



Secure Web Fingerprint Transmission (SWFT) Webinar

May 2015



Agenda

- Scanner Registration and Testing
- Additional SWFT 6.1 Enhancements
 - Email notifications
 - Scanner Registration Validation
 - eFP Search Tool
 - Smart Card Re-registration Improvement
- Resources and Communication
- Demo
- Q&A

Please mute your phones unless you are asking a question and do not use the hold feature



Scanner Registration & Testing

- Select the “Scanner Registration” button
- Select “Add Scanner”
- Complete the form and select “Submit”
 - Ensure that TCN Prefix is the appropriate format (next slide)
- You will receive e-mail notification when you are able to submit a test file
- SWFT 6.1 includes improved scanner search utility and ability for Site Admins to add and edit scanners



Home

Scanner Registration

Serial No./Server Identifier:

[Add Scanner](#)

Scanner Registration
Test Eramo - DMDC1

Home

Add Scanner Registration

Fields

*Indicates required field

Status: Registration Entered By FSO Date Submitted to OPM: *Device Type: Scanner

*Organization Name: Defense Manpower Data Center *Cage Code/Site: Select a CAGECode *Device Operation Mode: Stand-Alone

[Organization Administrator Information](#)

*Serial Number: *Hardware Vendor: *Software Vendor: *TCN Prefix: Help: [Scanner Configuration and Registration Guide](#)

*Device Model: *Operating System:

Physical Location of Scanner

*Address 1: Address 2: *City: *State/Country: Select State/Country *Zip Code:

Comments:

Its Active:

[Back to List](#)

For Official Use Only (FOUO)



Scanner Registration & Testing

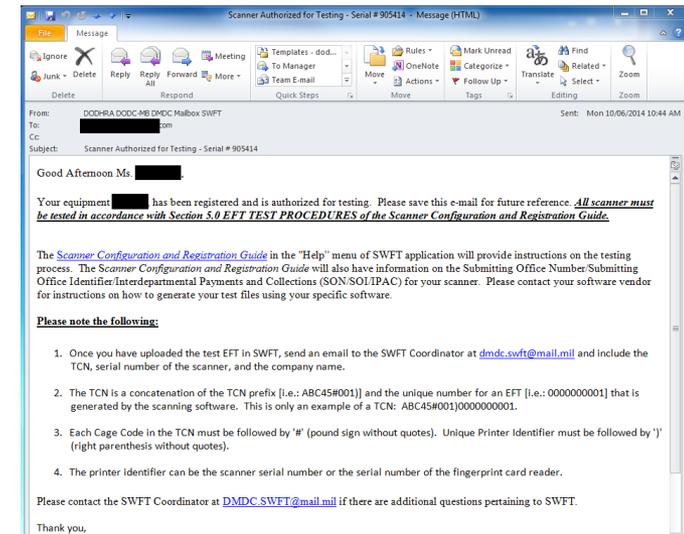
- TCN Prefix Format:
- <CAGE Code 1>#<Optional CAGE Code 2>#<Unique Printer Identifier>
 - CAGE Code 1 = Your company's CAGE Code or the CAGE Code of your parent company
 - Optional CAGE Code 2 = Your branch's CAGE Code or it can be omitted
 - Unique Printer Identifier = Serial Number
 - The TCN Prefix must end with the ")" and each component of the prefix must be separated by a "#."
- Example: 8L667#XB373#201206111523)

Note: This TCN Prefix Format applies to SWFT users only



Scanner Registration & Testing

- Submit a test EFT within 2 weeks of receiving approval to test notification
 - A test must be submitted before official usage can begin
 - If a test is not submitted within 60 days, the scanner registration will be suspended
- Email the SWFT Coordinator (dmdc.swft@mail.mil) after the test file is submitted
- Wait for Approval for Production notification or further instruction from the SWFT Coordinator
- Submissions from unregistered scanners will be automatically rejected by SWFT





Scanner Registration & Testing

- Re-registration and Re-testing required if:
 - Any part of the system is replaced (workstation, scanner, or both)
 - Software replacement or upgrade
 - Equipment re-location outside of the current building
- Additional information can be found on the PSA Website or in the Configuration Guide, which can be found in SWFT





Additional SWFT 6.1 Enhancements

- Automated Emails to be sent to all Users prior to account being locked
- Automated Emails to be sent to Organization Administrators when the registration status of a scanner is changed
- Scanner Registration Validation to be implemented so that EFPs are only accepted from scanners that are approved for production
- SWFT Reports reduced the number of SSN characters displayed from 4 to 2, in order to increase the protection of PII
- Organization Administrators will be prompted to correct differences in the name fields when creating an account for a user that has an existing account tied to the same SSN



Additional SWFT 6.1 Enhancements

- eFP Search Tool

Electronic Fingerprint Record Search Results

Last Name: <input type="text"/>	First Name: <input type="text"/>	SSN: <input type="text"/>	TCN: <input type="text"/>	<input type="button" value="Search"/>	<input type="button" value="Clear"/>
---------------------------------	----------------------------------	---------------------------	---------------------------	---------------------------------------	--------------------------------------

- Allows for easy search for status of subject's eFPs
- Login ID visible to Users when resetting Password as part of the Smart Card Re-registration process

User Settings

Email Example: xxx@company.com (must contain '@' and '.')
Phone Example: 703.325.9999, 703-325-9999, (703) 325-9999 or 7033259999

RE-REGISTER PIV, PIV-I OR ECA SMART CARD

To re-register a PIV, PIV-I or ECA Smart Card you will need your SWFT Login ID and Password for the Smart Card Registration page. Your Login ID is: **eramoaORGmultisite**

- Create a new password using the fields below. The new password is only valid for 72 hours. After 72 hours you must create another password.
- **IMPORTANT: Reset your SWFT password before your PIV or ECA Smart Card expires.**
- Enter the SWFT URL and select the new Smart Card certificate.
- You will be directed to the Smart Card Registration page, where you will enter your Login ID and Password.
- Once SWFT validates your information, access to SWFT is granted.

New Password
Verify New Password

Passwords in the SWFT system are complex and will expire in 72 hours. Passwords must be at least 15 characters, containing at least two upper case characters, two lower case characters, two digits, and two special characters.



Resources

- Visit the [PSA Website](#) to Find Additional Resources:
 - Newsletter
 - PKI Frequently Asked Questions
 - Release Notes
 - General Announcements
 - <https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=SWFT>
- [DoD approved PKI Vendors](#)
- [Access, Registration, and Test Guide](#)
- [PSSAR Sample](#), [Instructions](#), and [Checklist](#)
- DoD ECA approved vendors can be found [here](#) and approved Non-Federal Issuers including all of the Category II listed providers [here](#).



Communication

- Technical Assistance/PSSAR Submissions/Account Information:
dmdc.contactcenter@mail.mil
- SWFT Coordinator/SWFT Program Manager:
dmdc.swft@mail.mil



Demo



Questions



Backup



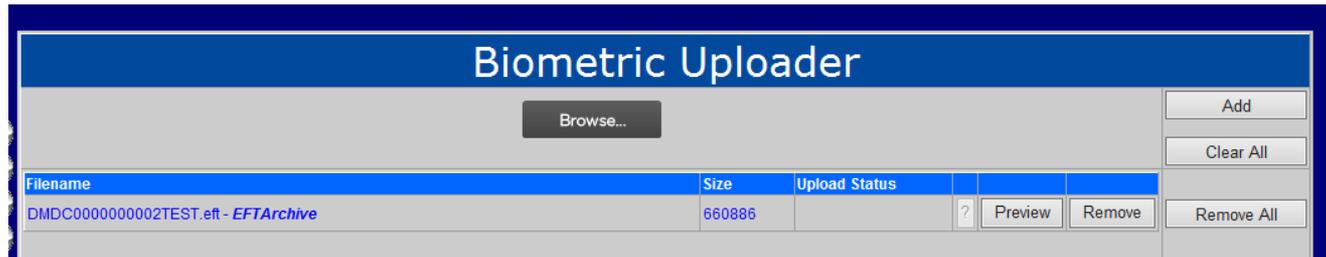
Smart Card Re-Registration

- PIV, PIV-I, and ECA users will need their SWFT Login ID and a Password to Re-Register their Smart Card
 - If you forgot your username, contact your Site or Organization Administrator
 - Login to SWFT to reset your password no more than 72 hours BEFORE your certificate expires
 - When you receive your new certificate (within 72 hours of resetting your password), return to SWFT and register your Smart Card
- CAC users will not need to Re-Register their Smart Cards
- Refer to Section 6.2 of the User Guide for more information

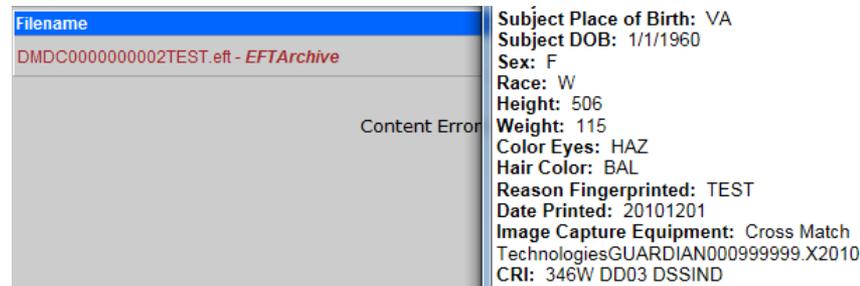


Biometric Upload - EFTArchive

- EFTArchive may appear after EFT filenames when uploading prints in the Biometric Uploader



- EFTArchive is the result of an unrecognized CRI
 - Contact the SWFT Coordinator to determine the appropriate corrective action:
 - If the CRI contains an error, the user will have to correct the error and resubmit
 - If the CRI needs to be approved by OPM, the Coordinator will request the approval and manually release the EFT to OPM



- Users should attempt to correct CRI issues prior to uploading to SWFT to prevent delays in the processing of the eFPs



Reports

- Select the “Reports” button
- Available Reports for All:
 - Status by Date, Name, SSN
 - Discrepancy
 - Archived Biometrics Status by Date, Name, or SSN
- Available Reports for Org/Site Admins:
 - Scanner Registration Status by CAGE Code or Hardware Vendor and Serial Number
 - Uploader Multi-Site Detail
 - Uploader Multi-Site Summary





Reports

- Archived Biometrics Status
 - Confirm that the SON/SOI/IPAC for the eFP were entered correctly
 - Contact the SWFT Coordinator
- Discrepancy Report:
 - Discrepancies between fields in the EFT and the e-QIP file will be highlighted
 - User's responsibility to manually adjust the incorrect information and resubmit
- EFTs that have an associated e-QIP are released to OPM every 30 minutes
- EFTs that do not match an e-QIP are released to OPM with a 24 hour delay



Suitability Investigations

- DMDC learned during a previous webinar that DoD customers ask NISP contractors to submit fingerprints in support of suitability investigations
 - DMDC alerted the Defense Security Service (DSS) Personnel Security Office for Industry (PSMO-I) who is working out how to address this issue
 - An update was made to the FAQ document stating that NISP contractors must obtain permission from DMDC prior to submitting fingerprints on behalf of DoD components



Secure Web Fingerprint Transmission (SWFT) Webinar

April 2015



Agenda

- SWFT Access
- Account Policies
- Scanner Registration and Testing
- Biometric Upload - EFTArchive
- Reports
- Release 6.1
- Resources and Communication
- Demo

Please mute your phones unless you are asking a question and do not use the hold feature



SWFT Access

- Users must be employed by a cleared contractor, have an approved PSSAR form, and up to date IA and PII training in order to receive a SWFT account
- As of 2 Mar 2015, there will be a new version of the PSSAR form
 - Previous version of the PSSAR form will not be accepted
 - Current version required for all account activations, modifications, and deletions
- The new PSSAR form will be available on the [PSA website](#)
- Refer to the [Access, Registration, and Test Guide](#) for additional information about getting started in SWFT.



Account Policies

- Accounts are locked after 30 days of inactivity
 - Site/Organization Admins can unlock accounts
 - DMDC Contact Center can unlock Organization Admin accounts
- Accounts are deactivated after 45 days of inactivity
 - Deactivated accounts are not able to be reactivated
 - Deactivated users will require a new UserID to access SWFT, which requires a new PSSAR to be submitted
- It is recommended that users set a calendar reminder with a 25-28 day recurrence in order to avoid having their accounts locked or deactivated
- Upcoming SWFT enhancement will provide automated email messages to warn users in advance of account expiration.



Scanner Registration & Testing

- Select the “Scanner Registration” button
- Select “Add Scanner”
- Complete the form and select “Submit”
 - Ensure that TCN Prefix is the appropriate format (next slide)
- You will receive e-mail notification when you are able to submit a test file



Scanner Registration - Add

*Indicates required field

Status: Date Submitted to OPM:

Company Name: *Cage Code/Site:

*Serial #:

*Hardware Vendor: *Software Vendor:

*Device Model: *TCN Prefix: [Help: Scanner Configuration and Registration Guide](#)

*Operating System:

Physical Location of Scanner

*Address 1:

Address 2:

*City: *State/Country: Zip Code:

Comments:



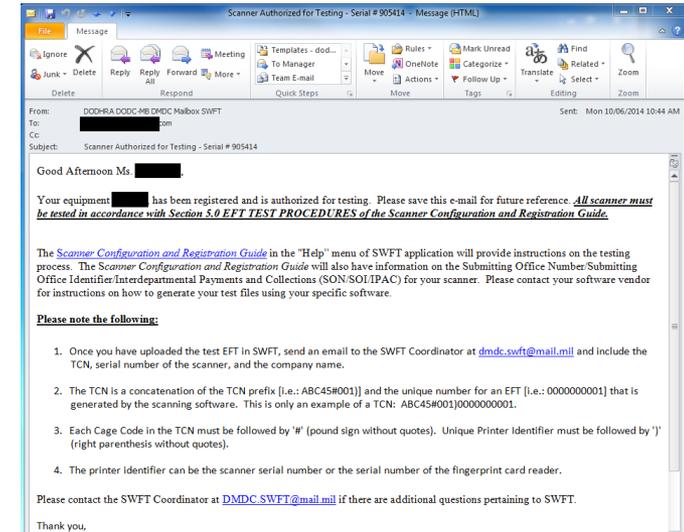
Scanner Registration & Testing

- TCN Prefix Format:
- <CAGE Code 1>#<Optional CAGE Code 2>#<Unique Printer Identifier>
 - CAGE Code 1 = Your company's CAGE Code or the CAGE Code of your parent company
 - Optional CAGE Code 2 = Your branch's CAGE Code or it can be omitted
 - Unique Printer Identifier = Serial Number
 - The TCN Prefix must end with the ")" and each component of the prefix must be separated by a "#."
- Example: 8L667#XB373#201206111523)



Scanner Registration & Testing

- Submit a test EFT within 2 weeks of receiving approval to test notification
 - A test must be submitted before official usage can begin
 - If a test is not submitted within 60 days, the scanner registration will be suspended
- Email the SWFT Coordinator (dmdc.swft@mail.mil) after the test file is submitted
- Wait for Approval for Production notification or further instruction from the SWFT Coordinator





Scanner Registration & Testing

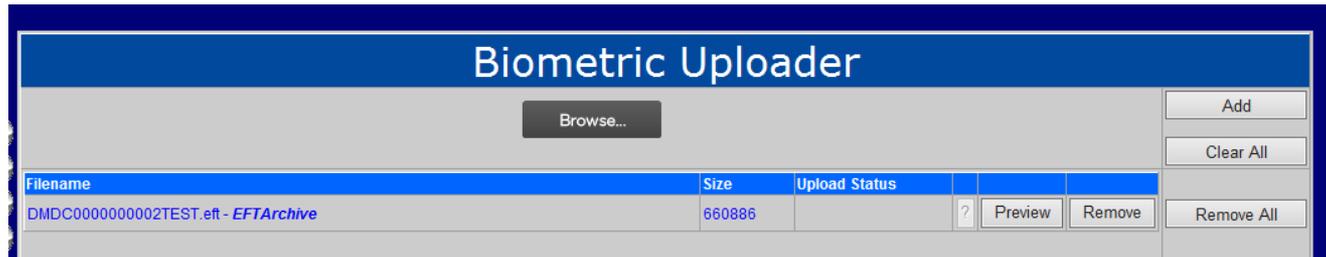
- Re-registration and Re-testing required if:
 - Any part of the system is replaced (workstation, scanner, or both)
 - Software replacement or upgrade
 - Equipment re-location outside of the current building
- Additional information can be found on the PSA Website or in the Configuration Guide, which can be found in SWFT



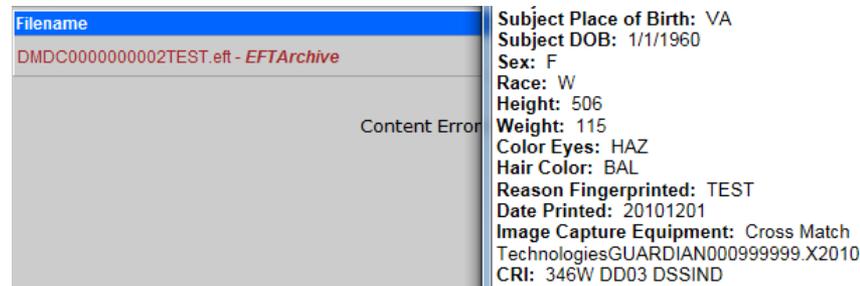


Biometric Upload - EFTArchive

- EFTArchive may appear after EFT filenames when uploading prints in the Biometric Uploader



- EFTArchive is the result of an unrecognized CRI
 - Contact the SWFT Coordinator to determine the appropriate corrective action:
 - If the CRI contains an error, the user will have to correct the error and resubmit
 - If the CRI needs to be approved by OPM, the Coordinator will request the approval and manually release the EFT to OPM



- Users should attempt to correct CRI issues prior to uploading to SWFT to prevent delays in the processing of the eFPs



Reports

- Select the “Reports” button
- Available Reports for All:
 - Status by Date, Name, SSN
 - Discrepancy
 - Archived Biometrics Status by Date, Name, or SSN
- Available Reports for Org/Site Admins:
 - Scanner Registration Status by CAGE Code or Hardware Vendor and Serial Number
 - Uploader Multi-Site Detail
 - Uploader Multi-Site Summary





Reports

- Archived Biometrics Status
 - Confirm that the SON/SOI/IPAC for the eFP were entered correctly
 - Contact the SWFT Coordinator
- Discrepancy Report:
 - Discrepancies between fields in the EFT and the e-QIP file will be highlighted
 - User's responsibility to manually adjust the incorrect information and resubmit
- EFTs that have an associated e-QIP are released to OPM every 30 minutes
- EFTs that do not match an e-QIP are released to OPM with a 24 hour delay



Release 6.1

- eFP Search Tool

Electronic Fingerprint Record Search Results

Last Name:	First Name:	SSN:	TCN:	<input type="button" value="Search"/>	<input type="button" value="Clear"/>
------------	-------------	------	------	---------------------------------------	--------------------------------------

- Allows for easy search for status of subject's eFPs
- Login ID visible to Users when resetting Password as part of the Smart Card Re-registration process

User Settings

Email Example: xxx@company.com (must contain '@' and '.')
Phone Example: 703.325.9999, 703-325-9999, (703) 325-9999 or 7033259999

RE-REGISTER PIV, PIV-I OR ECA SMART CARD

To re-register a PIV, PIV-I or ECA Smart Card you will need your SWFT Login ID and Password for the Smart Card Registration page. Your Login ID is: **eramoaORGmultisite**

- Create a new password using the fields below. The new password is only valid for 72 hours. After 72 hours you must create another password.
- **IMPORTANT: Reset your SWFT password before your PIV or ECA Smart Card expires.**
- Enter the SWFT URL and select the new Smart Card certificate.
- You will be directed to the Smart Card Registration page, where you will enter your Login ID and Password.
- Once SWFT validates your information, access to SWFT is granted.

New Password
Verify New Password

Passwords in the SWFT system are complex and will expire in 72 hours. Passwords must be at least 15 characters, containing at least two upper case characters, two lower case characters, two digits, and two special characters.



Release 6.1

- Automated Emails to be sent to all Users prior to account being locked
- Automated Emails to be sent to Organization Administrators when the registration status of a scanner is changed
- Scanner Registration Validation to be implemented so that EFPs are only accepted from scanners that are approved for production
- SWFT Reports reduced the number of SSN characters displayed from 4 to 2, in order to increase the protection of PII
- Organization Administrators will be prompted to correct differences in the name fields when creating an account for a user that has an existing account tied to the same SSN



Resources

- Visit the [PSA Website](#) to Find Additional Resources:
 - Newsletter
 - PKI Frequently Asked Questions
 - Release Notes
 - General Announcements
 - <https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=SWFT>
- [DoD approved PKI Vendors](#)
- [Access, Registration, and Test Guide](#)
- [PSSAR Sample](#), [Instructions](#), and [Checklist](#)
- DoD ECA approved vendors can be found [here](#) and approved Non-Federal Issuers including all of the Category II listed providers [here](#).



Communication

- Technical Assistance/PSSAR Submissions/Account Information:
dmdc.contactcenter@mail.mil
- SWFT Coordinator/SWFT Program Manager:
dmdc.swft@mail.mil



Demo



Questions



Backup



Suitability Investigations

- DMDC learned during a previous webinar that DoD customers ask NISP contractors to submit fingerprints in support of suitability investigations
 - DMDC alerted the Defense Security Service (DSS) Personnel Security Office for Industry (PSMO-I) who is working out how to address this issue
 - An update was made to the FAQ document stating that NISP contractors must obtain permission from DMDC prior to submitting fingerprints on behalf of DoD components



Multi-Site Uploader Role

- Service Provider Acts with Limited Privileges on Behalf of Another Company
 - Serviced Company must be registered in SWFT and have their own SWFT account
 - PSSAR required to become a Multi-Site Uploader
- Serviced company obtains account to generate detailed reports
- Service Provider is able to generate reports that identify the date and number of EFTs uploaded for the purpose of billing and accountability



Multi-Site Uploader Role

- **ONLY** one Cage Code is able to be assigned to a Multi-Site Uploader account
- Users with Multiple Cage Codes assigned to their accounts who wish to have the Multi-Site Uploader role should request a separate account
 - Maintains full reporting capabilities through your existing account with Multiple Cage Codes
 - Allows you the ability to upload eFPs for any company in SWFT through your separate Multi-Site Uploader account



Smart Card Re-Registration

- PIV, PIV-I, and ECA users will need their SWFT Login ID and a Password to Re-Register their Smart Card
 - If you forgot your username, contact your Site or Organization Administrator
 - Login to SWFT to reset your password no more than 72 hours BEFORE your certificate expires
 - When you receive your new certificate (within 72 hours of resetting your password), return to SWFT and register your Smart Card
- CAC users will not need to Re-Register their Smart Cards
- Refer to Section 6.2 of the User Guide for more information



Smart Card Re-Registration



Secure Web Fingerprint Transmission (SWFT)

Eramo, Andrew - DMDC1 - Last login time: 03/11/2014 20:55 GMT



- Home
- Biometric Upload
- Reports
- User Settings**
- Help
- Logout

User Settings

Email Example: xxx@company.com (must contain '@' and '.')
Phone Example: 703.325.9999, 703-325-9999, (703) 325-9999 or 7033259999

RE-REGISTER PIV, PIV-I OR ECA SMART CARD

To re-register a PIV, PIV-I or ECA Smart Card you will need your SWFT Login ID and Password for the Smart Card Registration page.

- Create a new password using the fields below. The new password is only valid for 72 hours. After 72 hours you must create another password.
IMPORTANT: Reset your SWFT password before your PIV or ECA Smart Card expires. If you forgot your Login ID, contact your Account Manager.
- Enter the SWFT URL and select the new Smart Card certificate.
- You will be directed to the Smart Card Registration page, where you will enter your Login ID and Password.
- Once SWFT validates your information, access to SWFT is granted.

New Password Passwords in the SWFT system are complex and will expire in 72 hours. Passwords must be at least 15 characters, containing at least two upper case characters, two lower case characters, two digits, and two special characters.
Verify New Password

Change

RE-REGISTER CAC SMART CARD

To re-register a CAC Smart Card

- Enter the SWFT URL and select the Smart Card certificate. Once the certificate is validated; access to SWFT is granted.



Secure Web Fingerprint Transmission (SWFT) Webinar

March 2015



Agenda

- SWFT Access
- Account Policies
- Suitability Investigations
- Scanner Registration and Testing
- Reports
- Resources and Communication
- Demo
- Q&A

Please mute your phones unless you are asking a question and do not use the hold feature



SWFT Access

- Users must be employed by a cleared contractor, have an approved PSSAR form, and up to date IA and PII training in order to receive a SWFT account
- As of 2 Mar 2015, there will be a new version of the PSSAR form
 - Previous version of the PSSAR form will not be accepted
 - Current version required for all account activations, modifications, and deletions
- The new PSSAR form will be available on the [PSA website](#)
- Refer to the [Access, Registration, and Test Guide](#) for additional information about getting started in SWFT.



Account Policies

- Accounts are locked after 30 days of inactivity
 - Site/Organization Admins can unlock accounts
 - DMDC Contact Center can unlock Organization Admin accounts
- Accounts are deactivated after 45 days of inactivity
 - Deactivated accounts are not able to be reactivated
 - Deactivated users will require a new UserID to access SWFT, which requires a new PSSAR to be submitted
- It is recommended that users set a calendar reminder with a 25-28 day recurrence in order to avoid having their accounts locked or deactivated
- Upcoming SWFT enhancement will provide automated email messages to warn users in advance of account expiration.



Suitability Investigations

- DMDC learned during the last webinar that DoD customers ask NISP contractors to submit fingerprints in support of suitability investigations
 - DMDC alerted the Defense Security Service (DSS) Personnel Security Office for Industry (PSMO-I) who is working out how to address this issue
 - An update was made to the FAQ document stating that NISP contractors must obtain permission from DMDC prior to submitting fingerprints on behalf of DoD components



Scanner Registration & Testing

- Select the “Scanner Registration” button
- Select “Add Scanner”
- Complete the form and select “Submit”
 - Ensure that TCN Prefix is the appropriate format (next slide)
- You will receive e-mail notification when you are able to submit a test file



Scanner Registration - Add

*Indicates required field

Status: Date Submitted to OPM:

Company Name: *Cage Code/Site:

*Serial #:

*Hardware Vendor: *Software Vendor:

*Device Model: *TCN Prefix: [Help: Scanner Configuration and Registration Guide](#)

*Operating System:

Physical Location of Scanner

*Address 1:

Address 2:

*City: *State/Country: Zip Code:

Comments:



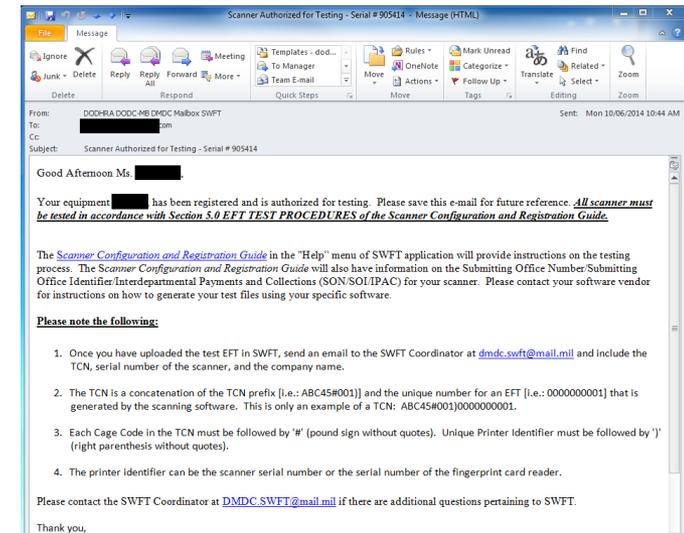
Scanner Registration & Testing

- TCN Prefix Format:
- <CAGE Code 1>#<Optional CAGE Code 2>#<Unique Printer Identifier>
 - CAGE Code 1 = Your company's CAGE Code or the CAGE Code of your parent company
 - Optional CAGE Code 2 = Your branch's CAGE Code or it can be omitted
 - Unique Printer Identifier = Serial Number
 - The TCN Prefix must end with the ")" and each component of the prefix must be separated by a "#."
- Example: 8L667#XB373#201206111523)



Scanner Registration & Testing

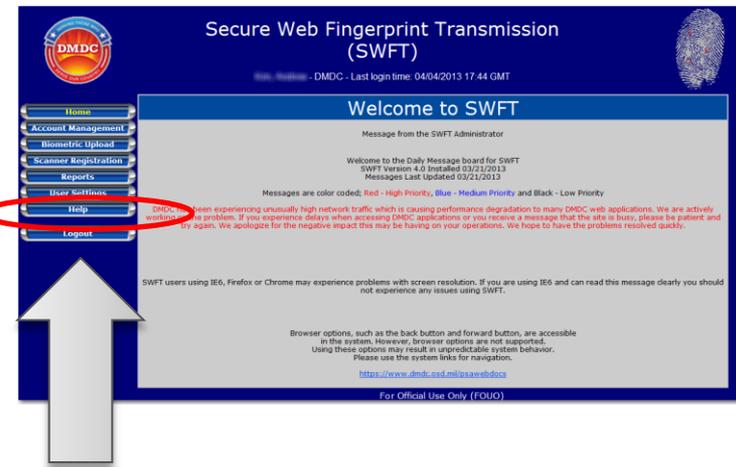
- Submit a test EFT within 2 weeks of receiving approval to test notification
 - A test must be submitted before official usage can begin
 - If a test is not submitted within 60 days, the scanner registration will be suspended
- Email the SWFT Coordinator (dmdc.swft@mail.mil) after the test file is submitted
- Wait for Approval for Production notification or further instruction from the SWFT Coordinator





Scanner Registration & Testing

- Re-registration and Re-testing required if:
 - Any part of the system is replaced (workstation, scanner, or both)
 - Software replacement or upgrade
 - Equipment re-location outside of the current building
- Additional information can be found on the PSA Website or in the Configuration Guide, which can be found in SWFT





Reports

- Select the “Reports” button
- Available Reports for All:
 - Status by Date, Name, SSN
 - Discrepancy
 - Archived Biometrics Status by Date, Name, or SSN
- Available Reports for Org/Site Admins:
 - Scanner Registration Status by CAGE Code or Hardware Vendor and Serial Number
 - Uploader Multi-Site Detail
 - Uploader Multi-Site Summary





Reports

- Archived Biometrics Status
 - Confirm that the SON/SOI/IPAC for the eFP were entered correctly
 - Contact the SWFT Coordinator
- Discrepancy Report:
 - Discrepancies between fields in the EFT and the e-QIP file will be highlighted
 - User's responsibility to manually adjust the incorrect information and resubmit
- EFTs that have an associated e-QIP are released to OPM every 30 minutes
- EFTs that do not match an e-QIP are released to OPM with a 24 hour delay



Resources

- Visit the [PSA Website](#) to Find Additional Resources:
 - Newsletter
 - PKI Frequently Asked Questions
 - Release Notes
 - General Announcements
 - <https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=SWFT>
- [DoD approved PKI Vendors](#)
- [Access, Registration, and Test Guide](#)
- [PSSAR Sample](#), [Instructions](#), and [Checklist](#)
- DoD ECA approved vendors can be found [here](#) and approved Non-Federal Issuers including all of the Category II listed providers [here](#).



Communication

- Technical Assistance/PSSAR Submissions/Account Information:
dmdc.contactcenter@mail.mil
- SWFT Coordinator/SWFT Program Manager:
dmdc.swft@mail.mil



Demo



Questions



Backup



Multi-Site Uploader Role

- Service Provider Acts with Limited Privileges on Behalf of Another Company
 - Serviced Company must be registered in SWFT and have their own SWFT account
 - PSSAR required to become a Multi-Site Uploader
- Serviced company obtains account to generate detailed reports
- Service Provider is able to generate reports that identify the date and number of EFTs uploaded for the purpose of billing and accountability



Multi-Site Uploader Role

- **ONLY** one Cage Code is able to be assigned to a Multi-Site Uploader account
- Users with Multiple Cage Codes assigned to their accounts who wish to have the Multi-Site Uploader role should request a separate account
 - Maintains full reporting capabilities through your existing account with Multiple Cage Codes
 - Allows you the ability to upload eFPs for any company in SWFT through your separate Multi-Site Uploader account



Smart Card Re-Registration

- PIV, PIV-I, and ECA users will need their SWFT Login ID and a Password to Re-Register their Smart Card
 - If you forgot your username, contact your Site or Organization Administrator
 - Login to SWFT to reset your password no more than 72 hours BEFORE your certificate expires
 - When you receive your new certificate (within 72 hours of resetting your password), return to SWFT and register your Smart Card
- CAC users will not need to Re-Register their Smart Cards
- Refer to Section 6.2 of the User Guide for more information



Smart Card Re-Registration



Secure Web Fingerprint Transmission (SWFT)

Eramo, Andrew - DMDC1 - Last login time: 03/11/2014 20:55 GMT



- Home
- Biometric Upload
- Reports
- User Settings**
- Help
- Logout

User Settings

Email Example: xxx@company.com (must contain '@' and '.')
Phone Example: 703.325.9999, 703-325-9999, (703) 325-9999 or 7033259999

RE-REGISTER PIV, PIV-I OR ECA SMART CARD

To re-register a PIV, PIV-I or ECA Smart Card you will need your SWFT Login ID and Password for the Smart Card Registration page.

- Create a new password using the fields below. The new password is only valid for 72 hours. After 72 hours you must create another password.
IMPORTANT: Reset your SWFT password before your PIV or ECA Smart Card expires. If you forgot your Login ID, contact your Account Manager.
- Enter the SWFT URL and select the new Smart Card certificate.
- You will be directed to the Smart Card Registration page, where you will enter your Login ID and Password.
- Once SWFT validates your information, access to SWFT is granted.

New Password Passwords in the SWFT system are complex and will expire in 72 hours. Passwords must be at least 15 characters, containing at least two upper case characters, two lower case characters, two digits, and two special characters.
Verify New Password

Change

RE-REGISTER CAC SMART CARD

To re-register a CAC Smart Card

- Enter the SWFT URL and select the Smart Card certificate. Once the certificate is validated; access to SWFT is granted.



Secure Web Fingerprint Transmission (SWFT) Webinar

February 2015



Agenda

- SWFT Access
- Account Policies
- Scanner Registration and Testing
- Reports
- Resources and Communication
- Demo
- Q&A

Please mute your phones unless you are asking a question and do not use the hold feature



SWFT Access

- Users must be employed by a cleared contractor, have an approved PSSAR form, and up to date IA and PII training in order to receive a SWFT account
- As of 2 Mar 2015, there will be a new version of the PSSAR form
 - Previous version of the PSSAR form will not be accepted
 - Current version required for all account activations, modifications, and deletions
- The new PSSAR form will be available on the [PSA website](#)
- Refer to the [Access, Registration, and Test Guide](#) for additional information about getting started in SWFT.



Account Policies

- Accounts are locked after 30 days of inactivity
 - Site/Organization Admins can unlock accounts
 - DMDC Contact Center can unlock Organization Admin accounts
- Accounts are deactivated after 45 days of inactivity
 - Deactivated accounts are not able to be reactivated
 - Deactivated users will require a new UserID to access SWFT, which requires a new PSSAR to be submitted
- It is recommended that users set a calendar reminder with a 25-28 day recurrence in order to avoid having their accounts locked or deactivated
- Upcoming SWFT enhancement will provide automated email messages to warn users in advance of account expiration.



Scanner Registration & Testing

- Select the “Scanner Registration” button
- Select “Add Scanner”
- Complete the form and select “Submit”
 - Ensure that TCN Prefix is the appropriate format (next slide)
- You will receive e-mail notification when you are able to submit a test file



Scanner Registration - Add

*Indicates required field

Status: Date Submitted to OPM:

Company Name: *Cage Code/Site:

*Serial #:

*Hardware Vendor: *Software Vendor:

*Device Model: *TCN Prefix: [Help: Scanner Configuration and Registration Guide](#)

*Operating System:

Physical Location of Scanner

*Address 1:

Address 2:

*City: *State/Country: Zip Code:

Comments:

Save Submit Cancel



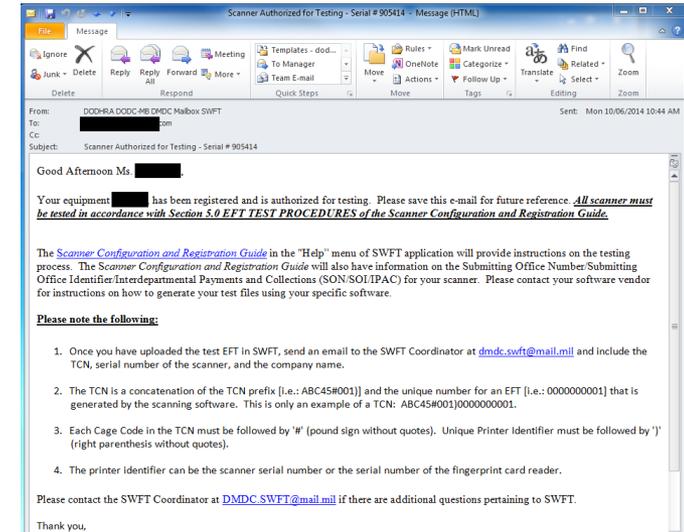
Scanner Registration & Testing

- TCN Prefix Format:
- <CAGE Code 1>#<Optional CAGE Code 2>#<Unique Printer Identifier>
 - CAGE Code 1 = Your company's CAGE Code or the CAGE Code of your parent company
 - Optional CAGE Code 2 = Your branch's CAGE Code or it can be omitted
 - Unique Printer Identifier = Serial Number
 - The TCN Prefix must end with the ")" and each component of the prefix must be separated by a "#."
- Example: 8L667#XB373#201206111523)



Scanner Registration & Testing

- Submit a test EFT within 60 days of receiving approval to test notification
 - A test must be submitted before official usage can begin
 - It is recommended that the test be submitted within two weeks of receiving approval to test
- Email the SWFT Coordinator (dmdc.swft@mail.mil) after the test file is submitted
- Wait for Approval for Production notification or further instruction from the SWFT Coordinator





Scanner Registration & Testing

- Re-registration and Re-testing required if:
 - Any part of the system is replaced (workstation, scanner, or both)
 - Software replacement or upgrade
 - Equipment re-location outside of the current building
- Additional information can be found on the PSA Website or in the Configuration Guide, which can be found in SWFT





Reports

- Select the “Reports” button
- Available Reports for All:
 - Status by Date, Name, SSN
 - Discrepancy
 - Archived Biometrics Status by Date, Name, or SSN
- Available Reports for Org/Site Admins:
 - Scanner Registration Status by CAGE Code or Hardware Vendor and Serial Number
 - Uploader Multi-Site Detail
 - Uploader Multi-Site Summary





Reports

- Archived Biometrics Status
 - Confirm that the SON/SOI/IPAC for the eFP were entered correctly
 - Contact the SWFT Coordinator
- Discrepancy Report:
 - Discrepancies between fields in the EFT and the e-QIP file will be highlighted
 - User's responsibility to manually adjust the incorrect information and resubmit
- EFTs that have an associated e-QIP are released to OPM every 30 minutes
- EFTs that do not match an e-QIP are released to OPM with a 24 hour delay



Resources

- Visit the [PSA Website](#) to Find Additional Resources:
 - Newsletter
 - PKI Frequently Asked Questions
 - Release Notes
 - General Announcements
 - <https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=SWFT>
- [DoD approved PKI Vendors](#)
- [Access, Registration, and Test Guide](#)
- [PSSAR Sample](#), [Instructions](#), and [Checklist](#)
- DoD ECA approved vendors can be found [here](#) and approved Non-Federal Issuers including all of the Category II listed providers [here](#).



Communication

- Technical Assistance/PSSAR Submissions/Account Information:
dmdc.contactcenter@mail.mil
- SWFT Coordinator/SWFT Program Manager:
dmdc.swft@mail.mil



Demo



Questions



Backup



Multi-Site Uploader Role

- Service Provider Acts with Limited Privileges on Behalf of Another Company
 - Serviced Company must be registered in SWFT and have their own SWFT account
 - PSSAR required to become a Multi-Site Uploader
- Serviced company obtains account to generate detailed reports
- Service Provider is able to generate reports that identify the date and number of EFTs uploaded for the purpose of billing and accountability



Multi-Site Uploader Role

- **ONLY** one Cage Code is able to be assigned to a Multi-Site Uploader account
- Users with Multiple Cage Codes assigned to their accounts who wish to have the Multi-Site Uploader role should request a separate account
 - Maintains full reporting capabilities through your existing account with Multiple Cage Codes
 - Allows you the ability to upload eFPs for any company in SWFT through your separate Multi-Site Uploader account



Smart Card Re-Registration

- PIV, PIV-I, and ECA users will need their SWFT Login ID and a Password to Re-Register their Smart Card
 - If you forgot your username, contact your Site or Organization Administrator
 - Login to SWFT to reset your password no more than 72 hours BEFORE your certificate expires
 - When you receive your new certificate (within 72 hours of resetting your password), return to SWFT and register your Smart Card
- CAC users will not need to Re-Register their Smart Cards
- Refer to Section 6.2 of the User Guide for more information



Smart Card Re-Registration



Secure Web Fingerprint Transmission (SWFT)

Eramo, Andrew - DMDC1 - Last login time: 03/11/2014 20:55 GMT



- Home
- Biometric Upload
- Reports
- User Settings**
- Help
- Logout

User Settings

Email Example: xxx@company.com (must contain '@' and '.')

Phone Example: 703.325.9999, 703-325-9999, (703) 325-9999 or 7033259999

RE-REGISTER PIV, PIV-I OR ECA SMART CARD

To re-register a PIV, PIV-I or ECA Smart Card you will need your SWFT Login ID and Password for the Smart Card Registration page.

- Create a new password using the fields below. The new password is only valid for 72 hours. After 72 hours you must create another password.
- **IMPORTANT: Reset your SWFT password before your PIV or ECA Smart Card expires. If you forgot your Login ID, contact your Account Manager.**
- Enter the SWFT URL and select the new Smart Card certificate.
- You will be directed to the Smart Card Registration page, where you will enter your Login ID and Password.
- Once SWFT validates your information, access to SWFT is granted.

New Password
Verify New Password

Passwords in the SWFT system are complex and will expire in 72 hours. Passwords must be at least 15 characters, containing at least two upper case characters, two lower case characters, two digits, and two special characters.

Change

RE-REGISTER CAC SMART CARD

To re-register a CAC Smart Card

- Enter the SWFT URL and select the Smart Card certificate. Once the certificate is validated; access to SWFT is granted.



Secure Web Fingerprint Transmission (SWFT) Webinar

January 2015



Agenda

- Scanner Registration and Testing
- Reports
- Account Policies
- Resources and Communication
- Demo
- Q&A

Please mute your phones unless you are asking a question and do not use the hold feature



Scanner Registration & Testing

- Select the “Scanner Registration” button
- Select “Add Scanner”
- Complete the form and select “Submit”
 - Ensure that TCN Prefix is the appropriate format (next slide)
- You will receive e-mail notification when you are able to submit a test file



Scanner Registration - Add

*Indicates required field

Status: Date Submitted to OPM:

Company Name: *Cage Code/Site:

*Serial #:

*Hardware Vendor: *Software Vendor:

*Device Model: *TCN Prefix: [Help: Scanner Configuration and Registration Guide](#)

*Operating System:

Physical Location of Scanner

*Address 1:

Address 2:

*City: *State/Country: Zip Code:

Comments:



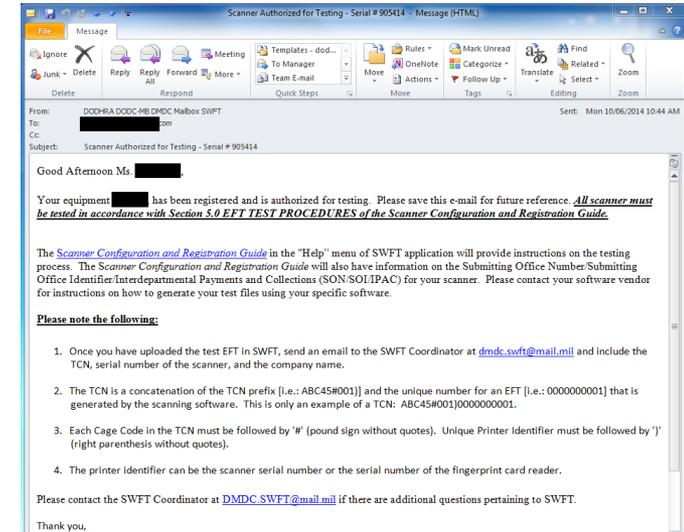
Scanner Registration & Testing

- TCN Prefix Format:
- <CAGE Code 1>#<Optional CAGE Code 2>#<Unique Printer Identifier>
 - CAGE Code 1 = Your company's CAGE Code or the CAGE Code of your parent company
 - Optional CAGE Code 2 = Your branch's CAGE Code or it can be omitted
 - Unique Printer Identifier = Serial Number
 - The TCN Prefix must end with the ")" and each component of the prefix must be separated by a "#."
- Example: 8L667#XB373#201206111523)



Scanner Registration & Testing

- Submit a test EFT within 60 days of receiving approval to test notification
 - A test must be submitted before official usage can begin
 - It is recommended that the test be submitted within two weeks of receiving approval to test
- Email the SWFT Coordinator (dmdc.swft@mail.mil) after the test file is submitted
- Wait for Approval for Production notification or further instruction from the SWFT Coordinator





Scanner Registration & Testing

- Re-registration and Re-testing required if:
 - Any part of the system is replaced (workstation, scanner, or both)
 - Software replacement or upgrade
 - Equipment re-location outside of the current building
- Additional information can be found on the PSA Website or in the Configuration Guide, which can be found in SWFT





Reports

- Select the “Reports” button
- Available Reports for All:
 - Status by Date, Name, SSN
 - Discrepancy
 - Archived Biometrics Status by Date, Name, or SSN
- Available Reports for Org/Site Admins:
 - Scanner Registration Status by CAGE Code or Hardware Vendor and Serial Number
 - Uploader Multi-Site Detail
 - Uploader Multi-Site Summary





Reports

- Archived Biometrics Status
 - Confirm that the SON/SOI/IPAC for the eFP were entered correctly
 - Contact the SWFT Coordinator
- Discrepancy Report:
 - Discrepancies between fields in the EFT and the e-QIP file will be highlighted
 - User's responsibility to manually adjust the incorrect information and resubmit
- EFTs that have an associated e-QIP are released to OPM every 30 minutes
- EFTs that do not match an e-QIP are released to OPM with a 24 hour delay



Account Policies

- Accounts are locked after 30 days of inactivity
 - Site/Organization Admins can unlock accounts
 - DMDC Contact Center can unlock Organization Admin accounts
- Accounts are deactivated after 45 days of inactivity
 - Deactivated accounts are not able to be reactivated
 - Deactivated users will require a new UserID to access SWFT, which requires a new PSSAR to be submitted
- It is recommended that users set a calendar reminder with a 25-28 day recurrence in order to avoid having their accounts locked or deactivated
- Upcoming SWFT enhancement will provide automated email messages to warn users in advance of account expiration.



Resources

- Visit the [PSA Website](#) to Find Additional Resources:
 - Newsletter
 - PKI Frequently Asked Questions
 - Release Notes
 - General Announcements
 - <https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=SWFT>
- [DoD approved PKI Vendors](#)
- [Access, Registration, and Test Guide](#)
- [PSSAR Sample](#), [Instructions](#), and [Checklist](#)
- DoD ECA approved vendors can be found [here](#) and approved Non-Federal Issuers including all of the Category II listed providers [here](#).



Communication

- Technical Assistance/PSSAR Submissions/Account Information:
dmdc.contactcenter@mail.mil
- SWFT Coordinator/SWFT Program Manager:
dmdc.swft@mail.mil



Demo



Questions



Backup



Multi-Site Uploader Role

- Service Provider Acts with Limited Privileges on Behalf of Another Company
 - Serviced Company must be registered in SWFT and have their own SWFT account
 - PSSAR required to become a Multi-Site Uploader
- Serviced company obtains account to generate detailed reports
- Service Provider is able to generate reports that identify the date and number of EFTs uploaded for the purpose of billing and accountability



Multi-Site Uploader Role

- **ONLY** one Cage Code is able to be assigned to a Multi-Site Uploader account
- Users with Multiple Cage Codes assigned to their accounts who wish to have the Multi-Site Uploader role should request a separate account
 - Maintains full reporting capabilities through your existing account with Multiple Cage Codes
 - Allows you the ability to upload eFPs for any company in SWFT through your separate Multi-Site Uploader account



Smart Card Re-Registration

- PIV, PIV-I, and ECA users will need their SWFT Login ID and a Password to Re-Register their Smart Card
 - If you forgot your username, contact your Site or Organization Administrator
 - Login to SWFT to reset your password no more than 72 hours BEFORE your certificate expires
 - When you receive your new certificate (within 72 hours of resetting your password), return to SWFT and register your Smart Card
- CAC users will not need to Re-Register their Smart Cards
- Refer to Section 6.2 of the User Guide for more information



Smart Card Re-Registration



Secure Web Fingerprint Transmission (SWFT)

Eramo, Andrew - DMDC1 - Last login time: 03/11/2014 20:55 GMT



- Home
- Biometric Upload
- Reports
- User Settings**
- Help
- Logout

User Settings

Email Example: xxx@company.com (must contain '@' and '.')

Phone Example: 703.325.9999, 703-325-9999, (703) 325-9999 or 7033259999

RE-REGISTER PIV, PIV-I OR ECA SMART CARD

To re-register a PIV, PIV-I or ECA Smart Card you will need your SWFT Login ID and Password for the Smart Card Registration page.

- Create a new password using the fields below. The new password is only valid for 72 hours. After 72 hours you must create another password.
IMPORTANT: Reset your SWFT password before your PIV or ECA Smart Card expires. If you forgot your Login ID, contact your Account Manager.
- Enter the SWFT URL and select the new Smart Card certificate.
- You will be directed to the Smart Card Registration page, where you will enter your Login ID and Password.
- Once SWFT validates your information, access to SWFT is granted.

New Password
Verify New Password

Passwords in the SWFT system are complex and will expire in 72 hours. Passwords must be at least 15 characters, containing at least two upper case characters, two lower case characters, two digits, and two special characters.

RE-REGISTER CAC SMART CARD

To re-register a CAC Smart Card

- Enter the SWFT URL and select the Smart Card certificate. Once the certificate is validated; access to SWFT is granted.



Secure Web Fingerprint Transmission (SWFT) Webinar

December 2014



Agenda

- Reports
- Multi-Site Uploader Role
- Account Policies
- Resources and Communication
- Demo
- Q&A

Please mute your phones unless you are asking a question and do not use the hold feature



Reports

- Select the “Reports” button
- Available Reports for All:
 - Status by Date, Name, SSN
 - Discrepancy
 - Archived Biometrics Status by Date, Name, or SSN
- Available Reports for Org/Site Admins:
 - Scanner Registration Status by CAGE Code or Hardware Vendor and Serial Number
 - Uploader Multi-Site Detail
 - Uploader Multi-Site Summary





Reports

- Archived Biometrics Status
 - Confirm that the SON/SOI/IPAC for the eFP were entered correctly
 - Contact the SWFT Coordinator
- Discrepancy Report:
 - Discrepancies between fields in the EFT and the e-QIP file will be highlighted
 - User's responsibility to manually adjust the incorrect information and resubmit
- EFTs that have an associated e-QIP are released to OPM every 30 minutes
- EFTs that do not match an e-QIP are released to OPM with a 24 hour delay



Multi-Site Uploader Role

- Service Provider Acts with Limited Privileges on Behalf of Another Company
 - Serviced Company must be registered in SWFT and have their own SWFT account
 - PSSAR required to become a Multi-Site Uploader
- Serviced company obtains account to generate detailed reports
- Service Provider is able to generate reports that identify the date and number of EFTs uploaded for the purpose of billing and accountability



Multi-Site Uploader Role

- **ONLY** one Cage Code is able to be assigned to a Multi-Site Uploader account
- Users with Multiple Cage Codes assigned to their accounts who wish to have the Multi-Site Uploader role should request a separate account
 - Maintains full reporting capabilities through your existing account with Multiple Cage Codes
 - Allows you the ability to upload eFPs for any company in SWFT through your separate Multi-Site Uploader account



Account Policies

- Accounts are locked after 30 days of inactivity
 - Site/Organization Admins can unlock accounts
 - DMDC Contact Center can unlock Organization Admin accounts
- Accounts are deactivated after 45 days of inactivity
 - Deactivated accounts are not able to be reactivated
 - Deactivated users will require a new UserID to access SWFT, which requires a new PSSAR to be submitted
- It is recommended that users set a calendar reminder with a 25-28 day recurrence in order to avoid having their accounts locked or deactivated



Resources

- Visit the [PSA Website](#) to Find Additional Resources:
 - Newsletter
 - PKI Frequently Asked Questions
 - Release Notes
 - General Announcements
 - <https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=SWFT>
- [DoD approved PKI Vendors](#)
- [Access, Registration, and Test Guide](#)
- [PSSAR Sample](#), [Instructions](#), and [Checklist](#)
- DoD ECA approved vendors can be found [here](#) and approved Non-Federal Issuers including all of the Category II listed providers [here](#).



Communication

- Technical Assistance/PSSAR Submissions/Account Information:
dmdc.contactcenter@mail.mil
- SWFT Coordinator/SWFT Program Manager:
dmdc.swft@mail.mil



Demo



Questions



Backup



Smart Card Re-Registration

- PIV, PIV-I, and ECA users will need their SWFT Login ID and a Password to Re-Register their Smart Card
 - If you forgot your username, contact your Site or Organization Administrator
 - Login to SWFT to reset your password no more than 72 hours BEFORE your certificate expires
 - When you receive your new certificate (within 72 hours of resetting your password), return to SWFT and register your Smart Card
- CAC users will not need to Re-Register their Smart Cards
- Refer to Section 6.2 of the User Guide for more information



Smart Card Re-Registration



Secure Web Fingerprint Transmission (SWFT)

Eramo, Andrew - DMDC1 - Last login time: 03/11/2014 20:55 GMT



- Home
- Biometric Upload
- Reports
- User Settings**
- Help
- Logout

User Settings

Email Example: xxx@company.com (must contain '@' and '.')

Phone Example: 703.325.9999, 703-325-9999, (703) 325-9999 or 7033259999

RE-REGISTER PIV, PIV-I OR ECA SMART CARD

To re-register a PIV, PIV-I or ECA Smart Card you will need your SWFT Login ID and Password for the Smart Card Registration page.

- Create a new password using the fields below. The new password is only valid for 72 hours. After 72 hours you must create another password.
IMPORTANT: Reset your SWFT password before your PIV or ECA Smart Card expires. If you forgot your Login ID, contact your Account Manager.
- Enter the SWFT URL and select the new Smart Card certificate.
- You will be directed to the Smart Card Registration page, where you will enter your Login ID and Password.
- Once SWFT validates your information, access to SWFT is granted.

New Password

Verify New Password

Passwords in the SWFT system are complex and will expire in 72 hours. Passwords must be at least 15 characters, containing at least two upper case characters, two lower case characters, two digits, and two special characters.

Change

RE-REGISTER CAC SMART CARD

To re-register a CAC Smart Card

- Enter the SWFT URL and select the Smart Card certificate. Once the certificate is validated; access to SWFT is granted.



Scanner Registration & Testing

- Select the “Scanner Registration” button
- Select “Add Scanner”
- Complete the form and select “Submit”
- You will receive e-mail notification when you are able to submit a test file



[Add Scanner](#) Scanner Registration

Scanner Registration - Add

*Indicates required field

Status: Date Submitted to OPM:

Company Name: *Cage Code/Site:

*Serial #:

*Hardware Vendor: *Software Vendor:

*Device Model: *TCN Prefix:

*Operating System: [Help: Scanner Configuration and Registration Guide](#)

Physical Location of Scanner

*Address 1:

Address 2:

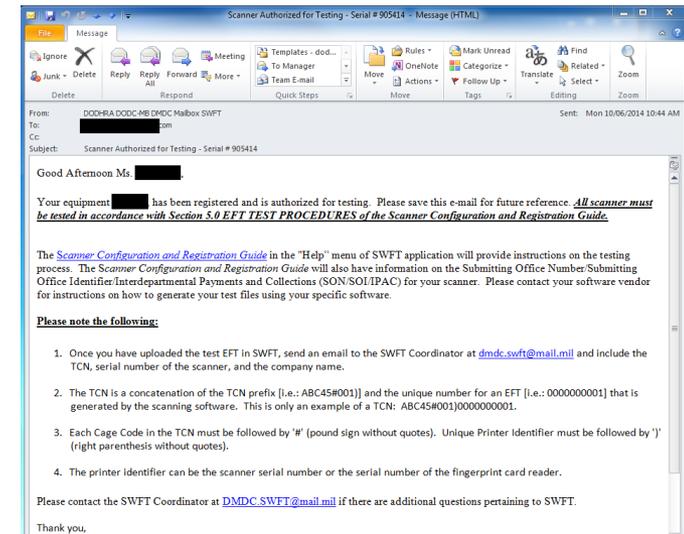
*City: *State/Country: Zip Code:

Comments:



Scanner Registration & Testing

- Submit a test EFT within 60 days of receiving approval to test notification
 - A test must be submitted before official usage can begin
 - It is recommended that the test be submitted within two weeks of receiving approval to test
- Email the SWFT Coordinator (dmdc.swft@mail.mil) after the test file is submitted
- Wait for Approval for Production notification or further instruction from the SWFT Coordinator





Scanner Registration & Testing

- Re-registration and Re-testing required if:
 - Any part of the system is replaced (workstation, scanner, or both)
 - Software replacement or upgrade
 - Equipment re-location outside of the current building
- Additional information can be found on the PSA Website or in the Configuration Guide, which can be found in SWFT





Secure Web Fingerprint Transmission (SWFT) Webinar

November 2014



Agenda

- Scanner Registration and Testing
- Multi-Site Uploader Role
- Reports
- Account Policies
- Resources and Communication
- Q&A

Please mute your phones unless you are asking a question and do not use the hold feature



Scanner Registration & Testing

- Select the “Scanner Registration” button
- Select “Add Scanner”
- Complete the form and select “Submit”
- You will receive e-mail notification when you are able to submit a test file



[Add Scanner](#) Scanner Registration

Scanner Registration - Add

*Indicates required field

Status: Date Submitted to OPM:

Company Name: *Cage Code/Site:

*Serial #:

*Hardware Vendor: *Software Vendor:

*Device Model: *TCN Prefix:

*Operating System: [Help: Scanner Configuration and Registration Guide](#)

Physical Location of Scanner

*Address 1:

Address 2:

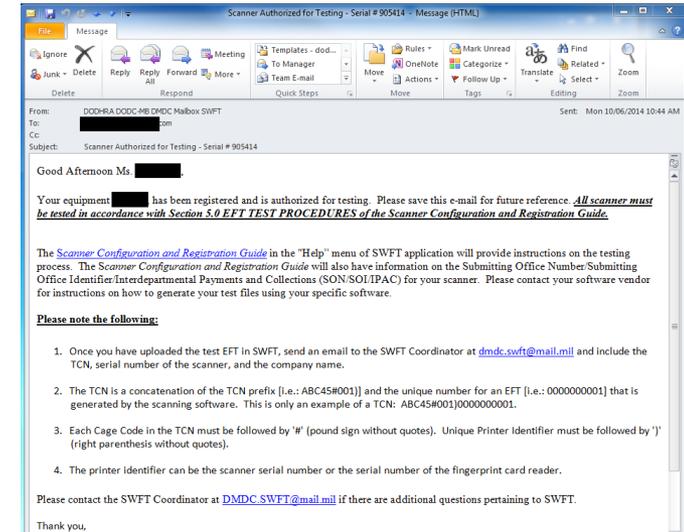
*City: *State/Country: Zip Code:

Comments:



Scanner Registration & Testing

- Submit a test EFT within 60 days of receiving approval to test notification
 - A test must be submitted before official usage can begin
 - It is recommended that the test be submitted within two weeks of receiving approval to test
- Email the SWFT Coordinator (dmdc.swft@mail.mil) after the test file is submitted
- Wait for Approval for Production notification or further instruction from the SWFT Coordinator





Scanner Registration & Testing

- Re-registration and Re-testing required if:
 - Any part of the system is replaced (workstation, scanner, or both)
 - Software replacement or upgrade
 - Equipment re-location outside of the current building
- Additional information can be found on the PSA Website or in the Configuration Guide, which can be found in SWFT





Multi-Site Uploader Role

- Service Provider Acts with Limited Privileges on Behalf of Another Company
 - Serviced Company must be registered in SWFT and have their own SWFT account
 - PSSAR required to become a Multi-Site Uploader
- Serviced company obtains account to generate detailed reports
- Service Provider is able to generate reports that identify the date and number of EFTs uploaded for the purpose of billing and accountability



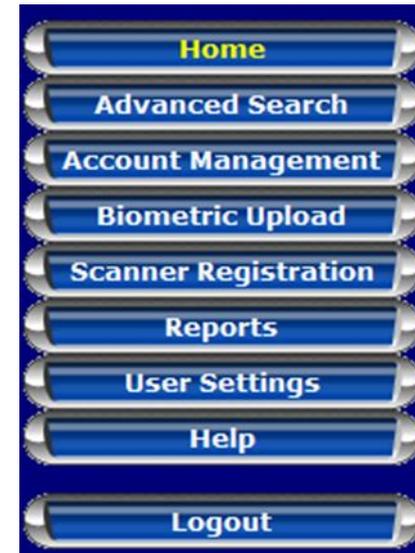
Multi-Site Uploader Role

- **ONLY** one Cage Code is able to be assigned to a Multi-Site Uploader account
- Users with Multiple Cage Codes assigned to their accounts who wish to have the Multi-Site Uploader role should request a separate account
 - Maintains full reporting capabilities through your existing account with Multiple Cage Codes
 - Allows you the ability to upload eFPs for any company in SWFT through your separate Multi-Site Uploader account



Reports

- Select the “Reports” button
- Available Reports for All:
 - Status by Date, Name, SSN
 - Discrepancy
 - Archived Biometrics Status by Date, Name, or SSN
- Available Reports for Org/Site Admins:
 - Scanner Registration Status by CAGE Code or Hardware Vendor and Serial Number
 - Uploader Multi-Site Detail
 - Uploader Multi-Site Summary





Reports

- Archived Biometrics Status
 - Confirm that the SON/SOI/IPAC for the eFP were entered correctly
 - Contact the SWFT Coordinator
- Discrepancy Report:
 - Discrepancies between fields in the EFT and the e-QIP file will be highlighted
 - User's responsibility to manually adjust the incorrect information and resubmit
- EFTs that have an associated e-QIP are released to OPM every 30 minutes
- EFTs that do not match an e-QIP are released to OPM with a 24 hour delay



Account Policies

- Accounts are locked after 30 days of inactivity
 - Site/Organization Admins can unlock accounts
 - DMDC Contact Center can unlock Organization Admin accounts
- Accounts are deactivated after 45 days of inactivity
 - Deactivated accounts are not able to be reactivated
 - Deactivated users will require a new UserID to access SWFT, which requires a new PSSAR to be submitted
- It is recommended that users set a calendar reminder with a 25-28 day recurrence in order to avoid having their accounts locked or deactivated



Resources

- Visit the [PSA Website](#) to Find Additional Resources:
 - Newsletter
 - PKI Frequently Asked Questions
 - Release Notes
 - General Announcements
 - <https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=SWFT>
- [DoD approved PKI Vendors](#)
- [Access, Registration, and Test Guide](#)
- [PSSAR Sample](#), [Instructions](#), and [Checklist](#)
- DoD ECA approved vendors can be found [here](#) and approved Non-Federal Issuers including all of the Category II listed providers [here](#).



Communication

- Technical Assistance/PSSAR Submissions/Account Information:
dmdc.contactcenter@mail.mil
- SWFT Coordinator/SWFT Program Manager:
dmdc.swft@mail.mil



Questions



Backup



Smart Card Re-Registration

- PIV, PIV-I, and ECA users will need their SWFT Login ID and a Password to Re-Register their Smart Card
 - If you forgot your username, contact your Site or Organization Administrator
 - Login to SWFT to reset your password no more than 72 hours BEFORE your certificate expires
 - When you receive your new certificate (within 72 hours of resetting your password), return to SWFT and register your Smart Card
- CAC users will not need to Re-Register their Smart Cards
- Refer to Section 6.2 of the User Guide for more information



Smart Card Re-Registration



Secure Web Fingerprint Transmission (SWFT)

Eramo, Andrew - DMDC1 - Last login time: 03/11/2014 20:55 GMT



- Home
- Biometric Upload
- Reports
- User Settings**
- Help
- Logout

User Settings

Email Example: xxx@company.com (must contain '@' and '.')

Phone Example: 703.325.9999, 703-325-9999, (703) 325-9999 or 7033259999

RE-REGISTER PIV, PIV-I OR ECA SMART CARD

To re-register a PIV, PIV-I or ECA Smart Card you will need your SWFT Login ID and Password for the Smart Card Registration page.

- Create a new password using the fields below. The new password is only valid for 72 hours. After 72 hours you must create another password.
IMPORTANT: Reset your SWFT password before your PIV or ECA Smart Card expires. If you forgot your Login ID, contact your Account Manager.
- Enter the SWFT URL and select the new Smart Card certificate.
- You will be directed to the Smart Card Registration page, where you will enter your Login ID and Password.
- Once SWFT validates your information, access to SWFT is granted.

New Password

Verify New Password

Passwords in the SWFT system are complex and will expire in 72 hours. Passwords must be at least 15 characters, containing at least two upper case characters, two lower case characters, two digits, and two special characters.

RE-REGISTER CAC SMART CARD

To re-register a CAC Smart Card

- Enter the SWFT URL and select the Smart Card certificate. Once the certificate is validated; access to SWFT is granted.



Secure Web Fingerprint Transmission (SWFT) Webinar

October 2014



Agenda

- Scanner Registration and Testing
- Multi-Site Uploader Role
- Reports
- Account Policies
- Resources and Communication
- Q&A

Please mute your phones unless you are asking a question and do not use the hold feature



Scanner Registration & Testing

- Select the “Scanner Registration” button
- Select “Add Scanner”
- Complete the form and select “Submit”
- You will receive e-mail notification when you are able to submit a test file



Scanner Registration - Add

*Indicates required field

Status: Date Submitted to OPM:

Company Name: *Cage Code/Site:

*Serial #:

*Hardware Vendor: *Software Vendor:

*Device Model: *TCN Prefix:

*Operating System: [Help: Scanner Configuration and Registration Guide](#)

Physical Location of Scanner

*Address 1:

Address 2:

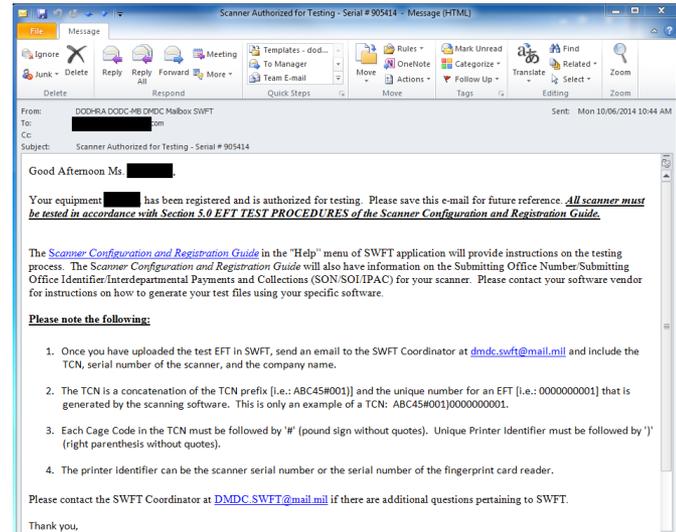
*City: *State/Country: Zip Code:

Comments:



Scanner Registration & Testing

- Submit a test EFT within 60 days of receiving approval to test notification
 - A test must be submitted before official usage can begin
 - It is recommended that the test be submitted within two weeks of receiving approval to test
- Email the SWFT Coordinator (dmdc.swft@mail.mil) after the test file is submitted
- Wait for Approval for Production notification or further instruction from the SWFT Coordinator





Scanner Registration & Testing

- Re-registration and Re-testing required if:
 - Any part of the system is replaced (workstation, scanner, or both)
 - Software replacement or upgrade
 - Equipment re-location outside of the current building
- Additional information can be found on the PSA Website or in the Configuration Guide, which can be found in SWFT





Multi-Site Uploader Role

- Service Provider Acts with Limited Privileges on Behalf of Another Company
 - Serviced Company must be registered in SWFT and have their own SWFT account
 - PSSAR required to become a Multi-Site Uploader
- Serviced company obtains account to generate detailed reports
- Service Provider is able to generate reports that identify the date and number of EFTs uploaded for the purpose of billing and accountability



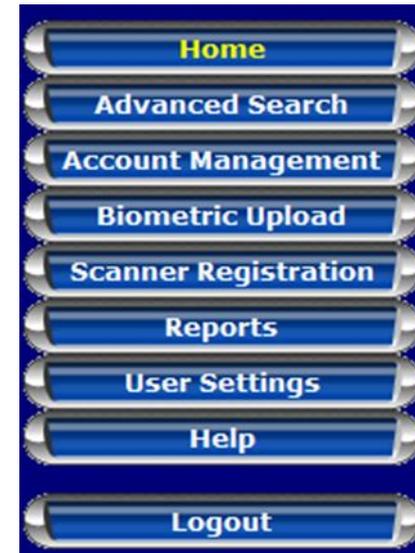
Multi-Site Uploader Role

- **ONLY** one Cage Code is able to be assigned to a Multi-Site Uploader account
- Users with Multiple Cage Codes assigned to their accounts who wish to have the Multi-Site Uploader role should request a separate account
 - Maintains full reporting capabilities through your existing account with Multiple Cage Codes
 - Allows you the ability to upload eFPs for any company in SWFT through your separate Multi-Site Uploader account



Reports

- Select the “Reports” button
- Available Reports for All:
 - Status by Date, Name, SSN
 - Discrepancy
 - Archived Biometrics Status by Date, Name, or SSN
- Available Reports for Org/Site Admins:
 - Scanner Registration Status by CAGE Code or Hardware Vendor and Serial Number
 - Uploader Multi-Site Detail
 - Uploader Multi-Site Summary





Reports

- Archived Biometrics Status
 - Confirm that the SON/SOI/IPAC for the eFP were entered correctly
 - Contact the SWFT Coordinator
- Discrepancy Report:
 - Discrepancies between fields in the EFT and the e-QIP file will be highlighted
 - User's responsibility to manually adjust the incorrect information and resubmit



Account Policies

- Accounts are locked after 30 days of inactivity
 - Site/Organization Admins can unlock accounts
 - DMDC Contact Center can unlock Organization Admin accounts
- Accounts are deactivated after 45 days of inactivity
 - Deactivated accounts are not able to be reactivated
 - Deactivated users will require a new UserID to access SWFT, which requires a new PSSAR to be submitted
- It is recommended that users set a calendar reminder with a 25-28 day recurrence in order to avoid having their accounts locked or deactivated



Resources

- Visit the [PSA Website](#) to Find Additional Resources:
 - Newsletter
 - PKI Frequently Asked Questions
 - Release Notes
 - General Announcements
 - <https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=SWFT>
- [DoD approved PKI Vendors](#)
- [Access, Registration, and Test Guide](#)
- [PSSAR Sample](#), [Instructions](#), and [Checklist](#)
- DoD ECA approved vendors can be found [here](#) and approved Non-Federal Issuers including all of the Category II listed providers [here](#).



Communication

- Technical Assistance/PSSAR Submissions/Account Information:
dmdc.contactcenter@mail.mil
- SWFT Coordinator/SWFT Program Manager:
dmdc.swft@mail.mil



Questions



Backup



Smart Card Re-Registration

- PIV, PIV-I, and ECA users will need their SWFT Login ID and a Password to Re-Register their Smart Card
 - If you forgot your username, contact your Site or Organization Administrator
 - Login to SWFT to reset your password no more than 72 hours BEFORE your certificate expires
 - When you receive your new certificate (within 72 hours of resetting your password), return to SWFT and register your Smart Card
- CAC users will not need to Re-Register their Smart Cards
- Refer to Section 6.2 of the User Guide for more information



Smart Card Re-Registration



Secure Web Fingerprint Transmission (SWFT)

Eramo, Andrew - DMDC1 - Last login time: 03/11/2014 20:55 GMT



- Home
- Biometric Upload
- Reports
- User Settings**
- Help
- Logout

User Settings

Email Example: xxx@company.com (must contain '@' and '.')

Phone Example: 703.325.9999, 703-325-9999, (703) 325-9999 or 7033259999

RE-REGISTER PIV, PIV-I OR ECA SMART CARD

To re-register a PIV, PIV-I or ECA Smart Card you will need your SWFT Login ID and Password for the Smart Card Registration page.

- Create a new password using the fields below. The new password is only valid for 72 hours. After 72 hours you must create another password.
IMPORTANT: Reset your SWFT password before your PIV or ECA Smart Card expires. If you forgot your Login ID, contact your Account Manager.
- Enter the SWFT URL and select the new Smart Card certificate.
- You will be directed to the Smart Card Registration page, where you will enter your Login ID and Password.
- Once SWFT validates your information, access to SWFT is granted.

New Password

Verify New Password

Passwords in the SWFT system are complex and will expire in 72 hours. Passwords must be at least 15 characters, containing at least two upper case characters, two lower case characters, two digits, and two special characters.

Change

RE-REGISTER CAC SMART CARD

To re-register a CAC Smart Card

- Enter the SWFT URL and select the Smart Card certificate. Once the certificate is validated; access to SWFT is granted.



Secure Web Fingerprint Transmission (SWFT) Webinar

September 2014



Agenda

- Multi-Site Uploader Role
- Reports
- Account Policies
- Resources and Communication
- Q&A

Please mute your phones unless you are asking a question and do not use the hold feature



Multi-Site Uploader Role

- Service Provider Acts with Limited Privileges on Behalf of Another Company
 - Serviced Company must be registered in SWFT and have their own SWFT account
 - PSSAR required to become a Multi-Site Uploader
- Serviced company obtains account to generate detailed reports
- Service Provider is able to generate reports that identify the date and number of EFTs uploaded for the purpose of billing and accountability



Multi-Site Uploader Role

- **ONLY** one Cage Code is able to be assigned to a Multi-Site Uploader account
- Users with Multiple Cage Codes assigned to their accounts who wish to have the Multi-Site Uploader role should request a separate account
 - Maintains full reporting capabilities through your existing account with Multiple Cage Codes
 - Allows you the ability to upload eFPs for any company in SWFT through your separate Multi-Site Uploader account



Reports

- Select the “Reports” button
- Available Reports for All:
 - Status by Date, Name, SSN
 - Discrepancy
 - Archived Biometrics Status by Date, Name, or SSN
- Available Reports for Org/Site Admins:
 - Scanner Registration Status by CAGE Code or Hardware Vendor and Serial Number
 - Uploader Multi-Site Detail
 - Uploader Multi-Site Summary





Reports

- Archived Biometrics Status
 - Confirm that the SON/SOI/IPAC for the eFP were entered correctly
 - Contact the SWFT Coordinator
- Discrepancy Report:
 - Discrepancies between fields in the EFT and the e-QIP file will be highlighted
 - User's responsibility to manually adjust the incorrect information and resubmit



Account Policies

- Accounts are locked after 30 days of inactivity
 - Site/Organization Admins can unlock accounts
 - DMDC Contact Center can unlock Organization Admin accounts
- Accounts are deactivated after 45 days of inactivity
 - Deactivated accounts are not able to be reactivated
 - Deactivated users will require a new UserID to access SWFT, which requires a new PSSAR to be submitted
- It is recommended that users set a calendar reminder with a 25-28 day recurrence in order to avoid having their accounts locked or deactivated



Resources

- Visit the [PSA Website](#) to Find Additional Resources:
 - Newsletter
 - PKI Frequently Asked Questions
 - Release Notes
 - General Announcements
 - <https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=SWFT>
- [DoD approved PKI Vendors](#)
- [Access, Registration, and Test Guide](#)
- [PSSAR Sample](#), [Instructions](#), and [Checklist](#)
- DoD ECA approved vendors can be found [here](#) and approved Non-Federal Issuers including all of the Category II listed providers [here](#).



Communication

- Technical Assistance/PSSAR Submissions/Account Information:
dmdc.contactcenter@mail.mil
- SWFT Coordinator/SWFT Program Manager:
dmdc.swft@mail.mil



Questions



Backup



Smart Card Re-Registration

- PIV, PIV-I, and ECA users will need their SWFT Login ID and a Password to Re-Register their Smart Card
 - If you forgot your username, contact your Site or Organization Administrator
 - Login to SWFT to reset your password no more than 72 hours BEFORE your certificate expires
 - When you receive your new certificate (within 72 hours of resetting your password), return to SWFT and register your Smart Card
- CAC users will not need to Re-Register their Smart Cards
- Refer to Section 6.2 of the User Guide for more information



Smart Card Re-Registration



Secure Web Fingerprint Transmission (SWFT)

Eramo, Andrew - DMDC1 - Last login time: 03/11/2014 20:55 GMT



- Home
- Biometric Upload
- Reports
- User Settings**
- Help
- Logout

User Settings

Email Example: xxx@company.com (must contain '@' and '.')

Phone Example: 703.325.9999, 703-325-9999, (703) 325-9999 or 7033259999

RE-REGISTER PIV, PIV-I OR ECA SMART CARD

To re-register a PIV, PIV-I or ECA Smart Card you will need your SWFT Login ID and Password for the Smart Card Registration page.

- Create a new password using the fields below. The new password is only valid for 72 hours. After 72 hours you must create another password.
IMPORTANT: Reset your SWFT password before your PIV or ECA Smart Card expires. If you forgot your Login ID, contact your Account Manager.
- Enter the SWFT URL and select the new Smart Card certificate.
- You will be directed to the Smart Card Registration page, where you will enter your Login ID and Password.
- Once SWFT validates your information, access to SWFT is granted.

New Password
Verify New Password

Passwords in the SWFT system are complex and will expire in 72 hours. Passwords must be at least 15 characters, containing at least two upper case characters, two lower case characters, two digits, and two special characters.

Change

RE-REGISTER CAC SMART CARD

To re-register a CAC Smart Card

- Enter the SWFT URL and select the Smart Card certificate. Once the certificate is validated; access to SWFT is granted.



Scanner Registration

- Select the “Scanner Registration” button
- Select “Add Scanner”
- Complete the form and select “Submit”
- You will receive e-mail notification when you are able to submit a test file



Scanner Registration

[Add Scanner](#)

Scanner Registration - Add

*Indicates required field

Status: Date Submitted to OPM:

Company Name: *Cage Code/Site:

*Serial #:

*Hardware Vendor: *Software Vendor:

*Device Model: *TCN Prefix:

*Operating System: [Help: Scanner Configuration and Registration Guide](#)

Physical Location of Scanner

*Address 1:

Address 2:

*City: *State/Country: Zip Code:

Comments:



Secure Web Fingerprint Transmission (SWFT) Webinar

July 2014



Agenda

- Resources and Communication
- Q&A

Please mute your phones unless you are asking a question and do not use the hold feature



Resources

- Visit the [PSA Website](#) to Find Additional Resources:
 - Newsletter
 - PKI Frequently Asked Questions
 - Release Notes
 - General Announcements
 - <https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=SWFT>
- [DoD approved PKI Vendors](#)
- [Access, Registration, and Test Guide](#)
- [PSSAR Sample](#), [Instructions](#), and [Checklist](#)
- DoD ECA approved vendors can be found [here](#) and approved Non-Federal Issuers including all of the Category II listed providers [here](#).



Communication

- Technical Assistance/PSSAR Submissions/Account Information:
dmdc.contactcenter@mail.mil
- SWFT Coordinator/SWFT Program Manager:
dmdc.swft@mail.mil



Questions



Backup



Smart Card Re-Registration

- PIV, PIV-I, and ECA users will need their SWFT Login ID and a Password to Re-Register their Smart Card
 - If you forgot your username, contact your Site or Organization Administrator
 - Login to SWFT to reset your password no more than 72 hours BEFORE your certificate expires
 - When you receive your new certificate (within 72 hours of resetting your password), return to SWFT and register your Smart Card
- CAC users will not need to Re-Register their Smart Cards
- Refer to Section 6.2 of the User Guide for more information



Smart Card Re-Registration



Secure Web Fingerprint Transmission (SWFT)

Eramo, Andrew - DMDC1 - Last login time: 03/11/2014 20:55 GMT



- Home
- Biometric Upload
- Reports
- User Settings**
- Help
- Logout

User Settings

Email Example: xxx@company.com (must contain '@' and '.')
Phone Example: 703.325.9999, 703-325-9999, (703) 325-9999 or 7033259999

RE-REGISTER PIV, PIV-I OR ECA SMART CARD

To re-register a PIV, PIV-I or ECA Smart Card you will need your SWFT Login ID and Password for the Smart Card Registration page.

- Create a new password using the fields below. The new password is only valid for 72 hours. After 72 hours you must create another password.
IMPORTANT: Reset your SWFT password before your PIV or ECA Smart Card expires. If you forgot your Login ID, contact your Account Manager.
- Enter the SWFT URL and select the new Smart Card certificate.
- You will be directed to the Smart Card Registration page, where you will enter your Login ID and Password.
- Once SWFT validates your information, access to SWFT is granted.

New Password Passwords in the SWFT system are complex and will expire in 72 hours. Passwords must be at least 15 characters, containing at least two upper case characters, two lower case characters, two digits, and two special characters.
Verify New Password

Change

RE-REGISTER CAC SMART CARD

To re-register a CAC Smart Card

- Enter the SWFT URL and select the Smart Card certificate. Once the certificate is validated; access to SWFT is granted.



Scanner Registration

- Select the “Scanner Registration” button
- Select “Add Scanner”
- Complete the form and select “Submit”
- You will receive e-mail notification when you are able to submit a test file



Scanner Registration - Add

*Indicates required field

Status: Date Submitted to OPM:

Company Name: *Cage Code/Site:

*Serial #:

*Hardware Vendor: *Software Vendor:

*Device Model: *TCN Prefix:

*Operating System: [Help: Scanner Configuration and Registration Guide](#)

Physical Location of Scanner

*Address 1:

Address 2:

*City: *State/Country: Zip Code:

Comments:



Organization and Site Administrator Roles

- Organization Administrator is typically the FSO
- Site Administrator allows large companies to better manage multiple sites by creating an additional layer of administration

	Organization Administrator	Site Administrator
Upload EFT	Yes	Yes
Run EFT Status Reports	Yes	Yes
Create/Edit/Deactivate Site	Yes	No
Add Users	Yes	Yes
Edit Users	Yes	Yes
Deactivate Users	Yes	Yes
Set Passwords	Yes	Yes
Scanner Registration	Yes	No
Multiple Site Uploader	Yes	Yes



SWFT Naming Conventions

- The PSSAR Form is in the process of being updated. Until it is revised, use the following conventions to request accounts

User Account

PSSAR Form:

18. SECURE WEB FINGERPRINT TRANSMISSION (SWFT)				
CAGE CODE(S): <input type="text"/>				
<input checked="" type="checkbox"/> USER	<input type="checkbox"/> MULT. COMPANY UPLOADER	<input type="checkbox"/> ACCOUNT MANAGER	<input type="checkbox"/> EXECUTIVE ACCOUNT MANAGER	<input type="checkbox"/> SWFT ADMINISTRATOR

Account Creation Page:

Permissions:						
<input checked="" type="checkbox"/> Upload EFT	<input type="checkbox"/> Multi Site Uploader	<input type="checkbox"/> Site Administrator	<input type="checkbox"/> Edit User and Site	<input type="checkbox"/> Set User Permissions	<input type="checkbox"/> Edit Company	<input type="checkbox"/> SWFT Admin



Organization and Site Administrator Roles

- Organization/Site Administrators must receive and keep on file a fully completed and validated PSSAR
 - Must be signed by the Requestor, Nominating Official (must be different from requestor), and Validating Official
- PSSARs must be kept on file until 6 months after the account is deactivated



Secure Web Fingerprint Transmission (SWFT) Webinar

June 2014



Agenda

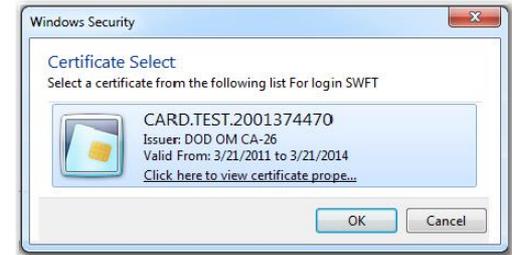
- Logging into SWFT
- Uploading EFTs
- Running Reports
- Account Management
- Scanner Registration
- Resources
- Q&A

Please mute your phones unless you are asking a question and do not use the hold feature



Logging Into SWFT for the First Time - Certificate Registration

- Select the Certificate and Enter PIN
- Enter Login ID and Password on the Smart Card Registration screen
 - Login ID and Password received from Org Admin, Site Admin, or Contact Center
 - Password for registration is only valid for 72 hours



Smart Card Registration

- When registering a Smart card, a PIN number is used for authentication and accessing SWFT. Once your Smart card is registered then all associated Login ID(s) and password(s) are disabled and cannot be used to access SWFT.
- Go to User Settings and reset your password if you need to re-register a Smart card, or register additional Smart cards. If you have forgotten your Login ID, contact your Organization Administrator.

Login ID

Password



Logging Into SWFT

- Select the registered Certificate and Enter PIN
- Acknowledge the DoD Notice and Consent
- Users with multiple accounts (ie: Multi-Site Uploaders, Org Admins) will need to select the desired account
- Select the Desired Site, if your account has multiple CAGE codes assigned



SWFT 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.

The U.S. Department of Defense is committed to making its electronic and information technologies accessible to individuals with disabilities in accordance with [Section 508 of the Rehabilitation Act \(29 U.S.C. § 794d\), as amended in 1999](#). Send feedback or concerns related to the accessibility of this website to: doDSection508@usd.mil. For more information about Section 508, please visit the [DoD Section 508 website](#). Last Updated: 09/06/2013

I acknowledge and accept the above access statement.

Enter

Account Selection

Select	Login ID	Role(s)	Company
<input checked="" type="radio"/>	Admin3	UploadEFT, EDR User and Site	Test Company
<input type="radio"/>	User20130918110403304	UploadEFT, EDR User and Site, EDR Company, SWFT Admin, Set User Permissions, Multiple Company Upload	Defense Security Service

Set Current Account

Site Selection

Select Site Location: **DMDC**

- DMDC
- East Coast
- Test City

Set Current Site



Smart Card Re-Registration

- Register your new PK certificate after the old expired
- PIV, PIV-I, and ECA users will need their SWFT Login ID and a Password to Re-Register their Smart Card
 - Users can reset their temporary password themselves if done before their old certificate expired
 - If you forgot your username, contact your Site or Organization Administrator
 - Login to SWFT to reset your password no more than 72 hours BEFORE your certificate expires
 - When you receive your new certificate (within 72 hours of resetting your password), return to SWFT and register your Smart Card with your username and temporary password
- CAC users will not need to Re-Register their Smart Cards



Smart Card Re-Registration



Secure Web Fingerprint Transmission (SWFT)

Eramo, Andrew - DMDC1 - Last login time: 03/11/2014 20:55 GMT



- Home
- Biometric Upload
- Reports
- User Settings**
- Help
- Logout

User Settings

Email Example: xxx@company.com (must contain '@' and '.')
Phone Example: 703.325.9999, 703-325-9999, (703) 325-9999 or 7033259999

RE-REGISTER PIV, PIV-I OR ECA SMART CARD

To re-register a PIV, PIV-I or ECA Smart Card you will need your SWFT Login ID and Password for the Smart Card Registration page.

- Create a new password using the fields below. The new password is only valid for 72 hours. After 72 hours you must create another password.
IMPORTANT: Reset your SWFT password before your PIV or ECA Smart Card expires. If you forgot your Login ID, contact your Account Manager.
- Enter the SWFT URL and select the new Smart Card certificate.
- You will be directed to the Smart Card Registration page, where you will enter your Login ID and Password.
- Once SWFT validates your information, access to SWFT is granted.

New Password Passwords in the SWFT system are complex and will expire in 72 hours. Passwords must be at least 15 characters, containing at least two upper case characters, two lower case characters, two digits, and two special characters.
Verify New Password

Change

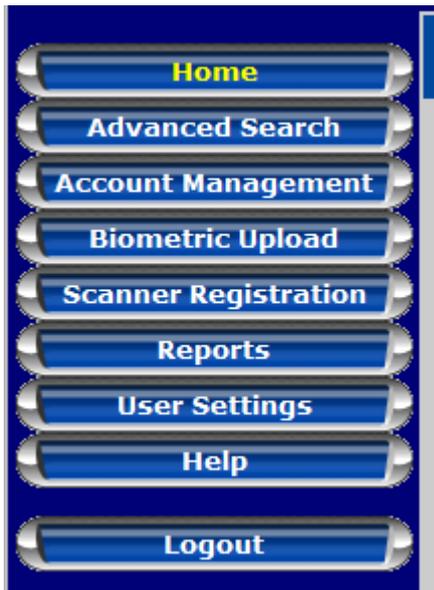
RE-REGISTER CAC SMART CARD

To re-register a CAC Smart Card

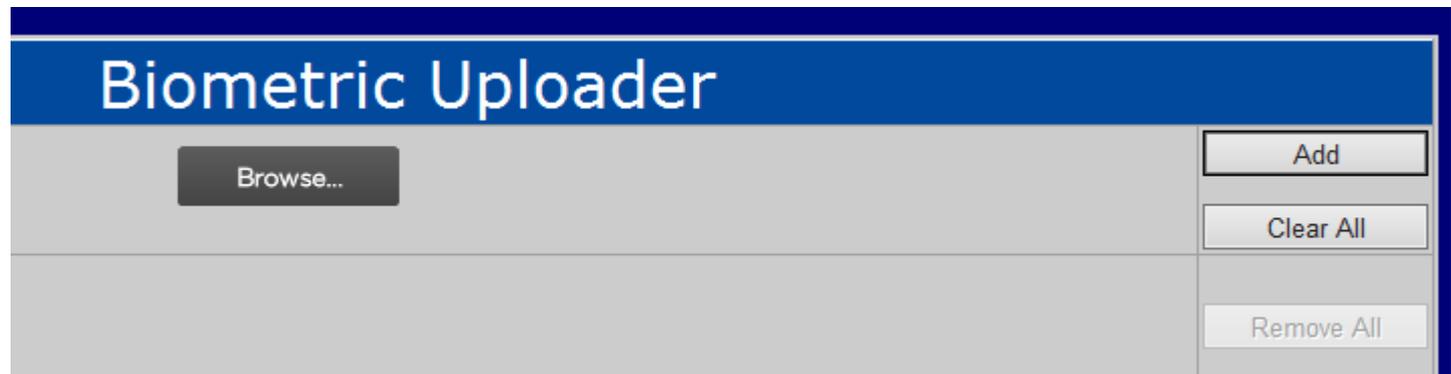
- Enter the SWFT URL and select the Smart Card certificate. Once the certificate is validated; access to SWFT is granted.



Uploading EFTs



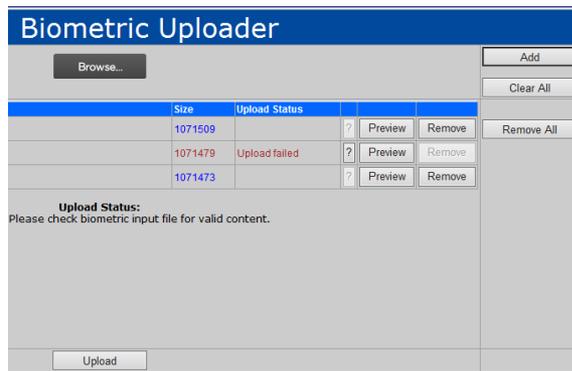
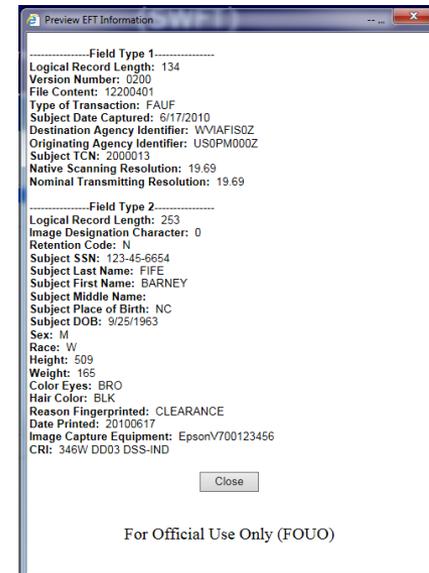
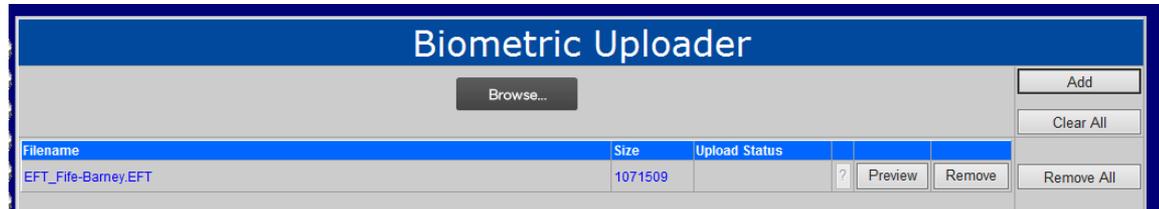
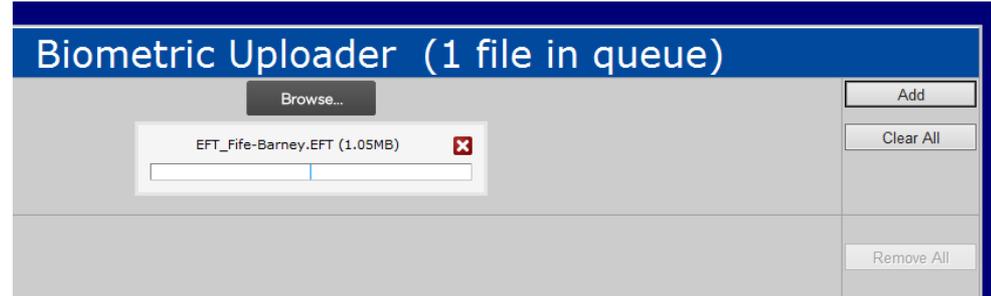
- Select “Biometric Upload”
- Browse for the desired fingerprint file
- Selecting multiple files will import multiple files at once





Uploading EFTs

- Select “Browse”
- Browse for the desired fingerprint file
- Select “Add”
- Select “Preview”
- Confirm that all information is correct
- Select “Upload” at the bottom of the page



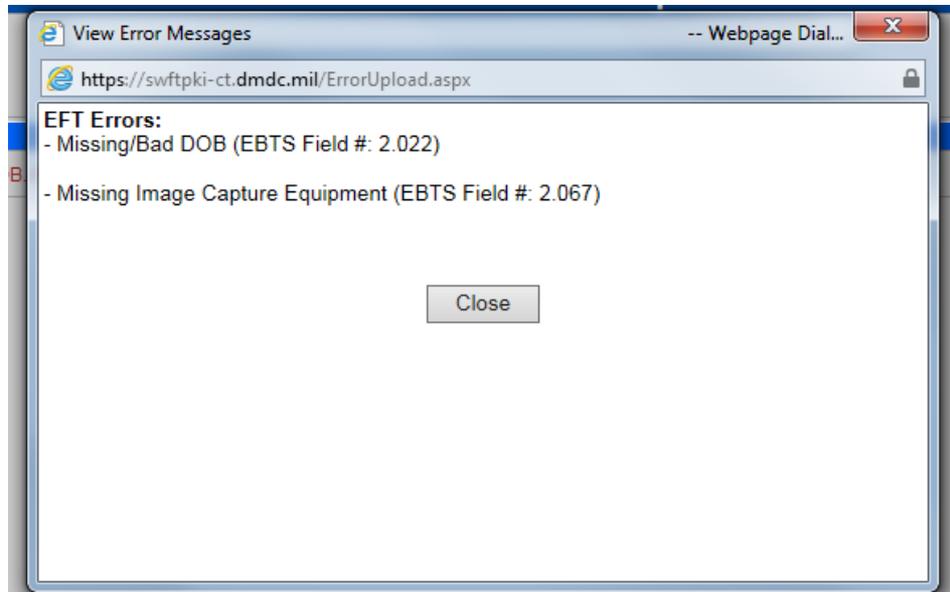


Uploading EFTs

- If you see an error indicator, select the “?” button
- Correct in the EFT the field that is identified in the Error Window
- Re-Load the corrected EFT file

Filename	Size	Upload Status			
EFT_File-Barney.EFT <i>Submitted to OPM on 6/10/2014</i>	1071509	Upload completed	?	Preview	Remove
EFT_Adams-Scott NO DOB.eft	1071479	Upload failed	?	Preview	Remove

Buttons: Add, Clear All, Remove All, Browse...





Running Reports

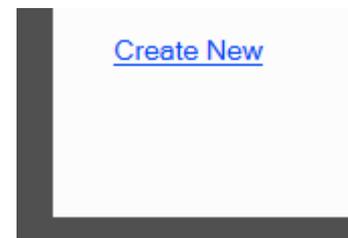
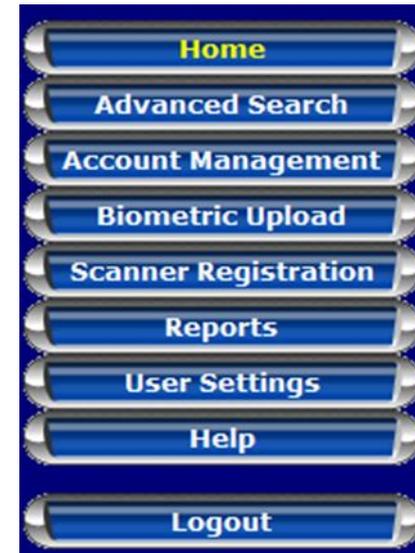
- Select the “Reports” button
- Available Reports for All:
 - Status by Date, Name, SSN
 - Discrepancy
 - Archived Biometrics Status by Date, Name, or SSN
- Available Reports for Org/Site Admins:
 - Scanner Registration Status by CAGE Code or Hardware Vendor and Serial Number
 - Uploader Multi-Site Detail
 - Uploader Multi-Site Summary





Account Management

- Select the “Account Management” button
- You will be brought to the “Users” Page
- Select “Create New” at the bottom of the page, or Select “Sites” to create a new site





Scanner Registration

- Select the “Scanner Registration” button
- Select “Add Scanner”
- Complete the form and select “Submit”
- You will receive e-mail notification when you are able to submit a test file



Scanner Registration - Add

*Indicates required field

Status: Date Submitted to OPM:

Company Name: *Cage Code/Site:

*Serial #:

*Hardware Vendor: *Software Vendor:

*Device Model: *TCN Prefix:

*Operating System: [Help: Scanner Configuration and Registration Guide](#)

Physical Location of Scanner

*Address 1:

Address 2:

*City: *State/Country: Zip Code:

Comments:



Resources

- Visit the [PSA Website](#) to find additional reference resources:
 - Newsletter
 - Frequently Asked Questions and PKI Frequently Asked Questions
 - Release Notes
 - General Announcements
 - <https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=SWFT>
- DoD ECA approved vendors can be found [here](#) and approved Non-Federal Issuers including all of the Category II listed providers [here](#).
- [DoD approved PKI Vendors](#)
- [Access, Registration, and Test Guide](#)
- [PSSAR Sample](#), [Instructions](#), and [Checklist](#)



Questions



Backup



Organization and Site Administrator Roles

- Organization Administrator is typically the FSO
- Site Administrator allows large companies to better manage multiple sites by creating an additional layer of administration

	Organization Administrator	Site Administrator
Upload EFT	Yes	Yes
Run EFT Status Reports	Yes	Yes
Create/Edit/Deactivate Site	Yes	No
Add Users	Yes	Yes
Edit Users	Yes	Yes
Deactivate Users	Yes	Yes
Set Passwords	Yes	Yes
Scanner Registration	Yes	No
Multiple Site Uploader	Yes	Yes



SWFT Naming Conventions

- As of April 15, 2014, SWFT changed the naming convention of the roles

New Roles	Previous Roles
User	User
Site Administrator	N/A
Organization Administrator	Account Manager
Executive Administrator	Executive Administrator
SWFT Administrator	SWFT Administrator
Multi-Site Uploader	Multi-Company Uploader

NOTE: The Executive Administrator and SWFT Administrator Roles are for internal DMDC use only, and will not apply to the majority of users.



SWFT Account Terminology

Organization Administrator (formerly Account Manager)

How to Request on the PSSAR Form (submitted to Contact Center):

18. SECURE WEB FINGERPRINT TRANSMISSION (SWFT)					
CAGE CODE(S): [REDACTED]					
<input type="checkbox"/> USER	<input type="checkbox"/> MULT. COMPANY UPLOADER	<input checked="" type="checkbox"/> ACCOUNT MANAGER	<input type="checkbox"/> EXECUTIVE ACCOUNT MANAGER	<input type="checkbox"/> SWFT ADMINISTRATOR	

Site Administrator

How to Request on the PSSAR Form (submitted to Organization Admin):

18. SECURE WEB FINGERPRINT TRANSMISSION (SWFT)					
CAGE CODE(S): OTHER: SITE ADMINISTRATOR					
<input type="checkbox"/> USER	<input type="checkbox"/> MULT. COMPANY UPLOADER	<input type="checkbox"/> ACCOUNT MANAGER	<input type="checkbox"/> EXECUTIVE ACCOUNT MANAGER	<input type="checkbox"/> SWFT ADMINISTRATOR	

How to Create on the Account Creation Page:

Permissions:						
<input checked="" type="checkbox"/> Upload EFT	<input type="checkbox"/> Multi Site Uploader	<input checked="" type="checkbox"/> Site Administrator	<input type="checkbox"/> Edit User and Site	<input type="checkbox"/> Set User Permissions	<input type="checkbox"/> Edit Company	<input type="checkbox"/> SWFT Admin

- Do NOT check “Site Administrator” on an Organization Administrator Account – This will reduce your account’s functionality



SWFT Naming Conventions

- The PSSAR Form is in the process of being updated. Until it is revised, use the following conventions to request accounts

User Account

PSSAR Form:

18. SECURE WEB FINGERPRINT TRANSMISSION (SWFT)									
CAGE CODE(S): <input type="text"/>									
<input checked="" type="checkbox"/>	USER	<input type="checkbox"/>	MULT. COMPANY UPLOADER	<input type="checkbox"/>	ACCOUNT MANAGER	<input type="checkbox"/>	EXECUTIVE ACCOUNT MANAGER	<input type="checkbox"/>	SWFT ADMINISTRATOR

Account Creation Page:

Permissions:													
<input checked="" type="checkbox"/>	Upload EFT	<input type="checkbox"/>	Multi Site Uploader	<input type="checkbox"/>	Site Administrator	<input type="checkbox"/>	Edit User and Site	<input type="checkbox"/>	Set User Permissions	<input type="checkbox"/>	Edit Company	<input type="checkbox"/>	SWFT Admin



SWFT Naming Conventions

Multi-Site Uploader

How to Request on the PSSAR Form:

18. SECURE WEB FINGERPRINT TRANSMISSION (SWFT)									
CAGE CODE(S): [REDACTED]									
<input checked="" type="checkbox"/>	USER	<input checked="" type="checkbox"/>	MULT. COMPANY UPLOADER	<input type="checkbox"/>	ACCOUNT MANAGER	<input type="checkbox"/>	EXECUTIVE ACCOUNT MANAGER	<input type="checkbox"/>	SWFT ADMINISTRATOR

- If your company has not been given a Multi-Site Uploader Account previously, a PSSAR will need to be submitted to the Contact Center to have the permission granted to your company.
- If your company has Multi-Site Uploader enabled, select the following:

How to Create on the Account Creation Page:

Permissions:													
<input checked="" type="checkbox"/>	Upload EFT	<input checked="" type="checkbox"/>	Multi Site Uploader	<input type="checkbox"/>	Site Administrator	<input type="checkbox"/>	Edit User and Site	<input type="checkbox"/>	Set User Permissions	<input type="checkbox"/>	Edit Company	<input type="checkbox"/>	SWFT Admin



Organization and Site Administrator Roles

- Organization/Site Administrators must receive and keep on file a fully completed and validated PSSAR
 - Must be signed by the Requestor, Nominating Official (must be different from requestor), and Validating Official
- PSSARs must be kept on file until 6 months after the account is deactivated



Secure Web Fingerprint Transmission (SWFT) Webinar

May 2014



Agenda

- SWFT Role Naming Convention Changes
- Organization and Site Administrator Roles
- Resources

Please mute your phones unless you are asking a question and do not use the hold feature



SWFT Naming Conventions

- As of April 15, 2014, SWFT changed the naming convention of the roles

New Roles	Previous Roles
User	User
Site Administrator	N/A
Organization Administrator	Account Manager
Executive Administrator	Executive Administrator
SWFT Administrator	SWFT Administrator
Multi-Site Uploader	Multi-Company Uploader

NOTE: The Executive Administrator and SWFT Administrator Roles are for internal DMDC use only, and will not apply to the majority of users.



SWFT Account Terminology

Organization Administrator (formerly Account Manager)

How to Request on the PSSAR Form (submitted to Contact Center):

18. SECURE WEB FINGERPRINT TRANSMISSION (SWFT)					
CAGE CODE(S): _____					
<input type="checkbox"/> USER	<input type="checkbox"/> MULT. COMPANY UPLOADER	<input checked="" type="checkbox"/> ACCOUNT MANAGER	<input type="checkbox"/> EXECUTIVE ACCOUNT MANAGER	<input type="checkbox"/> SWFT ADMINISTRATOR	

Site Administrator

How to Request on the PSSAR Form (submitted to Organization Admin):

18. SECURE WEB FINGERPRINT TRANSMISSION (SWFT)					
CAGE CODE(S): OTHER: SITE ADMINISTRATOR					
<input type="checkbox"/> USER	<input type="checkbox"/> MULT. COMPANY UPLOADER	<input type="checkbox"/> ACCOUNT MANAGER	<input type="checkbox"/> EXECUTIVE ACCOUNT MANAGER	<input type="checkbox"/> SWFT ADMINISTRATOR	

How to Create on the Account Creation Page:

Permissions:						
<input checked="" type="checkbox"/> Upload EFT	<input type="checkbox"/> Multi Site Uploader	<input checked="" type="checkbox"/> Site Administrator	<input type="checkbox"/> Edit User and Site	<input type="checkbox"/> Set User Permissions	<input type="checkbox"/> Edit Company	<input type="checkbox"/> SWFT Admin

- Do NOT check “Site Administrator” on an Organization Administrator Account – This will reduce your account’s functionality



SWFT Naming Conventions

Multi-Site Uploader

How to Request on the PSSAR Form:

18. SECURE WEB FINGERPRINT TRANSMISSION (SWFT)									
CAGE CODE(S): [REDACTED]									
<input checked="" type="checkbox"/>	USER	<input checked="" type="checkbox"/>	MULT. COMPANY UPLOADER	<input type="checkbox"/>	ACCOUNT MANAGER	<input type="checkbox"/>	EXECUTIVE ACCOUNT MANAGER	<input type="checkbox"/>	SWFT ADMINISTRATOR

- If your company has not been given a Multi-Site Uploader Account previously, a PSSAR will need to be submitted to the Contact Center to have the permission granted to your company.
- If your company has Multi-Site Uploader enabled, select the following:

How to Create on the Account Creation Page:

Permissions:													
<input checked="" type="checkbox"/>	Upload EFT	<input checked="" type="checkbox"/>	Multi Site Uploader	<input type="checkbox"/>	Site Administrator	<input type="checkbox"/>	Edit User and Site	<input type="checkbox"/>	Set User Permissions	<input type="checkbox"/>	Edit Company	<input type="checkbox"/>	SWFT Admin



Organization and Site Administrator Roles

- Organization Administrator is typically the FSO
- Site Administrator allows large companies to better manage multiple sites by creating an additional layer of administration

	Organization Administrator	Site Administrator
Upload EFT	Yes	Yes
Run EFT Status Reports	Yes	Yes
Create/Edit/Deactivate Site	Yes	No
Add Users	Yes	Yes
Edit Users	Yes	Yes
Deactivate Users	Yes	Yes
Set Passwords	Yes	Yes
Scanner Registration	Yes	No
Multiple Site Uploader	Yes	Yes



Organization and Site Administrator Roles

- Organization/Site Administrators must receive and keep on file a fully completed and validated PSSAR
 - Must be signed by the Requestor, Nominating Official (must be different from requestor), and Validating Official
- PSSARs must be kept on file until 6 months after the account is deactivated



Resources

- Visit the [PSA Website](#) to Find Additional Resources:
 - Newsletter
 - PKI Frequently Asked Questions
 - Release Notes
 - General Announcements
 - <https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=SWFT>
- DoD ECA approved vendors can be found [here](#) and approved Non-Federal Issuers including all of the Category II listed providers [here](#).
- [DoD approved PKI Vendors](#)
- [Access, Registration, and Test Guide](#)
- [PSSAR Sample](#), [Instructions](#), and [Checklist](#)



Questions



Backup



Smart Card Re-Registration

- PIV, PIV-I, and ECA users will need their SWFT Login ID and a Password to Re-Register their Smart Card
 - If you forgot your username, contact your Site or Organization Administrator
 - Login to SWFT to reset your password no more than 72 hours BEFORE your certificate expires
 - When you receive your new certificate (within 72 hours of resetting your password), return to SWFT and register your Smart Card
- CAC users will not need to Re-Register their Smart Cards



Smart Card Re-Registration



Secure Web Fingerprint Transmission (SWFT)

Eramo, Andrew - DMDC1 - Last login time: 03/11/2014 20:55 GMT



- Home
- Biometric Upload
- Reports
- User Settings**
- Help
- Logout

User Settings

Email Example: xxx@company.com (must contain '@' and '.')

Phone Example: 703.325.9999, 703-325-9999, (703) 325-9999 or 7033259999

RE-REGISTER PIV, PIV-I OR ECA SMART CARD

To re-register a PIV, PIV-I or ECA Smart Card you will need your SWFT Login ID and Password for the Smart Card Registration page.

- Create a new password using the fields below. The new password is only valid for 72 hours. After 72 hours you must create another password.
IMPORTANT: Reset your SWFT password before your PIV or ECA Smart Card expires. If you forgot your Login ID, contact your Account Manager.
- Enter the SWFT URL and select the new Smart Card certificate.
- You will be directed to the Smart Card Registration page, where you will enter your Login ID and Password.
- Once SWFT validates your information, access to SWFT is granted.

New Password

Verify New Password

Passwords in the SWFT system are complex and will expire in 72 hours. Passwords must be at least 15 characters, containing at least two upper case characters, two lower case characters, two digits, and two special characters.

RE-REGISTER CAC SMART CARD

To re-register a CAC Smart Card

- Enter the SWFT URL and select the Smart Card certificate. Once the certificate is validated; access to SWFT is granted.



SWFT Naming Conventions

- The PSSAR Form is in the process of being updated. Until it is revised, use the following conventions to request accounts

User Account

PSSAR Form:

18. SECURE WEB FINGERPRINT TRANSMISSION (SWFT)				
CAGE CODE(S): <input type="text"/>				
<input checked="" type="checkbox"/> USER	<input type="checkbox"/> MULT. COMPANY UPLOADER	<input type="checkbox"/> ACCOUNT MANAGER	<input type="checkbox"/> EXECUTIVE ACCOUNT MANAGER	<input type="checkbox"/> SWFT ADMINISTRATOR

Account Creation Page:

Permissions:						
<input checked="" type="checkbox"/> Upload EFT	<input type="checkbox"/> Multi Site Uploader	<input type="checkbox"/> Site Administrator	<input type="checkbox"/> Edit User and Site	<input type="checkbox"/> Set User Permissions	<input type="checkbox"/> Edit Company	<input type="checkbox"/> SWFT Admin



Secure Web Fingerprint Transmission (SWFT) Webinar

April 2014



Agenda

- SWFT Naming Convention Changes
- Organization and Site Administrator Roles
- Resources

Please mute your phones unless you are asking a question



SWFT Naming Conventions

- As of April 15, 2014, SWFT changed the naming convention of the roles

New Roles	Previous Roles
User	User
Site Administrator	N/A
Organization Administrator	Account Manager
Executive Administrator	Executive Administrator
SWFT Administrator	SWFT Administrator
Multi-Site Uploader	Multi-Company Uploader

NOTE: The Executive Administrator and SWFT Administrator Roles are for internal DMDC use only, and will not apply to the majority of users.



SWFT Naming Conventions

- The PSSAR Form is in the process of being updated. Until it is revised, use the following conventions to request accounts

User Account

PSSAR Form:

18. SECURE WEB FINGERPRINT TRANSMISSION (SWFT)				
CAGE CODE(S): <input type="text"/>				
<input checked="" type="checkbox"/> USER	<input type="checkbox"/> MULT. COMPANY UPLOADER	<input type="checkbox"/> ACCOUNT MANAGER	<input type="checkbox"/> EXECUTIVE ACCOUNT MANAGER	<input type="checkbox"/> SWFT ADMINISTRATOR

Account Creation Page:

Permissions:						
<input checked="" type="checkbox"/> Upload EFT	<input type="checkbox"/> Multi Site Uploader	<input type="checkbox"/> Site Administrator	<input type="checkbox"/> Edit User and Site	<input type="checkbox"/> Set User Permissions	<input type="checkbox"/> Edit Company	<input type="checkbox"/> SWFT Admin



SWFT Account Terminology

Site Administrator

PSSAR Form:

18. SECURE WEB FINGERPRINT TRANSMISSION (SWFT)
CAGE CODE(S): OTHER: SITE ADMINISTRATOR
 USER MULT. COMPANY UPLOADER ACCOUNT MANAGER EXECUTIVE ACCOUNT MANAGER SWFT ADMINISTRATOR

Account Creation Page:

Permissions:
 Upload EFT Multi Site Uploader Site Administrator Edit User and Site Set User Permissions Edit Company SWFT Admin

Organization Administrator

PSSAR Form:

18. SECURE WEB FINGERPRINT TRANSMISSION (SWFT)
CAGE CODE(S): [REDACTED]
 USER MULT. COMPANY UPLOADER ACCOUNT MANAGER EXECUTIVE ACCOUNT MANAGER SWFT ADMINISTRATOR



SWFT Naming Conventions

Multi-Site Uploader

PSSAR Form:

18. SECURE WEB FINGERPRINT TRANSMISSION (SWFT)				
CAGE CODE(S): [REDACTED]				
<input checked="" type="checkbox"/> USER	<input checked="" type="checkbox"/> MULT. COMPANY UPLOADER	<input type="checkbox"/> ACCOUNT MANAGER	<input type="checkbox"/> EXECUTIVE ACCOUNT MANAGER	<input type="checkbox"/> SWFT ADMINISTRATOR

Account Creation Page:

Permissions:						
<input checked="" type="checkbox"/> Upload EFT	<input checked="" type="checkbox"/> Multi Site Uploader	<input type="checkbox"/> Site Administrator	<input type="checkbox"/> Edit User and Site	<input type="checkbox"/> Set User Permissions	<input type="checkbox"/> Edit Company	<input type="checkbox"/> SWFT Admin

- An announcement will be posted on the PSA website when the PSSAR is updated.



Organization and Site Administrator Roles

- Organization Administrator is typically the FSO
- Site Administrator allows users in companies with multiple locations to manage CAGE codes that are assigned to them

	Organization Administrator	Site Administrator
Upload EFT	Yes	Yes
Run EFT Status Reports	Yes	Yes
Create/Edit/Deactivate Site	Yes	No
Add Users	Yes	Yes
Edit Users	Yes	Yes
Deactivate Users	Yes	Yes
Set Passwords	Yes	Yes
Scanner Registration	Yes	No
Multiple Site Uploader	Yes	Yes



Organization and Site Administrator Roles

- Organization/Site Administrators must receive and keep on file a fully completed PSSAR
 - Must be signed by the Requestor, Nominating Official (must be different from requestor), and Validating Official
- PSSARs must be kept on file until 6 months after the account is deactivated



Smart Card Re-Registration

- PIV, PIV-I, and ECA users will need their SWFT Login ID and a Password to Re-Register their Smart Card
 - If you forgot your username, contact your Site or Organization Administrator
 - Login to SWFT to reset your password no more than 72 hours BEFORE your certificate expires
 - When you receive your new certificate (within 72 hours of resetting your password), return to SWFT and register your Smart Card
- CAC users will not need to Re-Register their Smart Cards



Smart Card Re-Registration



Secure Web Fingerprint Transmission (SWFT)

Eramo, Andrew - DMDC1 - Last login time: 03/11/2014 20:55 GMT



- Home
- Biometric Upload
- Reports
- User Settings**
- Help
- Logout

User Settings

Email Example: xxx@company.com (must contain '@' and '.')
Phone Example: 703.325.9999, 703-325-9999, (703) 325-9999 or 7033259999

RE-REGISTER PIV, PIV-I OR ECA SMART CARD

To re-register a PIV, PIV-I or ECA Smart Card you will need your SWFT Login ID and Password for the Smart Card Registration page.

- Create a new password using the fields below. The new password is only valid for 72 hours. After 72 hours you must create another password.
IMPORTANT: Reset your SWFT password before your PIV or ECA Smart Card expires. If you forgot your Login ID, contact your Account Manager.
- Enter the SWFT URL and select the new Smart Card certificate.
- You will be directed to the Smart Card Registration page, where you will enter your Login ID and Password.
- Once SWFT validates your information, access to SWFT is granted.

New Password Passwords in the SWFT system are complex and will expire in 72 hours. Passwords must be at least 15 characters, containing at least two upper case characters, two lower case characters, two digits, and two special characters.
Verify New Password

Change

RE-REGISTER CAC SMART CARD

To re-register a CAC Smart Card

- Enter the SWFT URL and select the Smart Card certificate. Once the certificate is validated; access to SWFT is granted.



Resources

- Visit the [PSA Website](#) to Find Additional Resources:
 - Newsletter
 - PKI Frequently Asked Questions
 - Release Notes
 - General Announcements
 - <https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=SWFT>
- DoD ECA approved vendors can be found [here](#) and approved Non-Federal Issuers including all of the Category II listed providers [here](#).
- [DoD approved PKI Vendors](#)
- [Access, Registration, and Test Guide](#)
- [PSSAR Sample](#), [Instructions](#), and [Checklist](#)



Questions



Secure Web Fingerprint Transmission (SWFT) Webinar

March 2014



Agenda

- PK-Enabling Update
- Smart Card Re-registration
- PK-Enabling Q&A
- Resources
- Discussion of other topics, as time allows
 - Matching .EFT file with e-QIP file
 - Third Party Provider Options

Please submit questions using the chat feature



PK-Enabling Update

- Login with Log ID and Password will be discontinued with Release 5.2
 - Scheduled for **March 14, 2014**
 - All users will need a Medium Hardware Assurance Certificate on a Smart Card or a Medium Token Assurance Certificate on a USB Token after **March 14, 2014**
- **Less than 1 week left** for Username and Password Login
 - If you can access JPAS, you are able to access SWFT with the same PK credentials
- [PKI FAQs](#) and [Test Procedures](#) are available on SWFT [Homepage](#)



What the Changes Mean

- JPAS Users:
 - Will be able to use the same credential that is used for JPAS access
- Non-JPAS Users:
 - Will need to procure a CAC, PIV, ECA, or other approved Medium Token Assurance Certificate on a USB Token or a Medium Hardware Assurance Certificate on a Smart Card that is FIPS 140-2 compliant (See [PKI FAQs](#) for more info)
 - Users may need to procure additional software, middleware, and/or hardware in order to use their Smart Cards/USB Tokens (See [PKI FAQs](#) for more info)



Smart Card Re-Registration

- PIV, PIV-I, and ECA users will need their SWFT Login ID and a Password to Re-Register their Smart Card
 - If you forgot your username, contact your Account Manager
 - Login to SWFT to reset your password no more than 72 hours BEFORE your certificate expires
 - When you receive your new certificate (within 72 hours of resetting your password), return to SWFT and register your Smart Card
- CAC users will not need to Re-Register their Smart Cards



Smart Card Re-Registration



Secure Web Fingerprint Transmission (SWFT)

Eramo, Andrew - DMDC1 - Last login time: 03/11/2014 20:55 GMT



- Home
- Biometric Upload
- Reports
- User Settings**
- Help
- Logout

User Settings

Email Example: xxx@company.com (must contain '@' and '.')

Phone Example: 703.325.9999, 703-325-9999, (703) 325-9999 or 7033259999

RE-REGISTER PIV, PIV-I OR ECA SMART CARD

To re-register a PIV, PIV-I or ECA Smart Card you will need your SWFT Login ID and Password for the Smart Card Registration page.

- Create a new password using the fields below. The new password is only valid for 72 hours. After 72 hours you must create another password.
- **IMPORTANT: Reset your SWFT password before your PIV or ECA Smart Card expires. If you forgot your Login ID, contact your Account Manager.**
- Enter the SWFT URL and select the new Smart Card certificate.
- You will be directed to the Smart Card Registration page, where you will enter your Login ID and Password.
- Once SWFT validates your information, access to SWFT is granted.

New Password
Verify New Password

Passwords in the SWFT system are complex and will expire in 72 hours. Passwords must be at least 15 characters, containing at least two upper case characters, two lower case characters, two digits, and two special characters.

Change

RE-REGISTER CAC SMART CARD

To re-register a CAC Smart Card

- Enter the SWFT URL and select the Smart Card certificate. Once the certificate is validated; access to SWFT is granted.



PKI Resources

- Visit the [PSA Website](#) to Find Additional Resources:
 - Newsletter
 - PKI Frequently Asked Questions
 - Release Notes
 - General Announcements
 - <https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=SWFT>
- DoD ECA approved vendors can be found [here](#) and approved Non-Federal Issuers including all of the Category II listed providers [here](#).
- [DoD approved PKI Vendors](#)
- [Access, Registration, and Test Guide](#)



Questions



Backup



Matching EFT Files with e-QIP

- Recommended to submit EFTs immediately after submitting e-QIP file to PSMO-I
 - Users have 2 weeks to submit EFTs after the e-QIP is submitted
- EFT is matched to the e-QIP using SSN
- SWFT provides users with a Discrepancy Report
 - Report highlights differences between the EFT file and e-QIP
 - Allows the user to correct discrepancies before they reach OPM, thus saving time
 - The Discrepancy Report is unavailable to Multi-Company Uploaders
- Information on SWFT Reports can be found in the User's Guide



Submission of eFPs on Behalf of Other Companies

- Option 1: Multi-Company Uploader
 - Service Provider Acts with Limited Privileges on Behalf of Another Company
 - Serviced Company must be registered in SWFT and have their own SWFT account
 - PSSAR required to become a Multi-Company Uploader
 - Serviced company obtains account to generate reports
 - Service Provider is able to generate reports that identify the date and number of EFTs uploaded for the purpose of billing and accountability



Submission of eFPs on Behalf of Other Companies

- Option 2: Multi-CAGE SWFT Account
- Service Provider Acts with Full Privileges on Behalf of Another Company
 - Service Provider submits PSSAR form approved by Serviced Company
 - Service Provider is able to generate detailed reports, including PII data, for all CAGE codes that are assigned to the Service Provider's account
 - Serviced Company gives up all SWFT privileges for its CAGE code to the Service Provider



Secure Web Fingerprint Transmission (SWFT) Webinar

February 2014



Agenda

- PK-Enabling Update
- Matching .EFT file with e-QIP file
- Third Party Provider Options
- Resources
- Questions

Please submit questions using the chat feature



PK-Enabling Update

- Login with Log ID and Password will be discontinued with Release 5.2
 - Scheduled for **March 14, 2014**
 - All users will need a Medium Hardware Assurance Certificate on a Smart Card or a Medium Token Assurance Certificate on a USB Token after **March 14, 2014**
- Currently, Username and Password or Smart Card/USB Token are acceptable for SWFT Login – **less than 1 month left**
 - If you can access JPAS, you are able to access SWFT with the same PK credentials
- [PKI FAQs](#) and [Test Procedures](#) are available on SWFT [Homepage](#)



PKI Resources

- Visit the [PSA Website](#) to Find Additional Resources:
 - Newsletter
 - PKI Frequently Asked Questions
 - Release Notes
 - General Announcements
 - <https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=SWFT>
- DoD ECA approved vendors can be found [here](#) and approved Non-Federal Issuers including all of the Category II listed providers [here](#).
- [DoD approved PKI Vendors](#)
- [Access, Registration, and Test Guide](#)



Matching EFT Files with e-QIP

- Recommended to submit EFTs immediately after submitting e-QIP file to PSMO-I
 - Users have 2 weeks to submit EFTs after the e-QIP is submitted
- EFT is matched to the e-QIP using SSN
- SWFT provides users with a Discrepancy Report
 - Report highlights differences between the EFT file and e-QIP
 - Allows the user to correct discrepancies before they reach OPM, thus saving time
 - The Discrepancy Report is unavailable to Multi-Company Uploaders
- Information on SWFT Reports can be found in the User's Guide



Submission of eFPs on Behalf of Other Companies

- Option 1: Multi-Company Uploader
 - Service Provider Acts with Limited Privileges on Behalf of Another Company
 - Serviced Company must be registered in SWFT and have their own SWFT account
 - PSSAR required to become a Multi-Company Uploader
 - Serviced company obtains account to generate reports
 - Service Provider is able to generate reports that identify the date and number of EFTs uploaded for the purpose of billing and accountability



Submission of eFPs on Behalf of Other Companies

- Option 2: Multi-CAGE SWFT Account
- Service Provider Acts with Full Privileges on Behalf of Another Company
 - Service Provider submits PSSAR form approved by Serviced Company
 - Service Provider is able to generate detailed reports, including PII data, for all CAGE codes that are assigned to the Service Provider's account
 - Serviced Company gives up all SWFT privileges for its CAGE code to the Service Provider



Questions



Backup



What the Changes Mean

- JPAS Users:
 - Will be able to use the same credential that is used for JPAS access
- Non-JPAS Users:
 - Will need to procure a CAC, PIV, ECA, or other approved Medium Token Assurance Certificate on a USB Token or a Medium Hardware Assurance Certificate on a Smart Card that is FIPS 140-2 compliant (See [PKI FAQs](#) for more info)
 - Users may need to procure additional software, middleware, and/or hardware in order to use their Smart Cards/USB Tokens (See [PKI FAQs](#) for more info)



Secure Web Fingerprint Transmission (SWFT) Webinar

January 2014



Agenda

- PK-Enabling Update
- Multi-Company Uploader Options
- Submission of eFPs on Behalf of Other Companies
- Resources
- Questions

Please submit questions using the chat feature



PK-Enabling Update

- Login with Log ID and Password will be discontinued with Release 5.2
 - Scheduled for March 2014
 - All users will need a Medium Hardware Assurance Certificate on a Smart Card or a Medium Token Assurance Certificate on a USB Token after March 2014
- Currently, Username and Password or Smart Card/USB Token are acceptable for SWFT Login
 - If you can access JPAS, you are able to access SWFT with the same PK credentials
- [PKI FAQs](#) and [Test Procedures](#) are available on SWFT [Homepage](#)



Submission of eFPs on Behalf of Other Companies

- Option 1: Multi-Company Uploader
 - Service Provider Acts with Limited Privileges on Behalf of Another Company
 - Serviced Company must be registered in SWFT and have their own SWFT account
 - PSSAR required to become a Multi-Company Uploader
 - Serviced company obtains account to generate reports
 - Service Provider is able to generate reports that identify the date and number of EFTs uploaded for the purpose of billing and accountability



Submission of eFPs on Behalf of Other Companies

- Option 2: Multi-CAGE SWFT Account
- Service Provider Acts with Full Privileges on Behalf of Another Company
 - Service Provider submits PSSAR form approved by Serviced Company
 - Service Provider is able to generate detailed reports, including PII data, for all CAGE codes that are assigned to the Service Provider's account



Resources

- Visit the [PSA Website](#) to Find Additional Resources:
 - Newsletter
 - PKI Frequently Asked Questions
 - Release Notes
 - General Announcements
 - <https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=SWFT>
- DoD ECA approved vendors can be found [here](#) and approved Non-Federal Issuers including all of the Category II listed providers [here](#).
- [DoD approved PKI Vendors](#)
- [Access, Registration, and Test Guide](#)



Questions



Backup



What the Changes Mean

- JPAS Users:
 - Will be able to use the same credential that is used for JPAS access
- Non-JPAS Users:
 - Will need to procure a CAC, PIV, ECA, or other approved Medium Token Assurance Certificate on a USB Token or a Medium Hardware Assurance Certificate on a Smart Card that is FIPS 140-2 compliant (See [PKI FAQs](#) for more info)
 - Users may need to procure additional software, middleware, and/or hardware in order to use their Smart Cards/USB Tokens (See [PKI FAQs](#) for more info)



Secure Web Fingerprint Transmission (SWFT) Public Key Enabled (PKE) Logon Webinar

December 2013



Agenda

- What Is Changing
- Implementation Timeline
- What the Changes Mean
- Resources
- Demo

Please submit questions using the chat feature



What Is Changing

- Split Login - Username and Password or Smart Card/USB Token
- Username and Password Login to be phased out
 - Will need a Medium Token Assurance Certificate on a USB Token or a Medium Hardware Assurance Certificate on a Smart Card

SWFT 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.

The U.S. Department of Defense is committed to making its electronic and information technologies accessible to individuals with disabilities in accordance with [Section 508 of the Rehabilitation Act \(29 U.S.C. § 794d\), as amended in 1999](#). Send feedback or concerns related to the accessibility of this website to: DoDSection508@osd.mil. For more information about Section 508, please visit the [DoD Section 508 website](#). Last Updated: 09/06/2013

I acknowledge and accept the above access statement.

<p>Login ID <input type="text"/></p> <p>Password <input type="password"/></p> <p><input type="button" value="Login"/></p>	OR	 <p>CURRENTLY DISABLED Will be available Dec 16, 2013</p> <p>Insert your Smart Card into the card reader before attempting to login.</p> <p><input type="button" value="Login"/></p>
---	-----------	---

The process for obtaining a SWFT Account and resetting passwords will not change



Implementation Timeline

- Phase I: Transition to Smart Card Login
 - 16 Dec 13: Login available through Username/Password or Smart Card
 - Once a Smart Card is registered for a User Account, the Username/Password login method is disabled
 - Phase I will last approximately 3 months
- Phase II: Switch to Smart Card-Only Login
 - March/April 2014: Username/Password login option will be disabled
 - All users will need to use the PK-enabled login by this time



What the Changes Mean

- JPAS Users:
 - Will be able to use the same credential that is used for JPAS access
- Non-JPAS Users:
 - Will need to procure a CAC, PIV, ECA, or other approved Medium Token Assurance Certificate on a USB Token or a Medium Hardware Assurance Certificate on a Smart Card that is FIPS 140-2 compliant (See [PKI FAQs](#) for more info)
 - Users may need to procure additional software, middleware, and/or hardware in order to use their Smart Cards/USB Tokens (See [PKI FAQs](#) for more info)



Resources

- Visit the [PSA Website](#) to Find Additional Resources:
 - Newsletter
 - PKI Frequently Asked Questions
 - Release Notes
 - General Announcements
 - <https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=SWFT>
- DoD ECA approved vendors can be found [here](#) and approved Non-Federal Issuers include all of the Category II listed providers [here](#).
- [DoD approved PKI Vendors](#)



Demo



Questions