<table>
<thead>
<tr>
<th><strong>GlobalSCAPE, Inc. (GSB)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Corporate Headquarters</strong></td>
</tr>
<tr>
<td><strong>Address:</strong> 4500 Lockhill Selma Road, Suite 150, San Antonio, TX (USA) 78249</td>
</tr>
<tr>
<td><strong>Sales:</strong> (210) 308-8267</td>
</tr>
<tr>
<td><strong>Sales (Toll Free):</strong> (800) 290-5054</td>
</tr>
<tr>
<td><strong>Technical Support:</strong> (210) 366-3993</td>
</tr>
<tr>
<td><strong>Web Support:</strong> <a href="http://www.globalscape.com/support/">http://www.globalscape.com/support/</a></td>
</tr>
</tbody>
</table>

© 2008-2018 GlobalSCAPE, Inc. All Rights Reserved

*October 23, 2018*
# Table of Contents

**WTC & Workspaces**

WTC & Workspaces Administration................................................................. 9

Workspaces Overview.................................................................................. 9

Licensing Workspaces............................................................................... 10

Workspaces Licensing versus Web Transfer Client Licensing.................. 11

Enabling User Access to the Web Transfer Client...................................... 11

Enable and Configure EFT Workspaces.................................................... 12

Enable Workspaces to Send Files.............................................................. 14

Allow Secure File Sending....................................................................... 17

Enable-Disable Workspaces Reply Portal................................................. 17

Enable and Configure the Workspaces - Drop-Off Portal......................... 18

Localization (Language) Settings............................................................... 21

Restrict Workspaces Invitations to Specific Domains............................... 23

Transactional Workspaces....................................................................... 23

Workspaces Invitations........................................................................... 25

Workspaces Notifications......................................................................... 26

Workspaces Permissions.......................................................................... 29

Managing Workspaces in the VFS......................................................... 32

Workspaces Conditions.......................................................................... 33

Customizing the Email Interface............................................................. 35

Rebranding (Customizing) the Web Transfer Client................................ 36

Customizing the WTC............................................................................. 38

Disable CRC.......................................................................................... 41

Disabling “Update Your Browser” Prompts............................................. 42

Login to EFT (WTC).............................................................................. 42

Form-Based Authentication versus Basic Authentication...................... 43

Terms and Conditions............................................................................ 43

Upgrading the Web Transfer Client (HTML5 version)............................. 44
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conceal WTC and Its Content from Searches</td>
<td>46</td>
</tr>
<tr>
<td>Display Full Name of User in WTC on LDAP Site</td>
<td>46</td>
</tr>
<tr>
<td><strong>WTC &amp; Workspaces User Guide</strong></td>
<td>47</td>
</tr>
<tr>
<td>Overview of the Web Transfer Client</td>
<td>47</td>
</tr>
<tr>
<td>File-Naming Conventions</td>
<td>47</td>
</tr>
<tr>
<td>Unicode File Transfers</td>
<td>48</td>
</tr>
<tr>
<td>Enabling JavaScript in the Browser</td>
<td>51</td>
</tr>
<tr>
<td>Logging In</td>
<td>52</td>
</tr>
<tr>
<td>Logging Out</td>
<td>53</td>
</tr>
<tr>
<td>Automatic Log Out</td>
<td>53</td>
</tr>
<tr>
<td>Uploading Files and Folders</td>
<td>53</td>
</tr>
<tr>
<td>Downloading Files</td>
<td>55</td>
</tr>
<tr>
<td>Canceling a Transfer</td>
<td>56</td>
</tr>
<tr>
<td>Clearing the Upload Manager</td>
<td>56</td>
</tr>
<tr>
<td>Resuming Transfers</td>
<td>56</td>
</tr>
<tr>
<td>Filtering and Sorting the File Name Pane</td>
<td>57</td>
</tr>
<tr>
<td>Searching for Files</td>
<td>57</td>
</tr>
<tr>
<td>Creating Folders</td>
<td>58</td>
</tr>
<tr>
<td>Moving Files between Folders</td>
<td>58</td>
</tr>
<tr>
<td>Renaming a File or a Folder</td>
<td>58</td>
</tr>
<tr>
<td>Deleting a Folder or File</td>
<td>59</td>
</tr>
<tr>
<td>File Comments</td>
<td>59</td>
</tr>
<tr>
<td>Send/Email Files from within the WTC</td>
<td>60</td>
</tr>
<tr>
<td>Sharing Folders (Creating a Workspace)</td>
<td>62</td>
</tr>
<tr>
<td>Add Workspace Participants</td>
<td>65</td>
</tr>
<tr>
<td>Joining a Workspace</td>
<td>65</td>
</tr>
<tr>
<td>Expire a Workspace</td>
<td>67</td>
</tr>
<tr>
<td>Edit-Rmove Workspace Permission</td>
<td>67</td>
</tr>
<tr>
<td>Stop Sharing a Workspace</td>
<td>67</td>
</tr>
<tr>
<td>Notifications</td>
<td>68</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Edit Notification Options</td>
<td>69</td>
</tr>
<tr>
<td>Using the Drop-Off Portal</td>
<td>70</td>
</tr>
<tr>
<td>Picking Up Files</td>
<td>71</td>
</tr>
<tr>
<td>Reply Portal</td>
<td>72</td>
</tr>
<tr>
<td>Request Files</td>
<td>74</td>
</tr>
<tr>
<td>Guest Users</td>
<td>75</td>
</tr>
<tr>
<td>Changing Your Password</td>
<td>76</td>
</tr>
<tr>
<td>Error Messages</td>
<td>77</td>
</tr>
<tr>
<td>Logging</td>
<td>77</td>
</tr>
<tr>
<td>Glossary</td>
<td>79</td>
</tr>
<tr>
<td>Index</td>
<td>89</td>
</tr>
</tbody>
</table>
WTC & Workspaces

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:

- **Workspaces** - Users (with a Workspaces license) can share files and folders 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.

- **Web Transfer Client (WTC)** - The WTC is a 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.

  - If the user is trying to connect to the WTC with an older, unsupported browser, a "plain text" client (shown below) appears instead of the WTC.
  
  - If the administrator has not enabled the WTC for a Settings Template or user account, a "plain text" client appears instead of the WTC.

![WTC Client](image)

NOTE: Web Transfer Client Access has been disabled for this user or container. Reverting to basic client.
• 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. Refer to Mobile Transfer Client (MTC) for details.

• 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 Explorer - When logged in to the EFT computer, administrators can manage files on EFT using Windows 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 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. To allow an FTP session via a command line to accept double slashes // when navigating paths, in EFT v7.2 and later, you must enable the following registry setting on the EFT server:

```plaintext
HKEY_LOCAL_MACHINE\SOFTWARE\GlobalSCAPE Inc.\EFT Server 7.2\FixDoubleSlashInPathsForFTP 0 = disabled; 1 = enabled
```
WTC & Workspaces Administration

The topics in this section describe administration of the Web Transfer Client (WTC) and Workspaces. For instructions for using the Web Transfer Client Workspaces, refer to the WTC & Workspaces User Guide.

Workspaces Overview

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.

**Licensing Workspaces**

Licenses are purchased per number of Workspaces owners, not the number of Workspaces created. For example, if you purchase a 25-seat license, 25 users can create Workspaces; there is no limit to the number of Workspaces each owner may possess. During the EFT 30-day trial, you can have up to 100 Workspaces owners. You can allow or deny Workspaces creation to specific users.

- If you are using an EFT version prior to 7.4.7, you should *disallow* the creation of Workspaces on Guest accounts to ensure that Workspaces license are available for internal users. This applies all guest accounts, including those created when using the Drop-Off portal.
- In v7.4.7 and later, the ability to create Workspaces is disabled by default on the Guest Accounts Settings Template. Disabling creation of Workspaces on Guest Accounts ensures that Workspaces licenses are available for internal users. On the **Connections** tab, you can disable or enable the creation of Workspaces on the Guest Accounts Settings Template for all Guest accounts or on each Guest account individually. This applies all guest accounts, including those created when using the Drop-Off portal.
- After a guest has been invited to join a Workspace and has created an account and logged in, the guest account will appear (if so configured) in the Guest Users Settings Template. In EFT versions prior to 7.4.7, this account will consume a Workspaces license until you disallow the creation of Workspaces on that account or in the Settings Template. This applies all guest accounts, including those created when using the Drop-Off portal.

Workspaces are viewed and created in the Web Transfer Client (WTC); therefore, if a user does not have access to the Web Transfer Client, the user cannot create or access a shared Workspace. If the user cannot access the WTC, the “plain text client” (PTC) appears when the user logs in. Starting in EFT v7.4.6, during the EFT 30-day trial, you can have up to 100 Workspaces owners.
Workspaces Licensing versus Web Transfer Client Licensing

Workspaces are viewed and created in the Web Transfer Client (WTC); therefore, if a user does not have access to the Web Transfer Client, the user cannot create or access a shared Workspace. If the user cannot access the WTC, the "plain text client" (PTC) appears when the user logs in.

The flowchart below describes what occurs when a user logs in to EFT in a browser.

Enabling User Access to the Web Transfer Client

(Requires the HTTP/S module in EFT SMB/Express) 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.
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.

4. In the **Protocols** area, select the **Allow Web Transfer Client over HTTPS** check box.

   *HTTPS must also be enabled.*

5. Click **Apply**.

Enable and Configure EFT 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.

Refer to [Licensing Workspaces](#) for important information regarding Guest Accounts.

To enable Workspaces

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 **Workspaces** tab.

4. Select the **Enable Workspaces** check box. The Guest Accounts Settings Template appears under User Settings Templates.

5. Under **Workspaces Configuration**, specify whether to allow EFT users to send invitations to users not in the EFT user authentication database.
   - **Allow invitations to new EFT users for Workspaces**
     - (Optional) Specify the domains to which Workspaces users can send invitations, comma/semicolon delimited. Wildcards are supported (e.g., *.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 have specified *.domain.com, then the domain www.domain.com is allowed.
   - **Allow Workspaces shared with the 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.

6. 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.

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. (The default is to Disable account and 7 days; when set to 0, the account(s) will be cleaned up at midnight.)
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 w/s owner, regardless of any protocols used to access the account.

8. Click **Apply** to save the settings.

### To enable Workspaces for 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.
4. In the **Protocols** area, select the **Allow Creation of Workspaces** 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 the use of the Outlook add-in, ensure that the **Allow secure file sending** check box is selected.
6. Click **Apply**.

### Enable Workspaces to Send Files

Workspaces for Outlook is an enterprise ad hoc file transfer solution that allows employees to quickly and securely send large files right from within 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 can quickly and easily send large files via email from within Microsoft Outlook via the dedicated add-in, and 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.
• Before using this feature, the EFT administrator must enable Workspaces and install and enable the EFT Outlook Add-In, as described below.

• (In v7.4.7 and later) When you send a file using the WTC, 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.

To enable Workspaces for Outlook

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 Workspaces tab.
4. Select the Enable Workspaces check box, then click Apply.
5. To configure Workspaces, do one of the following:

   • Select the Enable secure file sending check box.

6. Under Authorized users 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.

9. 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.

10. Specify the **maximum expiration period for pickup links**. The default is 1 month.

11. Do one of the following to deploy the EFT Outlook add-in on end-users’ computers:
   - Use the EFT Outlook add-in installer:
     - Click **Browse** to open the EFT installation folder, get the EFT Outlook add-in installer, and install the EFT Outlook Add-In as described in Installing the EFT Outlook Add-In.
   - OR -
   - Use the **Outlook add-in deployment script**:
     a. Click **View** to open the **Outlook Add-in Deployment Script** box.
     b. Copy and paste the script into the tool you are using to deploy the Outlook Add-In across your organization.
     c. Click **OK** or press ENTER to close the **Outlook Add-in Deployment Script** box.
     d. Edit the script to match your environment (i.e., the EFTHOST IP address and port, username, password).
EFT supports Manual authentication, which is really Basic authentication, so you have to explicitly provide the user’s EFT username and password (that is, the username and password that this Add-In user uses to log in to EFT—not the admin credentials). EFT also supports Integrated Windows Authentication (IWA) where you don’t have to explicitly provide a username and password if you are logged into Windows with your domain account.

Edit the Add-In installer command-line arguments depending on the authentication type you want:

- **For manual authentication**, do the following (EFTUSERNAME and EFTPASSWORD values have to be substituted with the actual Add-in user’s EFT username and password):
  ```
  msiexec /Iv installation.log /qn /i EFTOutlookAddinInstaller.msi EFTHOST=https://WIN-KST875BEENP EFTPORT=443 EFTAUTHTYPE=MANUAL EFTUSERNAME=username EFTPASSWORD=test123! INSTALLLOCATION=%userprofile%\AppData\Roaming\GlobalSCAPE\EFT Outlook Add-in" FILESTORELOCATION=%userprofile%\AppData\Local\GlobalSCAPE\EFT Outlook Add-in"
  ```

- **For Integrated Windows authentication**, do the following (EFTUSERNAME and EFTPASSWORD don’t need to be supplied):
  ```
  msiexec /Iv installation.log /qn /i EFTOutlookAddinInstaller.msi EFTHOST=https://WIN-KST875BEENP EFTPORT=443 EFTAUTHTYPE=IWA INSTALLLOCATION=%userprofile%\AppData\Roaming\GlobalSCAPE\EFT Outlook Add-in" FILESTORELOCATION=%userprofile%\AppData\Local\GlobalSCAPE\EFT Outlook Add-in"
  ```

**Allow Secure File Sending**

Using Workspaces in the WTC and in Outlook, you can send files securely, and your recipients can reply to you securely. Before users can send the message body securely, you must first enable secure file sending on the **Workspaces - Send** tab and the Settings Template or User account must have **Allow secure file sending** enabled.

Refer to the topics below for details of enabling secure file sending in Workspaces and in Outlook.

- Enable and Configure EFT Workspaces
- Workspaces for Outlook
- Enable Workspaces to Send Files
- Reply Portal
- Drop-Off Portal

**Enable-Disable Workspaces Reply Portal**

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 the Reply portal (in EFT v7.4.7 and later). It is enabled by default.

*Disabling the Reply portal removes the Request File(s) functionality from the Web Transfer Client interface.*
To enable or disable the reply 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 **Workspaces - Send** tab.
4. Select or clear the **Enable reply portal** check box, then click **Apply**.
5. Click **Apply**.

Enable and Configure the Workspaces - Drop-Off Portal

The Workspace 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 and the **Workspaces - Drop Off** tab.

For additional security, you can configure Google's reCAPTCHA on the Site, as described below.

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. Ensure that **Workspaces** and **secure file sending** is enabled and configured.
4. In the right pane, click the **Workspaces - Drop-Off** tab.
5. Select the **Enable the “drop-off” portal** check box.

6. Specify a portal reserved path if you want something different from the default (/dropoff).

7. (Optional) **To use captcha**, select the **Enable reCAPTCHA** check box.
   - In the **Site Key** box, paste the Google Site Key.
   - In the **Secret Key** box, paste the Google Secret Key.

8. (Optional) Specify the period before a pickup link expires.

9. (Optional) Specify the **Maximum message size**.

   **Note:** If the **Maximum message size** check box is not selected, the maximum message size is 3 GB. Knowledgebase article #11389 describes a registry setting that you can use to set the maximum anonymous uploads size in GB. If the "MaxAnonymousAllUploadsSizeInGB" value in the registry is set to a value that is LESS than **Maximum message size** on the **Workspaces - Drop-Off** tab, an error occurs stating that the file is too large.

10. Specify the Secure the message body setting: **Always secure**, **Never secure**, or **User Choice**. User choice is the default.

11. (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. 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.

12. 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.

13. Click Apply.

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/admin and log in to your Google account.
2. Click reCAPTCHA v2. The Domains box appears.

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.

   ① Adding reCAPTCHA to your site
   • Keys

   Site key
   Use this in the HTML code your site serves to users.
   eLdkgEsUAAAAALDQyHh0GwThHLOMh1KcfvVRmUv

   Secret key
   Use this for communication between your site and Google. Be sure to keep it a secret.
   eLdkgEsUAAAAALDQyHh0GwThHLOMh1KcfvVRmUv

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.

Localization (Language) Settings

The EFT administrator can specify which language is the default by editing the WTC configuration file. However, the end-user’s browser settings take precedence over the default language setting. English is used if the browser and the default languages are not available.

For example, if the browser is set to German, it will automatically use German, no matter what is in the configuration file. You can also add other languages by translating the language file and adding it to the configuration file.

The language files, e.g., main_en.json, are saved in C:\Program Files (x86)\Globalscape\EFT Server Enterprise\web\public\EFTClient\jument\i18n. Be sure to not edit any of the code, just edit the display text. That is, in the example below, you would only change the highlighted text between the quotation marks.
Be sure to make a copy of the file and then edit the copy, so you can revert, if necessary. The language file must be named `main_<country code>.json`. A list of ISO 2-letter codes can be found online, such as [http://www.nationsonline.org/oneworld/country_code_list.htm](http://www.nationsonline.org/oneworld/country_code_list.htm).

For example, a French language file would be named `main_fr.json`, and the code in the configuration file would be:

```json
{   code: 'fr',   name: 'Française',   region: 'France' },
```

### To specify the default language setting

1. In `C:\Program Files (x86)\Globalscape\EFT Server Enterprise\web\public\EFTClient\jument\scripts`, find the `adminConfig.js` file. (There is a number in front of the name.)

2. Open the configuration file in a text editor, such as Notepad++.

3. Look for the “Defines the languages available” section and the following text:

   ```javascript
   ```

4. The default language appears first. For example, if you want German (`Deutsche`) to be the default language, move it to the top.

5. If you create your own language file, add it to the language section in the configuration file.
6. Instruct users to refresh the browser and/or clear the browser history to see the changes.

**Restrict Workspaces Invitations to Specific Domains**

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 **Workspaces** tab.

4. Under **Workspaces Configuration**, 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 (e.g., *.cisco.com or cisco.* or *.*). The setting is not selected by default. (**Allow invitations to new EFT users for Workspaces** must be selected.)

5. Click **Apply**.

**Transactional 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. The recipient only has download permission on the file(s) received. Transactional Workspace participants cannot see each other and cannot subscribe to notifications.
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

Related Topic

- Managing Workspaces in the VFS
**Workspaces Invitations**

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 e-mail 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 e-mail 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 e-mail address and a Workspace owner attempts to invite that address, an error will occur and the user will not be invited.**

**External (non-EFT) Users**

When external users are invited to join a Workspaces folder, they must individually accept and activate each and every Workspaces invitation. The recipient must accept each invitation and fill out the “Already Have an Account” form to gain access to the Workspaces folder.
- EFT doesn't provide any sort of visual indicator to distinguish between internal users vs. external users. When external users join a Workspaces folder, their user accounts are created under EFT's Default User Settings Template. External users are permitted to create Workspaces, but cannot invite new external users to share the folder. External 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. Externally invited users have 5 days to accept and activate a pending invitation, after which the invitation will expire. This is a hard-coded value and cannot be modified.

- Workspace owners and EFT administrators are not notified when an external 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. There is no resend-invitation option. In order to re-invite an external 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 to activate the account. Pending user status can only be viewed via the VFS Tab.

**Workspaces Notifications**

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 Enterprise`) and apply to all Sites on the Server. (The path is shown on the Server’s General tab, under General Settings > Server configuration settings.)
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.

The files are named per their function:

- **WorkspaceNotification.txt** - Used to notify the Workspace owner that a recipient took an action on a file.
- **WorkspacesAdminAddedParticipantMsg.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 (e.g., Notepad) opens with the invitation text.
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 (e.g., Notepad) opens with the verify text.

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

7. 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**
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.
Specify Custom Default Workspaces Sharing Permissions

By default, all Workspaces permissions are selected, and the user is expected to clear any permissions that you do want to give the invitee when a folder is shared. Alternatively, the EFT administrator can change the default permissions so that one or more permissions are NOT selected by default, and then the user sharing the folder has to explicitly enable the permission. Changing the defaults does NOT disable the permission; it simply is not selected by default. The sharing user can still enable it when inviting users to share a Workspace.

To specify default sharing permissions

1. In C:\Program Files (x86)\Globalscape\EFT Server Enterprise\web\public\EFTClient\jument\scripts, find the adminConfig.js file. (There is a number in front of the name.)
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. Look for the Default permissions section and the following text:

```javascript
gsb.config.defaultWSPermissions = {
  canUploadFile: true,
  canDownloadFile: true,
  canDeleteFile: true,
  canRenameFileFolder: true,
  canCreateFolder: true,
  canDeleteFolder: true
};
```
4. For the permission that you do NOT want selected by default, change true to false, then save the file. For example, if you do not want the **Delete File** permission selected by default, change `canDeleteFile: true` to `false`.

5. If you changed the name of the file to edit it, be sure to change it back.

### 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:
<table>
<thead>
<tr>
<th>Operation on file or comments</th>
<th>Required Owner EFT VFS permissions</th>
<th>Required Participant Workspace permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADD</td>
<td>PERMISSION_FILE_APPEND or PERMISSION_FILE_UPLOAD</td>
<td>canUploadFile</td>
</tr>
<tr>
<td>UPDATE</td>
<td>PERMISSION_FILE_APPEND or PERMISSION_FILE_UPLOAD</td>
<td>canUploadFile</td>
</tr>
<tr>
<td>DELETE</td>
<td>PERMISSION_FILE_APPEND or PERMISSION_FILE_UPLOAD</td>
<td>canUploadFile</td>
</tr>
<tr>
<td>GET</td>
<td>PERMISSION_DIR_LIST</td>
<td>N/A – Means that Participant can read comment because Owner invited them to Workspace.</td>
</tr>
</tbody>
</table>

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.

**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
- (In v7.4.7 and later) When you send a file using the WTC, a “WorkspacesSendMessage” folder is created in the **Virtual File System (VFS)**.

**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, however, the permissions may not be permitted. The **VFS** tab will appear to permit all user permissions to be granted to a Workspaces participant, however, the available permissions extend from the Workspaces owner’s folder permissions. 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.
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.

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

![Choose Folder Names](image)

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

![Edit Value](image)

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

![Specify Target Users](image)

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

The EFT administrator can customize (brand) the email interface with your company logo, color scheme, and so on.

Refer to Customizing the WTC for details of changing the logo and style of the page.
Rebranding (Customizing) the Web Transfer Client

Before you make any changes to the Web Transfer Client (WTC) files, make a backup copy of any files and images that you plan to edit. Deleting or incorrectly editing the WTC files can render the client unusable. When you upgrade to a new version of EFT, copy the *changes* to the new files; do not overwrite the new files with your custom files as numerous updates will have been made. Copy and then edit the files only in the custom folder as described in the procedure below.

When upgrading EFT, the web\custom\ and web\public\ folders are backed up and renamed with the date and time (e.g., customBackup_9-28-2010_16-18\ and publicBackup_9-28-2010_16-18\). The new versions of the files may have some updated content, so rather than overwriting the new files with your old files, you should manually copy your customizations to the new files after upgrading.

If you have upgraded EFT, please review the "To customize the themes style sheet" steps below, as the process may have changed since you last upgraded.

EFT provides for custom branding of the per-Site and per-Server login page, WTC interface, Plain-Text Client (PTC), Account Management interface, and AS2 Management interface. Save the edited files in the custom\ directory for the Site and/or Server. Each file is searched for independently, so you could have some files branded on the Server (under custom\EFTClient\), others branded on the Site (under custom\MySite\EFTClient\), and the rest left as they were originally installed (under public\EFTClient\).

EFT first looks in the Site's custom (branded) directory web\custom\MySite\EFTClient and loads any branded files. For files that are not present in the Site's custom\ directory, EFT checks the Server's custom\ directory, web\custom\EFTClient, and then loads the files that it finds there. Finally, for any other files, it will load the default files from web\public\EFTClient. Branded files that are Site-specific override any Server-wide branded and default files, while branded files that are Server-wide override the default (Globalscape-branded) files provided by the installer.

Upon initial installation, this custom\ directory is empty. You must create the directory structure for any Server (custom\EFTClient\) or Site (custom\MySite\EFTClient\) branded files. If you have multiple Sites, each Site can have different branding (e.g., one can be in English and one in French).

- The best practice is to have only customized files in the custom\ folder and to leave the default files unmodified in the web\public\EFTClient folder.

- The Site folder web\custom\[SiteName]\EFTClient\ should hold just those files that contain customizations for that Site.

- The Server folder web\custom\EFTClient\ should hold just those files that contain customizations for the Server.

- The Server-branded files will apply to all Sites defined on the Server, but any Site-branded files will override the Server-branded files.

- It is not necessary to restart the Site or Server to see your changes, but you will have to refresh or close and reopen your browser.
To customize the themes style sheet

The theme_override.css file in C:\Program Files (x86)\Globalscape\EFT Server Enterprise\web\public\EFTClient\jument\styles\defaults\styles is an older, minified version of the themes style sheet and contains no line breaks, which causes a challenge for editing. A non-minified version of this file is saved in C:\Program Files (x86)\Globalscape\EFT Server Enterprise\web\public\EFTClient\jument\styles\, which you can edit and then copy over the other one.

1. In C:\Program Files (x86)\Globalscape\EFT Server Enterprise\web\public\EFTClient\jument\styles\, right-click theme_override.css, and save it as a copy.
2. Open the file in a text editor that can recognize LF line endings, such as Notepad++ or Wordpad. (A basic text-editing program like Notepad will not show the line feeds.)
3. Make your edits, then save the file with the original file name.
4. Copy and save the file in `C:\Program Files (x86)\Globalscape\EFT Server Enterprise\web\public\EFTClient\jument\styles\defaults\styles`, overwriting the existing file.

**To customize files at the Site level**

1. Create a directory structure in the form `[SiteName]\EFTClient\` in the `\custom\` folder.
2. It is not necessary to copy all of the default files from public to custom. Copy the default files that you want to edit (rebrand) into the `\custom\SiteName\EFTClient` folder that you created.
3. Edit the copy of the file and save it in the `\custom\SiteName\EFTClient` folder.

When upgrading, the `\custom\` and `\public\` folders are backed up and renamed with the date and time (e.g., `\customBackup_9-28-2010_16-18` and `\publicBackup_9-28-2010_16-18`).

- If you lack the resources to edit CSS and HTML pages yourself, Globalscape’s Professional Services group can create custom web pages for you.

**To customize files at the server level**

1. In the `\web\custom` folder, create a folder named `EFTClient`.
2. Copy only the default files that you want to edit (rebrand) for the server into the `\web\custom\EFTClient` folder that you created. (It is not necessary to copy all of the default files.)
3. Make all customizations in the `\custom\EFTClient` folder following the instructions below or contact Globalscape Professional Services to request detailed customization services.

**Customizing the WTC**

You can customize the look and feel of the Web Transfer Client (HTML5 version) to suit your organization. The style sheets (CSS files) and index.html file are available in the installation folder (e.g., `C:\Program Files (x86)\Globalscape\EFT Server Enterprise\web\public\EFTClient\jument\`). The index.html file contains the links to the CSS files.

**To alter CSS files (styles)**

1. Navigate to `\web\custom\EFTClient\jument\styles\defaults\styles`. The CSS files are located in `\styles\defaults\styles`:
   - `vendor.css` – the default css from bootstrap and fancytree libraries (You should never have to remove the vendor.css reference from index.html)
   - `themes.css` – the "override" files of these vendor defaults
   - `main.css` – most of the CSS
2. Modify styling,
3. Copy all contents of the `defaults` folder from `\web\custom\EFTClient\jument\styles\` to `\web\custom\EFTClient\jument\`

4. If dialogs appear asking if you want to merge folders or replace existing files click Replace or Yes.

**To replace the Globalscape logo with your logo**

1. Copy the `*.GSB-Logo.png` (there are numbers in place of the asterisk) from the public directory to the corresponding custom directory.

2. Create your logo, sized 150 px by 30 px, and save it with the same name as the default logo.

3. Replace `\web\custom\EFTClient\jument\images\*.GSB-logo.png` with your logo.

4. Close and then reopen the browser to load the changes.

**To replace the Web Transfer Client logo with your logo**

1. Copy the `*-App-Logo.png` (there are numbers in place of the asterisk) from the public directory to the corresponding custom directory.

2. Create your logo, sized 245 px by 32 px, and save it with the same name as the default logo.

3. Replace `\web\custom\EFTClient\jument\images\*-App-Logo.png` with your logo.

4. Close and then reopen the browser to load the changes.
To replace the logo on the login page

1. Create your logo, sized 400 px by 120 px, and save it with the same name as the default logo.

2. Replace \web\public\EFTClient\Shared\images\gs-logo-lg.png with your logo. Maintain the same file name.

3. Close and then reopen the browser to load the changes.

To replace the English text with another language

NOTE: Subsequent versions are expected to allow for multiple languages. Meanwhile, in the Google Chrome browser, if your browser is set for a language other than English, Chrome will ask if you want to translate the page into your default language.

1. In ..\web\custom\EFTClient\jument\il8n, open main_en.json in a text editor to change the English text in the interface to the language that you want displayed. Save a copy of the file before making any changes.

2. In ..\web\custom\EFTClient\Account\, open the HTML files in a text editor to change the English text in messages to the language that you want displayed. Be careful to not change any tags in the file. Save a copy of the file before making any changes.

3. Close and then reopen the browser to load the changes.
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 cannot 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. In C:\Program Files (x86)\Globalscape\EFT Server Enterprise\web\public\EFTClient\jument\scripts, find the adminConfig.js file. (There is a number in front of the name.)
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. At the very bottom of the file, find the following text:

   gsb.config.crcVerifications = 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.
Disabling “Update Your Browser” Prompts

If end users do not have the necessary permissions to install an updated browser that supports certain features (such as folder uploads in Internet Explorer), administrators can enable a prompt that tells the user to update the browser, similar to the following prompt:

To disable prompts

1. In the /scripts/ folder, open adminConfig.js (in the format of HHHHHHHHHH.adminConfig.js, where H is a hex value) in a text editor. The file contains JavaScript similar to the following text:

   ```javascript
   'use strict';
   /* global gsb */
   gsb.config.disableSiteInitPopups = false;
   ```

2. Edit the last line to change it from false to true:

   ```javascript
   gsb.config.disableSiteInitPopups = false;
   ```

3. Save changes to the file.

Login to EFT (WTC)

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 e-mail 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. 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**.

3. Refer to [Web Transfer Client (WTC)](https://example.com) for details of transferring files.

**Form-Based Authentication versus Basic Authentication**

*(Requires the HTTP/S module in EFT SMB/Express)*

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 in the registry.

- 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 (registry enabled), 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).

**Terms and Conditions**

Web Transfer Client (HTML5 version) users can be asked to accept or decline a Terms and Conditions page before continuing to the WTC. It is not available by default.

**To enable the Terms and Conditions page**

1. Copy the `\EFTClient\` folder from `\web\public\` to `\web\custom\`. (Refer to [Customizing the WTC](https://example.com) for information about customizations.)

2. Create a file names `terms.html`.

3. Save the file in `\web\custom\EFTClient\jument`. 
To view an example Terms and Conditions file, right-click terms.txt, and then click Save As. You may use this example for your Terms and Conditions page, making sure to review and revise for your company. Be sure to save the file as terms.html in the appropriate folder as explained above.

When creating your terms.html file, you do not need the <html> and <body> tags, because the file will be inserted into a frame in the WTC. You do, however, need to use HTML tags for formatting things like headings, paragraphs, and quotation marks, as shown below:

```html
<h3>Web Transfer Client Terms and Conditions</h3>
<p>In using this website you are deemed to have read and agreed to the following terms and conditions:</p>
<p>The following terminology applies to these Terms and Conditions, Privacy Statement and Disclaimer Notice and any or all Agreements: &quot;Client&quot; and &quot;Your&quot; refers to you, the person accessing this website and accepting the Company's terms and conditions. &quot;The Company&quot;, &quot;Our(selves)&quot; and &quot;We&quot; and &quot;Us&quot; refers to our Company. &quot;Party&quot;, &quot;Parties&quot; or &quot;Ourselves&quot; refers to both the Client and ourselves, or either the Client or ourselves. All terms refer to the offer, acceptance and consideration of payment necessary to undertake the process of our assistance to the Client in the most appropriate manner, whether by formal meetings of a fixed duration, or any other means, for the express purpose of meeting the Client's needs in respect of provision of the Company's stated services/products, in accordance with and subject to, prevailing English Law. Any use of the above terminology or other words in the singular, plural, capitalization and/or he/she or they, are taken as interchangeable and therefore as referring to same.</p>
<h4>Privacy Statement</h4>
If you are not familiar with HTML code, Globalscape’s Professional Services team offers a range of professional services to complement your product solution.

**Upgrading the Web Transfer Client (HTML5 version)**

The HTML 5 version of the Web Transfer Client (WTC) has a separate upgrade wizard from EFT, so that you can upgrade the Web Transfer Client as changes are made available without reinstalling all of EFT. You can verify the current version by logging in to the WTC and clicking About.

**To upgrade the WTC**

1. Copy the installer (eft-wtc-installer.exe) to the EFT computer and double-click it. The WTC upgrader installer opens.
2. Click **Next**. The license agreement appears.

3. Scroll to read the agreement, then click **I Agree**. The WTC is upgraded.

4. Click **Show details** to view the process of updating.

5. After the upgrade is complete, click **Close**.
Conceal WTC and Its Content from Searches

The WTC/Workspaces pages and content is visible to Web searches. A file named robots.txt on the server tells web crawling robots whether to ignore the site. You can create a registry key to prevent WTC/Workspaces pages and content from appearing in search results. In EFT, the robots.txt file is located (by default) in C:\Program Files (x86)\Globalscape\EFT Server Enterprise\web\public\EFTClient.

To enable or disable searches

1. Create the following registry key:

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\GlobalSCAPE Inc.\EFT Server 7.4\ServeRobotsFile

2. Add a DWORD and name it ServeRobotsFile

3. Set the DWORD to 0 (disabled, the default) or 1 (enabled)

4. Restart the EFT server service.

The EFT.log file indicates that the key was read in at startup. (the first log is initial startup, 0, the second one is after changing it to 1 and then restarting the service:)

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>09-27-17</td>
<td>15:08:26</td>
<td>INFO AdvancedProperties &lt;&gt; - HKEY_LOCAL_MACHINE\SOFTWARE\GlobalSCAPE Inc.\EFT Server 7.4\ServeRobotsFile=0</td>
</tr>
<tr>
<td>09-27-17</td>
<td>15:57:26</td>
<td>INFO AdvancedProperties &lt;&gt; - HKEY_LOCAL_MACHINE\SOFTWARE\GlobalSCAPE Inc.\EFT Server 7.4\ServeRobotsFile=1</td>
</tr>
</tbody>
</table>

Display Full Name of User in WTC on LDAP Site

In the Web Transfer Client (WTC), you can display the full name of a user instead of the username by creating the registry setting described below.

(Workspaces must be enabled to display the full user name in the WTC.)

HKEY_LOCAL_MACHINE\ Software\ WOW6432Node\ GlobalSCAPE Inc.\ EFT Server 7.4\ DisplayUserFullNameInJument

Type: DWORD

Value name: DisplayUserFullNameInJument

Default Value: 1

Cached: yes

Backup/Restore: yes
WTC & Workspaces User Guide

Overview of the Web Transfer Client

The Web Transfer Client (WTC) is a browser-based file transfer client that allows you to transfer files over HTTPS to and from a server. Using the WTC, you can upload and download files to the server, pause and resume a transfer, cancel a transfer, move files between folders, create, rename, and delete folders and files, and share folders with other users.

File-Naming Conventions

EFT follows the standard Windows naming conventions, with a few exceptions. (Please refer to Unicode File Transfers and Unicode Exceptions for details of using Unicode characters.)

For example:

- You can name files using almost any character for a name, except for the following reserved characters:
  `< > : " / \ ? * %`
- The maximum length for a path is 255 characters. This limitation includes the drive letter, colon, backslash, directories, subdirectories, filename, and extension. If the relative path is too long, a warning message appears.
- Characters that are valid for naming files, folders, or shortcuts include any combination of letters (A-Z) and numbers (0-9), plus the following special characters.
For more information regarding file-naming conventions, refer to the Microsoft Windows Developer Network article Naming a File and the Microsoft TechNet article How NTFS Works.

**Unicode File Transfers**

EFT’s support for UTF-8 encoded Unicode characters extends to:

**Inbound protocols:**
- HTTP/S
- SFTP

**Event Rules:**
- Copy/Move and Download action wizards (all protocols) when specifying “UTF-8” as the filename encoding, and when using wildcards for the source filename, e.g. (*.dat, or *.*)
- Advanced Workflow Engine when passed filename-related context variables (e.g., %FS.PATH%, %FS.FILE_NAME%, etc.)

**Auditing:**
- EFT’s summary Client Log (CL)
- EFT’s extended client logs (e.g. LAN copy, FTP extended, and SFTP debug logs)
- EFT’s debug log (Log4Cplus)

**Exclusions:**
- FTP protocol (inbound)
- All Event Rule actions that process a filename related context variables (e.g. %FS.PATH%, %FS.FILE_NAME%, etc.); the only exception is Advanced Workflow Engine actions
Folder Monitor events. Windows will notify EFT when a Unicode file is dropped into a monitored folder, but EFT cannot (at present) pass the UTF-8 encoded filename context variable off to Event Rule actions for processing. The only exception being when the action is an AWE action, in which case UTF-8 encoding is preserved. Do not be tempted to use wildcards as the source filename for Folder Monitor rules (even if polling only is used), as this will lead to race conditions and other problems. Wildcards should only be used in rules that don’t use filename context variables, such as Timer, user, or system related events.

- ARM database and all logs not explicitly mentioned above
- No User Interface (UI) components. This means you cannot specify Unicode characters in Event Rules or anywhere else in the administration interface
- No COM API support for Unicode
- EFT does not support UTF-8 filenames over AS2

*UTF-8 will be more comprehensive in a future version. Refer to Unicode Exceptions for more information.

Unicode FAQs

The FAQs below are provided to answer questions you may have regarding EFT’s Unicode support.

Q. What is Unicode?
A. Unicode is a standard that provides a unique number for every character, regardless of platform, program, or language. Systems that don’t support Unicode and without the proper ANSI code page will render characters such as 大きい魚 ??了??? or ???.

Q. Does EFT support Unicode?
A. EFT partially supports Unicode and is moving towards full support.

Q. What about UTF-8?
A. UTF-8 is simply a popular mechanism for encoding Unicode characters using one or more bytes. Prior to supporting UTF-8, EFT used ANSI code pages to view filenames in the intended format (on the target system when browsing with the WTC or PTC).

Q. What other mechanisms for encoding Unicode characters does EFT support?
A. EFT uses full double byte UCS-2 encoding at the file system (I/O) level, UTF-8 encoding within EFT, and ASCII everywhere Unicode is not yet supported.

Q. Does EFT support UTF-8 for file transfers?
A. EFT preserves UTF-8 encoded filenames when transferring files over HTTP and SFTP when acting as a server, and over all supported protocols when acting as a client, when certain conditions are met (see next question).

Q. What about EFT’s Event Rules?
A. EFT’s Copy/Move and Download Action wizards (across all protocols) support Unicode when you specify “UTF-8” as the filename encoding method (radio button in the wizard), and when using wildcards for the source filename, e.g. (*.dat, or *.*). However, UTF-8 is not supported for these Actions if you use %FS.PATH% or any other variable for the source filename, which means the Folder Monitor Event cannot be used to offload files and conserve their Unicode format. In fact, the only Action that supports UTF-8-encoded filenames through context variables is an AWE workflow task.

Q. Which client applications can I use to see Unicode filenames when I transfer files to EFT?
A. EFT’s Web Transfer Client (WTC) supports UTF-8. For file transfer applications that do NOT support UTF-8, Unicode filenames will appear as “?????????.exe” when using them to transfer files to/from EFT. CuteFTP v9 supports UTF-8.

Q. Can EFT audit or log filenames or other data with Unicode characters?
A. EFT’s summary Client Log (CL), extended client logs (LAN transfer logs, FTP logs, SFTP debug logs), and debug log (eft.log), and AWE’s logs all support Unicode characters. EFT’s EX logs, cmd out logs, and ARM (both auditing and reporting) do NOT support Unicode characters.

Q. If this filename: 梅雨右折車線_XYZ.ISO is transferred to EFT, how will it appear on disk? In reports? In EFT’s Event Rules?
A. EFT will store the file to disk and conserve the original Unicode filename. The filename will be audited properly to EFT’s eft.log, but will be down converted to ASCII when audited to the EX log and to the ARM database, resulting in a filename that may look like this: ???????_XYZ.iso, which is also how it appears in EFT’s reports. The reason the last three characters and file extension are conserved is that UTF-8 and ASCII characters are identical for English characters (A-Z). So there is no loss of meaning (fidelity) after performing a UTF-8-to-ASCII conversion. This same UTF-8-to-ASCII conversion applies when EFT hands off the filename to the Event Rule dispatcher, except where an AWE action exists, in which case the filename context variable will retain the original UTF-8 encoded filename. Thus if data integration of UTF-8 encoded filenames is needed, you should consider deploying AWE tasks alongside EFT’s Event Rules.

Q. How do Unicode filenames appear in EFT’s administration interface?
A. EFT’s administration interface (AI) does not support Unicode characters. UTF-8 is always down converted to ASCII in the AI. This means you can’t specify a unique UTF-8 encoded filename in EFT’s offload wizard, a UTF-8 encoded username, path, or anything else for that matter. The ONLY way to process Unicode filenames in the Copy/Move and Download Actions is to use wildcards (*.*, *.dat, etc.) as the source filename, instead of using a specific filename such as 梅雨右折車線.ISO.

Q. Will Unicode encoded filenames be preserved in EFT Server’s context variables, such as FS.FILENAME or FS.PATH?
A. Yes and no. For all Event Rule Events, Conditions, and Actions EFT will down convert the UTF-8 characters into ASCII. The only exception is when those variables are passed to AWE. In that case alone, EFT conserves the UTF-8 encoded filename, so that AWE can consume the original UTF-8 encoded filename, as AWE is fully UTF-8 compliant.
Q. Does EFT’s internal handling of the file differ depending on whether the file was received in ASCII or Unicode?

A. In the guts of EFT it handles everything in Unicode. Conversion back to ASCII occurs only when working with a system or capability that doesn’t support Unicode.

**Enabling JavaScript in the Browser**

Many web pages use JavaScript (an entirely different language than Java) to make the user experience more dynamic. The Web Transfer Client uses JavaScript for this very reason. For the Web Transfer Client to work, JavaScript must be enabled in the browser.

Refer to the procedure below to edit the browser’s security settings to allow you to use JavaScript. See also Checking Java Runtime Versions.

---

*You might not have the appropriate permissions to access these settings. If necessary, contact your system administrator for assistance.*

To edit the browser settings

**In Internet Explorer:**

1. Click Tools > Internet Options. The Internet Options dialog box appears.
2. Click the Security tab, and then click Custom Level.
3. In the Security Settings dialog box, scroll down to the Scripting area, then under Active scripting, click Enable.
4. Click OK to close the Security Settings dialog box, and then click OK to close the Internet Options dialog box.

**In Firefox:**

1. In the address bar, type about:config.
2. Scroll down to or search for javascript.enabled.
3. Ensure that the Value column says “true.” If it says, “false,” double-click the line to change it to “true.”

**In Chrome:**

1. In the upper-right corner, click Customize and Control Google Chrome (the icon with 3 horizontal lines), then click Settings.
2. In the Settings page, scroll to the bottom and click Show advanced settings.
3. Under Privacy, click Content settings. The Content settings dialog box appears.
4. Under JavaScript, click Allow all sites to run JavaScript, then click Done.
Logging In

You can log in to the WTC and Workspaces with any supported browser. The server administrator will provide you with the URL (web address) and your login information.

To log in to the server

1. Open the web browser.
2. Type or click the web address provided to you by your system administrator. For example, type https://www.ourfileserver.com. The login page appears.

   - If you don’t know your username, click Forgot Username (if available). In the Lost Username dialog box, provide your email address and then click Submit.

   - If you don’t know your password, click Forgot Password (if available). In the Lost Password dialog box, provide your Username and Email address, then click Submit.

   Your request is sent to the server and an automated response will email you your username.

3. If you have been instructed to use secure sign-on, click SSO Login.
4. Provide your Username and Password, then click Log In.
5. If have been instructed to use two-factor authentication, you will be asked to provide a second response.

The EFT administrator can change the text that appears for the challenge. Refer to the article at https://kb.globalscape.com/KnowledgebaseArticle11267.aspx for details.

6. When the credentials are accepted by the server, the Web Transfer Client (WTC) appears.

Logging Out

The server ends the session immediately when the browser is closed or after a period of inactivity. When the session is ended, the directory listing and any other personal information is cleared, and the login page is displayed.

To log out

- Click Account > Logout. The WTC closes and the Log In page appears.

Automatic Log Out

After a period of inactivity (approximately 10 minutes), a message appears warning that you are about to be logged out. You can click Continue to stay connected.

Uploading Files and Folders

You can upload files and folders from your local computer to a remote server on which you have upload permission.

To upload files between your local system and the server

- Do one of the following:
  - To transfer files to the server, click File > File Upload.
To transfer folders to the server, click **File > Folder Upload**.

- **Folder uploads are available in Chrome, Firefox, or Opera browsers only.** If you want to upload folders in other browsers, you must compress them (make a ZIP file) and upload the ZIP file.

- Click and drag one or more files or folders from your local file system to the file list. (Empty folders will be ignored and not transferred.)

- In the **Upload Manager**, click the UPLOAD icon, then select the files and folders that you want to upload.

The **File Name** pane will refresh automatically after the upload is complete.

The **Upload Manager** displays the completed transfers, in-progress transfers (up to 5 at once), and pending transfers. The **Upload Manager** is cleared when the session ends or you log out.

- The **PAUSE** icon allows you to pause an in-progress transfer. If you want to clear the Transfer queue, you can click the **CANCEL** icon for each transfer or click the **CANCEL** icon at the top to clear all of the transfers.

**Notes:**

- When the file is transferred, if there is a file with a duplicate name already in your folder on the server, the server will run a comparison on the contents. If the file contents are the same, the file is not uploaded.

- You can upload multiple selected files at once by dragging and dropping from your local system to the WTC **Upload Manager**, or by clicking **File > Upload** and then selecting multiple files.

- If you have exceeded your allowed disk quota on the server, a message appears when you attempt to upload more files. To continue to upload files, you must delete some of your old files from the server or ask your administrator to increase your allowed disk quota.

- Before you can access the server using the WTC, the administrator must configure the server to allow WTC connections with your account.
If network connectivity is lost while the WTC is transferring files, you can retry transfers that previously failed or were incomplete. If a file partially transferred before the connection went down, the transfer will be resumed from the point that it left off.

**Downloading Files**

You can download files from the server to your local computer on which you have download permission. The mechanism for downloading files is browser dependent.

- 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.
- The default download timeout of 60 seconds can be increased if needed (as of v7.4.11).

**To download files**

- Select the check box of one or more files that you want to download, then click the download icon on the toolbar.
- The file will download to the folder defined in your browser’s configuration (e.g., C:\Users\myname\Downloads).

**To open your browser’s Downloads folder:**

- In Chrome, click the Settings icon, then click Downloads (or press CTRL+J).
  
  ![Chrome Downloads](image)

- In Internet Explorer, click the Settings icon, then click View Downloads (or press CTRL+J).
- In Firefox, click the green down-facing arrow to view most recent downloads, or type about:downloads in the address bar to view all downloads.
Canceling a Transfer

Most files that you transfer will transfer so quickly, you won’t even notice. Larger files, however, will show progress in the In Progress area of the Upload Manager. You can cancel an in-progress transfer.

To cancel a transfer

1. In the Upload Manager, while the transfer is in progress, click the PAUSE icon.
2. After the transfer is paused, a Play and a Cancel icon appear.
3. Click the Cancel icon to stop the transfer.

Clearing the Upload Manager

The Upload Manager displays uploads that are completed, in progress, and pending. The pane will clear automatically when you log out of the Web Transfer Client. (Removing the list of files from the pane only removes it from the display; the file is still saved in the folder into which you transferred it.)

To clear the Upload Manager

After a transfer is completed, the file moves from the In Progress queue to Completed.

Click the DELETE icon to remove all completed transfers from the queue.

Resuming Transfers

A file transfer can be interrupted for various reasons, such as a network glitch, or you might pause the transfer yourself. When a transfer is interrupted because of errors, it will resume automatically after network connection is reestablished (up to 10 retry attempts over a 5-minute period).

To resume a paused transfer

1. Transfers that have been interrupted appear in the In Progress queue.
2. Next to the paused file, click the PLAY icon. The transfer will resume where it left off.
Filtering and Sorting the File Name Pane

You can filter the display of the files to display only the files that you want, by name, file type, size, and/or date modified to limit the display to specific files and folders. Additionally, you can sort the File Name, Size, and Date panes by clicking the arrows in the pane header.

To filter the File Name pane

1. Click the funnel icon ▼ in the header of the File Name, Size, or Date pane or next to the Search box. The Filter dialog box appears.
2. Provide filter criteria such as name, size, or date, then click Apply Filter.
   - To search for a specific size, click Greater than or Less than and provide a size to search for.
3. To clear your filter and show all files, in the Filter dialog box, click Remove Filter.

Searching for Files

If you have a large number of files and subfolders, you can find file more quickly by using filters to search by name, size, or date, or typing text in the Search box to find the file.

The Search box merely matches the text string that you type. For example, it doesn’t know the difference between a PDF file and a PNG file (however, if you type png, the search results will show all files with png in the file name, including the extension). It is not case sensitive. Certain wildcards will return matching results. For example, w*n displays results that have a w, one or more other characters, and then an n, such as WEB_VPN_Instructions.docx and WindowsClustering.pdf. Wildcards are useful, for example, for finding files when you aren’t sure how they were named.

To search for files using a filter

1. In the search box, type your search term in the box, and then press ENTER, or click the down arrow to do a global search.
2. As you type, the WTC will find matches for what you have typed.
3. Click the found item to navigate to it.

4. Click the icon on the toolbar for what you want to do with the file (download, rename, delete, move, etc.).

**Creating Folders**

When you first log in to the Web Transfer Client (WTC), you are in the top folder that you are allowed to view, called your home folder. You can create sub folders within this folder, and those folders can have subfolders.

**To create sub folders**

1. In the **Folders** pane, click to select the folder under which you want to create a subfolder.
2. On the toolbar, click the NEW FOLDER icon.
3. Provide a name for the folder, then click **OK**. (Folder names follow standard Windows file naming conventions.)
4. The new folder appears in the **Folders** pane. You can now move files between folders and upload files to the new folder.

**Moving Files between Folders**

After you have created subfolders in your home folder, you can move files between those folders. Users with whom a Workspace is shared do NOT have permission to move files and folders out of the Workspace.

**To move one or more files to another folder**

1. Select the check boxes of one or more files that you want to move, then click the MOVE icon.
2. In the dialog box that appears, select the folder to which you want to move the file(s), then click **OK**.

   If a message appears that it failed to move the file(s), wait a minute to see if the file(s) appear in the folder. On large files, EFT will occasionally close the HTTPS connection after 60 seconds (default) of performing the move folder operation causing a timeout, which triggers the message even though the files are being moved.

**Renaming a File or a Folder**

You can rename folders and files in your home folder and in subfolders. The WTC follows Windows file-naming conventions. That is, the following characters are invalid for file naming:

```
<>:"/\?*%
```
To rename a file or folder

1. Select the check box for the file or folder that you want to rename.
2. On the toolbar, click the RENAME icon.
3. The Rename dialog box appears. Provide a new name, then click OK.

Deleting a Folder or File

You can delete folders and files in your home folder and in subfolders.

To delete a file or folder

1. Select the check box for the file or folder that you want to delete.
2. On the toolbar, click the DELETE icon.
3. The Delete confirmation message appears. Click OK.

File Comments

You can add and view comments on files in a shared Workspace.

To view or add comments to a shared Workspace

1. In a shared folder, select the check box next to a file. (NOTE: Clicking the file will attempt to open it.) The toolbar updates to show more options.
2. With the file selected, click the Comments icon. The Comments dialog box appears.
3. If no comments have been added, the Comments dialog box is blank.
4. To add comments, type in the text box, then click Save.

The dialog box updates to display the comment, the username of the user who entered the comments, and the date and time the comments was added.
5. Click the X in the top right corner to close the dialog box. (Cancel is used to clear a comment before you click Save. Once you click Save, the comment is added.)

**Send/Email Files from within the WTC**

EFT users who want to add files that are either located in their local machine or are in the WTC can do so securely from within WTC. Recipients of those files can pick up the files in their default browser.

- The browser will timeout after a period of inactivity. Files that are being uploaded are considered “activity.” Idle timeout occurs if you leave the browser open and stop composing your message with no activity. Upon timeout, the draft is lost. An “about to timeout” warning prompt is displayed when timeout is imminent, giving you the opportunity to keep the session alive.

- When you send a file using the WTC, a “WorkspacesSendMessage” folder is created in the Virtual File System (VFS).

**To email files**

1. [Log into the WTC](#).

2. Click the Send icon on the toolbar. The **Send files securely** form appears.

3. The **From** box is drop-down list if there is more than 1 email address for this user in EFT.
4. Select the files that you want to send:

5. To send the request securely, select the **Send message body securely** check box.

7. Under **Delivery Notifications**, specify if and when you want to be notified when your message is picked up.

8. Under **Authentication & Authorization**, specify whether an EFT account is required to pick up your message, and whether non-EFT users can reply to your message. The **Allow non-EFT users to reply** option is not available if reply is not allowed by administrator.

9. Under **Message Expiration Options**, specify when you want the message to expire.

10. Select the **Save as defaults** check box to use the same settings every time. (You can still edit them, as needed.)

11. Click **Apply**, then click **Send Message**. A message appears indicating whether the message was sent successfully or not.

The **Not Sent** message appears if you have EFT configured to send only to EFT users (most restrictive) and you try to send to non-EFT users. If you need to send to user accounts that are not defined in EFT, your EFT administrator will need to either change the setting on the **Workspaces - Send** tab of the EFT Site or add the account as an EFT user.

12. If sending the message was successful, the recipient(s) receive an email with a link to pick up the files.

**Sharing Folders (Creating a Workspace)**

Users can share a folder with other users through the Web Transfer Client. Additionally, you can, if the EFT administrator allows it, invite external users to share your folders. (To share folders, the administrator has to have enabled Workspaces in the EFT administration interface on the Workspaces tab of the Site.) Workspace participants who were invited to share a Workspace cannot add participants to that folder. However, they can create new folders.

The invitation recipient clicks the link embedded in the email and then signs in to EFT, if an account has previously been created, or creates an account on EFT.

- Workspaces invitations expire after 5 days.
- Administrators can see and manage invited (guest) accounts in the administration interface on the VFS tab.
To share a folder

1. Log in to the Web Transfer Client.

2. Select the check box of the folder that you want to share, then click the Share Folder icon 1, or click File > Share Folder. The Create a Workspace dialog box appears.

3. Provide up to 10 email addresses of users with whom you want to share the folder. (You can later add more participants, 10 at a time. To add more than 10, the EFT administrator can edit the WTC files. Refer to the Knowledgebase for details.)

4. To create a private workspace, select the Make this workspace private check box. When a Workspace is private, the Alerts/Notification icon, the Workspace participants icon, and the comments icon are hidden from the recipient.

5. Assign permissions by clearing or selecting the check box next to that permission. By default, all permissions are selected (enabled). Clear the check boxes of the permissions that you do not want to assign to the users.
The administrator can specify which permissions check boxes are selected by default, if any. The sharing user can still select the check box to enable the permission. Refer to Workspaces Permissions for details. Permissions that the administrator assigns to folders override any permissions that you assign. That is, if the folder that you are sharing does not have rename permission, you cannot assign that permission to the folder.

6. (Optional) In the Messages box, you can type comments. When you create a Workspace, the comment that you type in the Messages box appears in the invitation email.
   - View a history of comments added by clicking the shared folder and then clicking the comment icon.

7. In the Notifications box, you can specify the type and frequency of email notifications about this Workspace.

8. (Optional) To expire the Workspace, select the Workspace expiration check box, and then specify the expiration. The limit is specified in the administration interface on the Workspaces tab of the Site. (Alternatively, there is a Stop Sharing icon in the WTC toolbar.) The default expiration date appears, when defined in the administration interface on the Workspaces tab.

9. Click Share. A banner appears at the top of the folder list indicating that you are sharing the folder as a Workspace.

The users with whom you have shared the folder will see the shared folder in their Shared with Me tree. The username of the account that is sharing the Workspace appears in parentheses after the name of the folder (e.g., EFTWebAdmin (Imauser1)).
Add Workspace Participants

After you have created a Workspace and invited participants to join the Workspace, you might later want to add participants.

To add participants

1. On the tool bar, click the Add participants icon.
2. Provide one or more email addresses, assign permissions, then click Share.

Joining a Workspace

When a Workspace creator invites others to a shared folder, an email is sent to each invitee.

To join a Workspace

1. In the email invitation to join a Workspace (a shared folder), click View Folder (or right-click and then click Copy link address).
2. You are asked to either Join Workspace with new account or Log in with existing EFT account.
3. If you have EFT credentials, just login and click Join Workspace.

4. If you don’t have EFT credentials, create and confirm a password for a new account, and then click Create Account and Join Workspace. Your account is created, but now you have to verify the account.

5. In the confirmation email, click Verify Account. The account verification process occurs, and then you can log in.

6. Log in with your email address and the password that you created for the account. The Web Transfer Client appears. You can see which folder(s) was shared with you. The username of the Workspace creator appears next to the shared folder and in a banner above the folder list.
**Expire a Workspace**

**To expire the Workspace**

1. On the tool bar, click the **Edit Workspace** icon.
2. Specify the date that you want to expire the Workspace.
3. Click **OK**.

**Edit-Remove Workspace Permission**

The default settings for Guest Users 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.

To edit a Workspace participant’s permission or remove the user from the Workspace

1. On the tool bar, click the **Edit Workspace** icon.
2. Do one of the following:
   - To delete the user, click the delete icon (trash can).
   - To edit the user’s permissions, click the gear icon for the user that you want to edit, then make the changes to the user’s permissions, as needed.
3. Click **OK**.

**Stop Sharing a Workspace**

When you stop sharing a Workspace, the folder is removed from the Joined Workspaces tree.

To stop sharing the folder

1. Click the shared folder.
2. Click the stop sharing icon in the banner. The **Stop Sharing Workspace** message appears.
3. Click **Stop Sharing**

**Notifications**

Each Workspace participant can configure notifications to let them know when actions are performed on the Workspace, such as uploading or downloading.

**To enable notifications**

1. Select the check box for the folder for which you want notifications.
2. Click the notification icon (bell). The **Edit Notification Options** dialog box appears.
3. Specify the notification frequency (the default is daily) and which actions to be notified about (all are selected by default).
4. Click **OK** to save your changes.
Edit Notification Options

When you create a Workspace, you can specify how often you want to be notified regarding actions taken on the Workspace, such as when files are uploaded to your Workspace.

Notifications:

- Receive an email immediately after every action is taken
- Receive an email of all actions that were taken that day (sent at 12 am)
- Never receive emails on actions taken.
- Choose specific actions to be notified about, or none at all.

If you later want to change your notification settings, you can do so in the Edit Notifications Options dialog box.

To change notification options

1. On the toolbar, click the notification icon. The Edit Notification Options dialog box appears.
2. Make your changes and then click OK.
Using the Drop-Off Portal

The Drop-Off portal can be used by external users to send files to internal users on demand (ad hoc), without creating user credentials.

![Image](https://example.com/image.png)

The ability to create Workspaces is disabled be default on the Guest Accounts Settings Template. Disabling creation of Workspaces on Guest Accounts ensures that Workspaces licenses are available for internal users. On the Connections tab, you can **Allow Creation of Workspaces** on the Guest Accounts Settings Template for all Guest accounts or on each Guest account individually. This applies all guest accounts, including those created when using the Drop-Off portal.

To send a file using the Drop-Off portal

1. In your browser, go to the URL provided. (Your administrator or internal user will provide the address.) The Drop-Off portal appears.

2. The To box is not editable, unless the administrator has enabled it. If the To box is enabled, you are limited to addresses in the domains **defined by the administrator** or to lists defined in the EFT administration interface.

3. In the From box, provide the email address at which you want to receive responses.
4. In the **Subject** box, provide a clear topic of the email. (i.e., “Files for Wednesday’s Acme project meeting” is more clear than “The files you wanted.”)

5. In the **Message** box, provide a brief reason for the email.

6. Drag and drop or select the files to attach to the email.

7. To send the request securely, select the **Send message body securely** check box.

8. Click **Send Message**. A confirmation message appears.

9. If you want to send another file, click **Send Another**.
   - If the send was not successful, an error message appears. Click **Try Again** to verify the email address and resend the email.

10. The recipient will receive an email with a download link. If the recipient has an account on EFT and signs in to the **Pick-Up portal**, the recipient can reply to the sender.

### Picking Up Files

After a Workspaces or EFT Outlook Add-In user sends one or more files, the recipients can click a link in the email that they receive that opens their default browser to the Workspaces Pickup portal.

Depending on the administrator’s settings, the files might be available for download only once, after which the download links will expire.

> **In earlier versions, the recipient email contained a link to the Pickup Portal and another single-click link to the file(s) sent. In this version, automatic file download was added to the Workspaces templates and direct download links were removed. If you have upgraded to EFT v7.4.9, the earlier templates were not overwritten.**

### To download files in the Pickup portal

- In the notification email, click the **Workspace** link.
- The default browser opens to the Pickup portal.
For replies to requested files, the following Pick Up portal appears.

Secure File Pick Up

Re: Files that were requested
<dyelacic@mesal.local> has sent you and others one or more files.
Links to this page or to the files will expire on Wed Nov 08 2017.
Here are the requested files:

Select one or more files and click Download Selected to download multiple individual files or click Download All to download all of the files.

Reply Portal

After you have received a message sent through Workspaces, you can reply to the email (if so configured) and send files back.

Reply and Reply All buttons are displayed under the following conditions:

- For anonymous recipients, if the sender has enabled replies
- For authenticated recipients:
  - if the Workspaces license limit is not exceeded
  - if Enable reply portal check box is selected (on the Site Workspaces-Send tab)
  - if Workspaces and Send Files are both enabled (at the Site level)
- Reply All button is not displayed if sender is the only available recipient on the thread.
- The alias name is displayed if any recipient is from an alias list
To reply to the email

1. The **From**, **To**, and **Subject** lines are completed for you.

2. Compose a **Message**，“drag and drop” or browse for files, then click **Send Message**.

3. If the reply is in response to a request for files, an additional field appears:

4. To send the request securely, select the **Send message body securely** check box.

5. Complete the email and click **Send Message**.
Request Files

In the Web Transfer Client, a user can request files from another user, if Workspaces is enabled to send files.

To request files

1. Click the Request Files icon.

   The Request Files window appears, and the From address is completed for you.

2. Provide the To address, Subject, and Message.

3. To send the request securely, select the Send message body securely check box.

4. Click Request Options.

   • To set message expiration, click the Message Expiration Options list and click an option:

     You can set the message to expire immediately after first use, in 24 hours, in a week, or in a month.

   • Under Authentication & Authorization Options, specify whether the recipient of the request must have an account or can be anonymous.

5. Click Apply.

6. Click Send Request.

   The recipient will receive an email similar to the one below:
7. The recipient should click the “click here” link to open the Reply portal in which the recipient can attach the requested files to send to the requestor, who can pick them up in the Pick Up portal.

**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.

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.
Changing Your Password

The administrator may have set your password to expire periodically. You can change your password within the Web Transfer Client.

To change your password

1. In the upper-right corner, click Account, then click Password. The Change Password dialog box appears.
2. Provide your Current Password and New Password, and then Confirm Password. If the administrator requires complex passwords, a message will appear if your password does not meet the complex password or reuse password requirements.
3. Click OK.
Error Messages

Error messages and prompts appear for a variety of scenarios (e.g., if you attempt to upload a file whose path exceeds the Windows limit; attempt to create a folder when you do not have permission; the path exceeds the Windows limit; a folder with the same name exists; your disk quota is exceeded; and so on). If you have read the error message/prompt and are unable to resolve the error yourself, provide the text of the message to your system administrator.

Logging

All activity in the client is logged in the server. You can view the log of events in the client and export the log to send to the administrator for troubleshooting.

To view the log
1. Click Tools > Log.
   The log appears:

To export the log
1. Click the Export icon in the title of the log window.
   The log is exported to an HTML file in your browser.
2. Click anywhere in the HTML page of the log, and then:
   - **In a Windows operating system:** Press CTRL+A to select all, then CTRL+C to copy the contents that are selected. Then, click in an email or text file and press CTRL+V to paste it into the email or text file.
   - **In a Mac operating system:** Press Command+A to select all, then Command+C to copy the contents that are selected. Then, click in the email or text file and press Command+V to paste it into the email or text file.

To change logging settings
1. Click Tools > Log Options.
The Log Options dialog box appears.

2. The default logging level is INFO. To increase or decrease the level of logging, click the desired level. Note that each logging level will include the logging levels below it. For example, INFO includes all WARN, ERROR, and FATAL messages.
   - Click OFF if you want to turn logging off. It is a good idea to leave logging on at the default level in case of errors for which the administrator needs to review the logs.

3. Click OK to accept your changes and close the dialog box.
A

**Action**: Once an Event Rule is triggered and assuming all conditions are met, EFT launches one or more user-definable Actions, such as executing a command, sending an e-mail, offloading a file, or a combination of multiple actions.

**AD**: Active Directory. A Microsoft implementation of LDAP directory services used to provide central authentication and authorization services for Windows-based computers.

**administration interface**: The graphical user interface to EFT used to configure one or more physical servers, users, connections, Event Rules, and so on.

**ADO**: ActiveX Data Objects. A language-neutral object model that exposes data raised by an underlying OLE DB Provider.

**algorithm**: List of well-defined instructions that tell a computer the procedure and order of steps to perform a specific task. See cipher.

**ARM**: The Auditing and Reporting Module, an add-on to EFT, captures the transactions passing through EFT and provides an interface in the administration interface where you can use preconfigured or your own custom reports to query, filter, and view transaction data.

**AS2**: Applicability Statement 2. A specification for data exchange, to perform the task of sending and receiving data via a secure connection. AS2 is also referred to as EDIINT AS2 or EDI over the Internet AS2.

**AS2 Identifier**: Name by which trading partners identify themselves to each other when transferring files via the AS2 protocol.

**Asynchronous Receipt**: A receipt returned to the sender on a different communication session than the sender’s original message session.

**AWE**: EFT’s Advanced Workflow Engine adds additional automation capabilities, allowing you to add scripting and variables to workflows, then add these reusable workflows to Event Rules. A workflow is a series of steps that can perform file transfers, batch data processing, application testing, and so on, set to run automatically when started by some event.

B

**Base DN**: Base Distinguished Name. Specifies the necessary domain components of the LDAP server.
Certificate: Certificates are digital identification documents that allow both servers and clients to authenticate each other. A certificate file has a .crt extension.

certificate chaining: A certificate chain is used to establish a chain of trust from a peer certificate to a trusted CA certificate. Each certificate is verified using another certificate, creating a chain of certificates that ends with the root certificate.

cipher: Instructions (algorithm) for performing encryption. See SSL.

cluster: Group of tightly coupled computers that work together closely so that they can be viewed as though they are a single computer. A failover cluster has redundant nodes that are used to provide service when system components fail.

COM API: Component Object Model. A programmatic interface that allows you to control EFT from your own custom applications using any COM-enabled programming language.

Commands: EFT’s Commands can execute programs, scripts, or batch files with or without command line arguments, providing administrators almost limitless extensibility. These Commands can be invoked directly by a user from an FTP client (if permitted by the EFT administrator) or as an automated action from EFT’s Event Rules.

compensating control: Compensating controls may be considered when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints but has sufficiently mitigated the risk associated with the requirement through implementation of other controls. Compensating controls must 1) meet the intent and rigor of the original stated PCI DSS requirement; 2) repel a compromise attempt with similar force; 3) be “above and beyond” other PCI DSS requirements (not simply in compliance with other PCI DSS requirements); and 4) be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement.

Condition: Allows you narrow the trigger definition for an Event Rule. Conditions are optional; you do not have to define a condition on an Event Rule to make it trigger an action, but they allow more control over when an Action can take place.

Data remanence: Residual physical representation of data that has been in some way erased.

DER: Distinguished Encoding Rules. A method for encoding a data object, such as an X.509 certificate, to be digitally signed or to have its signature verified.

DMZ Gateway: Server designed to reside in the demilitarized zone to provide secured communications with EFT behind intranet firewalls without requiring any inbound firewall holes between the internal network and the DMZ.

DSN: Data Source Name. Data structure that contains the information about a database that an Open Database Connectivity (ODBC) driver needs to connect to it. Included in the DSN is information such as the name, directory, and driver of the database, and the ID and password of the user.
DSS: Data Security Standard. Represents a common set of industry tools and measurements to help ensure the safe handling of sensitive information and provides an actionable framework for developing a robust account data security process, including preventing, detecting, and reacting to security incidents.

Dual-Stack: EFT allows IPv4 and IPv6 protocols either independently or both at the same time.


EDI: Electronic Data Interchange. Transfer of data between companies using VANs or the Internet. An organization’s EDI standard describes the mandatory information for a particular type of document, which information is optional, and the structure of the document. For example, an architectural firm may require a particular file-naming convention.

EFS File Sharing: Encrypting File System. A file system driver with filesystem-level encryption available in Microsoft’s Windows 2000 and later operating systems. The technology transparently allows files to be encrypted on NTFS file systems to protect confidential data from attackers with physical access to the computer. EFS is susceptible to brute-force attacks against user account passwords.

EFT: Enhanced File Transfer

Event Rule: Used to specify an action to occur when an event takes place and/or a condition is present; e.g., send an e-mail when a file is uploaded.

FIPS: The Federal Information Processing Standard (FIPS) Publication 140-2 specifies the security requirements of cryptographic modules used to protect sensitive information.

Folders: In the administration interface, you can define and manage physical folders and virtual folders.

FTP: File Transfer Protocol. Protocol used for exchanging files over any network that supports TCP/IP (such as the Internet or an intranet). FTP servers by default listen on port 21 for incoming connections from FTP clients.

FTPS: File Transfer Protocol Secure (commonly referred to as FTP/SSL). A method by which software can perform secure file transfers, involving the use of a SSL/TLS layer below the standard FTP protocol to encrypt the control and/or data channels.

GeoTrust: Digital certificate provider, owned and operated by VeriSign.
GLBA: Gramm-Leach-Bliley Act. GLBA compliance is mandatory for financial services companies; a policy must be in place to protect financial information from foreseeable threats in security and data integrity.

Group: Allows the administrator to define access permissions to files and folders. Just as User Setting Levels control access to EFT resources such as bandwidth allowances and connectivity privileges, Groups control access to folders. See virtual folders.

HIPAA: Health Insurance Portability and Accountability Act. Enacted by the U.S. Congress in 1996; requires the establishment of national standards for electronic health care transactions; addresses the security and privacy of health data.

HSM: The High Security Module is an add-on to EFT to add high security features and facilitate ongoing compliance with PCI DSS, and other corporate and industry security standards.

HTML: HyperText Markup Language. Used to define the structure of a Web page. Compare to XML.

HTTP: Hypertext Transfer Protocol. An application protocol that runs on top of the TCP/IP suite of protocols used for Internet/intranet communications, typically over port 80.

HTTPS: Secure HTTP connection. HTTP is used, but with TCP port 443 and an additional encryption/authentication layer between the HTTP and TCP.

IDN: An internationalized domain name (IDN) is an Internet domain name that contains at least one label (e.g., www, globalscape, and com are each labels) that is displayed in a language-specific script or alphabet, such as Chinese, Russian, or the Latin alphabet-based characters with diacritics, such as French. These writing systems are encoded in multi-byte Unicode.

IETF: Internet Engineering Task Force. Develops and promotes Internet standards, cooperating closely with the W3C and ISO/IEC standard bodies; dealing in particular with standards of the TCP/IP and Internet protocol suite.

IIS: Microsoft Internet Information Services. Provides Web infrastructure security.

instance: An instance of the SQL Server 2000 database engine is one copy of the database software that operates as an operating system service.

intermediate certificate authority: There are two types of Certificate authorities (CAs): Root CAs and Intermediate CAs. A certificate signed by a Root CA is implicitly trusted by most Web browsers. A certificate signed by an Intermediate CA may not be implicitly trusted by most Web browsers. Intermediate CA certificates are sometimes called “chained root certificates.” An Intermediate CA signed certificate often costs significantly less than a Root CA signed certificate.
IPv6: Internet Protocol version 6 (IPv6) is a version of the Internet Protocol (IP) developed by the Internet Engineering Task Force (IETF) to deal with IPv4 address exhaustion, and is described in Internet standard document RFC 2460.


IUSR: IUSR_<computername> is an IIS account for anonymous access to IIS. If a Web site is set to use anonymous authentication, the user is mapped to the IUSR_<computername> account.

IWAM: Internet Server Web Application Manager. IWAM_<computername> is an IIS account for starting out-of-process applications in IIS 6.0 isolation mode.

keychain: Keychain is Apple Inc.’s password management system in iOS.

LDAP: Lightweight Directory Access Protocol. An application protocol for querying and modifying directory services running over TCP/IP.

LDAP Attribute: Denotes user names in the LDAP database. This allows you to specify the attribute from the queried list of users that denotes user names. Commonly used attributes are cn or uid.

LDAP Base DN: Base Distinguished Name. Specifies necessary domain components of the LDAP server. Some LDAP systems, such as Sun ONE Server and Microsoft’s Active Directory server, require the organizational unit (”ou”) that houses the users on that LDAP server to be included in the BaseDN to allow users to successfully authenticate. The organizational unit is the parent object that contains the user objects. For example, if the classObject that holds user accounts is person, the hierarchical parent node/container could be the organizational unit people. If the organizational unit is required by your LDAP server, prepend it to the distinguished name.

LDAP Port: Port of the LDAP server. The default is port 389; port 636 for SSL connections.

LDAP User Filter: EFT uses the User Filter to query the LDAP server for a list of users. The default setting is objectClass=person, which retrieves the users on the LDAP server that belong to the person ObjectClass.

MA: Multiple Attachments. The ability to transfer multiple documents within a single AS2 message.

MD5: A secure, one-way hash algorithm used in conjunction with digital signature allowed in AS2. SHA-1 is recommended.
MDN: Message Disposition Notification. The Internet messaging format used to convey a receipt; MDN is used interchangeably with receipt.

MFT: Managed File Transfer. Provides control over network file transfers, including securing the data by encrypting the transmission channel or the data itself, managing trading partners and the way they are authenticated, automating transfers to ensure that service level agreements are met, monitoring and reporting file transfer activity for accountability, and passing data through the DMZ to a backend server so that no sensitive data resides in the DMZ.

MIC: The message integrity check (MIC), also called the message digest, is the digest output of the hash algorithm used by the digital signature.

MIME: Multipurpose Internet Mail Extensions. A specification for formatting non-ASCII messages so that they can be sent over the Internet. S/MIME supports encrypted messages.

Mode Z: Mode Z compression compresses files on the fly for file transfers, saving bandwidth and improving transfer times.

N

NCSA: National Center for Supercomputing Applications.

NRR: Non-repudiation of receipt (NRR) is a legal event that occurs only when the original sender has verified the signed receipt returned from the recipient of the message, and has verified that the returned message integrity check (MIC) inside the MDN matches the previously recorded value for the original message. That is, the sender of the message obtains undeniable proof that the recipient received the message and that the message was not altered in transit. NRR is established when both the original message and the receipt use digital signatures.

NTLM: NT Lan Manager. A challenge/response form of authentication that was the default network authentication protocol in Windows NT 4.0.

O

ODBC: Open Database Connectivity. A standard database access method used to access any data from any application, regardless of which database management system (DBMS) is handling the data.

OpenPGP: Uses public-key cryptography and includes a system that binds the public keys to a user name.

OTP: One-Time Password. Intended to make it more difficult to gain unauthorized access. By constantly altering the password, as is done with a one-time password, this risk can be greatly reduced.

P

PAN: Primary Account Number. A unique sequence of numbers assigned to a cardholder account that identifies the issuer and type of financial transaction card.
PCI: Payment Card Industry. The PCI Security Standards Council is an open global forum for the ongoing development, enhancement, storage, dissemination, and implementation of security standards for account data protection.

PCI DSS: Multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures.

PEM: Privacy Enhanced Mail. Base64 encoded DER certificate, enclosed between -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----.

PerfMon: Microsoft utility. Allows you to view a running count of anonymous and nonanonymous users and other IIS objects.

Physical folder: Directory you create on your hard drive from within the EFT.

PNC: Peer Notification Channel. The outbound-initiated two way socket connection used for communication, typically on port 44500 in DMZ Gateway.

POP3: Post Office Protocol version 3. Used to retrieve e-mail from a remote server over TCP/IP. Compare to SMTP.

Private Key: The server’s private key decrypts the client’s session. The private key has a .key extension and is part of the public-private key pair.

protocol: Special set of rules between a client program and a server program in a network.

Public Key: A message encrypted with a recipient’s public key cannot be decrypted by anyone except the recipient possessing the corresponding private key. See Private Key.

Public Key Blob: A public key BLOB contains the public key in plaintext form.

Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names (IDN) that uniquely and reversibly transforms a Unicode string into an ASCII string.

RADIUS: Remote Authentication Dial In User Service (RADIUS) is a networking client/server protocol that runs in the application layer, using UDP as transport, and provides centralized Authentication, Authorization, and Accounting (AAA) management for computers to connect to and use a network service.

RDCW: The ReadDirectoryChangesW function, used in directory management, retrieves information that describes changes within a specified directory.

Receipt: The functional message that is sent from a receiver to a sender to acknowledge receipt of an EDI/EC interchange. This message may be either synchronous or asynchronous.

root certificate: Unsigned public key certificate or a self-signed certificate; part of a public key infrastructure scheme. The most common commercial variety is based on the ITU-T X.509 standard, which normally includes a digital signature from a certificate authority (CA).
RSA SecurID: A mechanism for performing two-factor authentication for a user to a network resource.

S

S/MIME: Secured Multi Purpose Internet Mail Extensions. A format and protocol for adding cryptographic signature and/or encryption services to Internet MIME messages.

SAN: Storage Area Network. An architecture to attach remote computer storage devices such as disk arrays, tape libraries and optical jukeboxes to servers in such a way that, to the operating system, the devices appear as locally attached devices.

sandboxed: A sandbox is a security mechanism for separating running programs, often used to execute untested code, or untrusted programs from unverified third-parties, suppliers, untrusted users and untrusted websites.

SAT: The Secure Ad Hoc Transfer module is an add-on to EFT allows your internal users to send and receive large e-mail file attachments to recipients outside of your organization quickly, reliably, and securely, without having to manually create or maintain FTP accounts on EFT. (Accounts are created and expire automatically.)

Secure Ad Hoc Transfer module: Allows internal users to send and receive large e-mail file attachments to recipients outside of your organization quickly, reliably, and securely, all without having to manually create or maintain FTP accounts on EFT.

Server: In the administration interface, a Server contains the settings for one or more EFTs, either locally or remotely.

Server Group: In the administration interface, Server Groups are at the top of EFT’s setting hierarchy and allow you to group multiple Servers.

Session Key: The client and the server use the session key to encrypt data; created by the client via the server’s public key. See Public Key.

SFTP: Secure File Transfer Protocol. A network protocol designed by the IETF to provide secure file transfer and manipulation facilities over the secure shell (SSH) protocol.

SHA-1: Secure, one-way Hash Algorithm used in conjunction with digital signature; the recommended algorithm for AS2.

Signed Receipt: A receipt with a digital signature.

Site: In the administration interface, a Site is similar to a virtual FTP server bound to one or more IP addresses.

SMTP: Simple Mail Transfer Protocol. Simple text-based protocol used to send e-mail using TCP on port 25 (by default). (Compare to POP3.)

SQL Server: SQL Server is a relational database management system (RDBMS) produced by Microsoft.
SSL: Secure Sockets Layer, a protocol designed and implemented by Netscape Communications, provides for encryption of a session, authentication of a server, and optionally a client, and message authentication.

Synchronous Receipt: A receipt returned to the sender during the same HTTP session as the sender’s original message.

TCP/IP: Transmission Control Protocol/Internet Protocol. Uses the client/server model of communication in which a computer user (a client) requests and is provided a service (such as sending a Web page) by another computer (a server) in the network.

TLS: Transport Layer Security. SSL has been merged with other protocols and authentication methods into this new protocol.

trading partner: Organizations that send or receive documents from each other. The trading partners agree on the specific information to be transmitted and how it should be used.

UNC path: Uniform Naming Convention path, e.g., \computername\sharedfolder\resource.

Unicode: A standard that provides a unique number for every character, regardless of platform, program, or language.

URL: Uniform Resource Locator. An Internet address. See also URI.

User Settings Template: Allows you to apply a setting configuration to an entire group of users. Every client account or user must be a member of a User Setting Level. User Setting Levels exist within a Site and consist of a group of settings used as a template. AKA Settings Level.

VAN: Value Added Network. Private network provider that leases communication lines to its subscribers. In the healthcare industry, a VAN is referred to as a "Clearinghouse" and has additional legal restrictions that govern protected healthcare information.

VFS: EFT’s Virtual File System allows you to grant access to files and folders on your system based on user and Group permissions. See virtual folder.

virtual folder: Similar to a Windows shortcut, a virtual folder points to an existing folder on the EFT computer or another system to which EFT has access.

VPN: Virtual Private Network. A communications network tunneled through another network and dedicated for a specific network.
W

**W3C:** World Wide Web Consortium

**Web Transfer Client:** Browser-based file transfer client that allows users to transfer files to/from an EFT using a connected Web browser.

**workflow:** A workflow is a series of steps that can perform file transfers, batch data processing, application testing, and so on, set to run automatically when started by some event.

**WSDL:** Web Services Description Language. An XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information.

X

**XCRC:** EFT's file integrity command. When an XCRC-enabled client performs a transfer, it can request EFT to do a checksum calculation on the file. If it matches the checksum on the client, then the transfer is deemed successful.

**XML:** Extensible Markup Language. A general-purpose markup language used to store any amount of text/data enclosed by a user-defined start and end tag. Compare to HTML.
Index

Add Workspace Participants .......................................................... 63
Allow Secure File Sending ............................................................ 15
Allow Web Transfer Client ............................................................ 9
Canceling a Transfer ................................................................. 54
Change
  Changing Your Password .......................................................... 74
Clearing the Transfers pane .......................................................... 54
Client access .............................................................................. 9
comments ............................................................................... 60
Conceal WTC and Its Content from Searches ..44
CRC ...................................................................................... 39
  XCRC .............................................................................. 39
Create
  Creating Folders ..................................................................... 56
Customizing .............................................................................. 34
Customizing the Email Interface .................................................. 33
Deleting a Folder or File ............................................................... 57
Disable CRC .............................................................................. 39
Disabling ................................................................................... 40
Display Full Name of User in WTC on LDAP Site ......................... 44
Downloading a File ...................................................................... 53
Edit Notification Options ............................................................. 67
Edit-Remove Workspace Permission ............................................. 65
Emailing Files from within the WTC ............................................. 58
Enable
  Enable and Configure EFT WorkSpaces ..................................... 10
  Enabling JavaScript in the Browser ............................................ 49
  JavaScript ............................................................................. 49
Enable and Configure the Drop-Off Portal .................................... 16
Enable-Disable Reply Portal ......................................................... 15
Enabling Java in the Browser ......................................................... 49
Enabling User Access to the Web Transfer Client ......................... 9
End-User Login In ....................................................................... 40
End-User Login In to EFT ............................................................ 40
Error Messages ......................................................................... 75
Error Messages and File Names .................................................... 75
Expire a Workspace .................................................................... 65
File Comments ........................................................................... 57
File-Naming Conventions ........................................................... 45
Filtering and Sorting the File List ................................................ 55
Filtering the Filesystem List ......................................................... 55
Guest Users .............................................................................. 73
HTTP ....................................................................................... 9
  HTTPS .................................................................................. 9
IWA ......................................................................................... 40
JavaScript .................................................................................. 49
Joining a Workspace ................................................................... 63
Licensing Workspaces .................................................................. 8
Localization (Language) Settings ................................................. 19
log
  Log In ................................................................................... 40
  Logging In to the WTC ........................................................... 50
  Logging Out of the WTC .......................................................... 51
  logins ................................................................................. 40
  logging in to EFT ................................................................. 40
Managing Workspaces in the VFS ............................................... 30
Moving Files Between Folders ...................................................... 45, 56
Notifications ............................................................................. 24, 66
Overview of the Web Transfer Client ........................................... 45
Picking up Files .......................................................................... 69
Rebranding .................................................................................. 34
Rebranding the Web Transfer Client ............................................ 34
Renaming
  Renaming a File ...................................................................... 56
Reply Portal ............................................................................... 70
Request Files ............................................................................. 72
Restrict Workspaces Invitations to Specific Domains .................... 21
  Resuming Transfers ............................................................... 54
Searching for Files ..................................................................... 55
Sharing Folders .......................................................................... 60
Stop Sharing a Workspace ......................................................... 65