

Frequently Asked Questions (FAQs)

NCAISS not loading in Firefox?

To access NCAISS using Firefox, you'll need to uncheck a setting in advanced options.

- Click on Tools->Options->Advanced
- Click on "Encryption"
- Uncheck "Use TLS 1.0"
- Click "Ok" and restart

What is NCAISS?

NCAISS is a web portal that provides identity and access management services to authenticate users and provide access to different DSS applications.

What is the Single Sign-on?

Single Sign-On capability makes it possible for users of NCAISS to log in once and access multiple systems/services. The advantage - users only need one account with a registered CAC/ECA to access all of the systems/services that are integrated within NCAISS.

How do I create an NCAISS account?

From the NCAISS login page, click on the "Register for an account" button to navigate to the self-enrollment form. Once the Self Enrollment form opens, please fill out the required information, and click "Next". You will be given the opportunity to review your information and continue. Once you have submitted your form, NCAISS will create your account and notify you via email when your account is ready for use.

During self-enrollment you will be required to enter a password. Once your account has been created, you will need this password to register your CAC/ECA. PLEASE keep passwords safe and DO NOT provide to others.

Which email address do I use for my NCAISS account?

You should use the email address that has been assigned by the organization for which you are accessing NCAISS.

How do I get notified that my DSS account has been created?

Once your account has been created an email will be sent to you, which will include your AccountID that you will need to use to register your CAC/ECA with NCAISS.

What happens if I do not receive the email notification from NCAISS?

NCAISS emails are sent from the following address: DoNotReply@dss.mil . It is possible that emails from this address may get filtered into your junk/spam mailbox. To avoid missing future notifications from NCAISS, please add DoNotReply@dss.mil to your safe senders list.

Which PKI Certificates does NCAISS accept?

NCAISS accepts all DoD-Approved PKIs. To find a list of all DoD-Approved PKIs go to <http://iase.disa.mil/pki-pke/interoperability/>

How do I associate CAC/ECA with my account?

From the NCAISS login page, navigate to the Register CAC/ECA page by clicking on "Register Certificate" button. Once on the Register CAC/ECA page, provide your NCAISS Account ID and password, click "Submit" and select your certificate when prompted. You will be presented with two certificate options – an authentication certificate and an email certificate. You must select the authentication certificate. Upon successful registration, you will be able to login to NCAISS using your CAC/ECA certificate by clicking on the "CAC/ECA Login" button.

What is a Common Access Card (CAC)?

A CAC is a United States Department of Defense (DoD) smart card issued as standard identification for active-duty military personnel, reserve personnel, civilian employees, other non-DoD government employees, state employees of the National Guard, and eligible contractor personnel.

The CAC is used as a general identification card as well as for authentication to enable access to DoD computers, networks, and certain DoD facilities. It also serves as an identification card under the Geneva Conventions. The CAC enables data encryption and cryptographic signing of email messages, facilitating the use of PKI authentication tools, and establishes an authoritative process for the use of identity credentials.

What are ECA certificates?

ECA certificates are PKI certificates that have been issued by a DoD-approved External Certificate Authority. They are issued to private contractors and other personnel who are affiliated with the DoD. Similar to CAC, an ECA certificate is used for authentication to enable access to DoD computers, networks, and certain DoD websites.

From where do I get an ECA certificate?

NCAISS supports ECA certificates that have been issued from the following three companies:

- VeriSign
- ORC
- IdenTrust

Check their website for more information on how to request a certificate.

Which certificate do I select when registering my CAC or ECA?

When registering your certificate, and subsequently logging into NCAISS, you are presented with two certificate options – an authentication certificate and an email certificate. You must select the authentication certificate when using NCAISS. Note: the email certificate can be easily identified as its name contains “Email”.

How do I log into NCAISS using my CAC/ECA?

From the NCAISS login page, click on the "CAC/ECA Login" button, and select your CAC/ECA certificate when prompted. You may be required to enter PIN number for your CAC/ECA. Upon successful authentication, you will be redirected to the NCAISS Home Page.

How do I reset my password?

A user has two options available for resetting a password.

1. Use the Forgotten Password self-service module, which is accessible through the "Register Certificate" button on the NCAISS login page. To use the Forgotten Password self-service module:
 - Navigate to the Register Certificate page and click the "Forgot your password?" link, you will then enter in your AccountID, which will take you to the reset password page, there you'll answer the three authentication questions that you set during the self-enrollment process
 - Then you will be asked to enter in a new password that is compliant with DoD standards.
 - Note: If you answer your authentication questions wrong three (3) times your account will become locked and you won't be able to reset your password. If this occurs, you'll have to call the DSS Call Center to have them unlock your account.
2. Contact the DSS Call Center ([DSS Call Center Information](#))

How can I find help?

For additional questions about using NCAISS refer to the NCAISS User Guide ([NCAISS User Guide](#)). If you need further assistance using NCAISS you may contact the DoD Security Services (Call) Center ([DSS Call Center Information](#)).

How do I report abuse or misuse within NCAISS?

Abuse and/or misuse within the NCAISS should be reported to the DoD Security Services (Call) Center ([DSS Call Center Information](#)). Abuse and/or misuse can include (but is not limited to) gaining unauthorized access to an NCAISS Role or DSS Application, sharing application login credentials with another person, knowingly granting access to an unauthorized user, etc.

CAC error message "Page cannot be displayed"?

There are two known circumstances when this will apply: the user has attempted to login or register an expired certificate, or the user has canceled out of the PIN entry window for their CAC. To rectify this

problem, close the existing browser window and open a new window; this will clear the cache and enable the user to continue.

To verify the expiration on your certificate using IE, select your certificate from the Select a Certificate window, highlight the correct certificate (see the “**Which certificate do I select when registering my CAC or ECA?**” FAQ for additional information), and click "Click here to view certificate properties." The certificate validity dates will be displayed at the bottom of the “General” tab. Your CAC also displays the expiration date on the right side on the face of the card. If you require further assistance with your CAC, you may refer to the DoD CAC website (<http://www.cac.mil>) or your organization’s IT support center.

Setting up Firefox to work with Card readers?

To Manually add ActivClient to Firefox:

- Open Firefox, go to **Tools** then **Options**.
- Select the **Advance** tab and then select the **Encryption** sub-tab and click Security Devices.
- The Device Manager window should appear, click on **Load**
 - Change the Module name to MYCAC or something else easy for you to identify
 - Click on Browse and navigate to
 - 32-bit windows: c:\Program files\ActivIdentity\Activclient\acpkcs211.dll
 - 64-bit windows: c:\Program files(x86)\ActivIdentity\Activclient\acpkcs211.dll
 - Click Open
 - Click OK; this result may prompt for your PIN to import the certificates.
- Click **OK** and look for **MYCAC** in the Security Modules and Devices list, if it is there then you are good to go. Click **OK** on all windows and you should now be able to log into CAC enabled Websites.
- If prompted for certificate information, most likely the DoD root Certs do not have defined exceptions within Firefox, just select and add to complete.
- The master password is your PIN to your CAC card.

Please visit www.militarycac.com -> Click “how Do I?” -> Click on “Use with Firefox” for more help