Defense Logistics Agency

Virtual Desktop: User Guide

February 2024

TABLE OF CONTENTS

Table of Contents 2
Section 1: Virtual Desktop Overview 5
1.1 Virtual Desktop Background 5
Section 2: Device Type - User Managed Computer (UMC) 5
2.1 Purpose 5
2.2 User Managed Computer (UMC) Usage Overview 5
2.3 User Managed Computer (UMC) Hardware Overview 5
2.4 User Managed Computer (UMC) Software Overview 6
2.5 User Managed Computer (UMC) Network Connect Instructions 6
2.6 User Managed Computer (UMC) Login Instructions 7
2.7 User Managed Computer (UMC) Sign Out Instructions 10
2.6 User Managed Computer (UMC) Sign Out Instructions 16
Section 3: Device Type – Zero Client 19
3.1 Purpose 19
3.2 Zero Client Usage Overview 19
3.3 Zero Client Hardware Overview 19
3.4 Zero Client Software Overview 19
3.5 Zero Client Login Instructions 20
3.6 Zero Client Sign Out Instructions 23
Section 4: Device Type – Traditional Laptop/Desktop, Government Furnished Equipment (GFE) 25
4.1 Purpose 25
4.2 Traditional Laptop/Desktop Usage Overview 25
4.3 Traditional Laptop/Desktop Hardware Overview 25
4.4 Traditional Laptop/Desktop Software Overview 25
4.5 Traditional Laptop/Desktop Login Instructions 25
4.6 Laptop/Desktop (GFE) Sign Out Instructions 29
Section 5: Device Type – Laptop/Desktop Contractor Furnished Equipment (CFE)/Personal Equipment (PE) 31
5.1 Purpose 31
5.2 Laptop/Desktop (CFE/PE) Usage Overview 31
5.3 Laptop/Desktop (CFE/PE) User Hardware Overview 31
5.4 Laptop/Desktop (CFE/PE) User Software Recommendations 31
5.5 Laptop/Desktop (CFE/PE) Login Instructions 33

5.6 Laptop/Desktop (CFE/PE) Sign Out Instructions.....37
Section 6.0 Appendix 39
6.1 Support.....39

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:

- User Managed Computer (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 workday, 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:

DEVICE	POLICY
UMC (User Managed Computer)	Approved for DLA office usage with Wi-Fi connection, approved for telework usage
Zero Client	Approved for DLA office usage with wired connection, not approved for telework usage
Traditional Laptop Thick Client	Approved for DLA office usage with wired/Wi-Fi connection, approved for telework usage
Traditional Desktop	Approved for DLA office usage with wired connection, not approved for telework usage
Contractor Equipment	Approved for DLA office usage with Wi-Fi Connection, approved for telework usage
Personal Equipment	Not approved for DLA office usage, approved for telework usage

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 - USER MANAGED COMPUTER (UMC)

2.1 Purpose

Provide an overview of the hardware, software, and steps to access the Virtual Desktop from a User Managed Computer (UMC).

2.2 User Managed Computer (UMC) Usage Overview

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

- Dell Latitude 5420 UMC used on non-Government network connections, i.e. home network, UMC office network, etc.. UMCs are approved for telework.

2.3 User Managed Computer (UMC) Hardware Overview

The UMC 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 Dell Latitude 5420 UMC uses wired (non-Government networks only) and Wi-Fi connections. The following sections will outline the steps required to access the Virtual Desktop:

As of January 2024, DLA is using the Dell Latitude 5420 UMC, which is set to be phased-out by February 2025.

DELL LATITUDE 5420 UMC

I. At a Glance

2.4 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/Remote-VDI and click on Citrix Workspace App for Windows.

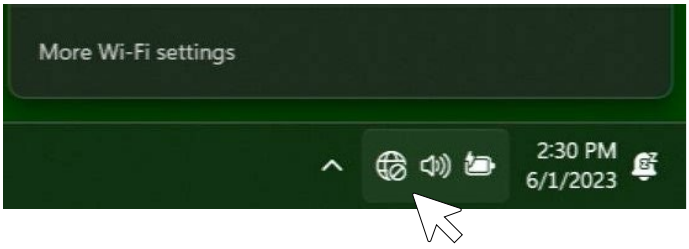
2.5 User Managed Computer (UMC) Network Connect Instructions

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.



2. Select "*DLA_UMC*" from the list of available wireless networks.

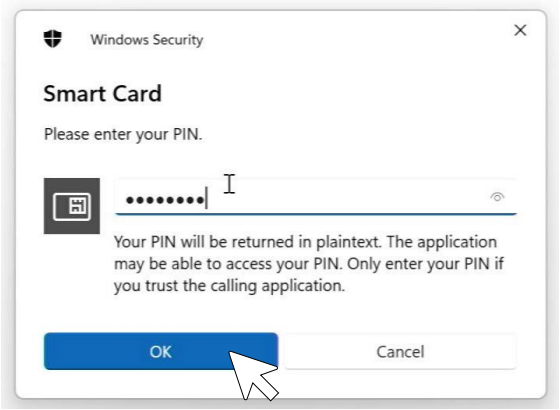
3. Enter the "security key" when prompted: **DLAUMCWIRELESS1**
4. After entering the security key your wireless icon will display an exclamation point. This is normal and you can continue to the VDI login page.

2.6 User Managed Computer (UMC) Login Instructions

The following steps outline the Virtual Desktop login process using a User Managed Computer (UMC):

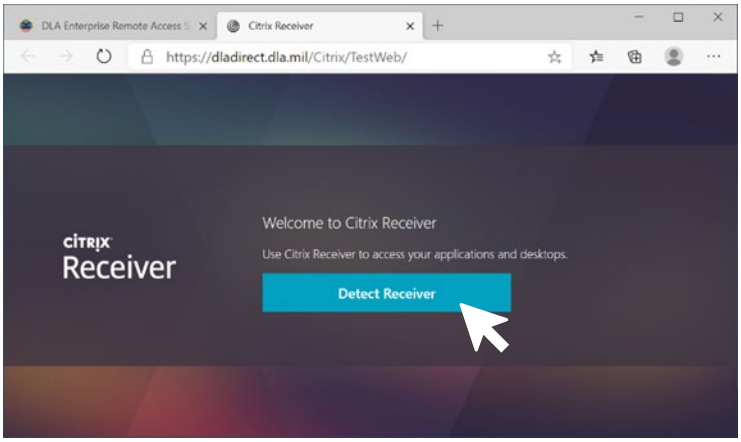
1. Power on Computer (no CAC is needed to login to the computer itself).
2. Insert CAC.
3. Click on Icon for VDI Login.

4. You will be prompted for your Certificate. Please choose the DOD Authentication certificate, and if prompted type in your PIN then click OK.

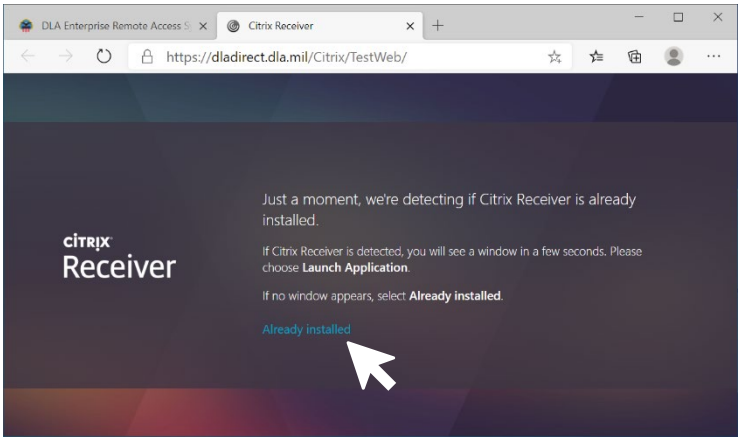


If prompted to Detect Receiver, please follow steps below. If not, please continue with step 6.

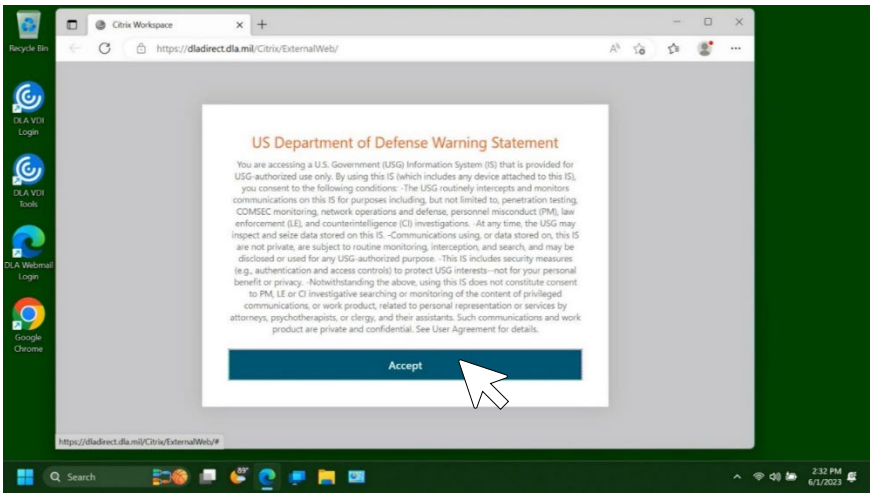
a. Click **Detect Receiver**.



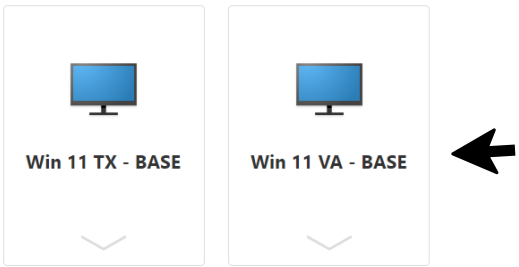
b. Click **Already installed**.



5. Click **Accept** on the Consent Prompt.



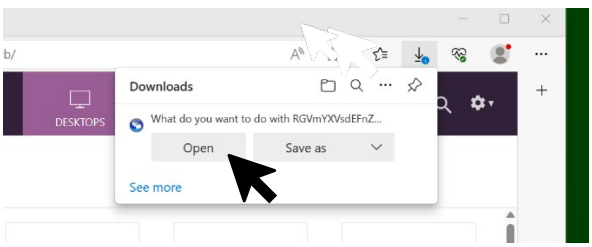
6. Select **either WIN 11 VA or WIN 11 TX DLA Desktop**. **You will see an icon that says either "WIN 11 TX - BASE" or "WIN 11 VA - BASE" depending on your geographical location.*



a. 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.

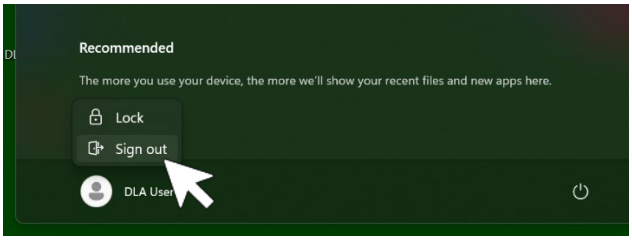


   iii. Continue to log into VDI with your Certificate and your desktop will load.

2.7 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 DLA User, then select **Sign out**.

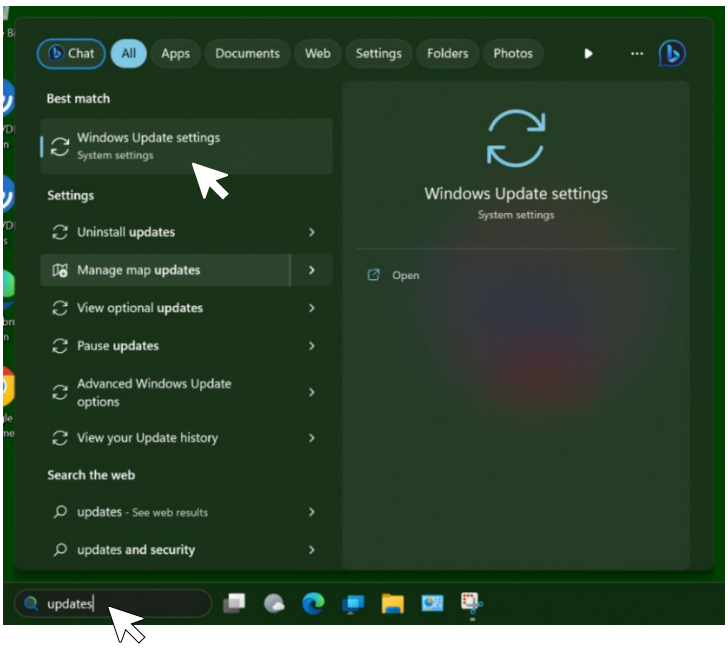


2.8 Updating User Managed Computer (UMC)

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 **Windows Update**. There are multiple ways to open this.
    a. Type "**updates**" into "Type here to search" on the Task Bar, then click "Windows Update Settings".

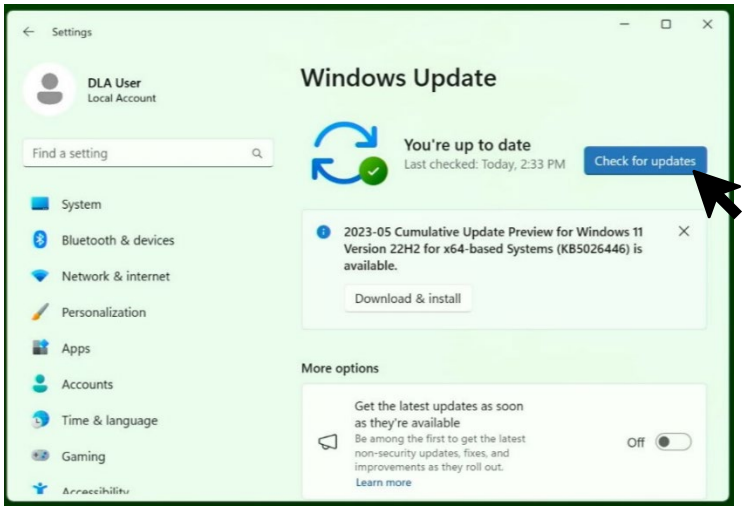


    b. Right Click on Start Menu and from the list choose **Settings**.

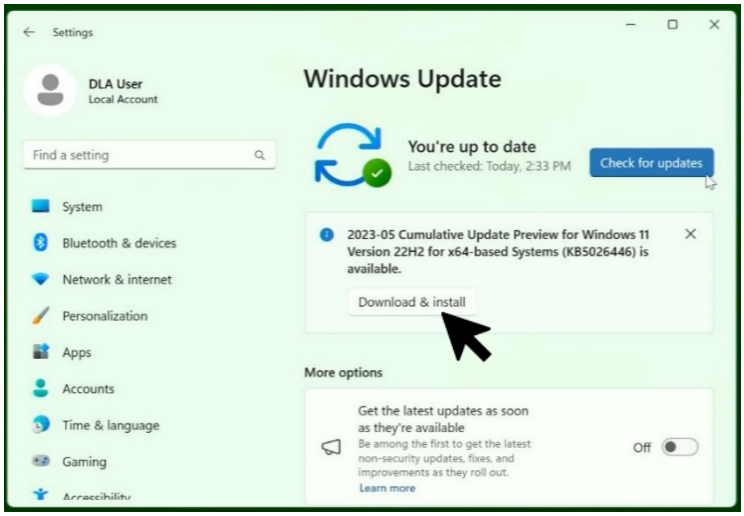
c. Left click start menu and look for **Settings** under "S" in the list.

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.**

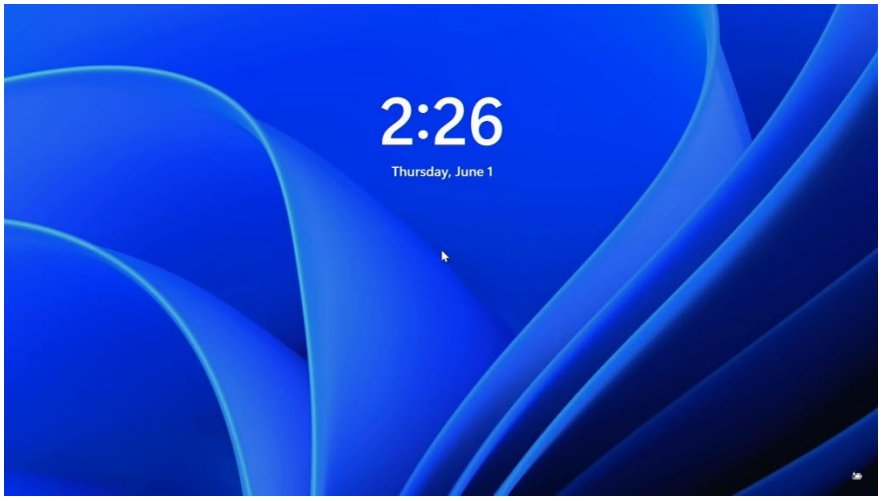


4. This will actively look for Windows current updates your computer needs and will start to install them. Some installs will need to have a system restart after, and it may need to check for updates again for confirmation that all current updates are installed.

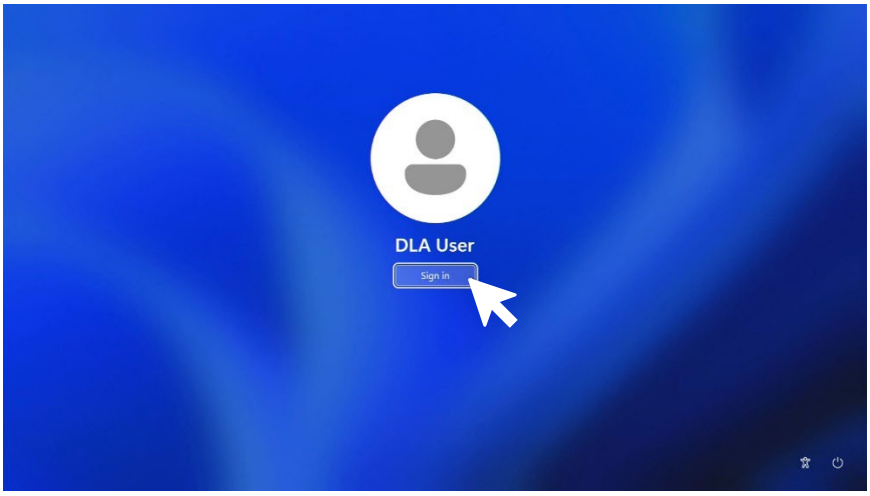


Wireless Network (External)

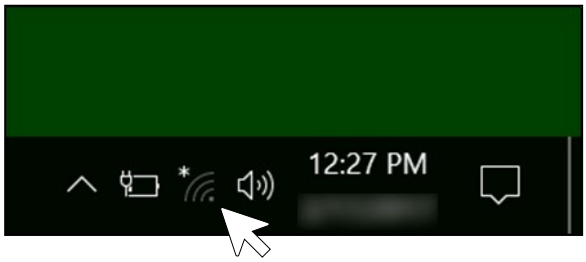
1. Press **Ctrl+Alt+Delete**.



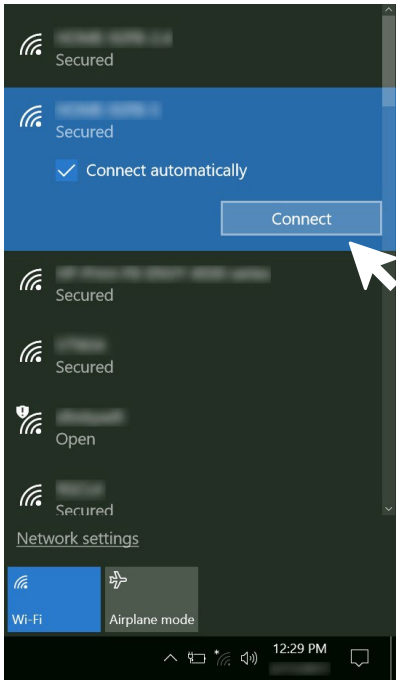
2. Select **Sign in**.



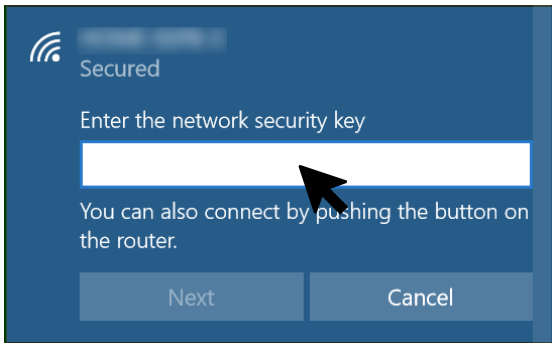
3. Select the **Network Options** Icon in the lower right-hand corner of the screen.



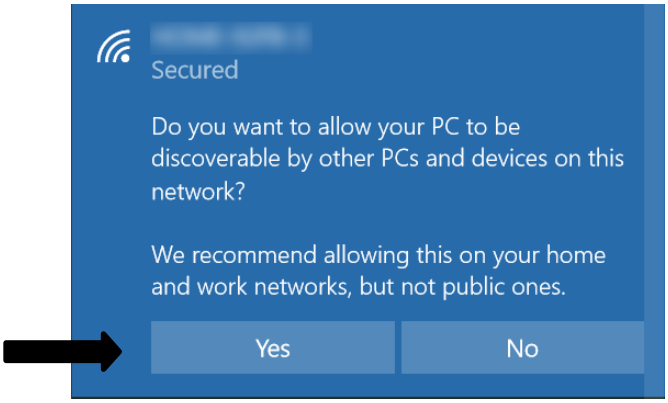
4. Select **Wireless Network** and choose **Connect**. Your list will vary depending on wireless options available to you.



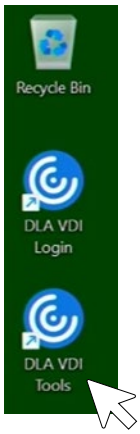
5. Enter **Wireless Network Password** and choose **Next**.



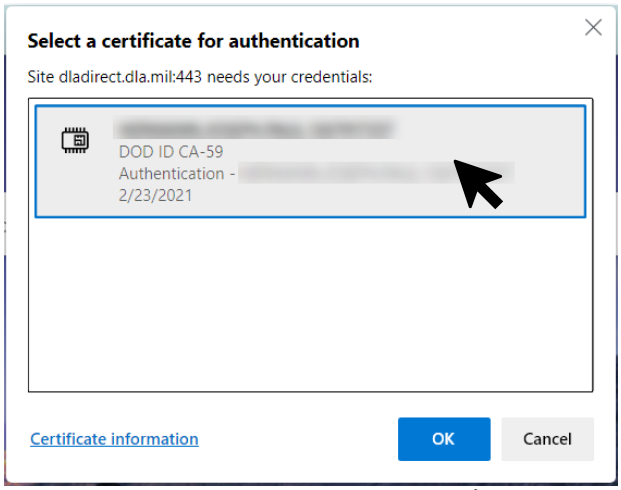
6. Select the appropriate option depending on whether the connection type is a home/work or public network.



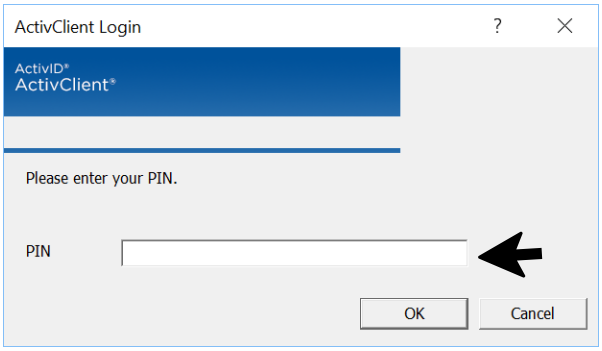
7. Select **DLA VDI Tools.**



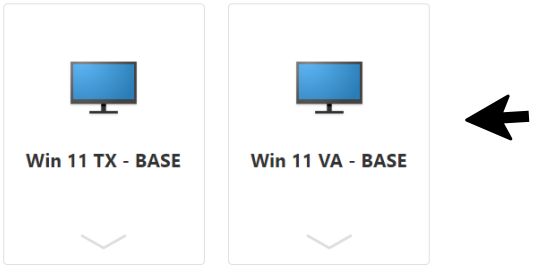
8. Choose the **DOD Authentication** certificate and Select **OK.**
   Note: Select More Choices if the DOD Authentication cert is not currently selected and confirm that you're selecting the correct Smart Card sign in option i.e. EDIPI(16 characters)@.mil.



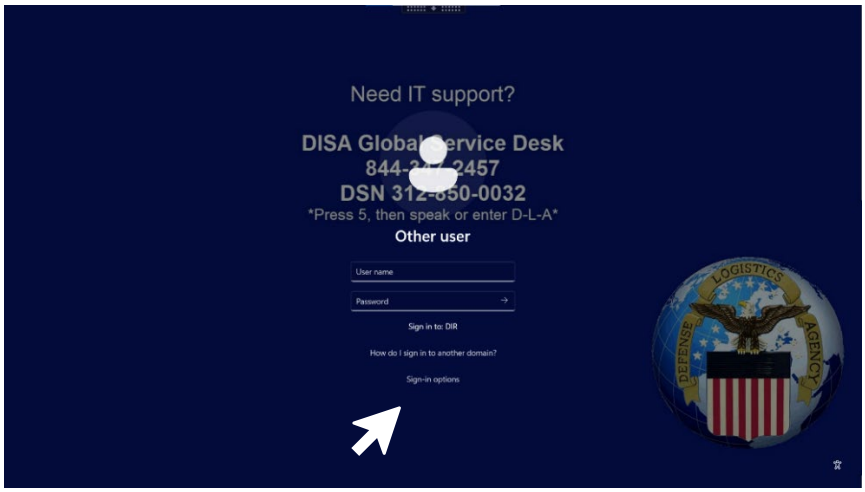
9. Enter **PIN**.



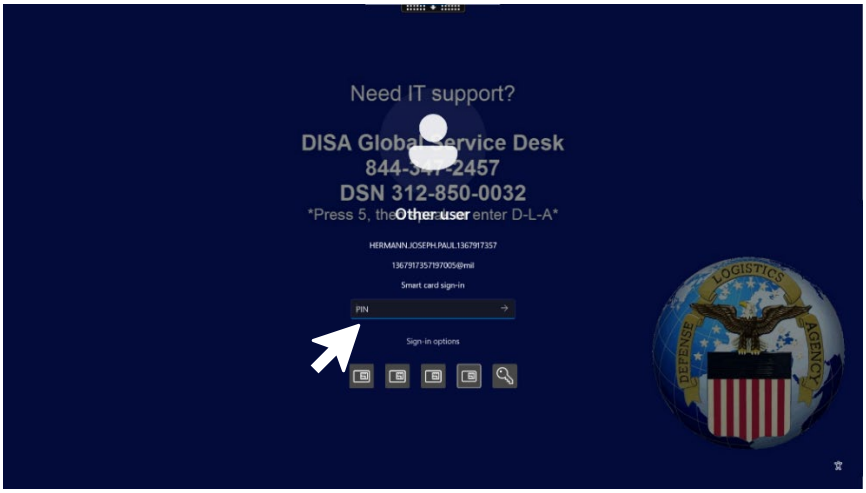
10. Select **WIN 11 VA or WIN 11 TX DLA Desktop.** Screen displays the Citrix Receiver Desktop Options. *You will see an icon that says either "WIN 11 TX - BASE" or "WIN 11 VA - BASE" depending on your geographical location.*



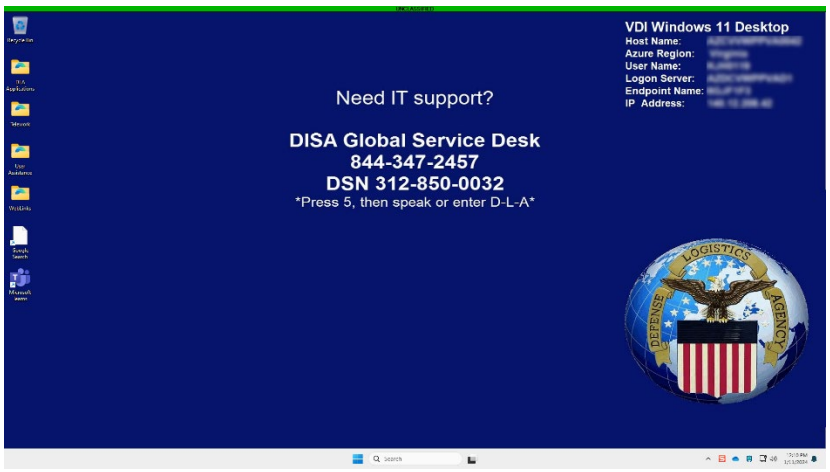
11. Select **Sign-in options**, then select the **Smart Card Login** as the CAC is being read. Choose the DOD Authentication certificate and Select **OK**. **Note**: Select **More Choices** if the DOD Authentication cert is not currently selected and confirm that you're selecting the correct Smart Card sign in option i.e. EDIPI(16 characters)@.mil.



12. Enter **PIN**.



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

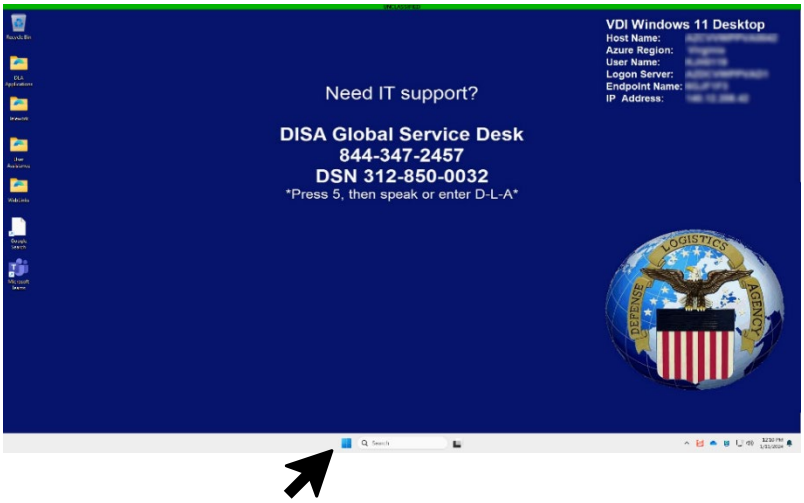


2.6 User Managed Computer (UMC) Sign Out Instructions

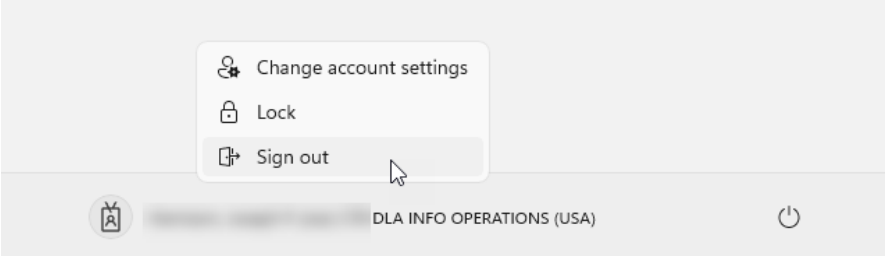
SIGN OUT FROM THE VIRTUAL DESKTOP

To sign out or terminate the active Virtual Desktop session and shut down the User Managed Computer (UMC) follow the below steps. Terminating your Virtual Desktop session will not allow you to transfer your session to another device.

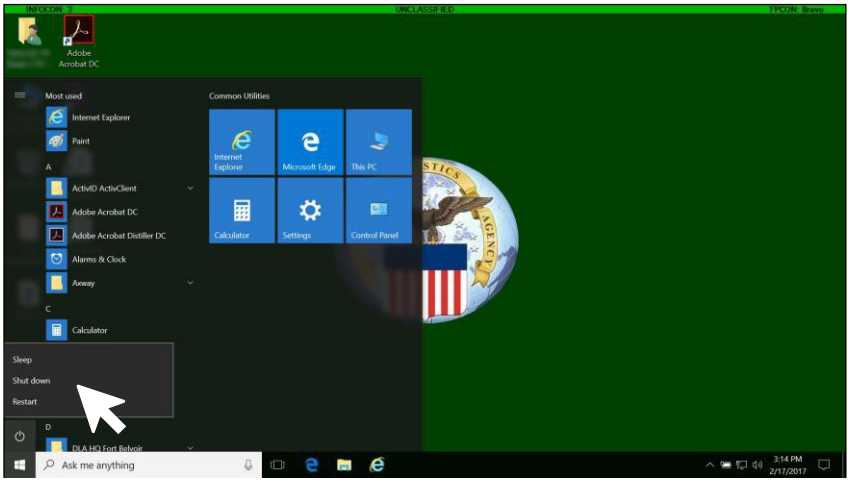
1. Select the Windows button in the lower left-hand corner of the screen (within Virtual Desktop session).



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 5070 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 2023, DLA is using the Dell Wyse 5070 Zero Client.

DELL WYSE 5070 ZERO CLIENT

I. At a Glance

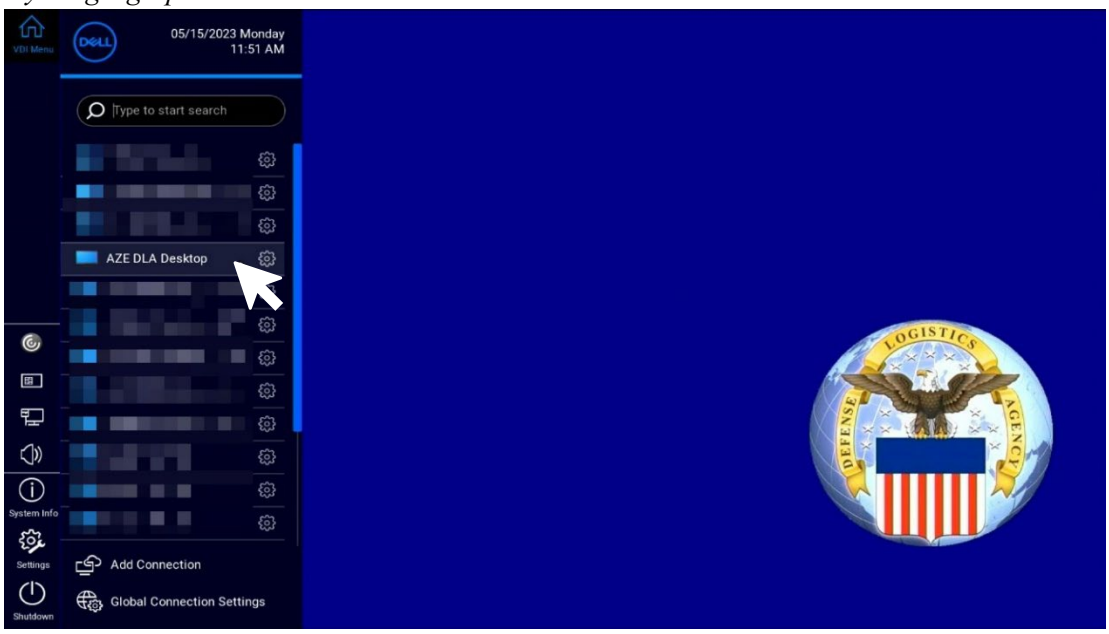
3.4 Zero Client Software Overview

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

3.5 Zero Client Login Instructions

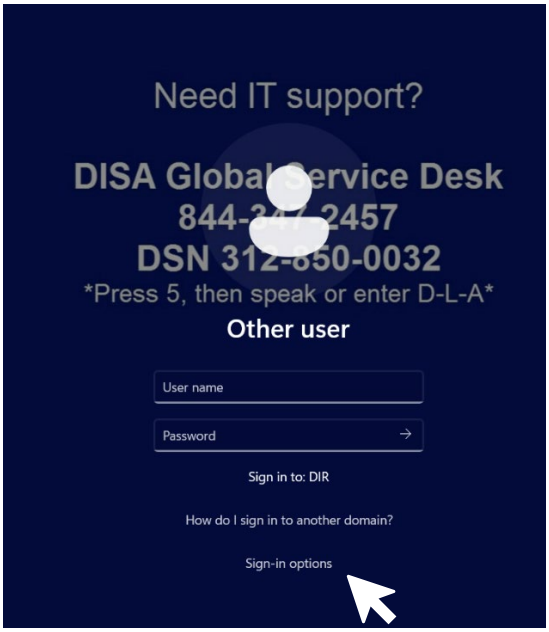
1. Insert Smart Card into Smart Card Reader and enter your PIN.

2. Select the appropriate Virtual Desktop option. **Note:** Desktop options shown will differ user to user. **You will see an icon that says either "WIN 11 TX - BASE" or "WIN 11 VA - BASE" depending on your geographical location.*

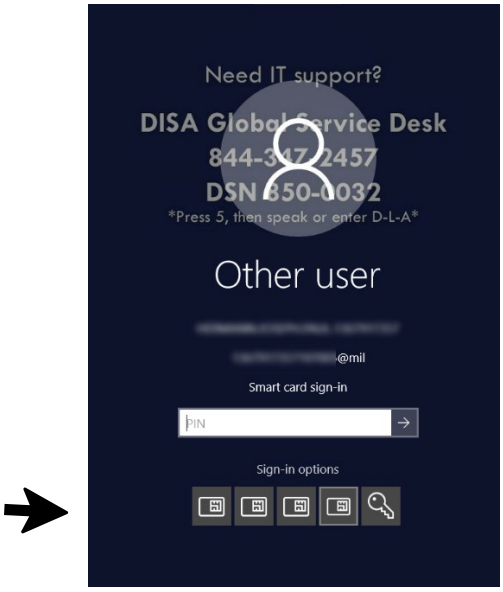


3. Select **OK.**

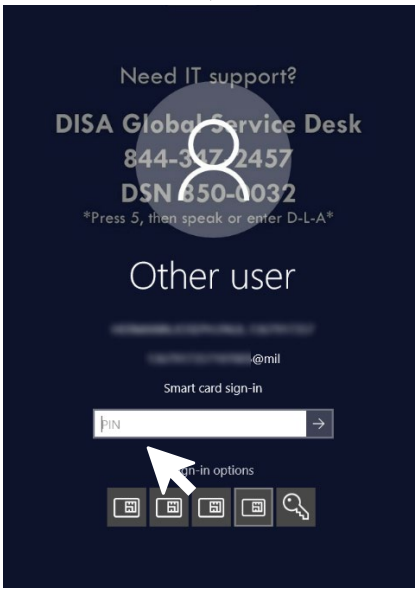
4. When you see this screen click **Sign-in options**.



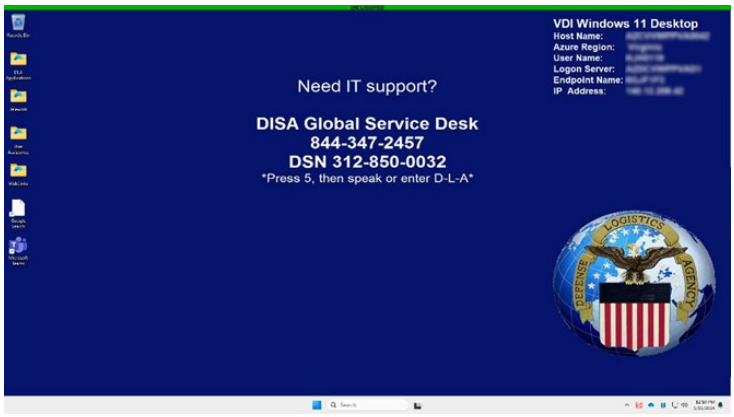
5. Select your proper certificate.



6. Enter your **PIN**, (you may have to scroll down).



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



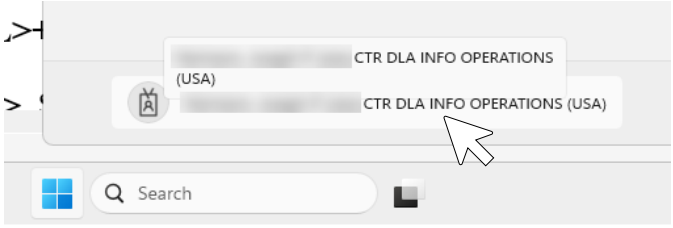
3.6 Zero Client Sign Out Instructions

SIGN OUT FROM THE VIRTUAL DESKTOP

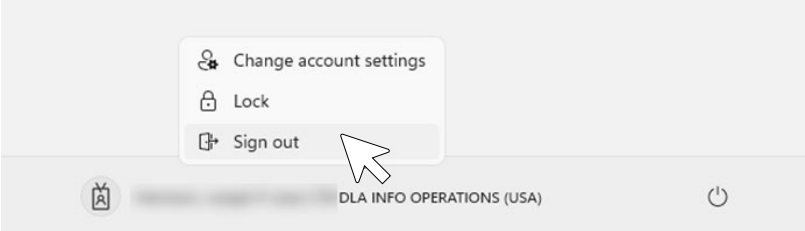
To sign out or terminate the active Virtual Desktop session and shut down the Thin Client follow the below steps. Terminating you Virtual Desktop session will not allow you to transfer your session to another device.

1. Close all open applications.
2. Click on the Windows icon in the bottom middle.

3. Select your user display name.



4. Select **Sign out** (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. 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

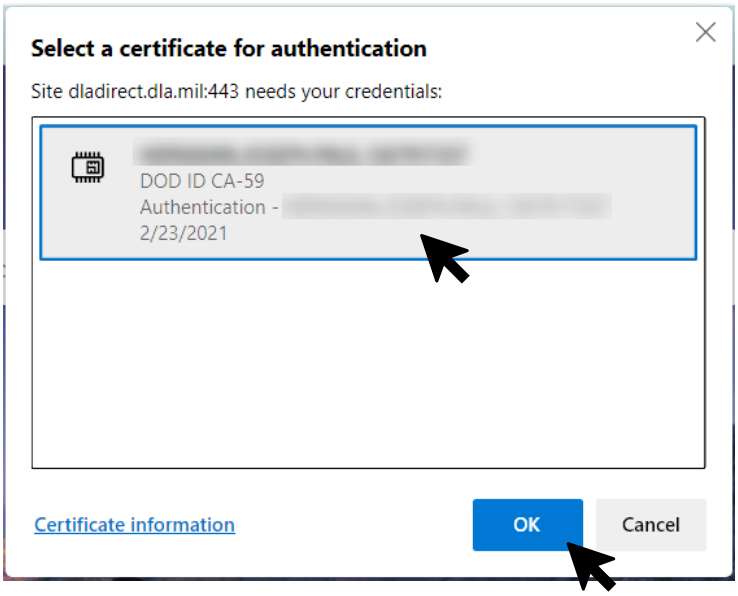
Virtual Desktop software is pre-installed on your machine and is ready to use.

4.5 Traditional Laptop/Desktop Login Instructions

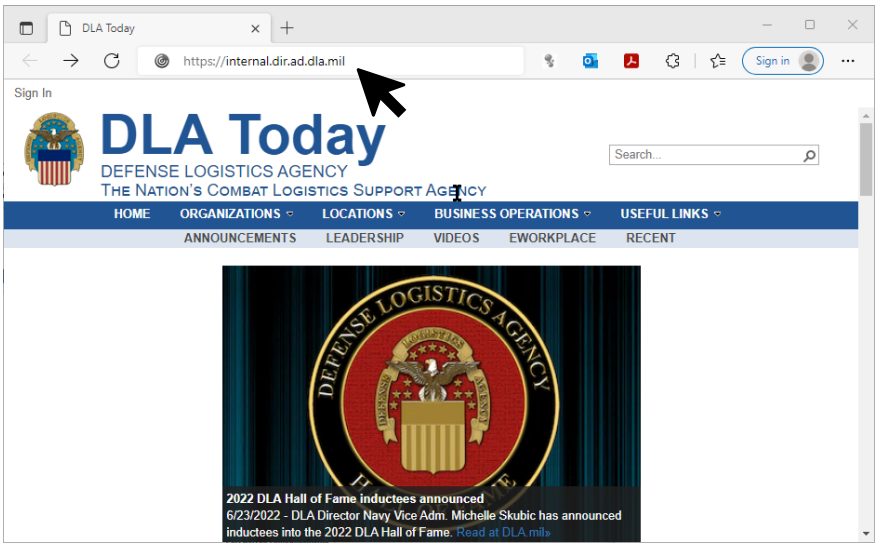
The following steps outline the Virtual Desktop login process using a traditional laptop/desktop:

1. Ensure CAC is inserted into CAC Reader.
2. Open Microsoft Edge and select **Authentication Certificate**. ***Note****: Select* ***More Choices*** *if the DOD Authentication cert is not currently selected*. Confirm that you're selecting the correct Smart Card sign in option i.e. EDIPI(16 characters)@.mil.

3. Click **OK**.

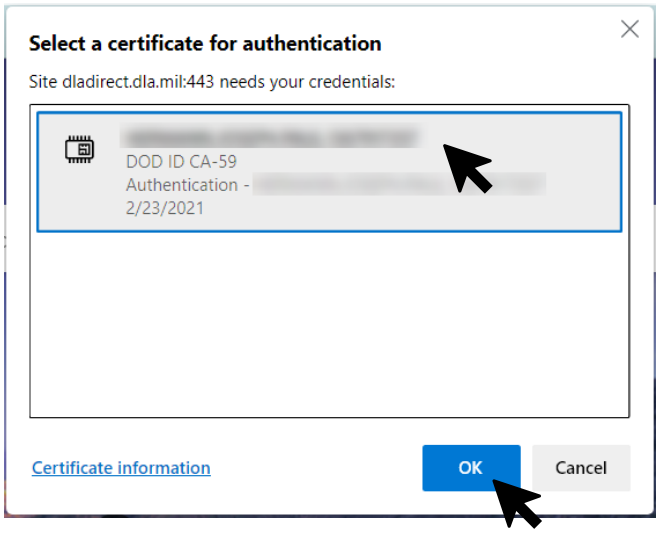


4. Enter the following URL: ***https://internal.dir.ad.dla.mil.***

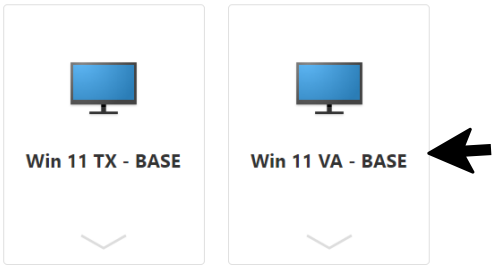


5. Choose the **DOD Authentication** certificate and Select **OK.** ***Note****: Select* ***More Choices*** *if the DOD Authentication cert is not currently selected.* Confirm that you're selecting the correct Smart Card sign in option i.e. *EDIPI*(16 characters)*@.mil.*

6. Click **OK**.

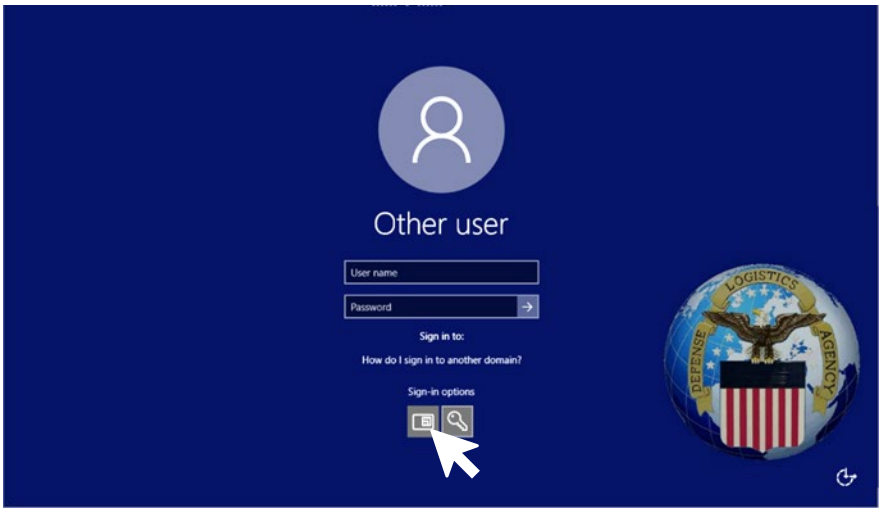


7. Select the **WIN 11 VA or WIN 11 TX DLA Desktop**, if needed. The Azure Desktop may open automatically. **You will see an icon that says either "WIN 11 TX - BASE" or "WIN 11 VA - BASE" depending on your geographical location.*

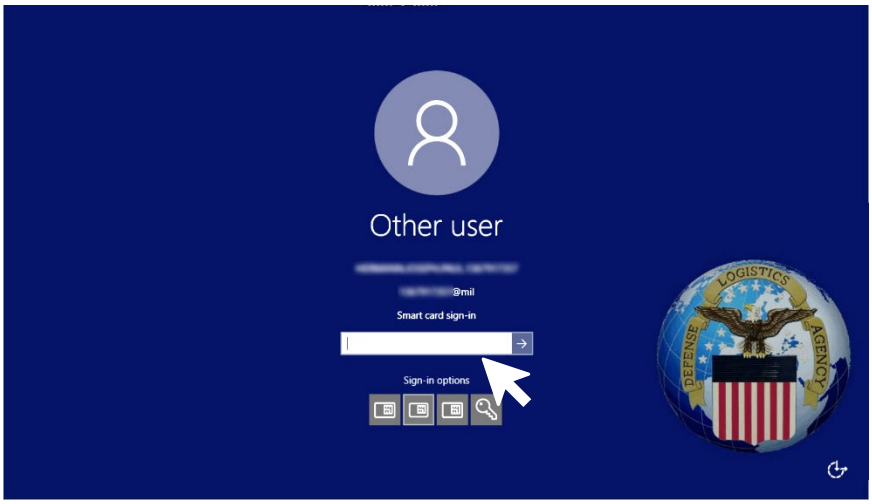


8. Click **OK**.

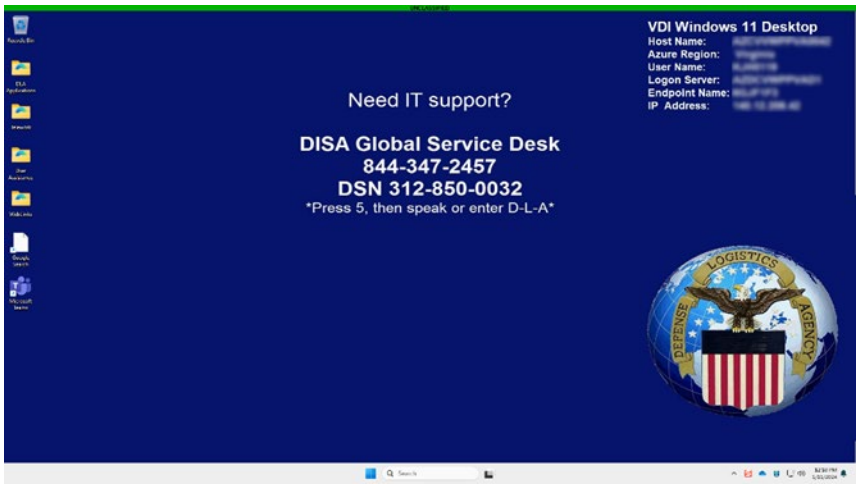
9. Select the **Smart Cart Login** as the CAC is being read. Do not navigate away from this window until the login process is complete. Doing so may result in your session timing out.



10. Enter **PIN**.



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



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

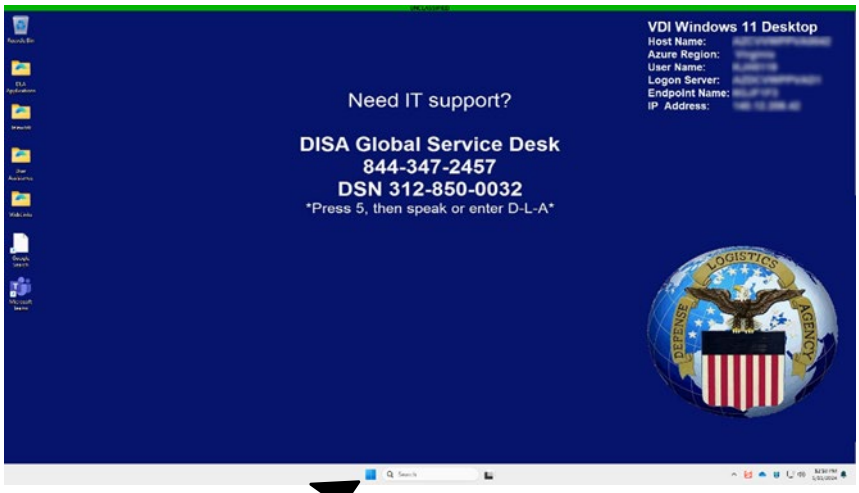
4.6 Laptop/Desktop (GFE) Sign Out Instructions

Sign out of the Virtual Desktop using the steps below:

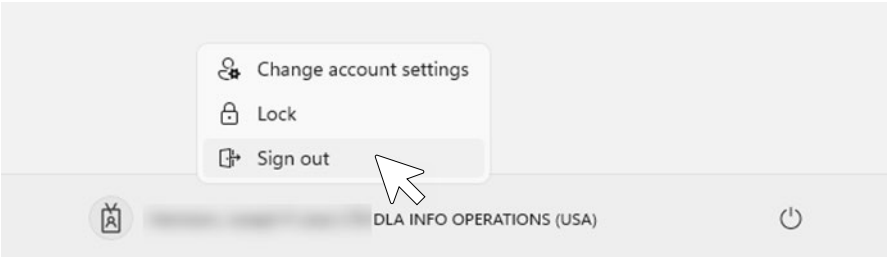
SIGN OUT OF VIRTUAL DESKTOP

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 bottom middle 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) 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.

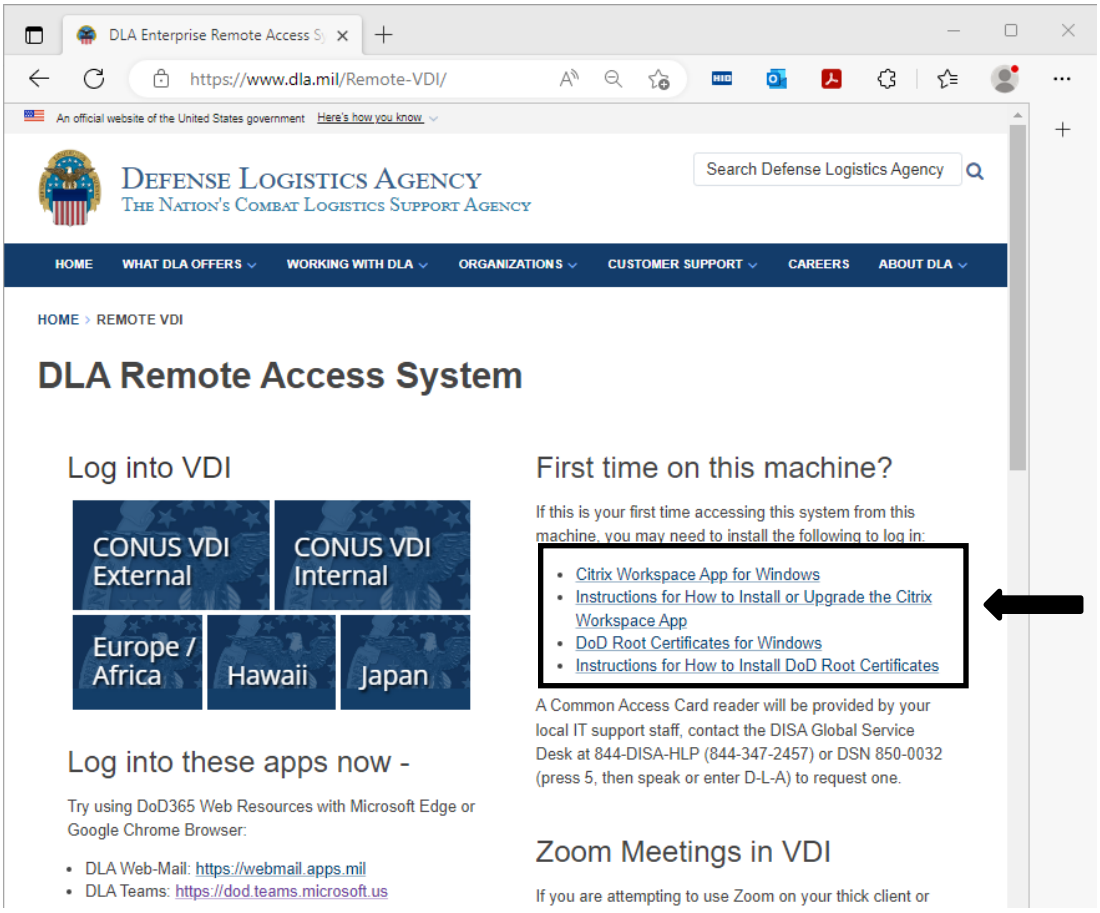
For best performance use following operating system/browser combinations, otherwise you may experience performance issues or inability to connect to the Virtual Desktop.

Operating System	Browser Version
Windows 10 32/64-bit Editions	Google Chrome 101.x
Windows 10 32/64-bit Editions	Microsoft Edge Chromium 101.x
Windows 10 32/64-bit Editions	Mozilla Firefox 91.x
Windows 10 32/64-bit Editions	Internet Explorer 11.x (has been deprecated)

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/Remote-VDI.

Follow these steps for downloading the appropriate software in Microsoft Edge. 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. Insert CAC into CAC Reader.
5. In Microsoft Edge navigate to DLA Enterprise Remote Access https://www.dla.mil/Remote-VDI 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.



***Note**: DoD Root Certificates are no longer needed for accessing DLA VDI desktops.*

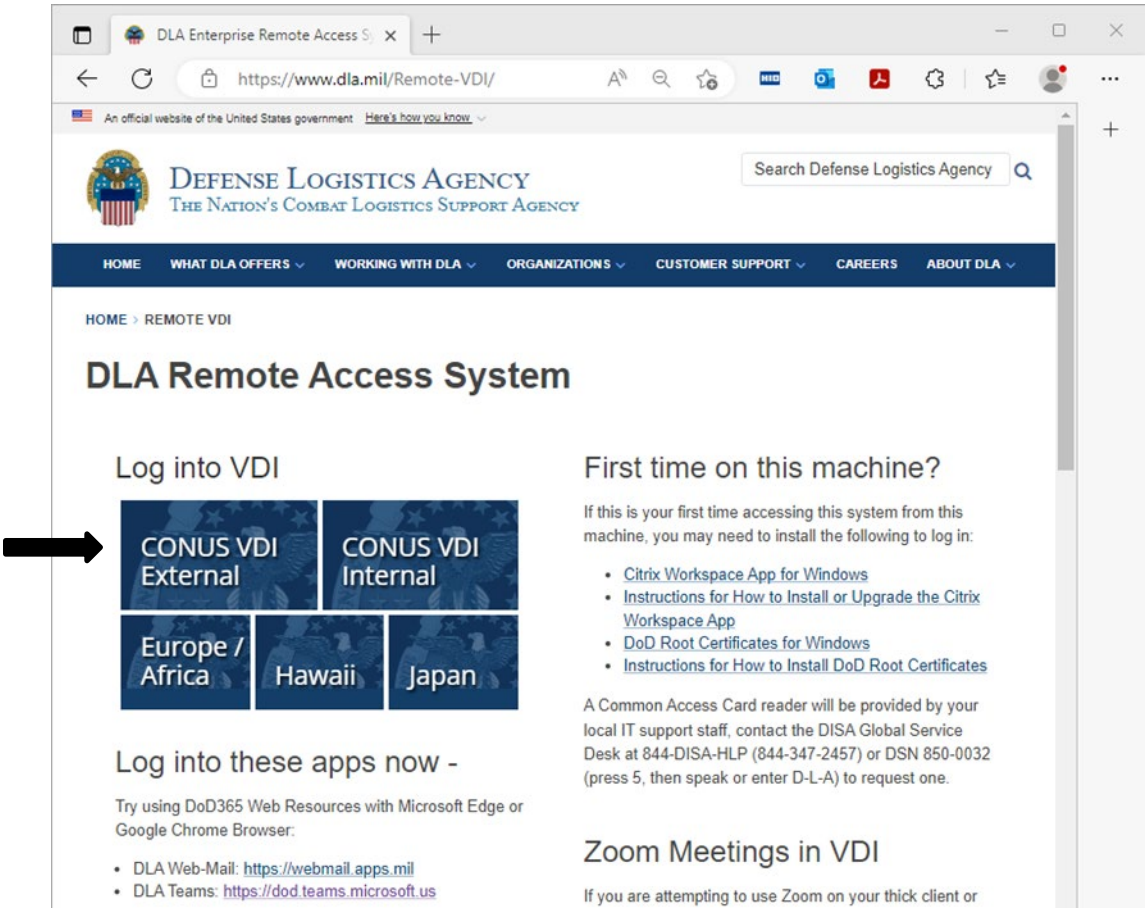
6. Reboot the computer. All required software is now available on the machine, and you are ready to the login to your Virtual Desktop. (See section 5.5 for login instructions.)

5.5 Laptop/Desktop (CFE/PE) Login Instructions

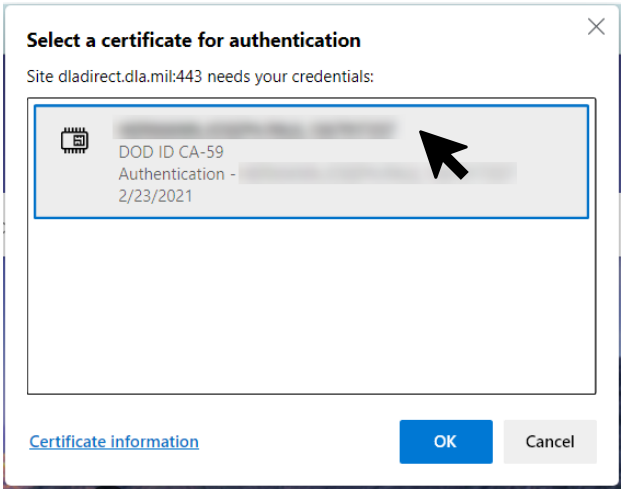
The following steps outline the Virtual Desktop login process using a CFE/Personal Machine:

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

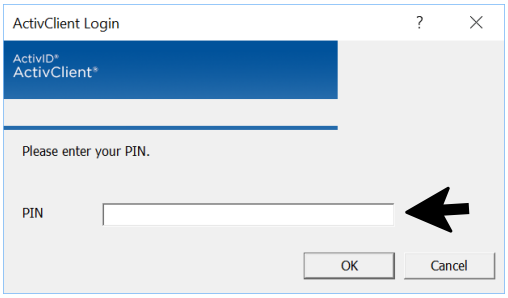
1. Insert CAC into CAC Reader
2. Open Microsoft Edge
3. Enter the following URL: https://www.dla.mil/Remote-VDI **(continue to step 4) or** https://dladirect.dla.mil **(continue to step 5)**
4. Select the **CONUS VDI - External** button



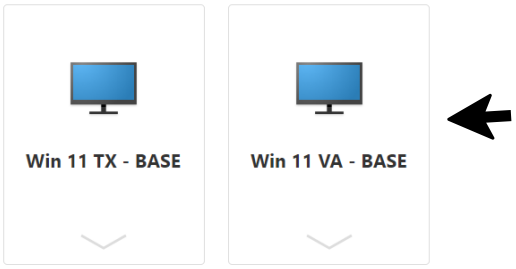
5. Choose the **DOD Authentication** certificate and Select **OK**. ***Note****: Select* ***More Choices*** *if the DOD Authentication cert is not currently selected.* Confirm that you're selecting the correct Smart Card sign in option i.e. EDIPI(16 characters)@.mil.



6. Enter **PIN**.

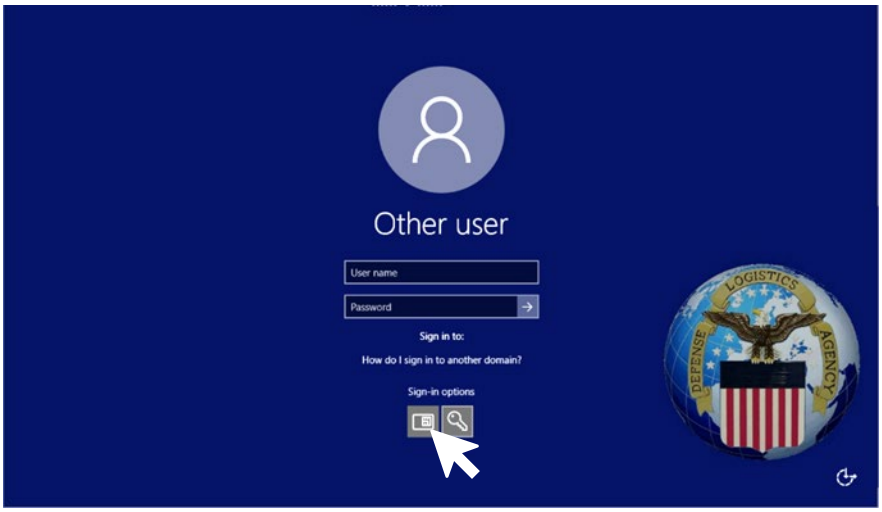


7. Select **WIN 11 VA or WIN 11 TX DLA Desktop.** Screen displays the Citrix Receiver Desktop Options. **You will see an icon that says either "WIN 11 TX - BASE" or "WIN 11 VA - BASE" depending on your geographical location*

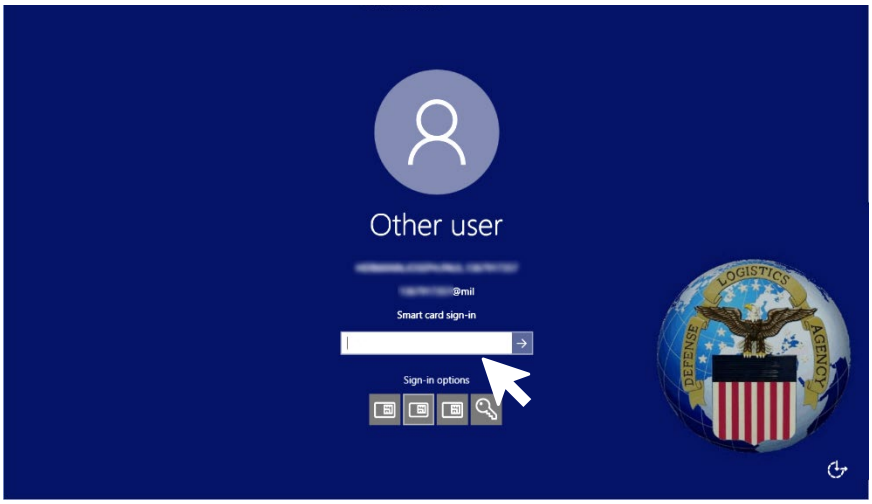


8. Select **OK**.

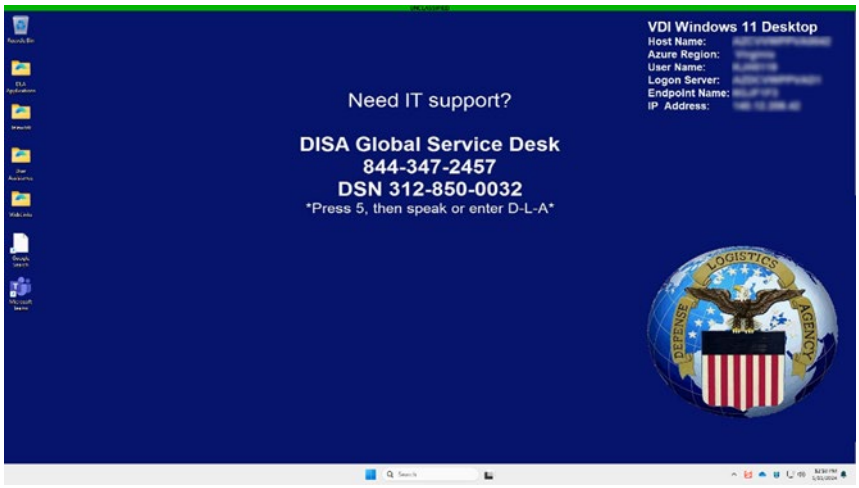
9. Select **Sign-in options**, then **Smart Cart Login** option while the CAC is being read and stay on this window until the login process is complete. Navigating away from this before the login process is complete may result in you session being timed out. If this happens you will need to login again.



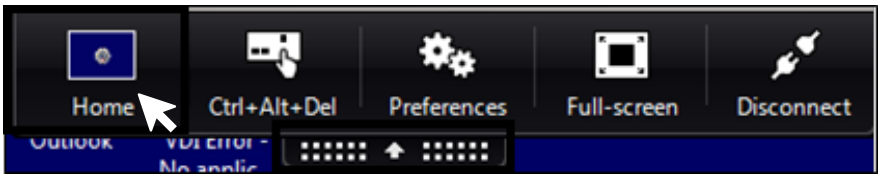
10. Enter **PIN**.



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 page and choose **Home**.

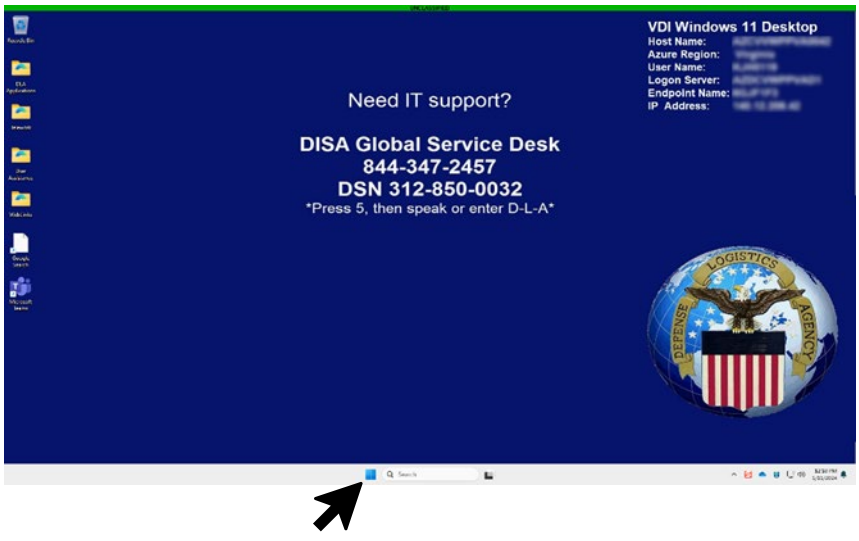


5.6 Laptop/Desktop (CFE/PE) Sign Out Instructions

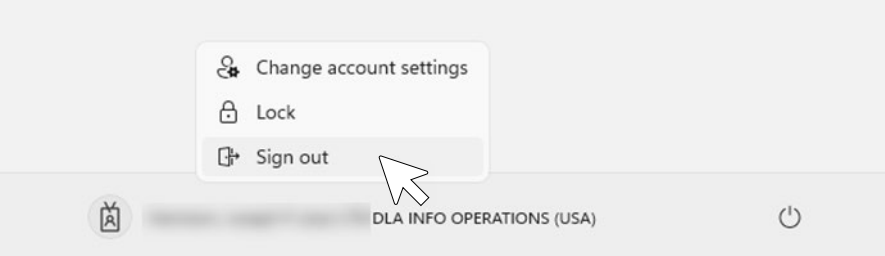
There are two ways to sign out of the Virtual Desktop.

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 bottom middle of your screen.



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



DISCONNECTING VDI SESSION

Note: User is leaving for lunch, meeting, break, etc. b[illegible]ntends 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 **Lock this computer** → Pull CAC
4. Select Keystrokes **<Windows>** + **<L>** → Pull CAC.

SECTION 6.0 APPENDIX

6.1 Support

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

You may put in a service request through ServiceNow

Phone: (844) 347-2457