



Citrix Home User Guide

Defense Logistics Agency

User Guide and Operational Procedures for Citrix

Version 1.20

Date: October 27, 2014

Table of Contents

1. About This Guide.....	3
1.1. Who Should Use It.....	3
2. Citrix – Introduction.....	4
2.1. Overview.....	4
2.2. Hardware and Software Required.....	4
2.3. Help Desk Support.....	5
2.4. Home Use Printing.....	6
3. Pre-connection and Configuration Activities.....	7
4. Establishing a Citrix Connection.....	13
Appendix A – Setting up Microsoft Outlook in Citrix.....	23
Appendix B – Tips and Common Error Solutions.....	28
Appendix C - Instructions for Configuring and Using Citrix with Mac OS.....	34
Appendix D – Approved Smart Card Readers.....	40
Appendix E – How to Map a Network Shared Folder.....	42
Appendix F – Instructions for Configuring and Using Citrix with Internet Explorer 11.....	44

Version History

Version	Description	Author	Date
1.7	Mac OS updates included	Damon Gatewood	June 5, 2012
1.8	Table of Contents, footers and screenshots updated to remote.dla.mil site	Kellie Clark	June 8, 2012
1.9	Additional updates	James Hasenbein	June 12, 2012
1.10	Additional updates	James Hasenbein	July 30, 2012
1.11	Updated Login Page	Gary Herchek	August 27, 2012
1.12	Rewrote Mac OS section	Valentyn Boginsky	January 18, 2013
1.13	Updated Mac OS Section	Arnaldo Garcia	February 25, 2013
1.14	Added instructions to create an Outlook Profile in Appendix A. Added Appendix F How to Map a Network Shared Folder	Gary Herchek	March 20, 2013
1.15	Removed FOUO stamp	Arnaldo Garcia	April 8, 2013
1.16	Added Appendix G (Instructions for Configuring and Using Citrix with Internet Explorer 11), added Internet Browser/OS combination to table, replaced Citrix Online Plug-in with Citrix Receiver	Gary Herchek/ Arnaldo Garcia	January 16, 2013
1.17	Updated screenshots to reflect new landing page (https://remote.dla.mil)	Serge Tare/ Arnaldo Garcia	April 30, 2014
1.18	Removed references to local printers for Home Use	Gary Herchek	May 14, 2014
1.19	Removed ActivClient from the Login Page	Arnaldo Garcia	June 5, 2014
1.20	Added Note about Receiver not functioning on Mac OS 10.10	Regan Newman	October 27, 2014

1. About This Guide

1.1. Who Should Use It

This user guide is intended to provide Defense Logistics Agency (DLA) personnel with instructions and operational procedures to connect to the DLA network via Citrix, using non-Government-Furnished Equipment (non-GFE). Non-GFE includes both Contractor-Furnished Equipment (CFE) and personal equipment (i.e., home computer).

Risks

There are potential risks associated with installing prerequisite software components (i.e., ActivClient, Citrix Receiver, DOD Root Certificates) and using the remote access system. It is not possible to test these components with all software and/or applications that are commercially available and that may be on your home computer. Therefore, it is possible that the prerequisite software components could conflict with other applications or software residing on your home computer. Use of this capability on your personal non-Government-furnished computer 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.

2. Citrix – Introduction

2.1. Overview

Citrix provides a secure means of teleworking using a remote user's personal or contractor-furnished computer. Citrix contains security configurations to prevent access to the user's local storage devices (i.e., hard drives and flash drives). Users connect to Citrix via their Web browser, enabling easy and secure access to available DLA applications as only keystrokes, mouse clicks, and display images are transmitted over an encrypted connection between the client computer and the Citrix environment.

2.2. Hardware and Software Required

Personal or contractor-furnished devices running on Windows XP, Windows Vista, Windows 7, Windows 8/8.1 or the latest versions of Mac OS can be used via the processes described in this document. The table below is a breakdown of all browser/operating system combinations that are supported by Citrix. It is highly recommended to use one of these combinations, as deviation could result in performance issues or inability to connect.

Browser	Operating system
Internet Explorer 11.x or later (32-bit mode)	Windows 8.1 64-bit Editions
	Windows 8.1 32-bit Editions
Note: Please refer to Appendix G for details	Windows 7 Service Pack 1(SP1) 64-bit Editions
	Windows 7 Service Pack 1(SP1) 32-bit Editions
Internet Explorer 10.x or later (32-bit mode)	Windows 8 64-bit Editions
	Windows 8 32-bit Editions
	Windows 7 Service Pack 1(SP1) 64-bit Editions
	Windows 7 Service Pack 1(SP1) 32-bit Editions
Internet Explorer 9.x or later (32-bit mode)	Windows 7 64-bit or higher
	Windows 7 32-bit or higher
	Windows Vista 32-bit Editions with Service Pack 2
	Windows Vista 64-bit Editions with Service Pack 2

Browser	Operating system
Internet Explorer 8.x (32-bit mode)	Windows 7 64-bit Editions Windows 7 32-bit Editions Windows XP Professional with Service Pack 3 Windows XP Professional x64 Edition with Service Pack 2 Windows Vista 32-bit Editions with Service Pack 2 Windows Vista 64-bit Editions with Service Pack 2
Safari 5.x	Mac OS X Snow Leopard 10.6
Safari 4.x	Mac OS X Leopard 10.5
Mozilla Firefox 4.x (32-bit mode)	Windows 7 64-bit Editions Windows 7 32-bit Editions Windows XP Professional with Service Pack 3 Windows XP Professional x64 Edition with Service Pack 2 Windows Vista 32-bit Editions with Service Pack 2 Windows Vista 64-bit Editions with Service Pack 2
Mozilla Firefox 3.x	Mac OS X Snow Leopard 10.6 Mac OS X Leopard 10.5 Windows XP Professional x32 Edition with Service Pack 3 Windows Vista 32-bit Editions with Service Pack 2 Windows 7 32-bit Editions Red Hat Enterprise Linux 5.4 Desktop

Additionally, there are three software components that are required in order to use Citrix - these are documented in Section 3 of this document.

Lastly, it is highly recommended that you use a high speed Internet connection, as opposed to dial-up or satellite.

2.3. Help Desk Support

All liability for issues and troubleshooting non-GFE lies with the end user. The DLA 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 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.

2.4. Home Use Printing

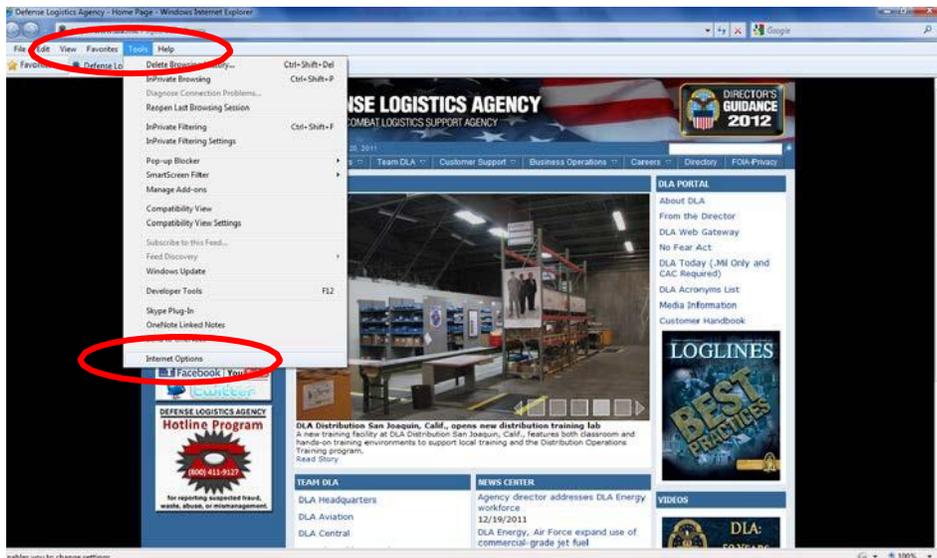
Home Use printing to your local printer is restricted by a DOD Security Policy and is therefore prohibited.

3. Pre-connection and Configuration Activities

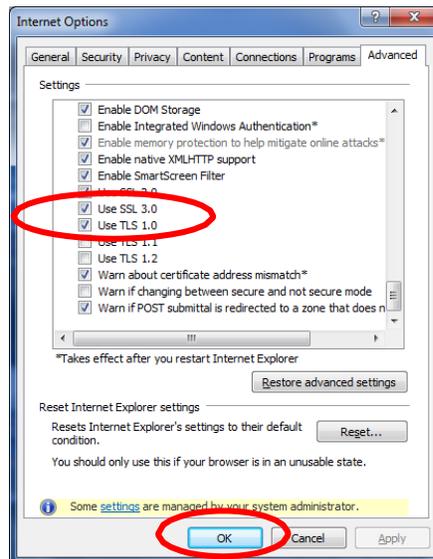
Before connecting to Citrix for the first time, certificates and client software, available on the DLA Enterprise Remote Access log-in page, need to be installed, followed by a machine reboot. This process is described in the following steps:

1. Connect your Common Access Card (CAC) Reader to an available USB Port on your Personal Computer System (Desktop/Laptop)
2. Turn on Personal Computer System (Desktop/Laptop).
3. Launch Internet Explorer V.7 or higher
4. Validate that required security protocols are enabled:

From Internet Explorer, select **Tools** and **Internet Options**



When the Internet Options window appears select the **Advanced** tab and ensure **Use SSL 3.0** and **Use TLS 1.0** are checked in the Security section.



Once these protocols are checked, click **OK**, close your Internet browser, and open a new Internet browser window.

5. Insert DLA CAC into CAC Reader
6. In your Internet browser, navigate to the DLA Enterprise Remote Access login page (URL below) to access pre- requisite files for download. Note that regardless of which DLA field site you are assigned to, everyone should obtain these files from this site.

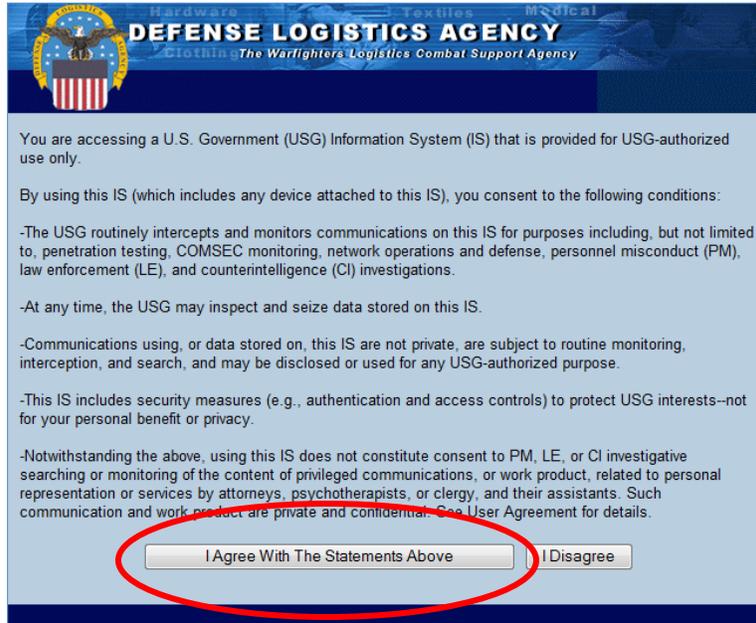
Type the following URL and click **Enter**

<https://remote.dla.mil>

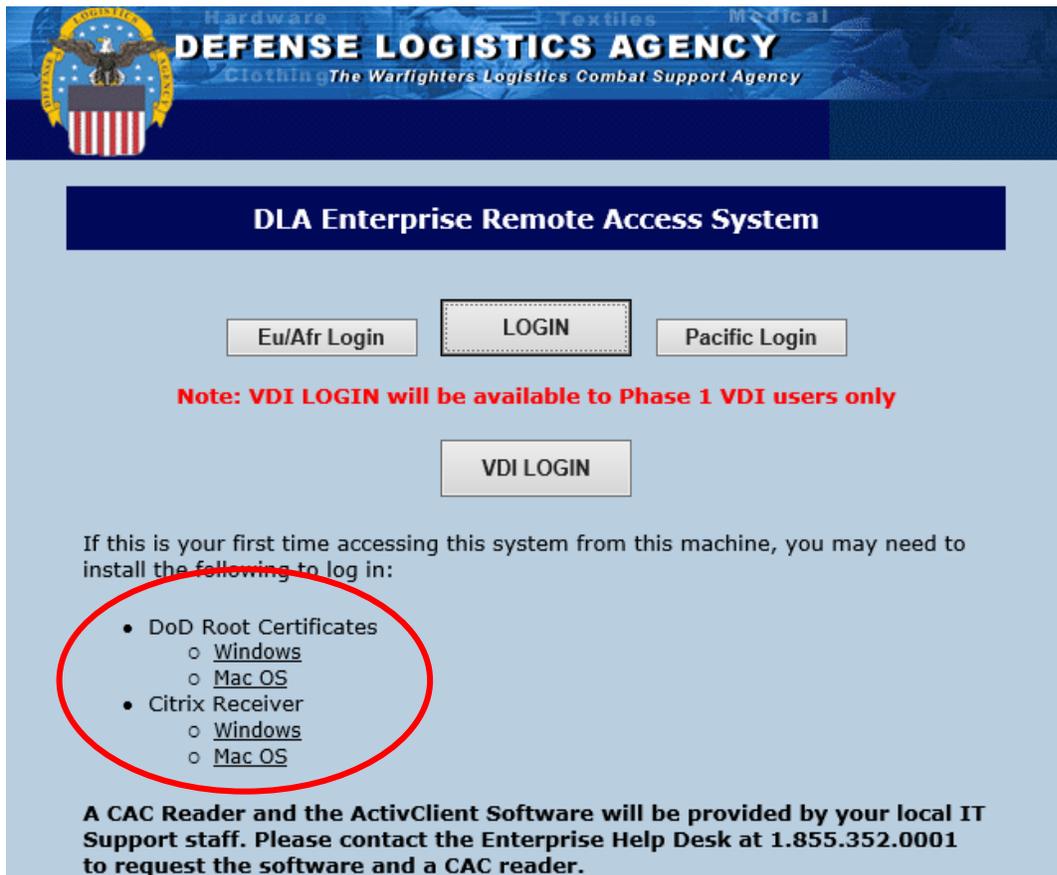
The first time navigating to this page, the user may see a warning message similar to the Web site below. If this appears, select **Continue to this Web site (not recommended)**



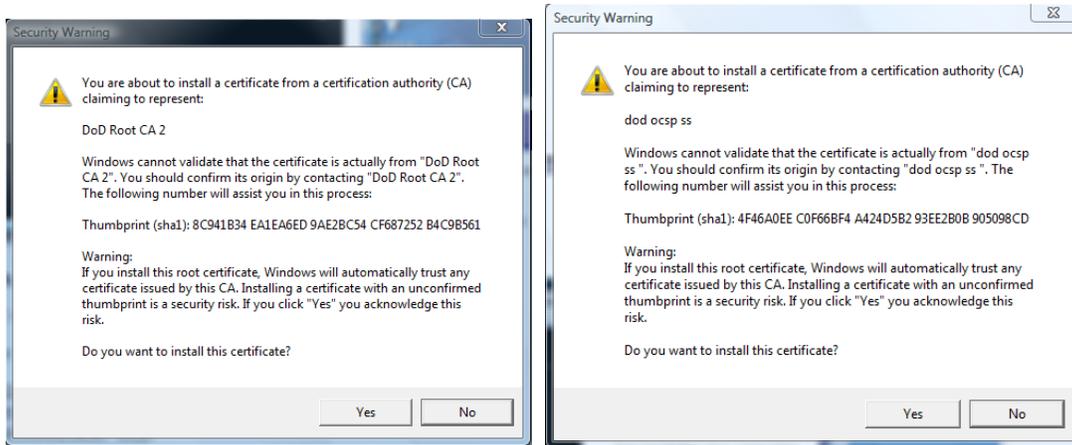
7. Select the **I Agree with the Statements Above** button



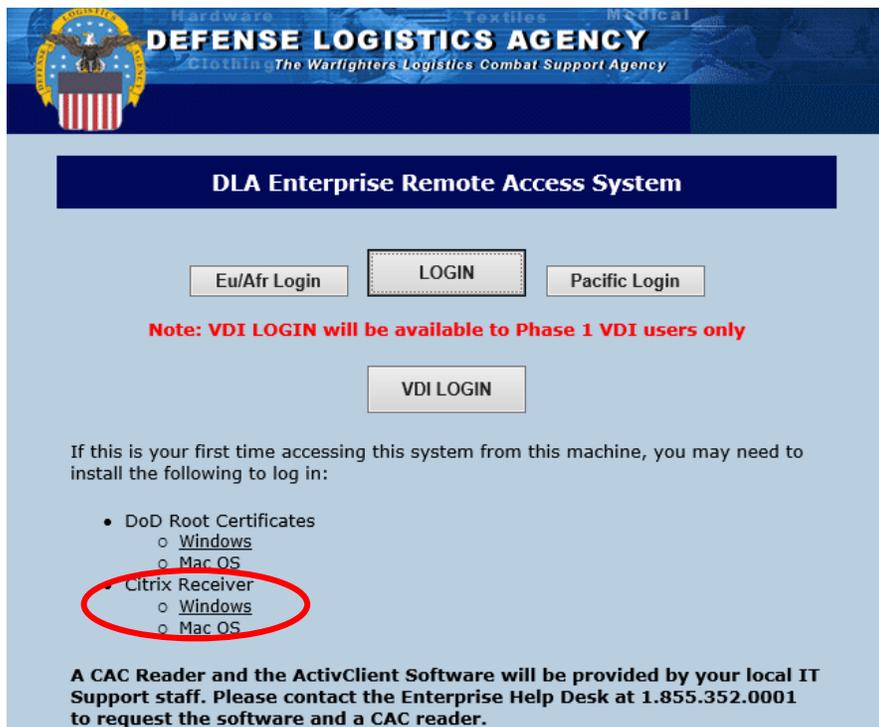
8. On the screen below you will see two links for components that need to be installed prior to establishing a connection to Citrix from each machine for the first time:



Select DOD Root Certificates -> Windows and select **Save** when prompted. Save this file to your computer, and after download is complete, locate file, right click on file, and select **Run as Administrator**. This exe file will install all required DOD Certificates to the appropriate location on your machine. These certificates are required to be installed on a machine when using a CAC. You may see two prompts issuing a security warning. These warnings are standard, and if you accept them, you should click **Yes** on both. Note that clicking **No** will prevent the machine from using Citrix.



9. On the same page, select Citrix Receiver

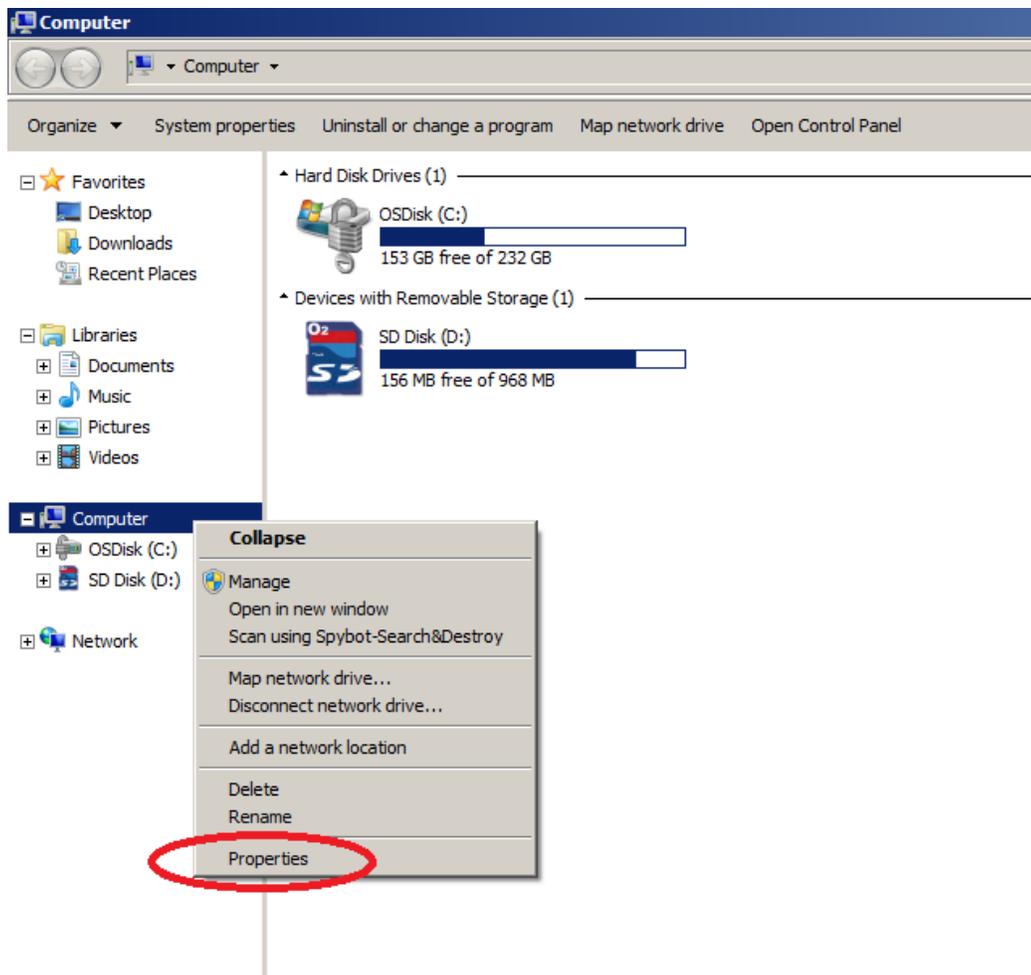


The Citrix Receiver is required to establish a secure connection with Citrix. This client supports Mac, Windows XP, Vista, Windows 7/8/8.1 operating systems. When prompted, run the file and accept all defaults.

10. Request latest version of ActivClient to your local IT Support Staff. Note there are two choices of ActivClient to install, which is based on the configuration of your operating system:

- 32-Bit
- 64-Bit

You can verify the version of your operating system by right-clicking the My Computer icon on your Desktop, and selecting Properties.



On the Screen that appears, it should state 32-bit or 64-bit Operating System.

Control Panel\System and Security\System

Control Panel > System and Security > System

Search Control Panel

Control Panel Home

- Device Manager
- Remote settings
- System protection
- Advanced system settings

View basic information about your computer

Windows edition

Windows 7 Enterprise
Copyright © 2009 Microsoft Corporation. All rights reserved.
Service Pack 1



System

Manufacturer: CIO Technology Services
Model: MPCWin7 November 2011
Rating: **5.9** Windows Experience Index
Processor: Intel(R) Core(TM) i5-2410M CPU @ 2.30GHz 2.30 GHz
Installed memory (RAM): 4.00 GB (2.00 GB usable)
System type: **64-bit Operating System**
Pen and Touch: No Pen or touch input is available for this Display

CIO Technology Services support

Website: [Online support](#)

Computer name, domain, and workgroup settings

Computer name: [Change settings](#)
Full computer name:
Computer description:
Domain:

Windows activation

Windows is activated
Product ID: [Change product key](#)

See also

- Action Center
- Windows Update
- Performance Information and Tools



Learn more online...

When prompted, run the install file and accept all defaults:



11. Reboot the computer after all prerequisite components have been installed.

4. Establishing a Citrix Connection

Note: Specific screenshots and images throughout this document may differ from site to site

The following steps detail the process for connecting to Citrix and launching applications once the prerequisite steps in Section 3 have been addressed.

1. Connect your Common Access Card (CAC) Reader to an available USB Port on your Personal Computer System (Desktop/Laptop)
2. Turn on Personal Computer System (Desktop/Laptop).
3. Launch Internet Explorer V.7 or higher
4. As an alternative to <https://remote.dla.mil>, the following URL addresses can be accessed as listed below:

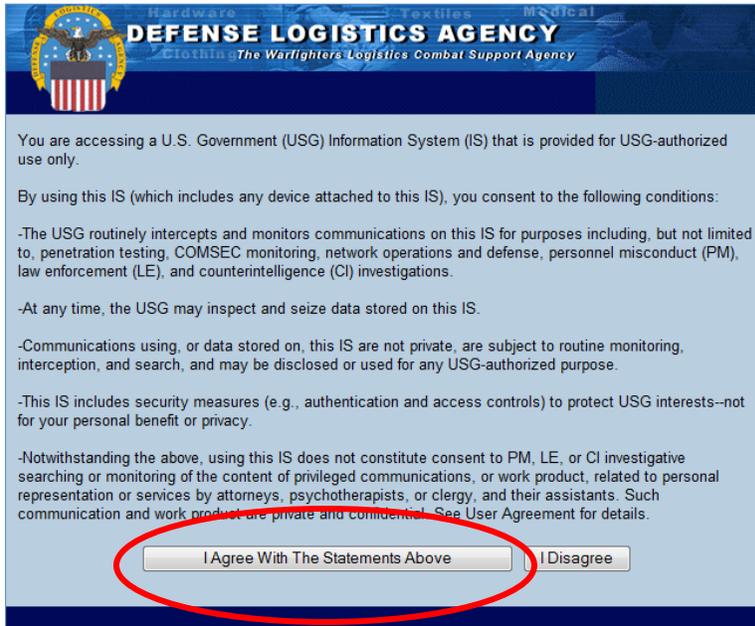
If you work at this DLA Site	Use this URL
Headquarters	https://fortbelvoir.citrix.hq.dla.mil
Aviation	https://rmt.aviation.dla.mil
Land and Maritime, Transaction Services, Logistics Information Services	https://remotec.dla.mil
Troop Support, Information Operations Ogden, Document Services	https://pubctx.troopsupport.dla.mil
Europe & Africa	https://wwc.europe.dla.mil

Pacific	https://remote.pacific.dla.mil/
Distribution	https://rmt.distribution.dla.mil Click "Continue to the Website"

Type the URL, and click **Enter**

Note: Some users may not be required to complete steps 5 and 6 due to site-specific Citrix configuration

5. Select the **I Agree With the Statements Above** button



6. Select DLA Enterprise Remote Access System location

1. For CONUS Users , Select **Login** link (Note: select the login link where you are based – which may be away from your normal location)



DEFENSE LOGISTICS AGENCY
Clothing The Warfighters Logistics Combat Support Agency

DLA Enterprise Remote Access System

Eu/Afr Login LOGIN Pacific Login

Note: VDI LOGIN will be available to Phase 1 VDI users only

VDI LOGIN

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

- DoD Root Certificates
 - [Windows](#)
 - [Mac OS](#)
- Citrix Receiver
 - [Windows](#)
 - [Mac OS](#)

A CAC Reader and the ActivClient Software will be provided by your local IT Support staff. Please contact the Enterprise Help Desk at 1.855.352.0001 to request the software and a CAC reader.

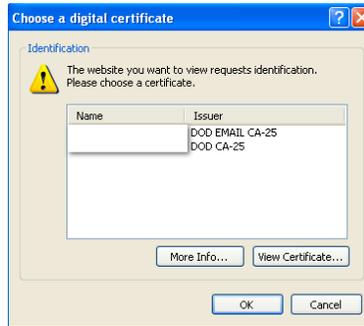
2. For OCONUS Users, Select **Eu/Afr Login** or **Pacific Login** link (Note: select the login link where you are based – which may be away from your normal location)



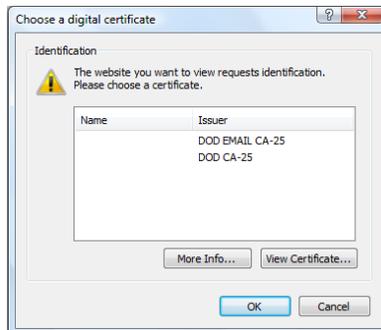
The image shows a screenshot of the DLA Enterprise Remote Access System login page. At the top left is the DLA logo featuring an eagle with wings spread, perched on a shield with the American flag colors. To the right of the logo, the text reads "DEFENSE LOGISTICS AGENCY" in large, bold, white letters, with "The Warfighters Logistics Combat Support Agency" in smaller text below it. The background of the top banner includes the words "Hardware", "Textiles", and "Medical" in a light blue font. Below the banner is a dark blue horizontal bar with the text "DLA Enterprise Remote Access System" in white. Underneath this bar are three buttons: "Eu/Afr Login", "LOGIN", and "Pacific Login". The "Eu/Afr Login" and "Pacific Login" buttons are circled in red. Below these buttons is a red note: "Note: VDI LOGIN will be available to Phase 1 VDI users only". Below the note is a button labeled "VDI LOGIN". Further down, there is a paragraph of text: "If this is your first time accessing this system from this machine, you may need to install the following to log in:". This is followed by a bulleted list: "• DoD Root Certificates" with sub-items "◦ Windows" and "◦ Mac OS"; and "• Citrix Receiver" with sub-items "◦ Windows" and "◦ Mac OS". At the bottom of the page, there is a bolded paragraph: "A CAC Reader and the ActivClient Software will be provided by your local IT Support staff. Please contact the Enterprise Help Desk at 1.855.352.0001 to request the software and a CAC reader."

7. When prompted select your **DOD EMAIL** certificate and click **OK**

Windows XP:



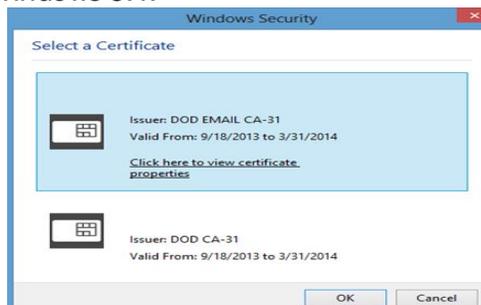
Windows Vista:



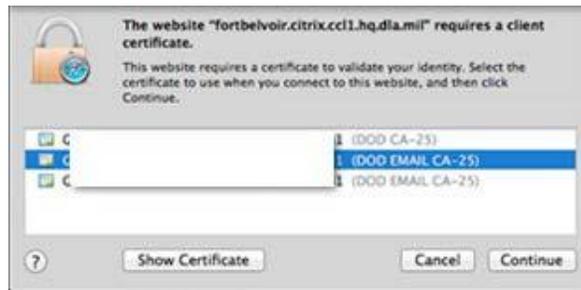
Windows 7:



Windows 8/ Windows 8.1:

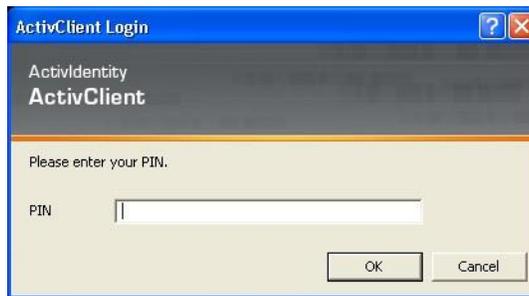


Mac OS:

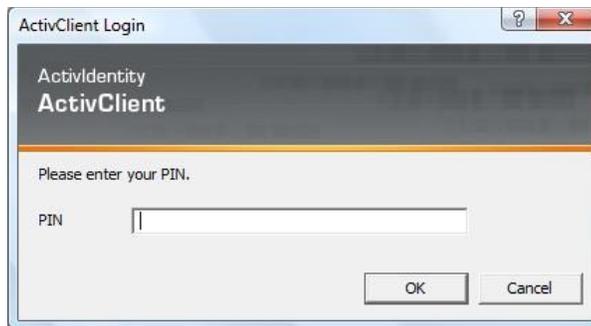


8. When prompted type your CAC

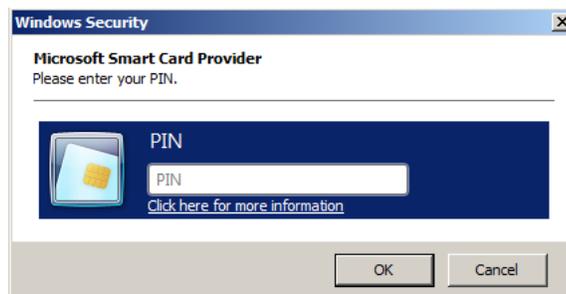
PIN: Windows XP:



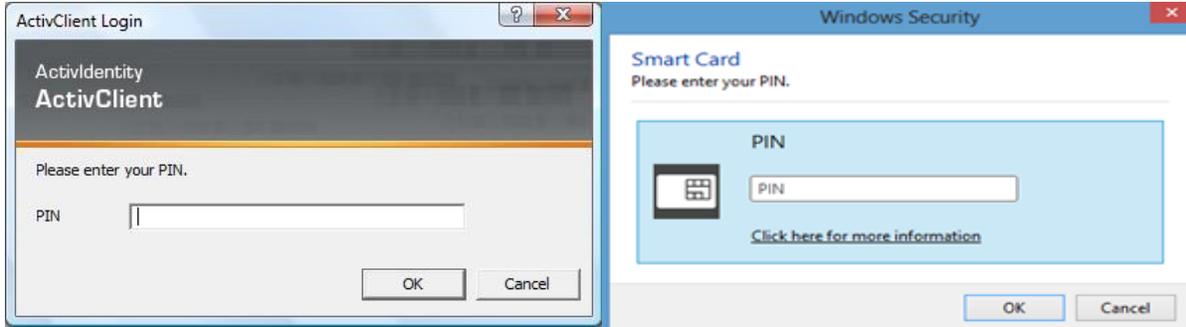
Windows Vista:



Windows 7:



Windows 8/ Windows 8.1:



Mac OS:



9. The next screen that appears will be the CITRIX Application window.

(Note: The icons you see upon logging in may differ from those shown below)



10. To launch an application, single (left) click on the icon for the program you wish to launch. When prompted, select your Certificate and enter your PIN.

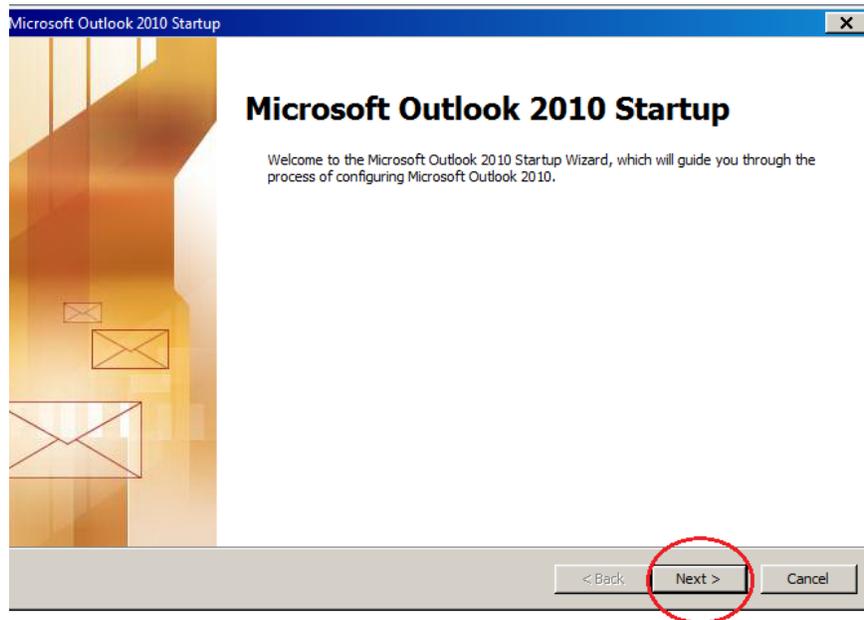
11. To Logoff, click on the **Log Off** in the upper right corner. The Web portal will log you off automatically after 20 minutes of the page being inactive. This does NOT log you out of your Citrix Session.



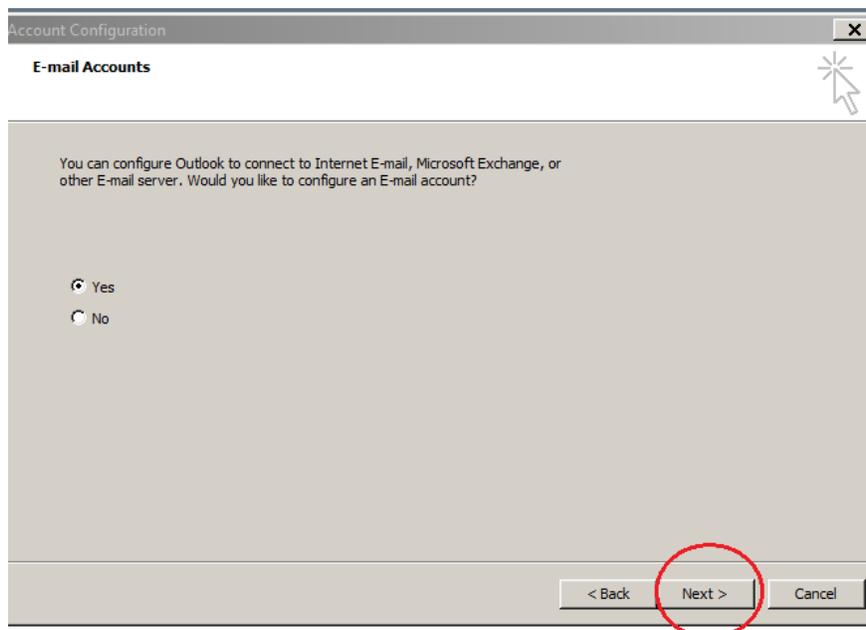
Appendix A – Setting up Microsoft Outlook in Citrix

First-time Outlook Setup

1. If, after launching Outlook, you're presented with the following message box, you will need to configure (or reconfigure) Outlook. Click Next and follow the instructions below to create all of your Outlook settings that will allow you to connect to the email server and download your mail.



2. Select Yes and click Next:



3. Select “Manually configure server settings or additional server types”. Click Next

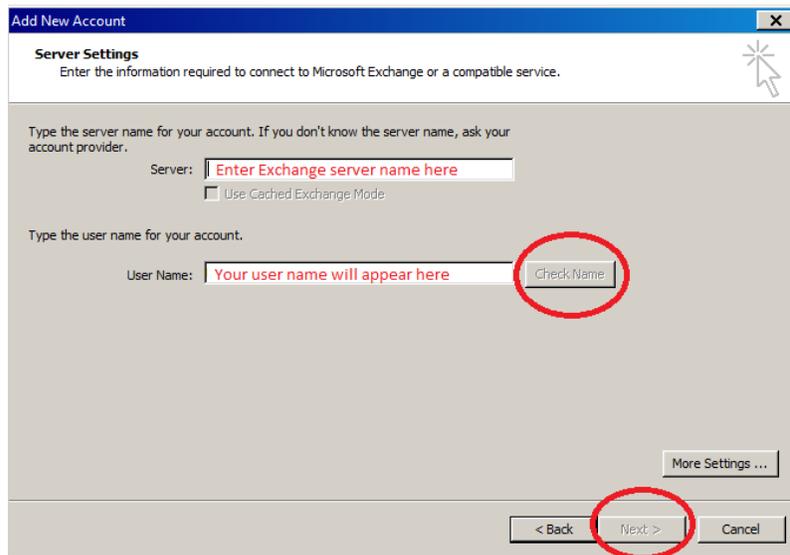
The screenshot shows the 'Add New Account' dialog box with the 'Auto Account Setup' section. The 'E-mail Account' option is selected. The 'Your Name' field contains the placeholder text 'Your name should appear here' and the 'E-mail Address' field contains 'Your email address should appear here'. The 'Manually configure server settings or additional server types' option is selected. The 'Next >' button is circled in red.

4. Select “Microsoft Exchange or compatible service”. Click Next

The screenshot shows the 'Add New Account' dialog box with the 'Choose Service' section. The 'Microsoft Exchange or compatible service' option is selected. The 'Next >' button is circled in red.

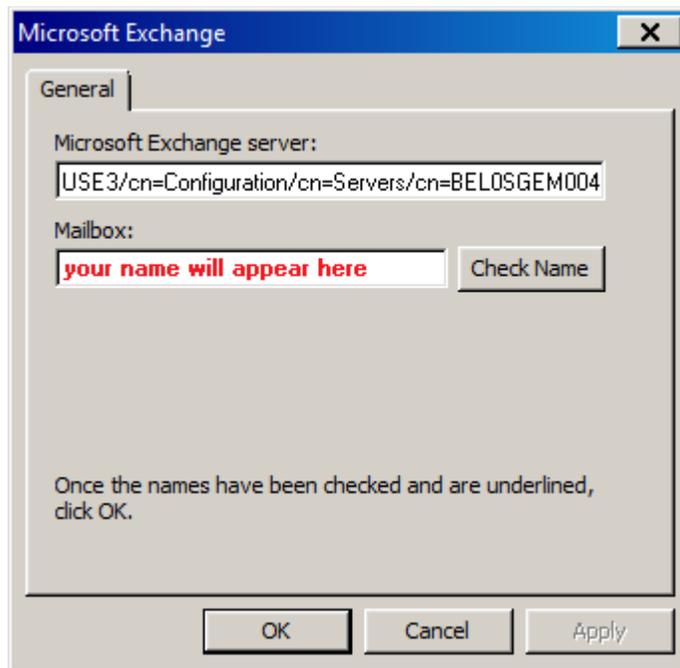
5. Your Server and User Name may (or may not) be auto-populated in the next panel of the wizard. If these values are auto-populated correctly, click Check Name.

If the server field is blank, you will need to call your Help Desk and ask them for your Exchange server name. They may need to know what DLA location you work at and possibly what domain you are associated with, if that information is available.



After you click Check Name, you should be able to click Next and move on to Step 6.

Sometimes a different window than the one shown above appears and the Server field is not initially blank and instead contains a string of text as shown here::



If you see a string of text such as this, you will need to delete all extraneous characters to the *left* of the Exchange server name, shown in **red** below.

=USE3/cn=Configuration/cn=Servers/cn=BEL0SGM004

Using the example above, the remaining text in the Server box would be:

BEL0SGM004

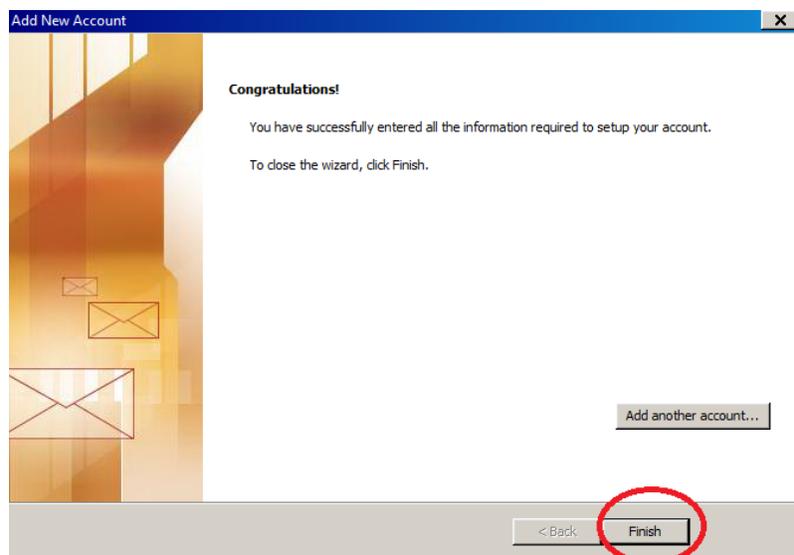
(NOTE: this is from the example, it may or may not be *your* mail server name)

Once the Exchange server name and your user name have been entered, click Check Name. After you click Check Name, the server name should be replaced with another longer string of text that may look as follows:

BEL0SGEM004.AD.DLA.MIL

You may now click OK.

6. Your Outlook Profile should now be created. Click Finished



Adding a Personal Folder (i.e., PST file) to your Outlook profile

1. Open Outlook through Citrix.
2. On the **File** menu, select **Open**, and then select **Outlook Data File**.
3. Select your U: drive from the drop-down menu.
*Distribution and J6N users select H: drive and the "outlookpst" folder.
4. Double-click the .PST file that you want to open, and then click OK (you may have to navigate through your subfolders to find the appropriate file).
5. Your .PST file should now be listed in your Outlook window.

How to add an Outlook Auto Signature to your Outlook profile

1. Open a new message. On the **Message** tab, in the **Include** group, click **Signature**, and then click **Signatures**.



2. On the **E-mail Signature** tab, click **New**.
3. Type a name for the signature, and then click **OK**.
4. In the **Edit signature** box, type the text that you want to include in the signature.
5. To format the text, select the text, and then use the style and formatting buttons to select the options that you want.
6. To add elements besides text, click where you want the element to appear, and then do any of the following:

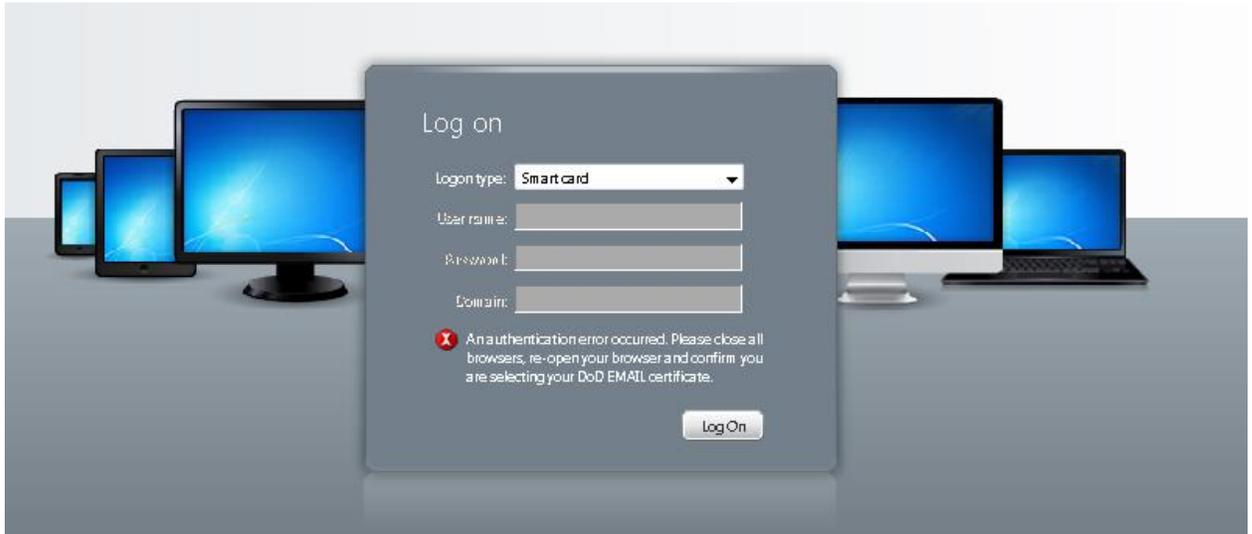
OPTIONS	HOW TO
To add an electronic business card	Click Business Card , and then click a contact in the Filed As list. Then click OK
To add a hyperlink	Click  Insert Hyperlink , type in the information or browse to a hyperlink, click to select it, and then click OK
To add a picture	Click  Picture , browse to a picture, click to select it, and then click OK . Common image file formats for pictures include .bmp, .gif, .jpg, and .png.

7. To finish creating the signature, click **OK**.

NOTE The signature that you just created or modified won't appear in the open message; it must be inserted into the message.

Appendix B – Tips and Common Error Solutions

1. If the following screen appears, preventing the user from selecting their certificate and logging in, all browser sessions should be closed. Upon logging in with a new browser session, the issue should be resolved.

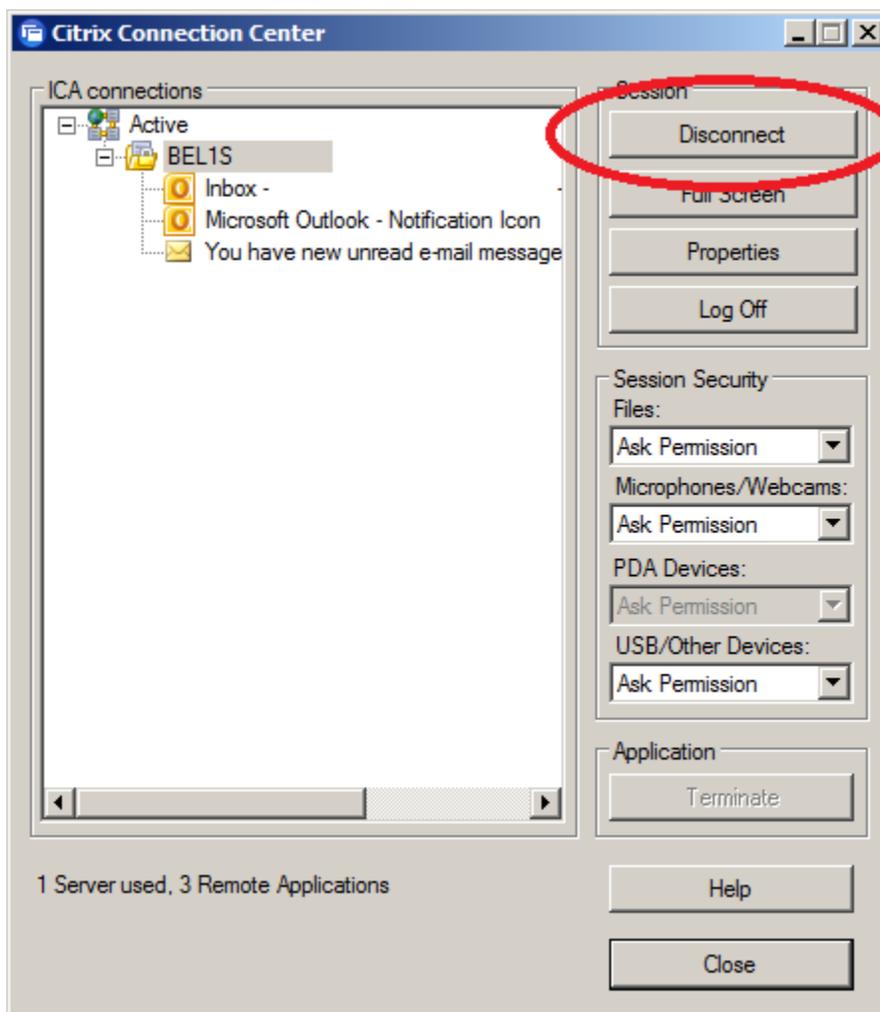


2. Occasionally in circumstances involving slow connectivity, Citrix applications may not immediately respond to attempts to launch applications. In this scenario users should refrain from repeatedly clicking the application icon as this will cause the application to 'queue up' multiple instances that will all begin launching, negatively impacting Citrix performance. If after waiting at least 30 seconds, an application does not launch or has appeared to fail during launch, then at that point click on the application's icon again as this may result in it launching properly. Users should also note that responsiveness and performance of the Citrix application should improve after the initial connection is established and the application launches.

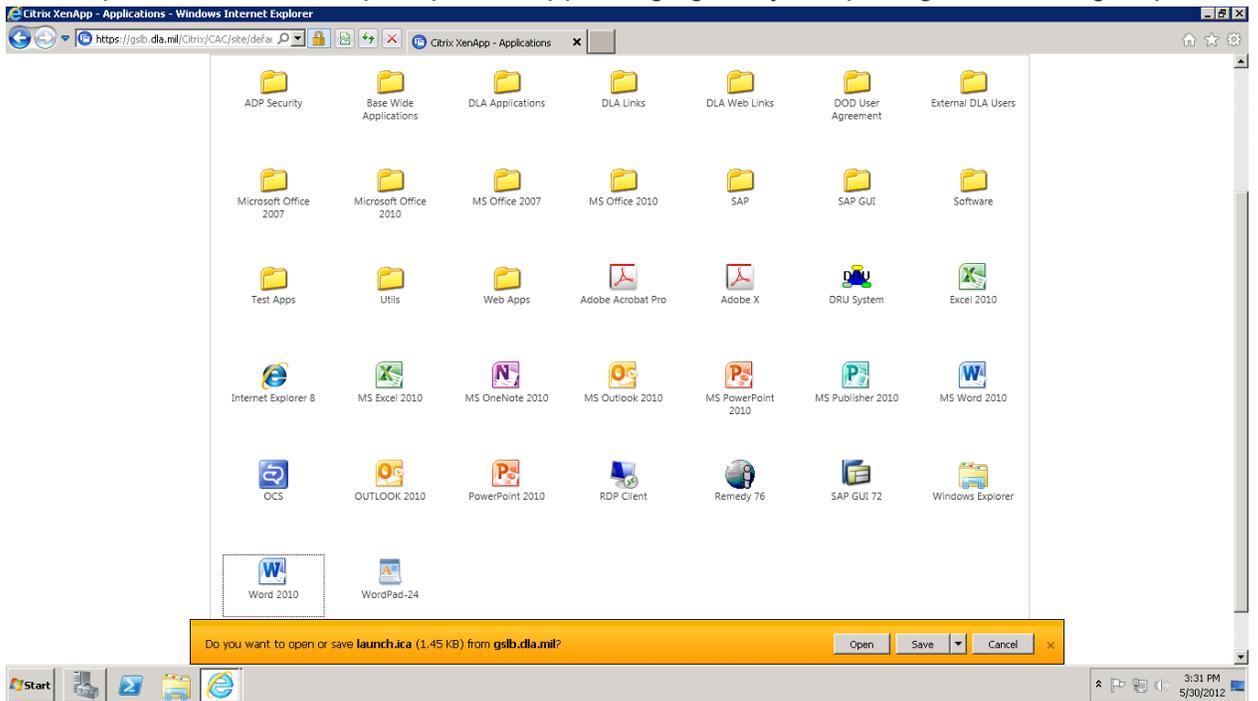
3. If you see a Windows Server account lock screen and you are no longer using Citrix, this screen can be closed by right clicking the Citrix Connection Center icon on your System Tray and selecting **Open Connection Center**.



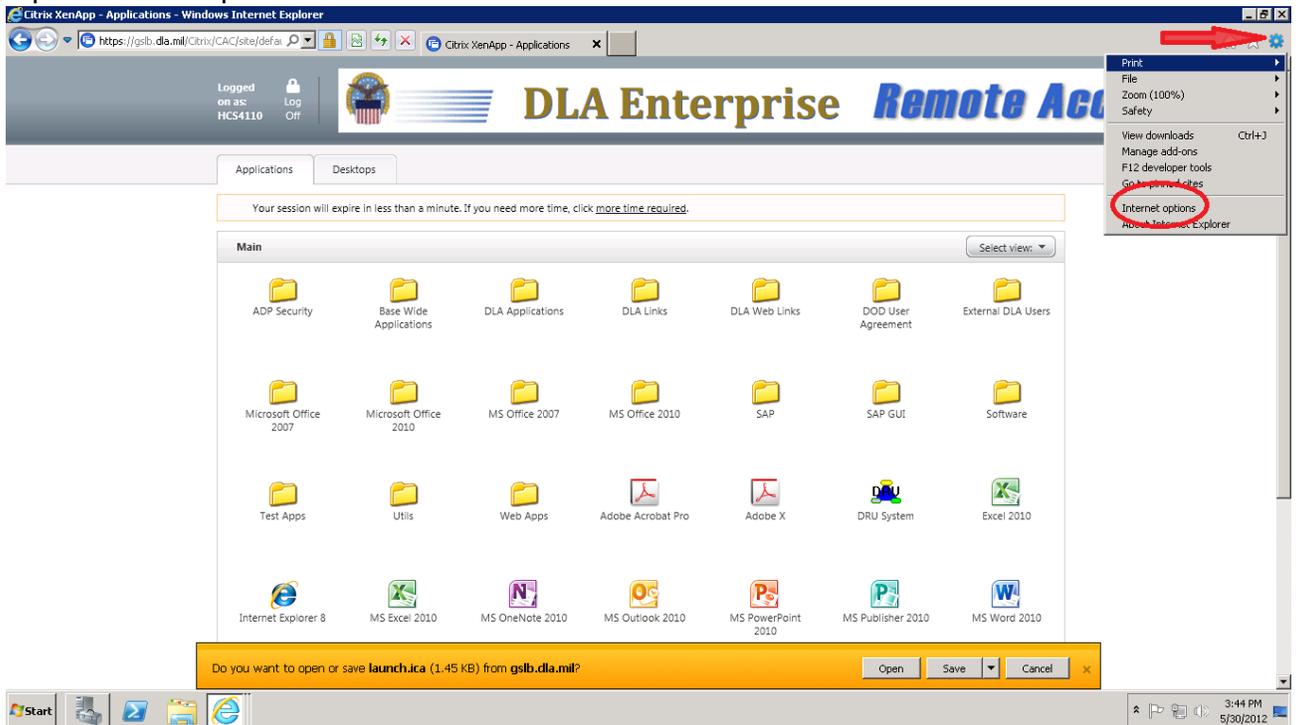
When the Citrix Connection Center Window appears, click the **Disconnect** button. This will close your Citrix session and Windows Server lock screen.



4. If you are using Internet Explorer version 9, and you receive the following prompt, you can click “Open” or remove this prompt from appearing again by completing the following steps:



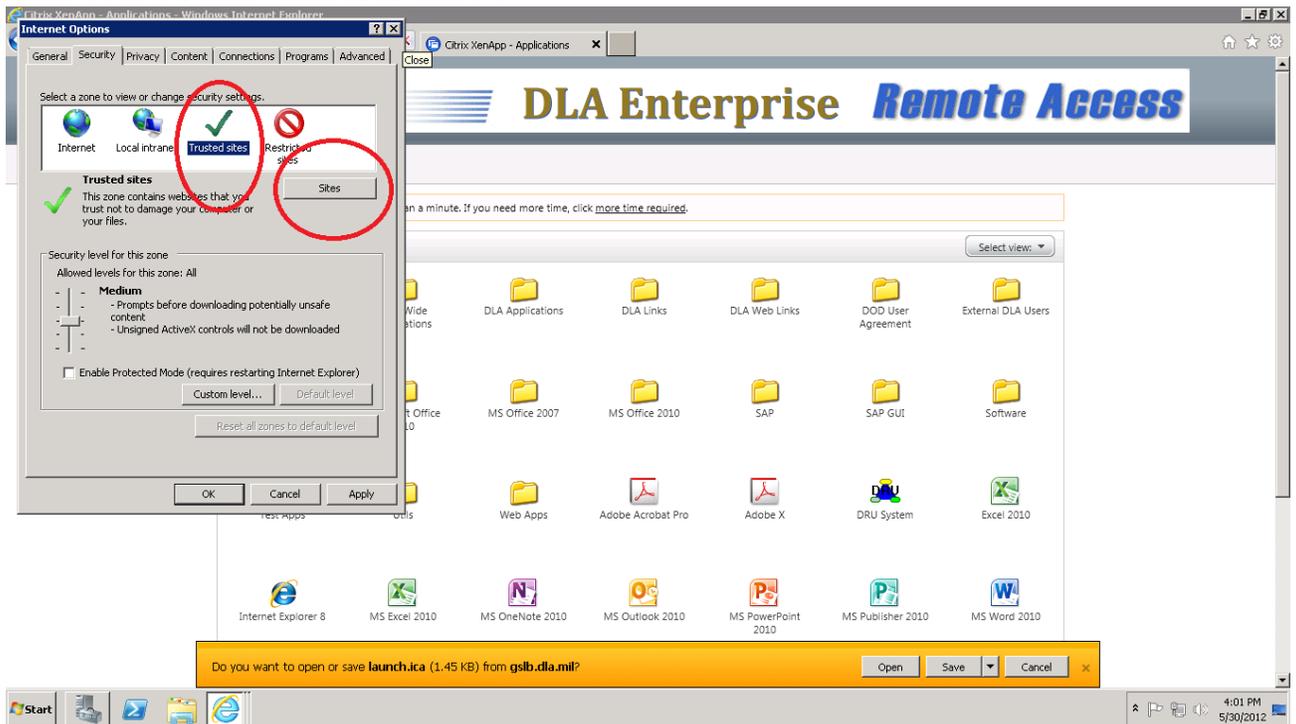
Open Internet Options:



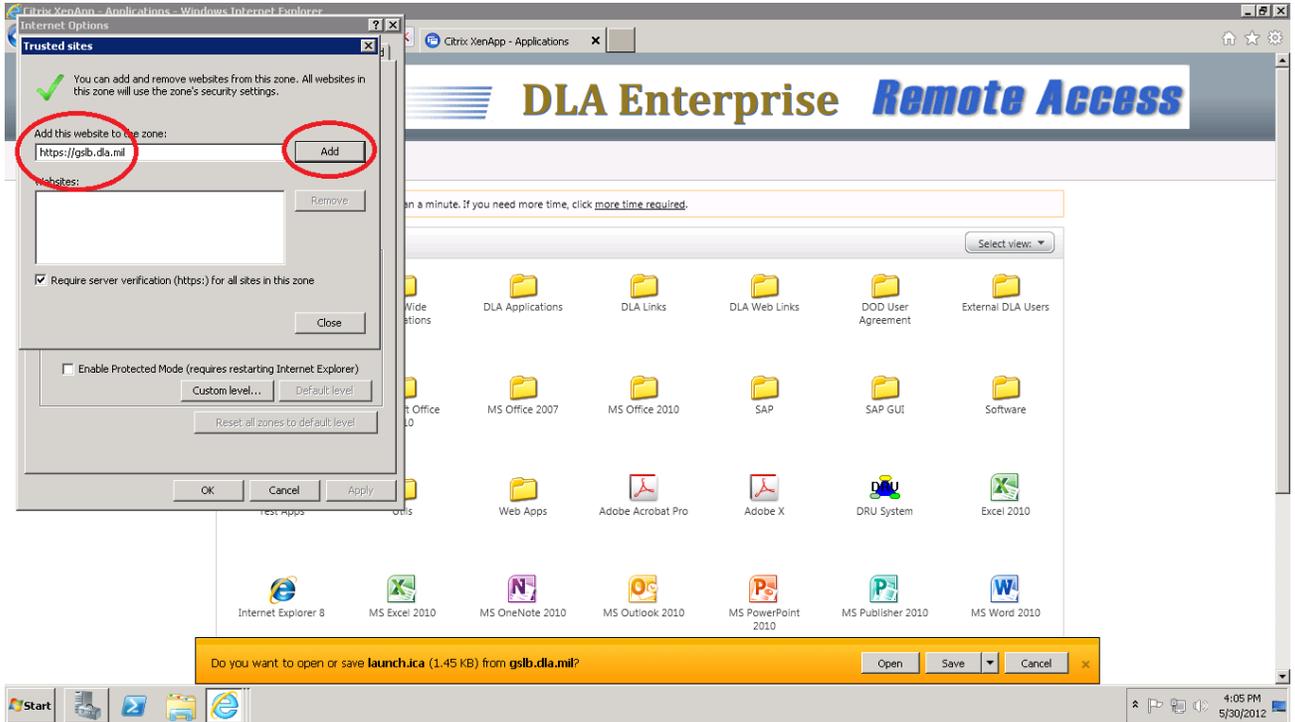
Click Security:



Click "Trusted Sites" then click "Sites":



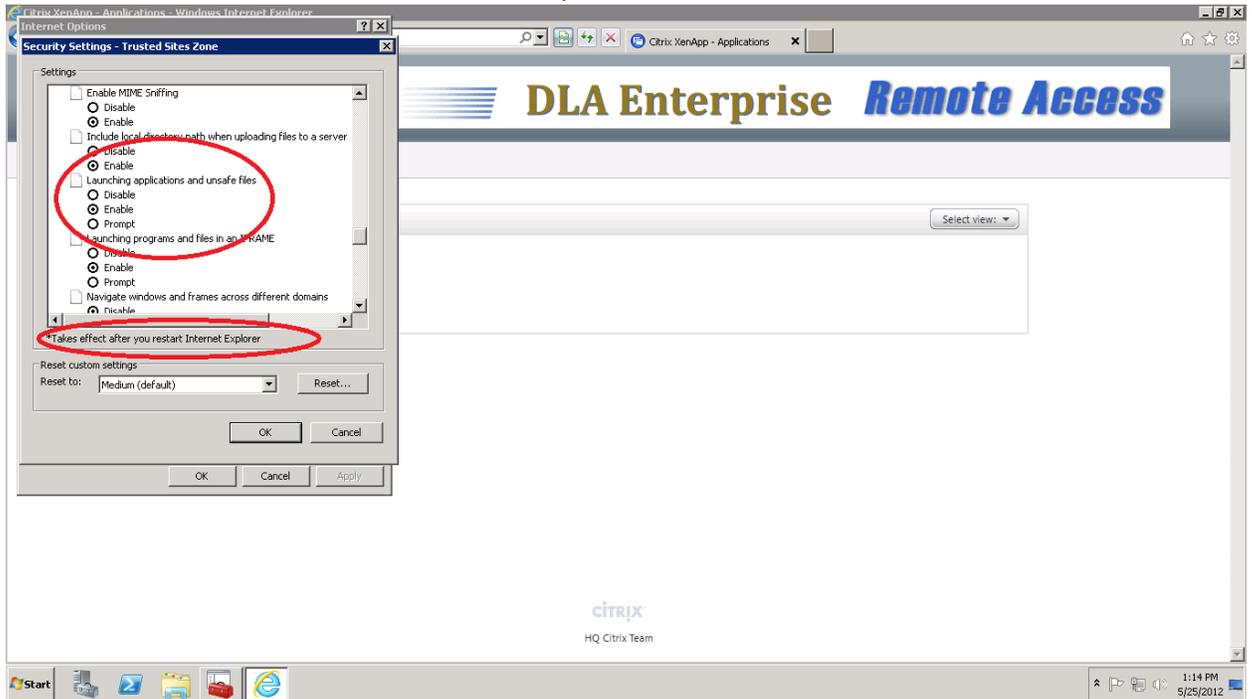
Click "Add" to add this web site then "Close":



Select "Custom Level":



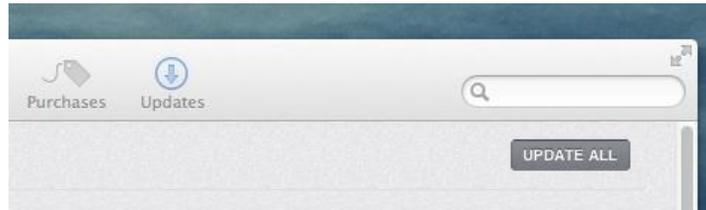
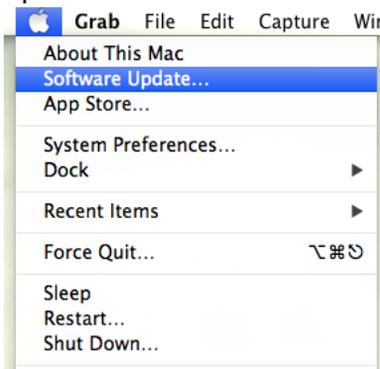
Scroll ¾ of the way down until you see “Launching applications and unsafe files”. Select “Enable”, Select “OK” and close Internet Explorer:



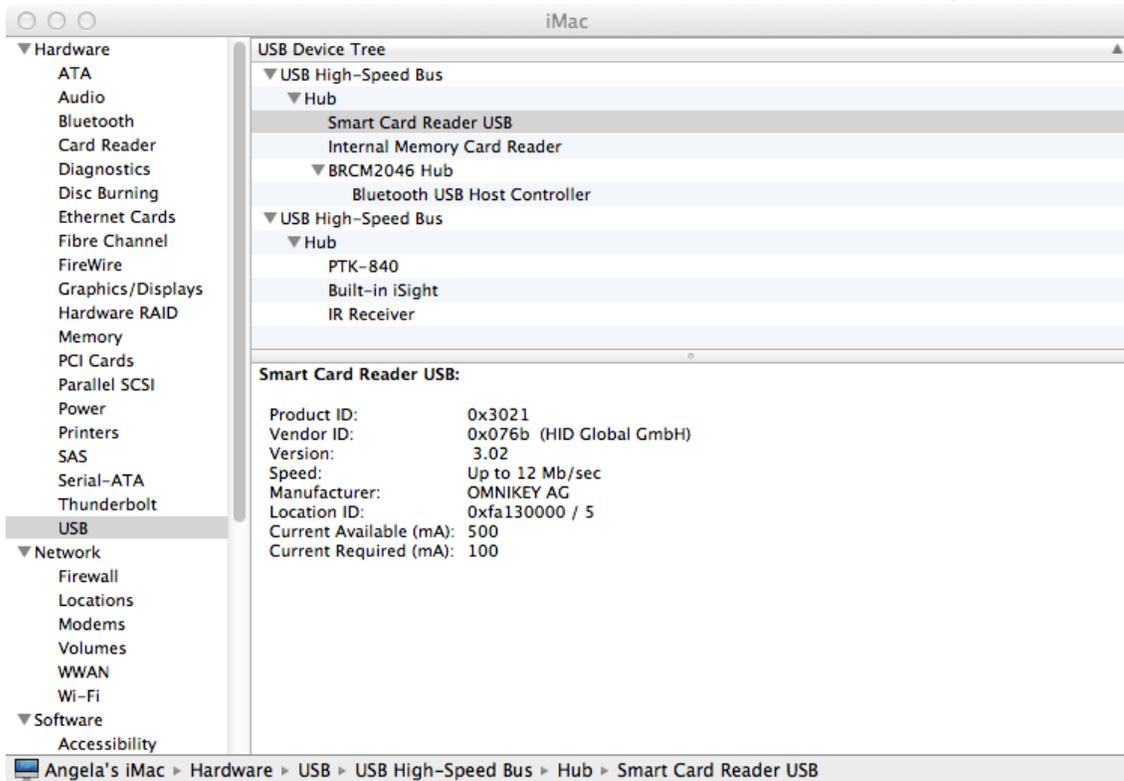
Appendix C - Instructions for Configuring and Using Citrix with Mac OS

Note: Currently, Citrix Receiver is not functioning using Mac OS 10.10, Yosemite. Citrix is working to rectify this situation and will release another version of Receiver that is compatible with Mac OS 10.10.

1. Ensure your system is updated to the latest software by navigating to the Apple icon in the upper left hand corner of the screen and select **Software Update**. Click **UPDATE ALL** if the option is available.

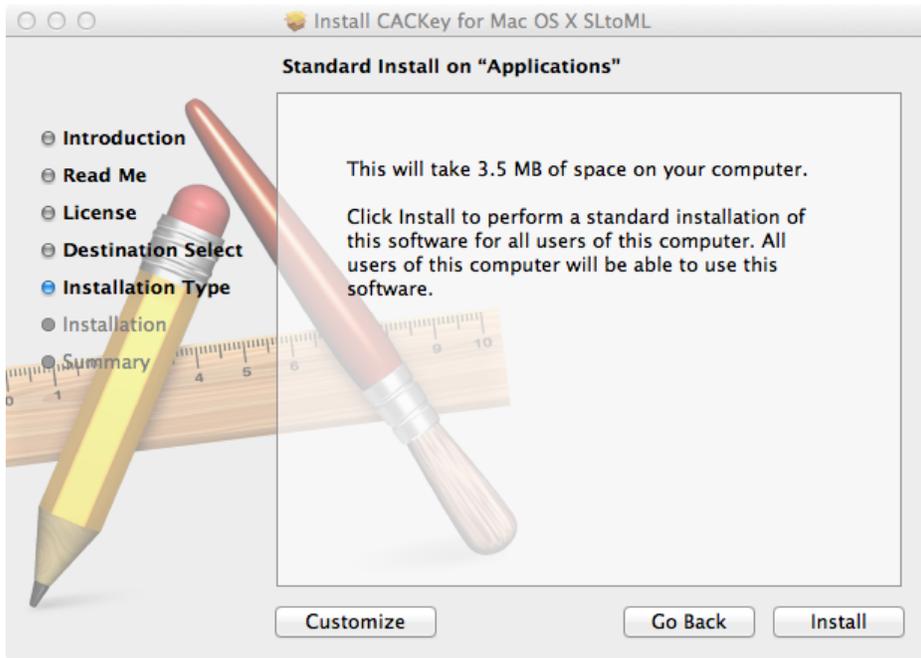


2. Plug in your CAC reader. Open Finder and navigate to **Applications** → **Utilities** → **System Profiler** (Mac OS 10.6) or System Information (Mac OS 10.7 or later versions). Select USB in the left hand pane and ensure that “Smart Card Reader” appears in the right hand pane.

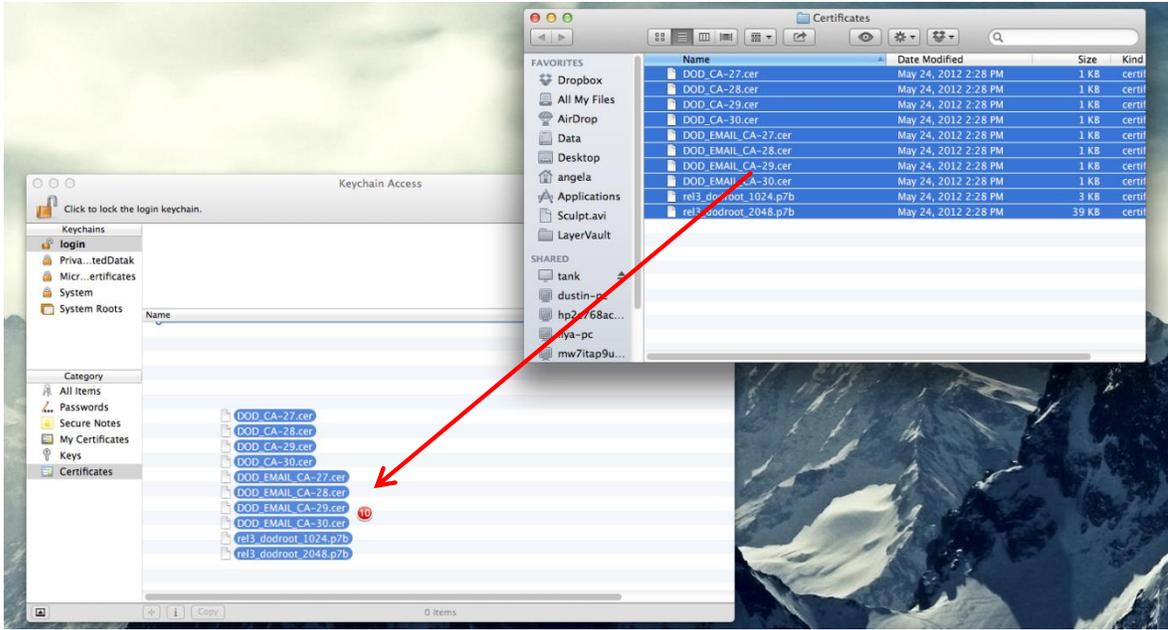


3. Download CACKey from www.militarycac.com/MAC/CACKey_0.6.5_Sltoml.pkg.tar.gz. Open the location where you downloaded the file (typically Downloads) and double-click on it to extract its contents.
4. Double click the newly extracted .pkg file to begin the installation of CACKey.

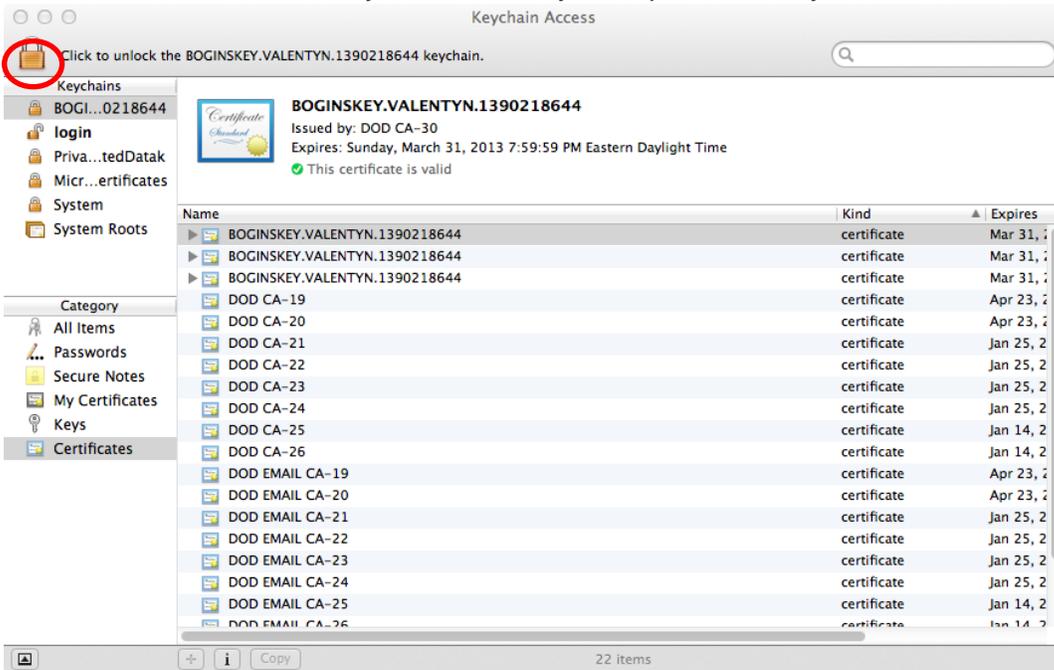
5. Read and acknowledge the first 3 screens by clicking Continue. Click **Agree** to the software license terms. Click **Install** to begin the installation of CACKey. Click **Close** when the successful installation window appears.



6. Download the Mac OS X DoD certificates from <https://remote.dla.mil/help/Certificates.zip>. Click on the downloaded folder to open it.
7. Open Finder and navigate to **Applications** → **Utilities** → **Keychain Access**. Click on the **login** Keychain in the left hand pane. Select all the certificates downloaded in the previous step and drag-and-drop them to the right hand pane of the Keychain Access window. Click **Add** once for each certificate if prompted.



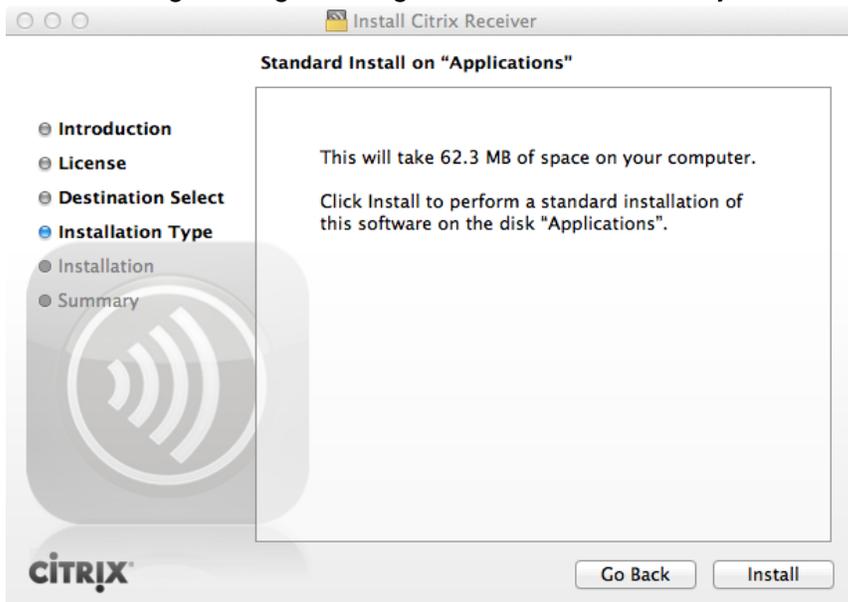
8. Insert your CAC card into the CAC reader. A new keychain labeled with your last name should appear above the **login** keychain. Select it and click on the padlock icon at the top of the window to unlock the keychain. The keychain password is your CAC PIN.



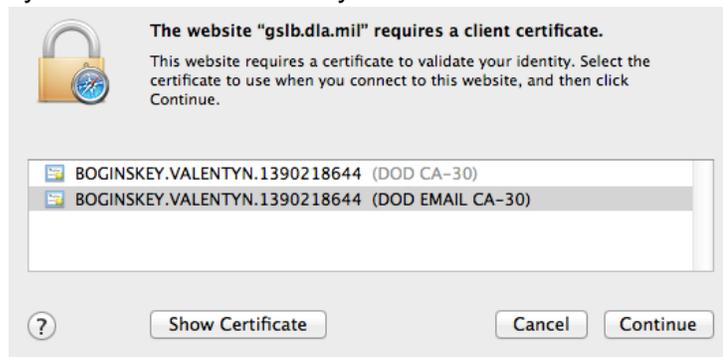
- Download the Citrix Receiver from <https://remote.dla.mil/help/MacCitrixReceiver.zip>. Double-click on the downloaded file to open **CitrixReceiver.dmg**. Double-click on **Install Citrix Receiver.pkg** to begin the installation.



- Click **Continue** to acknowledge the security prompt. Click **Continue** to acknowledge the next two windows, then click **Agree** to the software license terms, and then click **Install**, entering your password if prompted. Click **Close** to dismiss the successful installation window. Drag the original .dmg file to the trash can to eject the image.



11. Open a new Safari window, open Safari's Preferences by selecting Safari → Preferences from the Safari's tab menu. Click the 'Advanced' tab labeled. Place a check mark next to 'Show Develop menu in menu bar.'
12. Make sure to quit any previous instances of Safari. Open a new Safari window, click the Develop tab → click on User Agent and select Internet Explorer 8.0. Navigate to <https://remote.dla.mil>. Click **I Agree With The Statements Above** and click **LOGIN** on the following page. Select your E-mail certificate whenever prompted to authenticate, as many times as necessary (this should only occur the first time). If you get an authentication error, ensure the CAC keychain is unlocked in Keychain Access.



13. Click on any application to launch it. Enter your PIN again when prompted. The setup is now complete. (**Note**: If CAC card is removed from the CAC Reader or the Citrix Session times out, repeat steps 12 and 13)

Appendix D – Approved Smart Card Readers

Supplier	Product Name	Part Number
Cherry Electrical Products	Cherry Smart Terminal ST-1044U	ST-1044UB
Cherry Electrical Products	Cherry Smart Reader SR-4044	SR-4044
Cherry Electrical Products	SR-4300 ExpressCard Smart Card Reader	SR-4300
Cherry Electrical Products	ST-1210 SmartTerminal Smart Card Reader (XX1X)	ST-1210UAX-x
Dell Inc	Dell External USB Keyboard with Smart Card Reader	SK-3205
Dell Inc.	Broadcom USH2 Smartcard Solution	BCM5882
Dell, Inc	Broadcom USH Smart Card Solution	BCM5880
Dell, Inc.	Dell Latitude D430, D630,D830 w/ o2 Micro Smart Card	OZ77CR6
Dell, Inc.	Dell External USB Keyboard with Smart Card Reader	RT7D60
HID Corporation	iCLASS RK40	6130BKN00000-G3.0
HID Corporation	iCLASS OEM150	3121BNN0000-G3.0
HID Corporation	iCLASS RPK40	6136AKN00000-G3.0
HID Corporation	iCLASS RKL550	6170BKT00000-G3.0
HID Corporation	iCLASS RK40	6130CKN00000-G3.0
HID Corporation	iCLASS RPK40	6136CKN00000-G3.0
HID Corporation	iCLASS RMK40	6230CKN00000-G3.0
HID Corporation	iCLASS RMPK40	6236CKN00000-G3.0
HID Corporation	Omnikey 5321 USB Smart Card Reader	Omnikey 5321
HID Corporation	Omnikey 5321 CR USB Smart Card Reader	Omnikey 5321 CR
HID Corporation	Omnikey 5321 CL SAM USB Smart Card Reader	Omnikey 5321 CL SAM
HID Corporation	iCLASS RMP40	6225CKN0000-G3.0
HID Corporation	iCLASS RM40	6220CKN0000-G3.0
HID Global Corporation	iCLASS RP40	6125CKN0000-G3.0
HID Global Corporation	iCLASS R10	6100CKN0000-G3.0
HID Global Corporation	iCLASS R15	6140CKN0000-G3.0
HID Global Corporation	iCLASS R30	6110CKN0000-G3.0
HID Global Corporation	iCLASS RP15	6145CKN0000-G3.0
HID Global Corporation	iCLASS R40	6120CKN0000-G3.0
HID Global Corporation (formerly Omnikey Americas)	Omnikey 4321 ExpressCard SmartCard Reader	Omnikey 4321
Lenel Systems International	LNL-3121	LNL-3121
Lenel Systems International	Lenel OpenCard PIV Reader XF1100-PIV	LNL-XF1100D-PIV
Lenel Systems International	Lenel OpenCard PIV Reader XF2100-PIV	LNL-XF2100D-PIV

Lenel Systems International	Lenel OpenCard PIV Reader XF2110-PIV	LNL-XF2110D-PIV
SCM Microsystems Inc	SCR3500 USB Smart Card Reader	905141
SCM Microsystems, Inc.	SCR331 USB Smart Card reader	SCR331
SCM Microsystems, Inc.	SCR243 PCMCIA S/C Reader	SCR243
SCM Microsystems, Inc.	SCR3310 USB Smart Card Reader	SCR3310
SCM Microsystems, Inc.	SCR3311 USB Smart Card Reader	SCR3311
SCM Microsystems, Inc.	SCR131 Serial Port S/C Reader	SCR131
SCM Microsystems, Inc.	SCR531 Serial/USB S/C R/W	SCR531
SCM Microsystems, Inc.	SCR333 Drive Bay USB SC Reader	SCR333
SCM Microsystems, Inc.	SCR3340 ExpressCard 54 SC Reader	SCR3340
SCM Microsystems, Inc.	SDI010 Contact/Contactless Smart Card Reader	SDI010
SCM Microsystems, Inc.	PAT1312 Physical Access Reader	904565
SCM Microsystems, Inc.	PAT1322 Physical Access Reader	904566
SCM Microsystems, Inc.	SCR338 Smart Card Keyboard	903720
SCM Microsystems, Inc.	SCR3310 v2	SCR3310 v2
SCM Microsystems, Inc.	PAT1241	904322
SCM Microsystems, Inc.	SCR339	905174
SCM Microsystems, Inc.	SCR3310	905185
SCM Microsystems, Inc.	SCR3311V2	905194
SCM Microsystems, Inc.	SCR333V2	905195
SecuGen Corporation	SecuGen iD-USB SC/PIV	EA4-0516B
XceedID Corporation	Multi-Tech Wallmount Reader	XF1500P
XceedID Corporation	Multi-Tech Wallmount RS485 Reader	XF1500CS4
XceedID Corporation	Single-Frequency Mid-Range Keypad Reader	XF2210
XceedID Corporation	Single-Frequency Mid-Range Reader	XF2200
XceedID Corporation	OEM Module	OEM100
XceedID Corporation	Single-Frequency Mullion Reader	XF1200

Appendix E – How to Map a Network Shared Folder

Citrix users will be able to map a network shared folder by following the instructions below:

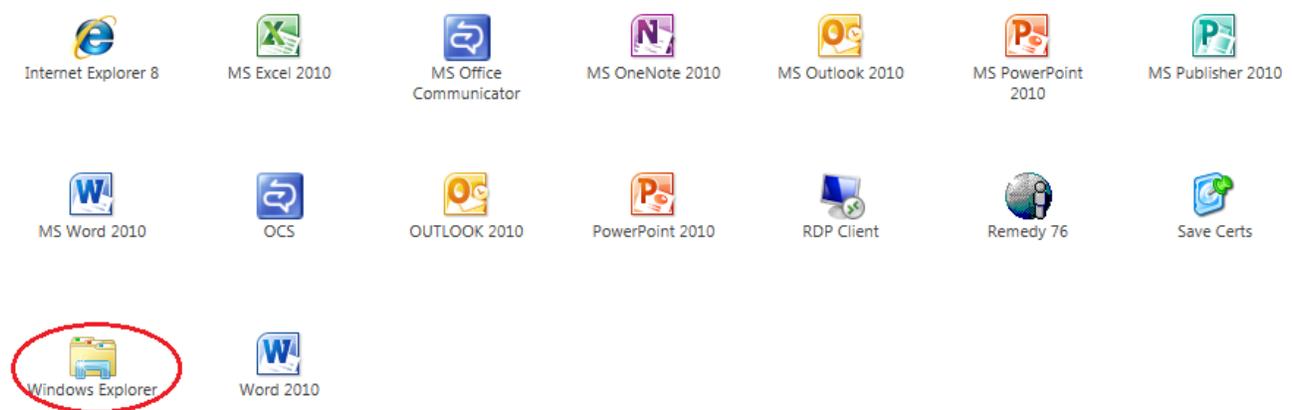
Note: In order to map a network shared folder, you will need the following information :

\\Server\Share

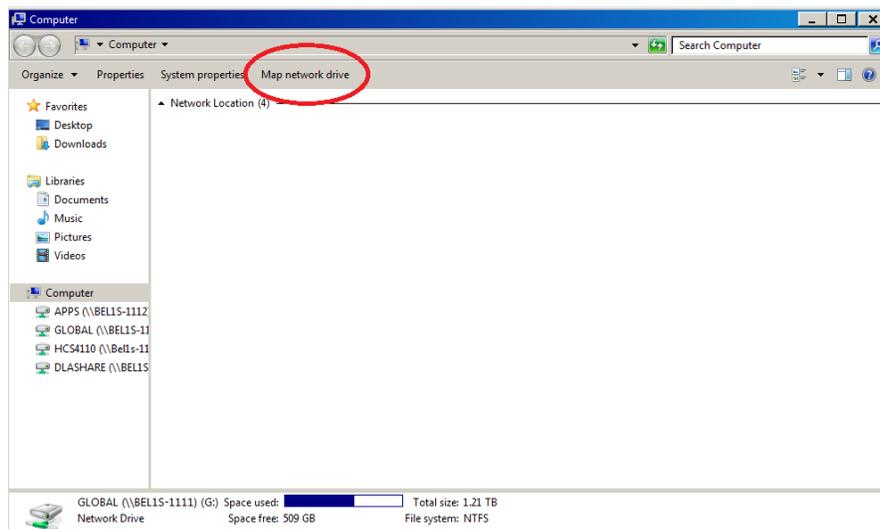
1. Server is the name of the server that is hosting your share. You will need to get this from your site IT resource
2. Share is the name of the folder that is assigned to store your personal information. This information also needs come from your site IT resource

Do not attempt to complete the following instructions without the above information as you will be asked for your Server and Share in the following dialogue boxes.

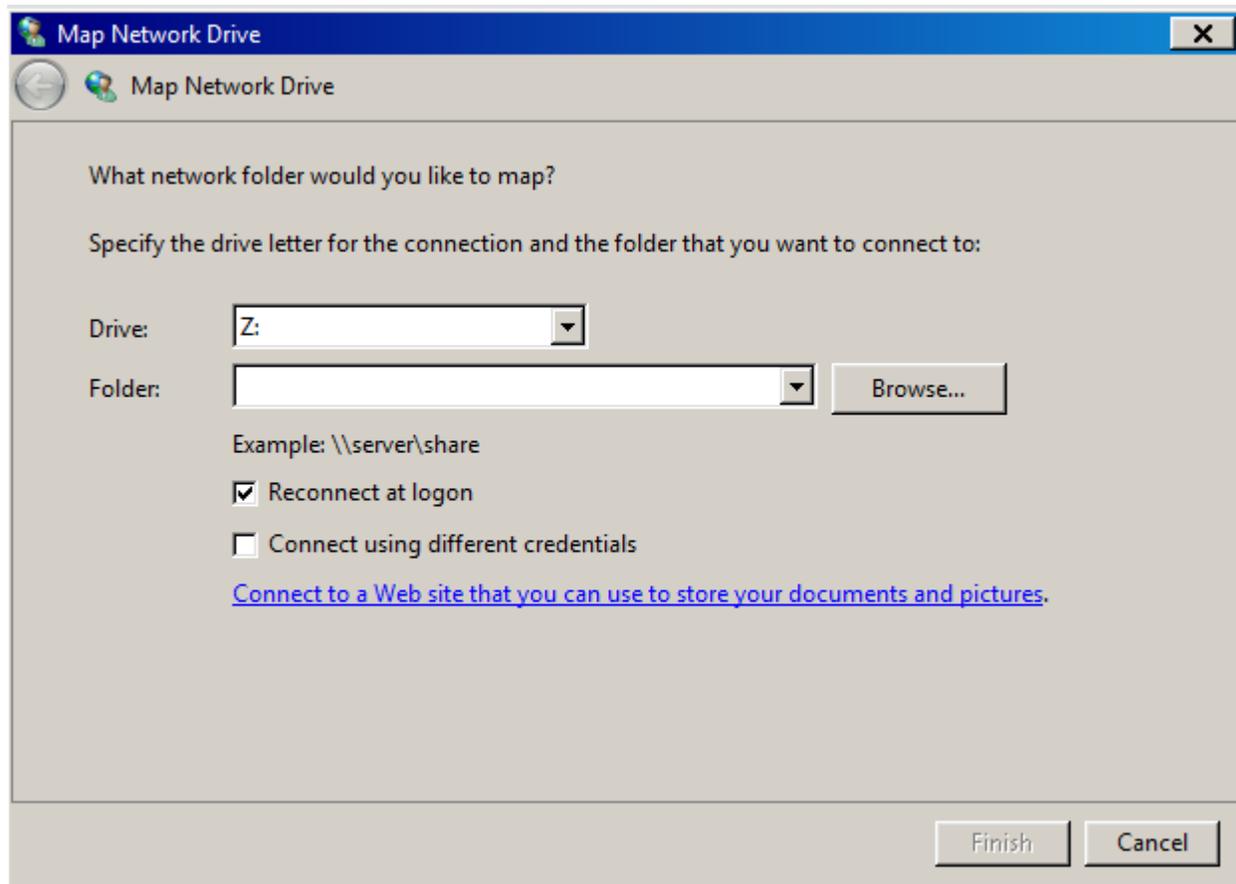
1. Launch Windows Explorer from the Citrix Application Web Interface:



2. Click “Map network drive”



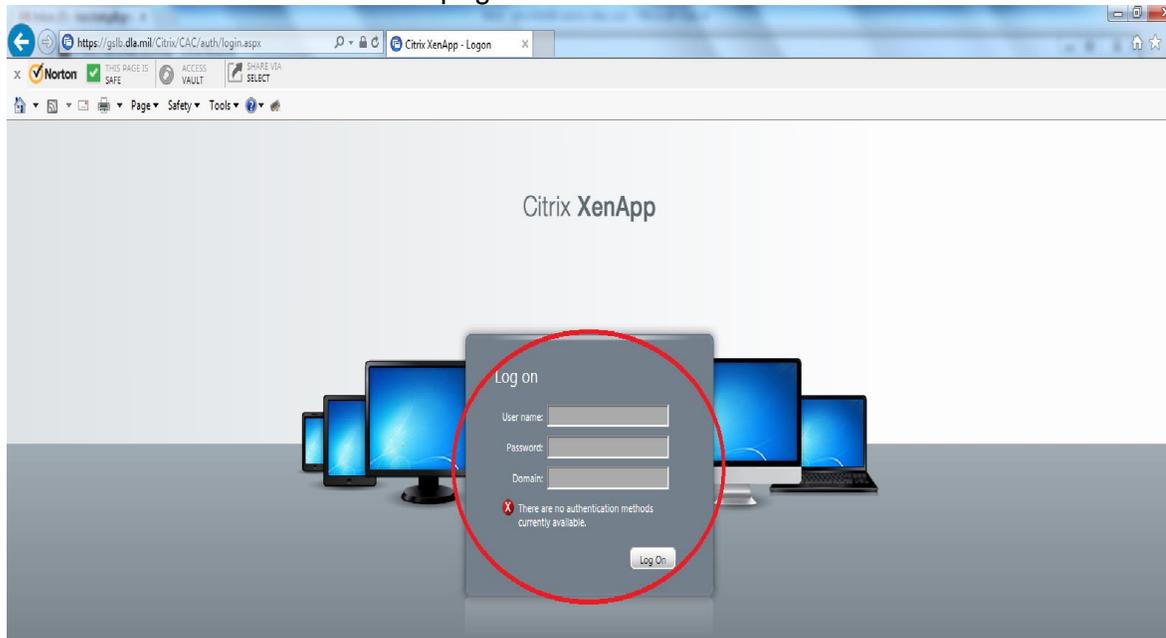
3. Click the drop down on the “Drive” field and select your drive letter. You can select any drive letter that is not in use. “H” is letter used at DLA to represent a user’s (H)ome folder. Select the dropdown box on the Folder field until you see your server and folder name appear. Select your server and folder then check the box to reconnect the next time you log in so that you do not have to repeat this process. Click Finish to complete the Map Network Drive process.



Appendix F – Instructions for Configuring and Using Citrix with Internet Explorer 11

Internet Explorer version 11 (IE 11) is not compatible with CAC authentication to <https://remote.dla.mil> without changing default settings described in this appendix. If either one of the following two screens are displayed, check which version of IE you are running.

1. You receive the following username/password authentication page instead of the typical DoD CAC PIN authentication page:



2. You receive “This page can’t be displayed” page:



This page can't be displayed

- Make sure the web address <https://gslb.dla.mil> is correct.
- Look for the page with your search engine.
- Refresh the page in a few minutes.

[Fix connection problems](#)

Select the white gear “Tools” icon in the far upper right-hand side of the page – it will turn blue when selected. Select “About Internet Explorer” to confirm IE 11 is the browser version installed on your computer.



If you are **NOT** running IE 11, follow the instructions (pictured below) from <https://remote.dla.mil>: “If this is your first time accessing this system from this machine...” or “Still not working? Try the following...”

DLA Enterprise Remote Access System

Eu/Afr Login
LOGIN
Pacific Login

Note: VDI LOGIN will be available to Phase 1 VDI users only

VDI LOGIN

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

- DoD Root Certificates
 - [Windows](#)
 - [Mac OS](#)
- Citrix Receiver
 - [Windows](#)
 - [Mac OS](#)

A CAC Reader and the ActivClient Software will be provided by your local IT Support staff. Please contact the Enterprise Help Desk at 1.855.352.0001 to request the software and a CAC reader.

→ Still not working? Try the following:

- Close all browser windows and try again.
- Confirm you are selecting your DoD EMAIL certificate when logging in.
- Review the [Home User Guide](#).
- For issues with multiple PIN prompts, make sure you have installed ActivClient (including the latest Hotfix) from the links above.
- **Known Internet Explorer 11 issue:** If asked to enter your "Username and Password" instead of DoD CAC PIN, complete the following two steps: In Internet Explorer Options > Security Tab, add https://*.dla.mil to "Trusted Sites"; In Internet Explorer > Tools > Compatibility View Settings add [dla.mil](https://*.dla.mil) to "Compatibility View".

If you are running IE 11, follow the instructions below from <https://remote.dla.mil>: “Known Internet Explorer 11 issue:” You will need to complete the following two steps.

DLA Enterprise Remote Access System

Eu/Afr Login LOGIN Pacific Login

Note: VDI LOGIN will be available to Phase 1 VDI users only

VDI LOGIN

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

- DoD Root Certificates
 - [Windows](#)
 - [Mac OS](#)
- Citrix Receiver
 - [Windows](#)
 - [Mac OS](#)

A CAC Reader and the ActivClient Software will be provided by your local IT Support staff. Please contact the Enterprise Help Desk at 1.855.352.0001 to request the software and a CAC reader.

Still not working? Try the following:

- Close all browser windows and try again.
- Confirm you are selecting your DoD EMAIL certificate when logging in.
- Review the [Home User Guide](#).
- For issues with multiple PIN prompts, make sure you have installed ActivClient (including the latest Hotfix) from the links above.
- **Known Internet Explorer 11 issue:** If asked to enter your "Username and Password" instead of DoD CAC PIN, complete the following two steps: In Internet Explorer Options > Security Tab, add https://*.dla.mil to "Trusted Sites"; In Internet Explorer > Tools > Compatibility View Settings add [dla.mil](https://*.dla.mil) to "Compatibility View".

Step 1: Select the white gear “Tools” icon in the far upper right-hand side of the page – it will turn blue when selected. Select “Internet Options”

DLA Enterprise Remote Access System

Eu/Afr Login LOGIN Pacific Login

Note: VDI LOGIN will be available to Phase 1 VDI users only

VDI LOGIN

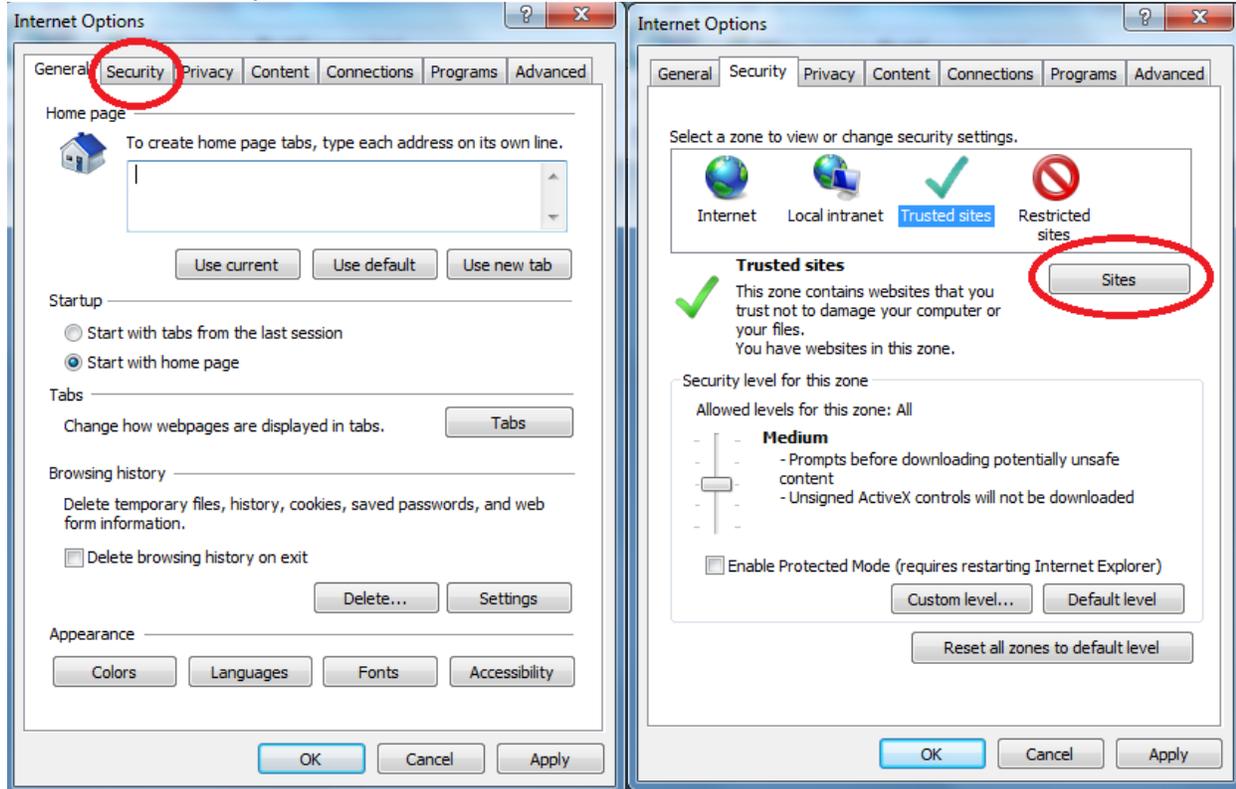
If this is your first time accessing this system from this machine, you may need to install the following to log in:

- DoD Root Certificates
 - [Windows](#)
 - [Mac OS](#)
- Citrix Receiver
 - [Windows](#)
 - [Mac OS](#)

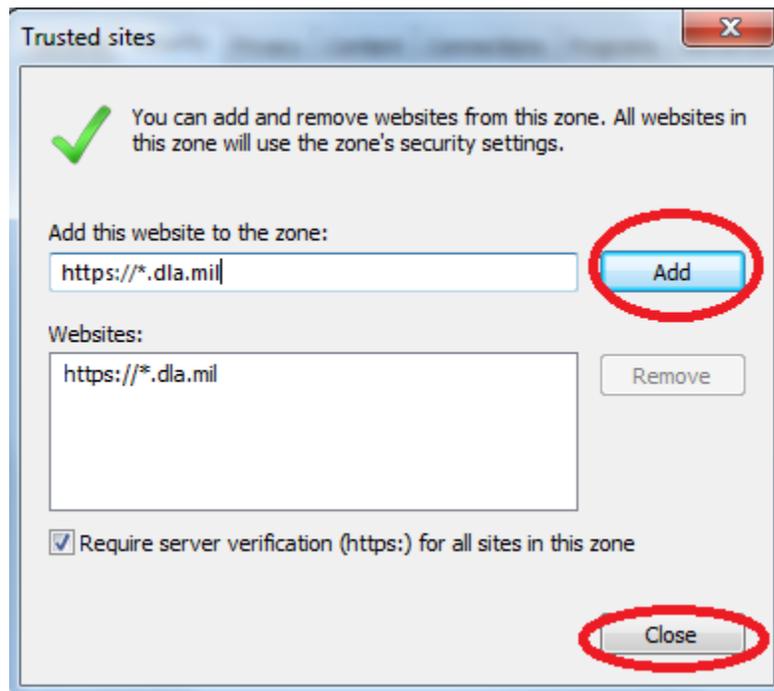
A CAC Reader and the ActivClient Software will be provided by your local IT Support staff. Please contact the Enterprise Help Desk at 1.855.352.0001 to request the software and a CAC reader.

Print
File
Zoom (100%)
Safety
Add site to Start menu
View downloads Ctrl+J
Manage add-ons
F12 Developer Tools
Go to pinned sites
Compatibility View settings
Report website problems
Internet options
About Internet Explorer

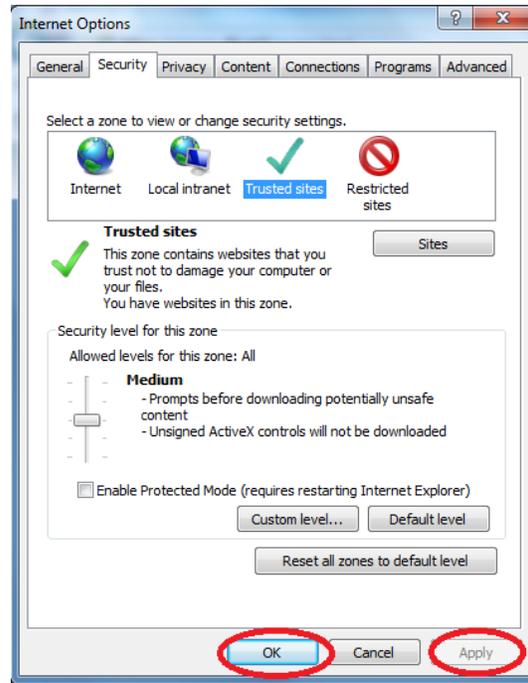
Select the "Security" tab. Then select "Sites"



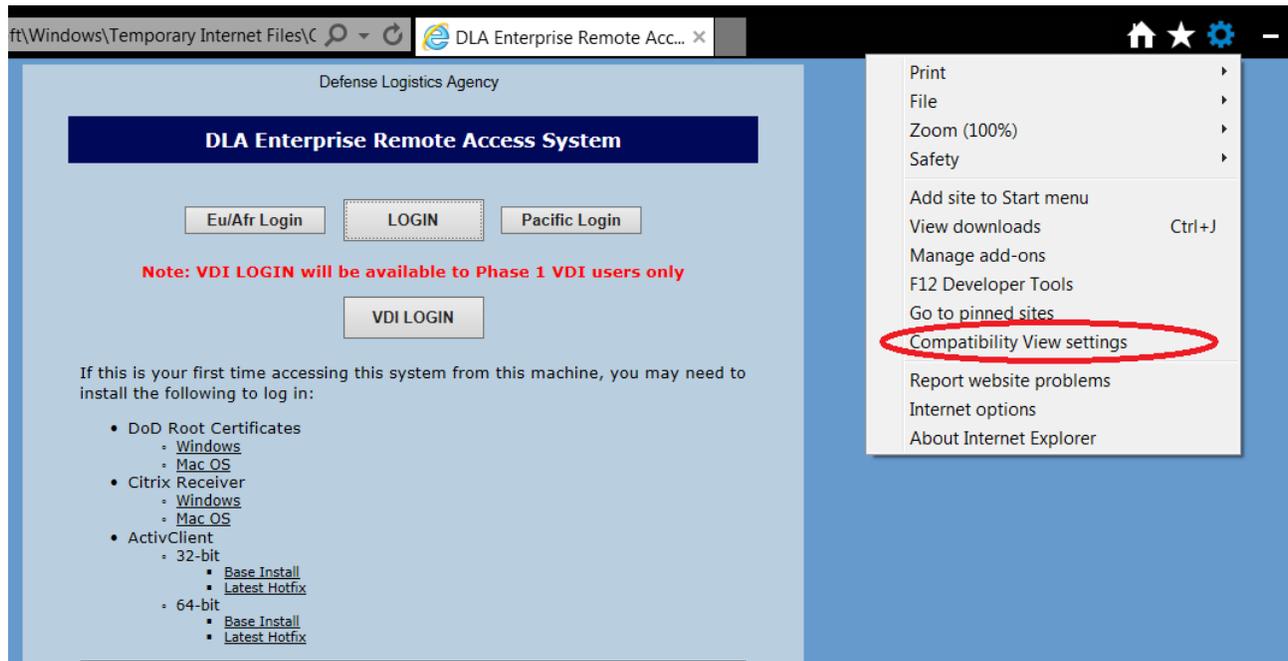
Enter https://*.dla.mil ("*" asterisk; followed by a "." period; then dla.mil). Select "Add" then "Close"



Select “Apply” then “OK”



Step 2: Select the white gear “Tools” icon in the far upper right-hand side of the page – it will turn blue when selected. Select “Compatibility View settings”



Enter "dla.mil" select "Add" then "Close".

