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:

<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>Dell Wyse 5010 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:

![Diagram showing Virtual Desktop infrastructure]

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.
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**

I. **At a Glance**

*Left Side View*  
*Front View*  
*Right Side View*

---

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><img src="image" alt="Power Cord Image" /></td>
<td>Power Cord</td>
</tr>
<tr>
<td><img src="image" alt="Docking Station Image" /></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 different instruction 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.*

![Screen displays the US Department of Defense Warning Statement.]

---

c. Insert CAC into the Smart Card Reader

*Screen displays the ThinPC Smart Card Input.*

![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. *EDIP*(10 characters)*@.mil*

*Screen displays the ThinPC PIN Input.*

![ThinPC PIN Input Screen](image)

e. Select **VDI Launcher Internal**

*Screen displays the Virtual Desktop Internal/External Login options.*

![VDI Launcher Options](image)
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.*

   ![Image of certificate selection](image)

   g. Enter **PIN**

   ![Image of PIN entry](image)

   h. Select **DLA Standard Desktop**

   *Screen displays the Citrix Receiver Desktop Options*

   ![Image of desktop options](image)
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 Card Login option*
k. Enter **PIN**.

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

![Image of screen displaying Pin request]

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

*Screen displays the Virtual Desktop.*

![Image of Virtual Desktop ready for use]
**Wireless Network (External)**

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.*

![Screen Displaying 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.*

![Screen Displaying ThinPC PIN Input]
e. Select the **Network Options** icon 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.*

![Screen displaying network security key entry window]

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

*Screen displays the network location options.*

![Screen displaying network location options]

---

**Virtual Desktop User Guide**

Last Updated February 2018
i. Select **VDI Launcher External**

*Screen displays the Virtual Desktop Internal/External Login options.*

![VDI Launcher External Screen](image)

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

![Select Certificate](image)

k. Enter **PIN**

![Enter PIN](image)
I. Select **DLA Standard Desktop**

*Screen displays the Citrix Receiver Desktop Options.*

II. Select OK.

*Screen displays the US Department of Defense Warning Statement.*

III. 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 Card Login option.*
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.*
2.6 Thin Client Log Off Instructions

I. **Log Off the Virtual Desktop**

To log off 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.

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 Log Off button (within Virtual Desktop session).

Screen displays the Virtual Desktop with log off button.

![Virtual Desktop with log off button]

![Log off button highlighted]

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

Screen displays the local machine desktop.

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>+<DEL>  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

![XenDesktop toolbar]

![Lock this computer option]
### 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**

---

**Front View**

I. **At a Glance**

- Power Button
- USB Ports
- Headphone Port

**Back View**

- Display Port
- USB Ports
- Power Adapter Port
- DVI Port
- Ethernet

---

Virtual Desktop
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><img src="image" alt="Power Cord" /></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

a. Insert Smart Card into Smart Card Reader

*Screen displays the Zero Client login image*
b. Enter **PIN**

*Screen displays the Zero Client login image*

---

![Citrix Receiver login screen](image)

---

**Note:** Desktop options shown will defer user to user

*Screen displays the Zero Client login desktop options*

---

![Desktop options](image)

---

c. Select the appropriate Virtual Desktop option

---

**Note:** Desktop options shown will defer user to user

*Screen displays the Zero Client login desktop options*

---

![Desktop options](image)

---

d. Select **OK**

*Screen displays the US Department of Defense Warning Statement.*
The Virtual Desktop is ready to use, just as you would use a traditional desktop.

*Screen displays the Virtual Desktop.*

3.6 Zero Client Log Off Instructions

I. **Log Off the Virtual Desktop**

To log off 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 **Log Off** button (within Virtual Desktop session).

*Screen displays the Virtual Desktop with log off 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>+<DEL>` → 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 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.
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

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*

![Certificate Selection](image)

- d.

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

  *Screen displays the Virtual Desktop Certificate Options*

  - ![Certificate Selection](image)

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

  *Screen displays the Virtual Desktop options*

  ![Virtual Desktop Options](image)

  - e.

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

  *Screen displays the Virtual Desktop options*

  - ![Virtual Desktop Options](image)

  f. Select **OK**.

  *Screen displays the US Department of Defense Warning Statement*

  ![Warning Statement](image)

  - f.

  Select **OK**.

  *Screen displays the US Department of Defense Warning Statement*

  - ![Warning Statement](image)
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*

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 drop-down at the top of the page and choose Home.

*Screen displays the XenDesktop Toolbar drop-down option*

---

4.6 Laptop/Desktop (GFE) Log Off Instructions

Log off of the Virtual Desktop using the steps below:

1. **Log Off 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.*

b. Select the Log Off button

*Screen displays the Virtual Desktop.*

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>+<DEL> → 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

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.

**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.

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Browser</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 10 64-bit Editions</td>
<td>Internet Explorer 11.x</td>
</tr>
<tr>
<td>Windows 8.1 64-bit Editions</td>
<td></td>
</tr>
<tr>
<td>Windows 8.1 32-bit Editions</td>
<td></td>
</tr>
<tr>
<td>Windows 7 64-bit Editions</td>
<td></td>
</tr>
<tr>
<td>Windows 7 32-bit Editions</td>
<td></td>
</tr>
<tr>
<td>Windows 10 64-bit Editions</td>
<td>Microsoft Edge 15.x</td>
</tr>
<tr>
<td>Windows 8.1 64-bit Editions</td>
<td></td>
</tr>
<tr>
<td>Windows 8.1 32-bit Editions</td>
<td></td>
</tr>
<tr>
<td>Windows 7 64-bit Editions</td>
<td></td>
</tr>
<tr>
<td>Windows 7 32-bit Editions</td>
<td>Mozilla Firefox 56.x</td>
</tr>
</tbody>
</table>
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 - From Internet Explorer, select Tools and then Internet Options.

*Screen displays the expanded Tools options in Internet Explorer.*
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.*

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.*
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).*

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

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.*

![Screen displays the DLA Enterprise Remote Access Webpage outlining the required software installs.](image)
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:
     - Select **Next**
     - Select **Next**
     - Select **Next**

- Select **Install**

  ![Install Root](image1)

- Select **Run InstallRoot**

  ![InstallRoot](image2)

  - A tutorial may open – *close / exit that window*

- Select **Restart as Administrator**

  ![Restart as Administrator](image3)

  - Select **Yes** to the User Account Control prompt

- Select **Install Certificate**

  ![Install Certificate](image4)
o Select OK

Note: The Number of Adds/Deletes will be different than the below screenshot

```
<table>
<thead>
<tr>
<th>Target Certificate Store</th>
<th>Adds</th>
<th>Deletes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Local Computer</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

o Select Save Settings

```
<!-- Image of the screen showing the save settings option -->
```

o Select X

```
<!-- Image of the screen showing the X option selected -->
```

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

Optional: Download ActivIdentity ActivClient – request the latest version of ActivClient from 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*

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

   Screen displays the location of Internet Options

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.*

q. Select **Apply** and **OK**.

*Screen displays the Internet Options – Security*

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*

![Image of Internet Options]

1. 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: https://remote.dla.mil/ (continue to step d) or https://dladirect.dla.mil (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)
e. Select the **VDI - External** button

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

![VDI External button](image)

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

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

![Certificate Options](image)

g. Enter **PIN**.

*Screen displays the PIN prompt for Win7 and Win10 OS*

![PIN prompt](image)
h. Choose **DLA Standard Desktop**. DLA Standard Desktop may open automatically.

*Screen displays the Virtual Desktop options available for the user*

![DLA Standard Desktop option]

---

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 your 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.*

![Smart Cart Login screen](image)

k. Enter **PIN** number

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

![PIN entry screen](image)
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.*
There are two ways to log off of the Virtual Desktop.

I. **Log Off the Virtual Desktop**

   a. This log off 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 **Log Off** button

   *Screen displays the Virtual Desktop with Log Off 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>+<DEL>` → 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

6.1 Support

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