Defense Logistics Agency



Virtual Desktop: User Guide

Updated October 2019



TABLE OF CONTENTS

Introduction	3
Section 1: Virtual Desktop Overview	4
1.1 Virtual Desktop Background	
Section 2: Device Type - Thin Client	4
2.1 Purpose	
2.2 Thin Client Usage Overview	
2.3 Thin Client Hardware Overview	5
2.4 Thin Client Software Overview	11
2.5 Thin Client Login Instructions	11
2.6 Thin Client Sign Out Instructions	24
Section 3: Device Type – Zero Client	26
3.1 Purpose	26
3.2 Zero Client Usage Overview	26
3.3 Zero Client Hardware Overview	26
3.4 Zero Client Software Overview	27
3.5 Zero Client Login Instructions	27
3.6 Zero Client Sig Out Instructions	31
On sting to Device Trees. The different Leaster (Device - One managet Francische d Francis	mant (CEE) 22
Section 4: Device Type – Traditional Laptop/Desktop, Government Furnished Equip	ment (GFE)33
4.1 Purpose	
4.1 Purpose	
4.1 Purpose 4.2 Traditional Laptop/Desktop Usage Overview	
 4.1 Purpose 4.2 Traditional Laptop/Desktop Usage Overview 4.3 Traditional Laptop/Desktop Hardware Overview 	
 4.1 Purpose	
 4.1 Purpose 4.2 Traditional Laptop/Desktop Usage Overview 4.3 Traditional Laptop/Desktop Hardware Overview 4.4 Traditional Laptop/Desktop Software Overview 4.5 Traditional Laptop/Desktop Login Instructions 4.6 Laptop/Desktop (GFE) Sign Out Instructions Section 5: Device Type – Laptop/Desktop Contractor Furnished Equipment (CFE)/P 	
 4.1 Purpose	33 33 33 33 33 34 34 37 ersonal 39
 4.1 Purpose 4.2 Traditional Laptop/Desktop Usage Overview 4.3 Traditional Laptop/Desktop Hardware Overview 4.4 Traditional Laptop/Desktop Software Overview 4.5 Traditional Laptop/Desktop Login Instructions 4.6 Laptop/Desktop (GFE) Sign Out Instructions Section 5: Device Type – Laptop/Desktop Contractor Furnished Equipment (CFE)/P Equipment (PE) 5.1 Purpose 	33 33 33 33 33 34 34 37 ersonal 39 39
 4.1 Purpose	33 33 33 33 33 34 34 37 ersonal 39 39 39
 4.1 Purpose	33 33 33 33 33 34 34 37 ersonal 39 39 39 39 39
 4.1 Purpose 4.2 Traditional Laptop/Desktop Usage Overview 4.3 Traditional Laptop/Desktop Hardware Overview 4.4 Traditional Laptop/Desktop Software Overview 4.5 Traditional Laptop/Desktop Login Instructions 4.6 Laptop/Desktop (GFE) Sign Out Instructions Section 5: Device Type – Laptop/Desktop Contractor Furnished Equipment (CFE)/P Equipment (PE) 5.1 Purpose 5.2 Laptop/Desktop (CFE/PE) Usage Overview 5.3 Laptop/Desktop (CFE/PE) User Hardware Overview 5.4 Laptop/Desktop (CFE/PE) User Software Recommendations 	33 33 33 33 33 33 34 37 ersonal 39 39 39 39 39 39
 4.1 Purpose	33 33 33 33 33 34 34 37 Personal 39 39 39 39 39 39 39 51
 4.1 Purpose	33 33 33 33 33 34 34 37 ersonal 39 39 39 39 39 51 51 56
 4.1 Purpose	33 33 33 33 33 34 37 (ersonal 39 39 39 39 39 39 51 56 56 58



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
- 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:

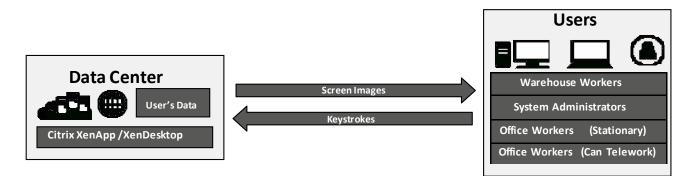
Device	Policy
HP MT42 Mobile Thin Client	Approved for DLA office usage with wired/Wi-Fi
	connection, approved for telework usage
Dell Wyse 5010 Zero Client	Approved for DLA office usage with wired
	connection, not approved for telework usage
Traditional Laptop	Approved for DLA office usage with wired/Wi-Fi
	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 - 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.



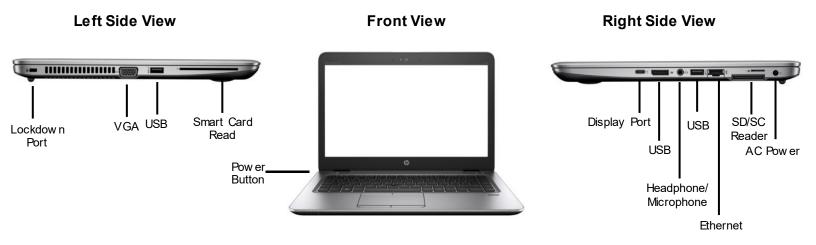
2.3 Thin Client Hardware Overview

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.

HP MT42 Mobile Thin Client





II. <u>Accessories</u>

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

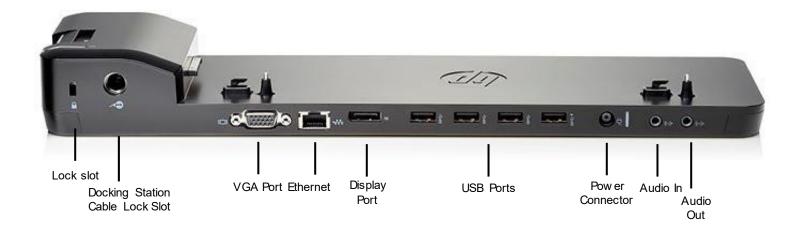
Image	Description
	Power Cord
*****	Docking Station



HP Ultra-light Docking Station

I. <u>At a Glance</u>





II. <u>Accessories</u>

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

Image	Description
	Power Cord



2.4 Thin Client Software Overview

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

[123] 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).

DLA Network (Internal)

a. Press Ctrl+Alt+Delete.

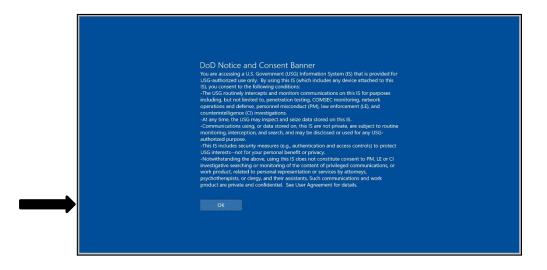
Screen displays the ThinPC login image.





b. Select OK.

Screen displays the US Department of Defense Warning Statement.



c. Insert CAC into the Smart Card Reader.

Screen displays the ThinPC Smart Card Input.





d. Enter PIN.

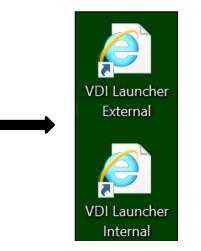
Note: Confirm that you're selecting the correct Smart Card sign in option i.e. *EDIPI*(10 characters)@.*mil.*

Screen displays the ThinPC PIN Input.

 Other user Sign-in options	
	⊕ ტ

e. Select VDI Launcher Internal.

Screen displays the Virtual Desktop Internal/External Login options.





f. Choose the **DOD EMAIL** certificate and Select **OK**. Note: Select **More Choices** if the DOD EMAIL cert is not currently selected.

Screen displays the DOD Certificate options.

lnternet Explorer		-	\times
	Windows Security ×		
	Select a Certificate		
	Site dladirect.dla.mil needs your credentials:		
	Signature -		
	Issuer: DOD EMAIL CA-44		
	Valid From:		
	Click here to view certificate properties		
	More choices		
	OK Cancel		

g. Enter PIN.

ActivClient Lo	gin		?	\times
ActivID* ActivClient*				
Please enter y	our PIN.			
PIN				
		ОК	Cano	el

h. Select DLA Standard Desktop 2016.

Screen displays the Citrix Receiver Desktop Options.





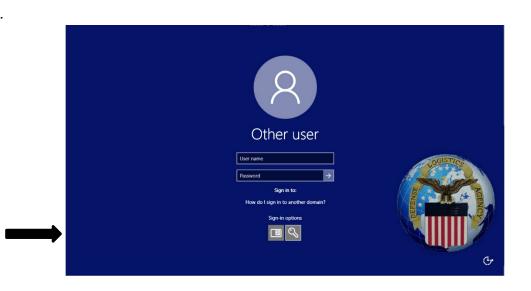
i. Select OK.

Screen displays the US Department of Defense Warning Statement.



j. Select the **Smart Card Login** as the CAC is being read.

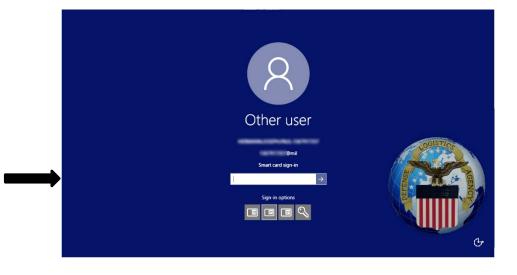
Screen displays the Virtual Desktop – Citrix Receiver requesting the user to select the Smart Cart Login option.



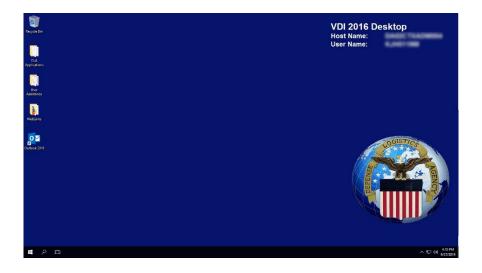


k. Enter PIN.

Screen displays the Virtual Desktop – Citrix Receiver requesting the user to enter their PIN.



The Virtual Desktop is ready to use, just as you would use a traditional desktop. *Screen displays the Virtual Desktop.*





Wireless Network (External)

a. Press Ctrl+Alt+De lete.

Screen displays the ThinPC login image.



b. Select OK.

Screen displays the US Department of Defense Warning Statement.

DoD Notice and Consent Banner You are accessing a U.S. Government (USO) Information System (IS) that is provided for USO-authorized use only. By using this IS (which includes any device attached to this
IS, you consent to the following conditions: -The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network
operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (C) investigations.
-At any time, the USG may inspect and seize data stored on this IS. -Communications using, or data stored on, this IS are not private, are subject to routine
monitoring, interception, and search, and may be disclosed or used for any USG- authorized purpose.
 This IS includes security measures (e.g., authentication and access controls) to protect USG interests—not for your personal benefit or privacy.
 Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or
work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work
product are private and confidential. See User Agreement for details.

-



c. Insert CAC into the Smart Card Reader. Screen displays the ThinPC Smart Card Input.



d. Enter PIN.

Note: Confirm that you're selecting the correct Smart Card sign in option i.e. *EDIPI*(10 characters)@.*mil.*

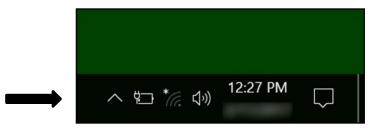
Screen displays the ThinPC PIN Input.

Other user	
Smart card sign-in	
Sign-in options	
	ው ወ



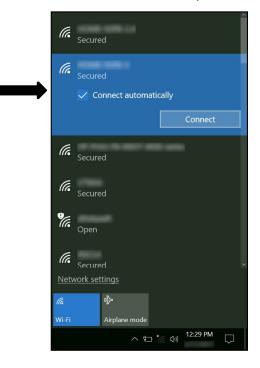
e. Select the Network Options lcon in the lower right-hand corner of the screen.

Screen displays the Thin Client desktop.



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

Screen displays the wireless network connection options.





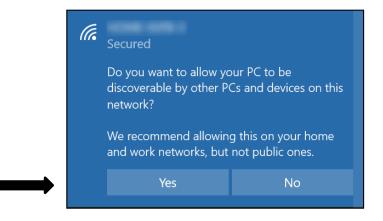
g. Enter Wireless Network Password and choose OK.

Screen displays window requiring network security key.

(7.	Secured	
	Enter the network secur	ity key
	You can also connect by the router.	pushing the button on
		Cancel

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

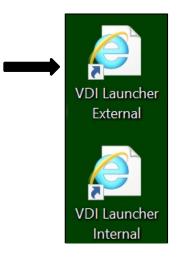
Screen displays the network location options.





i. Select VDI Launcher External.

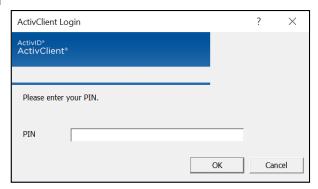
Screen displays the Virtual Desktop Internal/External Login options.



j. Choose the **DOD EMAIL** certificate and Select **OK**.

lnternet Explorer			-	
	Windows Security	×		
	Select a Certificate			
	Site dladirect.dla.mil needs your credentials:			
	Signature -			
	Issuer: DOD EMAIL CA-44			
	Valid From:			
	Click here to view certificate properties			
➡	More choices			
	OK Cancel			

k. Enter PIN





I. Select DLA Standard Desktop.

Screen displays the Citrix Receiver Desktop Options.



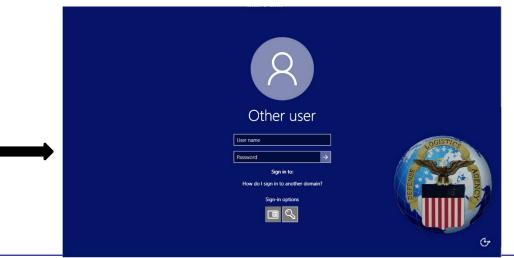
m. Select **OK**.

Screen displays the US Department of Defense Warning Statement.

 DeD Notice and Consent Banner The USG routine's use only. By using this IS (which includes any device attached to this is you consent to the following conditions: The USG routine's intercepts and monitors on ommerciality of for purposes individually intercepts and monitors commerciality of the other processing at USG over the following conditions: The USG routine's intercepts and monitors commerciality of the other processing at USG over the following conditions: The USG routine's intercepts and monitors commerciality of the other processing at USG routine's intercepts and monitors commerciality of the other processing at USG routine's intercepts and monitors intervent (US) we efforcement (US) and the other processing at USG routine's intervent (VI) we efforcement (US) and the other processing at USG routine's intervent (VI) we efforcement (US) and the other processing at USG routine's intervent (VI) we efforcement (US) and the other processing at USG routine's and routine's the other processing at USG routine's and routine's and routine's and routine's and routine's routine's routine's and routine's routine's routine's and routi	

n. Select the Smart Cart Login as the CAC is being read.

Screen displays the Virtual Desktop – Citrix Receiver requesting the user to select the Smart Cart Login option.

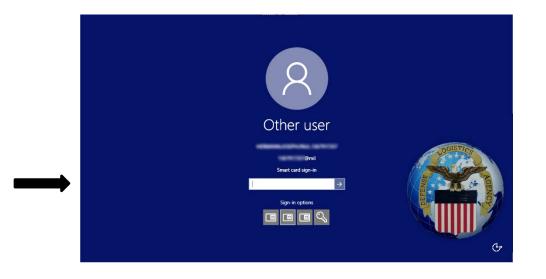


Virtual Desktop User Guide

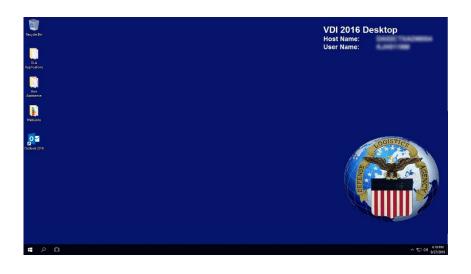


o. Enter **PIN**.

Screen displays the Virtual Desktop – Citrix Receiver requesting the user to enter their PIN.



The Virtual Desktop is ready to use, just as you would use a traditional desktop. *Screen displays the Virtual Desktop.*





년²³ 2.6 Thin Client Sign Out Instructions

I. <u>Sign Out from the Virtual Desktop</u>

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.

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

Screen displays the Virtual Desktop.





b. Select the **Sign Out** button (within Virtual Desktop session). Screen displays the Virtual Desktop with Sign Out button.

Roychen Roychen		VDI 2016 Desktop Host Name: User Name:
 Manuscuel Manuscuel	Connect tables	

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

Screen displays the local machine desktop.

INFOCON: 3		UNC	LASSIFIED	FPCON: Bravo
Adobe Acrobat DC				
Most used	Common Utilities	_		
Internet Explorer	and the second se	200 V		
Paint	Internet Explorer Micro	e 🤰		
	Explorer Micro	osoft Edge This PC	STICS	
ActivID ActivClient	*			
Adobe Acrobat DC		🛱 📼	and the second s	
Adobe Acrobat Distiller DC	Calculator Setti	igs Control Panel	E State	
S Alarms & Clock				
Акмау				
c				
Calculator				
lunes 1				
Sleep Shut down				
Snut down				
DLA HQ Fort Belvoir				
Ask me anything	8 🗆	e 🖬 é		수 등 및 40 ^{3:14 PM} 2/17/2017 및

II. 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:**

- Select Keystrokes <CTRL>+<ALT>+ → Select Lock → Pull CAC.
- From the XenDesktop toolbar at the top of the VDI session, Select Ctrl+Alt+Del → Select Lock this computer → Pull CAC.



• 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 device used to access the Virtual Desktop:

• Dell Wyse 5010 Zero Client is used in the office with wired DLA network. The Zero Client is not approved for telework.



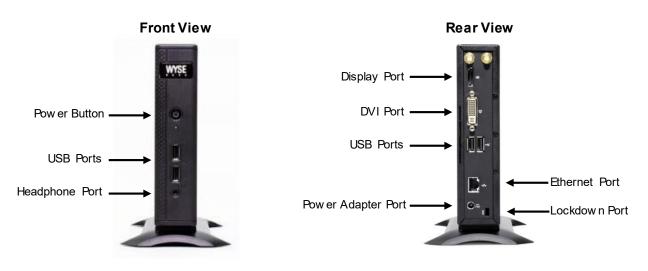
3.3 Zero Client Hardware Overview

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 2016, DLA is using the Dell Wyse 5010 Zero Client.

Dell Wyse 5010 Zero Client

I. <u>At a Glance</u>





II. <u>Accessories</u>

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

Image	Description
	Power Cord



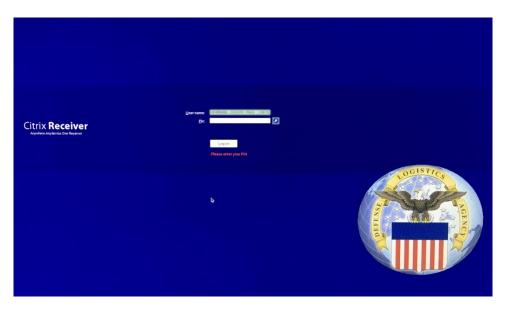
3.4 Zero Client Software Overview

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



a. Insert Smart Card into Smart Card Reader.

Screen displays the Zero Client login image.





b. 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*.

<u>U</u> ser name: <u>P</u> in:	Smartcard
IC Select :	Smartcard Credential
	<u>@mil</u> @mil
	<u>O</u> K <u>C</u> ancel

c. Enter PIN.

Screen displays the Zero Client login image.

→	Citrix Receiver Ayuhara Jacoferica Con Bactour	Bir I	Log on Please exter your POI	
			b	CO GISTICS



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

Screen displays the Zero Client login desktop options.



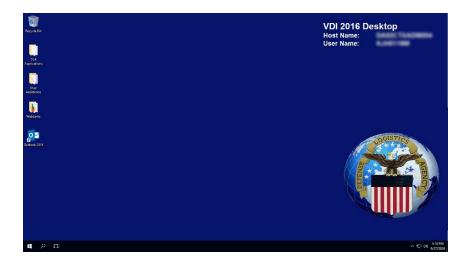
e. Select OK.

Screen displays the US Department of Defense Warning Statement.

DoD Notice and Consent Banner	
You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS) you corsent to the following conditions:	
-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network	
operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.	
 At any time, the USG may inspect and seize data stored on this IS. Communications using, or data stored on, this IS are not private, are subject to routine 	
monitoring, interception, and search, and may be disclosed or used for any USG- authorized purpose.	
-This IS includes security measures (e.g., authentication and access controls) to protect USG interestsnot for your personal benefit or privacy.	
 Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys. 	
work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.	



The Virtual Desktop is ready to use, just as you would use a traditional desktop. *Screen displays the Virtual Desktop.*





123 3.6 Zero Client Sign Out Instructions

I. Sign Out of 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.

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

Screen displays the Virtual Desktop.





b. Select the **Sign Out** button (within Virtual Desktop session).

Screen displays the Virtual Desktop with sign out button.

Most used Common UNities Sopping Tool	
Actical Conference on the series of the seri	

II. 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:**

- Select Keystrokes <CTRL>+<ALT>+ → Select Lock → Pull CAC.
- Right click on **<Windows>**, Select **<Shutdown or sign out>** → Select **<Disconnect>** → Pull CAC.
- 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:

- a. Ensure CAC is inserted into CAC Reader.
- b. Open Internet Explorer and select Email Certificate.

Screen displays Internet Explorer – Windows Security.

Conternet Explorer				()	
	Windows Security		×		
	Select a Certificate				
	Site dladirect.dla.mil needs you	r credentials:			
	Signature -	10. 10. 100 Test			
	Issuer: DOD EMAIL CA	-44			
	Valid From:	No. 22780-20198			
	Click here to view cert	ificate properties			
	More choices				
1	ОК	Cancel			

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

Screen displays Internet Explorer with address bar.





d. Choose the DOD EMAIL certificate and Select OK.

Screen displays the Virtual Desktop Certificate Options.



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

Screen displays the Virtual Desktop options.



f. Select OK.

Screen displays the US Department of Defense Warning Statement.





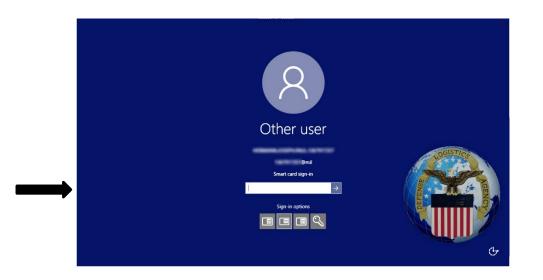
g. Select the **Smart Cart Login** as the CAC is being read. Do not navigate away from this window until the login process is complete. Doing so may result in your session being timed out.

Screen displays the Virtual Desktop – Citrix Receiver requesting the user to select the Smart Cart Login option.

O ther user	
 User name Password → Sign in to: How do I sign in to another domain? Sign-in options Image: Comparison options	er.

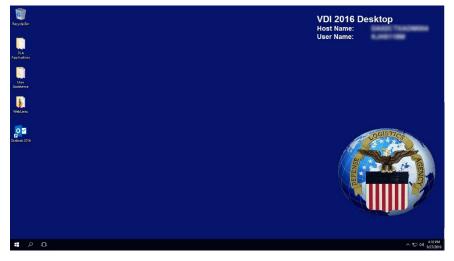
h. Enter **PIN**.

Screen displays the Virtual Desktop – Citrix Receiver requesting the user to enter their PIN.





The Virtual Desktop is ready to use, just as you would use a traditional desktop. *Screen displays the Virtual Desktop.*



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

Screen displays the XenDesktop Toolbar drop-down option.



4.6 Laptop/Desktop (GFE) Sign Out Instructions

Sign out of the Virtual Desktop using the steps below:

I. 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.



a. Select the *Windows* button in the lower left-hand corner of the screen. Screen displays the Virtual Desktop.

	seyde En Dig Splatere	VDI 2016 Desktop Host Name: User Name:
· ·		
	ु ड सरस 336	
	۵ A 🗈	ヘ 駅 (4)) 4 10 PM 9/27/2019

b. Select the Sign Out button.

Screen displays the Virtual Desktop.

Regele Bon DLA			
x X	Word 2016 Excel 2016 Excel 2016 Event: Viewer	Common Internet Explores	•
Change accor	Access 2016	Celculator	Settings
Sign out	AFCHIJTE ESH AEHocGov Azenzy		
0 • •	Prover D	*	

II. 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:**

- Select Keystrokes <CTRL>+<ALT>+ → Select Lock → Pull CAC
- From the XenDesktop toolbar at the top of the VDI session, Select Ctrl+Alt+Del
 → Select Lock this computer → Pull CAC



• 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

<u>Risks</u>

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.

Help Desk Support

All liability for issues and troubleshooting non-GFE is the responsibility of the equipment owner. The DLA Enterprise Help 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 Help 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 on Windows XP, Windows Vista, Windows 7, Windows 8/8.1, or 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
Windows 10 64-bit Editions	
Windows 8.1 64-bit Editions	Internet Explorer 11.x
Windows 8.1 32-bit Editions	
Window s 7 64-bit Editions Window s 7 32-bit Editions	
Window s 10 64-bit Editions	Microsoft Edge 15.x
Windows 10 64-bit Editions	
Windows 8.1 64-bit Editions	Mozilla Firefox 56.x
Windows 8.1 32-bit Editions	
Window s 7 64-bit Editions Window s 7 32-bit Editions	



Before connecting to the Virtual Desktop for the first time, certificates and client software will need to be installed. These are available on the DLA Enterprise Remote Access login page: https://remote.dla.mil.

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.

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

Screen displays the expanded Tools options in Internet Explorer.

C > C https://www.google.com/	D + B C G coogie ×	
		Print File Zoom (125%) Safety
		Add sile to Start menu View dominoads Ctrl+J Manager add enn 112 Developer Tools Gio to primed silen Compatibility View schargs
	Google	Report website problems tremet options About Internet Explorer
	1	
	Google Search I'm Feeling Lucky	
Advertising Business About		Privacy Terms Settings



e. When the Internet Options window appears select the **Advanced** tab and ensure **Use TLS 1.0, TLS 1.1, and TLS 1.2** are checked in the Security section. Select **OK**, then close the internet browser, and open a new internet browser window.

Screen displays the Advanced tab within the Internet Explorer Internet Options settings.

	Internet Options
	General Security Privacy Content Grand grams Advanced Settings Chable Integrated Windows Authentication* Chable SmartScreen Filter Enable SmartScreen Filter Send Do Not Track requests to sites you visit in Internet E Use SSL 2.0 Use SSL 3.0
	Use TLS 1.0 ✓ Use TLS 1.1 ✓ Use TLS 1.2 ✓ Warn about certificate address mismatch* Warn if changing between secure and not secure mode ✓ Warn if POST submittal is redirected to a zone that does n
	*Takes effect after you restart your computer
	Restore advanced settings
	Reset Internet Explorer settings
	Resets Internet Explorer's settings to their default Reset
	You should only use this if your browser is in an unusable state.
	Some <u>settings</u> are managed by your system administrator.
━	OK Cancel Apply

f. Insert CAC into CAC Reader.

 g. In the internet browser, navigate to DLA Enterprise Remote Access https://remote.dla.mil/ to access the files to download you will need to use remote access. If this is the first time you are navigating to this page, you may see a warning message similar to the website below. If this appears, select Continue to this Web site (not recommended).

Screen displays the Security Certificate Warning requesting the user to close this webpage or continue to this webpage.

(Θ)	thtps://remote.dla.mil/	ଳ ମ ଜ ନ ଜ
*		🦉 🔹 🔂 🔹 🖾 🗰 💌 Page 🔹 Safety 🕶 Tools 🕶 🔞 🖛
8	There is a problem with this website's security certificate.	
	The security certificate presented by this website was issued for a different website's address.	
	Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.	
	We recommend that you close this webpage and do not continue to this website.	
	Ø Click here to close this webpage.	
	Solution to this website (not recommended).	
	More information	



h. Select the I Agree with the Statements Above button.

Screen displays the DLA Enterprise Remote Access Webpage requesting user to accept the use of a U.S Government (USG) Information System (IS).



i. 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.

Screen displays the DLA Enterprise Remote Access Webpage outlining the required software installs.





- j. Download DOD Root Certificates.
 - Select DOD Root Certificates for Windows.

Note: This will install required DOD Certificates to the appropriate location on your machine. These certificates are required to be installed on a machine when using a CAC.

- Select Run when prompted.
- Windows Install Procedures:
 - o Select Next.



 $\circ~$ Select Next.

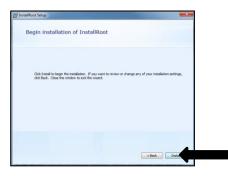
InstaliRoot Setup	
Choose a file location	
To install in this fielder, dick 'Next'. To install to a different fielder,	, enter it below or dick "Browse".
C: Users' yegan.newman(AppData)Roaming'Dc0-HE'UnstalRoot	<\ Browse
	< Back Next >

• Select Next.

InstallRoot Features Seect the features you with to initial. If Complexial Interface Command Line Tool
(9) Graphical Interface
Command Line Tool
< Box Next >



o Select Install.



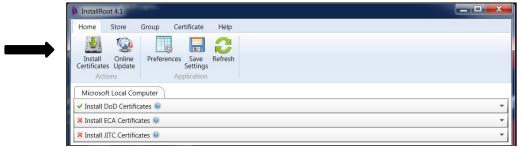
o Select Run InstallRoot.



- A tutorial may open *close / exit that window.*
- Select **Restart as Administrator.**

InstallRoot 4.1			
Home Store	Group Certificate	Help	
U		2 🗣	
Install Onlin Certificates Upda Actions	e Setting	Refresh Restart as Administrator	
Microsoft Currer		Sication	
✓ Install DoD Cert	ificates 🕑		-
🗙 Install ECA Cert	ficates 🥑		-
X Install JITC Cert	ficates 😟		•

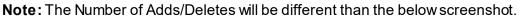
- o Select Yes to the User Account Control prompt.
- Select Install Certificate.



Virtual Desktop User Guide



Select OK.



DoD (47)		
Target Certificate Store	Adds	Deletes
Microsoft Local Computer	0	0
Microsoft Local Computer		

• Select Save Settings.

MinstallRoot 4.	1			
Home Sto	ore Group	Certificate	Help	
Home Sto	Q .		2	
Certificates Up	pdate Prefere	Settings	Refresh	
Actions Microsoft Loo	cal Computer	Application		
Microsoft Loo Install DoD Install ECA C				•
X Install ECA C	Certificates 🕝			•
X Install JITC C	Certificates 😨			•

◦ Select X.



- k. On the same page, download the *Citrix Receiver*. The Citrix Receiver is required to establish a secure connection with Citrix. This client supports Windows XP, Vista, and Windows 7/8/8.1 operating systems.
 - Select Windows Citrix Receiver.
 - When prompted, select **Run** and accept all defaults.



- I. **Optional** Download ActivIdentity ActivClient request the latest version of ActivClient the DLA Enterprise Help Desk (EHD). 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**.

Screen displays the Computer Drives and the properties of the Computer.

⊳ 🚖 Favorites	Hard Disk Dr			
 Generation Generation Generation Generation Generation Generation 	nents 🍯 149 GE			
> ∰ OS > ¶ Netw	Collapse Manage Open in new window Map network drive			
	Disconnect network drive Add a network location	urefederal.com Me pre(TM) i5-24	mory: 4.00 GB	

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.

Screen displays the properties of the Computer.

Control Panel +	System and Security + System		4 Search Control Ponel
Control Panel Home	View basic information	about your computer	
S Device Manager	Windows edition		
Remote settings	Windows 7 Enterprise		
System protection		oft Corporation. All rights reserved.	
Advanced system settings	Service Pack 1	a corporation. An ognis reserves.	
	System		
	Manufacturer	to compare fragment fragments	
	Model	Win7 April 2013	
	Rating:	5,8 Windows Experience Index	
	Processon	Intel(R) Core(TM) 3-2410M CPU @ 2.30GHz 2.30 GHz	
	Installed memory (RAM):	4.00 GB (3.90 GB usable)	
	System type:	64-bit Operating System	
See also.	Pen and Touch:	No Pen or Touch Input is available for this Display	
Action Center	Annalysis Colored Street of		
Windows Update	Research to the local data	1.000.001.000	
Performance Information and Tools	Transmiss.		



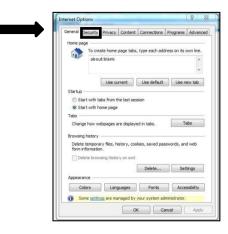
- m. Update Trusted Sites.
 - Open Internet Explorer.
 - Select **Tools** and then **InternetOptions**.

Screen displays the location of Internet Options.

Certification Control	・ C 🧐 Blank Page 🛛 🗙	
		Print
		File
		Zoom (100%)
		Safety
		Add site to Start menu
		View downloads
		Manage add-ons
		F12 Developer Tools
		Go to pinned sites
		Compatibility View sett
		Internet options
		About Internet Explorer

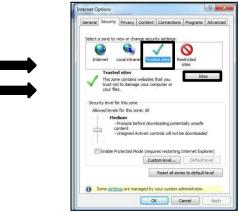
n. Select the Security tab.

Screen displays the Internet Options Security Tab.



o. Select the Trusted Sites and select Sites.

Screen displays the Internet Options - Security Tab.





p. Enter https://*.dla.mil ("*" asterisk; followed by a "." Period; then "dla.mil") Select Add and Close.

Screen displays the Trusted Sites.

Frusted sites	Constant Property -
this zone will use the zone's	ebsites from this zone. All website security settings.
Add this website to the zone:	C
https://*.dla.mil	Add
Websites:	
	Remove
Require server verification (https	::) for all sites in this zone
	112
	Close

q. Select Apply and OK.

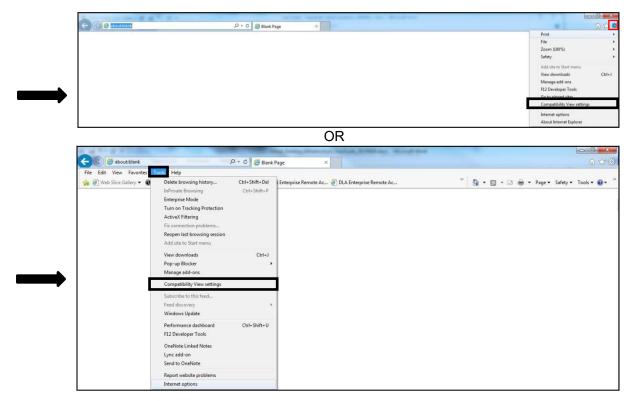
Screen displays the Internet Options – Security.

Enable Protected Mode (requires restarting Internet Explorer Custom level) Default leve	Internet Image: A set of the set of	General	Security	Privacy	Content	Connect	ions Pro	grams A
Stes Trusted sites Trusted sites Trustone contains websites that you trustone to damage your computure or your files. To have veloates in this zone. Security level for this zone Custom server Custom server Custom server To use the recommended settings, dick Default level Enable Protected Mode (requires restarting Internet Explore Custom level	Stes Trusted sites Trusted sites Trustone contains websites that you trustore domage your computer wor files. The contains of the contains of the contains The contains sites in this zone. Security level for this zone Contains sites Contains sites Contains	Select	a zone to	view or cha	nge secur	ity setting	s.	
Stes Trusted sites Trustone contains websites that you trustone to damage your computer your files. To have veloates in this zone. Security level for this zone Custom Custom security Custom security To use the recommended settings, click Default level To use the recommended settings. To use	Stes Trusted sites Trustone contains websites that you trustone to damage your compare wor files. The contains your compare The contains site of the zone Contains site of the zone Contains site of the contains Contains site of the containsin site of the contains Contains site of the contains Cont		2	L			0)
This cone contains websites that you by the tota damage your computer or your files. To have websites in this zone. Security level for this zone Cattom settings. Cattom settings. December 2015 To use the recommended settings, click Default level Detaile Noteched Mode (requires restarting Internet Daplore Cattom level) Default level	This cone contains websites that you trust to do same you computer or your files. To have websites in this zone. Security level for this zone Constant Security Security Security Security Constant Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Secu	Int	ernet	Local intra	net Trust	ted sites		ed
Custom Custon settings, - To home the settings, did Custom level, - To use the recommended settings, did Default leve - To use the recommended setting, did Default leve - Custom level Default leve	Cutom Cutom settings. - To druge the settings, click Custom level. - To use the recommended settings, click Default level - To use the recommended settings, click Default level - Custom level Reset all zones to default level	~	This zor trust no your file	ne contains ot to damag	e your co	mputer or	C	Sites
Custon settings. - To change the settings, click Custon level, - To use the recommended settings, click Defaul level - To use the recommended settings intermet. Explore Custom level	Custom settings. - To charge the settings, click Custom level. - To use the recommended settings, click Default level Enable Protected Mode (recuire restarting Internet Eucliver Custom level	Secur	ity level f	for this zone				
Custom level Default leve	Custom level Default level		-	Custom sett To change To use the	the settin recommen	nded settin	ngs, click l	Default lev
	Reset all zones to default leve	07	Enable P	Protected M				
Reset all zones to default leve					Cus			
	Some settings are managed by your system administrator.					Reset all	zones to	default lev

- r. Update Compatibility View Settings.
 - Open Internet Explorer.
 - Select Tools and then Compatibility View Settings.

Screen displays the Internet Explorer Browser.





s. Enter **dla.mil**, Select **Add**, and then **Close**.

Screen displays the Internet Options – Security.

Compatibility View Settings
Change Compatibility View Settings
Add this website: dia.mi Add
Websites you've added to Compatibility View:
Remove
☑ Display intranet sites in Compatibility View
Use Microsoft compatibility lists
Learn more by reading the Internet Explorer privacy statement
contrast by reduing the <u>interfet Explorer privacy statement</u>
Close

t. 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 Internet Explorer. User will need to use the proper web browser based on the operating system installed on the machine.

- a. Insert CAC into CAC Reader.
- b. Open Internet Explorer.
- c. Enter the following URL: <u>https://remote.dla.mil/</u> (continue to step d) or <u>https://dladirect.dla.mil</u> (continue to step f).
- d. Select the I Agree With The Statements Above button.

Screen displays the DLA Enterprise Remote Access Webpage requesting user to accept the use of a U.S Government (USG) Information System (IS).

🗧 🕤 🗇 https://semote.dia.mi/	D + & C × ⊕ DtA Interprise Resource Acc ×	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
	<image/> <section-header><section-header><section-header><section-header><text><text><text><list-item><list-item><list-item></list-item></list-item></list-item></text></text></text></section-header></section-header></section-header></section-header>	



e. Select the VDI - External button.

Screen displays the DLA Enterprise Remote Access Webpage requesting user to Login.



f. Choose the DOD EMAIL certificate and Select OK.

Screen displays the Virtual Desktop Certificate Options for Win7 and Win10 OS.



g. Enter PIN.

Screen displays the PIN prompt for Win7 and Win10 OS.

ActivClient Login	ActivClient Login ?	\times
Actividentity ActivClient	ActivD* ActivClient*	
Please enter your PIN.	Please enter your PIN.	
PIN	PIN	
OK Cancel	OK	Cancel



h. Choose **DLA Standard Desktop**. DLA Standard Desktop may open automatically.

Screen displays the Virtual Desktop options available for the user.



i. Select **OK**.

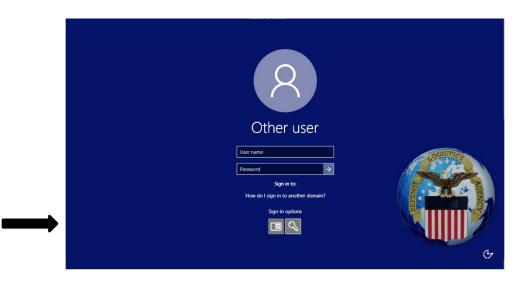
Screen displays the US Department of Defense Warning Statement.





j. Select the **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.

Screen displays the Virtual Desktop – Citrix Receiver requesting the user to select the Smart Cart Login option.



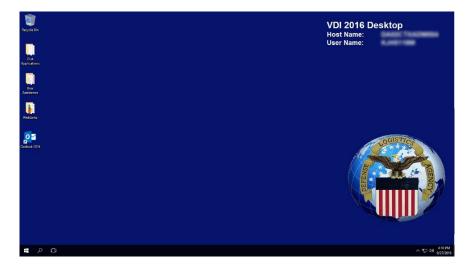
k. Enter **PIN** number.

Screen displays the Virtual Desktop – Citrix Receiver to enter PIN.

Other user
 Brail Smart card sign-in Sign-in options B B B C C



The Virtual Desktop is ready to use, just as you would use a traditional desktop. *Screen displays the Virtual Desktop.*



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

Screen displays the XenDesktop Toolbar drop-down option.





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

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

I. <u>Sign Out of the Virtual Desktop</u>

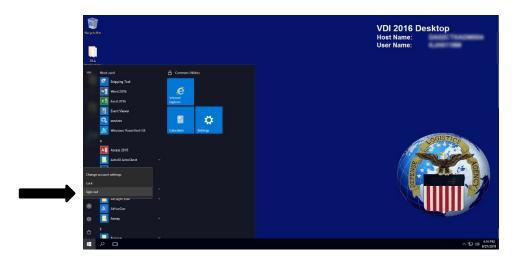
a. This sign out method will terminate your active Virtual Desktop session and you will not be able to transfer your session to another machine. Select the **Windows** button in the lower left-hand corner of your screen.

Screen displays the Virtual Desktop; user can navigate the desktop similarly to their traditional desktop.



b. Select the Sign Out button.

Screen displays the Virtual Desktop with Sign Out button.





II. 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:**

- Select Keystrokes <CTRL>+<ALT>+ → Select Lock → Pull CAC.
- From the XenDesktop toolbar at the top of the VDI session, Select Ctrl+Alt+Del → Select Lock this computer → Pull CAC.



• Select Keystrokes **<Windows> + <L> →** Pull CAC.



6.0 Appendix



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

Email: dlaenterprisehelpdesk@dla.mil Phone: (855) 352 - 0001