FileOpen Systems

FileOpen RightsManager

Manual Version 2.14

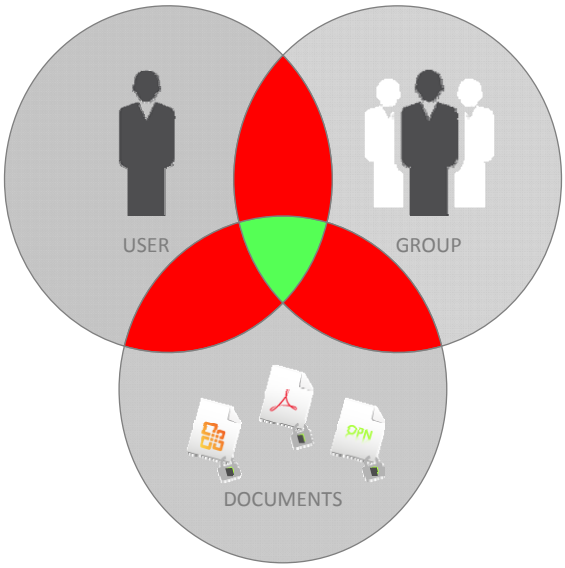
FileOpen RightsManager

FileOpen RightsManager contain a set of tools that may be used to control the opening and use of data stored in Adobe® Portable Document Format (PDF) or FileOpen's OPN format. The system is designed to provide document security and digital rights management (DRM), by enabling an author/Administrator to grant certain users document access and privileges, while granting different or denying privileges to other users. The system works by performing three processes:

- Encryption of Documents
- Authentication and authorization of Users based on User/Document/Group association
- Policy enforcement across multiple file formats and device platforms

The FileOpen software operates by enabling access to specific Documents for specific Users/Devices based on the relevant Groups/Policies. The fundamental rule is that a User may open a Document only if the User and the Document are both members of the same Group.

Figure 1: Group Overview



In addition to the User/Document/Group interaction, the system also supports a variety of additional controls to safeguard digital information from unauthorized use–both online and offline, inside and outside of the firewall. Administrators can define exactly how the recipient can use the information, such as who can open, modify, print, and/or take other actions with the information.

Sampling of Online and Offline Permissions

	Watermarking	Offline Watermarking
	Print Prevention / Restrictions	Offline Print Prevention / Restrictions
	Print Metering	Offline Print Metering
	Screenshot Prevention	Offline Screenshot Prevention
	Embargo	Offline Embargo
	Expiration by Time / Term	Offline Expiration by Time / Term
	Expiration by Date	Offline Expiration by Date
	Expiration by Use – View / Print	Offline Expiration by Use - Open
	Text Edit Prevention	Offline Text Edit Prevention
	Copy Prevention / Restrictions	Offline Copy Prevention / Restrictions
	Save Prevention	Offline Save Prevention
	Page-level View Restrictions	Offline Page-level View Restrictions
	Page-level Print Restrictions	Offline Page-level Print Restrictions
	Page-level Searching	Offline Page-level Searching

Concepts and Terms

An **Administrator** is an entity using a FileOpen solution to protect documents and enforce acceptable use policies.

RightsManager is a hybrid on-premise / cloud solution that allows businesses to encrypt documents on-premise, but authenticate users and manage policies through a cloud-based FileOpen PermissionServer.

PermissionServer is the central component of both the FileOpen RightsManager solution. The PermissionServer is defined as a Web-accessible module that supports the FileOpen client/server protocol. This module handles inbound Client requests and responds with well-formed protocol messages containing decryption keys, permission values and response messages. Additional functionality to handle print control, usage notifications, watermarking, message encryption, etc. may also be included. The syntax of the protocol is described in the FileOpen Developer Toolkit manual, available as part of the evaluation distribution or upon request.

The **WebUI** is a browser-based interface that allows Administrators manage Users, Documents, and Policies within their PermissionServer.

A **User** is a document recipient. Users are known to the system by their email address. Users may be members of Groups and from this membership obtain permissions. A User may be granted permission to open Documents on an arbitrary number of machines, though in practice only a small number of machines will typically be allowed; thus for practical purposes a User may be defined as that person's machine(s).

A **Document** is a PDF or OPN file encrypted by the system for protection. Documents are associated with Groups, and a User's ability to interact with a given Document is determined by the permissions granted to the Group with which that Document is associated.

A **Group** is a collection of Users and Documents governed by the same Policy Set. FileOpen software operates by enabling access to specific Documents for specific Users/Devices based on the relevant Groups/Policies. There is no limit to the number of Groups that maybe created, nor is there is a restriction to the number of (Dynamic) Groups to which a Document may belong, so an Administrator may create Groups as needed and according to whatever criteria is appropriate.

A **Dynamic Group** delivers Permission Policies for each document in the collection individually.

A **Static Group** delivers Permission Policies for all documents in the collection at once (e.g. permission list). Static Groups are valuable when granting Offline Permissions. The User must only authenticate / authorize once to receive the permissions for all files in the Group.

Important: Documents encrypted into Static Groups cannot be encrypted into a Dynamic Group and then moved into a Static Group. Documents may be moved between Dynamic Groups, but not in or out of Static Groups.

Online Permissions are those granted in real time by the PermissionServer. Such permissions are defined at the level of the Group through a Policy Set. Permissions may be added or revoked at any time, with the changes taking effect the next time a User opens a Document in that Group. Users must have an active internet connection to use Online Permissions.

Offline Permissions are granted by the PermissionServer during an initial Online interaction, and then stored on the User's local machine. Users with Offline Permissions may open files whether or not they have an active internet connection. Offline Permissions take precedence over Online Permissions, and the actions of users with Offline Permissions will not be logged, unless Offline Inverted Permissions were granted.

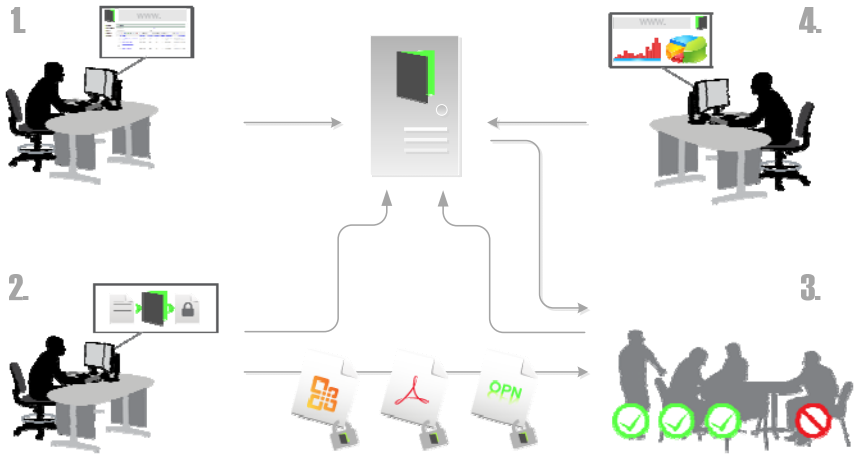
Offline Inverted (Auxiliary) Permissions are a combination of Online and Offline Permissions designed to permit the opening of files when a user who is ordinarily connected to the internet is temporarily offline. When Offline Inverted

Permissions are granted and the user has an active internet connection the system will use Online Permissions, but if the user has no internet connection the system will use Offline Permissions.

Architectural Overview

FileOpen RightsManager architecture is made up of a family of tools, applications, clients and native viewers. These tools all work together with a common PermissionServer to perform four primary processes: *provision document controls*, *encrypt documents*, *decrypt documents* and *enforce document use policy*. The general process is outlined in the Figure 2 below:

Figure 2: Architectural Overview



1.

The Administrator starts by Online Permissions **are those granted in real time by the PermissionServer. Such permissions are defined at the level of the Group through a Policy Set. Permissions may be added or revoked at any time, with the changes taking effect the next time a User opens a Document in that Group. Users must have an active internet connection to use Online Permissions.**

Offline Permissions **are granted by the PermissionServer during an initial Online interaction, and then stored on the User's local machine. Users with Offline Permissions may open files whether or not they have an active internet connection. Offline Permissions take precedence over Online Permissions, and the actions of users with Offline Permissions will not be logged, unless Offline Inverted Permissions were granted.**

Offline Inverted (Auxiliary) Permissions **are a combination of Online and Offline Permissions designed to permit the opening of files when a user who is ordinarily connected to the internet is temporarily offline. When Offline Inverted Permissions are granted and the user has an active internet connection the system will use Online Permissions, but if the user has no internet connection the system will use Offline Permissions.**

Defining Groups and Policy Sets within the PermissionServer using the WebUI. Administrator then imports Users and assigns them to the appropriate Group(s). This association governs how Users authenticate and what document-level permissions are applied.

2.

The Administrator then encrypts documents and associates document identifiers with their appropriate Groups in the PermissionServer[1]. Encryption may be performed individually or in batches through the Directory Monitor (Watched Folder) or the Command Line Encryptor. Once the document is encrypted, it can be securely distributed through whatever mechanism or

[1] Document content is never stored in the PermissionServer, just document identifiers.

	protocol is most appropriate. It is not necessary for the communication path to be secure since the document is intrinsically secure.
3.	When a User attempts to open the FileOpen-protected document, the appropriate FileOpen Clients & Viewers are invoked.[2] The Client communicates with the PermissionServer via HTTPs to authenticate the User and request the decryption key. If the User is authorized, the PermissionServer sends the decryption key and applicable Permission Policies to the client. When the User opens a Document, the User's machine identifiers are recorded within the PermissionServer as a Registered Machine; which, can later be leveraged to avoid multiple log-in prompts. The Client then opens the Document and then discards the decryption key. In this manner, the system can enforce changes in permission's and group memberships in real time[3].
4.	Administrators may also monitor Document and User activity through RightsManager WebUI.

System Components

Administrator Tools:

- **FileOpen WebUI** is a browser-based interface that allows Administrators to create Policies, manage Users and Documents, and monitor usage. Administrators may also configure options such as Authentication Policies, Watermarks, Message Sets, etc.
- **FileOpen Outlook® Add-in** is an application designed to create and distribute User/Device registration email messages without leaving Outlook.
- **FileOpen Command Line Encryptor** is a text-based user interface that encrypts documents and allows Group/Policy designation.
- **FileOpen Directory Monitor** is a drag-and-drop GUI application that encrypts documents and allows Group/Policy designation.
    - **FileOpen OPN Converter/Encryptor** is available through the Directory Monitor module, and converts standard PDF files into a custom viewer format called OPN. The OPN file format is fundamentally an implementation of the SWF file format and is designed to display protected documents to Users, in any Web browser running Adobe Flash Player version 11 or higher.
    - **Viewer.fileopen.com** is an optional service available with the Directory Monitor that publishes protected document to a dedicated webpage**.**

Clients & Viewers: Freely available clients or native applications that enable authorized Users access to FileOpen-protected documents.

- **FileOpen Plug-in for Adobe Reader/Acrobat** is a lightweight plug-in that provides authorized Users access to FileOpen-protected PDF documents in Adobe Acrobat and Reader
- **FileOpen Viewer™** allows authorized Users to access FileOpen-protected documents within a Web browser running Adobe Flash® Player version 11 or higher — no plug-ins or additional software required.
- **FileOpen Viewer for iPad and iPhone** is a native iPad/iPhone application that enables authorized Users access to FileOpen-protected documents.
- **FileOpen Viewer for Android** Distribute secure documents to display on Android tablets and phones.

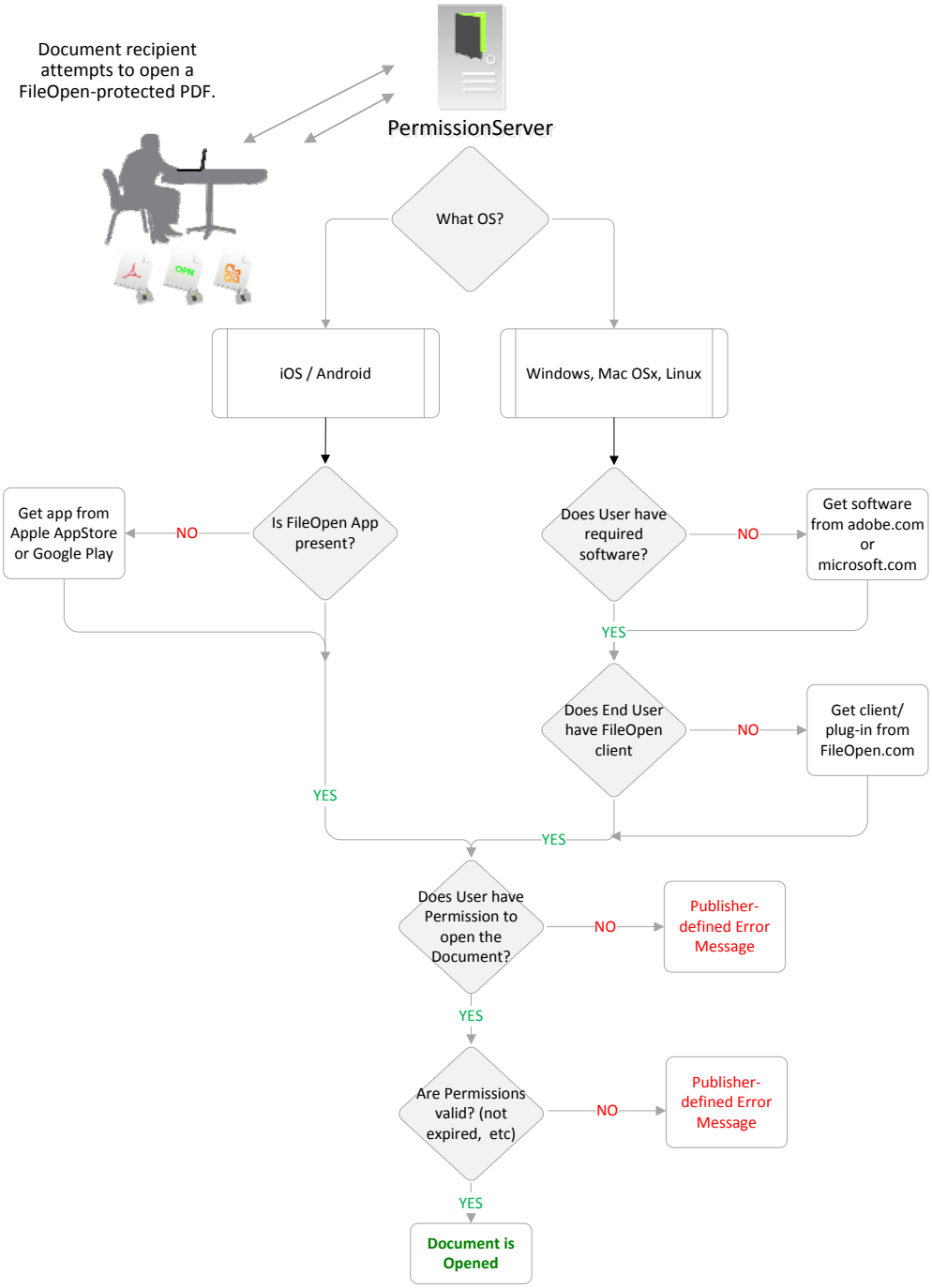
[2] If a FileOpen Client is required and is missing, the User is prompted to install the client.

[3] Permission cannot be edited or revoked if the User has been granted offline permissions and does not re-establish internet activity. See Online and Offline Permissioning for more information.

General Decryption Process

The decryption & permissioning process involves two steps: the installation of required software, which may include Adobe Flash Player, Adobe Reader/Acrobat, a FileOpen Client, and the acquisition of Permission from the PermissionServer and/or local machine.

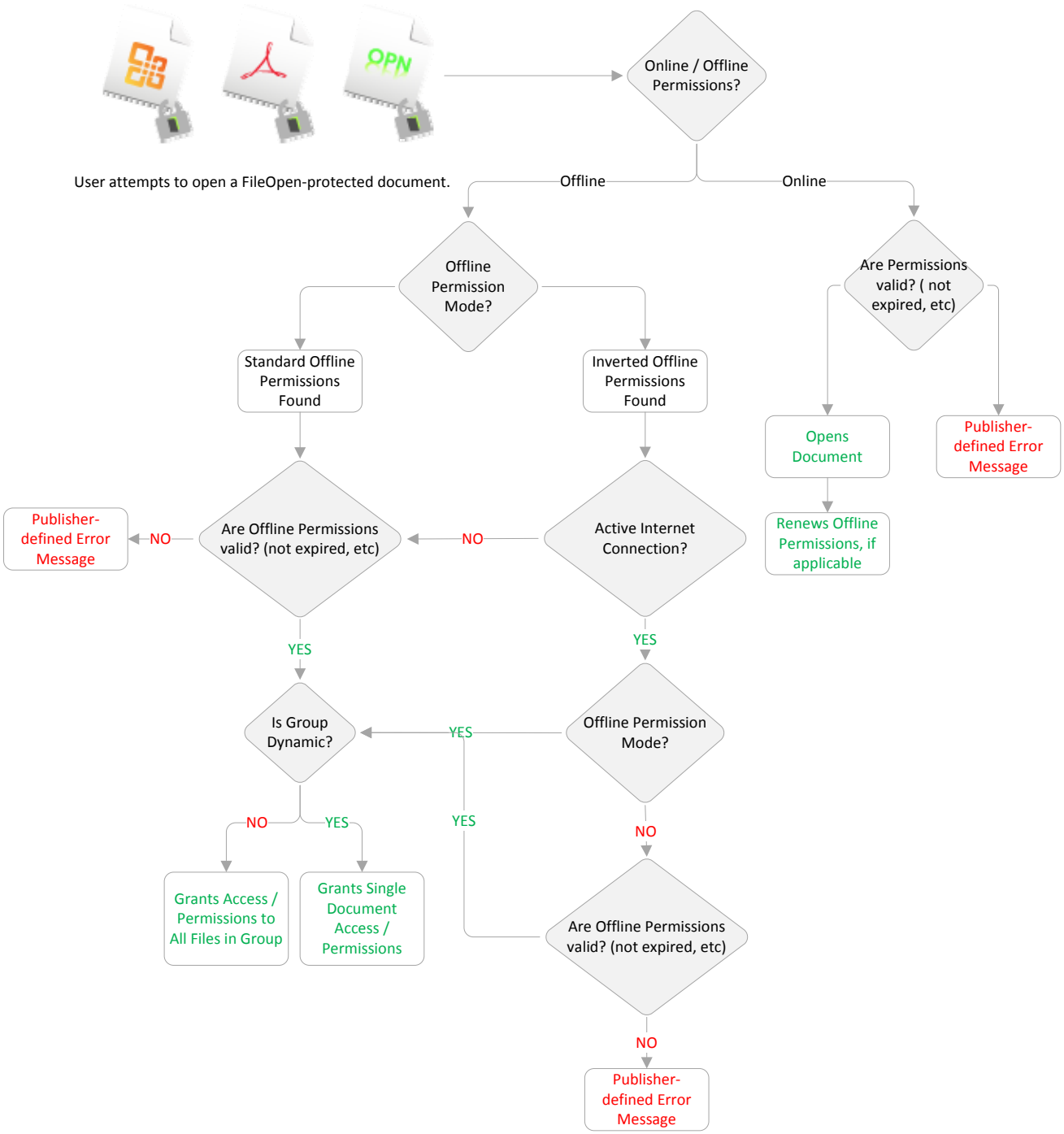
Figure 3: General Decryption Process



General Permissioning Process

Given the presence of the required software, the system performs either a local search for Permission for Offline Permissions or a client/server interaction with the PermissionServer for Online Permission. If Offline Inverted Permission has been granted the client will perform the online interaction only in the case where the machine has an active internet connection and the PermissionServer is reachable.

Figure 4: General Permissioning Process



Operating the WebUI

The FileOpen WebUI allows licensees of FileOpen RightsManager solution to create Policies, manage Users and Documents, and monitor usage. This guide explains how to use the FileOpen WebUI and describes the behavior of the default interface. Your installation might be customized. If so, the interface items you see might not always correspond to those described in this manual.

The following sections describe the process by which Policies, Groups, Users and Documents may be managed via the WebUI.

Groups

Group Concepts and Terms

A **Group** is a collection of Users and Documents governed by the same Policy Set. FileOpen software operates by enabling access to specific Documents for specific Users/Devices based on the relevant Groups/Policies. There is no limit to the number of Groups that maybe created, nor is there is a restriction to the number of (Dynamic) Groups to which a Document may belong, so an Administrator may create Groups as needed and according to whatever criteria is appropriate.

A **Dynamic Group** delivers Permission Policies for each document in the collection individually.

A **Static Group** delivers Permission Policies for all documents in the collection at once (e.g. permission list). Static Groups are valuable when granting Offline Permissions. The User must only authenticate / authorize once to receive the permissions for all files in the Group.

Important: Documents encrypted into Static Groups cannot be encrypted into a Dynamic Group and then moved into a Static Group. Documents may be moved between Dynamic Groups, but not in or out of Static Groups.

Online Permissions are those granted in real time by the PermissionServer. Such permissions are defined at the level of the Group through a Policy Set. Permissions may be added or revoked at any time, with the changes taking effect the next time a User opens a Document in that Group. Users must have an active internet connection to use Online Permissions.

Offline Permissions are granted by the PermissionServer during an initial Online interaction, and then stored on the User's local machine. Users with Offline Permissions may open files whether or not they have an active internet connection. Offline Permissions take precedence over Online Permissions, and the actions of users with Offline Permissions will not be logged, unless Offline Inverted Permissions were granted.

Offline Inverted (Auxiliary) Permissions are a combination of Online and Offline Permissions designed to permit the opening of files when a user who is ordinarily connected to the internet is temporarily offline. When Offline Inverted Permissions are granted and the user has an active internet connection the system will use Online Permissions, but if the user has no internet connection the system will use Offline Permissions.

Defining Groups

A “Group” may be considered as a “product” or a “collection”, though other categorizations are possible. There is no limit to the number of Groups that may be created, nor is there is a restriction to the number of (Dynamic) Groups to which a Document may belong, so an Administrator may create Groups as needed and according to whatever criteria is appropriate.

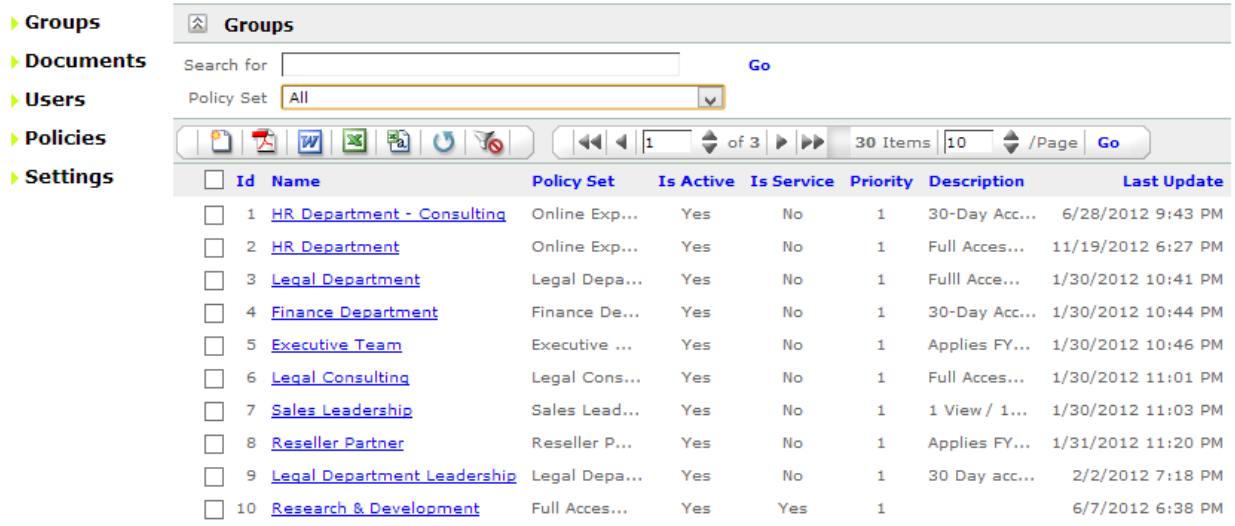
Here are some possible approaches:

> A newsletter publisher with two different publications might create a separate Group for each, in order that Users might be able to subscribe to one publication separately from the other, or to subscribe to both simultaneously. This approach may be described as “Content-defined Grouping”.
>
> An Administrator might choose to define Groups based on Permissions, e.g. a “Gold” Group offering unlimited viewing and printing, a “Silver” Group with fewer privileges, and a “Demo” Group with still fewer privileges. If the groups are Dynamic, then a given document may be included in all three Groups, thus permitting users to receive different permissions to the same document based on the Group to which they have been assigned. This approach may be described as “Permission-defined Grouping”.
>
> An Administrator distributing Documents as part of a subscription might elect to define Groups based on the length of subscription, e.g. to have one Group for single-year subscriptions and others for subscriptions of different lengths. This approach may be described as “Time-defined Grouping”.
>
> An Administrator distributing documents to a set of Users who are themselves categorized into sub-groups may choose to define Groups based on those existing categorizations, e.g. to have a group for employees in the Marketing Department and another Group for employees in Finance. This approach may be described as “Role-defined Grouping”.

This is not, of course, an exhaustive list, and Administrators may define additional methods as needed. For example, the above methods may be combined to increase specificity (One-year Gold Access to Newsletter #1, etc.)

Locate a Group

1. Navigate to Groups
2. Do one of these:
    a. Sort Groups by column headings, select the number of items to display, scroll through pages to find Users.
    b. In the search field, type information about the Group, and then click Search.
    c. Filter by associated Policy Sets.



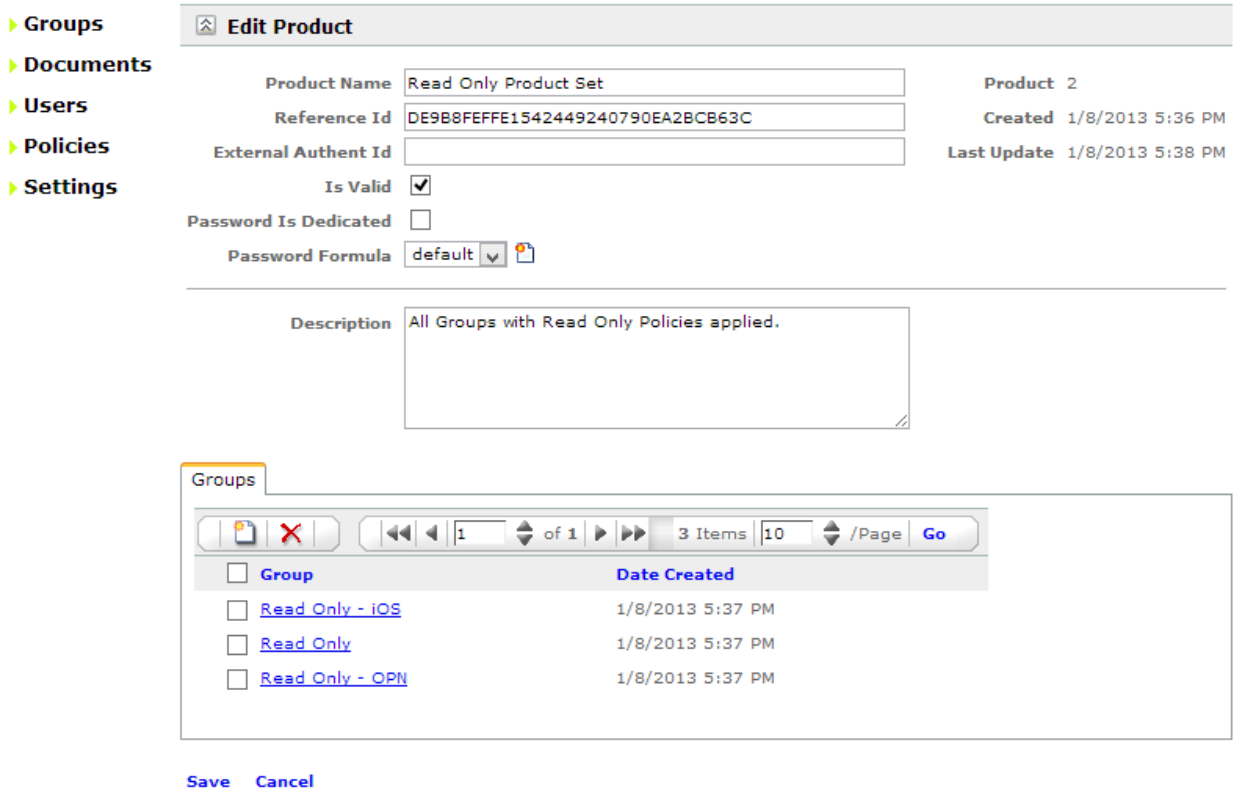
Note: A complete listing of Groups may be downloaded from this screen by selecting the file type download button above the column headings.

Add or create a Group

1. Navigate to Groups > Add Group
2. Populate Name – each Group is required to have a unique Name.
3. Select pre-configured Policy Set from the pull down menu – select the new/add icon  to create a new Policy Set. For more information on creating policies, see Policy Sets.
4. The checkbox Is Service indicates a Group is static. A static Group is defined as a collection of files that is defined by identifiers in the Documents themselves. Documents encrypted into a Static / Service Group may not be removed from that Group, nor may they be moved to another Group. Offline Permission may be given to all the files in a static Group in a single operation, and unless this is a requirement use of Static Groups is not recommended.
5. Select the Priority of the Group if appropriate. The Group's priority determines which Policies to enforce when a Document is in more than one Group with possibly conflicting Policies. That is, if a User who is a member of two Groups attempts to open a Document that is also a member of those two Groups the system will grant the Permissions from the Group with the highest Priority. If no priority is set then the earliest Group will take Priority. Priority is assigned numerically, with 1 being the highest priority, 2 being next, etc.
6. Reference ID is an optional internal classification field that can be used as the Administrator sees fit.
7. Log URL should be populated with a Web page you wish Users to receive as a result of a failed attempts to open a file.
8. The Description field is an optional internal classification field that can be used as the Administrator sees fit.

Group>Products

Product Groups allow Administrators to compile a collection of Groups into a unified product view. Implementation of Product Groups requires the FileOpen eCommerce Add On license and professional services. Contact us for more information.



Group Properties

Field	Description
Name (Group)	(Mandatory) Unique identifier for each Group.
Policy Set	A Policy Set defines a set of security policies associated to a Group (collection of Documents and Users). A policy set is composed of an Authentication Policy, a Permission Policy, a Minimum Client Set and Watermark Set.
Is Active (Group)	The checkbox Is Active controls the global state of the Group; if unchecked the Group is disabled and all Users associated with the Group will be denied Online Permission or the renewal of Offline Permissions to Documents contained in the Group.
Is Service	The checkbox Is Service indicates a Group is Static. A Static Group is defined as a collection of files that is defined by identifiers in the Documents themselves. A Static Group is useful in the case where the Administrator wishes to distribute files as a collection, and give User's Offline Permission to all those files in a single operation. Documents encrypted into a Static / Service Group may not be removed from that Group, nor may they be moved to another Group. Offline Permission may be given to all the files in a static Group in a single operation.
Priority	The Group's priority determines the appropriate Permissions to provide when a document is in more than one Group. That is, if a User who is a member of two Groups attempts to open a Document that is also a member of those two Groups the system will grant the Permissions from the Group with the highest priority. Priority is assigned numerically, with 1 being the highest priority, 2 being next, etc.

Reference ID	Reference ID is an optional internal classification field that can be used as the Administrator sees fit
Log URL (Group)	The URL / Web page an Administrator may route failed attempts to open a file.
Description	Optional field to be used as deemed appropriate.
Products (Group)	Product Groups allow Administrators to compile a set of Groups into a unified product for delivering documents with a diverse set of policies. Implementation of Product Groups requires the FileOpen eCommerce Add On license and professional services.

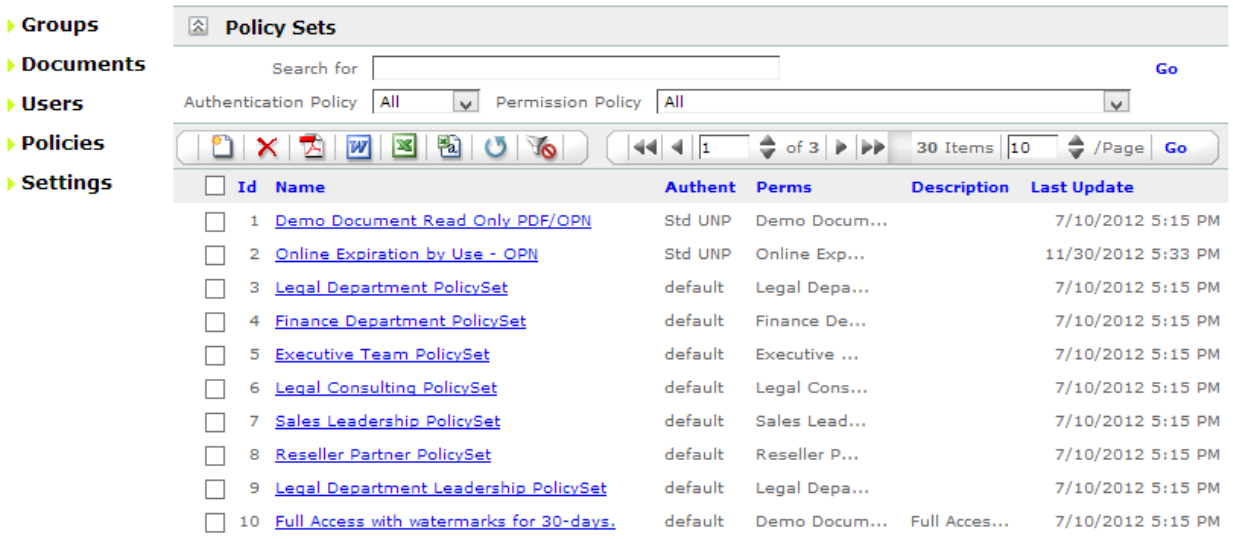
Figure 5: Group Properties

Policy Sets

Each Group is governed by a Policy Set that determines who can access the Document and what document-level permissions are applied. A policy set is composed of an Authentication Policy, a Permission Policy, a Minimum Client Set, a Message Set and Watermark Set all detailed below.

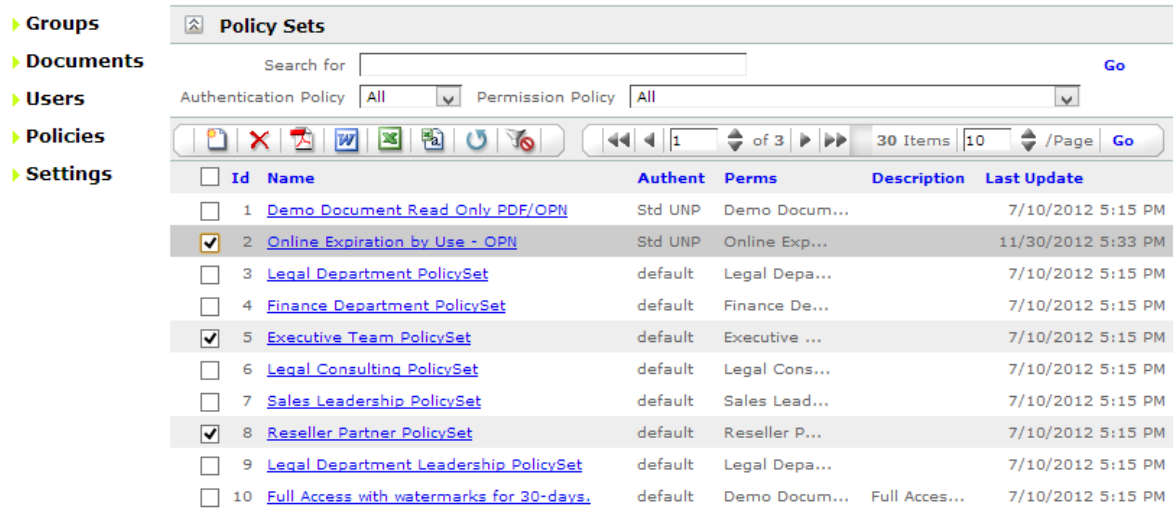
Locate a Policy Set

1. Navigate to Policies > Show Policy Set
2. Do one of these:
    a. Sort Documents by column headings, select the number of items to display, scroll through pages to find Document.
    b. In the search field, type information about the Policy Set, and then click Search.
    c. Filter by Last Updated, Authentication Policy or Permission Policy.



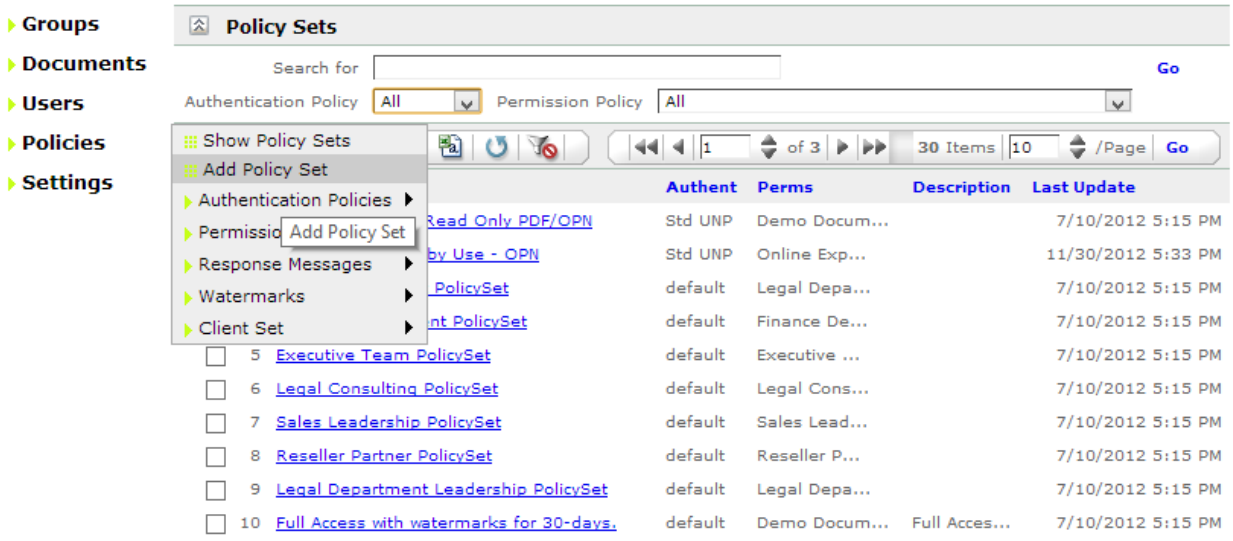
Delete a Policy Set

Administrators may delete Policy Sets by checking the boxes next to the Policy Set Id then click the Delete button. This action cannot be undone.

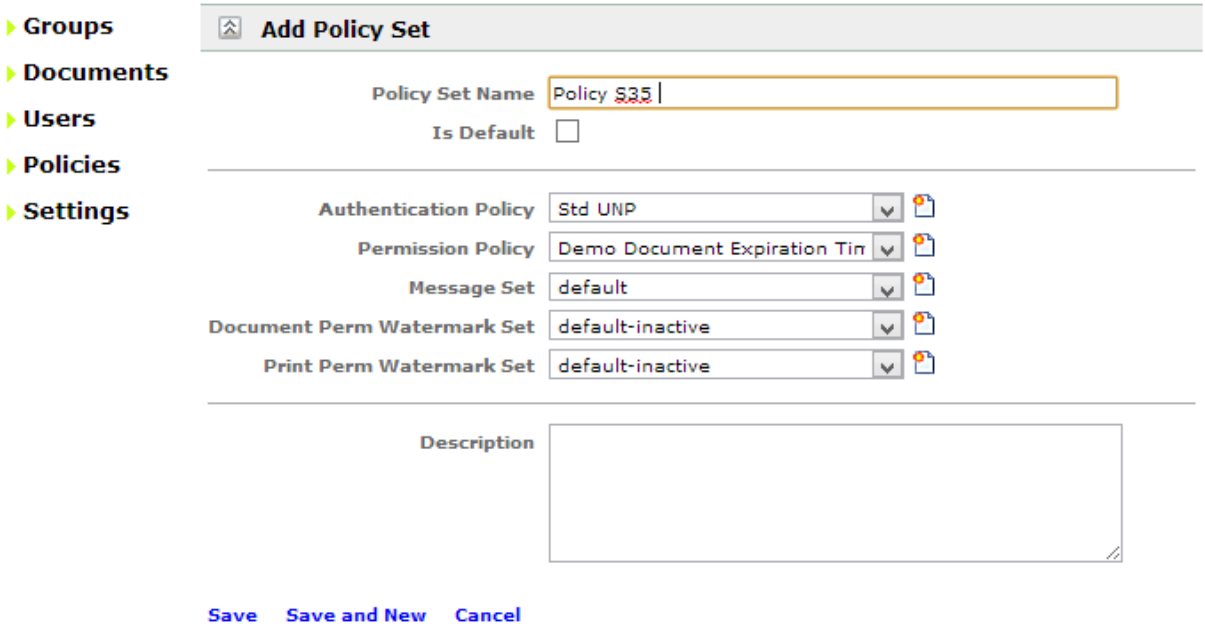


Add or Create a Policy Set

1. Navigate to Policies > Add Policy Set



2. Input a unique Policy Set Name.
3. Select an Authentication Policy from the pull down menu or select the new/add icon  to create a new Authentication Policy. For more information see, Authentication Policies.
4. Select a Permission Policy from the pull down menu or select the new/add icon to create a new Permission Policy. For more information see, Permission Policies.
5. Select a Message Set /Response Message Set from the pull down menu or select the new/add icon to create a new Message Set. For more information see, Message Sets / Response Messages.
6. To apply Watermarks each view of documents protected by this policy set, select a DocPerm Watermark Set. For more information see, Watermarks.
7. To apply Watermarks to a printed instance of documents protected by this policy set, select a PrintPerm Watermark Set from the pull down menu. For more information see, Watermarks.


Groups
Documents
Users
Policies
Settings
Add Policy Set
Policy Set Name
Policy S35
Is Default
Authentication Policy
Std UNP
Permission Policy
Demo Document Expiration Tin
Message Set
default
Document Perm Watermark Set
default-inactive
Print Perm Watermark Set
default-inactive
Description
Save
Save and New
Cancel

Authentication Policies

To access a FileOpen-protected Document a User must authenticate — prove to the system that they are who they say they are and have the proper authorization (Group membership). Default Authentication modes are Machine and User-based authentication. However, FileOpen software can employ additional means of authentication beyond the default pair.

Supported Authentication Modes:

- Machine Authentication is one of two default authentication modes delivered with RightsManager solution. With this mode, Users authenticate once and PermissionServer logs Machine identifiers for that User. All subsequent requests by that User / Machine combination are processed by validating one or more of the machine context identifiers; which, can later be leveraged to avoid multiple log-in prompts.
- User-based Authentication (Username/password) is also a default authentication mode delivered with RightsManager. This mode presents a dialog to the User and requests credentials. The UNP strings are not stored in the document, but rather are both defined and validated by the PermissionServer, so may be issued and withdrawn at will.
- Cookie-based Authentication is intended for use with a webserver. That server must deposit a cookie onto the local machine, and the document must contain a description of that cookie sufficient to enable the client to retrieve that cookie.[4]
- Doc Path URL Authentication allows Administrators to define a URL for encrypted Documents. When a User clicks on the defined URL, the PermissionServer checks the destination URL and choose to automatically authentication that User based on the client response.
- Domain Authentication allows Administrators to define acceptable Domains for traffic to encrypted Documents. When a User attempts to access a file, the PermissionServer checks the referring Domain and automatically authentications that User based on the client response.
- User log-in authentication (Machine Log-in) allows Administrators to leverage machine credentials in User authentication.[5]

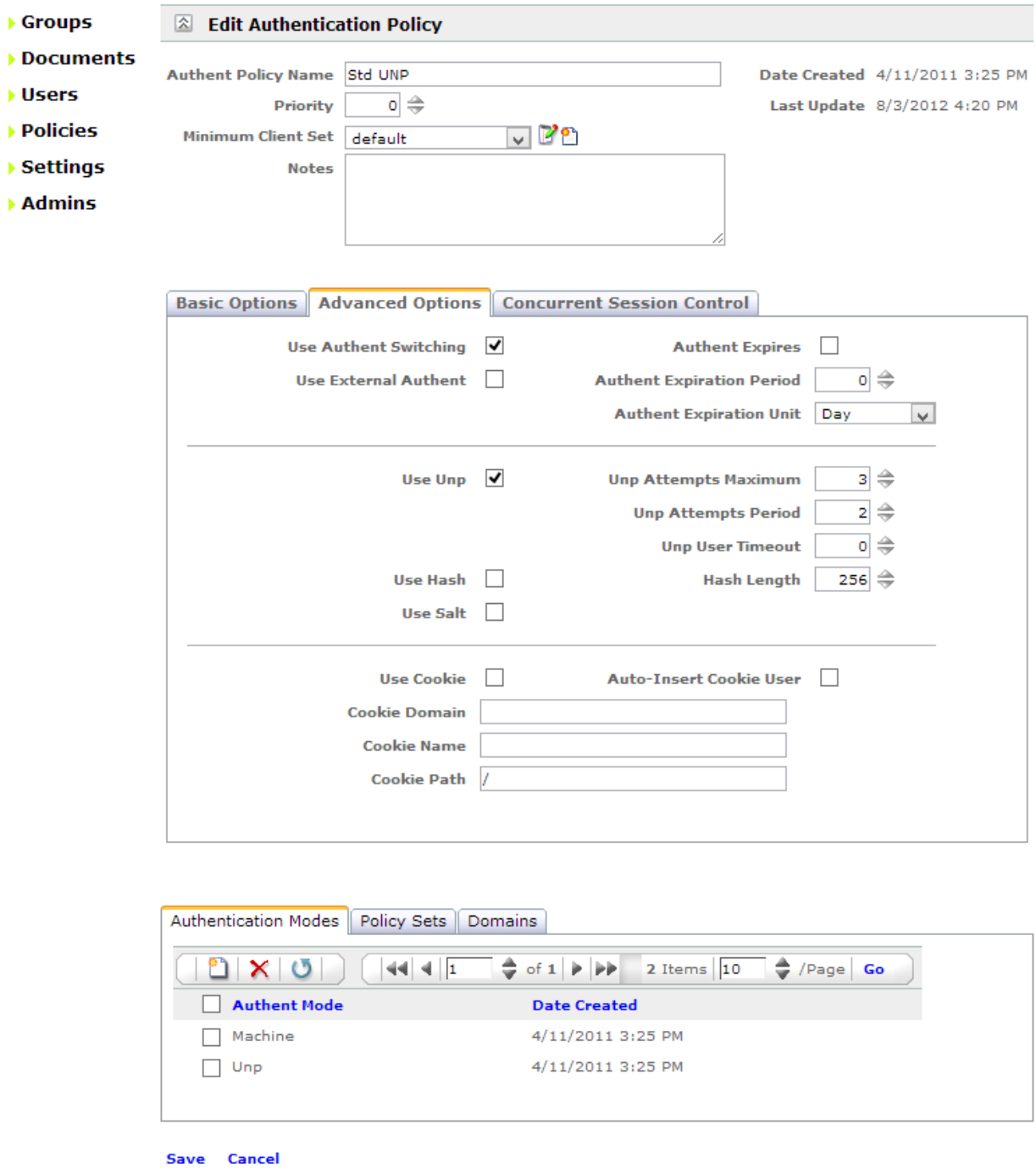
Authentication Switching

FileOpen software also supports conditional Authentication modes, called Authentication Switching. As an example, an Administrator may use Authentication Switching when they wish to use Cookie-based Authentication when the document is being delivered from the webserver but leverage User-based Authentication when the document is accessed from local storage.

As mentioned above, FileOpen RightsManager is delivered with two default authentication modes. The User-based Authentication mode deploys both standard Username/Password Authentication, as well as Machine Authentication, through Authentication Switching. The first time a User authenticates with Username/Password the PermissionServer records the Users machine identifiers. All subsequent attempts to access a protected document the User will not be prompted for credentials as long as the client/server interaction can validate the Machine identifiers previously collected.

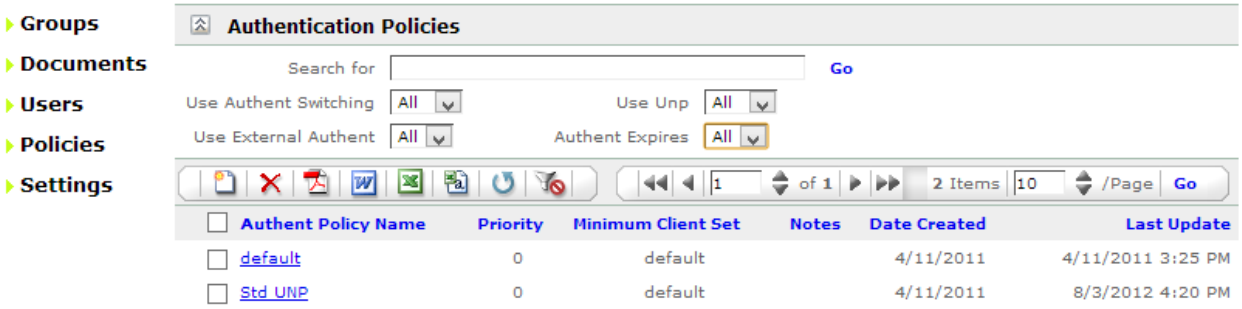
[4] Cookie authentication is not supported by the FileOpen PermissionServer without customization.

[5] External authentication is not supported by the FileOpen PermissionServer without customization.



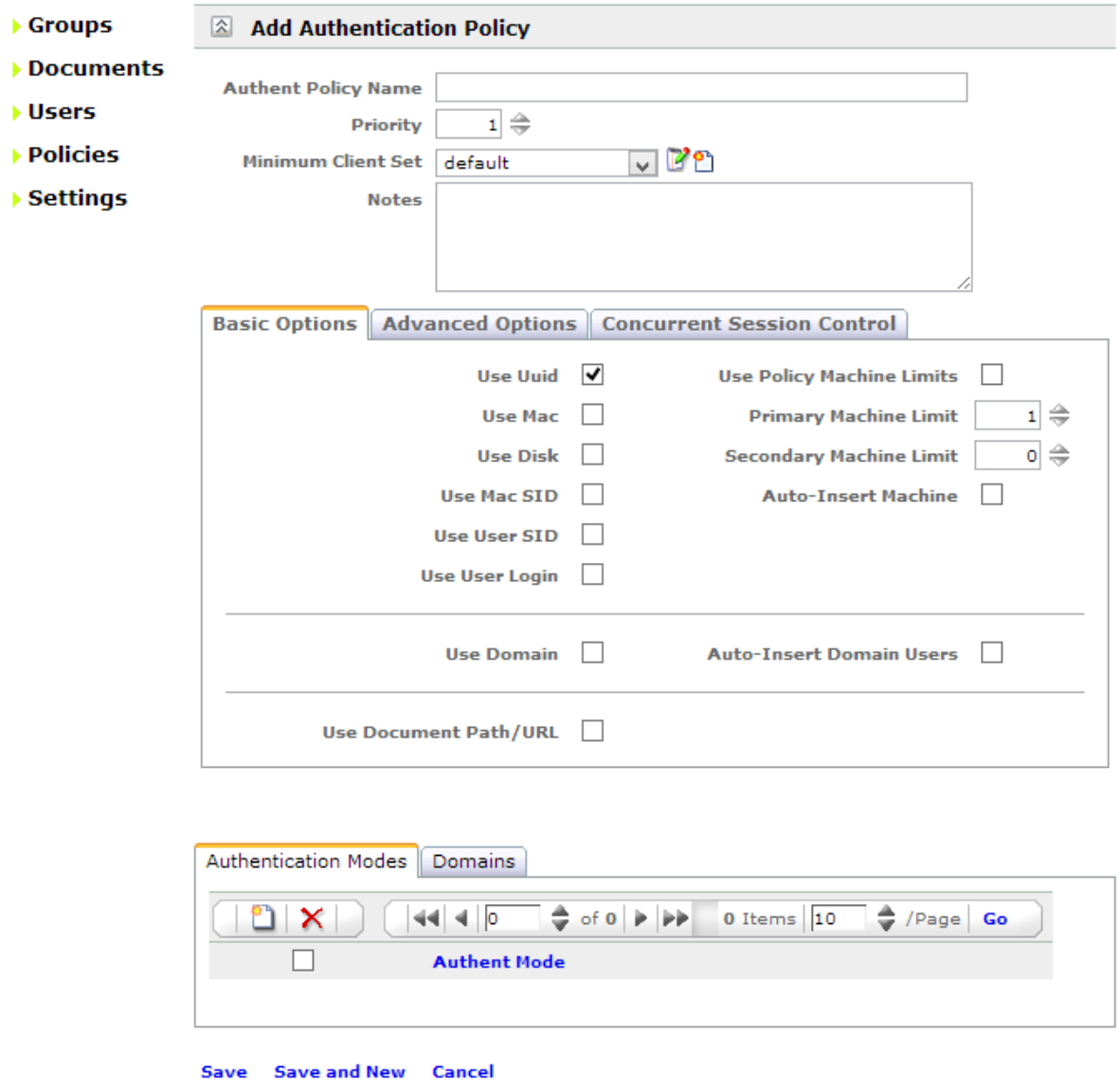
Locate an Authentication Policy

1. Navigate to Policies > Authentication Policies
2. Do one of these:
    a. Sort Authentication Policies by column headings, select the number of items to display, scroll through pages to find the Policy you are looking for.
    b. In the search field, type information about the Authentication Policy, and then click Search.
    c. Filter by Authentication Switching, External Authentication, Authentication Expires, and Use Unp.



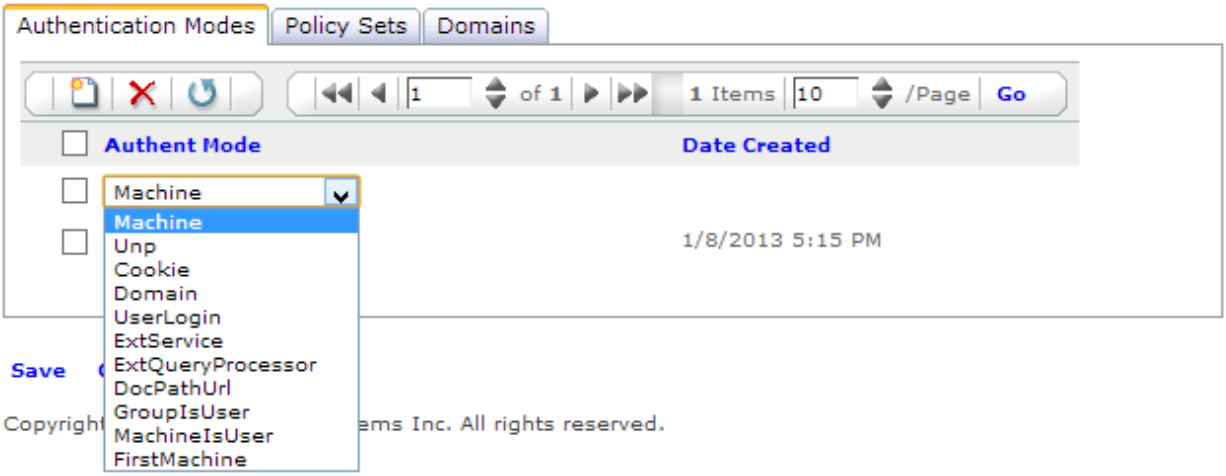
Add or create an Authentication Policy

1. To Add a new Authentication policy navigate to Policies > Authentication Policies > Add Authentication Policy

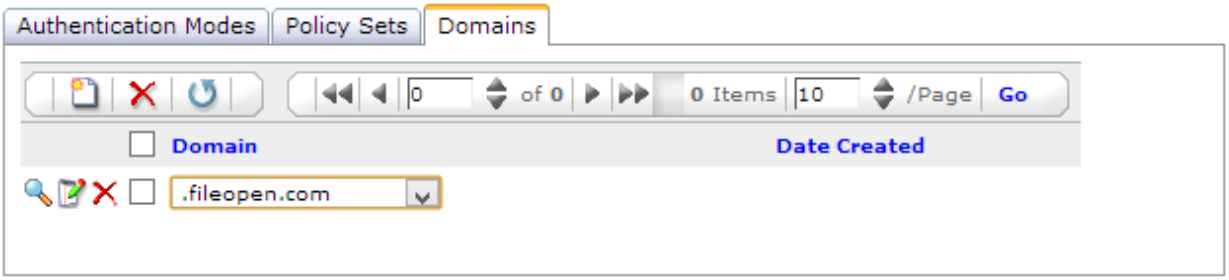


1. Input an Authentication Policy Name.
2. Priority for the Authentication Policy is **deprecated** and will be removed from the interface.

3. Set the Minimum Client Set required for Authentication. Note: Minimum client set can also be set at the Permission Policy level. If there is ever a conflict the highest build number wins.
    i. Visit http://plugin.fileopen.com for the latest client releases.
    ii. Visit http://www.fileopen.com/blog/?Tag=Client+Release for the latest features released with each client release.
4. Specify the appropriate Basic Options, Advanced Options and Concurrent Session Control Properties. For complete field list and definition. For field values and definitions, see Authentication Policy Properties.
2. Select the Authentication Mode you are configuring from the drop down menu.



3. If configuring Domain Authentication select the preconfigured domain from the pull down menu. New domains may be added from the new/add icon  .



Edit an Authentication Policy

To Edit an Authentication policy navigate to Policies > Authentication Policies and click on the Authent Policy Name.

Authentication Policy Properties

Field	Description
Use Uuid	This option enables client applications to use machine authentication when connecting to the server. A Universally Unique Identifier created the first time the FileOpen client loads. This will be different for each User. It should never change, but could in principle be

	deleted by the User and in that case would be re-generated.
Use Mac	This option enables client applications to use machine authentication when connecting to the server. A MachineID which is built using a part of the MAC address of the first card having a MAC address. It will be the same for all Users of the machine, but may change if the network connection type if changed (e.g. the machine goes from a wired connection to a wireless one, or vice versa)
Use Disk	This option enables client applications to use machine authentication when connecting to the server. A DiskID is built from the identifier of the first disk (the volume number written on the disk when it is hard formatted) and CPU data. It will be the same for all Users of the machine.
Use Mac SID	This option enables client applications to use machine authentication when connecting to the server. The Microsoft Windows operating systems Machine Security ID (SID). In the case of Apple OSx, a Machine UDID is used.
Use User SID	This option enables client applications to use machine authentication when connecting to the server. The Microsoft Windows operating systems User Security ID (SID).
Use User Login	This option enables client applications to use Operating System Login when authenticating with the server. In order to User Login Authentication to be used the User Login must be populated in the User record.
Use Policy Machine Limits	Enable a maximum allowable count of machines that a User can register per this policy. Note: If you enable Machine limits for an authentication policy it will override User level machine limits. However, the Policy machine limit will not disable machines already registered per your User Machine Limit.
Primary Machine Limit	This option enables Administrators to set the primary machine limit by policy. Note: If you enable Machine limits for an authentication policy it will override User level machine limits. However, the Policy machine limit will not disable machines already registered per your User Machine Limit.
Secondary Machine Limit	For use in a shared machine environment where the User may not have their own login on that machine. Note: If you enable Machine limits for an authentication policy it will override User level machine limits. However, the Policy machine limit will not disable machines already registered per your User Machine Limit.
Auto-insert Machine	If an Authentication mode other than Machine Authentication is used then the machine information will be collected and used to generate a new User record. If a

	User record already exists then this option is ignored.
Use Domain	This option enables client applications to use predefined domains to authenticate with the server.
Auto-Insert Domain Users	If an Authentication mode other than Domain Authentication is used then the domain and machine information will be collected and used to generate a new User record. If a User record already exists then this option is ignored.
Use Document Path/URL	This option enables client applications to use predefined Document Path URLs to authenticate with the server. Document URLs must be appended to each document record.
Use Authentication Switching	This option allows Administrators to set conditional Authentication modes. For example, in the case where an Administrator wishes to use cookie authentication when the document is being delivered from the webserver but Username/password authentication when the document is accessed from local storage.
Use External Authentication	This option enables client applications to use an external authentication scheme. Configuration of External Authentication requires professional services.
Authentication Expires	This option enables external authentication expiration.
Authentication Expiration Period	This option allows Administrators the ability to set an external authentication expiration period.
Authentication Expiration Unit	This option allows Administrators the ability to set an external authentication expiration unit. E.g. day, week, month, quarter or year.
Use Unp	Select this option to enable client applications to use Username/password authentication when connecting to the server.
Unp Attempts Maximum	Allows Administrators the ability to set the maximum Username and Password.
Unp Attempts Period	Timeframe (in minutes) for which maximum Username/password combinations can be attempted.
Unp User Timeout	Minutes that must be waited between password attempts to avoid timeout.
Use Hash	Cryptographic hash function that takes a string of any length (password) as input and produce a fixed-length hash value to be compared with the stored hash value.
Hash Length	The desired length of the hash value returned.
Use Salt	Enables random values to be concatenated into a hash to ensure each hash is unique.
Use Cookie	This option notifies client applications to identify and authenticate using Cookies passed from the Administrator's Web server. This mode of Authentication may require technical support and/or professional services upon initial install.
Cookie Domain	The required cookie domain established by the Administrator, which must be passed

	to the server by the client for Cookie Authentication.
Cookie Name	The required cookie name established by the Administrator, which must be passed to the server by the client for Cookie Authentication.
Cookie Path	The required cookie path established by the Administrator, which must be passed to the server by the client for Cookie Authentication.
Auto-insert Cookie User	If an Authentication mode other than Cookie Authentication is used then the cookie and machine information will be collected and used to generate a new User record. If a User record already exists then this option is ignored.
Concurrent Access Rules On	This option enables Users to use two client applications simultaneously.
Maximum Concurrent Sessions	Allows Administrators to set the maximum amount of concurrent sessions a User may establish.
Session Type	This field specifies how concurrent usage is identified and controlled. The options are Document and User which are detailed below. **Document:** Enables concurrent usage by document. E.g. only a certain amount of Users may open a Document governed **User / Username:** Enables concurrent usage by User.
Timeout Period	This option allows an Administrator to set a session length to be established and enforced when concurrent document usage by User is enabled.
Unit (Timeout Period)	Increment by which a period is measured. E.g. second, minute, day, week, etc.

Figure 6: Authentication Policy Properties

Permission Policies

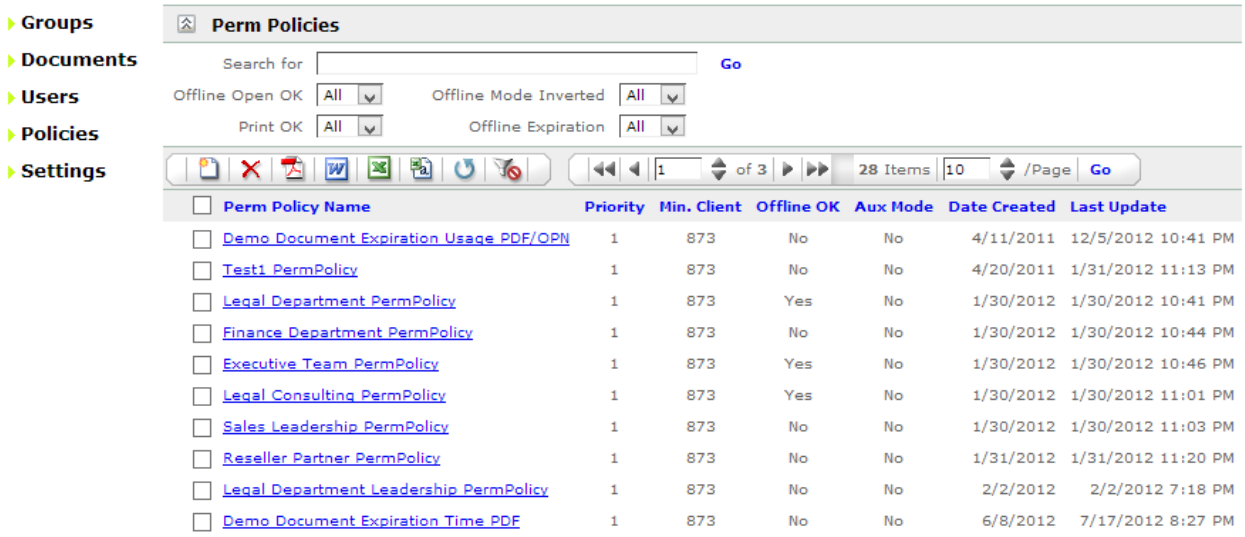
Permission Policies allow Administrators to set Document use policies to be executed at the Group Level. These Permission Policies are categorized as Online Permissions, Offline Permissions and Offline Inverted (Auxiliary) Permissions.

A. **Online Permission**: the User must have an active internet connection to open Documents, and all requests are routed to the PermissionServer.
B. **Offline Permission**: the User must have an active internet connection in order to get Offline Permissions, but once Offline Permission has been granted the User does not need any internet access to open Documents. If Offline Permission has been granted contingent upon expiration then the User must have an active internet connection to renew the Offline Permissions, if that has been allowed by the Administrator. If Offline Permission has been granted without expiration the User need never have an internet connection again.
C. **Offline Inverted (Auxiliary) Mode**: the User may open documents with or without an active internet connection. If the User has an active connection, the Permission is obtained using the Online Permission mechanism; otherwise the Offline Permission is consumed.

Offline Permissions do not require that the User have an active internet connection to open Documents, though the User must have an active internet connection to get the Offline Permissions. The system does not support a case where the User never has an internet connection.

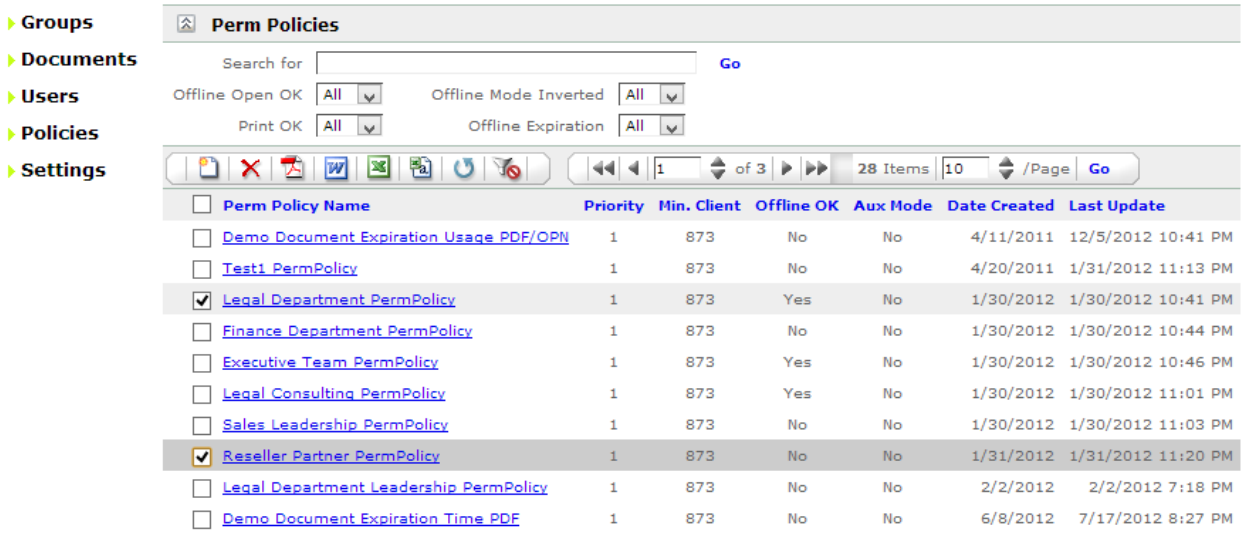
Locate Permission Policy

1. Navigate to Policies > Permission Policies
2. Do one of these:
    a. Sort Permission Policies by column headings, select the number of items to display, scroll through pages to find the Policy you are looking for.
    b. In the search field, type information about the Permission Policy, and then click Search.
    c. Filter by Offline Permissions or Print Permissions available.



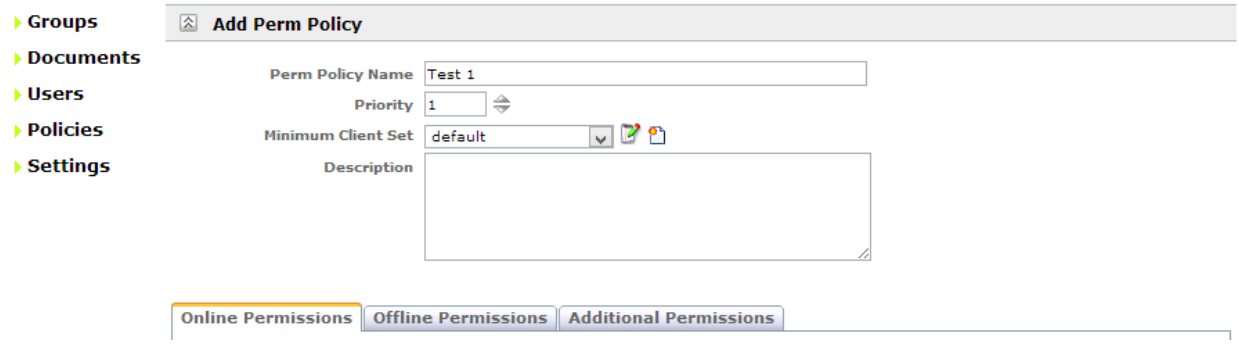
Delete Permission Policy

Administrators may delete Permission Policies by checking the boxes next to the Policy Name then click the Delete button  .



Add or create an Permission Policy

1. Navigate to Policies > Permission Policies > Add Permission Policy
    1. Name the Permission Policy
    2. Priority for the Permission Policy is **deprecated** and will be removed from the interface.
    3. Set the Minimum Client Set required for Policy. Note: Minimum client set can also be set at the Authentication Policy level. If there is ever a conflict the highest build number wins.
        i. Visit http://plugin.fileopen.com for the latest client releases.
        ii. Visit http://www.fileopen.com/blog/?Tag=Client+Release for the latest features released with each client release.
    4. Description may be populated as the Administrator deems fit.

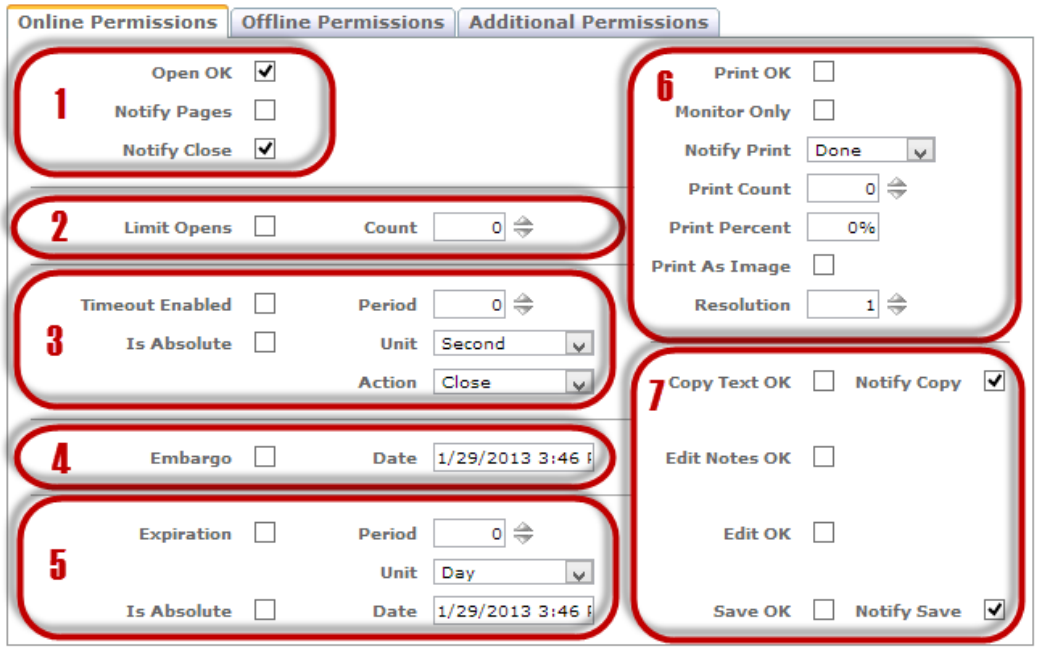


2. Specify the appropriate Online, Offline and any Additional Permissions.

Online Permissions

Online Permissions are those granted in real time by the PermissionServer. Such permissions are defined at the level of the Group/Policy, and may be added or revoked at any time, with the changes taking effect the next time a User opens a Document in that Group/Policy. Users must have an active internet connection to use Online Permissions.

Configuring Online Permissions:



1. This area allows the Administrator to specify if Documents within this Group/Policy maybe opened and if so, should the Client notify the PermissionServer to record open and close actions.
2. The Limit Opens function allows the Administrators to set the maximum allowable opens for members of this Group/Policy.
3. The Timeout Enabled option allows an Administrator to close a Document based on how long that Document has been open.
4. The Embargo option allows Administrators to designate a time in the future as to when a Document may be opened.
5. Expiration options that allow Administrators to revoke Document access after a certain date or time period.
    - Absolute (Fixed Date): in which a date is specified; when this date is reached the User will not be permitted to open any Document in the Group.
    - Relative: in which a period is specified from the User's initial access of any Document in the Group. When this period has been reached the User will no longer be permitted to open any Document in the Group.
6. This area allows Administrators to enable, monitor and/or restrict print functions.
    - The Print Count box permits a limit on the number of jobs and/or copies that may be printed of any given Document in the Group/Policy. More specifically with PDF document copies of printed documents may be limited to a specified count. That is, if the value is set to two the User may print one copy two times, or two copies one time. With OPN files, only the print jobs may be restricted. That is, if the value is set to two the User may print multiple copies two times.
7. This area allows Administrators to restrict the copying of text within the document, the Save As functionality, and the ability to Edit Notes.

For a full list of Permission fields and their definitions please see, Permission Policy Properties.

Offline Permissions

This tab permits specification of parameters for Offline Permissions, via the dialog shown below. As noted in the section above, the Publisher must make a determination about whether to grant Offline Permission exclusively, or as an auxiliary backup in case Online Permission is not available.

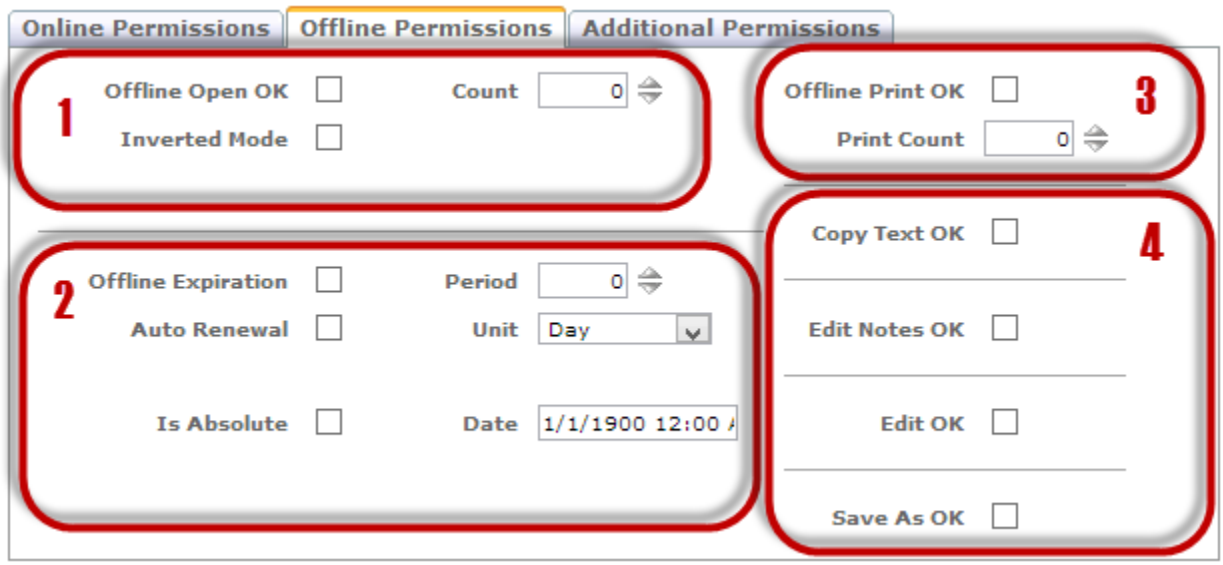
Important: Offline Permissions do not require that the User have an active internet connection to open Documents, though the User must have an active internet connection to get the Offline Permissions. The system does not support a case where the User never has an internet connection.

As noted above there are two types of Offline Permissions supported:

Offline Permissions are granted by the PermissionServer during an initial Online interaction, then stored on the User's local machine. Users with Offline Permissions may open files whether or not they have an active internet connection. Offline Permissions take precedence over Online Permissions, and the actions of users with Offline Permissions will not be logged, unless Offline Inverted Permissions were granted.

Offline Inverted (Auxiliary) Permissions are a combination of Online and Offline Permissions designed to permit the opening of files when a user who is ordinarily connected to the internet is temporarily offline. When Offline Inverted Permissions are granted and the user has an active internet connection the system will use Online Permissions, but if the user has no internet connection the system will use Offline Permissions.

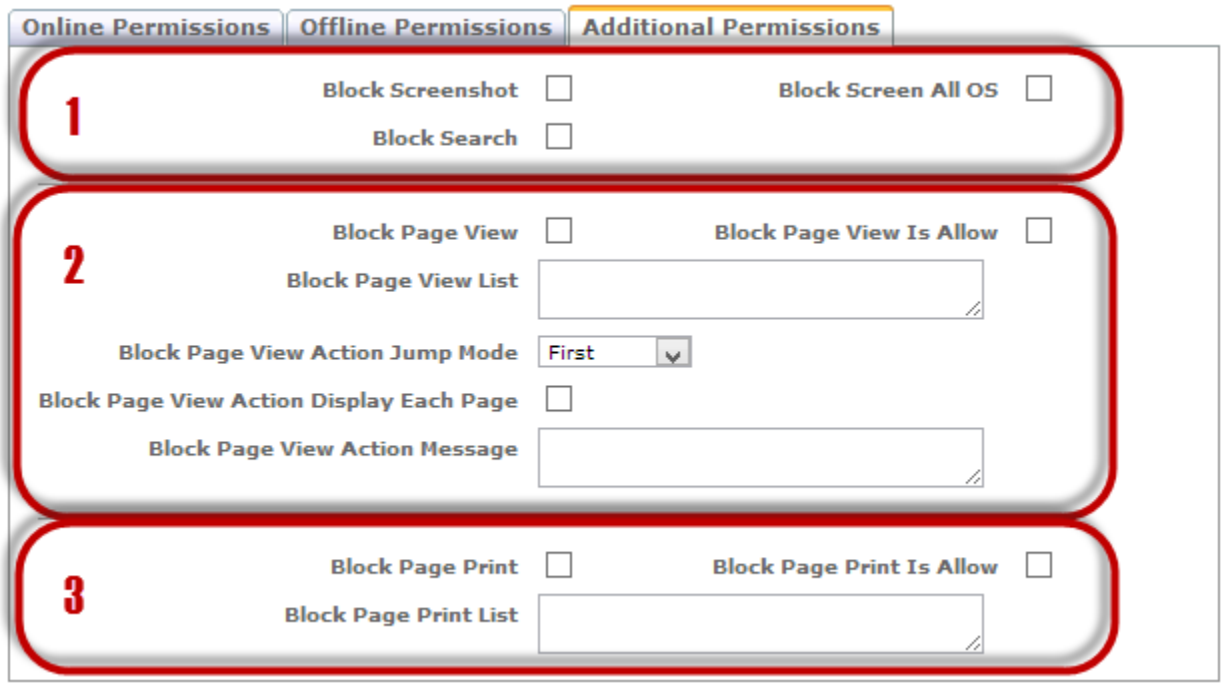
Configuring Offline Permissions:



1. Allows Administrators to specify if Offline Access allowed, if Inverted of Auxiliary Mode should be used and how many times access is allowed.
2. This area provides Offline Expiration and Renewal options. Expiration may be set to revoke access after a certain date or time period. Auto Renewal specifies if the Expiration Period can be extended or renewed provided the User performs an online client /server interaction.
3. Administrators may enable, disable and/or restrict print functions. More specifically with PDF document copies of printed documents may be limited to a specified count. That is, if the value is set to two the User may print one copy two times, or two copies one time.
4. Administrators may enable or disable the ability to copy text, edit text or save the document governed by this Group/Policy.

For a full list of Permission fields and their definitions please see, Permission Policy Properties.

Additional Permissions

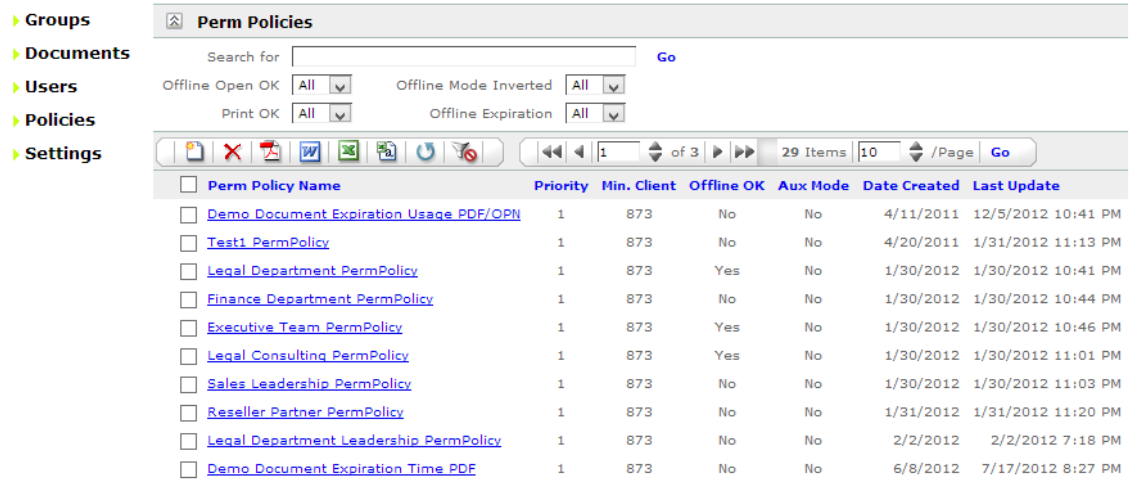


1. This area allows Administrators to Block Screenshots and third party snipping tools within Documents governed by this Group/Policy. When "Block Screenshot All OS" is checked FileOpen disables screenshot capabilities and third party snipping tools — it also prevents the opening of Documents in environments where screen capture cannot be disabled (iPad,iPhone, etc.).
2. Block Page View allows Administrators to block access to pages within a Document governed by this Group/Policy. If Block Page View is Allow is selected Administrators may designate which pages may be viewed. Depending on the option selected, Pages that should have access disabled or enabled should be listed in the Block Page View List. The Block Page View Action Jump Mode controls the behavior or the document viewer when a page(s) is blocked. There are three modes, as follows:
    a. **Standard:** reverts the User to the previous visible page or the next visible page of the document, depending on User's viewing action
    b. **First**: keeps the User on the first viewable page unless the User knows a viewable page and types that page number in the status bar.
    c. **Last**: keeps the User on the last viewable page unless the User knows a viewable page and types that page number in the status bar.
3. Block Page Print allows Administrators to block printing of pages within a Document governed by this Group/Policy. If Block Page Print is Allow is selected Administrators may designate which pages may be Printed. Depending on the option selected, Pages that should have printing disabled or enabled should be listed in the Block Page Print List.

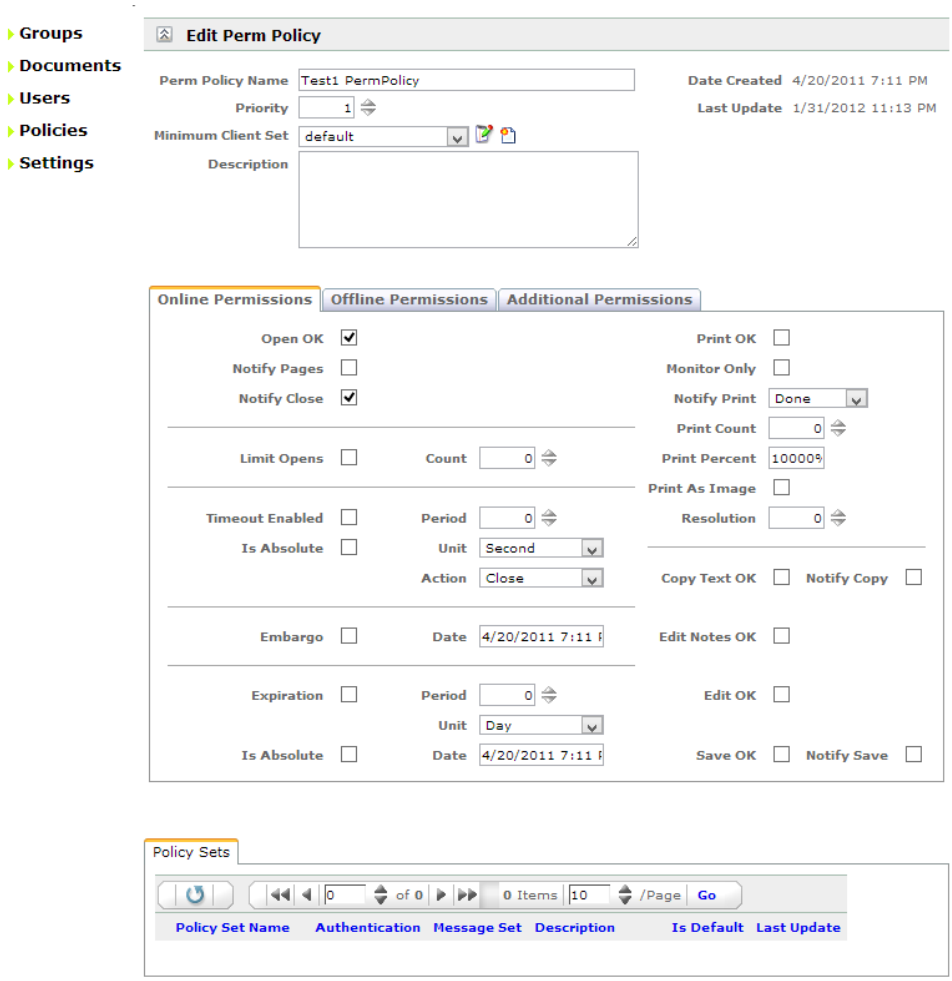
For a full list of Permission fields and their definitions please see, Permission Policy Properties.

Edit Permission Policies

Permission Policies may be edited at any time by Clicking into the Perm Policy Name in the main list of Permission Policies.



Once in the Edit Perm Policy screen Administrators may update policies to take affect immediately. For example, an Administrator may change the expiration date, limit opens, allow more print jobs, etc. All edits take effect immediately except in the case of offline permissions. Offline permission will only be updated / renewed if the Policy was created in Inverted Mode and the User has an active internet connection.



Permission Policy Properties

Field	Description
Priority (Permission Policy)	This option is deprecated and will be removed from the interface.
Minimum Client Set (Permission Policy)	This option sets the Minimum Client required for the User to Access a document. Note: Minimum client set can also be set at the Authentication Policy level. If there is ever a conflict the highest build number wins. • Visit http://plugin.fileopen.com for the latest client releases. • Visit http://www.fileopen.com/blog/?Tag=Client+Release for the latest features released with each client release.
Open OK	This option permits the User to open a Document that is protected with this policy.
Notify Pages	This option enables page view tracking. E.g. the Client notifies the PermissionServer to record the page view.
Notify Close	This option enables tracking of Document close. E.g. the Client notifies the PermissionServer to record the Document close.

Print OK	This option permits the User to print a Document that is protected with this policy.
Monitor Only	This option enables print monitoring rather than print control. E.g. Printing cannot be controlled or limited but can be tracked. This is executed through the native application print dialog rather than the FileOpen print dialog.
Notify Print	This option enables tracking of print jobs. E.g. the Client notifies the PermissionServer to record the print.
Print Count	Allows Administrators to input the maximum count of allowable print jobs.
Print Percent	Coming soon – Allows Administrators to set the percentage of pages printed.
Print as Image	This option enables Documents protected with this policy to be printed as an image.
Print Image Resolution	If Print as Image is enabled, resolution for print should be set. FileOpen recommends setting resolution to no less than 150dpi.
Limit Opens	This option allows Administrators to restrict the amount of Document opens.
Open Count	The specified maximum allowable opens.
Copy Text OK	This option permits the User to select and extract text within a Document that is protected with this policy.
Notify Copy	This option enables tracking of text copy (select and extract) within a Document.
Save OK	This option permits the User to save a local copy of a document that is protected with this policy.
Notify Save	This option enables tracking of the Save As function.
Edit OK	This option permits the User to Edit a Document that is protected with this policy.
Edit Notes OK	This option permits the User to Edit Notes within a Document that is protected with this policy.
Timeout enabled	This option allows an Administrator to close a Document based on how long that Document has been open.
Is Absolute (Timeout)	This field is deprecated and will be removed from the WebUI.
Timeout Period	The period for which a Document protected by this policy can stay open.
Timeout Unit	The Timeout period is defined by units. These are minutes, hours, days, weeks, etc.
Timeout Action	When timeout is enabled Administrators may select an action to take place upon timeout. **Close:** Instructions to close the document is sent. **Ask:** Asks the server at each interval if Timeout is required.

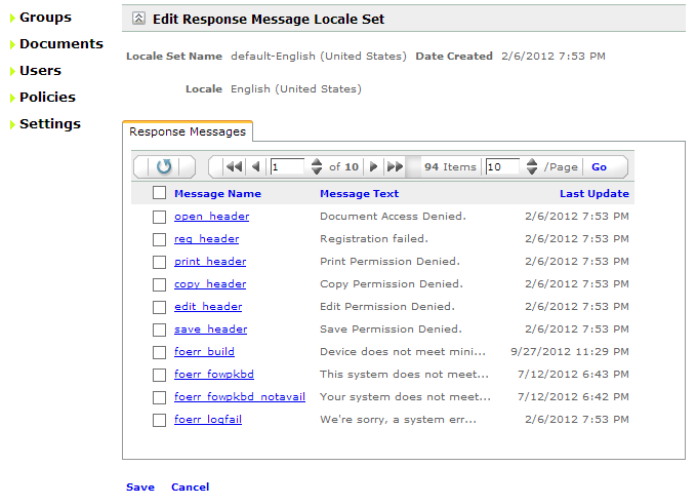
	Remove: The document timeout is removed.
Embargo	This option permits an Embargo to be imposed on a document that is protected with this policy.
Embargo Date	The date an Embargo is lifted / Document is accessible.
Expiration	This option permits Expiration by Time or Term to be imposed on a Document that is protected with this policy.
Is Absolute (Expiration)	This option indicates that the Expiration is Absolute and will expire on a specified date/time.
Expiration Date	The date a document protected by this policy will expire.
Expiration Period	The period for which a Document protected by this policy will expire.
Expiration Unit	The expiration period is defined by units. These are minutes, hours, days, weeks, etc.
Offline Open OK	This option permits offline opening of a Document protected by this policy.
Offline Mode Inverted	This option enables Inverted Offline access. Meaning the client first checks to determine whether the local machine has an active Internet connection. If so, the client operates in Online Mode. If no Internet connection is found, the client will consume Offline permissions.
Offline Open Count	The specified maximum allowable offline opens.
Offline Print OK	This option permits offline print jobs of a Document protected by this policy.
Offline Print Count	The specified maximum allowable offline print jobs.
Offline Expiration	This option enables offline expiration of a Document protected by this policy.
Is Absolute(Offline Expiration)	This option indicates that the Offline Expiration is Absolute and will expire on a specified date/time.
Offline Expiration Auto Renewal	This option enables automatic offline permission renewal provided the User performs an online client /server interaction.
Offline Expiration Unit	The specified expiration period is defined by units. These are minutes, hours, days, weeks, etc.
Offline Expiration Period	The period for which a Document protected by this policy will expire
Offline Expiration Date	The date a Document protected by this policy will expire.
Offline Copy Text OK	This option permits the User to copy text within a Document that is protected with this policy.
Offline Edit Notes OK	This option permits the User to edit notes within a Document that is protected with

	this policy.
Offline Edit OK	This option permits the User to edit a Document that is protected with this policy.
Offline Save As OK	This option permits the User to save a local copy of a Document that is protected with this policy.
Block Screenshot	This option disables screenshot capabilities and third party snipping tools but permits Documents to be opened in environments where screen capture cannot be disabled.
Block Screenshot All OS	This option disables screenshot capabilities and third party snipping tools and prevents the opening of Documents in environments where screen capture cannot be disabled.
Block Search	This option disables Document search capabilities.
Block Page View	Allows Administrators to block the view of pages listed in the Block Page View List.
Block Page View is Allow	Allows Administrators to designate which pages may be viewed. Viewable pages need to be listed in the Block Page View List.
Block Page View List	Text field that designates which pages within the document may or may not be viewed.
Block Page View Action Jump Mode	This option controls the behavior or the document viewer when a page(s) is blocked. There are three modes, as follows: **Standard:** reverts the User to the previous visible page or the next visible page of the document, depending on User's viewing action **First**: keeps the User on the first viewable page unless the User knows a viewable page and types that page number in the status bar. **Last**: keeps the User on the last viewable page unless the User knows a viewable page and types that page number in the status bar.
Block Page View Action Display Each Page	Check this box to message will be displayed each time the User attempts to view a blocked page.
Block Page View Action Message	Text field Administrators may populate with a custom message presented to Users when a page is blocked. For example a list of viewable pages by policy may be listed to inform the User of acceptable use.
Block Page Print	Allows Administrators to block the print of pages listed in the Block Page Print List.
Block Page Print is Allow	Allows Administrators to designate which pages may be printed. Printable pages need to be listed in the Block Page Print List.
Block Page Print List	Text field that designates which pages within the document may or may not be printed.

Figure 7: Permission Policy Properties

Message Sets / Response Messages

Message Sets are comprised of Response Messages presented to Users through the client viewer. Today FileOpen supports English, German, Spanish and French response messages. Further customization of response messages are available through customer support only, but will be available through the WebUI in the near future.



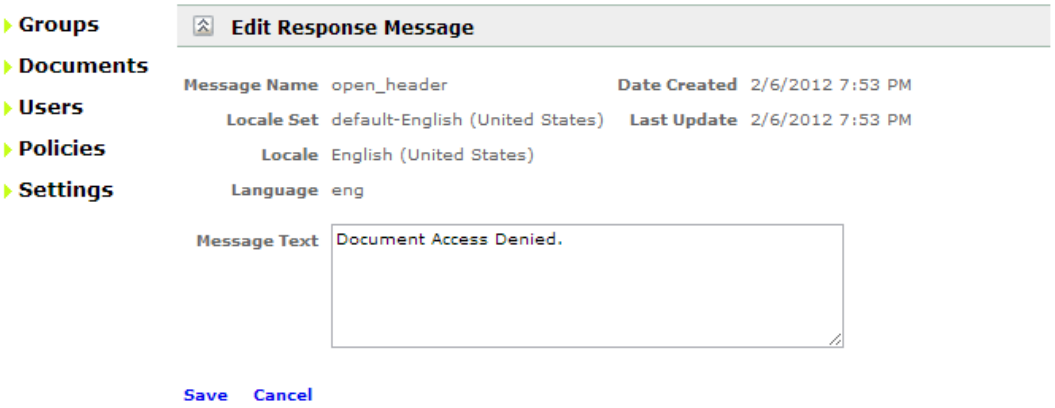
Locate Message Sets

1. Navigate to Policies > Response Messages
2. Navigate through the Message Set to the Message Local Set to review messages.

Groups
Documents
Users
Policies
Settings
Edit Response Message Locale Set
Locale Set Name default-English (United States) Date Created 2/6/2012 7:53 PM
Locale English (United States)
Response Messages
1 of 10 94 Items 10 /Page Go
Message Name Message Text Last Update
open_header Document Access Denied. 2/6/2012 7:53 PM
req_header Registration failed. 2/6/2012 7:53 PM
print_header Print Permission Denied. 2/6/2012 7:53 PM
copy_header Copy Permission Denied. 2/6/2012 7:53 PM
edit_header Edit Permission Denied. 2/6/2012 7:53 PM
save_header Save Permission Denied. 2/6/2012 7:53 PM
foerr_build Device does not meet mini... 9/27/2012 11:29 PM
foerr_fowpkbd This system does not meet... 7/12/2012 6:43 PM
foerr_fowpkbd_notavail Your system does not meet... 7/12/2012 6:42 PM
foerr_logfail We're sorry, a system err... 2/6/2012 7:53 PM
Save Cancel

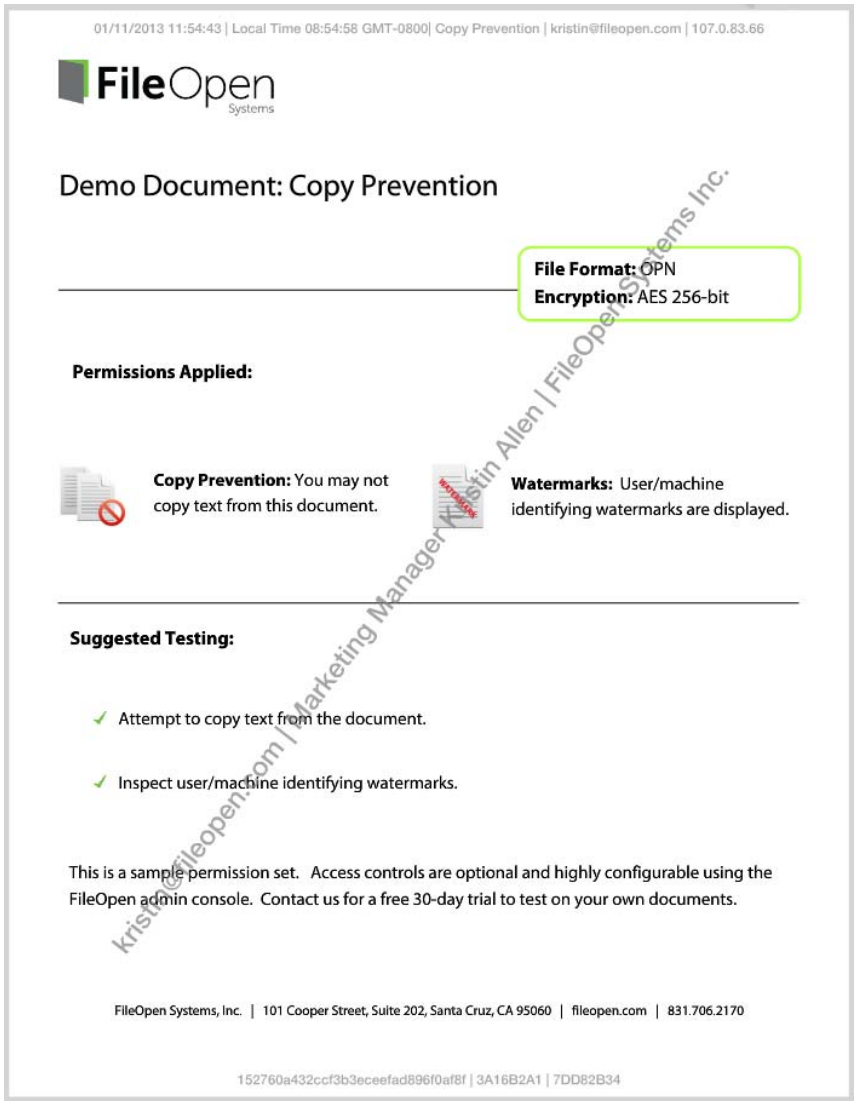
Editing Response Messages

In the near future, Administrators will be able to configure response messages to reflect brand and/or language through the WebUI.



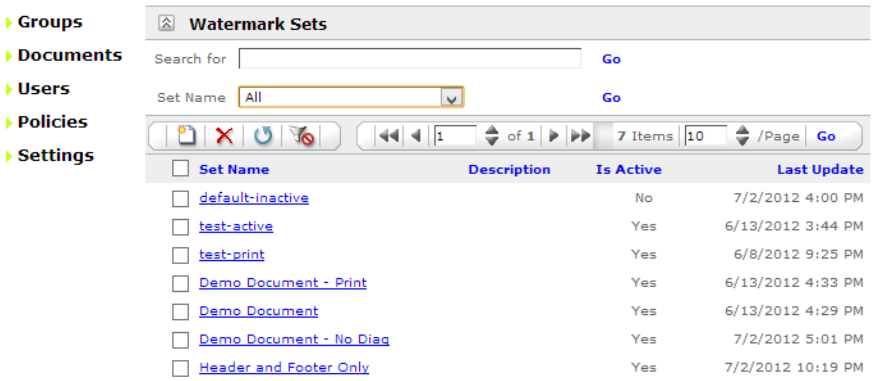
Watermarks

Using WebUI, Administrators can configure dynamic Watermarks that are displayed on each document view or print. The system is delivered with a default Watermark Set for both view and print, which can easily be edited. For more information see, Configure a Watermark Set.



Locate a Watermark Set

1. Navigate to Policies > Watermark Set
2. Do one of these:
    a. Sort Watermarks by column headings.
    b. In the search field, type information about the Response Message, and then click Search.

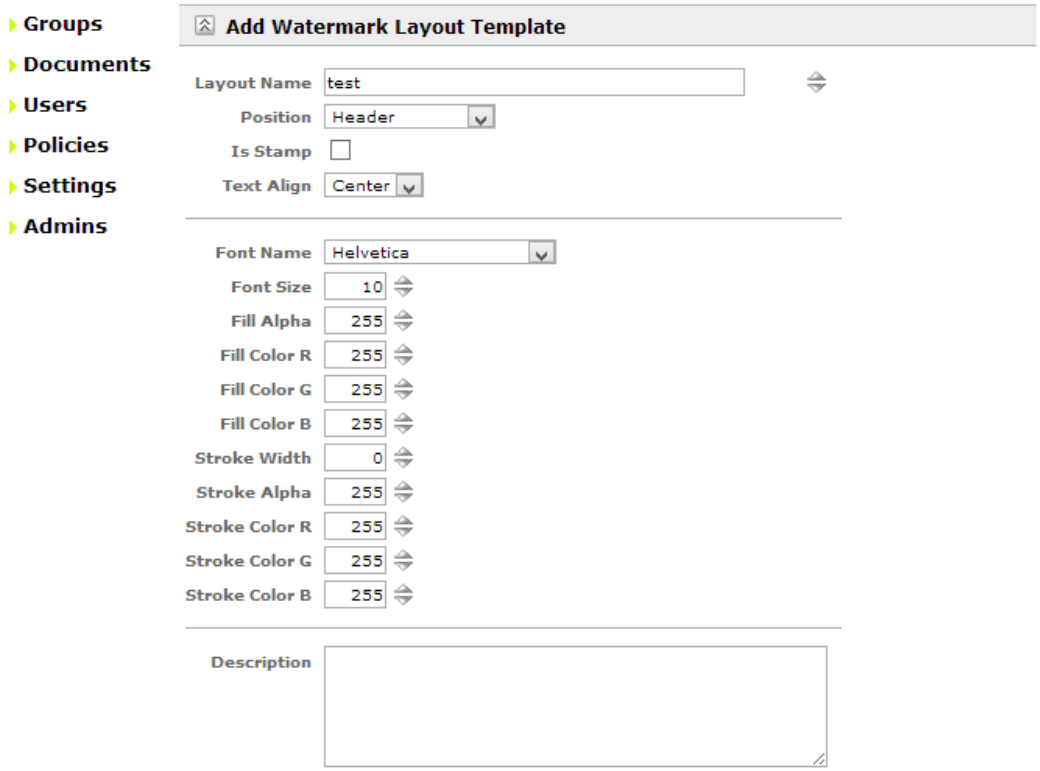


Add or Create a Watermark Set

To create a Watermark set for use within a Policy Administrators must first configure a Layout Template and a Text Template.

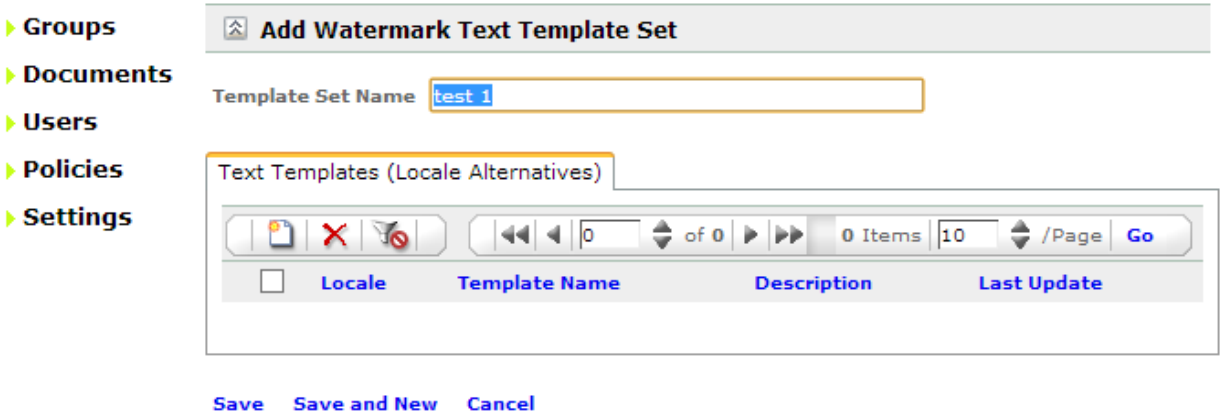
Add or create a Layout Template

1. Navigate to Watermarks > Layout Templates > Add Layout Template
2. Name the Layout Template and select the position (Header, Footer or Diagonal).
3. Check the “Is Stamp” checkbox if the watermark should be superimposed to the document text. If the checkbox is not check the watermark will be subjacent to the text of the document.
4. Designate the desired text alignment, font, font size, opacity and fill. Then save the Layout Template.

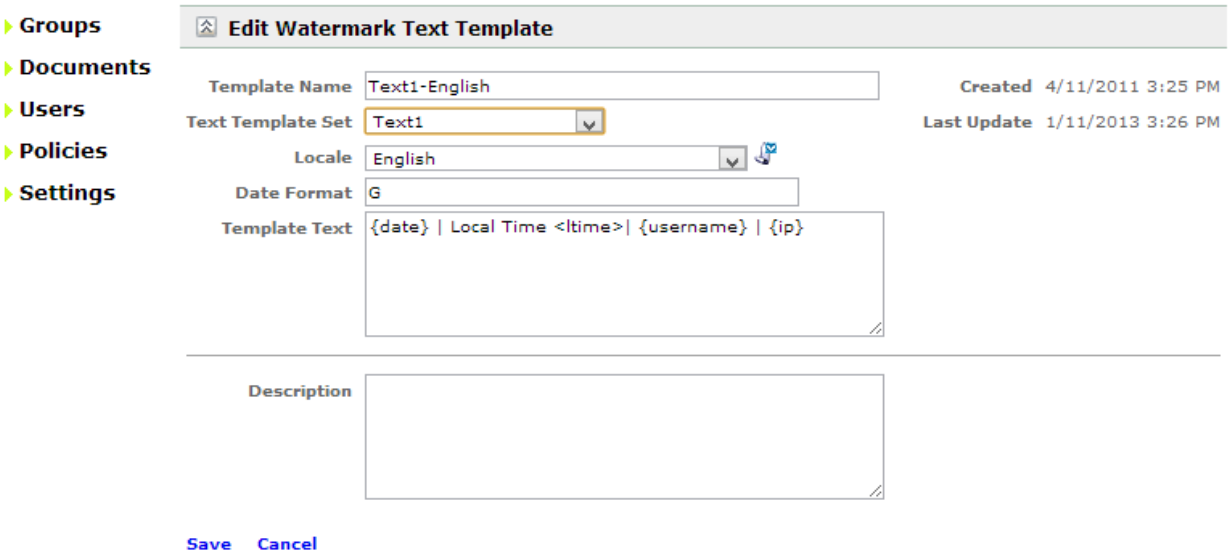


Add or create a Text Template

1. Navigate to Watermarks > Text Template Sets > Add Text Template Set.
2. Name the Template Set and Save.



3. The WebUI will redirect you to the Add Watermark Text Template dialog. Name the template, and select the locale from the pull down menu.
4. Input the Date Format as defined by the syntax guide. For more information, see Watermark Template Text: Date/Time format string syntax guide
5. Customize the Template Text to display the variables desired in the visible Watermark. For a full List of available variables, see Watermark Template Text: Available Properties.



Watermark Template Text: Date/Time format string syntax guide

Format specifier	Description	Examples
"d"	Short date pattern.	6/15/2009 1:45:30 PM -> 6/15/2009 (en-US) 6/15/2009 1:45:30 PM -> 15/06/2009 (fr-FR) 6/15/2009 1:45:30 PM -> 2009/06/15 (ja-JP)
"D"	Long date pattern.	6/15/2009 1:45:30 PM -> Monday, June 15, 2009 (en-US) 6/15/2009 1:45:30 PM -> 15 июня 2009 г. (ru-RU) 6/15/2009 1:45:30 PM -> Montag, 15. Juni 2009 (de-DE)
"f"	Full date/time pattern (short time).	6/15/2009 1:45:30 PM -> Monday, June 15, 2009 1:45 PM (en-US) 6/15/2009 1:45:30 PM -> den 15 juni 2009 13:45 (sv-SE) 6/15/2009 1:45:30 PM -> Δευτέρα, 15 Ιουνίου 2009 1:45 μμ (el-GR)
"F"	Full date/time pattern (long time).	6/15/2009 1:45:30 PM -> Monday, June 15, 2009 1:45:30 PM (en-US) 6/15/2009 1:45:30 PM -> den 15 juni 2009 13:45:30 (sv-SE) 6/15/2009 1:45:30 PM -> Δευτέρα, 15 Ιουνίου 2009 1:45:30 μμ (el-GR)
"g"	General date/time pattern (short time).	6/15/2009 1:45:30 PM -> 6/15/2009 1:45 PM (en-US) 6/15/2009 1:45:30 PM -> 15/06/2009 13:45 (es-ES) 6/15/2009 1:45:30 PM -> 2009/6/15 13:45 (zh-CN)
"G"	General date/time pattern (long time).	6/15/2009 1:45:30 PM -> 6/15/2009 1:45:30 PM (en-US) 6/15/2009 1:45:30 PM -> 15/06/2009 13:45:30 (es-ES) 6/15/2009 1:45:30 PM -> 2009/6/15 13:45:30 (zh-CN)
"M", "m"	Month/day pattern.	6/15/2009 1:45:30 PM -> June 15 (en-US) 6/15/2009 1:45:30 PM -> 15. juni (da-DK) 6/15/2009 1:45:30 PM -> 15 Juni (id-ID)

"O", "o"	Round-trip date/time pattern.	6/15/2009 1:45:30 PM -> 2009-06-15T13:45:30.0900000
"R", "r"	RFC1123 pattern. .	6/15/2009 1:45:30 PM -> Mon, 15 Jun 2009 20:45:30 GMT
"s"	Sortable date/time pattern.	6/15/2009 1:45:30 PM -> 2009-06-15T13:45:30
"t"	Short time pattern.	6/15/2009 1:45:30 PM -> 1:45 PM (en-US) 6/15/2009 1:45:30 PM -> 13:45 (hr-HR) 6/15/2009 1:45:30 PM -> 01:45 م (ar-EG)
"T"	Long time pattern.	6/15/2009 1:45:30 PM -> 1:45:30 PM (en-US) 6/15/2009 1:45:30 PM -> 13:45:30 (hr-HR) 6/15/2009 1:45:30 PM -> 01:45:30 م (ar-EG)
"u"	Universal sortable date/time pattern.	6/15/2009 1:45:30 PM -> 2009-06-15 20:45:30Z
"U"	Universal full date/time pattern.	6/15/2009 1:45:30 PM -> Monday, June 15, 2009 8:45:30 PM (en-US) 6/15/2009 1:45:30 PM -> den 15 juni 2009 20:45:30 (sv-SE) 6/15/2009 1:45:30 PM -> Δευτέρα, 15 Ιουνίου 2009 8:45:30 μμ (el-GR)
"Y", "y"	Year month pattern.	6/15/2009 1:45:30 PM -> June, 2009 (en-US) 6/15/2009 1:45:30 PM -> juni 2009 (da-DK) 6/15/2009 1:45:30 PM -> Juni 2009 (id-ID)
CUSTOM DATE/TIME FORMAT STRINGS		http://msdn.microsoft.com/en-us/library/8kb3ddd4.aspx

Watermark Template Text: Available Properties

Watermark variables are used in configuring the Watermark Text Template. Once inserted the variables are substituted by actual string values from the client (angle brackets required) or server (curly brackets required). All supported variables are listed below.

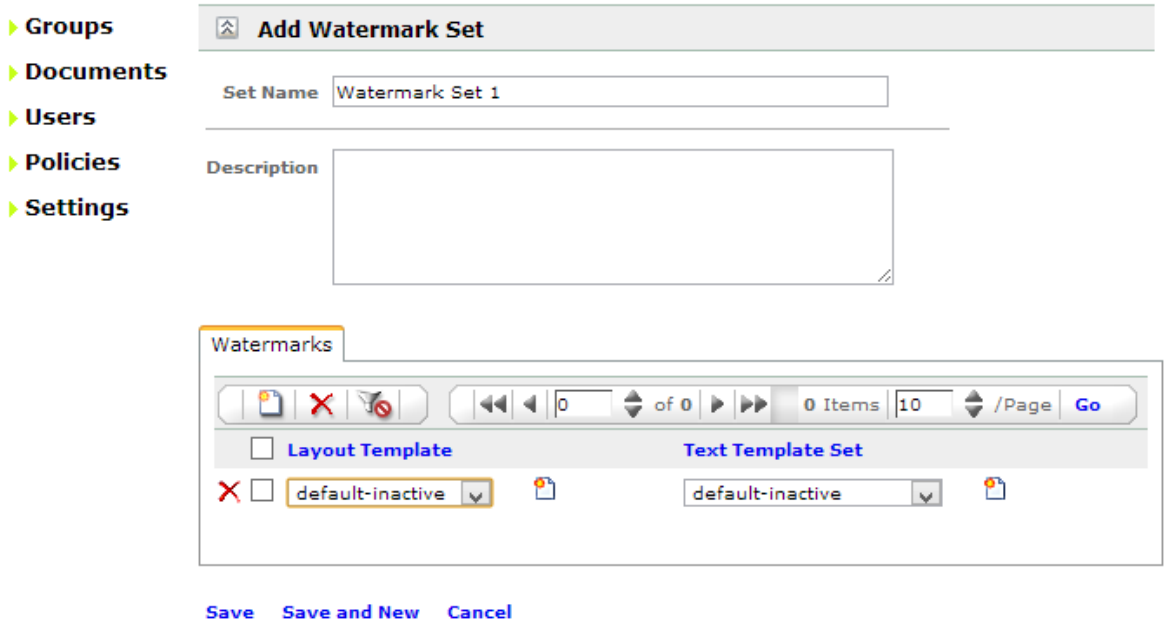
Entities	Description
{date}	Date / time inserted into the document view or print.
{email}	User email address.
{username}	User Username.
{fullname}	User Full Name.
{lastname}	User Last Name.
{firstnames}	User First Name.

{subscriberid}	User Subscriber ID.
{company}	User Company Name.
{category}	User User Category.
{group}	Applicable Group membership for the document / User combination.
{ip}	IP address.
{login}	String Login.
{hostname}	User HostName.
{uuid}	User Universally Unique Identifier (UUID).
{macid)	User MachineID - MAC address of the first card having a MAC address.
{diskid}	User DiskID - first disk (the volume number written on the disk when it is hard formatted) and CPU data.
{printer}	Name of the printer used by the recipient.
<ldate>	Local date
<ltime>	Local time
<ldatetime>	Local date and time
<ldatiext>	Local date and time in extended format
<gdate>	Gmt/Utm date
<gtime>	Gmt/Utm time
<gdatetime>	Gmt/Utm date and time
<gdatiext>	Gmt/Utm date and time in extended format
<serid>	Service Identifier
<docid>	Document Identifier
<phyhost>	Physical host name
<usersid>	User SID
<prntdriver>	Printer Driver

<prntport>	Printer port

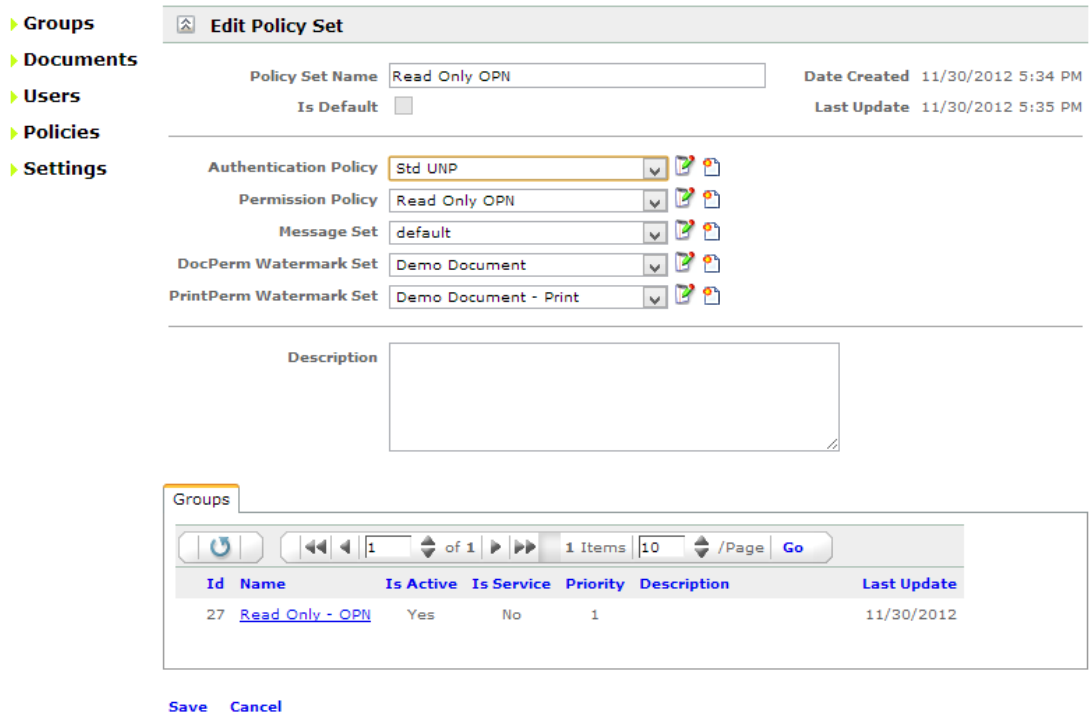
Configure a Watermark Set

1. Navigate to Policies > Watermarks > Add Watermark Set
2. Select the preconfigured Layout Template and Text Template from the pull down menus. Save the Watermark Set.



1. Apply a Watermark Set to a Policy

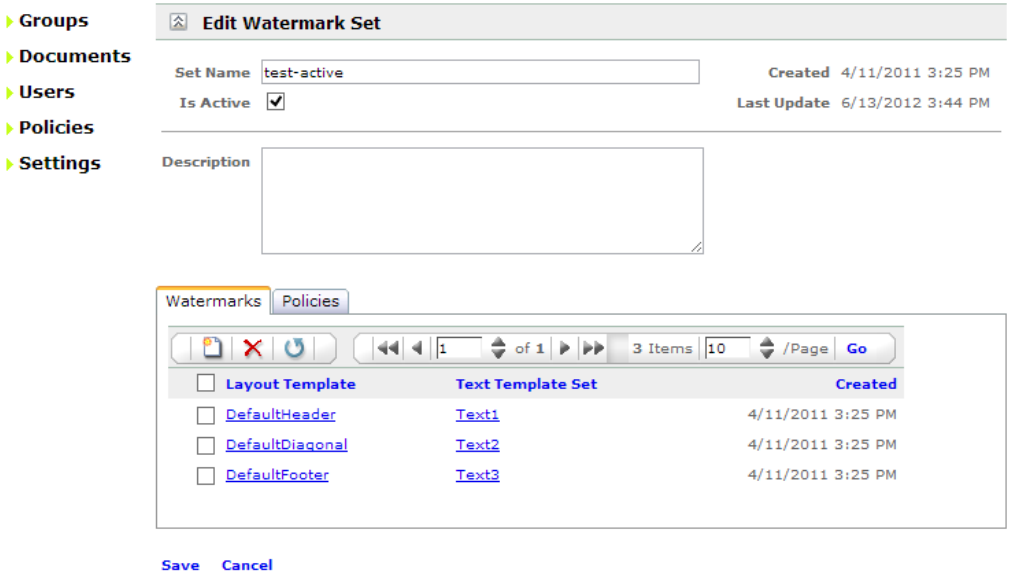
Watermarks are applied at the Policy Set Level. Administrators may designate a unique watermark for view (DocPerm Watermark Set) as well as for print (PrintPerm Watermark Set).



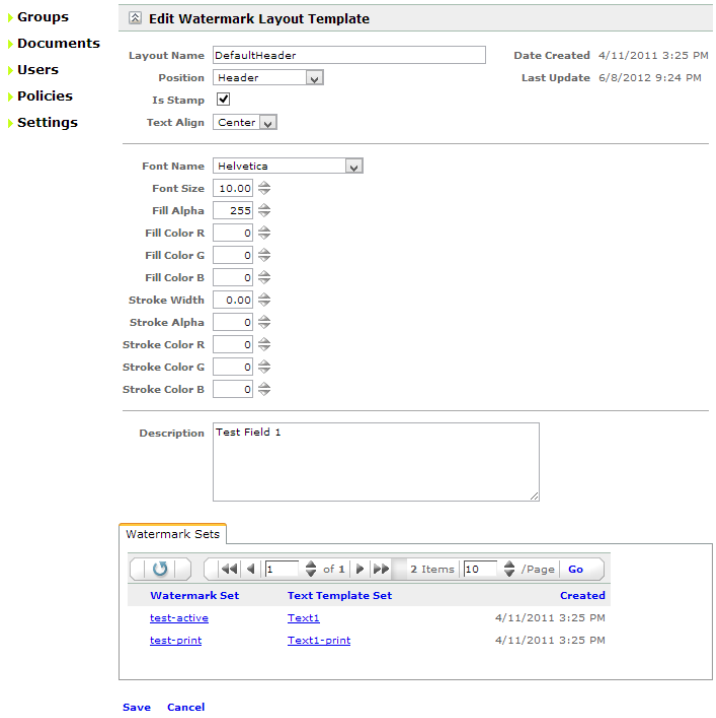
2. Edit a Watermark Set

The WebUI is delivered with three preconfigured watermark sets; which include three default Layout Templates (Header, Footer, Diagonal) and three Text templates. These may be edited as the Administrator deems fit.

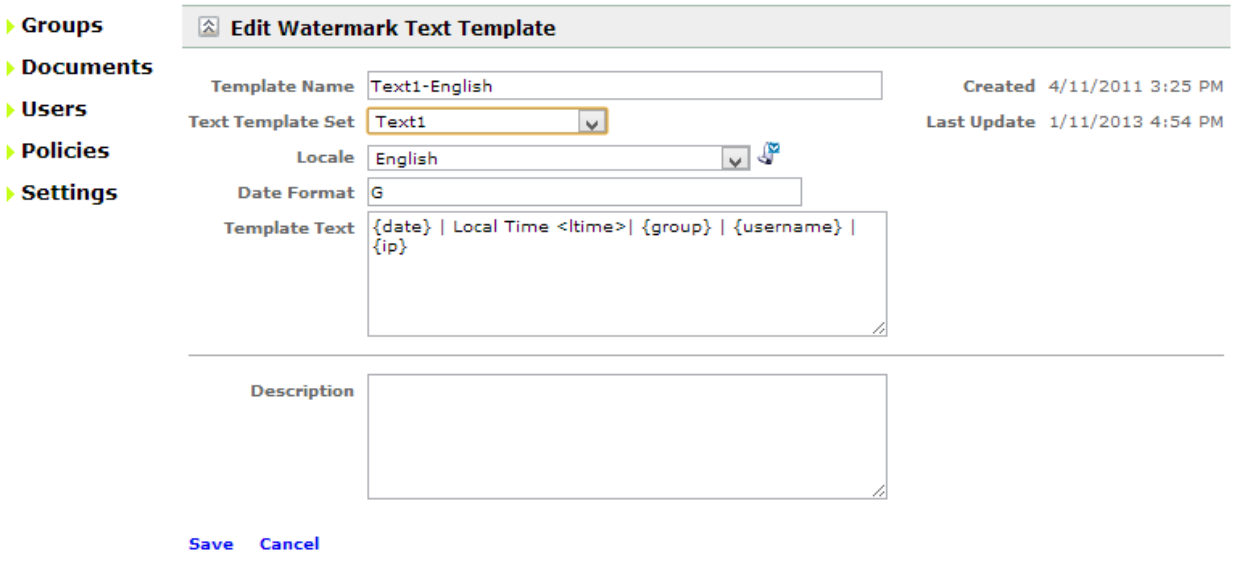
1. Navigate to Policies > Watermarks
2. Select a Watermark Set Name to open the edit dialog.



3. To remove watermarks from a Watermark Set check the box next to the Layout Template and hit the delete button .
4. Click into the individual Layout Templates to edit the font, fill, opacity and alignment.



5. Click into the individual Text template sets to modify variables populated on document view/print.



Users

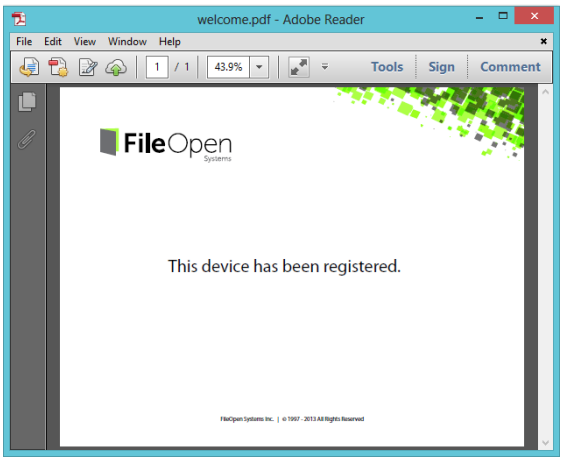
A User is a document recipient, known to the system by their email address. Users must be members of Groups to obtain permissions to access and use a document. A User may be granted permission to open Documents on an arbitrary number of registered machines, though in practice only a small number of machines will typically be allowed; thus for practical purposes a User may be defined as that person's registered device or machine(s).

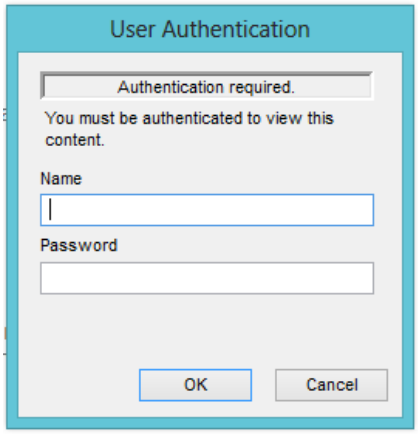
Registering Users

Registering a User is a process by which a User authenticates with the PermissionServer which stores machine identifiers within that User record. Once a User registers that machine, all subsequent access requests are processed by validating machine identifiers, thus allowing the User to avoid multiple log-in prompts.

Users register machines by either:

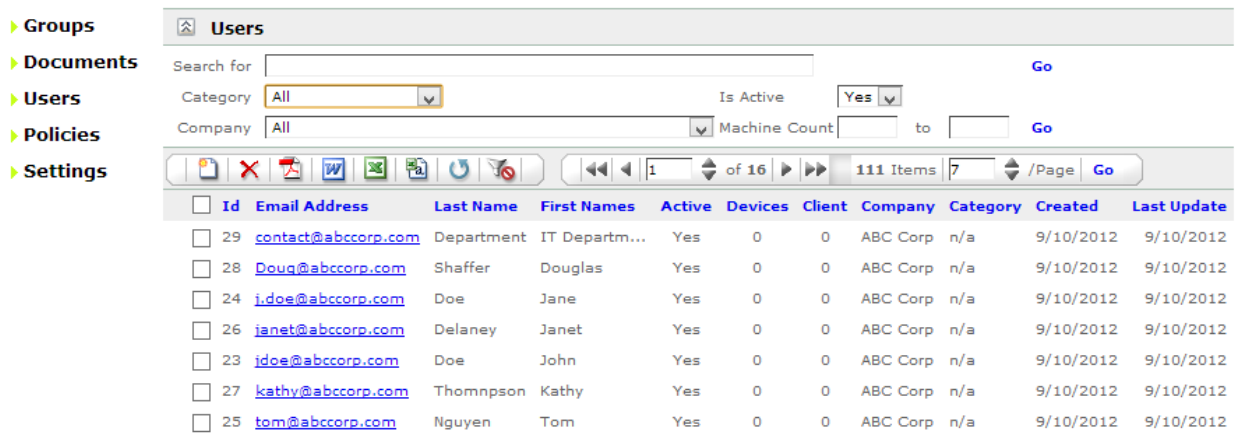
- Opening a specially encrypted Document, which an Administrator creates with the FileOpen Outlook Add-in
- Inputting Username/Password into the FileOpen User Authentication dialog.





Locate a User

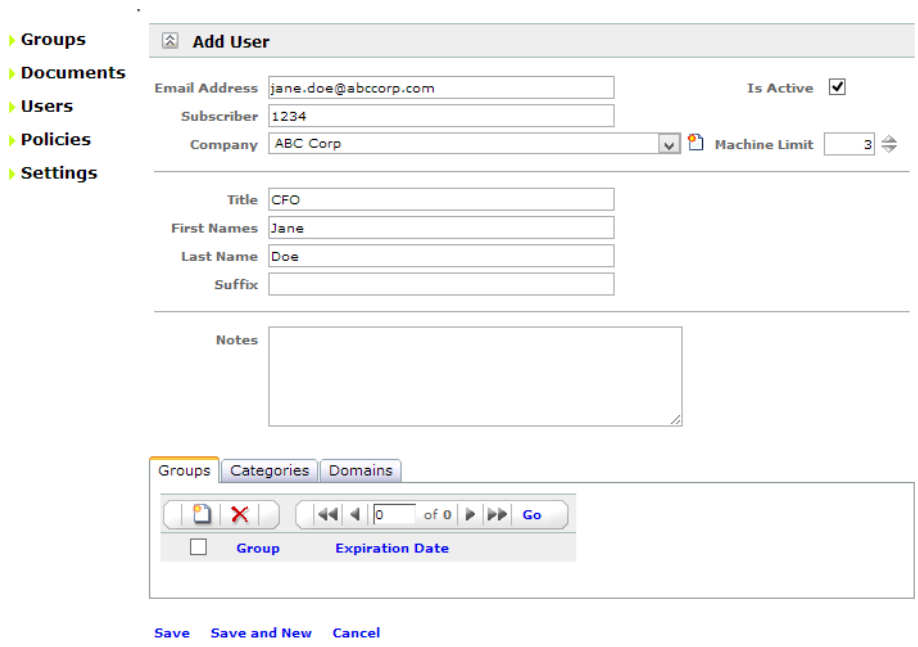
1. Navigate to Users > Show Users
2. Do one of these:
    a. Sort Users by column headings, select the number of items to display, scroll through pages to find Users.
    b. In the search field, type information about the User, and then click Search.



Note: A complete listing of Users managed may be downloaded from this screen by selecting the file type download button above the column headings.

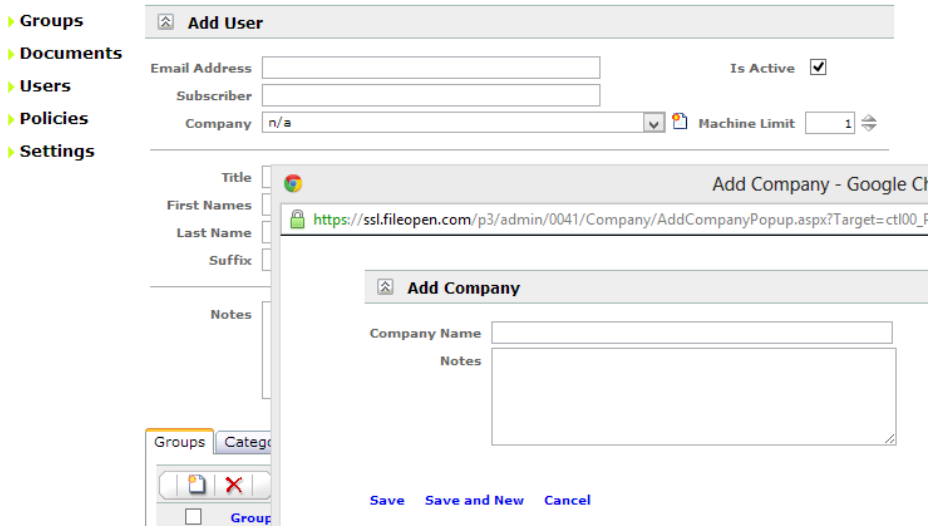
Add or Create a User

1. Navigate to Users > Add User
    a. Input the User's email address — each User entered into the system must have a unique value for Email Address.
    b. Input a value for First Name and Last Name.
    c. Input the acceptable Machine Limit for each User.



    d. Entering text into additional fields is optional and should be completed according to the Administrator's business requirements.

i. Entering text into the Company field by using the drop down menu. New companies may be added using the new/add icon .



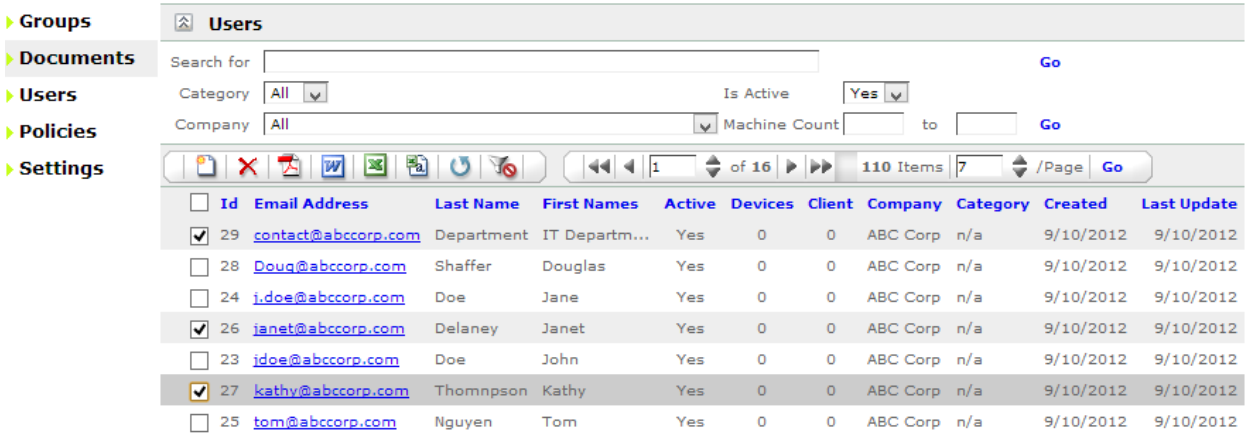
Import Users

Users may be imported into the database with the appropriate license or with professional services. Please send a request to support@fileopen.com for more information.

Delete a User

FileOpen recommends making Users inactive rather than deleting them from the database. However, Administrators may delete Users by:

1. Navigate to Users > Show Users
2. Select the User(s) for deletion by checking the boxes next to the User's email address then click the Delete button .

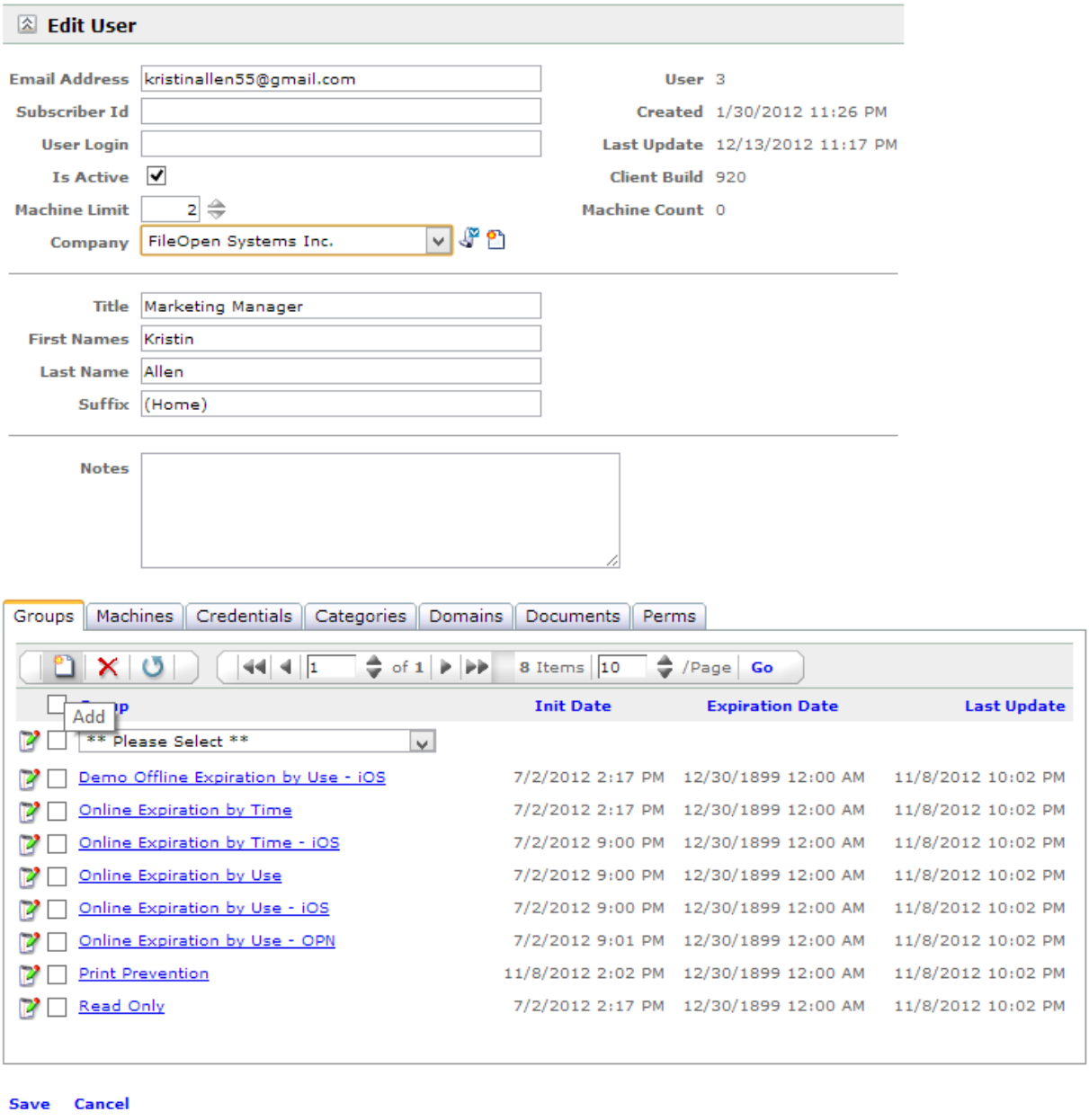


Edit a User

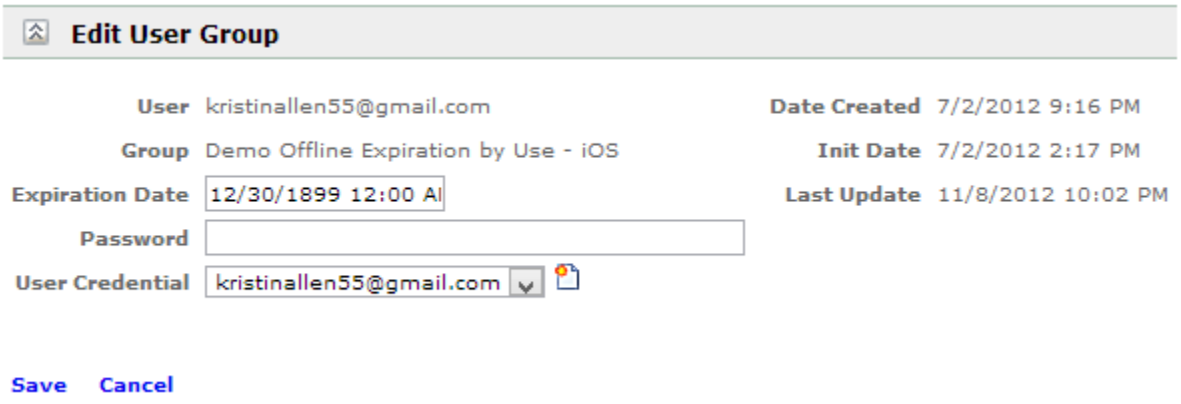
1. Navigate to Users > Show Users
2. Locate and click on the email address of User you wish to edit. From this screen you may edit properties associated to that User.
3. Within the Edit User screen the tabbed layout allows you to:

Edit User > Groups

From an Edit User Screen Administrator may add or remove a User from a Group. To remove a User from a Group, check the box next to the Group Name and click the delete icon  . To add a User to a specific Group, click the new/add icon  , select the Group from the pull down menu and save the record.



In the case where a User's membership to a specific Group should expire, Administrators may set the expiration date by clicking the edit record icon next to the Group Name. Input the appropriate expiration date and save the record.

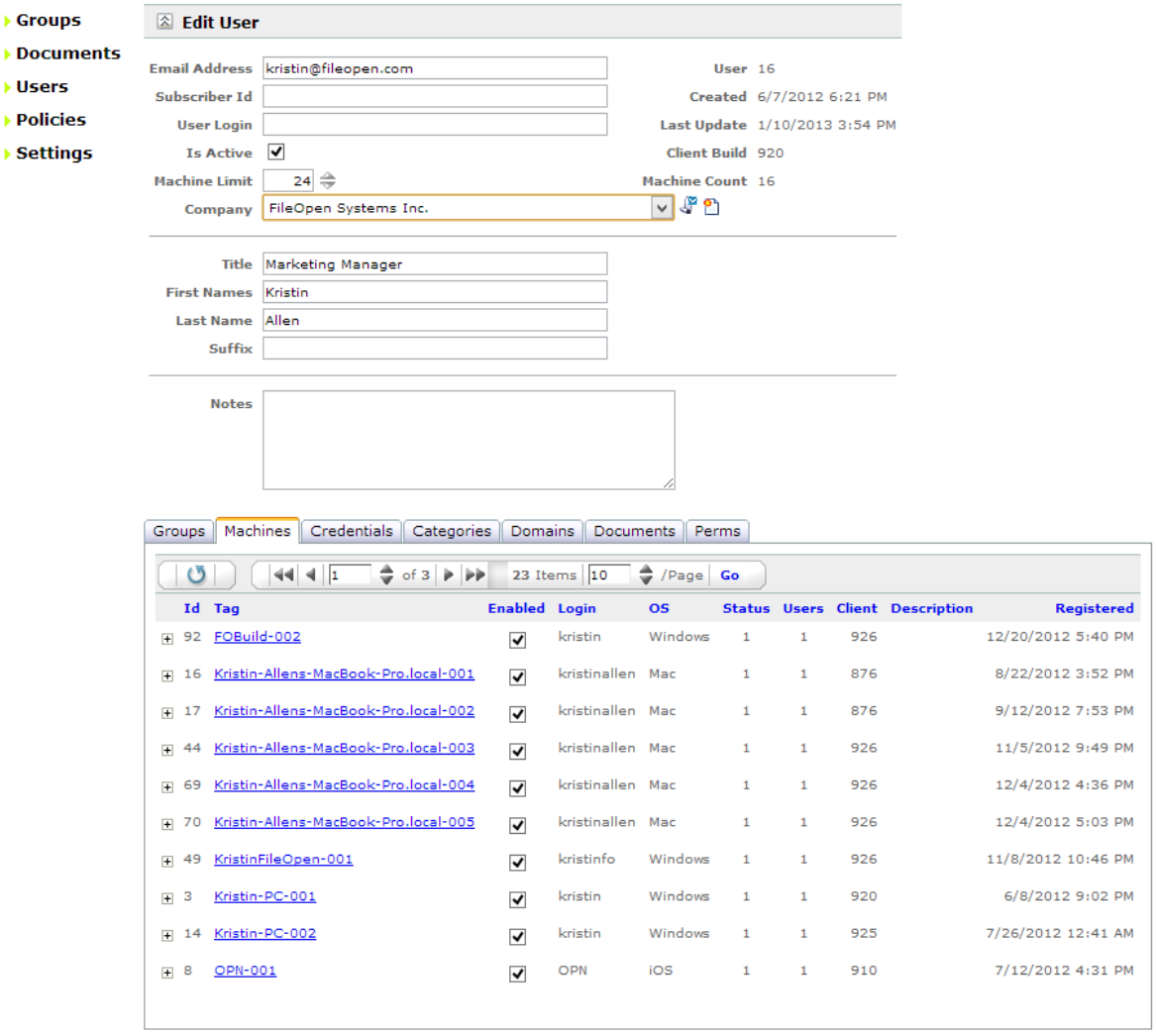


Edit User > Machines

In the top of the Edit User screen Administrators may assign: a Machine Limit to restrict the number of devices a User may register and use to open Documents. Once a User registers a machine, that machine will appear in the list on the Machines tab of the Edit User page, which will contain the date on which the device was registered and the MachineID value. For more information on registering users, see Registering Users.

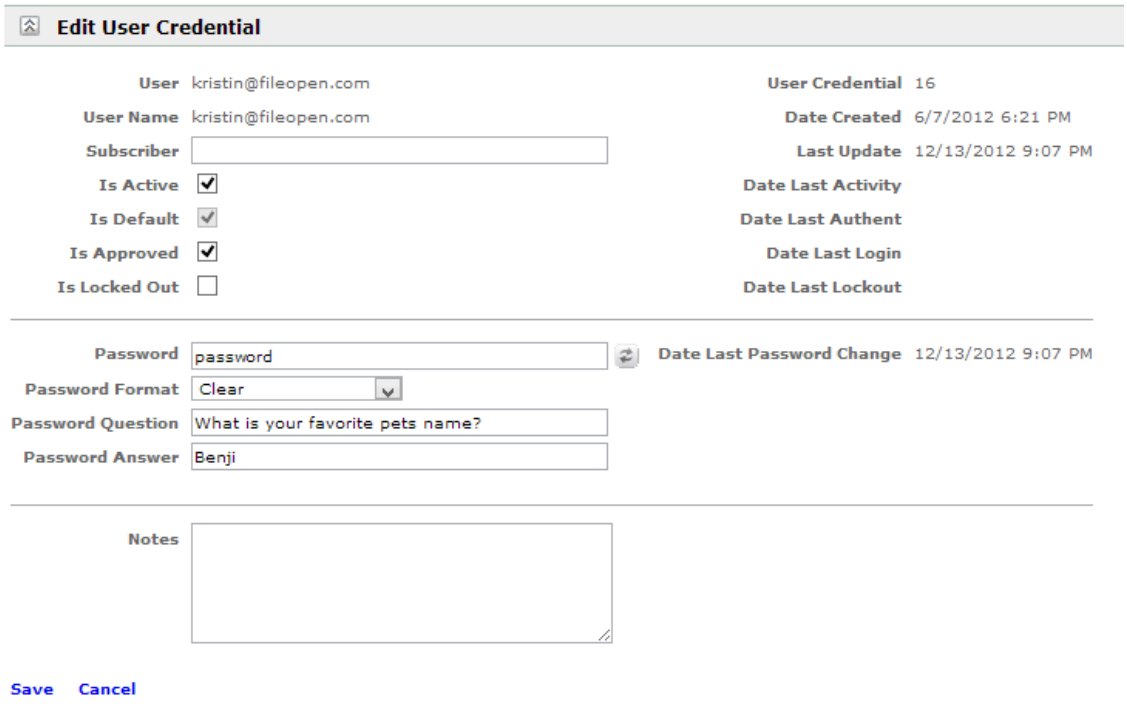
i. The Enabled checkbox will be checked for active Devices; unchecking this box will disable the Device. Disabling a registered device will allow the User to register another Device while keeping the total number of devices constant; that is, if a User given a Machine Limit of one gets a new computer, the Administrator may disable the previous Device and ask the User to open the Registration Document on the new Device.

Important: Enabling and disabling the registration of devices affects only Online Permission. The system does not currently offer a mechanism for transferring Offline Permission from one device to another. So a User with Offline Permission on one device who is given Offline Permission on a second device will have Offline Permission on both. However, if the Offline Permission has an expiration period, the User would not be able to renew that permission on the disabled device.



Edit User > Credentials

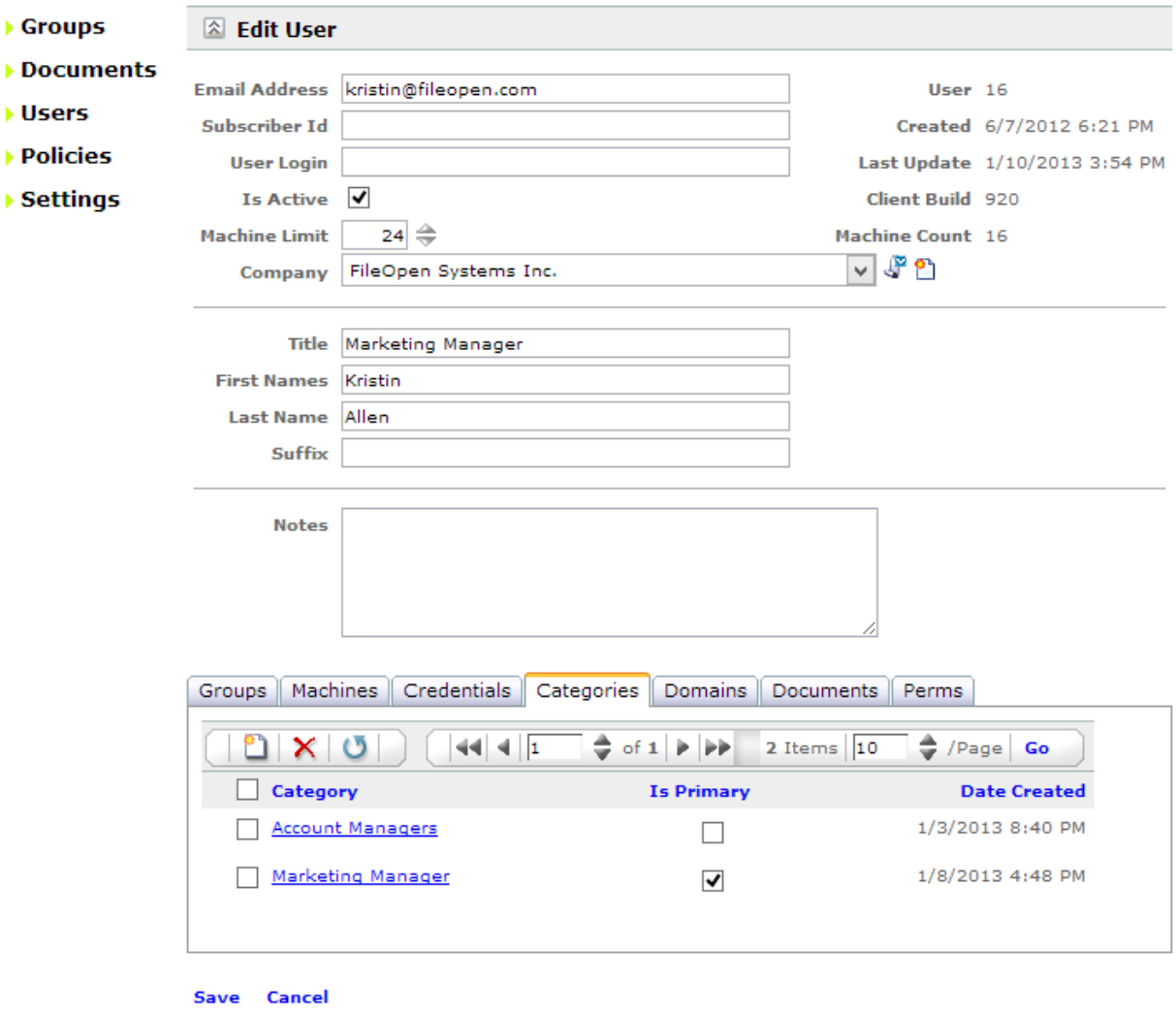
Administrators may maintain User credentials by clicking on the Users email address which opens the Edit User Credential window. From this screen Administrators can quickly edit/recover a User's password or revoke access. By default system generated passwords are eight alphanumeric lowercase characters.



Edit User > Categories

Administrators may classify Users into optional unique categories for internal classification requirements. Categories do not affect the permission logic in anyway.

ii. The Is Primary checkbox is intended to set the primary Category for a User in multiple Categories.
    1. Note: If a User is classified in more than one Category and no Primary has been set then the oldest Category classification is considered the Primary.

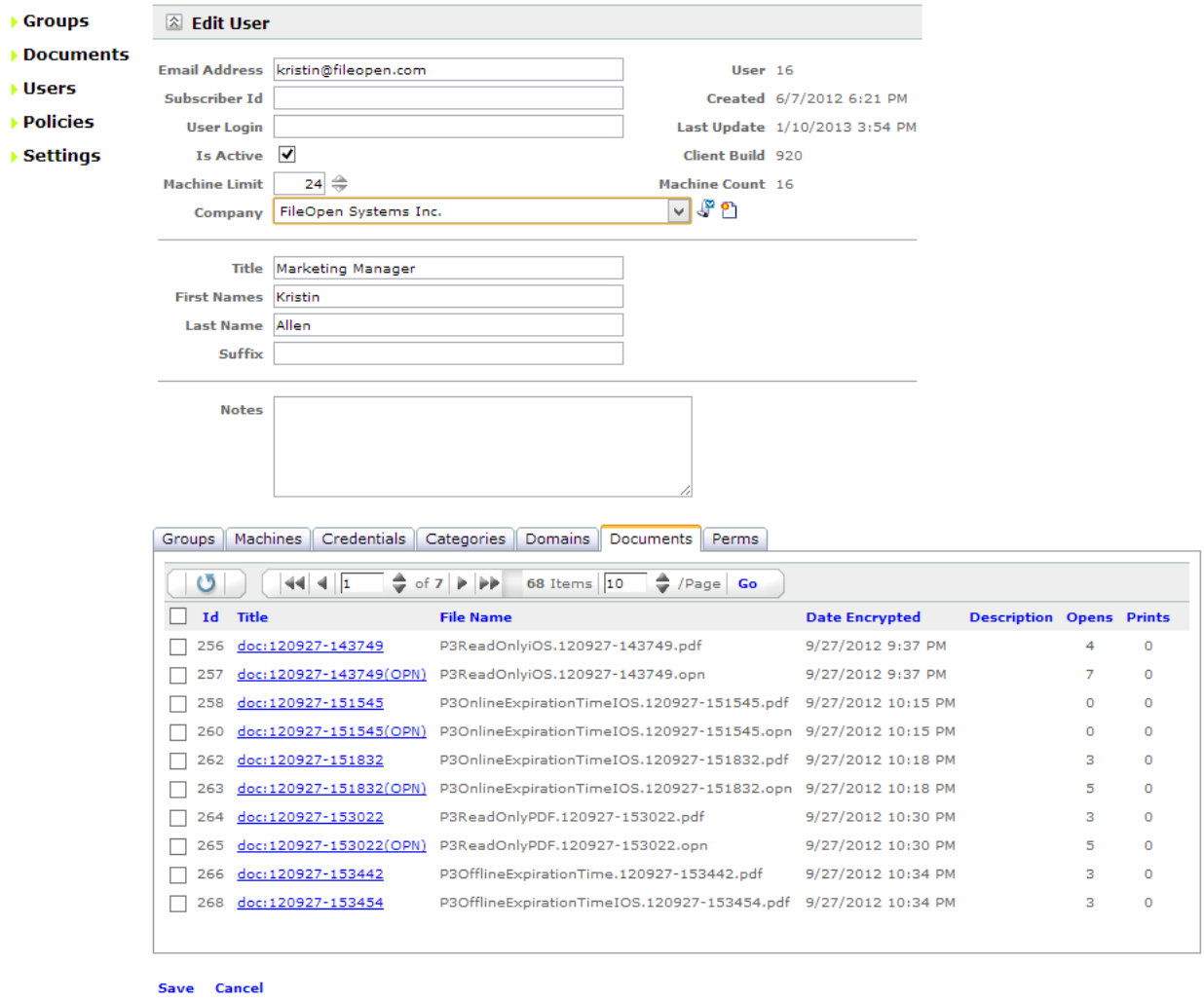


Edit User > Domains

Domain should only be populated when / if an Organization is using Domain Authentication. For more information, see document-level permissions are applied. .

Edit User > Documents

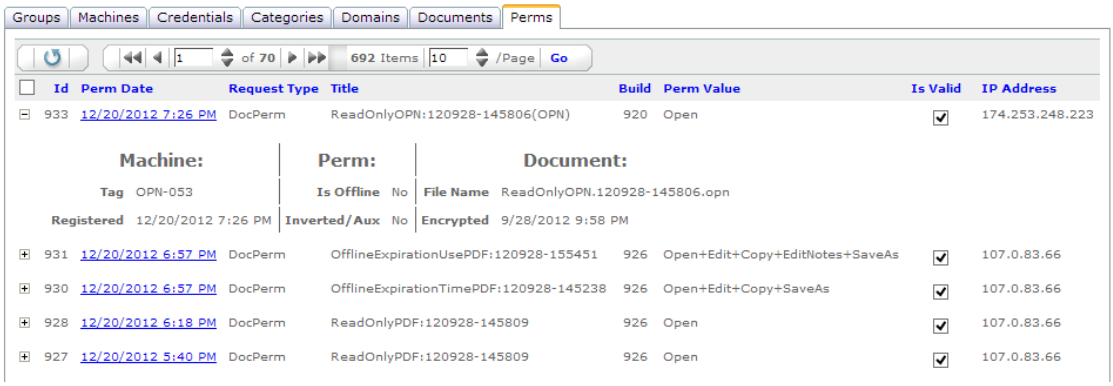
This tab provides quick access to Documents associated to this User, as well as a count of opens and prints. Administrators may also navigate into a specific Document record from this screen by clicking on the Document Title.



Edit User > Perms

This tab provides an audit record of which documents the User has opened, when and with what permissions.

iii. The checkbox Is Valid indicates the consumption of a permission. When necessary an Administrator may deselect this box to renew a User's permission.



User Properties

Field	Description
Email Address	(Mandatory) The unique identifier for a User.
Subscriber ID	Optional internal classification field that can be used as the Administrator sees fit. (Null or Unique values required)
User Login	Optional field tied to an User Login Authentication Policy.
Is Active (User)	Controls whether a User can consume permissions that have been granted. Unchecking this box will remove the User's global permissions and prevents the User from opening files or renewing access.
Machine Limit	Machine Limit determines the number of unique machines that a User may register, and therefore use to open Documents.
Company	Organization to which the User belongs
Title (User)	Prefix added to someone's name in certain contexts.
First Name	(Mandatory) User's given name
Last Name	(Mandatory) User's family name
Suffix	Western English-language naming tradition follows a person's full name and provides additional information about the person.
Notes	Optional field that can be used as the Administrator sees fit.
Machines	Users register machines by opening a FileOpen-protected document. Once a User has registered a machine, that machine will appear in the list on the Machines tab of the Edit User page.
Credentials	User identifying information used in User-based authentication (Username/password).
Categories	Administrators may classify Users into optional categories for internal classification / cataloging requirements. The Is Primary checkbox is intended to set the primary Category for a User in multiple categories. If no Primary is specified and Users are in multiple Categories then the oldest category classification will be considered Primary.
Domains (User)	Domain associated to a User in the context of Domain Authentication.

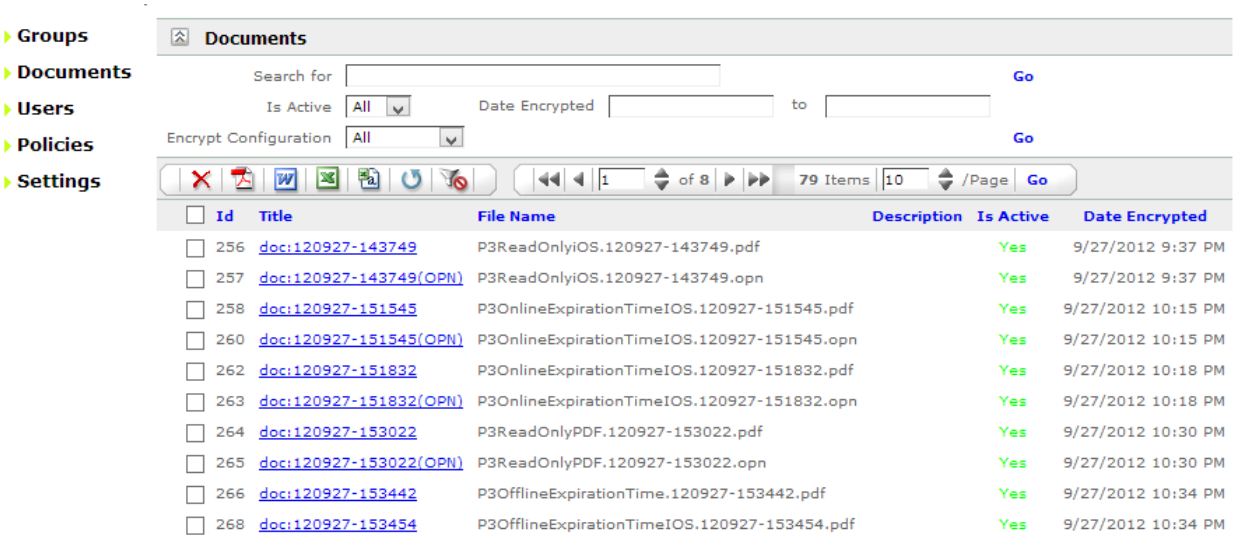
Figure 8: User Properties

Documents

The WebUI enables the management of document records, i.e. representations of encrypted documents. Documents are protected / encrypted locally through the Command Line Encryptor or Directory Monitor — no document content is ever stored on the PermissionServer nor is it accessible through the WebUI.

Locate a Document

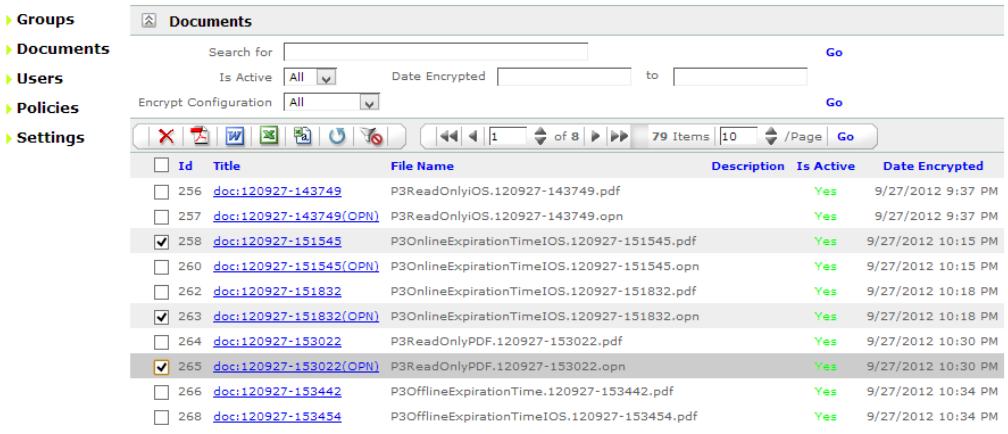
1. Navigate to Documents
2. Do one of these:
    a. Sort Documents by column headings, select the number of items to display, scroll through pages to find the Document.
    b. In the search field, type information about the Document, and then click Search.
    c. Filter by Date Encrypted, Document Status or Encryption Configuration.



Note: A complete listing of documents managed may be downloaded from this screen by selecting the file type download button above the column headings.

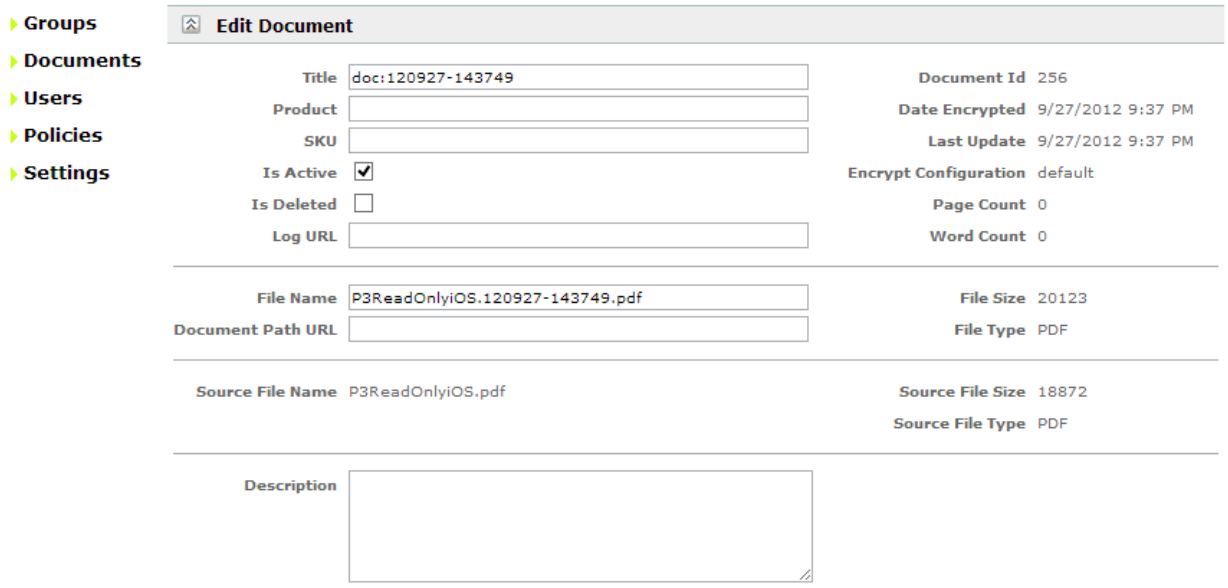
Delete a Document

1. FileOpen recommends making Documents inactive rather than deleting them from the database. However, Administrators may delete Documents by selecting the Document for deletion by checking the boxes next to the Document Id then click the Delete button .



Edit Document

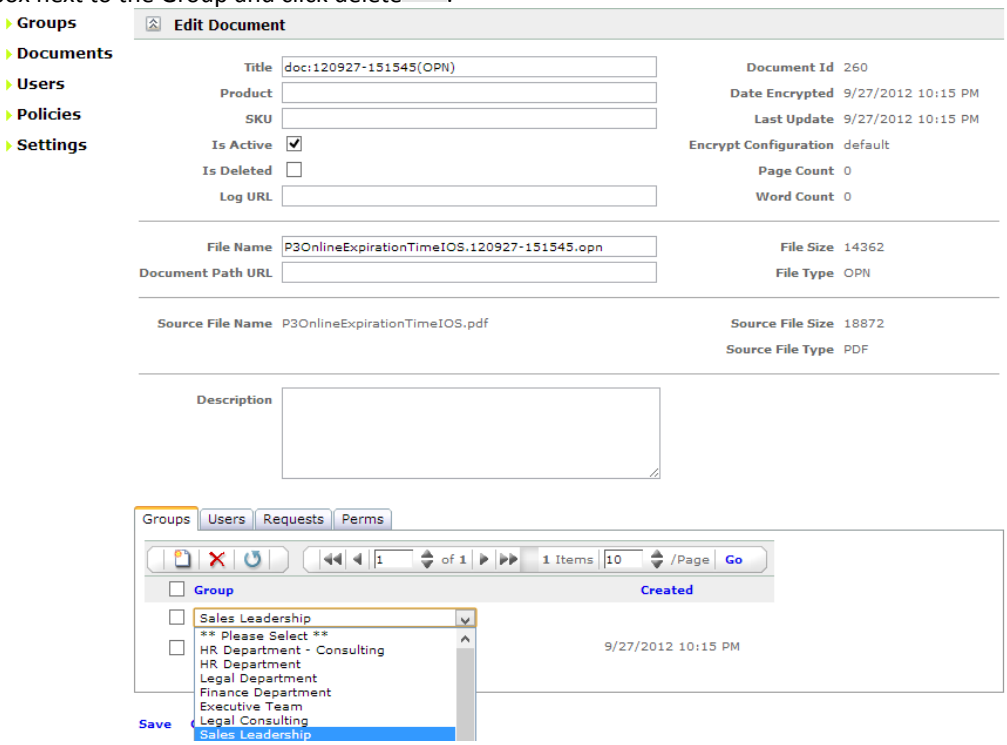
1. Navigate to Documents
2. Locate and click on the Document Title you wish to edit. From this screen you may edit document metadata and Group associations.
3. Within the Edit Document screen Administrators may modify document properties/metadata; such as, Title, File Name, Description, etc.
    i. The Document may also be disabled, and effectively removed from the system, by unchecking Is Active. Documents may be de-activated and re-activated at the Administrator's discretion.
    ii. Log URL at the document level should be populated with any parameters that should be appended to the Group level Log URL.
    iii. The Document Path URL should be populated only if the Administrator is using DocPath URL Authentication. If this is the case, the Administrator should input the specific URL from which a User may access the document.



Edit Document > Groups

Encrypted Documents may be added or removed from Groups via the Edit Document screen.

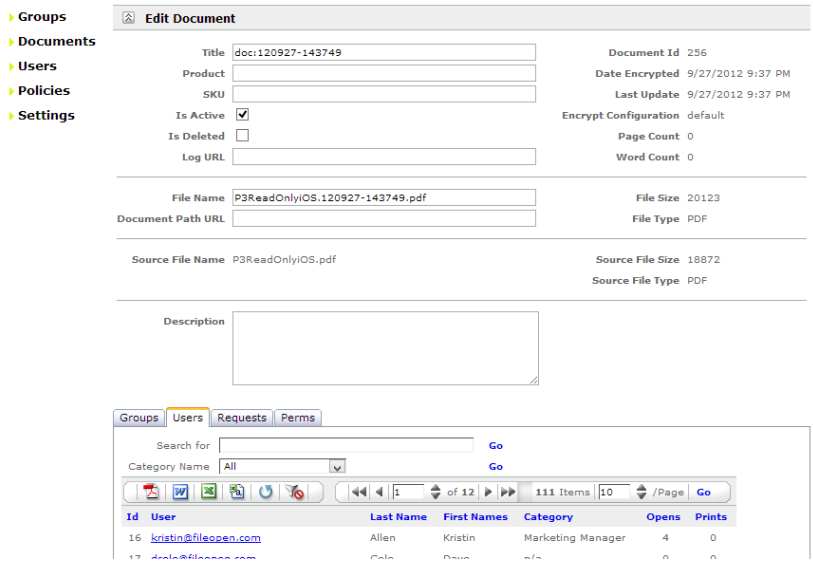
1. To add a Document to a group, navigate to the Group tab within the Edit Document screen. Click the new/add icon and select the appropriate Group from the pull-down menu.
2. To remove a Document from a Group, navigate to the Group tab within the Edit Document screen. Select the checkbox next to the Group and click delete.



Important: The freedom to place a Document into multiple Groups creates the potential for conflicting Permissions. The Group's priority determines the appropriate Permissions to provide when a document is in more than one Group. In the event of a conflict, permissions for the Group with the highest Priority will be granted. Priority is assigned numerically, with 1 being the highest priority, 2 being next, etc.

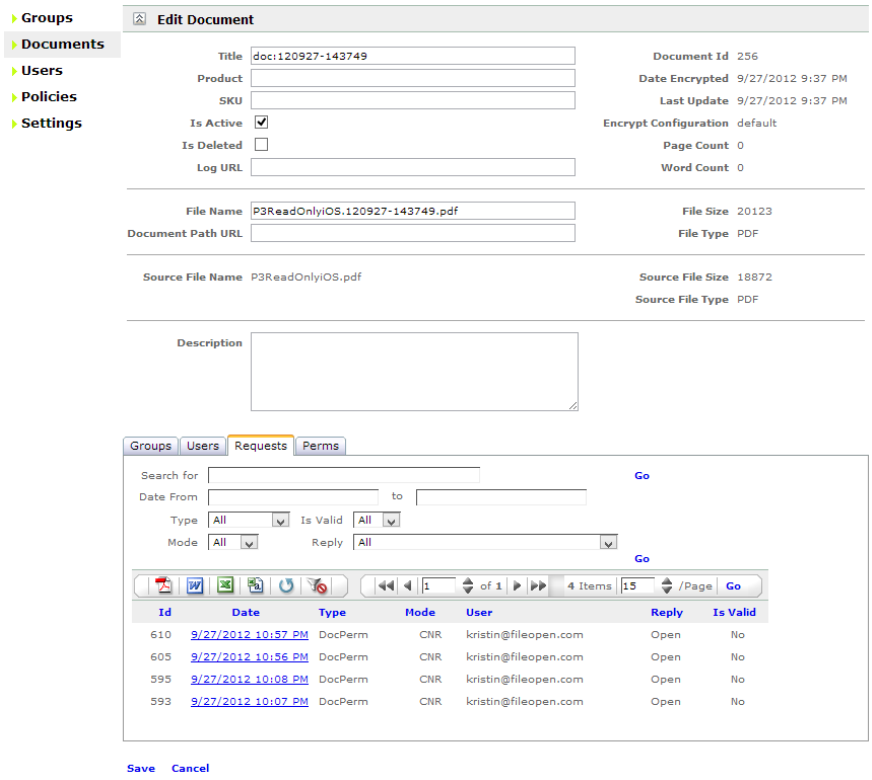
Edit Document > Users

This tab provides quick access to Users associated to this document. Administrators may navigate into a specific User record on-the-fly from this screen. User reports may be downloaded from this screen by selecting the file type download button above the column headings.



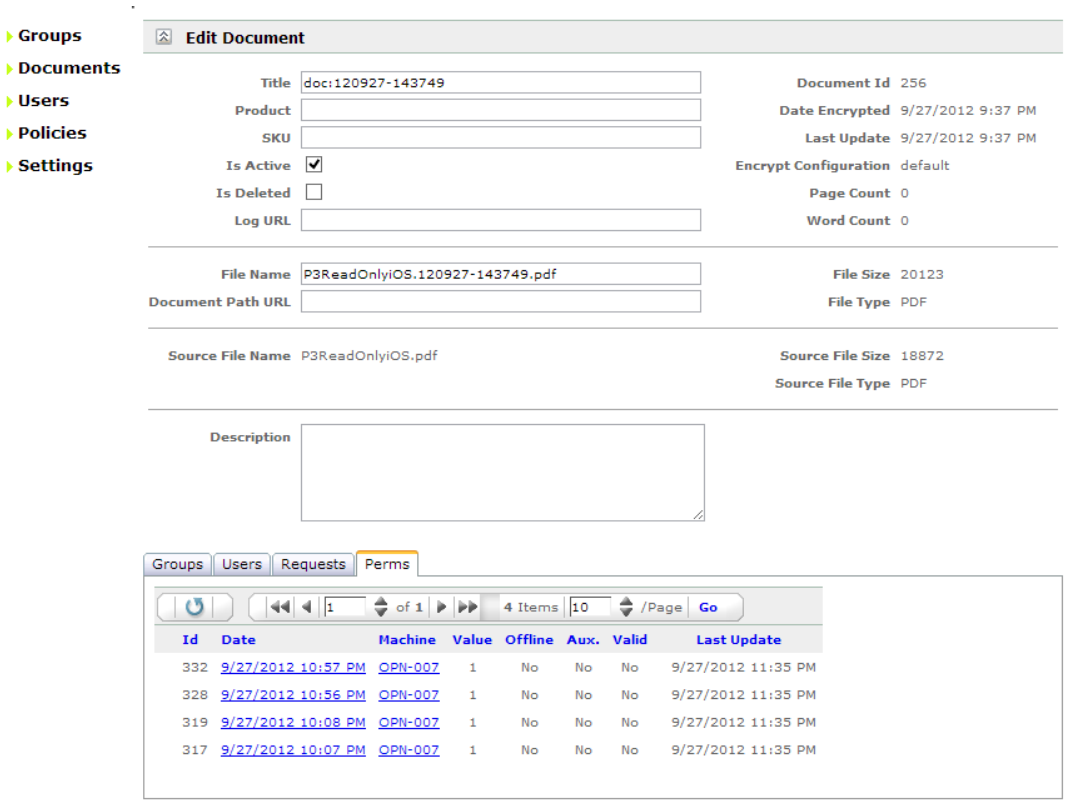
Edit Document > Requests

This tab provides a list of all Requests and Replies for access to a specific Document. Administrators may filter by date, type, mode, and Reply for Document use analysis. Request reports may be downloaded from this screen by selecting the file type download button above the column headings.



Edit Document > Perms

This tab provides a list of all permissions consumed for this specific Document.



Add or Create a Document

The Web UI is intended for User, Group and Policy management purposes. For more information on encrypting / protecting documents, see FileOpen Encryption Modules.

Document Properties

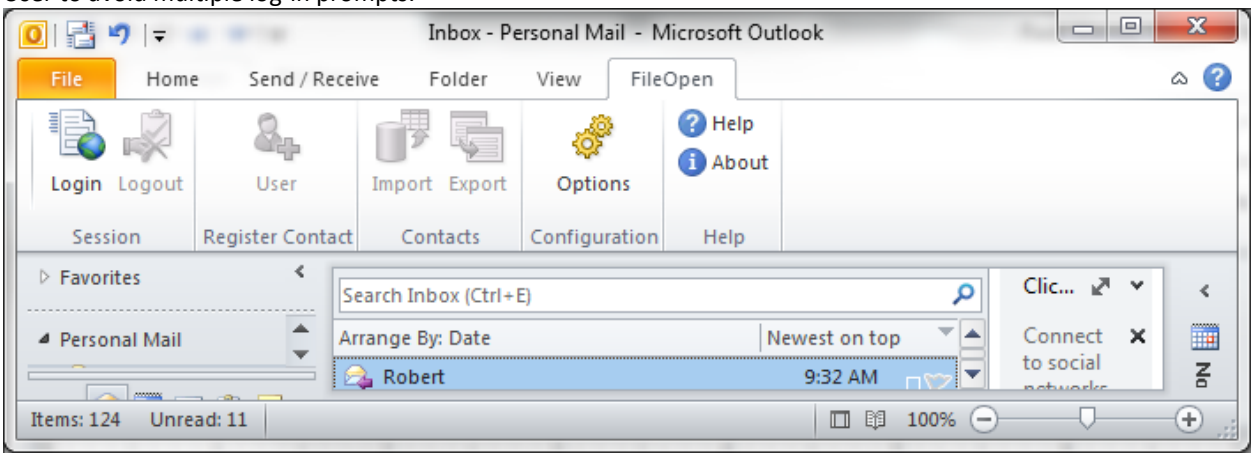
Field	Description
Title (Document)	The Document Title is a unique identifier, which is automatically created when the document is encrypted. Titles may be edited at any time but should always be unique.
Product (Document)	Documents may have a Product assigned for further segmentation or business purposes as deemed appropriate.
SKU	Documents may have SKUs assigned for further segmentation or business purposes as deemed appropriate.
Is Active (Document)	The checkbox Is Active controls the state of the Document; if unchecked the Document is disabled.
Is Deleted (Document)	The checkbox Is Deleted removes document visibility from the WebUI. This action cannot be undone form the WebUI. If you have deleted a Document in error please contact FileOpen Support.
Log URL (Document)	The URL / Web page an Administrator may route failed attempts to open a file.

File Name	The Document File Name is a concatenation of the original file name and automatically generated identifiers created when the document is encrypted.
Source File Name	The original/unencrypted source file name of the Document.
Document Path URL	Used in Doc Path URL authentication. Document Path URL allows Administrators to designate a particular URL that the Document may be access from.
Description	Optional field to be used as deemed appropriate.

Figure 9: Document Properties

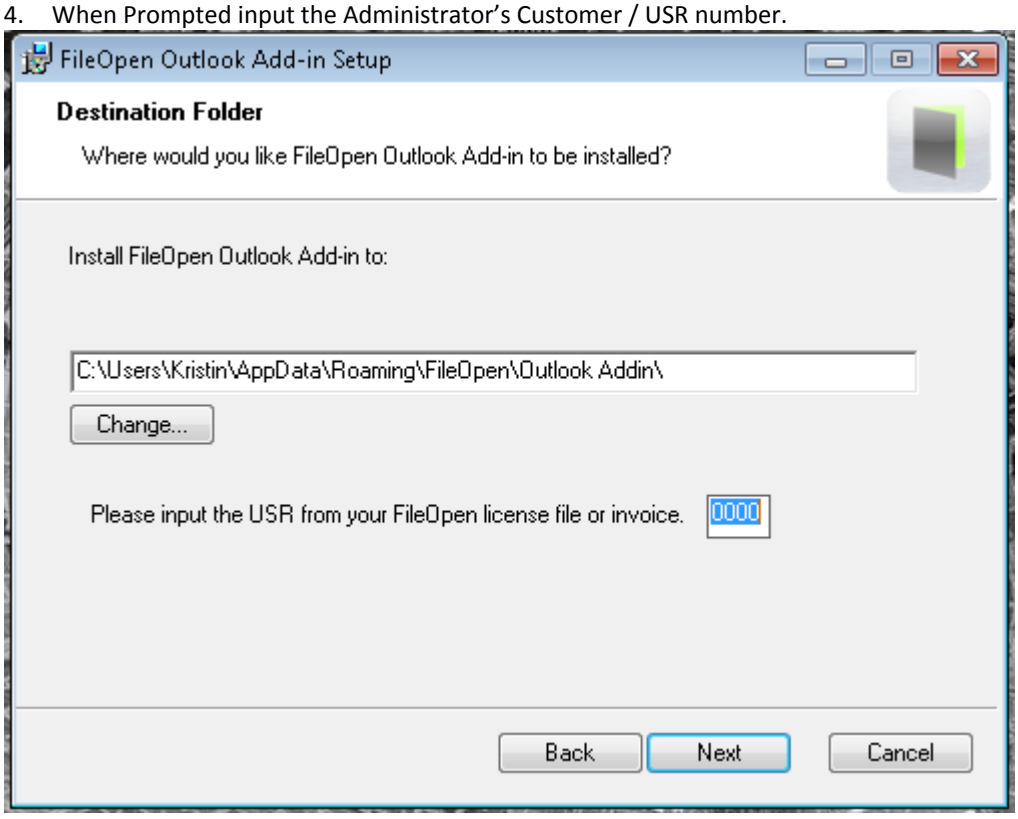
FileOpen Outlook Add-in

The FileOpen Outlook Add-in is an application designed to create and send machine/device registration invitations to Users. Once a User receives and opens a registration PDF, that User/Machine combination becomes registered in the PermissionServer. All subsequent access requests are processed by validating machine identifiers, thus allowing the User to avoid multiple log-in prompts.



Installing Outlook Add-in

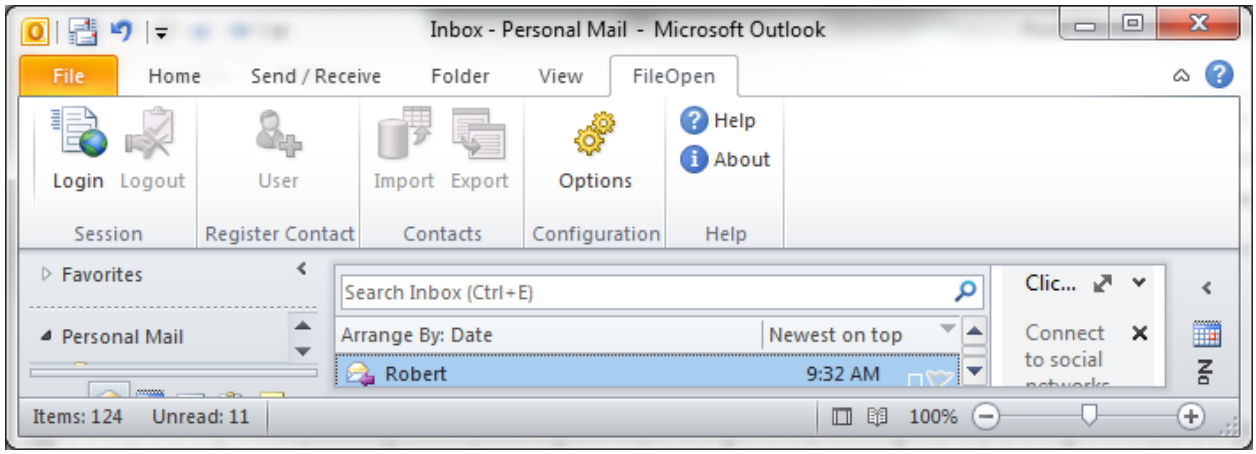
1. Download and save the FileOpen Outlook Add-in installer.
2. Double click the downloaded file to begin the installation.
3. Click on the **Run** button and follow the installation wizard instructions.
4. When Prompted input the Administrator's Customer / USR number.



Operating the Outlook Add-in

Login

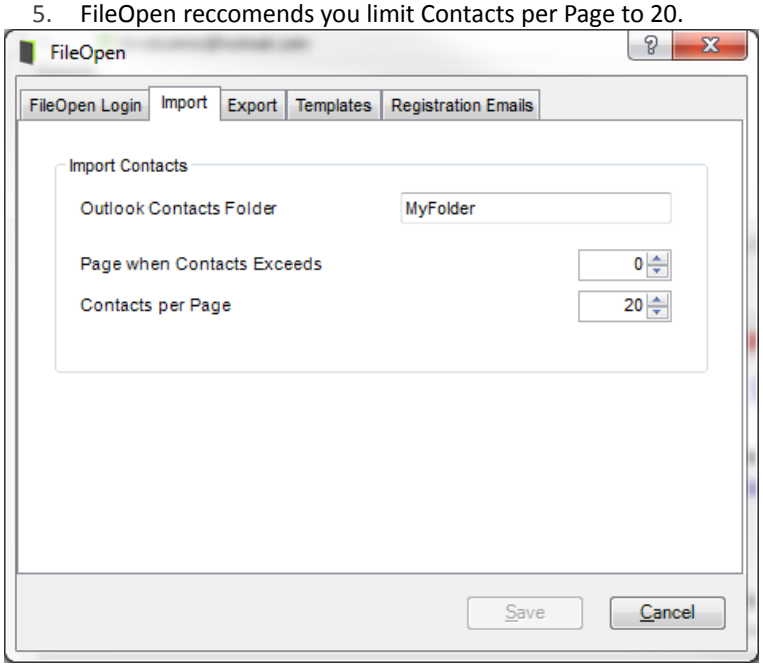
Once the Add-in is installed the Administrator will have a new FileOpen tab at the top of their Outlook Ribbon. Administrators will need to Login prior to using any of the functionality available here.



Importing Users

For ease of administration, an Administrator may import Users from the Permission Server into a Contact Folder within Outlook. Before this can be done the Administrator should specify preferences within the FileOpen Add-in.

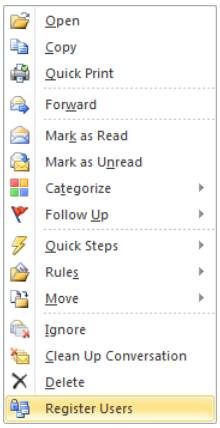
1. Navigate to Configuration>Options in the FileOpen ribbon menu.
2. Select the Import tab at the top of the dialog box.
3. Name the Outlook Contact Folder where imported Users will reside.
4. Throttle or page the amount of User records imported at one time. Leveraging this feature will ensure minimal impact to Outlook processes.
5. FileOpen reccomends you limit Contacts per Page to 20.



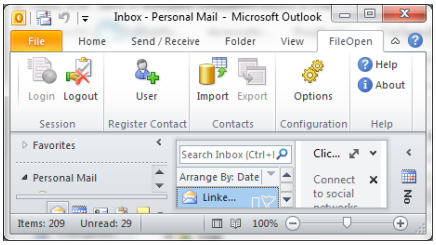
Creating a Registration Email

Administrators may create registration emails from the Contact or Email View. The Administrator may either:

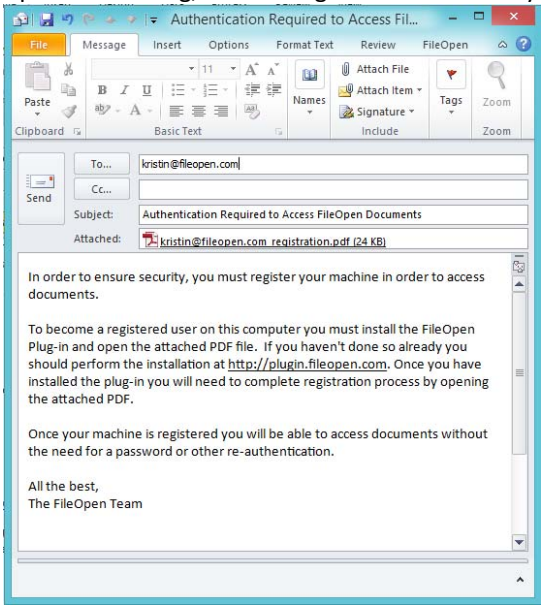
1. Right-click on the Contacts email address to expose the “Register User” icon.



2. Select Register User from the FileOpen Add-in Ribbon Menu.



The RegistrationPDF is then generated and attached to a registration email if the User. If the administrator has chosen to preview the Registration message prior to sending, the message will automatically open.

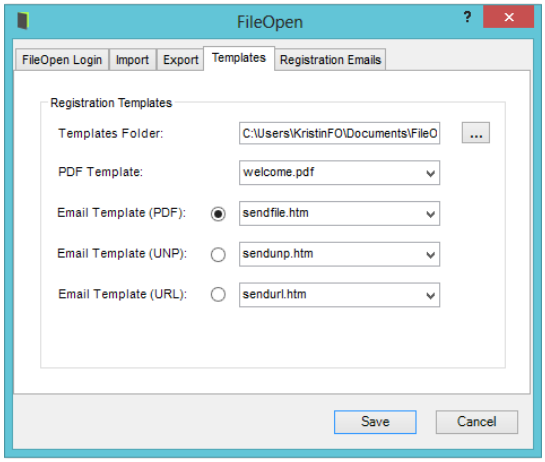


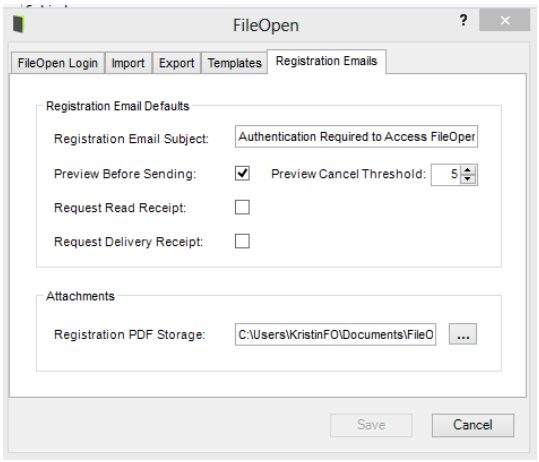
Administrators may create a registration email for any Contact that has a User record within the PermissionServer. If a User does not exist within the PermissionServer, the Outlook Add-in will not generate an email.

Editing Templates

Administrators may customize the Registration email message body and registration PDFs to match their brand or workflow requirements.

1. Navigate through a File/Windows Explorer to C:\Users\{Name}\Docuemtns\FileOpen\Templates.
    a. Add custom HTM files for the message body content.
    b. Add custom PDF files for the base registration PDF.
2. Navigate to Configuration>Options in the FileOpen ribbon menu.
3. On the Templates tab select the new Email Template (PDF) or PDF Template from their respective drop-down menus.
4. On the Registration Emails Tab Administrators may customize the subject line of the message.
5. Press Save to implement the change and close the dialog.





Outlook Add-in Properties

Label	Description
Session	The area allows the Administrator to log-in an out of their PermissionServer. NOTE: Control for the duration of a session is defined in the RightsManager.
Register Contact	The Register Contact function generates a specially encrypted PDF document and email message without leaving Outlook. The Registration PDF when opened is a means by which a User authenticates and registers their Machine with the PermissionServer.
Import Contacts	Coming Soon: Allows Administrators to import Users from the Permission Server into an Allows Administrators to import User record's from the PermissionServer into an Outlook Contacts Folder.
Page when Contacts Exceeds	Allows the Administrator to throttle the amount of User/Contact records imported from the PermissionServer at one time.
Contacts per Page	The increment by which User/Contact records are Paged.
Export Contracts **Coming Soon!**	Allows Administrators to export Outlook Contacts Folders to the PermissionServer.
Username	The Administrator's username used to establish a connection/session with their PermissionServer. By default all email addresses associated to that Outlook account will be available in the drop down menu. An Administrator may also add a Username if the appropriate value is not available.
Remember Last Login	This option allows Administrators to save the identified Username for future sessions.
Login Automatically	This option allows Administrators to automatically log-in to the PermissionServer when Outlook starts.
Password	The password that will be used to authenticate the Administrator with the PermissionServer.
Outlook Contacts Folder	Allows the Administrator to designate the Outlook Contacts Folder name used with the Import function.
Page when Contacts Exceeds	Allows the Administrator to throttle the amount of User/Contact records imported from the PermissionServer at one time.
Contacts per Page	The increment by which User/Contact records are Paged.
Templates Folder	Location registration email templates are stored.
PDF template	This drop-down menu allows Administrators to select the PDF template used with User registration emails.
Email template (PDF)	This drop-down menu allows Administrators to select the message body text to be used when registration PDFs are distributed to Users.
Email template (UNP)	This drop-down menu allows Administrators to select the message body text to be

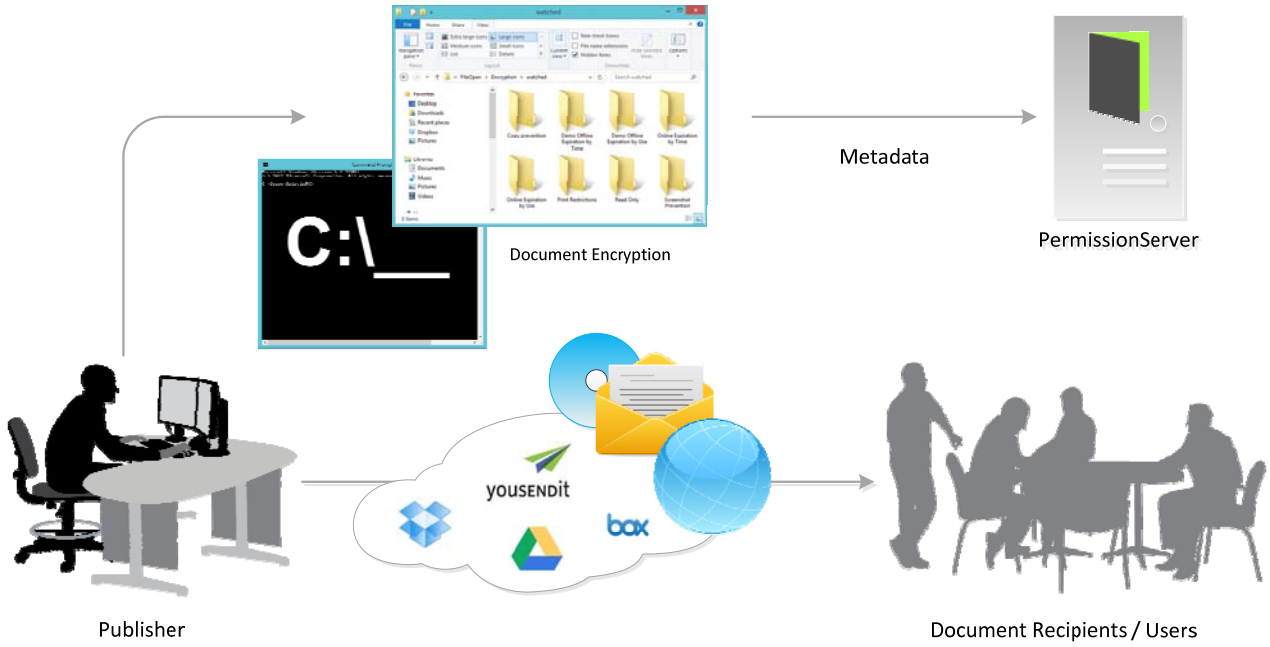
Coming Soon!	used when Username/Password credentials are distributed to Users.
Email template (URL) **Coming Soon!**	This drop-down menu allows Administrators to select the message body text to be used when authentication URLs are distributed to Users.
Registration Email Subject	Allows Administrators to specify the subject line of registration emails distributed to Users.
Preview Before Sending	This option allows Administrators to indicate whether they wish to preview registration emails before they are sent to Users.
Preview Cancel Threshold	Allows the Administrator to cancel the preview of registration emails when sending large batches.
Request Read Reciept	Provides Administrators a method to monitor the opening of a registration email.
Request Delivery Receipt	Provides Administrators a method to monitor the delivery of a registration email.
Registration PDF Storage	Location where encrypted Registration PDFs are stored.

Figure 10: Outlook Add-in Properties

FileOpen Encryption Modules

Documents are encrypted at a RC4 128-bit or AES 256-bit key in accordance with the specifications for that file format; details of which are available from Adobe Systems[6].

During the encryption step, each document is assigned an encryption key, Group information and a set of metadata. All metadata other than the Encryption Key is stored in the document and document identifiers and Group Information are stored in the PermissionServer. The Encryption Key is used to encrypt the document, and then is discarded. By design document content is never stored on the PermissionServer.



An Administrator encrypts documents on locally using the Commandline Interface or the Directory Monitor. Metadata from encryption process is stored on FileOpen PermissionServer. Encrypted documents may be distributed to end user via any channel (website, email, CD-ROM).

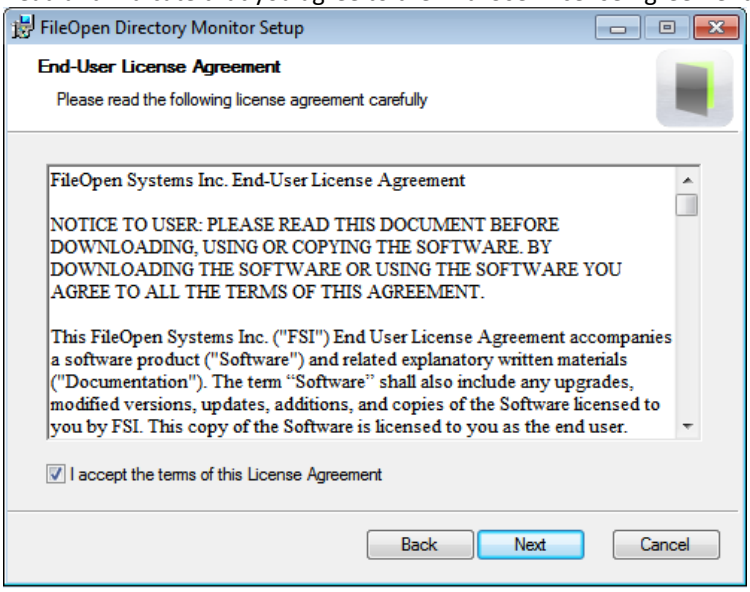
[6] http://partners.adobe.com/asn/tech/pdf/specifications.jsp

Directory Monitor

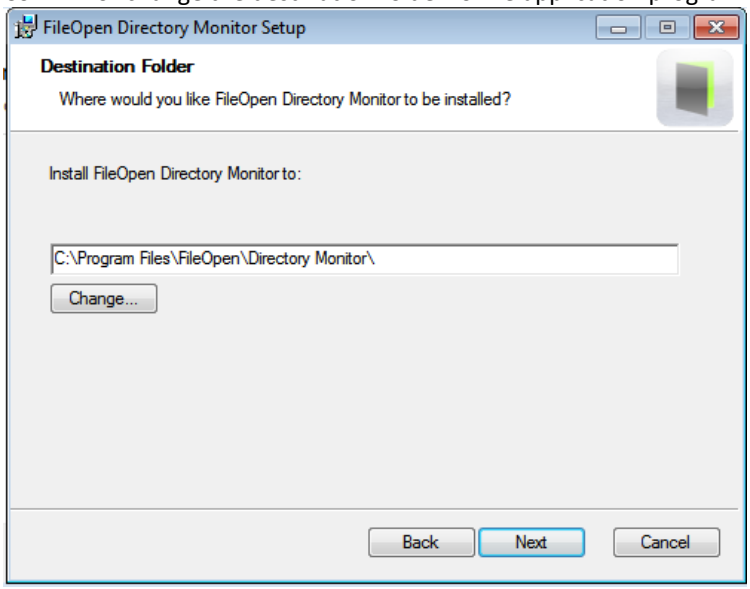
The FileOpen Directory Monitor Encryptor is a drag-and-drop GUI application that encrypts documents and allows Group/Policy designation.

Installing Directory Monitor

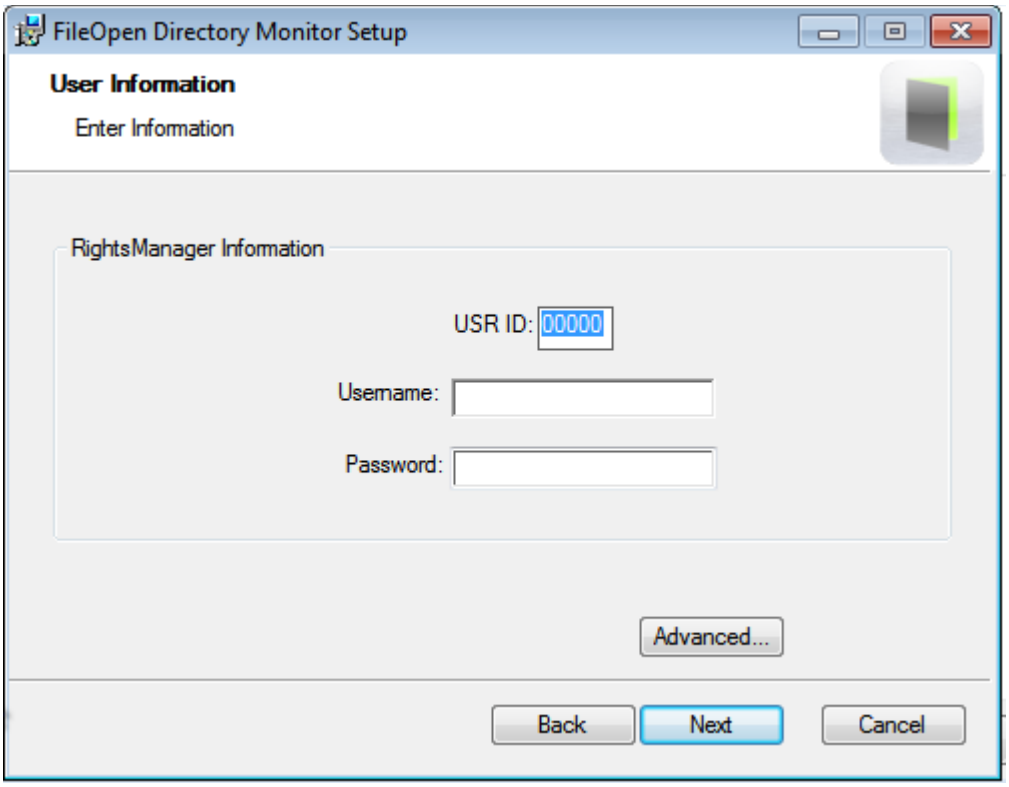
1. Download and save the FileOpen Directory Monitor installer from the link provided.
2. Double click the downloaded file to begin the installation.
3. Click on the Run button and follow the installation wizard instructions.
4. Read and indicate that you agree to the End-User License Agreement on screen one.



5. Confirm or change the destination folder for he application program files.



6. When Prompted input the Administrator's Username/Password, as well as the Customer / USR number.

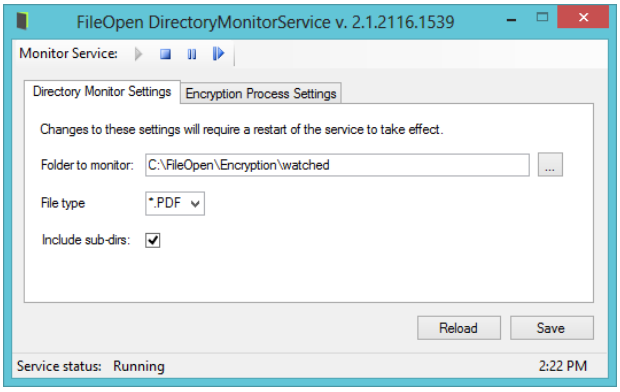


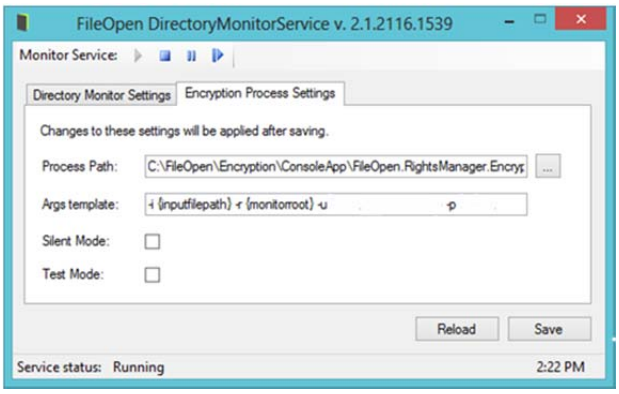
7. Select Next and Finish.

Configuring the Directory Monitor Service

The Directory Monitor Service is installed preconfigured defaults and in most cases will not need customization. However, Administrators may re-configure defaults as follows:

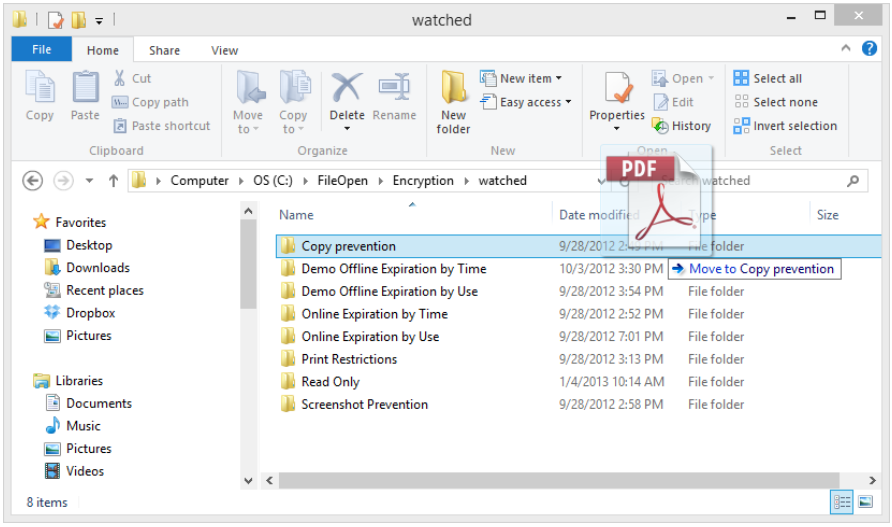
1. Launch the Directory Monitor Service from the Start Menu.
2. Within "Directory Monitor Settings"
    a. Administrators may edit which folder is watched or monitored
    b. Check Include Sub-directories to enable the use of Group designation / sub-folders within the Watched folder.
3. Within the "Encryption Process Settings"
    a. Administrators may append the "Args template" field with different Administrator credentials using the following syntax –u {insert username} –p {insert password}
    b. Administrators may edit the encrypted file output folder by adding –o command to the "args template".
        i. This should be a fully qualified path; use double quotes if the path contains any spaces.
    c. Silent Mode option disables the display of the Command Window.
    d. Test Mode creates a diagnostic file of the watched directory operation and interaction with the Command Line Encryptor.



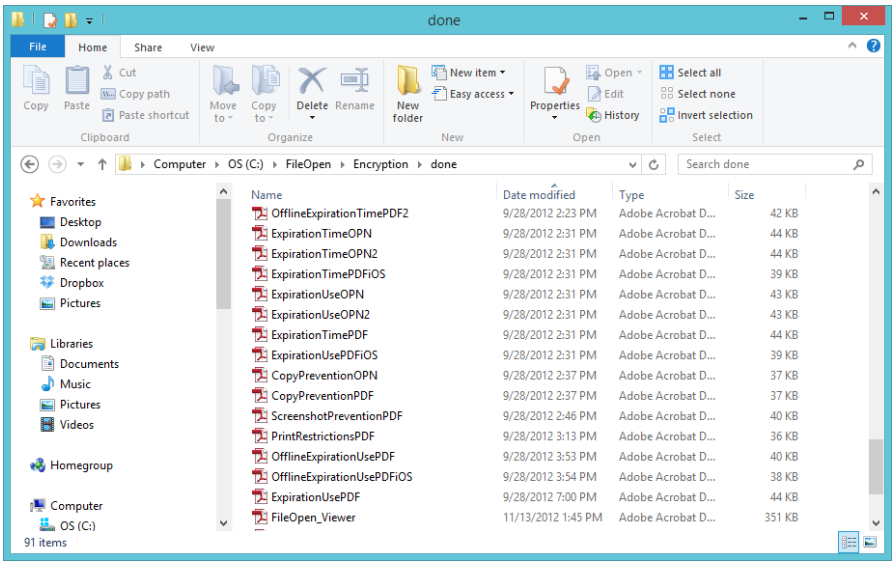


Operating the Directory Monitor

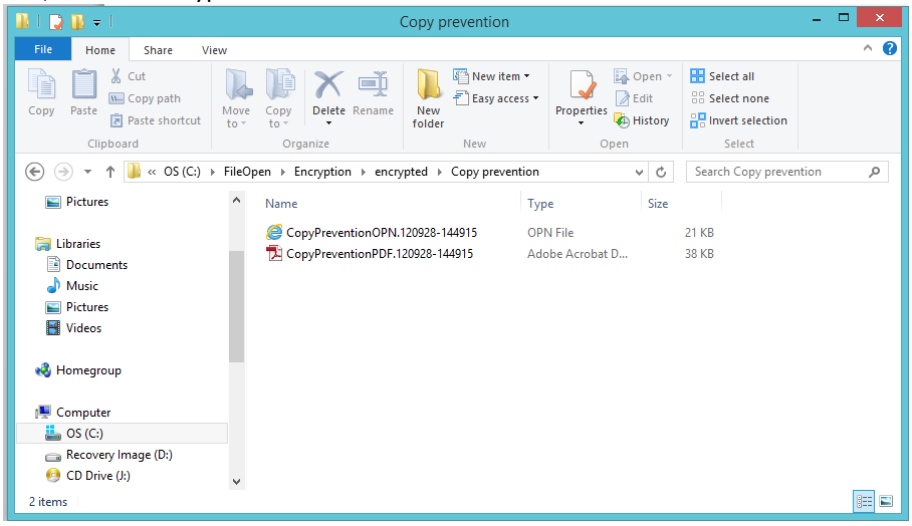
Once configured, Administrators simply drag source files into the desired Watched folder or sub-folder as demonstrated in the image below.



The unencrypted source file is moved and stored in the “done” folder.



As a result an encrypted version of the file appears within the Encrypted folder / sub-folder. Depending on the Administrators license, both an encrypted PDF and OPN format file is created.



Watched and Encrypted Folders / Sub-folders

Administrator may add sub-directories/sub-folders within the Directory Monitor watched folder to designate a document's membership within a Group. For more information of on creating and managing Groups, see Groups.

Important: Sub-folders created within the Watched folder to designate Group membership must be named exactly as the Group is named in the PermissionServer. Otherwise, the Directory Monitor will create a new Group within the PermissionServer with the default Policy Set.

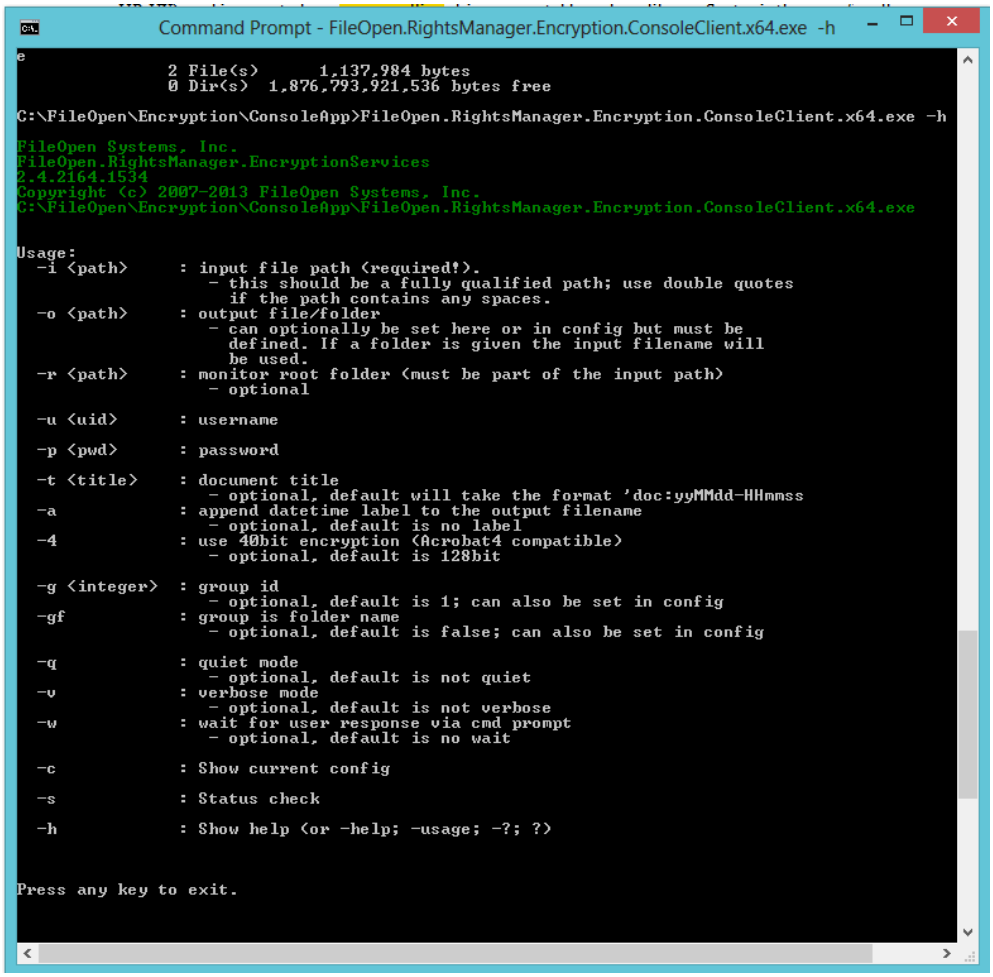
Command Line Encryptor

FileOpen Command Line Encryptor is a text-based user interface, and is operated as a commandline-driven executable. A license file with the suffix .lic must be present in the directory from which the Command Line Encryptor is run.

The Command Line Encryptor is an advanced Administrator tool and relies on a basic understanding of programming language.

Opening the Command Line interface

1. Navigate to the FileOpen Console App, typical installation is C:\FileOpen\Encryption\ConsoleAppFileOpen.RightsManager.Encryption.ConsoleClient.x64



Command Line Usage / Syntax

Syntax for and operation of the Command Line Encryptor is the same whether files are being encrypted offline on a desktop system or online on a server. It is irrelevant, from the perspective of the client software, when and where the file was encrypted.

Usage	Description
-i <path>	Input file/folder path. This should be a fully qualified path; use double quotes if the path contains any spaces. Recommended usage is single file input. Administrators should use folder input selectively – large folders will impact performance based on local machine and

	server resource availability.
-o <path>	Output file/folder. Can optionally be set here or in config but must be defined. If a folder is given the input filename will be used.
-r <path>	Monitor root folder (must be part of the input path). - optional
-u <uid>	Username
-p <pwd>	PasswordLimit
-t <title>	Document title - optional, default will take the format 'doc:yyMMdd-HHmmss
-a	Append datetime label to the output filename - optional, default is no label
-4	Use 40bit encryption (Acrobat4 compatible). Optional, default is 128bit
-g <integer>	group id- optional, default is 1; can also be set in config
-gf	group is folder name - optional, default is false; can also be set in config
-q	quiet mode - optional, default is not quiet.
-v	verbose mode - optional, default is not verbose
-w	wait for user response via cmd prompt - optional, default is no wait
-c	Show current config
-s	Status check
-h	Show help (or -help; -usage; -?; ?)

Errors Defined by Command Line Encryptor

Encryptor Library Errors

Class	Error #	Error name
Encryptor	9051	MemoryAlloc
	9052	InputFileNotFound
	9053	OutputFileNotFound
	9054	LicenseError
	9055	NotEncryptLicense
	9056	NotValid
	9057	InvalidLicenseSet
	9058	
	9059	InvalidInfoSettings

	9060	DocumentError
	9061	UnmanagedError
	9065	DeLinearized
CryptInfo		
XchInfo		

A typical error will be in the form:
- 9060 == Document error (the encryptor finds an error in the document)
- 1623 == Ill formed PDF file == The document was first created as a linearized document (it has a linearized dic) but was modified later (it has multiple xref tables).

There are two ways to encrypt such a document:
- The safe one: open it then resave it linearized (perhaps with another name) before encrypting it.
- The unsafe one: set the force bit; there is no guarantee that the encrypted file will be well-formed.

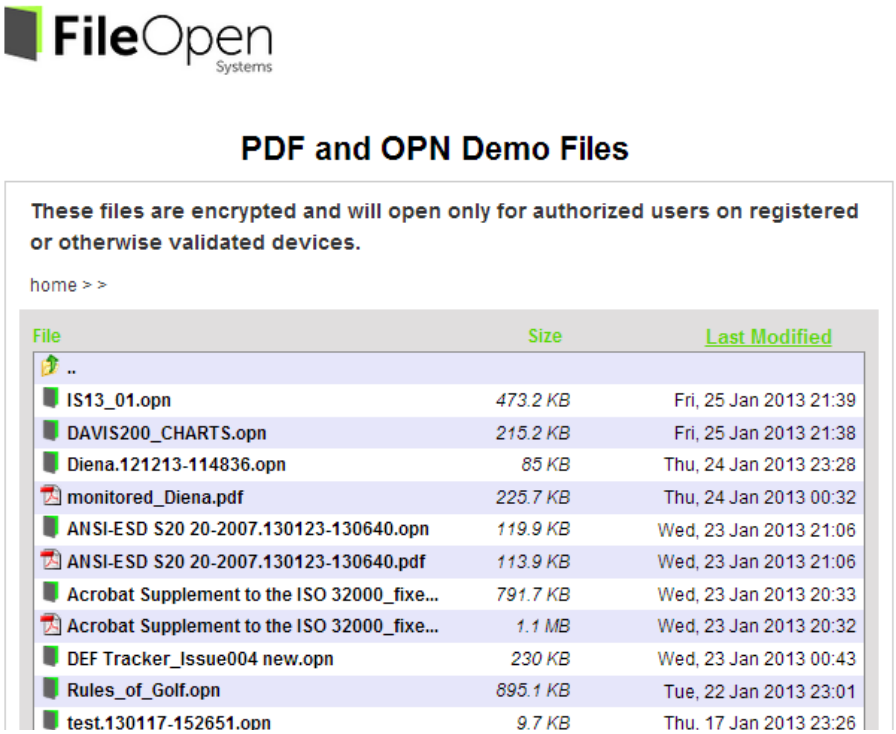
Error Condition	Error Number
ERROR_NONE	0
ERROR_CANNOT_OPEN_INPUT	1
ERROR_CANNOT_OPEN_OUTPUT	2
ERROR_ADD_NUMBER_NO_MEMORY	3
ERROR_NO_LENGTH_IN_STREAM_OBJECT	4
ERROR_WRITE_ERROR	5
ERROR_READ_ERROR	6
ERROR_BAD_STRING_LENGTH_ATTRIBUTE	7
ERROR_NUMBER_REF_NOT_FOUND	8
ERROR_NO_STREAM_BUFFER_MEMORY	9
ERROR_ENCRYPTION_FAIL	10
ERROR_STREAM_OBJECT_REF_NOT_FOUND	11
ERROR_NO_STARTXREF_FOUND	12
ERROR_FSEEK_FAILED	13
ERROR_FPUTS_FPRINTF_FAIL	14
ERROR_UNEXPECTED_READ_ERROR_OR_EOF	15
ERROR_NO_SIZE_IN_EXISTING_TRAILER	16
ERROR_FILE_ALREADY_ENCRYPTED	17
ERROR_INPUT_AND_OUTPUT_DIRS_ARE_SAME	18
ERROR_NO_MEMORY_FOR_OBJECTS	19
ERROR_LONG_NOT_SAME_SIZE_AS_INT	20
ERROR_INVALID_OBJECT_NUMBER	21
ERROR_LINE_ENDED_IN_STRING	22
ERROR_UNEXPECTED_BACKSLASH_ERROR	23
ERROR_STRING_TOO_LONG	24
ERROR_DUFF_HEX_STRING	25
ERROR_NO_EOF_FOUND	26
ERROR_BAD_ROOT_IN_TRAILER	27
ERROR_NO_ROOT_IN_EXISTING_TRAILER	28
ERROR_CANNOT_OPEN_KEYVALUE_FILE	29
ERROR_NO_EQUALS_SIGN_IN_KEYVALUE_FILE_LINE	30
ERROR_NO_NAME_OR_VALUE_IN_KEYVALUE_FILE_LINE	31

ERROR_ROOT_OBJECT_NOT_FOUND	32
ERROR_LONG_LONG_NOT_64	33
ERROR_ENCRYPTED_STRING_TOO_SMALL	34

viewer.fileopen.com

viewer.fileopen.com is an optional browser-based application that may be added to the Directory Monitor application to extend distribution capabilities. The application allows Administrators to selectively post protected documents to a dedicated URL as the document is encrypted.

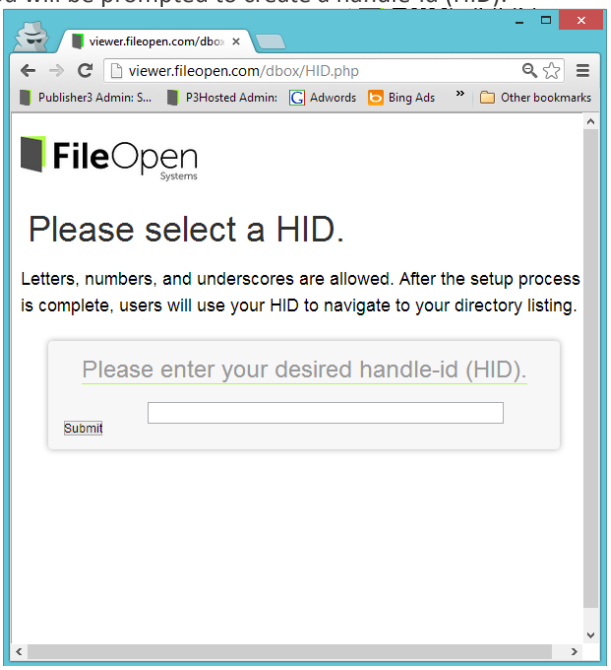
viewer.fileopen.com works in conjunction with standard file sharing sites; at present Administrators are required to have a Dropbox account. Keep in mind that once a Document is encrypted, it can be securely distributed through whatever mechanism or protocol most appropriate.



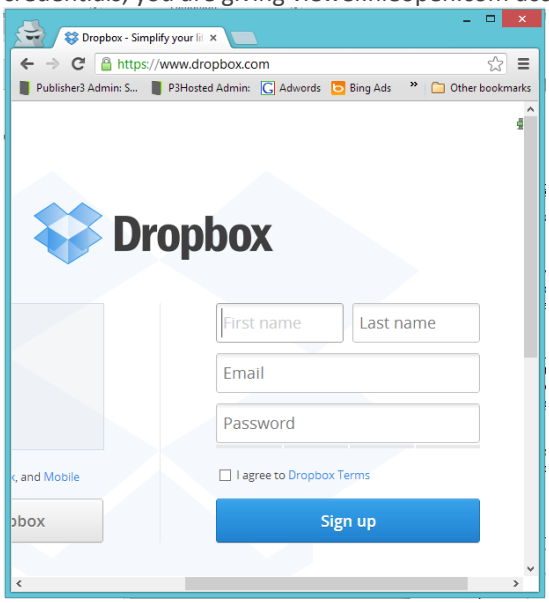
Configuring viewer.fileopen.com

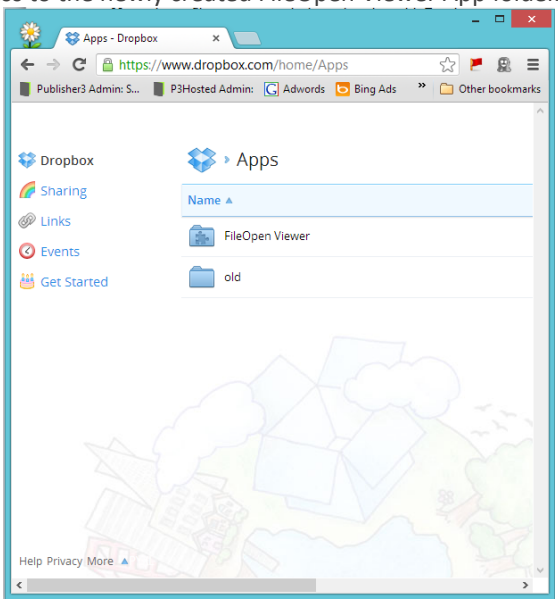
The first step in setting up viewer.fileopen.com is to create a handle-id. The handle-id created is added to the base URL of fo.pn/{handle-id}. This is the destination URL that Administrators share with their Users as a form of protected-document distribution.

1. Go to fo.pn/setup where you will be prompted to create a handle-id (HID).



2. Once you have created a HID, you will be redirected to Dropbox to provide your account credentials. After the authentication process is complete, a folder called FileOpen Viewer App is created in the Apps folder. If there is not yet an Apps folder located in your root Dropbox folder, one will be created. By providing Dropbox credentials, you are giving viewer.fileopen.com access to the newly created FileOpen Viewer App folder.

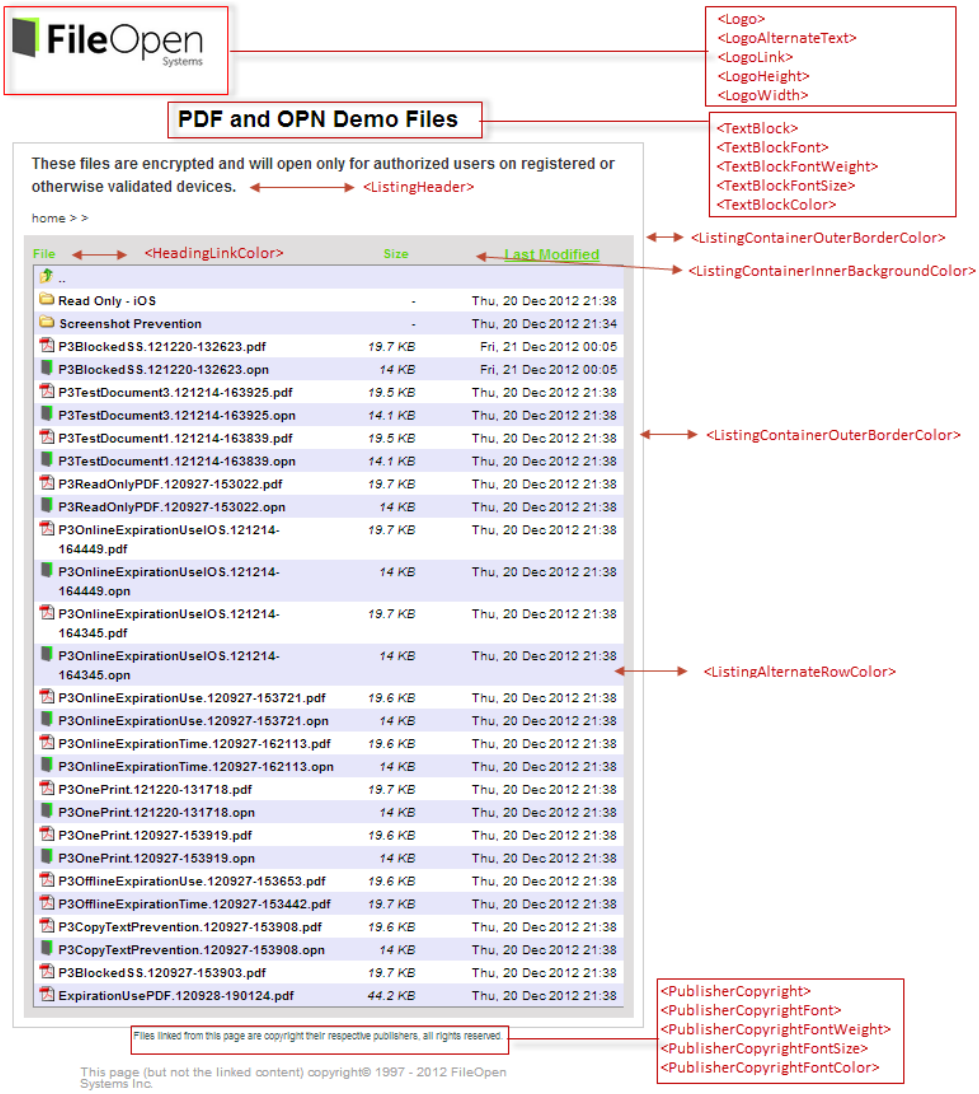




Customizing viewer.fileopen.com

Administrators may customize the presentation of viewer.fileopen.com according to brand and business requirements. This is done by editing the ListConfig.xml within the FileOpen Viewer app folder in Dropbox[7].

Administrators may edit the default XML elements as outlined and defined below.



[7] The config.xml file is only visible / editable by Administrators with the appropriate DropBox credentials.

Editable XML Elements

XML Tag	Description
<Title> </Title>	Text to be used as a title tag, which is the main text that describes the page. Title tags are also visible to Users within the top of a browser or applicable tabs.
<Logo> </Logo>	Source attribute of an HTML image tag that points to the Administrators logo. For example, http://viewer.fileopen.com/FileOpenlogo200.png
<LogoAlternateText> </LogoAlternateText>	Text to be presented to page visitor if the URL for the Logo fails.
<LogoLink> </LogoLink>	Destination URL used when a visitor clicks the Logo image.
<LogoHeight></LogoHeight>	Height of image, in pixels.
<LogoWidth></LogoWidth>	Width of image in Pixels.
<TextBlock></TextBlock>	Text block below the Logo.
<TextBlockFont></TextBlockFont>	CSS font property.
<TextBlockFontWeight> </TextBlockFontWeight>	CSS font property.
<TextBlockFontSize> </TextBlockFontSize>	CSS font property.
<TextBlockColor> </ TextBlockColor >	CSS color property.
<ListingContainerOuterBorderColor> </ListingContainerOuterBorderColor>	CSS color property.
<ListingHeader></ListingHeader>	Text to be presented.
<HeadingLinkColor> </HeadingLinkColor>	CSS color property.
<ListingContainerInnerBackgroundColor> </ListingContainerInnerBackgroundColor>	CSS color property.
<ListingAlternateRowColor> </ListingAlternateRowColor>	CSS color property.
<PublisherCopyright> </PublisherCopyright>	Text to be presented in copyright area.
<PublisherCopyrightFont> </PublisherCopyrightFont>	CSS font property.
<PublisherCopyrightFontWeight> </PublisherCopyrightFontWeight>	CSS font property.
<PublisherCopyrightFontSize> </PublisherCopyrightFontSize>	CSS font property.
<PublisherCopyrightFontColor> </PublisherCopyrightFontColor>	CSS color property.
<BackgroundColor> </BackgroundColor>	CSS color property.
<Icon></Icon>	URL for favicon.
<ListingItemHoverColor> </ListingItemHoverColor>	CSS color property.

Figure 11: viewer.fileopen.com - Editable XML Elements

Troubleshooting the config.xml

Each XML element is parsed to ensure the values you entered are valid; if there are any errors, the default values are used to generate your viewer.fileopen.com page. If you find that the default page is being loaded after you have made changes to ListConfig.xml, do the following:

1. Navigate to fo.pn/<handle-id>, where <handle-id> is your handle-id that you created during the setup process.
    - This will redirect you to the permanent URL of your listing, viewer.fileopen.com/dbox/index.php?HID=<handle-id>.
2. Append '&checkListConfig=1' to the end of your permanent URL and press 'Enter'.
    - Do not include the singles quotes
    - This will generate error messages that tell you which XML elements are not loading properly

If you followed the above steps and you do not see any error messages, try the following:

- Ensure that all of the XML tags have both and opening tag and closing tag. If there are any XML syntax errors, that page will not load.
- Double check that you saved ListConfig.xml in your FileOpen Viewer folder.
- Ensure that you did not rename the file, it must be named ListConfig.xml.

FileOpen Clients & Viewers

The decryption process has three main requirements; document owner / publisher permission, installation of the appropriate file type software (Adobe Reader/Acrobat, Flash Player, etc.), and a FileOpen Client (if applicable).

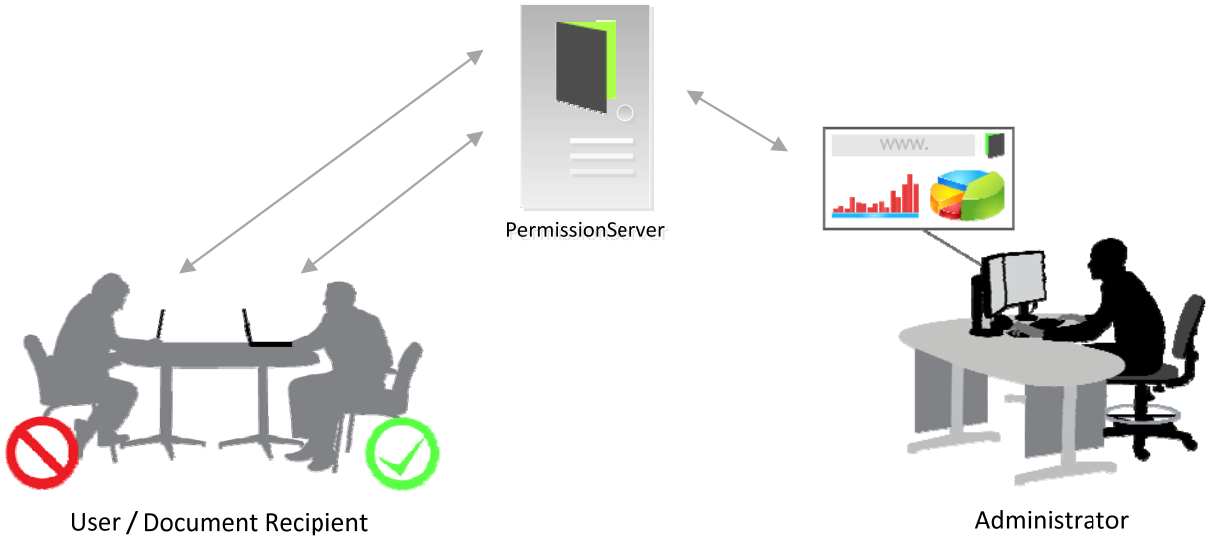


Figure 12: General Client Overview

The User attempts to open or print a FileOpen-protected document and the request is routed to the PermissionServer, which grants or denies the request based on the User's identity and Permission Policies. The Administrator tracks Document usage and modifies Policies as needed.

FileOpen Systems provides a versatile set of plug-ins/clients to access documents encrypted with the FileOpen software. These include:

- **FileOpen Plug-in for Adobe Reader/Acrobat** is a lightweight plug-in that provide authorized Users access to FileOpen-protected PDF documents in Adobe Acrobat and Reader
- **FileOpen Viewer™** allows authorized Users to access FileOpen-protected documents within a Web browser running Adobe Flash® Player version 11 or higher — no plug-ins or additional software required.
- **FileOpen Viewer for iPad and iPhone** is a native iPad/iPhone application that enables authorized Users access to FileOpen-protected documents.
- **FileOpen Viewer for Android** is a native Android application that enables authorized Users access to FileOpen-protected documents.

The FileOpen client software may be distributed to the User by the Administrator by a variety of methods: by linking to the http://plugin.fileopen.com/all.aspx from the publisher's website, by email attachment, on disc.

Flow Chart: General PDF Decryption

FileOpen-protected PDF documents can only be accessed when a User meets one of the two scenarios outlined below.

1) The User has Adobe Acrobat or Reader, FileOpen Plug-in for Acrobat/Reader, and permission from the PermissionServer.

AND/OR

2) The User has an iPad or iPhone with the FileOpen Viewer application and permission from the PermissionServer.

The process is as follows:

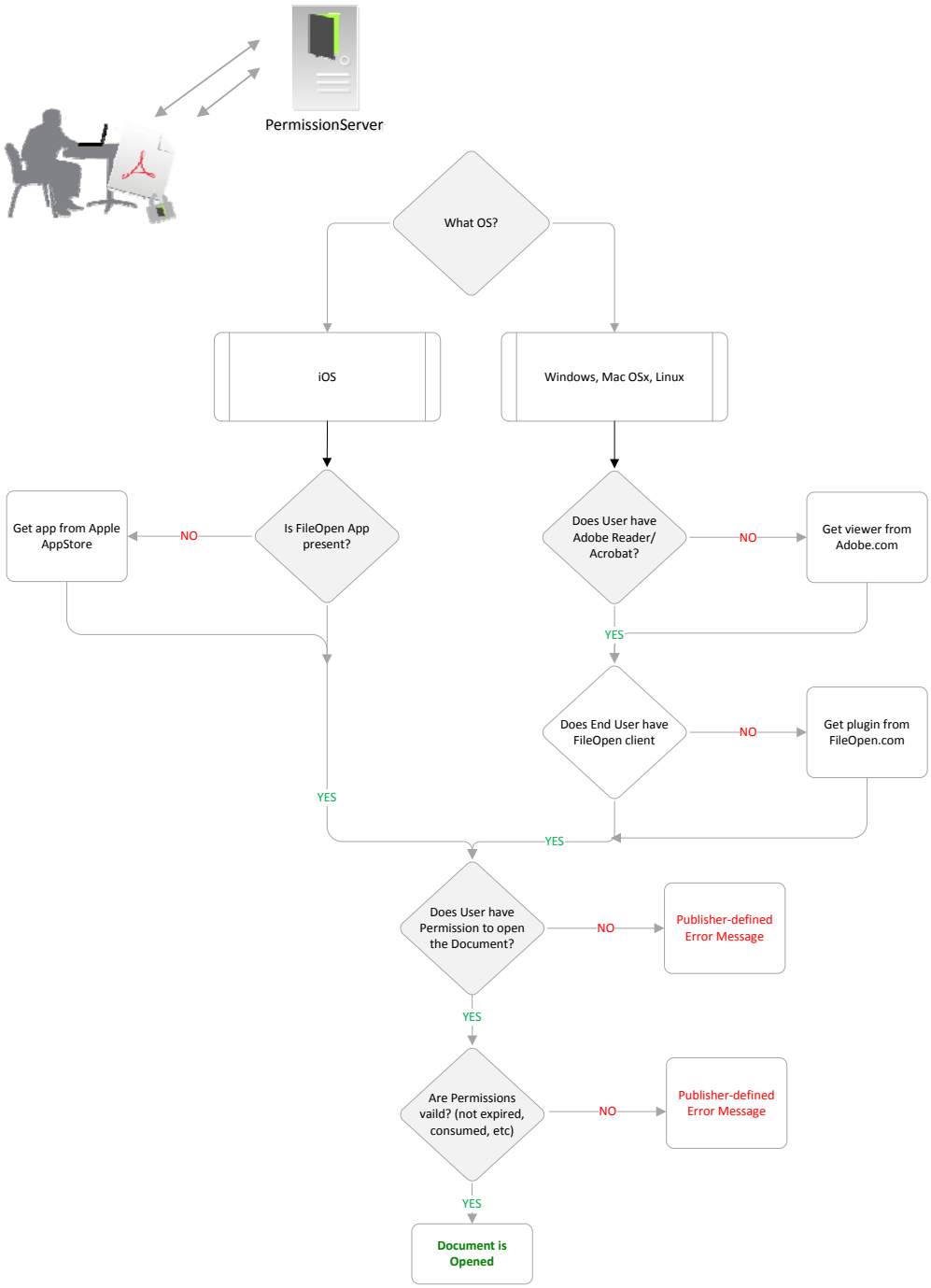


Figure 13: Generalized PDF Decryption

Flow Chart: General OPN Decryption

FileOpen-protected OPN documents can only be accessed when a User meets one of the two scenarios outlined below.

1) The User has Web browser, Adobe Flash Player 11+, and permission from the PermissionServer.

AND/OR

2) The User has an iPad or iPhone with the FileOpen Viewer application and permission from the PermissionServer.

The process is as follows:

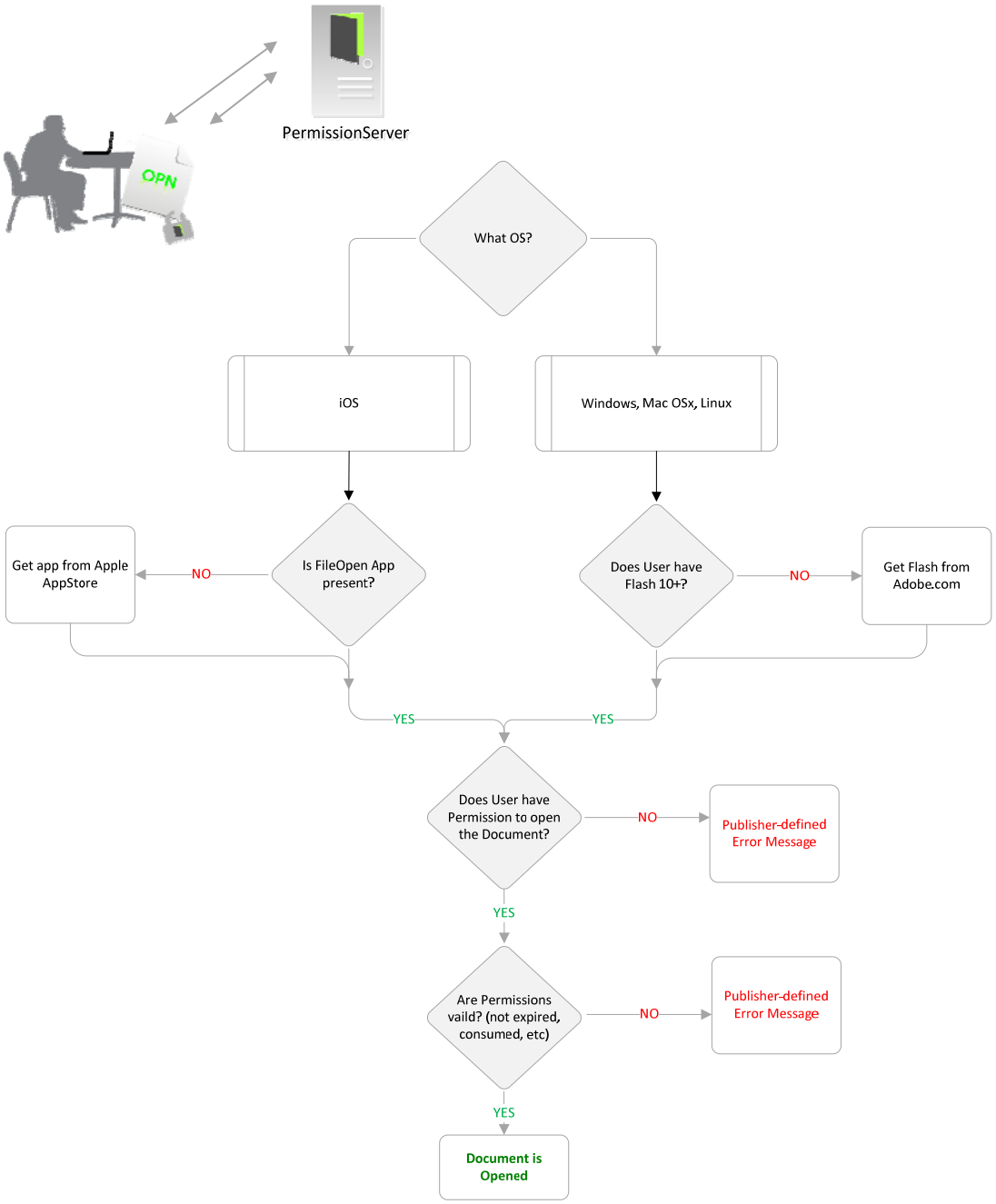


Figure 14: Generalized OPN Decryption

Index

Table of Figures

Appendix 1: System Requirements

Administrator Tools: Protection / Management

- Command Line Encryptor
  - Operating System: Windows 8.x, 7, Vista, XP
- Directory Monitor
  - Operating System: Windows 8.x, 7, Vista, XP
- WebUI
  - Operating System: Windows 8.x, 7, Vista, XP; Mac OSX, 10.4 or later; Linux Kernel 2.4 or later.

    Browsers:
    - Internet Explorer versions 7.0 or later
    - Mozilla FireFox Versions 3.5 through 16
    - Google Chrome Versions 6.x through 22
    - Safari Versions 4.x, 5.x, and 6

User Tools: Clients / Viewers

- **FileOpen Plug-in for Adobe Reader/Acrobat**
  - Operating System: Windows 8.x, 7, Vista, XP; Linux Kernel 2.4 or later.

    Browsers:
    - Internet Explorer versions 7.0 or later
    - Mozilla FireFox Versions 3.5 or later
    - Google Chrome Versions 6.x or later
  - Operating System: Mac OSX, 10.4 or later;

    Browsers:
    - Safari Versions 4.x, 5.x, and 6
- **FileOpen Viewer™**
  - Operating System: Windows 8.x, 7, Vista, XP; Mac OSX, 10.4 or later; Linux Kernel 2.4 or later.

    Browsers:
    - Internet Explorer versions 7.0 or later
    - Mozilla FireFox Versions 3.5 or later
    - Google Chrome Versions 6.x or later
    - Safari Versions 4.x, 5.x, and 6
- **FileOpen Viewer for iPad and iPhone**
  - Device Requirements: iPhone 3GS, iPhone 4, iPhone 4S, iPhone 5, iPod touch (3rd generation or later), and iPad. Requires iOS 4.0 or later.
  - FileOpen Viewer for Android: Device Requirements: Android 2.2 or later.
  -

FileOpen also supports other native PDF viewers such as, Foxit, BlueBeam, Nitro PDF or Nuance. Please contact support@fileopen.com for specifications.