



# Department of Defense Secure Access File Exchange (DoD SAFE)

## User Guide

For Public Release

Version 0.2d  
9/4/2019

Prepared by  
DCS Engineering

## Revision History

Revision	Author	Date	Section	Comment
0.1	DCS PMO Engineering	July 23, 2019	All	Initial document
0.2 and 0.2b	DCS PMO Engineering	July 30, 2019	All	Update based on feedback received from DCS Engineering & Service Manager
0.2.c	DCS PMO Engineering	July 31, 2019	Pages 10 and 13	Page 10 (changed the wording in the header); Page 13 (changed the wording in item 2)
0.2.d	DCS PMO Engineering	August 27 2019 and September 4 2019	All	Corrected the GSD email on page 4 Redacted name on page 5 Updated banners

## Table of Contents

Overview .....	4
Points of Contact (POC).....	4
Welcome to DoD SAFE .....	5
Creating a Drop-off (CAC Authenticated User) .....	6
Creating a Drop-off (Non-Authenticated User or Guest).....	10
Request a Drop-off (CAC Authenticated User) .....	12
Pick-up (Authenticated User and Non-Authenticated User or Guest) .....	13
Outbox (CAC Authenticated User) .....	14
Search for a Drop-off (CAC Authenticated User) .....	15
Recipient URL List (CAC Authenticated User) .....	17
Delete a Drop-off (CAC Authenticated User) .....	19
Resend a Drop-off (CAC Authenticated User).....	21
Encryption .....	23
APPENDIX: Acronyms .....	27

## Overview

DoD Secure Access File Exchange Service, DoD SAFE (<https://safe.apps.mil>) is an enterprise technical solution that provides the capability of secure data transfer of large files (8 GB maximum). There are no user accounts for SAFE; authentication is performed via common access card (CAC) and notification is done via email. SAFE is available for use by unauthenticated users also; however, a DoD CAC holder must initiate the exchange process. Users are identified as DoD users that authenticate to DoD SAFE using a CAC and non-DoD or non-CAC holders are referenced as *Guests*.

DoD SAFE services are on the Non-classified Internet Protocol Router Network (NIPRNet) and are accessible via the Internet. Users will need to follow the DoD SAFE Policy and Procedures such as reporting spillages and encrypting PII and PHI data. Users shall not neglect, disregard, nor knowingly circumvent any of the roles and responsibility standards associated with the DoD SAFE Service. DoD SAFE will retain data up to 7 days.

This user guide provides guidance on how to use DoD SAFE.

## Points of Contact (POC)

This table summarizes the list of contacts responsible for the implementation of DoD SAFE.

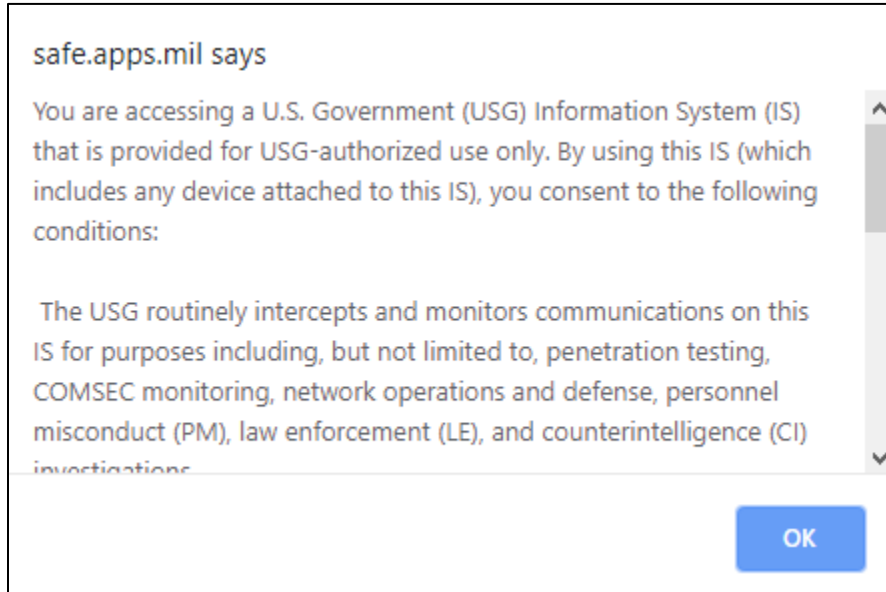
POC	Office	Email	Role
Tier I Support (8x5)	844-347-2457 DSN: 312-850-0032	<a href="mailto:disa.gsd.apps@mail.mil">disa.gsd.apps@mail.mil</a>	DISA Global Service Desk (Help Desk)

**Table 1: Point of Contacts**

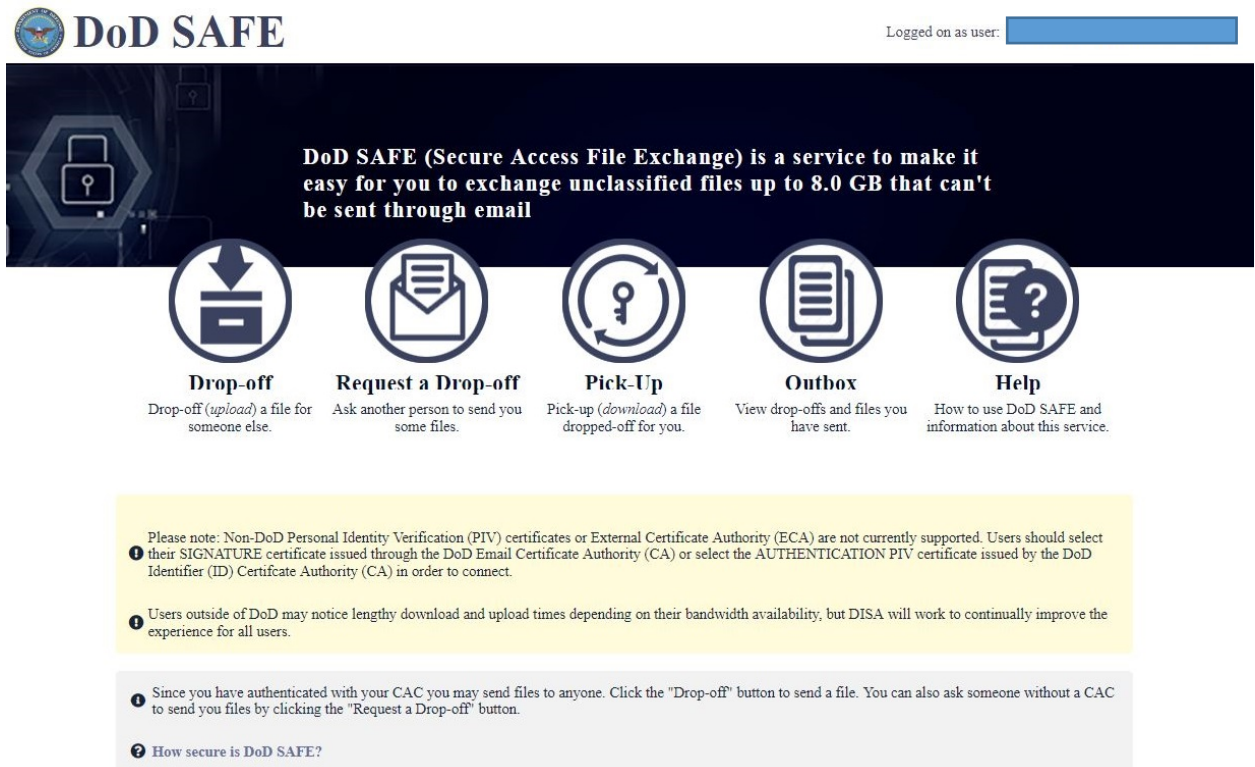
# Welcome to DoD SAFE

To access DoD SAFE, use the browser of your choice and navigate to <https://safe.apps.mil>

## 1. Accept User agreement



## 2. DoD SAFE homepage is loaded (Authenticated View)



**DoD SAFE** Logged on as user: [redacted]

**DoD SAFE (Secure Access File Exchange) is a service to make it easy for you to exchange unclassified files up to 8.0 GB that can't be sent through email**

- Drop-off**  
Drop-off (*upload*) a file for someone else.
- Request a Drop-off**  
Ask another person to send you some files.
- Pick-Up**  
Pick-up (*download*) a file dropped-off for you.
- Outbox**  
View drop-offs and files you have sent.
- Help**  
How to use DoD SAFE and information about this service.

**Please note:** Non-DoD Personal Identity Verification (PIV) certificates or External Certificate Authority (ECA) are not currently supported. Users should select their SIGNATURE certificate issued through the DoD Email Certificate Authority (CA) or select the AUTHENTICATION PIV certificate issued by the DoD Identifier (ID) Certificate Authority (CA) in order to connect.

Users outside of DoD may notice lengthy download and upload times depending on their bandwidth availability, but DISA will work to continually improve the experience for all users.

Since you have authenticated with your CAC you may send files to anyone. Click the "Drop-off" button to send a file. You can also ask someone without a CAC to send you files by clicking the "Request a Drop-off" button.

How secure is DoD SAFE?

3. DoD SAFE homepage is loaded (Non-authenticated, Guest View)

**DoD SAFE** Logged on as user: Guest

**DoD SAFE (Secure Access File Exchange) is a service to make it easy for you to exchange unclassified files up to 8.0 GB that can't be sent through email**

**Drop-off**  
Drop-off (*upload*) a file for a DoD user (**must have request code from recipient**).

**Pick-Up**  
Pick-up (*download*) a file dropped-off for you.

**Help**  
How to use DoD SAFE and information about this service.

Please note: Non-DoD Personal Identity Verification (PIV) certificates or External Certificate Authority (ECA) are not currently supported. Users should select their SIGNATURE certificate issued through the DoD Email Certificate Authority (CA) or select the AUTHENTICATION PIV certificate issued by the DoD Identifier (ID) Certificate Authority (CA) in order to connect.

Users outside of DoD may notice lengthy download and upload times depending on their bandwidth availability, but DISA will work to continually improve the experience for all users.

You have not authenticated with a CAC, so you can only retrieve files sent to you or upload files for someone else only if you have received a request from them.

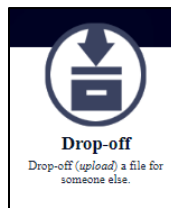
How secure is DoD SAFE?

Files are automatically deleted from DoD SAFE 7 days after you upload them.

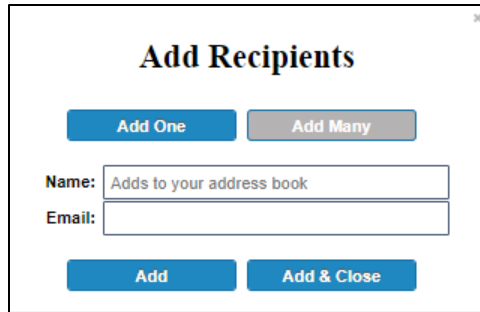
## Creating a Drop-off (CAC Authenticated User)

A drop-off allows you to upload a file and send to a CAC authenticated or non-CAC authenticated user.


1. Click Drop-off



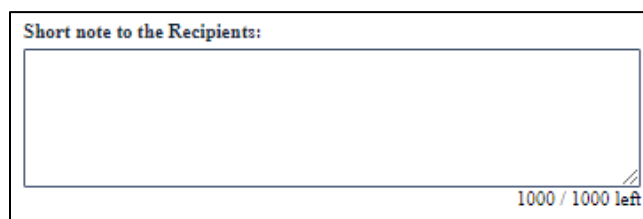
1. Enter some identifying information about the recipient(s) (name and email address).
  - a. For one recipient; add recipient's name and email address
  - b. Click "Add & Close"



- c. For more than one recipient, click “Add Many”
- d. Enter one recipient per line using this format: *Recipient's Name email@example.com*
- e. Click “Add & Close”



- 2. Add a short note to the Recipient(s)



- 3. As the sender you have two options; select the option you need:
  - a. Encrypt file
  - b. Send me an email when each recipient picks up the files

<input type="checkbox"/> <b>Encrypt every file (REQUIRED FOR PII/PHI)</b>
<input type="checkbox"/> <b>Send me an email when each recipient picks up the files</b>

4. Click to Add Files or Drag and Drop them

[Click to Add Files or Drag Them Here](#)

5. Add a description to each file if necessary
6. Click “Drop-Off Files” to send the files to the recipient

Filename	Size	Description
1: Capture.JPG	18.6 KB	<input type="text"/> ✖
18.6 KB / 8192 MB		
<a href="#">Drop-off Files</a>		

7. Confirm the files do not contain classified information and click “Ok”.

safe.st.apps.mil says

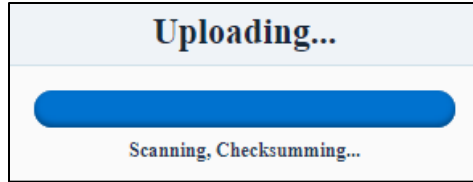
Confirm that the files in this upload do NOT contain classified information.

By clicking "OK", you are confirming that the files do not contain classified information and are aware that your organization will be held accountable for non-compliant data sent through the system.

[OK](#) [Cancel](#)

8. The file is uploaded and an automated email is sent to the recipient notifying them of the “drop-off”
  - a. NOTE: The image below depicts an upload for a hashed and unencrypted file drop-off. Depending on the speed of the upload, each user may or may not view the image depicted below.






9. As the sender, you are notified the drop-off is complete
  - a. The notification displays the filename, file size, the secure hash algorithm – 256 bit (SHA-256) and description. The sender enters the description prior to uploading the file.

### Drop-Off Completed

Your files have been sent successfully.

Filename	Size	SHA-256 Checksum	Description
 Capture.JPG	18.6 KB	288F85A8B8035DE22E868028663041448 BEB9EC8C359AC73E201881660974855D	Sample Screenshot

1 file

**From:**  
 on 2019-07-30 19:41

**To:**

**Comments:**

[Recipient URL List Show](#)

**Pickup History**  
 None of the files has been picked-up yet.

10. To view all packages sent, click "Outbox". NOTE: *The time the package was created is displayed in Zulu Time*

### Outbox

Click on a drop-off to view the information and files for that drop-off.

Show  entries Search:

Claim ID	Sender	Recipient	Size	Created
fxv2ag4mxPCeWJCa	< <input type="text" value="civ@mail.mil"/> >	< <input type="text" value="civ@mail.mil"/> >	18.6 KB	2019-07-23 18:26:53

Showing 1 to 1 of 1 entries

## Creating a Drop-off (Non-Authenticated User or Guest)

This type of drop-off allows a non-authenticated user (Guest) to upload a file that has been requested by an authenticated user. An authenticated user must first execute the "Request a Drop-Off" procedure to obtain a "Request Code" for external delivery to the non-authenticated user.

1. Click Drop-off



2. Enter Request Code (12 digits). This request code is sent to you by the requestor

Your Request Code

Request Code:

[Next](#)

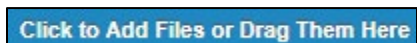
3. Click "Next"

4. Add a short note to the Recipient

Short note to the Recipients:

1000 / 1000 left

5. Click to Add Files or Drag and Drop them



6. Add a description to each file if necessary
7. Click "Drop-Off Files" to send the files to the recipient

Filename	Size	Description
1: Capture.JPG	18.6 KB	<input type="text"/> ✖
18.6 KB / 8192 MB		
<input type="button" value="Drop-off Files"/>		

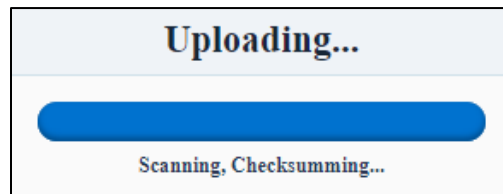
8. Confirm the files do not contain classified information and click "OK".

safe.st.apps.mil says

Confirm that the files in this upload do NOT contain classified information.

By clicking "OK", you are confirming that the files do not contain classified information and are aware that your organization will be held accountable for non-compliant data sent through the system.


9. The file is uploaded and an email will be sent to the recipient notifying them of the "drop-off"
  - a. NOTE: The image below depicts an upload for a hashed and unencrypted file drop-off. Depending on the speed of the upload, each user may or may not view the image depicted below.



10. You are notified the drop-off is complete

## Drop-Off Completed

Your files have been sent successfully.

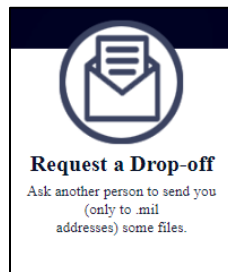
Filename	Size	SHA-256 Checksum	Description
 Capture.JPG	18.6 KB	288F05A8B035DE22E868D2B663041448 BEB9ECBC359AC73E20188166D974B55D	

1 file

## Request a Drop-off (CAC Authenticated User)

CAC authenticated users can request a drop-off from another CAC authenticated user or a non-CAC authenticated user (guest).

1. Click "Request a Drop-off"



2. Complete all entries associated with the drop-off request

### Request a Drop-off

This web page will allow you to send a request to someone requesting that they send (upload) one or more files for you. The recipient will receive an automated email containing the information you enter below and instructions for uploading the file(s).

The request created will be valid for 14 days.

**Your information:**

Name:  Email: @mail.mil Organization:

**Who do you want to send the request to:**

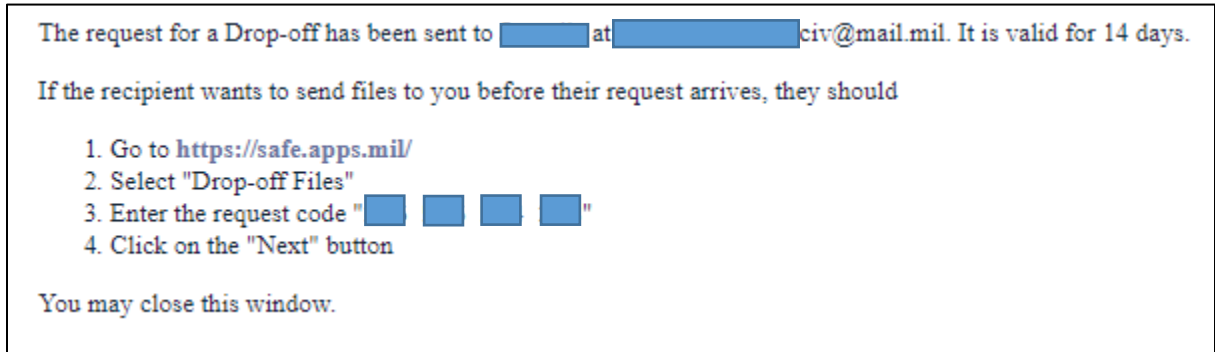
Name:  Email:

**Subject:**

**Note:** This will be sent to the recipient. It will also be included in the resulting drop-off sent to you.

1000 / 1000 left

3. Once complete, click "Send the Request"
4. A "Request Code" is displayed to the sender

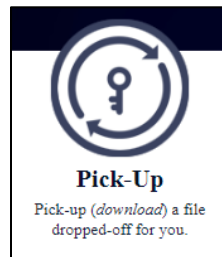


5. The recipient will receive an automated email containing the information you entered along with a URL, which allows them to upload the files for you. The URL also includes the request code, which also can be used to "drop-off" / upload a file.

## Pick-up (Authenticated User and Non-Authenticated User or Guest)

Pick-up a file dropped off for you

1. Click Pick-up



2. Enter the Claim ID, Recipient Code and Passcode.

These items will be sent you in an automated email or, conveyed to you by the initiator of the transfer. If you select the link in the automatic notification, the Claim ID, Recipient Code and Claim Passcode will be pre-filled automatically.

Please enter the claim id, recipient code, and claim passcode.

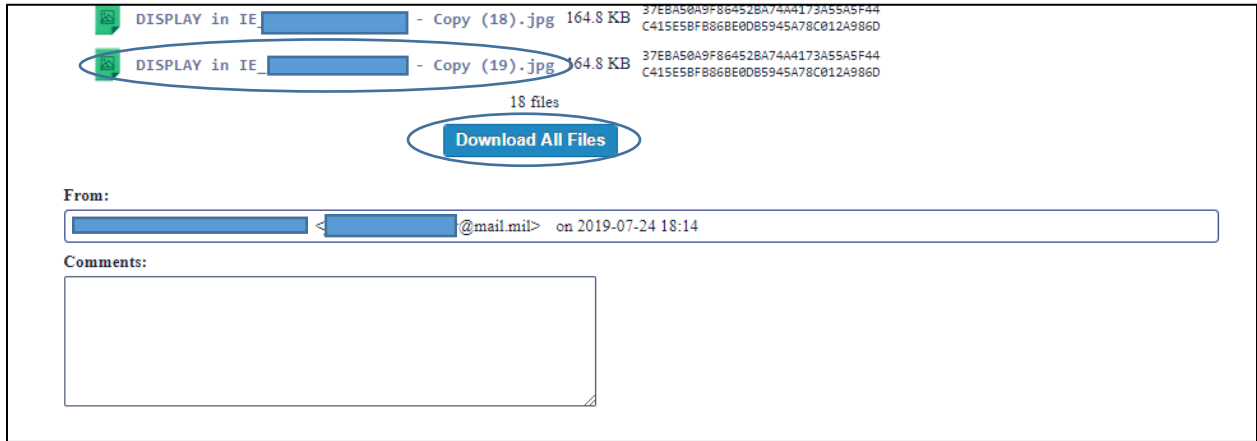
Claim ID:

Recipient Code:

Claim Passcode:

**Pick-up Files**

3. Click "Pick-up Files"
4. The user can either click "Download All Files" to download the package or download each individual file by clicking its hyperlink (i.e., the file depicted below is a hyperlink which can be clicked by the user for individual downloads).

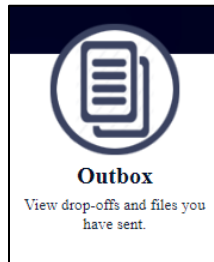


5. The files are downloaded to your workstation

## Outbox (CAC Authenticated User)

All drop-offs and files sent are viewed within the Outbox

1. Click "Outbox"



2. Click a package to see its details. NOTE: *The time the package was created is displayed in Zulu Time*

### Outbox

Click on a drop-off to view the information and files for that drop-off.

Show  entries Search:

Claim ID	Sender	Recipient	Size	Created
fxv2ag4mxPCeWJCa	[redacted]@mail.mil	[redacted]@mail.mil	18.6 KB	2019-07-23 18:26:53


Showing 1 to 1 of 1 entries « < 1 > »

3. The Drop-off Summary is displayed

### Drop-Off Summary

[Delete Dropoff](#) [Resend Dropoff](#)

Click on a filename to download that file.

Filename	Size	SHA-256 Checksum	Description
 Test Document.zip	3.8 MB	8DEE0F053E31B92FCA86E452AFA259F5 9ACFC2A2AAD95AD496285182AC83E8E	

1 file

[Download All Files](#)

**From:** [redacted]@mail.mil on 2019-07-30 16:19

**To:** Jeanelle <[redacted]@mail.mil>

**Comments:**

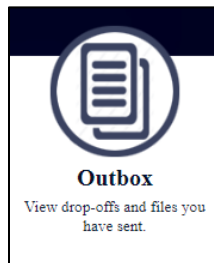
**Recipient URL List** Show

**Pickup History**  
None of the files has been picked-up yet.

## Search for a Drop-off (CAC Authenticated User)

As an authenticated user, you can search your Outbox to locate previous packages sent. The search criteria is based on claim id, sender, recipient, file size or the date the drop-off was created.

1. Click "Outbox"



2. Enter the search criteria for the package you need to locate.

### Outbox

Click on a drop-off to view the information and files for that drop-off.

Show 10 entries

Claim ID	Sender	Recipient	Size	Created
sE9VUydfp9QYA8UD	<[redacted]@mail.mil>	[redacted]@mail.mil>	2.0 MB	2019-07-29 14:50:51
NgaxiWCrSQ8chtEFZ	<[redacted]@mail.mil>	[redacted]@mail.mil>	683.3 KB	2019-07-29 14:44:48
39PmTWgZXh2NpAwG	<[redacted]@mail.mil>	[redacted]@mail.mil>	3.2 KB	2019-07-29 14:39:16
TM9HkDHehp2oQAZA	<[redacted]@mail.mil>	[redacted]@gmail.com>	747.8 KB	2019-07-29 14:24:45

3. The packages matching your search criteria are displayed.
4. Click on the package you need to view its details. NOTE: *The time the package was created is displayed in Zulu Time*
5. The Drop-off Summary is displayed

### Drop-Off Summary

Delete Dropoff
Resend Dropoff

Click on a filename to download that file.

Filename	Size	SHA-256 Checksum	Description
Test Document.zip	3.8 MB	8DEE0F053E31B92FCAB6E452AFA259F5 9ACFC2A2AADC95AD496285182AC83E8E	

1 file

Download All Files

**From:**

[redacted]@mail.mil> on 2019-07-30 16:19

**To:**

[redacted]@mail.mil>

**Comments:**

**Recipient URL List** Show

**Pickup History**

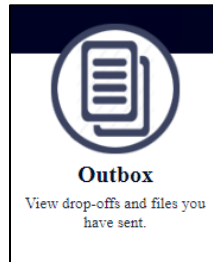
None of the files has been picked-up yet.



## Recipient URL List (CAC Authenticated User)

As the sender of files, you are able to view all of the URLs associated with your drop-offs. You can share this URL with recipients as required.

1. Click "Outbox"




2. Click a package to view its details. NOTE: *The time the package was created is displayed in Zulu Time*

<b>Outbox</b>					
Click on a drop-off to view the information and files for that drop-off.					
Show <input type="text" value="10"/> entries			Search: <input type="text"/>		
Claim ID	Sender	Recipient	Size	Created	
fxv2ag4mxPCewJCa	[redacted]@mail.mil	[redacted]@mail.mil	18.6 KB	2019-07-23 18:26:53	
Showing 1 to 1 of 1 entries					<< < 1 > >>

3. The Drop-off Summary is displayed

**Drop-Off Summary** Delete Dropoff Resend Dropoff

Click on a filename to download that file.

Filename	Size	SHA-256 Checksum	Description
 Test Document.zip	3.8 MB	8DEE0F053E31B92FCA86E452AFA259F5 9ACFC2A2AAD95AD496285182AC83E8E	

1 file

[Download All Files](#)

**From:**  
[redacted] <[redacted].civ@mail.mil> on 2019-07-30 16:19

**To:**  
[redacted] <civ@mail.mil>

**Comments:**  
[empty text box]

Recipient URL List [Show](#)

Pickup History  
None of the files has been picked-up yet.

6. Locate “Recipient URL List” and the bottom of the screen and click “Show”

**Recipient URL List Hide**

Claim Passcode: [redacted]

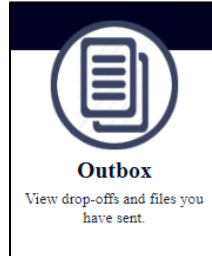
Download Link for [redacted]: <https://safe.apps.mil/pickup.php?claimID=DuqFnmjehm5BiWk> [Copy](#)

7. The URL and Claim Passcode are displayed. You can use the “Copy” button to copy and paste this URL and share it with the recipient

## Delete a Drop-off (CAC Authenticated User)

Users can delete drop-offs

1. Click "Outbox"



2. Click a package to view its details. NOTE: *The time the package was created is displayed in Zulu Time*

### Outbox

Click on a drop-off to view the information and files for that drop-off.

Show  entries Search:

Claim ID	Sender	Recipient	Size	Created
fxv2ag4mxPCeWJCa	[redacted]@civ@mail.mil	[redacted]@civ@mail.mil	18.6 KB	2019-07-23 18:26:53


Showing 1 to 1 of 1 entries << < 1 > >>

3. The Drop-off Summary is displayed

### Drop-Off Summary

[Delete Dropoff](#) [Resend Dropoff](#)

Click on a filename to download that file.

Filename	Size	SHA-256 Checksum	Description
 Test Document.zip	3.8 MB	8DDE0F053E31892FCAB6E452AFA259F5 9ACFC2A2AADC95AD496285182AC83E8E	

1 file

[Download All Files](#)

**From:**  
[redacted] <[redacted]@mail.mil> on 2019-07-30 16:19

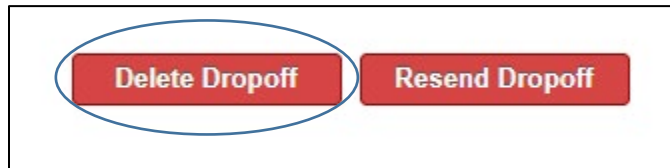
**To:**  
[redacted]@mail.mil

**Comments:**

[Recipient URL List Show](#)

[Pickup History](#)  
None of the files has been picked-up yet.

4. Click "Delete Drop-off"



5. Confirm you want to delete the drop-off, Click "Ok"

safe.apps.mil says

Do you really want to delete this dropoff?

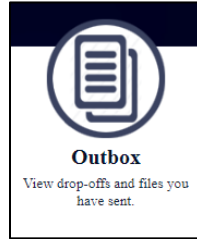
[OK](#) [Cancel](#)

6. The drop-off is deleted.

## Resend a Drop-off (CAC Authenticated User)

Users can resend drop-off to recipient

1. Click "Outbox"



2. Click a package to view its details. NOTE: *The time the package was created is displayed in Zulu Time*

### Outbox

Click on a drop-off to view the information and files for that drop-off.

Show  entries Search:

Claim ID	Sender	Recipient	Size	Created
fxv2ag4mxPCeWJCa	[redacted] civ@mail.mil>	[redacted] civ@mail.mil>	18.6 KB	2019-07-23 18:26:53


Showing 1 to 1 of 1 entries << < 1 > >>

3. The Drop-off Summary is displayed

### Drop-Off Summary

[Delete Dropoff](#) [Resend Dropoff](#)

Click on a filename to download that file.

Filename	Size	SHA-256 Checksum	Description
 Test Document.zip	3.8 MB	8DEE0F853E31892FCA86E452AFA259F5 9ACFC2A2AADC95AD496285182AC83E8E	

1 file

[Download All Files](#)

**From:** [redacted] civ@mail.mil> on 2019-07-30 16:19

**To:** [redacted] civ@mail.mil>

**Comments:**

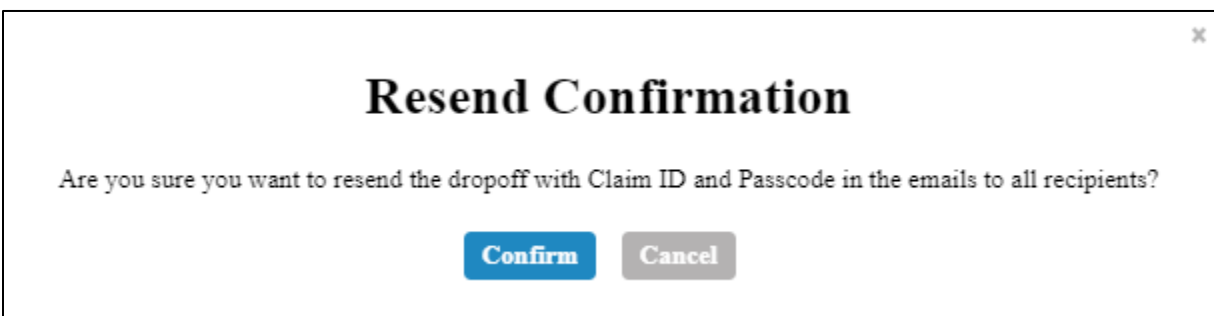
**Recipient URL List Show**

**Pickup History**  
None of the files has been picked-up yet.

4. Select the file you want to resend.
5. Click "Resend Drop-off"



6. To include Passcode and Claim ID, Click "Yes".



7. The drop-off is resent with Passcode and Claim ID.
8. The recipient receives an email containing the drop-off details.

## Encryption

Both CAC Authenticated and Guest users can encrypt files / packages before they are sent. **NOTE: NO CLASSIFIED INFORMATION IS ALLOWED ON DOD SAFE. Any files containing PII/PHI must be encrypted prior to uploading or by checking the Encrypt every file box as specified in the following steps.**

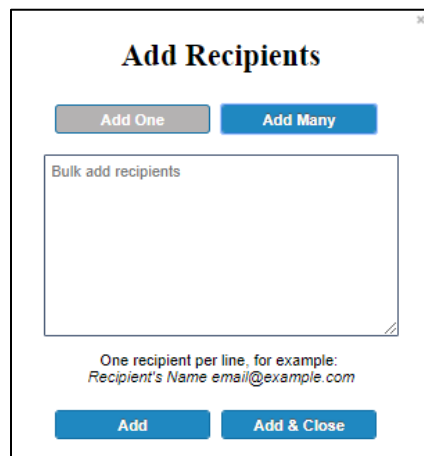
1. Click Drop-off



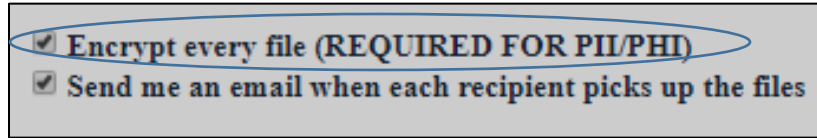
2. Enter some identifying information about the recipient(s) (name and email address).
  - a. For one recipient; add recipient's name and email address
  - b. Click "Add & Close"



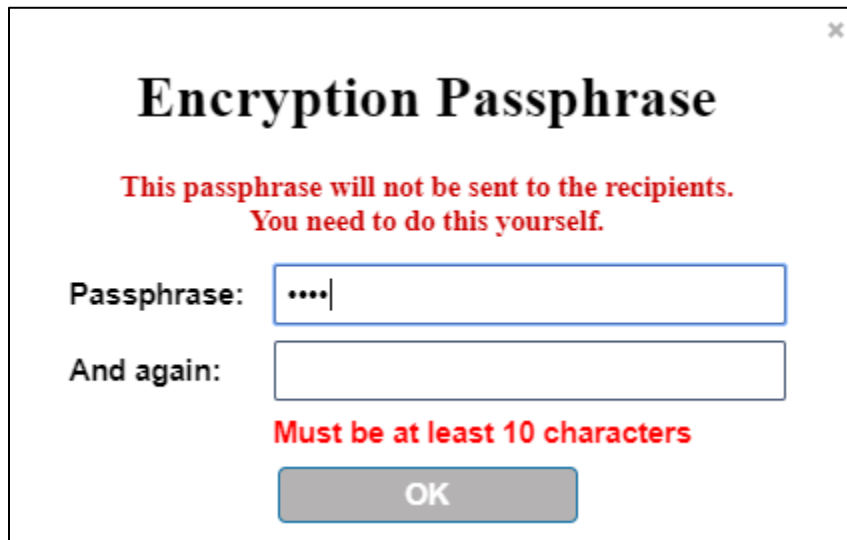
- c. For more than one recipient, click "Add Many"
- d. Enter one recipient per line using this format: *Recipient's Name email@example.com*
- e. Click "Add & Close"



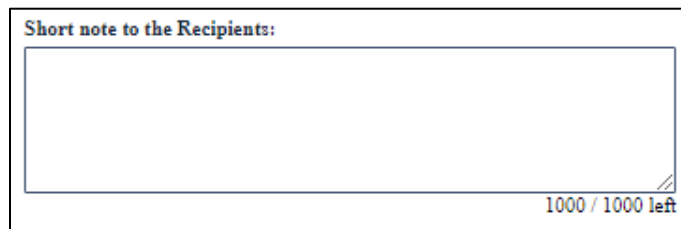
3. Check "Encrypt every file (REQUIRED FOR PII/PHI)"



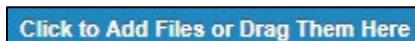
4. Create and remember your Encryption Passphrase. This passphrase will not be sent to the recipients. You will have to do this yourself. Your passphrase must be at least 10 characters long.



5. Click "OK"
6. Add a short note to the Recipient(s). NOTE: You may include your passphrase here or send in a separate email.



7. Click to Add Files or Drag and Drop them





8. Add a description to each file if necessary
9. Click “Drop-Off Files” to send the files to the recipient

Filename	Size	Description
1: Capture.JPG	18.6 KB	<input type="text"/> ✖
18.6 KB / 8192 MB		
<input type="button" value="Drop-off Files"/>		

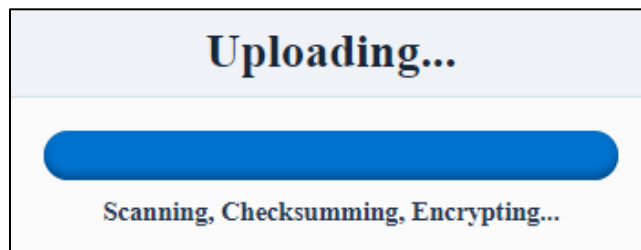
10. Confirm the files do not contain classified information and click “Ok”.

safe.st.apps.mil says

Confirm that the files in this upload do NOT contain classified information.

By clicking "OK", you are confirming that the files do not contain classified information and are aware that your organization will be held accountable for non-compliant data sent through the system.

11. The file is uploaded and an email will be sent to the recipient notifying them of the “drop-off”
  - a. NOTE: The image below depicts an upload for a hashed and encrypted file drop-off. Depending on the speed of the upload, each user may or may not view the image depicted below.




12. You are notified the drop-off is complete

- a. The notification notifies the sender that an encrypted file with a passphrase was successfully sent. It also notifies the sender of filename, file size, the secure hash algorithm – 256 bit (SHA-256) and description. The sender enters the description prior to uploading the file.

## Drop-Off Completed

Your files have been sent successfully.

This drop-off is encrypted with a passphrase known only to the sender.

Filename	Size	SHA-256 Checksum	Description
 Capture.JPG	18.6 KB	28BF05A8B035DE22E868D2B663041448 BEB9ECBC359AC73E20188166D974B55D	

1 file

## APPENDIX: Acronyms

Acronym	Definition
CAC	Common Access Card
DISA	Defense Information Systems Agency
DoD	Department of Defense
DoD SAFE	Department of Defense Secure Access File Exchange
NIPRNet	Non-classified Internet Protocol Router Network
PHI	Protected Health Information
PII	Personally Identifiable Information
PMO	Program Management Office
SHA-256	Secure Hash Algorithm – 256 bit