globalscape
by HelpSystems

# WTC and Workspaces Administration Guide EFT v8.0.7

## Copyright Terms and Conditions

Copyright HelpSystems, LLC and its group of companies.

The content in this document is protected by the Copyright Laws of the United States of America and other countries worldwide. The unauthorized use and/or duplication of this material without express and written permission from HelpSystems is strictly prohibited. Excerpts and links may be used, provided that full and clear credit is given to HelpSystems with appropriate and specific direction to the original content. HelpSystems and its trademarks are properties of the HelpSystems group of companies. All other marks are property of their respective owners.

202112160401

# Table of Contents

# WTC & Workspaces Administration

The topics in this section describe administration of the Web Transfer Client (WTC) and Workspaces.

## Introduction to Workspaces

Workspaces extends the secure and robust EFT file transfer platform with features that allow end users to easily share folders with existing and new user accounts, without burdening the IT administrator. Workspaces empowers end users to share folders quickly and easily, while IT administrators retain full control and visibility of the file transfer infrastructure, leveraging the highest levels of security, regulatory compliance, flexible authentication, and data encryption aspects of the EFT platform. No file sync and share vendors have the underlying security features empowered by EFT for Workspaces as a sharing solution (DMZ Gateway, multiple secure protocols, workflow automation, flexible authentication, etc.).

### Administrators Retain Control

IT administrators are able to delegate to end users the power of managing shared folders with existing and new users without losing governance, visibility, and control. End users are given a tool that fulfills the workflows they have become used to (online file sharing) in a way that conforms to corporate policy. Workspaces gives IT administrators the freedom to deny access to cloud-based file sharing services within their organization, because they have provided a safe alternative to their internal customers.

When a user's folders are shared, via the Web Transfer Client, the shared folder appears in the EFT administration interface on the **VFS** tab under the **Workspace** node.

Here, the administrator can see:

- With whom the folder is shared
- What the permissions are on each user account
- When the Workspace was created
- The physical path to the folder
- Who owns the folder

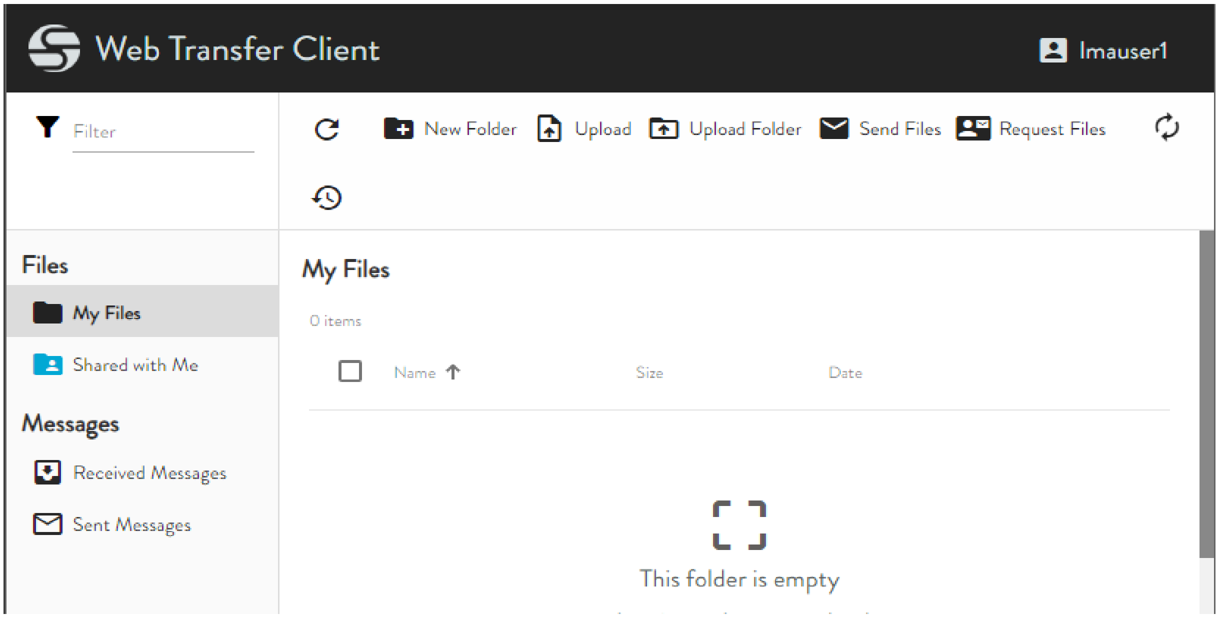
The administrator can also add or remove specific permissions on the folder for each participant.

# How Do I Share Files?

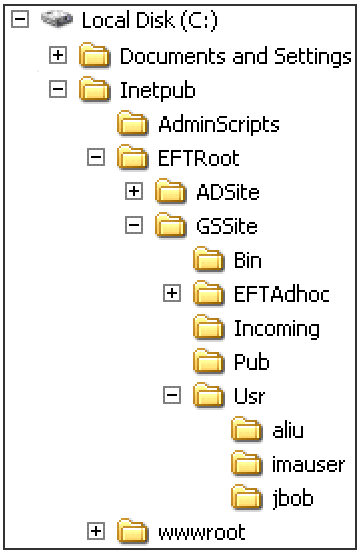
Any user from anywhere in the world who has a computer with Internet browser or FTP client can access EFT and share files—provided the computer on which the user is attempting to connect to EFT is allowed access, and the user has an account defined on EFT. The user account itself or the group to which it belongs must have the appropriate permissions (upload, download, create folders, and so on) assigned on the VFS tab of the administration interface. When users log in to EFT, they connect only to their home folders and cannot browse above their home folders.

EFT allows the following methods through which you can share files using EFT:

- **Web Transfer Client (WTC)** - The WTC is EFT's browser-based file transfer client that allows users to transfer files over HTTP or HTTPS. The WTC can resume transfers and can send multiple files concurrently. It also has drag-and-drop support, integrity validation, a transfer queue, and no file-size limit. The number of files a directory listing can contain, the characters a file/folder name can contain, and the path length of directories is limited by Windows conventions. Refer to File-Naming Conventions for details. For regarding file-naming conventions, refer to the *Microsoft Windows Developer Network* article *Naming a File and the Microsoft TechNet* article How NTFS Works.
- **Workspaces** - Users can create shared folders in which to share files with other EFT users through the Web Transfer Client. Additionally, if the EFT administrator allows it, you can share files with external users and share your Workspaces folders.



- **EFT Outlook Add-In** - With the EFT Outlook Add-In, users can send files via email and the recipient can pick them up in their web browser through Workspaces.
- **Mobile Transfer Client** (MTC) - The MTC is a mobile app that provides a way for iOS and Android phone and tablet users to securely connect to EFT and upload and download files while providing a number of centrally managed security controls for safeguarding your corporate data.
- **Globalscape's CuteFTP**® or a similar "FTP client" - Any FTP client can be used to connect to EFT and transfer files. For more information about CuteFTP, refer to https://www.globalscape.com/cuteftp or online help.
- **Windows File Explorer** - When logged in to the EFT computer, administrators can manage files on EFT using Windows File Explorer. By default, user files are stored in the **C:\Inetpub\EFTRoot\** folder in the **Usr** folder under the Site on which their account is defined (or, on HA implementations, in the shared configuration path, e.g., **\\x.x.x.x\inetpub\EFTRoot\mySite\Usr\username**). In the illustration below, user **imauser**, defined on **GSSite**, stores files in the **imauser** folder. Anyone with the proper permissions on the EFT computer can drag and drop, copy and paste, and create and delete files and folders, just like in Windows File Explorer. For example, suppose user **imauser** has gone over her quota and can no longer upload any files. Instead of increasing the quota for the folder, you can delete files from the **imauser** folder that **imauser** no longer wants, or move them to some other accessible storage.



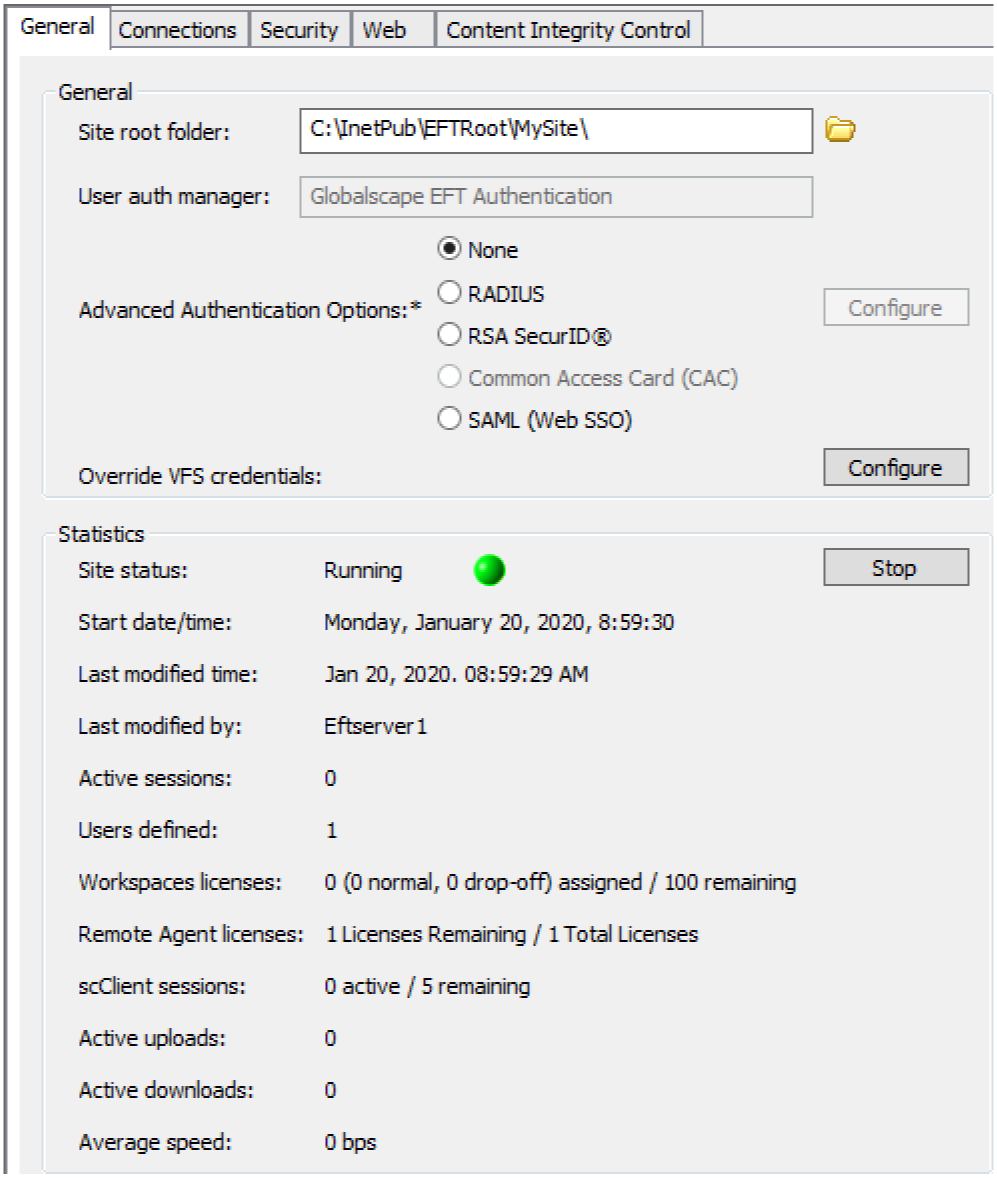
- **Command Prompt** - At a command prompt, you can enable an FTP session and transfer files, if you are familiar with basic DOS commands. Refer to the KB article "Can I use a Windows Command Prompt to send FTP commands to a server?" for list of common commands.

# Workspaces Licenses

In the EFT trial, you have a 100-seat license, meaning 100 users can create Workspaces. After you activate EFT, you have unlimited Workspaces licenses.

There is no limit to the number of Workspaces each owner may possess. Licenses are applied to number of Workspaces *owners* (per Site), not the number of Workspaces created. (The safe operating limit is 1,000 files and folders total). You can allow or deny Workspaces creation to specific users.

- The Site's **General** tab displays how many licenses are consumed (assigned) and how many remain.



General

Site root folder: C:\InetPub\EFTRoot\MySite\

User auth manager: Globalscape EFT Authentication

Advanced Authentication Options:*
● None
○ RADIUS
○ RSA SecurID®
○ Common Access Card (CAC)
○ SAML (Web SSO)

Override VFS credentials:

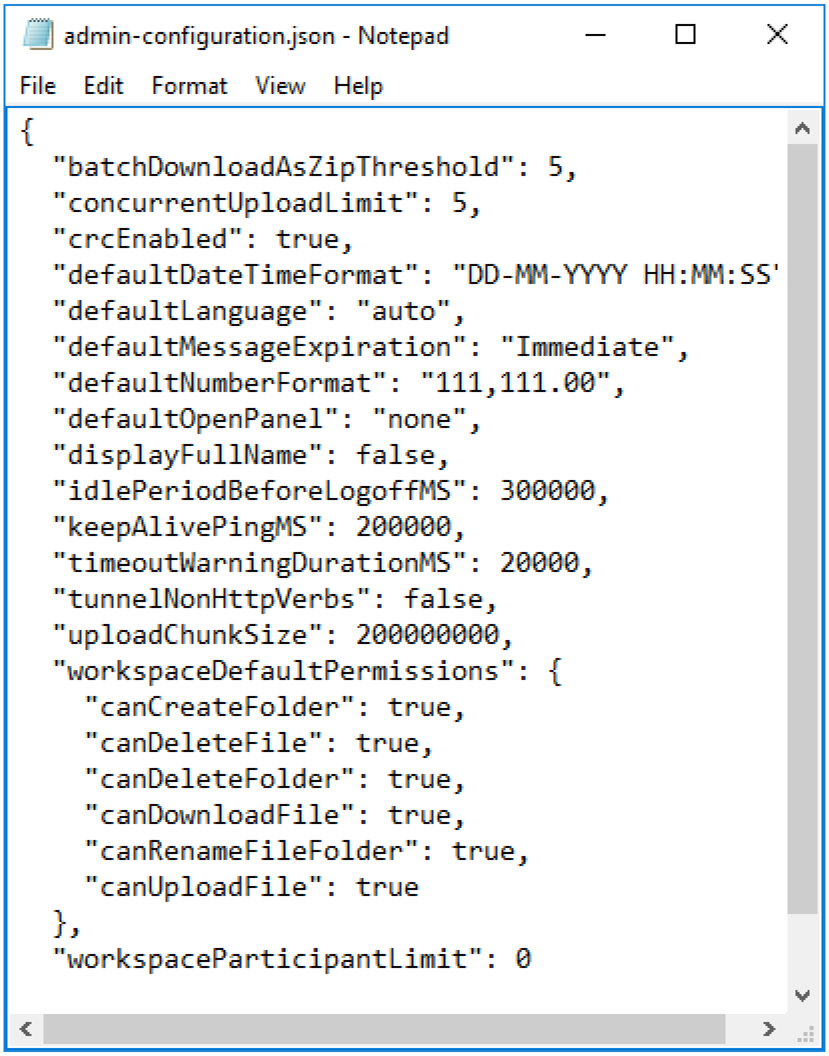
Statistics

Site status: Running ●
Start date/time: Monday, January 20, 2020, 8:59:30
Last modified time: Jan 20, 2020. 08:59:29 AM
Last modified by: Eftserver1
Active sessions: 0
Users defined: 1
Workspaces licenses: 0 (0 normal, 0 drop-off) assigned / 100 remaining
Remote Agent licenses: 1 Licenses Remaining / 1 Total Licenses
scClient sessions: 0 active / 5 remaining
Active uploads: 0
Active downloads: 0
Average speed: 0 bps

# WTC Admin-Configuration Settings

The EFT administrator can configure the defaults for the WTC settings, to better control the user experience.

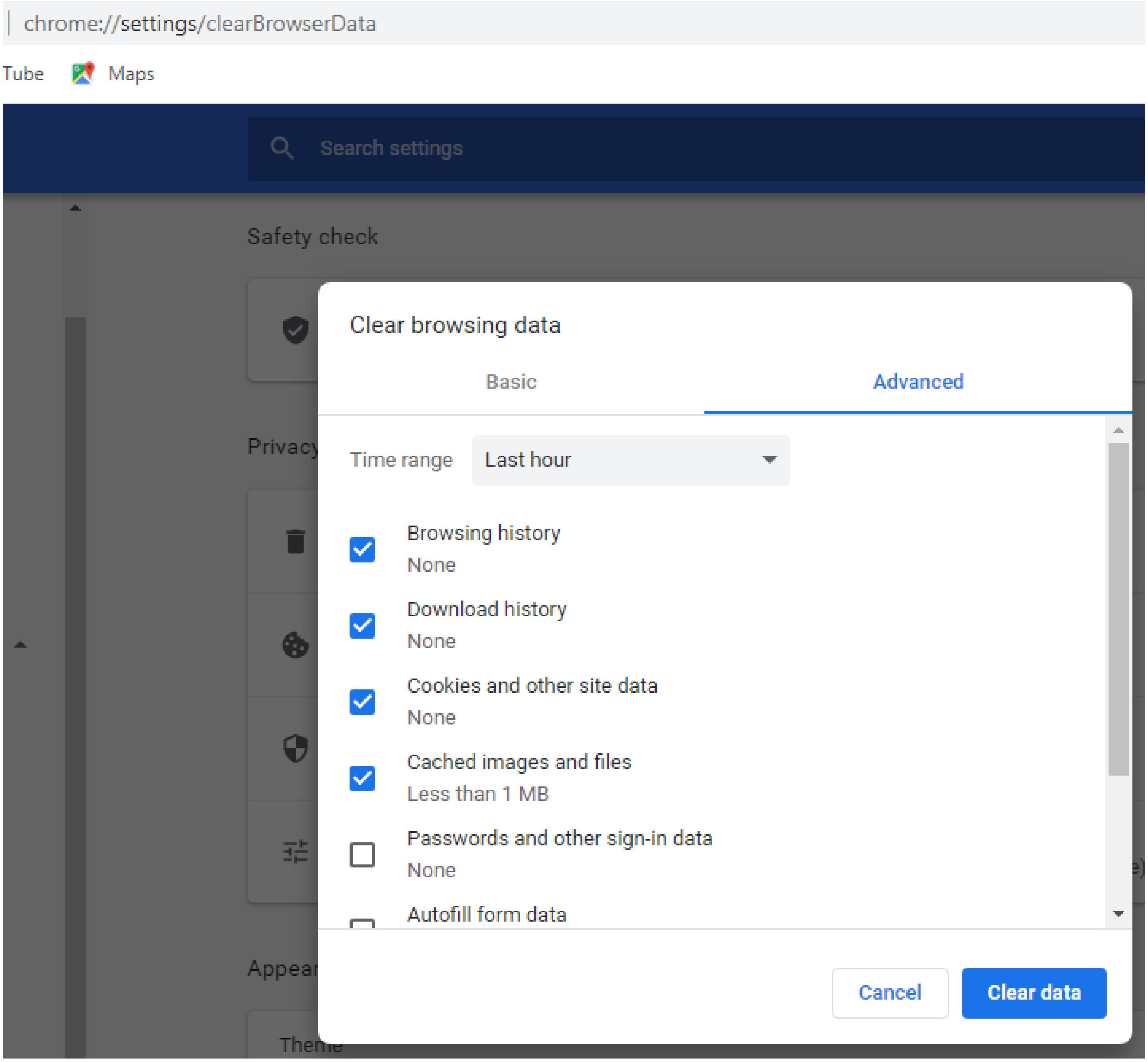
The **admin-configuration.json** file provides several default settings, shown below with the defaults. The default location of the file is:


admin-configuration.json - Notepad
File Edit Format View Help

```
{
  "batchDownloadAsZipThreshold": 5,
  "concurrentUploadLimit": 5,
  "crcEnabled": true,
  "defaultDateTimeFormat": "DD-MM-YYYY HH:MM:SS'
  "defaultLanguage": "auto",
  "defaultMessageExpiration": "Immediate",
  "defaultNumberFormat": "111,111.00",
  "defaultOpenPanel": "none",
  "displayFullName": false,
  "idlePeriodBeforeLogoffMS": 300000,
  "keepAlivePingMS": 200000,
  "timeoutWarningDurationMS": 20000,
  "tunnelNonHttpVerbs": false,
  "uploadChunkSize": 200000000,
  "workspaceDefaultPermissions": {
    "canCreateFolder": true,
    "canDeleteFile": true,
    "canDeleteFolder": true,
    "canDownloadFile": true,
    "canRenameFileFolder": true,
    "canUploadFile": true
  },
  "workspaceParticipantLimit": 0
```

These default settings can be overridden by the user's settings for time/date format, number format, language, and open panel. That is, if a user has logged in before on a particular browser, the previous preferences will take effect.

Deleting the local storage entries will allow a refresh for the administrator values to take effect. (For example, while logged out of the WTC in Chrome, click **Settings**, scroll down to and open **Clear browsing data,** then click **Advanced**. Ensure the **Cached images and files** check box is selected, then click **Clear data**.)



chrome://settings/clearBrowserData

Clear browsing data

Time range: Last hour

☑ Browsing history
None

☑ Download history
None

☑ Cookies and other site data
None

☑ Cached images and files
Less than 1 MB

☐ Passwords and other sign-in data
None

☐ Autofill form data

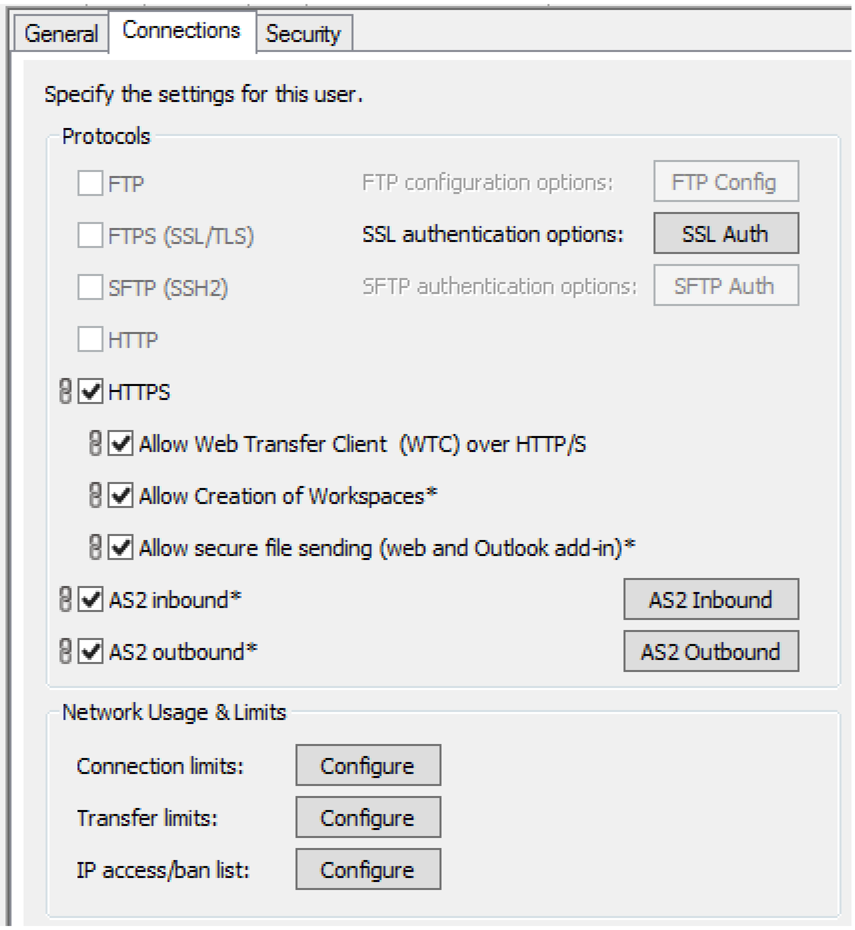
# Allow Users to Create Workspaces

**(Requires the HTTP/S module and Workspaces module)** Users must log in to Workspaces via the Web Transfer Client (WTC). The EFT administrator must configure EFT to allow connections from the WTC. See also Enabling User Access to the Web Transfer Client and Enable and Configure EFT Workspaces.

- Active Directory domain users must have logon permission on EFT computer in order to log on to EFT through the WTC. This is accomplished by adding AD domain users to the "Allow log on locally" list on the EFT computer. If an AD domain user is not in this list, logging on to EFT through the WTC will fail and an error message appears informing the user that Local login access is required to log on to EFT.
- Stopping and restarting the Site disconnects everybody who is connected; users must log back in.
- The user account that is creating the Workspace must have permissions on their home folder to create folders.

### To configure EFT to allow users to create Workspaces

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, click the Settings Template or user account.
3. In the right pane, click the **Connections** tab.



Specify the settings for this user.

Protocols

☐ FTP — FTP configuration options: FTP Config

☐ FTPS (SSL/TLS) — SSL authentication options: SSL Auth

☐ SFTP (SSH2) — SFTP authentication options: SFTP Auth

☐ HTTP

☑ HTTPS

- ☑ Allow Web Transfer Client (WTC) over HTTP/S
- ☑ Allow Creation of Workspaces*
- ☑ Allow secure file sending (web and Outlook add-in)*

☑ AS2 inbound* — AS2 Inbound

☑ AS2 outbound* — AS2 Outbound

Network Usage & Limits

Connection limits: Configure

Transfer limits: Configure

IP access/ban list: Configure

4. In the **Protocols** area, select the **Allow Creation of Workspaces** check box.

   HTTPS must also be enabled.

5. Click **Apply**.

# Changing Logo and Colors in the WTC and Login Page

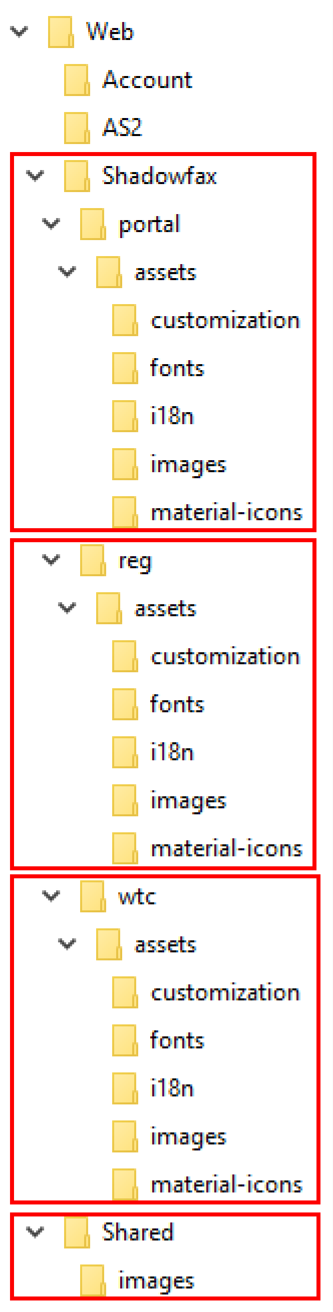
"Rebranding" the Web Transfer Client (WTC) is a common request from customers. This topic provides the procedures for changing the logo and colors in the Login pages and in the WTC itself.

- Please make a backup copy of any files that you plan to edit, in case you have to back out your edits.
- Do not attempt to make changes to the JS or PS files unless you are well versed in doing so. In most cases, it is not necessary to change them.
- You will need to install PowerShell if you don't have it already.

- Be aware when you upgrade from older versions to v8.0.5 or later, the file paths have changed. There is no longer an \EFTClient\ folder.

**NOTE:**
The Web folder contains shared files, reg files, WTC files, and Workspaces files. When changing logos, be aware of which images you need to edit.

- **https://localhost/Web/Account/Login.htm** page uses the logo in the **\Shared\images** folder
- **https://localhost/web/shadowfax/reg/register.html#/forgot-username** and **lost password** pages use the logo in the **\wtc\assets\images** folder



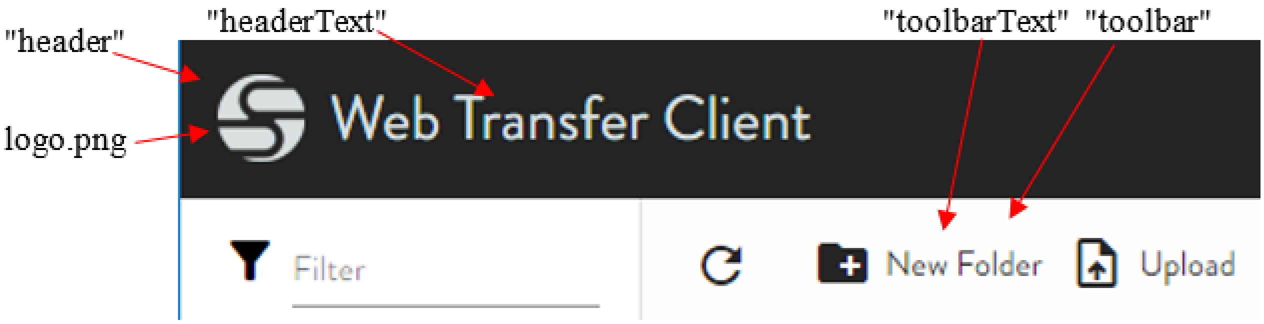
The **Shadowfax\portal\assets\customization** folder contains the **theme.json** file and the **customization-theme.ps1** file.

- **theme.json** is used to define the colors used in the WTC
- **customization-theme.ps1** is a PowerShell script used to change the colors throughout the product

**The procedures below describe how to change the colors, and then run the PowerShell script, as well as changing the logos.**

The default colors in the **theme.json** file are in hexidecimal.

- "primary": "#00a8d4", - blue, used for input field outlines, e.g., the border around the password and username boxes
- "accent": "#7400d4", - purple, used for check boxes
- "warn": "#f44336", - red, used as outline for input field errors, such as invalid characters in a password
- "header": "#232323", light black background
- "headerText": "#DAE0E2", the light gray text in the header, Web Transfer Client
- "toolbar": "#FEFEFE", light gray background
- "toolbarText": "#242424" light black text on the toolbar



The logo next to Web Transfer Client in the header is called **logo.png**. You can replace it with your company logo with the same file name (logo.png). The file is located in the **..\Globalscape\EFT Server\Web\Shadowfax\wtc\assets\images\** folder.

**To change the colors in the lost username or forgot password dialog box**

1. Open **theme.json** in a text editor such as Notepad.
2. Edit the colors as desired. (You can find color numbers on the Internet or use Adobe PhotoShop to identify the color number.)
3. Save the changes to **theme.json**.

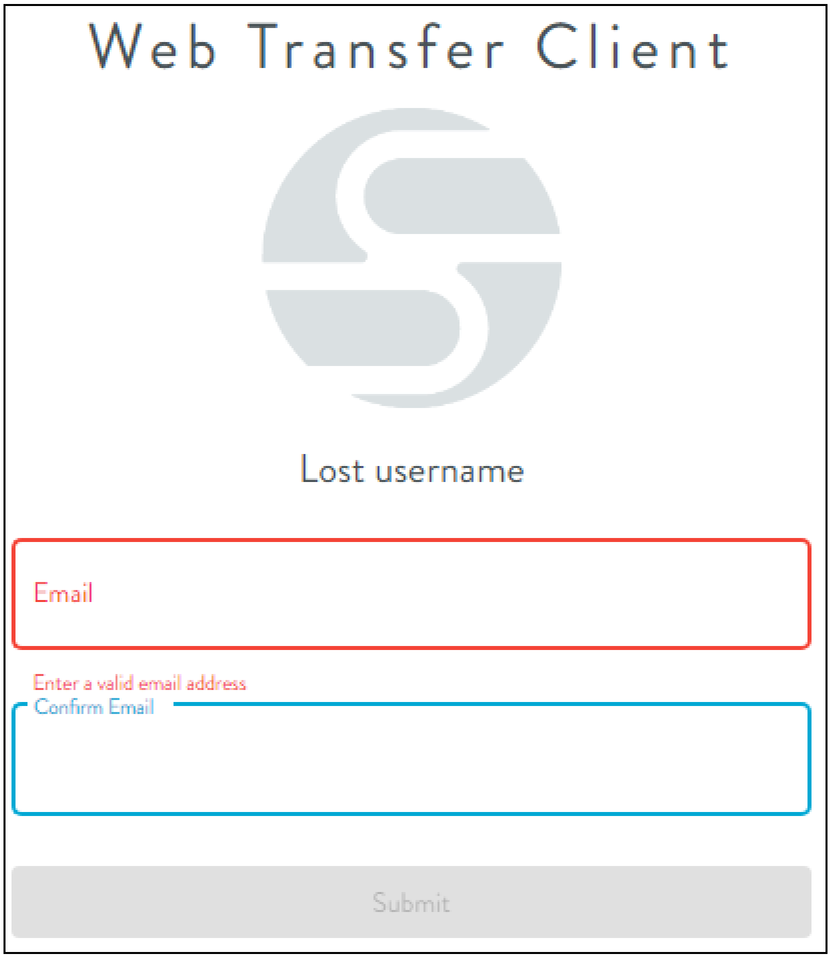
4. Open Windows PowerShell ISE (click **Start**, then **Search** to find it).
5. In PowerShell, open **customize-theme.ps1**, then click the **Run** icon.
6. Go to your WTC address, then click **Forgot Password** to open the forgot-username window. The text-entry boxes should be displayed in your new colors.

### To replace the logo on the login pages

Replace the logos with your own of a similar size, then restart the Site and/or clear the browser cache to see the changes.

The WTC login page comes from EFT; the username/password logos come from Workspaces:

The logo that appears on the forgot-password page is **..\web\shadowfax\wtc\assets\images\logo.png**:

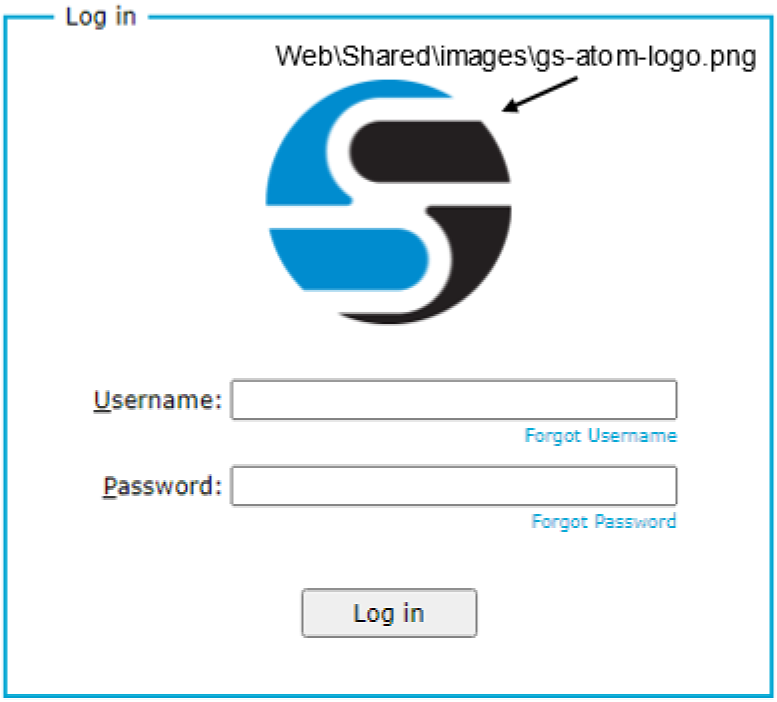


Web Transfer Client

Lost username

Enter a valid email address

The logo that appears on the WTC login page (for example, https://localhost/Web/Account/Login.htm), the logo is **\Web\Shared\images\gs-atom-logo.png**.



Web\Shared\images\gs-atom-logo.png

# Enable Multifactor Authentication

Multifactor authentication is the process of verifying the identity of a user in which the user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism: knowledge (something the user and only the user knows), possession (something the user and only the user has), and inherence (something the user and only the user is).

Two-factor authentication (2FA), a subset of multi-factor authentication, is a method of confirming users' identities by using a combination of different factors: 1) something they know, 2) something they have, or 3) something they are. A common example of 2FA is withdrawing money from an ATM: only the correct combination of a bank card (something the user possesses) and a PIN (something the user knows) allows the transaction to be carried out.

EFT offers multifactor authentication (MFA) for recipients in the Pickup portal, with which a time-based one-time passcode (OTP) is delivered automatically to the recipient's email address or via text message. When attempting authentication, the account is locked out for 5 minutes after 5 failed attempts in a 5-minute period. If the first attempt fails, a user can repeat registration and get a new verification code after 5 minutes have passed since the previous registration attempt.

Refer to Enable and Configure the Send Portal for MFA settings in Workspaces.

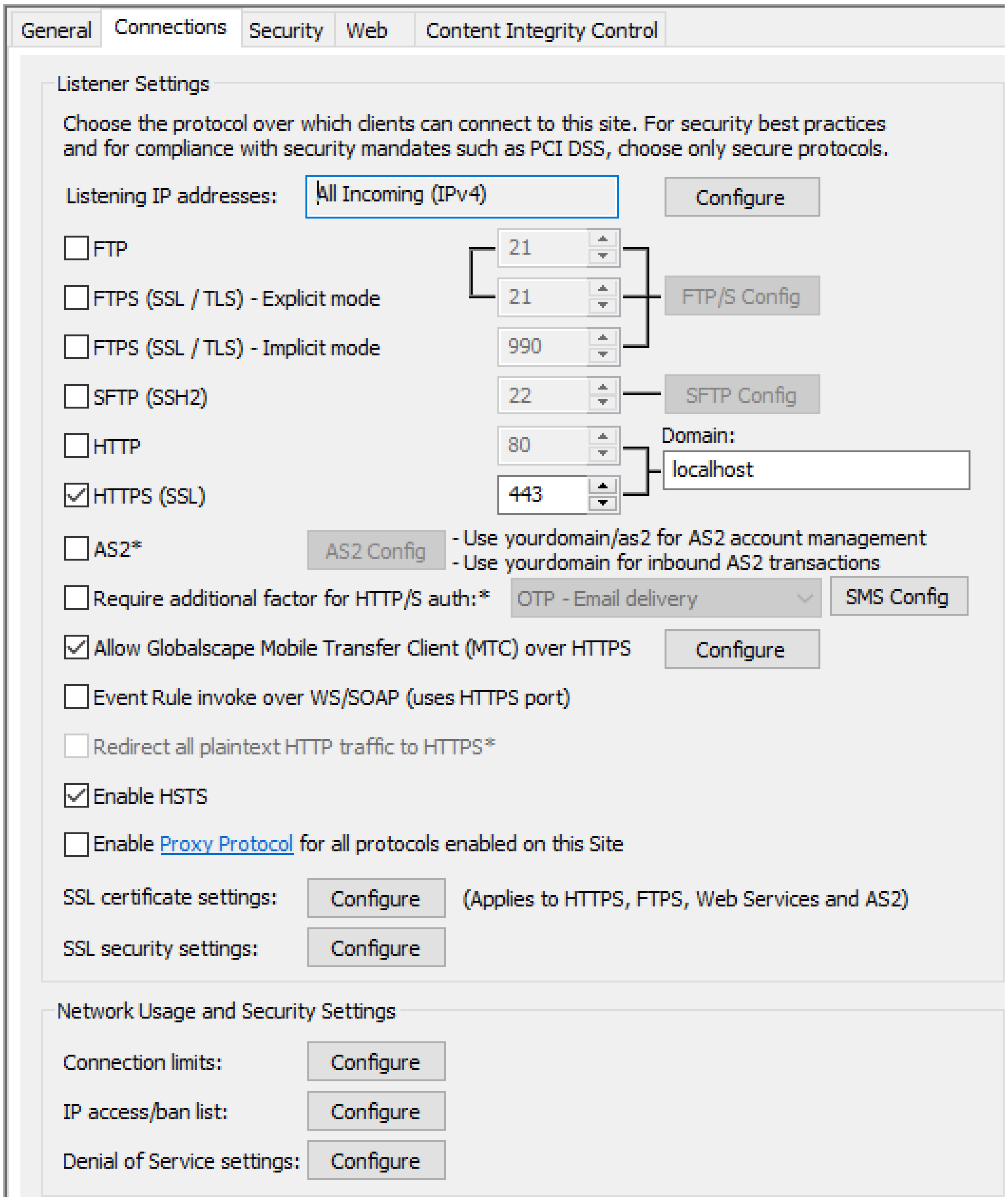
### How does MFA work in EFT?

1. When logging in to the WTC, if the **Require additional factor for HTTPS auth** check box is selected and configured (shown below), the WTC prompts for a passcode, and informs the recipient to check their email or text messages.
2. EFT generates a OTP and sends it in an email or text message to the recipient. (The user account details must be include their mobile phone number to use SMS; otherwise the email address is used. Therefore, for ad hoc interactions, you should specify email delivery of the OTP.)
3. The recipient checks email/text, and copies the passcode to the clipboard (or clicks the link).
4. The recipient pastes the passcode (or follows link) in the WTC.
5. If the passcode is verified, the WTC allows access.

### To enable and configure MFA

For SMS to work, you must first define an SMS profile on the **Site > Connections** tab. To enable MFA in Workspaces, refer to Enable and Configure Folder Sharing (Workspaces).

1. On the **Site > Connections** tab, enable and configure HTTPS, if not already done. (The MFA settings are inherited from the Site level, but you can enable or disable it on the Settings Template level also. You cannot enable/disable MFA at the user level.)
2. Select the **Require additional factor for HTTPS auth** check box. EFT does a quick scan of all users under that Site or Template, and if one or more users is found without an email address or mobile phone number defined, a prompt is displayed.



Listener Settings

Choose the protocol over which clients can connect to this site. For security best practices and for compliance with security mandates such as PCI DSS, choose only secure protocols.

Listening IP addresses: All Incoming (IPv4)

□ FTP 21

□ FTPS (SSL / TLS) - Explicit mode 21

□ FTPS (SSL / TLS) - Implicit mode 990

□ SFTP (SSH2) 22

□ HTTP 80

☑ HTTPS (SSL) 443

Domain: localhost

□ AS2* - Use yourdomain/as2 for AS2 account management - Use yourdomain for inbound AS2 transactions

□ Require additional factor for HTTP/S auth:* OTP - Email delivery

☑ Allow Globalscape Mobile Transfer Client (MTC) over HTTPS

□ Event Rule invoke over WS/SOAP (uses HTTPS port)

□ Redirect all plaintext HTTP traffic to HTTPS*

☑ Enable HSTS

□ Enable Proxy Protocol for all protocols enabled on this Site

SSL certificate settings: (Applies to HTTPS, FTPS, Web Services and AS2)

SSL security settings:

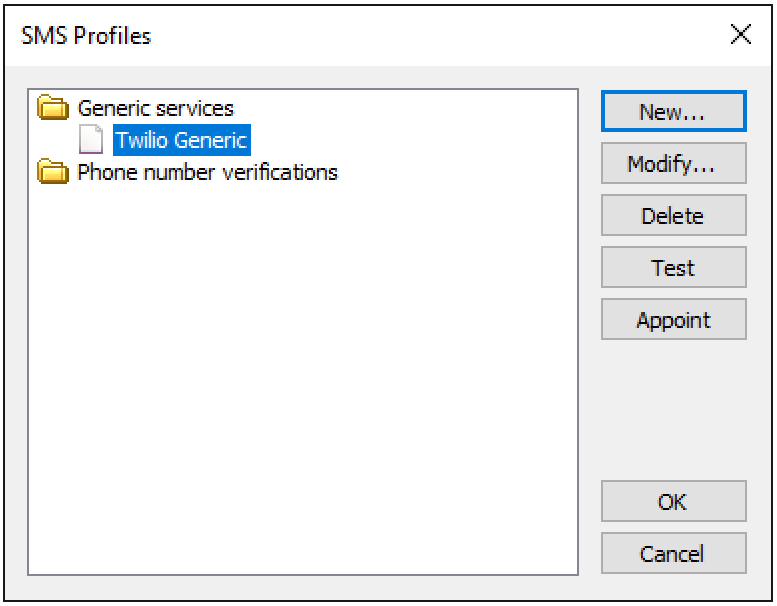
Network Usage and Security Settings

Connection limits:

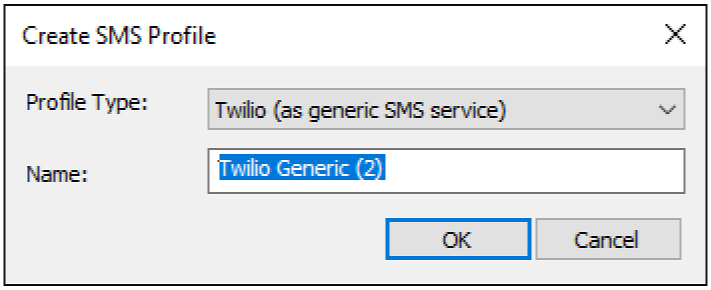
IP access/ban list:

Denial of Service settings:

3. Click the OTP drop-down list. In the **OTP** list, select the method of delivery:
   - **OTP - Email delivery** - EFT does not verify whether SMTP server configuration is completed correctly
   - **OTP - SMS delivery** - If no mobile number is available for the user, SMS delivery will fail.
   - **OTP - Try SMS then Email** - EFT first looks for mobile number in the user details. If no mobile number is defined, the email address is used.
4. To configure the Twilio for your SMS provider, use the settings provided when you set up your Twilio account. Click **SMS Configure**. If you chose SMS, the **SMS Profiles** dialog box appears:



   a. Click **New** to create a new profile.



Profile Type: Twilio (as generic SMS service)

Name: Twilio Generic (2)

   b. Click **Modify** to change a selected profile.
   c. Click **Appoint** to assign the selected profile to the Site.
5. Click **Test** to send yourself a test message.

6. Click **OK** to save the configuration.
7. In the **Message** box, leave it at the default or change the text, but keep the variable `%Account_Session_OTP%`. This variable is used by EFT to send the OTP.
8. Click **Test** to verify the connection. A message appears in which you can enter a mobile number to send a test message.
9. If the test is successful, click **OK**, then click **Apply** to save the configuration.
10. On the **Server > General Tab**, edit the **Authentication OTP message**, if needed.

### Important notes to consider

Multifactor activation is only applicable where account registration is required, and thus is not applicable to:

- Drop-off portal (no account is registered); Reply portal (you cannot reply unless you first pickup, which does require registration); Anonymous interactions (no account is registered)
- EFT skips 2FA for following user agents:
  - Anonymous ad hoc transfers (Send passcode via other means.)
  - Protocols other than HTTP/S
  - GlobalSCAPE-EFTApplet
  - JFileUpload
  - MSFT File Transfer Tool
  - EFT-Mobile-Client
  - Desktop Transfer Client
  - GlobalSCAPE-scClient
  - EFT-Outlook-Addin
  - Load Balancer Agent
  - ELB-HealthChecker/
  - EFT Remote Agent
  - When certain user-agents are defined (apply advanced property as described below).
- If MFA is enabled, then that additional factor (OTP) will be required and enforced by EFT. The exception to this rule is when the user-agent header is on EFT's list of special agent-headers (RAM agents, MTC, CuteFTP/9, OAI, etc.).
  - In addition, an advanced property override (**UserAgentHeaderSkipOTP**) is available so that administrators can add additional headers to the list, which would allow for non-Globalscape controlled clients (such as Fiddler, FileZilla, etc.) to connect over HTTPS but skip 2FA/MFA. If not defined in the advanced

property exclusion list or hard-coded exclusion list, then regardless of header, the additional factor will be required to complete authentication. For example:

For CuteFTP v9.3 or later, you could use the following advanced property to whitelist the user agent and connect successfully:

```
"UserAgentHeaderSkipOTP":"CuteFTP/9.3"
```

To skip the OTP for the Edge browser when OTP is enabled.

```
"UserAgentHeaderSkipOTP":"Edge/18.18363"
```

- If the OTP provided is incorrect, EFT will retry a few more times over a short period. If after all permitted retries have been exhausted, EFT will fail registration/verification, and the account will not be created nor associated with the Workspace, and all data will be discarded. (During the time when an “unverified” user is trying but failing to complete their verification, a “valid” user can still complete the registration/verification process.)

# Enabling User Access to the Web Transfer Client

**(Requires the HTTP/S module)** Before users can log in to EFT using the Web Transfer Client (WTC), EFT administrator must configure EFT to allow connections from the WTC. Active Directory domain users must have logon permission on EFT computer in order to log on to EFT through the WTC. This is accomplished by adding AD domain users to the "Allow log on locally" list on EFT computer. If an AD domain user is not in this list, logging on to EFT through the WTC will fail and an error message appears informing the user that Local login access is required to log on to EFT.

### Setting Defaults

The admin-configuration.json file is used to set defaults for all the WTC settings, providing better control over the end-user experience, such as upload limit, permissions, participant limit, and others. The file can be opened and edited in a text editor and is stored in the ..**\Web** directory. (The **\Web** directory is in the cluster share for HA installations.)

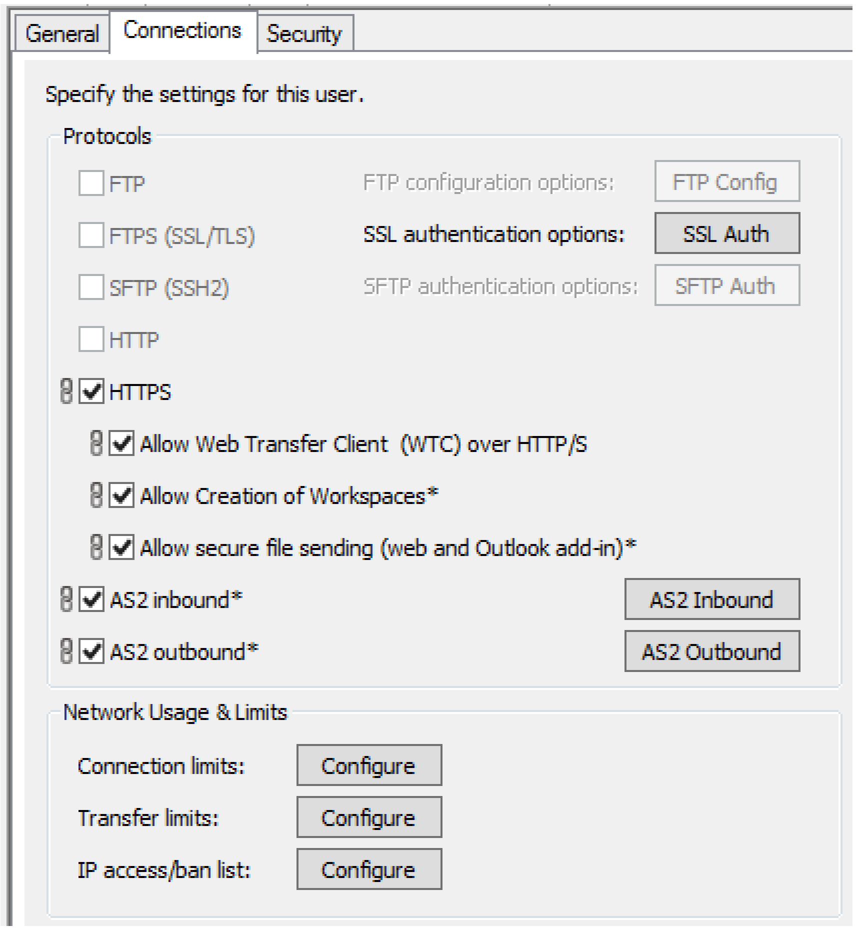
**\Web\Shadowfax\portal\assets\**

Refer also to Enable Multifactor Authentication for Workspaces

Stopping and restarting the Site disconnects everybody who is connected; users must log back in.

### To configure EFT to allow Web Transfer Client Connections

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, click the Settings Template or user account.
3. In the right pane, click the **Connections** tab.



General | Connections | Security

Specify the settings for this user.

Protocols

□ FTP — FTP configuration options: FTP Config

□ FTPS (SSL/TLS) — SSL authentication options: SSL Auth

□ SFTP (SSH2) — SFTP authentication options: SFTP Auth

□ HTTP

☑ HTTPS

☑ Allow Web Transfer Client (WTC) over HTTP/S

☑ Allow Creation of Workspaces*

☑ Allow secure file sending (web and Outlook add-in)*

☑ AS2 inbound* — AS2 Inbound

☑ AS2 outbound* — AS2 Outbound

Network Usage & Limits

Connection limits: Configure

Transfer limits: Configure

IP access/ban list: Configure

4. In the **Protocols** area, select the **Allow Web Transfer Client over HTTP/S** check box. HTTPS must also be enabled.

5. Click **Apply**.

# Enable and Configure Folder Sharing (Workspaces)

**(Requires HTTPS, Workspaces)** The Workspaces feature of EFT allows end users to share their folders with other users. The user account that is sharing the folder maintains control of permissions to the shared folder, and can revoke sharing privileges at any time. Workspaces provides the ability to easily share and collaborate on information that is securely managed by EFT, including existing authentication, access control, auditing, governance, and Event Rule workflow capabilities available in EFT.

If an unsigned or otherwise invalid certificate is used in the Chrome browser, downloads will fail, even if you add the certificate to your trusted list. To resolve this issue, use a valid, signed certificate. Alternatives include:

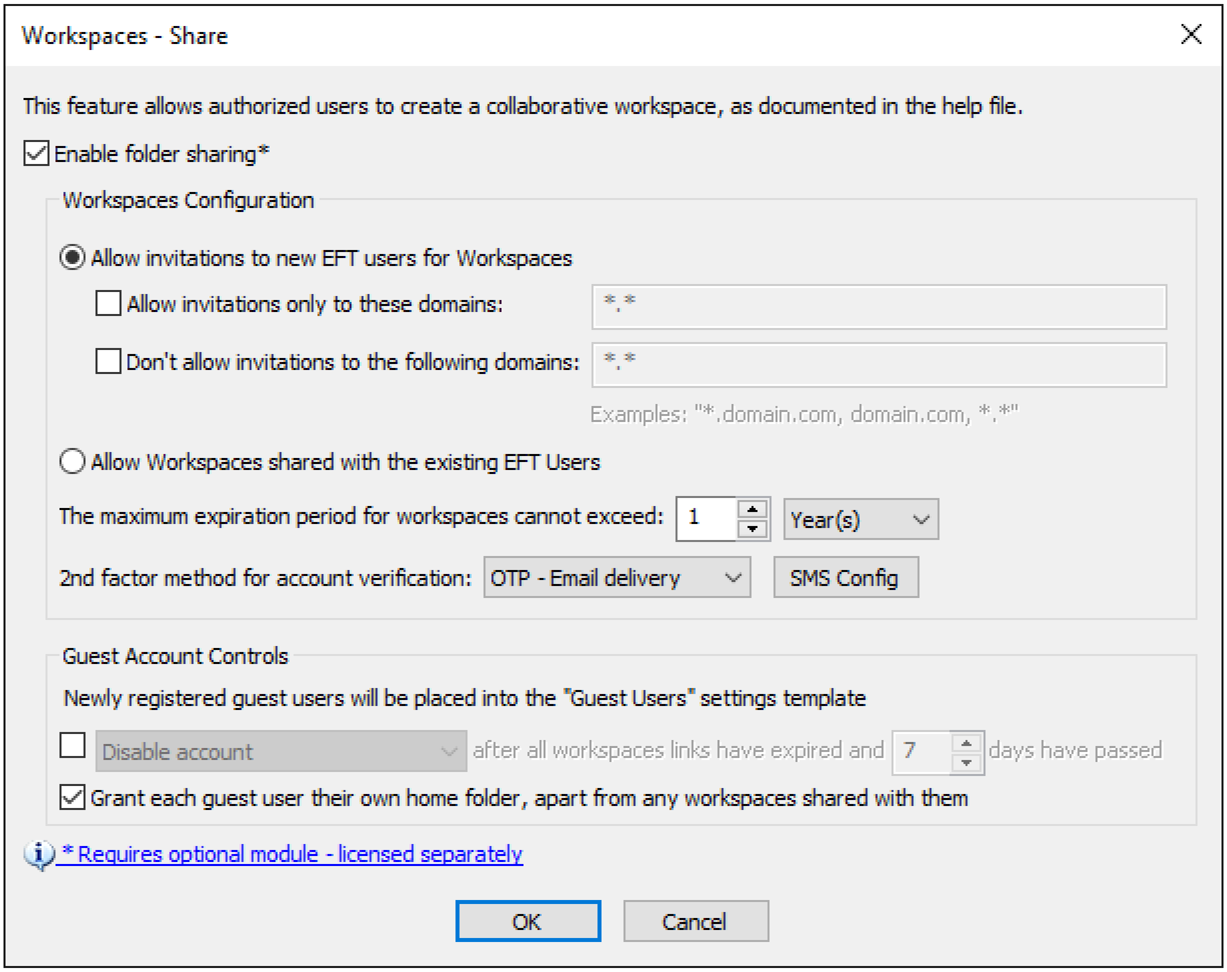
- Use a different browser
- Block downloads until you get a valid certificate
- Create a self-signed certificate outside of EFT, use a subject alternative name (SAN), then add the certificate to Chrome's trusted list.

Refer to Licensing Workspaces for important information regarding Guest Accounts.

### To enable Workspaces on the Site

(Refer to To enable Workspaces for a Settings Template or specific users below to disable/enable Workspaces for specific Settings Templates or users.)

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, click the Site you want to configure.
3. In the right pane, click the Web tab.
4. Next to **Folder sharing**, click **Configure**. The **Workspaces - Share** dialog box appears.



Workspaces - Share

This feature allows authorized users to create a collaborative workspace, as documented in the help file.

☑ Enable folder sharing*

Workspaces Configuration

● Allow invitations to new EFT users for Workspaces

□ Allow invitations only to these domains: *.*

□ Don't allow invitations to the following domains: *.*

Examples: "*.domain.com, domain.com, *.*"

○ Allow Workspaces shared with the existing EFT Users

The maximum expiration period for workspaces cannot exceed: 1 Year(s)

2nd factor method for account verification: OTP - Email delivery

Guest Account Controls

Newly registered guest users will be placed into the "Guest Users" settings template

□ Disable account after all workspaces links have expired and 7 days have passed

☑ Grant each guest user their own home folder, apart from any workspaces shared with them

* Requires optional module - licensed separately

5. Select the **Enable folder sharing** check box.
6. Under **Workspaces Configuration**, specify one of the following groups of users (any users or only existing EFT users) to whom users can send Workspaces invitations:
   - **Allow invitations to new EFT users for Workspaces**
     - (Optional) Select the **Allow invitations to these domains** check box, then specify the domains to which Workspaces users can send invitations, comma/semicolon delimited. Wildcards are supported (for example, *.domain.com or domain.com). The setting is not selected by default; that is, all domains *.* are allowed. (**Allow invitations to new EFT users for Workspaces** must be selected.) NOTE: Be sure wildcards are formatted correctly. That is, if you specify *.domain.com, then the domain www.domain.com is allowed.

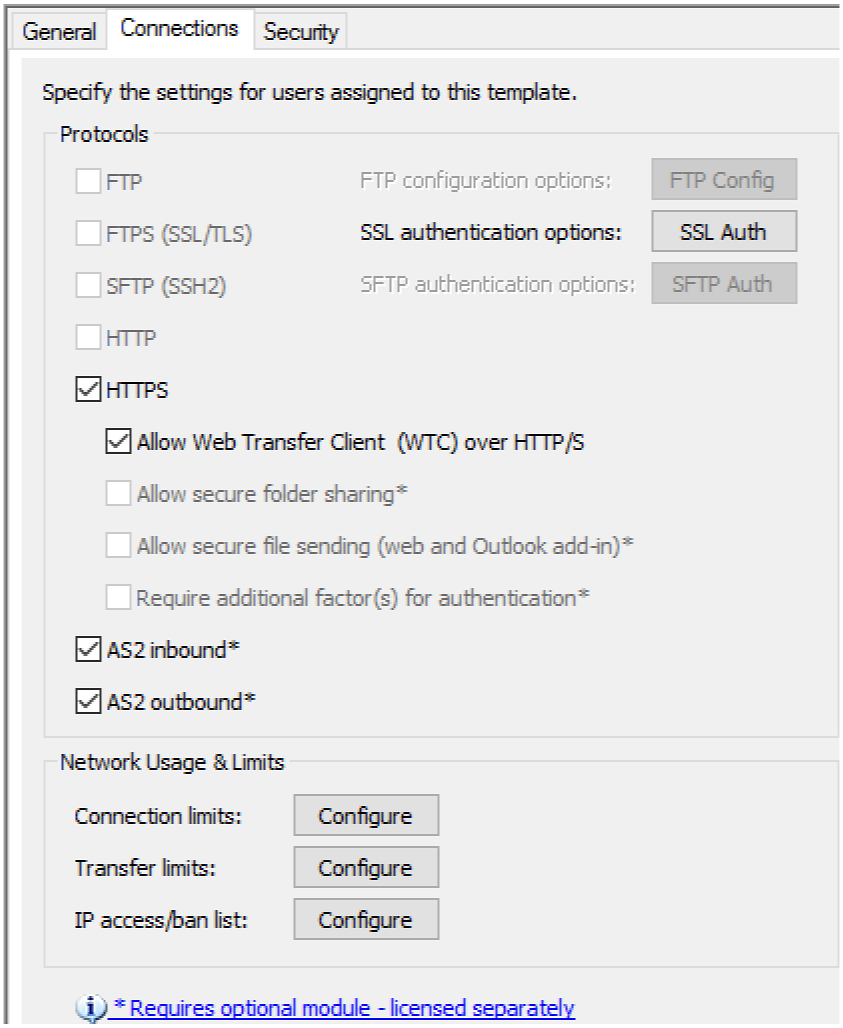
    - (Optional) Select the **Don't allow invitations to the following domains** check box, then specify the domains for which you do not want to allow access to Workspaces. The field is comma/semicolon delimited; wildcards are supported (for example, *.domain.com or domain.com). The setting is not selected by default; that is, no domains *.* are blocked. NOTE: Be sure wildcards are formatted correctly. That is, if you specify *.domain.com, then the domain www.domain.com is blocked.
  - **Allow Workspaces shared with existing EFT users**
    - On an LDAP-authenticated Site, when a sender types a recipient email to share a Workspace, if that email does not belong to a local (cached) account in EFT, EFT will extend its search to the LDAP authentication database.
  - Specify the **maximum expiration period** for a Workspace. Senders can set the expiration to happen sooner than what is defined on the server, but you cannot specify a longer period. (Refer to Enable Send Portal for information about retaining files after a Workspace link has expired.)
  - Specify **2nd factor method** for account verification (OTP) options. Refer to Enable Multifactor Authentication for directions.

7. Under **Guest Account Controls**:
   - Specify whether to **Disable account**, **Remove account and home folder**, or **Remove account only** after all Workspaces links have expired and *n* days have passed. When set to 0 days, the account(s) will be cleaned up at midnight. If the Guest account is disabled, the user will not be able to log in unless the EFT administrator enables or removes the account (and then the guest user would have to recreate their account). Refer to Workspaces Invitations for an example of using the **User Account** action to enable an expired Guest account.
   - To grant guest users their own home folder, select the **Grant each guest user their own folder** check box. Selecting the check box prevents guests from viewing other files in the Workspace's home folder.

     If the check box is ***not*** selected, the user has:
     - Read-only access to home folder.
     - List view of Workspaces with permissions as allowed by Workspaces owner, regardless of any protocols used to access the account.
8. Click **Apply** to save the settings.

### To enable Workspaces for a Settings Template or specific users

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, click the Settings Template or user account.
3. In the right pane, click the **Connections** tab.



Specify the settings for users assigned to this template.

Protocols

□ FTP — FTP configuration options: FTP Config

□ FTPS (SSL/TLS) — SSL authentication options: SSL Auth

□ SFTP (SSH2) — SFTP authentication options: SFTP Auth

□ HTTP

☑ HTTPS

☑ Allow Web Transfer Client (WTC) over HTTP/S

□ Allow secure folder sharing*

□ Allow secure file sending (web and Outlook add-in)*

□ Require additional factor(s) for authentication*

☑ AS2 inbound*

☑ AS2 outbound*

Network Usage & Limits

Connection limits: Configure

Transfer limits: Configure

IP access/ban list: Configure

* Requires optional module - licensed separately

4. In the **Protocols** area, select the **Allow secure folder sharing** check box. If this check box is not available, you have not activated the Workspaces licenses or the trial has expired; or you have not enabled Workspaces for the Site.

   HTTPS must also be enabled.

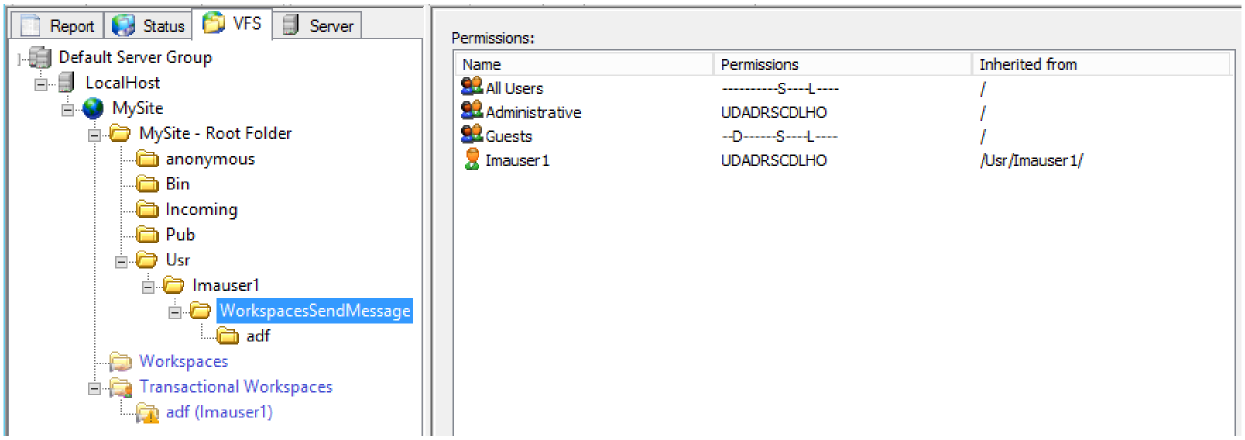
5. To also allow secure file sending in the WTC and in the Outlook add-in, ensure that the **Allow secure file sending** check box is selected.
6. (Optional) To enable additional authentication by email or SMS, select the **Require additional factor(s) for authentication** check box.
7. Click **Apply**.

# Enable and Configure the Send and Reply Portals

(Requires HTTPS, Workspaces) Workspaces is an enterprise ad hoc file transfer solution that allows employees to quickly and securely send large files from within the Web Transfer client or in Microsoft Outlook. Workspaces for Outlook allows organizations to address broad scale, risky file sharing practices while providing an easy-to-use interface for end users that requires little to no training from IT staff. Users benefit from an enhanced email experience with advance sending features, such as the ability to receive file pick up receipts. Recipients pickup their files in their web browser via a secure link. Administrators have the ability to manage user transactions behind the scenes, including the ability to set secure link expiration overrides and set policies for the automatic handling of exceedingly large file attachments.

- **MFA in the WTC** is disabled by default. Refer to Enable Multifactor Authentication for the WTC for instructions for enabling it.
- **MFA in Workspaces** is enabled by default. Refer to the procedure below for instructions for configuring it.
- To use Workspaces for Outlook, the EFT administrator must enable Workspaces and install and enable the EFT Outlook Add-In on end-users' computers, as described below.
- On the user account, the **Allow secure file sending** check box must be selected.
- When you send a file in the Web Transfer Client, a **WorkspacesSendMessage** folder is created under the sending user's home folder in the Virtual File System (VFS).

  Subfolders in the **WorkspacesSendMessage** folder are named for the Subject line of the message.

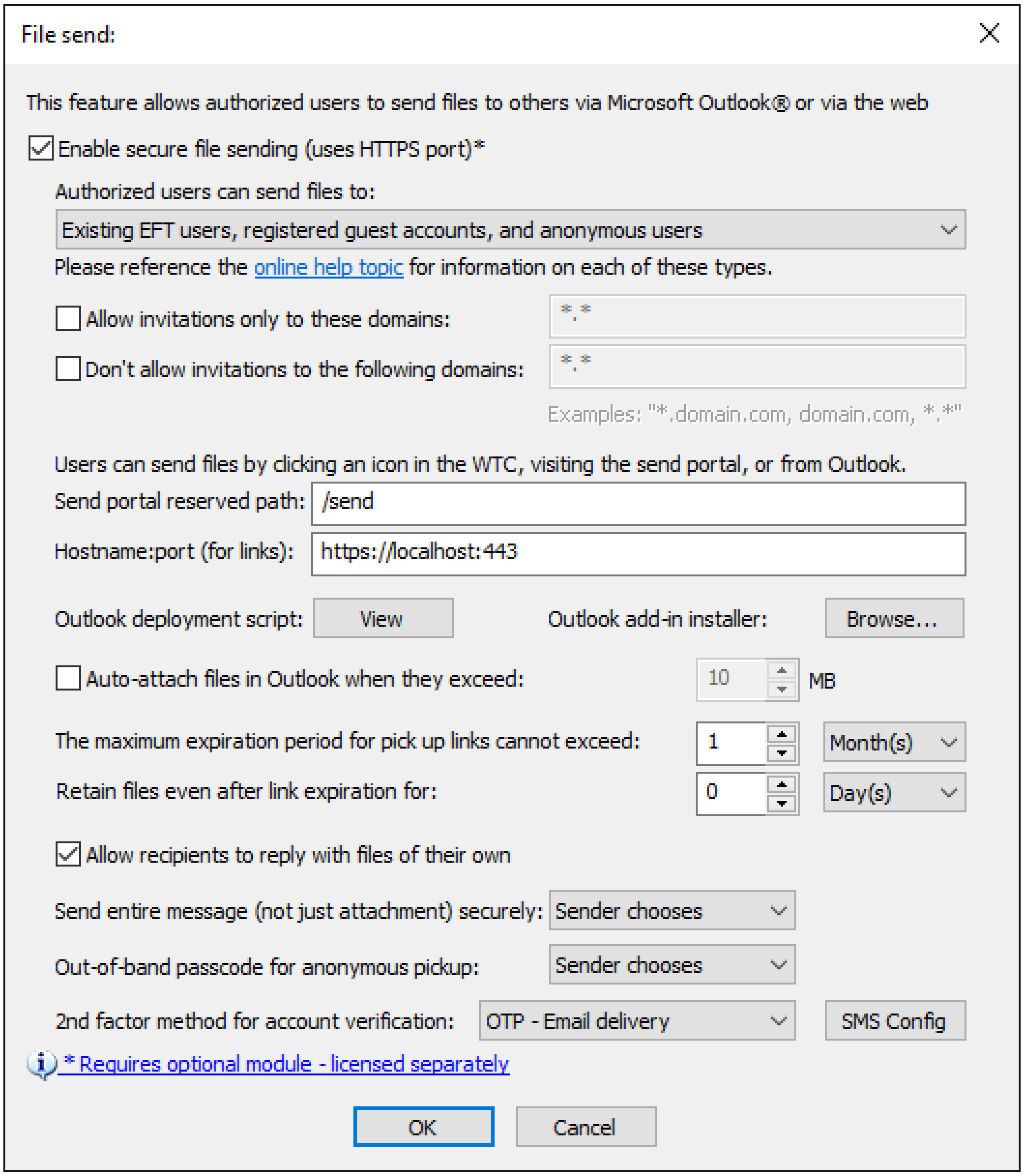


Permissions:

| Name | Permissions | Inherited from |
|---|---|---|
| All Users | ----------S----L---- | / |
| Administrative | UDADRSCDLHO | / |
| Guests | --D------S----L---- | / |
| Imauser1 | UDADRSCDLHO | /Usr/Imauser1/ |

### To enable Workspaces for sending files

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, click the Site you want to configure.
3. In the right pane, click the **Web** tab.
4. Next to **Send Portal,** click **Configure**. The **File send** dialog box appears.



File send:

This feature allows authorized users to send files to others via Microsoft Outlook® or via the web

☑ Enable secure file sending (uses HTTPS port)*

Authorized users can send files to:

Existing EFT users, registered guest accounts, and anonymous users

Please reference the online help topic for information on each of these types.

☐ Allow invitations only to these domains: *.*

☐ Don't allow invitations to the following domains: *.*

Examples: "*.domain.com, domain.com, *.*"

Users can send files by clicking an icon in the WTC, visiting the send portal, or from Outlook.

Send portal reserved path: /send

Hostname:port (for links): https://localhost:443

Outlook deployment script: View

Outlook add-in installer: Browse...

☐ Auto-attach files in Outlook when they exceed: 10 MB

The maximum expiration period for pick up links cannot exceed: 1 Month(s)

Retain files even after link expiration for: 0 Day(s)

☑ Allow recipients to reply with files of their own

Send entire message (not just attachment) securely: Sender chooses

Out-of-band passcode for anonymous pickup: Sender chooses

2nd factor method for account verification: OTP - Email delivery

5. Select the **Enable secure file sending** check box. This requires the HTTPS port to be configured and available.
6. Under **Authorizedusers can send files to**, select one of the following options:

- **Existing EFT users only (most restrictive)** - Allows EFT users to send files via Workspaces for Outlook only to other users with an EFT account
- **Existing EFT user and registered guest accounts** - Allows EFT users to send files via Workspaces for Outlook to other EFT user accounts and registered guest accounts
- **Existing EFT users, registered guest accounts, and anonymous users** - Allows EFT users to send files via Workspaces for Outlook to other EFT user accounts, registered guest accounts, and non-EFT user accounts. Non-EFT user accounts do not require credentials, making it easy for the recipient to pick up files, but makes the system less secure. To reduce this risk, the sender can make the pickup link "single use."

  Transactional Workspaces folders in the VFS that are shared with unregistered users will have an exclamation point on the anonymous-access folder.

7. In the **Send portal reserved path** box, specify the path for the **Send** portal. The default is **/send**.
8. In the **Hostname:port** box, specify the URL for file pick up. By default, this box will contain the same IP as the Domain box on the **Site > Connections** tab, but you can change it to an external-facing hostname, if needed (and if so configured in your network). Links that are sent for Workspaces invitations and file sharing will have this URL.
9. For using the Outlook deployment script or Add-In installer, refer to Deploy Outlook Add-In on End-User's Computers.
10. To require the use of Outlook for large files, select the **Auto-attach files in Outlook when they exceed** check box, and then specify a size.
11. Specify the **maximum expiration period for pickup links**. The default is 1 month.
12. Specify the length of time to **Retain files after link expiration**. The default is 0 days.
    - This value indicates the length of time between Workspace expiration and file removal, and cannot exceed **maximum expiration period**, above. On expiration, a "Workspace expired" Event is triggered and the Workspace becomes invisible to the administrator, owner, and participants, but the directory and files remain alive. At the end of the retention period, a "Workspace removed" Event is triggered, the Workspace information is wiped from EFT configuration, and the directory is physically removed from the file system. For example, if a transactional (guest user) Workspace is created to expire in 10 days and retain file for 10 days, if the Workspace expired on October 1, it will then be removed from disk on October 11.

13. Select the **Allow recipients to reply with files of their own** check box to allow people that you send file to reply with files of their own. Then you must enable the Request file page to specify the **Reply** path.

    After a recipient has received a message sent through Workspaces, the recipient can reply to the email in the Workspaces Reply Portal (if so configured) and send files back to the sender. If you do not want to allow that functionality, you can disable replies. Disabling the Reply portal removes the request files functionality from the Web Transfer Client interface.

14. Next to **Send entire message (not just attachment) securely**, click the **Sender chooses** drop-down list and click an option:
    - **Always secure** - Always send message and attachment securely
    - **Never secure** - Never send message and attachment securely
    - **Sender chooses** - Sender can choose whether to send message and attachment securely
15. **For anonymous recipients**: Next to **Out-of-band passcode for anonymous pick up**, specify whether a recipient requires a passcode to pick up files. Click the drop-down list and then click **Required** (sender must require a passcode), **Not required** (sender does not have to require a passcode), or **Sender chooses** (whether to require a passcode). (The sender's authentication options appear in the **Options** dialog in Workspaces.) When an out-of-band passcode is required, the passcode will appear for the sender after the message is sent. The sender then must provide the recipient the passcode via a non-Workspaces method (for example, phone, email, SMS, or message app).
16. Next to **2nd factor method for account verification**, click the list to choose one of the methods of delivery for the OTP:
    - **OTP - Email delivery** - EFT does not verify SMTP server configuration
    - **OTP - SMS delivery** - If no mobile number is available for the user, SMS delivery will fail.
    - **OTP - try SMS then Email** - EFT first looks for mobile number in the user details. If no mobile number is defined, the email address is used.

      Refer to Enable Multifactor Authentication for details of configuring SMS options, such as Twilio.
17. Click **OK**, then click **Apply** on the **Web** tab.

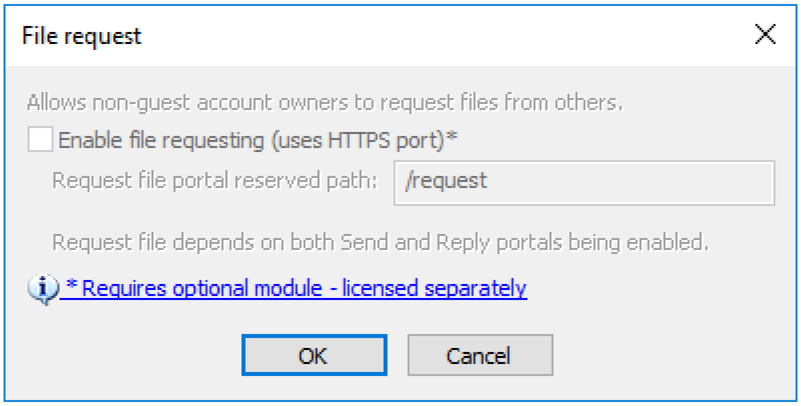
# Enable and Configure the Request File Portal

**(Requires HTTPS, Workspaces)** After you enable the Send and Reply portals, then you can enable the Request file portal and specify the **Request file portal reserved path** as described in the procedure below.

The Request file portal requires that the HTTPS port is enabled, as well as both the Send and Reply portals. (Select the **Allow recipients to reply with files of their own** check box in the **File Send** dialog box.)

### To enable the Request file portal

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, click the Site you want to configure.
3. In the right pane, click the **Web** tab.
4. Next to **Request file portal,** click **Configure**. The **File request** dialog box appears.



Allows non-guest account owners to request files from others.

□ Enable file requesting (uses HTTPS port)*

Request file portal reserved path: /request

Request file depends on both Send and Reply portals being enabled.

* Requires optional module - licensed separately

5. Select the **Enable file requesting** check box, then specify the reserved path.
6. Click **OK.**

# Enable and Configure the Drop-Off Portal

**(Requires HTTPS, Workspaces)** The Workspaces Drop-Off portal allows employees and partners to send files to internal users, with no attachment limits. The transfer of the email and attachments is encrypted and secure. The Drop-Off portal is configured at the Site level on the **Web** tab.

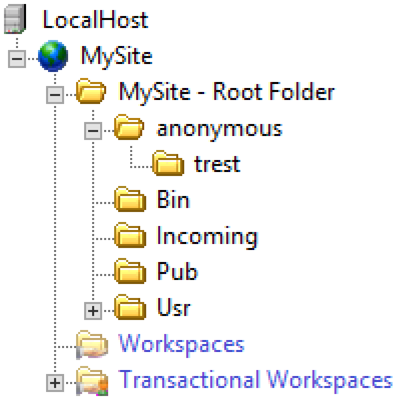
**A Workspaces license is consumed for each Drop-off portal message** no matter how many recipients the message has.

A Workspaces license is **not** consumed on replies.

A Workspaces license is **not** consumed on Send Portal messages.

You can avoid Workspaces licenses being consumed by the Drop-off portal by disabling the Drop-off portal. It is not enabled by default.

When someone uses the drop-off portal, that "someone" becomes a "Workspaces owner." This is because behind the scenes, a temporary, anonymous account is created to host the Workspace, thus consuming a license (assigned to that account). A folder, named with the Subject line of the email, appears under the **anonymous** folder in the VFS. Once the Workspace expires, the anonymous account is also removed, and the license is released to the pool.

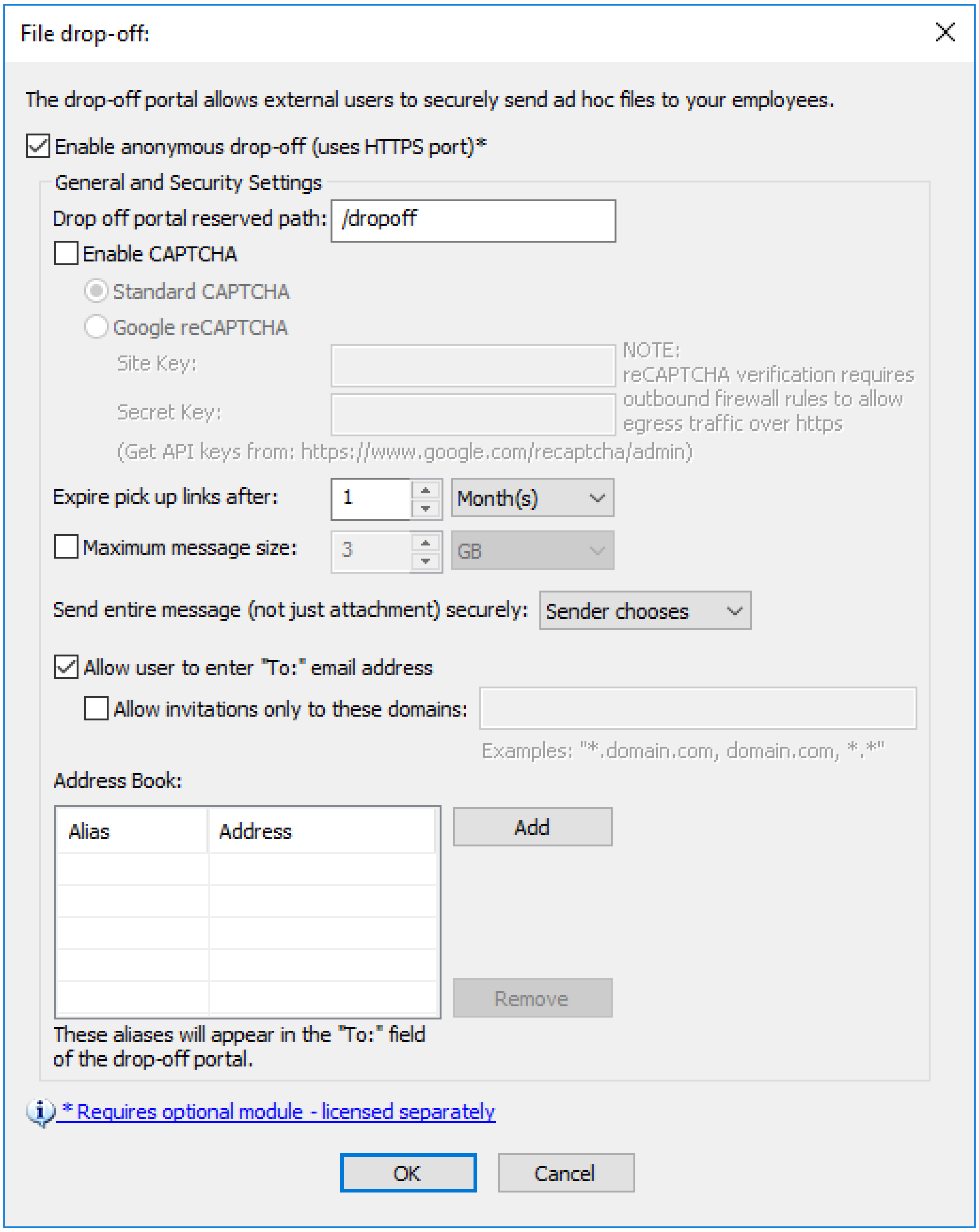


- For additional security, you can configure Google's reCAPTCHA on the Site, as described below.
- You will need to add Google's domain to the Content-Security-Policy (CSP) header for reCAPTCHA to work. Refer to https://kb.globalscape.com/KnowledgebaseArticle11435.aspx for details.

- Instruct Workspaces users that they must complete the CAPTCHA ***before*** they attempt to attach files to the portal. Otherwise, the files won't attach.

### To enable the Drop-Off portal

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, click the Site you want to configure.
3. On the **Web** tab, next to **Drop-Off portal**, click **Configure**. The **File drop off** dialog box appears.



File drop-off:

The drop-off portal allows external users to securely send ad hoc files to your employees.

☑ Enable anonymous drop-off (uses HTTPS port)*

General and Security Settings

Drop off portal reserved path: /dropoff

□ Enable CAPTCHA

● Standard CAPTCHA

○ Google reCAPTCHA

Site Key:

Secret Key:

NOTE:
reCAPTCHA verification requires outbound firewall rules to allow egress traffic over https

(Get API keys from: https://www.google.com/recaptcha/admin)

Expire pick up links after: 1 Month(s)

□ Maximum message size: 3 GB

Send entire message (not just attachment) securely: Sender chooses

☑ Allow user to enter "To:" email address

□ Allow invitations only to these domains:

Examples: "*.domain.com, domain.com, *.*"

Address Book:

| Alias | Address |
|---|---|

These aliases will appear in the "To:" field of the drop-off portal.

* Requires optional module - licensed separately

4. Select the **Enable anonymous drop-off** check box. This requires the HTTPS port to be configured and available.
5. Specify a portal reserved path if you want something different from the default (/dropoff). The hostname:port are configured in the File Send dialog box.
6. (Optional) To use captcha, select the **Enable CAPTCHA** check box.
   a. Specify whether to use **Standard CAPTCHA** or **Google reCAPTCHA**. reCATCHA verification requires outbound firewall rules to allow egress traffic over HTTPS.
   b. If you click **Google reCAPTCHA**, refer to the reCAPTCHA procedure below, then specify the following keys:
      - In the **Site Key** box, paste the Google Site Key.
      - In the **Secret Key** box, paste the Google Secret Key.

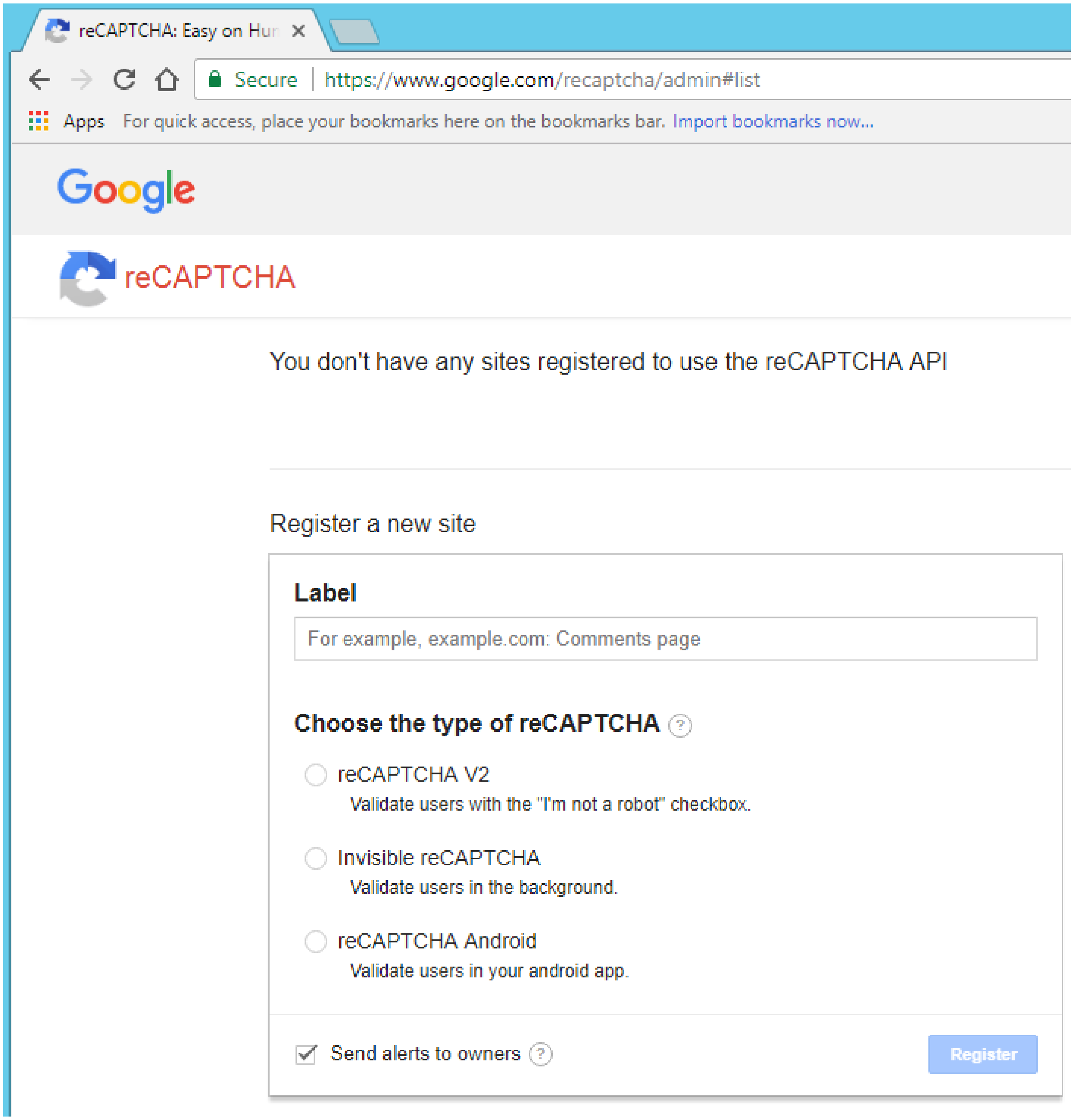
   If the Drop-Off portal is enabled, and Google reCAPTCHA is enabled, a prompt appears. You will need to add Google's domain(s) to the Content-Security-Policy (CSP) header for reCAPTCHA to work. Refer to https://kb.globalscape.com/KnowledgebaseArticle11435.aspx in the Globalscape Knowledgebase for instructions.
7. In the **Expire pick-up links after** boxes, specify the number of **Days**, **Weeks**, **Months**, or **Years** before a pick-up link expires. Be aware that using the Drop-Off portal consumes a Workspaces license, which is not released until the link expires. The default expiration is 1 month.
8. (Optional) Specify the **Maximum message size**. If the **Maximum message size** check box is not selected, the maximum message size is 3 GB. Knowledgebase article #11389 describes an advanced property that you can use to set the maximum anonymous uploads size in GB. If the **MaxAnonymousAllUploadsSizeInGB** advance property is set to a value that is LESS than **Maximum message size** in the **File drop-off** dialog box, an error occurs stating that the file is too large.
9. Specify the **Secure the message body** setting: **Always secure**, **Never secure**, or **User Choice**. **User Choice** is the default.
10. (Optional) Specify whether to allow users to enter a **To** email address.
    - If you are allowing users to enter a To email address, specify which domains are allowed (for example, *.mycompany.com, *.mypartner.com). If you leave the box blank, you have an "open-relay" server, which is not recommended. Suggested domains include your organizational domain(s) and other necessary domains.
11. In the **Address Book**, add one or more addresses and aliases that will appear in the **To** field.

- The **Alias** that you define in the address book will appear in the To box in the Drop-Off portal. Having the alias avoids leaving the complete email address exposed. This is useful in cases such as if you are mailing a PDF form to multiple clients who might not want you to share their email address with everyone.

12. Click **OK**, then click apply on the **Web** tab.

### To configure reCAPTCHA for the Drop-Off portal

1. If you want to enable CAPTCHA, before you enable and configure the Drop-Off portal, go to https://www.google.com/recaptcha/administrator and log in to your Google account.



reCAPTCHA: Easy on Hur
Secure
https://www.google.com/recaptcha/admin#list
Apps
For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...
Google
reCAPTCHA

You don't have any sites registered to use the reCAPTCHA API

Register a new site

**Label**

For example, example.com: Comments page

**Choose the type of reCAPTCHA** ?

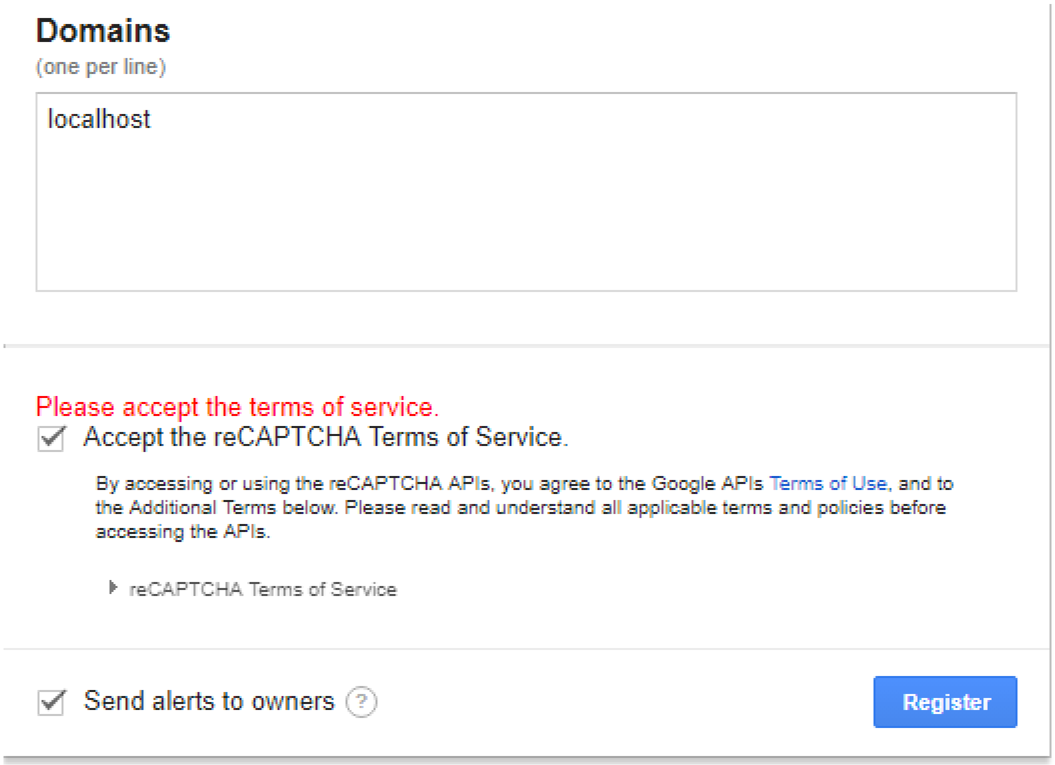
○ reCAPTCHA V2
Validate users with the "I'm not a robot" checkbox.

○ Invisible reCAPTCHA
Validate users in the background.

○ reCAPTCHA Android
Validate users in your android app.

☑ Send alerts to owners ?

2. Click **reCAPTCHA v2**. The **Domains** box appears.



**Domains**
(one per line)

localhost

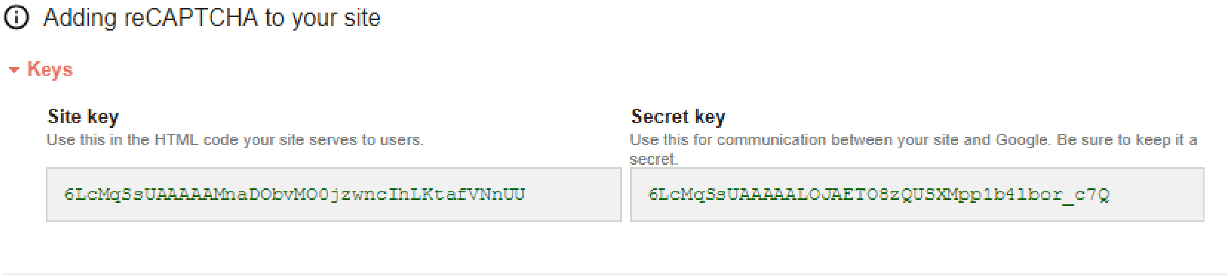
Please accept the terms of service.
☑ Accept the reCAPTCHA Terms of Service.

By accessing or using the reCAPTCHA APIs, you agree to the Google APIs Terms of Use, and to the Additional Terms below. Please read and understand all applicable terms and policies before accessing the APIs.

▸ reCAPTCHA Terms of Service

☑ Send alerts to owners

3. In the **Domains** box, type one or domains (Sites) that are to use reCAPTCHA.
4. Select the **Terms of Service** check box.
5. Click **Register**. The keys appear.



**Site key**
Use this in the HTML code your site serves to users.

```
6LcMqSsUAAAAAMnaDObvMO0jzwncIhLKtafVNnUU
```

**Secret key**
Use this for communication between your site and Google. Be sure to keep it a secret.

```
6LcMqSsUAAAAALOJAETO8zQUSXMpp1b4lbor_c7Q
```

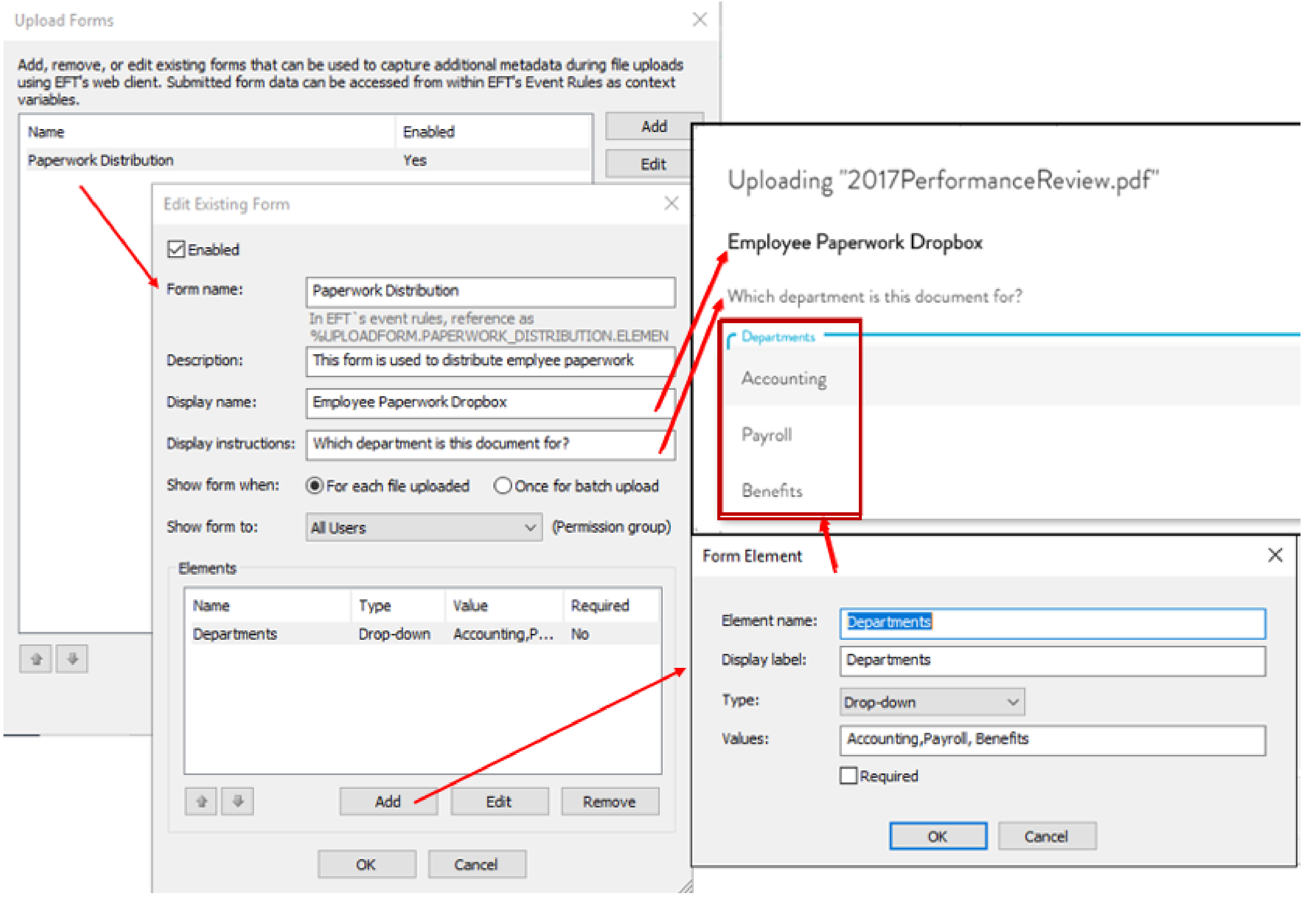
6. Save the Site key and Secret key. You will need these to configure the Drop-Off portal in EFT if you are enabling CAPTCHA.

# Upload Forms

(Requires SFM) Upload forms are custom web forms you can create to capture metadata during file uploads when using the web client. Metadata gathered by the upload form can be used in downstream event rules (that is, subsequent Actions) for conditional post processing.

**How does it work?** Upon initiating an upload of a file or batch of files, and if configured to do so, EFT will prompt the end user to complete one or more forms that you created. Upon completing and submitting the form, the web client will complete the upload. EFT administrators can now access and use the form data within EFT event rules as you would any other context variables. If required fields aren't completed or the user declines the form, the upload is aborted.

**When would I use upload forms?** Suppose you have an electronic drop box that collects files from employees that need to be routed to the correct department: Accounting, Payroll, and Benefits. With Upload forms, you could create a form that includes a drop-down list with values for Accounting, Payroll, and Benefits, as shown in the illustration below.



Upload Forms

Add, remove, or edit existing forms that can be used to capture additional metadata during file uploads using EFT's web client. Submitted form data can be accessed from within EFT's Event Rules as context variables.

| Name | Enabled |
|---|---|
| Paperwork Distribution | Yes |

Edit Existing Form

☑ Enabled

Form name: Paperwork Distribution

In EFT`s event rules, reference as %UPLOADFORM.PAPERWORK_DISTRIBUTION.ELEMEN

Description: This form is used to distribute emplyee paperwork

Display name: Employee Paperwork Dropbox

Display instructions: Which department is this document for?

Show form when: ● For each file uploaded ○ Once for batch upload

Show form to: All Users (Permission group)

Elements

| Name | Type | Value | Required |
|---|---|---|---|
| Departments | Drop-down | Accounting,P... | No |

Uploading "2017PerformanceReview.pdf"

Employee Paperwork Dropbox

Which department is this document for?

Departments

- Accounting
- Payroll
- Benefits

Form Element

Element name: Departments

Display label: Departments

Type: Drop-down

Values: Accounting,Payroll, Benefits

□ Required

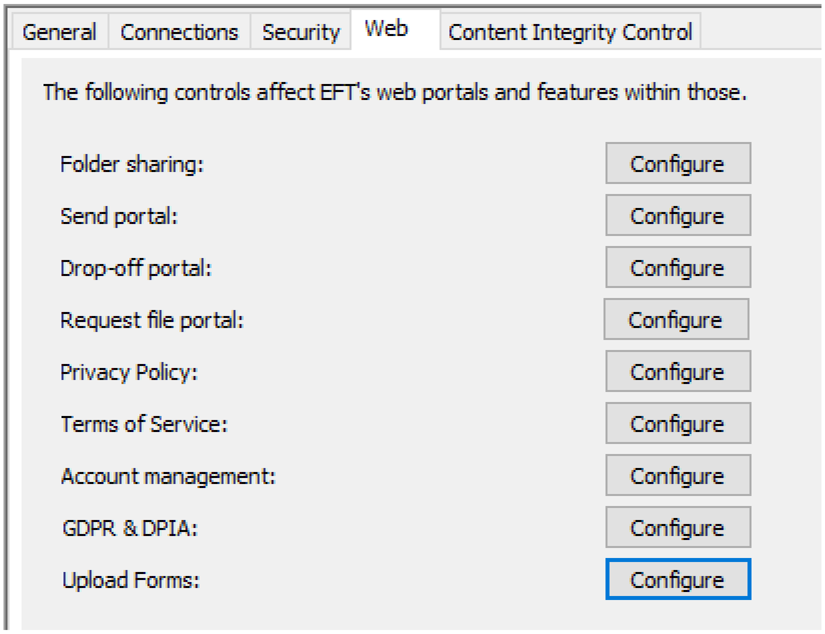
In EFT's **File Upload** event rule, you would conditionally disposition uploaded documents to the appropriate department (or perform other, department-specific operations) by adding the "If %Context_Variable% does equal to string" conditional statement. The name of the upload form context variable is a combination of "uploadform" followed by the form name and element name, in the following format: `%Uploadform.Form_name.Element_name%`.

In the example above, the context variable that references the Departments values would be: `%uploadform.Paperwork_Distribution.Departments%`. (If you have spaces in the Form name or Element name, replace the spaces with underscores.)

## How do I create upload forms?

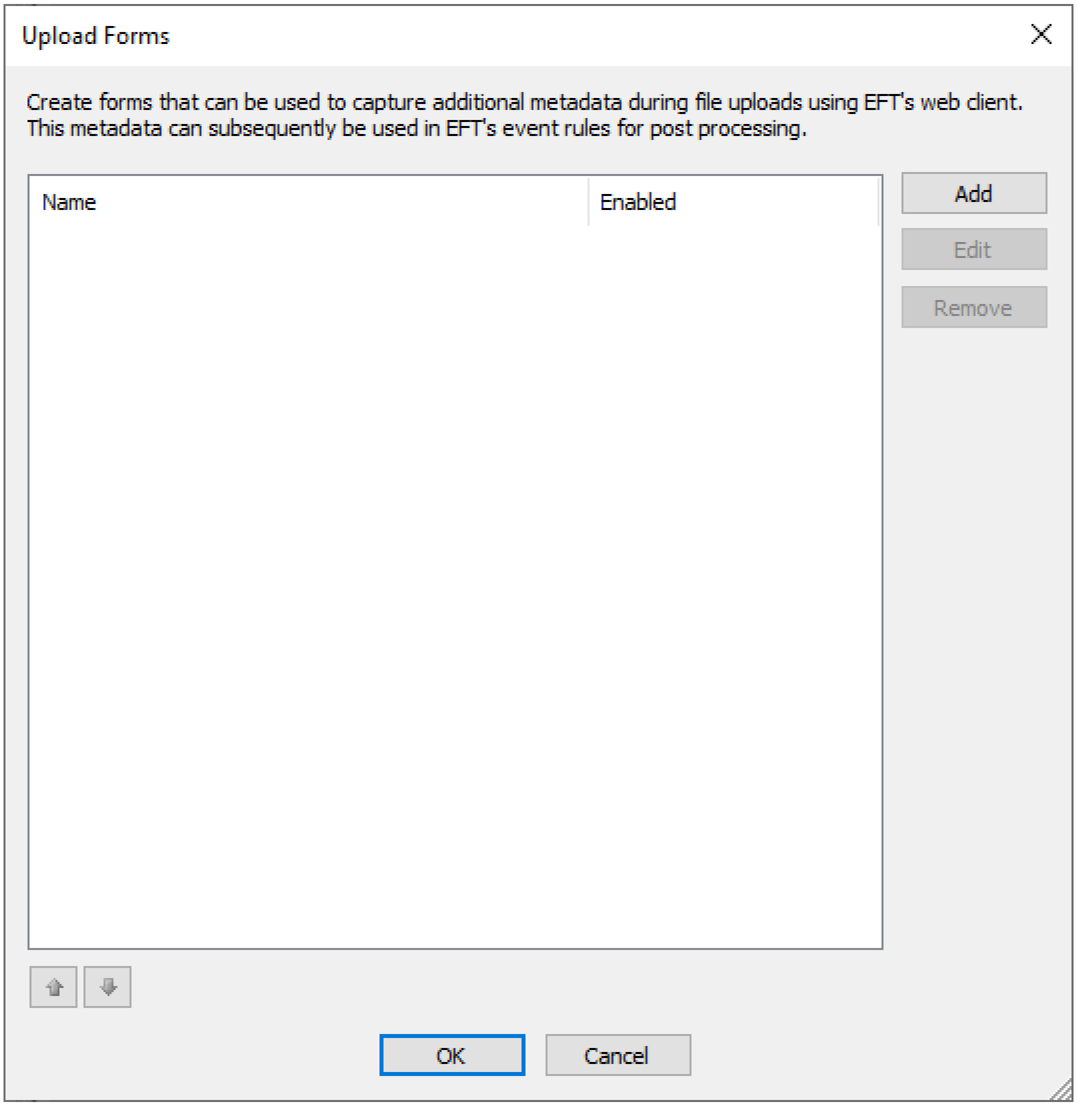
### To create a form

1. In the administration interface, connect to EFT and in the left pan, click the **Site**.
2. In the right pane, click the **Web** tab.



The following controls affect EFT's web portals and features within those.

3. Next to Upload Forms, click **Configure**. The **Upload Forms** dialog box appears.

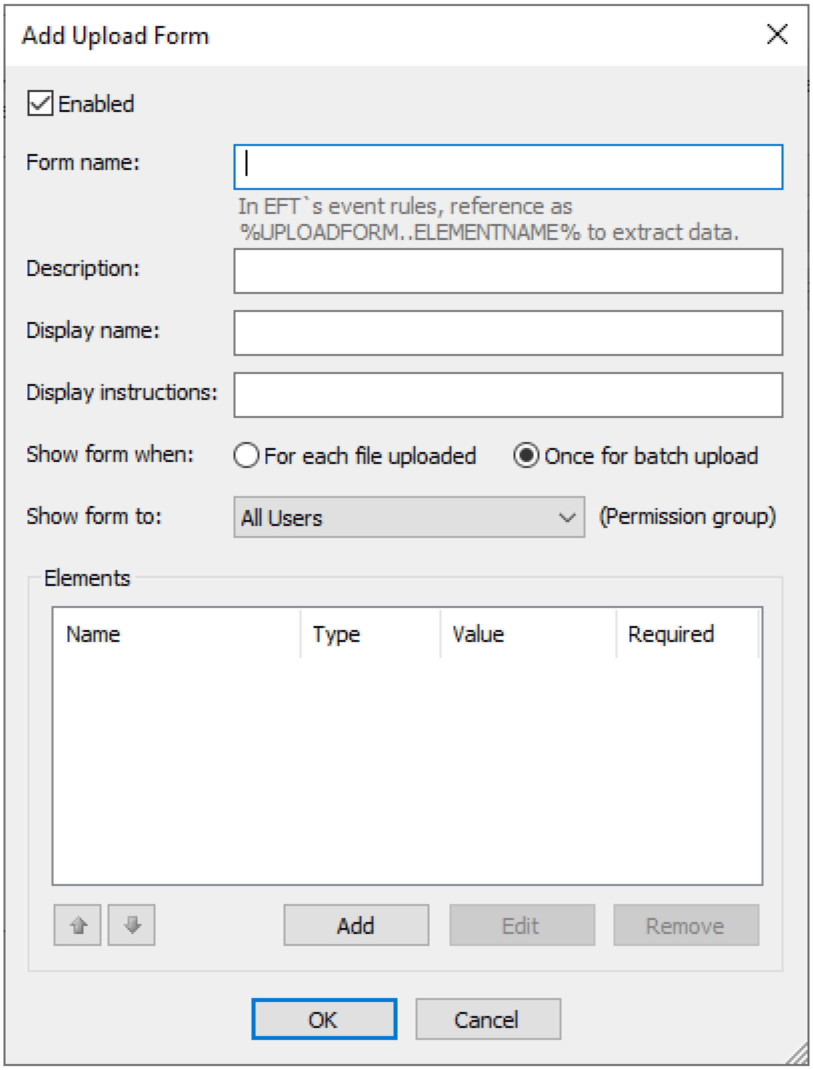


Upload Forms

Create forms that can be used to capture additional metadata during file uploads using EFT's web client. This metadata can subsequently be used in EFT's event rules for post processing.

4. In the **Upload Forms** dialog box, you can **Add**, **Edit**, or **Remove** a form. You can also sort them using the arrow icons in the lower left.

5. To add a form, click **Add**. The **Add Upload Form** dialog box appears.



Add Upload Form

☑ Enabled

Form name:

In EFT`s event rules, reference as %UPLOADFORM..ELEMENTNAME% to extract data.

Description:

Display name:

Display instructions:

Show form when: ○ For each file uploaded ● Once for batch upload

Show form to: All Users (Permission group)

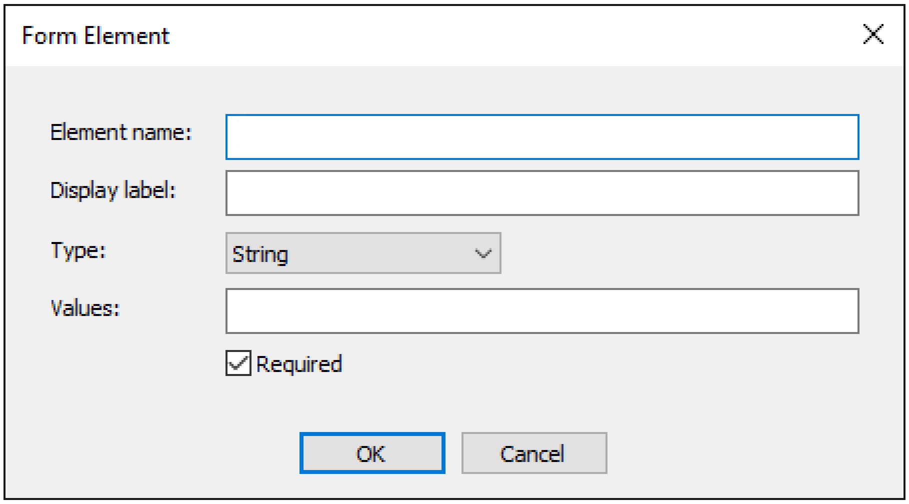
Elements

| Name | Type | Value | Required |
|---|---|---|---|

The **Enabled** check box is selected by default. If the check box is cleared, the form will not appear in the WTC.

6. In the **Form name** box, provide a unique name for the Upload Form.
7. (Optional) In the **Description** box, provide a description/purpose for this Upload Form.
8. In the **Display name** box, provide a name for the Upload Form that will appear in the WTC.
9. (Optional) In the **Display instructions** box, provide instructions for completing the form that will appear in the WTC.
10. Next to **Show form when**, specify whether to display the form **For each file uploaded**, or **Once for a batch upload**. The latter is useful if the metadata being provided will apply to all the files being uploaded as part of the batch.

11. Next to **Show form to,** specify the Permission Group that will see the form. If you need to show the form to a single user or small handful of users, you will need to create a Permission Group for those. If your Site is using Active Directory authentication (and authorization) then everyone will see the form, as currently there are no controls for only displaying the form to individual users.
12. The **Elements** section lists any added elements in the order they will be shown in the web form. You can change the order of the elements using the arrows, **Add** or **Remove** elements, or **Edit** existing elements. When editing or adding elements, the **Form Element** dialog box appears.



Form Element

Element name:

Display label:

Type: String

Values:

☑ Required

   a. In the **Element name** box, provide an element name (unique to this form) to be used as context variable name (defaults to field label). This value will be used by EFT's event rules as the "Element_Name" portion of the %UploadForm.Form_Name.Element_Name% variable.
   b. In the **Display label** box, provide a label associated with the element. This is displayed in the web form. (Form Elements must have labels to be in compliance with Section 508 standards for people with disabilities.)
   c. In the **Type** box, specify what type of value is used for the element: Drop-down list, Multistring, Radio buttons, String, or check box (Toggle).
   d. In the **Values** box, specify any values to appear for the drop-down list, radio buttons, or toggle names. Use commas to delimit multiple values.
   e. Select the **Required** check box, if this form is mandatory.
   f. Click **OK** to save the Element. If one or more mandatory fields is missing or invalid, a prompt appears: "One or more errors were encountered. Please enter all valid, required information and try again."
13. Create other Elements as needed.
14. Click **OK** to close the **Add New Form** dialog box.

15. Click **OK** to close the **Upload Forms** dialog box.
16. Click **Apply** to save the changes.

# GDPR Settings

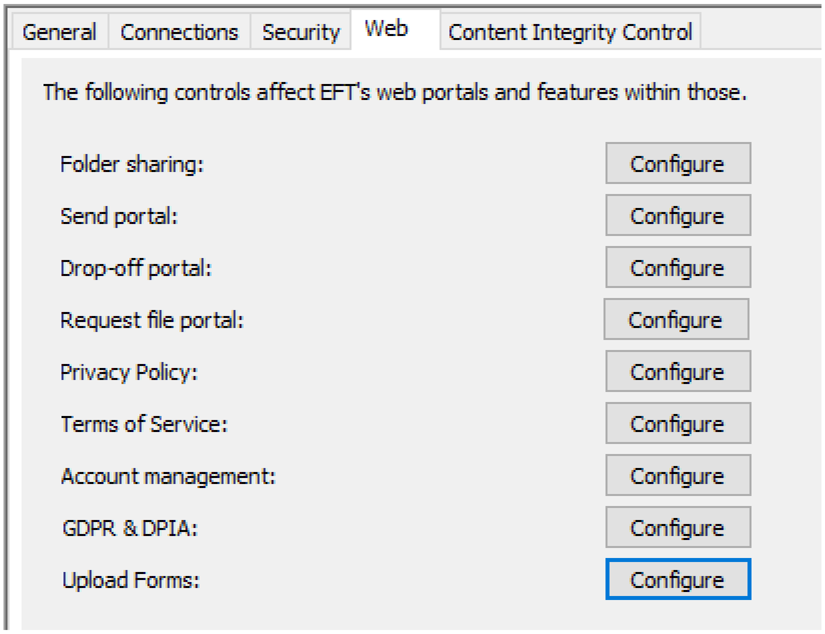
**(Requires Regulatory Compliance Module)** The General Data Protection Regulation (GDPR) is a part of European Union (EU) law regarding data protection and privacy in the EU and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas. The GDPR's primary aim is to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. The GDPR applies to any enterprise—regardless of its location and the data subjects' citizenship or residence—that is processing the personal information of data subjects. The GDPR Settings in EFT can also be used to address other privacy regulations, such as California's CCPA and HIPAA.

EFT and the Web Transfer Client provide settings so that you can address each relevant article in the GDPR for those who access EFT and the Web Transfer Client. For example, the "Right to be Forgotten" (delete account) is part of the GDPR's data privacy rules. A user can exercise their right to be forgotten in their account profile, if the EFT administrator has configure Article 17 to be "Exercised via EFT's web client."

**When the module expires,** the **GDPR Settings** dialog box is grayed out. However, you can still create Event Rules to an EU Data Subject's status, such as creating a **File Uploaded** event with a **User account** action set to change the user's status. Therefore, if your trial expires, examine your Event Rules and adjust as needed.

### To configure the GDPR settings

1. In the administration interface, connect to EFT and in the left pan, click the **Site**.
2. In the right pane, click the **Web** tab.



The following controls affect EFT's web portals and features within those.

Folder sharing:

Send portal:

Drop-off portal:

Request file portal:

Privacy Policy:

Terms of Service:

Account management:

GDPR & DPIA:

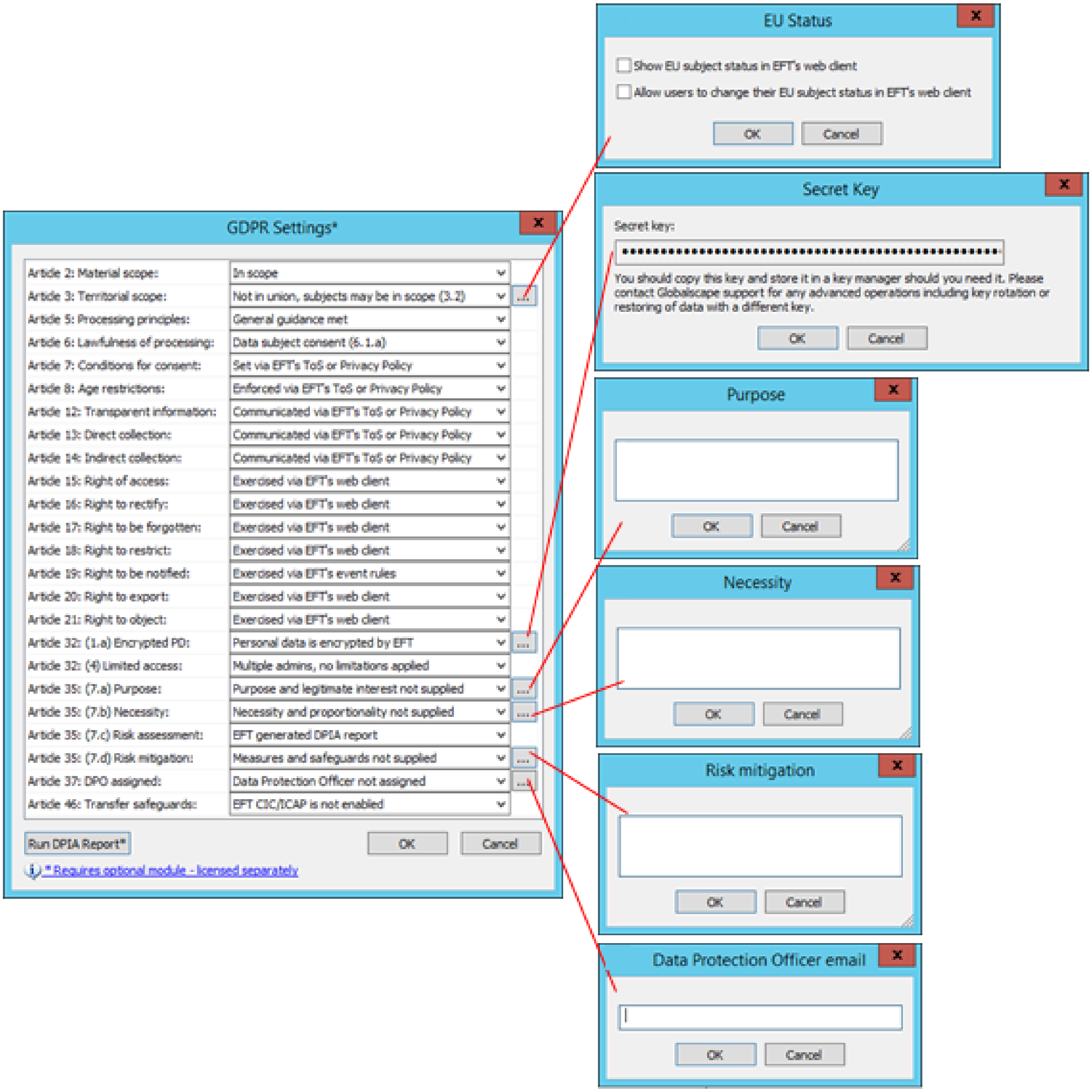
Upload Forms:

3. Next to GDPR & DPIA, click **Configure**. The **GDPR Settings** dialog box appears.
4. Refer to Article-by-Article settings below for guidance on how to configure each article.

The **GDPR Settings** dialog box is used to specify an Article-by-Article setting for user privacy policy for EFT web portals that may be accessed or shared with EU members.

Each of the applicable articles is listed in the **GDPR Settings** dialog box with a drop-down list with which you specify the setting. For example, the setting could be **Not applicable** or **Doesn't apply** if no EU members are expected to have user accounts on EFT.

For the Purpose, Necessity, Risk mitigation, and DPO assigned articles, when you click its **Browse** button, another dialog box appears in which you can provide additional data, such as the email address of the Data Protection Officer. A data protection impact assessment (DPIA) report can be run from this dialog box after the articles are each defined. The logged in administrator account must have **Manage reporting** and **Manage personal data permission** set in the server's **administration** tab. (The server administrator account is assigned these permissions by default when the account is created.)



| | |
|---|---|
| Article 2: Material scope: | In scope |
| Article 3: Territorial scope: | Not in union, subjects may be in scope (3.2) |
| Article 5: Processing principles: | General guidance met |
| Article 6: Lawfulness of processing: | Data subject consent (6.1.a) |
| Article 7: Conditions for consent: | Set via EFT's ToS or Privacy Policy |
| Article 8: Age restrictions: | Enforced via EFT's ToS or Privacy Policy |
| Article 12: Transparent information: | Communicated via EFT's ToS or Privacy Policy |
| Article 13: Direct collection: | Communicated via EFT's ToS or Privacy Policy |
| Article 14: Indirect collection: | Communicated via EFT's ToS or Privacy Policy |
| Article 15: Right of access: | Exercised via EFT's web client |
| Article 16: Right to rectify: | Exercised via EFT's web client |
| Article 17: Right to be forgotten: | Exercised via EFT's web client |
| Article 18: Right to restrict: | Exercised via EFT's web client |
| Article 19: Right to be notified: | Exercised via EFT's event rules |
| Article 20: Right to export: | Exercised via EFT's web client |
| Article 21: Right to object: | Exercised via EFT's web client |
| Article 32: (1.a) Encrypted PD: | Personal data is encrypted by EFT |
| Article 32: (4) Limited access: | Multiple admins, no limitations applied |
| Article 35: (7.a) Purpose: | Purpose and legitimate interest not supplied |
| Article 35: (7.b) Necessity: | Necessity and proportionality not supplied |
| Article 35: (7.c) Risk assessment: | EFT generated DPIA report |
| Article 35: (7.d) Risk mitigation: | Measures and safeguards not supplied |
| Article 37: DPO assigned: | Data Protection Officer not assigned |
| Article 46: Transfer safeguards: | EFT CIC/ICAP is not enabled |

* Requires optional module - licensed separately

□ Show EU subject status in EFT's web client

□ Allow users to change their EU subject status in EFT's web client

Secret key: ••••••••••••••••••••••••••••••••••••••••••••••••••

You should copy this key and store it in a key manager should you need it. Please contact Globalscape support for any advanced operations including key rotation or restoring of data with a different key.

Certain GDPR articles (described below in Article-by-Article settings) must be set to "Exercised via EFT's web client" for the setting to appear in the user account's profile in the WTC.

### Article-by-Article settings

Items in the list below that are marked with a single asterisk * are default settings. However, if Material scope is set to Not in scope, then all items below marked with a double asterisk ** become the defaults. The numbers indicate the level of risk with that setting. For example, "Not in scope" is 0 risk; Unknown or Undefined is 1 for that article. The higher the total number of all of the articles assessed, the more risk there is. With the default settings, the total risk number is 21.

- Article 2: **Material scope:** Specify whether the operations carried out by EFT, or users managed by EFT, fall within scope of GDPR regulations.
  - Unknown or undefined* 1
  - In scope 0
  - Not in scope (2.2) 0 (If you select this value, then all remaining controls are grayed out/unselectable, and the defaults marked with ** are applied.)
- Article 3: **Territorial scope:** Specify whether the territorial scope. Note that if **In Union** is chosen, all accounts will be marked as EU Data Subjects by default.
  - Unknown or undefined* 1
  - In Union, all subjects in scope (3.1) 0 (If you select this value, then EFT automatically, optionally, modifies each "Unknown" to "Yes" for EU data subject status.)
  - Not in union, subjects may be in scope (3.2) 0
  - In scope due to international laws (3.3) 0
  - Territory doesn't apply (not in scope)** 0
  - Click the browse button to specify that EU subject status should appear in the Web Transfer Client, and whether the user can change their EU subject status in the WTC.
- Article 5: **Processing principles**: Specify whether your assessment, with oversight from your Data Protection Officer, indicates that in context of EFT's operations, Article 5 principles have been met
  - Unknown or undefined* 1
  - General guidance not yet met 1
  - General guidance met 0
  - Principles don't apply (not in scope)** 0

- Article 6: **Lawfulness of processing:** Specify what the legal basis is for processing of PD with regard to EFT's file transfer operations or user account details or fields that might contain PD.
    - Unknown or undefined* 1
    - Data subject consent (6.1.a) 0 (If you select this setting, then EFT checks for users that are EU data subject accounts where consent was rescinded or denied and contain personal data.)
    - Contractual, vital interest, et. al. (6.1.b-f) 0
    - Other basis (6.2-4) 0
    - No PD is processed or stored for user 0
    - Not applicable (N/A)** 0
- Article 7: **Conditions for consent:** Specify whether data subjects have been provided with a mechanism for both providing or rescinding consent,  in context with personal data stored by EFT or transferred by EFT.
    - Unknown or undefined* 1
    - Set via EFT ToS or Privacy Policy agreement 0
    - Set via external ToS or Privacy Policy agreement 0
    - Other method that can be demonstrated 0
    - Not applicable (N/A)** 0
- Article 8: **Age restrictions:** Specify whether you have measures in place to adhere to the age-restriction rules specified under Article 8, with regard to minors, in the context of EFT operations.
    - Unknown or undefined* 1
    - Enforced via EFT ToS or Privacy Policy 0
    - Enforced via external ToS or Privacy Policy 0
    - Enforced via other means 0
    - Not applicable (N/A)** 0
- Article 12: **Transparent information:** Specify whether you have mechanisms in place to clearly communicate to EU data subjects how, when, where, and why personal data is collected, used, stored, etc.
    - Unknown or undefined* 1
    - Communicated via EFT's Privacy Policy 0
    - Communicated via external Privacy Policy 0
    - Communicated via other means 0
    - Not applicable (N/A)** 0

- Article 13: **Direct collection:** Specify how information is conveyed in compliance with Article 13 when personal data was obtained directly from the data subject (such as via account self-provisioning).
    - Unknown or undefined* 1
    - Communicated via EFT's Privacy Policy 0
    - Communicated via external Privacy Policy 0
    - Communicated via other means 0
    - Not applicable (N/A)** 0
- Article 14: **Indirect collection:** Specify how information is conveyed in compliance with Article 14 when personal data was obtained indirectly from the data subject (such as via Active Directory provisioning).
    - Unknown or undefined* 1
    - Communicated via EFT's Privacy Policy 0
    - Communicated via external Privacy Policy 0
    - Communicated via other means 0
    - Not applicable (N/A)** 0
- Article 15: **Right of access:** Specify the means by which users can access the personal data associated with their account or stored on their behalf or transferred by them, if applicable.
    - Unknown or undefined* 1
    - Exercised via EFT's web client 0
    - Exercised upon request 0
    - Exercised via other means 0
    - Not applicable (N/A)** 0
- Article 16: **Right to rectify:** Specify the means by which data subjects can modify (rectify) the personal data associated with their account or stored on their behalf or transferred by them, if applicable.
    - Unknown or undefined* 1
    - Exercised via EFT's web client 0
    - Exercised upon request 0
    - Exercised via other means 0
    - Not applicable (N/A)** 0

- Article 17: **Right to be forgotten:** Specify the means by which data subjects can request deletion of their account and removal of their personal data, were applicable, in context with EFT.
    - Unknown or undefined* 1
    - Exercised via EFT's web client 0
    - Exercised upon request 0
    - Exercised via other means 0
    - Not applicable (N/A)** 0
- Article 18: **Right to restrict:** Specify the means by which data subjects can restrict access to or use of the personal data associated with their account or stored on their behalf or transferred through EFT.
    - Unknown or undefined* 1
    - Exercised via EFT's web client 0
    - Exercised upon request 0
    - Exercised via other means 0
    - Not applicable (N/A)** 0
- Article 19: **Right to be notified:** Specify the means by which data subjects are notified if their personal data is modified or deleted, within EFT context, if applicable.
    - Unknown or undefined* 1
    - Exercised via EFT's event rules 0
    - Exercised upon request 0
    - Exercised via other means 0
    - Not applicable (N/A)** 0
- Article 20: **Right to export:** Specify the means by which EU data subjects can export a copy of the personal data associated with their account or stored on their behalf or transferred by them, if applicable.
    - Unknown or undefined* 1
    - Exercised via EFT's event rules
    - Exercised via EFT's web client 0
    - Exercised upon request 0
    - Exercised via other means 0
    - Not applicable (N/A)** 0

- Article 21**: Right to object:** Specify the means by which users can object to the use of the personal data associated with their account or stored on their behalf or transferred by them, if applicable.
  - Unknown or undefined* 1
  - Exercised via EFT's web client 0
  - Exercised upon request 0
  - Exercised via other means 0
  - Not applicable (N/A)** 0
- Article 32**: (1.a) Encrypted PD:** EFT selects the default based on current configuration, whether user account fields marked as personal data are encrypted. You can select a value, if desired.
  - EFT is not encrypting PD* 1
  - EFT is encrypting PD* 0
  - A compensating control is in place 0
  - Not applicable (N/A)** 0
- Article 32**: (4) Limited access:** EFT selects the default based on whether there is more than one EFT administrator, and if so, whether at least one does NOT have access to personal data.
  - Multiple administrators, no limitations applied* 1
  - Multiple administrators, limitations applied* 0 (EFT automatically sets the default depending on configuration; if set, the other items are not available for selection.)
  - Single administrator, requires full access* 0
  - A compensating control is in place 0
  - Not applicable (N/A)**

- Article 35: **(7.a) Purpose:** This article requires that you document the express purpose and legitimate interest for processing of personal data, for the DPIA report.
  - Purpose and legitimate interest supplied 0, not supplied* 1 (A **Browse** button opens a dialog box in which you can supply the purpose and legitimate interest. If data is in provided in the dialog box, then "supplied" is displayed; however, you can still select N/A if desired.)
  - Other or external measures 0
  - Not applicable (N/A)** 0
- Article 35: **(7.b) Necessity:** This article requires that you document the necessity and proportionality of the processing operations in relation to the purposes, for the DPIA report.
  - Necessity and proportionality supplied 0, not supplied* 1  (A **Browse** button opens a dialog box in which you can note the necessity. If data is in provided in the dialog box, then "supplied" is displayed; however, you can still select N/A if desired.)
  - Other or external measures
  - Not applicable (N/A)** 0
- Article 35: **(7.c) Risk assessment:** This article requires that you document the risks to the rights and freedoms of data subjects. EFT's DPIA report can assist with fulfilling this requirement.
  - EFT generated DPIA report* 0
  - Other or external measures 0
  - Not applicable (N/A)** 0
- Article 35: **(7.d) Risk mitigation:** This article requires that you document the measures and safeguards to mitigate risks to the rights and freedoms of data subjects.
  - Measures and safeguards supplied 0, not supplied* 1 (A **Browse** button opens a dialog box in which you can note the risk mitigation. If data is in provided in the dialog box, then "supplied" is displayed; however, you can still select N/A if desired.)
  - Other or external measures
  - Not applicable (N/A)** 0

- Article 37: **DPO assigned:** Specify the email address for the Data Protection Officer (DPO) or equivalent. (The email variable %SERVER.PRIVACY_DPO_EMAIL% can be used in Event Rules.)
  - Data Protection Officer assigned 0, not assigned* 1 (A **Browse** button opens a dialog box in which you can provide the email address of the DPO.)
  - Other or external measures 0
  - Not applicable (N/A)** 0
- Article 46: **Transfer safeguards:** Specify whether EFT is configured to use its Content Integrity Control (CIC) action or external process for identifying personal data contained within transferred files
  - EFT CIC/ICAP is enabled 0, not enabled* 1 (Similar to Article 32 (encryption), EFT will auto detect if ICAP is enabled and preselect the correct value accordingly. You can still change to external or N/A if desired.)
  - Other or external measures 0 (If ICAP is enabled, EFT checks if there are any affected rules that either process files, such as Folder Monitor, File Uploaded, Folder Downloaded, or have Copy/Move operations defined that are missing the CIC action.)
  - Not applicable (N/A)** 0

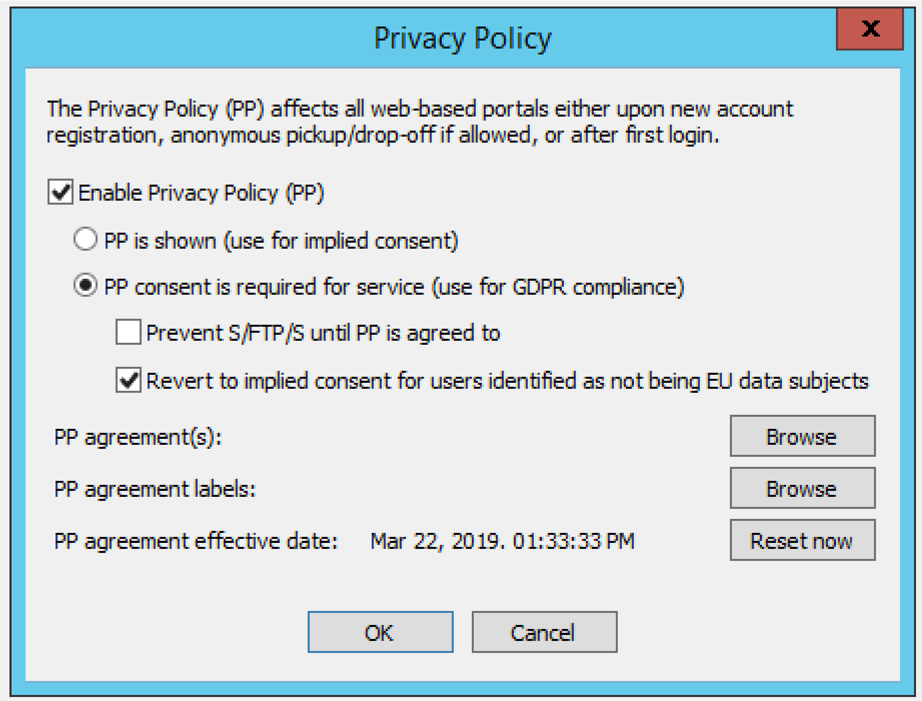
# Privacy Policy

**(Requires HTTP/S, Workspaces, RCM)** You can create and display a Privacy Policy for all web-based access to EFT. The Privacy Policy affects all web-based portals upon new account registration, anonymous pickup or drop-off, and upon first login. For user-specific settings, refer to Specify Terms of Service and Privacy Policy Options.

- If accessing EFT for the first time via FTP, FTPS, or SFTP, and the Privacy Policy consent is required for use, the connection will fail. The user must first connect via the Web Transfer Client (HTTPS portal) to consent to the policy. The administrator can instead set the status for the Privacy Policy for a given user manually, on user account's **General** tab in the EFT administration interface. Additionally, you can change the EFT login banner to provide instructions to login via the Web Transfer Client before logging in via FTP, FTP, or SFTP.
- If the Privacy Policy is set to the default (enabled, but not mandatory) and the user implicitly agrees to the policy by continuing to use the service, then no record is audited to the EFT database.
- For anonymous users, accepting the Privacy Policy sets a cookie for 12 hours so that the user doesn't have to consent for each action within that 12 hours.
- For an example of a Privacy Policy, refer to https://policies.google.com/privacy.

### To enable the Privacy Policy agreement

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, click the Site you want to configure.
3. On the **Web** tab, next to **Privacy Policy**, click **Configure**. The **Privacy Policy** dialog box appears.



The Privacy Policy (PP) affects all web-based portals either upon new account registration, anonymous pickup/drop-off if allowed, or after first login.

☑ Enable Privacy Policy (PP)

○ PP is shown (use for implied consent)

● PP consent is required for service (use for GDPR compliance)

□ Prevent S/FTP/S until PP is agreed to

☑ Revert to implied consent for users identified as not being EU data subjects

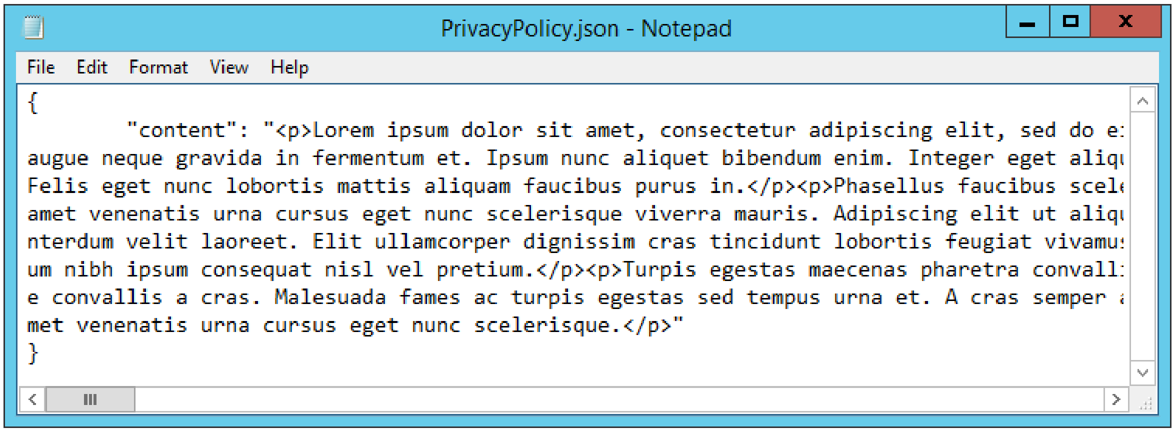
PP agreement(s):

PP agreement labels:

PP agreement effective date: Mar 22, 2019. 01:33:33 PM

4. Select the **Enable Privacy Policy** check box, then specify whether the agreement is **implied** or **required for service**. If the agreement is required, you can select the **Prevent** check box to prevent access over FTP, SFTP, or FTPS until the Privacy Policy agreement is accepted. The **Revert to implied consent for users identified as not being EU data subjects** is selected automatically.
5. To select or view the agreement(s) or the agreement labels, click **Browse**. Windows Explorer opens to the **\Web** folder.
6. The **\Templates** folder contains the **PrivacyPolicy.json** file. Replace the default text with your organization's Privacy Policy.

   The **PrivacyPolicy.json** file contains "dummy text" ("lorem ipsum dolor...") that you will replace with the text of your policy.



```
{
	"content": "<p>Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do e:
augue neque gravida in fermentum et. Ipsum nunc aliquet bibendum enim. Integer eget aliqu
Felis eget nunc lobortis mattis aliquam faucibus purus in.</p><p>Phasellus faucibus scel
amet venenatis urna cursus eget nunc scelerisque viverra mauris. Adipiscing elit ut aliq
nterdum velit laoreet. Elit ullamcorper dignissim cras tincidunt lobortis feugiat vivamu
um nibh ipsum consequat nisl vel pretium.</p><p>Turpis egestas maecenas pharetra convall
e convallis a cras. Malesuada fames ac turpis egestas sed tempus urna et. A cras semper
met venenatis urna cursus eget nunc scelerisque.</p>"
}
```

You can use basic HTML formatting tags (<p>, <li>, etc.). The "content" label must be kept, as well as opening and closing curly brackets { } :

```
{
 "content": "<p>This is our Privacy Policy ... </p>"
}
```

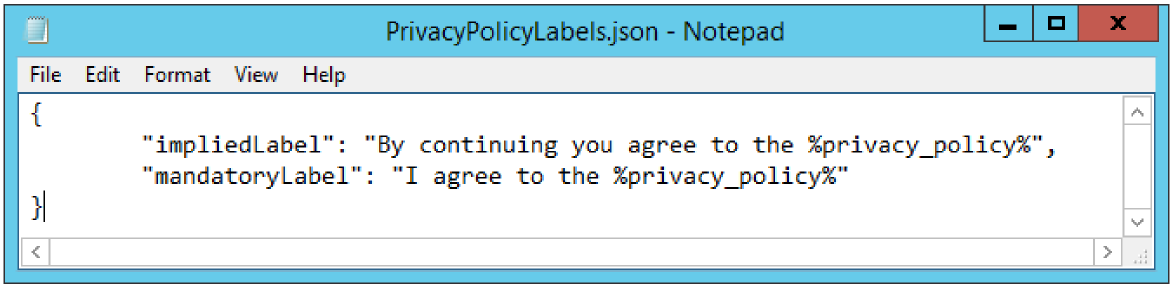
7. Refer to **Edit the Privacy Policy and labels** for how to edit the Privacy Policy and agreement labels files.
8. To reset the agreement effective date, such as when publishing a new agreement, click **Reset now**.
9. Click **OK**, then click **Apply** on the **Web** tab. A Site restart is required.

## Edit the Privacy Policy and Labels

The **PrivacyPolicy** and **PrivacyPolicyLabels** files are JSON files (similar to XML) that must be edited for your organization's agreement. (The labels in the JSON file are case-sensitive.)

1. Open the **PrivacyPolicyLabels.json** file and the **PrivacyPolicy**.json file in a text editor, such as Notepad.
2. Save a copy of each before you edit the originals so you have a backup.

   The **PrivacyPolicyLabels** file is used to change the default text that appears when you have specified that the Privacy Policy is implied or when it's mandatory to continue. For example, the default text when the agreement to the policy is mandatory is, in English, "I agree to the Privacy Policy."

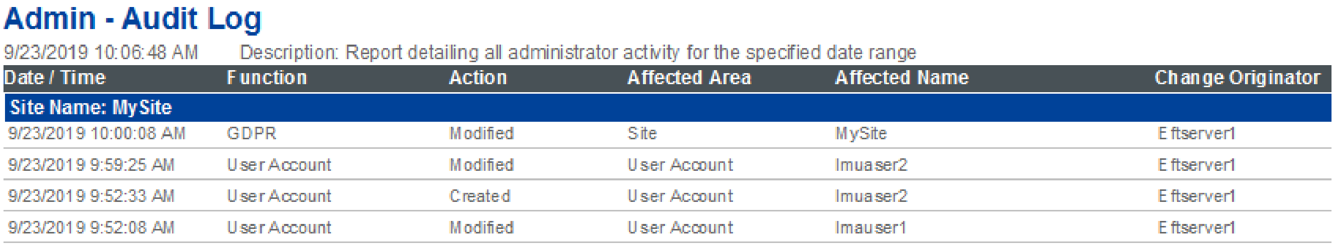

PrivacyPolicyLabels.json - Notepad
File Edit Format View Help

```
{
        "impliedLabel": "By continuing you agree to the %privacy_policy%",
        "mandatoryLabel": "I agree to the %privacy_policy%"
}
```

3. Change the value (By continuing...") to whatever your organization requires, or to another language. However, do not change any the label variables (impliedLabel, mandatoryLabel) or the text that is between the % signs. The opening and closing curly brackets { } are also required.

# Privacy Reports

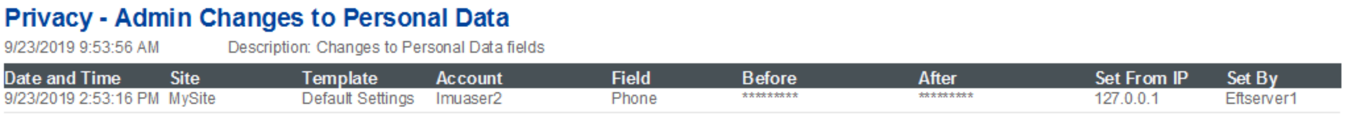
When changes are made to the GDPR settings, Privacy Policy, and Terms of Service, the changes are recorded in the database and can appear in reports:



**Admin - Audit Log**

9/23/2019 10:06:48 AM    Description: Report detailing all administrator activity for the specified date range

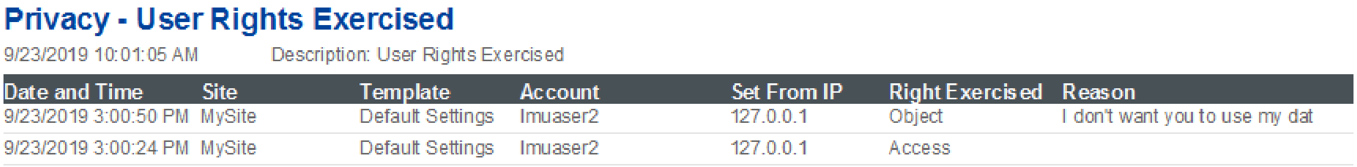
| Date / Time | Function | Action | Affected Area | Affected Name | Change Originator |
|---|---|---|---|---|---|
| Site Name: MySite | | | | | |
| 9/23/2019 10:00:08 AM | GDPR | Modified | Site | MySite | Eftserver1 |
| 9/23/2019 9:59:25 AM | User Account | Modified | User Account | Imuaser2 | Eftserver1 |
| 9/23/2019 9:52:33 AM | User Account | Created | User Account | Imuaser2 | Eftserver1 |
| 9/23/2019 9:52:08 AM | User Account | Modified | User Account | Imauser1 | Eftserver1 |



**Privacy - Admin Changes to Personal Data**

9/23/2019 9:53:56 AM    Description: Changes to Personal Data fields

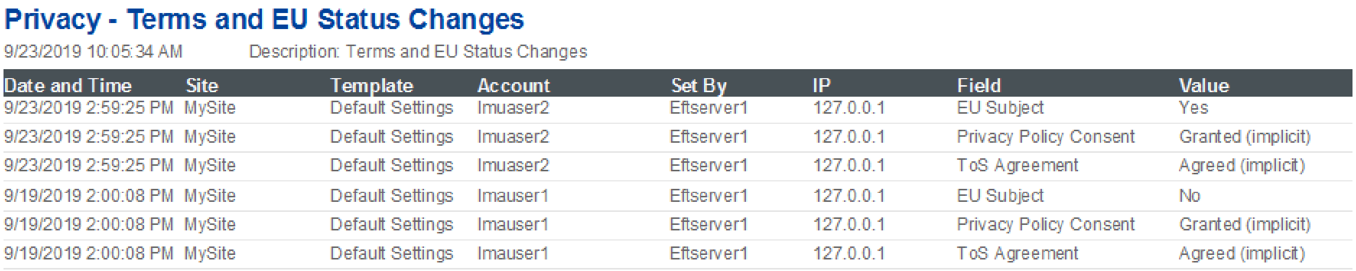
| Date and Time | Site | Template | Account | Field | Before | After | Set From IP | Set By |
|---|---|---|---|---|---|---|---|---|
| 9/23/2019 2:53:16 PM | MySite | Default Settings | Imuaser2 | Phone | ********* | ********* | 127.0.0.1 | Eftserver1 |



**Privacy - User Rights Exercised**

9/23/2019 10:01:05 AM    Description: User Rights Exercised

| Date and Time | Site | Template | Account | Set From IP | Right Exercised | Reason |
|---|---|---|---|---|---|---|
| 9/23/2019 3:00:50 PM | MySite | Default Settings | Imuaser2 | 127.0.0.1 | Object | I don't want you to use my dat |
| 9/23/2019 3:00:24 PM | MySite | Default Settings | Imuaser2 | 127.0.0.1 | Access | |



**Privacy - Terms and EU Status Changes**

9/23/2019 10:05:34 AM    Description: Terms and EU Status Changes

| Date and Time | Site | Template | Account | Set By | IP | Field | Value |
|---|---|---|---|---|---|---|---|
| 9/23/2019 2:59:25 PM | MySite | Default Settings | Imuaser2 | Eftserver1 | 127.0.0.1 | EU Subject | Yes |
| 9/23/2019 2:59:25 PM | MySite | Default Settings | Imuaser2 | Eftserver1 | 127.0.0.1 | Privacy Policy Consent | Granted (implicit) |
| 9/23/2019 2:59:25 PM | MySite | Default Settings | Imuaser2 | Eftserver1 | 127.0.0.1 | ToS Agreement | Agreed (implicit) |
| 9/19/2019 2:00:08 PM | MySite | Default Settings | Imauser1 | Eftserver1 | 127.0.0.1 | EU Subject | No |
| 9/19/2019 2:00:08 PM | MySite | Default Settings | Imauser1 | Eftserver1 | 127.0.0.1 | Privacy Policy Consent | Granted (implicit) |
| 9/19/2019 2:00:08 PM | MySite | Default Settings | Imauser1 | Eftserver1 | 127.0.0.1 | ToS Agreement | Agreed (implicit) |

# Terms of Service Agreement

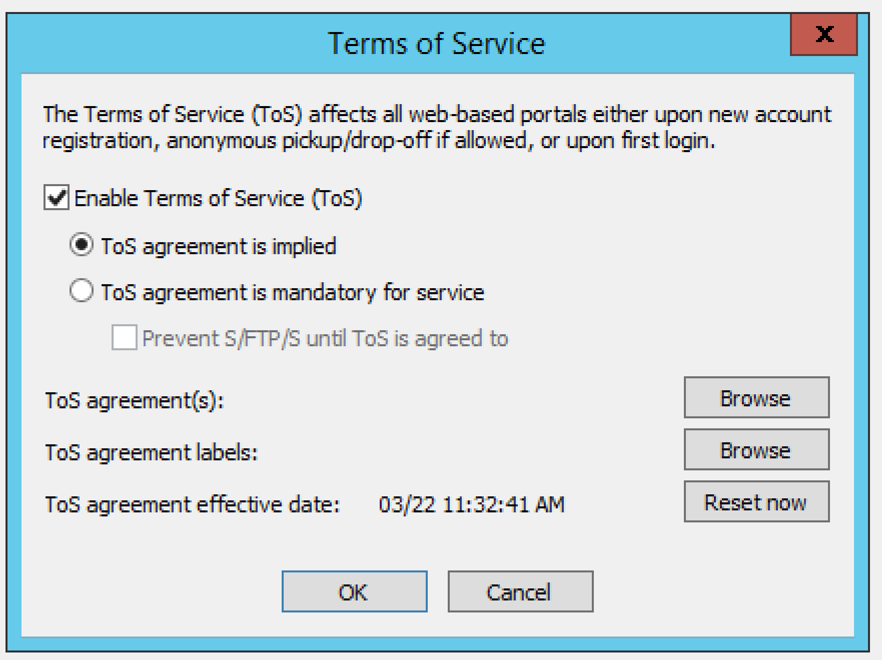
**(Requires HTTP/S, Workspaces, RCM)** The EFT web portal Terms of Service agreement can be used to identify or specify whether a user has consented to use of their personal data. This information can help you stay in compliance with GDPR and other privacy regulations.

From the Site's **Web** tab, you can configure the Terms of Service agreement, which affects all users on the Site, all web-based portals upon new account registration, anonymous pickup or drop-off, and upon first login. For user-specific settings, refer to Specify Terms of Service and Privacy Policy Options.

- If accessing EFT for the first time via FTP, FTPS, or SFTP, and the Terms of Service agreement is mandatory for service, the connection will fail. The user must first connect via the Web Transfer Client (HTTPS portal) to accept the Terms of Service. The administrator can instead set the status for the Terms of Service for a given user manually, on user account's **General** tab in the EFT administration interface. Additionally, you can change the EFT login banner to provide instructions to login via the Web Transfer Client before logging in via FTP, FTP, or SFTP.
- If the Terms of Service agreement is set to the default (enabled, but not mandatory) and the user implicitly agrees to the Terms of Service (by continuing to use the service), then no record is audited to the EFT database.
- For anonymous users, accepting the Terms of Service sets a cookie for 12 hours so that the user doesn't have to consent for each action within that 12 hours.
- For an example of a Terms of Service agreement, refer to https://policies.google.com/terms.

### To enable the Terms of Service agreement

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, click the Site you want to configure.
3. On the **Web** tab, next to **Terms of Service**, click **Configure**. The **Terms of Service** dialog box appears.



Terms of Service

The Terms of Service (ToS) affects all web-based portals either upon new account registration, anonymous pickup/drop-off if allowed, or upon first login.

☑ Enable Terms of Service (ToS)

● ToS agreement is implied

○ ToS agreement is mandatory for service

□ Prevent S/FTP/S until ToS is agreed to

ToS agreement(s):

ToS agreement labels:

ToS agreement effective date: 03/22 11:32:41 AM

4. Select the **Enable Terms of Service** check box, then specify whether the agreement is **implied** or **mandatory for service**. If the agreement is mandatory, select the **Prevent** check box to prevent access over FTP, SFTP, or FTPS until the Terms of Service agreement is accepted.
5. To view the agreement(s) or the agreement labels, click **Browse**. The Windows File Explorer opens to the EFT installation folder. (NOTE: You can't actually "browse for files." Instead, you must edit the JSON file, as described below.)
   - Refer to Edit the Terms of Service agreement and agreement labels for how to edit the Terms of Service agreement and agreement labels files.
6. To reset the agreement effective date, such as when publishing a new agreement, click **Reset now**.
7. Click **OK**, then click **Apply** on the **Web** tab.

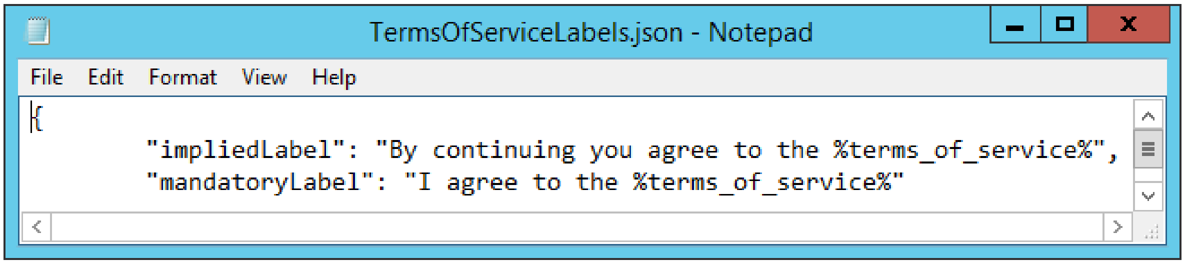
### Edit the Terms of Service Agreement and Agreement Labels

The **TermsOfService** agreement and **TermsOfServiceLabels** files are JSON files (similar to XML) that must be edited for your organization's agreement. (The labels in the JSON file are case-sensitive.)

1. Save a copy of each before you edit the originals so that you have a backup.
2. Open the **TermsOfServiceLabels.json** file and the **TermsOfService.json** file in the EFT installation folder, in a text editor, such as Notepad.

   **C:\Program Files (x86)\Globalscape\EFT Server\Web\Templates\**

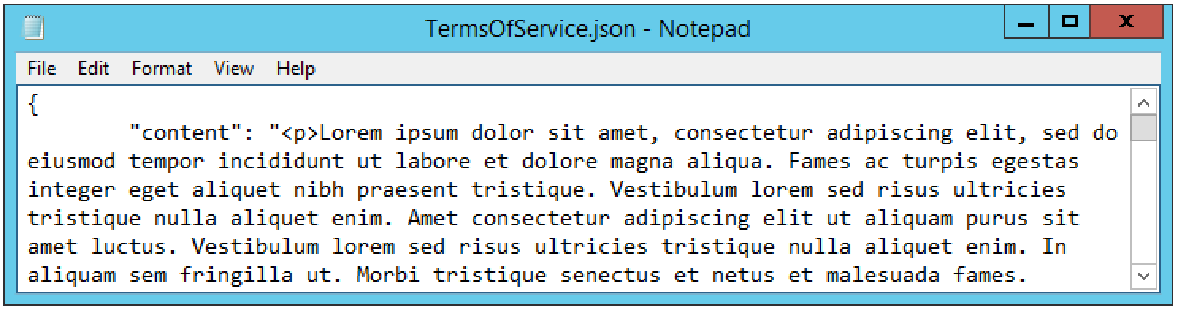
The **Labels** file is used to change the default text that appears when you have specified that the Terms of Service are implied or when it's mandatory to continue. For example, the default text when the agreement to the terms is mandatory is in English, "I agree to the terms of service."



```
{
        "impliedLabel": "By continuing you agree to the %terms_of_service%",
        "mandatoryLabel": "I agree to the %terms_of_service%"
```

3. Change the text to whatever your organization requires, or to another language. However, do not change any text that is between the quotation marks, as that is a variable used by EFT. The opening and closing curly brackets { } are also required.

   The **TermsOfService.json** file contains "dummy text" ("lorem inpsum dolor...") that you will replace with the text of your agreement:



```
{
        "content": "<p>Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do
eiusmod tempor incididunt ut labore et dolore magna aliqua. Fames ac turpis egestas
integer eget aliquet nibh praesent tristique. Vestibulum lorem sed risus ultricies
tristique nulla aliquet enim. Amet consectetur adipiscing elit ut aliquam purus sit
amet luctus. Vestibulum lorem sed risus ultricies tristique nulla aliquet enim. In
aliquam sem fringilla ut. Morbi tristique senectus et netus et malesuada fames.
```

4. Use basic HTML formatting tags (<p>, <li>, etc.) to create your Terms of Service. The "content" label must be kept, as well as opening and closing curly brackets { }.

```
{
 "content": "<p>These are the Terms of Service ... </p>"
}
```

5. You can make different Site-specific policies and language-specific policies:

   a. Site-specific: Create a custom **TermsOfServiceLabels.json** and **TermsOfService.json** file in the same folder, but place the name in the file name, such as MySite_TermsOfService.

   b. Language-specific: Create a custom **TermsOfServiceLabels.json** and **TermsOfService.json** file in the same folder, but place the 2-digit language code in the file name, such as MySite_fr_TermsOfService.

      You will need to clear the cache of the web browser to see your changes.

# Display Full Name of User in the WTC

In the Web Transfer Client (WTC), you can display the full name of a user if the following settings are true:

- The Advanced Property "displayFullName" value must be set to "true" in administrator-configuration.json.
- GDPR Article 15: "Right of Access" must be set to "Exercised via EFT's Web Client"
- The user's full name must have a value in EFT (not an empty string)

If any of these settings are not true, the WTC will display the username on the account instead of the Full name.

**administrator-configuration.json:**

```
{
  "batchDownloadAsZipThreshold": 5,
  "concurrentUploadLimit": 5,
  "crcEnabled": true,
  "displayFullName": true,
  "idlePeriodBeforeLogoffMS": 300000,
  "keepAlivePingMS": 200000,
  "timeoutWarningDurationMS": 20000,
  "uploadChunkSize": 200000000
}
```

# Changing the Language of the Client

EFT is used all over the world in a variety of languages. EFT has provided language files for some of the most-commonly requested languages. They are stored (by default) in **C:\Program Files (x86)\Globalscape\EFT Server\web\ ...**

- ..**\Shadowfax\portal\assets\i18n**

The international language (i18n) directory of the EFT installation folder includes the language files in JSON format.

- Instruct the user to specify their preferred language in the WTC in their user Profile.

This process for changing the language does not affect the EFT administration interface, just the Web Transfer Client after login. The initial login screen comes from EFT and is not localized.

# Disable CRC

The Web Transfer Client (WTC) can validate the integrity of files transferred to and from EFT. Cyclical Redundancy Check (CRC32) is enabled on the WTC by default. The EFT administrator must have enabled CRC in its FTP configuration to take advantage of this feature.

With CRC enabled, when the WTC transfers a file to or from EFT, it automatically queries EFT for the CRC value of the file, then compares it to the CRC value for the local file. If they match, the transfer is reported as successful. If they do not match, the system reports a "CRC Failure." The user can then retry the transfer, if necessary. The client does not automatically retry the transfer if they do not match.

If upload verifications are not required, you can disable CRC in the WTC configuration file.

The HTML5 version of the Web Transfer Client does not support a CRC-check for downloaded files because of the limited access of html/js to the client file system. The process of initiating a download is human driven and can NOT be intercepted by a JavaScript API; it is wholly managed by the browser itself, for security reasons. Further, the browser cannot arbitrarily read files on the local file system (for obvious security reasons), so EFT cannot read contents of downloaded files to do CRC32, and thus cannot issue a follow-up HEAD request to verify the integrity of the download.

### To disable CRC

1. Find the **admin-configuration.json** file.
   - **C:\Program Files (x86)\Globalscape\EFT Server\Web\Shadowfax\portal\assets**
2. Open the configuration file in a text editor, such as Notepad. (It may be necessary to change the extension from JS to TXT to view it properly.)
3. Find the following text:

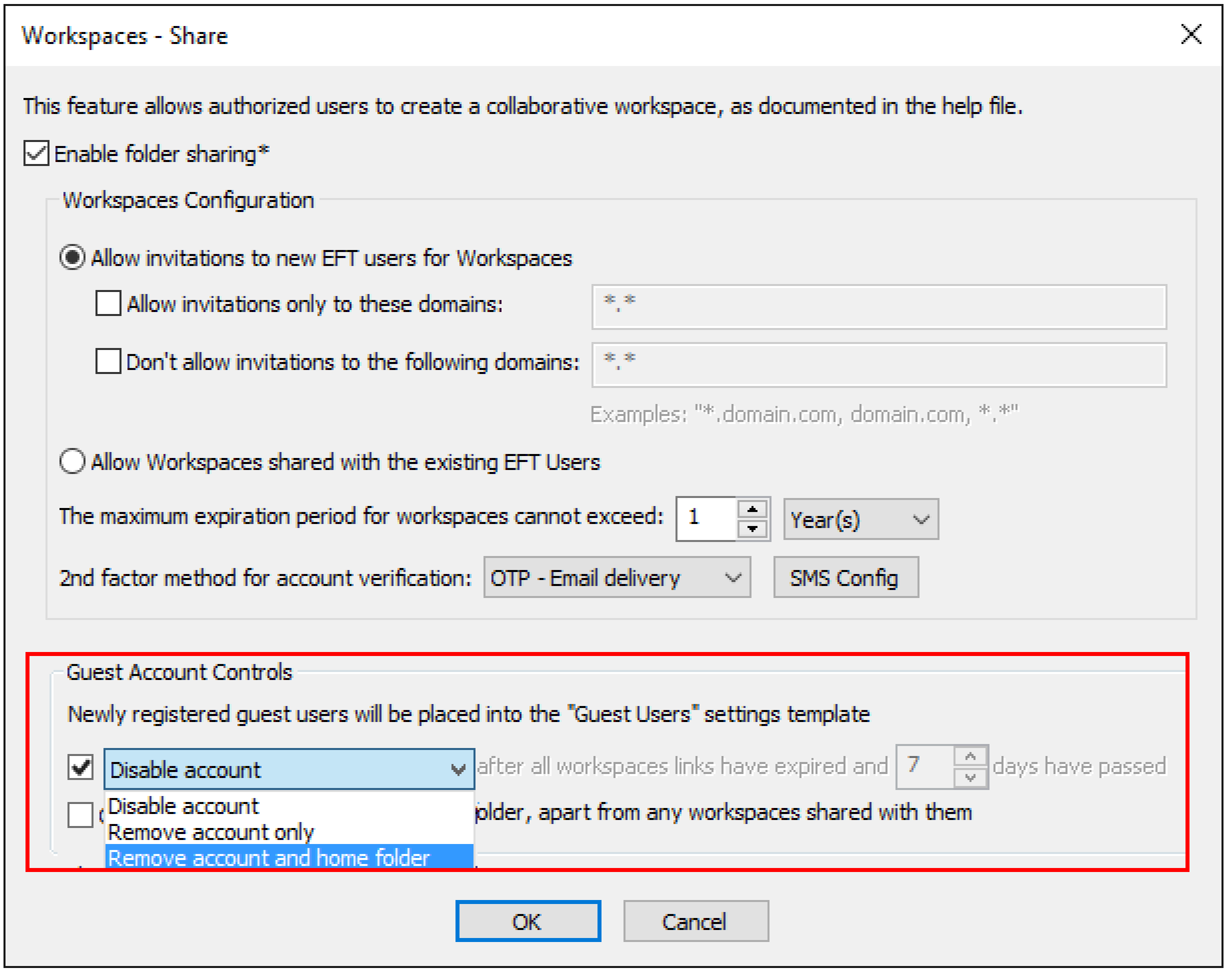
   ```
   “crcEnabled”: true,
   ```
4. Change `true` to `false`, then save the file.
5. If you changed the name of the file to edit it, be sure to change it back.
6. Now transfers will be processed without CRC.

# Guest Users

After a guest (non-EFT user) has been invited to join a Workspace, has created an account, and logged in, the guest account will appear (if so configured) in the **Guest Users** Settings template. The **Guest Users** Settings Template appears when Workspaces is enabled.

After the Workspace has expired, the guest account is either disabled or removed, depending on the settings on the **Site> Web > Folder sharing > Configure > Workspaces-Share** dialog box. If the guest account is disabled, the EFT administrator must remove it or enable it before they can receive any Workspaces invitations. Refer to "Guest Users" in Workspaces Invitations for details of re-enabling expired Guest accounts when new invitations are sent.

Guest users' permissions depend on what the EFT administrator configures in the Guest Users Settings Template. The default settings include **Download**, **Show this folder in parent list**, **Show files and folders in list**. Users with whom a Workspace is shared do NOT have permission to move files and folders out of the Workspace.



Workspaces - Share

This feature allows authorized users to create a collaborative workspace, as documented in the help file.

☑ Enable folder sharing*

Workspaces Configuration

● Allow invitations to new EFT users for Workspaces

□ Allow invitations only to these domains: *.*

□ Don't allow invitations to the following domains: *.*

Examples: "*.domain.com, domain.com, *.*"

○ Allow Workspaces shared with the existing EFT Users

The maximum expiration period for workspaces cannot exceed: 1 Year(s)

2nd factor method for account verification: OTP - Email delivery

Guest Account Controls

Newly registered guest users will be placed into the "Guest Users" settings template

☑ Disable account after all workspaces links have expired and 7 days have passed

- Disable account
- Remove account only
- Remove account and home folder

□ ( older, apart from any workspaces shared with them

# Login to EFT (WTC)

**(Requires the HTTP/S module)** The EFT administrator should inform end users which IP address, port, username, and password should be used to log in to a Site. Because many users are unfamiliar with <IP address:Port> formatting, be sure to provide users with the exact URL that they should access to log in, whether they are accessing a Site from the Web Transfer Client, "plain-text" client, a command line, CuteFTP, or any other FTP client.

For example, you could provide a link in an email or tell your users:

```
In the address box of Internet Explorer, type
https://wtc.mycompany.com:4434
```

### To log in to EFT to transfer files

1. Open a web browser to the address provided by the EFT administrator. For example, **https://mycompany.com/EFTClient/Account/Login.htm** Or **https://mycompany.com/Web/Account/Login.htm**. The login page appears.
2. Provide your EFT **Username** and **Password**, and then click **Log In**.

- If you have forgotten your username or password, click the applicable link. You will be asked for your email address to which the reset information will be sent.
- If the Web Transfer Client is not enabled, a less-featured version of the WTC appears.
- If it is configured in the EFT administration interface, users are prompted to change their password the first time they log in.
- If a security prompt appears asking you to accept the website's certificate, select the **Always trust** check box, and then click **Yes**.
- If a prompt appears to provide a passcode, use the method asked for in the prompt to retrieve your passcode (Email or SMS).

3. Refer to Web Transfer Client (WTC) for details of transferring files.

## Form-Based Authentication versus Basic Authentication

EFT uses form-based authentication for users that connect over a browser. It is important to note that a browser is defined merely by what is contained in the "user-agent" attribute provided in the HTTP headers. If EFT doesn’t recognize the user-agent (such as when connecting with a client application CuteFTP), then EFT will fall back to "basic authentication." There is nothing inherently wrong with basic authentication, especially if it is SSL encrypted, but form-based is considered superior because it facilitates true session management. However, there is another option, which is NTLM authentication, in which EFT attempts to reuse the user’s AD credentials as supplied by the browser (assuming the browser supports NTLM), resulting in a single-sign-on (SSO) experience. For example, the user authenticates on the company portal, and those credentials are reused by EFT without having to ask the user to re-enter them. The downside to NTLM-based authentication is that, like basic authentication, it does not support true sessions, so it is up to the users to close their browsers at the end of their sessions to truly log out. Another drawback is that when using NTLM, the end user won’t be able to choose between loading the Web Transfer Client or the Plain Text Client, won’t be able to access the lost username/password forms, and won’t see any of the custom branding. Each of these would be available to the user if they had used the default form-based authentication. Even in the case where NTLM is enabled, SSO will only apply for Active Directory-based sites (because we are talking about AD credentials), and the browser has to be a recognizable user-agent; otherwise, it will default to basic authentication (for non-browser) or form-based authentication (for non-AD sites), even if NTLM is turned on via advanced properties.

- If NTLM is off (by default), then EFT will use form-based authentication for recognized user-agents and basic-authentication for all others
- If NTLM is on (enabled in advanced properties), then EFT will use NTLM authentication for AD sites + recognized user-agent, form based authentication for

non-AD sites + recognized user agent, and basic authentication for all others (non-recognized user agents).

# Workspaces SSO Authentication

Workspaces can be configured to use SSO authentication (which can include JIT provisioning in the case of SAML SSO authenticated users) to be automatically directed to their Workspace or Pickup portal so that those users are not added as guest accounts.

Refer to SAML (Web SSO) Authentication more information about configuring SAML Web SSO authentication in EFT.

# Managing Workspaces in the VFS

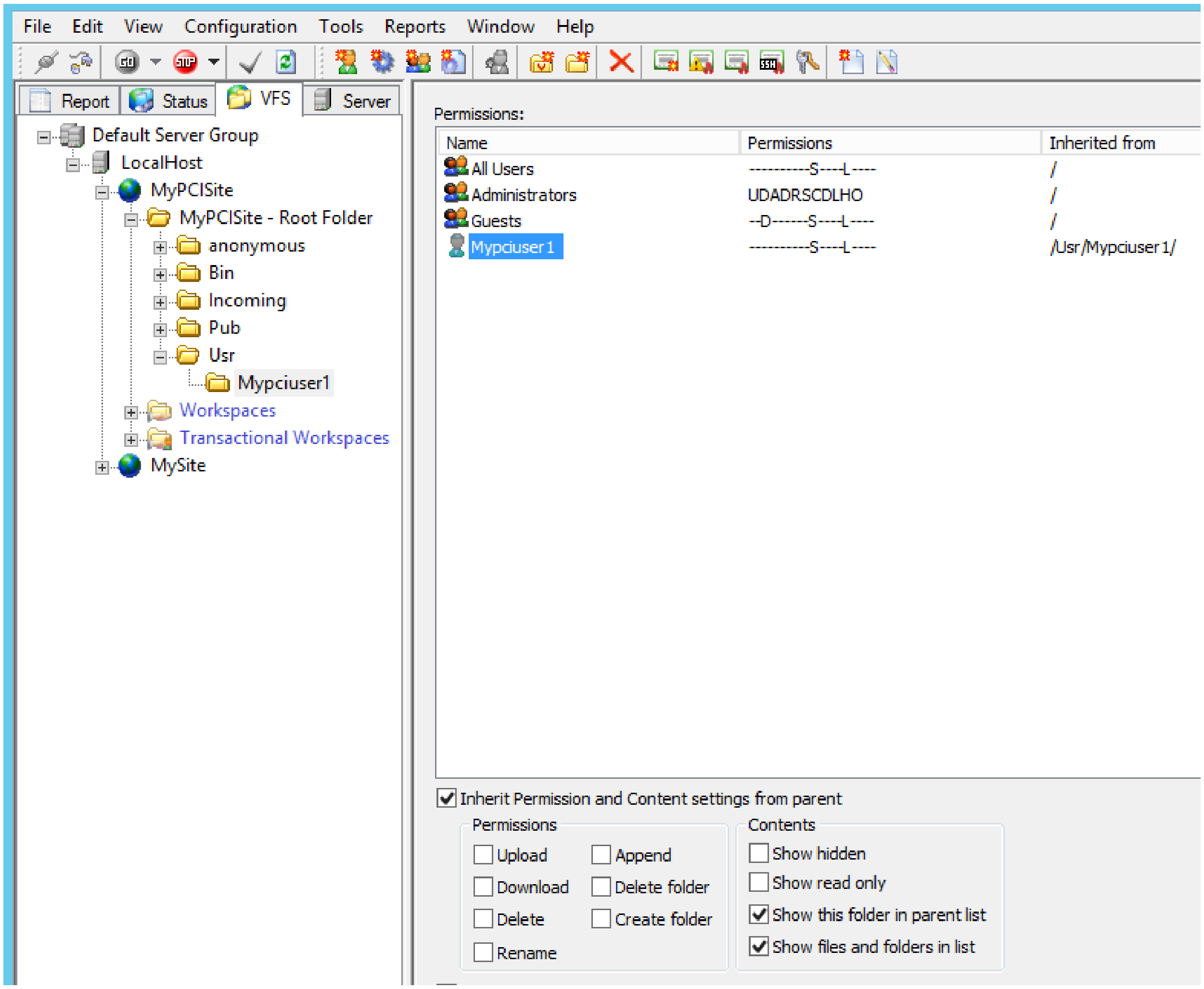
The **VFS** tab has a Workspaces view in which EFT Server- and Site-level administrators can:

- Delete shared Workspaces
- Add existing users to existing Workspaces
- Modify participant permissions of shared Workspaces

- When you send a file using the WTC, a "WorkspacesSendMessage" folder is created in the Virtual File System (VFS).
- The user account that is creating the Workspace must have the appropriate permissions on their home folder to create folders.
- You may have to refresh the administration interface to see any changes in the VFS tab (such as new Guest users and Workspaces added)

### Sharing folders via the VFS tab

- Workspaces cannot be created via the **VFS** tab.
- External users cannot be invited via the **VFS** tab. External users can only be invited via the WTC.
- Users joined to Workspaces via the **VFS** tab, unlike users joined via WTC, are not sent invitation notification emails.
- Workspaces permissions may be granted via the **VFS** Workspaces view.



Permissions:

| Name | Permissions | Inherited from |
|---|---|---|
| All Users | ----------S----L---- | / |
| Administrators | UDADRSCDLHO | / |
| Guests | --D------S----L---- | / |
| Mypciuser1 | ----------S----L---- | /Usr/Mypciuser1/ |

☑ Inherit Permission and Content settings from parent

Permissions

□ Upload
□ Download
□ Delete
□ Rename
□ Append
□ Delete folder
□ Create folder

Contents

□ Show hidden
□ Show read only
☑ Show this folder in parent list
☑ Show files and folders in list

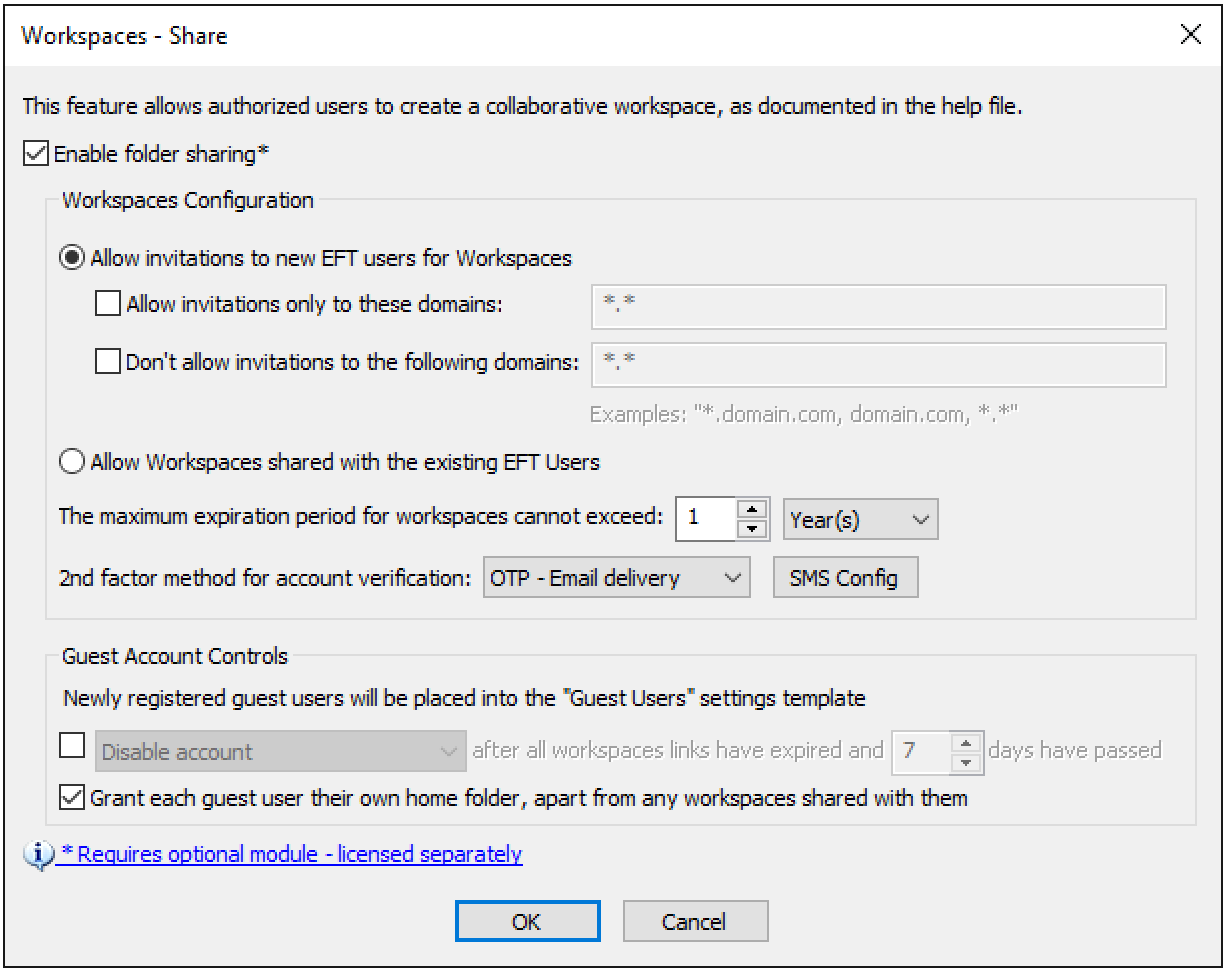
- The **VFS** tab will appear to permit all user permissions to be granted to a Workspaces participant. Suppose an EFT user creates a shared folder with only Upload permissions; an EFT administrator may invite participant1 to join the Workspaces folder, granting participant1 full administrative privileges to the folder. However, participant1 will receive an "access denied" response if they attempt to perform any actions within the folder other than upload, because the Workspaces folder respects the Workspaces owner's folder permissions.

# Restrict Workspaces Invitations to Specific Domains

**(Requires HTTP/S, Workspaces )** Administrators can configure Workspaces so that only specific domains can be invited to access a Workspace.

### To restrict Workspaces invitations

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, click the Site you want to configure.
3. In the right pane, click the **Web** tab.
4. Next to **Folder sharing**, click **Configure**. The **Workspaces - Share** dialog box appears.



Workspaces - Share

This feature allows authorized users to create a collaborative workspace, as documented in the help file.

☑ Enable folder sharing*

Workspaces Configuration

● Allow invitations to new EFT users for Workspaces

☐ Allow invitations only to these domains: *.*

☐ Don't allow invitations to the following domains: *.*

Examples: "*.domain.com, domain.com, *.*"

○ Allow Workspaces shared with the existing EFT Users

The maximum expiration period for workspaces cannot exceed: 1 Year(s)

2nd factor method for account verification: OTP - Email delivery

Guest Account Controls

Newly registered guest users will be placed into the "Guest Users" settings template

☐ Disable account after all workspaces links have expired and 7 days have passed

☑ Grant each guest user their own home folder, apart from any workspaces shared with them

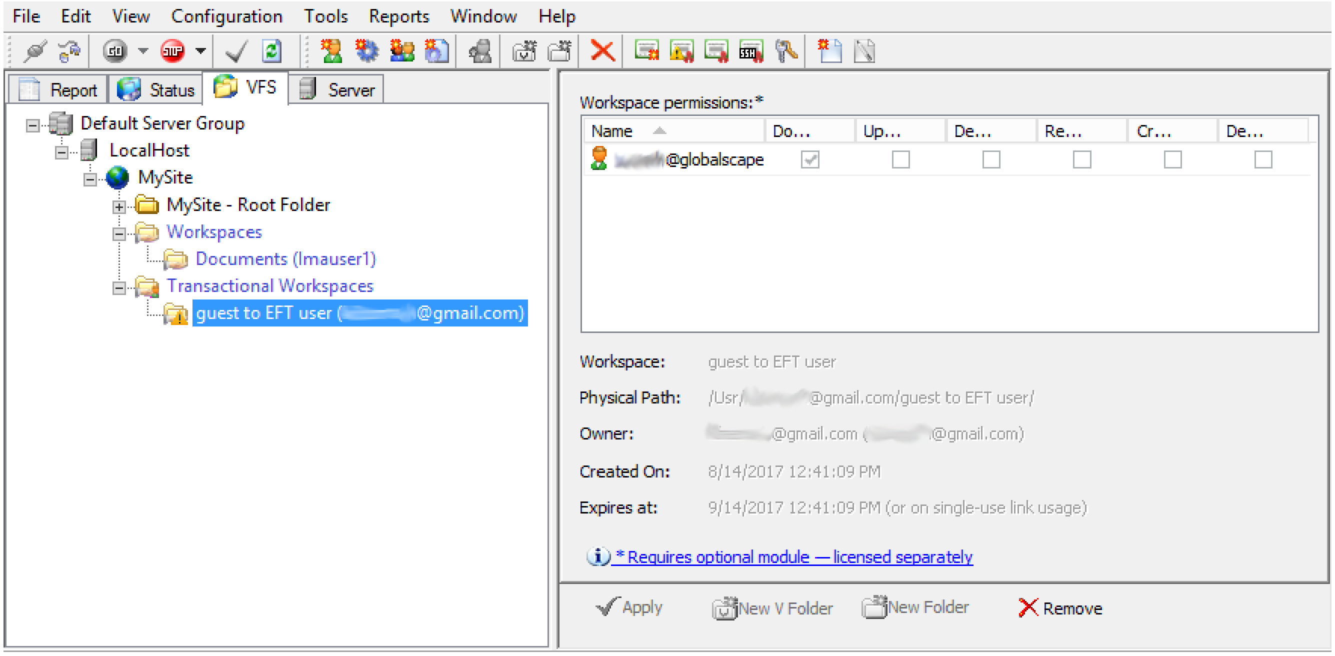
* Requires optional module - licensed separately

5. Select the **Enable folder sharing** check box and **Allow invitations to new EFT users for Workspaces** (if not already selected).

6. Select the **Allow invitations only to these domains** check box, then specify the domain (s) in the text box, comma/semicolon delimited. Wildcards are supported (for example, *.cisco.com or cisco.* or *.*). The setting is not selected by default.
7. Click **OK** to close the dialog box, then click **Apply**.

# Transactional Workspaces

**(Requires HTTP/S, Workspaces )** A Transactional Workspaces is a special kind of Workspace that results from sending a file for pick up from the EFT Outlook Add-In or Drop-Off portal. The recipient only has download permission on the file(s) received. Transactional Workspace participants cannot see each other and cannot subscribe to notifications.



Workspace permissions:*

| Name | Do... | Up... | De... | Re... | Cr... | De... |
|---|---|---|---|---|---|---|
| [redacted]@globalscape | ☑ | □ | □ | □ | □ | □ |

Workspace: guest to EFT user

Physical Path: /Usr/[redacted]@gmail.com/guest to EFT user/

Owner: [redacted]@gmail.com ([redacted]@gmail.com)

Created On: 8/14/2017 12:41:09 PM

Expires at: 9/14/2017 12:41:09 PM (or on single-use link usage)

* Requires optional module — licensed separately

This Workspace is different from normal Workspaces in that a Transactional Workspace:

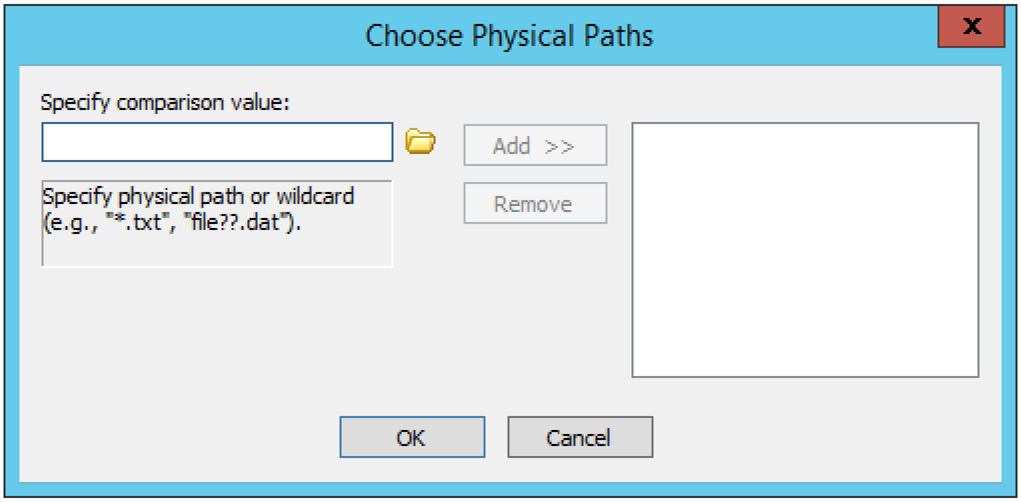
- Accepts anonymous access, if the administrator allows it and the owner/sender chooses
    - Contains folders in the VFS that have been shared via public links (unregistered users) and have an exclamation point on the anonymous-access folder
- Grants permission to download only
- Can't have participants added post creation
- Owner will have little power over it once created

- Is private access, in that participants can't see each other and can't subscribe to notifications (although owner/sender can)
- Is represented in the VFS tab using the Subject line and the sender's username
- Is represented differently in the WTC
- Content gets deleted when it expires
- Is more likely to have a shorter maximum expiration period than regular Workspaces
- Supports self-expiring, single-use file links, which are not supported in regular Workspaces

# Workspaces Conditions

You can apply these Conditions to File Uploaded events.

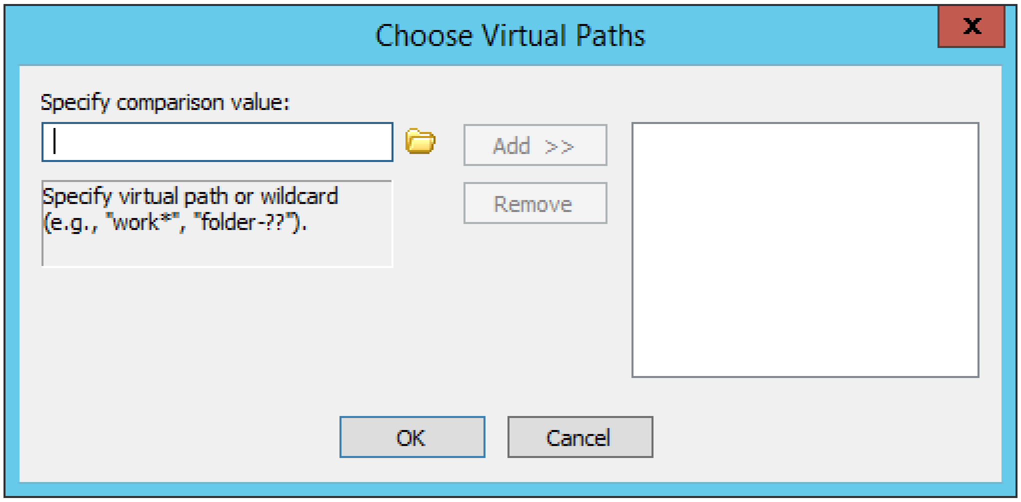
- **If Workspace Physical Path** - Tests whether the physical path does or does not match a path mask. Wildcards can be used.



Specify comparison value:

Specify physical path or wildcard (e.g., "*.txt", "file??.dat").

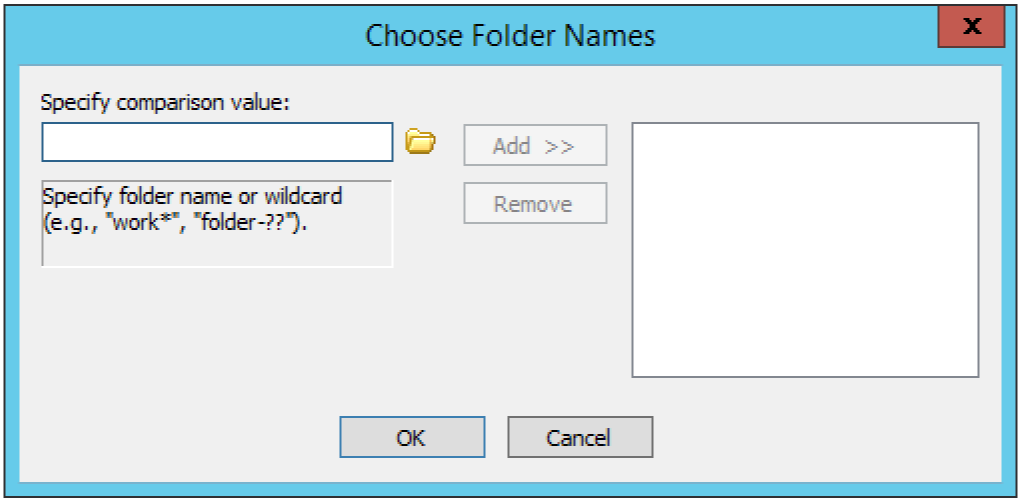
- **If Workspace Virtual Path** - Tests whether the virtual path does or does not match a path mask. Wildcards can be used.



Specify comparison value:

Specify virtual path or wildcard (e.g., "work*", "folder-??").

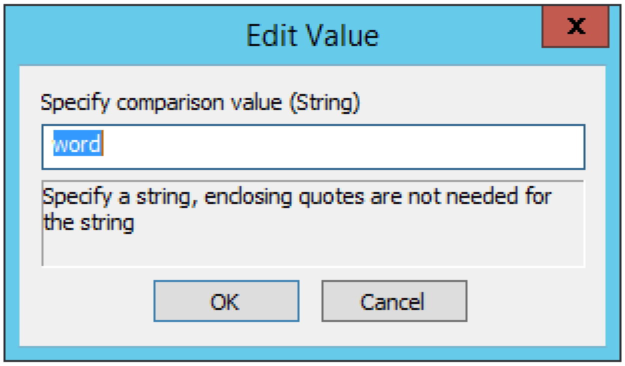
- **If Workspace Name** - Tests whether the folder name does or does not match a mask. Wildcards can be used.



Specify comparison value:

Specify folder name or wildcard (e.g., "work*", "folder-??").

- **If Workspace Participants List** - Tests whether the participant list does or does not contain a string specified.

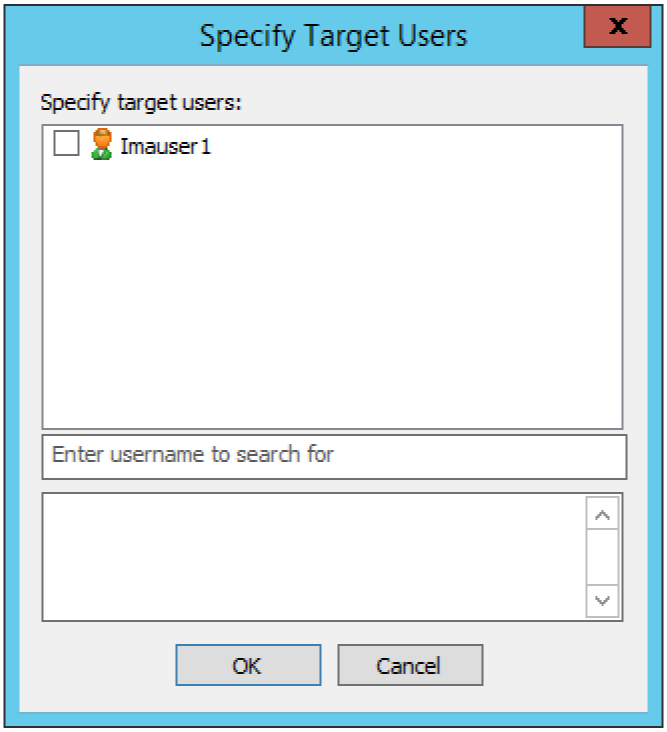


Specify comparison value (String)

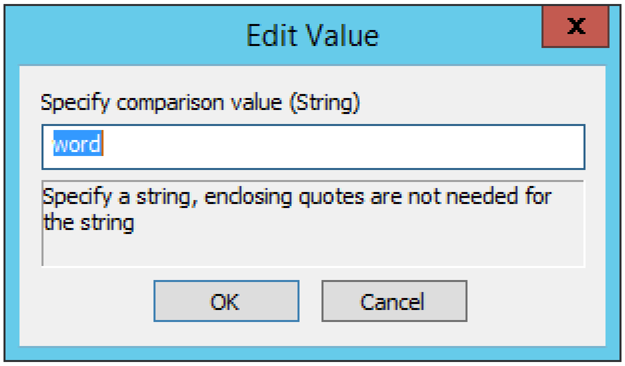
word

Specify a string, enclosing quotes are not needed for the string

- **If Workspace Owner** - Tests whether the Workspace Owner is or is not one of a list of specified users.



- **If Workspace Owner Email Address** - Tests whether the Workspaces Owner email address does or does not contain or is equal to a specified string.



Specify comparison value (String)

word

Specify a string, enclosing quotes are not needed for the string

# Workspaces Invitations

**(Requires HTTP/S, Workspaces )** An EFT administrator can invite internal users to join existing Workspaces in the **VFS** tab. External users cannot be invited via the **VFS** tab; they can only be invited by email address in the Web Transfer Client (WTC).

When a user is invited via the WTC, EFT follows the following logic flow:

1. EFT will first look for a matching email address in the existing Site user profiles and usernames. For example, let's say a Workspaces folder owner invites a user to share a folder with the email address test@gs.com. EFT will search for a user in the existing Site for either a username of "test@gs.com" or a username with an associated email of test@gs.com. If a match is found, then EFT sends an email to the invited user to let them know that they have been invited to share a Workspaces folder. Internal users are not invited, they are automatically joined.
2. If more than one internal user is associated with the invited email address, either by username or profile email address, EFT will decline to add the user.
3. If the email address is not associated with any internal username or email profile and the Site-level **Workspaces** tab has the **Allow invitation to new EFT users for Workspaces** option enabled, then EFT will add the user to the Workspaces folder as a "pending" user, and the user will be invited to create an EFT account to gain access to the shared folder. However, if the option is not enabled, then the invitation request will be denied.

### Internal Users

When adding participants to Workspaces folders, the email address is the unique participant identifier. Existing users will be added to a Workspaces folder only if there is one and only one match for the email address being invited. Before completing an invitation, EFT will check both the username and email address fields for all users on the Site for matching addresses.

- **If two internal EFT users on the same Site have the same email address**, they cannot both be joined to the same Workspaces folder. For example, if user accounts test2 and test3 each have the email address user@gs.com, and the administrator attempts to add users test2 and test3 to a Workspaces folder, EFT will not permit test3 to join, and will state that it's due to duplicate users. In the WTC, the "Unspecified error has occurred" message will appear. If Workspaces trace level logging is enabled, then the log will report the offending email address.
- If one user’s username is the same as another user account's email address and a Workspace owner attempts to invite that address, an error will occur and the user will not be invited.

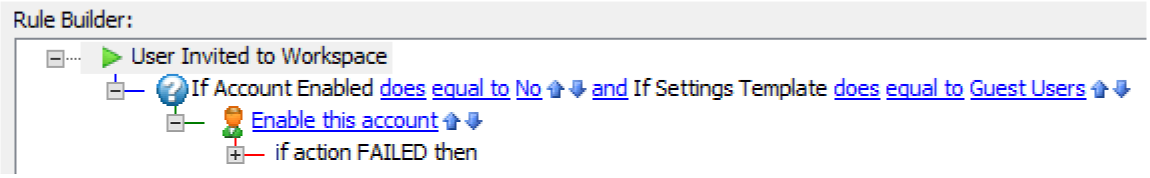
### Guest Users

When guest users are invited to join a Workspaces folder, they must individually accept and activate each Workspaces invitation, then create an account to gain access to the Workspaces folder.

- When guest users join a Workspaces folder, their user accounts are created under EFT's Guest User Settings Template. Guest users are permitted to create Workspaces, but cannot invite new guest users to share the folder. Guest users can only invite users who already have an EFT account.
- The EFT **VFS** tab indicates which users are in the "pending" state, meaning they have not yet accepted their invitations. Once a user accepts an invitation, the "Pending" status is removed. Invited users have 5 days to accept and activate a pending invitation, after which the invitation will expire.
  - You can change the number of days with an Advanced Property named `WorkspaceInviteExpirationPeriodDays`. You can set it to any numerical value. If not set, the default is 5. If set to 0, the invite expiration is the same as the Workspace link expiration.

    If the Workspace invitation has expired before the invitee attempts to register, a prompt appears that says the invitation cannot be found.
- Workspace owners and EFT administrators are not notified when an user's invitation expires. When an invitation expires, the user is automatically removed from the Workspaces folder and no longer will appear as a pending user. To re-invite a user whose invitation has expired, the Workspaces owner, via the WTC, has to re-invite the user, at which point the invited user will go back into a pending status and will again have 5 days (by default; see Advanced Property above) to activate the account.

  Pending user status can only be viewed via the **VFS** Tab.
- A guest account that has been disabled (for example, due to the Workspace expiring) doesn't automatically get re-enabled if a new invitation is sent to them. If you send an invite to an account that was previously disabled by EFT due to expired links, EFT can re-enable the account via an Event Rule using the "User Invited to Workspace" event, the "If Account Enabled," "If Workspace User Account Exists," and "If Settings Template" is Guest Users Conditions, and the "User Account" action set to Enable this account:



Rule Builder:

User Invited to Workspace

If Account Enabled does equal to No and If Settings Template does equal to Guest Users

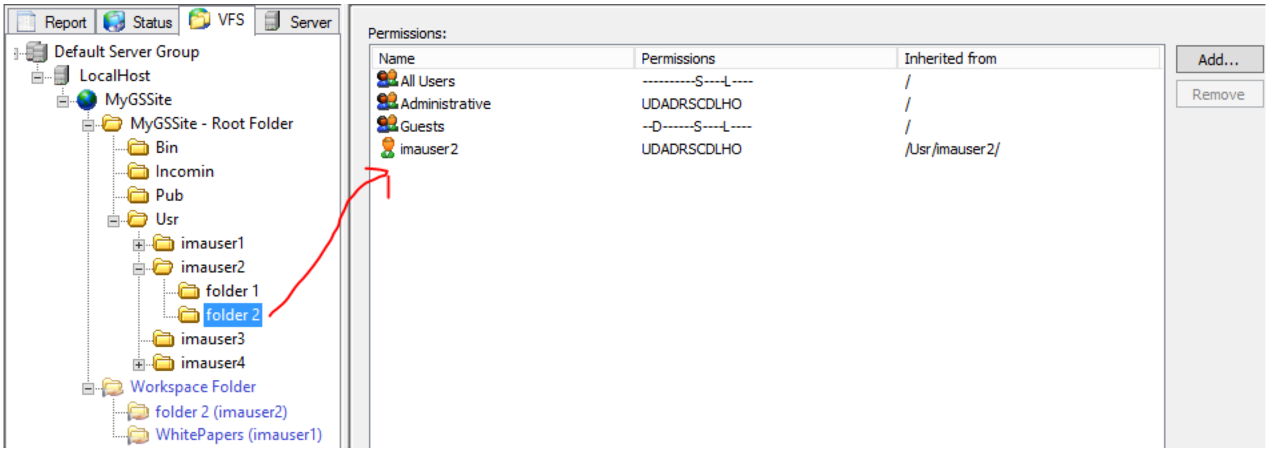
Enable this account

if action FAILED then

# Workspaces Permissions

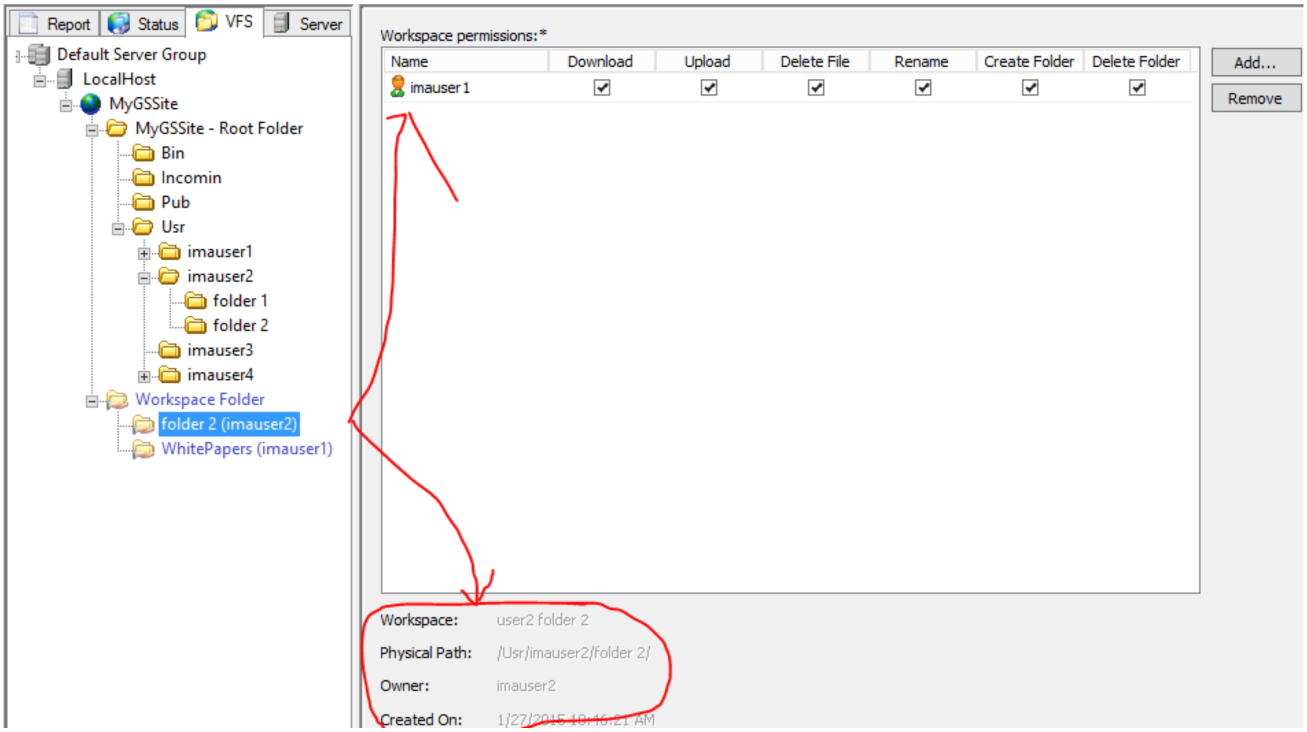
Workspaces permissions are separate from the VFS permissions, such as those permissions for the **Usr** folders. Users who have Workspaces permissions on a folder will not appear in the VFS permissions for that folder. For example (as shown below):

1. "imauser2" has full permissions on the \Usr\imauser2\ folder in VFS.
2. In Workspaces, "imauser2" has shared a folder called "folder 2" with "imauser1."
3. When the administrator clicks "folder 2" in the Workspace Folder tree, you can see that "imauser1" has Workspaces permissions on that folder.
4. However, only "imauser2" has VFS permissions on that folder.



Permissions:

| Name | Permissions | Inherited from |
|---|---|---|
| All Users | ----------S----L---- | / |
| Administrative | UDADRSCDLHO | / |
| Guests | --D------S----L---- | / |
| imauser2 | UDADRSCDLHO | /Usr/imauser2/ |



Workspace permissions:*

| Name | Download | Upload | Delete File | Rename | Create Folder | Delete Folder |
|---|---|---|---|---|---|---|
| imauser1 | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |

Workspace: user2 folder 2
Physical Path: /Usr/imauser2/folder 2/
Owner: imauser2
Created On: 1/27/2015 10:46:21 AM

## Workspaces Permissions on an Active Directory Site

Workspaces has the ability to invite external users on an Active Directory Site. Described below is what occurs when a non-AD account has been invited to a Workspace, what permissions the EFT Server enforces for file activity, and how that applies to the "Comments" feature of Workspaces. This is important because the basic behavior of an AD Site, independent of Workspaces, is that any client that logs in as an AD account will subsequently access all files exposed by EFT's protocol engines using that very same AD account used to log in (known as "impersonation"). Thus, it is not EFT that enforces file system permissions to local and UNC paths; it is the Windows operating system.

When EFT allows non-AD users to gain access to this Site (when we allow invitations to external parties) then we no longer impersonate an AD user and, therefore, our EFT application is limited in access by the service account under which it runs; ***however,*** this might be more permissive than the permissions for any individual user in the AD server.

For example, suppose your organization's AD users have READ/WRITE access to everything on a shared drive, and have explicit DELETE permission to our own folder but no one else's folder. Suppose the IT administrator set up a Folder Monitor rule against the shared drive. The IT administrator would have to run the EFT service as an AD account that had READ/WRITE/DELETE permissions across the whole shared drive so that the Folder Monitor workflows can move or delete files, or so that the EFTArchive operation worked, and so on.

Suddenly, there is a security concern: Any externally invited Workspace user will act against the shared drive the same as the EFT service account, not an individual AD account.

**THEREFORE**¸ our application itself must impose permissions checks on all file access for such accounts (which, by the way, is exactly how LDAP, Local, and ODBC authentication work).

EFT server will perform a permissions check on any assignment of Workspaces permissions to a participant (creation or modification time). EFT compares the OWNER permissions to the requested Workspaces permissions for a participant, and ensures at that moment that the OWNER does not grant MORE permission to a given folder than that which the owner of the folder holds.

All file activity within a Workspace is managed by EFT to conform to ONLY those permissions allowed by the Workspace configuration. Therefore, EFT enforces that Workspace permissions are equal to or less privileged than the owner's permissions, regardless of the service account under which EFT operates.

Below is a summary table that describes the permissions checks EFT applies to Workspace file and Comments activity for both **OWNERS** and for **PARTICIPANTS** upon adding or modifying participants in a Workspace:

| Operation on file or comments | Required Owner EFT VFS permissions | Required Participant Workspace permissions |
|---|---|---|
| ADD | PERMISSION_FILE_APPEND or PERMISSION_FILE_UPLOAD | canUploadFile |
| UPDATE | PERMISSION_FILE_APPEND or PERMISSION_FILE_UPLOAD | canUploadFile |
| DELETE | PERMISSION_FILE_APPEND or PERMISSION_FILE_UPLOAD | canUploadFile |
| GET | PERMISSION_DIR_LIST | N/A – Means that Participant can read comment because Owner invited them to Workspace. |

For example, for the invited user to be able to comments to files, ***both*** of the following conditions must be met:

- Owner must have **Append** or **Upload** EFT VFS permission for that file.
- Participant (invitee) must be granted the **Upload** Workspace permission by the inviter.

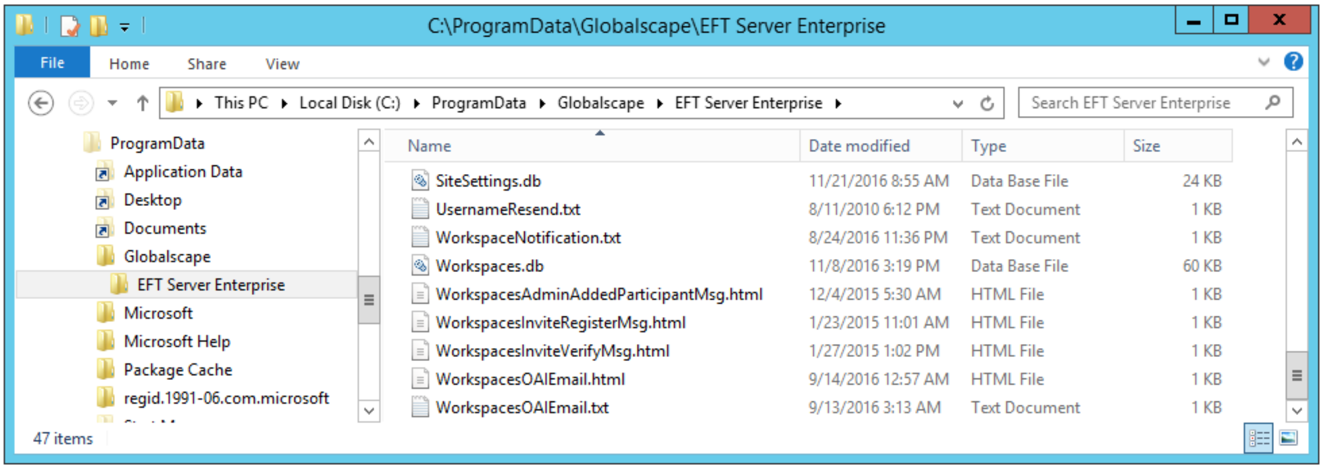
# Workspaces Notifications

**(Requires Workspaces)** When a Web Transfer Client user shares a folder, an invitation is sent to the user with whom the folder is shared. If the recipient does not have an account on EFT, the user can register the account. For invitations sent to non-EFT users, an email is sent to verify the account when the user registers the account.

The text for the invitation and verification emails is contained in an HTML file that can be customized for localization or to provide company-specific information.

Workspaces invitations expire after 5 days.

The files are stored in the ProgramData directory (by default, **C:\ProgramData\Globalscape\EFT Server**) and apply to all Sites on the Server. (The path is shown on the Server's **General** tab, under **General Settings > Server configuration settings**.)


C:\ProgramData\Globalscape\EFT Server Enterprise
File
Home
Share
View
This PC ▸ Local Disk (C:) ▸ ProgramData ▸ Globalscape ▸ EFT Server Enterprise ▸
Search EFT Server Enterprise
ProgramData
Application Data
Desktop
Documents
Globalscape
EFT Server Enterprise
Microsoft
Microsoft Help
Package Cache
regid.1991-06.com.microsoft
47 items

| Name | Date modified | Type | Size |
|---|---|---|---|
| SiteSettings.db | 11/21/2016 8:55 AM | Data Base File | 24 KB |
| UsernameResend.txt | 8/11/2010 6:12 PM | Text Document | 1 KB |
| WorkspaceNotification.txt | 8/24/2016 11:36 PM | Text Document | 1 KB |
| Workspaces.db | 11/8/2016 3:19 PM | Data Base File | 60 KB |
| WorkspacesAdminAddedParticipantMsg.html | 12/4/2015 5:30 AM | HTML File | 1 KB |
| WorkspacesInviteRegisterMsg.html | 1/23/2015 11:01 AM | HTML File | 1 KB |
| WorkspacesInviteVerifyMsg.html | 1/27/2015 1:02 PM | HTML File | 1 KB |
| WorkspacesOAIEmail.html | 9/14/2016 12:57 AM | HTML File | 1 KB |
| WorkspacesOAIEmail.txt | 9/13/2016 3:13 AM | Text Document | 1 KB |

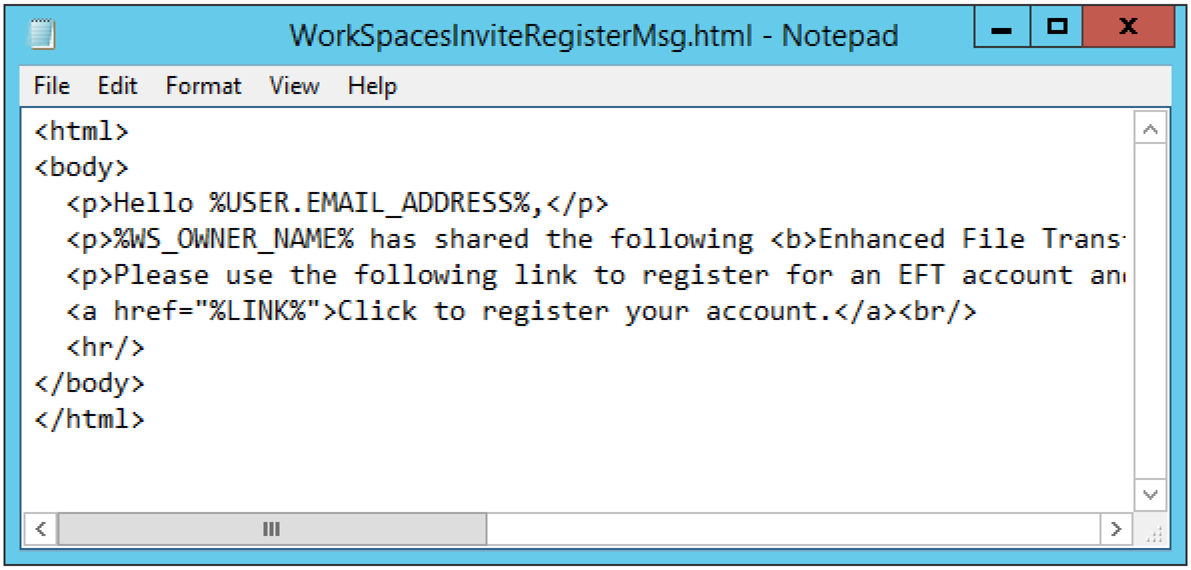
You can edit the files in any text editor. Note that the "WS" variables used in these notification templates are used only in these templates. They are not Event Rules variables. (Refer to Workspaces Events and Workspaces-Related Variables for additional means of notification.)

The files are named per their function:

- WorkspaceNotification.txt - Used to notify the Workspace owner that a recipient took an action on a file.
- WorkspacesadministratorAddedParticipantMsg.html - Used to notify recipients that a Workspace was shared with them.
- WorkspacesInviteRegisterMsg.html - Used to notify recipients that a Workspace was shared with them and they are invited to register an account on EFT.
- WorkspacesInviteVerifyMsg.html - Sent after recipient has registered for an EFT account and needs to verify the account.
- WorkspacesOAIEmail.html - Notification to recipients that a file has been sent from Outlook.
- WorkspacesOAIEmail.txt - Text version of the notification to recipients that a file has been sent from Outlook.
- WorkspacesOAIEmailWithSecureMB.html - Notification to recipients that a file has been sent from Outlook with secure message body.
- WorkspacesOAIEmailWithSecureMB.txt - Text version of the notification to recipients that a file has been sent from Outlook with secure message body.
- WorkspacesRequestFileEmail.html - Notification to sender that a file has been requested.
- WorkspacesRequestFileEmail.txt - Text version of the notification to sender that a file has been requested.

### To edit the Workspaces invite and verify messages

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, click the **Server** node.
3. In the right pane, click the **General** tab.
4. In the **General Settings** area, next to **Workspaces invite message**, click the browse icon. Your default text editor (for example, Notepad) opens with the invitation text in HTML.



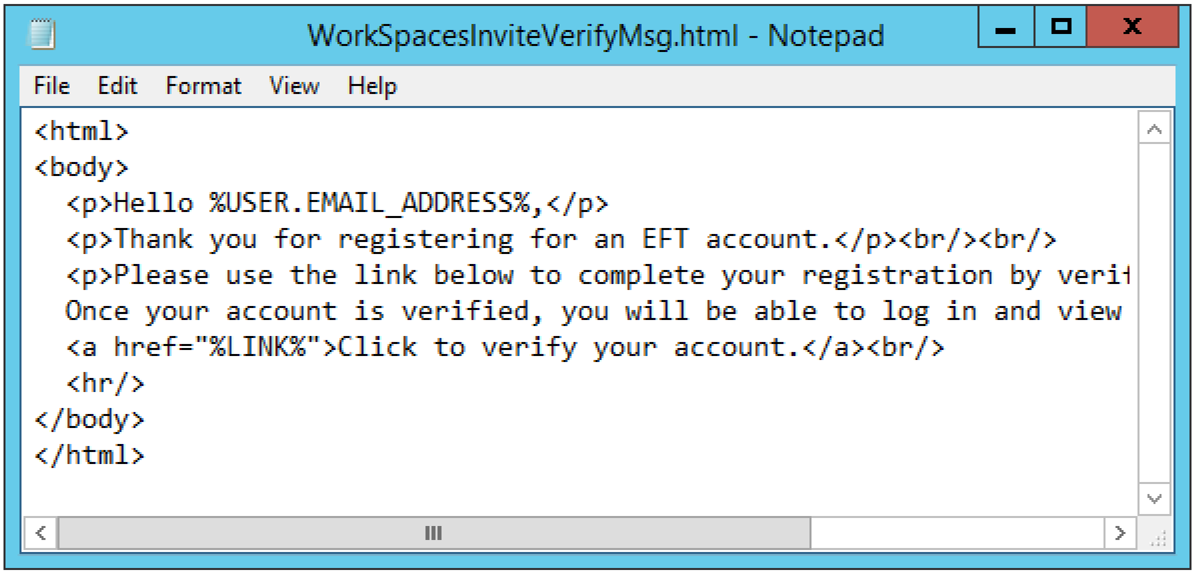
WorkSpacesInviteRegisterMsg.html - Notepad
File Edit Format View Help

```
<html>
<body>
  <p>Hello %USER.EMAIL_ADDRESS%,</p>
  <p>%WS_OWNER_NAME% has shared the following <b>Enhanced File Trans
  <p>Please use the following link to register for an EFT account an
  <a href="%LINK%">Click to register your account.</a><br/>
  <hr/>
</body>
</html>
```

Edit the text as needed, being careful not to delete the variables (%USER.EMAIL_ADDRESS%, %WS_OWNER_NAME%, %FOLDER_NAME%, %LINK%), then save the file and close the text editor.

The WS_ variables are not Event Rule variables. To use Workspaces variables in Event Rules, refer to the Variables list.

5. Next to **Workspaces verify message**, click the browse icon. Your default text editor (for example, Notepad) opens with the verify text in HTML.

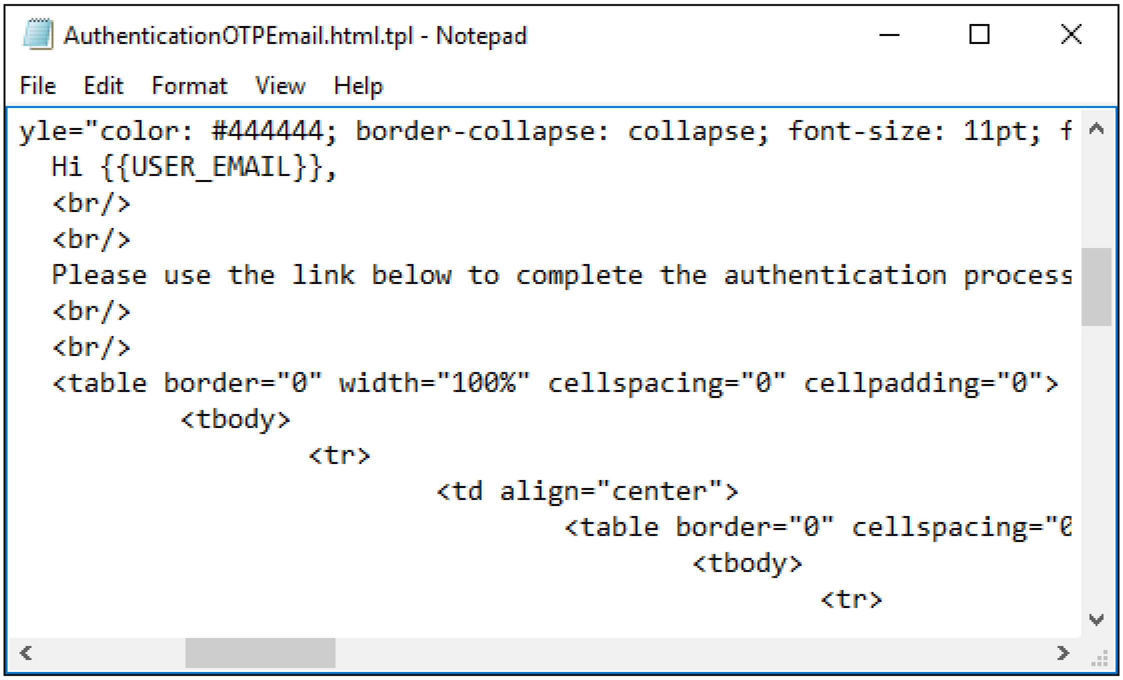


WorkSpacesInviteVerifyMsg.html - Notepad
File Edit Format View Help

```
<html>
<body>
  <p>Hello %USER.EMAIL_ADDRESS%,</p>
  <p>Thank you for registering for an EFT account.</p><br/><br/>
  <p>Please use the link below to complete your registration by veri
  Once your account is verified, you will be able to log in and view
  <a href="%LINK%">Click to verify your account.</a><br/>
  <hr/>
</body>
</html>
```

6. Edit the text as needed, being careful not to delete the variables (%USER.EMAIL_ADDRESS%, %LINK%).

7. In the **General Settings** area, next to **Authentication OTP message**, click the browse icon. Your default text editor (for example, Notepad) opens with the message text in HTML.



```
yle="color: #444444; border-collapse: collapse; font-size: 11pt; f
  Hi {{USER_EMAIL}},
  <br/>
  <br/>
  Please use the link below to complete the authentication process
  <br/>
  <br/>
  <table border="0" width="100%" cellspacing="0" cellpadding="0">
          <tbody>
                  <tr>
                          <td align="center">
                                  <table border="0" cellspacing="0
                                          <tbody>
                                                  <tr>
```

8. Edit the text as needed, being careful not to delete the variables, such as {{USER.EMAIL}}, then save the file and close the text editor.
9. Save the file and close the text editor.

### To create Site-specific versions

1. Make a copy of the existing template.
2. Make your edits (using a text editor, such as Notepad), being careful not edit any of the variables or necessary code.
3. Save the edited version with the Site name and an underscore prepended to the front if the filename. For example, name it `MyFrenchSite_PasswordResetMsg.html`