# TABLE OF CONTENTS

Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>4</td>
</tr>
<tr>
<td>Section 1: Virtual Desktop Overview</td>
<td>5</td>
</tr>
<tr>
<td>1.1 Virtual Desktop Background</td>
<td>5</td>
</tr>
<tr>
<td>Section 2: Device Type - Thin Client</td>
<td>5</td>
</tr>
<tr>
<td>2.1 Purpose</td>
<td>5</td>
</tr>
<tr>
<td>2.2 Thin Client Usage Overview</td>
<td>5</td>
</tr>
<tr>
<td>2.3 Thin Client Hardware Overview</td>
<td>5</td>
</tr>
<tr>
<td>2.4 Thin Client Software Overview</td>
<td>7</td>
</tr>
<tr>
<td>2.5 Thin Client Login Instructions</td>
<td>7</td>
</tr>
<tr>
<td>2.6 Thin Client Sign Out Instructions</td>
<td>18</td>
</tr>
<tr>
<td>Section 3: Device Type – Zero Client</td>
<td>20</td>
</tr>
<tr>
<td>3.1 Purpose</td>
<td>20</td>
</tr>
<tr>
<td>3.2 Zero Client Usage Overview</td>
<td>20</td>
</tr>
<tr>
<td>3.3 Zero Client Hardware Overview</td>
<td>20</td>
</tr>
<tr>
<td>3.4 Zero Client Software Overview</td>
<td>21</td>
</tr>
<tr>
<td>3.5 Zero Client Login Instructions</td>
<td>21</td>
</tr>
<tr>
<td>3.6 Zero Client Sign Out Instructions</td>
<td>26</td>
</tr>
<tr>
<td>Section 4: Device Type – Traditional Laptop/Desktop, Government Furnished Equipment (GFE)</td>
<td>27</td>
</tr>
<tr>
<td>4.1 Purpose</td>
<td>27</td>
</tr>
<tr>
<td>4.2 Traditional Laptop/Desktop Usage Overview</td>
<td>27</td>
</tr>
<tr>
<td>4.3 Traditional Laptop/Desktop Hardware Overview</td>
<td>27</td>
</tr>
<tr>
<td>4.4 Traditional Laptop/Desktop Software Overview</td>
<td>28</td>
</tr>
<tr>
<td>4.5 Traditional Laptop/Desktop Login Instructions</td>
<td>28</td>
</tr>
<tr>
<td>4.6 Laptop/Desktop (GFE) Sign Out Instructions</td>
<td>32</td>
</tr>
<tr>
<td>Section 5: Device Type – Laptop/Desktop Contractor Furnished Equipment (CFE)/Personal Equipment (PE)</td>
<td>33</td>
</tr>
<tr>
<td>5.1 Purpose</td>
<td>33</td>
</tr>
<tr>
<td>5.2 Laptop/Desktop (CFE/PE) Usage Overview</td>
<td>33</td>
</tr>
<tr>
<td>5.3 Laptop/Desktop (CFE/PE) User Hardware Overview</td>
<td>34</td>
</tr>
<tr>
<td>5.4 Laptop/Desktop (CFE/PE) User Software Recommendations</td>
<td>34</td>
</tr>
<tr>
<td>5.5 Laptop/Desktop (CFE/PE) Login Instructions</td>
<td>40</td>
</tr>
<tr>
<td>5.6 Laptop/Desktop (CFE/PE) Sign Out Instructions</td>
<td>44</td>
</tr>
<tr>
<td>Section 6: Device Type – User Managed Computer (UMC)</td>
<td>45</td>
</tr>
<tr>
<td>6.1 Purpose</td>
<td>45</td>
</tr>
<tr>
<td>6.2 User Managed Computer (UMC) Usage Overview</td>
<td>45</td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
</tr>
<tr>
<td>---------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>6.3</td>
<td>User Managed Computer (UMC) User Hardware Overview</td>
</tr>
<tr>
<td>6.4</td>
<td>User Managed Computer (UMC) Software Overview</td>
</tr>
<tr>
<td>6.5</td>
<td>User Managed Computer (UMC) Network Connect Instructions</td>
</tr>
<tr>
<td>6.6</td>
<td>User Managed Computer (UMC) Login Instructions</td>
</tr>
<tr>
<td>6.7</td>
<td>User Managed Computer (UMC) Sign Out Instructions</td>
</tr>
<tr>
<td>6.8</td>
<td>Updating User Managed Computer (UMC)</td>
</tr>
<tr>
<td>7.0</td>
<td>Appendix</td>
</tr>
<tr>
<td>7.1</td>
<td>Support</td>
</tr>
</tbody>
</table>
INTRODUCTION

This user guide provides all DLA Virtual Desktop users with Virtual Desktop background information, instructions for accessing the Virtual Desktop, and information for the specific devices used to access the Virtual Desktop. Readers of this user guide should have a basic knowledge of operating a personal computer and have all required certificates (i.e. CAC credentials and PIN) to access DLA’s secured network.

The Virtual Desktop can be accessed from any computing device with an internet connection. Accessing the Virtual Desktop allows you to view your workstation desktop virtually via a terminal machine rather than a local device (i.e. traditional desktop/laptop). This user guide will outline the procedures for accessing the Virtual Desktop from the following devices:

- Thin Client/UMC
- Zero Client
- Traditional Laptop/Desktop (Government Furnished Equipment)
- Contractor Furnished Equipment (CFE) / Personal Equipment (PE)

DLA Administrators will identify the device type you will use (i.e. one of the four machines listed above). If you work in an environment where you require access to multiple machines during the course of the work day, active sessions within the Virtual Desktop can be transferred between the above devices. For example, a user can log into the Virtual Desktop on one device, disconnect, and log in with a different device, and see the same active applications left running on the previous device.

DEVICE USAGE POLICY:

Please note the following usage policies for the endpoints that will access the Virtual Desktop:

<table>
<thead>
<tr>
<th>Device</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP MT42 Mobile Thin Client</td>
<td>Approved for DLA office usage with wired/Wi-Fi connection, approved for telework usage</td>
</tr>
<tr>
<td>HP MT42 UMC</td>
<td>Approved for DLA office usage with Wi-Fi connection, approved for telework usage</td>
</tr>
<tr>
<td>Dell Wyse 5010 Zero Client</td>
<td>Approved for DLA office usage with wired connection, not approved for telework usage</td>
</tr>
<tr>
<td>Dell Wyse 3040 Zero Client</td>
<td>Approved for DLA office usage with wired connection, not approved for telework usage</td>
</tr>
<tr>
<td>Traditional Laptop</td>
<td>Approved for DLA office usage with wired/Wi-Fi connection, approved for telework usage</td>
</tr>
<tr>
<td>Traditional Desktop</td>
<td>Approved for DLA office usage with wired connection, not approved for telework usage</td>
</tr>
<tr>
<td>Contractor Equipment</td>
<td>Approved for DLA office usage with Wi-Fi Connection, approved for telework usage</td>
</tr>
<tr>
<td>Personal Equipment</td>
<td>Not approved for DLA office usage, approved for telework usage</td>
</tr>
</tbody>
</table>
SECTION 1: VIRTUAL DESKTOP OVERVIEW

1.1 Virtual Desktop Background

Virtual Desktop is a capability that moves computer processing and storage away from local devices (laptop/desktops) and into the data center. The benefits of implementing Virtual Desktops in DLA include improved end user mobility (i.e. access to desktop anytime from anywhere), operational efficiencies (i.e. reduced capital and operational costs), and improved security (i.e. no data stored on lost devices). The below diagram shows the infrastructure of a Virtual Desktop:

SECTION 2: DEVICE TYPE - THIN CLIENT

2.1 Purpose

Provide an overview of the hardware, software, and steps to access the Virtual Desktop from a thin client.

2.2 Thin Client Usage Overview

The following is the type of Thin Client device used to access the Virtual Desktop:

- HP MT42 Mobile Thin Client Laptop used in the office with wired DLA network and Wi-Fi connection. The Mobile Thin Client is approved for telework.

2.3 Thin Client Hardware Overview

The thin client takes a user’s login request and connects to the desktop virtually. It is a streamlined machine with limited storage and a configurable operation system. The HP MT42 Thin Client uses wired and Wi-Fi connections. The following sections will outline all accessories and additional hardware required to use a thin client and the steps required to access the Virtual Desktop:

As of September 2016, DLA is using the HP MT42 Mobile Thin Client.
I. At a Glance

II. Accessories

The following accessories are included with the HP MT42 Mobile Thin Client:

<table>
<thead>
<tr>
<th>IMAGE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Power Cord</td>
</tr>
<tr>
<td></td>
<td>Docking Station</td>
</tr>
</tbody>
</table>

HP Ultra-Light Docking Station

I. At a Glance
II. Accessories

The following accessories are included with the HP Ultra-light Docking Station:

<table>
<thead>
<tr>
<th>IMAGE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Power Cord" /></td>
<td>Power Cord</td>
</tr>
</tbody>
</table>

2.4 Thin Client Software Overview

Thin Client and Virtual Desktop software is pre-installed on your machine and is ready to use.

2.5 Thin Client Login Instructions

The following steps outline the Virtual Desktop login process using the HP MT42 Mobile Thin Client and HP t620 Flexible Thin Client. There are different instructions for accessing the Virtual Desktop depending on how you are connecting, via DLA network (internal) or wireless network (external).

**NOTE:** If you’ve received a new CAC after July 31st, 2020, or you’ve been informed your DLA account has transitioned to PIV-Auth use the 16-digit PIV-Auth certificate when logging in, otherwise continue using the 10-digit DoD EMAIL certificate.
1. Press **Ctrl+Alt+Delete**.

2. Select **OK**.
3. Insert CAC into the Smart Card Reader, click **Sign-in options**, then the **Smart Card Login**. 
   **Note:** Select **More Choices** if the DOD EMAIL cert is not currently selected. Confirm that you’re selecting the correct Smart Card sign in option i.e. EDIPI(10 characters)@.mil.

4. Enter PIN.

5. Select **VDI Launcher Internal** option.
6. Choose the DOD EMAIL certificate and Select OK.
   **Note:** Select **More Choices** if the DOD EMAIL cert is not currently selected and confirm that you’re selecting the correct Smart Card sign in option i.e. EDIPI(10 characters)@.mil.

7. Enter PIN.

8. Select **DLA Standard Desktop 2016**. Screen displays the Citrix Receiver Desktop Options.
   
   *If you have been converted to using the Azure Desktop you will see an icon that says either “AZE DLA Desktop” or “AZC DLA Desktop” depending on your geographical location.*
9. Select **OK**.

10. Select **Sign-in options**, then select the **Smart Card Login** as the CAC is being read.
    
    **Note:** Select **More Choices** if the DOD EMAIL cert is not currently selected and confirm that you’re selecting the correct Smart Card sign in option i.e. EDIPI(10 characters)@.mil.
11. Enter **PIN**.

12. The Virtual Desktop is ready to use, just as you would use a traditional desktop.
**Wireless Network (External)**

1. Press **Ctrl+Alt+Delete**.

2. Select **OK**.
3. Insert your CAC into the Smart Card Reader, click Sign-in options, then the Smart Card Login. 
   Note: Confirm that you’re selecting the correct Smart Card sign in option i.e. EDIP(10 characters)@.mil.

4. Enter PIN.

5. Select the Network Options icon in the lower right-hand corner of the screen.
6. Select **Wireless Network** and choose **Connect**. Your list will vary depending on wireless options available to you.

7. Enter **Wireless Network Password** and choose **Next**.

8. Select the appropriate option depending on whether the connection type is a home/work or public network.
9. Select VDI Launcher Internal.

10. Choose the DOD EMAIL certificate and Select OK. Note: Select More Choices if the DOD EMAIL cert is not currently selected and confirm that you’re selecting the correct Smart Card sign in option i.e. EDIPI(10 characters)@.mil.

11. Enter PIN.


*If you have been converted to using the Azure Desktop you will see an icon that says either “AZE DLA Desktop” or “AZC DLA Desktop” depending on your geographical location.
13. Select **Sign-in options**, then select the **Smart Card Login** as the CAC is being read. Choose the DOD EMAIL certificate and Select **OK**.
   **Note:** Select **More Choices** if the DOD EMAIL cert is not currently selected and confirm that you’re selecting the correct Smart Card sign in option i.e. EDIPI(10 characters)@.mil.

14. Enter **PIN**.
15. The Virtual Desktop is ready to use, just as you would use a traditional desktop.

2.6 Thin Client Sign Out Instructions

**SIGN OUT FROM THE VIRTUAL DESKTOP**

To sign out or terminate the active Virtual Desktop session and shut down the Thin Client follow the below steps. Terminating your Virtual Desktop session will not allow you to transfer your session to another device.

1. Select the Windows button in the lower left-hand corner of the screen (within Virtual Desktop session).
2. Select the **Sign Out** button (within the Virtual Desktop session).

3. Select **Start Menu** and then select the **Shut Down** button (on local machine).

**DISCONNECTING VDI SESSION**

Note: User is leaving for lunch, meeting, break, etc. but intends to come back and continue work) Complete one of the following steps prior to removing CAC:

1. Select Keystrokes `<CTRL>+<ALT>+<DEL> → Select Lock → Pull CAC.

2. From the XenDesktop toolbar at the top of the VDI session, Select Ctrl+Alt+Del → Select Lock this computer → Pull CAC.

3. Select Keystrokes `<Windows> + `<L> → Pull CAC.
SECTION 3: DEVICE TYPE — ZERO CLIENT

3.1 Purpose

Provide an overview of the hardware, software, and steps to access the Virtual Desktop from a repurposed laptop/desktop.

3.2 Zero Client Usage Overview

The following is the type of Zero Client devices are used to access the Virtual Desktop:

- Dell Wyse 3040 and 5010 Zero Clients are used in the office with wired DLA network. The Zero Client is not approved for telework.

3.3 Zero Client Hardware Overview

The Zero Client takes a user’s login request and connects to the desktop virtually. It is a streamlined machine without an operating system. The Dell Wyse 5010 Zero Client uses a wired connection. The following sections outline all accessories and additional hardware required to use a Zero Client and the steps required to access the Virtual Desktop:

As of September 2019, DLA is using the Dell Wyse 3040 and 5010 Zero Clients.

DELL WYSE 3040 ZERO CLIENT

1. At a Glance
DELL WYSE 5010 ZERO CLIENT

I. At a Glance

II. Accessories

The following accessories are included with the Dell WYSE 3040 & 5010 Zero Clients:

<table>
<thead>
<tr>
<th>IMAGE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Power Cord Image]</td>
<td>Power Cord</td>
</tr>
</tbody>
</table>

3.4 Zero Client Software Overview

Virtual Desktop software is pre-installed on your machine and is ready to use.

3.5 Zero Client Login Instructions

**NOTE**: If you’ve received a new CAC after July 31st 2020, or you’ve been informed your DLA account has transitioned to PIV-Auth use the 16-digit PIV-Auth certificate when logging in, otherwise continue using the 10-digit DoD EMAIL certificate.
1. Insert Smart Card into Smart Card Reader.

2. If you have a PIV certificate on your CAC you may be presented with the below window. Confirm that you’re selecting the correct Smart Card sign in option i.e. EDIPI(10 characters)@.mil.
3. Enter PIN.

4. Select the appropriate Virtual Desktop option. **Note:** Desktop options shown will defer user to user.

*If you have been converted to using the Azure Desktop you will see an icon that says either “AZE DLA Desktop” or “AZC DLA Desktop” depending on your geographical location.*
5. Select OK.

6. When you see this screen click Sign-in options.
7. Select your proper certificate.

8. Enter your **PIN**, (you may have to scroll down).
9. The Virtual Desktop is ready to use, just as you would use a traditional desktop.

3.6 Zero Client Sign Out Instructions

SIGN OUT FROM THE VIRTUAL DESKTOP

To sign out or terminate the active Virtual Desktop session and shut down the Thin Client follow the below steps. Terminating your Virtual Desktop session will not allow you to transfer your session to another device.

1. Select the Windows button in the lower left-hand corner of the screen (within Virtual Desktop session).
2. Select the **Sign Out** button (within Virtual Desktop session).

![Virtual Desktop Interface](image)

**DISCONNECTING VDI SESSION**

Note: User is leaving for lunch, meeting, break, etc. but intends to come back and continue work) Complete one of the following steps prior to removing CAC:

1. Select Keystrokes `<CTRL>+<ALT>+<DEL>` → Select **Lock** → Pull CAC.
2. Right click on `<Windows>`, Select **Ctrl+Alt+Del** → Select **Lock this computer** → Pull CAC.
3. Select Keystrokes `<Windows>+<L>` → Pull CAC.

**SECTION 4: DEVICE TYPE – TRADITIONAL LAPTOP/DESKTOP, GOVERNMENT FURNISHED EQUIPMENT (GFE)**

**4.1 Purpose**

Provide an overview of the hardware, software, and steps to access the Virtual Desktop from a traditional laptop/desktop (GFE).

**4.2 Traditional Laptop/Desktop Usage Overview**

The following are two types of traditional machines used to access the Virtual Desktop:

- **Traditional Laptop** supplied by DLA can be used in the office with wired DLA network and Wi-Fi connection. The traditional laptop is approved for telework.

- **Traditional Desktop** supplied by DLA can only be used in the office with wired DLA network connection. The traditional desktop is not approved for telework. You may continue to use your traditional laptop provided by DLA (if applicable) or use your personal computers at home to telework (see Section 6).

**4.3 Traditional Laptop/Desktop Hardware Overview**

If you are using a traditional DLA issued laptop/desktop you will be provided with the necessary attachments and
accessories to use the Virtual Desktop.

4.4 Traditional Laptop/Desktop Software Overview

Virtual Desktop software is pre-installed on your machine and is ready to use.

4.5 Traditional Laptop/Desktop Login Instructions

**NOTE**: If you’ve received a new CAC after July 31st 2020, or you’ve been informed your DLA account has transitioned to PIV-Auth use the 16-digit PIV-Auth certificate when logging in, otherwise continue using the 10-digit DoD EMAIL certificate.

The following steps outline the Virtual Desktop login process using a traditional laptop/desktop:

1. Ensure CAC is inserted into CAC Reader.
2. Open Internet Explorer and select **Email Certificate**.  
   **Note**: Select **More Choices** if the DOD EMAIL cert is not currently selected. Confirm that you’re selecting the correct Smart Card sign in option i.e. EDIPI(10 characters)@.mil.
3. Click **OK**.
4. Enter the following URL: **https://internal.dir.ad.dla.mil**.
5. Choose the **DOD EMAIL** certificate and Select **OK**.
   
   *Note: Select **More Choices** if the DOD EMAIL cert is not currently selected. Confirm that you’re selecting the correct Smart Card sign in option i.e. **EDIP(10 characters)@.mil**.*

6. **Click OK.**

7. **Select the **DLA Standard Desktop**, if needed.** The DLA Standard Desktop may open automatically.

   *If you have been converted to using the Azure Desktop you will see an icon that says either “**AZE DLA Desktop**” or “**AZC DLA Desktop**” depending on your geographical location.*
8. If you are assigned multiple desktops and are unsure which one to choose, click the down arrow under the description to see the full name.

9. Click OK.

10. Select the **Smart Cart Login** as the CAC is being read. Do not navigate away from this window until the login
process is complete. Doing so may result in your session timing out.

11. Enter **PIN**.

12. The Virtual Desktop is ready to use, just as you would use a traditional desktop.
13. To switch between local machine and Virtual Desktop, expand the XenDesktop Toolbar drop-down at the top of the page and choose **Home**.

4.6 Laptop/Desktop (GFE) Sign Out Instructions

Sign out of the Virtual Desktop using the steps below:

**SIGN OUT OF VIRTUAL DESKTOP**

These steps will terminate the active Virtual Desktop session and you will not be able to transfer your session to another device.

1. Select the Windows button in the lower left-hand corner of the screen.
2. Select the **Sign Out** button (within Virtual Desktop session).

---

**DISCONNECTING VDI SESSION**

Note: User is leaving for lunch, meeting, break, etc. but intends to come back and continue work) Complete one of the following steps prior to removing CAC:

1. Select Keystrokes `<CTRL>+<ALT>+<DEL>` ➔ Select **Lock** ➔ Pull CAC.

2. From the XenDesktop toolbar at the top of the VDI session, Select **Ctrl+Alt+Del** ➔ Select **Lock this computer** ➔ Pull CAC.

3. Select Keystrokes `<Windows> + <L>` ➔ Pull CAC.

---

**SECTION 5: DEVICE TYPE – LAPTOP/DESKTOP CONTRACTOR FURNISHED EQUIPMENT (CFE)/PERSONAL EQUIPMENT (PE)**

5.1 Purpose

Provide an overview of the hardware, software, and steps to access the Virtual Desktop from a laptop/desktop (CFE/PE).

5.2 Laptop/Desktop (CFE/PE) Usage Overview

The following outlines the usage overview for CFE/PE when accessing the Virtual Desktop:

- CFE/PE can be used on non-Government network connections, i.e. home network, coffee shop network, contractor office network, etc. CFEs are approved for telework usage.
- Personal Equipment is not approved for use on the DLA network, but is approved for telework.
5.3 Laptop/Desktop (CFE/PE) User Hardware Overview

There are many types of CFEs and personal machines you can use to access the Virtual Desktop. The list below is the necessary hardware required to access the Virtual Desktop from either a CFE or personal machine:

- Desktop Computer or Laptop
- CAC Reader
- Ethernet port (with active internet connection) or Wi-Fi

5.4 Laptop/Desktop (CFE/PE) User Software Recommendations

Risks

There are potential risks associated with installing the necessary software (i.e., ActivClient, Citrix Receiver, DOD Root Certificates) in order to use the remote access system. It is not possible to test these components with all software and/or applications commercially available and may be on your home computer. Therefore, the software could conflict with other applications or software residing on your home computer. If you are using the remote access system on your personal non-Government-furnished computer it is at your own risk.

Disclaimer of Liability

With respect to installing prerequisite software components or using the remote access solution, neither the DOD, DLA, nor any employees within, provide any warranty, expressed or implied.

Or assume any legal or financial liability or responsibility for your non-Government computer system and/or damages or repairs that may result from system incompatibilities with the remote access solution. By installing prerequisite software and using this product, you signify your agreement to the preceding terms and conditions. If you do not agree to these terms and conditions, do not install or use this product.

Service Desk Support

All liability for issues and troubleshooting non-GFE is the responsibility of the equipment owner. The DLA Enterprise Service Desk will not provide support for issues with hardware/software not provided by DLA, including but not limited to non-GFE hardware, non-DLA networks (e.g., home routers, public hot spots), and non-DLA software compatibility issues with Citrix.

DLA Enterprise Service Desk resources will support troubleshooting issues that are not related to the non-GFE hardware/software, including but not limited to accounts, DLA applications, and server-side issues.

Personal machines or CFEs running Windows 10 can be used to access the Virtual Desktop. Use the tables below to identify the recommended browser you should use based on the operating system currently installed on your machine.

For best performance use following operating system/browser combinations, otherwise you may experience performance issues or inability to connect to the Virtual Desktop.

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Browser Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 10 32/64-bit Editions</td>
<td>Google Chrome 91.x</td>
</tr>
<tr>
<td>Windows 10 32/64-bit Editions</td>
<td>Internet Explorer 11.x</td>
</tr>
<tr>
<td>Windows 10 32/64-bit Editions</td>
<td>Microsoft Edge Chromium 90.x</td>
</tr>
<tr>
<td>Windows 10 32/64-bit Editions</td>
<td>Mozilla Firefox 78.x</td>
</tr>
</tbody>
</table>
Before connecting to the Virtual Desktop for the first time, Citrix client software will need to be installed. This is available on the DLA Enterprise Remote Access login page: https://www.dla.mil/RemoteVDI.

Follow these steps for downloading the appropriate software in Internet Explorer. Your will need to use the proper web browser based on the operating system installed on the machine (i.e. outlined in above table). Following these steps will result in a necessary machine reboot once completed.

1. Connect your Common Access Card (CAC) Reader to an available USB Port on your CFE/Personal Computer System (Desktop/Laptop).
2. Turn on your CFE/PE (Desktop/Laptop).
3. Launch your internet browser.
4. Validate that the required security protocols are enabled - From Internet Explorer, select Tools and then Internet Options.

5. When the Internet Options window appears select the Advanced tab and ensure Use TLS 1.2 is checked in the Security section. Select OK, then close the internet browser, and open a new internet browser window.
6. Insert CAC into CAC Reader.

7. In the internet browser of your choice (Google Chrome is recommended), navigate to DLA Enterprise Remote Access [https://www.dla.mil/RemoteVDI](https://www.dla.mil/RemoteVDI) to access the files to download you will need to use remote access. On the screen below you will see two links for software that needs to be installed prior to connecting to the Virtual Desktop from each machine for the first time.

![DLA Remote Access System](image)

**DLA Remote Access System**

**Log into VDI**

**Conus VDI External**

**Conus VDI Internal**

**Europe / Africa**

**Hawaii**

**Japan**

**First time on this machine?**

If this is your first time accessing this system from this machine, you may need to install the following to log in:

- [Citrix Workspace App for Windows](https://www.dla.mil/RemoteVDI)
- Instructions for How to Install or Upgrade the Citrix Workspace App

A Common Access Card reader will be provided by your local IT support staff. Contact the Enterprise Service Desk at 1-800-303-0001 to request one.

**VDI not working?**

Try the following first:

- Close all browser windows and try again.
- If you've received a new CAC after July 31, 2020, or you've been informed your DLA account has transitioned to PKM-Audit, use the 10-digit PKM-Audit certificate when logging in. Allow certificate enrollment.

**Zoom Meetings in VDI**

If you are attempting to use Zoom on your thin client or UM2, you should be using the Zoom VDI Plugin for Citrix Receiver for best results. If you are experiencing problems accessing your camera in a Zoom meeting, you may be missing the Zoom VDI Plugin for Citrix Receiver.

- Install the Zoom VDI Plugin.
Note: DoD Root Certificates are no longer needed for accessing DLA VDI desktops.

8. **Optional** Download ActivIdentity ActivClient – request the latest version of ActivClient the DLA Enterprise Service Desk (ESD). ActivClient is recommended for Windows 7 and not recommended for the following:
   - Windows 8 / 8.1
   - Windows 10

   Based on the configuration of your operating system will need to determine which ActivClient to install 32 bit or 64 bit.

   To verify the version of your operating system, right-click the My Computer icon on your Desktop and selecting **Properties**.

   ![My Computer Icon on Desktop]

   You will see on the next screen you will see 32-bit or 64-bit Operating System. Be sure to provide this information with your request for the ActivClient Software.

   ![Operating System Dialog]

9. **Update Trusted Sites**
   - Open Internet Explorer.
   - Select Tools and then Internet Options.
10. Select the **Security** tab.

11. Select the **Trusted Sites** and select **Sites**.

12. Enter `https://*.dla.mil` (**“*”** a starisk; followed by a `. Period; then “dla.mil”) Select **Add** and **Close**.
13. Select **Apply** and **OK**.

14. **Update Compatibility View Settings**
   - Open Internet Explorer.
   - Select **Tools and then Compatibility View Settings**.
   - OR

15. Enter **dla.mil**, Select **Add**, and then **Close**.
16. Reboot the computer. All required software is now available on the machine, and you are ready to login to your Virtual Desktop. (See section 5.5 for login instructions.)

5.5 Laptop/Desktop (CFE/PE) Login Instructions

The following steps outline the Virtual Desktop login process using a CFE/Personal Machine:

**NOTE**: If you've received a new CAC after July 31st 2020, or you’ve been informed your DLA account has transitioned to PIV-Auth use the 16-digit PIV-Auth certificate when logging in, otherwise continue using the 10-digit DoD EMAIL certificate.

**Note**: The following steps outline the process of logging in using Internet Explorer. User will need to use the proper web browser based on the operating system installed on the machine.

1. Insert CAC into CAC Reader.
2. Open Internet Explorer.
3. Enter the following URL: https://www.dla.mil/RemoteVDI (continue to step 4) or https://dladirect.dla.mil (continue to step 5).
4. Select the **VDI - External** button.
5. Choose the **DOD EMAIL** certificate and Select **OK**. **Note:** Select **More Choices** if the DOD EMAIL cert is not currently selected. Confirm that you’re selecting the correct Smart Card sign in option i.e. EDIPI(10 characters)@.mil.

![Certificate Selection](image)

6. Enter **PIN**.
7. Choose **DLA Standard Desktop**. DLA Standard Desktop may open automatically. *If you have been converted to using the Azure Desktop you will see an icon that says either “AZE DLA Desktop” or “AZC DLA Desktop” depending on your geographical location.*

![DLA Standard Desktop 2016](image)

8. Select **OK**.

![DoD Notice and Consent Banner](image)

9. Select **Sign-in options**, then **Smart Cart Login** option while the CAC is being read and stay on this window until the login process is complete. Navigating away from this before the login process is complete may result in you session being timed out. If this happens you will need to login again.
10. Enter **PIN**.

11. The Virtual Desktop is ready to use, just as you would use a traditional desktop.

To switch between local machine and Virtual Desktop, expand the XenDesktop Toolbar drop-down at the top of the screen.
page and choose **Home**.

![Virtual Desktop Interface](image1.png)

### 5.6 Laptop/Desktop (CFE/PE) Sign Out Instructions

There are two ways to sign out of the Virtual Desktop.

**SIGN OUT OF THE VIRTUAL DESKTOP**

1. This sign out method will terminate your active Virtual Desktop session and you will not be able to transfer your session to another machine. Select the **Windows** button in the lower left-hand corner of your screen.

![Virtual Desktop Interface](image2.png)

2. Select the **Sign Out** button.

![Virtual Desktop Interface](image3.png)
DISCONNECTING VDI SESSION

Note: User is leaving for lunch, meeting, break, etc. but intends to come back and continue work) Complete one of the following steps prior to removing CAC:

1. Select Key strokes `<CTRL>+<ALT>+<DELETE>` → Select Lock → Pull CAC.
2. From the XenDesktop toolbar at the top of the VDI session, Select `Ctrl+Alt+Del` → Select Lock this computer → Pull CAC.
3. Select Lock this computer → Pull CAC
4. Select Key strokes `<Windows> + <L>` → Pull CAC.

SECTION 6: DEVICE TYPE – USER MANAGED COMPUTER (UMC)

6.1 Purpose

Provide an overview of the hardware, software, and steps to access the Virtual Desktop from your UMC.

6.2 User Managed Computer (UMC) Usage Overview

The following outlines the usage overview for UMCs when accessing the Virtual Desktop:

- UMCs can be used on non-Government network connections, i.e. home network, UMC office network, etc.
- UMCs are approved for telework usage.

6.3 User Managed Computer (UMC) User Hardware Overview

The UMC is provided by DLA for DLA employees and will have a CAC reader installed with all appropriate network hardware as well.

6.4 User Managed Computer (UMC) Software Overview

Virtual Desktop software is pre-installed on your machine and is ready to use. To update to the latest client please visit https://www.dla.mil/RemoteVDI and click on Citrix Workspace App for Windows.

6.5 User Managed Computer (UMC) Network Connect Instructions

The following steps outline connecting to the user managed computer (UMC) network:

What is it - DLA_UMC is different from the existing production DLA Wireless network. DLA_UMC is restricted to only allow traffic to the VDI servers. Connectivity is still accomplished using the same wireless access points already in place. If you are in a location that has DLA Wireless it also has access to the DLA_UMC wireless network.
**How to Connect**

1. Click on the wireless network icon in the bottom right.

![Wireless Network Icon](image1)

2. Select “DLA_UMC” from the list of available wireless networks.

![Wireless Network Selection](image2)

3. Enter the "security key" when prompted: **UMC4DLA!**

4. After entering the security key your wireless icon will display an exclamation point. This is normal and you can continue to the VDI login page.

![Exclamation Point](image3)

**6.6 User Managed Computer (UMC) Login Instructions**

The following steps outline the Virtual Desktop login process using a user managed computer (UMC):

1. Power on Computer (no CAC is needed to login to the computer itself).

2. Insert CAC.

3. Click on Icon for VDI Login.

4. You will be prompted for your Certificate. Please choose the DOD Email certificate, and if prompted type in your PIN. Select **Sign-in options**, then select the **Smart Card Login** as the CAC is being read.
NOTE: If you’ve received a new CAC after July 31st 2020, or you’ve been informed your DLA account has transitioned to PIV-Auth use the 16-digit PIV-Auth certificate when logging in, otherwise continue using the 10-digit DoD EMAIL certificate.

If prompted to Detect, please follow steps below. If not, please continue with step 5.

a. Click **Detect Receiver**.

![Detect Receiver](image)

b. Click **Already Installed**.

![Already Installed](image)

5. Click **Accept** on the Consent Prompt.
6. Select your **Standard Desktop**.

**If you have been converted to using the Azure Desktop you will see an icon that says either “AZE DLA Desktop” or “AZC DLA Desktop” depending on your geographical location.**

a. If using Internet Explorer, click on your Desktop icon and VDI will launch.

b. If using Google Chrome or Microsoft Edge:
   
i. Click on your Desktop icon (This will create ICA file in the bottom left of the browser) or
   
ii. Click on the ICA file in the bottom left. This will launch your VDI session.

iii. Continue to log into VDI with your Certificate and your Desktop will Load.
6.7 User Managed Computer (UMC) Sign Out Instructions

These steps will terminate the active Virtual Desktop session and you will not be able to transfer your session to another device.

1. Close all open applications.
2. Click on the Windows icon in the lower left corner.
3. Select the Smiley face icon.
4. Select Sign out.

6.8 Updating User Managed Computer (UMC)

Follow these steps for updating your system at home on your home network.

*Note* - The UMC wireless network in the building will not allow for updates to take place.

1. Open Settings. There are multiple ways to open this.
   a. Type “Settings” into “Type here to search” on the Task Bar.
b. Right Click on Start Menu and from the list choose **Settings**.

c. Left click start menu and look for **Settings** under “S” in the list.

2. Once **Settings** is open, locate and click on **Update and Security**.

3. You will be now looking at Windows Update. Click on the button **Check for Updates**.

4. This will actively look for Windows current updates your computer needs and will start to install them. Some installs will need to have a system restart after, and it may need to check for updates again for confirmation that
all current updates are installed.

SECTION 7.0 APPENDIX

7.1 Support

DLA Enterprise Service Desk Support is available to provide any additional information concerning the Virtual Desktop implementation.

You may put in a service request through SPOE:

Phone: (855) 352-0001