



FileWay™ Administrator's Guide

Version 5



Copyright (c) 2003 - 2019 Everywhere Networks Corporation, All rights reserved.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording or otherwise) or for any purpose, without the express of a written permission from Everywhere Networks Corporation.

Everywhere Networks Corporation may have patents, patent applications, trademarks, copyrights or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Everywhere Networks Corporation, the furnishing of this document does not give you any license to these patents, trademarks, copyrights or other intellectual property.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Everywhere Networks Corporation – 185 Rideau St, Ottawa, Ontario, Canada



Table of Contents

1	About FileWay	7
1.1	What can users do with FileWay?	7
1.2	Is FileWay functionality customizable?	7
1.3	How to access FileWay?	7
1.4	What can you, as administrator, do with FileWay?	7
1.5	Who needs FileWay?	8
1.6	Who are FileWay's customers?	8
2	FileWay Components	9
3	FileWay User Interface	10
3.1	Preferences Menu	11
3.2	Search	12
3.3	Action Menu	13
3.3.1	Selecting Files and Folders	13
3.3.2	Moving and Copying Files and Folders	14
3.3.3	Sending Files as Email Attachments	14
3.4	Transfer Menu	15
3.5	AttachLink Menu	15
3.5.1	Sending Files as Links in Email Messages.....	16
3.5.2	Accessing AttachLink.....	17
3.5.3	Creating a Folder to which Email Recipients May Upload Files.....	21
3.5.4	Sharing a Folder to which Email Recipients May Upload Files	21
4	Requirements	23
4.1	Hardware Requirements	23
4.2	Software Requirements.....	23
4.2.1	FileWay FrontEnd Requirements	23
4.2.2	FileWay BackEnd and FileWay Manager Requirements	24
4.2.3	FileWay Drive Requirements	24
4.2.4	Supported Browsers for FileWay	24
4.2.5	Supported WebDAV clients for FileWay Drive.....	24
4.3	Network Requirements	25
4.4	Windows 2012, 2016 and 2019 Requirements	25
4.5	SQL Server Requirements.....	25



4.6	Creating a FileWay Worker Account.....	26
4.7	General Installation Requirements.....	26
5	Installing FileWay	27
5.1	Database Installation	29
5.2	FileWay BackEnd Installation.....	31
5.2.1	FileWay Manager Installation	32
5.2.2	Mail Server Setup.....	33
5.3	FileWay FrontEnd Installation	34
5.4	FileWay Drive Installation.....	35
5.5	SecureView Backend Installation (legacy)	36
5.6	FileWay OWA Integration (optional)	36
5.7	Windows Services	39
5.8	Troubleshooting Installation.....	40
6	Post-Installation Configuration Steps.....	41
6.1	AttachLink Configuration	41
6.1.1	Number of Files That Appear in AttachLink Email	41
6.1.2	Maximum Login Attempts	41
6.2	FileWay Integration with Exchange 2013 and 2016	41
6.3	Enabling SSL	42
6.3.1	FileWay Authentication Settings.....	43
6.3.2	HTTP Redirect Setting	45
6.4	Configuring the SecureView BackEnd Scheduled Task.....	46
6.5	Support for DUO Two Factor Authentication	47
7	FileWay and SharePoint Integration (optional).....	48
7.1	Integrating FileWay with SharePoint 2007.....	48
7.1.1	Installing FileWay	48
7.1.2	Configuring IIS	49
7.1.3	Configuring SharePoint	50
7.1.4	Creating an Access Point from SharePoint to FileWay	50
7.1.5	Creating a Hyperlink inside SharePoint	51
7.1.6	Adding FileWay to SharePoint 2007 as a WebPart.....	51
7.2	Integrating FileWay with SharePoint 2010.....	55
7.2.1	Installing FileWay	55



7.2.2	Configuring IIS.....	56
7.2.3	Configuring SharePoint	57
7.2.4	Creating an Access Point from SharePoint to FileWay	57
7.2.5	Creating a Hyperlink inside SharePoint	57
7.2.6	Adding FileWay to SharePoint 2010 as a WebPart.....	57
7.3	Integrating FileWay with SharePoint 2013.....	62
7.3.1	Installing FileWay.....	62
7.3.2	Install Authentication Module	62
7.3.3	Adding FileWay to SharePoint 2013 as WebPart.....	63
8	Branding FileWay.....	66
9	Localizing FileWay	66
10	Customizing FileWay FrontEnd.....	67
11	Ziping and Unicode.....	67
12	Using FileWay Drive.....	68
12.1	IIS, Authentication & SSL	68
12.2	Tested WebDAV Clients.....	68
12.3	Connect to FileWay Drive	68
12.3.1	Connect FileWay Drive to the Built-in WebDAV Clients in Windows 7 and Later	68
12.3.2	Connect to the Built-in WebDAV Client in Apple's OSX.....	69
12.3.3	Connect to Third Party WebDAV Clients	69
13	Configuring FileWay	73
13.1	Rulesets	73
13.1.1	Ruleset Resources.....	73
13.1.2	Ruleset Members.....	73
13.1.3	Ruleset Options.....	73
13.1.4	Planning Access Rules for Multiple Users	74
14	Using FileWay Manager.....	75
14.1	Starting FileWay Manager	75
14.2	Specifying Global Settings for FileWay	76
14.3	Managing Ruleset Members, Options and Resources.....	91
14.3.1	Creating a Ruleset.....	91
14.3.2	Adding Members to a Ruleset	93
14.3.3	Adding Resources to a Ruleset	95



14.3.4 Managing Ruleset Options.....	97
14.3.5 Modifying Rulesets	98
14.4 Adding Icons for New File Types.....	100
14.5 Saving Data in FileWay Manager	101
14.6 Managing FileWay Database with FileWay Manager	101
14.6.1 Adding Trusted Domains.....	101
14.6.2 Viewing Current Contents of the Database	103
14.6.3 Updating the Database with Latest Changes.....	103
14.6.4 Manage File Locks.....	103
14.6.5 Manage AttachLinks.....	104
14.6.6 Manage Logs	106
14.6.7 Password Encryptor	107



1 About FileWay

FileWay is on-premises secure remote file access software that provides your organization's web-enabled users with access to their documents, no matter their location or the device they are using. Your users can remotely access important files, and folders, whether they're at home, on the road, or on-site with a customer.

1.1 What can users do with FileWay?

Users accessing their documents with FileWay can perform all the standard functions; create new folders, rename files and folders, delete files and folders, and copy and move files and folders. They can upload and download documents from and to the device they are using (mobile or desktop).

Users can view the content of documents online using FileWay's rendering engine. Through secure time-expiry links, users can send and receive documents and share folders with others for collaboration.

Users can edit documents online from remote locations as if they are on their desktop computer.

1.2 Is FileWay functionality customizable?

Yes, FileWay functionality is customizable. Your network administrator, using FileWay Manager, can choose which user or groups of users, from your Active Directory, can access FileWay. The administrator can specify which internal resources users can access from FileWay and what they can do with these resources. FileWay functionality (listed above) can be customized on a user-by-user or group-by-group basis as you see fit. The administrator can specify how users access FileWay whether from a browser or mobile device, or by mapping it to users' desktop computers.

1.3 How to access FileWay?

The network administrator can configure FileWay to be accessed in a number of ways and provide different access methods to different users.

FileWay can be accessed from any browser or mobile device. Authorized users can map FileWay resources to their desktop computers and access their remote files from their operating system.

A network administrator can integrate FileWay with Outlook for Web Access (OWA) and provide users with a single point of access and single sign-on to both emails and documents.

A network administrator can integrate FileWay with SharePoint for ease of access and to bring access to private resources (such as home folders) to SharePoint without adding them to SharePoint library.

1.4 What can you, as administrator, do with FileWay?

Users working from home, occasionally or on regular basis, can map FileWay resources to their desktop computer giving them access to work documents on corporate servers directly and securely without the use of VPN. You can configure FileWay so that your mobile workers can access certain documents and only be able to view their content online and be able to email those documents to customers.

Request for Proposals (RFP) can be handled easily using FileWay's AttachLink feature. RFP documents may be emailed as secure time-expiry links and with an option for the recipient to reply with proposals. When the deadline comes, the links expire and no one can submit new proposals. There will be a record of delivered proposals and email confirmations.

School assignments can be emailed to students with an option to submit the work to the teacher by a certain date and time.



Large documents, such as videos, which are too large to send by email, can be exchanged with others through secure time expiry links.

Secure documents that shouldn't be emailed can be exchanged with others through secure time expiry links. Those documents remain on your server and are not transferred to a cloud service.

Folders can be shared with others for collaboration. The folders remain on the server and are not moved to a cloud service or unsecure location on the network. The access to the shared folders will expire at a set time. All changes to shared documents will be archived and nothing will be deleted or overwritten.

1.5 Who needs FileWay?

- Anyone wanting to work remotely
- Workers on the move such as sales staff
- Users who need to exchange secure or large documents with others
- Users who need to collaborate with others

1.6 Who are FileWay's customers?

- School, colleges and universities
- Municipal governments
- Government departments
- Legal and accounting firms
- Enterprise customers with remote workers



2 FileWay Components

FileWay provides users with secure remote access to corporate resources over the Internet using their browser. With FileWay, users can view, email, manage, download and upload files and folders from any location. The following figure shows the end-users' graphical interface to FileWay.

FileWay comprises the following components:

- FileWay FrontEnd
- FileWay BackEnd
- FileWay Manager
- FileWay Drive (optional)
- OWA integration (optional)

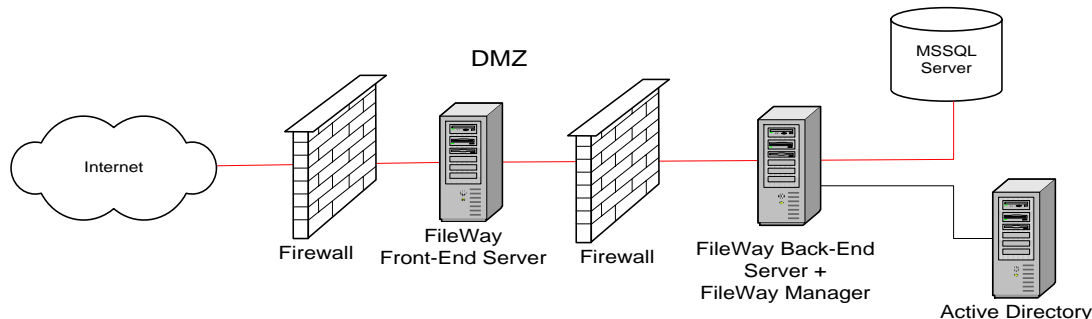
FileWay FrontEnd provides the FileWay user interface.

FileWay BackEnd performs the FileWay functions requested by users via the FileWay FrontEnd.

FileWay Manager is a Windows application that Administrators use to specify users' access rights for corporate drives and shared folders.

FileWay Drive is a WebDAV class 2 compliant server that acts as a WebDAV gateway to the internal network and allows users to access their files and folders through WebDAV clients.

These components can be installed together on the same server or separately depending on the configuration you choose. The figure below shows a typical FileWay installation.



The optional FileWay OWA integration component adds a FileWay button to the OWA tool bar to provide OWA users with access to FileWay from OWA.

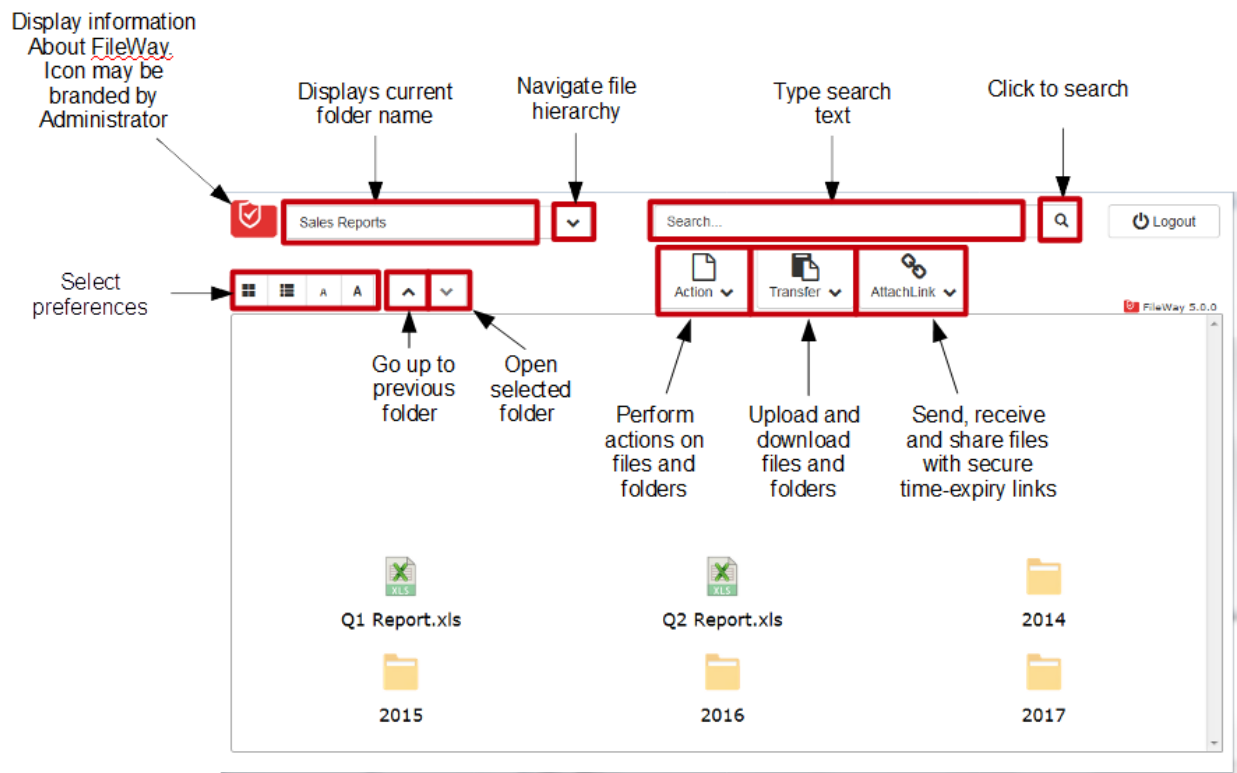


3 FileWay User Interface

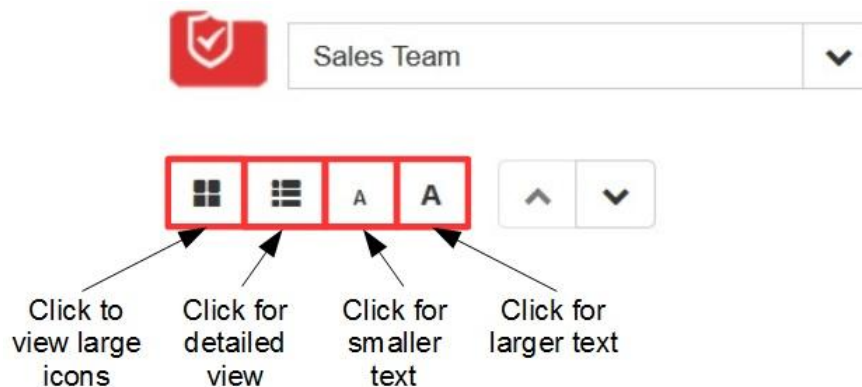
When users access FileWay using their browser, with the URL provided by the network administrator, the following login window appears.



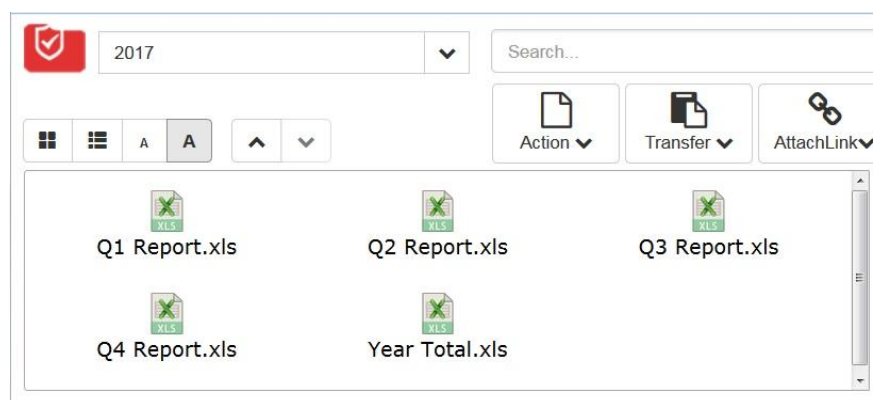
After users log on, the following window appears.



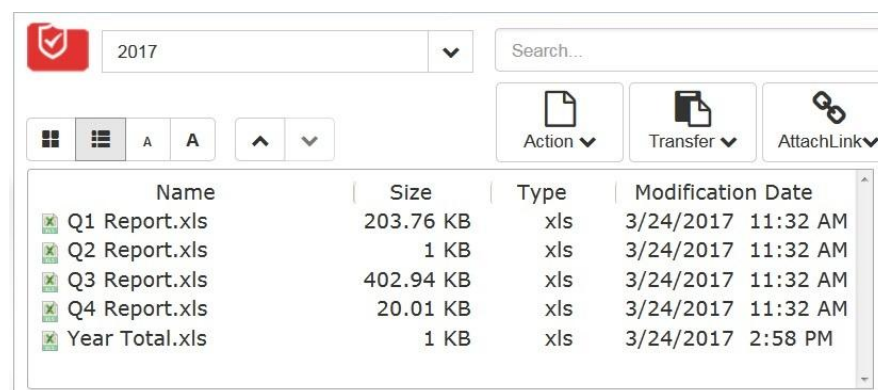
3.1 Preferences Menu



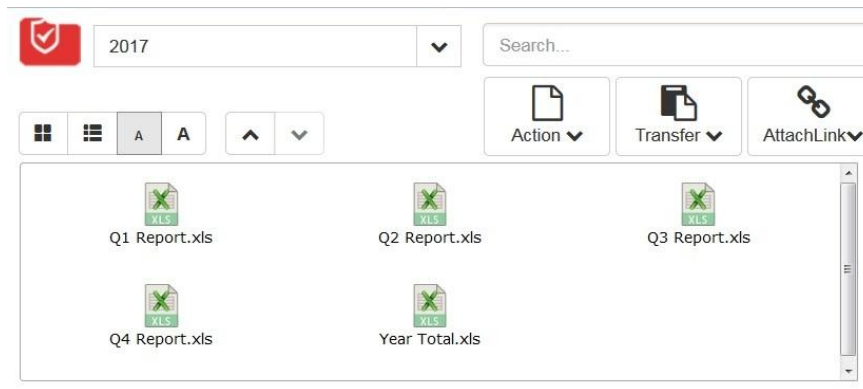
Large Icons View



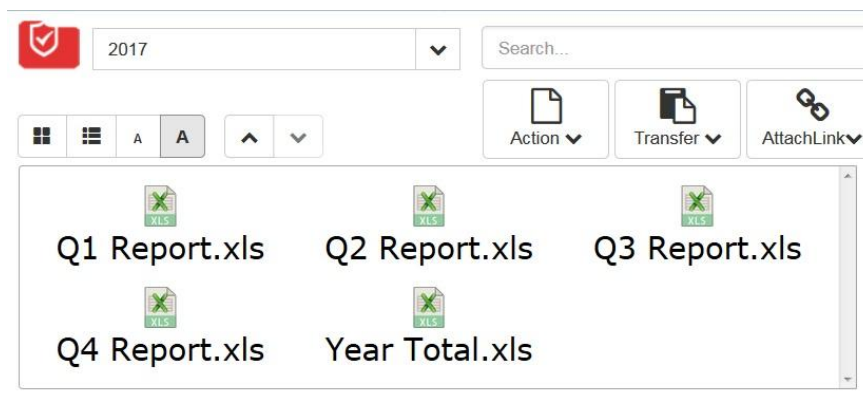
Detailed View



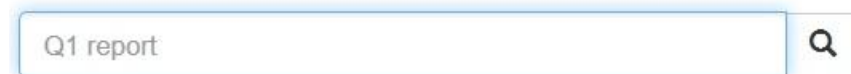
Smallest Text



Largest Text



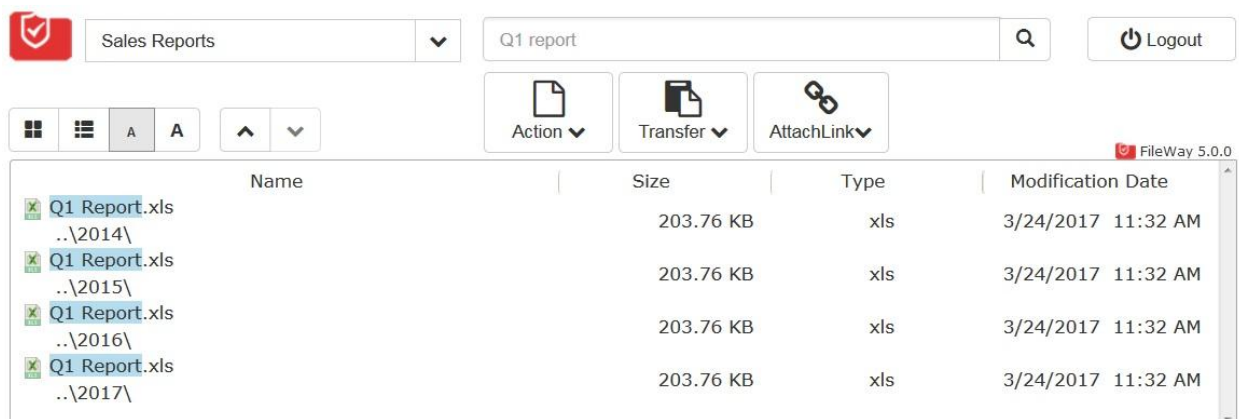
3.2 Search



The Search function allows users to find files and folders using search text contained in file or folder names.

The user can type what they are looking for in the search text box and press **Enter** or click the magnifying glass icon. The asterisk (*) can be used as substitute for characters.

Search results are listed with the path:

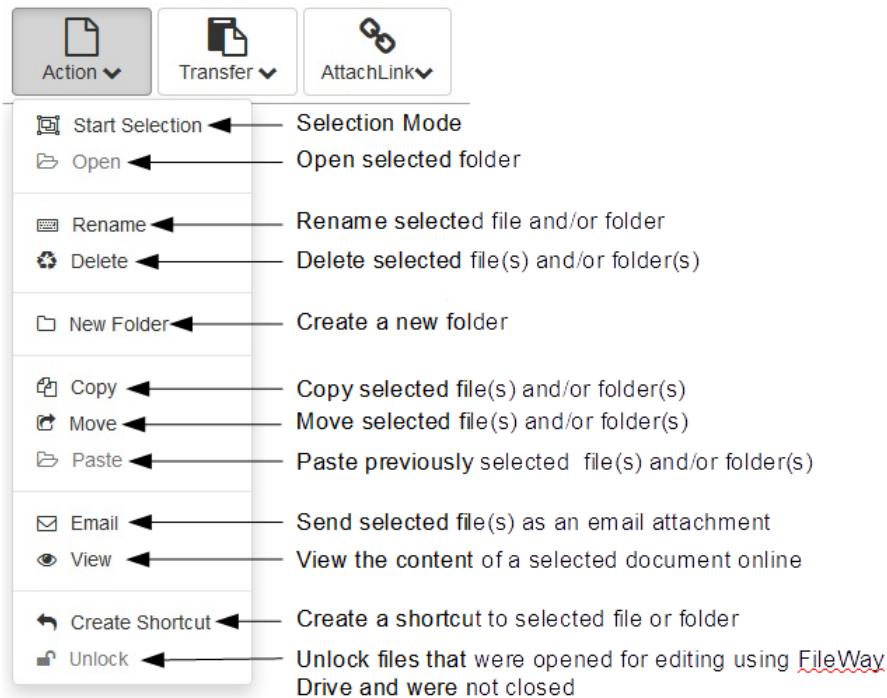


To quit searching and go back to previous location, the user can click the **Up** button, or click in the Search text box and press **Enter** to clear the search string.

If the user double-clicks a folder name then FileWay will exit search and will open that folder. All FileWay functions are available on any selected file in the search result list.

The Minimum Length of String to Search with and Maximum Allowed Results can be configured by the Administrator using FileWay Manager.

3.3 Action Menu

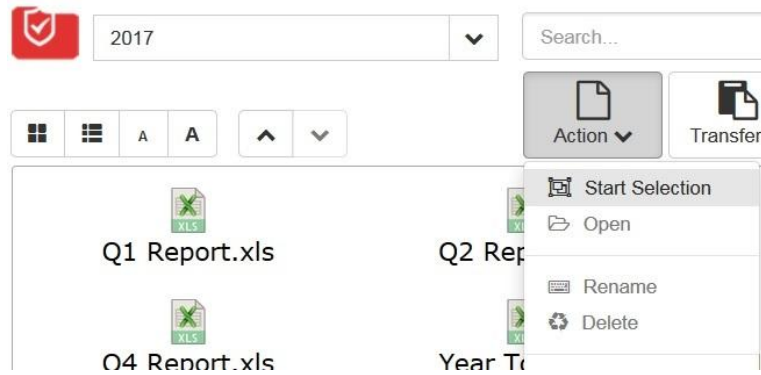


3.3.1 Selecting Files and Folders

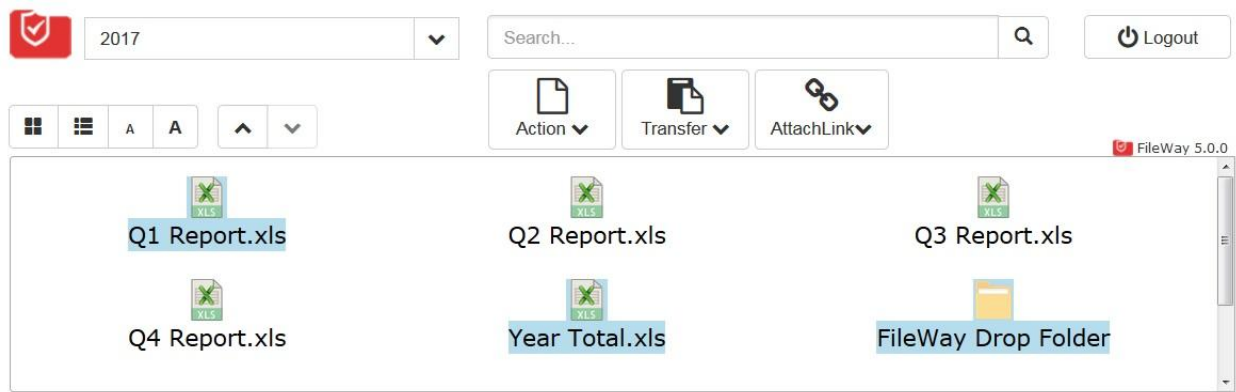
Users select/deselect files and folders in FileWay the same way they do with their desktop computers using the mouse in combination (optionally) with the Shift and Control keys (Command key on Macs).

Selecting/deselecting files and folders on portable devices such as mobile phones only allows users to select one file or folder at a time. However, clicking **Actions > Start Selection** (see figure below) lets users select/deselect multiple files by clicking each one in turn. While this function is most useful on mobile devices, users may also use with their desktop computers.





Users can select multiple files and folders without pressing the Shift or Control key. See figure below.



Clicking **Actions > Stop Selection** resets file/folder selection to the default setting.

3.3.2 Moving and Copying Files and Folders

Moving or copying files and folders is a two-part process. First you select the file(s) and/or folder(s) and then click **Action > Move** or **Action > Copy**. Alternatively, you can right-click the file to get the context menu and then click **Move** or **Copy**. Then you browse to the location to which you want to move them and then click **Action > Paste**. When the items are pasted, a suffix (consisting of a number within brackets), is appended to the file/folder name(s) if files/folders already exist with the same name; for example test (1).

3.3.3 Sending Files as Email Attachments

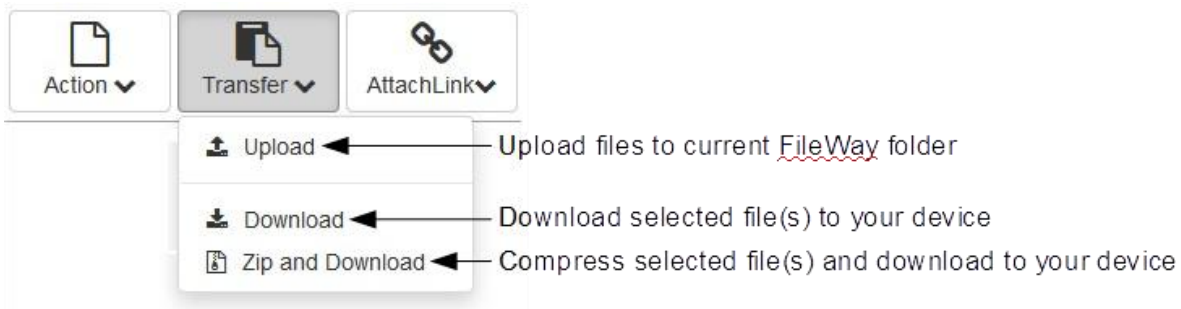
There is a file size limit when sending files as email attachments; the limit is set by the Administrator. If the file(s) you want to send are too big, you can email them as links instead; the recipient(s) will then be able to download or view the file(s). Refer to Section 3.5.1.

Select file(s) and/or folder(s) that you want to send and then click **Action > Email**. The following email form appears.



Once you have filled out the form, click **Send**.

3.4 Transfer Menu

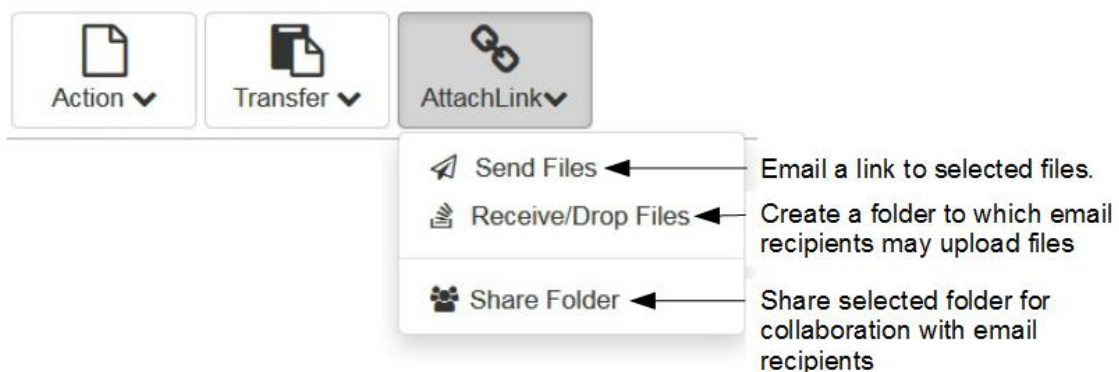


Upload: Sends files up from the local device to the FileWay server.

Download: Sends files from FileWay down to the local device.

Zip and Download: Compresses files on the FileWay server and sends to the local device.

3.5 AttachLink Menu



3.5.1 Sending Files as Links in Email Messages

Users select one or more files or a folder and clicks **AttachLink > Send Files**. The following email form appears:

The screenshot shows an email composition window titled 'Send'. It contains the following fields and options:

- To:** [Empty text box]
- Cc:** [Empty text box]
- Bcc:** [Empty text box]
- Subject:** [Empty text box]
- Attachment:** A dropdown menu showing 'Q1 Report.xls'.
- Allow Recipient to:** Three checked checkboxes: ☒ View, ☒ Download, and ☒ Drop.
- Link Expiry:** A text box containing '7/18/2017 7:43 PM'.
- Allowed Extensions:** A text box containing 'All selected'.

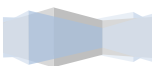
Users can choose to allow recipients to view and/or download them. Users can also allow recipients to upload files to the Drop Folder. If the **Allow Drop** checkbox is selected, a Drop Folder will be created in current directory.

If a folder is selected and the user clicks **AttachLink > Send Files** then the files in the root level of this folder will be sent. Any subfolders and files within subfolders of the selected folder will be not included. The files within the selected folder will be listed in the combo box as shown in the figure below.

This screenshot shows the same 'Send' email form, but with the 'Attachment' dropdown menu open. The menu lists the following files:

- Q1 Report.xls (highlighted in blue)
- Q2 Report.xls
- Q3 Report.xls
- Q4 Report.xls
- Year Total.xls

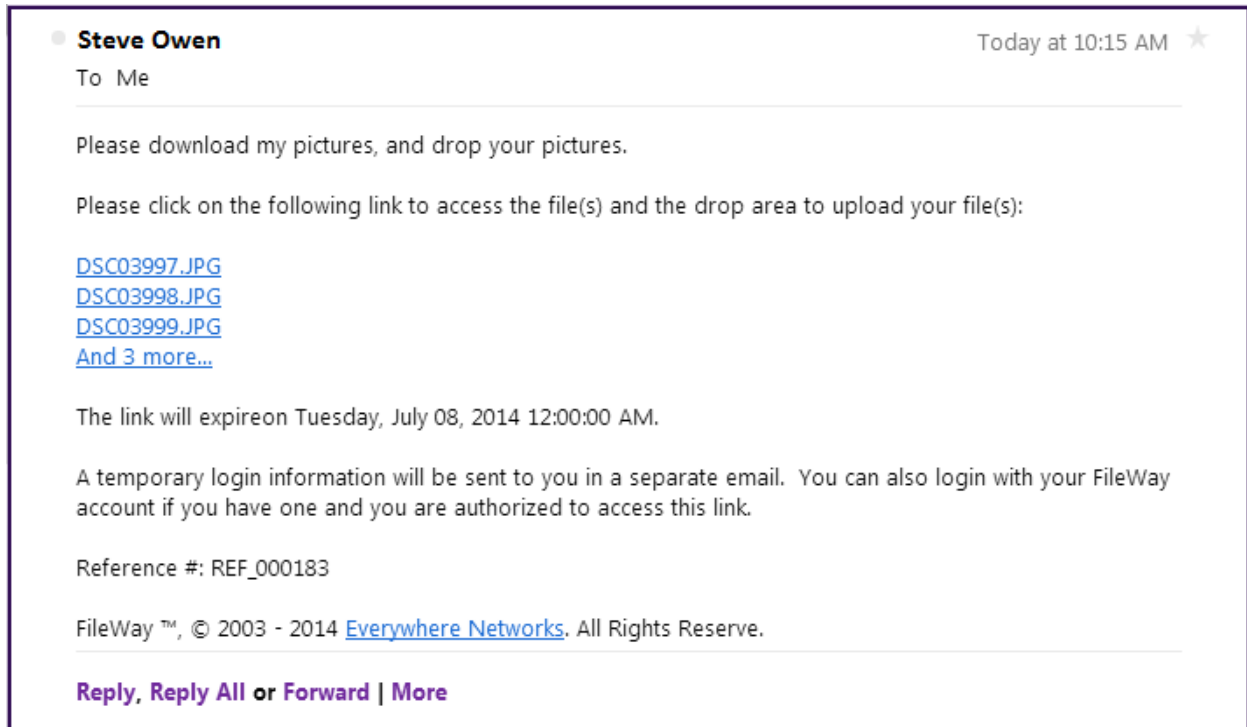
Users can set an expiry date for the Drop Folder (Link Expiry text box). The Default Expiry and Maximum Link Expiry may be configured using FileWay Manager. Users can also specify which types of files may be uploaded to the Drop Folder (Allowed Extensions text box).



Once the user clicks the **Send** button, two emails will be sent to the recipients; one for the link (see Section 3.5.2) and the other one for the temporary login information.

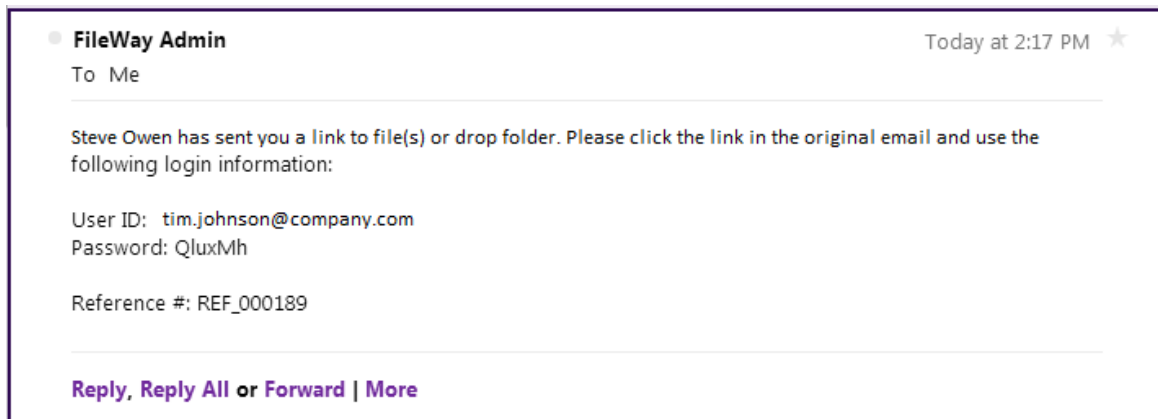
3.5.2 Accessing AttachLink

The first email a recipient will receive contains the link and related information of the attached files (see figure below).



In the email body, three file names appear (see figure above). The Administrator can configure the number of file names that appear.

The second email (see below), which is sent from an admin account, contains a temporary username and password to access attached files through AttachLink.



The user clicks the link in first email and a login window appears (see figure below).





The login screen features a background image of a laptop keyboard. On the left, the FileWay logo is displayed, consisting of a red square with a white checkmark and the word "fileway" in black lowercase letters with a trademark symbol. To the right of the logo, the text "Enter your login information" is centered. Below this, there are two input fields: "Username" with the value "tim.johnson@company" and "Password" with masked characters. A "Login" button is positioned to the right of the password field. At the bottom, a copyright notice reads: "Copyright 2003 - 2017 [Everywhere Networks](#) Corporation. All rights reserved. [version: 5.0.0]"

The user types the temporary login ID and password from the second email or using their FileWay user account if they have one.

A Captcha appears if the login fails three times (see figure below).

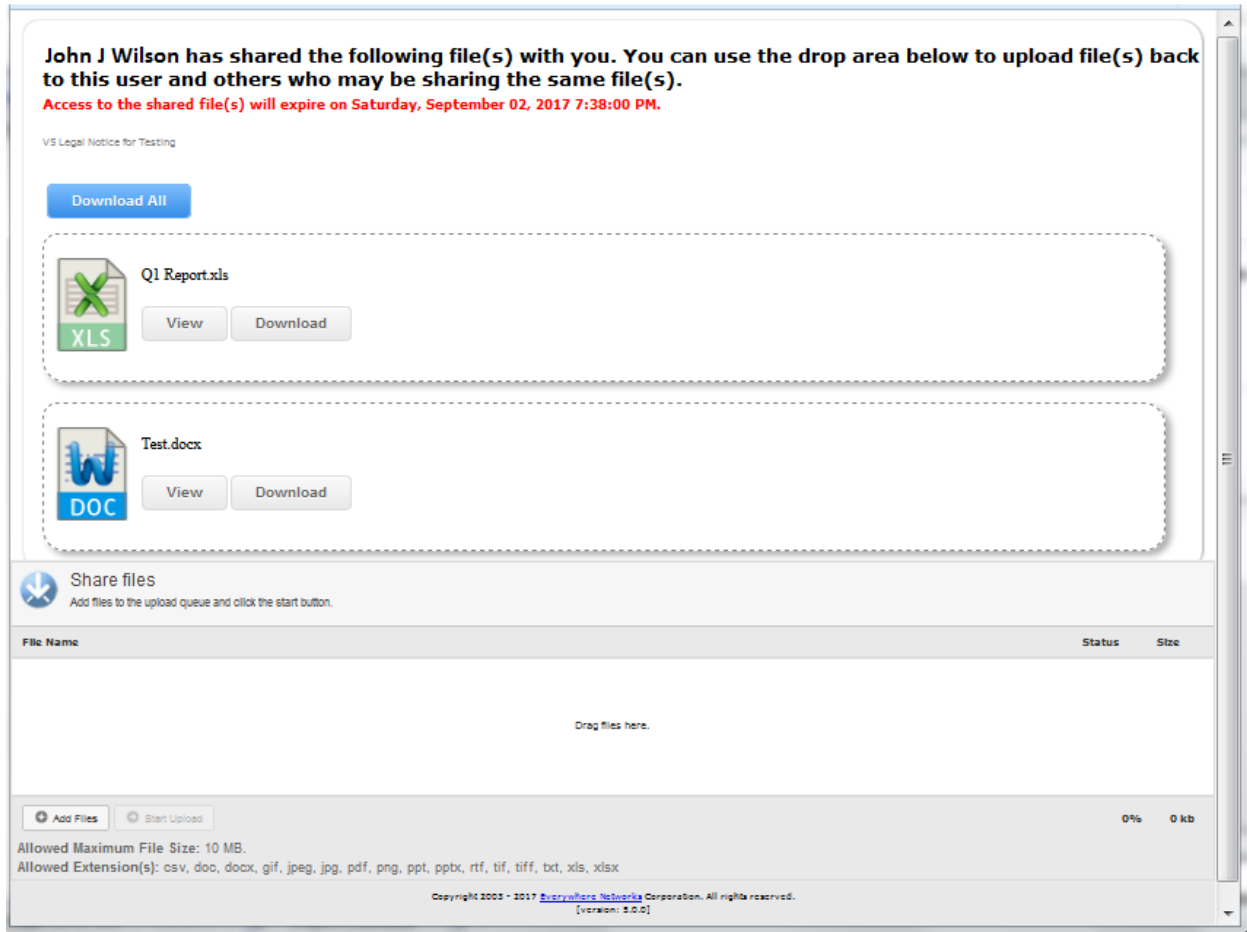


This screen is similar to the first one but indicates a failed login. The title "Please login to access:" is centered. The "Username" field still contains "tim.johnson@company" and the "Password" field is masked. A new "FSMTY" captcha is displayed to the right of the password field, with a "Click to regenerate" link below it. A red "Invalid Login!" message is shown below the "Login" button. The background and logo remain the same. The copyright notice at the bottom is identical: "Copyright 2003 - 2017 [Everywhere Networks](#) Corporation. All rights reserved. [version: 5.0.0]"

The Administrator can configure the number of login attempts.

The following AttachLink page appears once the user is logged in.

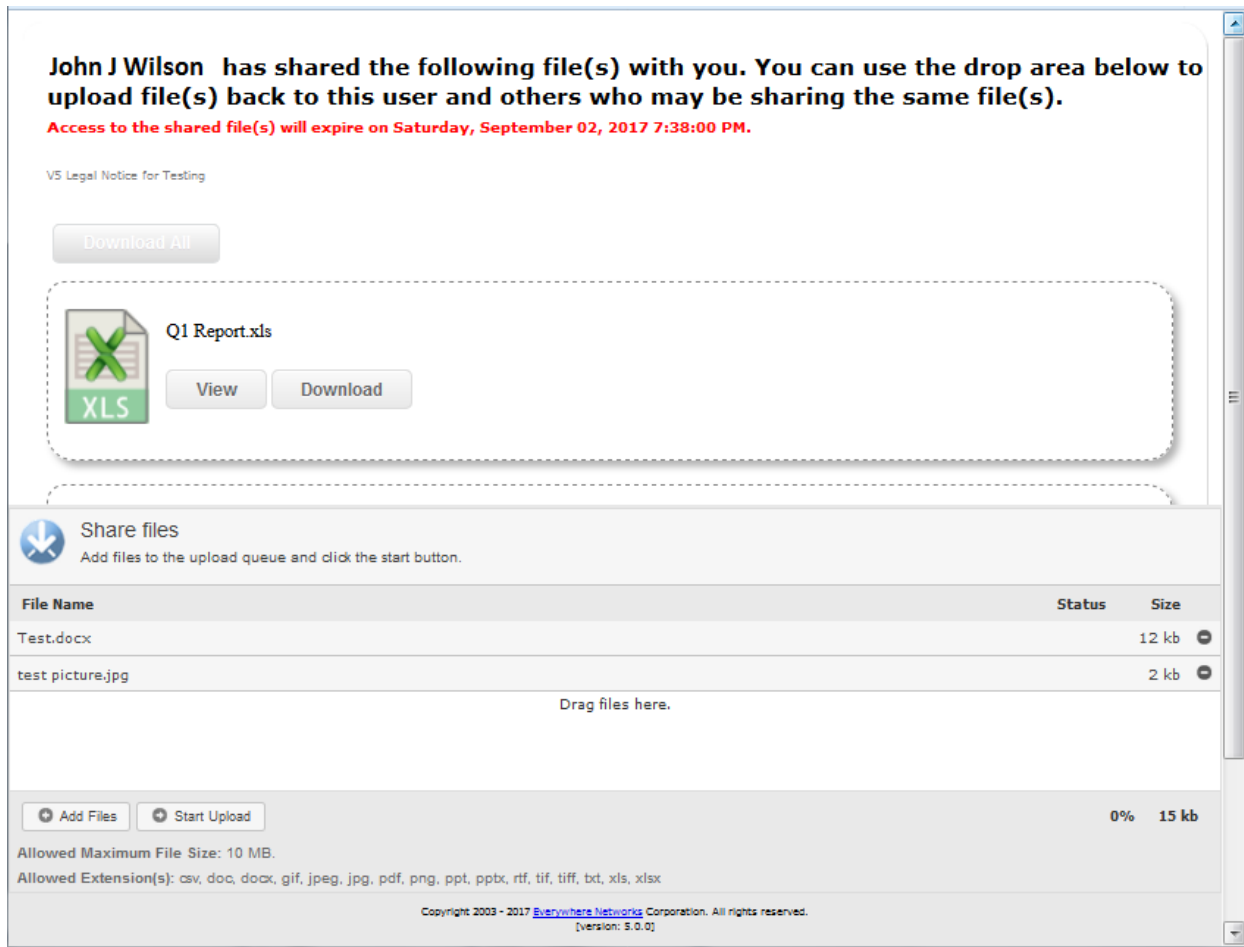




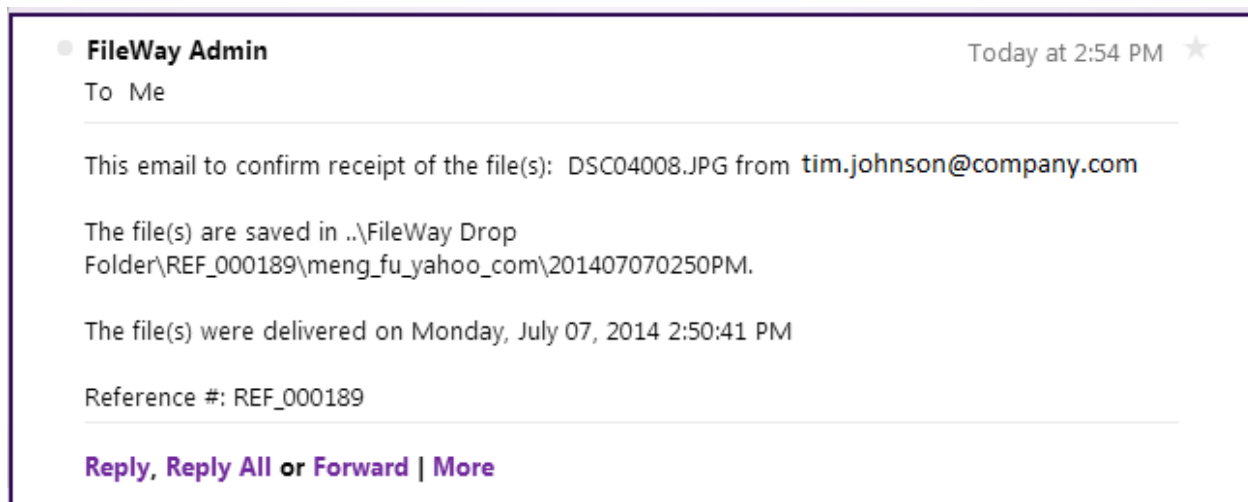
For each attachment, the user can click either the **View** or **Download** button.

If **Allow Drop** was selected when the original sender created this email, the Drop files section will appear in the **AttachLink Landing Page**. Recipients can select files by dragging and dropping them to the Drop Folder or by clicking the **Add Files** button. The selected files will be uploaded by clicking the **Start Upload** button.





Once the files are uploaded, a Receipt Notification Email will be sent to Original Sender and/or Recipients.



To configure AttachLink, refer to the AttachLink Screen section in Section 14.2 Specifying Global Settings for FileWay.



3.5.3 Creating a Folder to which Email Recipients May Upload Files

Users can email a link to others to send them documents.

Once users choose **Receive/Drop Files** from the AttachLink menu, a Drop Folder will be created in the current location or Home Folder if the administrator configured that option and an email form appears.

The screenshot shows an email composition window titled 'Send'. It includes fields for 'To:', 'Cc:', 'Bcc:', and 'Subject:'. The 'Drop Attachment:' field contains a file path: '\\WIN-4K41C7HLD6L\\Sales Folder\\Sales Reports\\2017\\FileWay Drop Folder\\'. The 'Link Expiry:' field is set to '9/2/2017 7:12 PM'. The 'Allowed Extensions:' field is set to 'All selected'. There is a large empty text area at the bottom of the form.

Users can set an expiry date for the Drop Folder (Link Expiry text box). Users can also specify which types of files may be uploaded to the Drop Folder (Allowed Extensions text box).

Once the user clicks the **Send** button, two emails will be sent to the recipients; one containing the link (see Section 3.5.2) and the other one for the temporary login information.

3.5.4 Sharing a Folder to which Email Recipients May Upload Files

Users can select a folder to share with others for collaboration. All files on the root level of the selected folder will be shared. Users sharing the selected folder can modify any of the files and upload new files.

Once users choose **Share Folder** from the AttachLink menu in the Toolbar, an email form appears.

The screenshot shows an email composition window titled 'Send'. It includes fields for 'To:', 'Cc:', 'Bcc:', and 'Subject:'. The 'Attachment:' field shows a dropdown menu with 'Q1 Report.xls' selected. The 'Link Expiry:' field is set to '9/2/2017 7:17 PM' and there is a checkbox labeled 'Link does not expire' which is currently unchecked. The 'Allowed Extensions:' field is set to 'All selected'. There is a large empty text area at the bottom of the form.



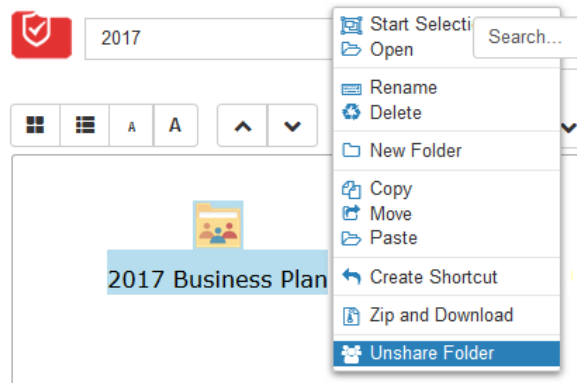
Users can set an expiry date for the Share Folder (Link Expiry text box). Users can also specify which types of files may be uploaded to the Drop Folder (Allowed Extensions text box). If the ruleset option “AttachLink Set Expiry Date” is enabled then the option to “Link does not expire” will be displayed.

Once the user clicks the **Send** button, two emails will be sent to the recipients; one containing the link (see Section 3.5.2) and the other one for the temporary login information.

The shared folder shows up with special icon as shown in the figure below.



Users can right-click the shared folder and Unshare it.



Shared Folders can be shared again with different recipients.



4 Requirements

This chapter describes the minimum system requirements for installing FileWay.

4.1 Hardware Requirements

Each Intel-based server must be configured with the following:

- Minimum Intel Itanium 2 Processor
- Minimum of 4 GB RAM
- Minimum 20 GB Hard Disk
- Single Ethernet Adapter

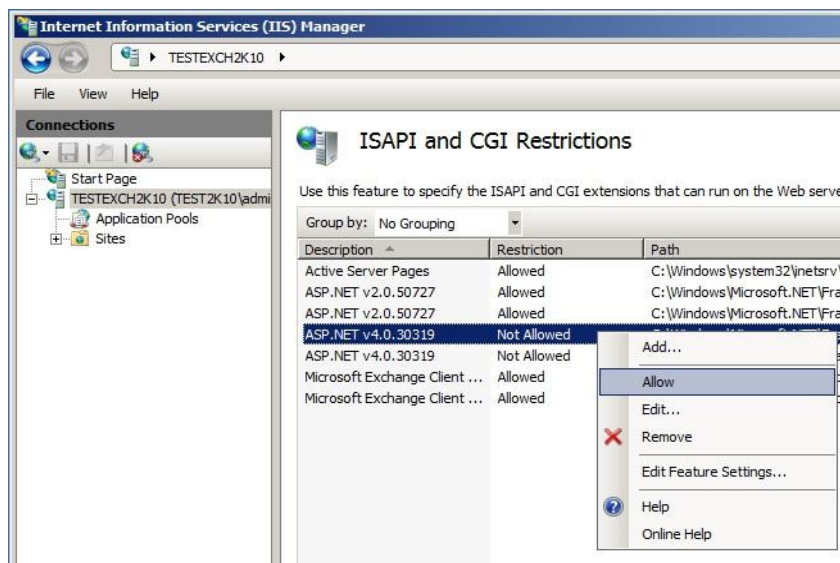
4.2 Software Requirements

4.2.1 FileWay FrontEnd Requirements

- FileWay FrontEnd should be installed on a server within the Domain if using Basic Authentication. If using Form-Based Authentication it is not necessary.
- Microsoft Windows 2012, 2016 or 2019 Server, Standard, Small Business, or Enterprise Edition, 32 bit or 64 bit, any service pack. Microsoft Internet Information Server (IIS) 8 or later.

Note: Support continues to be provided for existing installations on Windows 2008 and 2008 R2. All new installations will require Windows 2012 or higher.

- **OPTIONAL:** If installing the FileWay for OWA Integration component, Microsoft Exchange 2013 or 2016, is required.
- Microsoft .NET Framework version 4.0 or higher. You should check ISAPI and CGI Restrictions for .NET 4.0 with IIS Manager, and change them to Allowed (see figure below).



- For Windows 2012 (IIS 8) be sure to add the required IIS Role Services as specified in the Windows 2012, 2016 and 2019 Requirements in Section 4.4.



4.2.2 FileWay BackEnd and FileWay Manager Requirements

- FileWay BackEnd and FileWay Manager need to be installed on only one server in the Domain. This can be the same server as where FileWay FrontEnd is installed, or a separate server.
- Microsoft Windows 2012, 2016 or 2019 Server, Standard, Small Business, or Enterprise Edition, 32 bit or 64 bit, any service pack.
- **Note:** Support continues to be provided for existing installations on Windows 2008 and 2008 R2. All new installations will require Windows 2012 or higher.
- Any of the following SQL Server versions: SQL Server 2012 and 2014, Express Standard and Enterprise. If you do not have an existing database server, FileWay installer will install SQL Server 2017 Express Edition during the FileWay BackEnd installation. This version of SQL Server requires Windows 2012 or higher.
- For Windows 2012 (IIS 8), Windows 2016 (IIS 10) or Windows 2019 (IIS 10) be sure to add the required IIS Role Services as specified in the Windows 2012, 2016 and 2019 Requirements Section 4.4.
- Microsoft .NET Framework version 4.0 or higher.

4.2.3 FileWay Drive Requirements

- Microsoft Windows 2012, 2016 or 2019 Server, Standard, Small Business, or Enterprise Edition, 32 bit or 64 bit, any service pack
- **Note:** Support continues to be provided for existing installations on Windows 2008 and 2008 R2. All new installations will require Windows 2012 or higher.
- Microsoft .NET Framework version 4.0 or higher
- FileWay Drive should be installed on a server within the Domain
- IIS Basic Authentication Server Security Role

4.2.4 Supported Browsers for FileWay

FileWay supports the following browsers:

- Internet Explorer 9.0 and up (Windows)
- Google Chrome (Windows and Macintosh)
- Firefox version 32 and up (Windows and Macintosh)
- Safari v6.0 and up (Macintosh)

4.2.5 Supported WebDAV clients for FileWay Drive

Below is a list of 3rd party WebDAV clients we tested with FileWay Drive; however, Drive will work with other clients:

- [BitKinex](#) (Windows)
- [NetDrive](#) (Windows)
- [WebDrive](#) (Windows)
- CyberDuck v4.7 (Macintosh)
- WebDAV Nav (iOS and Android)
- My WebDAV (iOS)
- GoodReader (iOS)



4.3 Network Requirements

FileWay components must be installed in an environment where they are able to communicate with each other via TCP/IP and Windows File Sharing.

4.4 Windows 2012, 2016 and 2019 Requirements

Requirements for Installing FileWay Components on Window 2012 (IIS 8) , Windows 2016 (IIS 10) and Windows 2019 (IIS 10) are as follows:

- .NET Framework Version 4.0 (or higher) should be installed on the Server.
- IIS 7 Server Roles Requirements for FileWay BackEnd and FileWay FrontEnd servers. These Server Roles must be installed AND the following "role services" should be selected:
 - Default Document
 - Static Content
 - HTTP Errors
 - HTTP Redirection
 - ASP.NET
 - .NET Extensibility
 - ASP
 - ISAPI Extensions
 - ISAPI Filters
 - ALL the security roles (Basic, Windows, Digest, etc.)
 - IIS Management Console
 - IIS 6 Metabase Compatibility
 - IIS 6 WMI Compatibility
- In IIS at the Site Level, the Feature Delegation 'Error Pages' must be set to Read/Write.

4.5 SQL Server Requirements

Any of the following SQL Server versions are supported: SQL Server 2012 and 2014, Express, Standard and Enterprise. If you do not have an existing database server, FileWay installer will install SQL Server 2017 Express Edition during the FileWay BackEnd installation.

Starting at version 3.8.0, FileWay supports database transactions. If you wish to enable transactions when saving to the database you will need to set the **UsingTransaction** flag to true.

```
<add key="UsingTransaction" value="true" />
```

Note: If you are using SQL Server 2008 Express (which comes with the older release of FileWay) then run **FileWay_Database_Upgrade_Setup**, which is part of the upgrade package, to upgrade your database to SQL Server 2008 R2 SP3 and run patch KB4057113 to support TLS 1.2. If you do not need TLS 1.2 support, you can upgrade FileWay only by running **FileWay Setup**.

If you are running a version of SQL server that is older than 2008 Express then please upgrade it manually to a newer version.

For all other SQL servers, please refer to the following link for patches and updates to support TLS 1.2
<<https://support.microsoft.com/en-ca/help/3135244/tls-1-2-support-for-microsoft-sql-server>>



4.6 Creating a FileWay Worker Account

The network administrator installing FileWay will need to create a user account in Active Directory for use by FileWay (FrontEnd and BackEnd). This account will not need access to anything on the existing network; it only needs to be a Domain User account.

The account can be named anything, for example, FileWay Worker. This user account will be referred to as the **FileWay Worker** account from here on.

4.7 General Installation Requirements

In order to install FileWay, you must log into your server as a Domain Administrator (or as a Domain User with administrative rights) to the server where you want to install FileWay.



5 Installing FileWay

There are two basic approaches to installing FileWay. How you choose to install the components depends on your network environment and preferences.

- Install all components on the same server (known as installing the Single-Host solution). All FileWay components (as per your registration key) will be installed on the current server.
- Install components on separate servers. The BackEnd Server must always be installed first.

FileWay components should be installed in the following order:

- FileWay BackEnd
- FileWay FrontEnd
- FileWay Drive
- SecureView BackEnd (legacy optional)
- OWA integration (optional)
- SharePoint integration (optional)

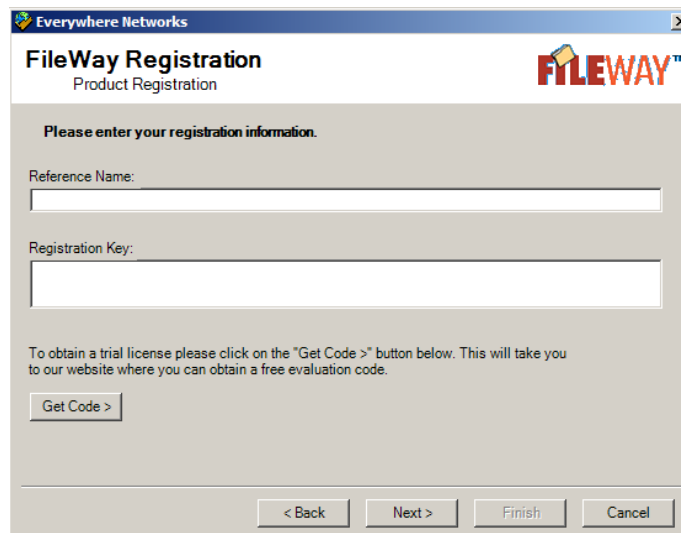
The FrontEnd server is the component that the user connects to through the web. Some Administrators prefer to have this component on a server separate from the FileWay BackEnd server.

FileWay Drive must be installed in the same Domain as the FileWay BackEnd server.

The procedure for installing FileWay components on separate servers is similar to installing on a single server. The only difference is that when you run the installer, you explicitly specify the component you want to install on a given server. You will need to copy the installation files to each server on which you want to install a component.

Begin the installation as follows:

1. Run the **FileWay vX.X.X Setup.exe**. (Note that the name of the Setup.exe changes with version numbers – e.g. FileWay v5.2.0 Setup.exe.) The following dialog appears.



The image shows a screenshot of the 'FileWay Registration' dialog box. The title bar says 'Everywhere Networks'. The main title is 'FileWay Registration' with 'Product Registration' below it. The FileWay logo is in the top right. The text 'Please enter your registration information.' is centered. There are two text input fields: 'Reference Name:' and 'Registration Key:'. Below these is a note: 'To obtain a trial license please click on the "Get Code >" button below. This will take you to our website where you can obtain a free evaluation code.' There is a button labeled 'Get Code >'. At the bottom are four buttons: '< Back', 'Next >', 'Finish', and 'Cancel'.

2. Type the registration details that you have obtained from Everywhere Networks in the **Reference Name** and **Registration Key** text boxes.



If you do not have a registration key and would like to evaluate FileWay, you can obtain a trial license by clicking **Get Code**. When you upgrade your trial license to a full license, you will not need to reinstall the software. You will be given a new license key along with instructions on how to install the new key.

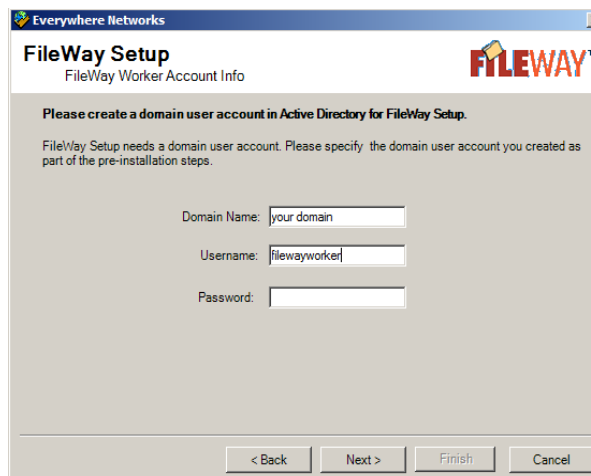
3. Click **Next**. The following dialog appears.



4. To install all FileWay components on the same server, click the **Single-Host: FrontEnd, BackEnd and FileWay Drive** button.

To install FileWay on separate servers, FileWay BackEnd must be installed before any of the other FileWay components; click **FileWay BackEnd**.

5. Click **Next**. The following dialog appears.

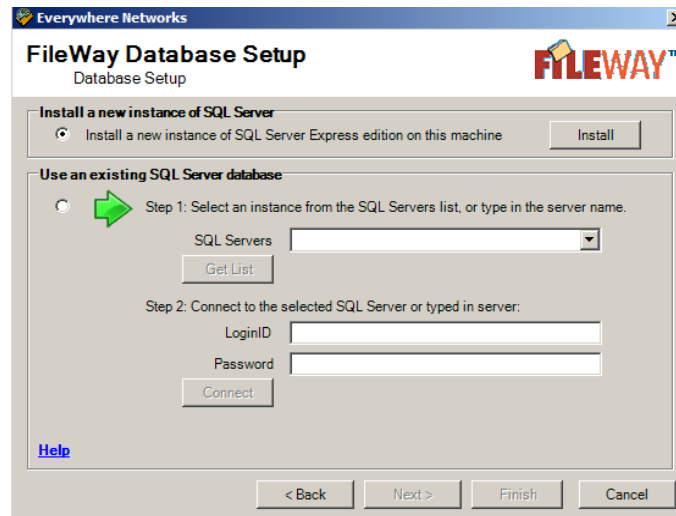


6. Type the domain name, and the user name and password you created in Section 4.6 Creating a FileWay Worker Account.
7. Click **Next**. The **FileWay Database Setup** dialog appears. Continue the installation procedure in Section 5.1.



5.1 Database Installation

This procedure applies if you are installing all FileWay Components on the same server or if you are installing FileWay BackEnd. The **FileWay Database Setup** dialog should currently appear on your screen.



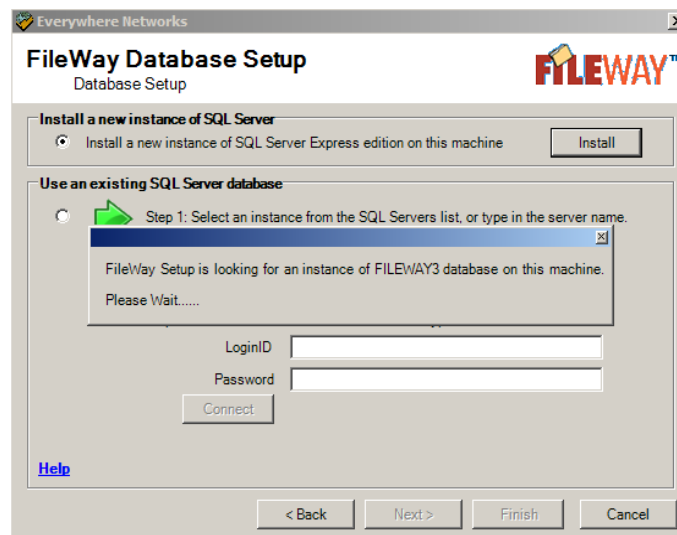
FileWay requires a SQL Server Login and thus requires the SQL Server Instance that it uses to be configured with Mixed Mode Authentication turned on. Database authentication with a Domain account will not work. The SQL Account you use should have Create Database permissions at a minimum. In addition, the SQL Server Instance should be configured to allow Remote Access and allow TCP/IP connections.

If your existing SQL Server Instances are not configured as described above, please consider allowing the FileWay Installer to install an new Instance of SQL Server Express Edition for FileWay use.

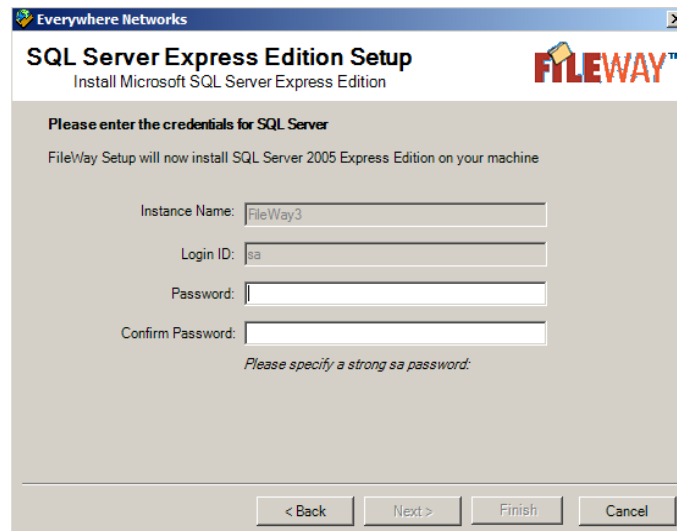
A - New SQL Server Installation

1. If you do not have any existing SQL Servers, click **Install a new instance of SQL Server Express edition on this machine** and then click **Install**.

FileWay Setup will try to detect any pre-existing instance of **FILEWAY3**. This can take some time. Refer to the figure below.



If the installer does not find an instance of the FILEWAY3 database, the following dialog appears.



2. Type an 'sa' password for SQL Server. The credentials will be saved in the BackEnd **web.config** file in the application settings section.

```
<appSettings>
```

```
...
```

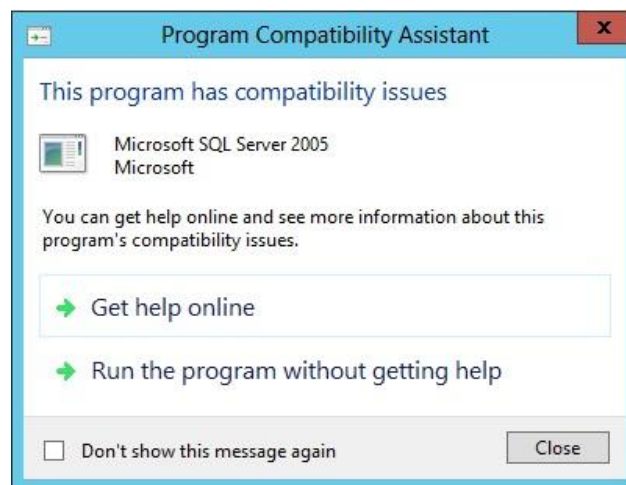
```
<add key="ConnectionString2" value="your connection string"/>
```

It is possible to create a new SQL Server login and use it instead if you don't want to expose the 'sa' credentials in the **web.config** file.

Also, note that SQL Server's default out-of-the-box memory limit is set to a very high value of 2147483647 MB. This maximum limit can be changed to a lesser amount to accommodate your requirements.

3. Continue the installation procedure in Section 5.2.

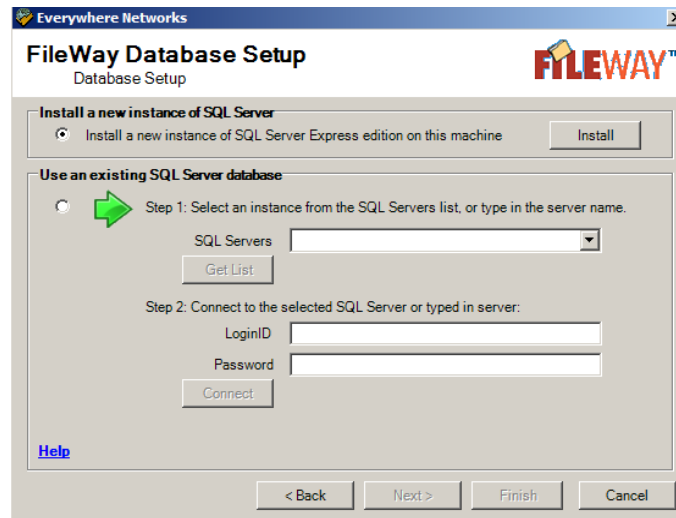
Note: For Windows 2012, following dialog might appear:



If this dialog appears, click **Run the program without getting help**.



B - Existing SQL Server

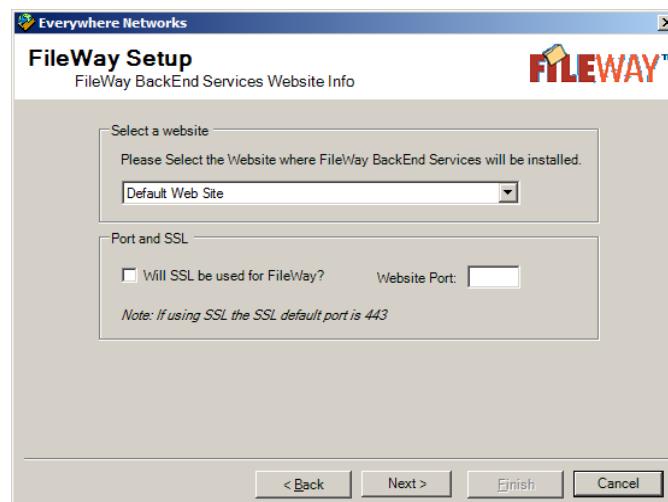


1. If you have an existing database instance that you would like to use, type the name of the database instance in the **SQL Servers** text box. Alternatively, click **Get List** to search for databases on your network. Setup will display the databases in the SQL Servers text box. If there is more than one database, you can view them using the SQL Servers pull-down menu.
2. Then type the SQL Server credentials and click **Connect**; then click **Next**.
3. Continue the installation procedure in Section 5.2.

5.2 FileWay BackEnd Installation

If you are in the process of installing all FileWay Components on the same server, the FileWay BackEnd installer will begin automatically and the **FileWay BackEnd Services Website Info** dialog should appear on your screen (see figure below).

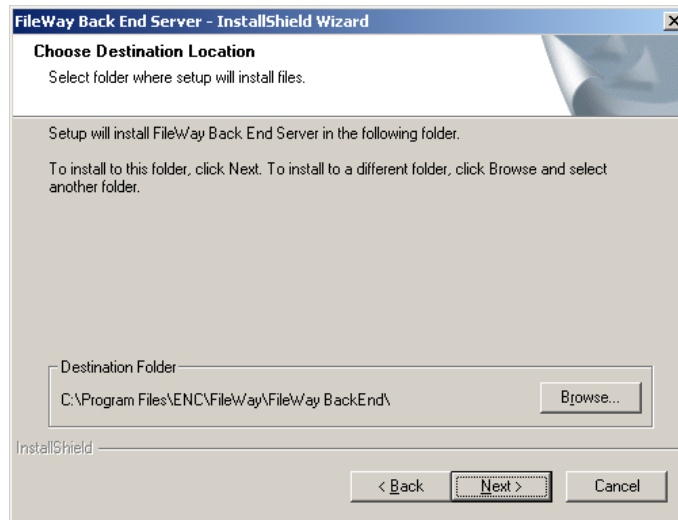
If you want to install FileWay BackEnd on its own server, run the installer on the relevant server. The installation will begin with the **FileWay Database Setup** dialog; refer to Section 5.1 Database Installation. Once the database setup is complete, the BackEnd installer will start automatically.



The **FileWay BackEnd Services Website Info** dialog lists the websites found in IIS.



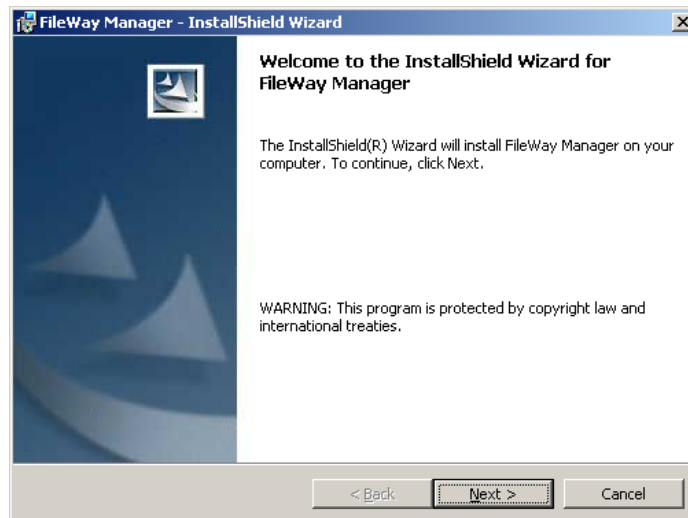
1. Click the website under which you want to install FileWay BackEnd and click **Next**. The following dialog appears.



2. To install in the default location, click **Next**.
To install in a different location, click **Browse**.
3. Continue the installation procedure in Section 5.2.1.

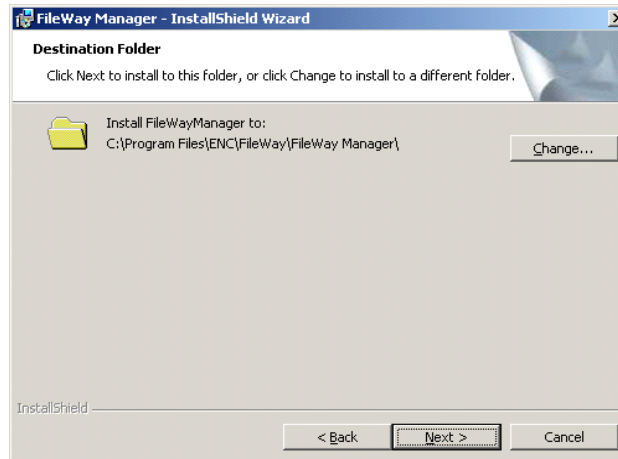
5.2.1 FileWay Manager Installation

This procedure applies if you are installing all FileWay Components on the same server or if you are installing FileWay BackEnd. The **FileWay Manager InstallShield Wizard** should currently appear on your screen (see figure below).



1. Click **Next**. The following dialog appears.





2. To install in the default location, click **Next**. The installation begins and FileWay Manager is installed.

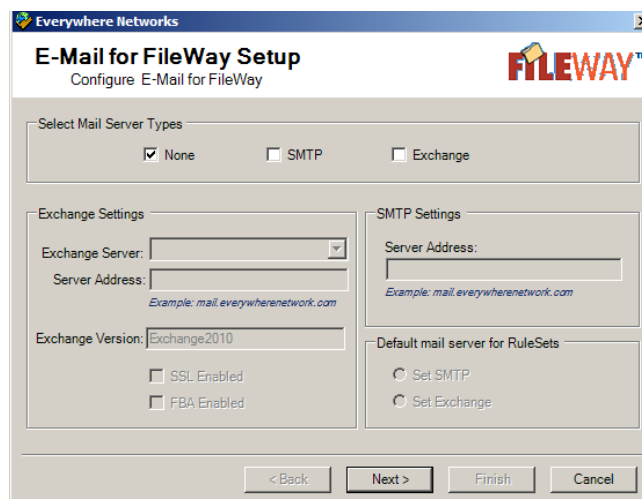
To install in a different location, click **Change**.

3. Continue the installation procedure in Section 5.2.2.

5.2.2 Mail Server Setup

This procedure applies if you are installing all FileWay Components on the same server or if you are installing FileWay BackEnd. The **E-Mail for FileWay Setup** dialog should currently appear on your screen (see figure below).

FileWay Setup is configuring FileWay to allow end-users to send files as email attachments within FileWay. Those settings will provide means for email functionality within FileWay for all the users in that particular Ruleset. This means that you can have different Rulesets pointing to different mail server settings. For more on information on Mail Server Settings refer to Section 14.2 Specifying Global Settings for FileWay.



Complete the email server information and click **Next**.

If you are installing all FileWay Components on the same server, continue the installation procedure in Section 5.3.

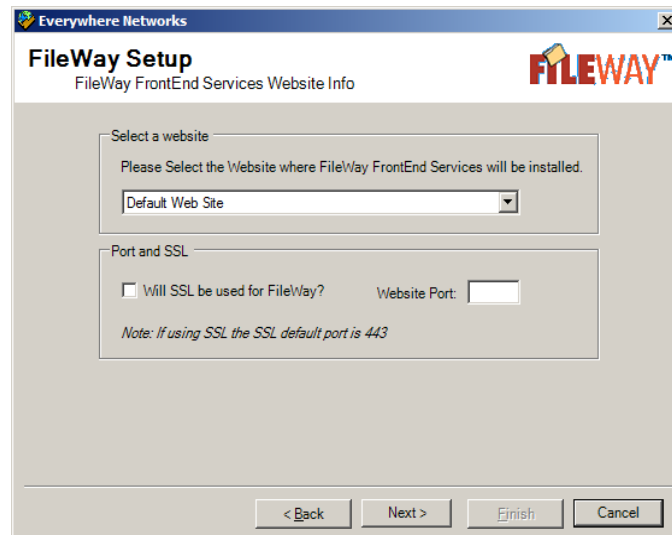
If you are installing FileWay BackEnd on its own server, the installation process is complete.



5.3 FileWay FrontEnd Installation

If you are in the process of installing all FileWay Components on the same server, the FileWay FrontEnd installer will begin automatically and the **FileWay FrontEnd Services Website Info** dialog should appear on your screen (see figure below).

If you want to install FileWay FrontEnd separately, run the installer on the relevant server. The installation will begin and the **FileWay FrontEnd Services Website Info** dialog should appear on your screen (see figure below).



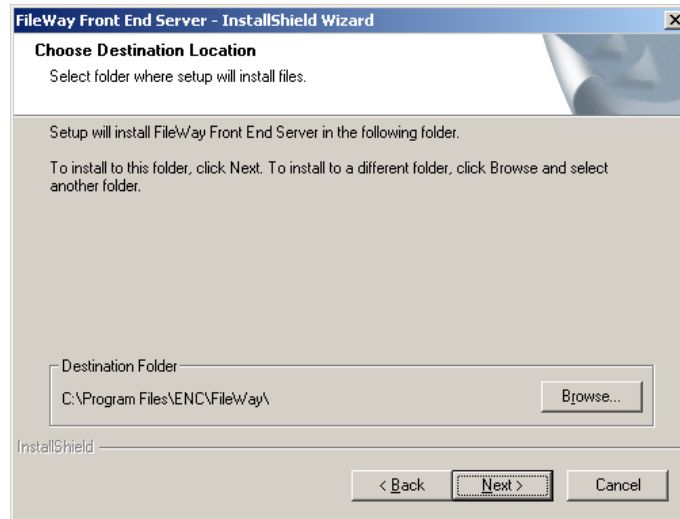
The **FileWay FrontEnd Services Website Info** dialog will list the websites found in IIS. Click the web site under which you would like to install FileWay FrontEnd. Then installation of FileWay FrontEnd Installer will start automatically.

If you would like to use FileWay FrontEnd with SSL to connect to the BackEnd Web Services, select the **Will SSL be used for FileWay** check box (see figure above). These settings are stored in the FrontEnd **web.config** file under **ENC.FileWay.FileWayFrontEnd.Properties.Settings**. If using SSL, FileWay Setup will replace **http** by **https** during the setup. For more information about SSL, refer to Section 6.3 Enabling SSL.

```
<ENC.FileWay.FileWayFrontEnd.Properties.Settings>
  <setting name="FileWay_FileWayBackEnd_DEWIO_DEWIO" serializeAs="String">
    <value>http://localhost/BackEnd/DEWIO.aspx</value>
  </setting>
  <setting name="FileWay_FileWayBackEnd_DBLayer_DBLayer" serializeAs="String">
    <value>http://localhost/BackEnd/DBLayer.aspx</value>
  </setting>
  <setting name="FileWay_FileWayBackEnd_WS_FWBEWS" serializeAs="String">
    <value>http://localhost/BackEnd/FWBEWS.aspx</value>
  </setting>
</ENC.FileWay.FileWayFrontEnd.Properties.Settings>
```

Click **Next**.





To install in the default location, click **Next**. The installation begins and FileWay FrontEnd is installed.

To install in a different location, click **Browse**.

If you are installing all FileWay Components on the same server, continue the installation procedure in Section 5.4.

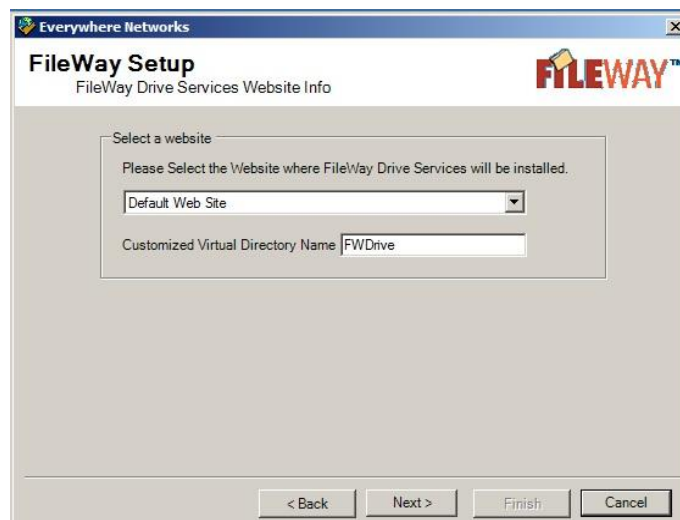
If you are installing FileWay Front End on its own server, the installation process is complete.

5.4 FileWay Drive Installation

If you are in the process of installing all FileWay Components on the same server, the FileWay Drive installer will begin automatically and the **FileWay Drive Services Website Info** dialog should appear on your screen (see figure below).

If you want to install FileWay Drive separately, run the installer on the relevant server. The installation will begin and the **FileWay Drive Services Website Info** dialog should appear on your screen (see figure below).

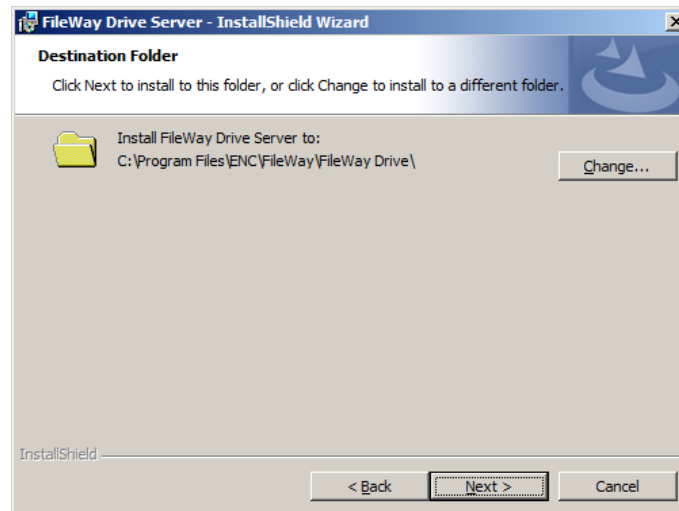
Existing customers upgrading their FileWay installation to v4 will require a new license key to enable FileWay Drive. Please contact our Support Team to obtain a new license key.



You can give a Customized Virtual Directory Name for your FileWay Drive. The default name is FWDrive.

Note: FileWay Drive is installed with Basic Authentication; therefore, if you want to use SSL, you will have to manually configure it using IIS Manager.

When you click **Next**, the following dialog appears.



To install in the default location, click **Next**. The installation begins and FileWay FrontEnd is installed.

To install in a different location, click **Change**.

If you are installing all FileWay Components on the same server, continue the installation procedure in Section 5.6.

If you are installing FileWay Drive on its own server, the installation process is complete.

5.5 SecureView Backend Installation (legacy)

If your license (registration key) allows you to install SecureView then you may install the SecureView BackEnd component with other FileWay components or on its own server. To install SecureView BackEnd on the same server with FileWay components, click **Next**. Otherwise, click **Cancel**.

If you click Next, Secure View Installer will start automatically. You can use an existing SecureView Backend or install a fresh version of it.

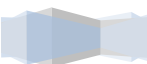
5.6 FileWay OWA Integration (optional)

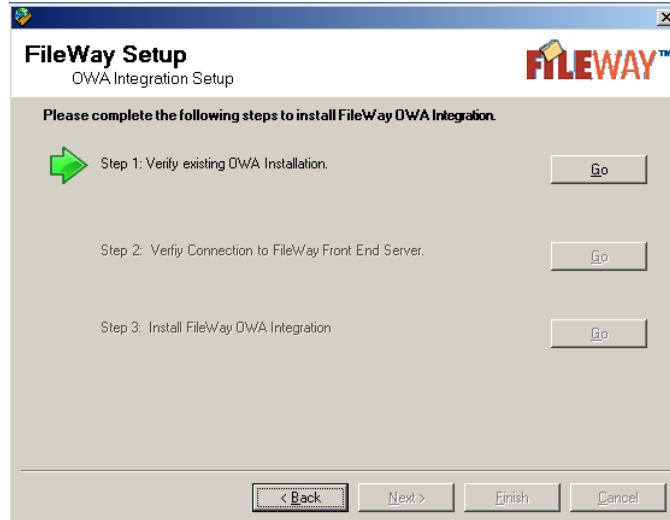
Note: This component may only be installed on the server hosting the Exchange Server.

If you are in the process of installing all FileWay Components on the same server (Exchange), the FileWay OWA Integration installer will begin automatically and the **OWA Integration Setup** dialog should appear on your screen (see figure below).

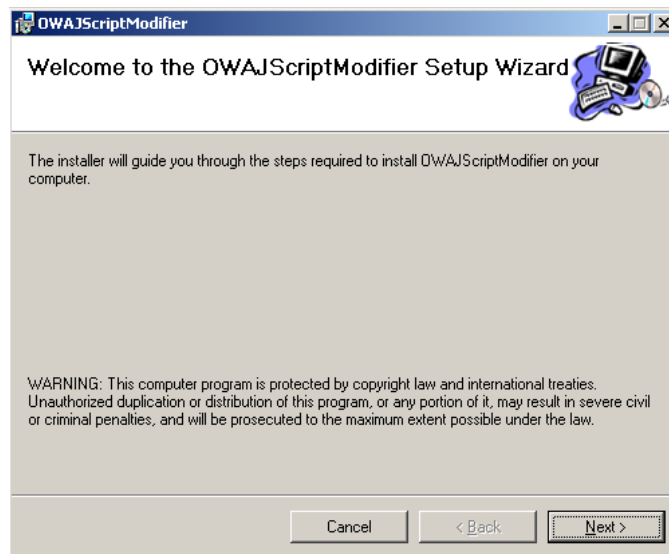
If you want to install FileWay OWA separately, run the installer on the Exchange Server. The installation will begin and the **OWA Integration Setup** dialog should appear on your screen (see figure below).

If your Exchange Configuration is Exchange Front End Proxy Server with Exchange Back End on different Server, you should run FileWay Setup and install FileWay OWA Integration on Exchange Back End Server.



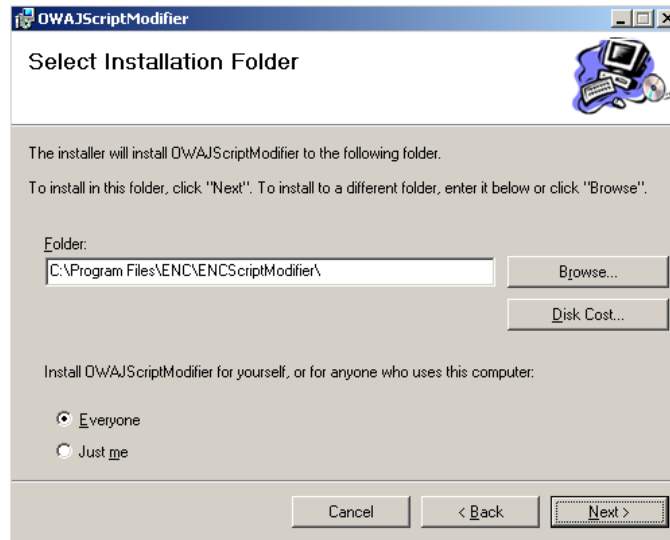


1. Click **Go** to verify the OWA installation.
2. When the verification is complete, click the second Go button to verify the connection to the FileWay FrontEnd server.
3. When the verification is complete, click the third Go button to Install FileWay OWA Integration. The following dialog appears.

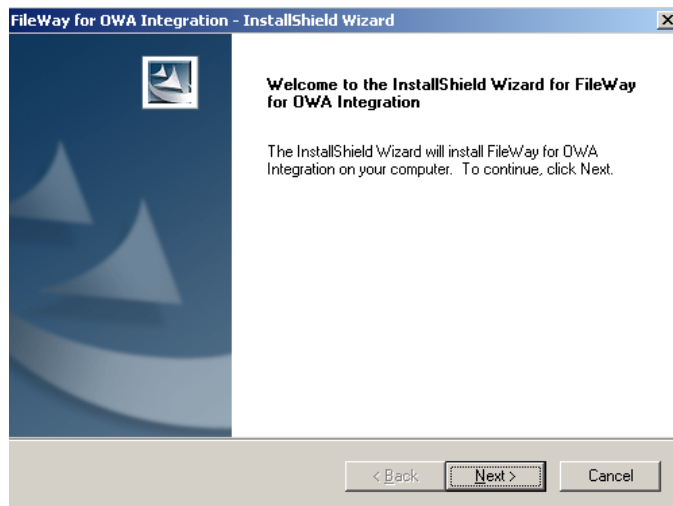


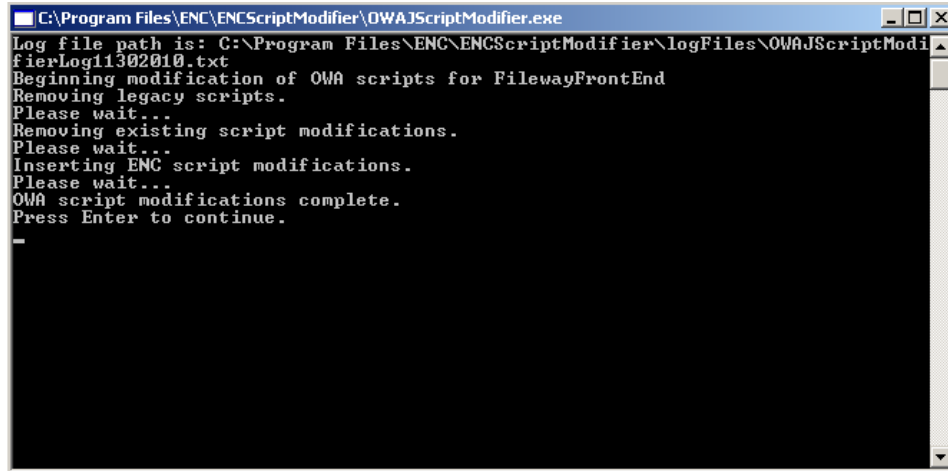
4. Click **Next**. The following dialog appears.





5. Choose whether to make the ENC Script Modifier available to all users or just the user currently logged on. The Script Modifier is used to reinstall FileWay OWA Integration code occasionally after Exchange patches and upgrades are applied to the server.
6. Click **Next**. The Script Modifier is now installed.
7. Click **Close** to continue the OWA Integration installation. FileWay OWA Integration Installer will start automatically (see figure below).





```

C:\Program Files\ENC\ENCScripModifier\OWAJScriptModifier.exe
Log file path is: C:\Program Files\ENC\ENCScripModifier\logFiles\OWAJScriptModi
fierLog11302010.txt
Beginning modification of OWA scripts for FileWayFrontEnd
Removing legacy scripts.
Please wait...
Removing existing script modifications.
Please wait...
Inserting ENC script modifications.
Please wait...
OWA script modifications complete.
Press Enter to continue.

```

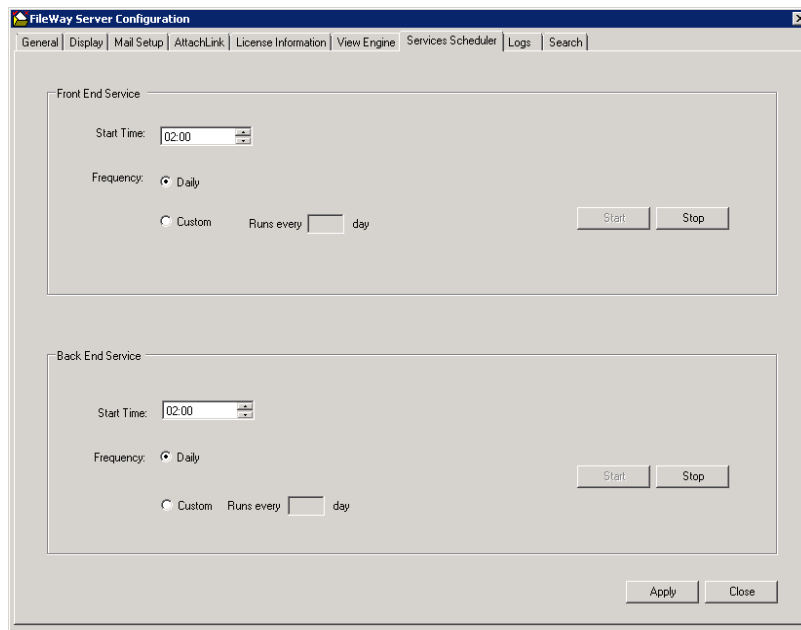
FileWay OWA Integration is now installed. To complete the installation follow the post installation steps in Section 6.2 to configure FileWay for integration with Exchange 2013 and 2016.

5.7 Windows Services

During the installation, FileWay Setup creates 2 Windows Services:

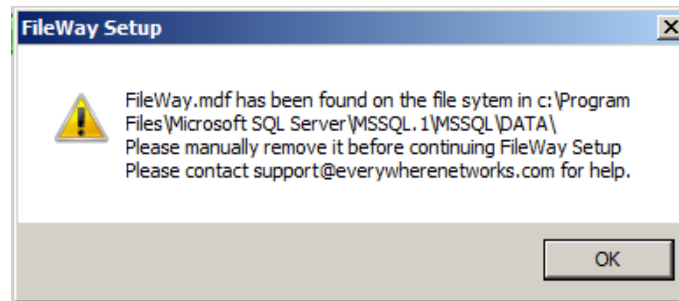
- FileWay BackEnd Services
- FileWay Services (Front End Service)

Each of those Services is required to clean old/unused data. You can modify the running frequency using the **FileWay Server Configuration** dialog (see figure below).



5.8 Troubleshooting Installation

During the database installation, if FileWay was previously installed on your machine, the following error may appear:



Simply navigate to the path described in the message (usually Program Files\Microsoft SQL Server\MSSQL\Data) and delete the **FileWay.mdf** and **FileWay_log.log** files. Then try re-installing FILEWAY3 database.



6 Post-Installation Configuration Steps

6.1 AttachLink Configuration

6.1.1 Number of Files That Appear in AttachLink Email

As per Section 3.5.1 **Sending Files as Links in Email Messages**, when a user sends files as links in an email, the recipient sees a list of files in the email body (see Section 3.5.2). The Administrator can configure the number of file names that appear in the email body as follows:

1. Navigate to C:\Program Files (x86)\ENC\FileWay\FileWay BackEnd\FileWayWS.
2. Open the **web.config** file and find the following key:

```
<add key="AttachLinkNumberOfAttachedFiles" value="3" />
```
3. Change the value to the number you want and save the file.

6.1.2 Maximum Login Attempts

When a user sends files as links in an email, the recipient must log in to access the files. (The Administrator can configure the maximum number of login attempts as follows:

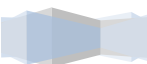
1. Navigate to C:\Program Files (x86)\ENC\FileWay\FileWay FrontEnd\FileWay.
2. Open the **web.config** file and find the following key:

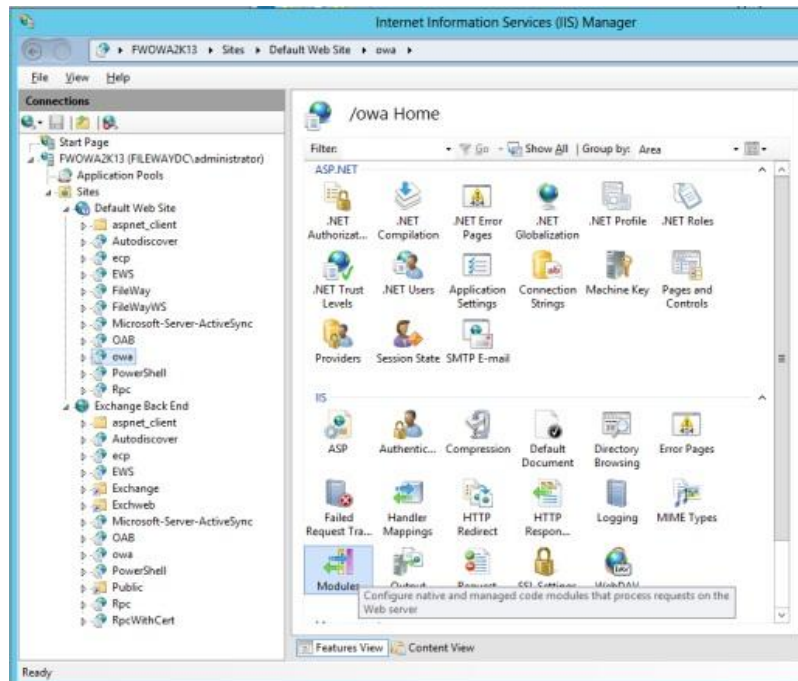
```
<add key="AttachLinkLoginAttemptsLimit" value="3" />
```
3. Change the value to the number you want and save the file.

6.2 FileWay Integration with Exchange 2013 and 2016

When integrating FileWay with Exchange 2013 or 2016 there are a few additional post configuration steps that must be followed in order for FileWay to work properly with Exchange 2013 and 2016.

1. Add the **ENCAuthModule** module in IIS in order to enable single sign on. This will allow users to click the FileWay button from within OWA and not be prompted for authentication again.
2. Browse to the folder **C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa** and create a folder named **bin** if it does not exist.
3. Copy the **ENCAuthModule.dll** file (default location: Program Files\ENC\FileWay\FileWay FrontEnd\ENCAuthModule\ENCAuthModule.dll) to the **bin** folder you created in the previous step, i.e., C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\bin.
4. Open IIS Manager and click **owa** under the website where Exchange Front End is located.





5. In the **Features** view, double-click **Modules**.
6. On the **Modules** page, in the **Actions** pane, click **Add Managed Module**.
7. In the **Add Managed Module** box, in the **Name** box, type a name for the managed module, e.g. ENCAuthenticationModule
8. In the **Type** box, type exactly the following text: ENCAuthModule.ENCAuthModule.
9. Click **OK**

Now users can click the FileWay button within OWA and not be prompted for user credentials before launching FileWay

6.3 Enabling SSL

FileWay FrontEnd, BackEnd and FileWay Drive support SSL. We recommend that FileWay FrontEnd, FileWay BackEnd and FileWay Drive installations that are externally accessible run under SSL.

To enable SSL on FileWay components, ensure that the website under which the applications are installed in IIS have SSL enabled (or bound in IIS) and that you have an SSL certificate installed in IIS. Then require SSL communication for the IIS application under the website. For FileWay FrontEnd, the application is named **FileWay** and for FileWay BackEnd, the application is named **FileWayWS**.

Note: When FileWay FrontEnd is installed on an OWA server for Exchange 2013 or 2016 in default configuration, SSL is already enabled on the OWA website.

If you have enabled SSL on the FileWay BackEnd, you have to alter the FileWay FrontEnd configuration as follows:

1. On the FileWay FrontEnd server, open the **web.config** file in the FileWay installation folder, that is, **\Program Files (x86)\ENC\FileWay\FileWay FrontEnd\FileWay \web.config**. Note that there are other **web.config** files in other locations in your FileWay installation path. Make sure you follow the path indicated above.



2. Find the following section in the file.

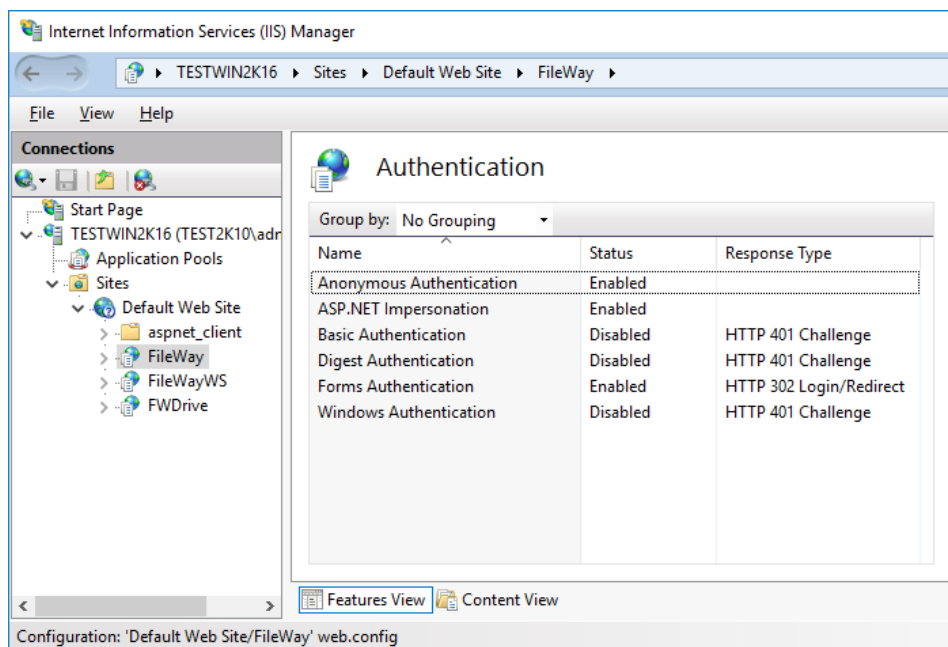
```
<applicationSettings>
<ENC.FileWay.FileWayFrontEnd.Properties.Settings>
  <setting name="FileWay_FileWayBackEnd_DEWIO_DEWIO" serializeAs="String">
    <value>https:// domain /FileWayWS/DEWIO.asmx</value>
  </setting>
  <setting name="FileWay_FileWayBackEnd_DBLayer_DBLayer" serializeAs="String">
    <value>https://domain/FileWayWS/DBLayer.asmx</value>
  </setting>
  <setting name="FileWay_FileWayBackEnd_WS_FWBEWS" serializeAs="String">
    <value>https:// domain /FileWayWS/FWBEWS.asmx</value>
  </setting>
</ENC.FileWay.FileWayFrontEnd.Properties.Settings>
</applicationSettings>
```

3. Change all occurrences of HTTP to HTTPS in the three URLs and save the changes and close the file.

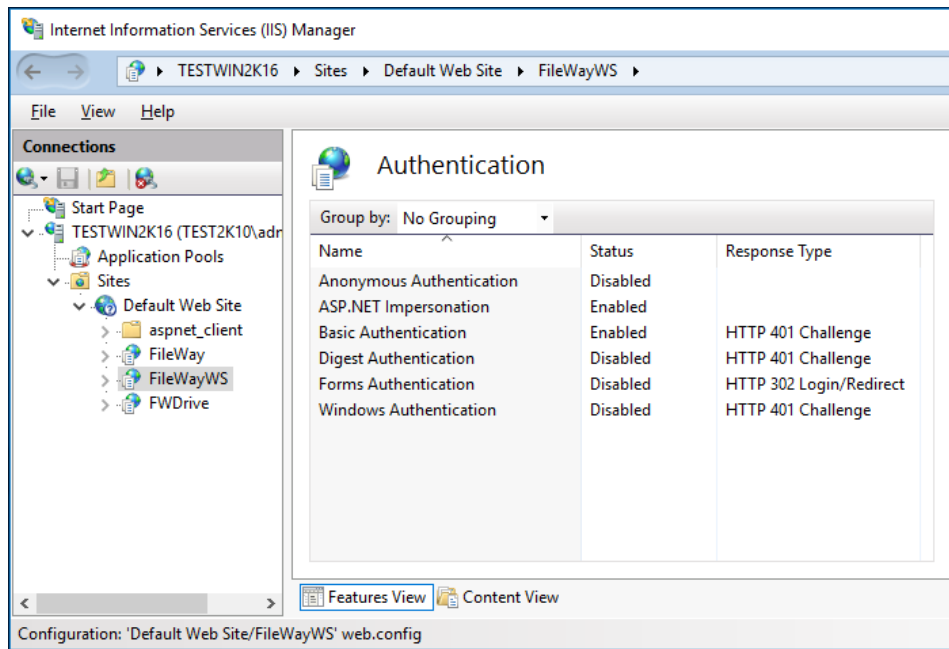
6.3.1 FileWay Authentication Settings

Using IIS Manager, verify that the settings appear as shown in the three figures below.

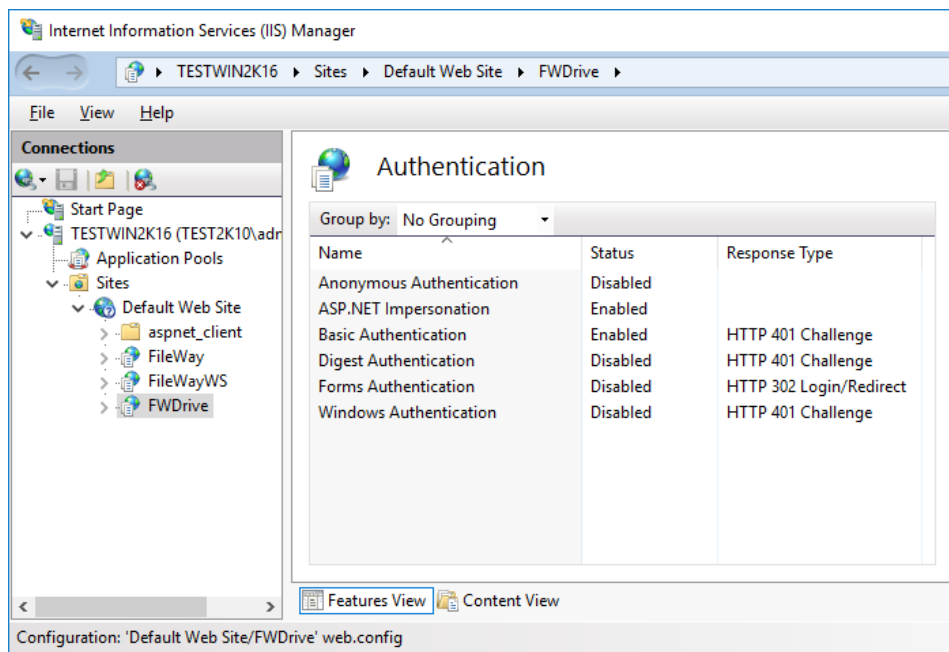
FileWay FrontEnd



FileWay BackEnd

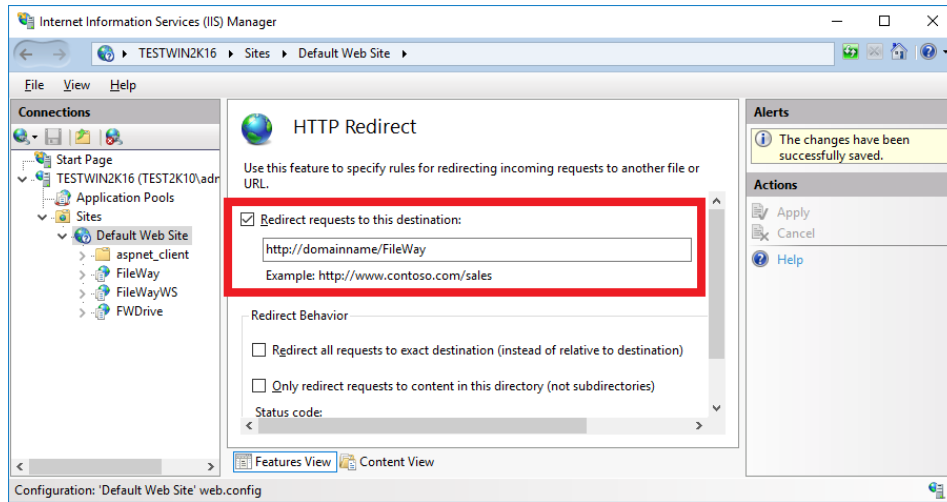


FileWay Drive

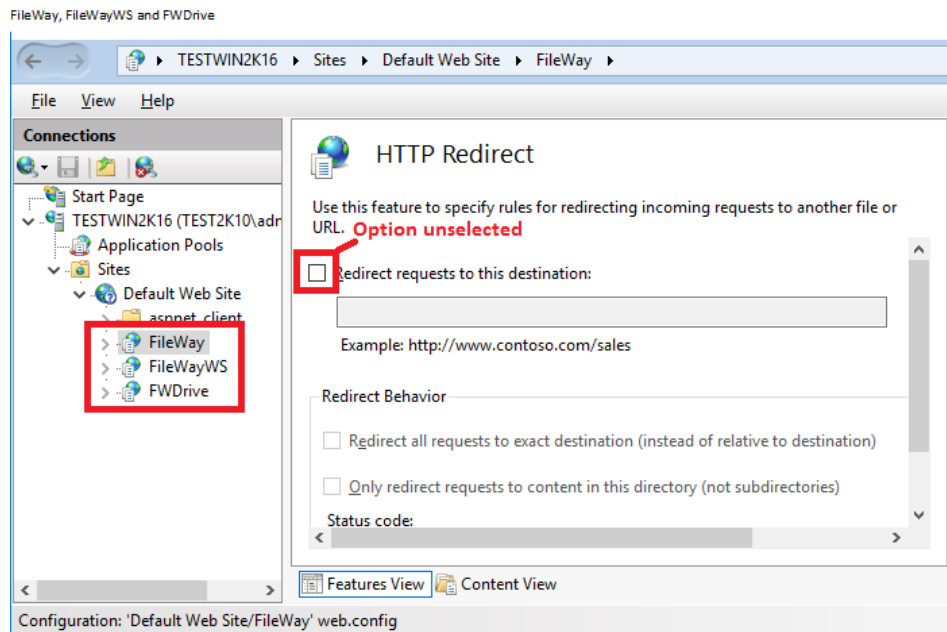


6.3.2 HTTP Redirect Setting

When you set HTTP Redirect at the Web Site Level, it applies to all the virtual directories under the web site (see figure below).

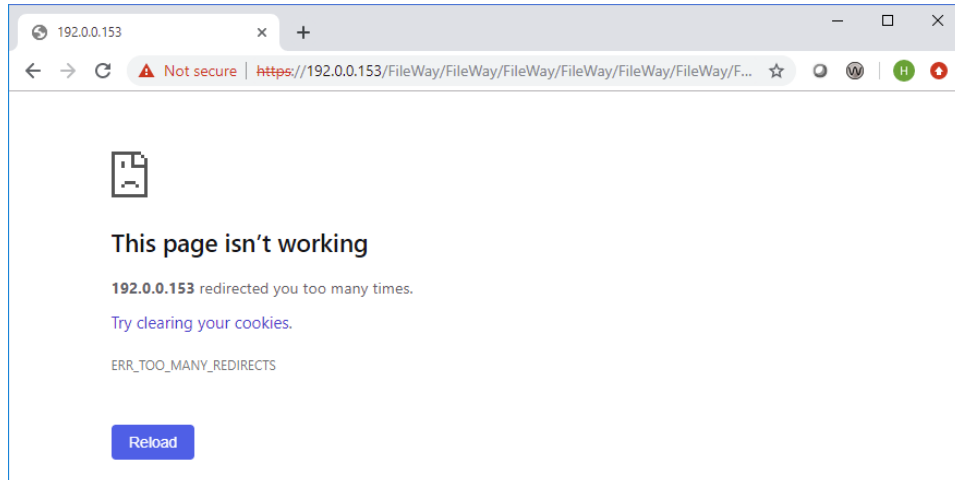


To avoid infinite HTTP Redirects, make sure that HTTP Redirect is not set for the FileWay, FileWayWS and FWDrive virtual directories (see figure below).



If the message shown below appears in the browser (Chrome in the following example), it is caused by an incorrect HTTP Redirect setting.

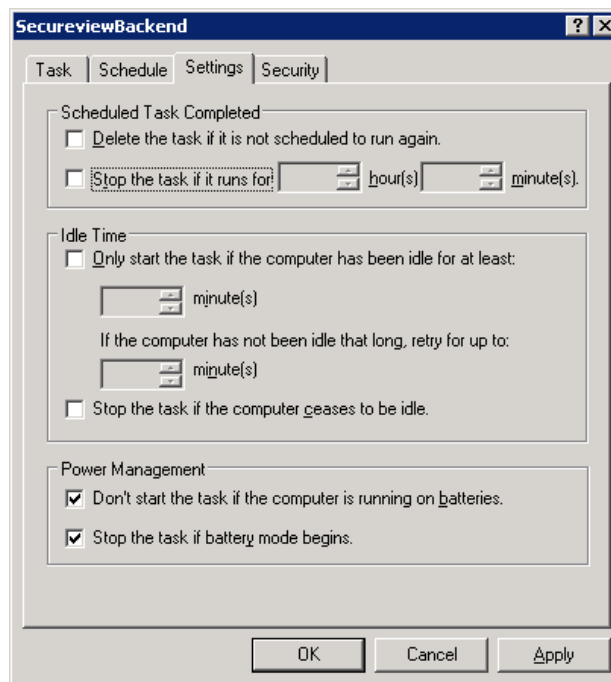




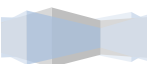
6.4 Configuring the SecureView BackEnd Scheduled Task

As part of the installation, if your license allows SecureView BackEnd, a scheduled task is automatically created to ensure that SecureView runs continuously. In this section, you will configure the scheduled task as follows:

1. Open Scheduled Tasks (Start->Control Panel->Scheduled Tasks), right-click **SecureView Backend** and click **Properties**.
2. In the **Settings** tab, ensure that the **Stop the task if it runs for** check box is not selected. If it is selected, clear it and then click **OK**.



value="Enter your login information"></add>



6.5 Support for DUO Two Factor Authentication

"Duo Security" is a cloud computing service that provides a second login step for additional security protection when accessing important systems and services, sensitive institutional data, and personal information. This function, called Two-Step Login, pairs something you know (Username & password) with something you have (an enrolled device) to complete a secure login.

Duo offers several options to verify that logins are legitimate:

- a mobile push notification with one-tap verification of identity on a smartphone (requires installation of the free Duo Mobile app)
- a one-time code generated in the Duo Mobile app on a smartphone (tap the green key symbol)
- a one-time code generated by Duo and sent to a cell phone or tablet via text message
- a telephone call to a landline phone that will prompt you to verify the login request



In practice, a user enters his/her username and password, and then selects the method to verify the login. If the user has multiple devices enrolled (recommended) the default device is always selected, but the user can change to another enrolled device for that login using the drop-down list. The user can choose a method (push-notification, text message, phone call, or a one-time code) that is supported by the device type to gain secure, verified access to an application.

To enable duo authentication in FileWay, you will need to uncomment following keys in **FileWay Frontend web.config** and provide values.

```

<add key="EnableDuoAuthentication" value="true" />
<add key="Duo_IKEY" value="" />
<add key="Duo_SKEY" value="" />
<add key="Duo_AKEY" value="" />
<add key="Duo_APIHostName" value="" />
  
```

DUO API provides these keys:

Duo_IKEY = Duo integration key value

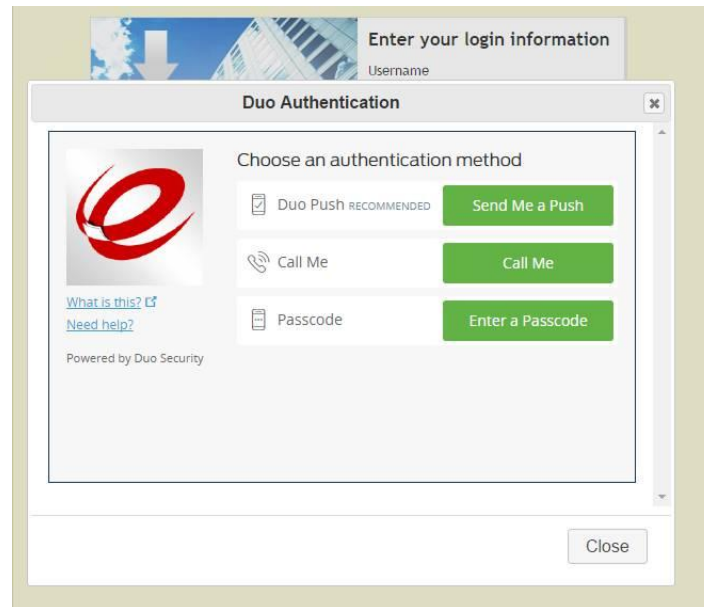
Duo_SKEY = Duo secret key

Duo_APIHostName = Duo API hostname

Duo_AKEY = Customers private key value.

After the users login in with their FileWay credentials, they will be presented with the following dialog.





7 FileWay and SharePoint Integration (optional)

This chapter describes the steps required to integrate FileWay with SharePoint 2007, 2010 and 2013.

7.1 Integrating FileWay with SharePoint 2007

This section describes the integration of FileWay with SharePoint 2007.

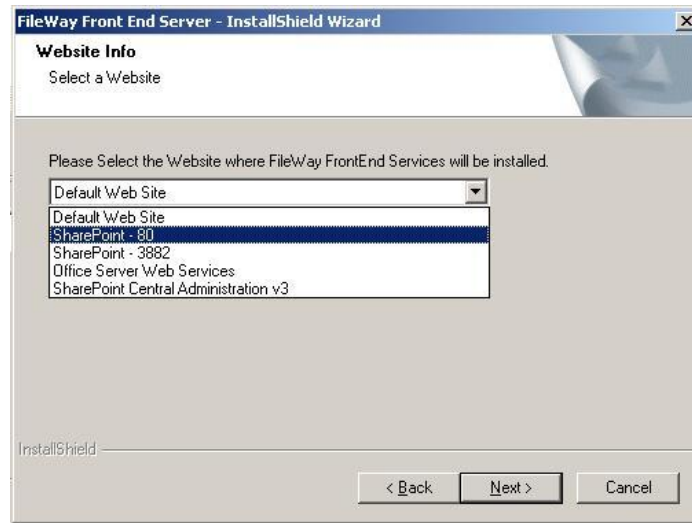
1. Install SharePoint and make sure the portal is fully functional.
2. Install and configure FileWay.
3. Configure IIS.
4. Configure SharePoint.
5. Create an access point from SharePoint to FileWay.

7.1.1 Installing FileWay

To install FileWay, refer to Section 5.

FileWay must be installed under the SharePoint Website. If choosing to install FileWay in a two server solution, the FileWay FrontEnd must be installed under the SharePoint website.





Once FileWay is installed, add the following text to both the FrontEnd and BackEnd **web.config** files. Add the text at the bottom of the file just above `</configuration>`.

```
<system.web>
  <trust level="Full" originUrl="" />
</system.web>
```

The FrontEnd **web.config** is located here:

```
C:\Program Files\ENC\FileWay\FileWay FrontEnd\FileWay\web.config
```

The BackEnd **web.config** is located here:

```
C: \Program Files\ENC\FileWay\FileWay BackEnd\FileWayWS\web.config
```

Do this for both FrontEnd and BackEnd **web.config** files.

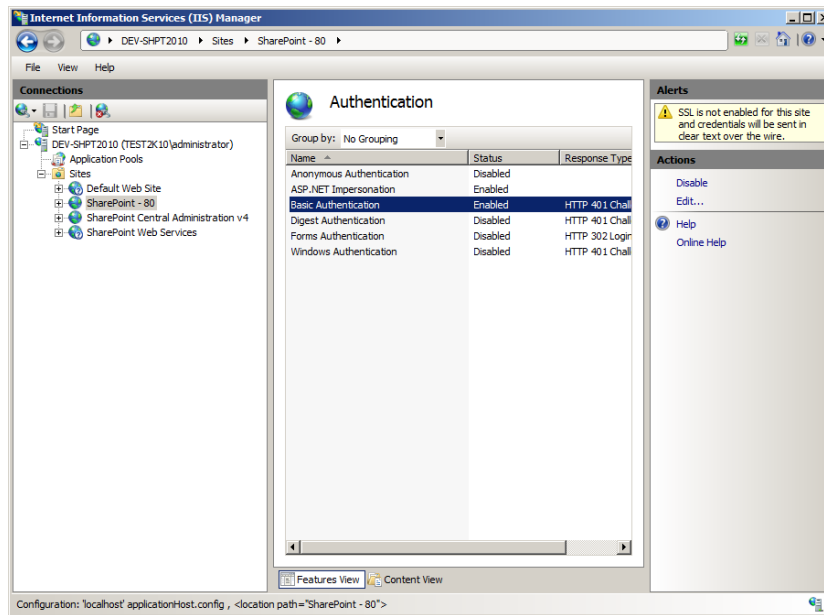
7.1.2 Configuring IIS

Once FileWay is installed, configure IIS.

By default, SharePoint configures IIS to use Windows authentication. FileWay requires IIS to use Basic Authentication. To configure IIS to use Basic Authentication, proceed as follows:

1. Open **IIS > ServerName (Local Computer) > Web Sites**.
2. Click the **SharePoint – 80** website and click **Authentication**.





3. Disable other authentications, and then enable **ASP .NET Impersonation** and **Basic Authentication**.
4. Restart the **SharePoint – 80** website.

7.1.3 Configuring SharePoint

1. Using Windows Explorer, browse to the **web.config** file for the SharePoint Website:

C:\Inetpub\wwwroot\wss\VirtualDirectories\80\web.config

2. Open this file in Notepad to edit it.
3. In this file, search for Trust level. You should find this tag:


```
<trust level="wss_minimal"/>
```
4. Edit this tag so that the trust level is WSS Medium instead of minimal as follows:


```
<trust level="WSS_Medium"
```
5. Save and close the file.
6. From a command prompt type iisreset to restart IIS.

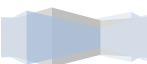
Now users will be able to log on to FileWay.

Note: If, at some point, you remove the portal, and add a new one, you will need to repeat the steps in this section.

7.1.4 Creating an Access Point from SharePoint to FileWay

There are two ways to add a link from SharePoint to FileWay:

- Creating a Hyperlink inside SharePoint
- Adding FileWay to SharePoint as a WebPart



7.1.5 Creating a Hyperlink inside SharePoint

After configuring SharePoint to allow requests to FileWay, create a hyperlink from SharePoint to FileWay as follows:

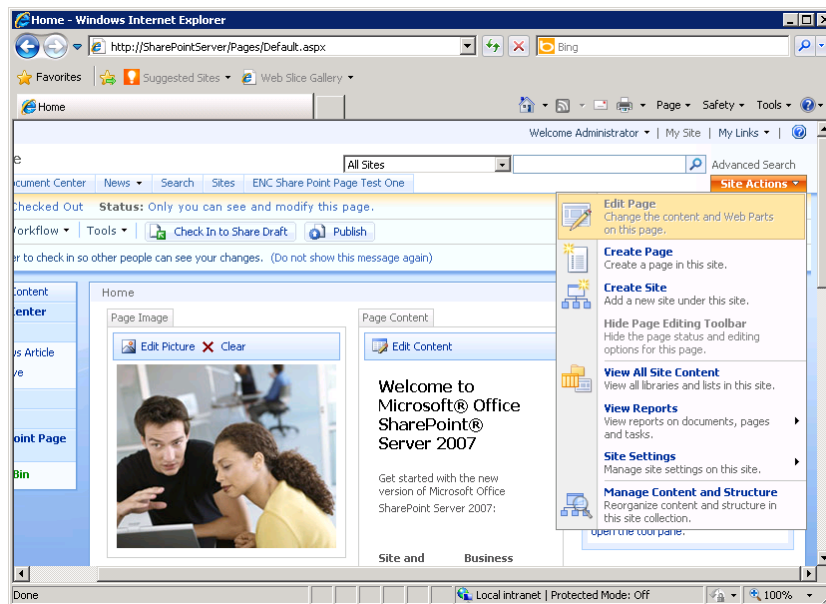
1. Log on to the SharePoint Portal <http://servername>.
2. Click **My Site**.
3. Under **my links summary – Add new link**.
4. Create a link to FileWay <http://servername/FileWay>.
5. Test the link. You should not be prompted for a username and password a second time.

7.1.6 Adding FileWay to SharePoint 2007 as a WebPart

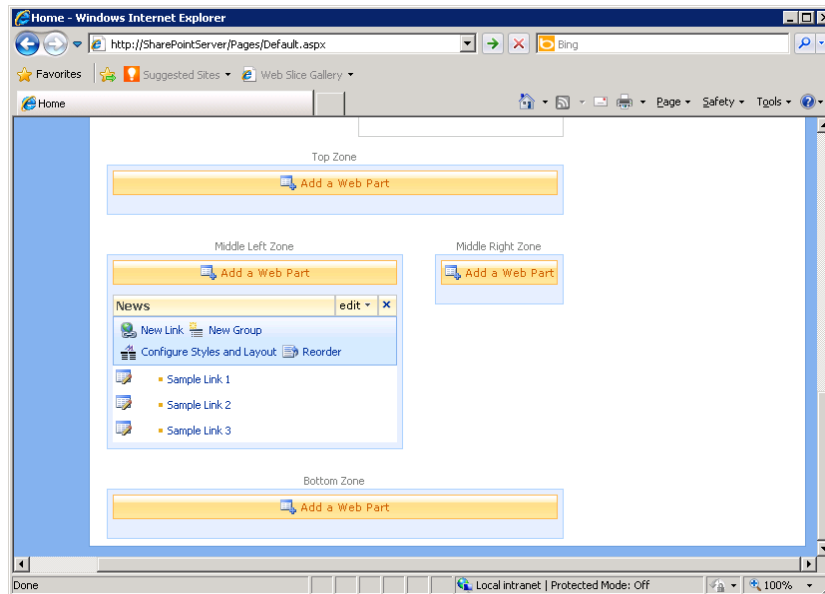
This section describes how to add FileWay to SharePoint as a WebPart. Before you can add FileWay to SharePoint as a WebPart, you must have single sign-on working above.

Proceed as follows:

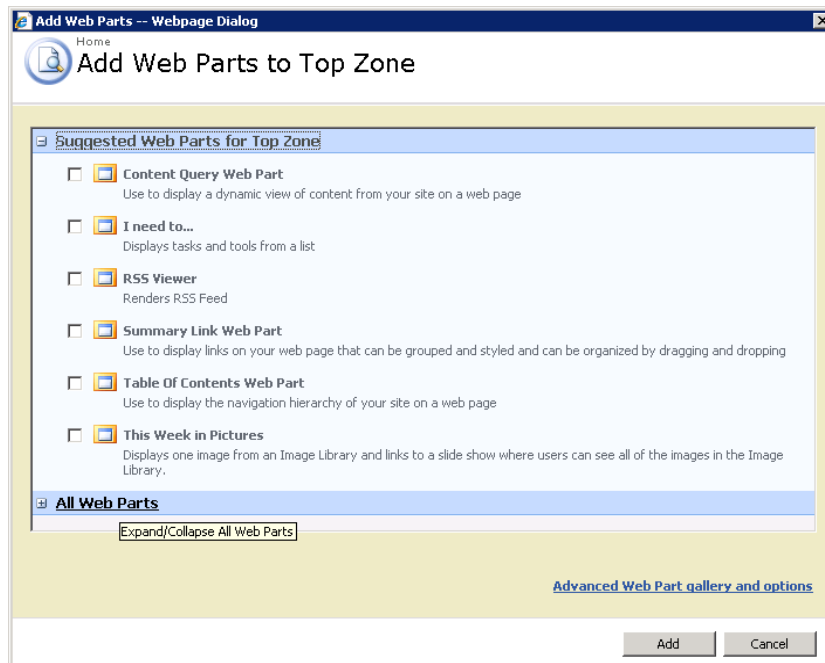
1. Log on to SharePoint as Administrator.
2. Add Page Viewer Web Part. The following window appears.



3. From Site Action, click **Edit Page**. The following window appears.

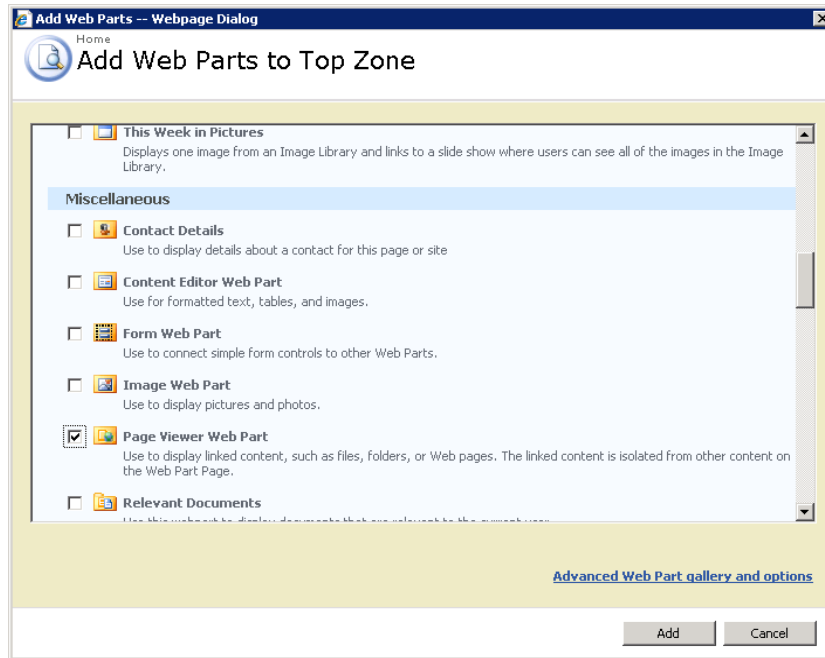


4. Click **Add a Web Part**. The following window appears.

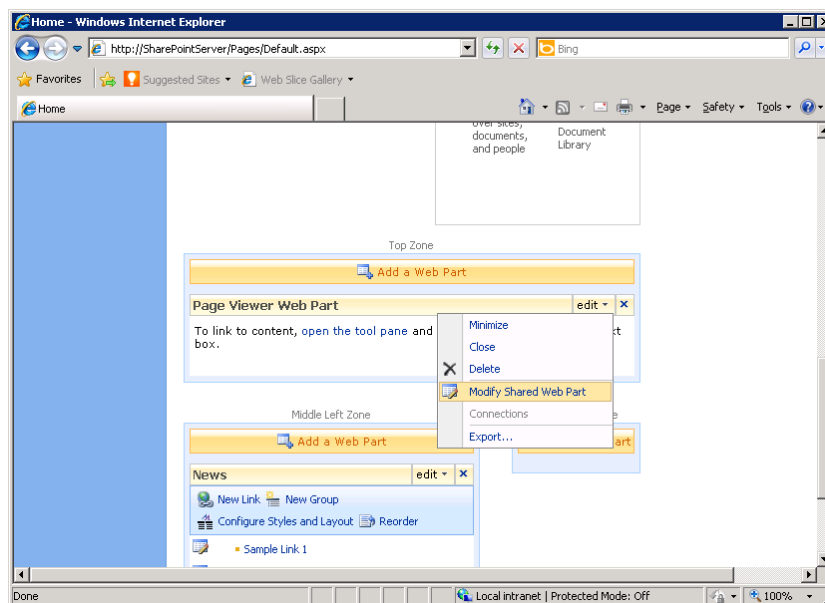


5. Click **All Web Parts** to expand it. The following window appears.



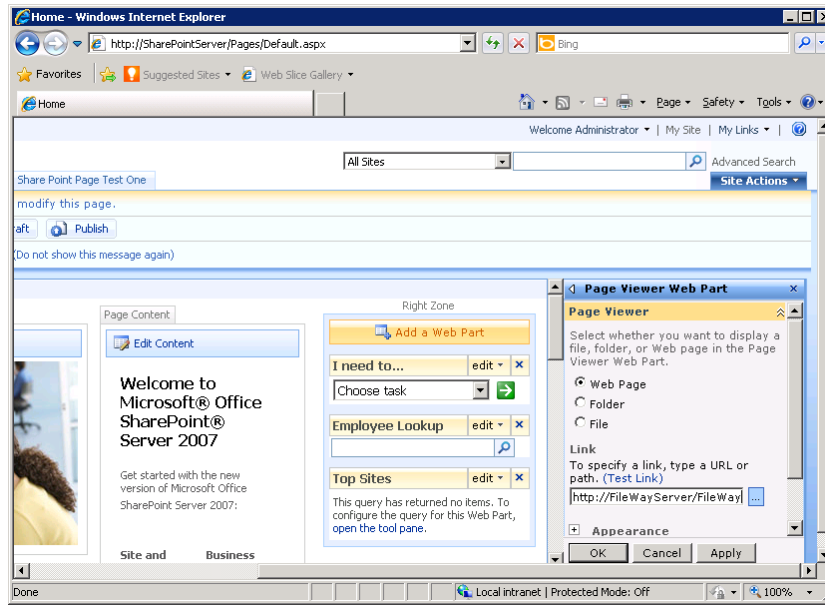


6. Select the **Page Viewer Web Part** check box and then click **Add** (you might need to scroll down to find Pager Viewer Web Part). The following window appears.

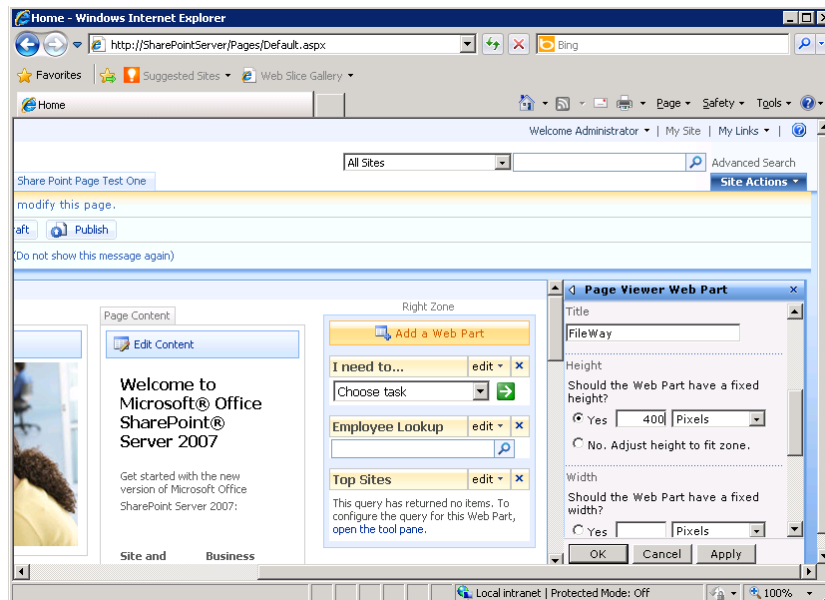


7. Click **edit** and then click **Modify Shared Web Part**. The following window appears.



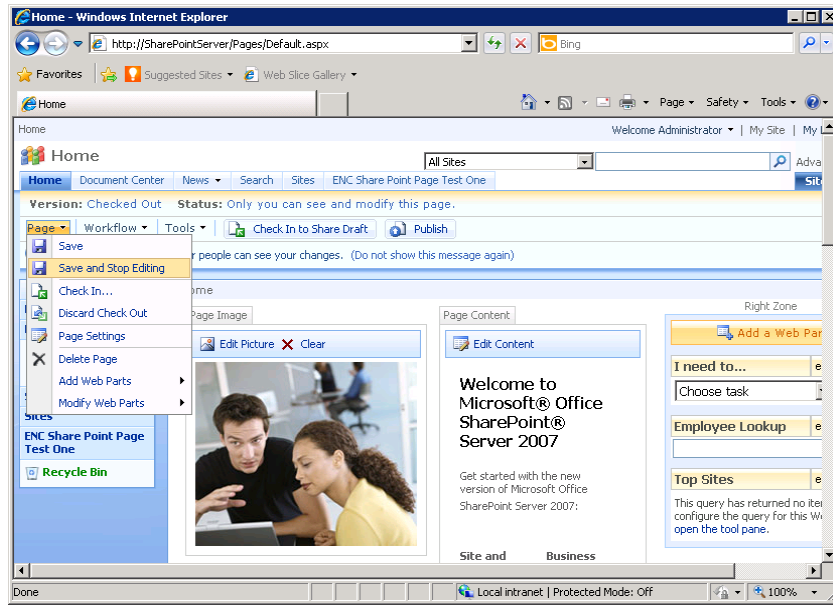


8. In the **Link** text box, type the FileWay URL, and then click **Appearance** to expand it. The following window appears.



9. Type the title in **Title** text box. Specify the height and width. Click **Apply**. FileWay appears in the web part. Adjust Height and Width to meet your requirements. Click **OK**. The following window appears.





10. Under **Page**, click **Save and Stop Editing**. FileWay appears in SharePoint.

7.2 Integrating FileWay with SharePoint 2010

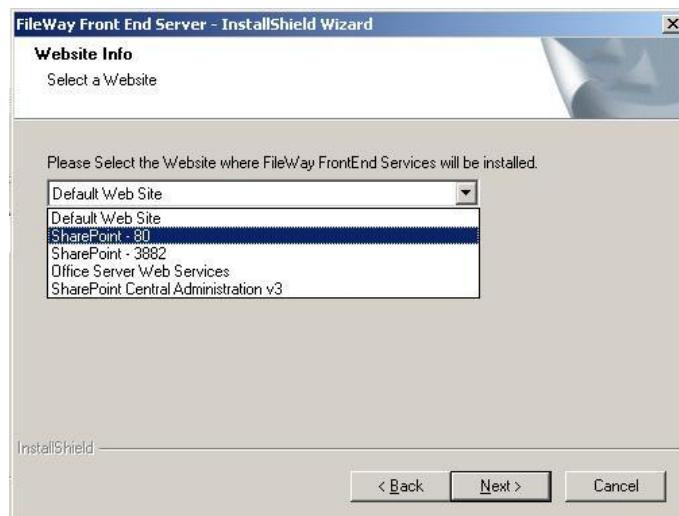
This section describes the integration of FileWay with SharePoint 2010.

1. Install SharePoint and make sure the portal is fully functional.
2. Install and configure FileWay.
3. Configure IIS.
4. Configure SharePoint
5. Create an access point from SharePoint to FileWay.

7.2.1 Installing FileWay

To install FileWay, refer to Section 5.

FileWay must be installed under the SharePoint Website. If choosing to install FileWay in a two server solution, the FileWay FrontEnd must be installed under the SharePoint website.



Once FileWay is installed, add the following text to both the FrontEnd and BackEnd **web.config** files. Add the text at the bottom of the file just above `</configuration>`.

```
<system.web>
  <trust level="Full" originUrl="" />
</system.web>
```

The FrontEnd **web.config** is located here:

```
C:\Program Files\ENC\FileWay\FileWay FrontEnd\FileWay\web.config
```

Or if it is 64 bit system,

```
C:\Program Files (x86)\ENC\FileWay\FileWay FrontEnd\FileWay\web.config
```

The BackEnd **web.config** is located here:

```
C:\Program Files\ENC\FileWay\FileWay BackEnd\FileWayWS\web.config
```

Or if it is 64 bit system,

```
C:\Program Files (x86)\ENC\FileWay\FileWay BackEnd\FileWayWS\web.config
```

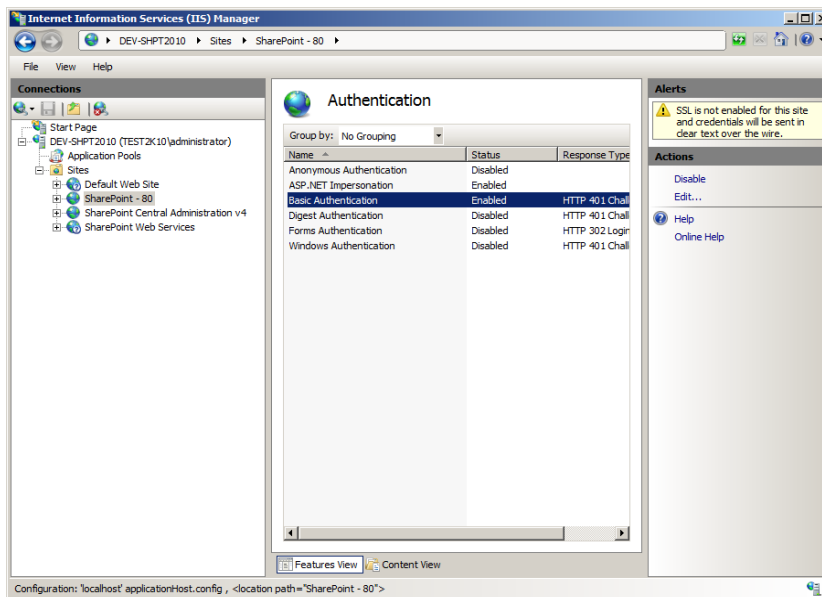
Do this for both FrontEnd and BackEnd **web.config** files.

7.2.2 Configuring IIS

Once FileWay is installed, configure IIS. By default, SharePoint configures IIS to use NTLM authentication. FileWay requires IIS to use Basic Authentication.

To configure IIS to use Basic Authentication, proceed as follows:

1. Open **IIS > ServerName(Local Computer) > Web Sites**.
2. Click the **SharePoint – 80** website and click **Authentication**.



3. Disable other authentications, then enable **ASP .NET Impersonation** and **Basic Authentication**.
4. Restart **SharePoint – 80** website.



7.2.3 Configuring SharePoint

To configure SharePoint 2010, proceed as follows:

1. Using Windows Explorer, browse to the **web.config** file for the SharePoint Website:

```
C:\Inetpub\wwwroot\wss\VirtualDirectories\80\web.config
```

2. Open this file in Notepad to edit it.
3. In this file, search for **Trust level**. You should find this tag:

```
<trust level="wss_minimal"/>
```

4. Edit this tag so that the trust level is WSS Medium instead of minimal as follows:

```
<trust level="WSS_Medium"
```

5. Save and close the file.
6. From a command prompt type iisreset to restart IIS.

Now users will be able to log on to FileWay.

7.2.4 Creating an Access Point from SharePoint to FileWay

There are two ways to add a link from SharePoint to FileWay:

- Creating a **Hyperlink** inside **SharePoint**
- Adding **FileWay** to **SharePoint** as **WebPart**

7.2.5 Creating a Hyperlink inside SharePoint

After configuring SharePoint to allow requests to FileWay, create a hyperlink from SharePoint to FileWay as follows:

1. Log on to the SharePoint Portal <http://servername>.
2. Click **Lists**.
3. Click **Links**.
4. Under the **links summary – Add new link**.
5. Create a link to FileWay as follows: <http://servername/FileWay>
6. Test the link. You should not be prompted for a username and password a second time.

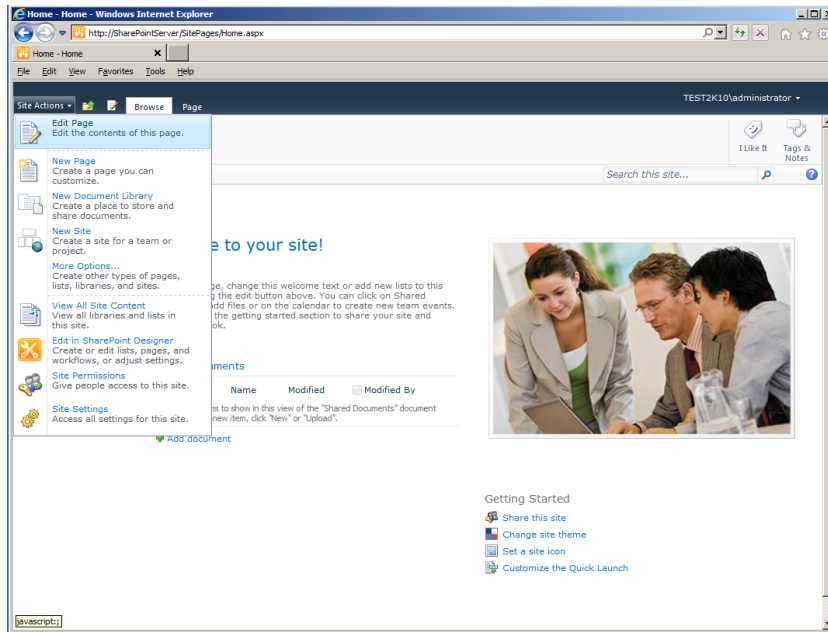
7.2.6 Adding FileWay to SharePoint 2010 as a WebPart

This section describes how to add FileWay to SharePoint as a WebPart.

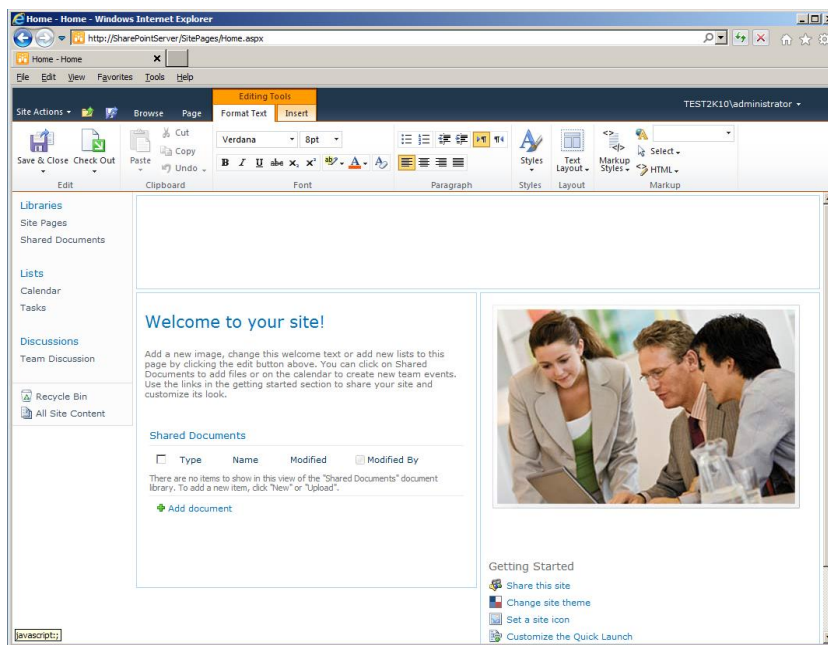
Proceed as follows:

1. Log on to SharePoint 2010 as Administrator.
2. Add Page Viewer Web Part. The following window appears.



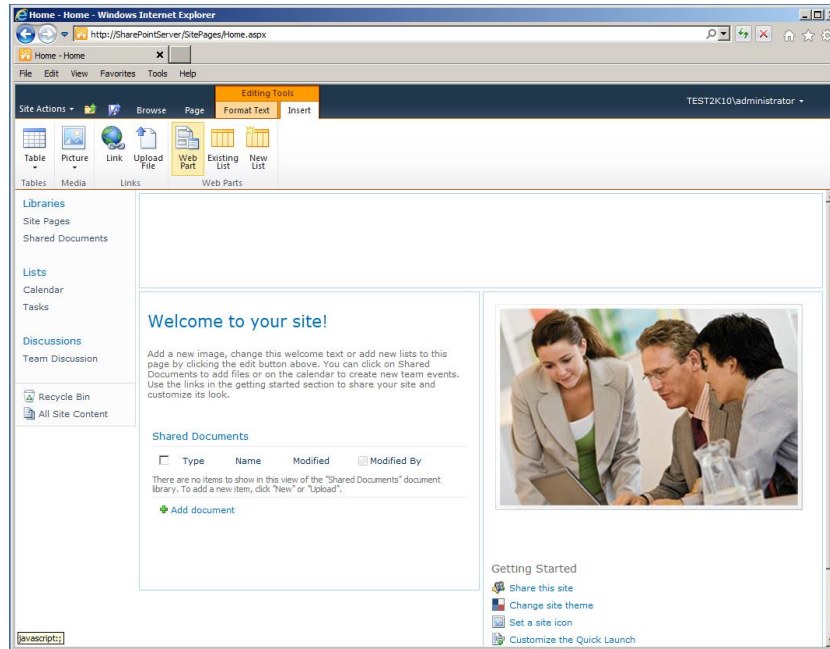


3. Under **Site Actions**, click **Edit Page**. The following page appears.

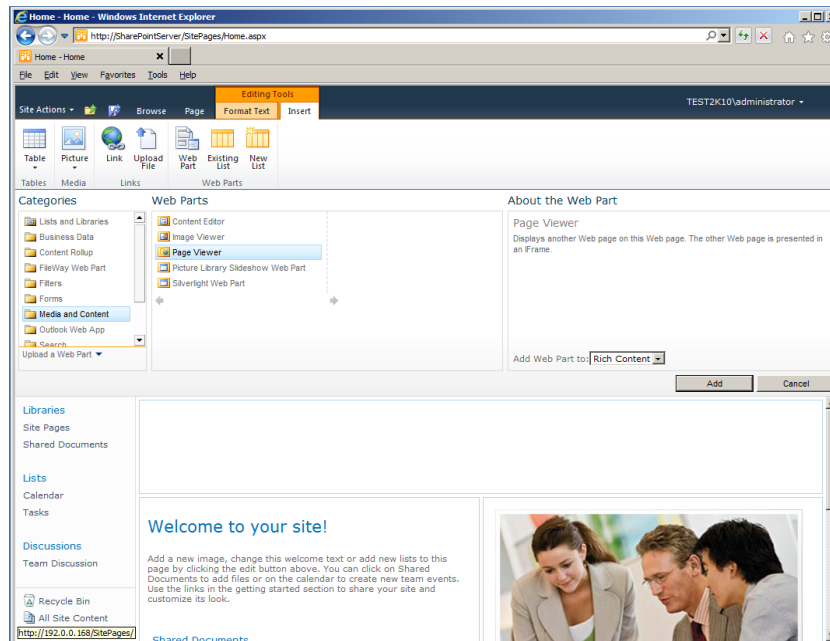


4. Click the **Insert** tab. The following window appears.



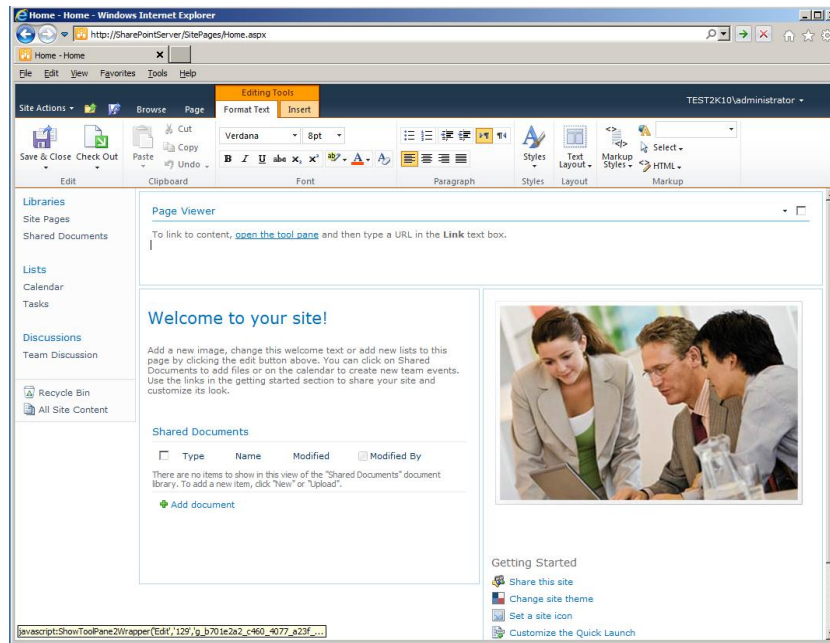


5. Click **Web Part**. The following window appears.

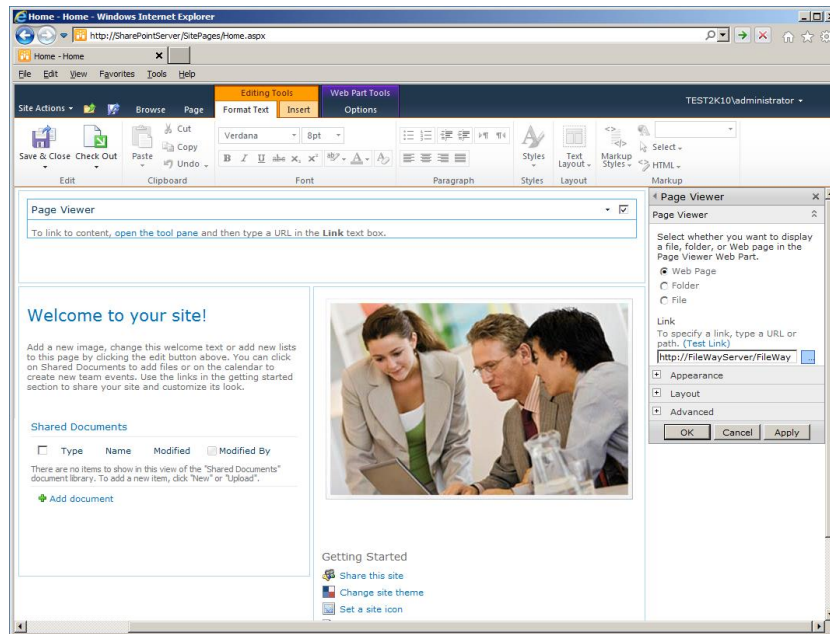


6. Under **Categories**, click **Media and Content**. Under **Web Parts**, click **Page Viewer**. Click the **Add** button. The following window appears.



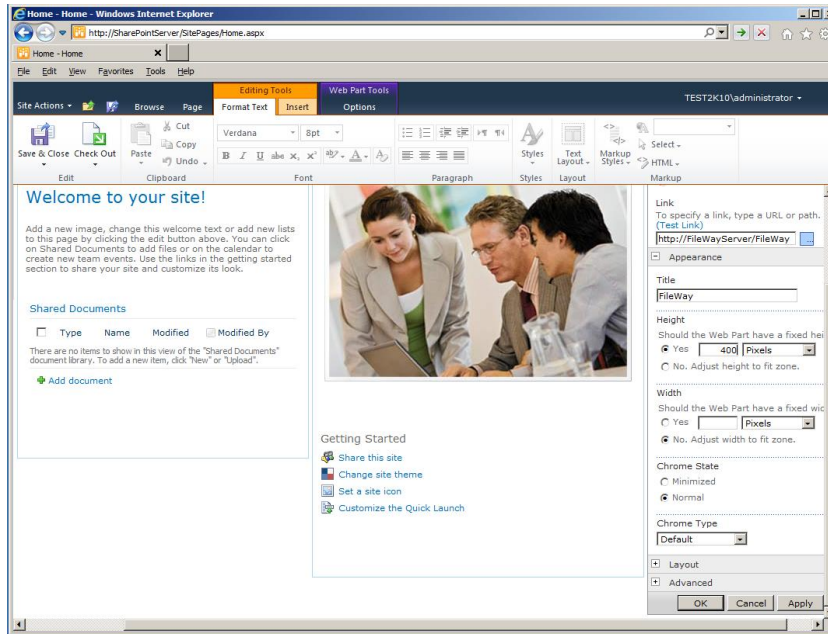


7. Under **Page Viewer**, click **open the tool panel**. The following window appears.

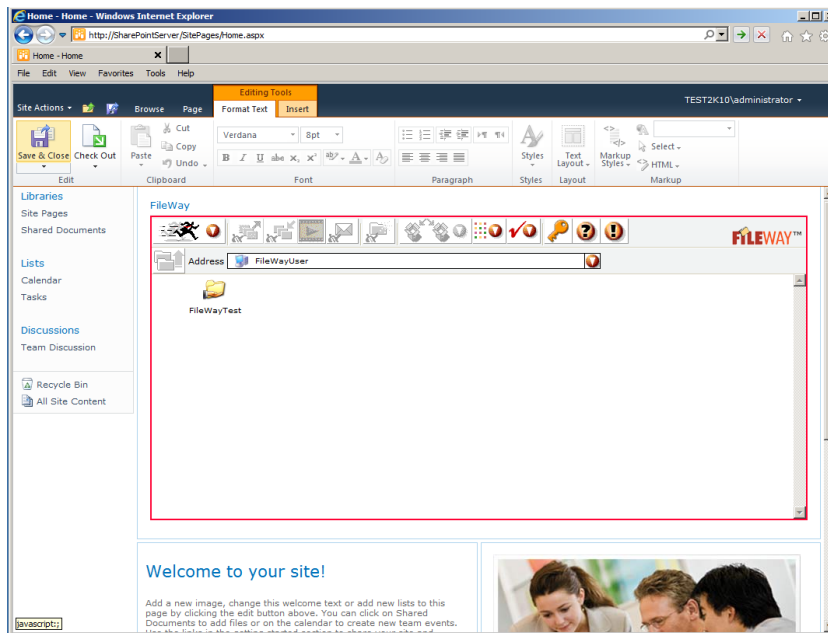


8. In the **Link** text box, type the FileWay URL and then expand **Appearance**. The following window appears.





9. In the **Title** text box, type the title. Type the height and width, and then click **Apply**. You will see FileWay in the web part. Adjust Height and Width to meet your requirements. Click **OK**. FileWay appears in the Page Viewer web part. The following window appears.



10. Click **Save & Close** to exit editing page. FileWay appears in the SharePoint window.



7.3 Integrating FileWay with SharePoint 2013

This section describes the integration of FileWay with SharePoint 2013.

1. Install SharePoint and make sure the portal is fully functional.
2. Install and configure FileWay.
3. Install Authentication Module.
4. Add FileWay to SharePoint 2013 as WebPart.

7.3.1 Installing FileWay

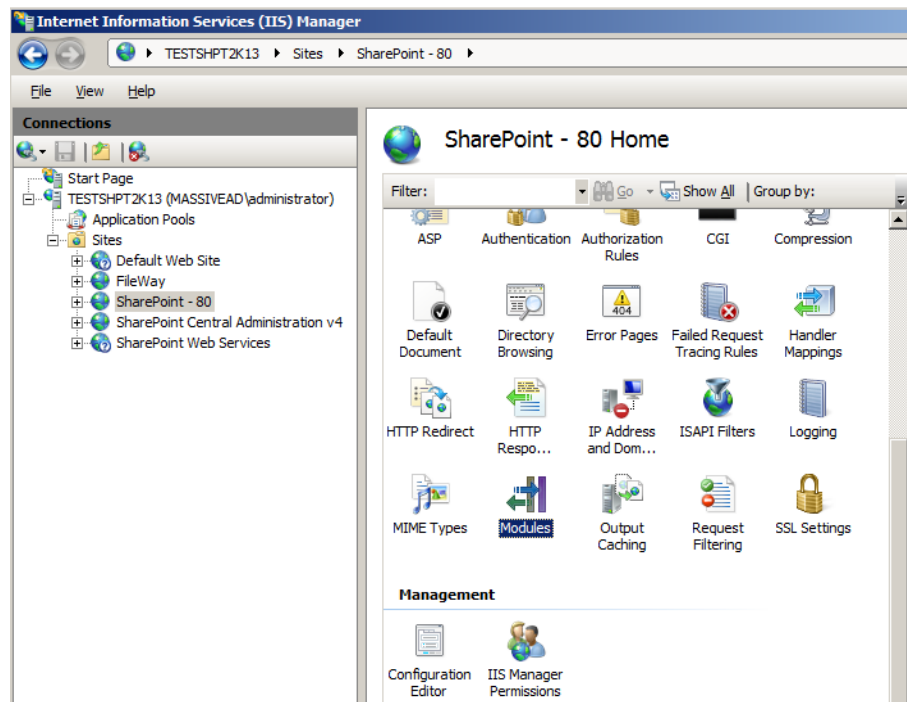
FileWay must be installed on SharePoint Server, but under different website with SharePoint Website.

To install FileWay, refer to Section 5.

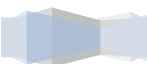
7.3.2 Install Authentication Module

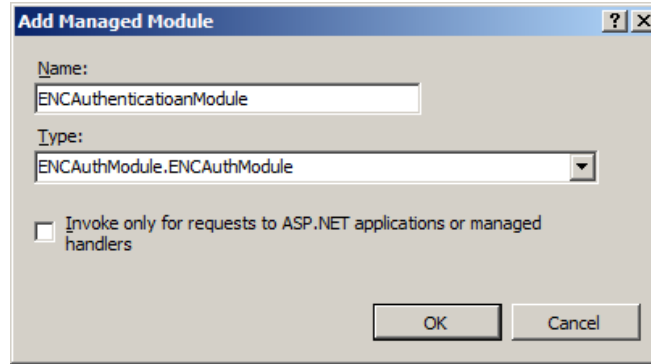
When integrating FileWay with SharePoint 2013, ENC Authentication Module must be added to SharePoint to make Single Sign On work.

1. Copy the **ENCAuthModule.dll** (default location: Program Files\ENC\FileWay\FileWay FrontEnd\ENCAuthModule\ENCAuthModule.dll) to SharePoint **bin** folder (default location: C:\inetpub\wwwroot\wss\VirtualDirectories\80\bin)
2. Open IIS Manager and click the website, SharePoint - 80.



3. In **Features View**, double-click **Modules**.
4. On the **Modules** page, in the **Actions** pane, click **Add Managed Module**. The following window appears.





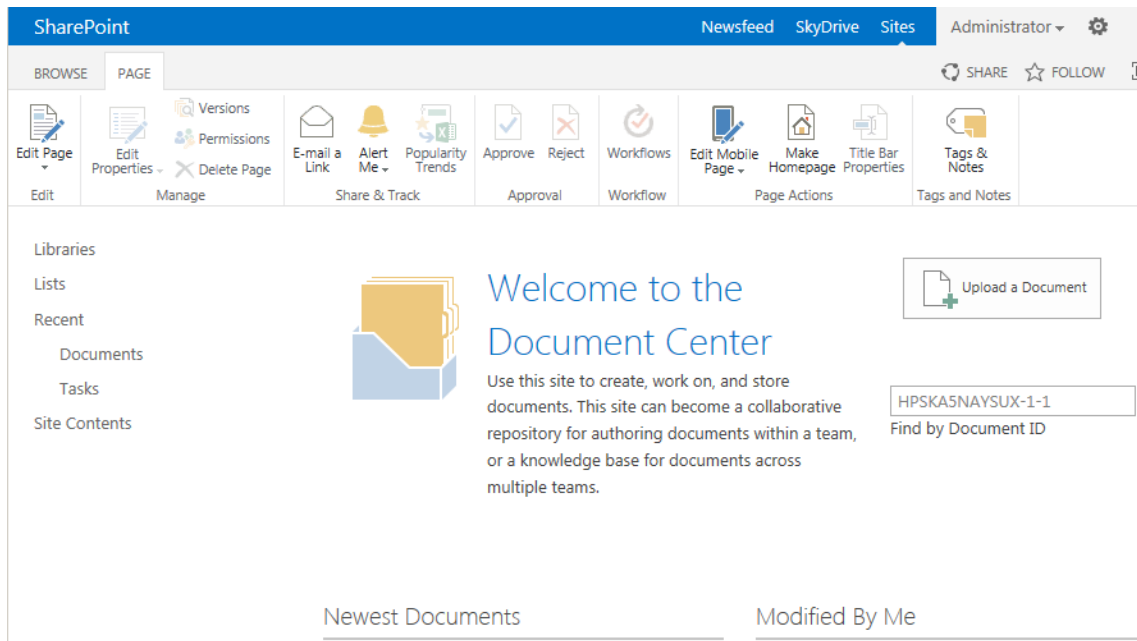
5. In the **Add Managed Module** dialog, in the **Name** text box, type a name for the managed module, e.g. ENCAuthenticationModule
6. In the **Type** box, type exactly the following text: ENCAuthModule.ENCAuthModule
7. Click **OK**.

7.3.3 Adding FileWay to SharePoint 2013 as WebPart

This section describes how to add FileWay to SharePoint as a WebPart.

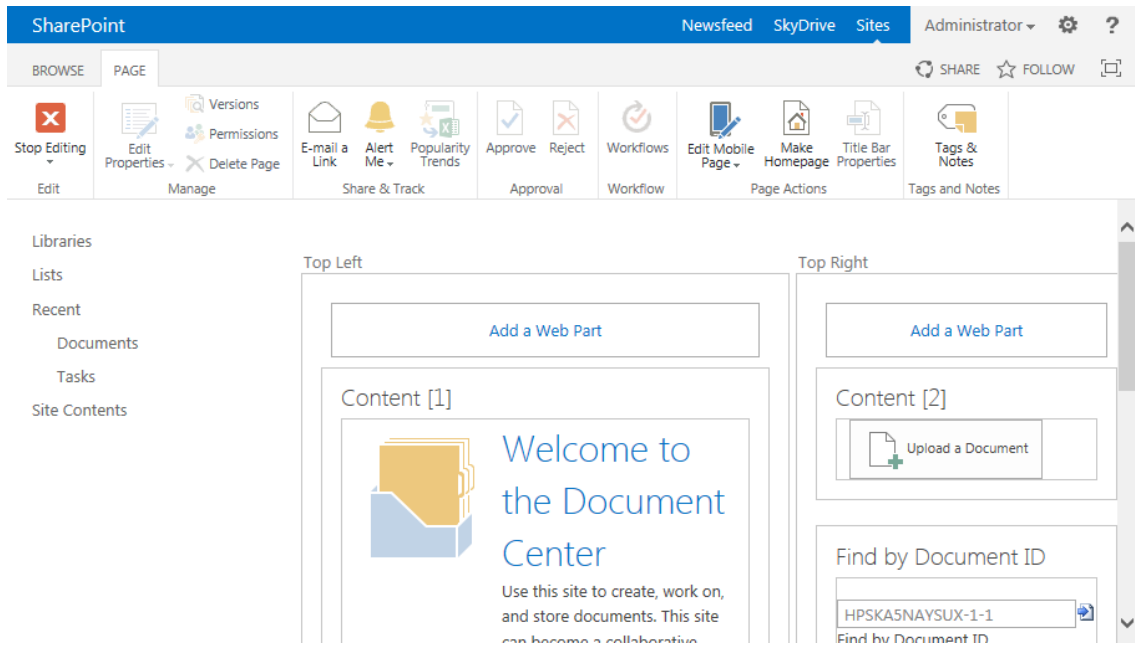
Proceed as follows:

1. Log on to SharePoint 2013 as Administrator and click **PAGE** tab. See figure below.

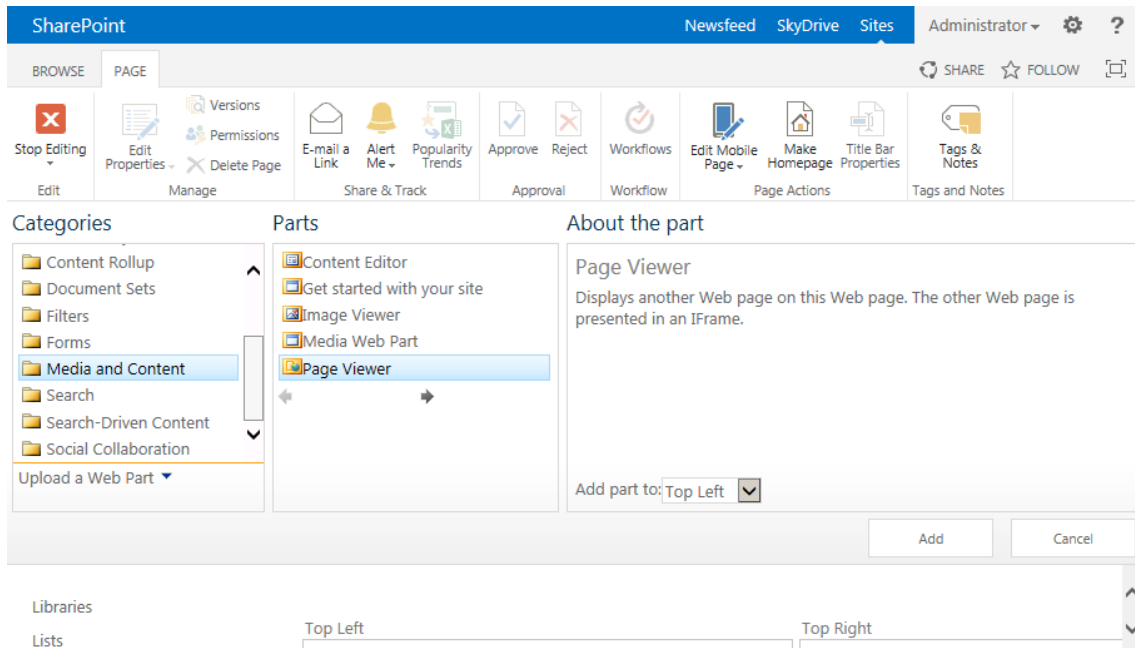


2. Click **Edit Page**. See figure below.



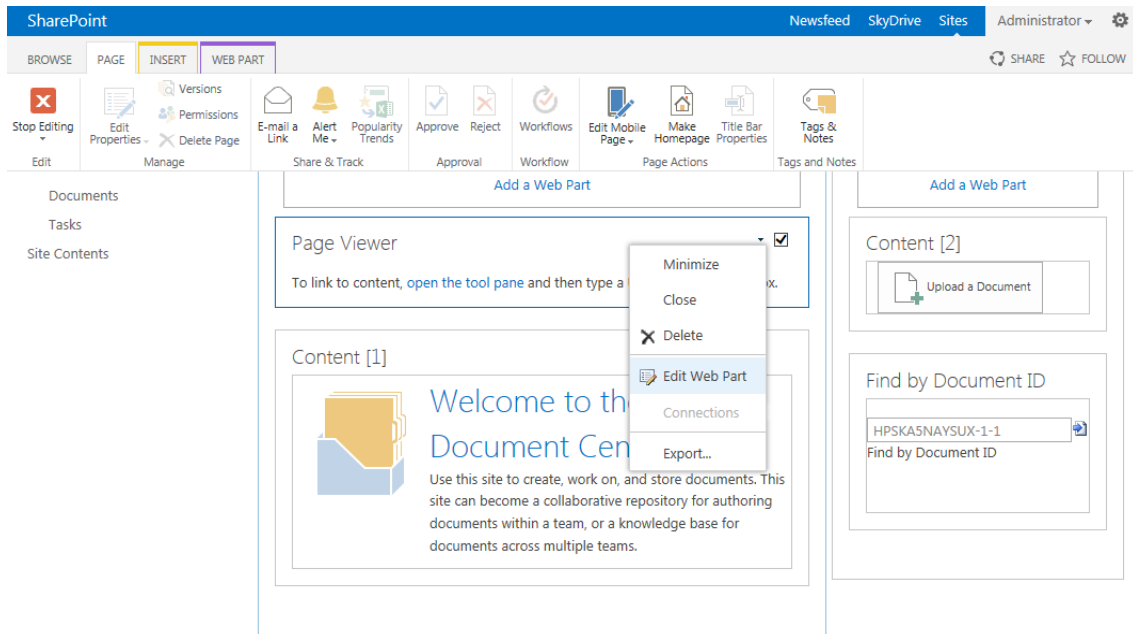


3. Click **Add a Web part**. See figure below.

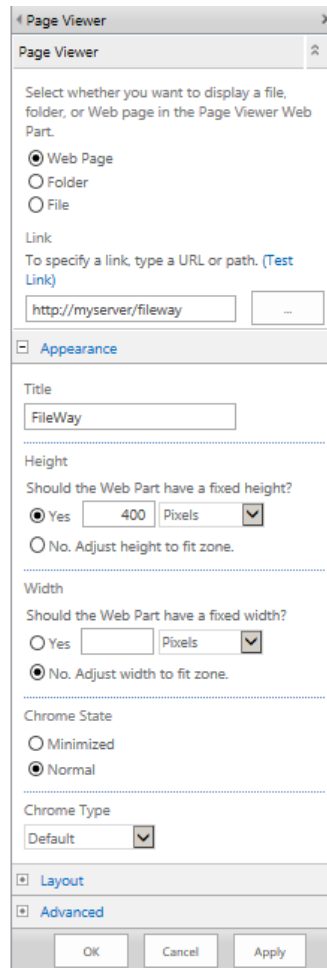


4. Under Categories, click **Media and Content**, **Page Viewer**, and then click **Add**. See figure below.





5. On the **Page Viewer Web Part**, click **Edit Web Part**. The window is updated; see figure below.



6. The FileWay **URL**, the **Title** of FileWay Web Part and specify the height of the Web Part. Then, click **OK** and click **Stop Editing**.
7. When FileWay users login to SharePoint, they will have the FileWay Web Part appear.

8 Branding FileWay

There are two images in FileWay that you can replace with your organization's logo; one is in the login page and the other one is in the FileWay main browser page.

Replace the following files with your logo:

For Login page background: [FileWay directory]\Images\login.jpg, image size 500 x 300 (WxH).

For the main page: [FileWay directory]\Content\Images\logoicon.png, image size 48 x 48 (WxH).

9 Localizing FileWay

FileWay v5.0 and later comes with support for several languages but not everything has been translated yet. That will be done in future releases. If you have already localized your previous version of FileWay, then those translations will still work along with the new items.

This section explains how to localize FileWay for languages other than English US.

1. Browse to Program Files\ENC\FileWay\FileWay FrontEnd\FileWay\languages. There you will see the **Default** folder. This folder contains the new translations.
2. The files in the Default folder have the following format CULTURE-XX-description.txt. For example, en-xx-ui.txt is the default English file for the UI elements.
3. Select a set of files you want to modify or translate from the Default folder and copy them into the Custom folder. You can use the "en" files or any other language we support. Do not modify the default files or delete them.
4. Rename the files you copied by replacing the "XX" in the name to match your country code. For example, fr-XX-UI.txt can be named fr-ca-ui.txt or fr-ch-ui.txt.
5. Edit the files to translate or modify. Change only the text between quotation marks following the "=" sign.

FileWay will try to find the matching language in the Custom folder first. If it fails then it will look in the Default folder for a matching culture and if there is no such match it will use the default English files.



10 Customizing FileWay FrontEnd

There are many ways to customize FileWay FrontEnd to match your company's requirements.

This customization can be done using either FileWay Manager or modifying the FrontEnd **web.config** file. The FrontEnd **web.config** file is usually found in the folder **Program Files\ENC\FileWay\FileWay FrontEnd\FileWay**. You can install different FrontEnds and configure each one differently.

If you choose to use the FrontEnd **web.config** as way of customization you will need to first update the application setting called **UseConfigSettings**:

```
<appSettings>
  <add key="UseConfigSettings" value="true"/>
```

If set to **true**, FileWay will use the data in the **web.config** file instead of using the data stored in the database.

All these options are customizable from either the **web.config** file or FileWay Manager:

```
<add key="DomainName" value="your domain" />
<add key="UPNLoginEnabled" value="false" />
<add key="BrowserBorderColor" value="#ff0033" />
<add key="MediaFileExtensions" value="mov,wma,wmv,avi,mpeg,wav,mp3,mid,mp4" />
<add key="ViewAsTextExtensions" value="txt,cs,css,js,xml,xhtml,xht" />
<add key="FileWaySessionTimeout" value="20"/>
<add key="DownloadOnDbClick" value="true" />
<add key="ZoomIntensityForMobileDevice" value="Low" />
<add key="FileWay_Upload_CSS_File" value="default-jquery-ui.css" />
<add key="GlobalViewOptionEnabled" value="true" />
```

Note: Be aware that some customizations made to FileWay will be lost whenever FileWay is upgraded. However, if using the database to store (`<add key="UseConfigSettings" value="false"/>`) the customization items will be preserved during upgrade. Make note of what changes are made if using the **web.config** file to store customization items.

11 Zipping and Unicode

The FileWay Zip and Download function supports Unicode files. However, older archiving tools, including the built-in compression tools, do not always support Unicode file names inside zip archives. If you find that your zip and downloaded files do extract successfully but that the names of the file(s) inside the archive file are not appearing as Unicode text, we recommend that you use the latest version of 7-zip (<http://www.7-zip.org>) or WinRAR to successfully restore the file from the zip files created by FileWay.



12 Using FileWay Drive

FileWay Drive is a WebDAV Class 2 RFC2518-compliant server. For information about the WebDAV protocol, refer to www.webdav.org.

FileWay Drive allows users to upload and download multiple files and folders on all networked servers without having to install any components on these servers. It also allows users to edit files online without having to download them. FileWay "marks" any opened files that are being edited by a user as "locked". This feature prevents other users from simultaneously opening those same files. When accessing files through the browser, users will see locked files marked with a special icon. Hovering the mouse over a locked file will display the name of the user who is using that file. When the file is saved and unlocked, other users can have access to the most recent version of the file.

Note: FileWay Drive does not support file versioning (Delta V).

12.1 IIS, Authentication & SSL

FileWay Drive is required to run as Basic Authentication and it supports WebDAV over SSL to keep important documents secure.

If using FileWay Drive on IIS it is recommended to remove the **WebDAV Publishing** role service for the server. If using IIS, if you had previously installed the WebDAV extension module it is recommended to remove it.

Also, make sure that impersonation is set to true in the **web.config** file or in the IIS Manager interface.

12.2 Tested WebDAV Clients

FileWay Drive supports most WebDAV clients and was tested extensively with the following clients:

- BitKinex (Windows)
- NetDrive (Windows)
- WebDrive (Windows)
- CyberDuck v4.7 (Macintosh)
- WebDAV Nav (iOS and Android)
- My WebDAV (iOS)
- GoodReader (iOS)

Most Microsoft Windows built-in WebDAV clients seem to have limitations and do not fully work with FileWay Drive.

Apple's OS X built-in clients seem to work well with FileWay Drive but are very slow especially with large numbers of files. CyberDuck v4.7 works very well.

12.3 Connect to FileWay Drive

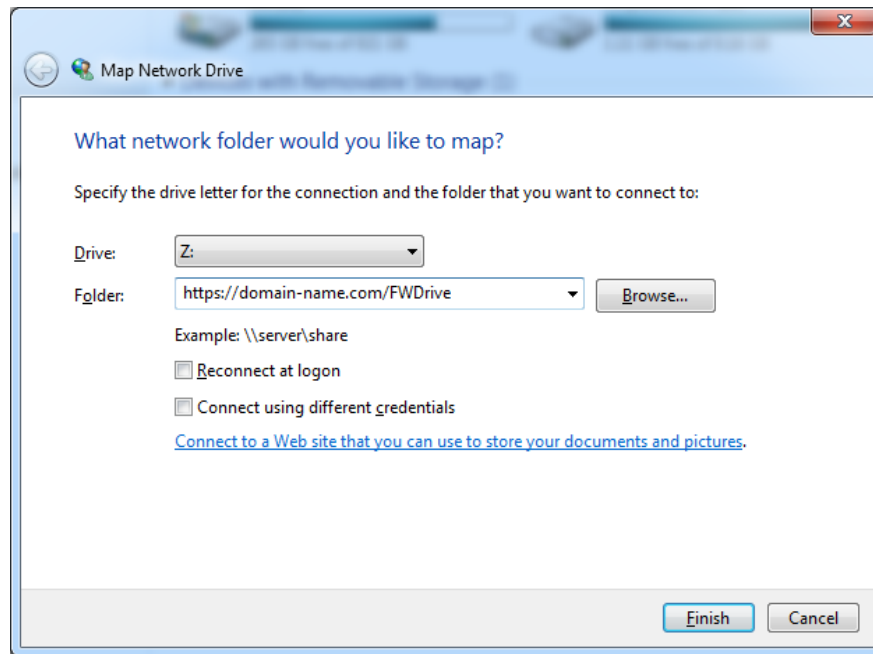
You can connect to FileWay Drive through the built-in WebDAV clients in Windows, Apple's OSX and Linux. Or, you can connect FileWay Drive to third party WebDAV clients.

12.3.1 Connect FileWay Drive to the Built-in WebDAV Clients in Windows 7 and Later

1. Open Windows Explorer.
2. Click **Map Network Drive**.
3. In the **Map Network Drive** dialog, click a letter for the drive.



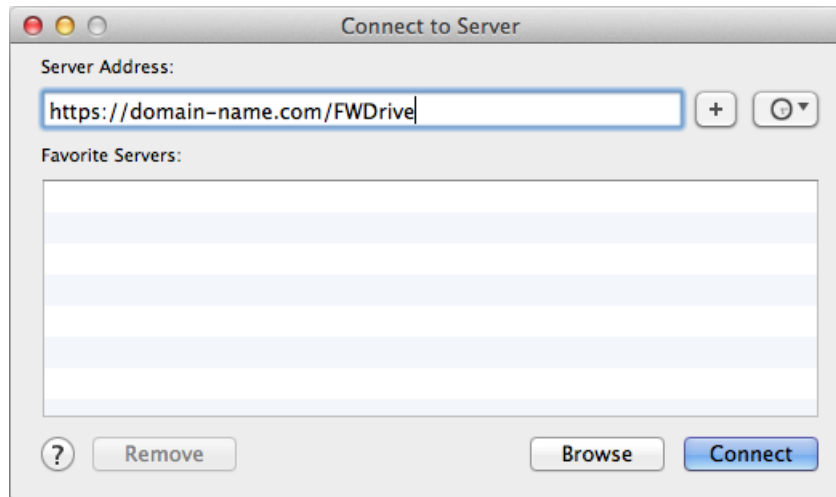
4. Type the URL of the FileWay Drive in Folder box as follows: `http(s)://DomainName/FWDrive`.



5. Click **Finish**. The **Login** dialog appears. Type user credentials as `DomainName\UserName` and password to login.

12.3.2 Connect to the Built-in WebDAV Client in Apple's OSX

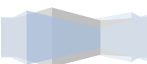
1. From the Finder's Go menu, click Connect to Server.
2. Type the FileWay Drive URL as shown in the figure below.



3. Click **Connect**. The **Login** dialog appears. Type user credentials as `DomainName\UserName` and password to login.

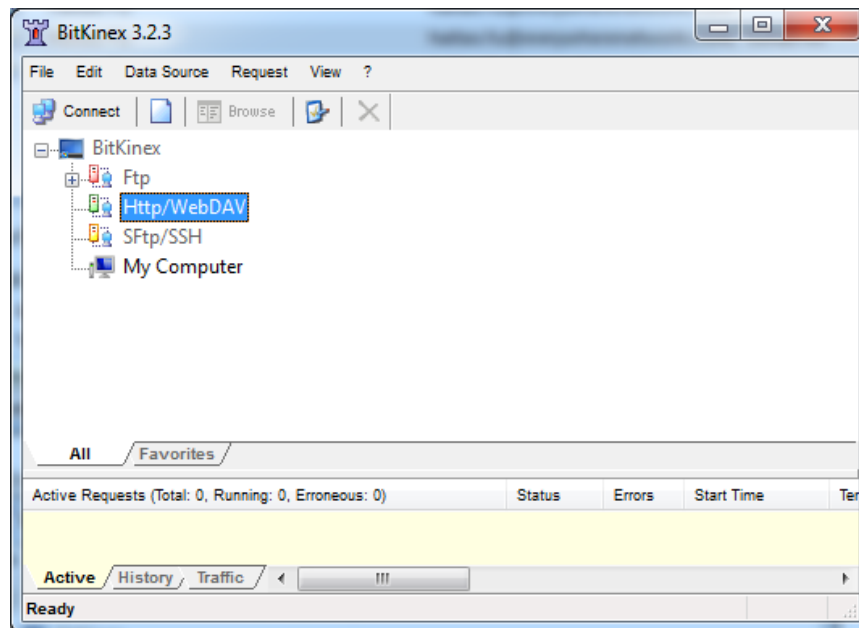
12.3.3 Connect to Third Party WebDAV Clients

We will give the example using BitKinex. The configurations of other third party WebDAV clients could be slightly different. You can find the instructions that are supplied with the WebDAV clients or in the Help.

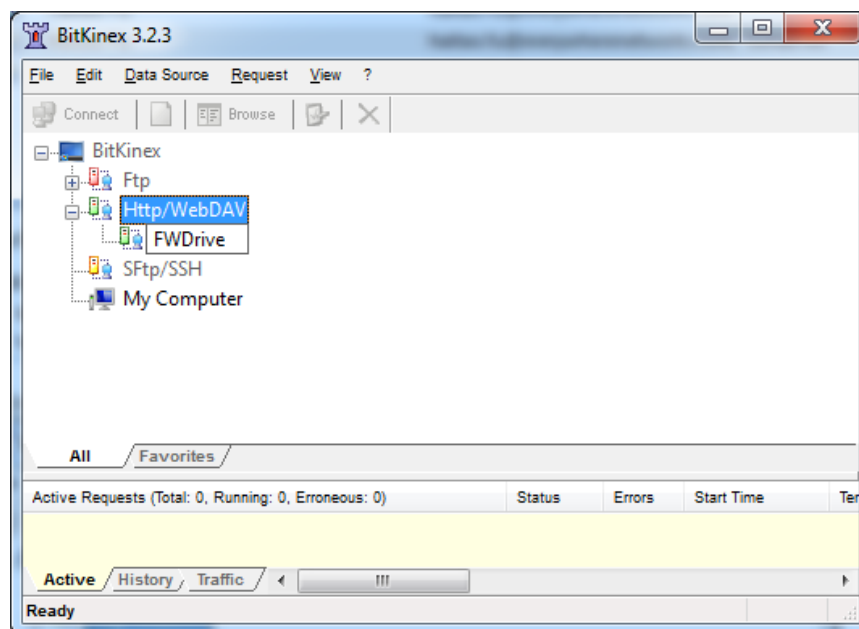


12.3.3.1 Connect FileWay Drive Using BitKinex

1. Download and install BitKinex.
2. Run BitKinex. Right-click Http/WebDAV -> New -> Http/WebDAV.

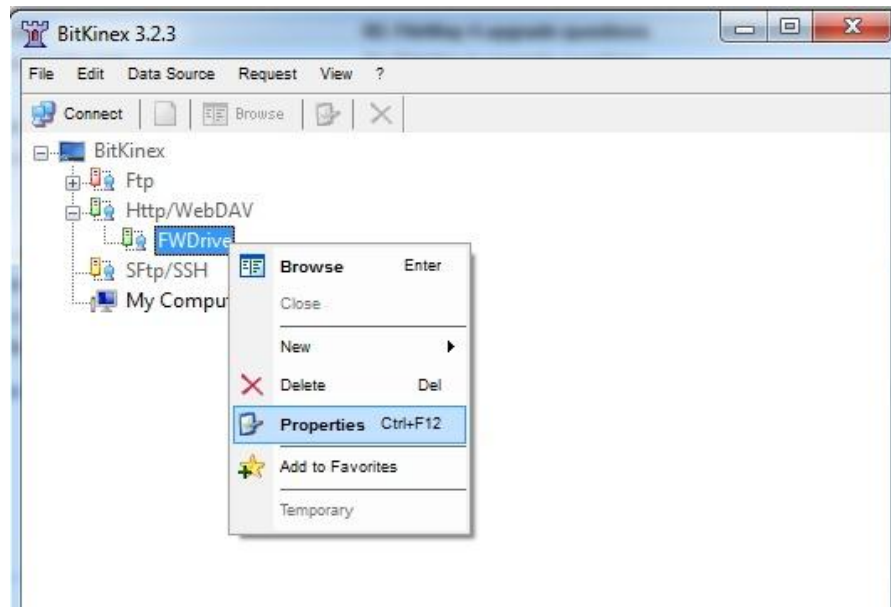


3. Type name, for example, FWDrive, MyDrive.

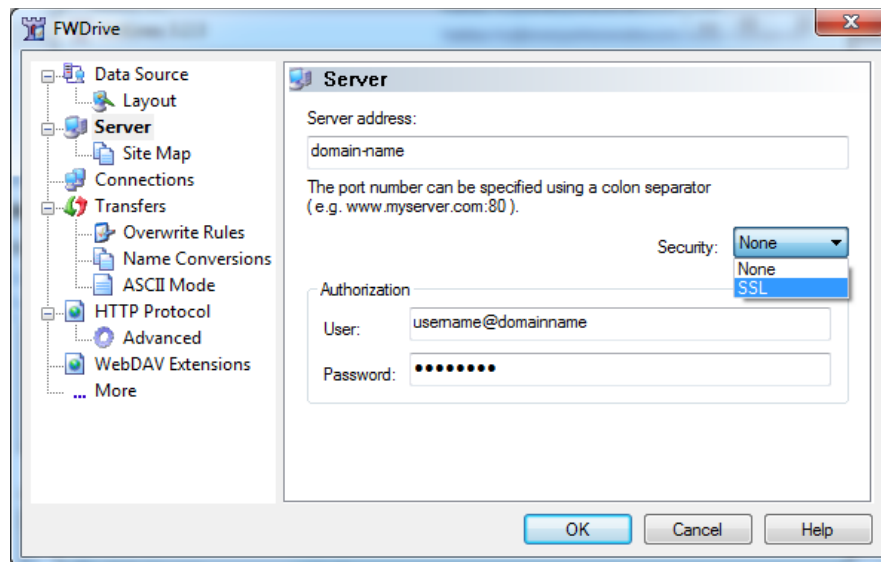


4. Right-click the name and click **Properties**.



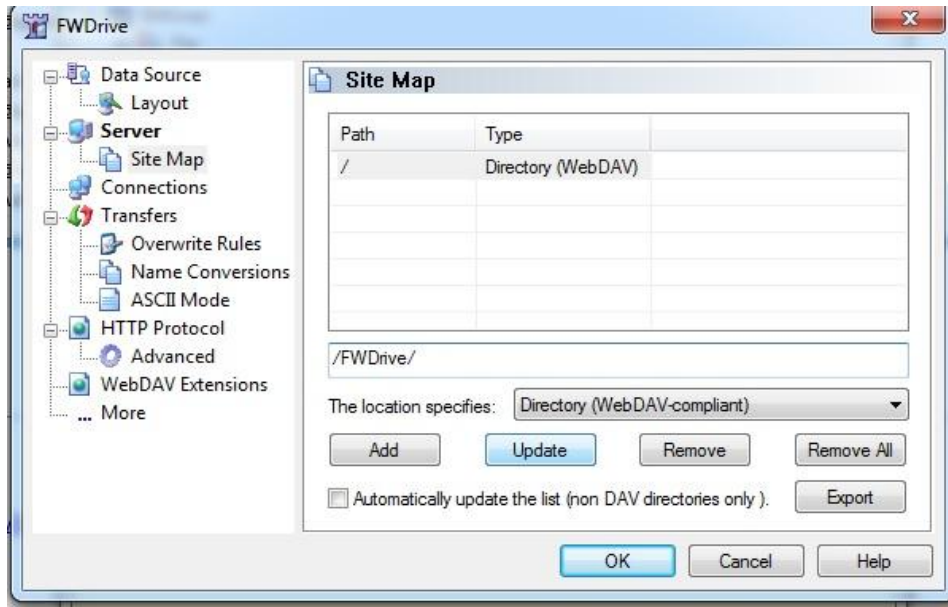


5. In **Properties** dialog, type the domain name. Set SSL if it is used. Then type user credentials. Now click **Site Map**.

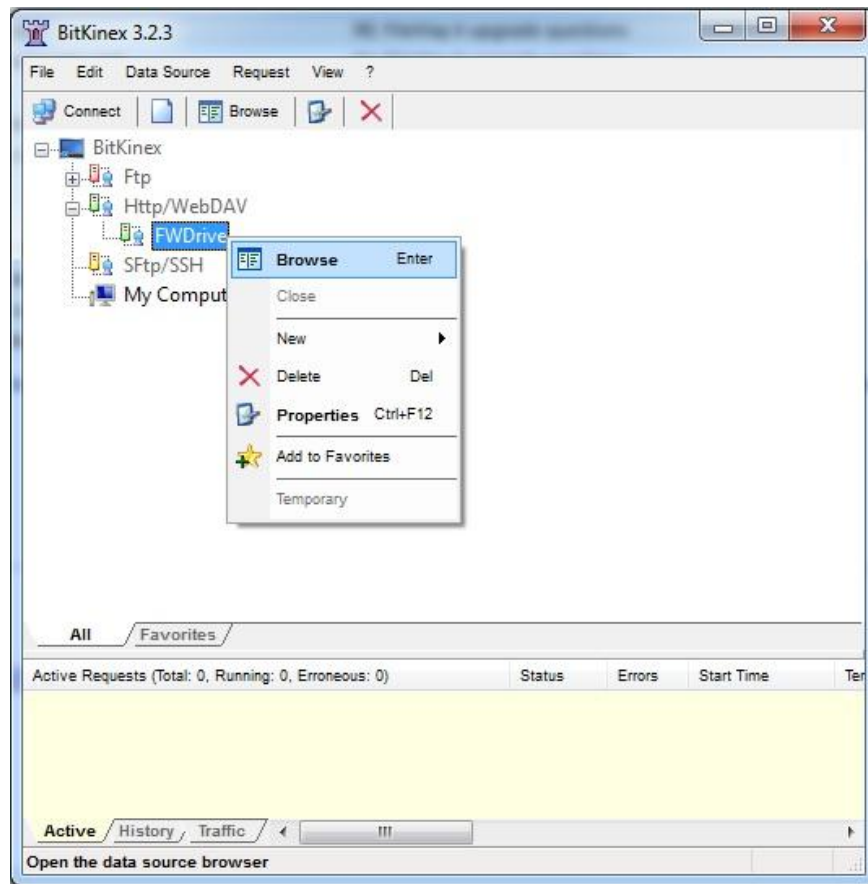


6. Select the Path. Modify it as /FWDrive/ which is the virtual directory name of FileWay Drive. Click **Update**. Then click **OK**.





7. Right-click the server and click **Browse**. The Browser appears.



13 Configuring FileWay

As an Administrator, you can specify access Rules for many users at a time based on a variety of criteria.

13.1 Rulesets

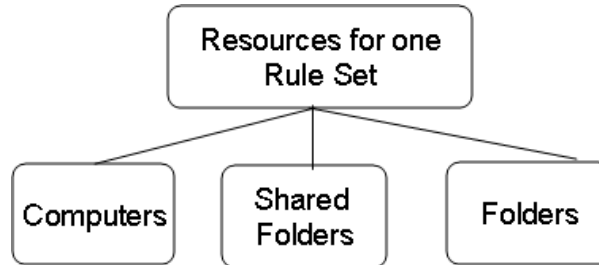
Rulesets comprise the following elements:

- Members
- Resources
- Options

Rulesets combine members (i.e. users) resources and options to create access Rules in a way that is logical for a given Ruleset. For example, a Ruleset called Sales could contain all employees working in the Sales department and would provide those employees with access to the resources that they need.

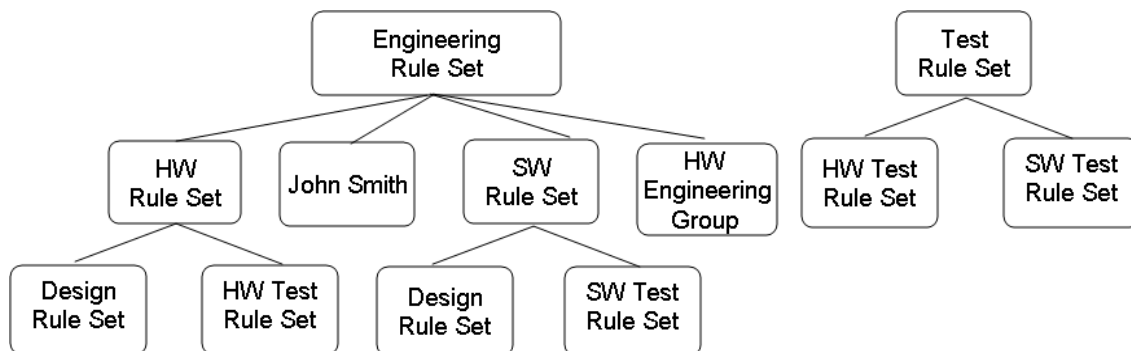
13.1.1 Ruleset Resources

Resources contain multiple references to folders and shares from different computers and servers. Resources can also contain multiple references to computers. Refer to the following figures.



13.1.2 Ruleset Members

Members can contain references to individual users, groups and organizational units in your Active Directory. Rulesets can also contain references to other Rulesets. A user can be a member of multiple Rulesets. Refer to the following figures.



13.1.3 Ruleset Options

Ruleset options allows administrator to specify which actions users may perform on files and folders using FileWay.



13.1.4 Planning Access Rules for Multiple Users

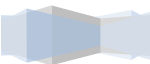
As described in the concepts section above, you have several components to work with: groups in your Active Directory, Rulesets, folders, shares and computers. You should plan how to group these components.

Begin with Rulesets. Rulesets can be named according to functional groups within your organization, for example, Sales, Marketing, Engineering and Research could be four Rulesets. The name of the Ruleset will appear to end-users as a virtual machine when they login to FileWay.

Next, decide which members should be part of a given Ruleset (i.e. users and groups). These users and groups come from your organization's Active Directory. For example, a Ruleset called Sales would likely contain one or more existing groups or Organizational Units.

Next, decide which resources must be added to the Sales Ruleset. Resources are a collection of references to folders, shares and computers.

Once you have planned your Rulesets, members, resources and attributes, start using FileWay Manager.



14 Using FileWay Manager

FileWay Manager allows you to

- Specify global settings for FileWay
- Manage Ruleset members (users), resources and options

14.1 Starting FileWay Manager

FileWay Manager should have been installed on the same server as the FileWay BackEnd Server. There should be a FileWay Manager short cut on the desktop. Double-click the short cut to start FileWay Manager.



14.2 Specifying Global Settings for FileWay

In previous versions of FileWay, global settings were specified using the **web.config** file. Since version 3.7, global settings are specified using the **FileWay Configuration Server** window. The global settings are stored in the database.

FileWay Server Configuration Window – General Tab

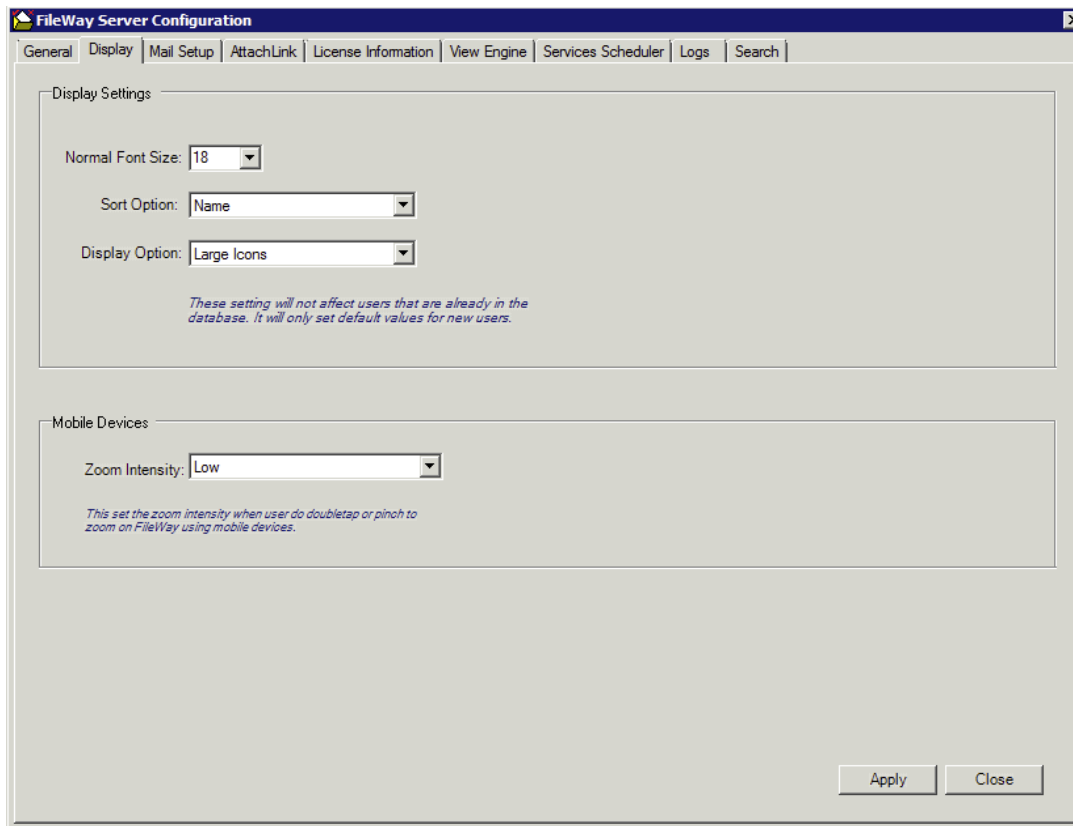
Domain Name: Stores the domain name (NetBIOS name) to use during FBA Authentication and UPN Enabled logins.

Session Timeout: User Session timeout value. (For both concurrent and normal users)

UPN Enabled: If you want to set the FileWay account as UPN login, enable it. But if enabled Domain Name value should also be provided.

Download on Double Click Instead of View: This setting allows users to download a file by double-clicking the file name instead of viewing it.





FileWay Server Configuration Window – Display Tab

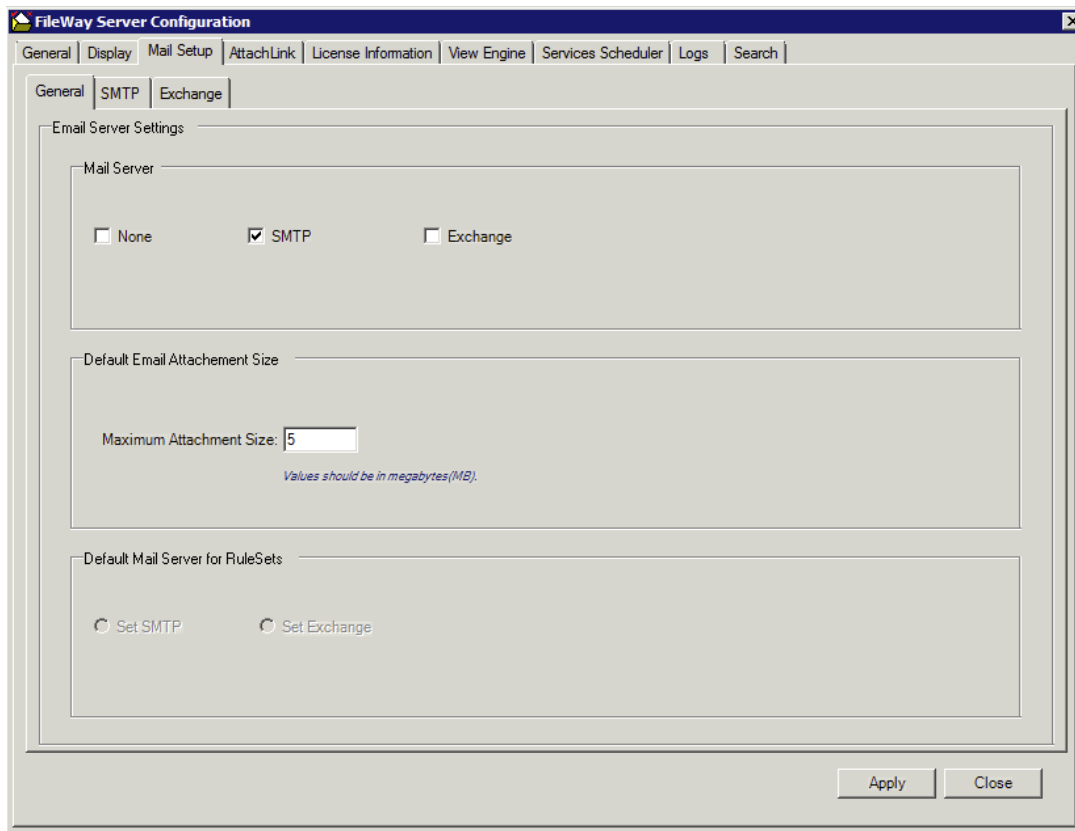
Normal Font Size: Select the default display font size.

Sort Option: Select the default option to sort file list.

Display Option: Select the desired starting display option.

Zoom Intensity: Specifies the pinch to zoom intensity in mobile devices.





FileWay Server Configuration Window – Mail Setup Tab – General

Mail Server: Specify your mail server type. If you select SMTP and Exchange, Rulesets can specify which mail server to use.

Mail Attachment Size: Set default email attachment size.

Default mail server for Rulesets: Set the default mail server for Rulesets.



FileWay Server Configuration

General | Display | Mail Setup | AttachLink | License Information | View Engine | Services Scheduler | Logs | Search

General | **SMTP** | Exchange

SMTP Settings

Server Address: Port Number:

Example: mail.everywherenetwork.com

☐ Enable SSL

☐ Require Authentication

☐ User Account ☒ Administrator Account

Administrator Email Account

Sender Name: Username:

Sender Email: Password:

Apply Close

FileWay Server Configuration Window – Mail Setup Tab – SMTP

Server Address [SMTP Settings]: Should contain SMTP mail server address.

Port Number: Port number.

Enable SSL: Check this if SSL is enabled.

Require Authentication: Choose either User Account or Administrator Account if authentication is required.

Administrator Email Account:

SMTP Sender Name: The sender's name for the temporary login ID email if using SMTP.

Sender Email: The sender's email address for the temporary login ID email if using SMTP.

Username: The username of sender account.

Password: The password for sender account.



The screenshot shows the 'FileWay Server Configuration' window with the 'Mail Setup' tab selected. The 'Exchange' sub-tab is active. The 'Exchange Settings' section contains the following fields and options:

- Exchange Server:** A dropdown menu with 'Exchange2013' selected.
- Exchange Version:** A text field containing 'Exchange2013'.
- Server Address:** A text field containing 'everywherepwa2013'. Below it is a small example: 'Example: mail.everywherenetwork.com'.
- SSL Enabled:** A checked checkbox.
- FBA Enabled:** An unchecked checkbox.
- Administrator Email Account:** A section containing:
 - Username:** A text field containing 'administrator'.
 - Password:** A text field with masked characters (dots).

At the bottom right of the window are 'Apply' and 'Close' buttons.

FileWay Server Configuration Window – Mail Setup Tab – Exchange

Exchange Server: Exchange server version list.

Server Address [Exchange Settings]: Should contain exchange server address.

Exchange Version: editable exchange version. Leave it if you are using default version setting for exchange.

SSL Enabled: check this if your Exchange server is using SSL.

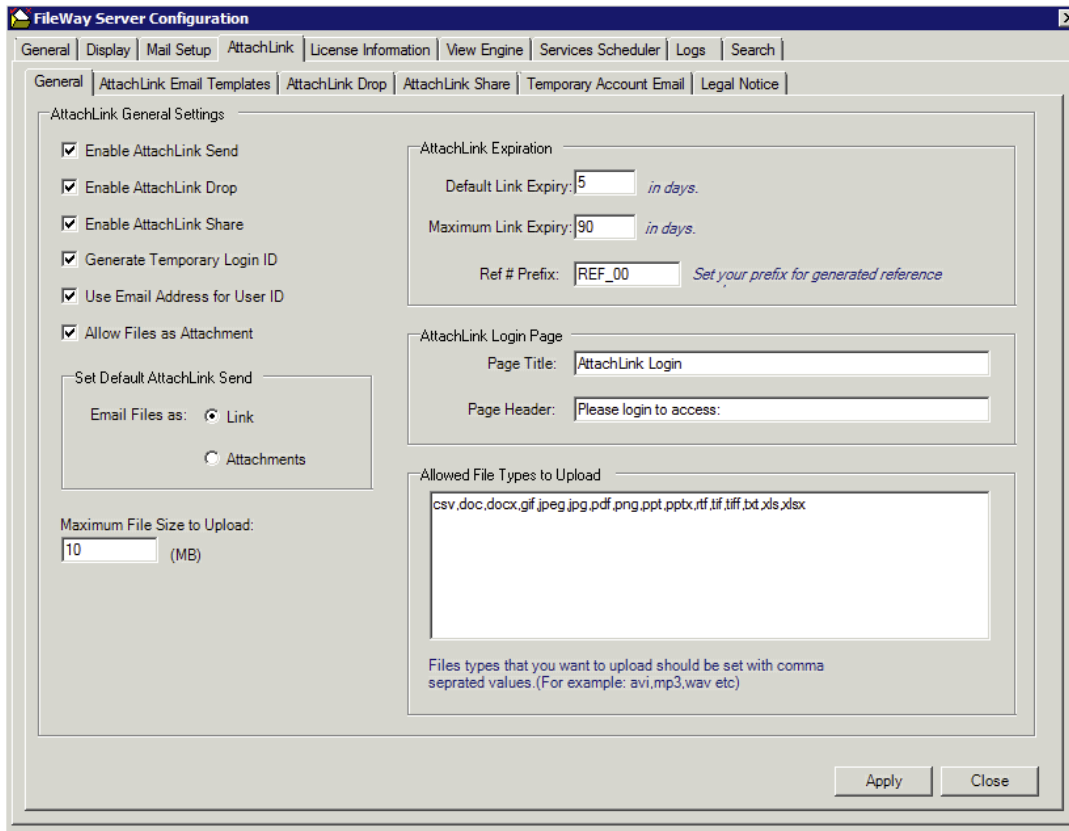
FBA Enabled: check this if your Exchange server is using Form Based Authentication (FBA).

Administrator Email Account:

Username: The login ID for the Exchange account to send the temporary login ID email from.

Password: The password for the Exchange account to send the temporary login ID email from.





FileWay Server Configuration Window – AttachLink Tab – General

Enable AttachLink Send: If Enable AttachLink Send is selected, email file attachments will be sent as links instead of sending the actual files. This works in conjunction with Ruleset Options.

Enable AttachLink Drop: If Enable AttachLink Drop is selected, users can create Drop Folder and send a link to other users to upload files into the Drop Folder. This works in conjunction with Ruleset Options.

Enable AttachLink Share: If Enable AttachLink Share is selected, users can share files in selected folders with others for collaboration. This works in conjunction with Ruleset Options.

Generate Temporary Login ID: Generate temporary accounts that are used to access file attachments; otherwise users can only use FileWay accounts to access files.

Use Email Address for User ID: If Use Email Address for User ID is selected, no Temporary Login ID is generated. Users can use their email address as login ID.

Allow Files as Attachments: If Allow Files as Attachments is selected, the sender can choose whether to send the file as a link or regular attachment.

Set Default AttachLink Send: Set default for email file attachments.

Default Link Expiry: The default number of days the link will be valid.

Maximum Link Expiry: The Maximum number of days users can set when they email files as AttachLink.

Ref # Prefix: Set the prefix for a randomly generated reference number for each AttachLink transaction.

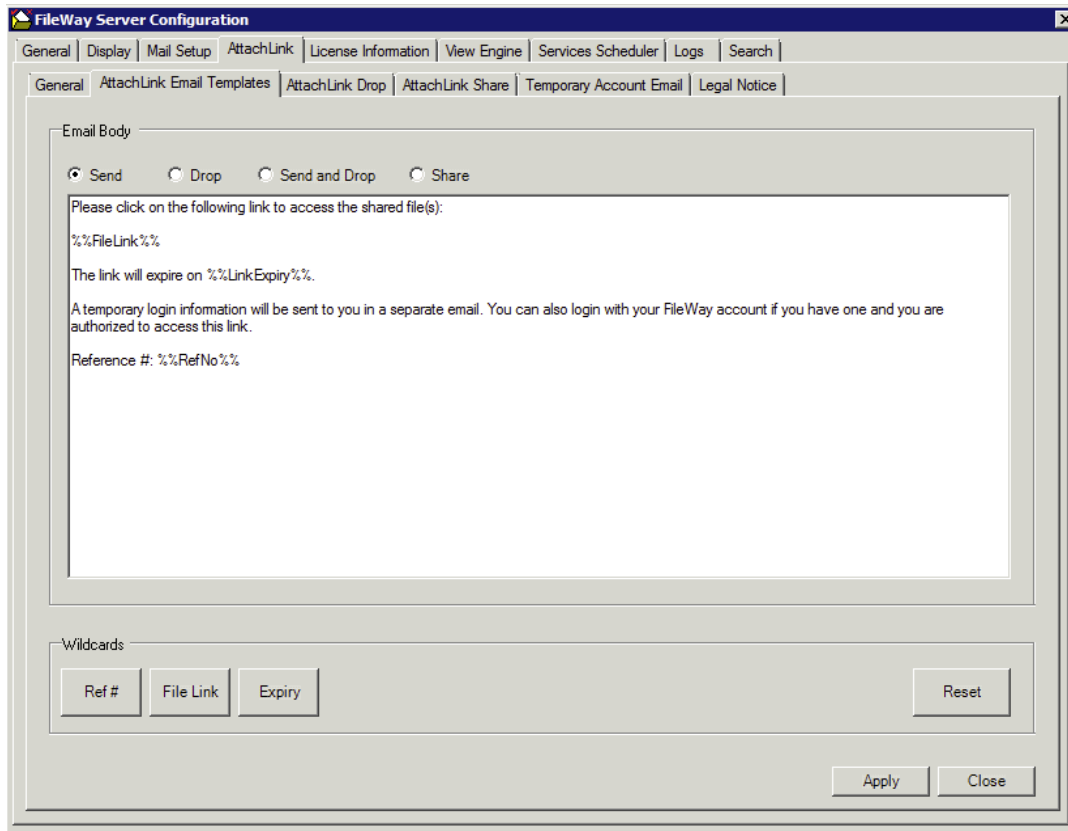
AttachLink Login Page Title: Set the title of the AttachLink login page.

AttachLink Login Page Header: Set the header of the AttachLink login page.

Maximum File Size to Upload: The maximum file size that can be uploaded to Drop Folders.

Allowed File Types to Upload: The COMMA delimited strings of file extensions that are allowed to be uploaded





FileWay Server Configuration Window – AttachLink Tab – AttachLink Email Templates

Email Body [Send]: Create a template for the email body of emails containing the link to attachments. This message will be appended to the sender's email body.

Email Body [Drop]: Create a template for the email body of emails containing the link to the Drop Folder. This message will be appended to the sender's email body.

Email Body [Both]: Create a template for the email body of emails containing the link to attachments and the link to the Drop Folder. This message will be appended to the sender's email body.

Wildcard [Ref #]: Insert Ref #.

Wildcard [File Link]: Insert File Link.

Wildcard [Expiry]: Insert link expiry date.

Reset: Reset email body to default templates.



FileWay Server Configuration

General | Display | Mail Setup | **AttachLink** | License Information | View Engine | Services Scheduler | Logs | Search

General | AttachLink Email Templates | **AttachLink Drop** | AttachLink Share | Temporary Account Email | Legal Notice

Receipt Notification Email

Send To: ☒ Original Sender ☒ Recipients
Original Sender - who creates and owns the Drop Folder
 Recipients - who will make the drop

☐ Use Single Folder Structure on Drop
☐ Force Drop in Home Folder

Default Name for Drop Folder:

Receipt Notification Email Template

Email Subject:

Message to Append to User's Email:

Wildcards

Ref #	Recipients Email Address	Original Subject	Uploaded Time	Partial Path to Drop Folder	Uploaded File Names	Reset
-------	--------------------------	------------------	---------------	-----------------------------	---------------------	-------

Apply Close

FileWay Server Configuration Window – AttachLink Tab – AttachLink Drop

Receipt Notification Email: Send an email notification to Original Sender and/or Recipients when documents are dropped.

Use Single Folder Structure: All dropped files will be saved in a single folder instead of multiple folders structure.

Force Drop in Home Folder: All dropped files will be saved in user's home folder if one is defined, otherwise, the drops will be in the folder where the user initiated the action.

Default Name for Drop Folder: The default folder name when users create Drop Folders.

Receipt Notification Email Template [Email Subject]: The subject line for the temporary login ID email.

Receipt Notification Email Template [Message to Append to User's Email]: Create the template of email body.

Wildcard [Ref #]: Insert Ref #.

Wildcard [Recipients Email Address]: Insert email addresses of recipients.

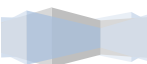
Wildcard [original Subject]: Insert Original Subject of the Original Email with File Links and/or Drop Folder Link.

Wildcard [Upload Time]: Insert the Time when files are dropped.

Wildcard [Partial Path to Drop Folder]: Insert Partial Path of Drop Folder.

Wildcard [Uploaded File names]: Insert Uploaded File Names.

Reset: Reset email body to default template.



FileWay Server Configuration

General | Display | Mail Setup | **AttachLink** | License Information | View Engine | Services Scheduler | Logs | Search

General | AttachLink Email Templates | AttachLink Drop | **AttachLink Share** | Temporary Account Email | Legal Notice

Receipt Notification Email

Send To: ☒ Original Sender ☒ Recipients
Original Sender - who creates and owns Shared Folder
 Recipients - who will make the drop

☒ Archive Old Files

Default Name of Archive Folder:

Receipt Notification Email Template

Email Subject:

Message to Append to User's Email:

Wildcards

Ref #	Recipients Email Address	Original Subject	Uploaded Time	Partial Path to Drop Folder	Uploaded File Names	Reset
-------	--------------------------	------------------	---------------	-----------------------------	---------------------	-------

Apply Close

FileWay Server Configuration Window – AttachLink Tab – AttachLink Share

Receipt Notification Email: Send an email notification to Original Sender and/or Recipients when shared documents are replaced or uploaded.

Archive Old Files: Archive the original files when uploading new files with the same names.

Default Name of Archive Folder: The default archive folder name when Archive Old Files is enabled.

Receipt Notification Email Template [Email Subject]: The subject line for the temporary login ID email.

Receipt Notification Email Template [Message to Append to User's Email]: Create the template of email body.

Wildcard [Ref #]: Insert Ref #.

Wildcard [Recipients Email Address]: Insert email addresses of recipients.

Wildcard [original Subject]: Insert Original Subject of the Original Email with File Links and/or Drop Folder Link.

Wildcard [Upload Time]: Insert the Time when files are dropped.

Wildcard [Partial Path to Drop Folder]: Insert Partial Path of Drop Folder.

Wildcard [Uploaded File names]: Insert Uploaded File Names.

Reset: Reset email body to default template.



FileWay Server Configuration

General | Display | Mail Setup | **AttachLink** | License Information | View Engine | Services Scheduler | Logs | Search

General | AttachLink Email Templates | AttachLink Drop | AttachLink Share | **Temporary Account Email** | Legal Notice

Email Subject

Temporary Login ID for: %%OriginalSubject%%

Temporary Account Email Message

%%SendersName%% has sent you a link to file(s) or drop folder. Please click the link in the original email and use the following login information:

User ID: %%LoginID%%
 Password: %%Password%%
 Reference #: %%RefNo%%

Wildcards

Ref # | Senders Name | Original Subject | Expiry | Login ID | Password | Reset

Apply | Close

FileWay Server Configuration Window – AttachLink Tab – Temporary Account Email

Email Subject: The subject line for the temporary login ID email.

Temporary Email: Create the template of email body

Wildcard [Ref #]: Insert Ref #.

Wildcard [Sender Name]: Insert original Sender Name.

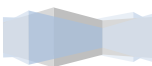
Wildcard [original Subject]: Insert original subject of the original email with File Links.

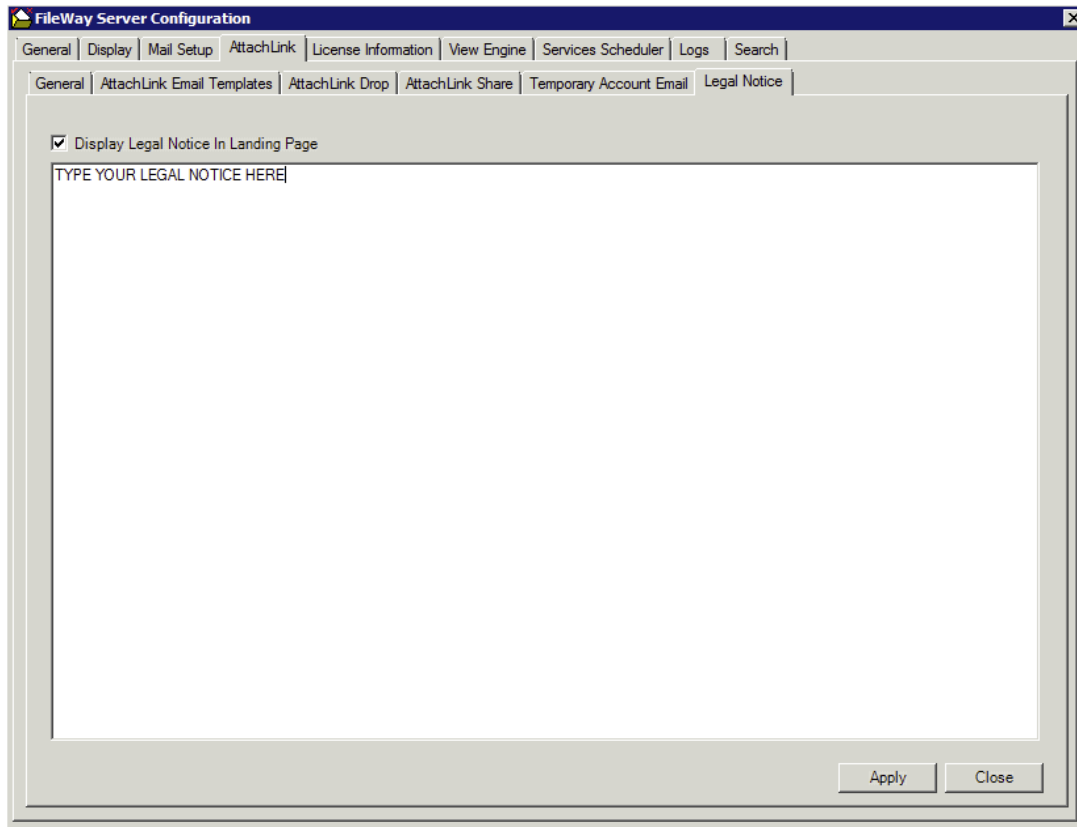
Wildcard [Expiry]: Insert link expiry date.

Wildcard [Login ID]: Insert temporary Login ID.

Wildcard [Password]: Insert temporary password.

Reset: Reset email body to default template.

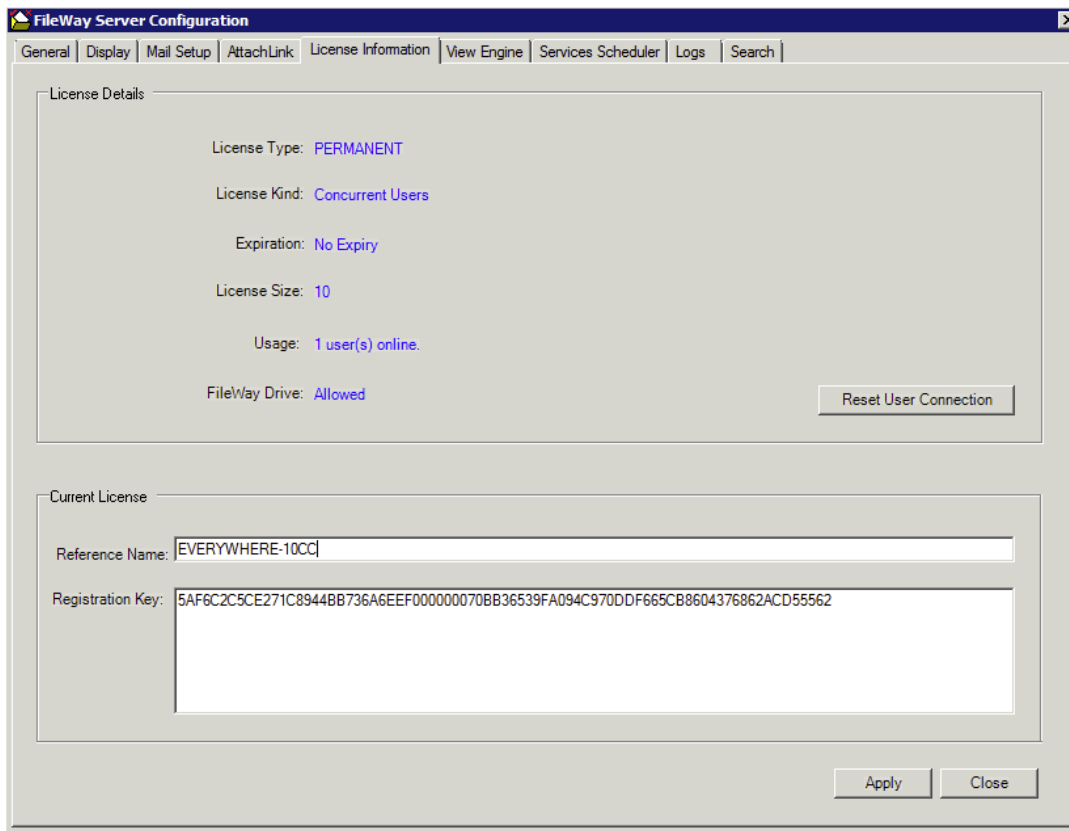




FileWay Server Configuration Window – AttachLink Tab – Legal Notice

Display Legal Notice in Landing Page: If the **Display Legal Notice on AttachLink Landing Page** check box is selected; the legal notice will be displayed in the AttachLink Landing Page.

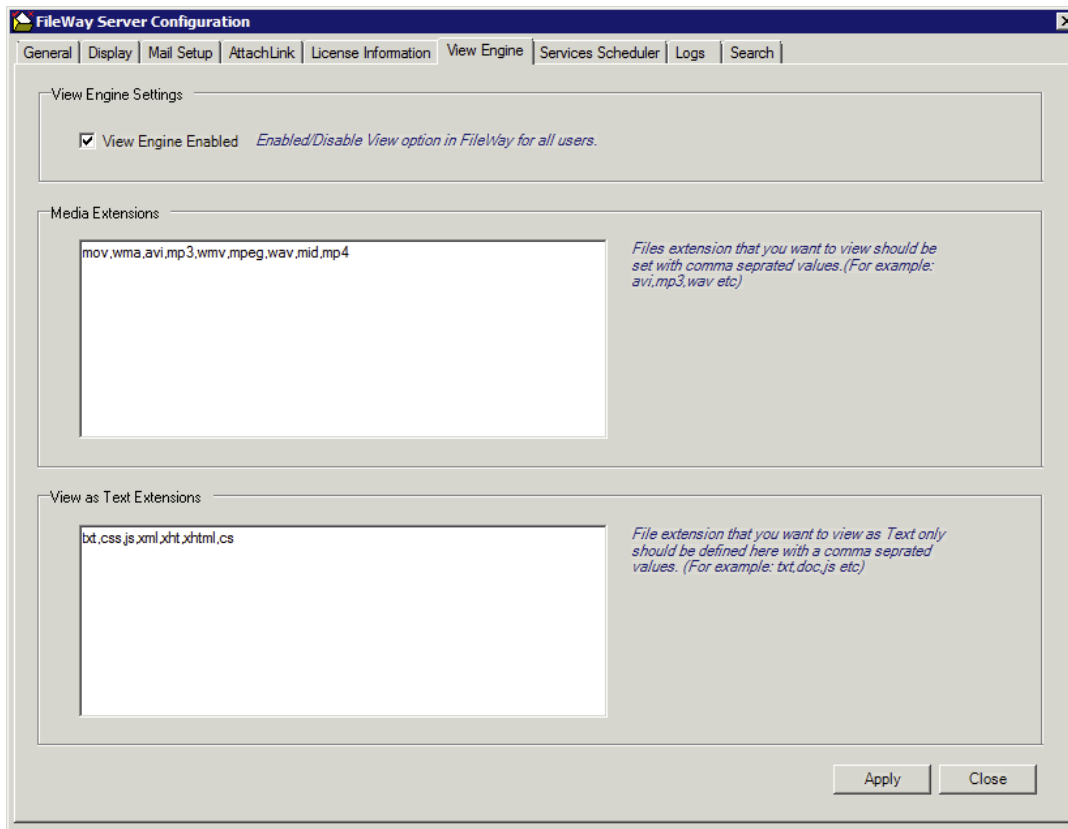




FileWay Server Configuration Window – License Information Tab

Note: This window provides information about your FileWay license. It also provides the number users that are currently online. The **Reset User Connection** button is only visible when the license kind is **Concurrent Users**. Clicking this button resets all the user sessions...meaning all FileWay user sessions end immediately.



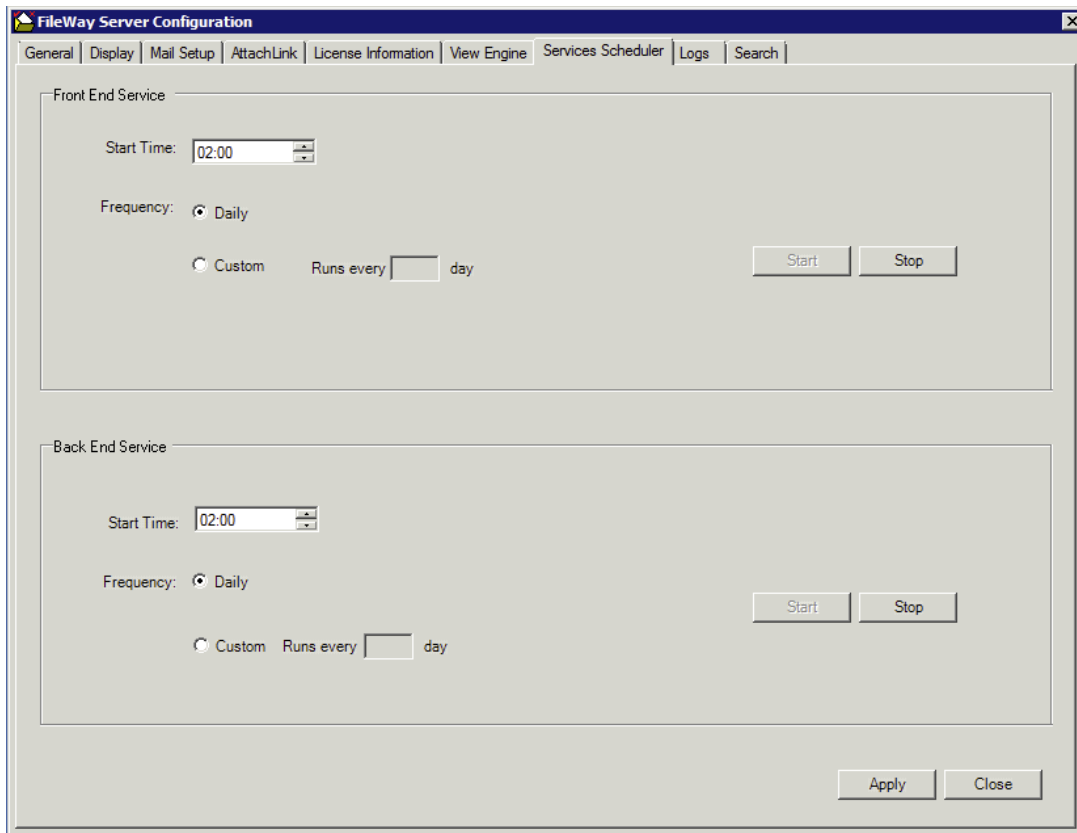


FileWay Server Configuration Window – View Engine Tab

Media Extension: This all extension will be treated as media files Extension. Make sure if you add new media extension you should also specify it MIME type in IIS.

View ad Text Extension: This all extension will be treated as text extension for view engine.

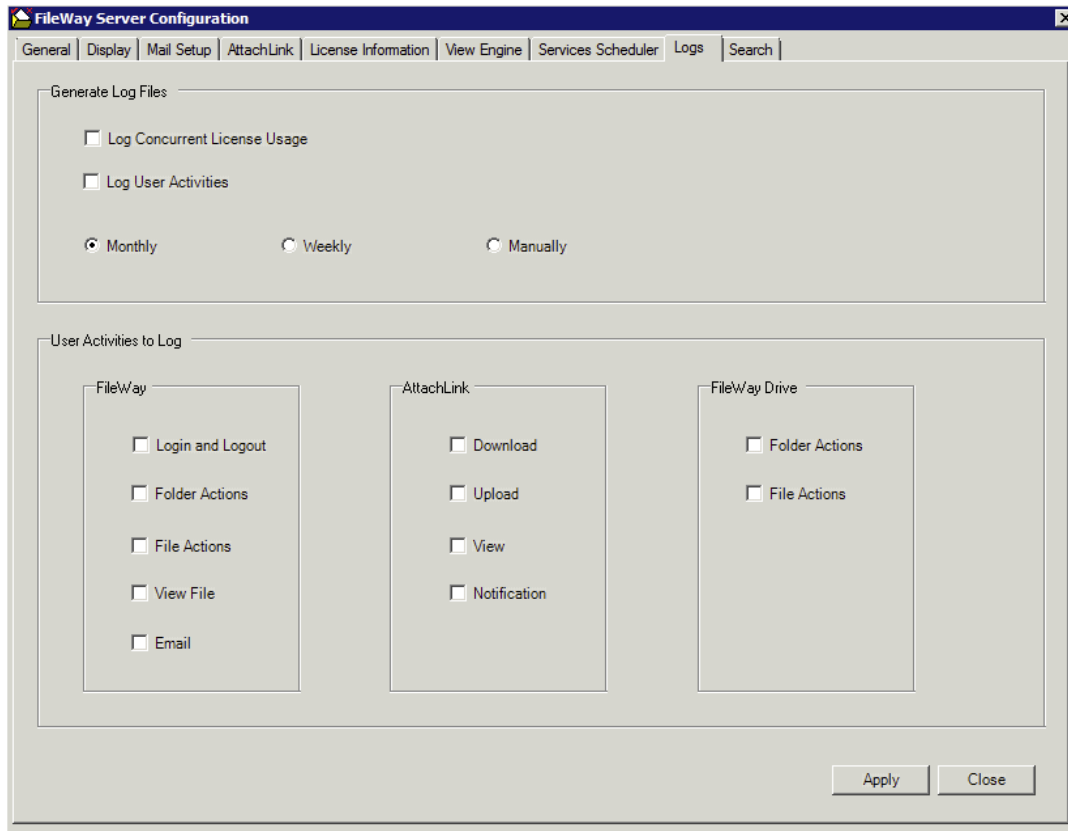




FileWay Server Configuration Window – Services Scheduler Tab

This tab allows you to change the start time and the frequency of the Windows Services.





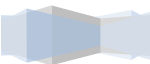
FileWay Server Configuration Window – Logs Tab

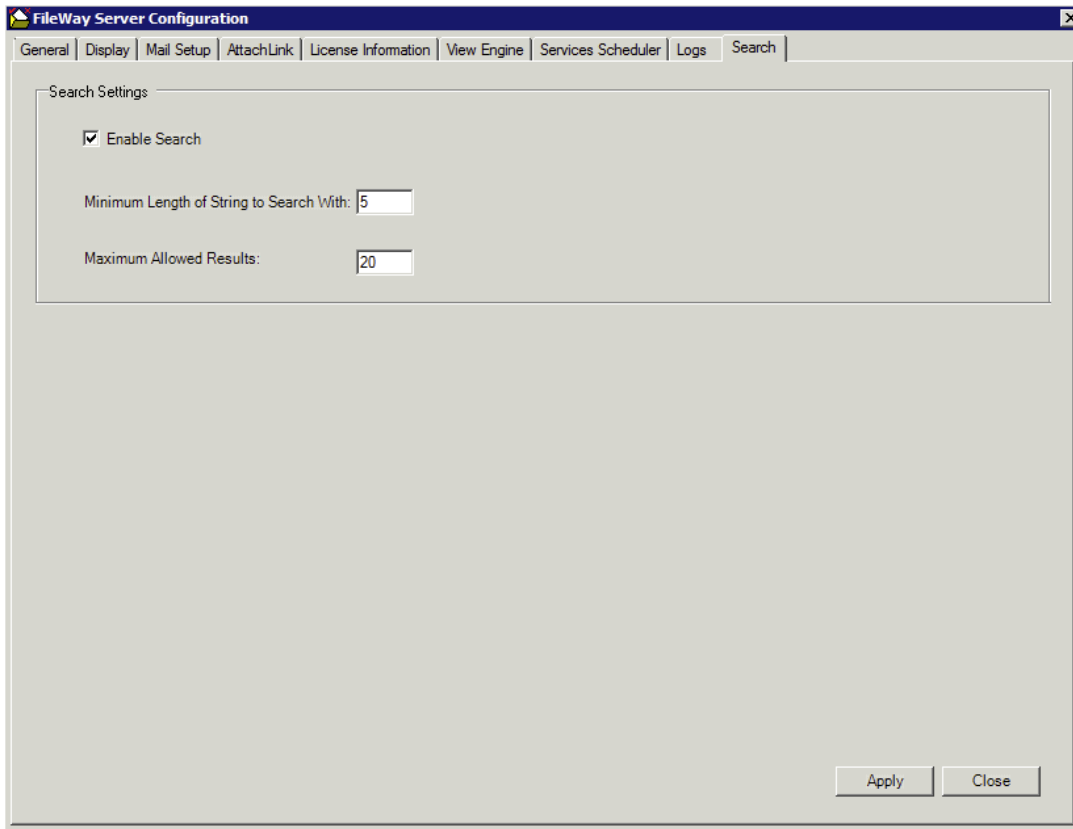
Log Concurrent License Usage: If enabled, Concurrent License Usage Logs will be generated.

Log User Activities: If enabled, User Activities Logs will be generated.

Generate Log Files: Choose how often to export log files into CVS format files. If you choose Manually then log data are not exported and the administrator can generate reports from the Tools menu in FileWay Manager. After log data have been exports the old log data will be removed.

User Activities to Log: The different actions to log.





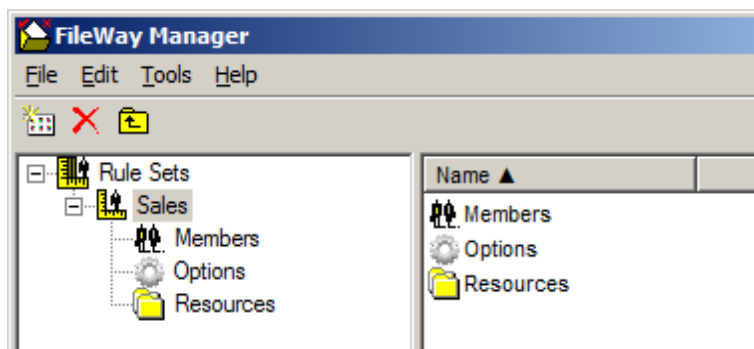
FileWay Server Configuration Window – Search Tab

Enable Search: If enabled, users can search files and folders.

Minimum Length of String to Search With: Minimum number of characters in search text.

Maximum Allowed Results: Maximum number of search results can be returned.

14.3 Managing Ruleset Members, Options and Resources

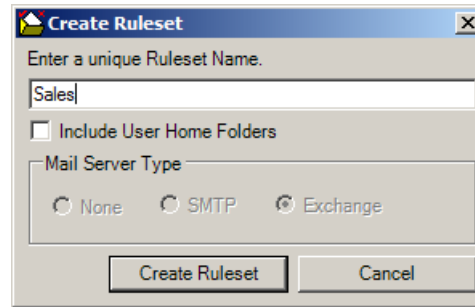


14.3.1 Creating a Ruleset

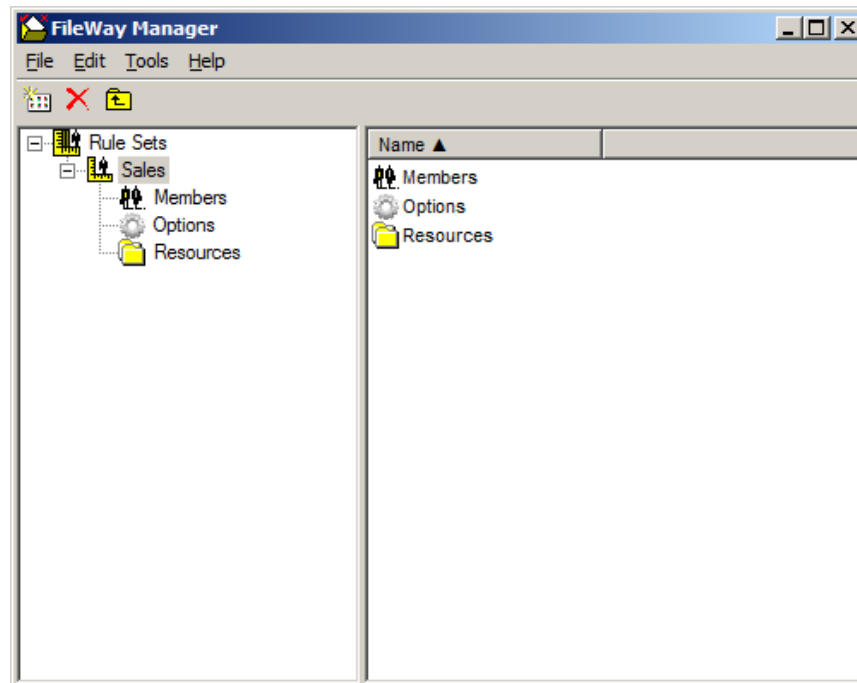
To create a Ruleset, proceed as follows:

1. Right-click the **Rulesets** icon. A pop-up menu appears.
2. In the pop-up menu, click Create Ruleset. The Create Ruleset dialog appears.





3. In the **Ruleset Name** text box, type a name for the Ruleset, for example, **Sales**. End-users will select this virtual machine to access the resources of the Ruleset.
4. Select the **Include User Home Folders** check box if you want users to be able to access their home directory.
5. The **Mail Server Type** options are automatically selected. To modify those options, see section 14.2
6. Click **Create Ruleset**. The main **FileWay Manager** window re-appears displaying the new Ruleset in the right pane.
7. Double-click the new Ruleset to expand it. The three elements of the new Ruleset appear: Members, Options and Resources. Refer to the figure below.

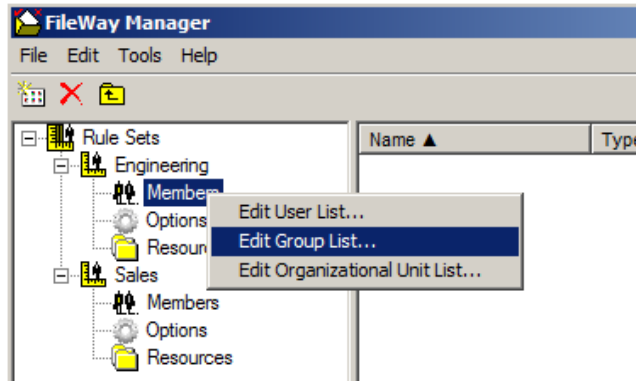


14.3.2 Adding Members to a Ruleset

Members can be AD Groups, AD Users, AD Organization Units or other Rulesets.

14.3.2.1 Adding Groups to a Ruleset

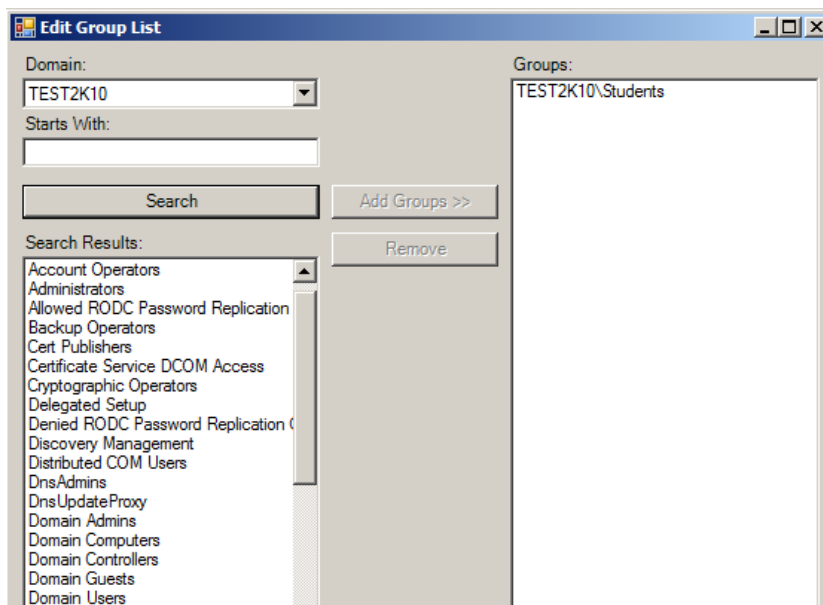
1. Right-click **Members**. A pop-up menu appears.



2. From the pop-up menu, click **Edit Group List**.

The **Edit Group List** dialog appears. Use this dialog to search for the group(s) you need, for example, Sales.

If the group of users that you would like to add is contained in an Organizational Unit (OU), then you can click **Edit Organizational Unit List**. From here you can search for the OU you need. The steps are exactly the same as they are for adding a Group.



3. Click the Domain from which you want to add a group.

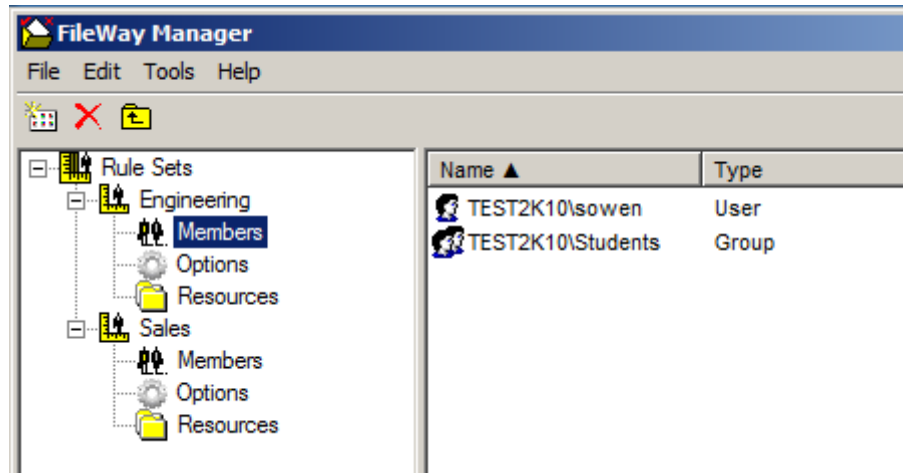
Note: Before you can select trusted domains, you must first add the trusted domains to the FileWay domain list. Refer to Section 14.6.1 Adding Trusted Domains.

4. In the **Starts With** text box of the **Edit Group List** dialog, type the name of the group you want and click **Search** to find the group in Active Directory. If you prefer to browse for the group name, type

nothing in the **Starts With** text box and click **Search**. The result of the search appears below the **Search Results** list.

5. Select one or more groups you want, and click **Add Groups**. You can also double-click a group to select it. The selected groups appear in the **Groups** list.
6. Click **OK** when you have selected all the groups you need.

The main **FileWay Manager** window reappears displaying the group(s) you just added. The domain to which the group belongs also appears.

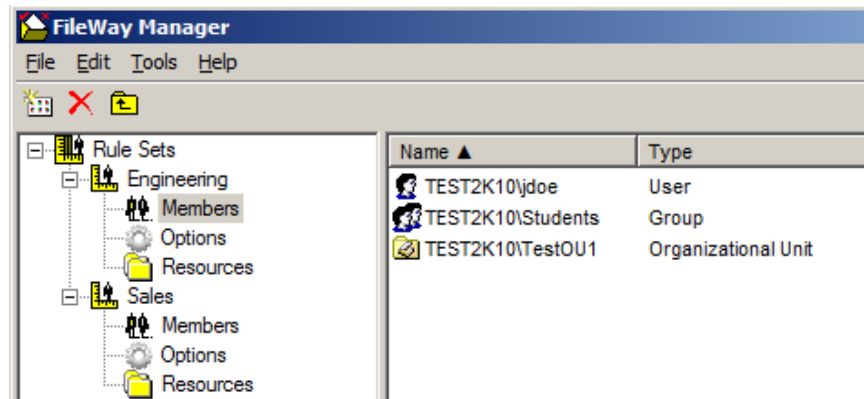


14.3.2.2 Adding Users to a Ruleset

The process for adding users is almost identical to adding groups. From the **Members** pop-up menu, click **Edit User List** and the **Edit User List** dialog appears. From that point, the process is the same as adding groups.

14.3.2.3 Adding Organizational Units to a Ruleset

The process for adding OUs is almost identical to adding groups. From the **Members** pop-up menu, click **Edit Organizational Units List** and the **Edit Organizational Units List** dialog appears. From that point, the process is the same as adding groups.



14.3.3 Adding Resources to a Ruleset

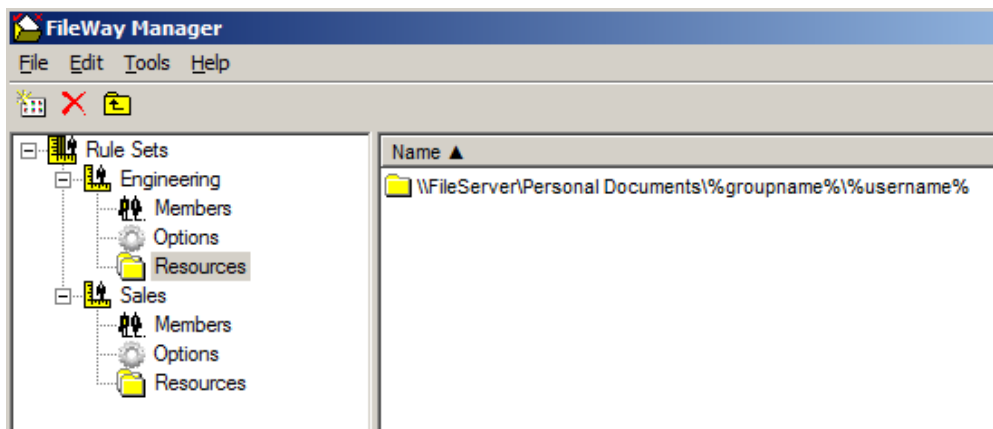
There are two approaches to specifying resources within a Ruleset:

- You may specify a computer, share or a folder within a share to be accessible by all members of the Ruleset.
- You may specify a custom resource with fields that are replaced when the resource is written to the FileWay database.

14.3.3.1 Assigning Resources to Members of a Ruleset

Proceed as follows to add resources to your Ruleset:

Note: This procedure assumes that the **Members** and **Resources** icons appear in the right and left panes for the selected Ruleset as shown below. If necessary, expand the **Rulesets** icon and/or the Ruleset you want to modify.

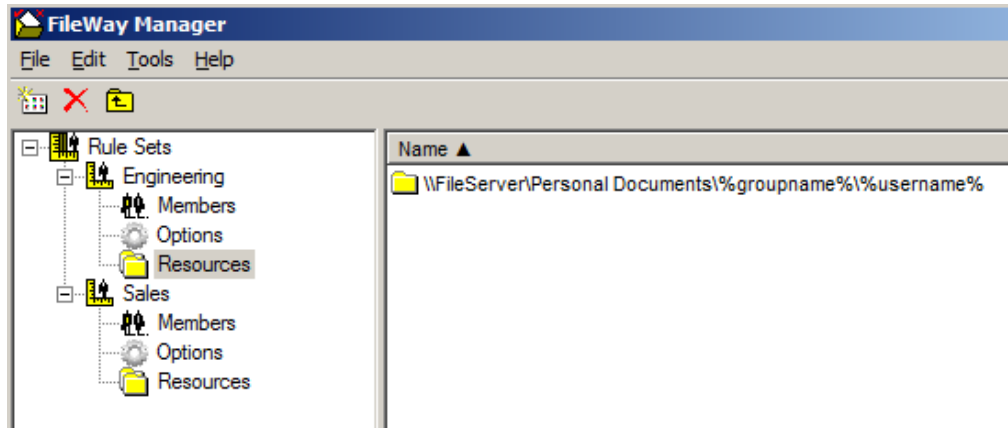


1. Right-click **Resources** and then click **Add Resources** from the pop-menu. The **Add Resources** dialog appears.



2. Expand the various items in the left pane until you locate the folder(s), share(s) or computer(s) that are applicable to your Ruleset.
3. To select a resource from this dialog, right-click the resource and click **Add Resources**. The main **FileWay Manager** window re-appears displaying the resource you added in the right pane.





Note: When you add a computer to a Ruleset's resources, only the computer's shares will be accessible to the members of the Ruleset. Also, the computer will appear to users as a network drive icon instead of a computer icon. Refer to the figure below.



At this point, you have created a Ruleset containing users and resources. Repeat the process to create more Rulesets.

14.3.3.2 Assigning Custom Resources to Members of a Ruleset

FileWay Manager provides assignable fields that you can use when assigning resources to a Ruleset. The fields are: **%groupname%** and **%username%**.

This approach simplifies the creation of custom Rulesets for individual groups or users; without the fields, you would need to create a separate Ruleset for each user and/or group.

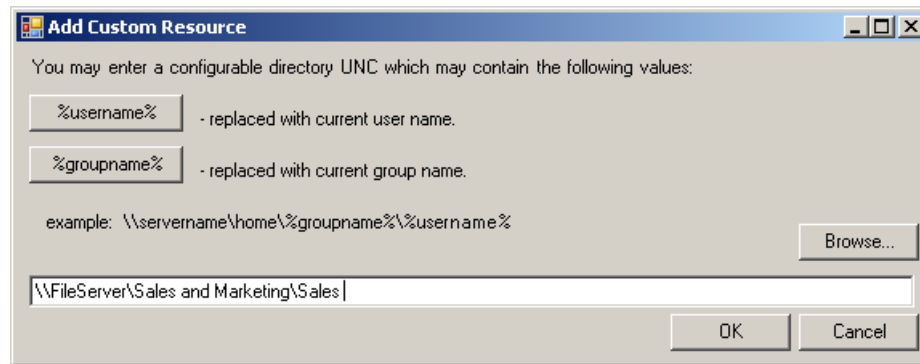
Proceed as follows to add custom resources to your Ruleset:

Note: This procedure assumes that the **Members** and **Resources** icons appear in the right and left panes for the selected Ruleset as shown below. If necessary, expand the **Rulesets** icon and/or the Ruleset you want to modify.

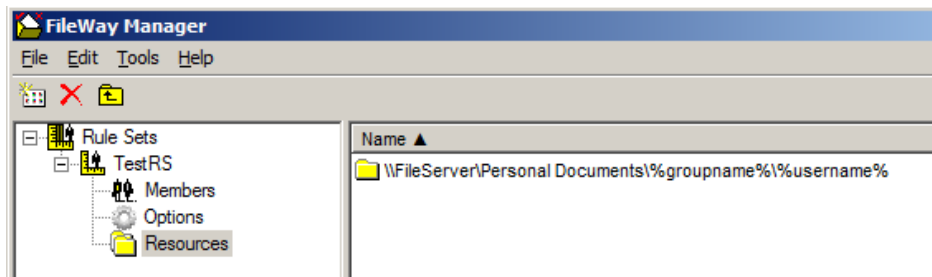
1. Right-click **Resources** and then click **Add Custom Resource** from the pop-menu. The **Add Custom Resource** dialog appears.
2. Browse to the location of the resource you want to add.
3. Once the path to the resource appears in the field at the bottom of the **Add Custom Resource** dialog, type a backslash at the end of the path.
4. Click **%username%** to insert the user name field in the resource path. This will be replaced by the current user name when the Ruleset information is written to the FileWay database. Click **%groupname%** to insert the group name field in the resource path. This will be replaced by the current group name when the Ruleset information is written to the FileWay database.



The main FileWay Manager window re-appears displaying the resource you added in the right pane.



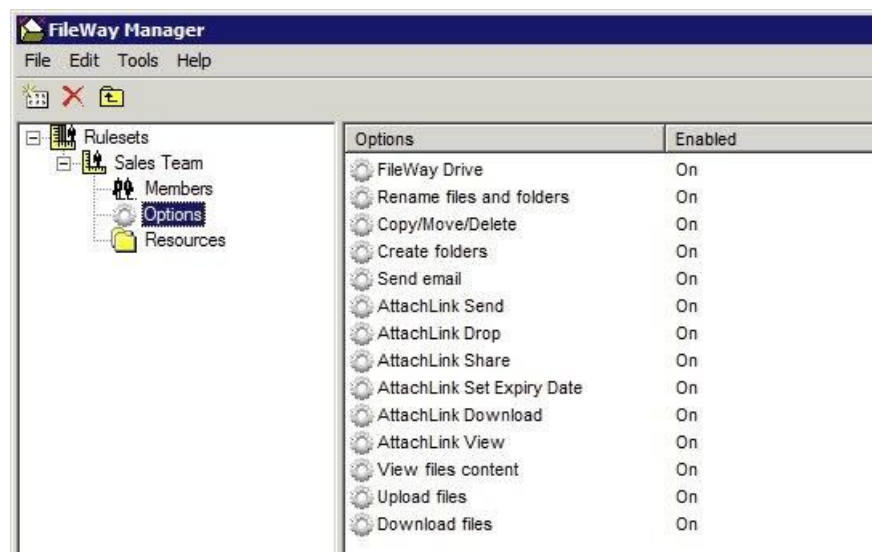
- Many users who have a large environment with many computers and users find it easier to just type in the UNC path to a resource. This can be done from the **Add Custom Resource** dialog.



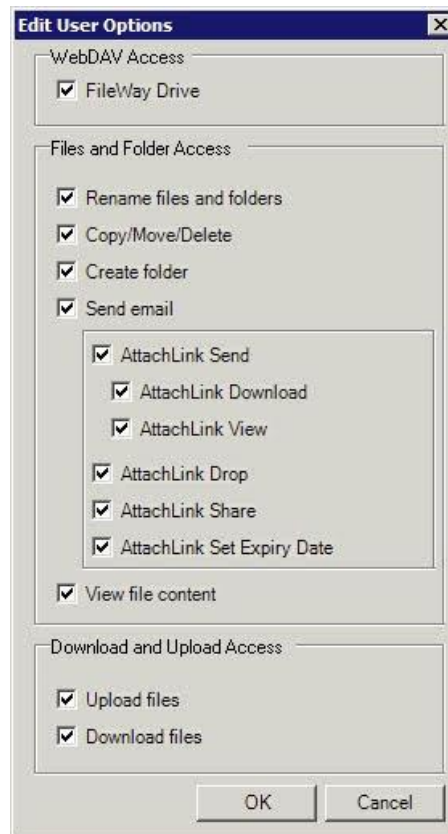
Also if you have a large environment you may know the server where your resource is located but still need to browse to find a share. You can type the server name and then click **Browse** and only the shares on that server will appear.

14.3.4 Managing Ruleset Options

Ruleset options allow administrators to specify which FileWay and FileWay Drive operations are associated with a Ruleset. Refer to the figure below.



Enable/disable each option by double-clicking the option; this toggles the value from true to false and vice versa. Alternatively, right-click **Options** to display a window with all the options with check boxes as shown in the figure below.



14.3.5 Modifying Rulesets

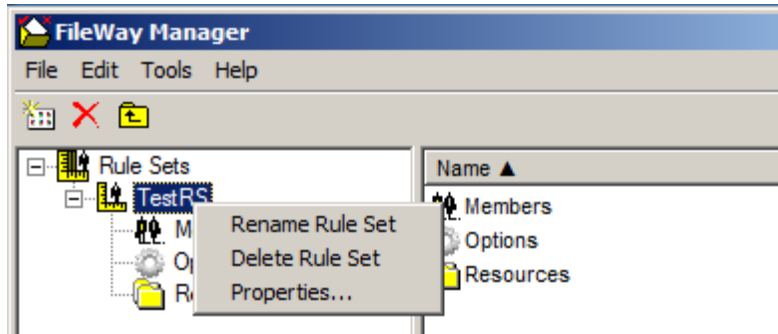
The right-click menu offers multiple options for renaming, deleting and editing the Rulesets.

You can make the following changes to a Ruleset:

- Renaming a Ruleset
- Deleting a Ruleset
- Changing Ruleset Properties
- Changing Members of a Ruleset
- Deleting a single or multiple users from a Ruleset
- Adding Resources to the Ruleset
- Deleting a single or multiple Resources from a Ruleset

Note: When you make any changes in FileWay Manager, and you want the changes to take effect immediately, update the FileWay database by selecting the following command from the **Tools** menu: **Write Configuration to FileWay Database**.





14.3.5.1 Adding or Deleting Multiple Users to or from a Ruleset

To add and/or delete multiple users from a Ruleset, proceed as follows:

1. Right-click **Members** in the left pane.
A pop-up menu appears.
2. From the pop-up menu, click **Edit User List**.
The **Edit User List** dialog appears displaying users that are already members of the Ruleset.
Use this dialog to search for the user(s) you need.
3. In the **Starts With** text box of the **Edit User List** dialog, type the name of the user that you want to add.
If you prefer to browse for the group name, type nothing in the **Starts With** text box and click **Search**.
The result of the search appears in the **Search Results** list.
4. Select one or more users that you want and click **Add Users**. You can also double-click a user to select it.
The selected users appear in the **Members** list.
5. You can delete multiple users from the Ruleset by selecting them in the **Members** list and clicking **Remove**. A verification dialog will appear asking you to confirm the deletion.
6. Click **OK** in the **Edit User List** dialog when you have selected all the users you need.
The main FileWay Manager window reappears displaying the users(s) you added.

14.3.5.2 Deleting a Single Group from a Ruleset

To delete a group, proceed as follows:

1. Right-click the group that you want to delete and then click **Delete Group**.
A verification dialog appears asking you to confirm the deletion.
2. Click **Yes**.
The main FileWay Manager window reappears displaying the remaining members in the right pane.



14.3.5.3 Adding or Deleting Multiple Groups to or from a Ruleset

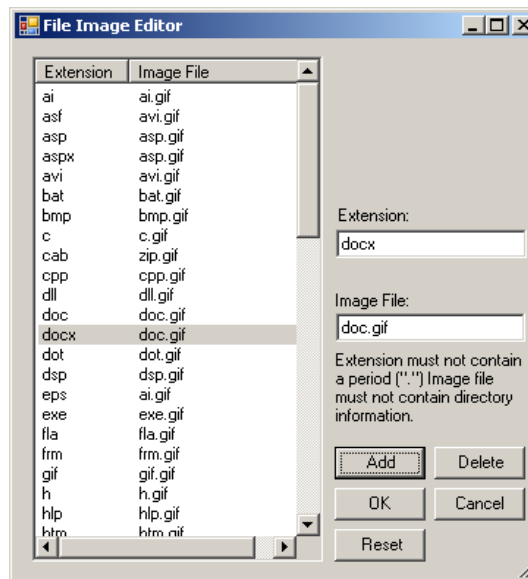
The process for adding and/or deleting multiple groups is almost identical to adding and/or deleting multiple users. From the **Members** pop-up menu, click **Edit Group List** and the **Edit Group List** dialog appears. From that point, the process is the same as adding and/or deleting multiple users.

14.4 Adding Icons for New File Types

If you notice that a certain file type does not have an icon in FileWay, you can add an icon for that file type in FileWay Manager. For example Office 2007 and later, use the extension docx for Word documents. You can associate this type of file with an icon so that it will now have the Word icon rather than a generic icon.

To associate a file type with an icon, proceed as follows:

In FileWay Manager, click **Tools** in the menu bar and then click **File Image Editor**. The following dialog appears. The database already contains a number of icons that are associated with file types.



To add a new file type, type the extension in the **Extension** text box. Then type the image file name, for example, extension docx and the Word doc icon.

Then copy the new file images to the appropriate folders on the FileWay Frontend, ENC/FileWay/FileWay FrontEnd/FileWay/Images/filetypes. You will need one image for each file type you add. Images must be 64 x 64 pixels in transparent mode.



14.5 Saving Data in FileWay Manager

To stop FileWay Manager, click **File > Exit**.

You will be prompted to update the FileWay Database. If you update the FileWay Manager database, any changes you made since the last time the database was updated will take effect. This is important if you changed access privileges in some way, for example, deleting a Ruleset.

If you do not update the FileWay Manager database, any changes you made since the last time the database was updated will only take effect the next time the FileWay Manager scheduled task is executed.

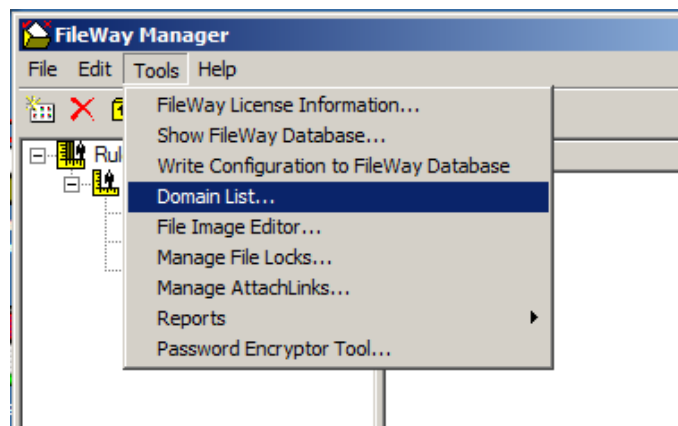
14.6 Managing FileWay Database with FileWay Manager

14.6.1 Adding Trusted Domains

When creating Rulesets, you can choose users, groups and resources from trusted domains within your organization; however, before you can access trusted domains from within FileWay, you must add the trusted domains to the list of domains that FileWay can use.

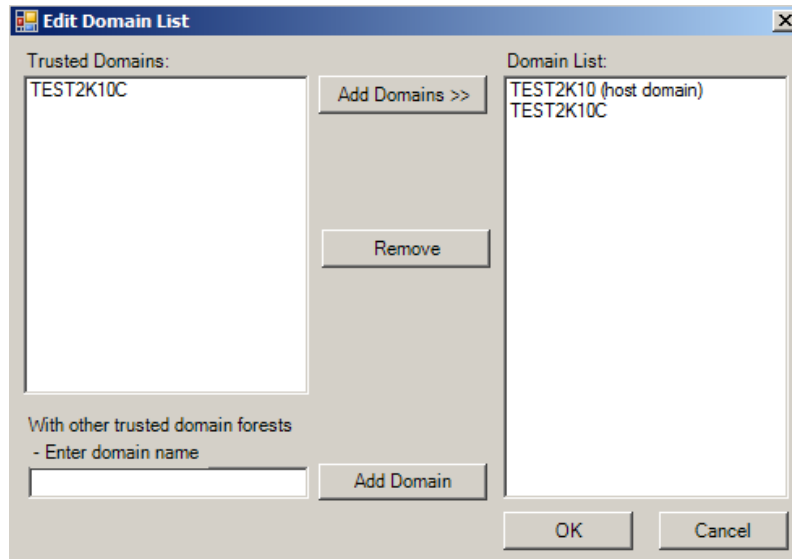
Proceed as follows:

1. Click **Tools > Domain List**.



The following dialog appears listing all the trusted domains within your organization. The host domain is the one in which FileWay is installed.





2. Select the trusted domain you want and click **Add Domains**.
If you need to add domains from the trusted domain forest, type the domain name in the **Trusted Domains** column and then click **Add Domains**.
3. You can also add domain in other trusted domain forests by typing the domain name and clicking **Add Domain**.
4. Click **OK** to finish.

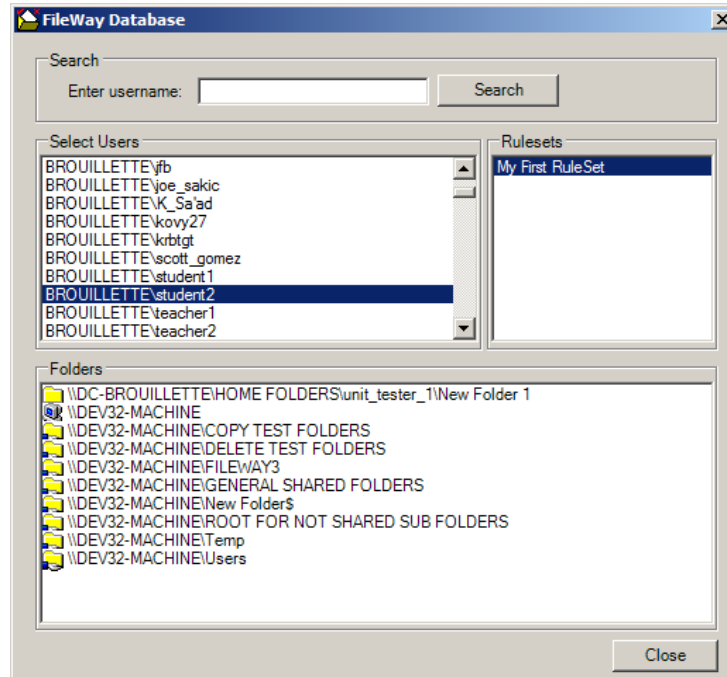


14.6.2 Viewing Current Contents of the Database

Click **Tools > Show FileWay Database** to get a quick and complete view of all Rulesets and their members and resources, as well as individual users and their virtual machines and resources. Refer to the figure below.

Note: You should update the FileWay Manager database before viewing the contents of the database in this manner. Viewing the database in this way allows you to quickly check whether changes you made in FileWay Manager were written to the database.

Viewing the database is useful for debugging purposes, for instance, to check if a certain user has access to a certain resource.



14.6.3 Updating the Database with Latest Changes

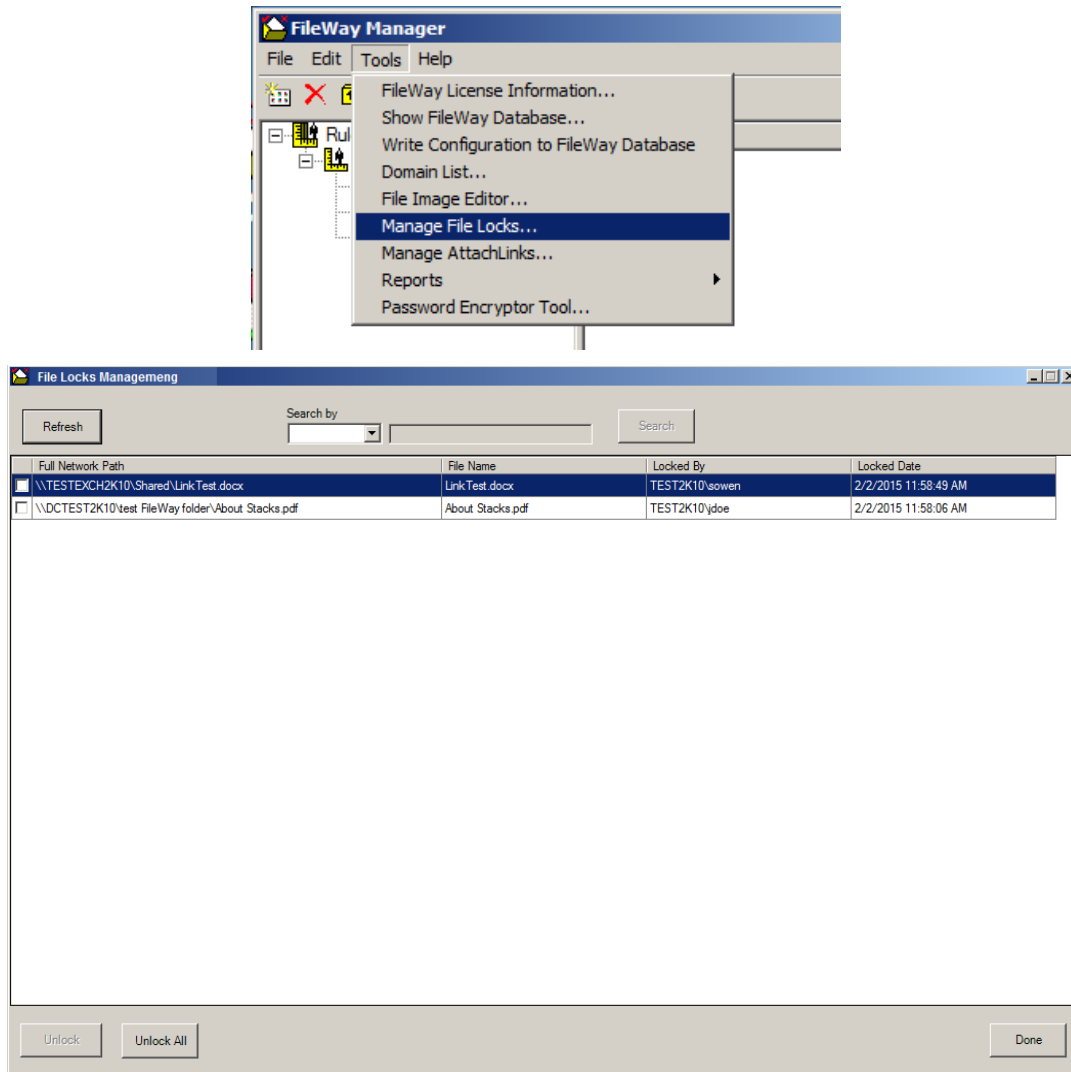
When you make any changes in FileWay Manager, and you want the changes to take effect immediately, update the FileWay database by clicking **Tools -> Write Configuration to FileWay Database**.

If changes are made to Active Directory that impact FileWay, for example, removal of users or groups, run **Write Configuration to FileWay Database**. If you find that the changes were not propagated to FileWay Manager, Active Directory will need to be closed and re-opened.

14.6.4 Manage File Locks

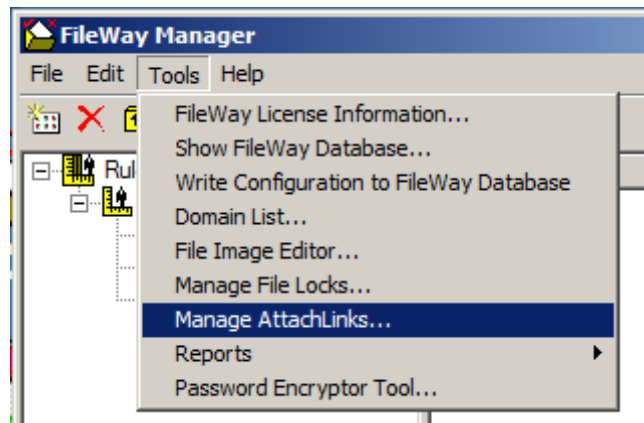
Some WebDAV clients allow users to lock/unlock files. Some of them also allow users to open, edit and save documents. Opening a file will lock it; saving it will unlock it. A locked file can only be unlocked by the user who locked it. Administrators can manage File Locks through FileWay Manager as shown in the figure below.

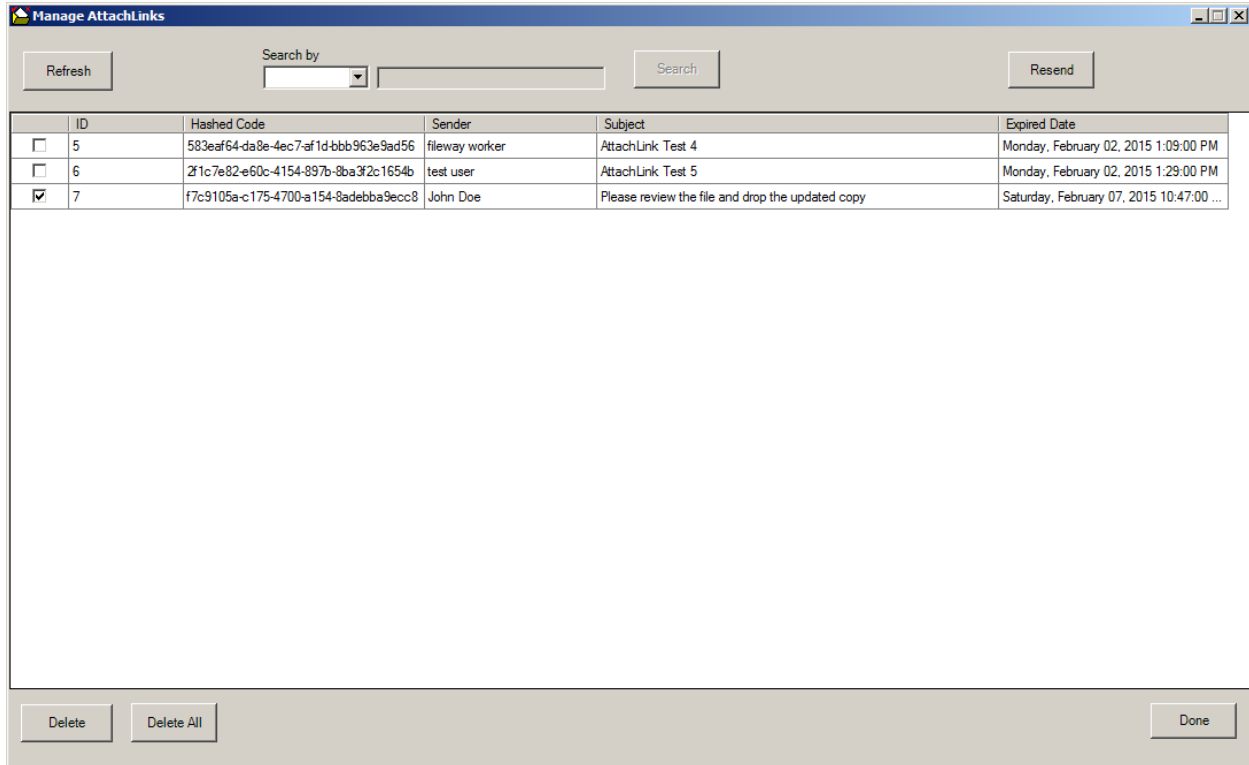




14.6.5 Manage AttachLinks

Administrators can manage AttachLinks through FileWay Manager as shown in the figure below.

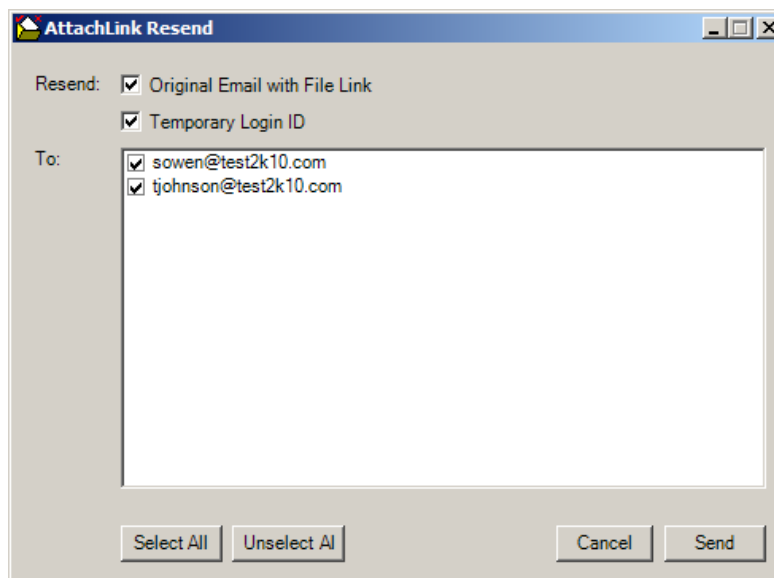




The Administrator can delete selected AttachLinks by selecting the checkboxes and clicking **Delete**.

Clicking **Delete All** will delete all AttachLinks.

If AttachLink Email is not received by recipients, the Administrator can resend the original email with the File Link and/or the Email with Temporary Login ID. To resend an AttachLink, select an item from the list and click **Resend**.

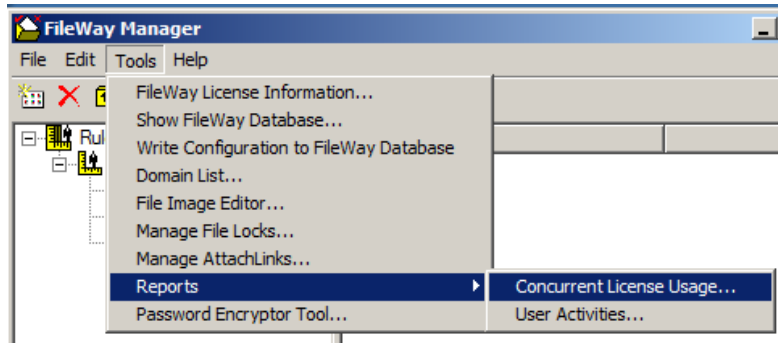


The Administrator can choose what to send and which recipients to send to.

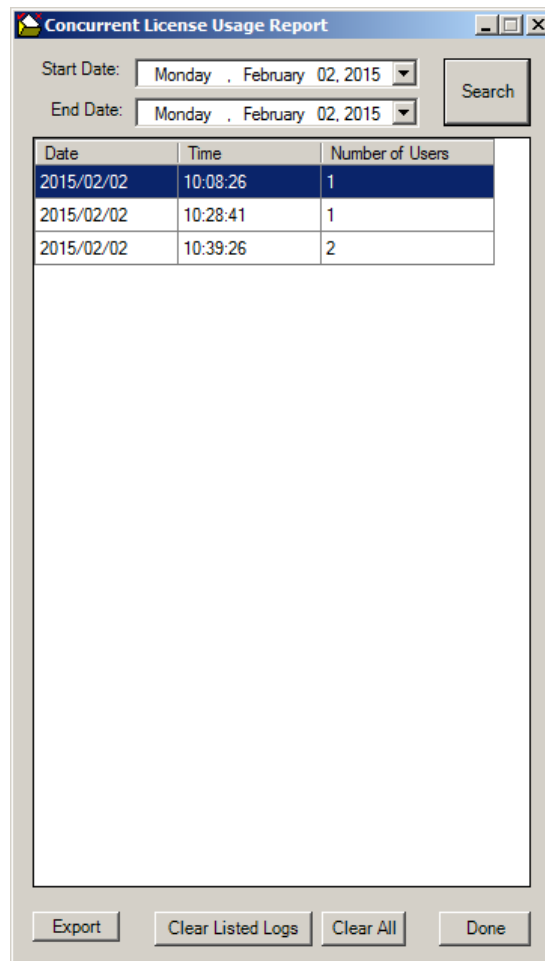


14.6.6 Manage Logs

The Administrator can generate reports on Concurrent License Usage or User Activities and export those reports to CSV format files.



See figures below to view the reports.



Concurrent License Usage Report Dialog



User Activity Report

Start Date: Monday, February 02, 2015
End Date: Monday, February 02, 2015

Search

Date	Time	Domain	User Name	Action	Method	File Name	Folder Name	Path	New Name	New Path	AttachLink Ref #
2015/02/02	10:08:13	TEST2K10	TESTUSER	Logout	Browser						
2015/02/02	10:08:26	TEST2K10	TESTUSER	Login	Browser						
2015/02/02	10:28:41	TEST2K10	JDOE	Login	Browser						
2015/02/02	10:38:34	TEST2K10	JDOE	Login	Browser						
2015/02/02	10:39:26	TEST2K10	SOWEN	Login	Browser						
2015/02/02	10:39:55	TEST2K10	SOWEN	Create	Browser		My Docs	\\DCTEST2K10\test FileWay folder			
2015/02/02	10:43:08	TEST2K10	SOWEN	Login	Browser						
2015/02/02	10:45:54	TEST2K10	SOWEN	Login	Browser						
2015/02/02	10:46:08	TEST2K10	SOWEN	Upload	Browser	README.txt		\\TESTEXCH2K10\Shared\			
2015/02/02	10:47:03	TEST2K10	JDOE	Login	Browser						
2015/02/02	10:47:39	TEST2K10	JDOE	Upload	Browser	LinkTest.docx		\\TESTEXCH2K10\Shared\			
2015/02/02	10:49:40	TEST2K10	JDOE	Email	AttachLink Send	LinkTest.docx	Shared	\\TESTEXCH2K10\Shared\LinkTest...			REF_007
2015/02/02	10:49:40	TEST2K10	JDOE	Email	AttachLink Drop		FileWay Drop Folder	\\TESTEXCH2K10\Shared\FileWay ...			REF_007
2015/02/02	10:59:28		SOWEN@TEST2K10.COM	Login	AttachLink						
2015/02/02	10:59:43	TEST2K10	SOWEN@TEST2K10.COM	View	AttachLink	LinkTest.docx		\\TESTEXCH2K10\Shared\LinkTest...			REF_007
2015/02/02	10:59:47		SOWEN@TEST2K10.COM	Download	AttachLink	LinkTest.docx		\\TESTEXCH2K10\Shared\LinkTest...			REF_007
2015/02/02	11:00:35		SOWEN@TEST2K10.COM	Upload	AttachLink	LinkTest.docx		\\TESTEXCH2K10\Shared\FileWay ...			REF_007
2015/02/02	11:00:36		SOWEN@TEST2K10.COM	Notification Email	AttachLink Drop	LinkTest.docx		..FileWay Drop Folder\REF_007\sow...			REF_007
2015/02/02	11:00:36		JDOE@TEST2K10.COM	Notification Email	AttachLink Drop	LinkTest.docx		..FileWay Drop Folder\REF_007\sow...			REF_007

Export Clear Listed Logs Clear All Done

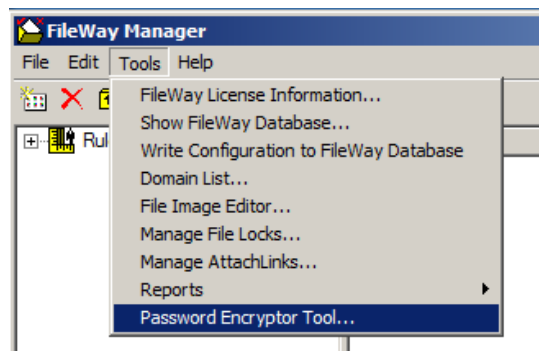
User Activities Report Dialog

The Administrator can display logs by date, and then click **Export** to generate the report in CSV format files. Reports will be placed in the **\Program Files (x86)\ENC\FileWay\FileWay BackEnd\FileWayLog** folder, and can be opened with Microsoft Excel.

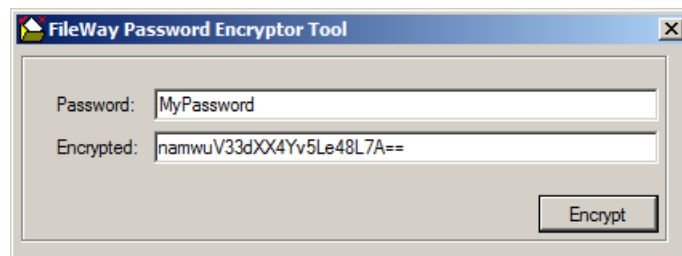
The Administrator can also clear selected logs by clicking **Clear Listed Logs**, or all logs by clicking **Clear All**.

14.6.7 Password Encryptor

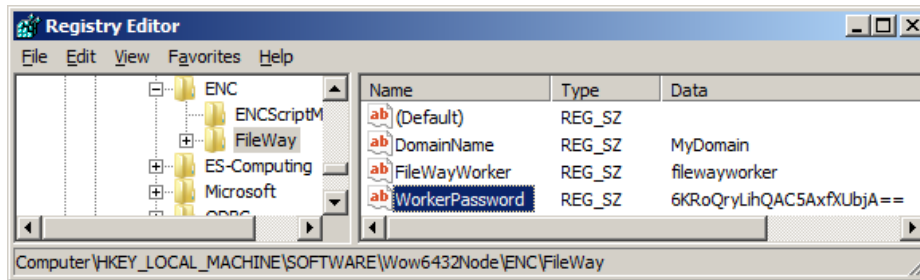
FileWay Worker's username and encrypted password are saved in FileWay Registry Keys. If the password is changed, the registry key must be changed.



In the **FileWay Password Encryptor Tool** dialog, type the new password and click **Encrypt**.



Then, update the value of **Worker Password** in FileWay Registry Key:
 Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ENC\FileWay,



and Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ENC\FileWay.

