

## ATHOC SELF-SERVICE LOGIN INSTRUCTIONS (PRODUCTION)

DIA deployed the ATHOC alert notification system that will primarily be used to rapidly and effectively alert DIA personnel about emergencies or incidents that affect one's duty location. The system will be referred to as the 'DIA Alert Self-Service system' from this point forward.

Listed below are the steps to login to the DIA Alert Self-Service system. This site allows alert recipients to update their profile so they can receive alerts across different platforms. The login steps can vary slightly depending where a user logs in (government facility, vendor facility, home), type of computer used (Mac, PC), and browser selected (Chrome, Internet Explorer, Edge, Safari).

### Pre-Requisites:

1. You must have a DIA issued CAC card that works on NIPRNet.
2. The DIA Alert Self-Service system is best used with Chrome. It can also be used with Internet Explorer, Edge and Safari.
3. The DIA Alert Self-Service system cannot be used with Firefox.
4. All users accessing the DIA Alert Self-Service system must have the following certificates installed on their local machine.
  - [Intermediate Certification Authorities should contain DOD SW CA-53](#)
  - [Trusted Root Certification Authorities should contain DoD Root CA 3](#)

If the above certificates are not installed on the local machine, users will not be prompted for their CAC credentials after hitting the URL in Step 1. Chrome users will see an error similar to the one below - while Internet Explorer, Edge, and Safari users will see something slightly different. In this particular situation, the user is unable to access the DIA Alert Self-Service system and should proceed to the bottom of this document and follow the procedures to install the latest Windows or Mac client certificates.



## Your connection is not private

Attackers might be trying to steal your information from **athoc-test.dodiis.mil** (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR\_CERT\_INVALID

☐ Help improve Chrome security by sending [URLs of some pages you visit, limited system information, and some page content](#) to Google. [Privacy policy](#)

Hide advanced

Reload

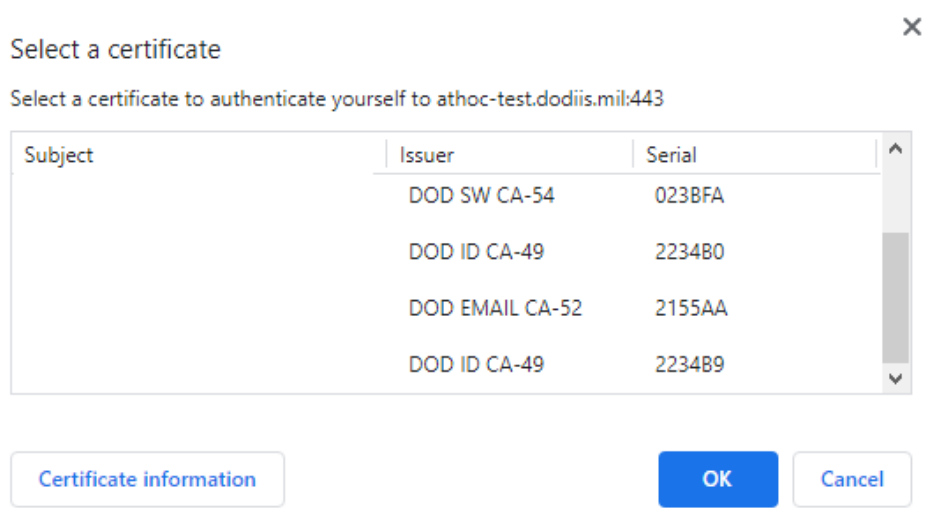
athoc-test.dodiis.mil normally uses encryption to protect your information. When Google Chrome tried to connect to athoc-test.dodiis.mil this time, the website sent back unusual and incorrect credentials. This may happen when an attacker is trying to pretend to be athoc-test.dodiis.mil, or a Wi-Fi sign-in screen has interrupted the connection. Your information is still secure because Google Chrome stopped the connection before any data was exchanged.

You cannot visit athoc-test.dodiis.mil right now because the website sent scrambled credentials that Google Chrome cannot process. Network errors and attacks are usually temporary, so this page will probably work later.

**Step 1:** Open your browser and go to the following URL:

<https://athoc.dodiis.mil/SelfService/dia>

**Step 2:** You should be prompted to select a CAC certificate. Select your PIV-Auth certificate (a.k.a. Authentication certificate) and click **OK**. If you are at a DIA facility, this should be the certificate you used to log into your workstation. If you are not at a DIA facility, you might need to follow the instructions below to identify the PIV-Auth certificate.



**Note:** Most DoDIIS NIPRNet users will have migrated to their PIV-Auth certificate when attempting to access the DIA Alert Management system. However, there is a slight chance that you will attempt to access the DIA Alert Management system prior to your migration. In this scenario, try your 'Email' certificate and proceed to the steps below. You will be notified of your migration to the PIV-Auth certificate through DoDIIS email similar to below.

*Dear Customer,*

*On Wednesday, August 26, 2020 at 12:00 AM EST, you will be transitioned to PIV login for your NIPRNet account d145995. After this time, you will need to select the certificate containing the text **124589519197005@mil** when logging in.*

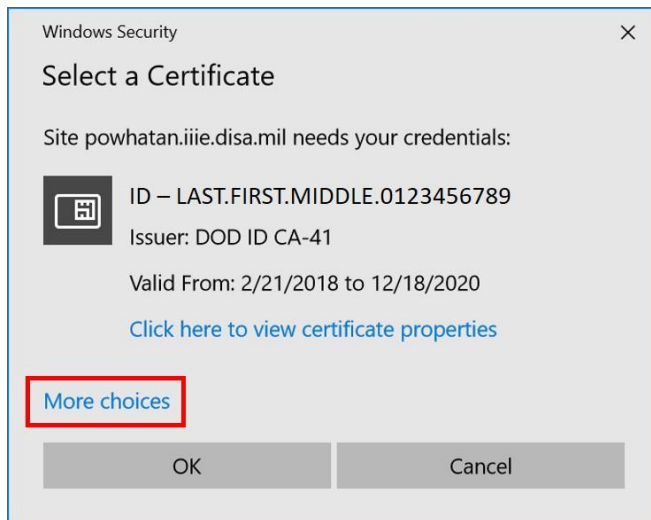
*To ensure you experience a smooth transition, please ensure that you are logged out of your DoDIIS NIPRNET workstation prior to **Wednesday, August 26, 2020 at 12:00 AM EST**. For more information, please visit the [CAC Modernization](#) page.*

### **How to Identify your PIV-Auth certificate**

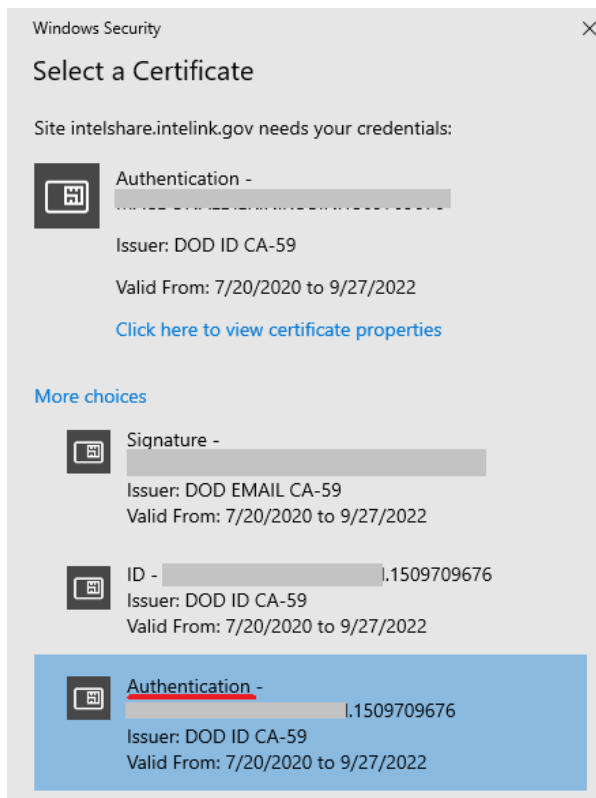
To find out which certificate is your PIV-Auth certificate, you will need to be able to distinguish between the various certificates available for authentication when prompted in order to select the correct certificate for a given site. The instructions that follow describe how to identify your PIV-Auth certificate in common browser certificate prompts.

## Internet Explorer (IE) & Edge - PIV-Auth Certificate

In Windows IE and Edge browsers, the PIV-Auth certificate can usually be identified directly within the Windows certificate prompt. If the PIV-Auth is not easily identifiable as the default certificate displayed, click **More choices**.



On workstations running ActiveClient, the PIV-Auth certificate will be displayed as:

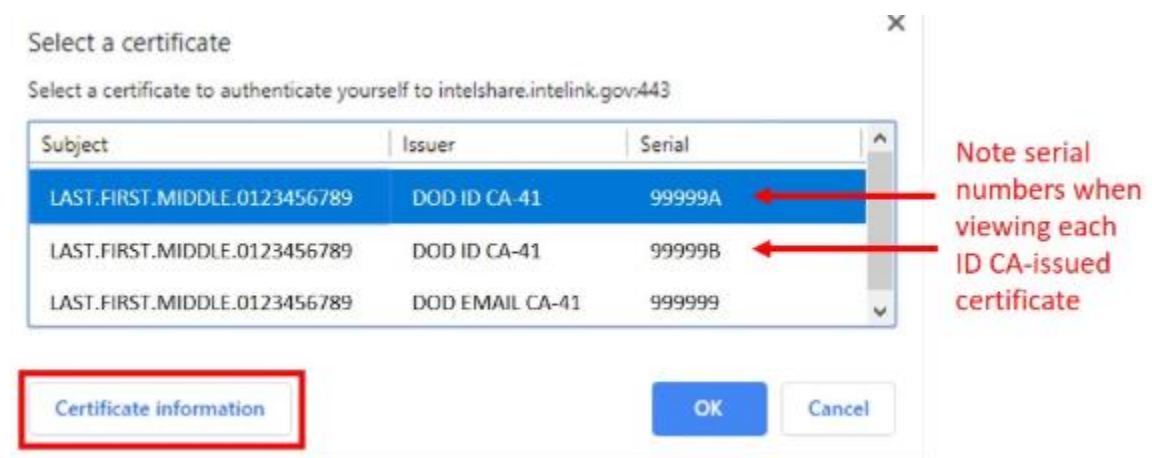


## Chrome – PIV-Auth Certificate

Chrome does not allow users to easily distinguish between certificates in the main certificate prompt. However, the certificates can be uniquely identified by serial number within the main prompt. As a result, users can initially perform additional steps to determine which serial number corresponds to their PIV-Auth certificate and make a note of that serial number for use going forward.

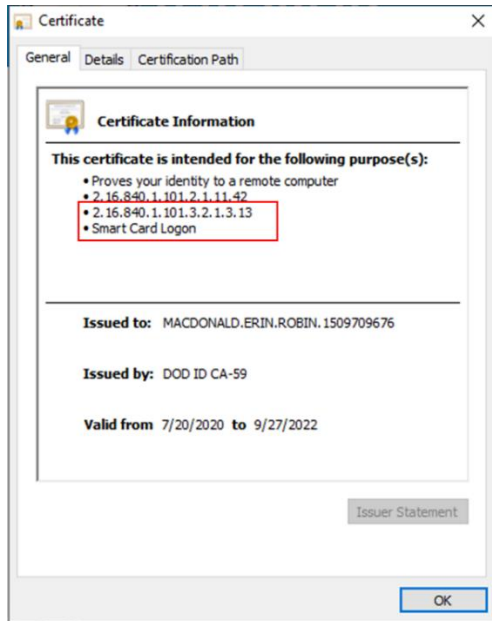
PIV-Auth certificates have the following characteristics that can be used to distinguish them from other authentication certificates on the CAC:

- a. Are issued from DOD ID CAs (not EMAIL CAs) This differentiates the PIV-Auth certificate from the Email Signature certificate.
  - b. Contain Subject Alternative Name (SAN) and Extended/Enhanced Key Usage (EKU) extensions This differentiates the PIV-Auth certificate from the ID certificate.
1. From the main certificate prompt, select the first **DoD ID CA-issued certificate** and click **Certificate information** to view the certificate.



2. In the certificate display, look for "**Smart Card Logon**" in the list of certificate purposes: this will be present in the PIV-Auth certificate but not the ID certificate.

Note: The inclusion of the numerical string 2.16.840.1.101.3.2.1.3.13 in this list is also unique to the PIV-Auth certificate. Each person will have a unique numerical string like this in their PIV-Auth certificate.

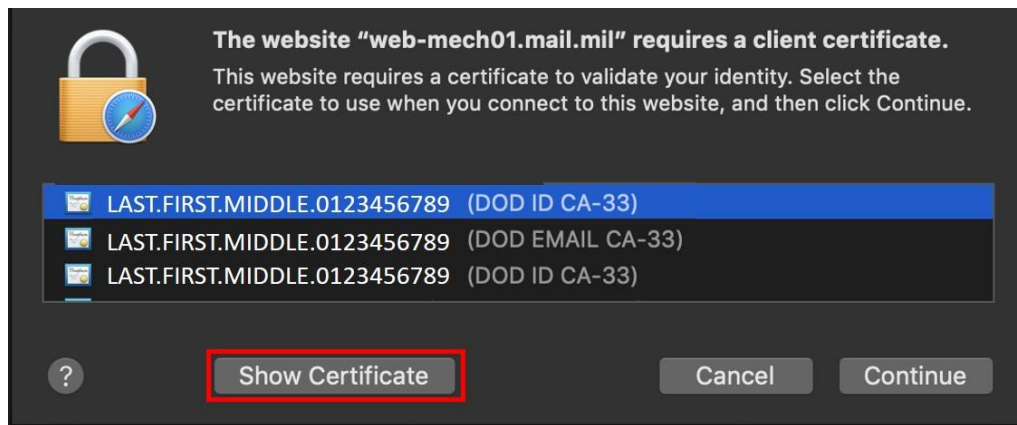


3. If the first certificate does not include that purpose, repeat the process in **step 1** but select the second **DoD ID CA-issued certificate**.
4. Make a note of the serial number of the certificate that contains the "**Smart Card Logon**" purpose for easy future selection.

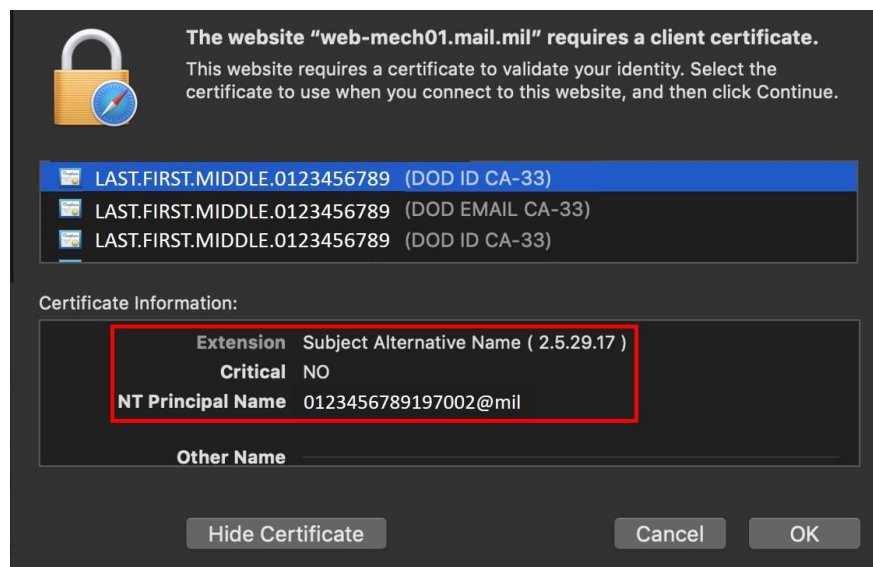
### **MacOS – PIV-Auth Certificate**

MacOS does not allow users to easily distinguish between certificates in the main certificate prompt. In order to identify the PIV-Auth certificate, users must view certificate details.

1. From the main certificate prompt, select the first **DoD ID CA-issued certificate** and click **Show Certificate** to view the certificate.



2. Look for the Subject Alternative Name extension containing an NT Principal Name value of 16 digits @mil. This is the PIV-Auth certificate.



**Step 3:** Once the PIV-Auth certificate is selected, enter your CAC pin and click **OK**.

**Step 4:** You will be routed to the 'U.S. Government' authorization screen where you will click **Agree**.

## WARNING STATEMENT

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:

The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

At any time, the USG may inspect and seize data stored on this IS.

Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

This IS includes security measures (e.g., authorization and access controls) to protect USG interests--not for your personal benefit or privacy.

Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

[Agree](#)

**Step 5:** If you selected the correct certificate you will be taken into the DIA Alert Self-Service system. Proceed to step 6.

**Note:** If an incorrect certificate was selected, you will be routed to one of the screens shown below. At this point, you should clear your browser cache, shutdown your browser, re-open a new browser, and execute steps 1 and 2 again. Be sure to carefully follow the procedures to select your PIV-Auth certificate when attempting to login.

Server Error in '/SelfService' Application.

### Runtime Error

**Description:** An application error occurred on the server. The current custom error settings for this application prevent the details of the application error from being viewed remotely (for security reasons). It could, however, be viewed by browsers running on the local server machine.

**Details:** To enable the details of this specific error message to be viewable on remote machines, please create a <customErrors> tag within a "web.config" configuration file located in the root directory of the current web application. This <customErrors> tag should then have its "mode" attribute set to "Off".

<!-- Web.Config Configuration File -->

```
<configuration>
  <system.web>
    <customErrors mode="Off"/>
  </system.web>
</configuration>
```

**Notes:** The current error page you are seeing can be replaced by a custom error page by modifying the 'defaultRedirect' attribute of the application's <customErrors> configuration tag to point to a custom error page URL.

```
<!-- Web.Config Configuration File -->

<configuration>
  <system.web>
    <customErrors mode="RemoteOnly" defaultRedirect="mycustompage.htm"/>
  </system.web>
</configuration>
```





DIA

## An error has occurred

We're sorry, we were unable to retrieve your Smart Card credentials. Please contact your administrator.

**BlackBerry AtHoc**



BlackBerry AtHoc

English (US) Copyright ©2019 BlackBerry Limited. All Rights Reserved.

**Step 6:** Once you are in the application select the **My Profile** tab across the top of the page.

athoc-test.dodis.mil/selfservice/ActivityFeed

BlackBerry AtHoc **Inbox** My Profile DIA ▾

Home

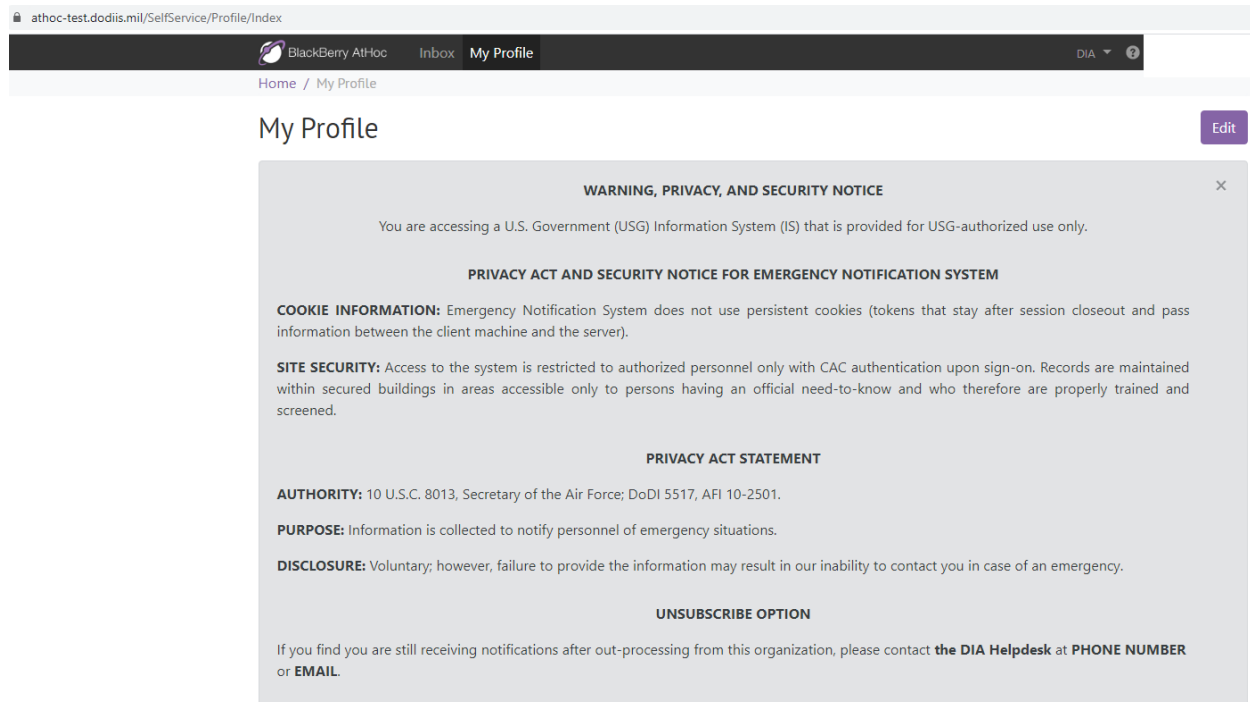
### Inbox

Updated 08/05/2020 14:26:05

Search by Title or Body   Advanced

Showing 1 - 19 of 19 items

**Step 7:** Click the **Edit** button on the top right of the screen to update your profile.



athoc-test.dodis.mil/SelfService/Profile/Index

BlackBerry Ath-Hoc Inbox My Profile DIA ?

Home / My Profile

## My Profile [Edit](#)

**WARNING, PRIVACY, AND SECURITY NOTICE** ×

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

**PRIVACY ACT AND SECURITY NOTICE FOR EMERGENCY NOTIFICATION SYSTEM**

**COOKIE INFORMATION:** Emergency Notification System does not use persistent cookies (tokens that stay after session closeout and pass information between the client machine and the server).

**SITE SECURITY:** Access to the system is restricted to authorized personnel only with CAC authentication upon sign-on. Records are maintained within secured buildings in areas accessible only to persons having an official need-to-know and who therefore are properly trained and screened.

**PRIVACY ACT STATEMENT**

**AUTHORITY:** 10 U.S.C. 8013, Secretary of the Air Force; DoDI 5517, AFI 10-2501.

**PURPOSE:** Information is collected to notify personnel of emergency situations.

**DISCLOSURE:** Voluntary; however, failure to provide the information may result in our inability to contact you in case of an emergency.

**UNSUBSCRIBE OPTION**

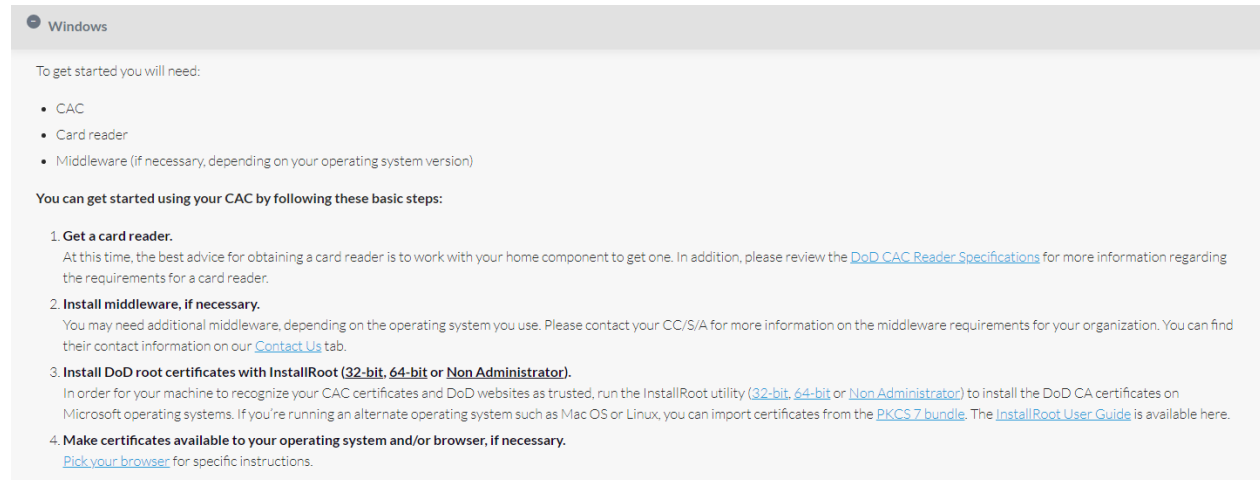
If you find you are still receiving notifications after out-processing from this organization, please contact **the DIA Helpdesk** at **PHONE NUMBER** or **EMAIL**.

**Step 8:** Update your profile to receive alert notifications to your email, phone, and text messaging device. You can also enter your work location to receive location based alerts. Click **Save** at the top right of the page when you're finished updating your profile.

# DOD Certificates Installation Guide for Windows OS

**Step 1:** Go to this website to do a fresh install of the latest DoD certificates: <https://public.cyber.mil/pki-pke/end-users/getting-started>

**Step 2:** Expand the Windows section.



The screenshot shows a web page titled "Windows" with a sub-header "To get started you will need:". Below this is a bulleted list: "• CAC", "• Card reader", and "• Middleware (if necessary, depending on your operating system version)". A section titled "You can get started using your CAC by following these basic steps:" follows, containing four numbered steps. Step 1 is "Get a card reader." with a note about working with the home component and a link to "DoD CAC Reader Specifications". Step 2 is "Install middleware, if necessary." with a note about contacting the CC/S/A for middleware requirements and a link to "Contact Us". Step 3 is "Install DoD root certificates with InstallRoot (32-bit, 64-bit or Non Administrator)." with a detailed note about running the InstallRoot utility and links to "32-bit", "64-bit", "Non Administrator", and "PKCS 7 bundle". Step 4 is "Make certificates available to your operating system and/or browser, if necessary." with a link to "Pick your browser".

Windows

To get started you will need:

- CAC
- Card reader
- Middleware (if necessary, depending on your operating system version)

You can get started using your CAC by following these basic steps:

1. **Get a card reader.**  
At this time, the best advice for obtaining a card reader is to work with your home component to get one. In addition, please review the [DoD CAC Reader Specifications](#) for more information regarding the requirements for a card reader.
2. **Install middleware, if necessary.**  
You may need additional middleware, depending on the operating system you use. Please contact your CC/S/A for more information on the middleware requirements for your organization. You can find their contact information on our [Contact Us](#) tab.
3. **Install DoD root certificates with InstallRoot (32-bit, 64-bit or Non Administrator).**  
In order for your machine to recognize your CAC certificates and DoD websites as trusted, run the InstallRoot utility ([32-bit](#), [64-bit](#) or [Non Administrator](#)) to install the DoD CA certificates on Microsoft operating systems. If you're running an alternate operating system such as Mac OS or Linux, you can import certificates from the [PKCS 7 bundle](#). The [InstallRoot User Guide](#) is available here.
4. **Make certificates available to your operating system and/or browser, if necessary.**  
[Pick your browser](#) for specific instructions.

**Step 3:** Assuming you have a CAC Reader you can skip step 1. You can also skip number 2.

**Step 4:** Execute number 3.


- a. Most people have a 64-bit machine at home and have administrative rights on their own machine. If this is the case, click on the 64-bit hyperlink and proceed. **MOST PEOPLE WILL SELECT THIS OPTION.**
- b. If you have an older machine at home, you have to install the 32-bit version. If this is the case, click on the 32-bit link and proceed.
- c. If for some reason you do not have administrative access on your own machine, click on the Non-Administrator hyperlink and proceed.

**Step 5:** Execute number 4. Click on the "Pick your browser" hyperlink and follow the set of instructions for IE and Chrome.

# DOD Certificates Installation Guide for MAC OS

**Step 1:** Go to this website to do a fresh install of the latest DoD certificates: <https://public.cyber.mil/pki-pke/end-users/getting-started>

**Step 2:** Expand the MAC section.


 Mac

To get started you will need:

- CAC (see [note](#) below)
- Card reader

You can get started using your CAC on your Mac OS X system by following these basic steps:

- 1. Get a card reader**  
Typically Macs do not come with card readers and 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.
- 2. 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. Please refer to [this page](#) for specific installation instructions.
- 3. 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. 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.
- 4. 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

 Keychain Access

**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.

**Step 3:** Assuming you have a CAC Reader you can skip number 1.

**Step 4:** Execute number 2.

**Step 5:** Execute number 4 to configure Chrome and Safari.