

Frequently Asked Questions

DISA Storefront User Administration Functions include creating and maintaining your account and roles.

GENERAL INFORMATION

Q: What browsers are supported by DISA Storefront?

ACCOUNT CREATION

Q: Do I need an account to access DISA Storefront?

Q: How do I create an account?

CAC LOG-IN

Q: How do I log in using a CAC with Internet Explorer?

Q: How can I view my certificates in Internet Explorer?

Q: How do I log in using a CAC with Mozilla Firefox?

Q: The Client Authentication window does not appear after clicking "Log in with CAC." How do I resolve this?

REQUESTING ROLES

Q: How do I request a role?

Q: What roles do I need?

Q: Who approves my roles?

Q: How long does it take for role approvals/denials?

ACCOUNT MAINTENANCE

Q: My certificate is expired. How do I receive a new one?

Q: My certificate is revoked. How do I receive a new one?

Q: What do I do if I get a new CAC due to replacing a lost or expired CAC/PKI card?

Q: What if I leave or change positions and no longer need an account?

Q: What if I change positions and am no longer responsible for performing requesting and/or approval functions?

Q: If I move from one agency to another do I need to create a new USERID and get roles again?

Q: What is 'Change User Info' used for?

Q: What is the 'Manage Routing' link used for? Who uses this link?

ERROR MESSAGES

Q: I see an error page indicating that an error has occurred with my CAC log in. What does this mean?

Q: After placing my CAC in the reader, I get the following message: "You have three (3) attempts to correctly enter your Personal Identification Number for your CAC." Why am I receiving this message?

If your question is not included in this list of FAQs, please contact *DISA Customer Care Center at (618) 692-0032, DSN850.*

What browsers are supported by DISA Storefront?

Internet Explorer (IE) is the recommended browser for certificate registration and log in to DISA Storefront. DISA Storefront also supports the browsers Google Chrome and Mozilla Firefox. Please see the CAC LOG-IN section for more information on using DISA Storefront with Google Chrome and Mozilla Firefox.

ACCOUNT CREATION

Do I need an account to access DISA Storefront?

You must create an account and request the appropriate role(s) for your account to have access to DISA Storefront. If you do not have a DISA Storefront account please see ‘How do I create an account?’ in the next section.

DISA.mil also provides information about the services that DISA provides.

How do I create an account?

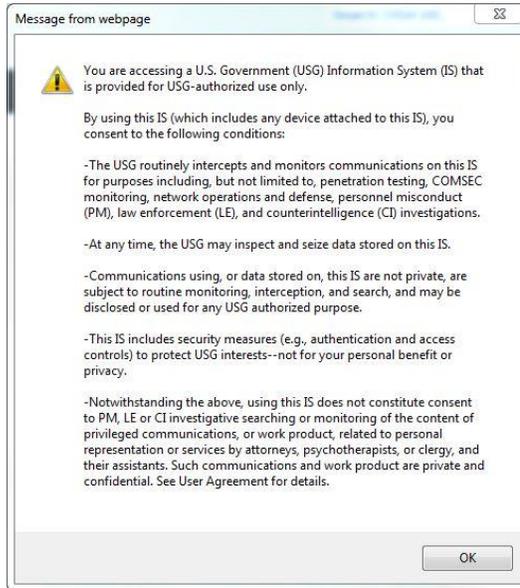
1. Insert CAC into the CAC reader.
2. Open the Internet Explorer browser and navigate to the DISA Direct Home page at <https://www.disadirect.disa.mil>.
3. The “Choose a digital certificate” window will appear, displaying the user’s certificate(s). Select the certificate; click “OK”. [Note: More than one certificate may be displayed; see Section 1.3 for instructions on viewing certificate details.



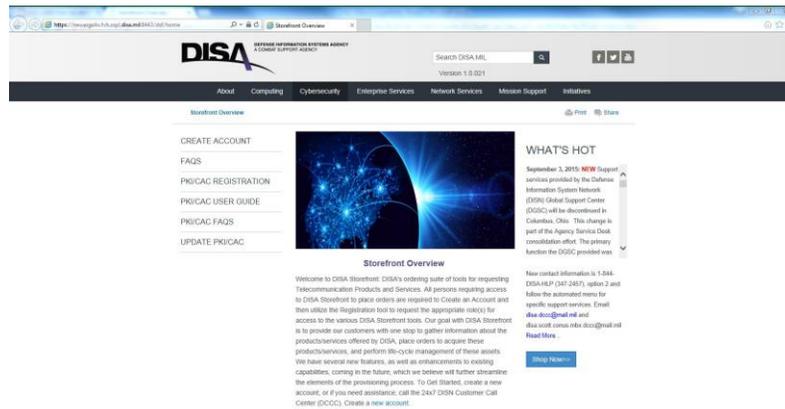
4. The “ActivClient Login – Enter PIN” window appears. Enter the CAC pin; and click "OK".



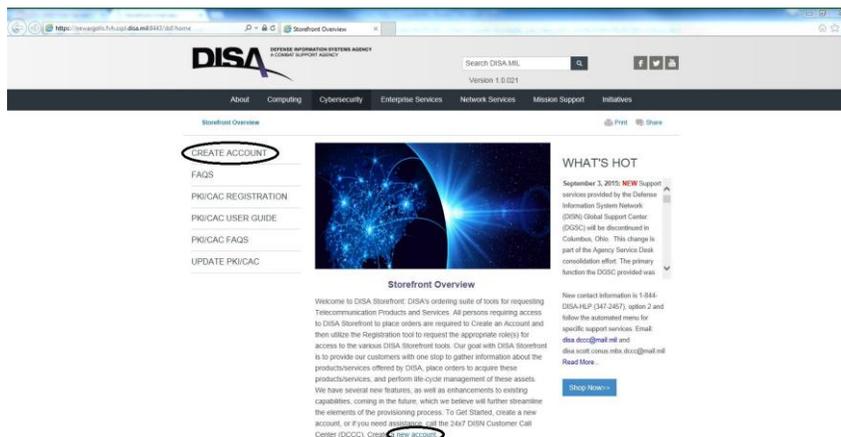
- The system will display a disclaimer notice; click "OK" to continue.



- The DISA Direct home page appears.



- From here select "Create Account" on the left hand side or "New Account" at the bottom of the page.



- Fill out all fields with an * next to them with the appropriate information. NOTE: If you selected the Order Now button on DISA.mil, DISA Storefront or TIBI application via links or bookmarks, you will be directed to the login page. From there, if you don't have an account, you may also select the "Create Account" link, which will bring you to this page.

The screenshot shows the 'Create Userid' form on the DISA Storefront. The form is titled 'Create Userid' and includes a search bar for DISA.MIL. The form is divided into several sections: 'ACCOUNT INFORMATION', 'CHANGE USER INFO', 'ROLE INFORMATION', and 'REQUEST NEW ROLE(S)'. The 'Create Userid' section includes a 'Submit' button and a 'View PKUCAC Certificate' link. The form also includes a 'Phone Number' section with fields for 'Cell Phone', 'DIN Phone', 'Pager', 'Fax', and 'User E-mail'.

- Select "submit" at the bottom of the page once completed.
- You will see the following message at the top of the page once your account has been successfully created. "The save was successful. Your new user account is USERID."
- You may now request the desired role for your new account. For help doing this please the 'Requesting Role(s)' page.

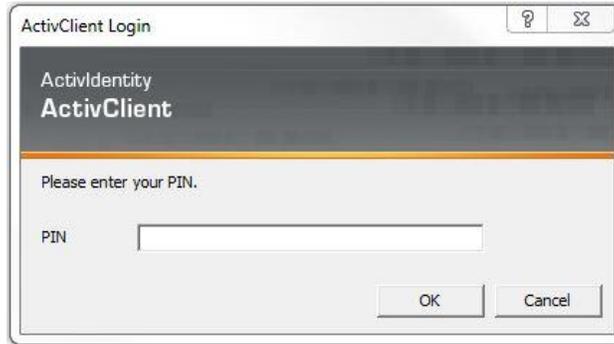
CAC LOG-IN

How do I log in using a CAC with Internet Explorer?

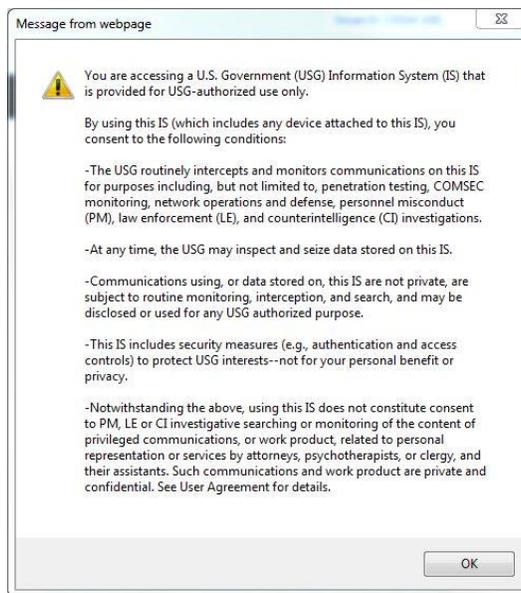
- Insert CAC into the CAC reader.
- Open the Internet Explorer browser and navigate to the DISA Direct Home page at <https://www.disadirect.disa.mil>.
- The "Choose a digital certificate" window will appear, displaying the user's certificate(s). Select the certificate; click "OK".



- The “ActivClient Login – Enter PIN” window appears. Enter the CAC pin; and click "OK".



- The system will display a disclaimer notice; click "OK" to continue.



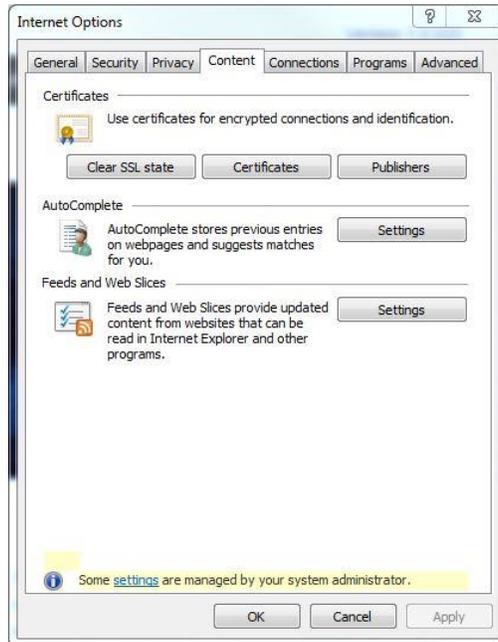
- The DISA Direct home page appears. If you have registered your CAC, you can access any application you are authorized.
- Select ‘Shop Now’ in the lower right corner of the Storefront Overview page.



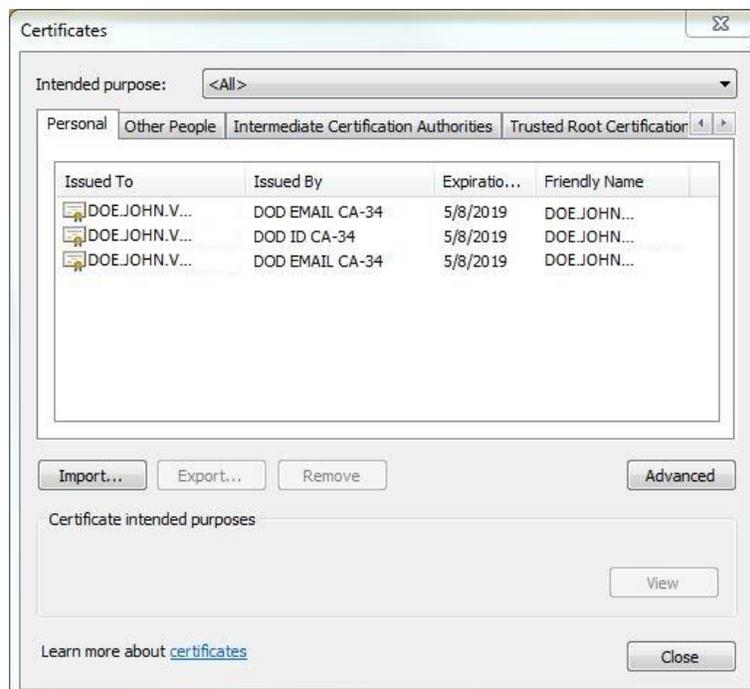
- The ‘Storefront Login’ page will now appear. Select the correct USERID and then click ‘Use PKI/CAC’ to log in.

How can I view my certificates in Internet Explorer?

1. Open an Internet Explorer browser session.
2. From the top menu, navigate to Tools/Internet Options/Content; the following window will display.
3. Click on “Certificates”.



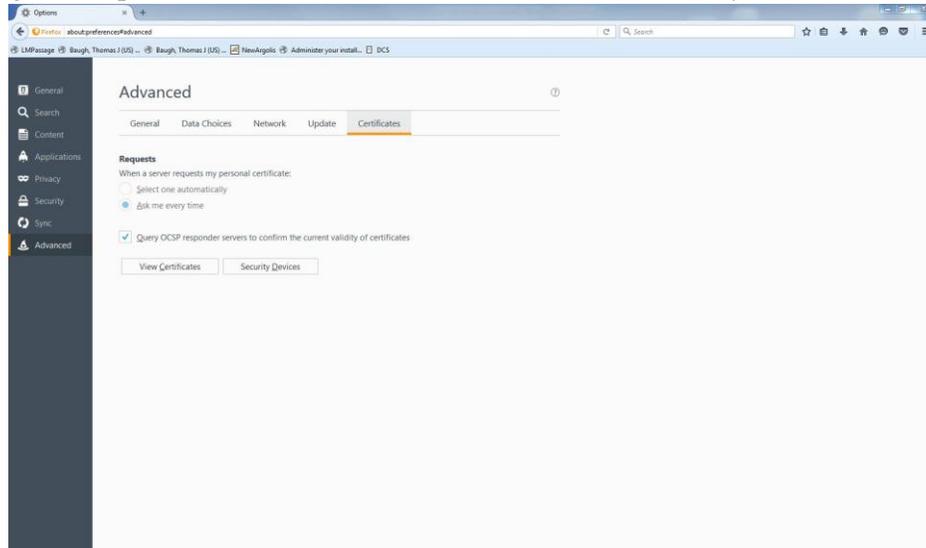
4. The “Certificates” window will appear. You should see the certificates that are associated with your CAC.



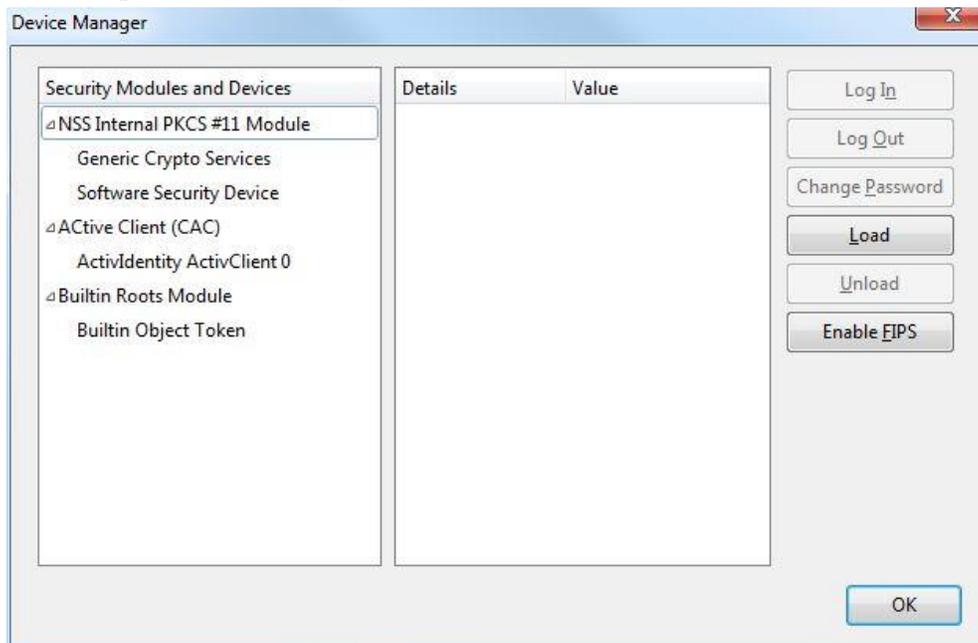
How do I log in using a CAC with Mozilla Firefox?

NOTE: Mozilla Firefox requires additional configuration steps prior to enable your CAC authentication prior to logging into DISA Storefront.

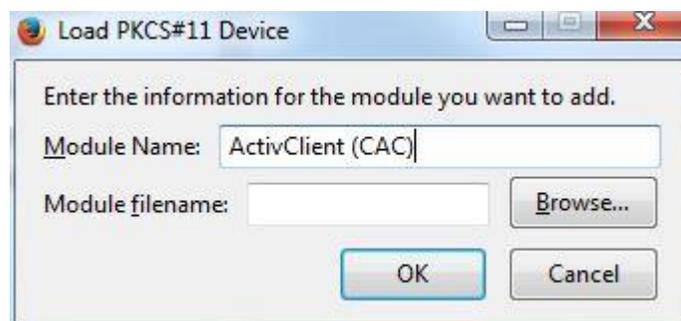
1. Navigate to Options/Advanced/Certificates. Then click on Security Devices.



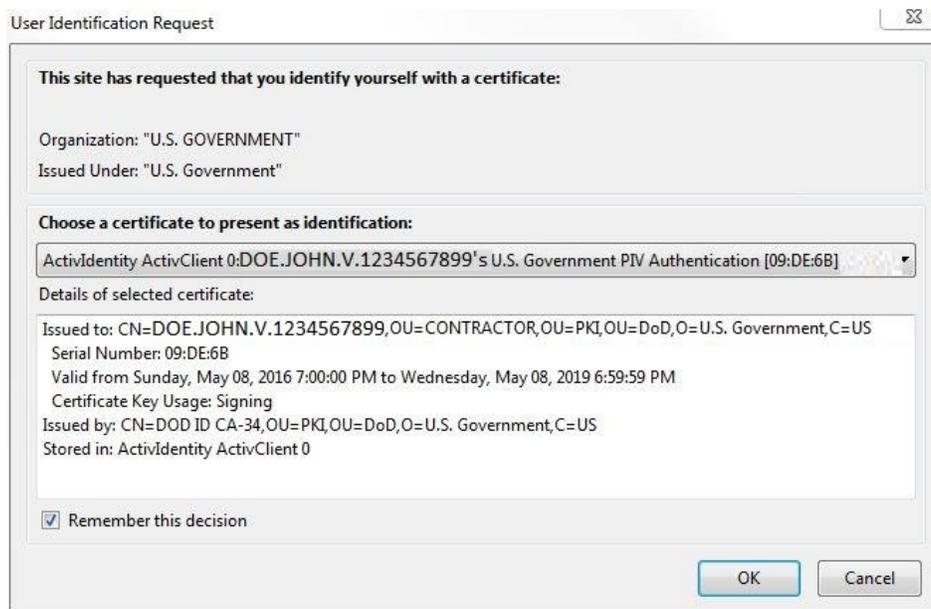
2. The “Device Manager” window will appear. If you do not have a tab that says ActivClient (CAC) then proceed by clicking on Load



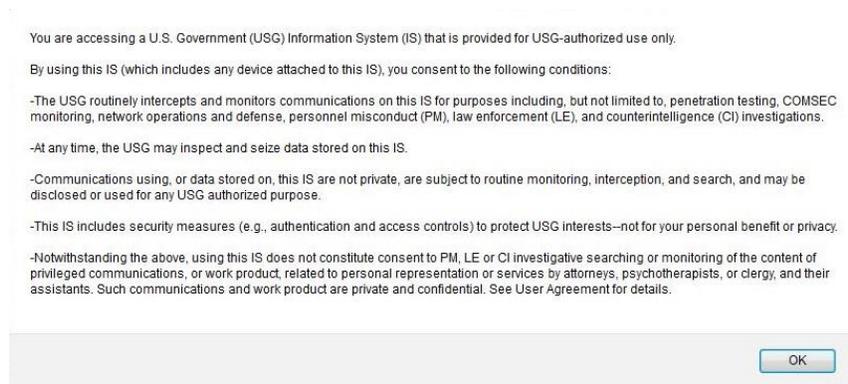
3. Once the “Load PKCS#11 Device’ window appears change the module name to “ActivClient (CAC)”



4. Click on Browse and navigate to the following file path “C:\Program Files (x86)\ActivIdentity\ActivClient\acpkcs211.dll”
5. Press OK on the Load PKCS#11 Device Window and the Device Manager Window. Now you must close Mozilla Firefox.
6. Reopen Mozilla Firefox and insert CAC into the CAC reader.
7. Open the Mozilla Firefox browser and navigate to the DISA Direct Home page at <https://www.disadirect.disa.mil>.
8. The “User Identification Request” window will appear. Choose your non-email certificate and press OK.



9. The system will display a disclaimer notice; click "OK" to continue.



10. The DISA Direct home page appears. If you have registered your CAC, you can access any application you are authorized.

The Client Authentication window does not appear after clicking "Log in" How do I resolve this?

You may need to close the active browser window(s) and open a new one to attempt the process again. This scenario will occur when a user has cancelled out of a portion of the registration process. The browser will store a previous selection in its cache, which will require the user to clear the cache before making a different selection.

REQUESTING ROLES

How do I request a role?

1. Once logged into DISA Storefront you will be directed to the 'Manage Account' page.
2. Select 'REQUEST NEW ROLE(S)'
3. The 'Request New Role(s)' page is displayed. Select the appropriate choice of three options to select the type of role(s) needed.

Request Authorized Official Role(s)-This is the most common option where the most roles are located -Continue to step 4.

Registration Official (RO)- This role is limited to a few persons within the Agency– Continue to Step 7.

Request Subscription Official (SO) role- This role is limited to a few persons within the Agency– Continue to Step 10.

DISA STOREFRONT FAQs



Manage Account » Request New Role(s)

- ACCOUNT INFORMATION
- CHANGE USER INFO
- ROLE INFORMATION
- REQUEST NEW ROLE(S)

Request Role(s)

GENERAL DISA STOREFRONT ROLES

If you wish to perform one or more of the following functions, select **Request Authorized Official Role(s)**.

- Create, submit Telecom Requests (TRs), and access the tracking tools (Track TR); select the **Authorized Requesting Official (ARO)** role.
- Be part of the routing of the TR approval process only and access the tracking tools (Track TR); select the **Authorized Approving Official (AAO)** role.
- Approve PDC(s) and funding within the TR routing process and access and update TIBI, select the **Lead Authorized Funding Official (LAFO)** role.
Note: This role is also responsible for approving role requests for AFOs and Authorized Billing Officials (ABOs).
- Approve PDC(s) and funding within the TR routing process and access and update Telecommunications Inventory Billing Information (TIBI); select the **Authorized Funding Official (AFO)** role. Be prepared to list the Program Designator Codes (PDCs) you want access to.
- View only access to TIBI, select the **Authorized Billing Official (ABO)** role. Be prepared to list the Program Designator Codes (PDCs) you want access to.
- Create, edit, and delete routing offices, lists, and matrices for your Agency TR Routing Rules, select the **Routing List Official (RLO)** role.
- Create, edit, and delete routing offices, lists, and matrices for your Agency TR Routing Rules, select the **Routing List Official (RLO)** role.
Note: This role is usually limited to a few persons within the Agency.
- Maintain the Central Address Directory (CAD) Point of Contact (POC) records for your Agency/Organization, select the **Address Directory Official (ADO)** role.
Note: This role is usually limited to a few persons within the Agency.
- Access the tracking tools (Track TR) only; select the **Authorized Tracking Official (ATO)** role.
- Access and run Queries against the DISA storefront database, select the **Authorized Query Official (AQO)** role.
- Access TIBI to view IT Requirements Only information, select the **IT Requirements Reviewer (ITRR)** role.

DISA ONLY ROLES

- Create, submit TRs, view requirements for all Agencies, access the tracking tools (Track TR), and TIBI read only access; select the **Authorized Provisioning Official (APO)** role.
Note: This role is for DISA personnel that require access to all agency requirements; otherwise the ARO role is sufficient.
- DISA/DITCO contracting personnel only. View TIBI for all agencies; select the **Contracting Official (CO)** role.
- DISA/Chief Financial Executive (CFE) personnel only. View and update all PDCs in TIBI; select the **Billing Team Member (BTM)** role.

HIGH LEVEL AGENCY ROLES ONLY

If you are responsible for assigning roles for personnel within your Agency, select **Request Registration Official (RO) role**.

Note: This role is usually limited to a few persons within the Agency.

If you are responsible for ordering and managing DISN Subscriptions within your Agency, select **Request Subscription Official (SO) role**.

Note: This role is usually limited to a few persons within the Agency.

About DISA

- Our Work
- Our Leaders
- Our Organization Structure
- Our Strategic Plan
- Our History
- Issuances/Policy

News & Events

- News
- Press Releases
- Conferences/Events
- General Inquiries
- Media Inquiries

Services

- Command & Control
- Computing
- Contracting
- Cybersecurity
- Engineering
- Enterprise Services
- Network Services
- Spectrum
- Testing

Initiatives

- Acquisition of Services
- Cyberworkforce Development
- Defense Collaboration Services
- Joint Regional Security Stacks (JRSS)
- Service Support Environment

Careers at DISA

- Search for Opportunities
- Federal Benefits
- Leadership/Training Benefits
- Work/Life Benefits
- Pathways Program
- New Employees

Legal & Regulatory

- Accessibility Notice
- Inventories & Schedules
- FOIA
- No Fear Act
- Whistleblower
- Security/Privacy
- Privacy Impact Assessments
- Privacy Office
- Data Rights
- Intellectual Property

Defense Information Systems Agency

Contact Us

Newsletter Sign-Up

Enter Email Address

DISA STOREFRONT FAQs

4. Select the 'Request Authorized Official Role(s)' link.

[Back to Top](#)

The screenshot shows the DISA Storefront interface. At the top, there is a search bar for 'DISA.MIL' and a 'Logout' button. Below the search bar is a navigation menu with links: 'Return to DISA Storefront', 'Manage Account', 'Manage Roles', and 'Manage Routing'. The main content area is titled 'Request New Role(s)' and contains a sidebar with links: 'ACCOUNT INFORMATION', 'CHANGE USER INFO', 'ROLE INFORMATION', and 'REQUEST NEW ROLE(S)'. The main content area is titled 'Request Role' and contains a dropdown menu with the following options: 'Address Directory Official (ADO)', 'Authorized Approving Official (AAO)', 'Authorized Billing Official (ABO)', and 'Authorized Funding Official (AFO)'. Below the dropdown menu is a 'Continue' button. A note at the bottom of the page reads: 'To select more than one role in the Listbox, hold the control key down.'

5. On the Request Roles page, select the role or roles you require to perform your functions. You may select multiple roles by holding the CTRL button on your keyboard and clicking on the desired roles. When clicking on a role, the description is given below. You can also view role descriptions under 'ROLE INFORMATION' -> 'View Roles Descriptions'. Once all the roles that are desired are selected, press 'Continue'.
6. On the 'Get Approval' page, select an RO Approver and click continue. The approvers are notified of your request. It may take 24 hours for the role to be approved. Once your roles are approved, you may log into DISA Storefront or TIBI
7. If you selected 'Request Registration Official (RO) role' in step 3, the following 'Request Role' page is displayed.

The screenshot shows the DISA Storefront interface. At the top, there is a search bar for 'DISA.MIL' and a 'Logout' button. Below the search bar is a navigation menu with links: 'Return to DISA Storefront', 'Manage Account', 'Manage Roles', and 'Manage Routing'. The main content area is titled 'Request New Role(s)' and contains a sidebar with links: 'ACCOUNT INFORMATION', 'CHANGE USER INFO', 'ROLE INFORMATION', and 'REQUEST NEW ROLE(S)'. The main content area is titled 'Request Role' and contains a blue box with the following text: 'Select the box and click the 'I Accept' button to continue with the role request or click the 'Return to Registration Home' button.' Below the blue box is a checkbox with the following text: 'I understand that I have the responsibility of approving or denying role requests submitted by persons within my Agency. I will ensure that all role requests are approved or denied within a timely manner.' Below the checkbox are two buttons: 'I Accept' and 'Return to Registration Home'.

8. If you accept the responsibility of the RO role check the box and click 'I Accept'. If not, click 'return to Registration Home' to return to the previous page.
9. A request will be sent to the all TRAO's in your Agency. The TRAOs in your Agency who approve the RO requests are notified of your request. It may take 24 hours for the role to be approved. Once your roles are approved, you may log into DISA Storefront and perform Role approvals for your Agency.
10. If you selected 'Request Subscription Official (SO)' role in step 3, the TRAOs in your Agency who approve the SO requests are notified of your request. It may take 24 hours for the role to be approved. Once your roles are approved, you may log into DISA Storefront and Subscription Orders for your Agency.

What roles do I need?

[Back to Top](#)

The DISA Direct roles are dependent upon the user's responsibilities. For descriptions on the roles, select the 'Registration' hyperlink and 'Request New Roles'. Next select the 'View Role Descriptions'.

Who approves my roles?

Most roles are approved by a Registration Official of the same agency of the user requesting the role(s). The user selects Registration Officials from a list of names to send the role request to. Some roles require a TRAO or LAFO to approve, and some roles require that you complete and submit a 2875 form before your role request may be approved.

How long does it take for role approvals/denials?

Approvals/denials of roles are dependent upon the Registration Official. If the user does not get a reply back on the role request within 24 hours, advise the user contact the Registration Official(s) that the role request(s) was sent to.

ACCOUNT MAINTENANCE

My certificate is expired. How do I receive a new one?

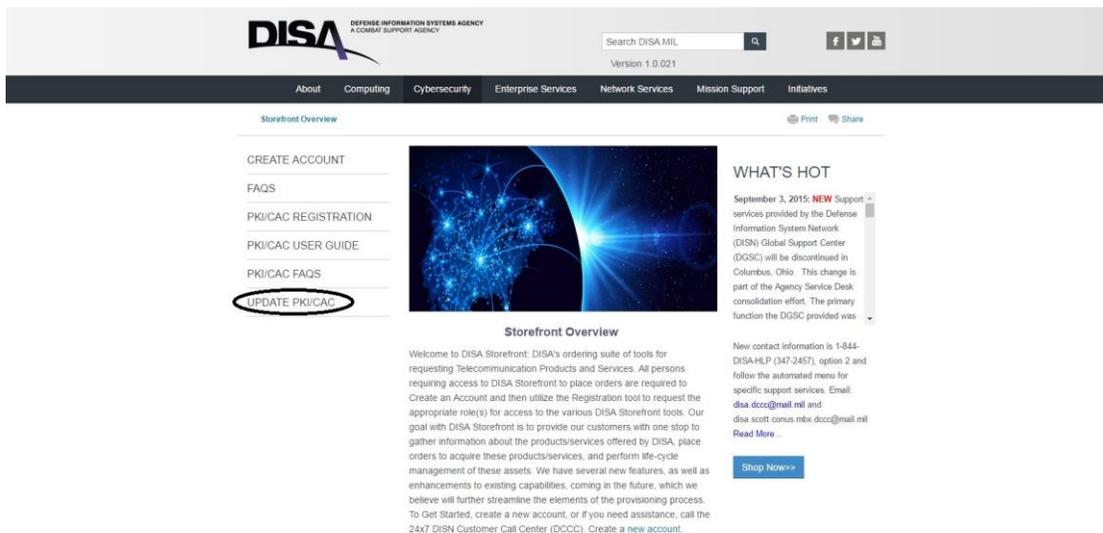
Each certificate has a validity period after which it expires. This period is set when the certificate is written to your CAC. Contact your local Security Officer.

My certificate is revoked. How do I receive a new one?

Your card may have been reported lost, stolen, or compromised. Contact your local Security Officer.

What do I do if I get a new CAC due to replacing a lost or expired CAC/PKI card?

The user must register their DISA Storefront account with the new CAC. From the Storefront Overview Page, select UPDATE PKI/CAC to associate the new CAC/PKI credential with your account(s).



What if I leave or change positions and no longer need an account?

[Back to Top](#)

Resolve outstanding activity in DISA Storefront, and then delete their existing Account by selecting the 'Change User Info' hyperlink on the 'Manage Account' page and then selecting the 'Delete USERID' on the bottom of the page. If you have an approver role and are a member of one or more approval offices, you must contact your RLO to have them remove your account from all approval offices before you can delete your account. Please coordinate with the RLO to ensure that alternate or replacement approvers have accounts created and are members of the approval office(s) before your account is deleted. If you have any DRAFT orders or Orders pending approval, you should either reassign the orders to another requestor or delete your obsolete orders.

What if I change positions and am no longer responsible for performing requesting and/or approval functions?

Resolve outstanding activity in DISA Storefront. If you no longer require any access to DISA Storefront or TIBI, delete your existing Account by selecting the 'Change User Info' hyperlink on the 'Manage Account' page and then selecting the 'Delete USERID' on the bottom of the page. If you still require access to TIBI or DISA Storefront for report or status information, retain your Account, but take the following actions.

If you have an approver role and are a member of one or more approval offices, you must contact your RLO to have them remove your account from all approval offices before. Please coordinate with the RLO to ensure that alternate or replacement approvers have accounts created and are members of the approval office(s).

If you have any DRAFT orders or Orders pending approval, you should either reassign the orders to another requestor or delete your obsolete orders.

If I move from one agency to another do I need to create a new USERID and get roles again?

Yes, the user should delete their existing account by selecting the 'Change User Info' hyperlink on the 'Manage Account' page and then selecting the 'Delete USERID' on the bottom of the page. The user will be required to create a new account and request roles with the new agency's Registration Officials.

What is 'Change User Info' used for?

The Change User Info application is used to modify the user's name, phone numbers, agency address information, and e-mail addresses. In addition, the user may change their password and also delete their USERID from this application.

What is the 'Manage Routing' link used for? Who uses this link?

Request Routing is an application that is accessed only by a DISA Direct User that has a role of Routing List Official (RLO). Each agency is required to have at least one RLO. This person is responsible for creating and maintaining the routing business rules for routing a TR. It is driven by the Program Designator Code (PDC).

I see an error page indicating that an error has occurred with my CAC log in. What does this mean?

This is likely due to an unavailable resource on DISA Direct. If the login page does not display your account(s) associated with our CAC/PKI, return to the Storefront Overview Page and select "Update PKI/CAC". This will reassociated your CAC with your accounts and often this resolves the issue. If the problem persists, please contact the DISA Customer Care Center at (618) 692-0032, DSN850.

After placing my CAC in the reader, I get the following message: "You have three (3) attempts to correctly enter your Personal Identification Number for your CAC." Why am I receiving this message?

After the third consecutive attempt, your CAC is locked and you will not have access to your PKI certificates. You may have your CAC unlocked at a CAC PIN Reset (CPR) workstation. DISA Customer Care Center at (618) 692-0032, DSN850.