Defense Cyber Crime Center (DC3) Standard Operating Procedure	
Title	DC3 Remote Access User Guide
Version	3.1
Effective Date	28 May 2020
Approved By	Andrew K. Nelson, Chief Network Operations

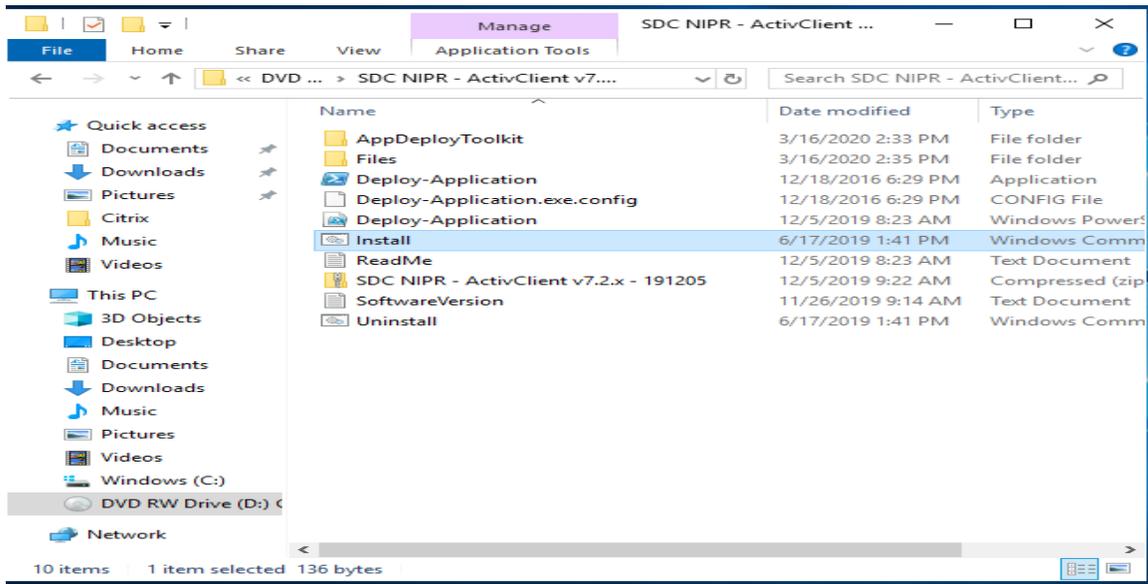**Mac users are advised to call helpdesk for Citrix receiver installation.**

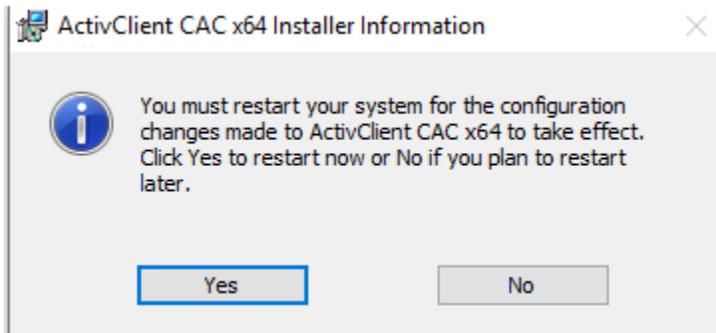**Access from a personal Windows Computer**

Requirements

1. NIPR-ActivClientV7.2x (ActivClent installation)

2. A CAC Reader

3. A Valid CAC with valid email certificate

4. A CAC Compatible Web browser (Internet Explorer 10 or 11) or Google Chrome

5. Installation of "InstallRoot 5.5" from DISA or provided as a link from DC3 website

6. Installation of FBCA cross-certificate removal tool from DISA or provided as a link from DC3 website

7. HomeUser Cert Tool_V04

8. Citrix Workspace App (Citrix Receiver)

Installing Active Client:

1. Open a browser and type this link https://www.dc3.mil/DC3/Employees/Remote-Access/

2. On the page click "Remote Access" in the middle of the page

3. NIPR-ActivClientV7.2xand run the "Install.bat".

4. Right click and run as Administrator

5. Laptop will ask for a reboot.

ActivClient CAC x64 Installer Information

You must restart your system for the configuration changes made to ActivClient CAC x64 to take effect. Click Yes to restart now or No if you plan to restart later.

Yes   No

6. After a reboot, ensure you can view ActivClent in the System tray

7. Continue to STEP1 below

Note: Before you can access DC3 Remote Access Portal, you must perform step 1 through 8 to install the required Citrix Receiver software, ActivClient and DoD CA certificates. This is a one-time installation.

| Defense Cyber Crime Center (DC3) Standard Operating Procedure	
Title	DC3 Remote Access User Guide
Version	3.1
Effective Date	28 May 2020
Approved By	Andrew K. Nelson, Chief Network Operations

STEP 1: Downloading and installing InstallRoot 5.5x64

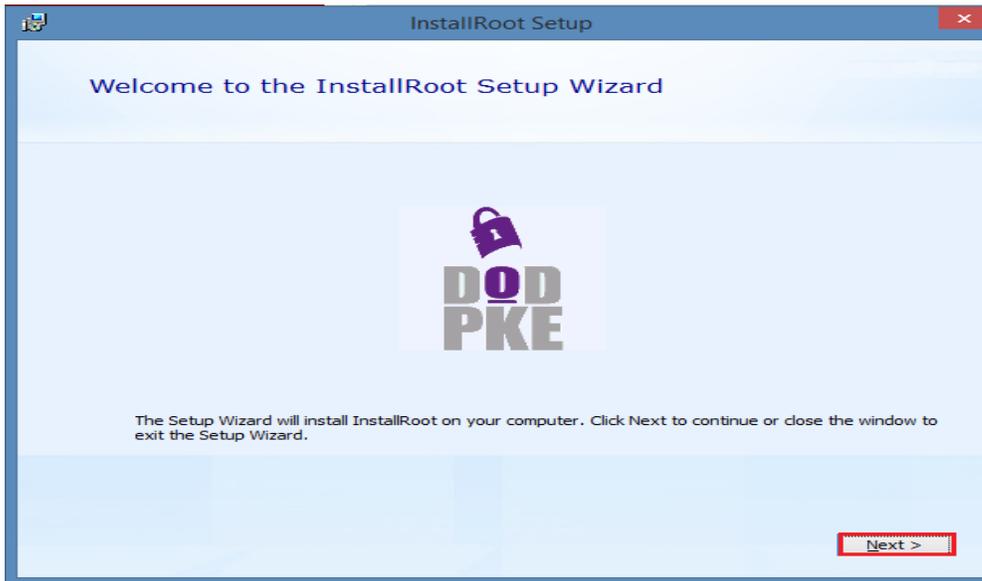- You must download and install InstallRoot 5. Download and instruction available on dc3.mil/remote access

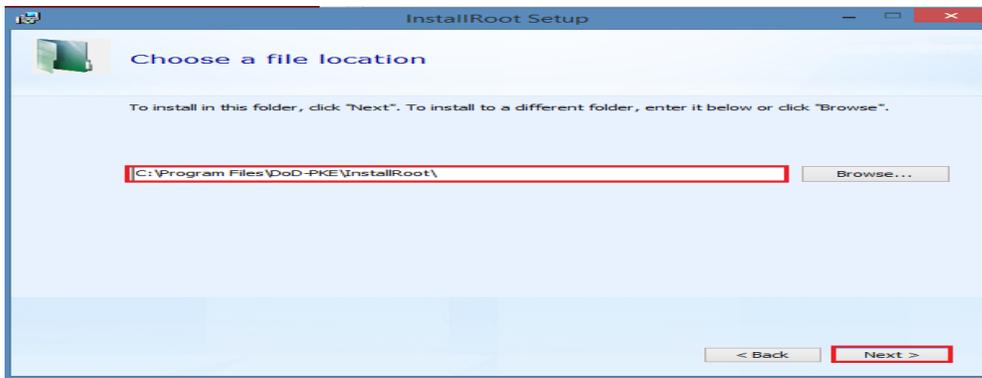7.1 Save "InstallRoot_5.5x64.msi" to your local computer drive
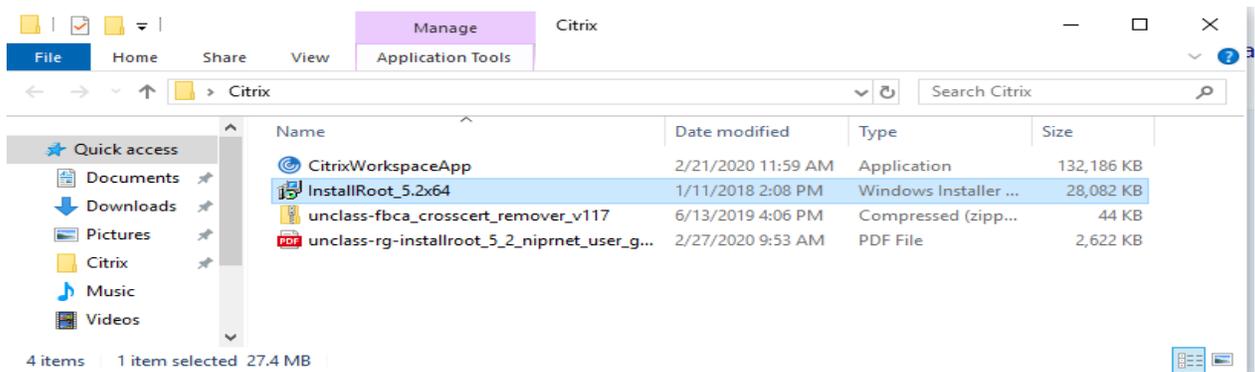
7.2 Once the download has completed, open the file location, and then double- click on "InstallRoot_5.2x64.msi"
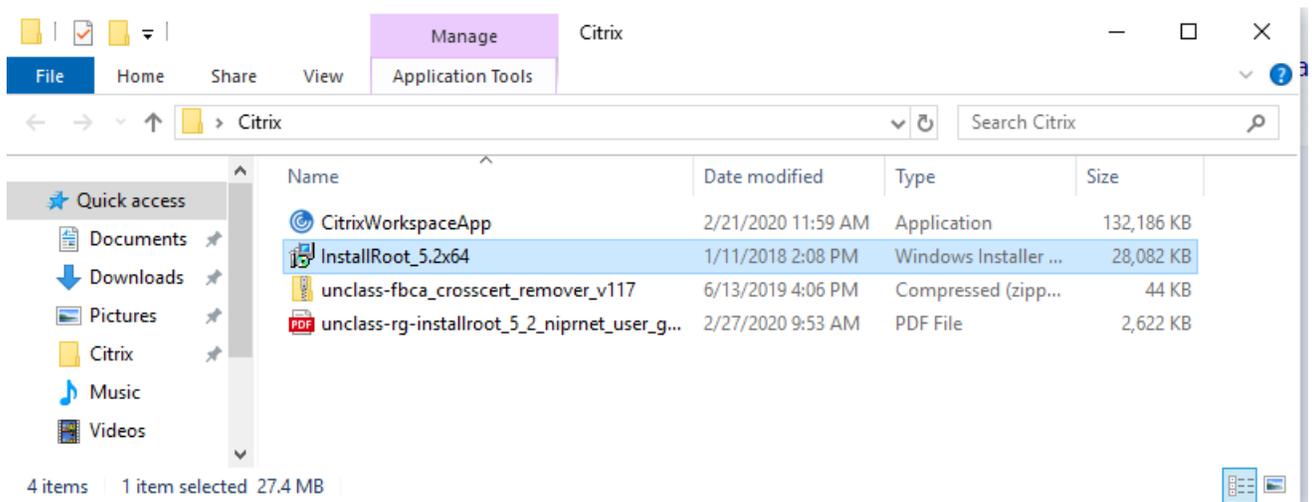
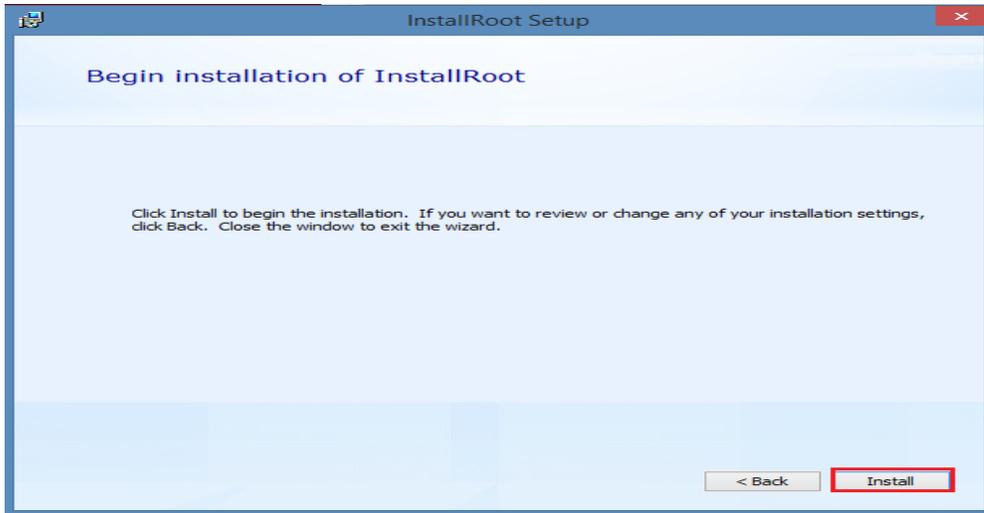7.3 Follow the installation process. At "Welcome to the InstallRoot Setup Wizard" click
Next

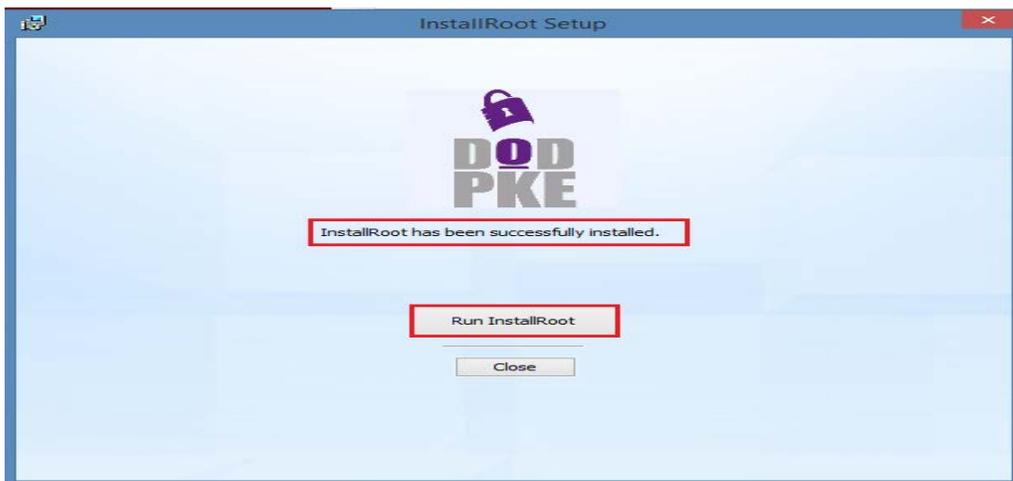7.4 At "Choose file Location" page, accept the default, and then click next

7.5 At "InstallRoot Features" page, all feature is checked by default. click Next
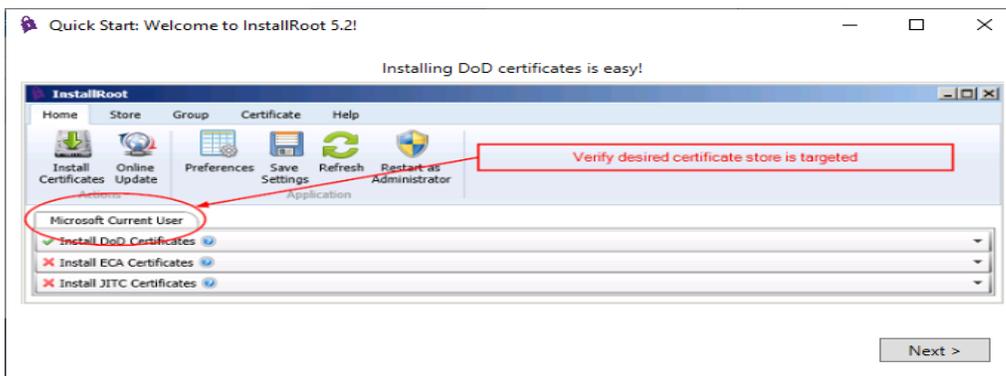
7.6 At "Begin installation of InstallRoot" page, click Install


7.8 You will see InstallRoot has been successfully installed, click Run Install root

7.9 Click next on Quick Start : welcome to installRoot 5.5 page (**Next on each page**)
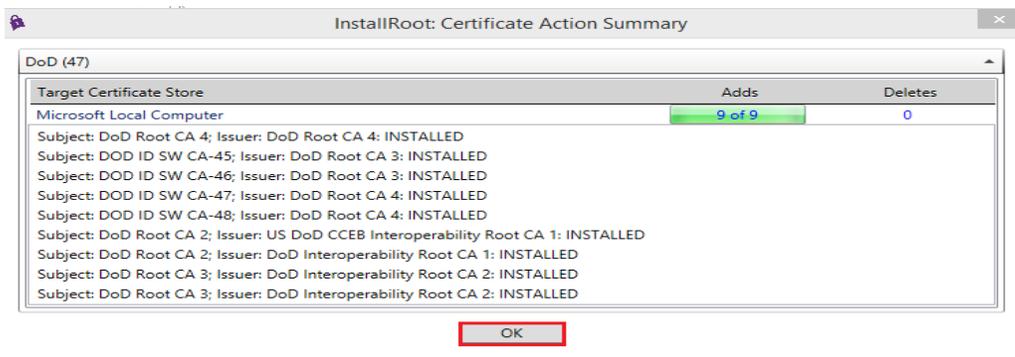

7.10   Make sure Local Computer store is selected, if not, click on the Store Tab, select Local Computer, click on the drop-down arrow on the right to display all DoD certificates, and then select all the Certificates
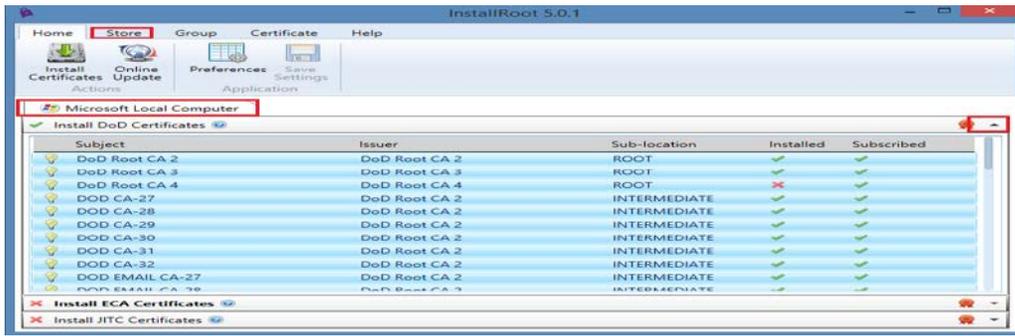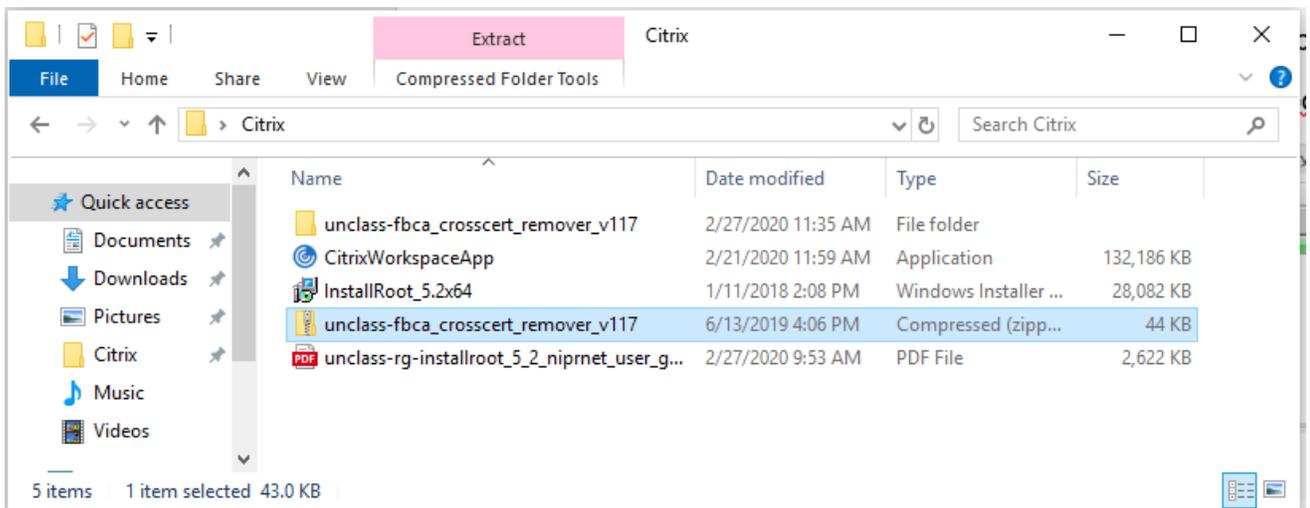
7.11 Click Home Tab, and then Click Install Certificates

7.12 Click OK, and then close InstallRoot

STEP 2: Installing FBCA cross-certificate removal tool

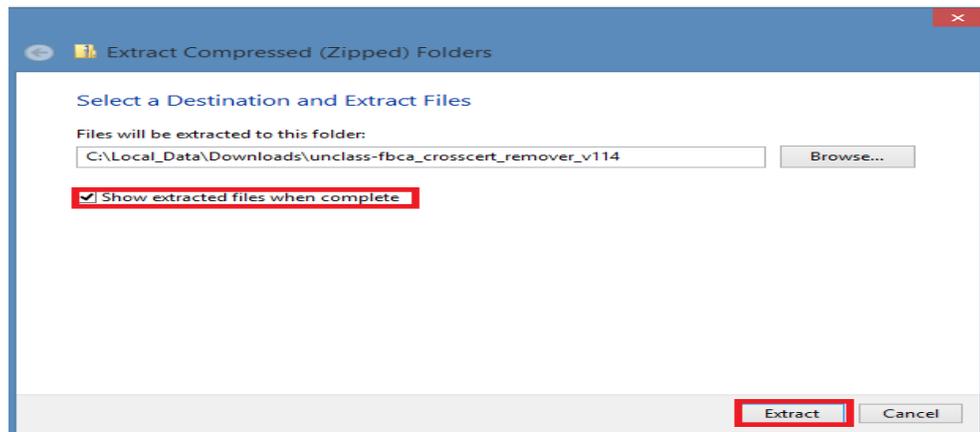7.13 Open the folder where unclass-fbca_crosscert_remover_v117 zip file is downloaded.

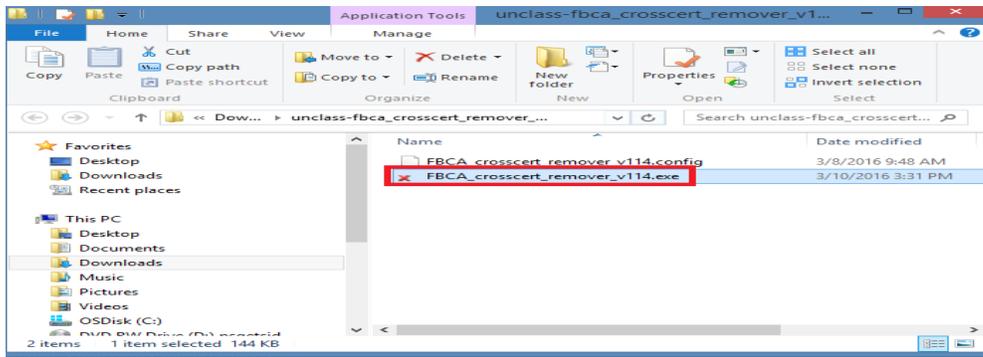| Defense Cyber Crime Center (DC3) Standard Operating Procedure	
Title	DC3 Remote Access User Guide
Version	3.1
Effective Date	28 May 2020
Approved By	Andrew K. Nelson, Chief Network Operations
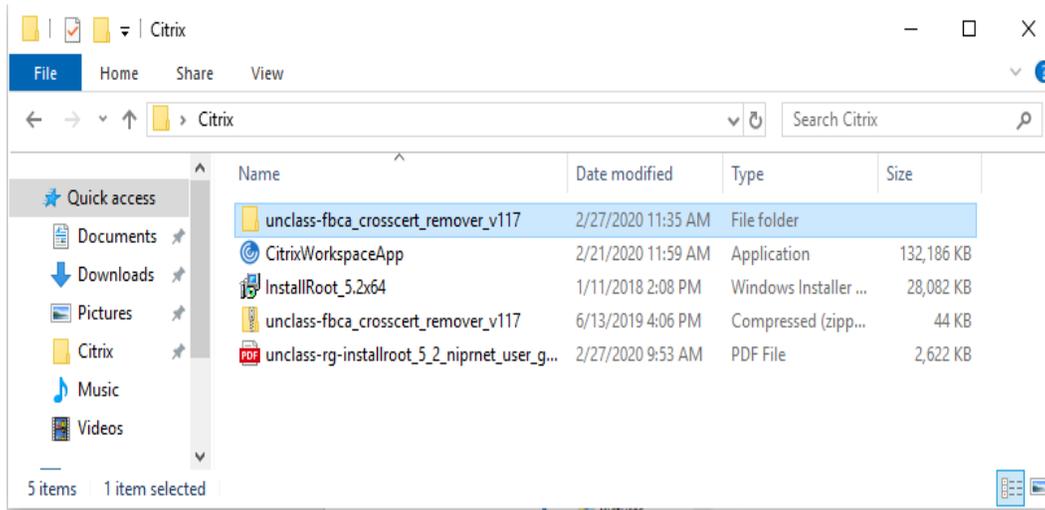
7.14 Navigate to where you saved the file, right-click "unclass-fbca_crosscert_remover_v114.zip", and then Click Extract All

7.15 Check "Show extracted files when completed" box, and then click Extract

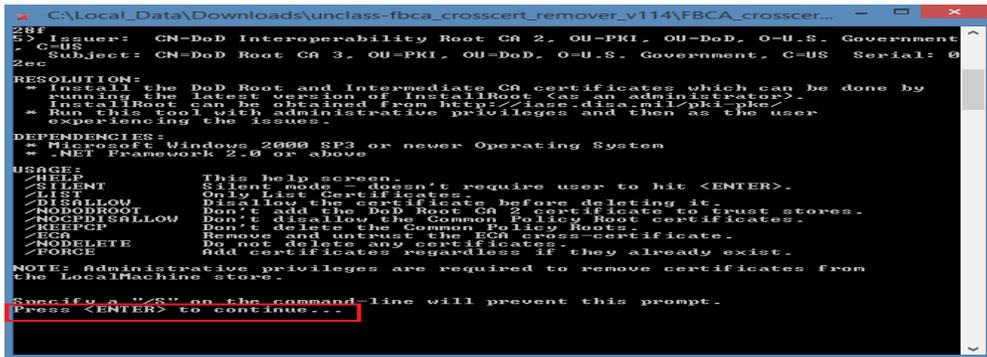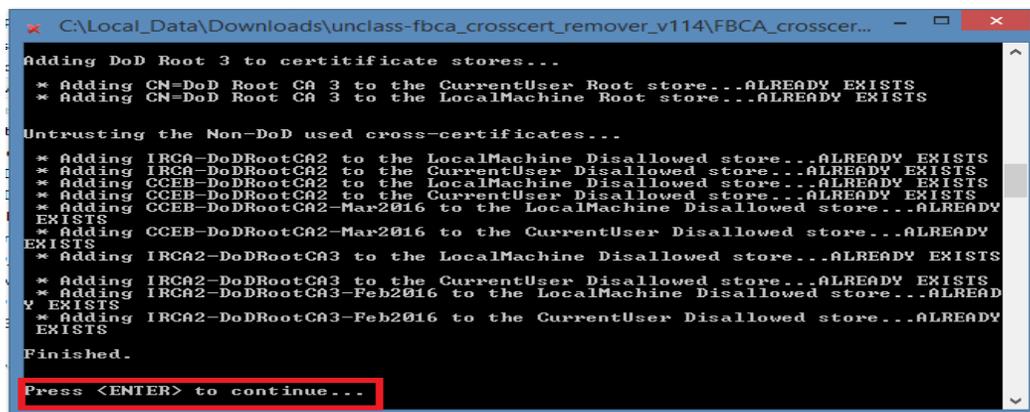7.16 Double-click "FBCA_crosscert_remover_v114.exe"

7.17 Press "enter" to continue

7.18 Press "enter" to close the window

STEP 3: Downloading and installing Citrix Workspace App (Citrix Receiver)

7.19 In the same Folder, Click and install Citrix Workspace App
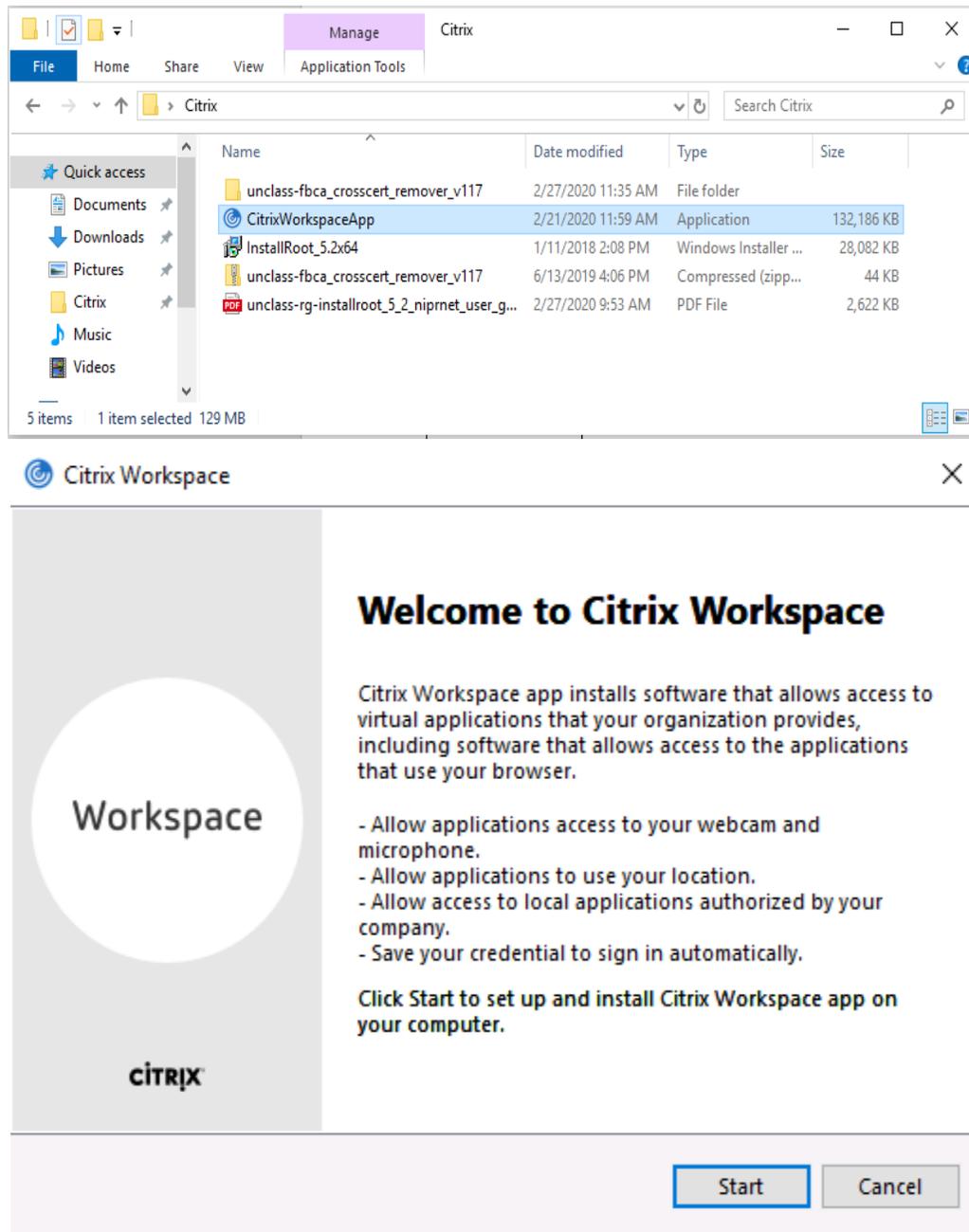
7.20 At Citrix Workspace page, Click Start.
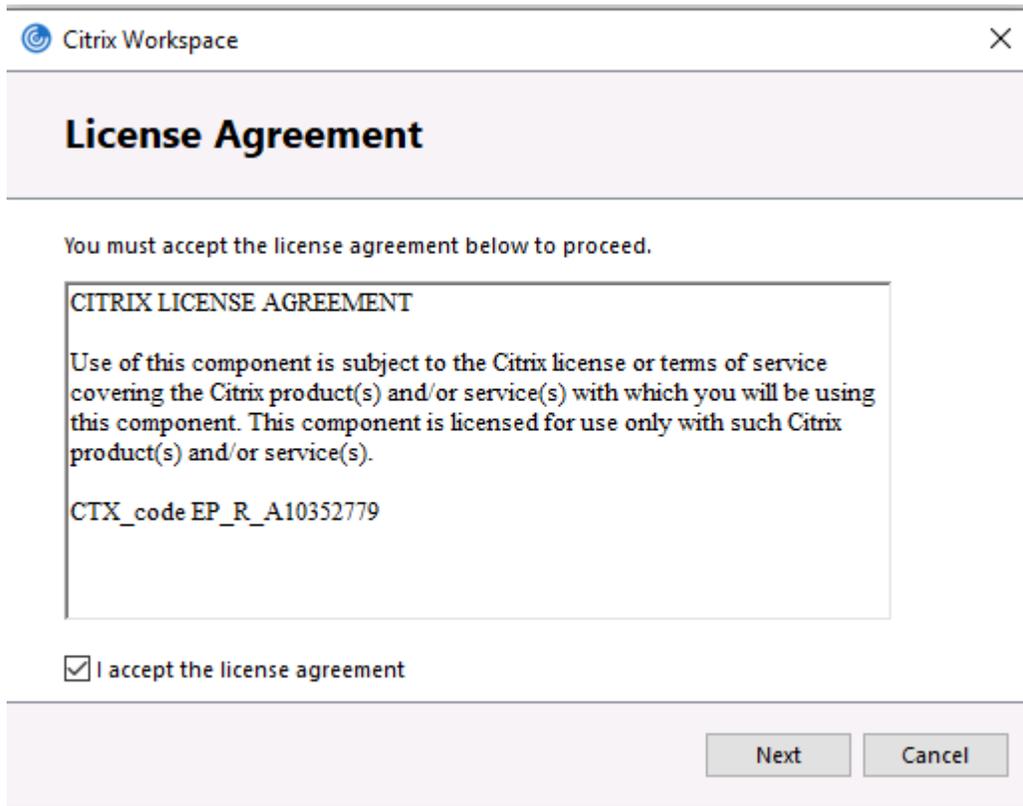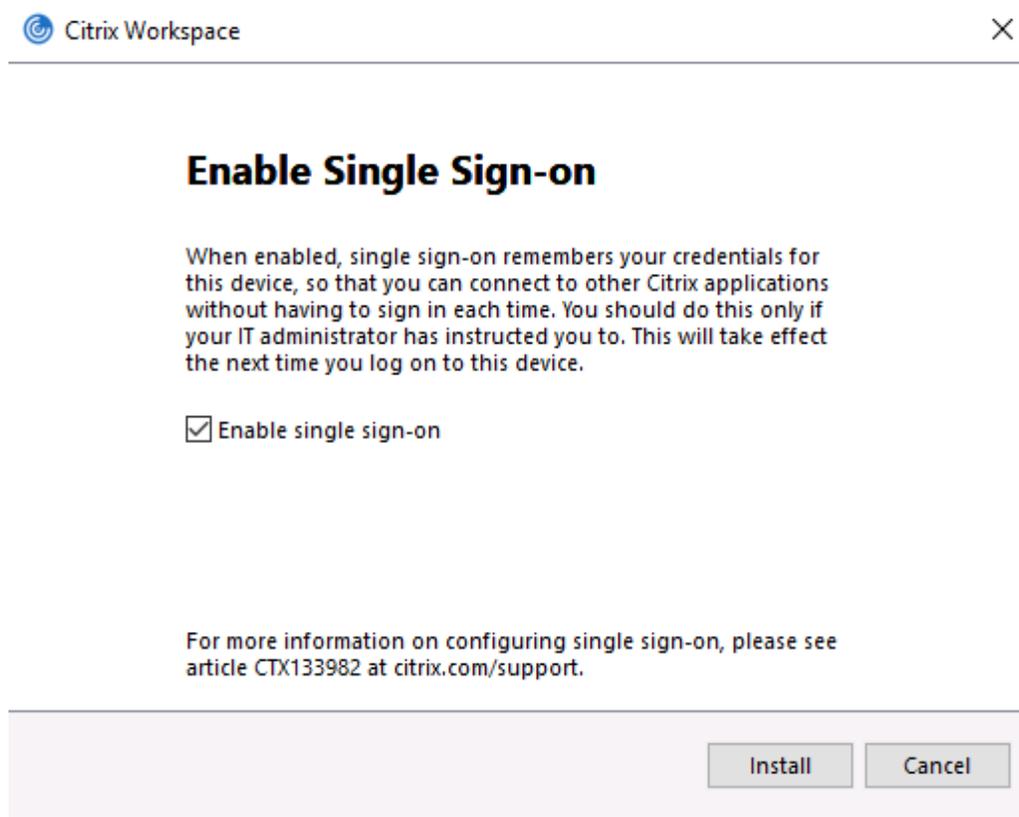
7.21 Check "I accept the license agreement" and click next.

Defense Cyber Crime Center (DC3) Standard Operating Procedure	
Title	DC3 Remote Access User Guide
Version	3.1
Effective Date	28 May 2020
Approved By	Andrew K. Nelson, Chief Network Operations

7.22 Check "Enable Single Sign-on" then click install

7.23 Click Finish
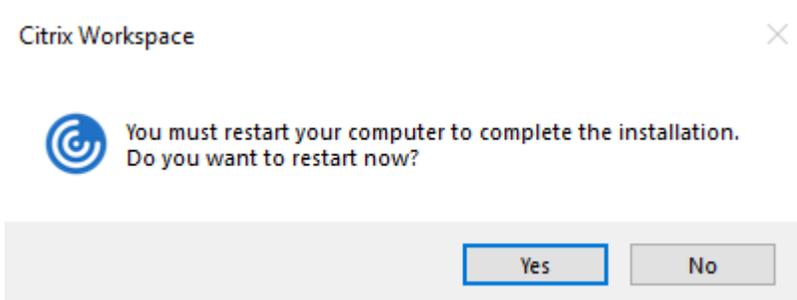
7.24 Click "Yes" to restart your computer.

7.25 Install **"HomeUser Cert Tool_V04"** by double clicking and following the prompt.

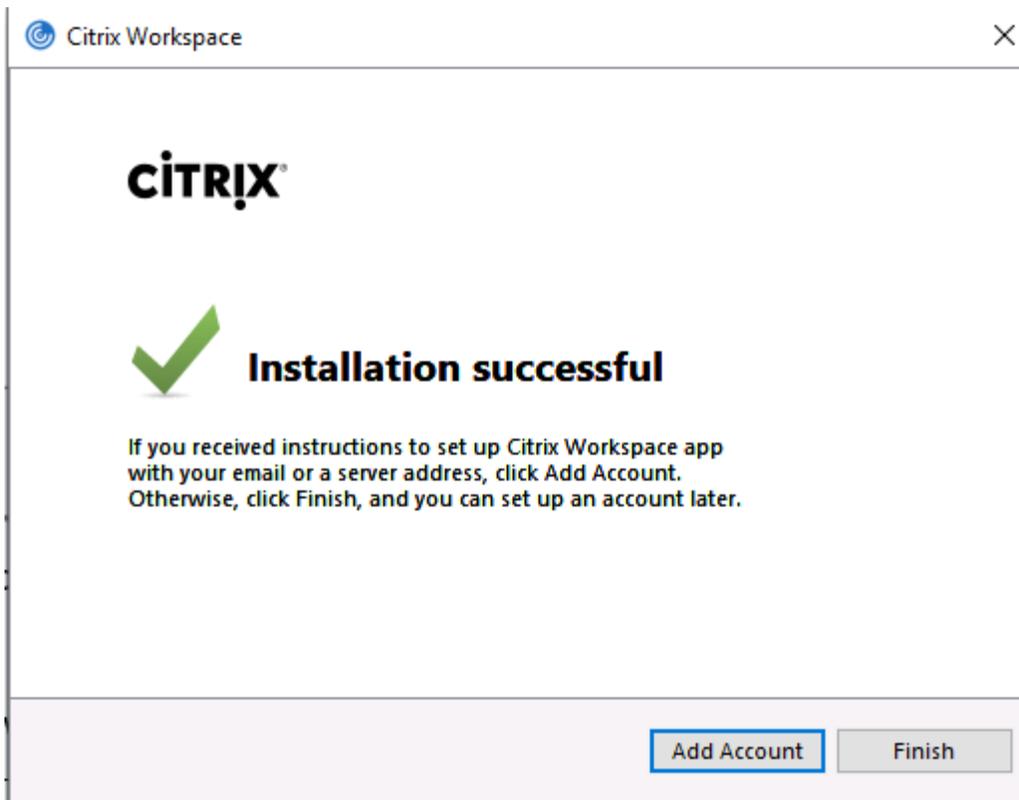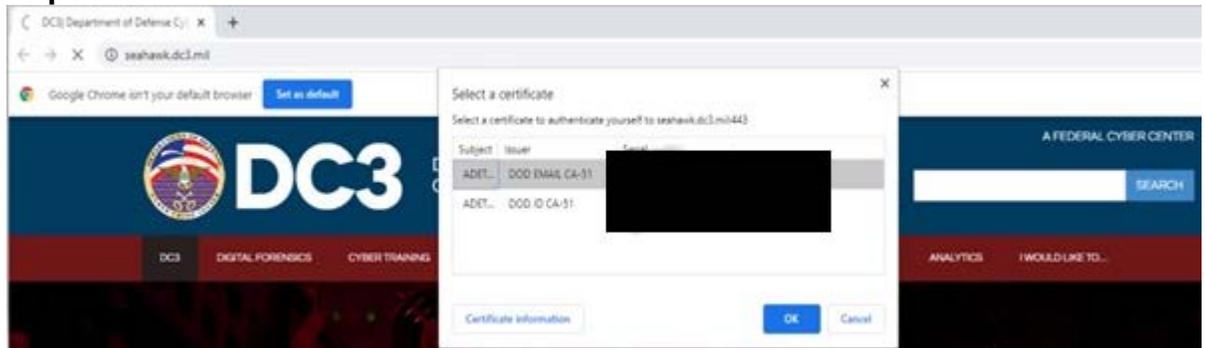| Defense Cyber Crime Center (DC3) Standard Operating Procedure	
Title	DC3 Remote Access User Guide
Version	3.1
Effective Date	28 May 2020
Approved By	Andrew K. Nelson, Chief Network Operations

Accessing Citrix Remote page

. After a reboot, please complete the following task to use Remote on your personal computer.

8.1 Use any browser "Chrome or Internet Explorer" to connect to **https://seahawk.dc3.mil**

8.2 You will be prompted for a CAC Certificate.

8.3 Select your Email Certificate, and then click OK.

8.4 The PIN prompt screen will display

8.4   Enter your PIN and then Click OK.

8.4. Click Detect Receiver.

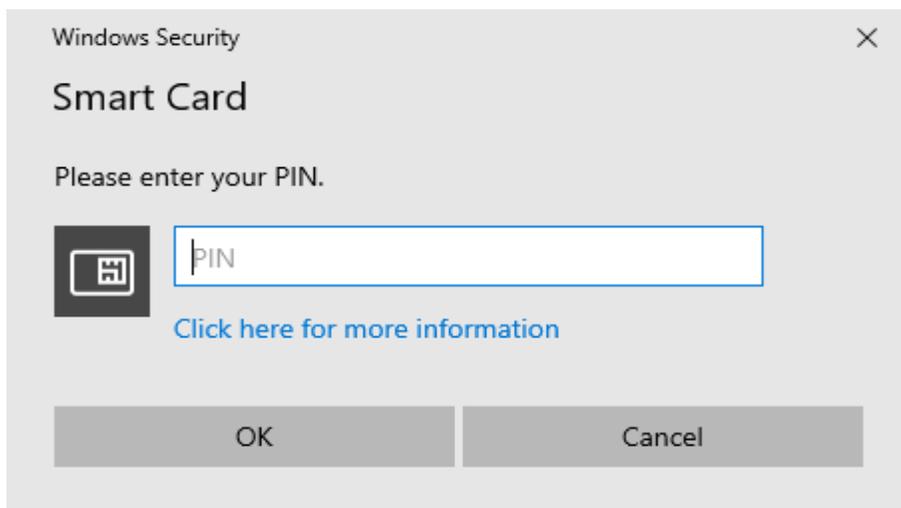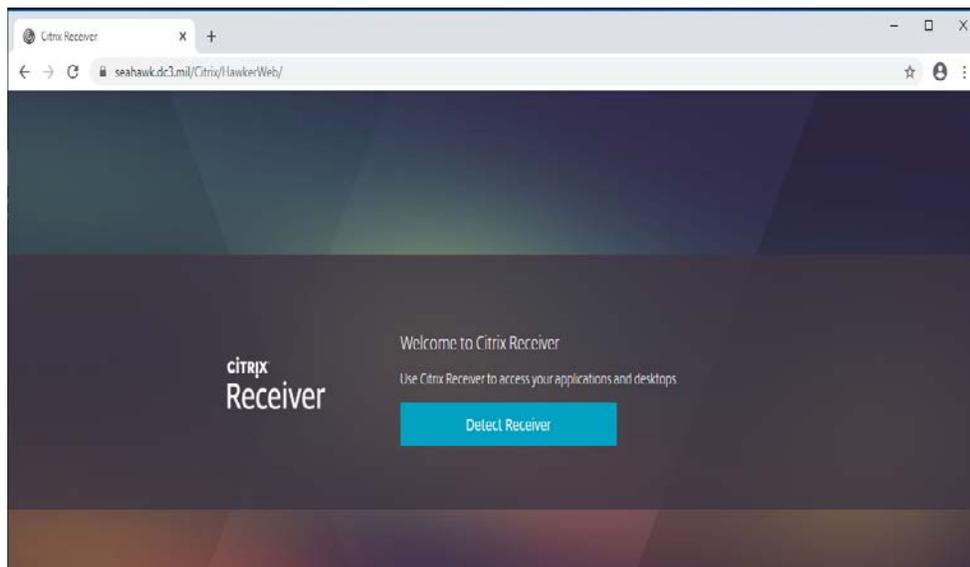| Defense Cyber Crime Center (DC3) Standard Operating Procedure	
Title	DC3 Remote Access User Guide
Version	3.1
Effective Date	28 May 2020
Approved By	Andrew K. Nelson, Chief Network Operations
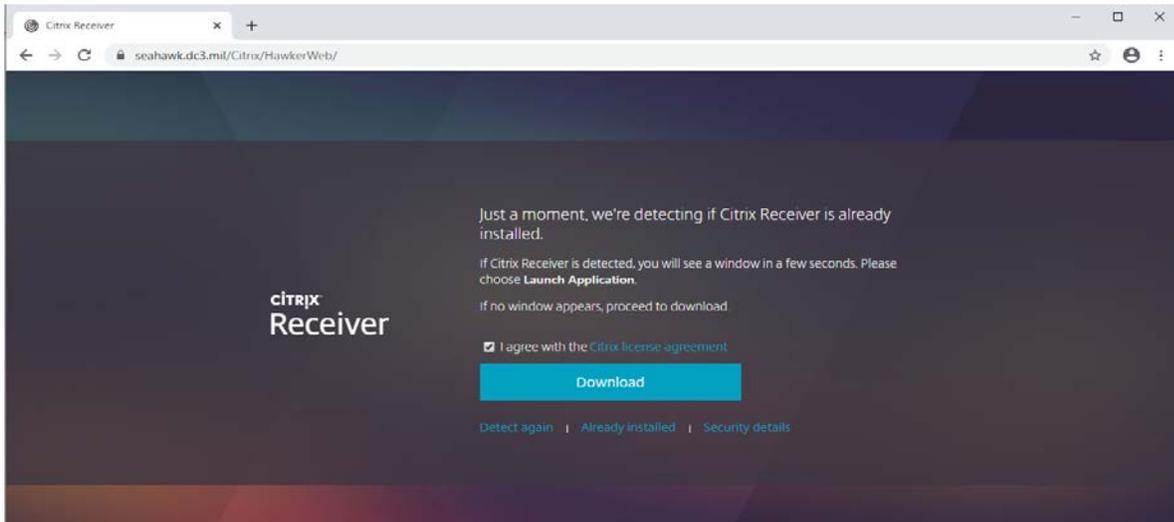
8.5. Check "I agree with the Citrix License agreement", then Click Already Installed.

8.6 DoD Warning statement will display

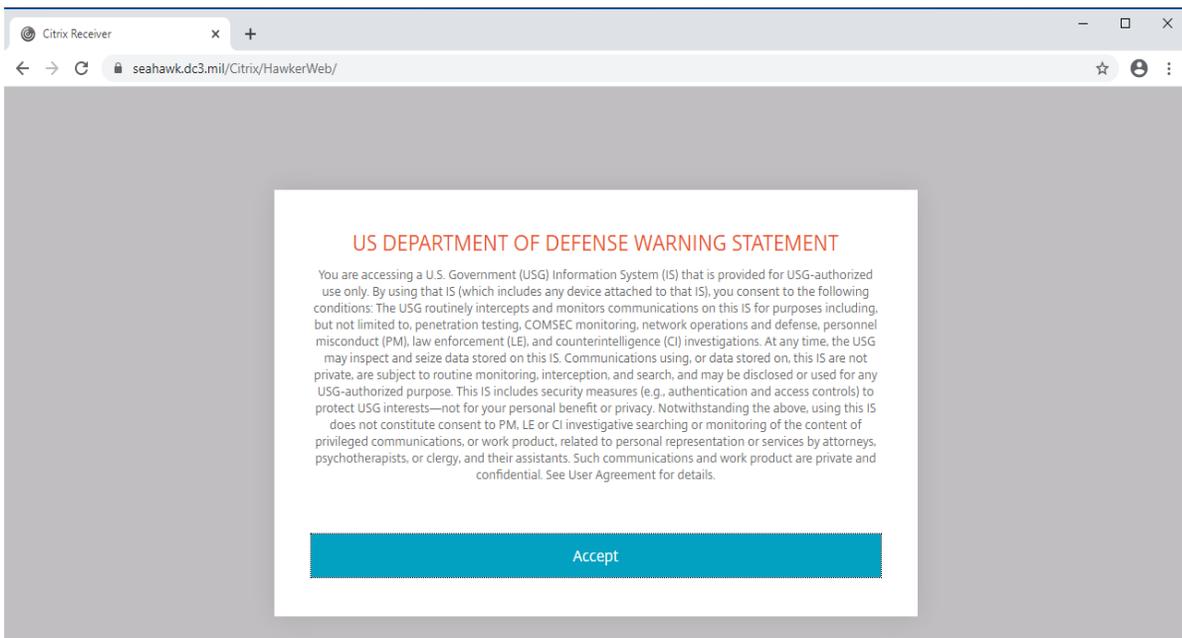| Defense Cyber Crime Center (DC3) Standard Operating Procedure	
Title	DC3 Remote Access User Guide
Version	3.1
Effective Date	28 May 2020
Approved By	Andrew K. Nelson, Chief Network Operations

8.7 Read and accept the DoD Warning statement.

8.8 After Accepting the DoD Warning Statement, your desktop will automatically launch, if not, the portal home page will display the Desktops and Applications which are available to you.
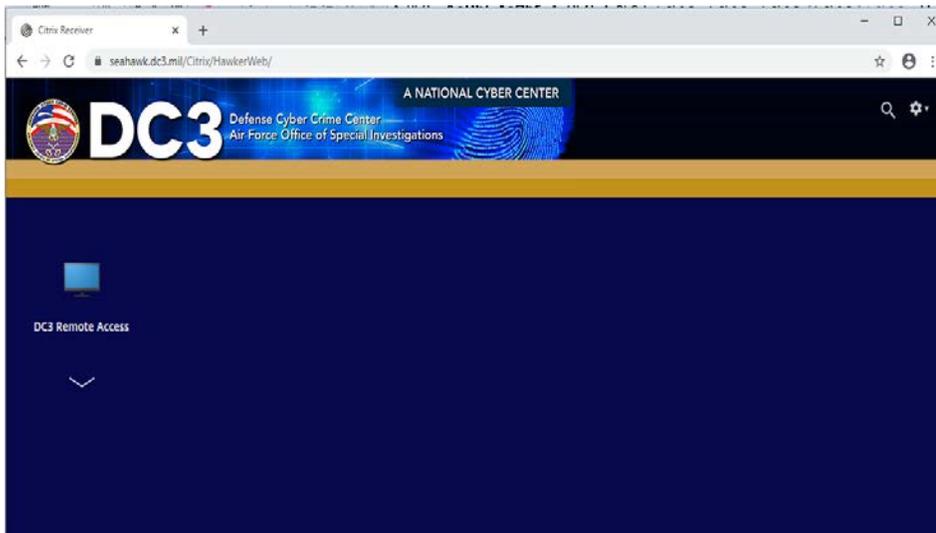
8.9 To access a Desktop, click on **"DC3 Desktops"** icon.

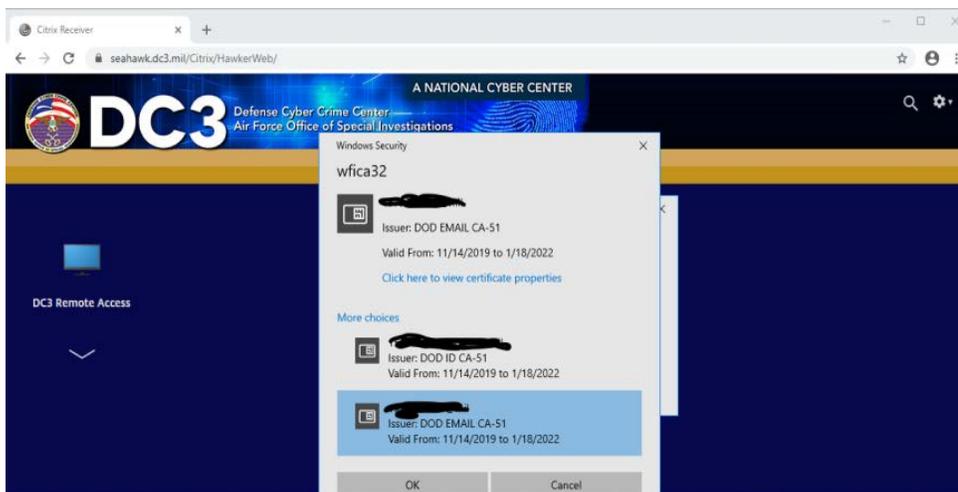8.10 The Certificate prompt will display, select your Email Certificate, and then click ok

Defense Cyber Crime Center (DC3) Standard Operating Procedure	
Title	DC3 Remote Access User Guide
Version	3.1
Effective Date	28 May 2020
Approved By	Andrew K. Nelson, Chief Network Operations

8.11 Click "OK" to accept DoD Warning Statement (see figure 20).
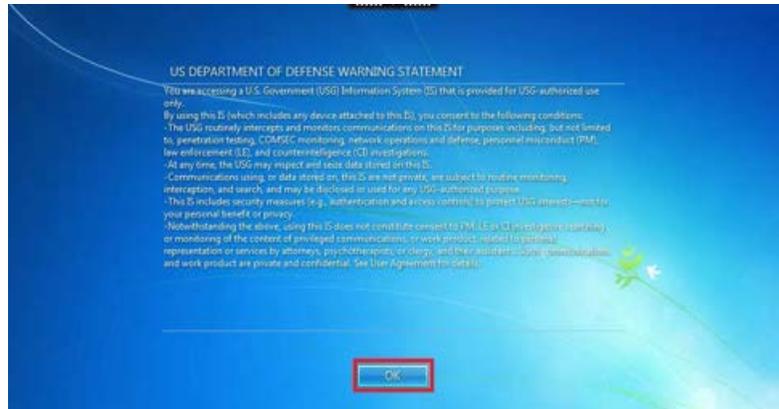
8.12 Windows login screen will display. Click "Switch User" to Login with your CAC Email Certificate (see figure 21).
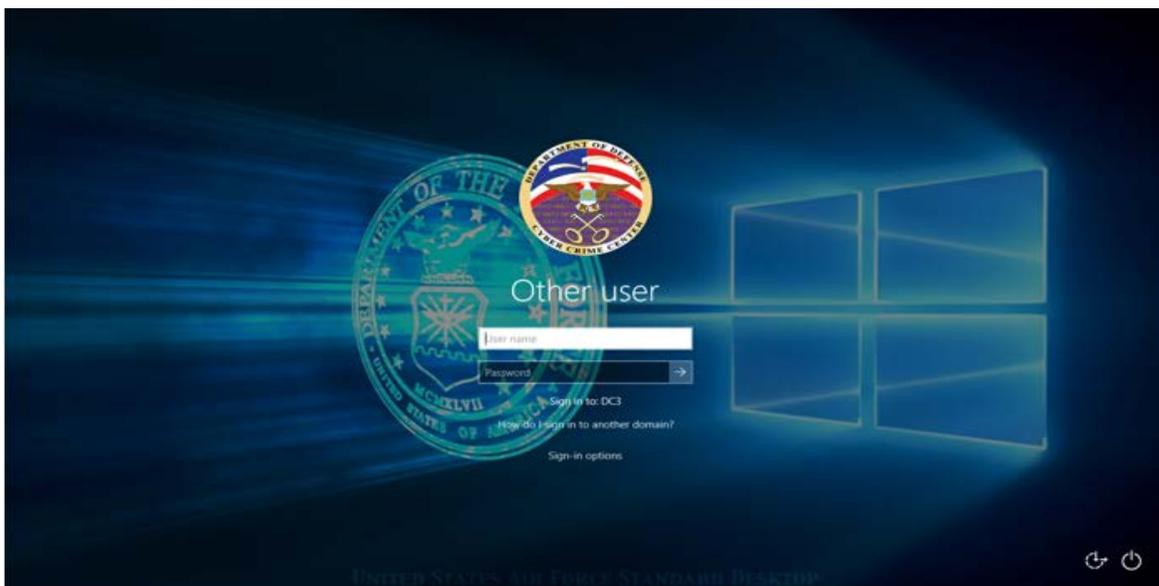
Defense Cyber Crime Center (DC3) Standard Operating Procedure	
Title	DC3 Remote Access User Guide
Version	3.1
Effective Date	28 May 2020
Approved By	Andrew K. Nelson, Chief Network Operations

8.13 Select your Email certificate if is not preselected and enter your PIN and then click the forward arrow or press enter. (see figure 22).

8.14 Wait for Windows to load your profile. You can start using the Desktop after you have successfully logged on (see figure 23). The experience will be similar to sitting at your desk in the office.

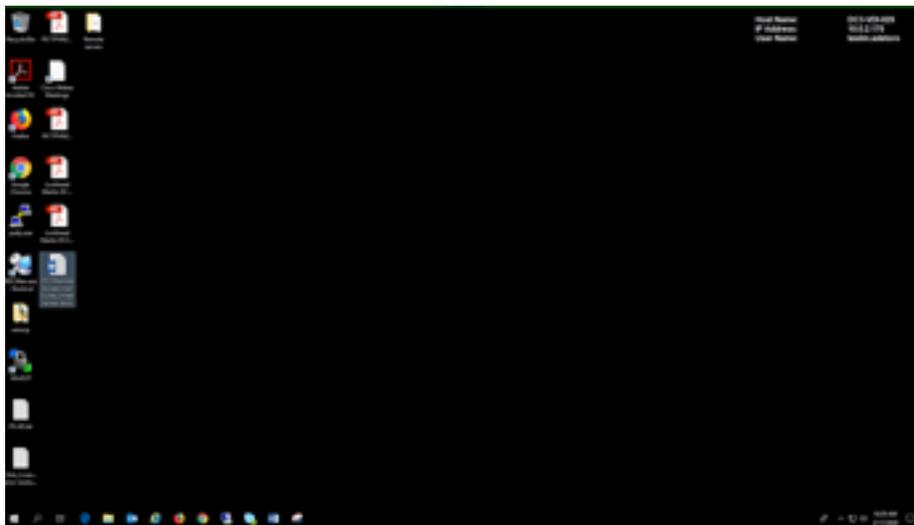**Figure 23. Virtual Hosted Desktop**
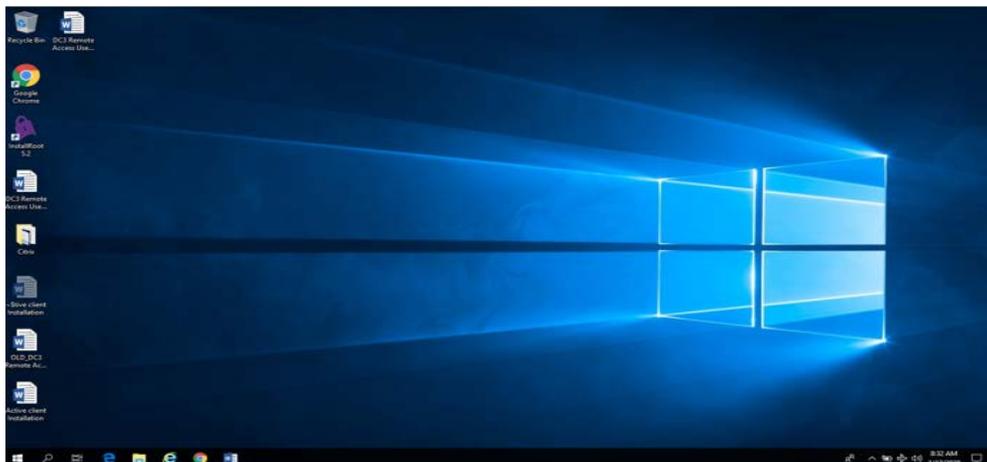
Defense Cyber Crime Center (DC3) Standard Operating Procedure	
Title	DC3 Remote Access User Guide
Version	3.1
Effective Date	28 May 2020
Approved By	Andrew K. Nelson, Chief Network Operations

NOTE: You will be prompted for your PIN after 30 minutes of inactivity on the remote access portal page. To avoid PIN prompt after 30 minutes of inactivity, please **click** on cancel when prompted, and close the portal page. Press Alt+Tab or click on desktop viewer icon on the taskbar to go back to your virtual hosted desktop to continue using your desktop session.

8.15 After you have successfully logged on, you can access files and application from your desktop (see figure 24).


Figure 24. Access Home Page

8.16 Please logoff properly after you finish using the Desktop. To log off, click on the Windows icon on the bottom left corner of the desktop, and then click on the logoff button.

8.17 After you have logged off from the Desktop if the portal page is still active Logoff from the portal page. To log off, click on the Wheel button at the top right corner, and then click on the logoff button (see figure 25).
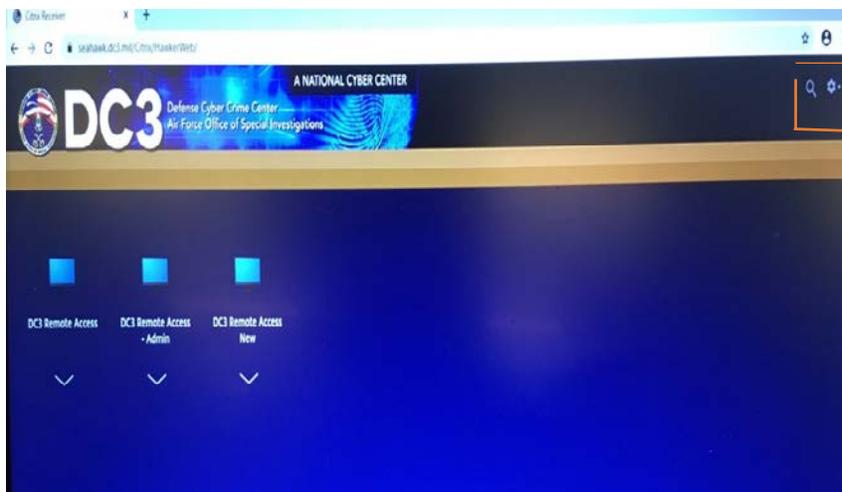
Figure 25. Logoff

Defense Cyber Crime Center (DC3) Standard Operating Procedure	
Title	DC3 Remote Access User Guide
Version	3.1
Effective Date	28 May 2020
Approved By	Andrew K. Nelson, Chief Network Operations

ACRONYMS   DEFINITION

CAC   Common Access Card

DC3   Defense Cyber Crime Center

DoD   Department of Defense

EPA   Endpoint Analysis

LAN   Local Area Network

PIN   Personal Identification Number

SOP   Standard Operating Procedure

USB   Universal Serial Bus