

BAE SYSTEMS
SECURE FILE TRANSFER SYSTEM (SFTS)
TRAINING GUIDE

Table of Contents

DESCRIPTION.....3

 FILE AND ACCOUNT MANAGEMENT4

SFTS WEBSITE4

 BAE Systems Users – Single Sign-On4

 Temp Users (Non-BAE Systems Users) – Manual Login4

AUTHENTICATION – REGULAR USERS5

 Information regarding regular, non-temporary users:5

AUTHENTICATION – TEMPORARY USERS.....5

INITIAL SIGN ON.....7

 The password requirements are:7

MultiFactor Authentication Setup (External Users Only)8

 Authenticator App on Mobile Device (Example).....12

 Authenticator App on Desktop14

HOW TO SEND A PACKAGE20

NEW PACKAGE NOTIFICATION24

ADDRESS BOOK.....25

 Adding users25

 Deleting/Removing users25

LOGS25

NAVIGATION TIPS26

DESCRIPTION

The BAE Systems Secure File Transfer System [SFTS] does the following:

- SFTS is for UNCLASSIFIED use only.
- SFTS policy for Information controlled by the U.S. International Traffic in Arms Regulations (ITAR) is that it may not be exported to a foreign person/entity without proper authorization by the U.S. Department of State or the Department of Commerce.
- SFTS has an approved Certificate of Networkiness (CoN) from the United States Army. This certification involves a review of how the system meets Army requirements for network security, integration, interoperability, and ease of management and support.
- SFTS safely and securely collects, temporarily stores, manages and distributes data, all while meeting SSA compliance.
- SFTS encrypts the data in transit to and from as well as at rest within the SFTS system. If your data requires additional security such as protection even after it has been downloaded by the customer consider using a third party encryption tool or 7zip to apply password protection your file.
- SFTS offers the ability to transfer data via a secure web interface (HTTPS), as well as via an SFTP client on a per business case basis.
- SFTS retains user uploaded files for 30 days while in your home directory or shared folder and package data sent to or received from customers for 10 days.

Note: SFTS is a free service offered to internal BAE Systems employees and external clients. All SFTS file transfer activity is logged for auditing purposes.

FILE AND ACCOUNT MANAGEMENT

Uploaded content is subject to additional rules to protect items to prevent system overload, such as the following:

- SFTS is only approved for the transfer of UNCLASSIFIED data
- Maximum ad hoc file transfer package size: 500MB with exceptions made on a per user basis
- Maximum times a file can be downloaded: 20 times*
- Package expiration: 10 days*

There are regular 'non-temporary' accounts and temporary accounts. Account policies include the following:

- Regular accounts expire after 6 months of inactivity
- Temporary accounts are automatically locked after 30 days of inactivity, and deleted 1 day after the 30 days of inactivity
- SFTS accounts are locked after 5 incorrect password attempts within 30 minutes. Accounts will automatically unlock after 15 minutes.
- Temporary account passwords must be reset every 90 days*, exemptions are made on a per user basis.

* This setting is subject to policy change.

SFTS WEBSITE

The SFTS system is accessible via a web browser.

BAE Systems Users – Single Sign-On

- To access the site, open up an Internet Explorer browser and go to the following URL: <https://sfts.us.baesystems.com/saml/signon.aspx>

Temp Users (Non-BAE Systems Users) – Manual Login

- To access the site, open up an Internet Explorer browser and go to the following URL: <https://sfts.us.baesystems.com/>

AUTHENTICATION – REGULAR USERS

Information regarding regular, non-temporary users:

BAE Systems GOLDLNK users can login to SFTS using single sign-on (SSO). You can go to the SFTS page <https://sfts.us.baesystems.com/> or you can click the teal and white "Try Single Signon with SAML" button towards the bottom of the login page and then it will automatically log you in after that.

AUTHENTICATION – TEMPORARY USERS

- Temporary users are automatically created when a regular, BAE Systems user sends a package to an external user that does not have an existing Temp account.
- To authenticate, the temporary users must enter their e-mail address as their user name and the password provided via e-mail when the account was created.
- Upon initial sign-on to SFTS, the temporary user will be prompted to reset their password to an 8 character password of their choosing and setup multifactor authentication via Google Authenticator (or similar authenticator app on mobile phone). The password the temp user changes it to, is good for 90 days. A new password is not to be generated for each new package sent as long as the recipient already has an SFTS account.
- Temporary users are automatically deleted after 30 days of inactivity. Once the temp user gets deleted. The BAE Systems user will have to send a new package to re-create the temp user's account. A new temporary password will be sent to the

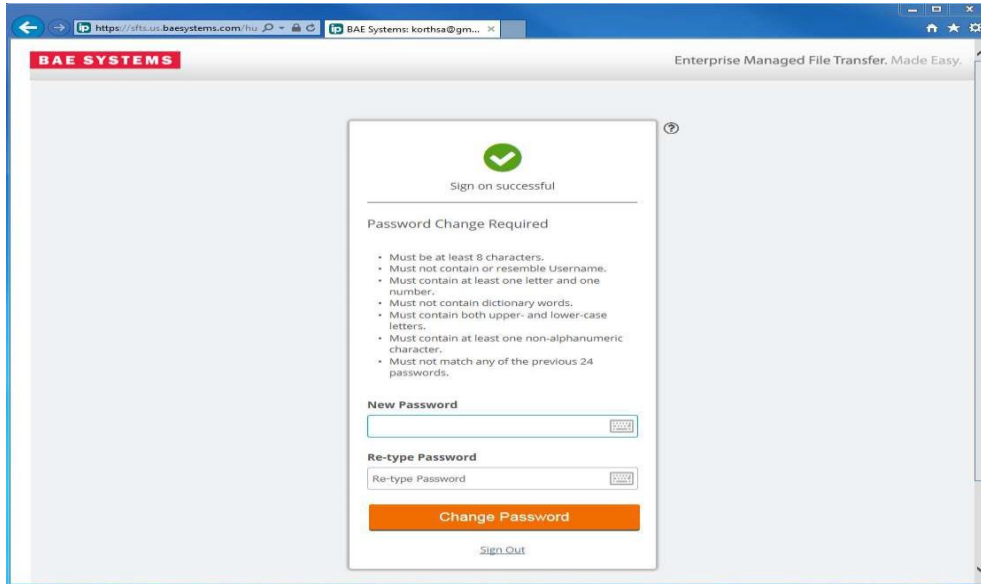
temp user.

- Temporary users have the ability to send messages/packages back to only the sender of which they received the message/package. For example, john.smith@baesystems.com sends a message/package to jane.doe@computersystems.com. Jane Doe can only send/receive files to/from John Smith.

Non-temporary users that are not on GOLDLNK, such as a WHITELNK, GREENLNK, SANDLNK, etc. users, must have their accounts manually created by a BAE Systems (GOLDLNK) user. To authenticate, the user must enter their email address and then provide their local password.

INITIAL SIGN ON

Upon the first log in, temporary (external) users will be prompted to change their passwords.

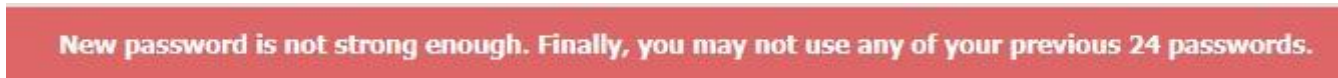


The password requirements are:

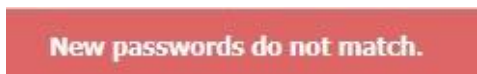
- Must be at least 8 characters.
- Must not contain or resemble Username.
- Must contain at least one letter and one number.
- Must contain both upper- and lower-case letters.
- Must contain at least one non-alphanumeric character.
- Must not contain dictionary words.**
- Must not match any of the previous 24 passwords.**

NOTE: Pay Special Attention to the bottom two requirements as these are the most common causes of password change failures.

If the password strength criteria is not met, the following warning is displayed:



If the new passwords entered twice do not match, the following warning is displayed:



MultiFactor Authentication Setup (External Users Only)

BAE requires MultiFactor Authentication for all external users and offers two different methods to satisfy this requirement. You can elect to configure one or both of these methods.

Email Code Generation

Authenticator App (Desktop or Mobile)

Email Code Generation

Note: This email will only be sent to the email address used to create the external account.

New User Setup

When your account is first created and you have successfully set your new password you will be prompted to configure MultiFactor Authentication for the first time.



Password change successful

Security Requirement

Multi-factor authentication is required for this account. Click "Learn more" or click **Continue** to complete this one-time setup.

[Learn more](#)

Continue

[Sign Out](#)

After you click Continue you will be prompted for which type of MultiFactor Authentication to use.

Set Up Multi-Factor Authentication

Choose how you want to receive the verification code:

- Authenticator App**
Generate verification code from a synchronized authenticator app installed on your mobile device.
[How to download this?](#)
- Email**
Send verification code to the email configured for this account:

Continue

[Sign Out](#)

To use email based code generation select **Email** and click **Continue**.

A code will be emailed to you to complete this setup.

Multi-Factor Authentication Setup Code

User [redacted] is attempting to set up multi-factor authentication and has requested a verification code via email. Enter the following code into the browser and click Verify to complete the setup of multi-factor authentication:

114 376

Regards,
BAE Systems Secure File Transfer System (SFTS) Notification Service. This is an auto-generated message. Please do not reply to this email. Contact the sender of the package or the BAE Service Desk if you require assistance.

Enter the Code from the email into the Verificaiton Code box and click Verify.

Set Up Multi-Factor Authentication

A verification code has been sent to the email configured to this account:

[Request another code](#)

Enter Verification Code

Verify

[Sign Out](#)

Click **Continue** to proceed to your home page.



Multi-factor authentication setup successful

You can modify these settings under **My Account**.

Continue

[Sign Out](#)

Existing User Setup

Login to your SFTS Account and Click on **My Account** at the top left

The screenshot shows the top navigation bar of the BAE Systems portal. On the left is the BAE SYSTEMS logo. On the right, it says "Signed onto BAE Systems as" followed by a user name, and then links for "MY ACCOUNT", "SIGN OUT", and "HELP". A red arrow points to the "MY ACCOUNT" link. Below the navigation bar is a "HOME" button with a house icon. The main content area contains a privacy notice: "You are accessing a BAE Systems, Inc. information system, which includes: (i) this computer, (ii) the computer network to which it is connected, (iii) all computers connected to such network, and (iv) all devices and storage media attached to such network or to a computer on such network. This information system is provided for BAE Systems, Inc. authorized use only. Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties. By using this information system, you understand and consent to the following: (a) you have no reasonable expectation of privacy regarding any communications or data transiting or stored on this information system, and at any time BAE Systems, Inc. may monitor, record, collect, intercept, search, and seize any communication or data transiting or stored on this information system, (b) any communications or data transiting or stored on this information system may be disclosed or used for any lawful purpose, and (c) your consent is final and irrevocable. This system contains Controlled Unclassified Information (CUI) with specific requirements imposed by the Department of Defense, and its use may be subject to other specified requirements associated with certain types of CUI, such as Export Controlled information."

Scroll Down to the Multi-Factor Authentication section.

Multi-Factor Authentication...

Available Methods

In order to use multi-factor authentication you must enable one or more of the methods below. (Enabling more than one method allows choice of verification method at sign on.) Site policy requires that multi-factor authentication be enabled for this account. [Learn more](#)

Authenticator App ✔ Enabled	Reset...	Disable
Email Send verification code to the email configured for this account		Enable...

Click **Enable** on the Email verification code option.

An email will be sent to your registered email address containing the verification code.

Multi-Factor Authentication Setup Code

User is attempting to set up multi-factor authentication and has requested a verification code via email. Enter the following code into the browser and click Verify to complete the setup of multi-factor authentication:

114 376

Regards,
BAE Systems Secure File Transfer System (SFTS) Notification Service. This is an auto-generated message. Please do not reply to this email. Contact the sender of the package or the BAE Service Desk if you require assistance.

Enter this verification code into the box and click **Verify**

Set Up Multi-Factor Authentication Using Email

A verification code was sent to the following email address:

[Request another code](#)

Enter the code you received via email:

Verify

Cancel

NOTE: You may now login to SFTS with a code sent to your email address **OR** your existing Authenticator app.

Authenticator App on Mobile Device (Example)

Note: SFTS Supports most third party authenticator apps this example uses the Google Authenticator.

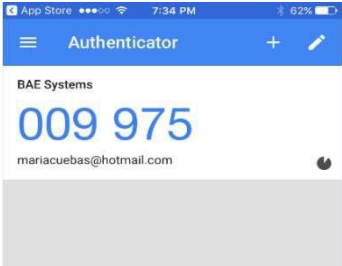
- 1. Download Google Authenticator onto your mobile device. Open the application and then click **Continue** on the SFTS screen prompt.



- 2. Using the authenticator app on your mobile device, scan the QR code on the SFTS screen prompt to sync your authenticator app with your SFTS account.



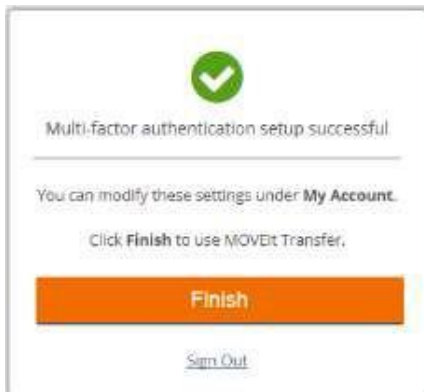
- 3. You will be provided a 6-digit code in the authenticator app.



4. Enter the 6-digit code on the Set Up Multi- Factor Authentication screen in the Enter Verification Code box and click **Verify**.



5. Click **Finish**.



Authenticator App on Desktop


The use of an authenticator application on your desktop (i.e., the same device you are using to access the SFTS site) is not encouraged, however, we realize this option may be necessary.

Please note that the software required to run an authenticator application from your desktop is not supported by BAE Systems, Inc. Installation and other troubleshooting is not available through the BAE Service Desk.

1. When prompted to scan the QR code using your mobile device, click the Show Key link to show the secret key to be used in configuring the desktop authenticator application.

Set Up Multi-Factor Authentication

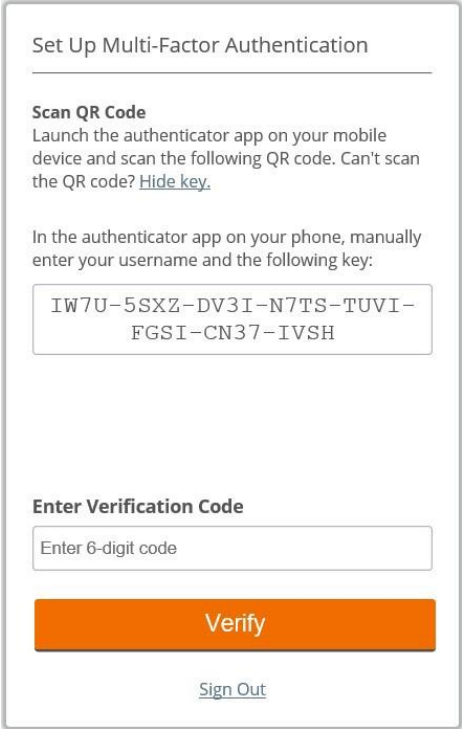
Scan QR Code
Launch the authenticator app on your mobile device and scan the following QR code. Can't scan the QR code? [Show key.](#)



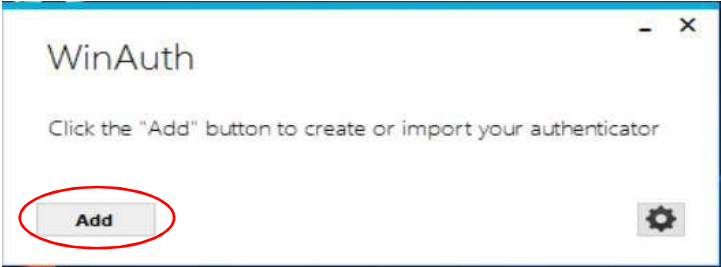
Enter Verification Code

Verify

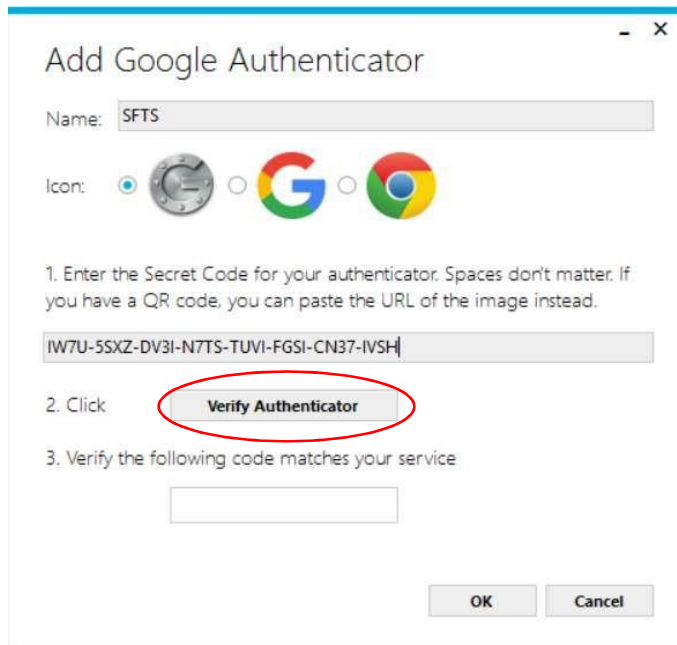
[Sign Out](#)



- 2. Navigate to <https://github.com/winauth/winauth/releases/download/3.6.2/WinAuth-3.6.2.zip> and download WinAuth. Save the file to your PC in the location of your choice.
- 3. Find the file that you just downloaded, unzip it, and double-click on the WinAuth application file to run the application.
- 4. Click **Add** to add an authenticator to the WinAuth app. In the drop-down, select Google.




- 5. In the "Add Google Authenticator" window, type a name for your configuration, such as SFTS or BAE SFTS.



6. In the box that says "Enter the Secret Code for your authenticator; cut, copy, and paste or type the key that the SFTS site provided when you clicked the "Show Key" link.
7. Click **Verify Authenticator**.
8. A 6-digit code will appear. Type the 6-digit code provided into the SFTS site and click **Verify** to complete configuration. You must enter the code and click Verify before the time below the code runs out. **Note, setup of WinAuth is NOT complete, please see the next page to complete setup.*

Add Google Authenticator

Name:

Icon:   

1. Enter the Secret Code for your authenticator. Spaces don't matter. If you have a QR code, you can paste the URL of the image instead.

2. Click

3. Verify the following code matches your service

Set Up Multi-Factor Authentication

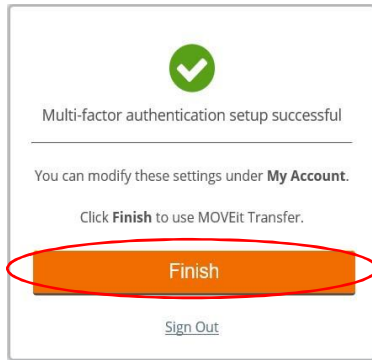
Scan QR Code
Launch the authenticator app on your mobile device and scan the following QR code. Can't scan the QR code? [Hide key.](#)

In the authenticator app on your phone, manually enter your username and the following key:

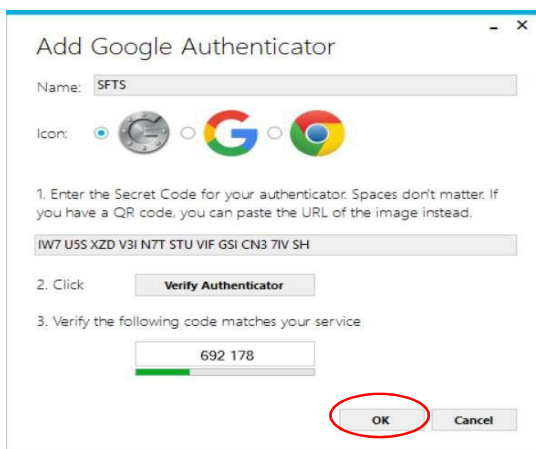
Enter Verification Code

[Sign Out](#)

9. When SFTS tells you that multi-factor authentication setup was successful you can click Finish and you will be logged into SFTS.



10. Return to your WinAuth App and click **OK**.

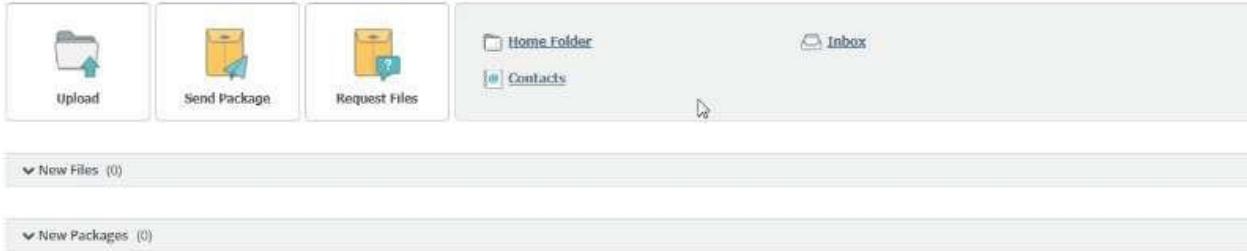


11. Uncheck the cyan checkbox, "Protect with my own password" You will not be prompted to enter a password for WinAuth each time you open the application. Click **OK** to complete the setup.

Once you have successfully configured the account for multi-factor authentication, you can upload, download, send, and request files.

4. YOU HAVE NO RIGHT TO OR EXPECTATION OF PRIVACY REGARDING YOUR USE OF COMPANY IT ASSETS. See BAE Systems, Inc. Management Policy 901 (Acceptable Use) for additional guidance.

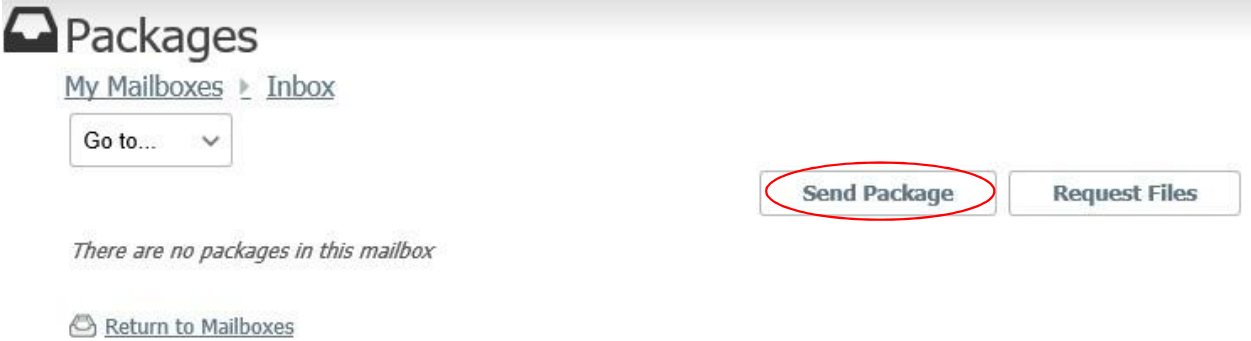
By clicking "OK" or viewing this notice, you acknowledge and consent to these terms of use.



After Multi-Factor Authentication has been configured for the new account, all subsequent logins will require the user's password followed by the current 6-digit code provided by whichever authenticator application that the user has chosen to use.

HOW TO SEND A PACKAGE

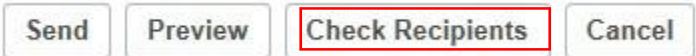
1. On the Home page find the '**Package Actions**' section and click '**Send Package**'.



2. The '**New Package**' e-mail will appear. Enter an e-mail address in the To field. Multiple e-mail addresses must be comma separated.



3. Once complete, click on the '**Check Recipients**' box.



4. The message '**Recipients checked OK**' confirms that the recipients can receive a package.



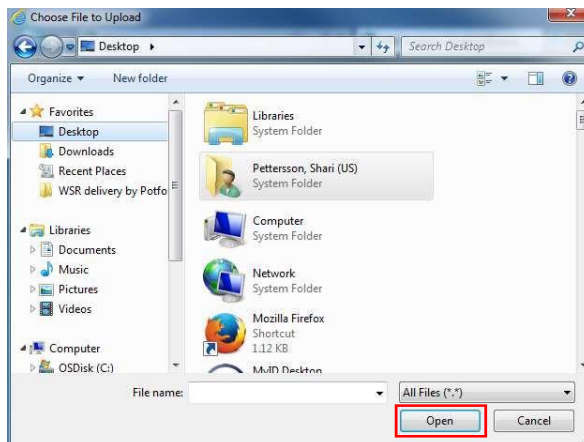
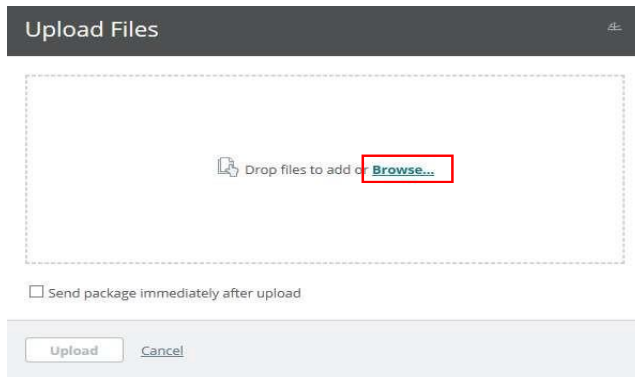
- 5. If the error message '**Not allowed to send to any recipients matching <recipient e-mail>**' is displayed, this indicates that the recipient has an existing account but the account has been locked due to a security violation, or has been marked for deletion due to inactivity. In this event, please contact the Service Desk to have the account reviewed and unlocked.



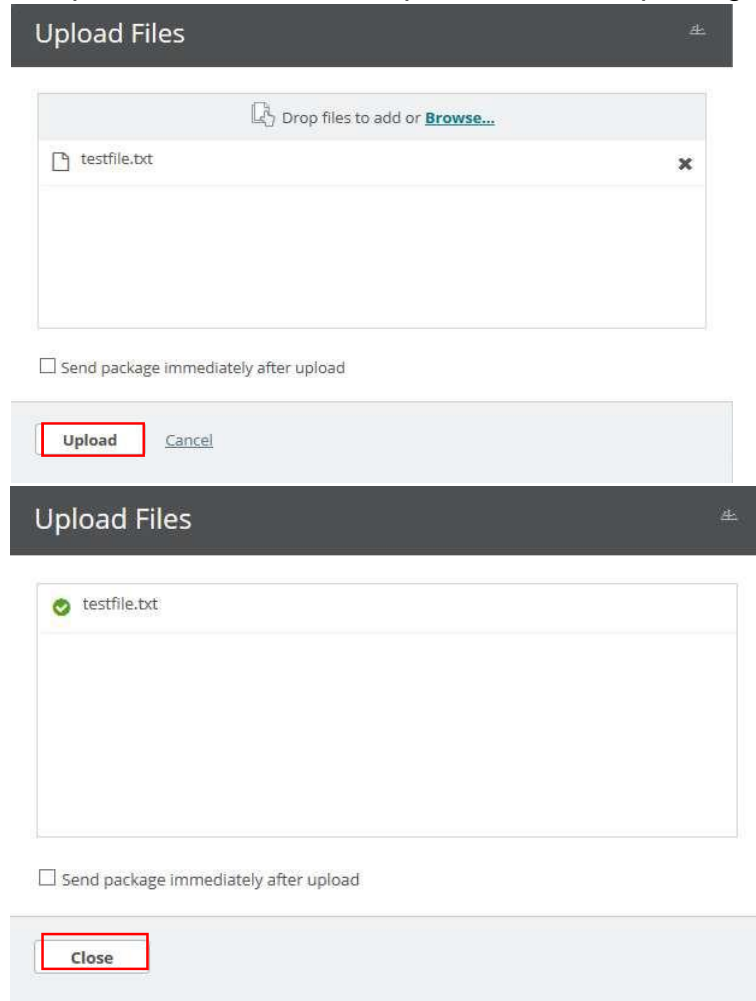
- 6. Enter a '**Subject**'. This field is required.
- 7. Option 1: Drag and drop files from your computer into the Files box. Option 2: Click Upload Files to open the Upload Files dialog box:



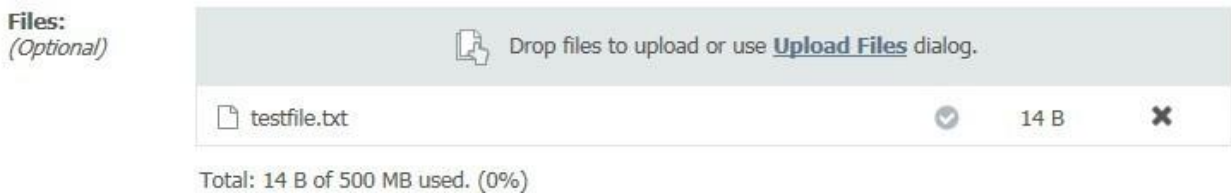
- 8. Click Browse in the Upload Files dialog box and then select your file(s) to upload and click Open:



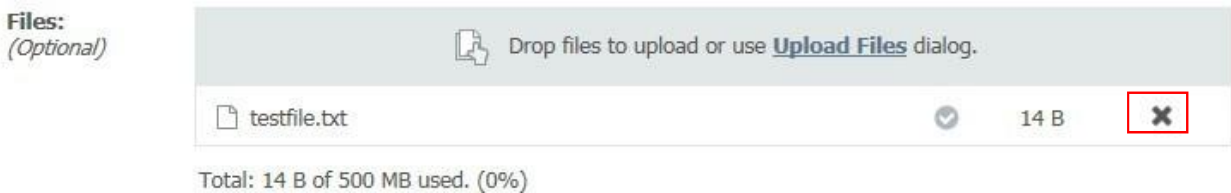
Click **'Upload'** to upload the file, then **'Close'** after the upload completes. The file will be uploaded into the package.



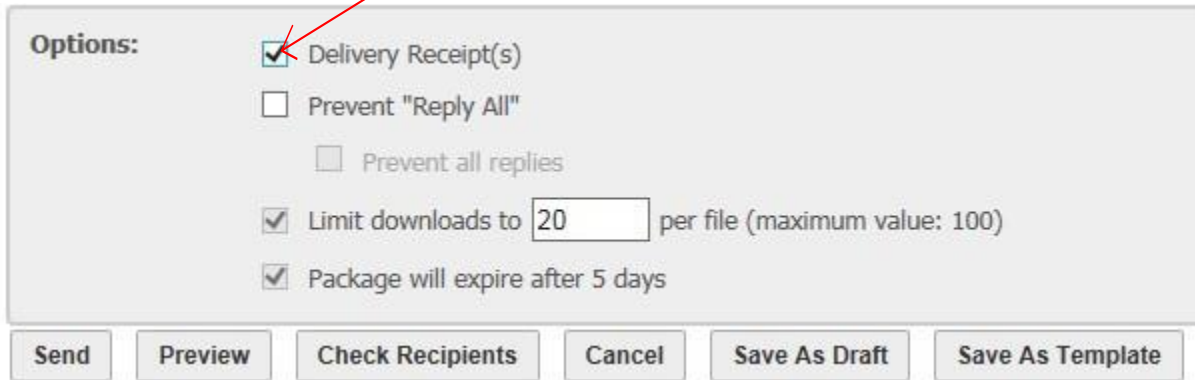
The file chosen will appear under the 'Files:' section.



You can delete a file/attachment by clicking the X beside the file/attachment name.

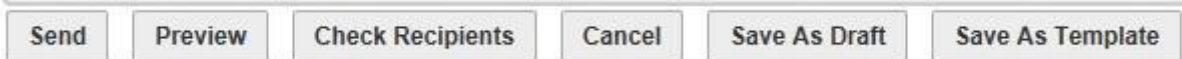


- 9. Add options below: You can click **Delivery Receipt(s)** to ensure that the receipt(s) have received the message/package that you sent them.



The screenshot shows a dialog box titled "Options:" with several checkboxes and a text input field. A red arrow points to the "Delivery Receipt(s)" checkbox, which is checked. Other options include "Prevent 'Reply All'", "Prevent all replies", "Limit downloads to 20 per file (maximum value: 100)", and "Package will expire after 5 days". At the bottom of the dialog are buttons for "Send", "Preview", "Check Recipients", "Cancel", "Save As Draft", and "Save As Template".

- 10. The package can also be saved as a draft, or saved as a template. Additional details on these features can be reviewed in the Online Manual.



A horizontal row of six buttons: "Send", "Preview", "Check Recipients", "Cancel", "Save As Draft", and "Save As Template".

- 11. Click on **'Send'** 

- 12. After clicking **'Send'**, you will be prompted to choose a password for any **'temporary user'** accounts that have been created. A default password is provided. It is recommended that you have the Temp user cut and paste the suggested (temporary) password. Alternatively, you can customize the password as well. Click the **'OK'** button to use the suggested password auto generated by the SFTS system.

Provide Password



The screenshot shows a dialog box with the text: "Please select or enter a password for recipient cosmicuniverse@gmail.com. The password will be automatically emailed to the recipient." There are two radio buttons: "Use Suggested Password: A=j!8WFz" (which is selected) and "Type Custom Password". At the bottom are "OK" and "Cancel" buttons.

- 13. Once a password has been chosen. The following message will appear, notifying you that the package has been successfully sent (the ID number will differ). Subsequent packages sent to the temporary user (with an existing

account) will not require a new password to be generated.

Mailbox	New Packages	All Packages	Actions
Inbox	-	-	
Drafts	-	-	
Sent	-	1	
Templates	-	-	
Trash	-	-	

- 14. Temporary users can ONLY send packages to the original sender. Temporary users can send packages to other recipients who have not sent them package ONLY if an administrator adds the address to the 'Address Book'. This request must be placed with the Service Desk.

NEW PACKAGE NOTIFICATION

The recipient of the package will receive a 'New Package Notification' via email (see example below), alerting them that a new package is waiting, and that they are to log into the SFTS system using the link provided. They must use their email address, or SFTS account name if one exists, password, and 6-digit code from Google or Microsoft Authenticator to login.

New Package Is Waiting Inbox x

john.vasicek via BAE Systems Notification Service. This is an auto-generated message. 7:06 PM (1 minute ago) ☆

New Package Notification

Welcome to BAE Systems! A new package has been posted for you.

From: john.vasicek

Your account information is as follows:

Username: cosmicuniverse@gmail.com
Password: A=j!8WFz

Please use the following URL and your username/password to login and view this package. You will also be given the opportunity to compose a secure reply to this package.

(<https://sfts.us.baesystems.com/human.aspx?OrgID=3097&Arg12=message&Arg06=260177319&Arg08=3r8ased618h57u68&username=cosmicuniverse%40gmail.com>)

Regards,
BAE Systems Notification Service. This is an auto-generated message. Please do not reply to this email. Contact the sender of the package or the BAE Service Desk if you require assistance.

ADDRESS BOOK

Adding users

There should be no need to manually add usernames and/or e-mail addresses to your Address Book. Once you send a temporary (external) user a new message or package via SFTS, that user will get automatically added to your Address Book by SFTS.

Deleting/Removing users

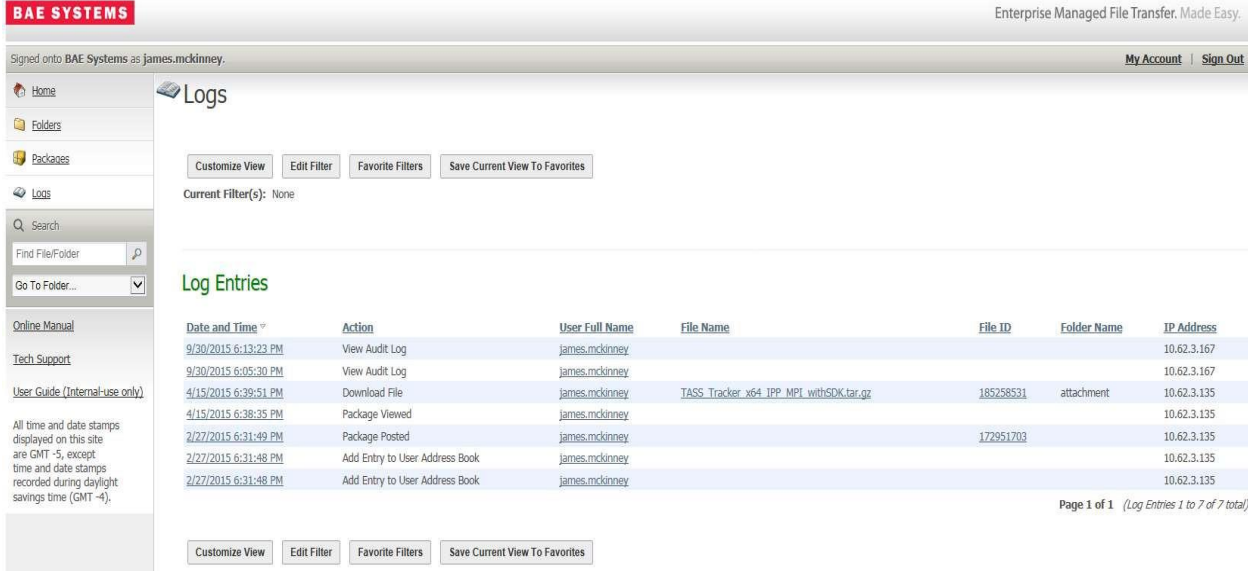
If a temporary (external) user does not sign onto the Secure File Transfer System (SFTS) every 30 days or more from the time you initially sent them a package. Their SFTS account gets deleted by the system due to inactivity. Therefore, that particular user will get deleted from your Address Book.

LOGS

You can review your logs for a listing of your SFTS activity, and for auditing. The 'Logs' link can be found on the left hand menu. Then click the 'Apply Filters' button. **Note:** This only applies to BAE Systems (GOLDLNK) users. Temporary (external) users cannot access Logs.

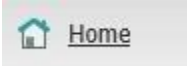
The screenshot shows the BAE Systems SFTS interface. At the top, it says "Signed onto BAE Systems as james.mckinney." and "Enterprise Managed File Transfer. Made Easy." with links for "My Account" and "Sign Out". The left-hand navigation menu includes "Home", "Folders", "Packages", "Logs", a search bar, and links for "Online Manual", "Tech Support", and "User Guide (Internal-use only)". The "Logs" link in the menu is highlighted with a red box. The main content area is titled "Filter Logs..." and contains several filter fields: "Date" with a checkbox for "Display only log entries within this date range:", "Start Date/Time" (2016 Feb 2 12:00 AM), "End Date/Time" (2016 Feb 2 11:59 PM), "Action" (Any), "User" (james.mckinney), "File" (FileID Contains, FileName Contains), "Size" (Comparison: Any, Size (kb)), "Folder" (FolderPath Contains), "Agent Brand" (Contains), and "Success/Failure" (Any). The "Apply Filters" button at the bottom of the filter section is also highlighted with a red box.

The logs screen will be displayed. It will show a listing of all of your SFTS activity and can be used for auditing purposes.



NAVIGATION TIPS

Navigation options follow you through every screen allowing quick access to the following:



Return to main screen.



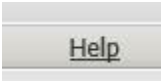
See package actions such as sending a package, managing the address book, or review mailboxes (Inbox, Sent, Drafts, Templates, etc.)



View status of sent jobs and SFTS activity (This only applies to BAE Systems (GOLDLNK) users.



Search for a file or folder.



View the Online Manual, obtain Tech Support by contacting the BAE Systems Service Desk at 1-888-223-4223, or view the SFTS Training Guide.