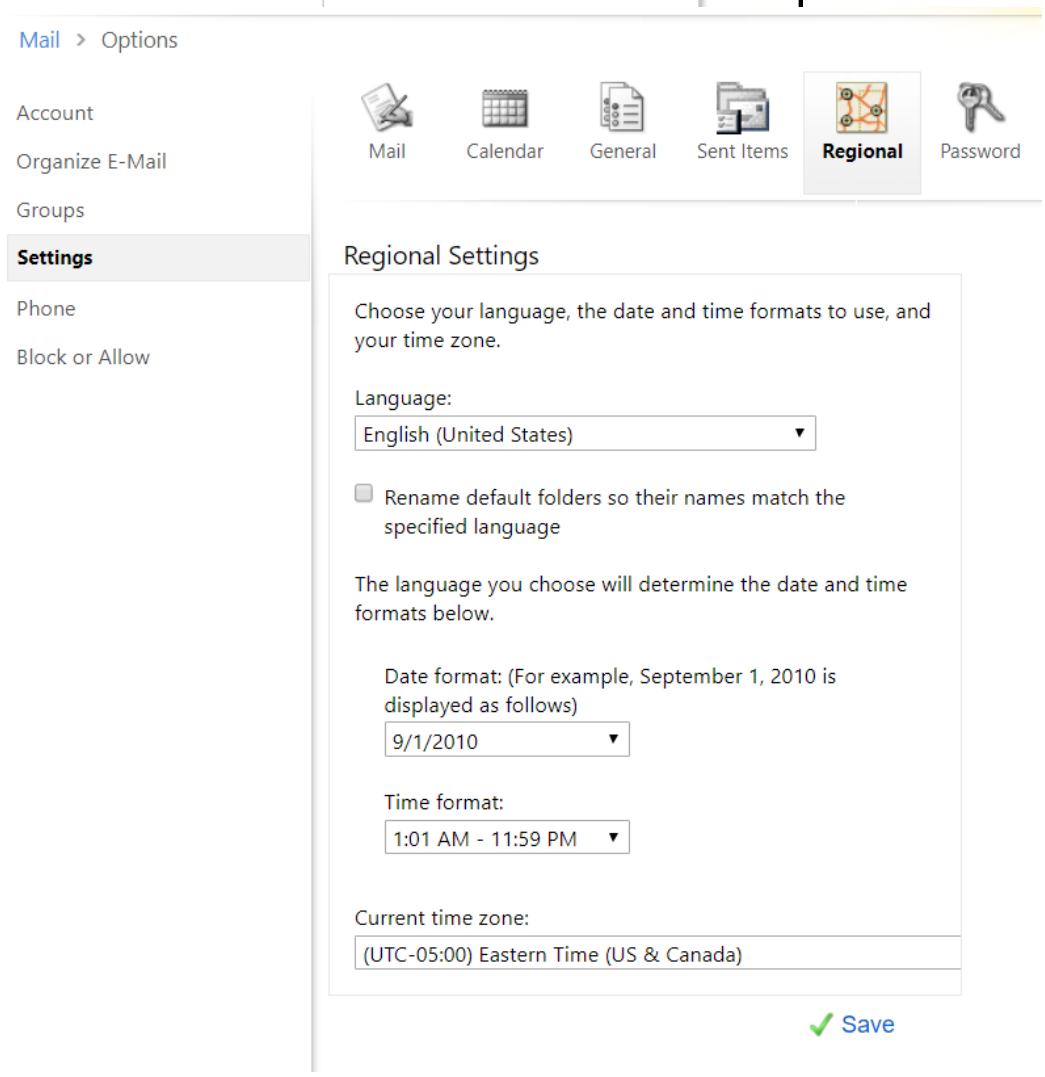
3.6.1 The OWA client does not utilize the time zone on your computer or in your Outlook Desktop Client. It must bet set.

3.6.2 When accessing a supervisor's calendar, there is a known issue that the displayed calendar times are not accurate even though they are correct in the delegator's (supervisors) calendar.

3.6.3 Setting to Universal Time Coordinated (UTC) will offset your calendar.

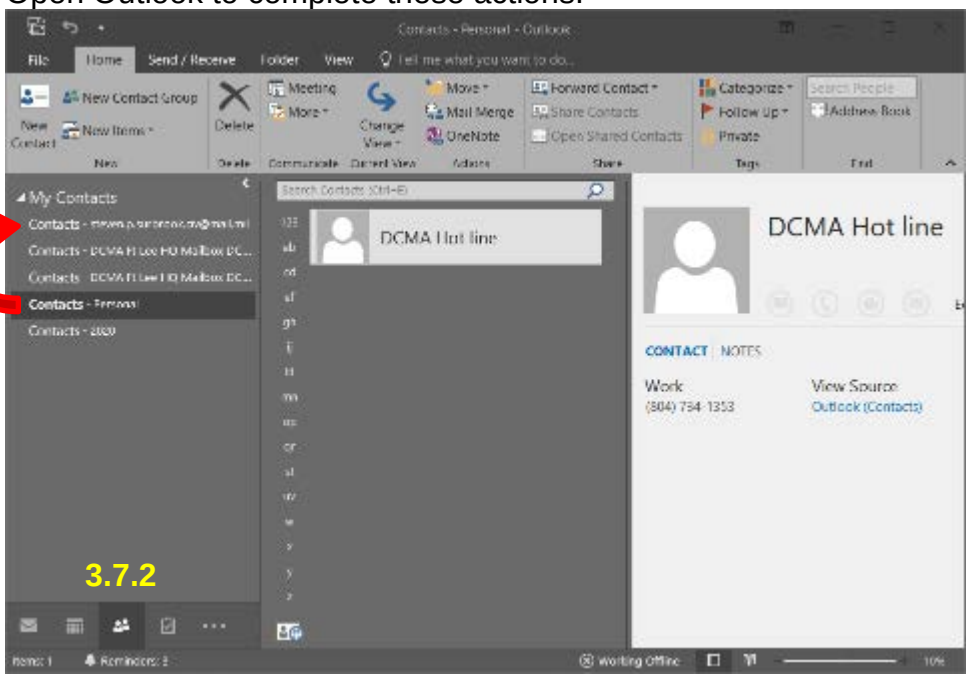
3.6.5 Under your name, click **Options**>**See All Options…**>**Settings**>**Regional**.





3.7 Copy contacts to your DEE mailbox

3.7.1 Open Outlook to complete these actions.



3.7.2 Click the **Contacts** icon.

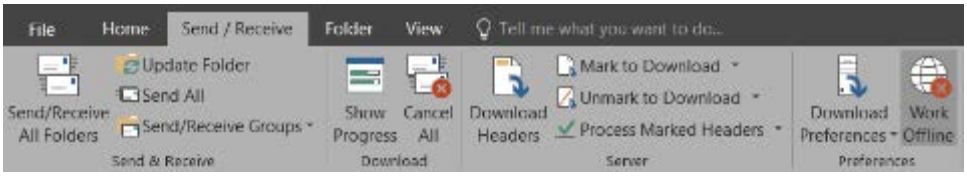
3.7.3 Drag and drop all contacts saved in PST's to your mail.mil Contacts folder. These contacts will become available in OWA.

3.8 Accessing email in a PST

3.8.1 You will need to place Outlook in a **Work Offline** mode.

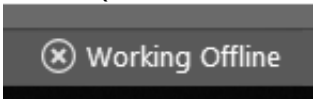
3.8.2 This will prevent Outlook from requesting a CAC certificate when accessing information (e.g. email in a PST).

3.8.3 Click the **Send / Receive** tab then the **Work Offline** button.



3.8.4 Two additional offline status indicate are:

Outlook status (bottom of the screen)



Outlook task bar icon

3.8.5 Revert after the non-peak restriction hours (0800-1800 ET) for mailbox synchronization.

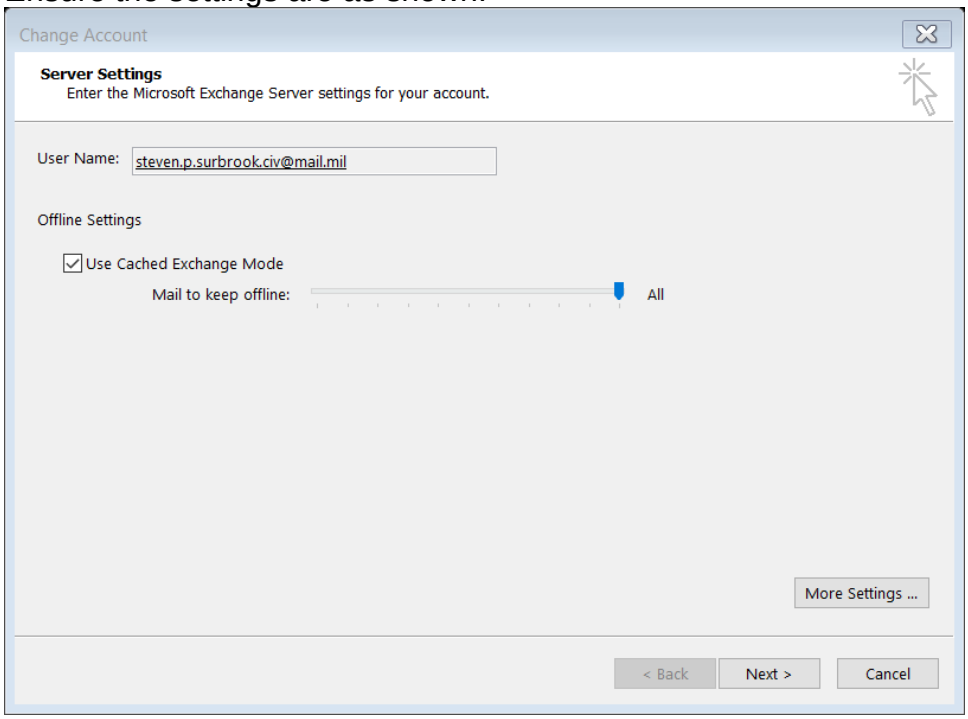
3.9 Turning on Cached Mode in Outlook

3.9.1 Cached Exchange Mode enables a better experience when you use an Exchange account. In this mode, Outlook saves a local copy on your computer. This copy provides quick access to your data, and only synchronizes the changes with the Microsoft Exchange server.

3.9.2 To check Cached Mode status, click **File**>**Account Settings**>**Account Settings…**

3.9.3 Double-click the email account.

3.9.4 Ensure the settings are as shown:

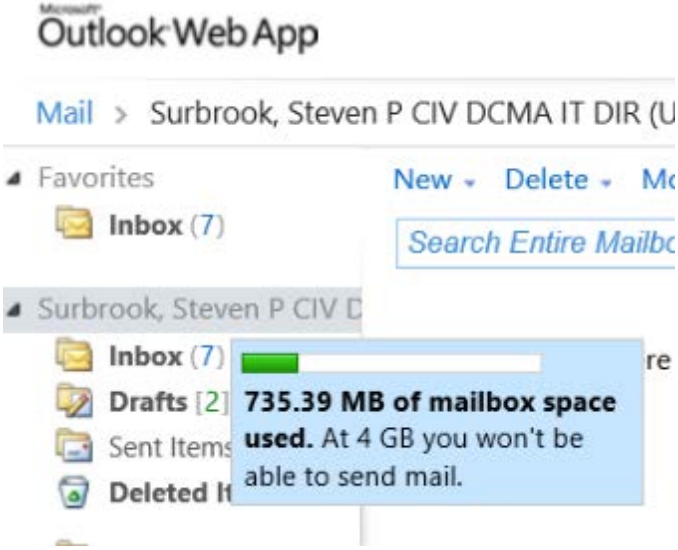


3.10 Mailbox Cleanup

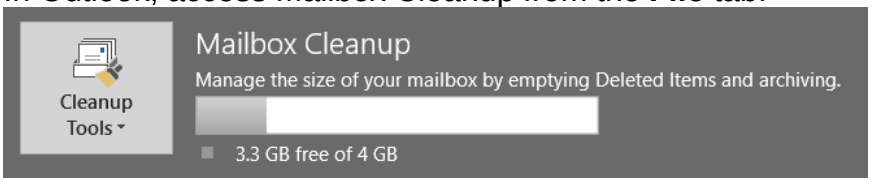
3.10.1 A 4GB mailbox size is of concern since OWA does not access PST's or apply rules associated with PST's.

3.10.2 You need to monitor this size.

3.10.3 In OWA, hover over your name on the left and the usage displays.



3.10.4 In Outlook, access Mailbox Cleanup from the **File** tab.



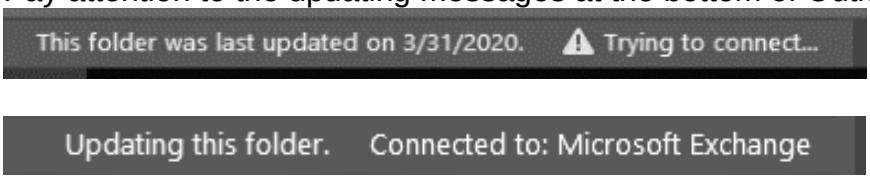
3.10.5 Customer's need to plan this work outside of the 0800-1800 ET restricted Outlook hours.

3.10.6 Disconnect from all DCMA360 shared calendars. You will receive a Send/Receive error.

3.10.7 Turn off **Work Offline**. Authentication will begin. Restart Outlook.

3.10.8 Expect synchronization time to take an extensive amount of time…may be hours!

3.10.9 Pay attention to the updating messages at the bottom of Outlook!



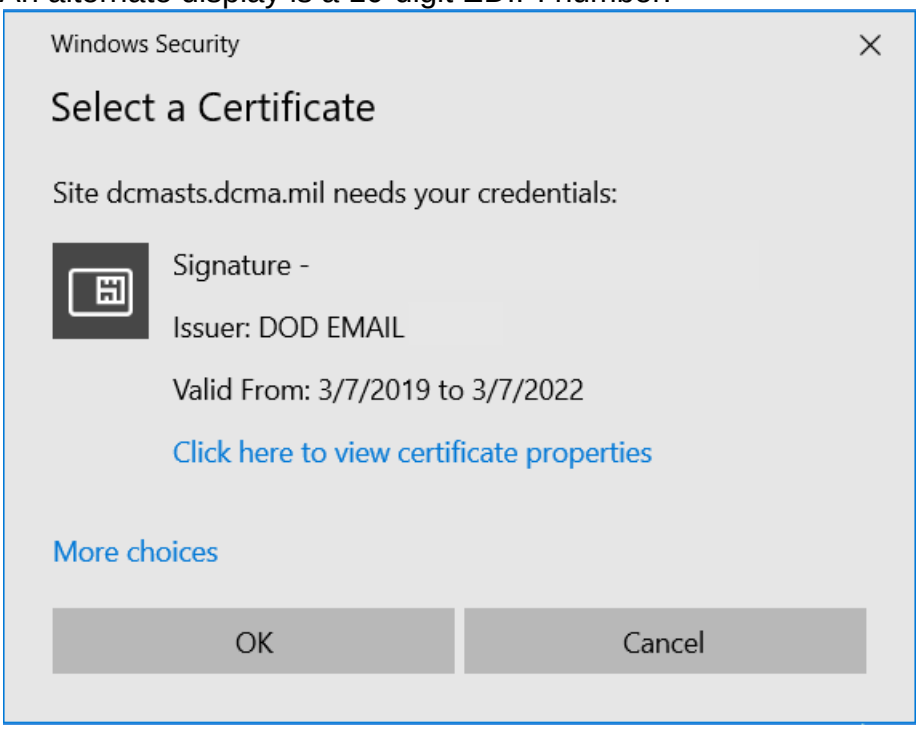
3.10.10 Email displayed in OWA may not show in the Outlook client immediately.

4. CAC Certificate Selection

4.1 Signature (email) certificate

4.1.1 Use this certificate to access DCMA related apps and sites (e.g. DCMA360, eTools, etc.)

4.1.2 An alternate display is a 10-digit EDIPI number.

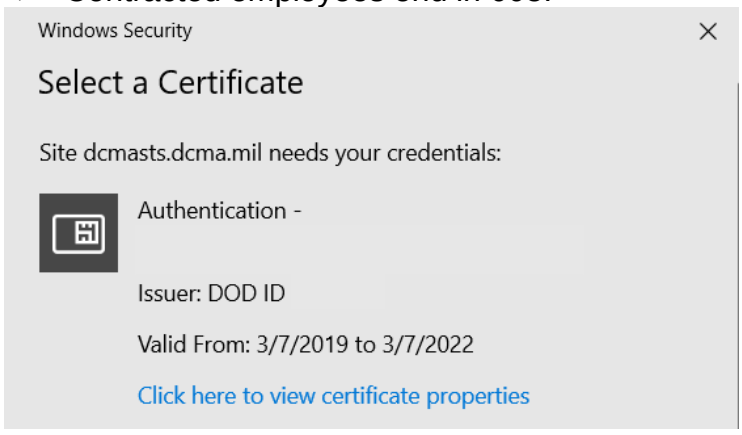


4.2 Authentication / PIV certificate

4.2.1 Used to access DISA related apps and sites (refer to chart in Step 4.3.1).

4.2.2 An alternate display is a 16-digit EDIPI number.

- Civilians end in 002.
- Military end in 004.
- Contracted employees end in 005.



4.3 Other CAC enabled sites

4.3.1 Refer to the table below for the site itself for the recommended certificate.

Service	Cert
Outlook for DEE	Authentication / PIV Cert
Outlook Web App (Web Mail for DEE)	Authentication / PIV Cert
DEPS SharePoint	Authentication / PIV Cert
DCS Chat	Authentication / PIV Cert
Defense Collaboration Services (DCS)	Authentication / PIV Cert
Global Video Services (GVS)	Authentication / PIV Cert
milDrive	Authentication / PIV Cert
Defense Travel System (DTS)	ID or Authentication / PIV Cert
DLA and DFAS Apps	Signature / Email Cert
Defense Agencies Initiative (DAI)	Any Cert
MyPay	Any Cert
milConnect	Any Cert

5. Terminal Server

5.1 Used for select applications

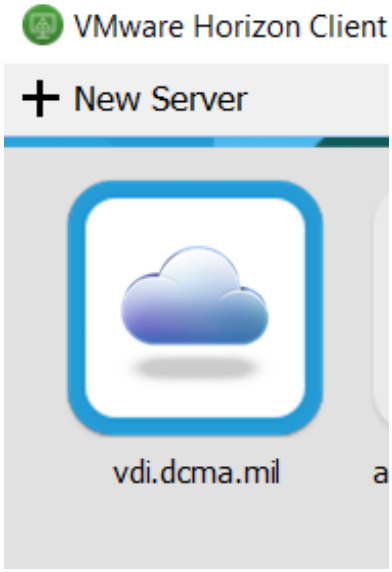
5.1.1 The Terminal Server desktop is pre-populated.

5.1.2 You cannot save information on the desktop like your computer. It is a temporary instance.

5.1.3 Click the Windows flag.

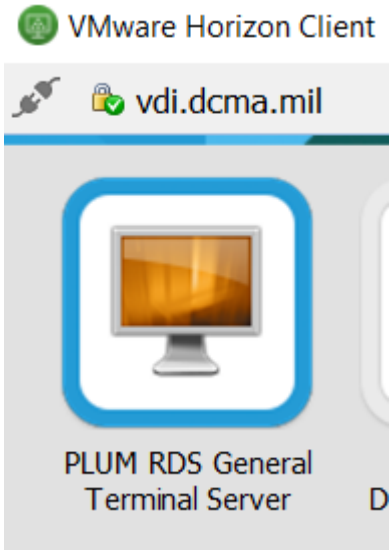
5.1.4 The **VMWare Horizon Client** app is on the Start menu of your computer.

5.1.5 If your VMWare session does not match the image below, click the **+ New Server** button.



5.1.6 Type **vdi.dcma.mil** in the field followed by the **Connect** button.

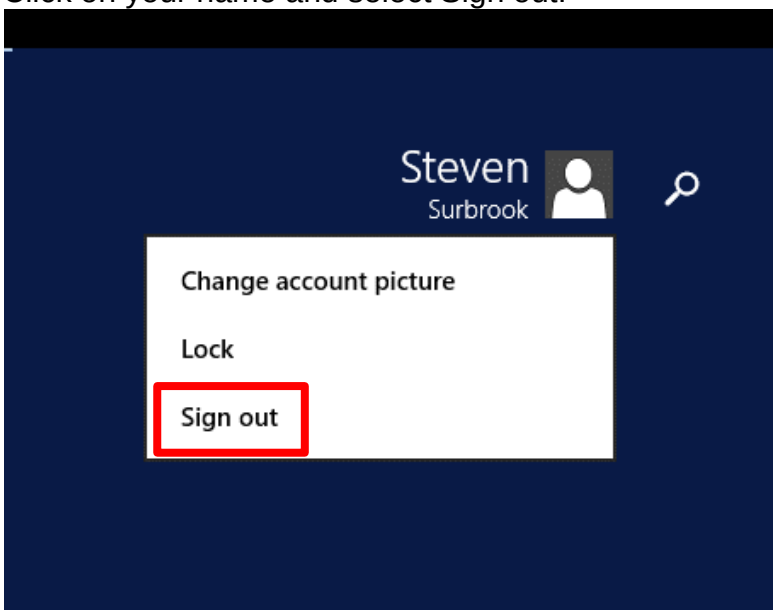
5.1.7 Click the terminal server option shown.



5.1.8 Logging in is similar to your computer.

5.1.9 When you are finished, sign out vs closing the Horizon view client.

5.1.10 Click on the Windows Flag (Start) in the lower left corner. This will bring you to the Start screen. In the upper right hand corner, you will see your name. Click on your name and select Sign out.



5.1.11 This will free a TS connection for another customer to use.

6. Large File Transfers

6.1 DoD SAFE

6.1.1 Use as an alternate secure file transfer vehicle for files up to 8GB.

6.1.2 The URL: https://safe.apps.mil/

6.1.3 Users should select their SIGNATURE certificate issued through the DoD email Certificate Authority (CA) or select the AUTHENTICATION PIV certificate issued by the DOD Identifier (ID) Certificate Authority (CA) in order to connect.

6.1.4 Users outside of DoD may notice lengthy download and upload times depending on their bandwidth availability.

6.1.5 Seven days after upload, DoD SAFE deletes the files.

7. Home Network Troubleshooting

7.1 My computer is slower at home than in the office.

7.1.1 Call your Internet Service Provider (ISP) to determine the level of service you should be receiving for your monthly payment.

7.1.2 Most ISP's provide a speed test site that will measure the present download and upload speed you are currently receiving. Speedtest.net,

(www.speedtest.net), is a generic alternative that will provide the same information.

7.1.3 The ISP will run remote diagnostics and determine if their equipment is faulty or needs updating. If there is no issue on their end, the fault will lie with your home networking equipment.

7.1.4 There are many components in play to provide internet in a home. A simple check of the major components (personally owned modem and router or an ISP provided gateway) usually will repair most issues.

7.2 Rebooting a privately owned modem

7.2.1 The first step is to unplug the power to the modem for a length of 60 seconds then plug it back in and allow 2-3 minutes for the modem to fully initialize.

7.2.2 If you have owned your modem for a while, there has been a significant change in modem technology. The Data over Cable Service Interface Specification (aka DOCSIS) continues to update resulting in improvements to security and new internet technology.

7.2.3 The current industry standard is DOCSIS 3.1 as of 2016, bringing with it another massive leap in both up and downstream speeds. This iteration brought the cap to 10 Gbps for download speed and 1 Gbps for upload speed.

7.2.4 This is a 2014 YouTube video demonstrating the difference in modem technology between DOCSIS 2.0 and 3.0, (https://www.youtube.com/watch?v=QrmchiDbIVg).

7.3 Rebooting a privately owned router

7.3.1 If you find that the modem has not corrected the issue, the next step is to unplug the power to the router for a length of 60 seconds then plug it back in and allow 2-3 minutes for the router to initialize and establish connectivity with the devices on your home network.

7.4 Resetting your router

7.4.1 If it becomes necessary to reset your router, be advised that you will lose all of your previously configured settings. The router will reset to the factory default settings. To name just a few, these settings will include:

1) Wireless network (SSID) name;
2) Wireless password; and
3) Channel settings

7.4.2 Most routers will have a small access hole in the back by the Ethernet ports (where you plug your wired connects). Insert a pen or reshaped paper clip and press the recessed button for a period of 5-10 seconds.

7.4.3 Here is a generic example from YouTube on resetting a router, https://www.youtube.com/watch?v=BAdikT_JmP4.

7.5 Updating your router's firmware

7.5.1 From time to time, manufacturers will publish new firmware for your specific make and model to allow it to perform better. Consult your manufacturer's website to determine if a firmware update is available.

*****NOTE: If applied incorrectly, there is a chance you will "brick" your router and make it nonfunctional. *****

7.6 Prioritizing data in your router settings

7.6.1 Newer routers allow for more enhanced control over how it handles your data. Technologies such as Voice over Internet Protocol (VoIP) may need priority to ensure a smooth and consistent phone call. You may want this for your video streaming application also.

8. ISP Provided Equipment

ISP provided equipment is convenient method of ensuring access to the internet, TV, etc., while having the modem and router in a single package it also removes the potential for equipment compatibility concerns. However, even with these units, the occasion may arise that resetting / rebooting is necessary.

8.1 Rebooting a leased ISP gateway device

8.1.1 If you pay a monthly lease fee for a device from your ISP, generally speaking, the rebooting process is similar to that of a privately owned device.

8.1.2 Although it is always best to consult your ISP on the functionality of their equipment, the process is typically the same. Unplug the power to the device for a length of 60 seconds then plug it back in and allow 2-3 minutes for the device to fully initialize.

9. List of Major CONUS Internet Service Providers

Below is a list of the major ISP providers within the continental United States. Some have “Self-Help” videos available on deeper technical content.

9.1 Sparklight:
https://support.sparklight.com/hc/en-us

9.2 Optimum:
https://www.optimum.net/support/alticeone-picker/?referer=%2fsupport%2f

9.3 Spectrum:
https://www.spectrum.net/support/?cmp=slp-con-ica-res-twc

9.4 Xfinity:
https://www.xfinity.com/support/contact-us

9.5 Cox Communications:
https://www.cox.com/residential/contactus.html

9.6 Mediacom:
http://mediacomcc.custhelp.com/

9.7 Midcontinent Communications:
https://www.midco.com/support/

9.8 RCN:
https://www.rcn.com/hub/help/

9.9 AT&T:
https://www.att.com/support/topic/u-verse-high-speed-internet/

9.10 Verizon:
https://www.verizon.com/support/residential/home