



ISFD PKI Enablement

Background:

During the Fall of 2012 Defense Security Service will be integrating ISFD with the Identity Management (IdM) Solution, in compliance with the Joint Task Force-Global Network Operations requirement that "all components allow only certificate-based client authentication to private Department of Defense (DoD) Web servers using certificates issued by DoD Public Key Infrastructure (PKI) Certificate Authorities." Following the integration effort, ISFD users will no longer be permitted to access ISFD directly from the web, but will be required to authenticate through IdM prior to logging into ISFD.

Impact:

Users will be required to undergo a registration process* of up to three steps. Instructions detailing the ISFD PKI related registration processes are contained within the following pages**.

- 1) IdM Account Registration
- 2) Certificate (CAC/PKI) Registration
- 3) ISFD Account Request (new ISFD users only)

***This process serves as a precursor to Certificate-only access for ISFD, coming in 2013.**

****Final screens and data fields are subject to change.**



IdM Account Registration



IdM Account Registration

Step 1: The User navigates to <https://sso.dss.mil>.

Step 2: The IdM Solution displays the IdM Portal Disclaimer.

Step 3: The User selects “I Accept” to proceed.

Defense Security Service Portal

DSS Portal Disclaimer

This is a Department of Defense computer system. This computer system, including all related equipment, networks and network devices (specifically including internet access), are provided only for authorized U.S. government use. DoD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored. Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal or adverse action. Use of this system constitutes consent to monitoring for these purposes.

I Accept ← **Click here**

FOR OFFICIAL USE ONLY
Copyright © 2011 - Defense Security Service | All Rights Reserved.



IdM Account Registration

Step 4: The User is shown the unauthenticated IdM Portal page and clicks “Register for an account” to proceed.

Note: If you have recently used your CAC/ECA to login, you may not be prompted for your PIN and/or Certificate.

Login to DSS Portal

CAC/ECA Login

Register CAC/ECA

Register Certificate

Self Enrollment

Register for an account

Threat Advisory

Read more

Links

DSS Applications

- ★ ODAA

FAQs

- ★ How to Setup Firefox to use ActivClient?
- ★ DSS Portal not loading in Firefox?
- ★ What is the DSS Portal?
- ★ What is the Single Sign-on?
- ★ How do I register for a DSS account?
- ★ How to reset your password?
- ★ How do I associate CAC/ECA with my account?
- ★ From where do I get an ECA certificate?
- ★ How do I log into DSS Portal using my CAC/ECA?
- ★ How can I find help?
- ★ CAC error message "Page cannot be displayed"?
- ★ See ALL FAQs

Click here



IdM Account Registration

Step 5: The User is presented with the IdM Portal account request form, completes all required form fields, and clicks "Next".

Request a DSS Account

Complete the following form to create your DSS account

First Name * Middle Name Last Name *

Your Email Address * Confirm Email Address *

Password * Confirm Password *

Please answer at least 3 of the following questions.

Question	Answer
What is your Mother's Maiden Name?	<input type="text" value="Smith"/>
What is your Favorite Color?	<input type="text" value="Blue"/>
What was your First Car Model?	<input type="text" value="Ford"/>
What is your Place of Birth?	<input type="text"/>
What is your Favorite Movie?	<input type="text"/>
What is your First Child's Name?	<input type="text"/>
What was your High School Mascot?	<input type="text"/>
What is your Favorite Vacation Location?	<input type="text"/>

Complete form



Click Next



IdM Account Registration

Step 6: The User is shown a confirmation screen with the IdM Privacy Act Statement, reviews the user information, reads and accepts the terms of the privacy policy, and clicks "Register".

Step 7: The IdM Solution automatically creates the User's account and notifies the User via email.

User Information

Account Type	User
First name	John
Middle name	
Last name	Doe
E-mail address	john.doe@dss.mil

Privacy Act Statement

Please read and accept this following text

AUTHORITY:
Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.

PURPOSE:
To record names, and Social Security Numbers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form.

ROUTINE USES:
In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside DoD as a routine use pursuant to 5 U.S.C. 552a(b) (3) as follows: To a Federal, State, or local law enforcement agency when your agency becomes aware of a violation or possible violation of civil or criminal law; to the

I have read and understand the terms of the privacy policy.

Register

Edit

Cancel

Click here to acknowledge the privacy policy

Then click here



Certificate Registration



Certificate Registration

Step 1: The User navigates to <https://sso.dss.mil>.

Step 2: The IdM Solution displays the IdM Portal Disclaimer.

Step 3: The User selects “I Accept” to proceed.

Step 4: The User is shown the unauthenticated IdM Portal page and clicks “Register Certificate” to proceed.

Defense Security Service Portal

Note: If you have recently used your CAC/ECA to login, you may not be prompted for your PIN and/or Certificate.

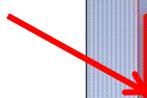
- Login to DSS Portal**
CAC/ECA Login
- Threat Advisory**
NTAS
NO ACTIVE ALERTS
www.DHS.gov/alerts
Read more
- FAQs**
 - How to Setup Firefox to use ActivClient?
 - DSS Portal not loading in Firefox?
 - What is the DSS Portal?
 - What is the Single Sign-on?
 - How do I register for a DSS account?
 - How to reset your password?
 - How do I associate CAC/ECA with my account?
 - From where do I get an ECA certificate?
 - How do I log into DSS Portal using my CAC/ECA?
 - How can I find help?
 - CAC error message "Page cannot be displayed"?
 - See ALL FAQs
- Register CAC/ECA**
Register Certificate
- Self Enrollment**
Register for an account
- Links**
- DSS Applications**
 - ODAA

Contact DSS | FAQs | Accessibility | USA.gov | Security and Privacy Notice | No Fear Act | FOIA | Terms of Use

FOR OFFICIAL USE ONLY

Copyright © 2011 - Defense Security Service | All Rights Reserved.

Click here





Certificate Registration

Step 5: The User enters their IdM Portal Account ID (supplied in the account creation email) and the password that he/she set during the self-enrollment process.

Step 6: The User clicks “Submit”.

Defense Security Service Portal

Home » CAC/ECA Register

Login to DSS Portal

CAC/ECA Login

Self Enrollment

Register for an account

Forgot your password?

Register CAC/ECA

Enter your Account ID and Password and click Submit to associate your CAC/ECA certificate account. You must have an account in order to register your CAC/ECA certificate.

Account ID: sl.aoadmin

Password: [masked]

Submit

Provide IdM Portal Username and Password

FAQs

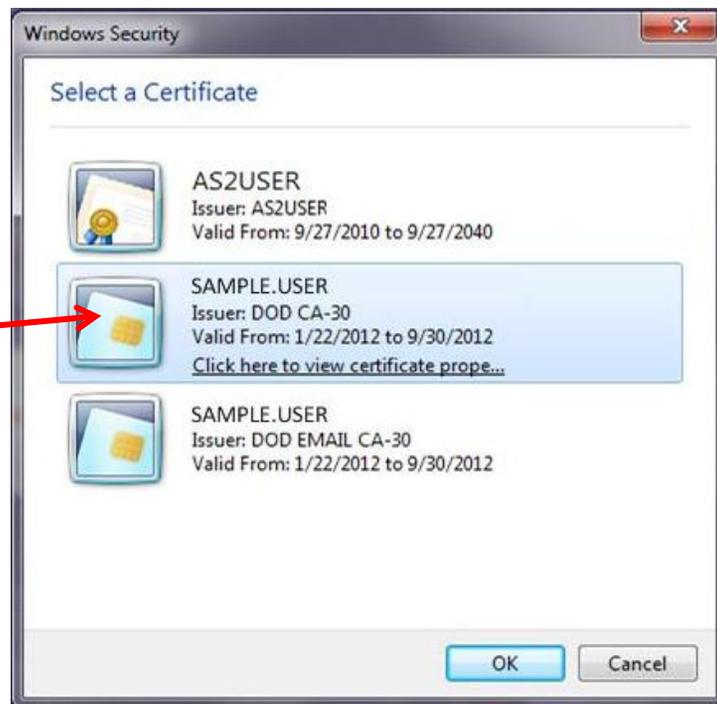
- How to Setup Firefox to use ActivClient?
- DSS Portal not loading in Firefox?
- What is the DSS Portal?
- What is the Single Sign-on?
- How do I register for a DSS account?
- How to reset your password?
- How do I associate CAC/ECA with my account?
- From where do I get an ECA certificate?
- How do I log into DSS Portal using my CAC/ECA?
- How can I find help?
- CAC error message "Page cannot be displayed"?
- See ALL FAQs



Certificate Registration

Step 7: Upon clicking submit, a pop-up box containing a list of digital certificates will appear; the User selects the appropriate certificate.

Select appropriate certificate





Certificate Registration

Step 8: The User enters his/her PIN.

ActivClient Login

ActivIdentity
ActivClient

Please enter your PIN.

PIN

OK Cancel

Enter PIN



Certificate Registration

Step 9: If successful, a confirmation message will be displayed informing the User that their certificate was registered successfully, and the User enters the IdM Portal.

The screenshot displays the Defense Security Service Portal. At the top, there is a banner with an American flag and the text "Defense Security Service Portal". Below the banner, a breadcrumb trail shows "Home » CAC/ECA Register".

On the left side, there are two main navigation boxes:

- Login to DSS Portal**: Contains a button labeled "CAC/ECA Login".
- Self Enrollment**: Contains a button labeled "Register for an account".

On the right side, there is a confirmation message:

i Your CAC/ECA certificate has been registered successfully. You may now Login with your new CAC/ECA certificate. **Note: You will not be prompted for PIN and/or Certificate.**

Below the message is a section titled "FAQs" with a list of questions:

- ★ How to Setup Firefox to use ActivClient?
- ★ DSS Portal not loading in Firefox?
- ★ What is the DSS Portal?
- ★ What is the Single Sign-on?
- ★ How do I register for a DSS account?
- ★ How to reset your password?
- ★ How do I associate CAC/ECA with my account?
- ★ From where do I get an ECA certificate?
- ★ How do I log into DSS Portal using my CAC/ECA?
- ★ How can I find help?
- ★ CAC error message "Page cannot be displayed"?
- ★ See ALL FAQs

At the bottom of the page, there is a footer with the following text:

Contact DSS | FAQs | Accessibility | USA.gov | Security and Privacy Notice | No Fear Act | FOIA | Terms of Use

FOR OFFICIAL USE ONLY

Copyright © 2011 - Defense Security Service | All Rights Reserved.



CAC/PKI Authentication from ISFD Homepage



CAC/PKI Authentication from ISFD Homepage

Step 1: Select “CAC/PKI Login” from the unauthenticated ISFD page.

The screenshot shows the top of the Defense Security Service website. The header includes the DSS logo, the text "U.S. Department of Defense DEFENSE SECURITY SERVICE", and navigation links for "Site Map" and "A-Z Index". Below the header is a dark navigation bar with links for "Home", "About Us", "Directorates", "Services", "Information Systems", and "Contact Us". The breadcrumb trail reads "Home + Information Systems + Industrial Security Facilities Database (ISFD)". The main heading is "Industrial Security Facilities Database (ISFD)". A green button labeled "ISFD LOGIN" is highlighted with a red box, and a red arrow points to it with the text "Click here". Below this, there are three paragraphs of text and a numbered list of instructions for users unable to access the system.

Home | [Information Systems](#) | [Industrial Security Facilities Database \(ISFD\)](#)

Industrial Security Facilities Database (ISFD)

ISFD LOGIN ← Click here

The ISFD will provide users with a nationwide perspective on National Industrial Security Program related facilities, as well as facilities under DSS oversight in the DoD conventional AA&E program. ISFD data will also provide source data for the DoD Joint Personnel Adjudicative System (JPAS) and the Facility Verification Request (FVR) application.

If you request a Facility Verification for a company that you have previously verified, ISFD will return the following error message: "A Facility Verification Request by user (user name) already exists for subject CAGE code (cage of requested company)."

This is a change to ISFD functionality. If you experience difficulty finding your previous verification, call the DoD Security Services Center at 1-888-282-7682 for assistance.

Some users have been unable to access ISFD. After entering their user ID and password, the system returns a blank screen. If this occurs, please perform the following:

1. Turn off Internet Explorer (IE) popup blocker:
 - a. In Internet Explorer, on the 'Tools' menu,
 - b. Select 'Pop-up Blocker', and then
 - c. Select 'Turn off pop-up blocker'.
2. Clean out temporary internet cookies and files:
 - a. In Internet Explorer, on the 'Tools' menu,
 - b. Select 'Internet Options',
 - c. Select 'Delete Cookies' under 'Temporary Internet files' on the 'General' tab for Internet Options',



CAC/PKI Authentication from ISFD Homepage

Step 2: The IdM solution displays the IdM Portal Disclaimer.

Step 3: User selects “I Accept” to proceed.

Welcome | DSS Portal - Windows Internet Explorer

https://sso.dss.mil/openso/cert/login

Welcome | DSS Portal

Defense Security Service Portal

DSS Portal Disclaimer

This is a Department of Defense computer system. This computer system, including all related equipment, networks and network devices (specifically including internet access), are provided only for authorized U.S. government use. DoD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored. Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal or adverse action. Use of this system constitutes consent to monitoring for these purposes.

I Accept ← Click here

FOR OFFICIAL USE ONLY

Copyright © 2011 - Defense Security Service | All Rights Reserved.



CAC/PKI Authentication from ISFD Homepage

Step 4: The IdM solution displays the unauthenticated IdM homepage.

Step 5: User selects “CAC/ECA Login”.

Defense Security Service Portal

Welcome STEPP user

Note: If you have recently used your CAC/ECA to login, you may not be prompted for your PIN and/or Certificate.

Login to DSS Portal

CAC/ECA Login

Register CAC/ECA

Register Certificate

Self Enrollment

Register for an account

Threat Advisory

NTAS
NO ACTIVE ALERTS
www.DHS.gov/alerts

Click here

Links

DSS Applications

- Return to STEPP
- ODAA

FAQs

- How to Setup Firefox to use ActivClient?
- DSS Portal not loading in Firefox?
- What is the DSS Portal?
- What is the Single Sign-on?
- How do I register for a DSS account?
- How to reset your password?
- How do I associate CAC/ECA with my account?
- From where do I get an ECA certificate?
- How do I log into DSS Portal using my CAC/ECA?
- How can I find help?
- CAC error message "Page cannot be displayed"?
- See ALL FAQs



CAC/PKI Authentication from ISFD Homepage

Step 6: User selects appropriate certificate.

The screenshot shows a Windows Internet Explorer browser window displaying the Defense Security Service Portal. The address bar shows the URL <https://sso.dss.mil/opensso/cert/login>. The page content includes a header with the DSS logo, a navigation bar, and several main sections: "Login to DSS Portal" with a "CAC/ECA Login" button, "Register CAC/ECA" with a "Register Certificate" button, and "Self Enrollment" with a "Register for an account" button. A "Windows Security" dialog box is overlaid on the page, titled "Select a Certificate". It lists three certificates:

- AS2USER
Issuer: AS2USER
Valid From: 9/27/2010 to 9/27/2040
- SAMPLE.USER
Issuer: DOD CA-30
Valid From: 1/22/2012 to 9/30/2012
[Click here to view certificate prop...](#)
- SAMPLE.USER
Issuer: DOD EMAIL CA-30
Valid From: 1/22/2012 to 9/30/2012

The second certificate, "SAMPLE.USER" issued by "DOD CA-30", is highlighted with a red rectangular box. A red arrow points from the text "Click here" to the top-left corner of this red box. The dialog box has "OK" and "Cancel" buttons at the bottom.



CAC/PKI Authentication from ISFD Homepage

Step 7: User enters PIN when prompted.

The screenshot shows a web browser window displaying the Defense Security Service Portal. The browser's address bar shows the URL <https://sso.dss.mil/opensso/cert/login>. The page features a purple header with the text "Defense Security Service Portal" and the DSS logo. A modal dialog box titled "ActivClient Login" is overlaid on the page. The dialog box contains the text "ActivIdentity ActivClient" and "Please enter your PIN." Below this text is a text input field labeled "PIN" which is highlighted with a red rectangular border. A red arrow points from the text "Enter PIN" to the input field. The dialog box also includes "OK" and "Cancel" buttons at the bottom. The background page shows various navigation options like "CAG/ECA Login", "Register CAC/ECA", and "Self Enrollment".



CAC/PKI Authentication from ISFD Homepage

Step 8: The IdM solution authenticates the User and redirects him/her to the ISFD Username/Password Login page.

Step 9: User agrees to the disclaimer, enters his/her ISFD Username and Password, and clicks “Log In”.

Industrial Security Facilities Database: Login

Please read the following and check the checkbox for acknowledgement.

DOD NOTICE AND CONSENT BANNER

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., authentication 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.

I acknowledge and accept the above access statement.

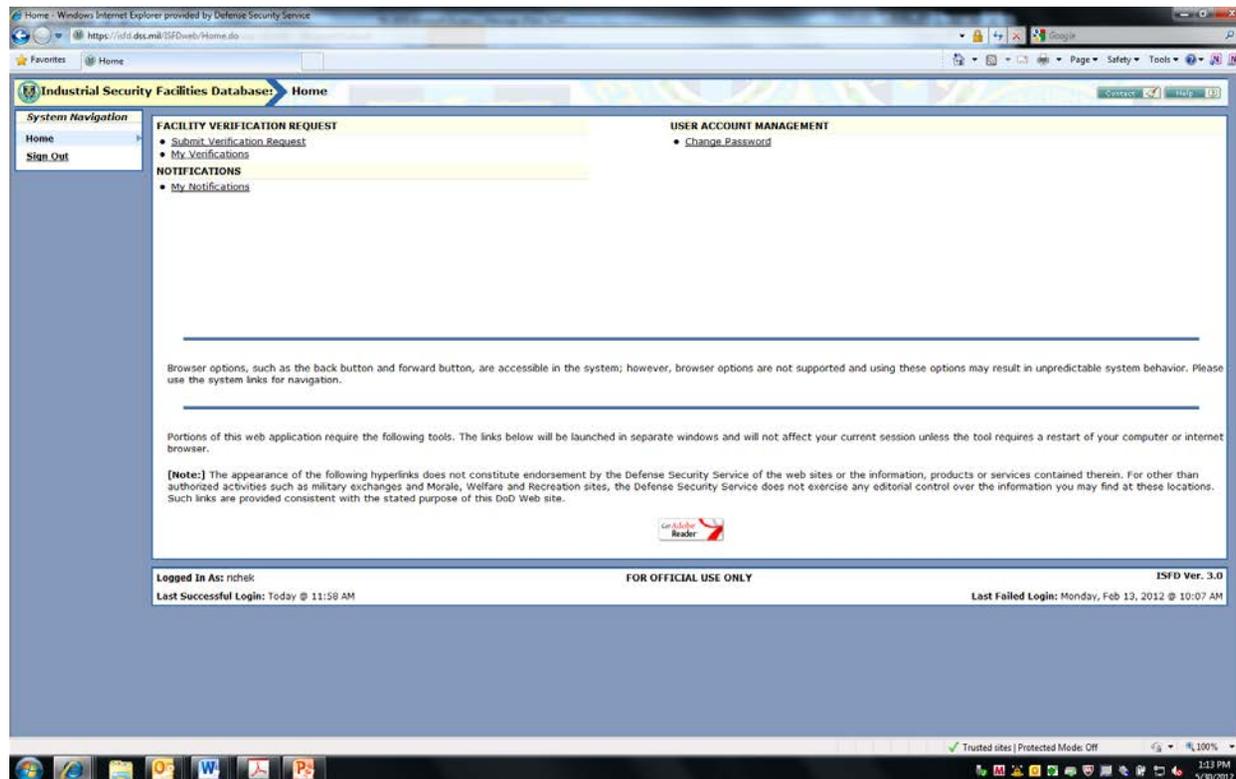
Enter your user name and password. If you do not have one, please see your system administrator for assistance.

User Name
Password



CAC/PKI Authentication from ISFD Homepage

Step 10: ISFD authenticates the User and allows full access.





ISFD Access from IdM



ISFD CAC/PKI Authentication from IdM

Step 1: The User navigates to <https://sso.dss.mil>.

Step 2: The IdM Solution displays the IdM Portal Disclaimer.

Step 3: The User selects “I Accept” to proceed.

Steps 4-7: Continue as previously referenced.

The screenshot shows a Windows Internet Explorer browser window displaying the Defense Security Service Portal. The address bar shows the URL <https://sso.dss.mil/opensso/cert/login>. The page title is "Welcome | DSS Portal". The main content area features a banner with the text "Defense Security Service Portal" and the DSS logo. Below the banner is a "DSS Portal Disclaimer" box with the following text: "This is a Department of Defense computer system. This computer system, including all related equipment, networks and network devices (specifically including internet access), are provided only for authorized U.S. government use. DoD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored. Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal or adverse action. Use of this system constitutes consent to monitoring for these purposes." Below the disclaimer text are two buttons: "I Accept" and "Click here". At the bottom of the page, there is a footer that reads "FOR OFFICIAL USE ONLY" and "Copyright © 2011 - Defense Security Service | All Rights Reserved."



ISFD CAC/PKI Authentication from IdM

Step 8: The IdM Solution authenticates the User and displays the IdM Portal Home Page.

Step 9: User selects the “Access ISFD” link.

Logged in as: james.lee

RETURN TO DSS PORTAL LOGOUT HELP

Defense Security Service Portal

Home Work Items Delegations Profile

Welcome, James Lee.

Last Successful Login: Mon, 21 May 2012 08:08:11 CDT

DSS Portal Quick Links

- [Request a DSS Portal Role](#)
- [Request a Privileged DSS Portal Role](#)

OBMS Quick Links

- [Request/Manage OBMS Access](#)

STEPP Quick Links

- [Create a new STEPP Account](#)
- [Register an Existing STEPP Account](#)

ISFD Quick Links

- [Request ISFD Account](#)
- [Access ISFD](#)**

Approvals 0

Contact DSS | FAQs | Accessibility | USA Gov | Security and Privacy Notice | No Fear Act | FOIA | Terms of Use

FOR OFFICIAL USE ONLY



ISFD CAC/PKI Authentication from IdM

Step 10: The IdM Solution redirects the User to the ISFD Username/Password page.

Step 11: User agrees to the disclaimer, enters his/her ISFD Username and Password, and clicks “Log In”.

Industrial Security Facilities Database: Login

Please read the following and check the checkbox for acknowledgement.

DOD NOTICE AND CONSENT BANNER

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., authentication 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.

I acknowledge and accept the above access statement.

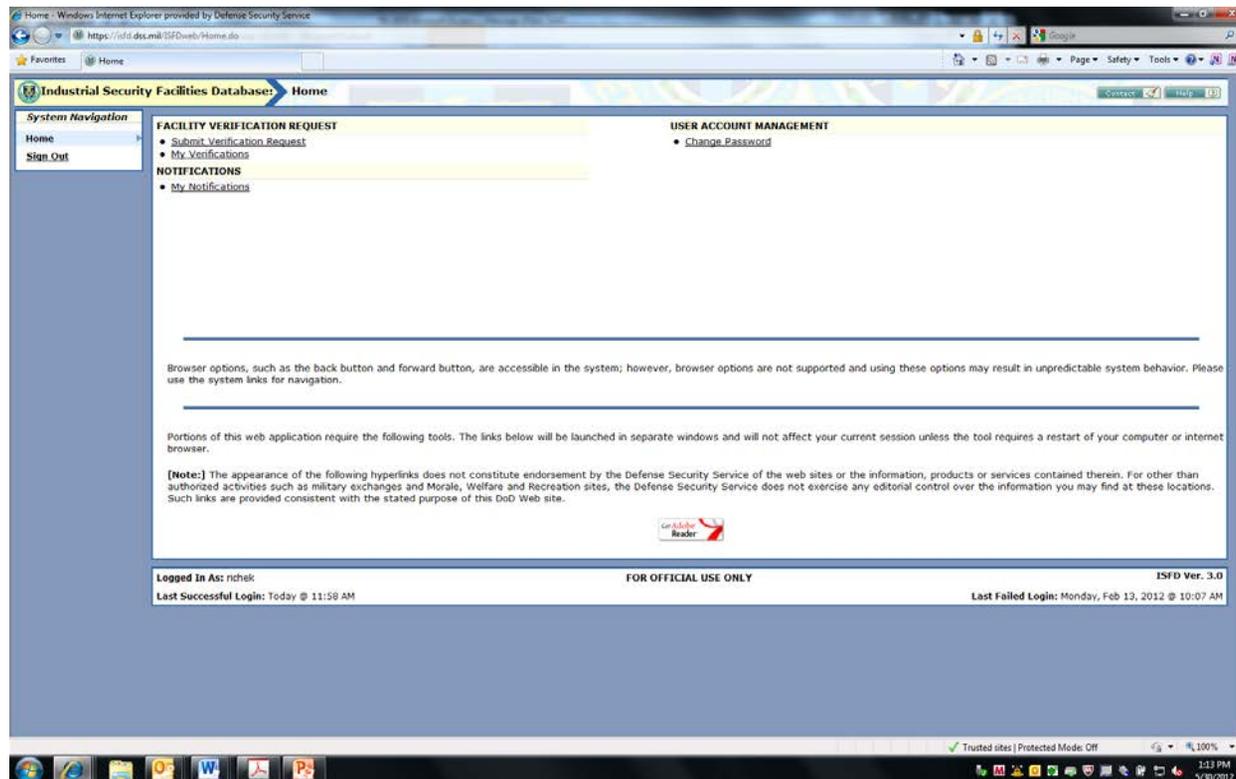
Enter your user name and password. If you do not have one, please see your system administrator for assistance.

User Name
Password



ISFD CAC/PKI Authentication from IdM

Step 12: ISFD authenticates the User and allows full access.





Request an ISFD Account (new ISFD users only)



Request an ISFD Account

Step 1: The User navigates to <https://sso.dss.mil>.

Step 2: The IdM Solution displays the IdM Portal Disclaimer.

Step 3: The User selects “I Accept” to proceed.

Steps 4-7: Continue as previously referenced.

The screenshot shows a Windows Internet Explorer browser window displaying the Defense Security Service Portal. The address bar shows the URL <https://sso.dss.mil/opensso/cert/login>. The page title is "Welcome | DSS Portal". The main content area features a large banner with the text "Defense Security Service Portal" and the DSS logo. Below the banner is a "DSS Portal Disclaimer" box with the following text: "This is a Department of Defense computer system. This computer system, including all related equipment, networks and network devices (specifically including internet access), are provided only for authorized U.S. government use. DoD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored. Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal or adverse action. Use of this system constitutes consent to monitoring for these purposes." Below the disclaimer text is a red button labeled "I Accept" and a red arrow pointing to the text "Click here". At the bottom of the page, there is a dark grey footer with the text "FOR OFFICIAL USE ONLY" and "Copyright © 2011 - Defense Security Service | All Rights Reserved."



Request an ISFD Account

Step 8: The IdM Solution authenticates the User.

Step 9: User selects "Request ISFD Account" button

Logged in as: email.test

Defense Security Service Portal

RETURN TO DSS PORTAL LOGOUT HELP

Home Work Items Delegations Profile

Welcome, Email Test.

Last Successful Login: Tue, 22 May 2012 08:46:53 CDT

DSS Portal Quick Links

- [Request a DSS Portal Role](#)
- [Request a Privileged DSS Portal Role](#)

OBMS Quick Links

- [Request/Manage OBMS Access](#)
- [Access OBMS](#)

STEPP Quick Links

- [Create a new STEPP Account](#)
- [Register an Existing STEPP Account](#)

ISFD Quick Links

- [Request ISFD Account](#) ← **Click here**



Request an ISFD Account

Step 10: The IdM solution displays the ISFD account request form.

Step 11: User provides the required information and submits the form.

Request ISFD Account Workflow

Click "Submit" to submit your ISFD request , "Cancel" to return to the Home tab.

1. Type of User ← **Select Type of User**

DoD (Military or Civilian) DoD Contractor Non-DoD NISP Non-DoD

2. Type of Request ← **Select Type of Request**

Create Account Delete Account Name Change

For Name Changes, please provide the following:

New First Name: New Last Name:

3a. User Information On File

Please verify the information shown below. This will be used to create your ISFD account.

First Name:	Email
Last Name:	Test
Email Address:	idmtest@deloitte.com
Current Roles:	

← **Prepopulated information**

3b. User Information Requested

Update Sponsor Email:

Please enter your SSN (format: xxx-xx-xxxx): *

Please enter your Date of Birth: *

Please enter your Place of Birth: *

Job Title/Rank/Grade: *

← **Provide user information**



Request an ISFD Account

Step 10: The IdM solution displays the ISFD account request form.

Step 11: User reviews the account information and submits the form

Telephone Number: *

Fax Number:

4. Applications

Industrial Security Facilities Database (ISFD)

5. User Certification

Please read then certify below:

I hereby certify that I understand that by signing this System Access Request, I am solely responsible for the use and protection of the user ID and password that I will be provided. I also understand that I am not authorized to share my user ID and password with any other individuals. I will utilize all tools and applications in accordance with the Account Management Policy and Security Policy, as well as all applicable

Please certify by entering your initials here: *

6. Privacy Policy Statement

Please read and accept this following text

AUTHORITY:
Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.

PURPOSE:
To record names, and Social Security Numbers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form.

ROUTINE USES:
In addition to those disclosures generally permitted under 5 U.S.C.

I have read and understand the terms of the privacy policy. *

← **Sign initials**

← **Accept privacy statement**

← **Click Submit**