## DOCUMENT REVISION HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Updated By</th>
<th>Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>22 MAR 2019</td>
<td>1</td>
<td>McCoy, William SITECII</td>
<td>Initial version</td>
</tr>
</tbody>
</table>
TABLE OF CONTENTS

1. INTRODUCTION .............................................................................................................................................. 5
2. PREREQUISITES ............................................................................................................................................. 6
3. HARDWARE INSTALLATION INSTRUCTIONS ....................................................................................... 7
4. SOFTWARE INSTALLATION INSTRUCTIONS ........................................................................................ 9
5. ACCESSING SOF-U OWA............................................................................................................................. 17
6. SSL VPN CONFIGURATION........................................................................................................................... 19
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. – Introduction</td>
<td>Provides the User with a general overview of the OWA and SSL VPN User Manual.</td>
</tr>
<tr>
<td>2. – Prerequisites</td>
<td>Explains hardware requirements and software installation guidance.</td>
</tr>
<tr>
<td>3. – Hardware Installation Instructions</td>
<td>Explains how to install a smart card reader.</td>
</tr>
<tr>
<td>4. – Software Installation Instructions</td>
<td>Explains how to download and install required software.</td>
</tr>
<tr>
<td>5. – Accessing SOF-U OWA</td>
<td>Provides instructions on accessing OWA.</td>
</tr>
<tr>
<td>6. – SSL VPN Configuration</td>
<td>Explains how to connect to USASOC's SSL VPN - for users running Windows Vista or 7.</td>
</tr>
</tbody>
</table>

**LIST OF TABLES**

*Table 1: List of Acronyms*...41
1. INTRODUCTION

The United States Army Special Operations Command (USASOC) Outlook Web Access and Secure Socket Layer (SSL) Virtual Private Network (VPN) Home Users' Manual provides instructions for installation and configuration of software and hardware necessary for accessing SOF OWA and the SOF-U Network via SSL VPN. See Table 1-1 for an overview of document sections.

This User Manual will serve:

- To guide users through the installation and configuration of all software and hardware required to access SOF Outlook Web Access (OWA) Non-Secure Internet Protocol Router Network (NIPRNet) e-mail on a personal computer (PC) running a Windows 10 operating system (OS).

- To guide users through the installation and configuration of all software and hardware required to access SOF-U Secure Socket Layer (SSL) Virtual Private Network (VPN) on a PC running Windows version 10 operating system.

NOTE

Windows 10 is required for SSL VPN to allow Remote Desktop Protocol (RDP). Linux or Apple Operating Systems have not been tested.

- To provide instructions for users to access OWA and the SSL VPN.

DISCLAIMER

Other than this document, the USASOC G6 will not provide customer service support for the installation or use of any personal use software or hardware. This includes, but is not limited to, the software covered in this installation guide. This guide is provided to USASOC users for the purpose of accessing OWA or SSL VPN using their personal computers and a government-provided or personally-owned smart card reader. Support and additional information can be acquired through AKO - https://www.us.army.mil/suite/page/241504 or at the commercial website - http://militarycac.com/.
2. **PREREQUISITES**
You will need to know your AKO Username and Password ([https://www.us.army.mil](https://www.us.army.mil)) in order to download required root certificates during the software installation process. You should also have the following two pieces of essential hardware:

- A computer with Windows 10

- A USB smart card reader. Some laptops have a built-in smart card reader. If you are using a desktop, you will be required to provide a smart card reader. Smart card readers are available in a variety of shapes and sizes. SCM Microsystems SCR-3310 model works very well. Readers can be ordered from various online retailers like the ones listed below. On the respected sites, do a search for 'smart card reader'.
  - [http://www.cdw.com](http://www.cdw.com)
  - [http://www.amazon.com](http://www.amazon.com)
  - [http://www.buy.com](http://www.buy.com)
3. HARDWARE INSTALLATION INSTRUCTIONS

3.1. Smart Card Reader

In most cases, your smart card reader will install automatically with the Windows New Hardware Wizard or without user intervention.

3.1.1. Install Smart Card Reader Driver

3.1.1.1. Plug in your smart card reader into an available USB port on your computer.

3.1.1.2. If the drivers do not install automatically, follow the driver installation procedures for the smart card reader purchased.

3.1.2. Determine if Smart Card Reader Driver Installed Properly

Directions for determining if your smart card reader driver was installed properly can be found below according to the type of operating system you are running on your PC.

3.1.2.1. Open the Control Panel by typing 'control panel' in the “Type here to search” box by the Start button and hit enter

3.1.2.2. Select 'Hardware and Sound'

3.1.2.3. Click on 'Devices and Printers'

3.1.2.4. You will see your smart card reader in the device list.

3.1.2.5. If your smart card reader is not listed, you will need to download the correct driver for the hardware you purchased
4. SOFTWARE INSTALLATION INSTRUCTIONS

4.1. Software Required for OWA and SSL VPN

To access OWA, in addition to installing Smart Card Reader drivers, (See Section 3.1), you may also be required to install the following software:

- DoD Install Root 5.2 certificates
- ActivClient 7.1.0.153 (Should not be required with newer CAC please visit www.militarycac.com for installation instructions if needed.)

To access the SSL VPN, you must ensure that the following required software is installed on your computer:

- Microsoft Edge
- Java (Version 6 or higher)
- DoD InstallRoot 5.2 certificates
- ActivClient 7.1.0.153 (Should not be required with newer CAC please visit www.militarycac.com for installation instructions if needed.)

**WARNING**

If you have a PIV II compliant CAC (back shows: "GEMAL TO DLGX4 144" or "Oberthur ID One 128 v5.5 Dual" at the top above the magnetic strip), you may be able to use your CAC without installing ActivClient. More details are found at http://militarycac.com/activclient.htm.

4.2 Install Java 8


4.3. Install DoD InstallRoot 5.2

4.3.1. Automatic installation

4.3.1.1. Open Microsoft Edge and navigate to https://iasecontent.disa.mil/pkipke/InstallRoot_5.2x32_NonAdmin.msi

4.3.1.2. Select ‘Run’
4.3.1.3. The following steps are to be completed in order:

Select *Next >*

Leave the default installation location, then select *Next >*
Select Next >

Select Install
Wait for it.

Select *Run InstallRoot*.
Click *Install Certificates*

Select *Yes*, (this screen may show 2 - 3 times) as it is installing the DoD Root CA 2, 3, 4, & 5 certificates.
Select OK (your number of Adds will vary)
5. **ACCESSING SOF-U OWA**

5.1. Put your CAC into the smart card reader

5.2. Go to 'https://mail.socom.mil/my.policy' read the agreement text and if you agree, click 'OK, Proceed to Application'

5.3. Choose your 'DoD EMAIL' Digital Certificate and click 'OK' (left). Then enter your PIN and click 'OK' (right)
6. SSL VPN CONFIGURATION

You will need to disable User Access Control (UAC). It will remain off until your first successful SSL VPN connection. After successfully connecting, you can re-enable UAC. It is strongly recommended by Microsoft that you re-enable this feature. When it is turned off, all users are considered Administrators on the system and can add, remove and modify programs and the system even if the user was created as a Limited User.

6.1. In the ‘Type here to search’ to the right of the start menu type ‘Internet Options’ and hit ‘Enter’

6.2. Click on the 'Security' tab (left), then click on 'Local intranet' (right)
6.3. Click on 'Sites' (left) then click 'Advanced' (right)

6.4. Enter 'https://usasoc-ssl.soc.mil' and click 'Add', (left) then click 'Close' (right)
Click 'OK' (left) on the 'Security' tab; click 'Custom level...' (right)

6.5. Scroll down and select the radio button beside 'Prompt' under 'Download unsigned ActiveX controls'. (left) Then scroll down and select the radio button beside 'Prompt' under 'Initialize and script ActiveX controls not marked as safe for scripting' (right)
6.6. Then click 'OK'

6.7. Using Microsoft Edge go to 'https://usasoc-ssl.soc.mil'
6.8. When prompted, select your 'DoD Email' Certificate and click 'OK' (left) Then enter your CAC PIN and click 'OK' (right)

6.9. When prompted, click 'Continue'

At this time unless you received an authentication error you are connected the VPN you will need

6.10. You will right click on the windows icon and select ‘Run’ (note doing these steps in the Windows 10 search box will result in a connection error. You must use the Run function)
6.11. Type the following in the Run dialog box:

```
mstsc /v:usasoc-remote.sof.socds.mil
```

6.12. You will be prompted to enter your CAC PIN

6.13. If the following certificate error warning is displayed select ‘Yes’
THE FOLLOWING 3 STEPS MAY BE NEED TWICE


6.15. Select the CAC card icon beside the key icon under the Username and password prompt

6.16. Enter your CAC Pin and hit Enter
6.17. If the following warning pops up select ‘Yes’

You will now be fully logged into the USASOC SSL/VPN
## APPENDIX E. ACRONYMS

### Table 1: List of Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AD</td>
<td>Active Directory</td>
</tr>
<tr>
<td>AKO</td>
<td>Army Knowledge Online</td>
</tr>
<tr>
<td>CAC</td>
<td>Common Access Card</td>
</tr>
<tr>
<td>CIO</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>COR</td>
<td>Contracting Officer Representative</td>
</tr>
<tr>
<td>DoD</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>EITC</td>
<td>Enterprise Information Technology Contract</td>
</tr>
<tr>
<td>EMAIL</td>
<td>Electronic Mail</td>
</tr>
<tr>
<td>IE</td>
<td>Internet Explorer</td>
</tr>
<tr>
<td>NIPR</td>
<td>Non-Secure Internet Protocol Routable</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>OWA</td>
<td>Outlook Web Access</td>
</tr>
<tr>
<td>PC</td>
<td>Personal Computer</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number</td>
</tr>
<tr>
<td>POC</td>
<td>Point of Contact</td>
</tr>
<tr>
<td>RDP</td>
<td>Remote Desktop Protocol</td>
</tr>
<tr>
<td>SSL</td>
<td>Single Sockets Layer</td>
</tr>
<tr>
<td>UAC</td>
<td>User Access Control</td>
</tr>
<tr>
<td>USASOC</td>
<td>United States Army Special Operations Command</td>
</tr>
<tr>
<td>USB</td>
<td>Universal Serial Bus</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
</tbody>
</table>