

SWFT Access, Registration, and Testing Procedures

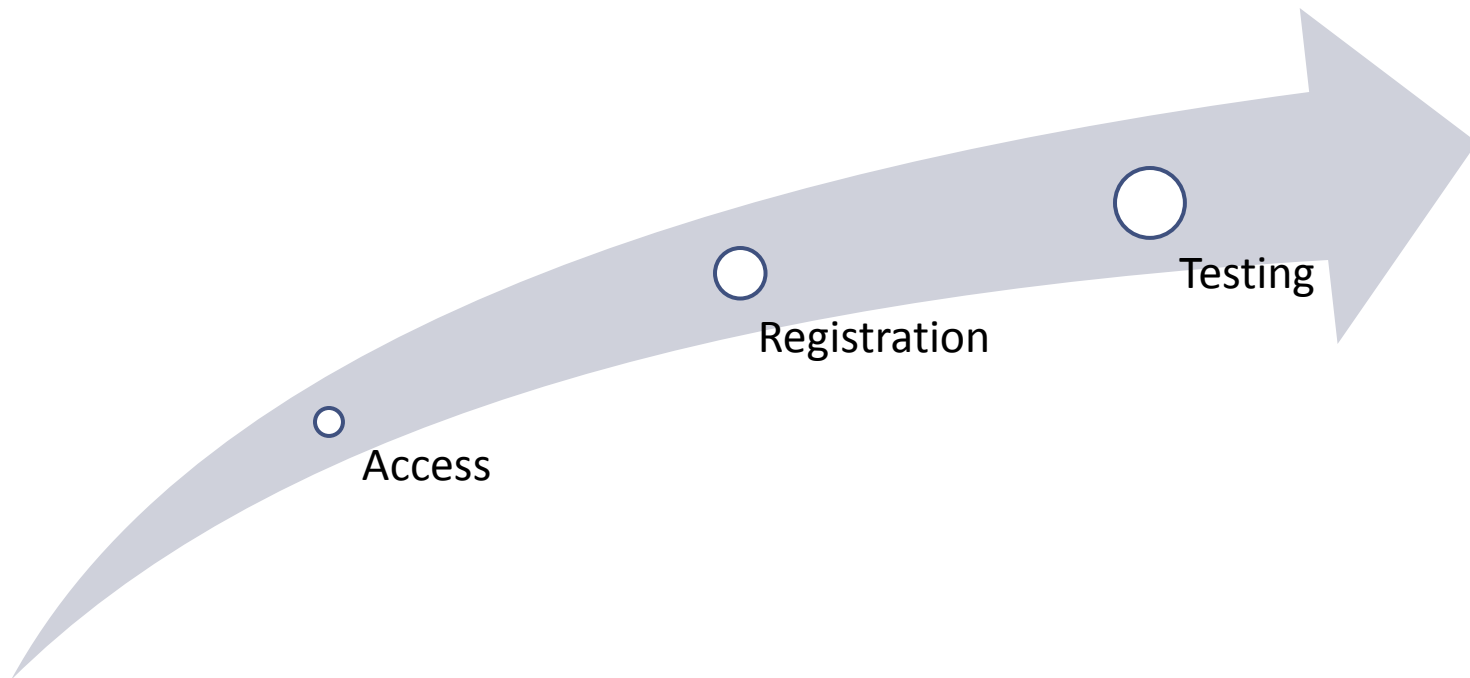
Version 3.2



*Please refer to the SWFT Access,
Registration, and Testing Procedures
document for more detailed information*

Getting Started

There are three phases that an Authorized Organization Representative must complete before a cleared National Industrial Security Program (NISP) organization or U.S. Military component can submit electronic fingerprints (eFPs) to the Secure Web Fingerprint Transaction (SWFT) Web Application.



Access (Personnel Security System Access Request (PSSAR))

Completed PSSAR forms for Organization Administrators must be submitted to the Defense Manpower Data Center (DMDC) Contact Center.

After obtaining a SWFT account, Organization Administrators will be responsible for processing PSSARs, and creating and managing all other user accounts for their organization_or facility. See the Organization and Site Administrator Guide for details.

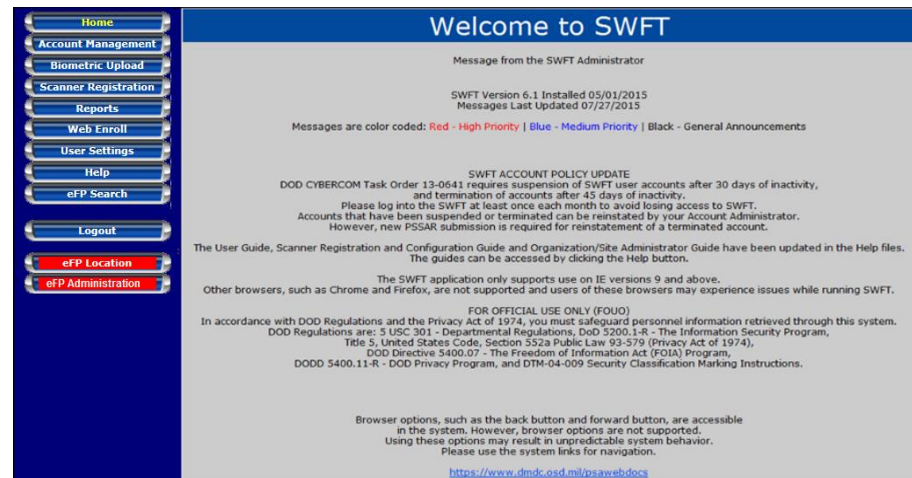
[illegible]

Getting Started

Registration

Any fingerprint capture hardware and software must meet Federal Bureau of Investigation (FBI) certification guidelines. Each fingerprint enrollment workstation must be registered with SWFT and approved by the Office of Personnel Management (OPM) or the Registration Authority.

An Online Scanner Registration form is available in the SWFT Web Application, which provides an automated tool for registering a new fingerprint enrollment workstation or editing the existing one. SWFT shares the registration data with the registration authority.



Getting Started

Testing

All fingerprint scanner equipment and software must first be tested with SWFT and the registration authority before it can be used for production e-fingerprint (referred to as eFP) submissions.

The SWFT+ Coordinator assists with scheduling and coordinating a test session with the registration authority, and will also assist with resolution of potential issues with the test eFPs.

Re-registration and Re-testing

All fingerprint scanner equipment and software must be re-registered and re-tested under the following circumstances (contact the SWFT+ Coordinator when unsure):

- Any component of the fingerprint enrollment workstation is replaced (laptop, scanning device, or both)
- Hardware part repair or replacement
- Software replacement, upgrade, modification, or configuration change
- Transfer of the equipment to another location

SWFT Server/Web-based Fingerprint Systems

Server-based/web-based fingerprint systems typically involve two components: 1) One or more fingerprint scanning devices; 2) Server that integrates fingerprint images and biographic data and generates the eFP file.

Multiple scanning devices can be connected to a single server. At least one scanner-server pair must be registered and tested with SWFT/DMDC and the registration authority. The registration must prove that the hardware and software components in the server-based/web-based system meet the FBI certification guidelines. The test of the scanner-server pair must prove that the system is properly configured and generates eFP files that comply with the FBI Electronic Biometric Transmission Specification (EBTS) and OPM or other registration authority specifications.

Additional scanning devices that communicate with a server-based solution that have already been approved for production by SWFT/DMDC and the registration authority must also be registered, but do not have to be tested. Scanning devices that will connect to an approved server-based system must include in the comments section of the SWFT registration form a reference to the previously registered and approved server.

Submission of eFPs on Behalf of Other Companies

Option One: Multi-Site Uploader - Service Provider Acts with Limited Privileges on Behalf of Another Organization

Any SWFT account holder can act as a service provider for other Organizations if the “Multi-Site Uploader” role is enabled for that account. This allows the service provider to submit eFPs for another Organization, but will not permit accessing reports with detailed PII data for any of the serviced entities. Serviced Organizations must obtain their own SWFT account before a Multi-Site Uploader can begin submitting eFPs on their behalf.

Organizations are strongly encouraged to enter into a service agreement that will address handling and protection of the Personally Identifiable Information (PII) data. The permission of the “Multi-Site Uploader” requires submission of a valid PSSAR to the DMDC Control Center.

Note: Users with the Multi-Site Uploader permission can upload eFPs for any Org/CAGE Code that has been registered in the SWFT system. Once the permission is granted, the Multi-Site Uploader does not need to seek the SWFT pre-approval for uploading eFPs associated with any registered Org/CAGE Code. Organizations are encouraged to use their own SWFT accounts to monitor fingerprint transactions that have occurred on their behalf.

Submission of eFPs on Behalf of Other Companies

Option Two: Multi-Site SWFT Account - Service Provider Acts with Full Privileges on Behalf of Another Organization

The user acting as a Service Provider must have their own SWFT account that has been established for the organization for which the user will be providing the services. This account must be explicitly associated with the Org/CAGE Codes of the serviced entity.

A SWFT account under the serviced organization grants the service provider the ability to submit eFPs on the serviced organization's behalf. The SWFT User who provides the service can access SWFT reports and PII data for Org/CAGE Codes assigned to the service provider's SWFT account.

Each request for adding an additional Org/CAGE Code to an existing SWFT account requires a PSSAR that has been approved by the appropriate nominating official from the serviced organization.

Note: It is not necessary to own and operate a fingerprint capture device to obtain a SWFT account or to submit eFPs. Organizations can submit e-fingerprint files that were generated by a Service Provider with a SWFT-approved and registered workstation.



Access

Security officers and specialists who intend to use the services of a Third Party Vendor for capturing the fingerprints and generating eFP files need to follow only Steps 1 and 2 in the Access portion of the ART Procedures. The Registration and Testing procedures are applicable only to applicants who intend to operate fingerprint enrollment workstations.

Your Organization must verify that the Organization/Third Party Vendor that will generate the eFPs for you had their equipment registered and approved for production by SWFT/DMDC and the registration authority. Access to the verification tool requires a SWFT account.

To confirm the registration status of a fingerprint capture workstation, perform the following steps:

- Obtain either the scanning device Make and Serial Number, or the Org/CAGE Code from the Service Provider.
- Log into SWFT.
- Access the Reports section and run the report “Scanner Registration Status by Hardware Vendor and Serial Number” or “Scanner Registration Status by Org/CAGE Code” as appropriate.




Access

Step 1: The Authorized Organization Representative obtains the PSSAR from the Personnel Security/Assurance (PSA) website at the following link:

<https://www.dmdc.mil/psawebdocs/docPage.jsp?p=SWFT>

Please follow the instructions on the PSSAR and provide all relevant information as requested. PSSARs with errors will be returned to the submitting organization for correction. Corrected PSSARs for Organization Administrator accounts must be returned to the DMDC Contact Center before a SWFT account can be created.

Note: The Annual Cyber Awareness and Personally Identifiable Information training must be completed by the individual requesting the account. The training links are located on the PSA website at <https://www.dmdc.mil/psawebdocs/docPage.jsp?p=SWFT>. On the PSSAR, Part 3, numbers 18 and 19 must be checked and the completion date of the training must be filled in.



DMDC
Serving Those who Serve our Country

Personnel Security/Assurance

[PSA Home](#) | [DCII](#) | [JPAS](#) | [SWFT](#)

[SWFT Login](#)

Access Request

- [- Access, Req., Test Guide](#)
- [- Access Registration-Slideshow](#)
- [- PSSAR Checklist](#)
- [- PSSAR Form](#)
- [- PSSAR Instructions](#)
- [- PSSAR Sample](#)
- [- Training Requirements](#)

Last Updated: 4 February 2016

(01/4/2016) Regular Periodic Maintenance Outage:
SWFT system is unavailable every Thursday and Friday 9 PM – 1 AM ET due to maintenance. Other system outages may be scheduled and announced as needed.

(11/5/2015) Updated Personnel Security System Access Request (PSSAR) Form:
Updated Personnel Security System Access Request (PSSAR) Form DD 2962 has been posted and made available for use. Effective 01 December 2015, the previous version (20141203 DRAFT - OMB No. 0704-0496) will be obsolete and no longer accepted.



Access

Step 2: The PSSARs for the Organization Administrators are submitted to the DMDC Contact Center by e-mail to dmdc.contactcenter@mail.mil. Use of encrypted e-mail for transmitting any Privacy Act Data is required. Instructions on how to utilize digital encryption when sending an e-mail to the DMDC Contact Center can be found at the following link:

https://www.dmdc.mil/psawebdocs/docRequest/filePathNm=PSA/appld=560/app_key_id=1559jsow24d/siteld=7/ediPnld=0/userId=public/fileNm=Contact+Center+Encryption.pdf

Step 2 (continued): Direct all questions regarding the PSSAR processing status to the DMDC Contact Center via phone at 1-800-467-5526 or via e-mail to dmdc.contactcenter@mail.mil.

Step 2 (continued): Once the SWFT account has been created, the DMDC Contact Center will e-mail the Organization Administrator their user identification (ID), and will request that they call the DMDC Contact Center to obtain a temporary password.

Step 3: Log into the SWFT application and use your User ID and temporary password to register your Public Key (PK)token. Temporary passwords are only valid for 72 hours.



Access

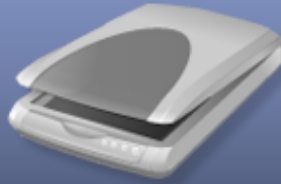
Step 4: Procure live scan or card scan equipment, if not done already.

The list of FBI certified products and software is at <https://www.fbibiospecs.cjis.gov/Certifications>.

Note #1: Organizations that plan to procure and operate their own equipment should first obtain access to SWFT to access additional guides and documentation.

Note #2: Any scanning equipment that is intended for producing eFPs must meet the FBI certification guidelines, and must be registered with SWFT.
SWFT will collect and send all required registration information to the registration authority.

Note #3: The registration and testing of the scanning equipment can be requested and conducted only by an authorized SWFT User. Any other entity that intends to provide electronic fingerprinting services must seek sponsorship from a cleared contractor organization or other authorized SWFT user entity in order to be able to register their scanning equipment.



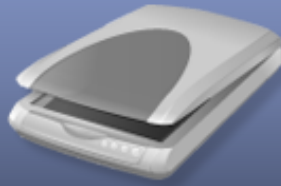
Registration

Step 4: Log into SWFT.

Please note that only the Organization Administrator has the necessary permissions to register the fingerprint scanning hardware and software. For information on how to register the scanner and software, click the “Help” button in the SWFT application to access the *Scanner Configuration and Registration Guide*.

Step 4 (Continued): Upon completing the entry of the scanner registration information, the Organization Administrator submits the scanner registration to the SWFT+ Coordinator by clicking the “Submit” button. The SWFT+ Coordinator reviews the scanner registration. Registration data that does not pass the validation check will be rejected. The Organization Administrator must then correct and re-submit the registration data. Completed scanner registration data is forwarded to the registration authority for approval.

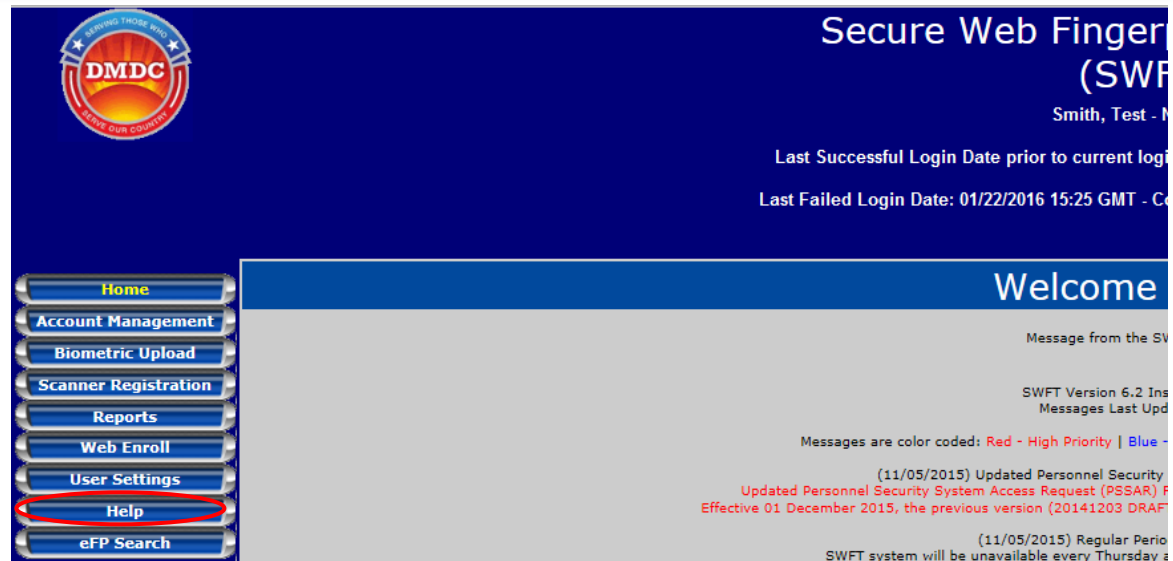
Note: When registering the scanner, ensure that the Transaction Control Number (TCN) Prefix complies with the convention that is outlined in the *Scanner Configuration and Registration Guide*. Each fingerprint scanner and fingerprint card scanner must have its own unique TCN Prefix. The *Scanner Configuration and Registration Guide* can be accessed by clicking the “Help” button in SWFT.



Registration

Step 5: After successful registration of the scanner hardware and software data, the SWFT+ Coordinator notifies the Organization Administrator via e-mail that the scanner is ready for testing. The scanner must be properly configured before producing test or production eFP files. Refer to the *Scanner Configuration and Registration Guide* which can be accessed by clicking the “Help” button in SWFT.

Note: It is not necessary to re-register or re-test the scanner workstation separately for each new Org/CAGE Code that the workstation will support. The same applies to a scanner workstation that is being sponsored by an authorized SWFT account holder.





Testing

Step 6: The Organization Administrator uploads the test eFP to SWFT and notifies the SWFT+ Coordinator by e-mail at DMDC.SWFT@mail.mil after the eFP is successfully uploaded. Refer to the *Scanner Configuration and Registration Guide* for detailed instructions pertaining to the enrollment and upload of a test eFP. Please note the following before uploading a test eFP to SWFT:

Note #1: The maximum acceptable eFP file size is 1MB for both test and production submissions. If the eFP file size is greater than 1MB, consult the vendor on how to set the scanner resolution and/or file compression to bring the size of the eFP file within 700–1,000KB range.

Note #2: Fingerprint card scanning equipment often exports only the fingerprint images from the paper card. As a result, you may have to re-enter all the biographical data manually. Please contact the appropriate software vendor for information how your card scanner should be configured to generate eFPs meeting the OPM and other registration authority standards.



Testing

Step 7: The SWFT+ Coordinator reviews the uploaded eFP and reports any issues. If errors are identified in the eFP, the SWFT+ Coordinator works with the Organization Administrator on resolution. This process might require re-submission of a corrected eFP to SWFT. Verified test eFP files are forwarded to the registration authority for validation.

Step 7 (Continued): An automated e-mail notification is sent to the Organization Administrator when the test eFP file has been submitted to the registration authority. The SWFT+ Coordinator receives notification of the test result via e-mail from OPM within one business day after submission of the test eFP to OPM.

Note: Currently, only OPM sends a confirmation e-mail to the SWFT+ Coordinator after a test eFP has been received. This may change in the future for other registration authorities.



Testing

Step 8: For each test eFP submitted to the registration authority the SWFT+ Coordinator communicates one of the following possible test results by e-mail to the Organization Administrator:

Result #1: The test eFP was successfully processed and the scanner/software is authorized to submit eFPs to production.

Result #2: The test eFP was rejected by the Registration Authority. The SWFT+ Coordinator will provide assistance with resolving the issues with the test eFP. Errors found during the registration authority validation of the test eFP will require resubmission of a corrected eFP to SWFT. Steps 6–8 will be repeated until the scanner has been approved for production use by the Registration Authority.



For any questions or concerns, please
contact the Defense Manpower Data Center Contact Center at

DMDC.contactcenter@mail.mil

Or contact the SWFT+ Coordinator at

DMDC.SWFT@mail.mil