## Contents

1. **Quick Tips for Teleworkers** ................................................................. 1
   1.1 Connecting to a Wi-Fi network ............................................................... 1
   1.2 Accessing Personal Storage Table (PST) files ........................................ 3
   1.3 Do not leave websites open that are not actively in use ......................... 3
   1.4 Leave your computer powered on and connected .................................... 3

2. **What is a Virtual Private Network (VPN)?** ........................................... 3
   2.1 The DCMA f5 BIG-IP Edge client ............................................................ 3
   2.2 Split vs Full tunnel mode ........................................................................ 4
   2.3 Which VPN am I using? ......................................................................... 4

3. **Cloud Based Internet Solution (CBII)** .................................................. 5
   3.1 CBII and the VPN tunnel ....................................................................... 5

4. **Outlook Web Access (OWA)** ............................................................... 5
   4.1 Connecting for the first time ..................................................................... 6
   4.2 Encrypted email via Internet Explorer ...................................................... 9
   4.3 Encrypted email via Microsoft Edge ......................................................... 12
   4.4 Email attachments ................................................................................. 15
   4.5 Accessing another email account (Personal or Organizational) ............... 15
   4.6 Contact lists ......................................................................................... 17

5. **Importing PST Data to Outlook 365** .................................................... 17
   5.1 Transferring PST data to the Outlook 365 mailbox ................................. 18

6. **CAC Certificate Selection** .................................................................... 19
   6.1 Authentication / PIV certificate ............................................................... 19

7. **DoD365 OneDrive** ................................................................................. 19
   7.1 Initial Setup ......................................................................................... 20
   7.2 Sync Errors ........................................................................................ 23

8. **Terminal Server** ................................................................................... 25
   8.1 Initial Setup ......................................................................................... 25

9. **Large File Transfers** ............................................................................ 28
   9.1 DoD SAFE .......................................................................................... 28

10. **Home Network Troubleshooting** ......................................................... 29
    10.1 My computer is slower at home than in the office ................................. 29
    10.2 Rebooting a privately owned modem .................................................. 29
    10.3 Rebooting a privately owned router ...................................................... 29
10.4 Resetting your router .................................................................30
10.5 Updating your router’s firmware .............................................30
10.6 Prioritizing data in your router settings ..................................30

11. ISP Provided Equipment ..............................................................30
11.1 Rebooting a leased ISP gateway device .....................................30

12. List of Major CONUS Internet Service Providers .......................31
12.1 Sparklight: ..................................................................................31
12.2 Optimum: ....................................................................................31
12.3 Spectrum: ....................................................................................31
12.4 Xfinity: ........................................................................................31
12.5 Cox Communications: ...............................................................31
12.6 Mediacom: ..................................................................................31
12.7 Midcontinent Communications: ...............................................31
12.8 RCN: ............................................................................................31
12.9 AT&T: ............................................................................................31
12.10 Verizon: ......................................................................................31
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 one of the following icons in the system tray located in the lower right of your screen.

or

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.

![Image of wireless network selection](image)

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.

1.2.1 PST files are not accessible when using Outlook Web Access (OWA). If this need arises, open the Outlook desktop client to access the required information.

1.3 Do not leave websites open that are not actively in use
1.3.1 With each website open (eTools, DCMA360, DCPDS, etc., data is continually attempting to be refreshed.

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

1.4 Leave your computer powered on and connected
1.4.1 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 in use due to their high bandwidth usage. Computers not allowed to receive their updates and patches will be denied access to the DCMA network.

2. What is a Virtual Private Network (VPN)?
A VPN (Virtual Private Network) is a service that puts web traffic in a secure, encrypted tunnel and prevents others from accessing it. A VPN secures your connection to the internet, making it extremely difficult for hackers, marketers, government entities, or ISP (internet service providers) to keep track of your actions online.

2.1 The DCMA f5 BIG-IP Edge client
2.1.1 All DCMA laptops have the f5 Big-IP Edge Client installed. This VPN is an “Always On” connection that will allow connection to .mil websites and resources.
2.1.2 Most commercial traffic for .com, .net, etc. does not go across the VPN but connects directly from the customer’s internet service provider.

2.2 Split vs Full tunnel mode
2.2.1 Split tunnel: A VPN feature that divides your internet traffic and sends some of it through an encrypted VPN but routes the rest through a separate tunnel on the open network as referenced in 2.1.1 and 2.1.2.

2.2.2 Full tunnel: This VPN feature sends all traffic through an encrypted VPN. This is used in specific circumstances where split tunnel failing or geographic blocking is enforced. The use of Full tunnel requires DCMAIT to add the customer to the proper Active Directory group.

2.3 Which VPN am I using?
2.3.1 DCMAIT provides two VPN’s. One is through the Columbus (COLS) datacenter, while the other is through the San Antonio (SATX) datacenter.

2.3.2 Below are the two URL’s for the VPN’s.

   **COLS URL:** v1-cols.dcma.mil  
   **SATX URL:** v1-satx.dcma.mil

2.3.3 To determine if your VPN connection, perform the following steps.
2.3.3.1 Navigate to the following URL:

   https://etools.dcma.mil/showip

   ![Source IP](https://etools.dcma.mil/showip)

   Connection source address appears to DCMA as:  

   2.3.3.2 If the above URL returns x.x.130.x or x.x.216.x, the connection is to SATX.
   2.3.3.3 If the above URL returns x.x.128.x or x.x.16.x, the connection is to COLS.
2.3.4 If the need arises to utilize the full tunnel, connect to the VPN service opposite to the displayed connection. This will avoid potential connection issues.

3. Cloud Based Internet Solution (CBII)
DISA cybersecurity solutions must keep pace with quickly evolving and sophisticated cyber-threats. The evolution and complexity of browser-based attacks on DoD networks continues to rise as DoD continues to leverage cloud-based technologies.

Cloud Based Internet Isolation (CBII) transfers Internet browsing sessions from traditional desktop browsers to a secure, isolated cloud-platform. The service isolates potential malicious code and content within the cloud-platform, separating the threat from direct connections to DOD networks.

3.1 CBII and the VPN tunnel
3.1.1 Without CBII, it is necessary to route all external (.com) web browsing traffic through NIPR users’ VPN connection, so that all applicable browsing policies and security scanning can take place on the traffic.

3.1.2 With CBII, there is no need to utilize the VPN connection for .com browsing. Blacklisting and web categorization blocks happen at the CBII service. CBII browsing traffic bypasses the Internet Access Point (IAP) security stack, so there is no reason for this traffic to come into NIPR through the VPN tunnel and then head directly back out to the internet. File downloads through CBII continue to utilize the VPN so that the files are inspected by the security tools at the IAP.

4. 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.

*** NOTE: Do not use personal computers. ***

*** NOTE: OWA for the DoD365 Joint Tenant is only available on the NIPRNET (network or F5 VPN). ***

*** NOTE: Perform the same steps for both Edge Chromium and Internet Explorer browsers in these steps. ***

*** NOTE: Neither Google Chrome nor Mozilla Firefox are supported. ***
4.1 Connecting for the first time

4.1.1 Open MS Edge and enter https://webmail.apps.mil into the address bar.

4.1.2 Enter your mail.mil email address in the Sign in field.

4.1.3 Under the blue Sign in button, click the Sign in with CAC/PIV link.
4.1.4 Select your **Authentication** certificate. If it is not immediately available, click **More choices** to reveal your additional certificates.

![Select a Certificate](image)

4.1.6 If prompted with the option to **Stay signed in?**, click the **Yes** button.

*** NOTE: Clicking the “Don’t show this again” checkbox will not prevent this from displaying due to a policy setting set by DISA. ***

4.1.7 In the MS Edge address bar, click the **Add to Favorites** star icon. The icon will turn blue.
4.1.8 Click the “>” icon to reveal the addition in the favorites bar. Edge adds new favorites to the bottom of the list.

*** NOTE: Click and drag favorites to new locations to change the display order. A right-click on the favorite reveals the EDIT button to change the name. ***

4.1.9 Enter your mail.mil email address when prompted.
4.1.10 Under the blue Sign in button, click the Sign in with CAC/PIV link.

4.1.11 Select your Authentication certificate.

4.1.12 If prompted with the option to Stay signed in?, click the Yes button.

4.1.13 OWA should open.

4.2 Encrypted email via Internet Explorer

*** NOTE: Internet Explorer is not the preferred browser. Effective June 15, 2022 IE will be retired. ***

4.2.1 Open Internet Explorer and type https://webmail.apps.mil.

4.2.2 Sign in as required, using the Authentication certificate.

4.2.3 In OWA, click the gear Settings icon, and then View all Outlook settings at the bottom of the pane.
4.2.4 In the popup window, select **Mail**, then **S/MIME**.

S/MIME lets you encrypt and digitally sign email messages you send, view encrypted content in messages you receive, and verify sender’s digital signatures. [Learn more](#)

This computer has the most recent version of the S/MIME control installed: 4.0800.20.20.729.1. You can set your email security preferences below. To reinstall the S/MIME control, [click here](#).

- [ ] Encrypt contents and attachments for all messages I send
- [x] Add a digital signature to all messages I send
- [ ] Automatically choose the best certificate for digital signing

4.2.6 Click the **Run** button in the popup at the bottom of the screen.
4.2.7 Click the **OK** button to confirm completion of the successful installation.

![Microsoft S/MIME Control](image)

The S/MIME control was successfully installed on this computer. Before you can send and view S/MIME messages in Outlook Web App, you need to restart your browser.

4.2.9 In OWA, click **New Message**.

![Outlook New message](image)

*** NOTE: DO NOT USE the "Encrypt" button that is on the default toolbar.

This does not utilize the Department of Defense Common Access Card (CAC) Public Key Infrastructure (PKI) technology. ***

4.2.11 Click **Show message options**...
4.2.12 Check both Encrypt this message (S/MIME) and Digitally sign this message (S/MIME).

Message options

Sensitivity
Normal  
- Request a read receipt
- Request a delivery receipt
- Encrypt this message (S/MIME)
- Digitally sign this message (S/MIME)

OK  Cancel

4.2.14 Click the OK button to finalize the encryption.

4.2.15 Perform this process for each email requiring encryption as the setting is for that email.

4.3 Encrypted email via Microsoft Edge

*** NOTE: Edge contains Internet Explorer mode if required. ***

4.3.1 Open Edge and type edge://extensions.

4.3.2 Click the Details link under the Microsoft S/MIME extension.
4.3.3 Click the Extension options link.

What website do you use to sign in to Outlook on the web?

S/MIME can encrypt and decrypt messages using Outlook on the web. To enable S/MIME, choose which website does:

- Microsoft websites. For example, Office.com or Outlook.com.
- Other work or school website domains. For example, if you sign in to Outlook on the web with https://mail.Only add domains that you trust.

webmail1.apps.mil

Save

4.3.5 Restart Edge as directed.

4.3.6 Open Edge and type http://webapps.mail.mil.

4.3.7 If prompted, enter your mail.mil credentials on the Sign in page, along with your Authentication certificate.

4.3.8 Click the OK button to confirm completion of the successful installation.
4.3.9 In OWA, click **New Message**.

**NOTE:** DO NOT USE the "Encrypt" button that is on the default toolbar. This does not utilize the Department of Defense Common Access Card (CAC) Public Key Infrastructure (PKI) technology. **

4.3.11 Click **Show message options...**

4.3.12 Check both **Encrypt this message (S/MIME)** and **Digitally sign this message (S/MIME)**.
4.3.14 Click the **OK** button to finalize the encryption.

4.3.15 Perform this process for each email requiring encryption.

4.4 Email attachments
4.4.1 Unlike the previous version of OWA, email attachments are displaying as expected.

4.5 Accessing another email account (Personal or Organizational)
4.5.1 If you were able to access another person’s email assets (Inbox, Calendar, etc.) or a Non-Person Entity (aka Organizational Mailbox) using Outlook, that access is available through OWA.

4.5.2 With OWA open, right-click **Folders** in the left pane.
4.5.3 Click **Add shared folder**.

**NOTE:** Pay close attention as distribution lists and mailboxes are easily confused and incorrectly chosen. **

4.5.6 The additional email account will display in the list.
4.6 **Contact lists**

4.6.1 On the left of the screen, click on the **People** icon.

---

5. **Importing PST Data to Outlook 365**

With the migration to DoD Office 365 comes the need to import Outlook data (emails, folders, archives, etc.) normally stored in PST files.

There are a few reasons you should do this:
- Migration to DoD Office 365 increased your available Outlook storage to 100GB. Outlook 365 does not support the use of PSTs.
- OneDrive prohibits the synchronization of PST file types will not back up to the cloud.
- Eventually, all office productivity will be through DoD Office 365.
5.1 Transferring PST data to the Outlook 365 mailbox

***NOTE: DO NOT IMPORT A PST FILE IN A SINGLE ACTION. Due to network bandwidth of both DCMA and DISA, along with the potential volume of DCMA and the DISA tenant employee base performing this action simultaneously, file transfers may take several hours up to days to complete.***

5.1.1 Log into the client (desktop icon) Outlook application.

5.1.2 Ensure the PST data files are open in Outlook.

5.1.3 Select and drag data from the PST (see image callout B), and drop into the Inbox (see image callout A) in small amounts (recommend 10-15 day clusters).

5.1.5 After moving all data from the PST to the Inbox, close that PST file in the Outlook client and delete the PST file from the computer.
5.1.6 The data transfer can take a long time. Schedule time for the transfer during non-peak work times, or transfer data in small chunks (recommend 10-15 day clusters).

***NOTE: While Outlook imports data from the PSTs, there will be NO access to email. However, email is accessible through OWA. ***

5.1.7 If you wish to maintain folder/file integrity of your imported PST, recreate the structure in the Inbox before importing data as shown in the graphic of Step 5.4, callout C.

5.1.8 Certain items (draft emails, acknowledge calendar invites) seem to prove challenging in the transfer. Outlook provides a warning that recreating items in the Inbox may take a while. Cancelling the process will cancel the entire transfer. Remove or delete these items from the PST file before beginning the migration.

5.1.9 If you run into difficulties with the transfer, please contact the DCMA Global Service Center for support.

6. CAC Certificate Selection

6.1 Authentication / PIV certificate

6.1.1 Unless specifically noted, the Authentication / PIV certificate is the certificate used to access all apps and sites.

7. DoD365 OneDrive

*** NOTE: DoD365 OneDrive will not synchronize specific file extensions in the cloud. These include, but are not limited to, EXE, COM, ISO, and PST. ***
7.1 Initial Setup

7.1.1 Click the Windows start button and scroll to the OneDrive app.
7.1.3 Click the **Sign in with CAC/PIV** and use your authentication certificate.
7.1.5 Click the **Next** button to accept the default folder.

Your IT department wants you to back up your important folders

Selected folders will sync in OneDrive. New and existing files will be added to OneDrive, backed up, and available on your other devices even if you lose this PC. [Learn more.]

![OneDrive location](image)

Space left in OneDrive after selection: 1,022 GB

This is the new OneDrive location. Use this location to back up and sync saved files.

![OneDrive tree view](image)
7.2 Sync Errors

7.2.1 DoD365 OneDrive and SharePoint will not synchronize specific file extensions in the cloud. These include, but are not limited to, EXE, COM, ISO, and PST. A sync issue similar to the image below requires moving the file out of the OneDrive folder system (example above) and under the computer folder system also shown above.
7.2.5 If you click on the **Open in Office to merge changes**, the office application will open and allow for a change. The **Keep both files** option will result in the second image.
7.2.6 Below are the various types of sync status icon displayed along with their description.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🟡</td>
<td>A red circle with a white cross means that a file or folder cannot be synced. You'll see this in File Explorer or on the OneDrive notification area icons. Click the blue or white OneDrive icon in the notification area to learn more about the problem.</td>
</tr>
<tr>
<td>🔴</td>
<td>A grayed-out OneDrive icon in the taskbar means you're not signed in, or OneDrive setup hasn't completed.</td>
</tr>
<tr>
<td>⏸️</td>
<td>The paused symbol over the OneDrive icon means your files are not currently syncing. To resume syncing, click the OneDrive icon in the notification area. Directions to allow resume syncing display.</td>
</tr>
<tr>
<td>🔥</td>
<td>The circular arrows over the OneDrive icon signifies that sync is in progress. This includes when you are uploading files, or OneDrive is syncing new files from the cloud to your PC.</td>
</tr>
<tr>
<td>⌚️</td>
<td>OneDrive will also check for other file or folder changes and may show &quot;Processing changes&quot;. If OneDrive shows &quot;Processing changes&quot; for a long time, it could be because you have an online file open, a very large file syncing, a lot of files stuck in a queue.</td>
</tr>
<tr>
<td>👇️</td>
<td>If you see a yellow warning triangle over your OneDrive icon, it means your account needs attention. Select the icon to see the warning message displayed in the activity center.</td>
</tr>
<tr>
<td>🌤️</td>
<td>A blue cloud icon next to your OneDrive files or folders indicates that the file is only available online. Online-only files don't take up space on your computer.</td>
</tr>
<tr>
<td>🔄️</td>
<td>When you open an online-only file, it downloads to your device and becomes a <em>locally available</em> file. You can open a locally available file anytime, even without Internet access. If you need more space, you can change the file back to online only. Just right-click the file and select &quot;Free up space.&quot;</td>
</tr>
<tr>
<td>🟢</td>
<td>Files that you mark as &quot;Always keep on this device&quot; have the green circle with the white check mark. These always available files download to your device and take up space, but they're always there for you even when you're offline.</td>
</tr>
</tbody>
</table>

8. Terminal Server

8.1 Initial Setup

8.1.1 The Terminal Server desktop is pre-populated.

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

8.1.3 Double-click on the desktop shortcut similar to the below
8.1.4 If this is the initial logon, click the **Add Server** button.

8.1.6 In the licensing window, click the **Accept** button.

8.1.7 Select the Authentication certificate.

8.1.8 Enter your PIN.

8.1.9 Click the PLUM RDS General Terminal Server icon.
8.1.10 To change to a single monitor, click the 3-dot ellipse on the PLUM RDS icon, then click **Display** and select **Fullscreen – Single Monitor**.

8.1.12 Sign in as you would on your physical machine.

8.1.13 When you are finished, sign out vs closing the Horizon view client.
8.1.14 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.

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

9. Large File Transfers

9.1 DoD SAFE

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

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

9.1.3 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.

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

9.1.5 Seven days after upload, DoD SAFE deletes the files.
10. Home Network Troubleshooting

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

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

10.1.2 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.

10.1.3 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.

10.1.4 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.

10.2 Rebooting a privately owned modem

10.2.1 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.

10.2.2 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.

10.2.3 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=QrmchiDblVg).

10.2.4 As of 2016, the current industry standard is DOCSIS 3.1. This iteration brought the cap to one Gbps for download speed. (https://www.youtube.com/watch?v=cCmlwWMn-os).

10.3 Rebooting a privately owned router

10.3.1 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.
10.4 Resetting your router

10.4.1 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

10.4.2 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.

10.4.3 Below is a link on generically resetting a router, (https://www.youtube.com/watch?v=BAdikT_JmP4).

10.5 Updating your router’s firmware

10.5.1 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.***

10.6 Prioritizing data in your router settings

10.6.1 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.

11. 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.

11.1 Rebooting a leased ISP gateway device

11.1.1 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.
11.1.2 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.

12. 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.

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

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

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

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

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

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

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

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

12.9 AT&T:

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