SOFNET-U OWA Access for Users Migrated to the O365 Cloud (Personal Computer use only)

March 2020 | Version 1.1

Section 1.0: INTRODUCTION

This document provides instructions for gaining access to SOFNET-U OWA for users who have been migrated to the O365 Cloud.

Section 2.0: URL FOR OWA ACCESS

For SOCOM users migrated to the cloud from their home (personal) computer, paste the following URL into a web browser to access Outlook Web Access (OWA): https://webmail.socom.mil

Note: Users will not have access to other O365 web applications like Word, Excel, Teams, OneDrive, etc., from personal computers.

2.1 PKI-protected Content

Those who have a valid, authorized need to access DoD Public Key Infrastructure (PKI)-protected information but do not have access to a government site or government-furnished equipment need to configure their home systems to access PKI-protected content.

Accessing DoD PKI-protected information is most commonly achieved using the PKI certificates stored on your Common Access Card (CAC). The certificates on your CAC can allow you to perform routine activities such as accessing OWA, signing documents, and viewing other PKI-protected information online.

Section 3.0: WINDOWS COMPUTERS

This section provides instructions to users with Windows computers.

3.1 Prerequisites and Installation

The following are needed to access SOFNET-U OWA from a Windows computer:

- CAC
- Card reader

To get started using your CAC, follow these steps:

- Obtain a card reader. You may take your CAC reader from your SOFNET-U system home with you. (Ensure you bring it back to SOCOM when you return to work)
- 2. They are also available from many commercial sources.
- Install DoD root certificates with InstallRoot (32-bit, 64-bit or Non Administrator) from the following source: <u>https://public.cyber.mil/pkipke/end-users/</u>
- 4. Enable your machine to recognize your CAC certificates and DoD websites as trusted by running the InstallRoot utility (32-bit, 64-bit or Non Administrator) to install the DoD CA certificates on Microsoft operating systems. If you are running an alternate operating system such as Mac OS or Linux, you can import certificates from the PKCS 7 bundle.

To do this, complete the following steps:

a. Enter the following URL into a Web browser: https://public.cyber.mil/pki-pke/end-users/page

The DoD Cyber Exchange page opens, as shown below.

Developers			КВ		
For RAs, LRAs, KRAs & TAs	0	FBCA Cross-Certificate Remover 1.15 User	234.46	30 Nov 2018	Tools (19) Configuration Files (1)
Policies	_	Guide	KD		
Mobile Devices & Purebred >	•	FBCA Cross-Certificate Remover 1.18	38.95 KB	24 Oct 2019	TARGET AUDIENCE
RSS Feeds	0	InstallRoot 5.2: User Guide	2.56 MB	30 Nov 2018	Administrators (16)
	0		27.98 MB	24 Oct 2019	End Users (11)
Training	0	InstallRoot 5.5 NIPR 64-bit Windows Installer	28.62 MB	24 Oct 2019	 DoD Partners (6) Developers (3) Purebred Agents (1)
	0	InstallRoot 5.5 NIPR Non-Administrator 32-bit	27.73 MB	24 Oct 2019	
Web Content Filtering / Break and		Windows Installer			RAs, LRAs, KRAs and T

b. Click **Tools** on the left sidebar of the page, then click the **InstallRoot link**, as shown in the figure.

The InstallRoot Setup Wizard page opens, as shown below.



c. Click Next.

The Choose a File Location page opens, as shown below.



d. Click Next.

The InstallRoot Features page opens, as shown below.

🖟 InstallRoot Setup	:
InstallRoot Features	
Select the features you wish to install.	
Graphical Interface	
Command-Line Tool	
Windows Service	
	< Back Next >

e. Ensure all three options are checked, then click Next.

The Begin Installation of InstallRoot page opens, as shown below:

歸 InstallRoot Setup	×
Begin installation of InstallRoot	
Click Install to begin the installation. If you want to review or chang click Back. Close the window to exit the wizard.	e any of your installation settings,
	< Back

f. Click Install

The DoD PKE page opens, as shown below:

6	
non	
DVE	
FRE	
stalRoot has been successfully installed.	
Run InstallRoot	
d	
Close	
	The second secon

g. After the program finishes running, click *Run InstallRoot The InstallRoot 5.5 page opens, as shown below.*

Se InstallRoot 5.5	1 <u></u> 1		×
Home Store Group Certificate Help			
Install Online Update Preferences Save Restart as Settings Administrator Application			
✓ Install DoD Certificates			•
× Install ECA Certificates 💿		1	. -
× Install JITC Certificates 🐵			
× Install WCF Certificates			•

h. Click Install Certificates

After complete, you will see several new certificates, as shown in the figure below.

InstallRoot 5.5				_		>	×
Home Store Group Certifica	te Help						
💆 👰 🛄 .							
Install Online Preferences Sav Certificates Update Setti	ngs	×					
Actions Application		afarmed as calling					
🐉 Microsoft Local Computer	update and found new T	AMP messages.					
 Install DoD Certificates 							*
Subject	lssuer	Sub-location	Installed	Subscrib	ed		
💡 DoD Root CA 2	DoD Root CA 2	ROOT	×	×		_	
💡 DoD Root CA 3	DoD Root CA 3	ROOT	×	×			
💡 DoD Root CA 4	DoD Root CA 4	ROOT	×	×			
💡 DoD Root CA 5	DoD Root CA 5	ROOT	×	×			
💡 DoD Root CA 5	DoD Root CA 5	ROOT	×	×			
💡 DOD EMAIL CA-33	DoD Root CA 2	INTERMEDIATE	×	×			
💡 DOD EMAIL CA-34	DoD Root CA 2	INTERMEDIATE	×	×			
💡 DOD EMAIL CA-39	DoD Root CA 2	INTERMEDIATE	×	×			
💡 DOD EMAIL CA-40	DoD Root CA 2	INTERMEDIATE	v	×			
💡 DOD EMAIL CA-41	DoD Root CA 3	INTERMEDIATE	×	×			
	DoD Poot CA 2	INTEDMEDIATE					
× Install ECA Certificates 💿							*
× Install JITC Certificates 💿						۲	•
× Install WCF Certificates							*

This will complete the installation of certificates.

i. Close the *InstallRoot* program.

Running this InstallRoot makes certificates available to your operating system and/or browser, if necessary. This is a one-time requirement; you should not need to run InstallRoot again.

3.2 Accessing OWA

You should now be able to go to https://webmail.socom.mil and access your OWA by following these steps.

1. Read the Department of Defense greeting page, then click **OK**, **Proceed to Application**.



2. When prompted for a CAC certificate, select your email certificate.

Note: You **may** see a F5 page and on the left panel a small "Click Here to Continue" link. If you do, then click *the link*.



- 3. When prompted enter your PIN.
- 4. When prompted by the Microsoft Trident, as shown below enter your *full SMTP email address*.

	Microsoft			
Sig	gn in			1
so	omeone@example	.com		_
Can	't access your accour	nt?		
			Next	
				1

Next, it will briefy show a message like the one in the figure below, then it should open your OWA.

Microso	ft	
Taking v	ou to your	
organiza	tion's sign-in page	
Cancel		

Section 4.0: MAC COMPUTERS

This section provides instructions to users with Mac computers.

4.1 Prerequisites and Installation

The following are needed to access SOFNET-U OWA from a Mac computer:

- CAC
- Card reader

To get started using your CAC on your Mac OS X, follow these steps:

1. Obtain a card reader.

Typically, Macs do not come with card readers; therefore, an external card reader is necessary. At this time, the best advice for obtaining a card reader is through working with your home component. In addition, please review the **DoD CAC Reader Specifications** for more information regarding card reader requirements.

 Download and install the OS X Smartcard Services package. The OS X Smartcard Services Package allows a Mac to read and communicate with a smart card. In order for your machine to recognize your CAC certificates and DoD websites as trusted, the installer will load the DoD CA certificates on OS X. Address the cross-certificate chaining Issue.

These instructions walk through adjusting the trust settings on the Interoperability Root CA (IRCA) > DoD Root CA 2 and the US DoD CCEB IRCA 1 > DoD Root CA 2 certificates to prevent cross-certificate chaining issues.

Note: This can make it appear that your certificates are issued by roots other than the DoD Root CA 2 and can prevent access to DoD websites.

3. Configure Chrome and Safari, if necessary.

Safari and Google Chrome rely on Keychain Access properly recognizing your CAC certificates.

- a. In Finder, navigate to **Go > Utilities** and launch *KeychainAccess.app.*
- b. Verify that your CAC certificates are recognized and displayed in Keychain Access.

	11. A. 1108570515 Reycham.	Ge	
Keychains PIV-DOE.JOHN.A.1108570519 iogin SystemCACertificates System	Configure DOE.JOHN.A.110 Issued by: DOD CA-30 Expires: Thursday, Oct This certificate is val	8570519 ober 8, 2015 7:59: lid	59 PM Eastern Daylight Ti
System Roots	Name	A Kind	Expires
	DOE.JOHN.A.1108570519	certificate	Oct 8, 2015 7:59:59 PM
	DOE.JOHN.A.1108570519	certificate	Oct 8, 2015 7:59:59 PM
Category	DOE.JOHN.A.1108570519	certificate	Oct 8, 2015 7:59:59 Pf
All Items All Items Secure Notes My Certificates Keys			
Certificates	_		
A	(+) (L) Copy]	3 items	

Note: CACs are currently made of different kinds of card stock. To determine what card stock you have, look at the back of your CAC above the magnetic strip. Most CACs are supported by the Smartcard Services package, however Oberthur ID One 128 v5.5 CACs are not. Third-party middleware is available that will support these CACS; two such options are Thursby Software's PKard and Centrify's Express for Smart Card.

c. Configure Firefox to trust the DoD PKI and use the CAC. To configure Firefox to communicate with the CAC, follow these steps to install the DoD root and intermediate CA certificates into the Firefox NSS trust store, load the CoolKey library, and ensure the Online Certificate Status Protocol (OCSP) is being used to perform revocation checking.

Once this is done, follow the steps in Section 3.2 above, Accessing OWA.

Note: The USSOCOM CSD provides IT service support to the SOF warriors and communities across the globe. We are open 24 hours a day, 365 days a year. Call toll-free **833-818-8751**.