# File Access Manager

# Administrator Guide

Version: 8.3 Revised: March 30, 2022

# Contents

Contents

# Terminology: Users and User Permissions

The terms used in the File Access Manager website and File Access Manager Administrative Client refer to users and user permissions in two different contexts:

1. **Business Resource Users**

   Entities within the organization, their access permissions to various company resources, and the activities they perform on these resources.

   **Users**

   Entities such as company employees and bots with access to company resources.

   **User permissions**

   Permissions such as reading and writing to a windows file server, sending emails, writing to Google Drive, deleting files, etc.

2. **File Access Manager Users**

   Administrators and users of File Access Manager and their access permissions to various parts of the application. What reports they can run, what resources they are allowed to view, etc.

The following terms are used to define the users and access permissions in these contexts:

| Context<br><br>Term | Business Resource Users<br>(#1 above) | File Access Manager website users<br>(#2 above) | File Access Manager Administrative Client users |
|---|---|---|---|
| User | "User" | "User" | "User" |
| Groups of users | "Group"<br>Such as:<br>Active Directory group | "Group Account" | |
| Permission | "Permission"<br>Such as:<br>Read<br>full access<br>Delete | "Right"<br>Such as:<br>Run report<br>Access<br>Dashboard | "Permission"<br>Such as:<br>Add Application<br>Load New Package<br>New Scheduled Task |
| Group of permissions | | "Capability"<br>Such as:<br>Administrator | "Role"<br>Such as:<br>API User |

| Context<br><br>Term | Business Resource Users<br><br>(#1 above) | File Access Manager website users<br><br>(#2 above) | File Access Manager Administrative Client users |
|---|---|---|---|
| | | Data Owner | Read Only |
| Resources user is allowed to access | Part of "Permissions" | "User Scope"<br><br>(* The user can access these resources in the context of File Access Manager, and not the resources themselves) | "User Data Role" |
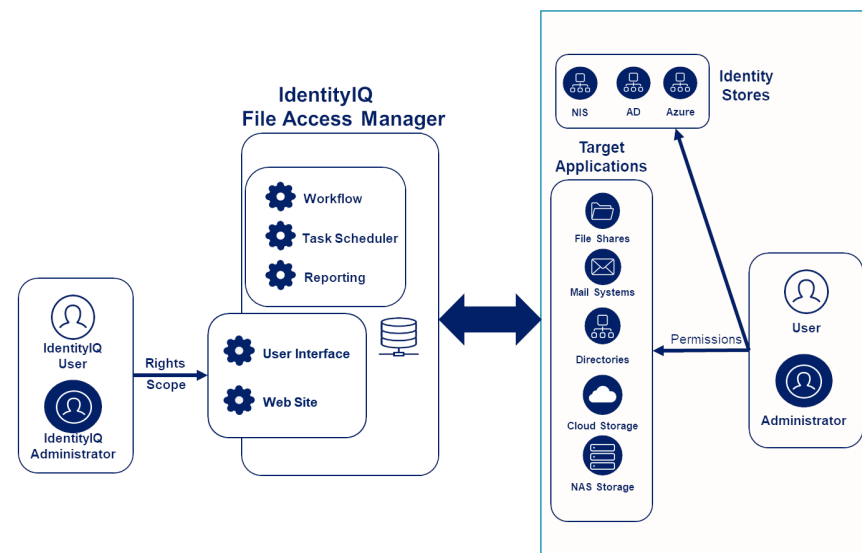


**Permissions** define the access rights of application users to files on those resources.

**Rights** and **Scope** define the rights of users on File Access Manager to access specific screens and actions, accessing resources within the users' scope. .

# Rebranding Note

This section is relevant for upgrades from versions earlier than File Access Manager 8.0.

With the rebranding of SecurityIQ to File Access Manager in release 8.0, the terms below have been converted. Some of the legacy terms might still appear in some of the application screens and the accompanying documentation.

File Access Manager release 8.0 is the next release following SecurityIQ release 6.1

| File Access Manager term | Legacy term |
|---|---|
| File Access Manager | SecurityIQ |
| Capability | Role |
| Right | Permission |

# Application Capabilities and Architecture

The following information will be provided to expand on the application capabilities and architecture:

- Capabilities
- Services
- Architecture
- Inter-service Communication

## Capabilities

This section describes the main File Access Manager capabilities, and provides a technical mapping of each service to a set of capabilities. You can find more information on each capability in the relevant chapters of this guide.

### *Activity Monitoring*

Activity monitoring involves capturing information about events that users perform on monitored applications.

An activity includes the following elements:

- *Who***?** – A user
- *Performed what action?* – Read, write, or delete
- *Where?* – On what business resource (for example, a file, a file folder, a SharePoint site, or an Exchange mailbox)
- *When?* – Date and time (Displayed in the user's local time)

### *Real-Time Alerts*

Issue real-time alerts (based on pre-defined alert rules) regarding suspicious activities.

### *Threshold Based Alerts*

Issue threshold alerts when the number of activities in a given time frame exceeds a defined threshold. An example of a threshold alert would be: "Alert me when a user reads more than 1000 files in an hour".

### *Crawling*

Crawling is a process that discovers the business resources (BRs) of a specific application, such as folders, mailboxes, et cetera. It is the first task performed on an application, since BRs are required for many other capabilities, such as Permissions Collection and data classification.

### *Permissions Collection*

Permissions Collection is a process that discovers and collects permissions on the BRs of an application. These permissions are later used and displayed in Permissions Forensics, Access Certification campaigns, Access Requests, and in other locations.

### *Data Classification*

The File Access Manager Data Classification mechanism provides the ability to discover and classify resources and files containing sensitive information, such as credit cards, personal information, and health records.

### *Identity Collection*

Identity collection is the technical process of collecting and aggregating users and groups from different identity repositories, such as Active Directory, Azure, and NIS. This information is used in Permissions Collection, as well as to analyze users, groups, users' membership in groups, the structure of groups, and other information.

### *Access Certification*

Access Certification is a process (run as a campaign) to certify and/or remove stale or unneeded permissions (or identities).

### *Access Requests*

Access Requests are users' requests to gain permission to BRs. File Access Manager manages and automatically fulfills these access requests, using approval workflows.

### *Access Fulfillment*

Access Fulfillment automatically adds or removes permissions to users' BRs.

### *Discovery of Data Owners*

Since most organizations have many business resources, this makes discovering the data owners of those BRs a complex task. Normally, IT personnel need the help of an organization's business users to discover which data owners own a specific business resource. File Access Manager automates the discovery process by collecting data on the activities and permissions of specific folders, and asking business owners who owns those folders.

## Services

### Server Services

The following table describes server services (installed by the File Access Manager Server Installer) and their relation to File Access Manager capabilities and main processes.

| Service Name | Description | Capabilities |
|---|---|---|
| Event Manager | Responsible for getting activities from the Activity Monitors, enriching the activity records with additional useful information about the users and the business resources being accessed, evaluating alert and discard rules, and saving activities to the database and to Elasticsearch. | Activity Monitoring<br>Real-time Alerts<br>Threshold Based Alerts |
| Agent Configuration Manager | Communicates with the Activity Monitors, Permission Collectors, and Data Classification Collectors to receive health checks and provide configurations. It is also the entry point for the | Activity Monitoring<br>Permissions Collection<br>Data Classification |

| Service Name | Description | Capabilities |
|---|---|---|
| | installation process of Activity Monitors and Collectors. | |
| Activity Analytics | Performs the Threshold Alerts calculations in near real-time and sends the alerts when a threshold is met. | Threshold Based Alerts |
| Central Permissions Collector | When installed in a simple architecture deployment, it connects to the applications and collects resources and permissions data. When deployed in a distributed architecture, it sends resources to the collector and aggregates the permissions data received from collectors through the message broker. | Crawling<br><br>Permissions Collection |
| Central Data Classification | When installed in a simple architecture deployment, it connects to the applications and classifies sensitive business resources based on the defined data classification policy. When deployed in a distributed architecture, it sends classification data to the collector and aggregates the classification data received from collectors through the message broker. | Data Classification |
| Reporting | Generates all reports. | |
| Scheduled Task Handler | Schedules and dispatches scheduled tasks when they are due, and runs all maintenance tasks. | Schedule Tasks<br><br>DB Cleanup task<br><br>Events Deletion task<br><br>Events Re-Indexing task<br><br>Application Deletion task<br><br>Periodic Elasticsearch & RabbitMQ health checks |
| User Interface | Responsible for communication with the File Access Manager administrative client. | |
| Business Website | The website service running the File Access Manager web interface | |
| API | RESTful API service. This service provides a platform neutral schema and extension model for representing users, groups and other resource types in JSON format. | |
| Workflow | Access certification campaign ("Campaign") creation and management of review processes. | Access Certification Campaigns |

| Service Name | Description | Capabilities |
|---|---|---|
| | | Access Requests |
| | | Business Asset Compliance |
| Collector Synchronizer | Performs Identity Collection and the Access Fulfillment tasks | Identity Collection |
| | | Access Fulfillment |
| Crowd Analyzer | Creates and manages data owners' election goals | Data Owners Discovery |
| Elasticsearch | This full text indexing database retains all data on activities collected by the Event Manager. | Activity Monitoring |
| | | Threshold Based Alerts |
| RabbitMQ | This service is a secure message broker for communication between the Central Permissions Collector and Central Data Classification services, to/from the Permissions and Data Classification Collectors | Permissions Collection |
| | | Data Classification |

## Collector Services

These services are installed by the Collector Manager:

| Service Name | Description | Capabilities |
|---|---|---|
| Activity Monitor | The service connects to the application and collects activity data ("Who did what?"). A dedicated Activity Monitor service must be installed for each application. | Activity Monitoring |
| Permissions Collector | When the RabbitMQ service is installed, the Permissions Collector can be installed to extend the Central Permissions Collector service. "Architecture" on page Architecture has additional information on collector and cloud-based architecture. | Crawling<br>Permissions Collection |
| Data Classification Collector | When the RabbitMQ service is installed, the Data Classification Collector can be installed to extend the Central Data Classification service. "Architecture" on page Architecture has additional information on collector and cloud-based architecture. | Data Classification |

## Databases

### *Elasticsearch*

Elasticsearch is a search database engine, optimized for text searches. File Access Manager uses Elasticsearch to store and query activity data. It is installed by the File Access Manager Server Installer.

### *SQL Database*

---

The SQL database, the heart of the File Access Manager, maintains all File Access Manager information. This database is created during the initial module installation. The SQL database is used as a backup for the Elasticsearch database.

# Architecture

This section provides an overview of File Access Manager architecture.
It can be deployed in one of the following deployment models:

- Simple

- Cloud-Based

The Cloud-Based deployment model provides a solution for these common use cases:

1. Deploy the File Access Manager Services (the central services that provide the core functionality) in a cloud environment with on-premises collectors that harvest information from target applications.

2. Use this model in non-cloud implementations to scale the Permissions Collection and Data Classification processes to more than a single service per application. This decreases the time for crawling, collecting permissions, and classifying data in large applications.

Administrators can deploy File Access Manager using either deployment model, and can also begin with the Simple model, and later progress to the Cloud-Based model by installing the File Access Manager Message Broker and adding Collectors. Consult a certified implementer before installation to determine the best configuration for your organization.

File Access Manager supports a disaster recovery solution, enabling the administrator to transfer the operation to a backup site if required. See details in the Server Implementation and the Disaster Recovery procedure guides.

> When installed in a High-availibility environment, RabbitMQ is used to synchronize data between IIS servers, making sure all users see up to date data in our web site. If your installation uses more than one IIS you should make sure you install RabbitMQ.

## Simple Deployment Model

See Server Services for the description and capability of each service.
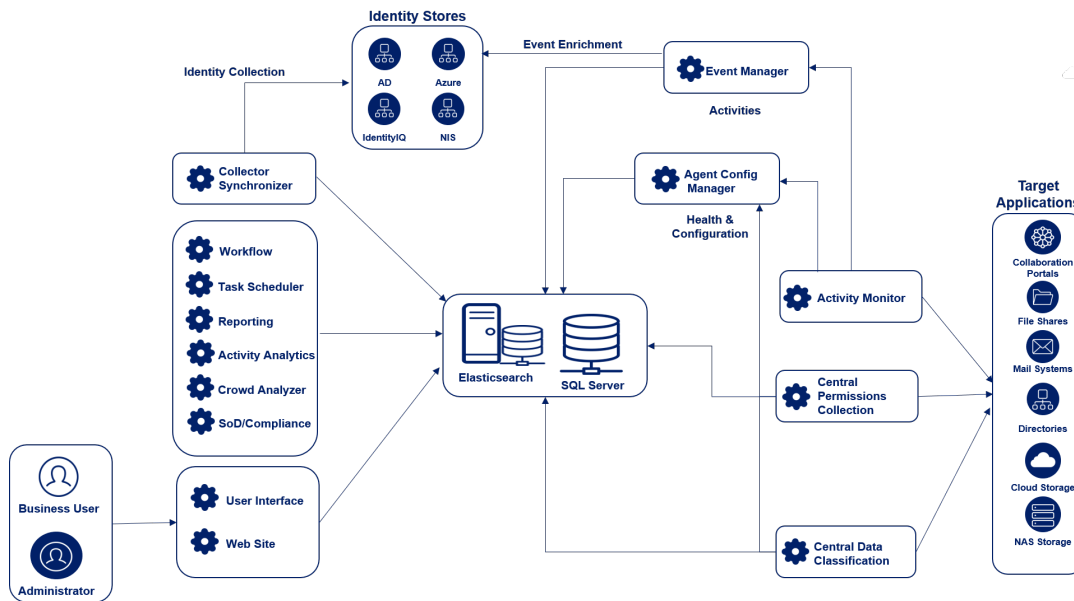
## Cloud-Based Deployment Model

File Access Manager, can be deployed in a cloud environment with on-premises collectors that harvest information from target applications. This adaptive connectivity model enhances performance and scalability for large sets of data.

The collectors focus on completing the work assigned to them by the File Access Manager Central Permissions Collector and Central Data Classification services. These collectors pass processed information – through the File Access Manager Message Broker (RabbitMQ), which provides secure communication – back to File Access Manager Services.

The information is then persisted to the database.

Each application can be processed by as many collectors running in parallel as necessary. When it is no longer necessary to process large amounts of data, such as after the first full analysis of the environment, the data classification capacity can be reduced to manage a relatively smaller number of modifications to sensitive data within the environment.

This adaptive connectivity model allows for the progressive analysis of permissions collection and data classification without having to wait for the complete data set to be processed. Each collector is tasked with processing a small subset of the environment, and as it completes each task, it sends its results (through the File Access Manager Message Broker) back to the File Access Manager Services, which persists it to the File Access Manager database.

As a result, usable information about the file system or other resources becomes available as it is processed, which decreases the time-to-value ratio, since it is no longer required to analyze an entire data set before obtaining useful results.

## Disaster Recovery

To support continued service following a natural or human induced disaster, you can install an additional environment in standby mode, to be activated if and when required.

See details in the Server Implementation and the *Disaster Recovery procedure* guides.

## Collector Overview

Connector / Collector terminology:

---

***Connector***

> Refers to the collection of features, components and capabilities that comprise support for an endpoint.

***Collector***

> Refers only to the "Agent" component or service in a Data Classification and or Permission Collection architecture.

***Engine***

> Refers to the core service counterparty of such architecture.

***Identity Collector***

> The logical component used to fetch identities from an identity store and holds the configuration, settings for that identity store, and the relations between these identities. It has no "physical" manifest.

The collection work is performed by the Collector Synchronizer.

Data Classification and Permission collection are the only collectors.

The connector is not the same as a collector.

Connectors are services that connect the to the target applications for:

- Permissions Collection (PC)
- Data Classification (DC)

A connector is a micro-service that accesses work items (business resources) through the message broker, connects and retrieves metadata from the target application, and then sends the processed information back to the central service. Connectors communicate with the central services through a third-party messaging broker service (RabbitMQ), which implements a persistent queue.

In a hybrid cloud / on-premise implementation, connectors send data to the cloud through the message broker, which eliminates the need for direct database access from on-premise to the cloud.

Connectors are not mandatory. When the cloud is not being used and/or when horizontal scaling is not required, there is no need to install RabbitMQ. If RabbitMQ is not installed, it is not possible to install Permissions Collection/Data Classification connectors, and the central services act as both the engine and the collector.

## Application > Central Service > Collector Relations

File Access Manager provides an adaptive connectivity model, allowing multiple deployment configurations that fulfill the needs of basic single-site implementations, as well as those of distributed geo-distributed implementations.

The following describe the relations among Applications, Central Permissions Collection/Data Classification services, and Collectors:

- Multiple Central Permissions Collection/Data Classification services can be installed by the File Access Manager Server Installer.
- A single File Access Manager Application can be associated with a single Central Permissions Collection/Data Classification service.

- Multiple File Access Manager Applications can be associated with the same Central Permissions Collection/Data Classification service.

- A Permissions Collection/Data Classification Collector is always associated with a single Central Permissions Collection/Data Classification service.

- Multiple Permissions Collection/Data Classification Collectors can be installed and associated with the same Central Permissions Collection/Data Classification service.

## *Possible Deployment Options*

In the simplest form, an Application can be associated with a Central Permissions Collection/Data Classification service, but without installed Collectors:



The same Application can be extended to use a single Collector if it is a cloud-based implementation. Also, if the application is located in a remote site over a slower network, the Collector can be located closer to the application.



Since each Central Permissions Collection/Data Classification service can serve a single application at a time, it is possible to install multiple Central Permissions Collection/Data Classification services.



Multiple Applications can be associated with the same Central Permissions Collection/Data Classification service, such as for small scale applications that can be processed by a single sequential Central Permissions Collection/Data Classification service.

**Application**

**Application**
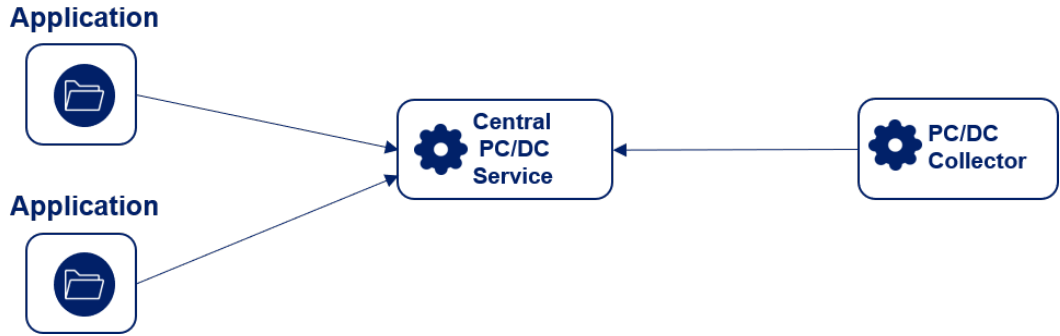
Multiple Collectors can be installed and associated with the same Central DC/PC service, which:

- Improves performance and

- Reduces the time for Crawl/Permissions Collection/Data Classification processes to run.

### *Horizontal Scaling of Collectors*

The installation of multiple Collectors reduces the operational time of Crawl/Collect Permissions/Data Indexing. The Central DC/PC service distributes the business resources among the collectors by serving them resources through the Message Broker. Each collector is in charge of processing a subset of resources, and as it completes each task, it sends its results back, through the File Access Manager Message Broker, to the File Access Manager Services, which persists it in the database.

Since each business resource is an atomic work item, adding more Collectors results in near linear-scale performance.

# Inter-service Communication

File Access Manager uses SSL communications for all its deployed services.

SSL communications use Server and Client Certificates which, by default, are self-signed and created when each service is installed. While the operating system may "not trust" these certificates, File Access Manager components do "trust" them.

The table below lists the relationships among the services and clients.

| Service | Clients | Default Port |
|---------|---------|--------------|
| Agent Configuration Manager | Activity Monitor<br>Event Manager<br>Central Data Classification<br>Central Permissions Collector<br>Data Classification Collector<br>Permissions Collector<br>Collector Installation Manager | 8000 |
| Event Manager | Activity Monitor<br>User Interface<br>Central Data Classification | 8001 |

| Service | Clients | Default Port |
|---------|---------|--------------|
| | Scheduled Task Handler<br>Central Permissions Collection<br>Web Server | |
| Reporting Service | User Interface | 8006 |
| User Interface | File Access Manager Administrative Client | 8005 |
| Workflow | User Interface | 8008 |
| Elasticsearch | Event Manager<br>Reporting Service<br>Scheduled Task Handler<br>User Interface<br>Web Server | 9200 |
| RabbitMQ | Central Permissions Collector<br>Central Data Classification<br>Permissions Collector<br>Data Classification Collector | 5671 |
| RabbitMQ | Schedule Task Handler | 15671 |
| Activity Analytics | None | 8010 |

It is a best practice for all components to be in a safe, secure network, behind firewalls, even though SSL secured communication is enabled.

## Using Trusted Certificates

Administrators can provide their own certificates for the server services only. To be trusted, server certificates must conform to the following guidelines:

- Certificates are signed by a Certificate Authority (CA), trusted by all servers in the organization, whether the CA is commercial or in-house.

- Certificates are issued to each server hosting one of the WCF hosting services (as described below).

- Certificates include the server name as it is to be used by File Access Manager (whether it is a short name or a Fully Qualified Domain Name (FQDN) in the Subject or in the Subject Alternative Names list.

- The certificate must have the following extensions defined:

  - Key Usage: Digital Signature, Key Encripment.

  - Enhanced Key Usage: Server Authentication, Client Authentication.
    The certificate may have other key usages, but must have at minimum those mentioned above.

> See the installation guide for a detailed description on using local certificates for File Access Manager., and configuring the website to use SSL.

## OAuth Support

File Access Manager offers full support of standard OAuth 2.0 Authentication for compatible connectors, replacing the legacy user and password approach. This enables including users with multi-factor authentication requirements enabled, shifting the login process to the native concent flow, using existing tokens.

To set up the authentication, you have to have or create an app in the provider's app management console. See the connector installation guides for a detailed description of installing the File Access Manager app, and configuring the OAuth connectivity.

> To reduce the likelihood of exceeding the API call quotas and encountering throttling issues, it is recommended to use multiple service-accounts in each token category and use a separate set of service-accounts for Activity Monitoring.

Supported applications:

- SharePoint Online

- Exchange Online

- DropBox

- Box

- Google Drive

- OneDrive

### *The OAuth2 Authentication Flow*

**Preliminary Setup**

An app is registered in the provider's app management console. See description per application in the relevant connector installation guide.

App registration generates a set of identifiers: *ClientId* and *ClientSecret* - these identify the app uniquely and are used for issuing token requests.

App registration includes definition of a redirect URI - that is used for user redirection upon completion of the authentication process.

Upon successful authentication and consent, the provider will redirect the user - the redirection URI will be appended with a user authorization code in the URL query string.

**Authentication Flow**

- An end-user browses to a special App Authorization URL - this is typically a credentials' input form at the provider's website

- The end-user logs in to the provider, with one of the following outcomes:

    - Login Failure

      The end-user is redirected to the app's redirect URI with an error message in the query string.

- Login Success

  The end-user is presented with a consent form in that lists the permissions that the app is requesting. There are two possible outcomes:

  - Consent Declined

    The end-user is redirected to the app's redirect URI with an error message in the query string.

  - Consent Given

    The end-user is redirected to the app's redirect URI with a user authorization code in the query string.

- A web page, or some other code, issues a token request using the user authorization code. This code is active for roughly 30 seconds.

- The provider responds with a token set.

- The access token can be used to issue requests to OAuth2-enabled services exposed by the provider.



**Web Application**

1 User visits Application web page

2 Application redirects user to Consent screen

3 User logs in & grants access to App

4 Provider redirects user with an Authorization Code

5 App exchanges Authorization Code for Access Token

**App**
Registered with Provider

**OAuth Provider in Cloud**
(OneDrive, Google Drive, Dropbox)
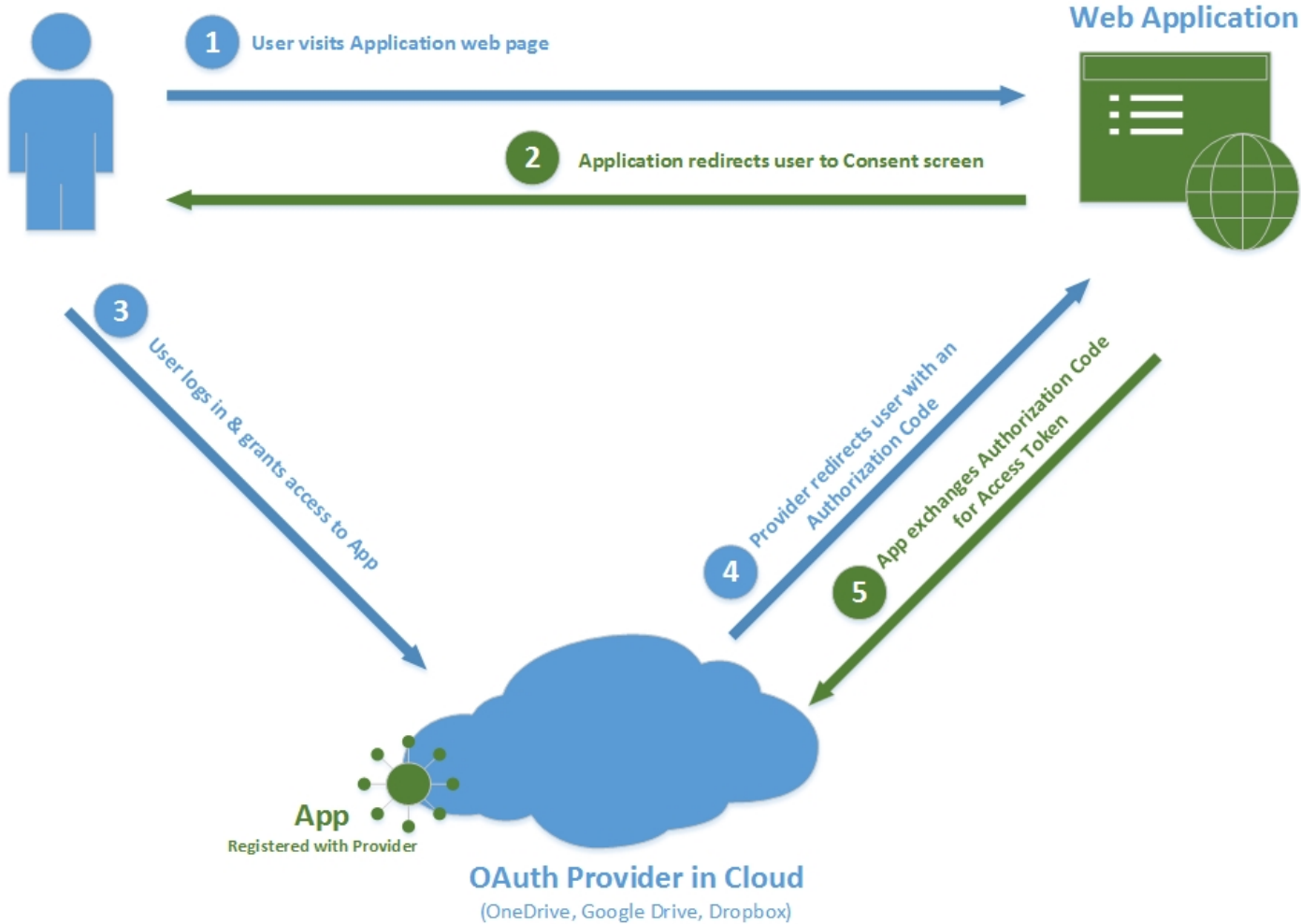
## *OAuth2 Token Management in File Access Manager*

### OAuth2 Mini-site or OAuthWebsite

The OAuth2 mini-site was deployed to ease the management of File Access Manager's interface to OAuth2-based services.

The mini-site enables storage of all provider-specific configuration in a unified location, thus enabling us to modify it from a single location.

The mini-site provides the following:

- Storage of global info, including provider specific information:

    - ClientId

    - ClientSecret

    - URL for user authentication

    - URL for token requests

    - Scope, for providers that allow dynamic permission requests

- Handling of OAuth2 flow operations:

### *UserRequest.ashx*

Redirecting the end-user to the appropriate provider's website to start the authentication process.

### *Callback.aspx*

The target of Redirect URI, extracting the User Authorization Code or error message from a query string and displaying it in a user friendly format.

### *AccessToken.ashx*

Encapsulating initial requests for access tokens, exchanging a User Authorization Code for a Token Set.

### *RefreshToken.ashx*

Encapsulating requests for token refresh, exchanging a Refresh Token for a new Token Set.
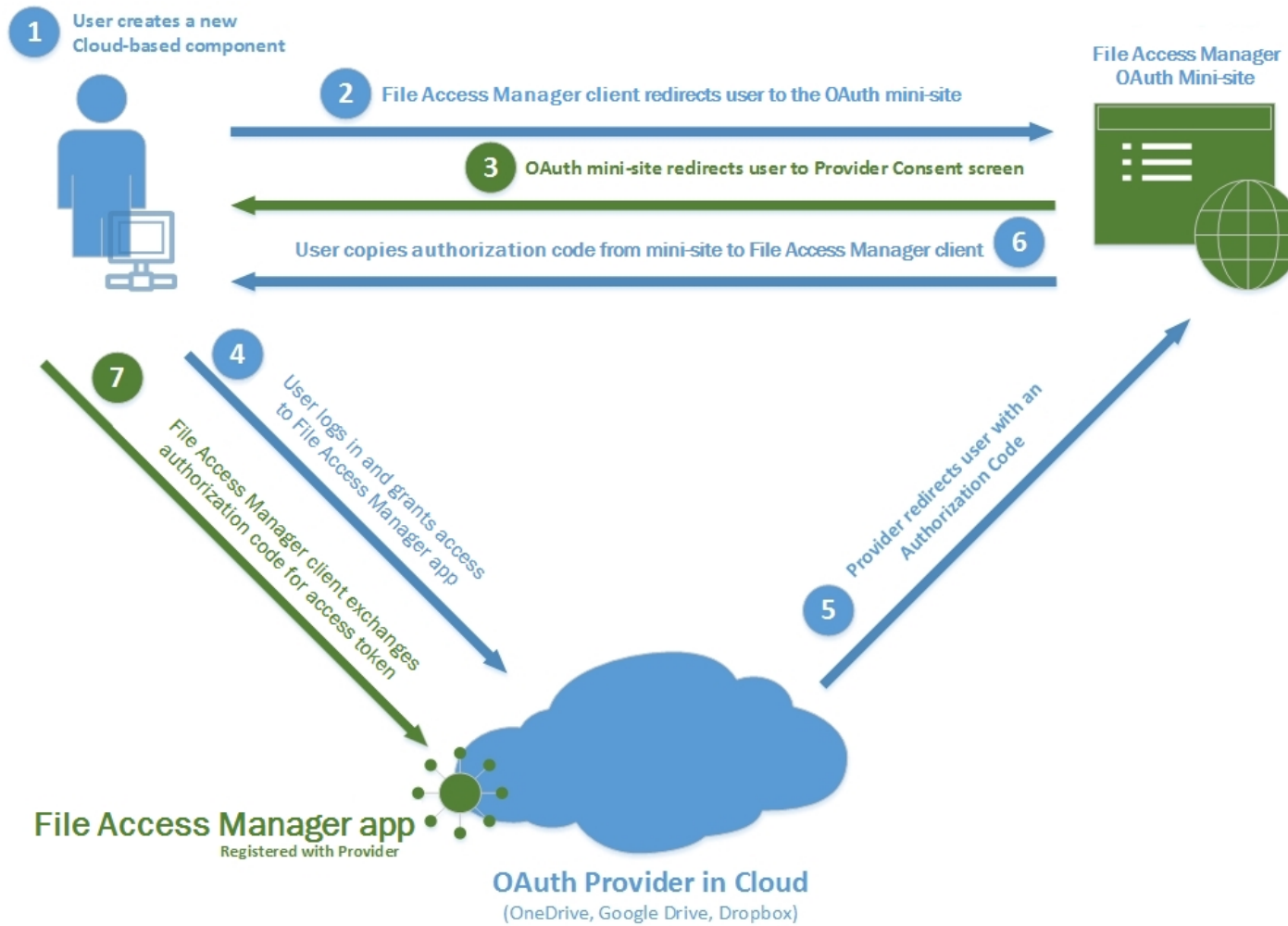
## Agent Configuration Manager - TokenRefreshServer

This central service is responsible for refreshing all OAuth2 tokens automatically and providing a token retrieval interface for other File Access Manager components.

The logic described here is implemented in: `AgentConfigurationManager\src\TokenRefreshServer.cs`

- Interface Operations

    - Upon token request - the requested token will be sent as a response

    - If no such token is loaded, the service will attempt to load it from the database.

- Automatic Operations

    - Upon startup - the service loads all available tokens from the BAMs' (application's) configurations.

    - Whenever a token is approaching expiry- it will be automatically refreshed and updated in the database.

    - If a token refresh fails - the token will be removed from the memory cache

- This mechanism allows automatic release of expired / failed tokens, this protects the service from endless refresh attempts.

  ***Failed Refresh***

  There are various reasons for a failed refresh, such as modified or deleted consent user, expired app key, network errors etc.

- A token reload and refresh will be re-attempted if / when it is requested again through the ACM token management interface.

- The TokenRefreshServermust is the only File Access Manager component that executes token refresh operations.

  - This provides a solution for security mechanisms whereby upon refresh all but the latest token are canceled.

  - A centralized point for token management makes for easier logging, debugging and troubleshooting.
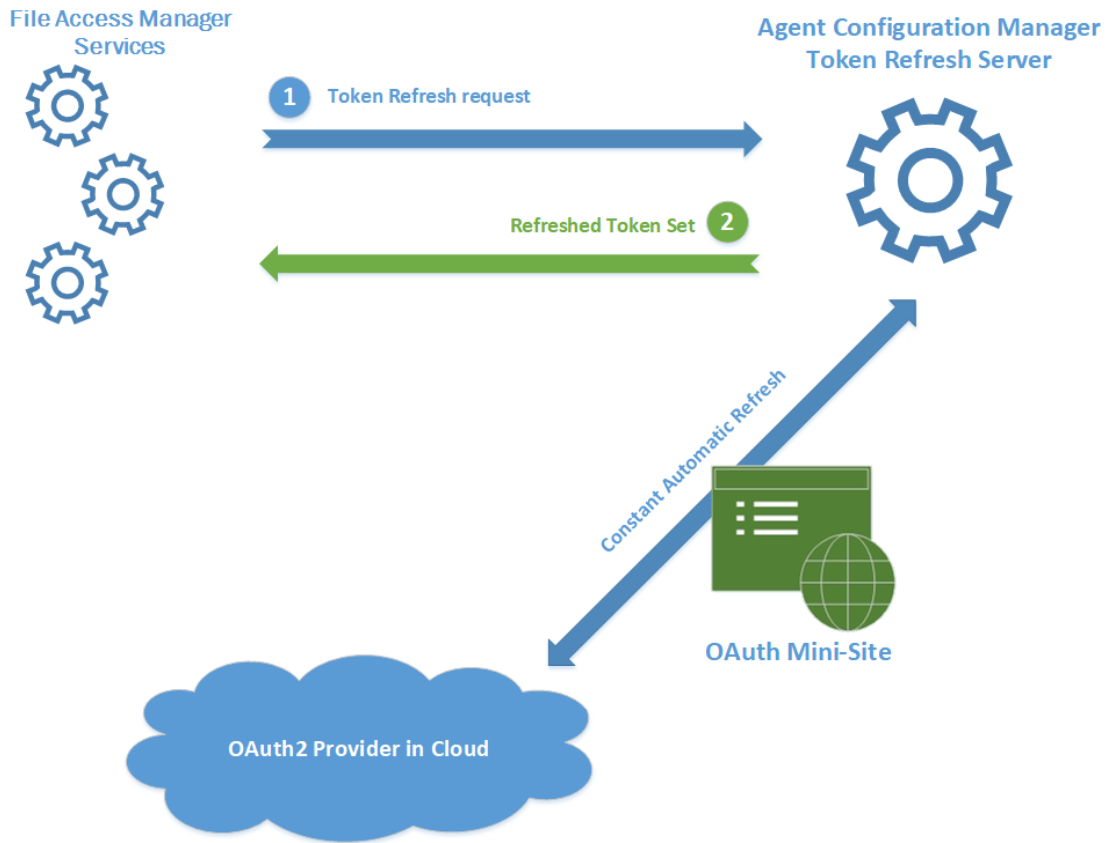


## Troubleshooting Notes

When a user first launches the administrative client while using the self-signed certificates, the system displays a message, requesting that the user trust the certificate.
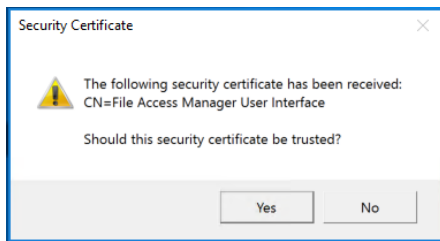
*Yes*

> Trust the certificate and open the client. This message will not display again.

*No*

> The client will display an error message, and close.

# Ensuring HTTP/2 Support

Services will only accept http/2 connections (version 8.2 uses gRPC as the communication protocol, the requires http2).

Once fully upgraded File Access Manager services should work seamlessly with http2. In some cases, some communication middleware components (such as load balancers, e.g.) may not be configured to support http/2, which may cause for communication failure and cause the upgrade to halt. As a pre-upgrade step ensure all servers and communication middleware components are configures to support http/2.

# Connection Errors

Following a successful upgrade to version 8.2, services will only accept http2 connections (version 8.2 uses gRPC as the communication protocol, the requires http2).

Once fully upgraded, File Access Manager services should work seamlessly with http2. In instances where the customer upgrade halts after a successful Agent Configuration upgrade, one potential cause could be that the communication middleware (such as a load balancer) is not configured to work with http2.

The following error will be shown in the log of services trying to connect to the Agent Configuration manager:

> Unable to connect to test.domain.com with user_name Grpc.Core.RpcException: Status(StatusCode-e=Internal, Detail="Bad gRPC response. Response protocol downgraded to HTTP/1.0.")at Grpc.Net.Client.Internal.HttpClientCallInvoker.BlockingUnaryCall[TRequest,TResponse](Method`2 method, String host, CallOptions options, TRequest request)at Grpc.Core.Interceptors.InterceptingCallInvoker.<BlockingUnaryCall>b__3_0[TRequest,TResponse](TRequest req, ClientInterceptorContext`2 ctx)at Grpc.Core.ClientBase.ClientBaseConfiguration.ClientBaseConfigurationInterceptor.BlockingUnaryCall[TRequest,TResponse](TRequest request, ClientInterceptorContext`2 context, BlockingUnaryCallContinuation`2 continuation)at Grpc.Core.Interceptors.InterceptingCallInvoker.BlockingUnaryCall[TRequest,TResponse](Method`2 method, String host, CallOptions options, TRequest request)

If such errors appear in the log files, make sure all communication middleware components are configured to work over http/2, and the connection is not downgraded to http/1.

In case the error appears in a service that is still in version 8.1, the errors may be safely ignored. Once the service is fully upgraded the errors will stop showing in the log.

# Audit Log

The Audit log registers all activities in the web application for auditing and regulatory purposes.

The audit log data is stored in the database, and an administrator can run a report to retrieve all or part of the audit log, according to predefined filters and/or schedule.

The ability to configure the audit log is accessible to Administrator capability only, by default.

Running this report requires the **Reports > Report Templates > Report Templates Administrator** right.

The audit log functionality is on by default.

## Audit Log Format

The audit log stores the following information:

- User
- Role
- Host IP address
- Timestamp (UT)
- Action
- Action Description

The report is limited to one million rows.

# File Access Manager User Interfaces

There are three user interfaces to File Access Manager:

### File Access Manager Administrative Client

This is a windows based application installed on site. This interface is accessible to administrators, and other specific users defined in the system. It includes configuration and activation of File Access Manager services and activities.

**Authentication:** Login and Password

This interface is in the process of being phased out, as functionality is converted into the File Access Manager website.

### File Access Manager website

A web based interface, accessible to all users in the system's domain.
Within the File Access Manager website, users' access to data and functionality is set to fit the users' role in the company, and data they are authorized to view. Screens and buttons within screens that a user does not have the right to use are disabled, or not displayed. In the web client.

*Authentication*: Login to the system is auto-authenticated through IIS, or via supported SSO sources.

### File Access Manager API

A standard RESTful API supporting SCIM standard for identity management. the API documentation can be found in the installed server at the URL

[Installed server]/IdentityIQFAMapi/docs/index.html

**Authentication**: The File Access Manager API uses OAuth 2.0 as well as Basic Authentication across HTTP.

To set up the File Access Manager website on HTTPS, See File Access Manager Website SSL.

## File Access Manager Administrative Client

This section describes the administrative client, the main capabilities and navigation paths.

The image below shows the *System module* of the File Access Manager Administrative Client user interface.
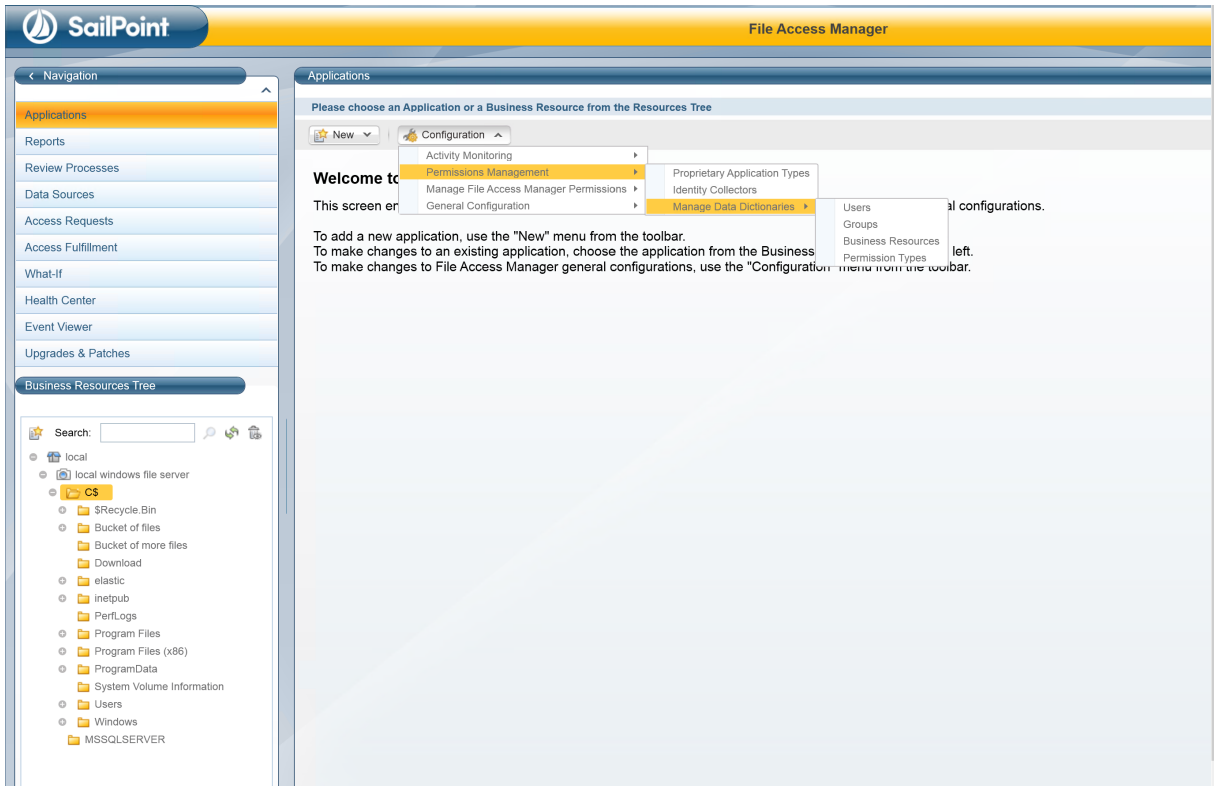
## Getting Around

This section describes the main areas, content, and purposes of the user interface.

Throughout this guide, directory paths are in bold, as follows:
*Main Navigation> Secondary Navigation> Menu > Submenu*

Navigation through the application will usually be accompanied with an indication of the user interface used

Admin Client

*Permissions > Identities and Permissions Forensics*

Web Client

*Settings > Account Exclusions*

## *Main User Interface*

The following image shows the different areas of the main screen:
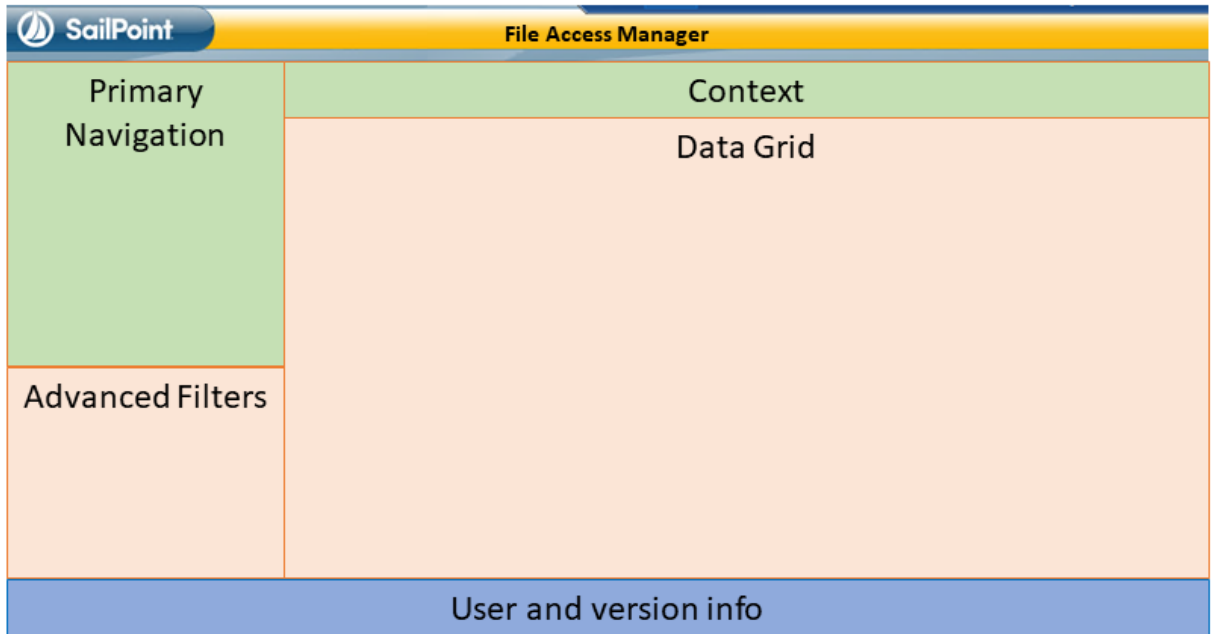
**Primary Navigation**

The *Main Navigation* panel (also called system *Modules*), which controls the primary parts of the system, include:

- Applications
- Reports
- Review Processes
- Data Sources
- Access Requests
- Access Fulfillment
- What-If
- Health Center
- Event Viewer
- Upgrades & Patches

**Secondary Navigation**

Some panels in the primary navigation have sub-panels, which users can select from the list at the upper left side of the Secondary Navigation area.

Currently, Secondary Navigation options (also called Screens) are in all modules except for the Activities module.

***What-If***

Displays a simulation panel to describe the permission changes that would be created by adding / removing users to / from groups.

***Access Requests***

Displays the access requests created in the web application.

### *Applications*

Includes the following capabilities:

### *Application configurations*

Identity collectors

### *File Access Manager permissions*

Alert responses configuration

### *Authentication store management Reports*

For reports created in other panels in the administrative client. This panel enables the user to customize, save, and add schedules for these reports.

### *Review Processes*

Defines static and dynamic review process workflows for use in Access Certification processes.

### *Data Sources*

Manages data sources.

### *Access Fulfillment*

Provides oversight of pending fulfillment requests.

Performs actions on fulfillment requests (such as Rollback or Retry).

### *Health Center*

Tracks the status of File Access Manager services.

### *Event Viewer*

Displays important updates from File Access Manager services.

### *Upgrades & Patches*

Includes system upgrades and patch downloads.

## *Context*

Most File Access Manager operations operate within the context of a Business Resource (BR), which is a monitored application object.

Examples of BRs are:

- Exchange Mailbox folder
- Active Directory objects
- SharePoint folders
- Shares on a File Server

Monitored applications include file servers, Microsoft™ Outlook, Microsoft SharePoint, Microsoft Active Directory, or any other system that can be monitored and assessed. The working business resource displays in the content area of the Main Navigation window. Users can select a business resource or a specific attribute using advanced filtering in the Secondary Navigation area.

> If a user accesses a screen or panel for which he or she has permission, but no valid user scope, the screen / table / report will be empty. Opening such a screen is accompanied with an information panel stating that the contents of the screen might be limited or empty due to the user scope of the user.

## Resource Tree

The resource tree appears in the File Access Manager administrative client (In the File Access Manager website it is replaced by the Resource Explorer). It, represents all the applications, and BRs available.

The items in the resource tree display in their natural, hierarchical order.

The resource tree contains the following:

- The resource tree's children, which are all the Containers in the system
- The Container's children, which are all the Applications, and their children, which, in turn are the BRs

The image below shows a sample resource tree, with containers, applications, and BRs.
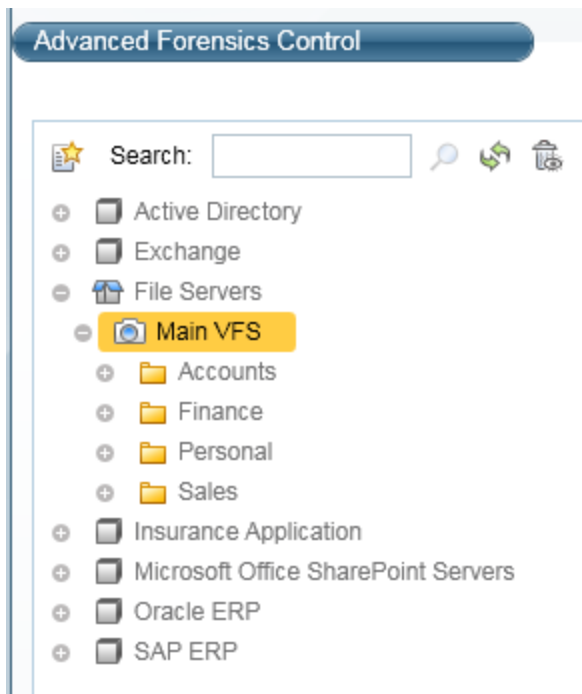


### Search

There can be tens of millions of resources in a resource tree of a medium-to-large-sized organization. The system searches for object names, rather than object paths.

### Deleted Objects

By default, File Access Manager filters deleted objects from the resource tree and search results. Selecting the trash bin icon on the upper right of the resource tree displays the deleted objects in that tree.

### Refresh Resources Structure

File Access Manager constantly updates the BR tree when it monitors live systems, but does not auto-update every change, to improve system performance. Selecting the refresh icon (two arrows in a circle) refreshes the BR tree.

# File Access Manager Website

This section describes the File Access Manager website, the main capabilities and navigation paths.

The image below shows the *System module* of the File Access Manager website user interface.
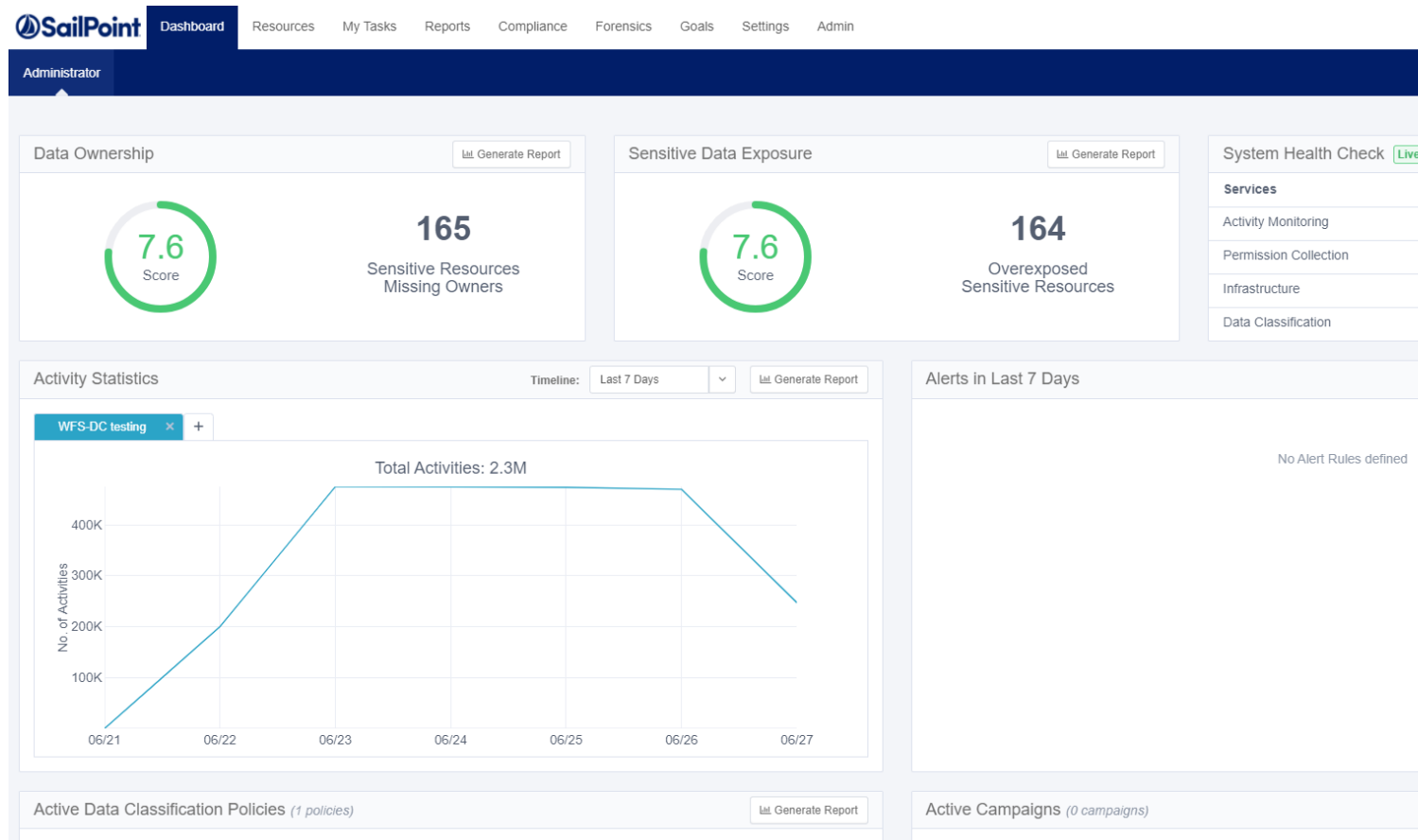


## File Access Manager Website Dashboard

This section describes the Dashboard in the File Access Manager website, including its capabilities and navigation procedures.

### *General*

Traditionally, IT personnel or security personnel determine which individuals can access specific operations on specific resources. However, since they are not always directly involved with those resources on a daily basis, they often rely on other people to decide who should have access to each resource, or type of resources.

Users who work with resources on a daily basis can best determine which users would be the most likely data owners of specific resources. These are not necessarily IT personnel or even project managers.

This dashboard makes it easier for IT and security personnel to enlist the cooperation of resource users to indicate which resources are at risk.

This screen has two tabs:

- Administrator
- Data owner

These tabs are accessible according to the user's capabilities. By default, they are available to administrators, and data owners respectively. An administrator who is also a data owner will see both tabs.

## Viewing the Data Owners on the Dashboard

The Date Owner tab is in the web client (**Dashboard > Data Owner**)is available for users in the Data Owner capability, who have user scope assigned to them.

The Data Owner tab of the Dashboard in the Web user interface consists of the following sections:

- My Resources
- Did You Know
- My Tasks
- Owner Leaderboard
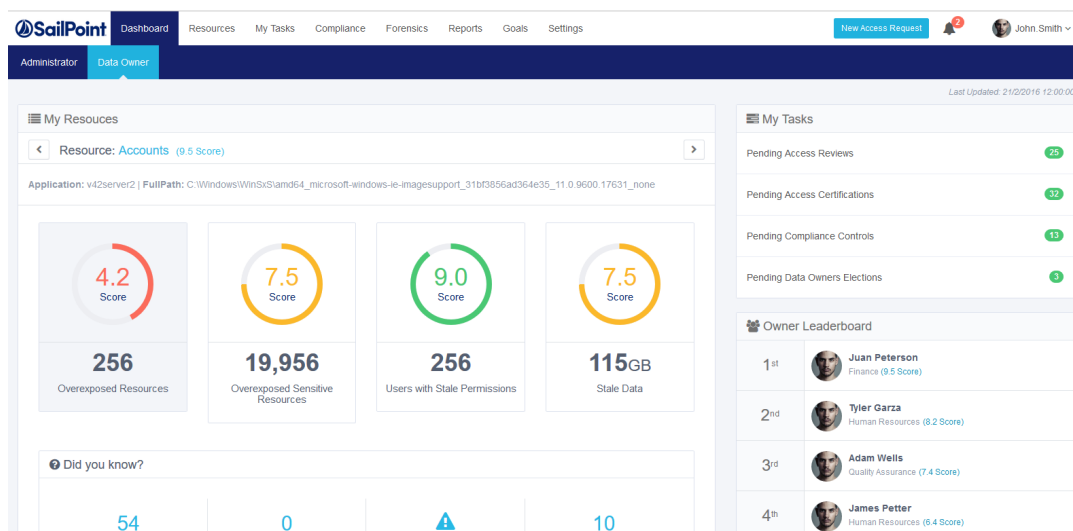


The following subsections describe each area of the Dashboard (administrator display) in detail.

**My Resources**

The My Resources section is located at the top of the main Dashboard display by following *Dashboard > Data Owner > My Resources*.

The dashboard shows statistics for the resources within the user's scope.

The score in parentheses after the name of the resource is the average score of all the Key Performance Indicators (KPIs). The name of the application and its full path are beneath the resource name.

The KPIs change based on the resource selected.

Each of the KPIs lists the number of indicators and their weighted scores (from 1-10) are also displayed in a color-coded circle graph.

The KPIs are:

- Overexposed Resources

- Overexposed Sensitive Resources

- Users with Stale Permissions (permissions older than 12 months)

- Stale Data - data older than 12 months, expressed in number of megabytes or gigabytes

- The color-coded scores are:

    - **Red** (0-5)

    - **Yellow** (5-7.5)

    - **Green** (7.5-10)

For a full description of stale data, and how it is calculated, see Stale Data.

To see the details of a specific KPI with the applicable filters, scope, and permission type:

1. Click a KPI from My Resources or navigate to **Resources > Path** (for example, C:) > *KPI*

2. Select a KPI to see details, with the relevant filters, scope, and permission type.

    > If the user does not have the right to access the drill down screen, the drill down link will be disabled.

3. To return to the Dashboard view, click the Dashboard tab.

**Did You Know?**

The "Did you Know?" area of the Dashboard contains useful information about an owned resource. This information includes statistics, resource information about logged in users, and warnings. Information may include identification of users who can access resources with specific permission types or the number of users that used a specific resource within a defined period. This information is updated for each logged-in user.

To navigate the Did You Know carrousel:

1. Click the **>** to the right (or the **<** to the left) of the displayed entries.

2. Click on a specific **Did You Know** item to review it.

3. Use touch selection and navigation (left or right) when viewing Did You Know information on a tablet.

The carrousel displays four items at a time, and automatically moves to the next four items every 5 seconds. The progress dots at the bottom of the Did You Know section indicate how many total pieces of information (in groups of four) are available. For example, if the Did You Know section displays five dots, there are twenty total pieces of information.

1. Click **Review Now** to display the details of any item of information in Did You Know.

> If the user does not have the right to access the drill down screen, the drill down link will be disabled.

**My Tasks**

The My Tasks section, at the top right of the Dashboard, lists the number of pending items in the following categories:

- Access Certifications
- Access Requests
- Owners Election

You can navigate directly to the My Tasks view for a task by selecting that task.

**Owner Leaderboard**

The owner Leaderboard section of the Dashboard displays information about the data owners with the highest-ranking score per owned resource.

Owner Leaderboard scores are ranked only for data owners, displaying the identities and scores of the top five data owners and the score of the logged in user (displayed as "Me"). The "Me" entry indicates whether the user's rank has increased (a green arrow pointing up) or has decreased (a red arrow pointing down).

## Application Main Screen

The Applications page enables a user to view, add, modify or delete applications. The Applications grid provides the following columns:

- Name – Name of application
- Description – Additional information about the application
- Type – Common search or grouping criteria
- Tags – Allows users to group applications together
- Actions – Provides multiple options for the user, including editing or deleting the application

The amount of rows displaying applications can be changed with the **Rows per page** drop down at the bottom left of the page.

The user can also click through pages with the left and right arrows at the bottom right of the page.

The following are options throughout the Application page:

***Add New***

> This options allows the user to add a new application.

***Filters***

> Allows the user to have a more defined search. Searchable items are Name, Type, and Tags.

***Edit***

> Allows various details about the application to be edited.

***Delete***

Allows the user to delete the chosen application. The deleted application will not be available on the grid and a task will be created to clean the application references and data. This deletion task can be monitored on the Tasks screen.

### Exclude Top Level Resources

Function allowing the user to exclude top level resources from being retrieved by a crawler action.

### Download Installation Files

Download command-line script for a silent installation of the Windows File Server Application Activity Monitor. Download Installation File is supported only by the Windows File Server application type.

### Manage Resources

Browse and manage all resources within the application. This action moves the user to the Resource Explorer.

### Managed Normalized Resources

View, modify, and manage all normalized resources within the application. Here, the user can also enable or disable the normalization, set or modify the normalization configuration and report on all normalized resources.

Managed Normalized Resources isn't supported by all the application types and there are specific settings which should be defined during creation of the application in order to see this option

## Adding Applications

An application is a component that represents the monitored system, such as, Microsoft Outlook, Active Directory, MS Windows file servers.

All active applications can be seen in **Admin > Applications**. You can add tags to applications to group the applications by (Called containers in previous versions of File Access Manager).

In order to integrate with a component, we must first create an application entry. This entry includes the identification, connection details, and other parameters necessary to create the link.

To add a standard application, use the **New Application Wizard**.

> The actual configuration pages and fields vary according to the application type you are adding. For a detailed description see the relevant connector installation guide in Compass.

> For homegrown applications - see Proprietary Application Permissions Collection (Homegrown Apps)

> For bulk application loading - use the Bulk Application Wizard. See the connector installation guide. For example: Adding New Bulk Application(CIFS only)

1. Navigate to **Admin > Applications**

2. Click **Add New** to open the wizard.

3. Click **Standard Application**

4. Click **Next** to open the **General Details** page.

### *Application Type*

Select the application type from the dropdown list

### *Application Name*

Logical name of the application

### *Description*

Description of the application

### *Tags*

Select tags for the application from the dropdown menu, and / or type a new name, and press **Enter** to create a new tag. The dropdown list of tags filters out matching tags as you type and displays up to 50 tags.

> The **tags** replace the **Logical container** field that was used when creating applications in releases before 8.2

### *Event Manager Server*

This option is available if there are more than one event manager servers configured in the system.

Select an event manager from the drop down menu.

### *Identity Collector*

Select from the Identity Collector dropdown menu.

- You can create identity collectors in the administrative client. **Applications > Configuration > Permissions Management > Identity Collectors**.

  See section "OOTB Identity Collection" in the Collector Installation ManagerFile Access Manager Administrator Guide for further details.

- If adding a new identity collector, press the **Refresh** button to update the Identity Collector dropdown list.

The next configuration pages include all or part of the following :

### *Connection Details*

Server and user credentials to connect to the remote system

### *Crawler and Permission Collection*

Associate an application with a Central Permission Collector Service. This service is responsible for running the Permission Collector and Crawler tasks.

> The Crawler task progress bar will progress based on the number of resources scanned.

### *Data Classification*

Associate the application with a Central Data Classification Service. This service is responsible for running the Data Classification tasks.

### Activity Configuration and DECs

Change the default values of the activity monitoring attributes

### Access Fulfillment

Allow File Access manager to add and remove permissions

See the relevant connector installation guide for full details.

# Using the Manage Resources Page

The Manager Resources page on the website lists the resources per application.

You can use this page to

- Enable normalization for resources of supported applications

- Set monitored actions for top level resources of supported applications

### Navigation

To navigate through the resources, click a child resource to change the level displayed, and display the child resource content, or click a path on the cookie crumb list on top of the screen, to move up to the level selected.

### Filtering

The filter allows narrowing down the selection of resources. The results are filtered as you type.

The filter can be used to search for object names, rather than object paths.

**Only Search Inside** [current folder] - search from this folder and downwards.

**Name Contains** - Toggle the search behavior between "Starts with" and "Contains".
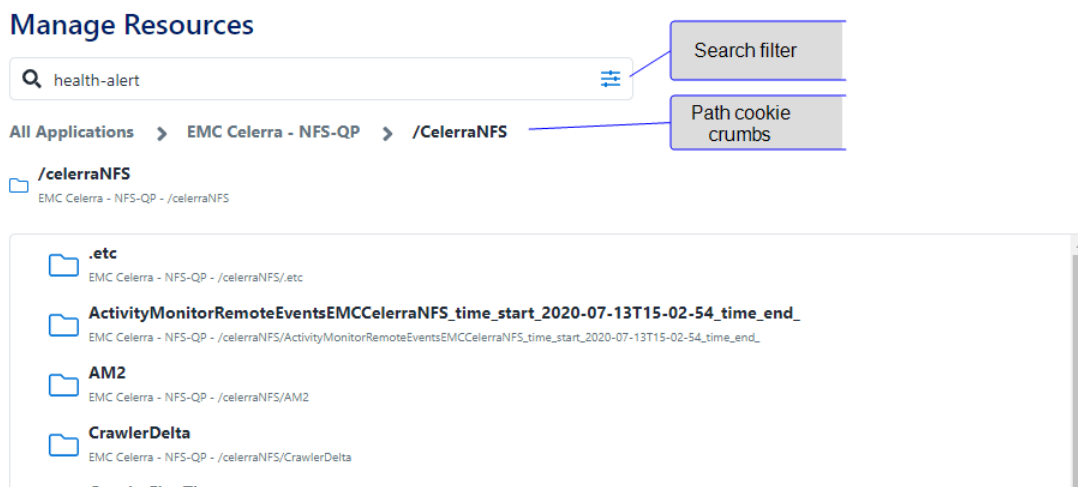


### Manage Normalization

The Manage Normalization button appears in applications that support fulfillment. Press the Manage Normal-ization button on the row of a resource to enable or disable normalization for the resource.

**How to Handle Inexact Permissions Matches**

During the normalization process, the application has to decide what to do with permissions that do not match the normalized permissions.

- Fail the normalization process

- Elevate to the nearest permission match

- Revoke the permission
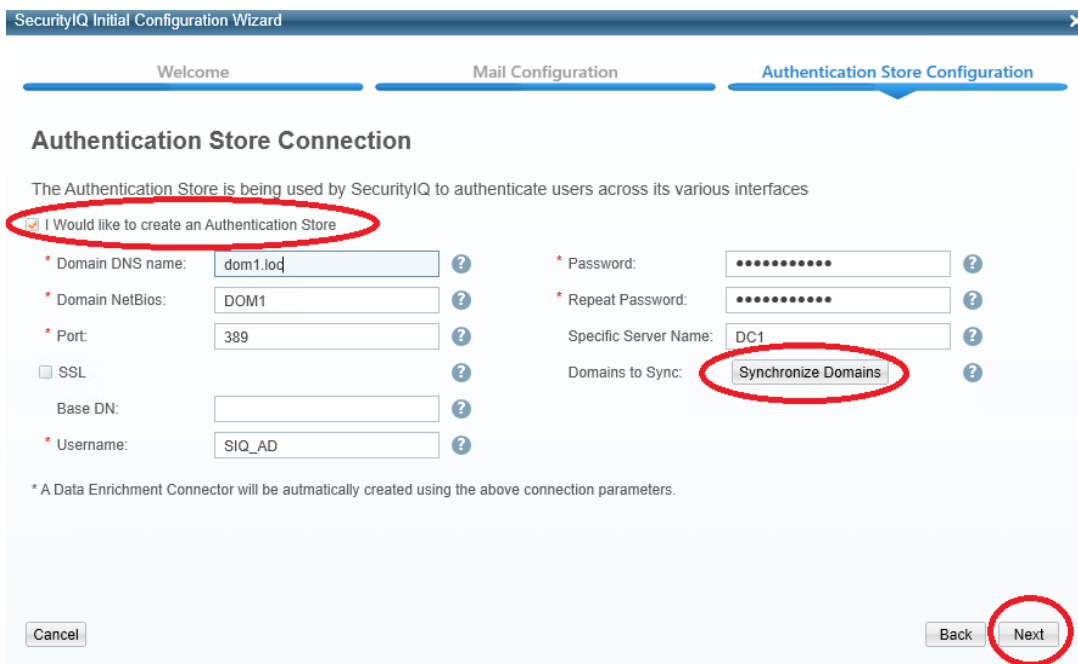
# File Access Manager Initial Configuration

This section describes how to use the Initial Configuration Wizard to get started with File Access Manager.

## File Access Manager Initial Configuration Wizard

To initially configure, perform the following steps:

1. Double-click on the File Access Manager Client icon.

   The *SailPoint File Access Manager Login application page displays.*

2. Type **wbxadmin** in the Username field.

3. Type **wbxadmin** in the Password field. (It is required to change this initial Password later.)

4. Click **Login**.
   *The File Access Manager Initial Configuration Wizard window opens.*

5. Click **Yes, Let's get started**.

6. Click **OK** to open the Authentication Store Connection window.



7. Check the **I would like to create an Authentication Store** check box and type the relevant data into the following fields:

   a. The domain DNS name in the **Domain DNS name** field

   b. The domain NetBIOS name in the **Domain NetBios** field

   c. The port number in the **Port** field

   d. The Base DN (relative to the DNS domain name) in the **Base DN** field
   (For example, if the domain DNS is **seri.example.com** then the base domain DN will be **DC=seri,**

**DC=example, DC=com**. To add the OU called **Allowed Users** under the domain, the base DN should be **OU=Allowed Users**.)

> More than one base DN may be included (using | or; or any other separator)

> For example, to include Allowed Users, and Europe and the United States, type: `OU=Allowed Users | OU=Europe | OU=US` or `OU=Allowed Users; OU=Europe; OU=US`

   e.  The user name in the **Username** field

   f.  The password in the **Password** field

> The password requirements are a minimum of 12 characters in length, a least one capital, one lower-case, and one special character. The password must be changed every 120 days and cannot be reused with 10 password change cycles. The account will be locked after 10 unsuccessful password attempts.

   g.  The password in the **Repeat Password** field

8. The specific domain controller name in the **Specific Server Name** field ((if empty identities are collected from any available DC).

9. Check the **SSL** check box, if required.

10. Click **Synchronize Domains** and then select the domains/forests you want to include in the Authentication Store from the *Domains to Sync* field.

11. Click **Next**.
*The Authentication Store Scheduling window opens*.
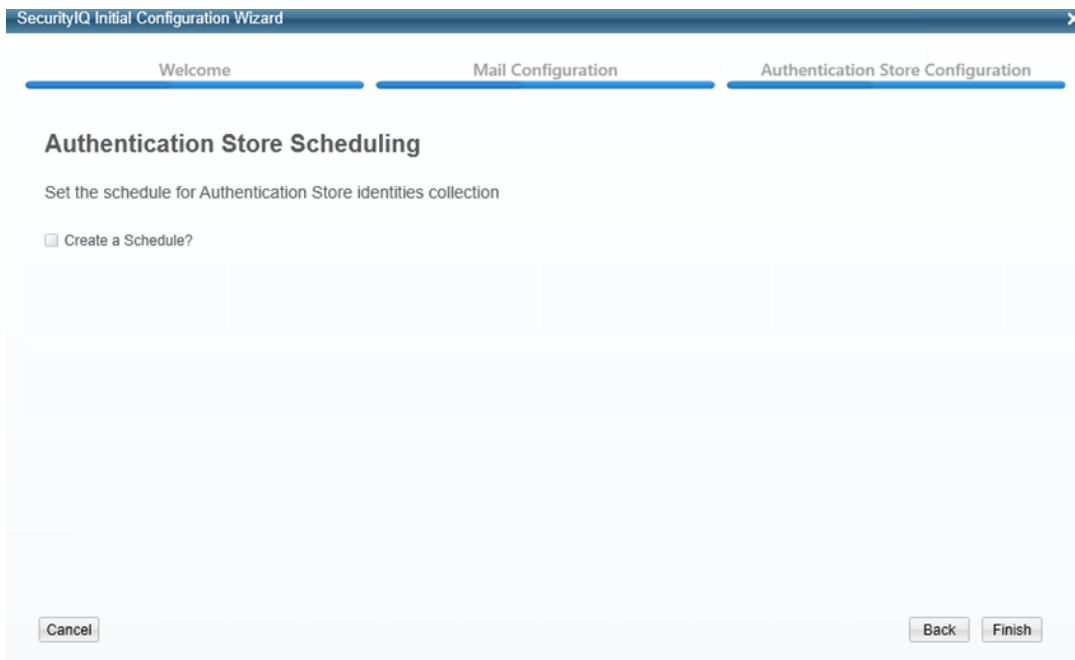
12. Check the **Create a Schedule** box.
*The Authentication Store Scheduling details window opens.*
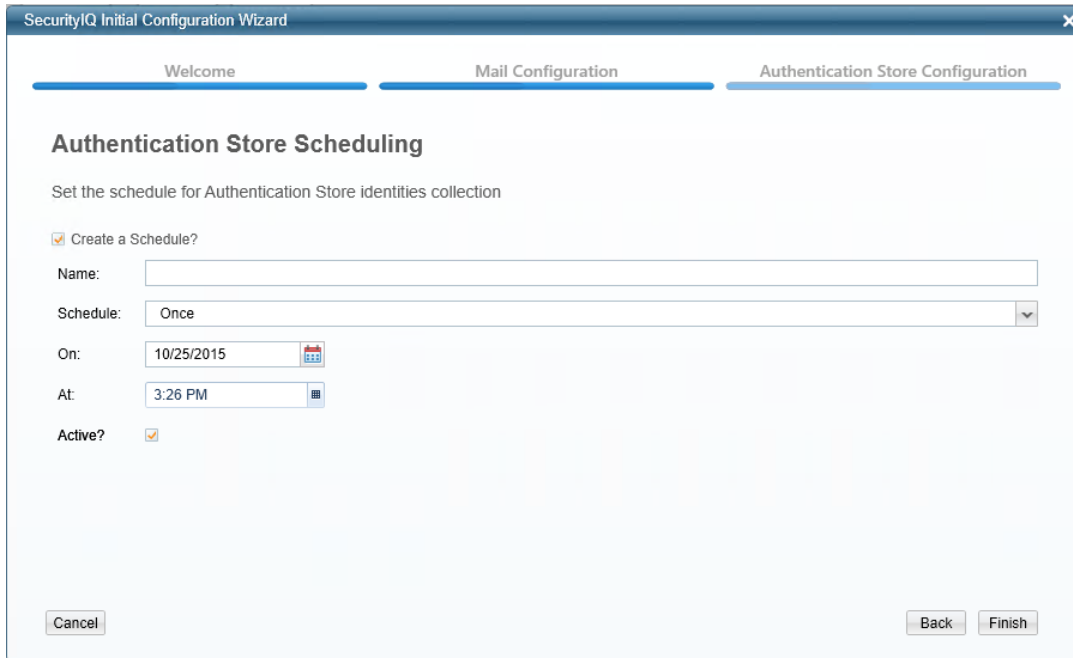


13. Type the relevant data into the following fields:

    The definition fields change according to the schedule type selected.

    a. The schedule name in the Name field

    b. The schedule frequency in the Schedule field

    c. The date the schedule begins in the On field

    d. The time the schedule begins in the **At** field

14. Check the **Active** check box to activate/deactivate the schedule.

15. Click **Finish**.

The File Access Manager Initial Configuration Wizard ends and File Access Manager is ready to operate.

## Session Management

Once the user data is retrieved from the DB, the user is stored in IIS sessions in-memory object. The sessions in the application are configured to store data for 10 minutes (sliding expiration). If there are any requests made to the server during the last 10 minutes, session objects are distracted and authentication flow will resume on the next access to the DB.

The 'iisreset' command deletes sessions objects immediately.

> In HA/DR configurations, each IIS server stores the sessions in each server separately.

## File Access Manager website Authentication

Only users defined in the authentication store can log into the web application, and only after the collector synchronizer task completed.

When configuring File Access Manager for the first time, either wait for the initial scheduled time, or schedule the authentication store identity collection to **run now**.

To check the Collector Synchronizer task status in the administrative client health center:

1. Open the Health Center.

   In the administrative client Click **Health Center** on the left menu.
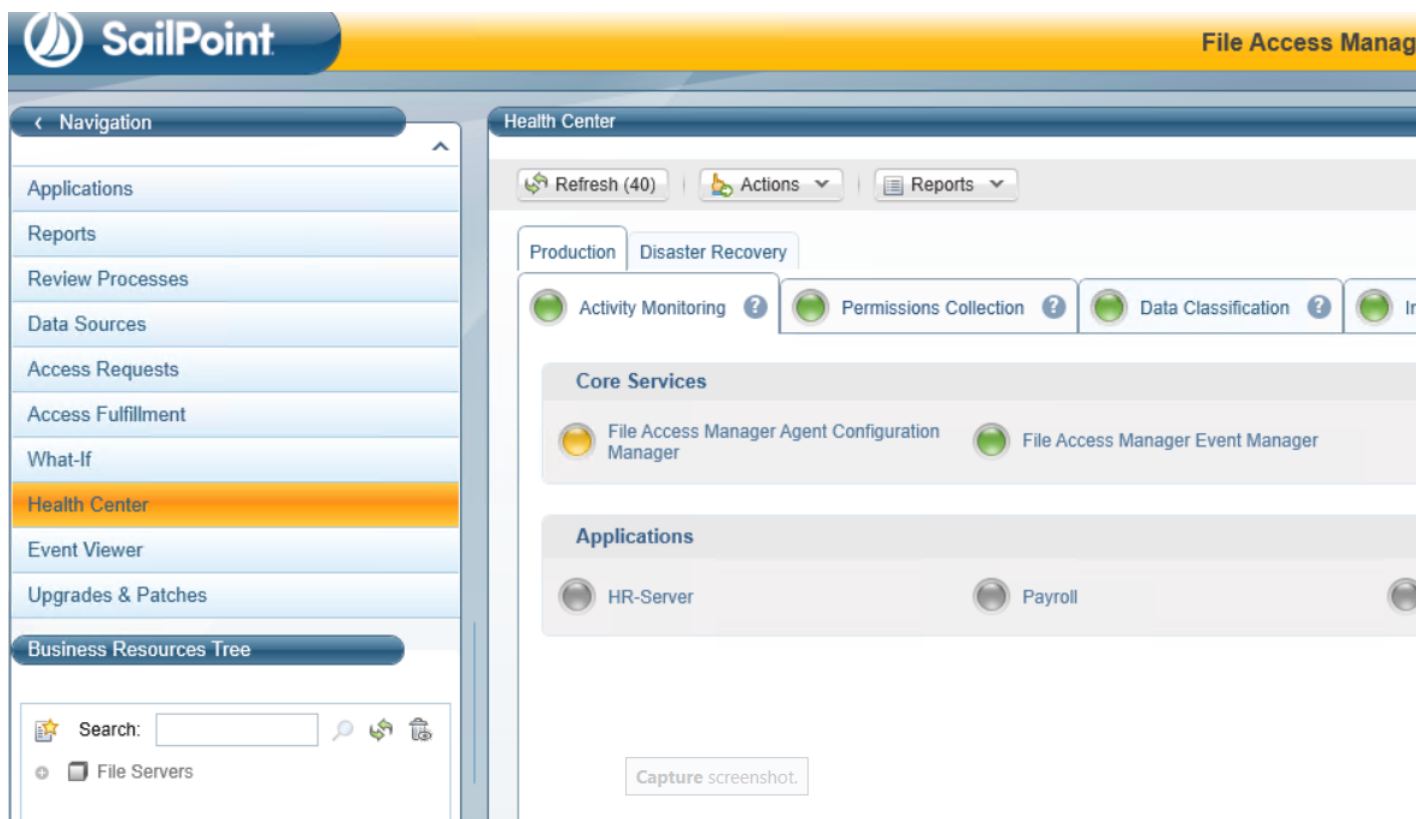


2. Select the **Permission Collection** to open a permission collection related panel.

3. Select the **File Access Manger Collector Synchronizer**

4. Select the **tasks** panel.

5. Click **Show Tasks from all users**.

6. Check the **Synchronize Identity Collector** task status.

# Activities

This chapter describes the collecting and monitoring activities (events), as well as the File Access Manager services of the activity collection process.

> This section does not discuss how to monitor specific types of applications.
> The Collector Installation guides provide information on the installation and configuration of specific collectors.

## Monitoring Activities

Monitoring activities in involves capturing information about events that users perform on monitored applications.

An activity includes the following elements:

***Who?***

A user performing the action

***Performed what action?***

Read, write, or delete

***Where?***

On what business resource, for example a file, a file folder, a SharePoint site, or an Exchange mailbox

***When?***

Date and time The timestamp is stored in UTC, and displayed to the user in its current time-zone, based on the computer from which he or she is connecting

### Event Example

1.  User jsmith, performed a write action on the \\file_server\Finance\2015\cashflow.xlsx at 7:35 pm at 16 March 2015.

2.  User contextual information for this activity are added from additional data sources, including:

    *   Attributes from the user's Active Directory, such as the user's display name, groups to which the user belongs, the user's company, title

    *   The department of the user, normally obtained from the Human Resources system

    *   Data classification information, for example, when information contains sensitive data about the business resource

3.  Finally, activity monitoring sends alerts regarding suspicious activities, based upon sets of pre-defined rules.
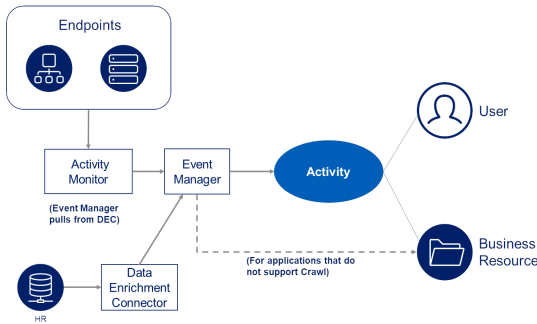
# Terminology

### Event

An event is anything that occurs in an application.

### Activity

An activity is a monitored File Access Manager event, such as the execution or modification of a file on a file system, enriched with security attributes (such as details of the executing user from the Active Directory).

### Alert

The system sends an alert when an activity violates a File Access Manager real-time rule. File Access Manager can issue alerts within the system or send them to other systems, such as SIEM for monitoring.

### Activity Monitor

Each Collector Installation guide contains specific installation and configuration instructions.

The Activity Monitor is a software module that monitors and collects events from an application. Each application type has a specific activity monitor. Most File Access Manager Activity Monitors work in an agentless architecture, and can monitor and capture events without having to install anything on the application itself.

### Event Manager

The Event Manager is a service, installed by the File Access Manager Server Installer, which:

1. Receives events from Activity Monitors.

2. Uses Data Enrichment Connectors (DECs) to enrich events with security attributes.

3. Evaluates discard and alert rules.

4. Saves events to the Elasticsearch and database.

### Data Enrichment Connector (DEC)

The previous name for a DEC was Whitebox Policy Connector (WPC).

Activities

The Data Enrichment Connector (DEC) is a software module that facilitates communication between File Access Manager and an organizational/security system. File Access Manager enables the definition of multiple DECs and uses them to enrich monitored activities with information retrieved from various organizational systems, such as Human Resources or Security Infrastructure.

File Access Manager offers DECs for many commonly used systems including:

- Active Directory

- SailPoint IdentityIQ

- LDAP

- SQL DB

# Activity Flow

This section describes the flow of events in File Access Manager, from the Activity Monitor to the Elasticsearch and database.

## Overview

The system sends and analyzes all monitored application activities in the same way, regardless of the event's origin. Since the event collection infrastructure is agnostic to event types, the system handles an event from a Windows File Server in the same way it handles an event from Microsoft SharePoint or Microsoft Exchange.

The activity path diagram below shows a high-level process flow of events, through components, from the Activity Monitor to the Event Manager, with each blue square representing a separate component.

The following sections explain the flow of events in detail.

## Activity Path

For Windows File Server, the path listed for the activity is always the physical path. This is to avoid duplication, and to avoid ambiguity of ownership and access rights.

**Administrator Guide**                                                                 56
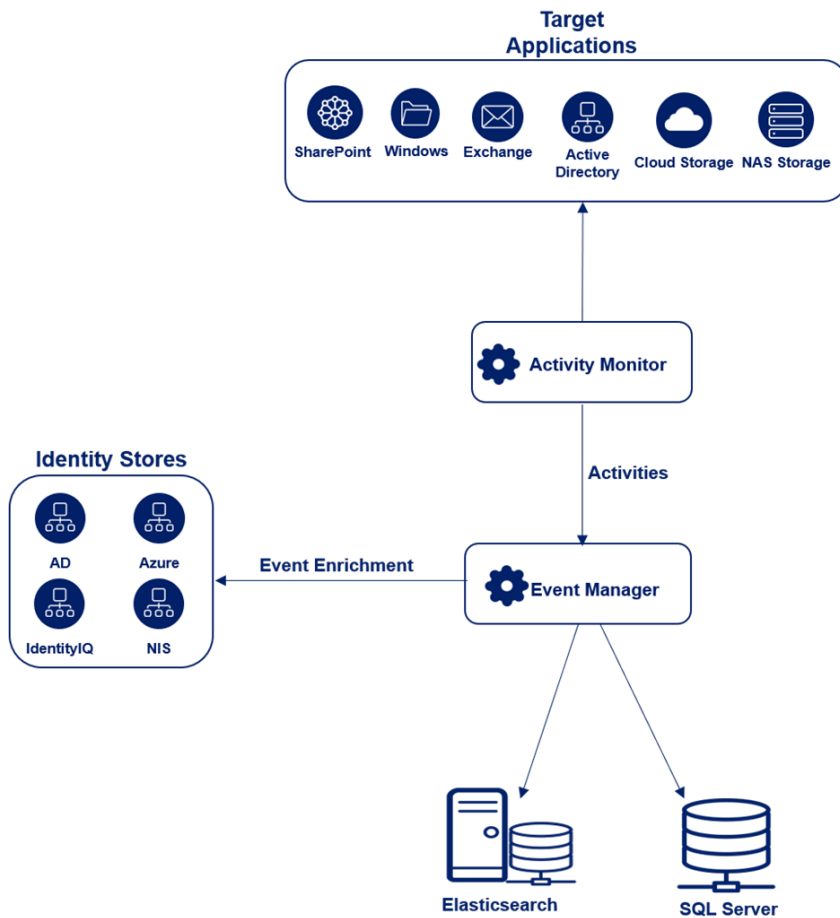
## From Activity Monitor to Event Manager (Stage I to II)

| Activity | Event |
|----------|-------|
| Monitor | Extract the events from the monitored system using the relevant technology (to be discussed later). |
| Exclude | Raw exclusion of event is available per type of monitor. Exclusion at this level means the event will not be sent. |
| Aggregate | Similar events within the same polling interval are unified into a single event. |
| Send | Events are transformed into standard event format. The bulk is compressed, and then sent. |
| Receive | The Event Collector (inside the Event Manager) receives the events. |

## From the Event Manager to the Elasticsearch and Database (Stage II to III)

| Activity | Event |
|---|---|
| Collect | Get the events from the various monitors.<br><br>Verify the structure and validity, and send to a memory queue. |
| Fetch | Get the events from the memory queue and start processing. |
| Discard | Discard rules, based on event data only, are evaluated first. |
| Enrich | If required, enrich the data with identity data. |
| Evaluate | Access Rules, requiring identity data, are evaluated.<br><br>Alert responses are sent. |
| Save | Save events to Elasticsearch and to the database. |
| Create BRs | For applications that do not support crawl – if the event is on a resource that is not listed in the database yet – add this resource. |

## Application Level Indexing (Stage IV)

After the system saves the event, Elasticsearch indexes the event data so users can construct queries on that data. By using Elasticsearch's near real-time indexing capabilities, events are available for querying immediately after they are saved.

## SQL Server Event Backups Toggle

Event activity is stored in Elasticsearch and also backed up to the configured File Access Manager SQL Server. These SQL event backups are preserved in case it is necessary to recreate the events in Elasticsearch. This section explains how to disable aspects of this feature to save space in SQL or to improve performance when saving and deleting events.

Two new system configuration options are supported in the DB table system_configuration_value:

- Store event backups to SQL Server

- Remove SQL backups on event deletion

The default behavior for both values is set to True. Events will be stored to Elastic and backups of those events will also be saved to SQL. When events are deleted, the corresponding SQL events backups will also be deleted.

If **Store event backups to SQL Server** is set to False, the event manager(s) will save events to Elastic only; backups to SQL will not be made.

If **Remove SQL backups on event deletion** is set to False, event deletion tasks will only delete events from Elastic; any existing SQL event backups will be retained. Any existing SQL event backups that are skipped from being deleted in this way will not be delete-able from File Access Manager using deletion tasks, even if **Remove SQL backups on**

**event deletion** is reset to True. When setting **Remove SQL backups on event deletion** to False, the user is responsible for the lifetime and ultimate deletion of those skipped events.

# Defining a Data Enrichment Connector

A Data Enrichment Connector (DEC) is a software module that facilitates communication between File Access Manager and an organizational / security system. File Access Manager enables the definition of multiple DECs and uses them to enrich monitored activities with information retrieved from various organizational systems, such as Human Resources or Security Infrastructure.

To define a Data Enrichment Connector (DEC), perform the following steps:
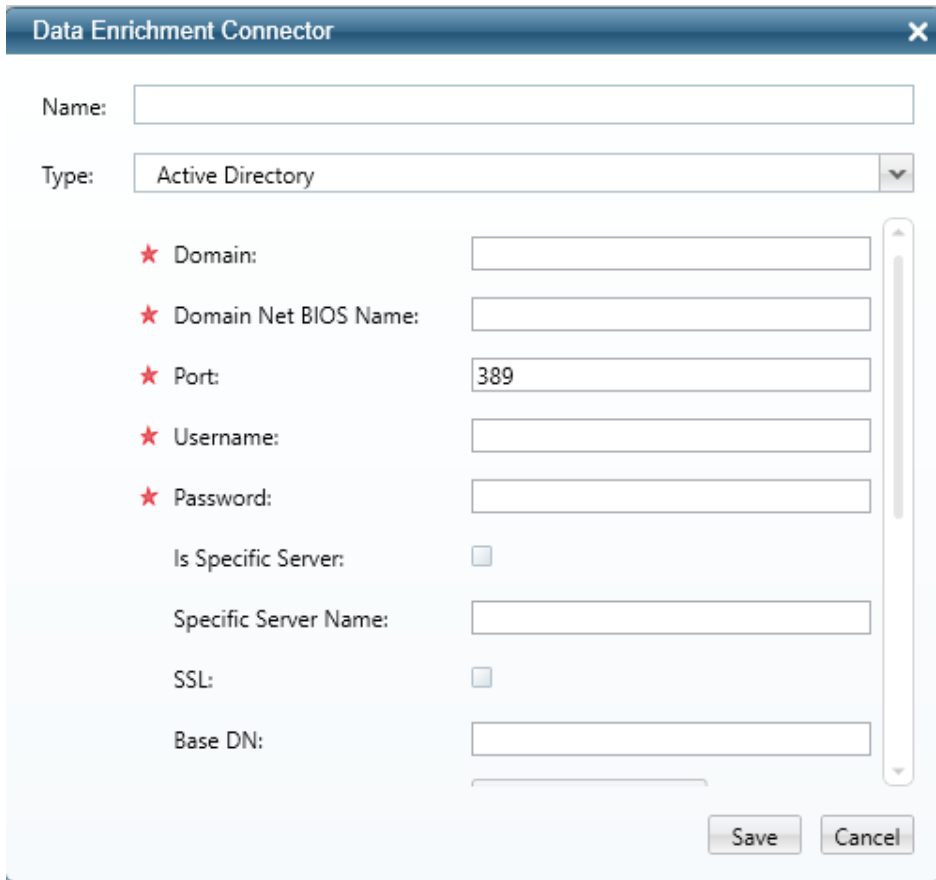
1. Navigate to **Applications > Configuration > Activity Monitoring > Data Enrichment Connectors**

   The general Data Enrichment Connectors window displays.

2. Click **New**.
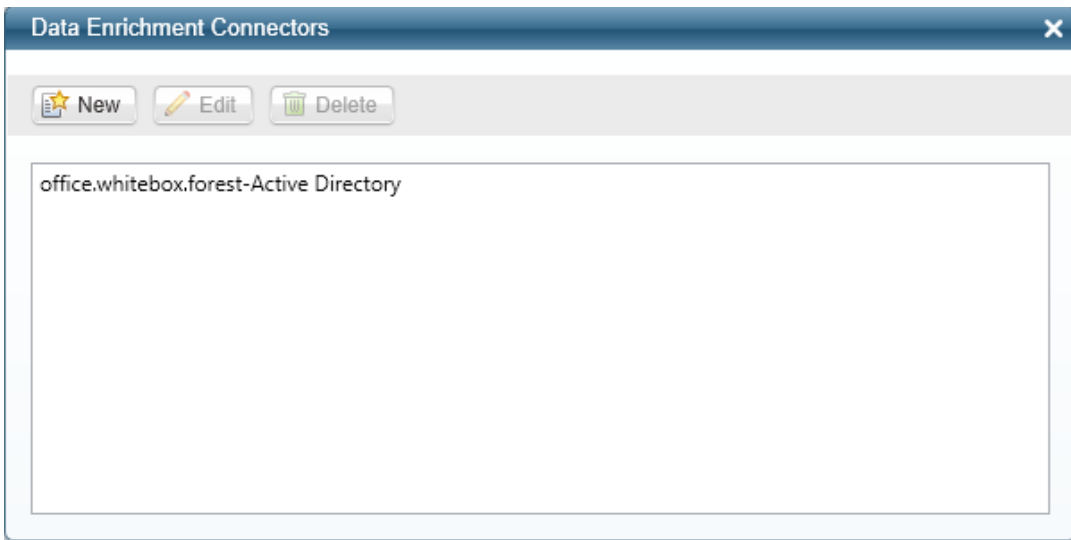


   The New Data Enrichment Connector window displays.

3.  Type a Name for the new DEC in the **Name** field.

4.  Select one of the following types from the **Type** field:

    -   Active Directory (default)

    -   File Access Manager

    -   Database

5.  The configuration fields displayed under the **Type** field vary, based upon the type of DEC selected.

    > The configuration fields in the data enrichment connector configuration tab (above) depend upon the selection of the Active Directory as the DEC type.

6.  If Active Directory is the DEC type, type in all the associated configuration fields, which for Active Directory, include:

    -   Domain

    -   Domain Net BIOS Name

    -   Port

    -   Username

- Password

    Optional configuration:

    Check the **Is Specific Server** check box to bind to a specific server, and then provide the server's name in the **Specific Server Name** field.

    Check the **SSL** check box to connect with SSL.

- Is Specific Server – Connect to a specific server (domain controller) instead of using the domain name.

- Specific Server Name – The name of the server to connect to if "Is Specific Server" is checked. Could be a short name or a FQDN as long as it's reachable.

- SSL – Connect using Secure Socket Layer / Transport Layer Security (SSL/TLS) or use unencrypted communication.

- Base DN – The Distinguished Name of the Organizational Unit to use as the root of the tree. Defaults to the root of the domain.

The following properties are only used by the data enrichment connector (DEC) to enrich activities, not by an Identity Collector that uses the DEC as a reference:

7. 
    - Groups Fetch – Whether to fetch the names of groups that users are members of (memberOf information).

    - Groups Receive – Whether to fetch memberOf information recursively.

    - Groups Recursive Levels – How many recursive levels of memberOf information to fetch.

    - User Account Control Fetch – Whether to fetch user account control information.

    - Pool Size – Number of Active Directory connection objects to keep open (effectively the number of queries that can be run in parallel).

    - Timeout – Active Directory connection attempt timeout in seconds.

    - Report Interval – Health report and configuration refresh interval.

8. If IdentityIQ is the data enrichment connector (DEC) type, follow the connector guide **Integrating IdentityIQ with File Access Manager for Enrichment**.

9. If Database is the DEC type, type in all the associated configuration fields, which for Database, include:

    - Database Type

    - User

    - Password

    - Query

    - Query Timeout (minutes)

    - Database Server

    - Database Name

# Alert Rules

Alert Rules define activity-based criteria for generating system alerts, including notifications and customized responses, such as email, SysLog, or UserExit.

For defining alert rules, navigate to **Compliance > Alert Rules**

For viewing and investigating alerts, navigate to **Forensics > Activities**

Examples of alert rules include:

- A file under \\FileStorageApplication\HR is deleted by a user who is not a member of the HR department.

- A specific user reads more than 1000 files in one minute (considered a suspicious activity, regardless of whether the user or malware initiated the activity).

***To view existing alert rules:***

1. Navigate to **Compliance > Alert Rules**.

All alerts, including alerts in the Resources section, display in this screen.

2. Click **Include Resource-based Rules** to view alerts from Resources.

3. You can filter the screen by:

- *Rule Name*

- *Status* - Activate or deactivate an alert rule from the main screen – there is no need to access the rule.

## Creating Alert Rules

***To create an alert rule:***

1. Navigate to **Compliance > Alert Rules**.

2. Click **New Rule** at the top right of the screen to open the *New Alert Rule* screen.

3. Select the Rule Type in the Trigger section.

    a. For a "Single Activity" trigger, a single activity matching the Rule Criteria creates an alert.
    For example, an Email notification will be sent for each Add Permission action on a Sensitive resource.

    b. For a Threshold trigger, multiple activities matching the Rule Criteria, and occurring within a specific time window, create an alert.
    Users can configure threshold alerts, based on suspicious behavior, and not just based on a single action.
    For example, the fact that one user has performed 500 activities on a specific resource might be more suspicious than if the user had performed a single activity on that resource.

4. All mandatory fields should be full before saving the rule.

5. See sections below for more information on Scope, Filters, and Responses for alerts.

## Managing Alert Rules

To access the alert rules, Navigate to **Compliance > Alert Rules**.

To open an alert rule for edit, double click the alert rule to edit.

### *To edit an alert rule:*

1. Make changes to the relevant parameters of the General, Scope, Filters, Triggers, and Response sections of the Rule Criteria section, as appropriate.

An Administrator can define and customize response options in the administrative client.
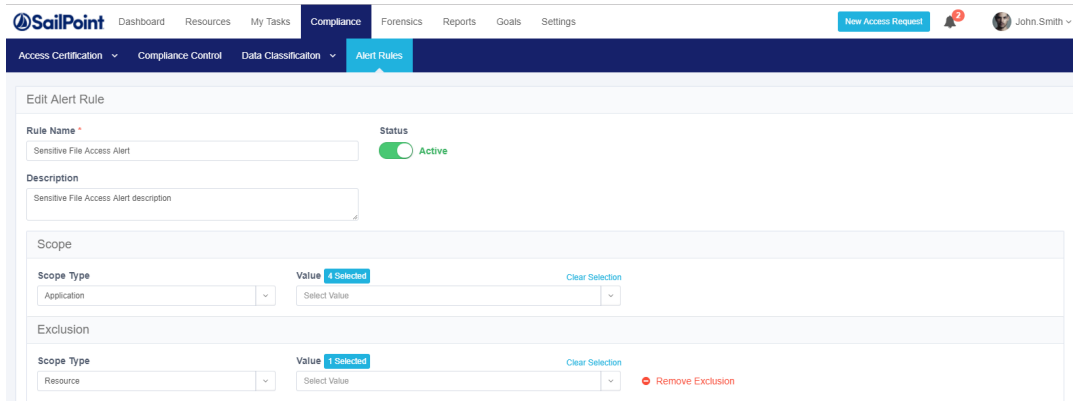


### *To duplicate an alert rule:*

1. Click **Duplicate** from *Actions* in the alert rule to be edited.

2. The Duplicate Alert Rule screen displays, with all the definitions of the duplicated rule already filled in.

3. Make any required modifications.

Duplicate a discard rule to create a new rule with definitions that resemble those of an existing discard rule.

### *To delete an alert rule:*

1. Click **Delete** from *Actions* in the alert rule to be deleted.

2. A delete confirmation question displays.

## Selecting Scope for Alert Rules

Use Scope to select a relevant running target.

- Scope inclusion enables users to specify application type, application, or specific business resource to run an alert rule.

- Scope exclusion allows users to avoid running a rule on an irrelevant application type, application, or specific business resource.

- If the same resource is selected for both inclusion and exclusion, the resource will be excluded since exclusions always overrule inclusions.

- Resource scope selection allows users to select or unselect a subfolder to run a rule by checking the "Including subfolders" checkbox:

- For example, if the business resource "Sensitive folder" has a sub-folder, called "Non sensitive folder" if the user deselects the "Including subfolders" checkbox, the rule will only run on the main resource, which is "Sensitive folder".

## Filters

> If an application has a Data Enrichment Collector (DEC), the attributes of that DEC also display. However, you select more than one application from same application type, and the applications share the same DEC, only the DEC attributes common to all of the applications' DECs display. If there are no DECs in common, only attributes relevant to the application type of the selected applications display.

Filter criteria allows users to specify suspicious behavior, based on the selected filter criteria parameters.

The available filter criteria attributes depend on the scope selected.

The list below is the basic list of attributes:

- Action Type
- Category
- Domain
- Event Date
- Event Time
- Path
- User Name

If you limit the application selection by selecting an application type or one or more applications, only the attributes relevant to the selected application type display.

Users can use queries saved in **Forensics > Activities** queries by clicking on **Load Query**, to display a list of all saved queries.

When the query is loaded, all the information in the Rule Criteria section (Scope and Filters) is overridden by the loaded query filters. If a query cannot be loaded, an error message displays.

The following queries are not available:

- Queries on alerts (since only existing queries on activities can be loaded)
- Mismatched queries
- Queries involving users from more than one domain

## Alert Rule Response

The Response section allows users to define a response for an alert.

For example, when a new permission is added to a sensitive resource, all the Data Owners of that resource can receive an email, notifying them that a new permission was added.

***To set an alert rule response:***

1. Open the Alert Rules page, at **Compliance > Alert Rules**.

2. Double click the alert rule to edit and scroll to the Response section.

A Response may be one of the following:

- Email to specific email addresses, and / or to the Data Owners who own the resource.

  Currently, the Data Owners option is available for Single Activity Alerts, but not for Threshold Alerts.

- Syslog

- User Exit

1. A Response object is created / edited in the File Access Manager administrative client.



2. Click **Advanced Settings** to select additional option responses.

  Use the administrative client to define and customize response options.

  File Access Manager Alert Response is the automatic default, since it retains the alert in the database. A user cannot opt out of the File Access Manager Alert Response.

## *Configuring a Response*

Complete the following steps:

1. Within the Administrative Client, navigate to **System > Configuration > Activity Monitoring > Responses > Manage Response Configurations**.

2. Select **Syslog** in the Showing Response Configuration of Type drop-down.

3. Click **New**.

4. Enter the syslog configuration.

5. Click **Save**.

6. Navigate to **System > Configuration > Activity Monitoring > Response > Manage Responses**.

7. Create a new Syslog response type. Use the selections on the right side to add variable information to the syslog message.

8. Click **Save**.

The response is now available to use in **Advanced Settings > Other Responses** of Alert Rules in the Web interface under Compliance.

## Resource-based Alert Rules

Data Owners can activate Resource-Based Alert Rules (out-of-the-box alert rules) in the **Resource > Alerts** screen.

Administrators can navigate to **Compliance > Alert Rules** to perform the following operations on Resource-Based rules that were created by Data Owners:

- View the rule

- Change the rule's name/description

- Change the rule's status (active/inactive)

- Delete the rule

## Troubleshooting Activities

The best way to troubleshoot activities is to follow their activity trail.

Use a specific Collector Installation and Configuration Guide to troubleshoot a specific monitoring issue for that Activity Monitor.

The lists below are suggestions of what to look for in the various services.

### Application

- All prerequisites were completed successfully

- Activities are generated when relevant
(For example, check that relevant activities are generated in the Event Log in Active Directory or that they are included in the Exchange Audit log.)

### Activity Monitor Log

- The log has errors

- Events were received (by viewing the Monitor Statistics file)

- Events were monitored, but not sent (by checking the monitoring mode – full, semi, and discard)

### Event Manager

- New events were entered (by viewing Event Collector statistics) and then moved to the memory queue

- Events were saved in the Event Manager (one Connector at a time, or through a dedicated Event Manager)

- The Event Manager log has errors

## Events Backup

File Access Manager includes a backup mechanism for events streaming into the Event Manager. Incoming events are serialized to disk as compressed bulk events.

- This backup mechanism allows for re-streaming the backed-up event bulks into the event manager in case of a failure in the events processing flow.

- A separate file is created daily, containing the bulk events received that day.

The behavior of the Events Backup mechanism is defined by several parameters under the <appSettings> tag in the Event Manager's app.config files:

| Parameter | Type | Description | Default |
|---|---|---|---|
| BackupEvents | True/ False | Enables / Disabled the Events Backup mechanism | True |
| WaitForBackupSeconds | Number | Number of seconds the Event Managers service waits for the backup process to finish serializing in-memory events, on service shutdown, before it terminates the process | 5 (seconds) |
| BackupEventsDir | Text | Directory path for the event backup files | EventsBackup in the service home dir |
| RestoreBackedupEvents | True/False | Activates backed up events restore on service startup | False |
| BackupRetentionDays | Number | Number of days to retain events backup files, before backup files are deleted. | 7 (days) |
| CleanOldBackups | True/False | Enables/Disables automatic cleanup of expired backup files (older than *BackupRetentionDays*) | True |

**To enable events backup**

- Set the **BackupEvents** to True (default). This will cause the Backup mechanism to start

- The **BackupEventsDir** by default will be set to `EventsBackup` in the service's home directory. This folder will be created by the service if it is not already there. If you wish events to be backed up to another location, change the **BackupEventsDir** parameter accordingly before the service is started, or restart it after the change. Make sure the drive containing the backup folder has enough space. (Space requirements depend on events traffic).

- Make sure the **RestoreBackedupEvents** parameter is set to false – if you don't wish to restore existing backups.

- Ensure all other parameters suit your needs, or configure accordingly.

**To restore events from previous backup**

- Set the **RestoreBackedupEvents** to True before you start the service, or restart it after the change .

- Once the service is running with **RestoreBackedupEvents** set to True, it will attempt to restore all backup files, and will stream all backed up events, back to the Event Manager, to be processed and stored.

- If you do not wish to restore all the backup files, but only specific files (days), you should copy the unnecessary files to another location .

- In case restoring the events fails, a new file contained the un-restored events will be created, with the **.recreated** suffix, indicating this file contains events that failed to be restored, and will not be re-attempted.

**To retain backups for specific dates or longer periods**

- Either disable the automatic cleanup of backup files, by setting the **CleanOldBackups** parameter to True, or modify the **BackupRetentionDays** parameter to suit the retention policy you wish to configure.

- When modifying app.config parameters, changes will take place only the next time the service is started, as app.config parameters are read on service startup.

## Threshold Alert Rules

### *Architecture and Flow*

The Activity Analytics service is responsible for the threshold calculation and issuing threshold-based alerts.

Activities are evaluated against threshold alert rules by the Event Manager during the processing of the activities, and if they match, they are marked as candidates for a threshold calculation.

The Activity Analytics queries the Elasticsearch every defined interval to bring activities candidate for threshold alerts. It then aggregates the activities and when the threshold is met, issues an alert and a response according to the definition in the threshold alert rule.

### *Limitations*

Activities received more than 15 min after the Activity time (as the result of a temporary disconnection between the Activity Monitoring and the Event Manager) will be kept in the Database with the original Activity time, but will not be included in the Threshold Alert Rules calculation. However, if an Alert has already been created, the Activities that originated in the Alert timeframe, but were received after the 15-minute time window, will be updated in the relevant existing Alert record. (As a result, the total number of Activities in the existing Alert record will increase.)

The 15-minute time window helps limit the memory required for the Threshold Alert Rules calculation.

Please review the Compass forum for best practices. If required, the PS team can change the time window in the Database.

If Windows activities have more than one shared path, the system will send duplicate activities for a threshold alert calculation. For example, if Folder1 can be accessed by \\MyServer\Folder1 and by \\MyServer\C$\Main\Folder1, each activity performed in Folder1 will appear twice in the Database, each time, with a different shared path.

To prevent duplicate activities from being calculated in the total number of activities required to create a threshold alert, select "Windows" as the application type in the scope, and set the following filter in the **Alert Rule > Rule Criteria Filter** section:
Attribute = Original Access Path (OAP)
Operator = Empty

All duplicated Activities have the OAP field as part of the original path. Adding this filter causes the Threshold Alert Rule to ignore all duplicated Activities and to calculate only the original Activity.

### *Create/Edit a Threshold Alert Rule*

See Creating Alert Rules.

Only administrators (not data owners) can view threshold alerts in Activity Forensics or in Reports.

## Stale Data

As a general rule, File Access Manager stale data calculations are based on activity data, and default to using activity data it gathers.This may include read activity, if such activity is audited for the application type.

In cases where no activity data are available for the resource, the stale data calculation is based on the last access date tracked by the operating system. If such a date is not available, the initial collection date is considered as the last access timestamp. This is the case for all resources when we start the collection process.

> The method for recording the last accessed date may differ between application types, and according to the operating systems' support for last access tracking. For example, most SMB/CIFS-enabled file system disable last access tracking for read activity by default due to performance considerations.

## Stale Data Report

To get an updates list of stale data in your system, configure and run the stale data report.

1. Navigate to **Reports > Templates**

2. Search for "Stale Data" to find the report template

3. To configure the stale data report: Select "Duplicate Template" from the dropdown menu on the report template

4. Configure the report to fit your requirements:

    - Classification category

    - Last used (months) - time definition of stale data for this type of data. Default: 6 months

    - Resource minimal size (MB). Default is 0

- Scope type : By application or folder name

- Additional tags: To help find this report

5. **Scheduling**

    Set the requested schedule for the stale data report

    **Run Now**

    Saves the schedule, and runs the report now

6. **Save**

    Saves the schedule, and runs the report according to the schedule

# Crawling Overview

Crawling is the process that discovers the business resources (BRs) of a specific application type. It is the first task involving an application, since BRs are required for many other activities involving applications, such as Permissions Collection and Access Certification.

For example, a crawler may discover folders (BR) on a file server (an application type), or mailboxes and folders (BRs) on Exchange (an application type).

Before beginning the crawling process, you must install and run the permissions collection service for each application.

The crawling process involves the following:

- Discovery of business resources and the population of a BR tree.

- business resource size calculation.

| File Name | File Type | Size |
|---|---|---|
| Finance Balance Sheet.xls | Excel (*.xls) | 2 M |
| Finance Salaries.docx | Word (*.docx) | 1 M |
| Finance Departments.txt | Text (*.txt) | 3 M |
| Finance Organization.ppt | PowerPoint (*.ppt) | 5 M |
| Finance Other Files | (An uncommon file type) | 4 M |

- Summary of business resource size by file type

| Category Name | Size |
|---|---|
| Office Files | (2M + 1M + 5M) = 8M |
| Text Files | 3M |
| Finance Other Files | 4M |

The Business Resource Trees display the results of crawling in various locations in File Access Manager.

## Interaction of Crawling with Permissions Analysis

The permissions analysis process, in brief:

- The crawling process collects applications BRs.

- In parallel, the Identities Collector collects users and groups (which may occur before the crawler collects the BRs, since these collections are unrelated).

- The Permissions Collector collects the BRs, users, and groups, and associates them with permission types to create permissions.



Creates when new/custom permissions found
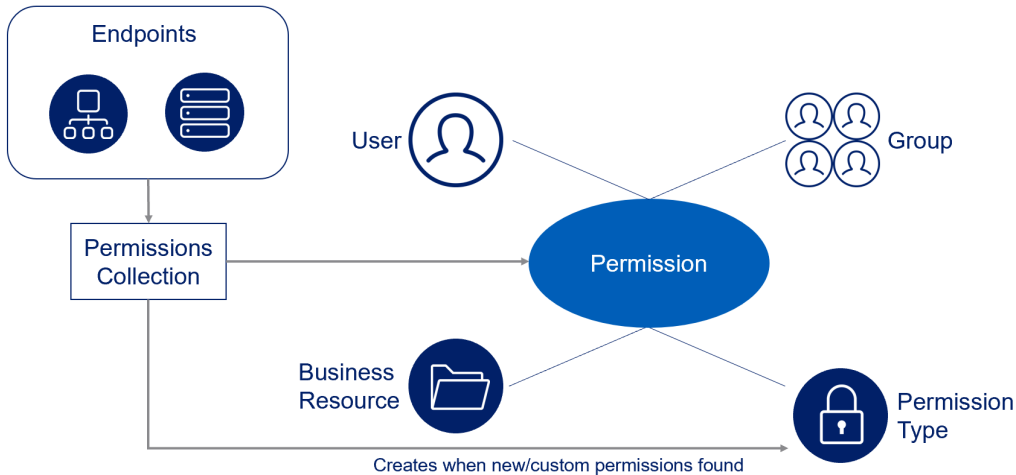
## Configuring and Scheduling the Crawler

***To set or edit the Crawler configuration and scheduling***

- Open the edit screen of the required application.

    a. Navigate to **Admin > Applications**.

    b. Scroll through the list, or use the filter to find the application.

    c. Click the edit icon ✎ on the line of the application.

- Press **Next** till you reach the **Crawler & Permissions Collection** settings page.

    The actual entry fields vary according to the application type.

***Crawl Mailboxes, Crawl Public Folders***

Valid for Exchange and Exchange Online only

Select the types of folders to scan

***Crawl Snapshots Folders***

Only for NetApp - CIFS / NetApp - NFS

***Calculate Resources' Size***

This option is not relevant for Active Directory, Exchange, Exchange on-line, SQL Server, and Windows DFS

Determine when, or at what frequency, File Access Manager calculates the resources' size.

Select one of the following:

- Never

- Always

- Second crawl and on (This is the default)

### *Exclude CloudTrail Logs*

For AWS S3 only

Check this box to exclude CloudTrail logs from being crawled and analyzed. There could be a very large number of these log files, and scanning them will have a negative impact on performance.

The default is checked.

### *Create a Schedule*

Click to open the schedule panel. See Scheduling a Task

## *Setting the Crawl Scope*

There are several options to set the crawl scope:

- Setting explicit list of resources to include and / or exclude from the scan.

- Creating a regex to define resources to exclude.

**Including and Excluding Paths by List**

*To set the paths to include or exclude in the crawl process for an application*

- Open the edit screen of the required application.

     a. Navigate to **Admin > Applications**.

     b. Scroll through the list, or use the filter to find the application.

     c. Click the edit icon ⬚ on the line of the application.

- Press **Next** till you reach the **Crawler & Permissions Collection** settings page.

     The actual entry fields vary according to the application type.

1. Scroll down to the Crawl configuration settings.

2. Click **Advanced Crawl Scope Configuration** to open the scope configuration panel.

3. Click Include / Exclude Resources to open the input fields.

4. To add a resource to a list, type in the full path to include / exclude in the top field and click **+** to add it to the list.

5. To remove a resource from a list, find the resource from the list, and click the *x* icon on the resource row.

> When creating exclusion lists, excludes take precedence over includes.

**Excluding Paths by Regex**

*To set filters of paths to exclude in the crawl process for an application using regex*

- Open the edit screen of the required application.

    a. Navigate to **Admin > Applications**.

    b. Scroll through the list, or use the filter to find the application.

    c. Click the edit icon [edit] on the line of the application.

- Press **Next** till you reach the **Crawler & Permissions Collection** settings page.

    The actual entry fields vary according to the application type.

1. Click **Exclude Paths by Regex** to open the configuration panel.

2. Type in the paths to exclude by Regex, See regex examples in the section below. Since the system does not collect BRs that match this Regex, it also does not analyze them for permissions.

**Crawler Regex Exclusion Examples - General**

> For each application according to the structure and rules of the application. See specific examples in the following section for AWS, Google Drive, and Linux.

The following are examples of crawler Regex exclusions:

# Exclude all shares which start with one or more shares names:

Starting with \\server_name\*shareName*

Regex: `\\\\server_name\\`*shareName*`$`

Starting with \\server_name\shareName or \\server_name\*OtherShareName*

Regex: `\\\\server_name\\(`*shareName*`|`*OtherShareName*`)$`


# Include ONLY shares which start with one or more shares names:

Starting with \\server_name\*shareName*

Regex: `^(?!\\\\server_name\\`*shareName*`($|\\.*)).*`

Starting with \\server_name\*shareName* or \\server_name\*OtherShareName*

Regex: `^(?!\\\\server_name\\(`*shareName*`|`*OtherShareName*`)($|\\.*)).*`

## Narrow down the selection:

*Include ONLY* the C$ drive shares: \\server_name\*C$*

```
Regex: ^(?!\\\\server_name\\C\$($|\\.*)).*
```

Include ONLY one folder under a share: \\server\share\*folderA*

```
Regex: ^(?!\\\\server_name\\share\$($|\\folderA$|\\folderA\\.*)).*
```

Include ONLY all administrative shares

Regex: ^(?!\\\\server_name\\[a-zA-Z]\$($|)).*

> To write a backslash or a Dollar sign, add a backslash before it as an escape character.

> To add a condition in a single command, use a pipe character "|" .

**Crawler Regex Exclusion Examples - Linux**

### *Exclude a path*

Example:  The path /root

```
^\/root($|\\.*)
```

### *Exclude multiple paths*

Example: /root and /media

```
^(\/root|\/media)($|\\.*)
```

### *Include only a path (example: /home)*

Please note that the parent directories must also be added, in this example we added the path '/'

```
^(?!(\/|\/home)($|\/.*)).*
```

### *Include multiple paths*

Example: /home and /boot

Please note that their parent directories must also be added, in this example we added the path '/'

```
^(?!(\/|\/home|\/boot)($|\/.*)).*
```

> To write a slash or a Dollar sign, add a backslash before it as an escape character.

> To add a condition in a single command, use a pipe character "|" .

**Crawler Regex Exclusion Examples - Google Drive**

*Exclude all drives that start with one or more user names:*

Example:  Starting with John.Doe

```
^Users\\John\.Doe@.*
```

Example:  Starting with John.Doe or Jane.Doe

```
^Users\\(John|Jane)\.Doe@.*
```

*Include ONLY drives that start with one or more user names*

Example: Starting with John.Doe

```
^(?!Users\\John\.Doe@.*).*
```

Example: Starting with John.Doe or Jane.Doe

```
^(?!Users\\(John|Jane)\.Doe@.*).*
```

**The AWS Path Structure in File Access Manager**

File Access Manager uses a path name in the following structure:

Path Structure: Root/[OU]/[Account]/[Bucket Path]/[Folder]/[Filename]

Component structure: Root/[OU]/[OU2]/[Account name](#[Account ID])/s3.[region].[bucket name]/[folder]/[file name]

Example: Root/Example-OU/Example-Account(#420269343516)/s3.north-east-17.HR3In-putDataBucket/Prospects/CVs/SueSmithPM.Docx

*Root*

All paths start with "Root/"

*OU*

The organizational unit. This could be empty, or include a sting of one or more OUs, according to the BR hierarchical structure.

*Account*

Since account names are not unique under an organization, this string includes the account ID and the account name

```
[Account name](#[Account ID])
```

*Bucket Path*

The bucket section of the path starts with "s3." and includes the region

```
s3.[region].[bucket]
```

**Crawler Regex Exclusion Examples - AWS S3 Buckets**

The following are examples of crawler Regex exclusions:

## Exclude all Folders Which Start With One or More Folder Names

***Starting with bucket_name/folderName***

Regex: bucket_name/folderName$

***Starting with bucket_name/folderName or bucket_name/OtherFolderName***

Regex: bucketName/(folderName|OtherFolderName)$


## Include ONLY Folders Which Start With One or More Folder Names

***Starting with bucket_name/shareName***

Regex: ^(?!bucket_name/shareName($|/.*)).*

***Starting with bucket_name/folderName or bucket_name/OtherFolderName***

Regex: ^(?!bucket_name/(folderName|OtherFolderName)($|/.*)).*

> To write a backslash or a Dollar sign, add a backslash before it as an escape character.

> To add a condition in a single command, use a pipe character "|" .


**Excluding Top Level Resources**

Use the top level exclusion screen to select top level roots to exclude from the crawl. This setting is done per application.

***To exclude top level resources from the crawl process***

1. Open the application screen

   *Admin > Applications*

2. Find the application to configure and click the drop down menu on the application line. Select **Exclude Top Level Resources** to open the configuration panel.

3. ***Run Task***

   The Run Task button triggers a task that runs a short detection scan to detect the current top level resources.

   Before running the task for the first time, the message above this button is:

   **"Note: Run task to detect the top-level resources"**

   If the top level resource list has changed in the application while yo u are on this screen, press this button to retrieve the updated structure.

   Once triggered, you can see the task status in

   *Settings > Task Management > Tasks*

> This will only work if the user has access to the task page

When the task has completed, press **Refresh** to update the page with the list of top level resources.

4. Click the top level resource list, and select top level resources to exclude.

5. Click *Save* to save the change.

6. To refresh the list of top level resources, run the task again. Running the task will not clear the list of top level resources to exclude.
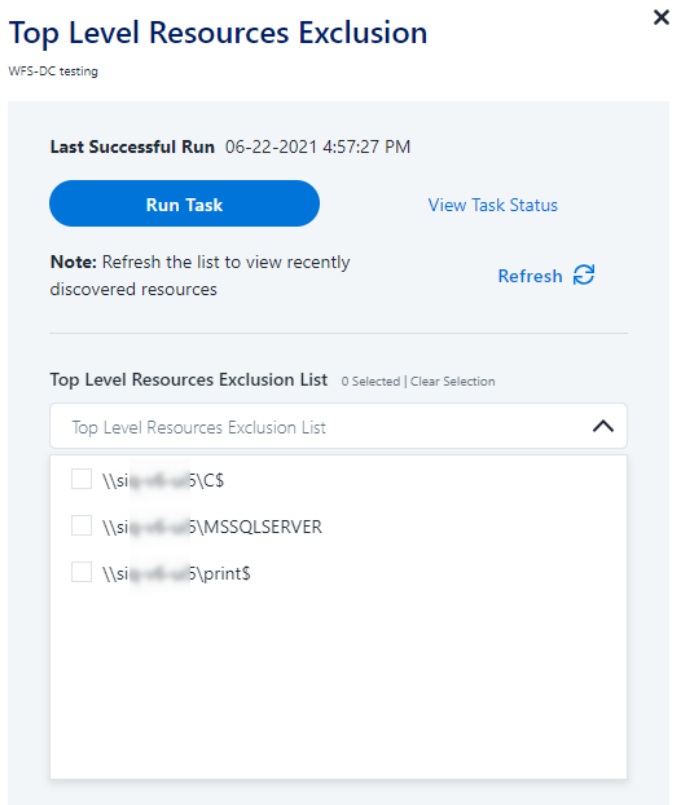


**Special Consideration for Long File Paths in Crawl**

If you need to support long file paths above 4,000 characters for the crawl, set the flag

**`excludeVeryLongResourcePaths`**

in the Permission Collection Engine App.config file to true.

By default this value will be commented out and set to false.

This key ensures, when enabled, that paths longer than 4000 characters are excluded from the applications' resource discovery (Crawl), to avoid issues while storing them in the SQLServer database.

When enabled, business resources with full paths longer than 4000 characters, and everything included in the hierarchical structure below them, will be excluded from the crawl, and will not be collected by File Access Manager. This scenario is extremely rare.

| You should not enable exclusion of long paths, unless you experience an issue.

### *Background*

File Access Manager uses a hashing mechanism to create a unique identifier for each business resource stored in the File Access Manager database. The hashing mechanism in SQLServer versions 2014 and earlier, is unable to process (hash) values with 4,000 or more characters.

Though resources with paths of 4000 characters or longer are extremely rare, File Access Manager is designed to handle that limitation.

### *Identifying the Problem*

When using an SQL Server database version 2014 and ealier

The following error message in the Permission Collection Engine log file:

```
System.Data.SqlClient.SqlException (0x80131904): String or binary data would be
truncated.
```

In all other cases, this feature should not be enabled.

### *Setting the Long Resource Path Key*

The Permission Collection Engine App.config file is `RoleAnalyticsServiceHost.exe.config`, and can be found in the folder

%SailPoint_Home%\FileAccessManager\[Permission Collection instance]\

Search for the key **excludeVeryLongResourcePaths** and correct it as described above.

## Business Resource Structure

The table below lists additional information on the Business Resource Structure.

| Applic-ation Type | Business Resource Type | Business Resource Full Path Structure | Example |
|---|---|---|---|
| Active Dir-ectory | Every LDAP Object | Distinguished Name | CN=Howard,C-CN=Users,DC=Example,DC=com |
| Box | Folder | Users/<user email>/<Folder-Path> /All Files/<Folder-Path> | Users/alice@co.and.co/Points of Interest/Data Classification /All Files/doc/Chinese |
| DropBo-x | Folder | Team Members/<user email>/<Folder-Path> Public/<Folder-Path> | Team Mem-ber-s/Bat-man@bruce-wain.Example.com/Hobbies/Caving Public/Villains/Joker/Hobbies/Product Man- |

| Applic-ation Type | Business Resource Type | Business Resource Full Path Structure | Example |
|---|---|---|---|
| | | | agement |
| EMC Celerra - CIFS | Folder | \\<Server->\<Share>\<Folder-Path> | \\celerra-cifs\Users\Ed |
| EMC Celerra - NFS | Directory | /<Export>/<Directory-Path> | /users/ed |
| EMC Isi-lon | Folder | \\<Server->\<Share>\<Folder-Path> | \\emc-isilon\Finance\Budget\Last Year |
| Exchan-ge Online | Mailbox Folder | Mailboxes\<Mailbox-Owner-UPN>:\<Folder-Path> | tom@whereabouts. Example.-com:\Inbox\Scripts\Cast Away |
| | Public Folder | Public Folders\<Public-Folder-Path> | Public Folder-s\Assets\Assessments\Assorted |
| Exchan-ge On-premis-e | Mailbox Folder | Mailboxes\<Mailbox-UPN>:\<Folder-Path> | Mail-boxes\inigo.-montoya@Example.com:\Inbox\Bugs |
| | Public Folder | Public Folders\<Public-Folder-Path> | Public Folders\Public\Private |
| Gen-eric NFS | Directory | /<Export>/<Directory-Path> | /export/goods |
| Google Drive | Folder | Users/<user email>/<Folder-Path> | Users/glenn@501. Example.com /Things to do/Done |
| Win-dows File Server | Folder | \\<Server->\<Share>\<Folder-Path> | \\winserver\C$\Program Files<br><br>\\winserver\Public\Presentations |
| NetApp - CIFS | Folder | \\<Server->\<Share>\<Folder-Path> | \\netapp\share\with\the\World |
| NetApp - NFS | Directory | /<Export>/<Directory-Path> | /projects/next_iphone |
| OneDri-ve for | Folder | Personal/<user email>/<Folder-Path> | Perosnal/watson@company. Example.-com/Diagnostics/Recent |

| Applic-ation Type | Business Resource Type | Business Resource Full Path Structure | Example |
|---|---|---|---|
| Busi-ness | | | |
| ShareP-oint | Site Col-lec-tion/List/Fold-er | http://<SharePoint-Server>/<Site-Col-lec-tion>/<Site>/List-s/<List>/<Folder> | http://share-point2013.Example.-com/TeamSite/Lists/ListOfStuff/Really Important |
| ShareP-oint Online | Site Col-lec-tion/List/Fold-er | https://<Company-Name>.share-point.com/<Site-Col-lec-tion>/<Site>/List-s/<List>/<Folder> | https://sailpoint.sharepoint.com/Wayback Site/Lists/Songs/New York/New York |

# Permissions

This section describes the File Access Manager permissions and the operations available under the Permissions menu in the Administrative Client and Forensics menu within the website.

## General

Many of the key File Access Manager Permissions use cases involve every aspect, from gaining visibility to actual act-ive involvement of management in permission reviews.

Permissions describe the access that a specific User or Group must a specific Business Resource.

Examples of permissions include:

- Mary Jones has Read access to the Finance folder directly
- John Smith has Write access to the Finance folder because he is a member of the Finance AD Group
- Larry Taylor has Write access to the Finance folder directly because he is a member of the Admins AD Group

Atypically, a permission may also include an Allow/Deny modifier.

### *Permission Modeling*

Basic rules are used to model permissions from various systems into a single coherent view.

Every permission consists of a combination of the following four elements:

- User
- Group

- Permission

- BR

Not all components are required for all permissions, since some systems provide direct permissions to users, while others only enable permissions through groups.
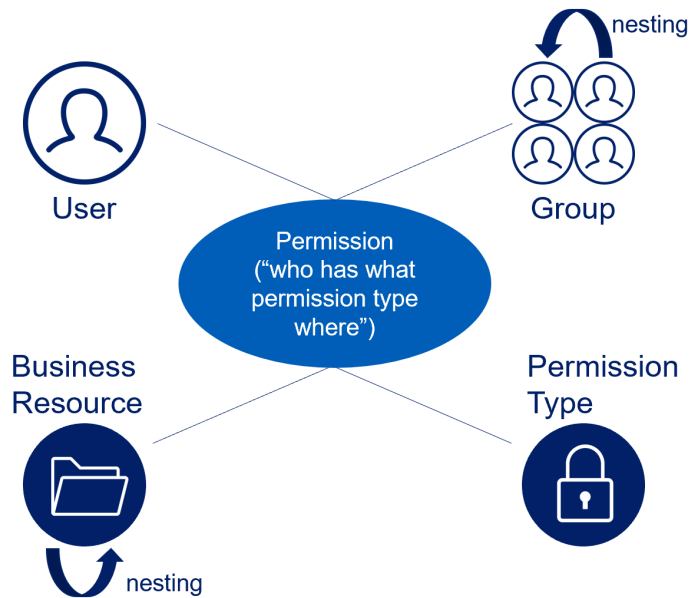


## User

The user is an object that represents an account associated with a permission.

Standard user attributes include:

### User type

> User, orphan, or local

### User disabled / enabled


### User domain

> The security domain in the identity store in which the user is defined. For example, you can define the identity store as an Active Directory forest, in which you define the User in one of the domains of the forest.

User data is commonly part of an identity collector connected to a relevant identity store.

For example:

- **Identity Store** = Organization's Active Directory.
- Extended Attributes:
    - Department
    - Manager

## *Group*

A Group is a container of users that represents a Group, Responsibility, or Profile.

Some endpoint systems only set permissions through groups.

Standard Group attributes include:

- **Group Type** is often provided in accordance with the group type, depending on the type of endpoint system.
- For example:
    - SharePoint local groups—"SharePoint group"
- **Group Domain** is the security domain in the identity store in which a group is defined. For example, the identity store is an Active Directory forest, with the Group defined within one of the forest domains.

## *Group Nesting*

Normally, it is possible to nest Groups (one group resides within another group). For example, assume that Group A contains both User A and User B. If Group A is also a member of Group B, then it follows that Group B also contains User A and User B. File Access Manager examines all nested groups when it analyzes which entities are effective group members for a given group.

## *Permissions*

Permissions are functions enabled, or denied to, a user or group.

Permissions are identified for out-of-the-box supported systems.

The standard permission attributes (that provide context) include:

- **Permission Type** – The function name
- Access Control List (ACL) Allowed – Allow/Deny
- **Is Inherited** – Defined locally or inherited

"Is Inherited" is crucial to Permission queries, since it eliminates permission duplication by showing only unique permissions.
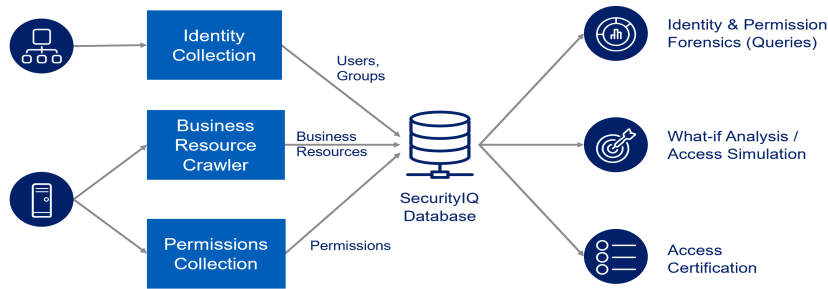
## *Owner Permission*

Most permission mechanisms utilize a special Owner permission type. Typically, the Owner permission cannot be blocked, revoked, or customized, and provides full access rights.

Different applications and permission mechanisms may interpret Owner permission differently. The table below describes the permission types that File Access Manager treats as an Owner permission. For each platform, the Owner permission is defined and named (queried by the listed name in the AFM query filter controls).

| Permission Scheme | Description |
|---|---|
| Microsoft ACL | Microsoft Access Control Lists contain a special field that indicates the owner user/group) of the resource (for example, a file or a folder).<br><br>There can be only one entity defined as the Owner (but that Owner can be a group).<br><br>Since an Owner has full control of the ACL, the Owner effectively grants all permissions.<br><br>The Microsoft ACL Owner applies to:<br><br>• Windows File Server<br><br>• Active Directory<br><br>• Microsoft Exchange / Microsoft Exchange Online<br><br>• NetApp – CIFS<br><br>• EMC Celerra – CIFS<br><br>• EMC Isilon – CIFS |
| Unix | When a file(/folder) is created in Unix/Linux, its creator is automatically set as the Owner.<br>Permissions are categorized by:<br><br>• Owner |

| Permission Scheme | Description |
|---|---|
| | • Users in the Owner's group |
| | • Other Users |
| | There can only one owner user and one owner group per file/folder. |
| | Since only the Owner (or root) can change file permissions, an Owner effectively grants all permissions. |
| | The Unix file system Owner applies to: |
| | • NFS (when using Unix permissions, but not NFSv4 ACLs) |
| | • NetApp – NFS |
| | • EMC Celerra – NFS |
| SharePoint | A SharePoint server features Site Collection containers, which function as separate entities, and permission scopes. Different Site Collections may have different users, groups, and permission types. |
| | One or more users in a Site Collection may be defined as a Site Collection Administrator. The Administrator has full control of the resources in the Site Collection's inner structure. |
| | The SharePoint Site Collection Administrator applies to: |
| | • Microsoft SharePoint |
| | • Microsoft SharePoint Online |
| | • Microsoft OneDrive |
| Cloud Storage Providers | Typically, cloud storage providers include a permission type named "Owner" which grants full access rights to the resource (file, folder etc.). |
| | The generic "Owner" permission is employed in: |
| | • Box.com |
| | • Dropbox |
| | • Google Drive |

## Business Resource

A business resource (BR) is a monitored application object, such as a folder on a file server, a site on SharePoint, or a mailbox on Exchange.

Business resources can have child BRs, and can inherit permissions from a parent resource.

Standard business resource attributes include:

- **Name** – The name of the resource

- **Full Path** – The path with all its hierarchy levels (a unique business resource identifier, for example C:\Finance\CTO)

- **Inherits Permissions** – A flag identifying whether or not a business resource inherits permissions

In cases of applications which support file level permissions, the business resource tree will include BRs on a file level, where:

    a.  The application is configured in the setup to includes file level permissions

    b.  The file has unique permissions, compared to its parent nodes.

### *Inheritance*

While inheritance can make management easier, it also can result in unnecessary duplication.

Permission analysis analyzes inheritance by determining whether a business resource inherits permission, and whether a specific permission is inherited.

The table below lists the relationships involved in permission analysis.

| Business Resource Inherits Permission | Permission is Inherited | Result |
|---|---|---|
| True | True | **The permission is not unique** and derives from the father permission. |
| True | False | **The permission is unique** and even though the business resource inherits permissions, the specific permission is not inherited. This is a common scenario in NTFS. |
| False | False | The permission is unique. |
| False | True | The permission is unique. |

> The last case in the table is a situation that occurs in a few specific end systems (as it is logically inconceivable). For example, the system enforces SharePoint Policy Rule Permissions from the Web application level. Therefore, even if the business resource does not explicitly inherit any permissions, permissions are still inherited.

### *Permission Examples*

The table below lists examples of the results of combining specific permission elements.

| BR | Permission | User | Group | Result |
|---|---|---|---|---|
| Folder X | Read | Asmith | Group1 | User Asmith has read permission on Folder X derived from Group1. |

| BR | Permission | User | Group | Result |
|---|---|---|---|---|
| Folder X | Read | Asmith | | User Asmith has a direct read permission on Folder X. |
| Folder X | Read | | Group1 | Group1 has read permissions on Folder X. The group is empty. |

## The Permissions' Collection Process

Permissions Collection is a process that discovers and collects permissions on the BRs (business resources, such as folders) of an application. These permissions are later used and displayed in Permissions Forensics, Access Certification campaigns, Access Requests, and in other locations.

The task itself is a "Permissions Collection" task.

The permission collection uses one Permissions Collector Engine and zero or more Permissions Collectors.

*Permissions Collector*

Collects permissions from the application, usually installed near (network wise) the application itself so it will be easier for it to read the permissions.

This service must be linked to exactly one existing "Permissions Collector Engine", which will supply the work. By work we mean - how to connect to the application and which resources to get the permissions for.

**Prerequisites for installation**

- There is at least one engine

- RabbitMQ is configured

*Permissions Collector Engine*

There are two configuration modes:

1. With one or more "Permissions Collectors".

   In this case, the engine will give work to the collectors, get all the permissions back from them and write everything to the DB.

   The Engine and Collectors communicate through the RabbitMQ.

2. Without any "Permissions Collectors".

   RabbitMQ is not relevant in this case.

   In this case, it acts as both an Engine and Collector.

   This service is usually installed near the DB, in order to increase the performance of reading / writing the data.

# Permissions Collection Components
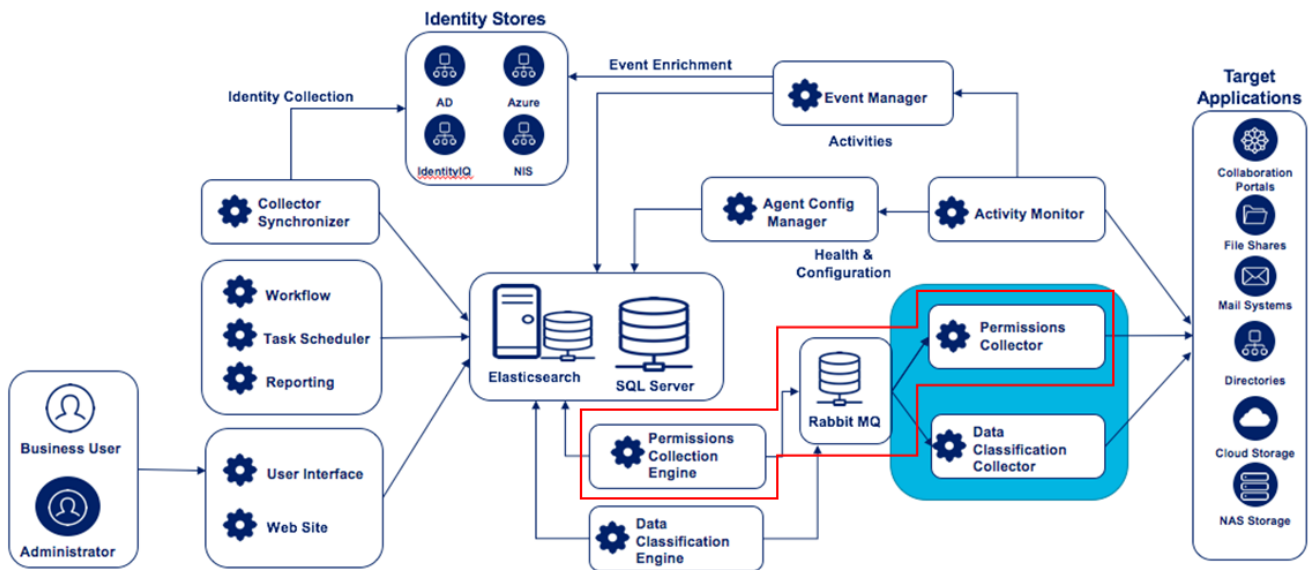
## *Configuring and Scheduling the Permissions Collection*

Permissions can be analyzed to determine the application permissions of an out-of-the-box application, provided you have defined an identity store for File Access Manager to use in its analysis, and you have run a crawl for the application.

The permission collector is a software component responsible for analyzing the permissions in an application.

The Central Permission Collector Service is responsible for running the Permission Collector and Crawler tasks.

If the "File Access Manager Central Permission Collector" wasn't installed during the installation of the server, this configuration setting will be disabled.

### *To configure the Permission Collection*

- Open the edit screen of the required application.

    a.  Navigate to **Admin > Applications**.

    b.  Scroll through the list, or use the filter to find the application.

    c.  Click the edit icon  on the line of the application.

- Press **Next** till you reach the **Crawler & Permissions Collection** settings page.

    The actual entry fields vary according to the application type.

When entering this page in edit mode, you can navigate between the various configuration windows using the **Next** and **Back** buttons.

### Central Permissions Collection Service

Select a central permission collection service from the dropdown list. You can create permissions collection services as part of the service installation process. See section "Services Configuration" in the File Access Manager Administrator Guide for further details.

### Analyze Files with Unique Permissions

Application type(s): OneDrive

### Analyze all Objects in S3 Bucket

Application type(s): AWS

If checked – collect and analyze files in the buckets, and not only buckets and folders.

Default is unchecked.

### Analyze the "Shared Link" permissions on files

Application type(s): Box

Click to collect the permissions of Shared Links. A Resource will be created for each Shared Link with unique permissions, which will display.

### Analyze the "Collaborators" permissions on files

Application type(s): Box

Click to collect permissions for files assigned directly to Collaborators. A Resource will be created for each file with Collaborators and its permissions will display.

### Analyze ACL Permissions

Application type(s): Linux, AWS

Click to fetch and analyze ACL-type Permissions.

S3 ACLs is a legacy access control mechanism that predates IAM. AWS recommends using S3 bucket policies or IAM policies for access control.

If checked, ACLs will be collected for business resources, which will impact the performance of the Permission Collector. For cases with a large number of resources, skipping the ACL permission fetch can improve the service run time considerably .

This option is checked by default

> If ACL is not supported by your server, make sure this field is unchecked.

### Calculate Effective Permissions

Application type(s): Active Directory, Exchange, Exchange Online, Windows File Server, EMC Celerra CIFS, EMC Isilon, HDS, NetApp CIFS

Calculate effective permissions during the permissions collection run

### Calculate Riskiest Permissions

Application type(s): Active Directory, EMC Celerra-CIFS, Exchange, Exchange Online, HDS, NetApp-CIFS,Windows File Server

Calculates the riskiest permission on a resource – for example, Full Control is riskier than Read permissions if both are on a resource

This option is available when selecting **Calculate Effective Permissions**.

Valid for EMC Celerra-CIFS only

Valid for NetApp-CIFS only

### *Skip Identities Sync during Permission Collection*

Skip identity synchronization before running permission collection tasks when the identity collector is common to different connectors.

| Connector | Checkbox Displayed | Default Value |
|---|---|---|
| DFS \ Generic Table | No | Not stored |
| AWS | No | True |
| Box \ DropBox \ Google Drive | Yes | Unchecked |
| All other connectors | Yes | Checked |

### *Permissions Source*

Application type(s): EMC Celerra-CIFS, HDS, NetApp-CIFS

NTFS, Share, Both

This option is available when selecting **Calculate Effective Permissions**

Valid for EMC Celerra-CIFS only

Valid for NetApp-CIFS only

### Permission Collection Setup Notes for NetApp

The permissions are managed either on the NTFS level, or on the Share Level.

When the shares are configured with Full Control to Everyone, and all the permissions are defined in the folders, you should select NTFS, which is the default.

### Permissions Comments on Isilon for the CIFS server

The permissions are managed on the NTFS level, or on the Share Level (as when the shares are configured with Full Control to Everyone, and all the permissions are defined in the folders, in which case you should select NTFS, which is the default).

**Scheduling a Task**

*Create a Schedule*

Click on this option to view the schedule setting parameters.

*Schedule Task Name*

A name for this scheduling task

When creating a new schedule, the system generates a default name in the following format:

{appName} - {type} Scheduler

You can override or keep this name suggestion.

*Schedule*

Select a scheduling frequency from the dropdown menu.

- *Schedule Types and Intervals*

  *Once*

  Single execution task runs.

  *Run After*

  Create dependency of tasks. The task starts running only upon successful completion of the first task.

  *Hourly*

  Set the start time.

  *Daily*

  Set the start date and time.

  *Weekly*

  Set the day(s) of the week on which to run.

  *Monthly*

  The start date defines the day of the month on which to run a task.

  *Quarterly*

  A monthly schedule with an interval of 3 months.

  *Half Yearly*

  A monthly schedule with an interval of 6 months.

  *Yearly*

  A monthly schedule with an interval of 12 months.

*Date and time fields*

Fill in the scheduling times. These fields differ, depending upon the scheduling frequency selected.

***Active check box***

> Check this to activate the schedule.

Click **Next**.

## *Homegrown Application Permissions Collection*

For more information on the homegrown application permissions collection process, see Creating a Homegrown Application  and Proprietary Application Permissions Collection (Homegrown Apps).

## *File level Permission Collection*

In applications that support file level permissions, and where activated, the Permission Collector will read all files/objects with unique permissions – objects with different permissions than the resource where they reside. These will be considered as business resources in the resource tree, and will support data ownership.

## OOTB Identity Collection

The identity collector is a software component responsible for synchronizing identity data (for example, accounts and attributes) from identity stores.

Examples of identity collectors include Active Directory (the most common Identity Store), NIS Identity Collector (used in Linux/Unix environments), Microsoft Azure Active Directory (used for cloud applications), and a Data Source Identity Collector.

You define the first Identity Collector in the Welcome Wizard (Getting Started), which represents the main Active Directory Domain, (or Authentication Store).

The section below describes how to create/edit an Active Directory identity collector. The process for creating/editing both NIS and Azure identity collectors is like that for creating/editing an Active Directory identity collector, with the main difference being actual configuration.

Section Configuring the Permissions Collector describes how to configure users, groups, and user-groups for homegrown Permissions Collection, which is like configuring a Data Source Identity Collector.

## *Creating or Editing an Active Directory Identity Collector*

**To create or edit an Active Directory Identity Collector:**

1. Open the Identity Collectors panel by navigating to **Applications > Configuration > Permissions Management > Identity Collectors.**

2. Click **New** to open the Identity Collector Configuration Wizard .

**Identity Collector Configuration Welcome panel**

1. Select an Identity Collector type from one of the following:

---

**Administrator Guide**                                                                                                      **91**

- Active Directory Identity Collector

- Azure Active Directory Identity Collector

- Data Source-based Identity Collector

- NIS-based Identity Collector

2. Click **Next**.

The Identities Collection window displays.

### Identity Collector Configuration Identity Collector panel

> The Identity Collector is responsible for collecting information about users and groups and the relationships between them. If required, you can map collected fields to data dictionary fields (for users and groups).

1. Type the name of the Identity Collector in the Name field.

2. Click **Enable Access Fulfillment for this Identity Collector** to enable access fulfillment for this Identity Collector.

> You can only enable access fulfillment for Active Directory identity collectors. If you enable access fulfillment, the system can add and remove users from groups in this identity collector.

3. Click **Next**.

The Active Directory Identity Collector Users Collection (1 of 5) window displays.

4. Click **DEC** to fill the Identity Collector with pre-configured data in DEC or click **By Properties** to select a property manually from a list of defined properties.

   a. If you selected **DEC**, select the relevant DEC from the dropdown list, and click **Next**.

   > If you configured DEC to connect to Active Directory, you can re-use that configuration here.

5. If you click **By Properties**, type the following data in the relevant fields:

   ***Domain NetBios***

   Domain NetBios name

   ***Port***

   The port number must be 389, or 636 if SSL is enabled

6. Check the **SSL**, **Server Bind**, and **Base DN** check boxes, as required.

7. By default, File Access Manager retrieves several properties from Active Directory, such as Department, Email, and Display Name. Check the **Properties to Fetch** check box, and type the relevant properties to retrieve.

   The properties you retrieve come from the Active Directory, and will be available later for mapping to the Data Dictionary fields.

8. Click **Next** to open the **Identity Collector: Users Collection (2 of 5)** window.

9.  Verify that the system retrieved the requested information successfully.

    > Only the first ten results display.

10. Click **Next**.

The Identity Collector: Users Collection (3 of 5) window displays:
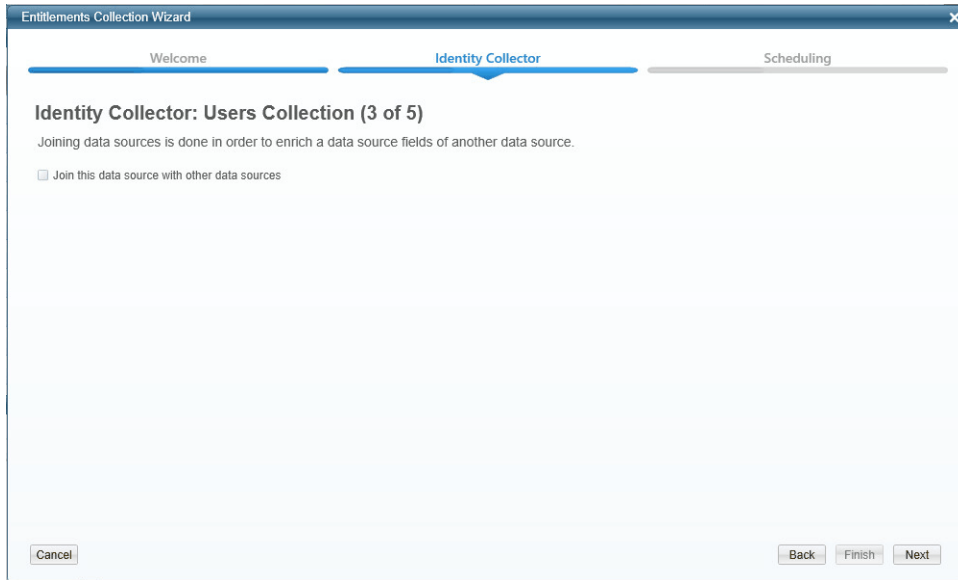


11. Data sources are created that contain user fields so that the Identity Collector can collect the Users.

12. Check the **Join this data source with other data sources** check box to join this data source to other data sources.

13. You can use one of the Identity Collector fields as the local key to gather additional user fields from other data sources by joining those data sources. Chapter contains additional information on joining data sources.

14. Type the relevant Data Source, Local Key, and Remote Key.

    > After you type the relevant data, click Test Data Sources to verify that the system has accepted the data.

15. Click **Next**.

    The Identity Collector: Users Collection (4 of 5)/ Dynamic Fields window displays.

16. Type the Dynamic Fields Mapping data from the **Dictionary Field** and **Mapped Field** dropdown lists.

    > When integrating with AWS, ADDomain has to be selected for the first Dictionary Field.

    > Use the **X** / **+** buttons to remove / add fields, as required.

17. Click **Next**.

The Identity Collector: Users Collection (5 of 5)/Hierarchy and Authentication Users Mapping window displays:
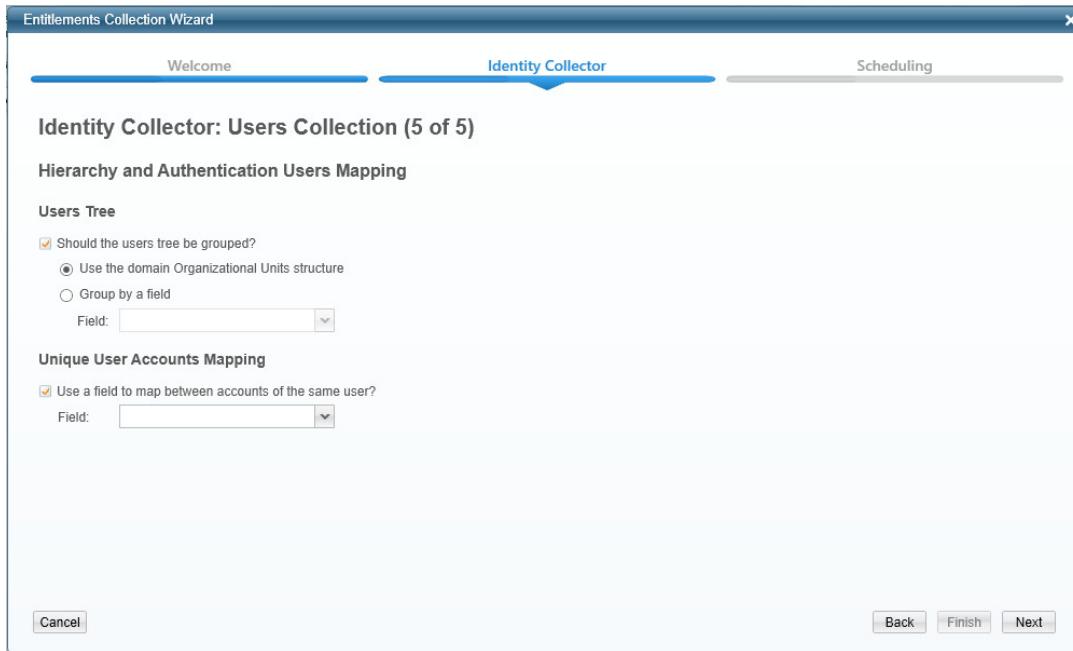
18. Click **Should the users tree be grouped**, and select one of the following:

     a. Use the domain Organization Units structure

     b. Group by a field (then select the field from the dropdown list)

          The Users Tree grouping is the same as that of the Users Tree in Advanced Forensics Control.

          "Use the Domain Organizational Unit's Structure" is only available for an Active Directory Identity Collector.

          The Email Field Mapping section will only be displayed for the Active Director Identity Collector and if it is defined in the Authentication Store. In order to have fields in the dropdown, you must first define a field mapping.

19. Check the Use a field to map between accounts of the same user check box.

          The Access Request wizard uses this mapping to match multiple accounts belonging to the same user so users can request permissions on those accounts.

20. Select a field from the dropdown list.

21. All of the accounts in various Identity Collectors with the same value in the selected field map to the same user. When the user logs into the web application to issue an Access Request, that user can request access to a specific account mapped to the logged in account.

22. Click **Next**.

23. In addition to the standard properties that File Access Manager retrieves, you can retrieve additional properties for Active Directory groups.

24. Type additional properties to retrieve.

25. Click **Next**.

26. Verify that the system retrieved the requested information successfully.

> Only the first ten results display.

27. Click **Next**.

The Identity Collector: Groups Collection (3 of 4) window displays:
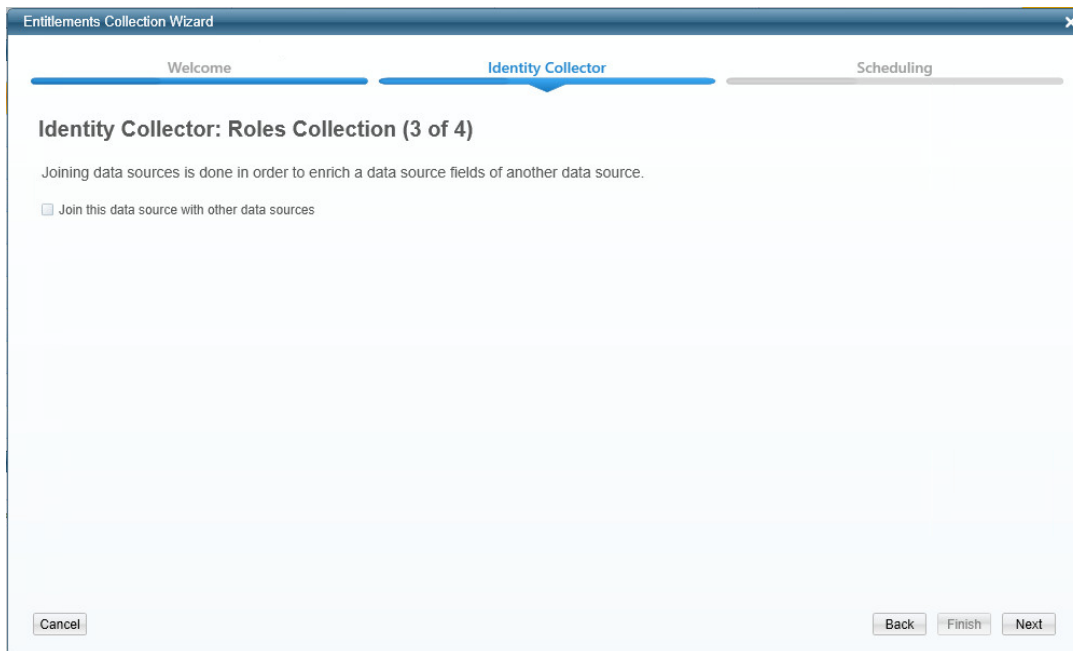


28. File Access Manager creates data sources that contain user fields so that the Identity Collector can collect the Users.

29. Check the **Join this data source with other data sources** check box to join this data source to other data sources.

30. You can use one of the Identity Collector fields as the local key to gather additional user fields from other data sources by joining those data sources. Chapter has additional information on joining data sources.

31. Type the Data Source, the Local Key, and the Remote Key.

> After you type the relevant data, select Test Data Sources to verify that the system has accepted the data.

32. Click **Next**.

33. Enter the Dynamic Fields Mapping data from the *Dictionary Field* and *Mapped Field* dropdown lists.

> Use the **X** / **+** buttons to remove / add fields, as required.

34.  Click **Next**.

The Identity Collector Scheduling window displays.

**Identity Collector Configuration scheduling panel**

.
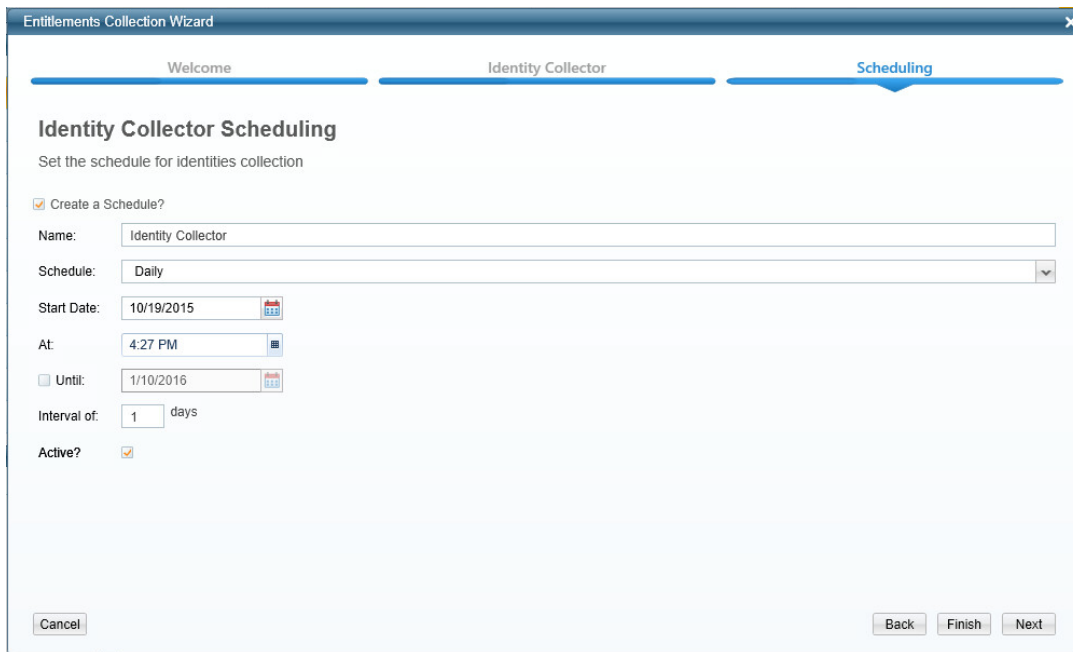


1.  Enter the relevant scheduling values.

2.  Click **Finish** to end the wizard or click **Next** to run an identity collection now.

> If you are running the task now, you can view the task progress in the relevant service view in Health Center or in the File Access Manager website,
> **Settings > Task Management > Tasks screen.**

> If you are running the task as part of the initial configuration, you will not have access to the File Access Manager web application until the task has completed. In this case, you can view the status of the identity collection task in the Health Center by navigating to **Health Center > Permission Collection > File Access Manager Collector Synchronizer > Tasks**.

## *Displaying an Active Directory Thumbnail Photo*

This section explains how to import the Active Directory thumbnail photo to display it for each user on the Website.

Before you import thumbnail photos, set all photo properties for the users in the organization's main Active Directory. (Otherwise, File Access Manager will not be able to update the photo automatically for those users.)

To display an Active Directory thumbnail photo on the web application, perform the following steps:

1. Create an Identity Collector that contains the users and roles for the organization's main Active Directory.

2. Set the Identity Collector that you just created as the Authentication Store.

3. Using the Health Center, locate the File Access Manager server, in which the Collector Synchronizer service is installed.

4. Once you have located that server, browse to the location of the collector service (normally located in - %SAILPOINT_HOME%\%SAILPOINT_APP_NAME%\CollectorSynchronizer).

5. Edit the CollectorSynchronizerServiceHost.exe.config file as follows:

    a. Find the following line:

       `<!-- <add key="getADUserThumbnail" value="false"/> -->`

    b. Replace the above line with the following line:

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

6. Restart the Collector Synchronizer.

7. Run the Identity Collector Synchronization task for the identity collector.

8. When the Identity Collector Synchronization task has ended successfully, log into the File Access Manager website with a user who has a thumbnail photo in Active Directory.

9. Verify that thumbnail photo appears in the user's profile.

### *Creating or Editing an Azure Identity Collector*

**Azure AD Connector Full OAuth 2.0 Support**

File Access Manager now offers full support of standard OAuth 2.0 Authentication for the Azure AD connector.

The new authorization sequence will direct the user through a standard Microsoft O365 consent flow, to grant the File Access Manager Azure AD Connector app the privilege to acquire and refresh access tokens.

The new authentication method replaces the previous Basic Authentication flow, that required admins to provide user and password credentials.

This enhancement brings full OAuth support to the Azure AD Identity Collector, instead of the legacy user and password approach.

This means the configuration will resemble other connectors for cloud applications such as OneDrive.

- Configuring the Identity Collector, instead of providing a username and a password, you will click on a link that sends you to a Microsoft login page.

- Enter the relevant user credentials and give your consent for the File Access Manager Azure AD O365 Application to access your directory data.

- You will then copy the resulting Authorization Code to the appropriate field, which will then be used to generate the first access token.

- The access token will be used in all requests to the tenant's Azure AD and will be automatically refreshed when needed.

**Configuration**

Complete the following steps:

1. In the Identity Collector Configuration Wizard enter your O365 Domain name, then click on the "OAuth User URL" link to generate an Authorization Code.
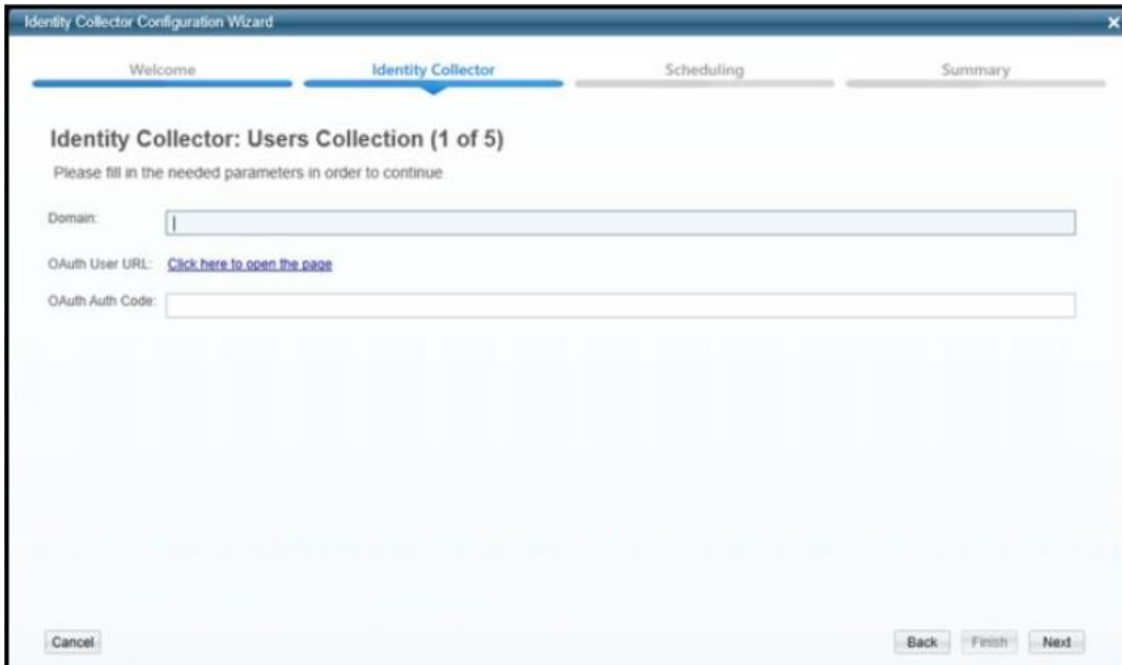


2. You will then be redirected to the Microsoft O365 Login Screen Login with the user that should be used by the Identity Collector.
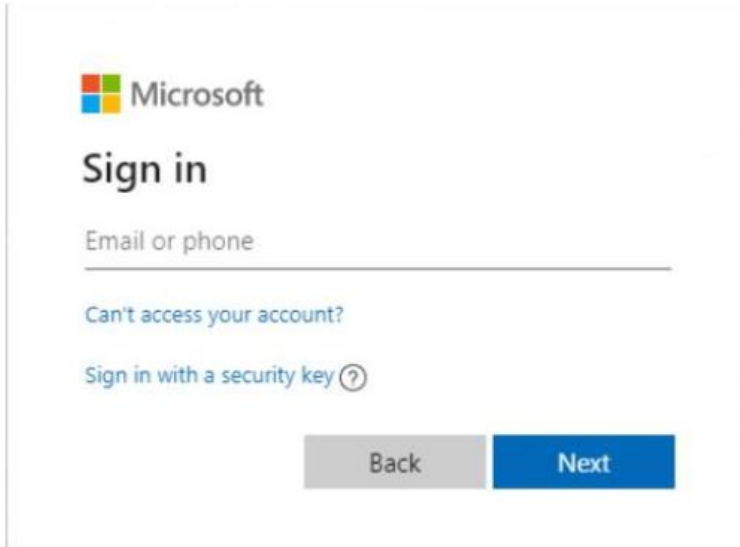


3. You will then be prompted to consent to granting access to the File Access Manager Azure Connector Accept to receive an Authorization Code and continue with generating the Access Token.
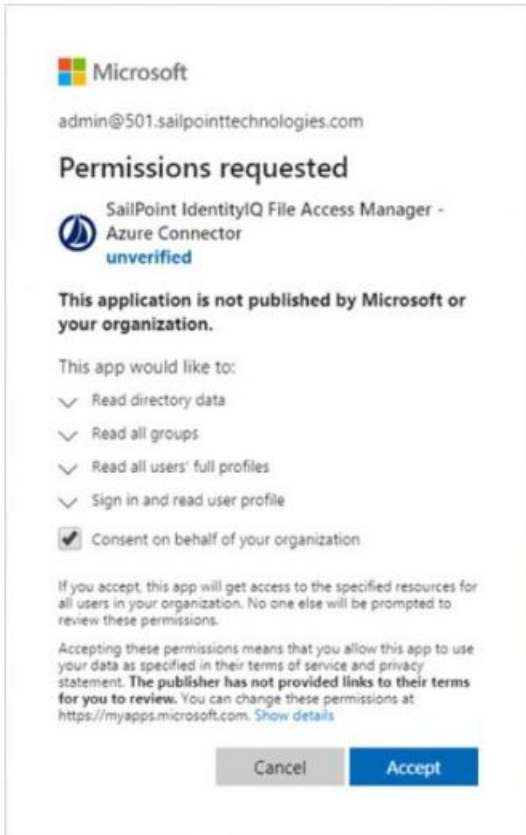
4. A final redirect will lead you to the File Access Manager Cloud Application Authorization Service, and will present the received Authorization Code.
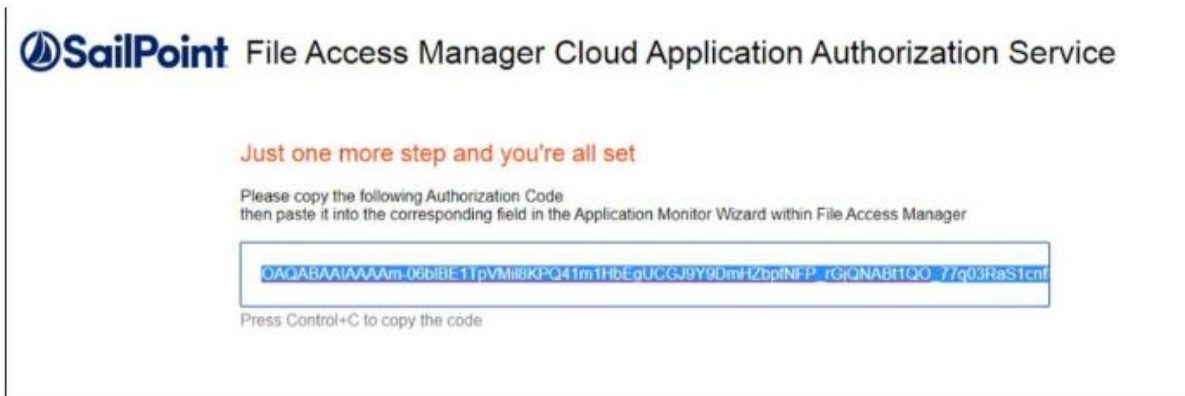


5. Copy that code and past it in the Auth Code field in the Identity Collector Configuration Wizard screen.

6. Click **Next** and complete the Identity Collector configuration flow.

## Permissions

The File Access Manager Azure AD Connector requires the following permissions:

- Directory.Read.All –This Permission grants read only access to AAD contents (by default, all domain users can read all AAD data).

## Azure Active Directory Connectivity Requirements

File Access Manager uses the AzureAD graph API – which works exclusively in HTTPS.

The API base path is : `https://graph.windows.net/{tenant_domain_name}` where the tenant domain name is the customer assigned domain name on Microsoft cloud. It is usually in the format of domain_name.on-microsoft.com, but might be changed in your configuration.

***A list of resources that are accessed by File Access Manager using the REST graph API include:***

> https://graph.windows.net/{tenant_domain_name}/tenantDetails
>
> https://graph.windows.net/{tenant_domain_name}/users
>
> https://graph.windows.net/{tenant_domain_name}/users/{user_id}
>
> https://graph.windows.net/{tenant_domain_name}/groups/{group_id}
>
> https://graph.windows.net/{tenant_domain_name}/directoryRoles
>
> https://graph.windows.net/{tenant_domain_name}/directoryRoles/{role_id}

## Administrator's Consent Requirements

To grant a third-party application (ISV) with the Directory.Read.All permission requires an administrator consent, which can be given by users with one of the following roles:

- Global Administrator (Company Administrator)
- Cloud Application Administrator
- Application Administrator

Hence, during the initial configuration phase (while generating the token for the first time), the service account dedicated to the File Access Manager Azure AD Connector must have one of the above-mentioned roles. Once consent is given, the role can be removed from the user.

The Consent flow will appear different for users with different roles.

Non-admin user trying to access the consent screen will be presented with the following screen:
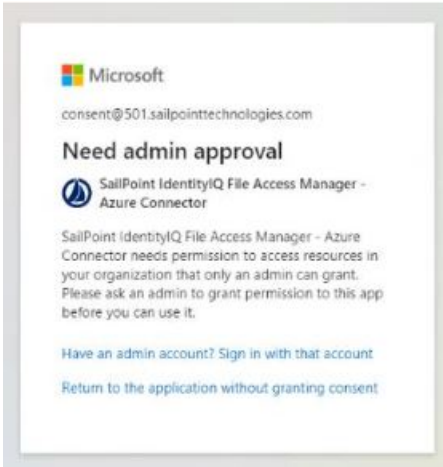
Application Administrators trying to access the consent screen, will be presented with a request to consent and grant the File Access Manager Application the Read Directory Data permissions:
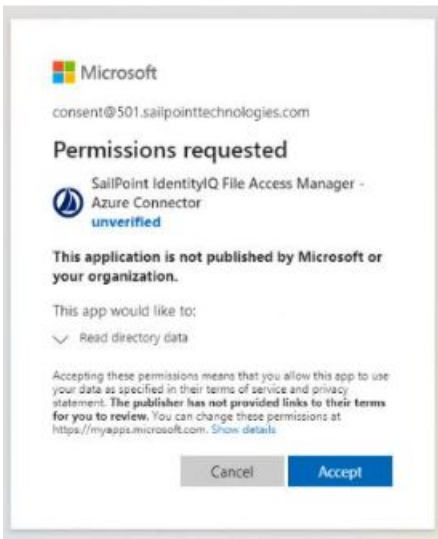


Users with the Global Administrator role trying to give consent to an application will be presented with a screen containing an additional checkbox (Consent on behalf of your organization):
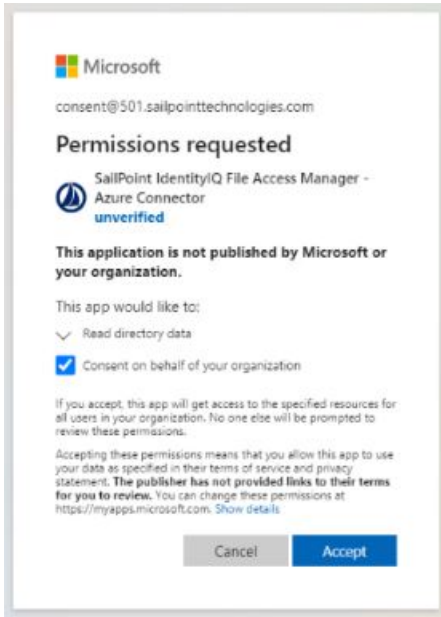
This extra checkbox consents to give permissions to the applicationon behalf of all other users in the organization, thereby ensuring no other user would have to explicitly give consent to the app to run on its behalf.File Access Manager does not require this checkbox to be checked, as our applicationonly needs to run on behalf of the consenting user.

Checking this option is optional, and not mandatory.

### Avoiding the Administrative Roles Grant

To avoid granting an administrative role the service account, even if only for the duration of the consent sequence, you may use Azure's "AdminConsentRequests".

This relatively new feature lets non-admin users indirectly give consent to applications that require admin consent by requesting an admin's authorization.

This feature can be enabled on the tenant's level, and allows setting one of the three above-mentioned administrator roles as are viewer:

Activities
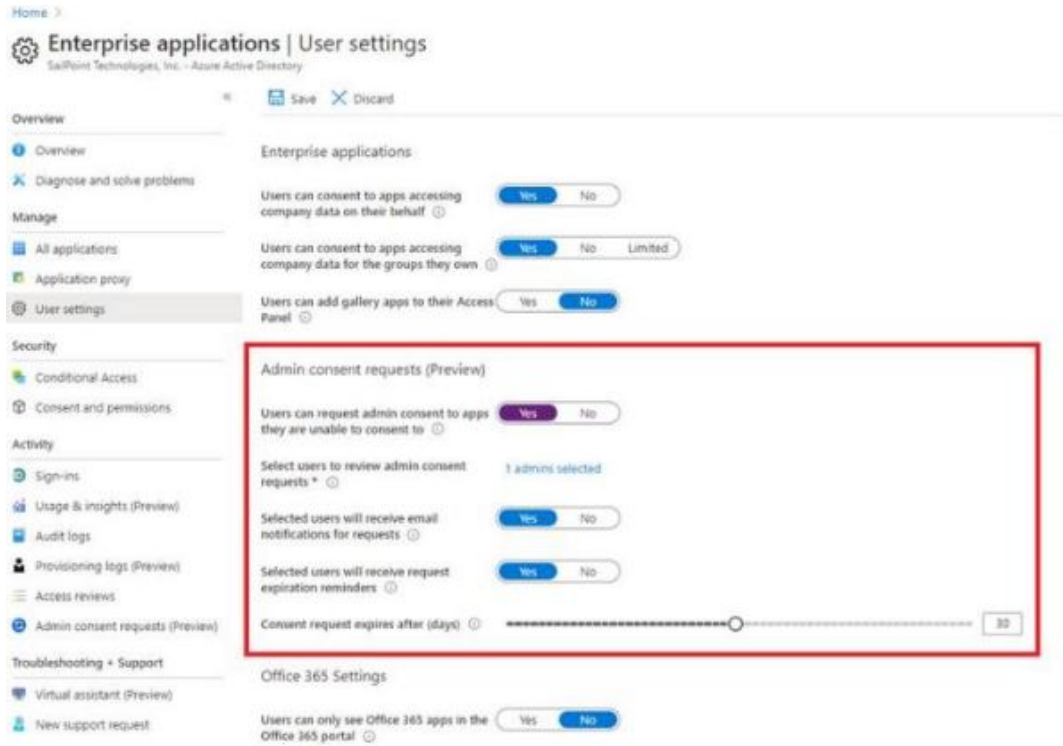


When users without one of these administrative roles go through the normal consent flow, they will be presented with the screen:
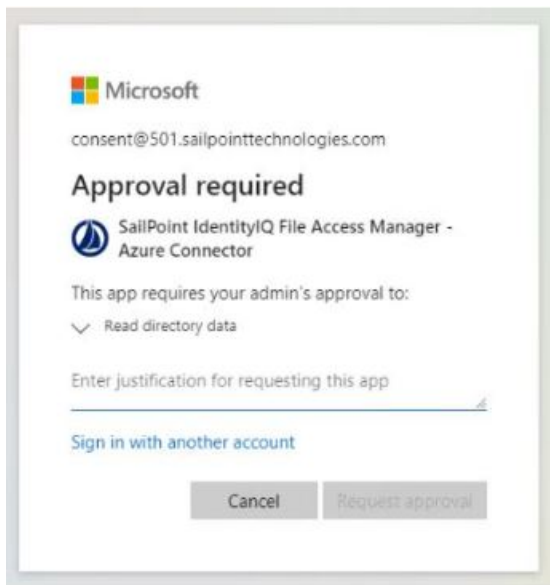


The requested is required to provide a justification for granting consent to the application and a request is sent to the administrator listed in the configuration as reviewers.

When clicking on "Request approval" to continue ,the following screen appears:
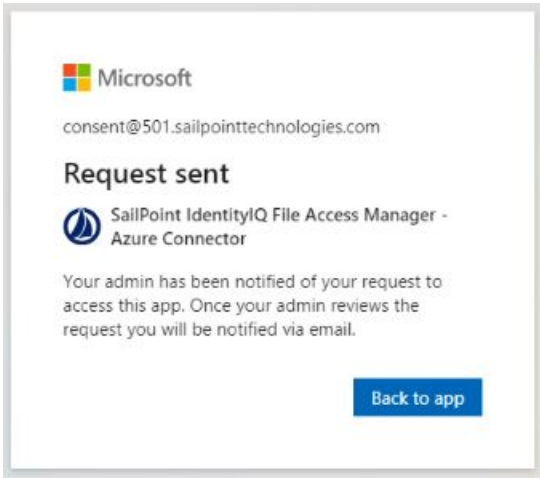
Clicking on "Back to app" would just return an "access denied" error as access was not yet granted. This screen can be safely closed while waiting for admin consent.

The reviewing administrator will either receive an email notifying them of the request, or have to go to the "Admin Consent Requests" screen and check for new requests:
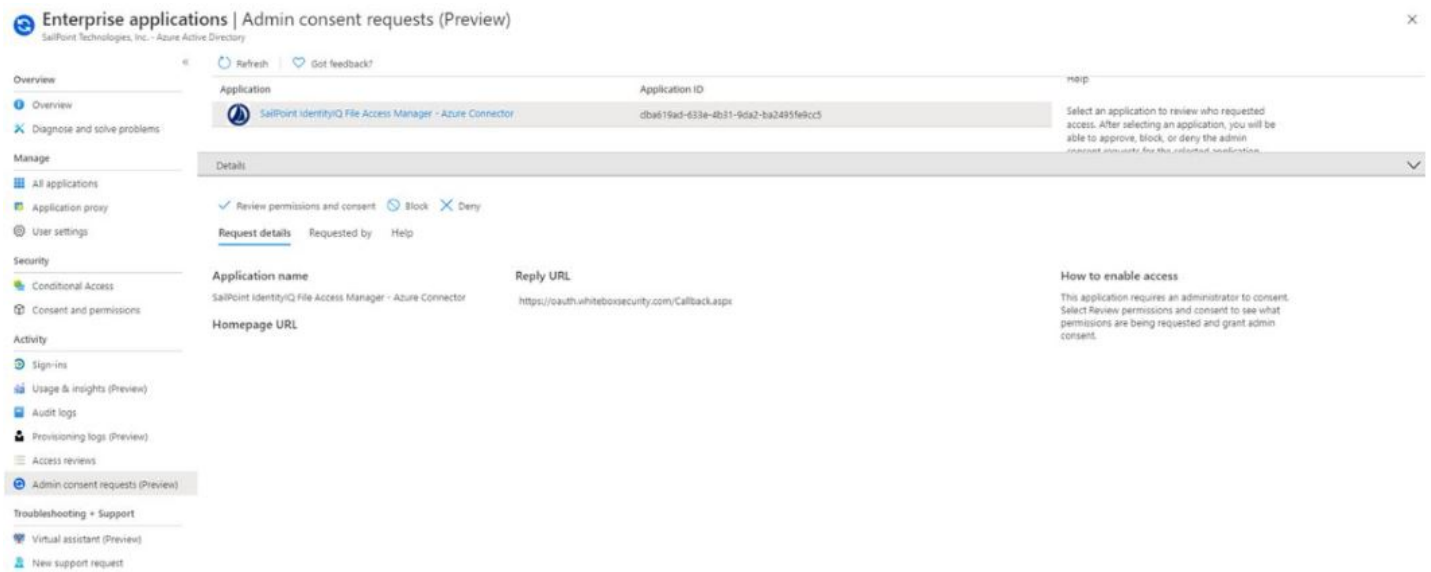


To approve a request, the administrator will go through the "Review permissions and consent" flow, where they will be presented with the familiar consent screen:
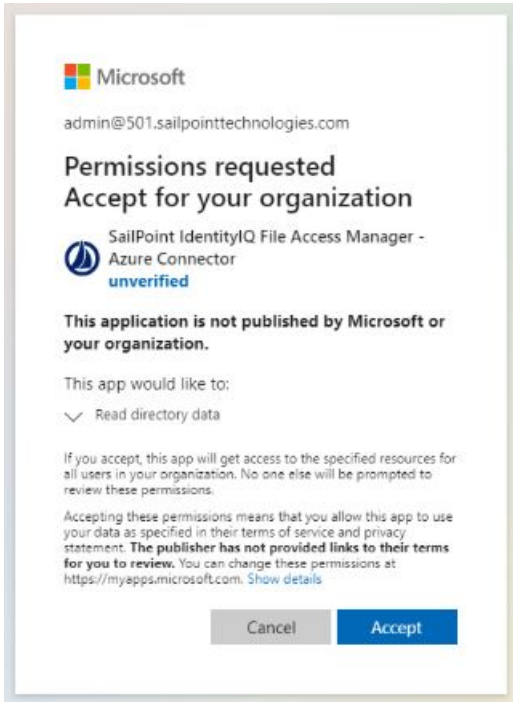
After an administrator "Accepts", non-administrator users will have to go the through token generation sequence again.

However ,this time the consent screen will be skipped entirely, and the flow will lead directly to the Authorization code.

> This method gives consent to the app on behalf of the entire organization, similar to when a Global Administrator ticks the checkbox to enables the Consent on behalf of your organization, as described above.

### Creating or Editing an NIS Identity Collector

To create an NIS Identity Collector, follow steps 1-7 of Creating or Editing an Active Directory Identity Collector .

The NIS Identity Collector Users Collection (1 of 5) window displays.

### Creating or Editing a Data Source Identity Collector

Section Configuring the Permissions Collector, describes the initial steps involved in the creation of a Data Source Identity Collector, up to the stage that the Data Source Identity Collector Users Collection (1 of 5) window displays.

### Editing an Identity Collector

> You can edit an identity collector in one of two ways:

- By selecting **Edit** in the Identity Collector screen.

-Or-

- By checking **Edit the selected identity collector** in the Permissions Collector Wizard.

1. Click **Use Existing Collector.**

2. Follow the Steps 8-29 in section Creating or Editing an Active Directory Identity Collector (Until the scheduling screen).

3. Click **Finish** to end the wizard without creating a permissions Collector schedule.

4. Click **Next** to continue the Permissions Collection process, and to create a permissions Collector schedule.

   The Permissions Collector Scheduling window displays.
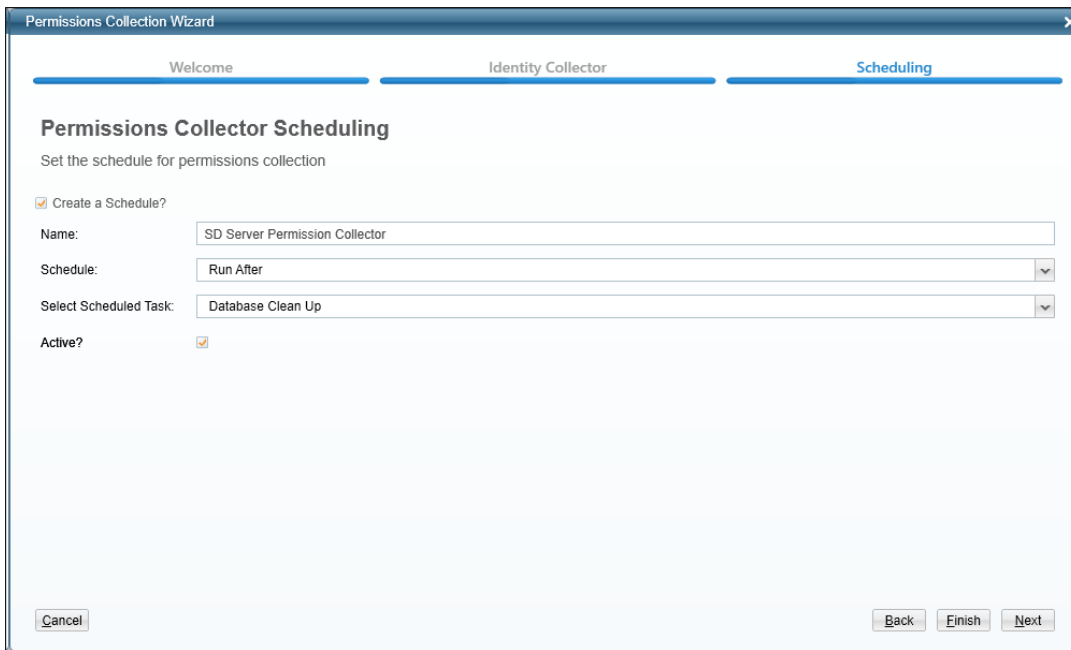


5. Enter the Scheduling values for:

   - *Create a Schedule?* (Check/Uncheck)

   - *Name*

   - *Schedule*

   - *Select Scheduled Task*

   - *Active*? (Check/Uncheck)

6. Click **Finish** to end the identity collection process.

7. Click **Next** to continue the identity collection process.

   The Permissions Collector Summary window displays.

8. Check **Run Identities and Permissions Collection Now**.

9. Click **Finish**.

   An Information window displays to indicate that a Task is successfully created.

10. Click **OK** to end the wizard.

11. To view the task progress open the web client and navigate to **Settings > Task Management > Tasks**.

## Proprietary Application Permissions Collection (Homegrown Apps)

Proprietary applications can be commercial off-the-shelf applications or applications that an organization has developed in-house.

The Collector Synchronizer Service is the software component responsible for analyzing the permissions of a homegrown application.

To model, analyze, and collect the permissions for a homegrown application, File Access Manager must have information on the following data types.

> This information may include from where to bring this data type, its unique identifier, and other data type fields to query later:

- User – The list of all the Application's Users

- Group – The list of all the Application's Groups, and their parent-child nesting (if any)

- User-Group Relationships – Which Group contain which Users (or which users are members in which group)

- Permission Types – All the possible permission types for the application (for example, Read, Write, Full Control)

- Business Resources – The list of all the Business Resources of the application, and the hierarchy parent-child relationships (if any) of the business resources

- Group-Permission Type-Business Resource Relationships – If the application allows granting permissions through Groups, File Access Manager must know which group provides which permission type on which business resource (for example, the Technical Write Group grants Full Control Permission on the Documents folder).

- User-Permission Type-Business Resource Relationships – If the application allows granting direct user permissions to business resources, File Access Manager needs to know which users are assigned which permission type on which business resource (for example, John has direct Full Control permission on the Documents folder).

The first step in defining a Permissions Collection for a homegrown application involves determining from where to bring the above information. First, define one or more Data Sources for each data type (using a simplified, single data source for all the data types above, as shown in the example below). The data source tables will be used to map various entities when the Permissions Collection process is defined later.

For example, it is possible to easily map a homegrown application that uses LDAP as the identity store and a RDBS database for the rest of the information by:

- Defining one or more data sources to bring the information on the Users, Groups, and User-Group relationships, and

- Defining another data source to collect the information on the business resources, permission types, and the user/group-permission type-business resource relationships

The table below lists sample permissions data in a single Data Source table.

| User Name | Group Name | Permissions Type | Business Resource |
|---|---|---|---|
| Jonathan | Technical Writer | Full Control | Docs\Guides |
| John | Technical Writer | Full Control | Docs\Guides |
| Matt | Engineer | Full Control | R&D |
| Avi | QA | Read | R&D |

The table below lists the distinct columns for each type of Data Source mapping. As the table shows, there are four distinct users, three distinct groups, two distinct Permission types, and two distinct business resources.

| User | Group | Permission Type | Business Resource |
|---|---|---|---|
| Jonathan | Technical Writer | Full Control | Docs\Guides |
| John | Engineer | Read | Docs\Guides |
| Matt | QA | | R&D |
| Avi | | | |

The example above shows a homegrown application that does not have direct user permissions, or nested groups, but does have its hierarchical business resources delimited by the '\' char. The following example examines the relationships between data types.

| Group | Members |
|---|---|
| Technical Writer | Jonathan, John |
| Engineer | Matt |
| QA | Avi |

| Group | Permission Type | Business Resource |
|---|---|---|
| Technical Writer | Full Control | Docs\Guides |
| Technical Writer | Full Control | Docs\Guides |
| Engineer | Read | R&D |
| QA | Read | R&D |

## *Creating a Homegrown Application*

***To create a homegrown application (as part of the configuration of a permission collector):***

1. In the administrative client, navigate to **Application > New > Application**.

   The New Application Wizard displays.

2. Click **Proprietary – Use this to add a Homegrown application**.

3. Type the application type in the **Application Type** field.

> If there are no application types, select the Create New Application Type link.

4. Enter the following information:

   ***Name***

   Name of the Application Type

   ***Description***

   Text description of the Application Type

   ***Active Directory Authentication Yes/No***

   Whether or not to perform AD authentication and use an AD Identity Collector

   The same application types will have the same permission types, and you will be defining permission types collector for each application type

5. Click **Save**.

6. Click **Next**.

   The General Details window displays.Enter the following information:

   ***Name***

   Name of the Application Type

   ***Description***

   Text description of the Application Type

   ***Container***

   Name of the selected Container

   If there is no suitable container, click to create a new one.

   ***Identity Collector***

   Name of the identity collector to link to

   If there is no suitable identity collector, click to create a new one.

7. Click **Next**.

   The Permissions Collector Scheduling window displays.

8. To end the New Application Wizard without creating a schedule, click **Finish**.

9. To create a schedule, check the **Create a Schedule** check box, and enter the scheduling details:

10. Click **Finish**.

A successful completion notice displays.

11. Click **Open Permissions Collection Wizard** to configure Permissions Collection parameters.

12. Click **Close** to close the Wizard without configuring permissions collection parameters.

## *Configuring the Permissions Collector*

1. To open the Permissions Collector Configuration wizard:

   a. Click **Open Permissions Collection Wizard** at the end of the Homegrown Application definition, or by

   b. Select a homegrown application to the context by double-clicking on it, and then clicking on **Permissions Collection**.

### Welcome tab

The Permissions Collection Wizard displays.

1. Click **Next** to open the Identities Collection window.

   #### *Use Existing Collector*

   Select a collector from the dropdown list

   #### *Edit the Selected Identity Collector*

   To edit an existing collector

   #### *Create a New Collector*

   To create a new collector

2. If you want to create a new collector, click **This application uses Groups** check box in the Groups Configuration section if applicable. Unchecking this box precludes the need to map the Group data or Group Permission types of Business Resource relations and you can skip those steps in the wizard.

If you chose to create a new collector, the page **Identity Collector: Users Collection (1 of 3)** displays.

   Under Main Data Source, the Data Source displays automatically.

3. Under Mandatory Fields, select a User Name from the dropdown menu.

4. Under Optional Fixed Fields, check the check box next to each relevant optional fixed field, and select the field from the corresponding dropdown menu.

5. Click **Next** to open the User Collection (2 of 3) screen .

6. Under Fields Mapping, select a field from the **Dictionary Field** dropdown menu (or if none exists, select **Create a new Field** next to Fields Mapping).

7. Select a field from the **Mapped Field** dropdown menu.

8. Click **Next**.

The Identity Collector: Users Collection (3 of 3) displays.

9. If relevant, under Users Tree, check the **Should the users tree be grouped** box. This will affect how the users will look in the Users Tree under the Advanced Forensics Control.

10. If you checked that box, select a field grouping from the **Field** dropdown menu.

11. If relevant, under Unique User Accounts Mapping, check the **Use a field to map between accounts of the same user** box.

12. If you checked that box, select the field from the **Field** dropdown menu.

13. Click **Next**.

The Identity Collector: Groups Collection (1 of 2) window displays.

Under Main Data Source, the Data Source displays automatically.

14. Under Mandatory Fields, select a Group Name from the dropdown menu.

15. Under Optional Fixed Fields, check the check box next to each relevant optional fixed field, and select the field from the corresponding dropdown menu.

16. Click **Next**.

The Identity Collector: Groups Collection (2 of 2) displays.

17. Under Fields Mapping, select a field from the **Dictionary Field** dropdown menu (or if none exists, click **Create a new Field** next to **Fields Mapping**.

18. Select a field from the **Mapped Field** dropdown menu.

19. Click **Next**.

The Groups Hierarchy Support window displays.

20. Select This Identity Collector uses Groups Hierarchy if relevant.

21. Under Main Data Source, the Data Source displays automatically.

22. Under Mandatory Fields, select a Child Group Name and a Parent Group Name from their respective dropdown menus.

23. Under Mandatory Fields, select a Parent Group Name from the dropdown menu.

24. Under Optional Fixed Fields, check the check box next to each relevant optional fixed field, and select the field from the corresponding dropdown menu.

25. Click **Next**.

The Identity Collector: Users Membership in Groups (1 of 1) window displays.

26. Under Main Data Source, the Data Source displays automatically.

27. Under Mandatory Fields, select a Group Domain Name, Group Name, and Username from the respective dropdown menus.

28. Under Mandatory Fields, select a Parent Group Name from the dropdown menu.

29. Under Optional Fixed Fields, check the **User Domain Name** check box if relevant, and select the field from the

corresponding dropdown menu.

30. Click **Next**.

The Business Resources Collection (General) window displays.

31. Click **This application uses Business Resources** if applicable.

> If you do not check this check box, File Access Manager creates a Business Resource (in the background) and associates it with all permissions.

32. Type the name in the **Name** field.

33. Click **Next** to open the Business Resources collection .

## Permission Collection Resources Tab

The Business Resources Collection (1 of 2) window displays. Select the data source that contains Business Resource Data type information from the **Data Source** dropdown menu or click **Create a new Data Source** to create a new data source.

1. If you click **Create a new Data Source**, the **Data Source Wizard** displays.

2. Select a resource unique identifier from the **Resource Unique Identifier**dropdown menu under Mandatory Fields.

3. This field must identify the Business Resource uniquely (for example C:\Docs\Finance), and should match Business Resource Unique Identifier selected in the User/Group-Permission Type-Business Resource relationships defined in the following steps.

4. Check the **Resource Name** check box under Optional Fixed Fields, if applicable, and select the column that represents the source name.

5. Click **Next**.

The Business Resources Collection (2 of 2) window displays.

6. This section allows dynamic field mapping for the Business Resource data type. The relevant fields will be available later for query and display in the Permission Forensics page. You can use it in Access Certification Campaigns and Access Requests to display meaningful information for permission reviewers.

7. Select a dictionary field from the **Dictionary Field** dropdown men.

8. Select a mapped field from the **Mapped Field** dropdown menu.

9. Click **Next**.

The Business Resources Hierarchy Support window displays.

10. Check the This Business Resources Collector uses Resources Hierarchy check box to support parent-child hierarchy.

11. Type in a unique identifier for the hierarchical string in the String to be used as a delimiter to break the string into resources field.

12. An example of a group hierarchy follows:

If the nested groups are:
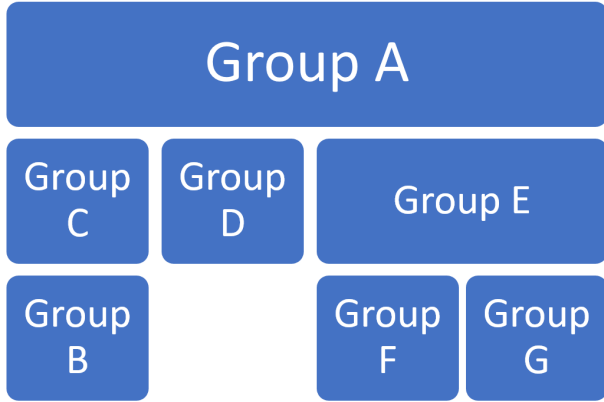
The Data Source table of parent-child group associations would be:

| Parent Group | Child Group |
|---|---|
| Group A | Group C |
| Group A | Group D |
| Group A | Group E |
| Group C | Group B |
| Group E | Group F |
| Group E | Group G |

13.   Click **Next** to open the Permission Types Collection tab.

## Permission Types Collection Tab

The Permission Types Collection window displays.
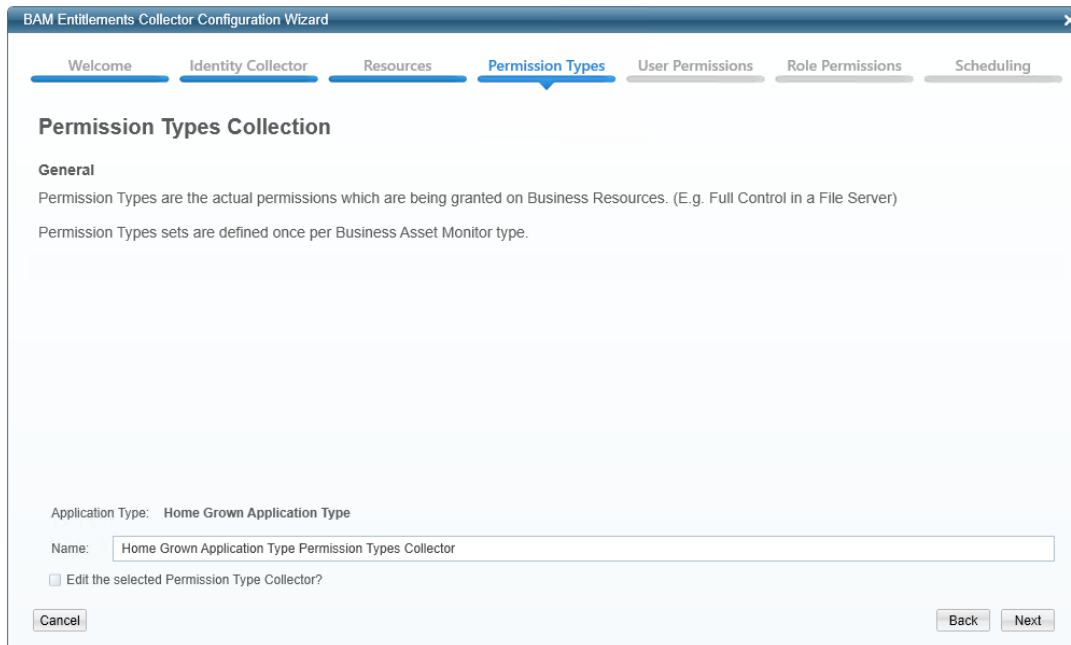
The Permission Type collector is associated with the Application type, so all homegrown applications of the same type will share the same permission type collector, and the same permission types

1. Check the **Edit the selected Permission Type Collector** check box to edit the permission type collector.

The Permissions Types Collection (1 of 2) window displays.

2. Select the data source with information on the Permission Type data type from the **Data Source** dropdown menu, or click **Create a new Data Source**.

3. Select a Mandatory Field from the **Permission Type Name** dropdown menu.

4. This field must identify the Permission Type uniquely (for example, Read), and should match the Permission Type Name selected in the User/Group-Permission Type-Business Resource relationships defined in the following steps.

5. Check optional fixed fields, if applicable, from the **Optional Fixed Fields** check boxes.

6. Click **Next**.

The Permission Types Collection (2 of 2) window displays.

This section allows dynamic field mapping for the Permission Type data type. The relevant fields will be available later for query and display in the Permissions Forensics screen, and you can use them in Access Certification Campaigns and Access Requests to display meaningful information for permission reviewers.

7. Click "Create a new Field" under **Fields Mapping** if applicable.

The Manage Permission Types Data Dictionary window displays.

8. Type a name in the **Name** field.

9. Select a WH Question from the **WH Question** dropdown menu.

10. A WH Question will determine under which question this field display in the Advanced Forensics Control under the *Permissions > Identity and Permissions Forensics* window, when you create a new query.

11. Click **Save** to save the new field or click **Cancel** to return to the previous window.

12. The *Permission Types Collection (2 of 2)* window displays again.

13. Select a dictionary field from the **Dictionary Field** dropdown men.

14. Select a mapped field from the **Mapped Field** dropdown menu.

15. Click **Next** to open the Users' Direct Permissions Collection tab.

**Users' Direct Permissions Collection Tab**
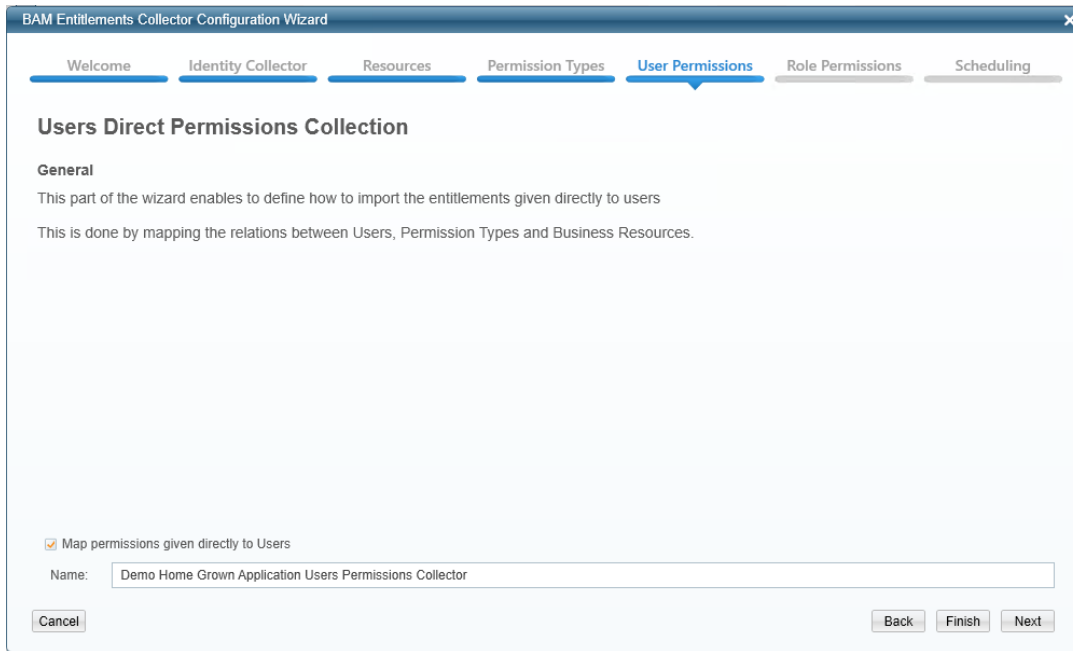
Activities

In this portion of the Permissions Collector Configuration Wizard, you determine how to import permissions given directly to users. This is done by mapping the relations between sers, permission types, and business resources.

> The Name field contains the name you provided.

1. Click the **Map permissions given directly to Users** check box to map those permissions.

2. Click **Finish** if you do not need to map the permissions, or click **Next** to continue with the Users' Direct Permissions Collection portion of the wizard.

   If you click **Next**, the Users Direct Permissions Collection (1 of 1) window displays.

**Administrator Guide** 115
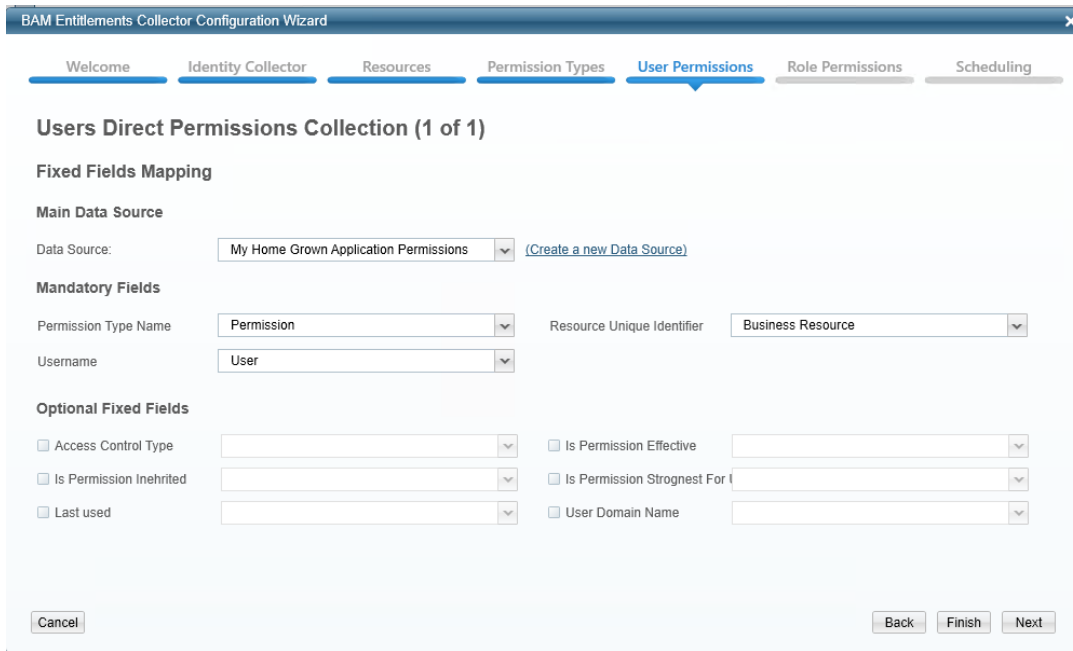
3. Select the Main Data Source from the **Data Source** dropdown menu that contains the information on the User-Permission Type-Business Resource relationships or click **Create a new Data Source**.

4. Select the mandatory fields from the following dropdown menus:

   - *Permission Type Name* – This field value must match the permission type name selected in the Permission Type collector.

   - *Username* – This field value must match the user name selected in the Users Collector defined in the identity collector.

   - *Resource Unique Identifier* – This field value must match the business resource unique identifier selected in the Business Resources collector.

5. Check optional fixed fields, if applicable, from the **Optional Fixed Fields** check boxes.

6. Click **Next** to open the Groups' Direct Permissions Collection tab.

   Groups Direct Permissions' Collection Tab
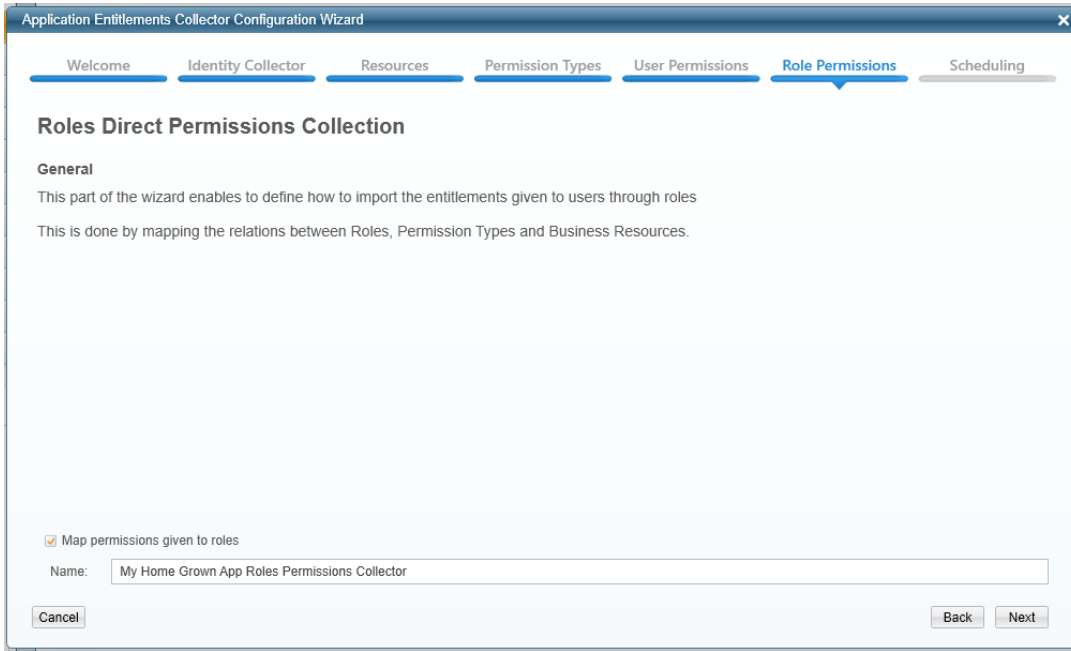
In this portion of the Permissions Collector Configuration Wizard, you determine how to import permissions given to users through rules by mapping the relations between Groups, Permission Types, and Business Resources.

1. Check the **Map permissions given to groups** check box if applicable.

   The Name field contains the name you provided.

2. Click **Finish** if you do not need to map the permissions, or click **Next** to continue with the Groups Direct Permissions Collection portion of the wizard.

If you click **Next**, the Groups Direct Permissions Collection (1 of 1) window displays.
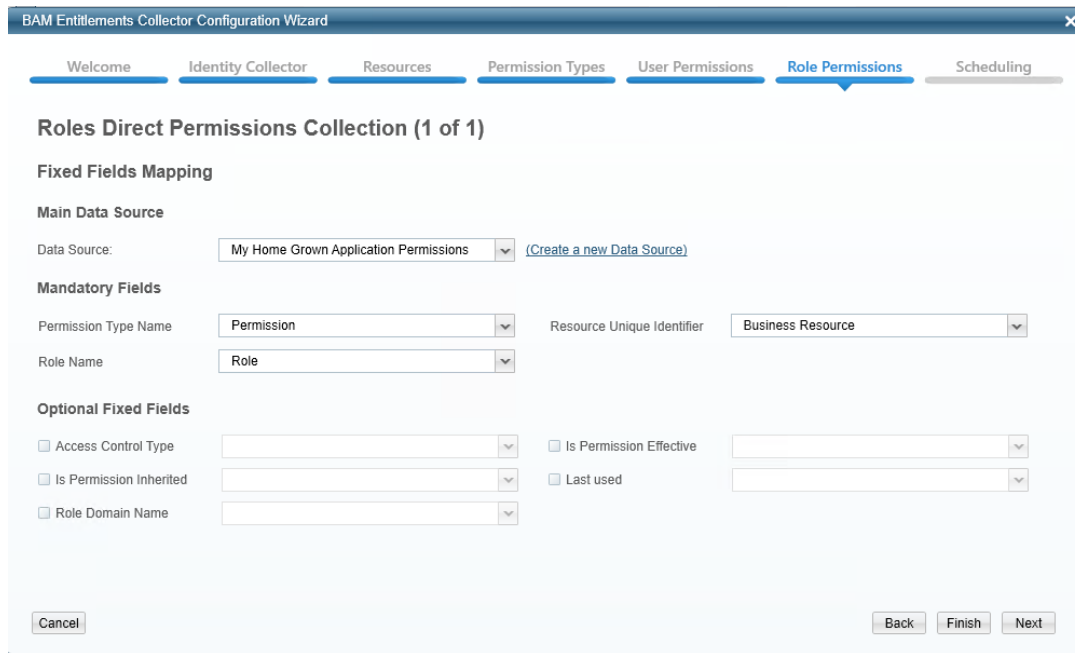


3. Select the Main Data Source from the **Data Source** dropdown menu that contains on the Group-Permission Type-Business Resource relationships or click **Create a new Data Source**.

4. Select the mandatory fields from the following dropdown menus:

   - Permission Type Name – This field value must match the permission type name selected in the Permission Type collector.

   - Group Name – This field value must match the group name selected in the Groups Collector defined in the identity collector.

   - Resource Unique Identifier – This field value must match the business resource unique identifier selected in the Business Resources collector.

5. Check **Optional Fixed Fields**, if applicable, from the **Optional Fixed Fields** check boxes.

6. Click **Next** to open the Permission Collector scheduling tab.

### Permissions Collector Scheduling Tab

1. Click **Finish** if you do not want to create a schedule.

2. Check the **Create a Schedule** check box to create a schedule for identities, groups, and permissions collection.

3. Click **Next** to open the summary tab.

### Permissions Collection Summary Tab
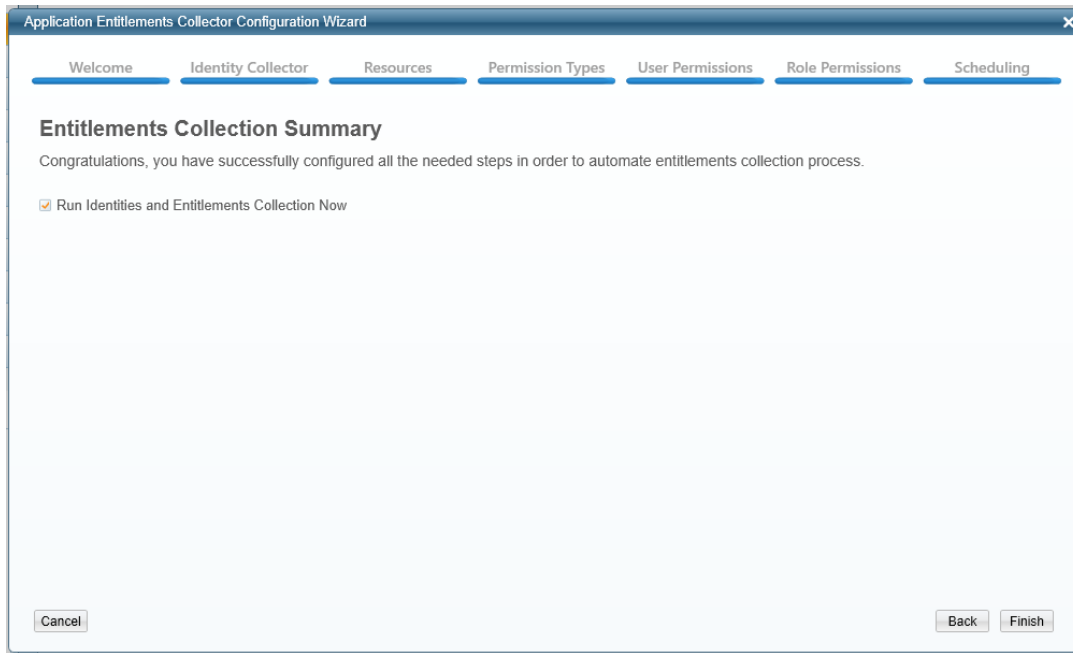
1. Click the Run Identities and Permissions Collection Now check box to run the collection.

2. Click **Finish**.

   The Permissions Collector Summary window displays.

3. Check the "Run Identities and Permissions Collection Now" and click **Finish**.

   An Information window displays to indicate that the system created a Task successfully.

4. To view the task progress, go to **Settings > Task Management > Tasks**.

5. Click **OK** to end the wizard.

> It is possible to reuse the Identity collectors for user, group, and the user-group relationships and the Permission Types collector. However, it is only possible to use the Business Resources collectors and the two Business Resource Relationships collectors once, since they are associated with specific applications. One or more Data Sources collect all the above data types, but there must be a separate mapping from the Data Source to each of the data types.

### *Viewing Permissions Collection Results*

The permission results can be seen in the Permission Forensics screen. See Permission Forensics

You can view the results of the permissions collection that you defined from the Permission tab.

### Permission Capabilities Overview

This section describes the Permission capabilities available, including:

- What-If Scenarios

- Access Certification

- Access Requests

## *What-If Scenarios*

"What-If" is a component that simulates the addition or removal of users to and from groups.

The output contains the resources and permissions for which the user loses or gains permissions.

## *Access Certification*

Access Certification is a component that manages permission review campaigns. These campaigns fine tune user permissions by enabling managers, data owners, or other relevant personnel to review user current permissions.

## *Access Requests*

File Access Manager can accept, process, and manage user requests and provide users with access to certain system resources.

The Access Request module manages and controls the access request process.

## *Fixing Faulty Permissions*

Faulty permissions may occur in CIFS-based applications, where:

- Permission set on a parent Business Resource is not inherited by sub-resources, although inheritance is configured.

- A Business Resource includes an inherited permission, which is missing on the parent Business Resource.

Contact the SailPoint support team for assistance in configuring File Access Manager to identify and fix faulty permissions.

## Fulfillment of Access Permission Changes

There are several scenarios where the system will be required to change a user's access permissions on a resource:

- A user making a direct access request (See New Access Request Wizard)

- A campaign, verifying that a user's existing permissions fit the required permissions

Depending on the company's policies, an administrator may want to review all revoked permissions before making such changes. In this case the system sends approved permission changes, resulting from the review, to the Access Fulfillment process. This process is handled differently for managed, and unmanaged BRs, as described below.

## *Access Fulfillment for Managed BRs*

The system handles access fulfillments on managed BRs automatically, once the requests go through the approval process.

## *Access Fulfillment for Unmanaged BRs*

For unmanaged BRs, the user can either create a custom script for access fulfillment, or create manual process. This manual process includes fulfillment and review. using a static, single-level access fulfillment process. Manual ful-

fillment must be defined To handle unmanaged BRs, either an access request path or an access certification path must first define manual fulfillment on unmanaged BRs.

***To run manual access fulfillment on an unmanaged business resource through the Access Request path:***

1. In the administrative client, navigate to **Access Requests > Configuration > Manage Access Request Templates**.

2. Complete the Access Request Template, described in Creating an Access Request Template .

***To run manual access fulfillment on an unmanaged business resource through an Access Certification path:***

1. In the Web Client, navigate to **Compliance > Access Certification > Campaign Templates**.

2. Complete the Access Certification Template, as discussed in Campaign Templates.

3. Select either None or Fulfill Permissions Revoke Requests from the dropdown menu in the Fulfillment field.

If you selected Fulfill Permissions Revoke Requests in the previous step, select a review process from the Manual Fulfillment Review Process field.

> The system assigns a one-step review process for manual fulfillment to Access requests for non-managed resources and identity collectors.

Access Fulfillment Advanced Forensics Control (AFC) Filter, has additional information on forensics control.

Different applications and permission mechanisms may interpret Owner permission differently. The table below describes the permission types that File Access Manager treats as an Owner permission. For each platform, the Owner permission is defined and named (queried by the listed name in the AFM query filter controls).

Owner Permission Types

| Permission Scheme | Description |
|---|---|
| Microsoft ACL | Microsoft Access Control Lists contain a special field that indicates the owner user / group) of the resource (for example, a file or a folder).<br><br>There can be only one entity defined as the Owner (but that Owner can be a group).<br><br>Since an Owner has full control of the ACL, the Owner effectively grants all permissions.<br><br>The Microsoft ACL Owner applies to:<br><br>• Windows File Server<br><br>• Active Directory<br><br>• Microsoft Exchange / Microsoft Exchange Online<br><br>• NetApp – CIFS<br><br>• EMC Celerra – CIFS |

| Permission Scheme | Description |
|---|---|
| | • EMC Isilon – CIFS |
| Unix | When a file(/folder) is created in Unix/Linux, its creator is automatically set as the Owner.<br>Permissions are categorized by:<br><br>• Owner<br><br>• Users in the Owner's group<br><br>• Other Users<br><br>There can only one owner user and one owner group per file/folder.<br><br>Since only the Owner (or root) can change file permissions, an Owner effectively grants all permissions.<br><br>The Unix file system Owner applies to:<br><br>• NFS (when using Unix permissions, but not NFSv4 ACLs)<br><br>• NetApp – NFS<br><br>• EMC Celerra – NFS |
| SharePoint | A SharePoint server features Site Collection containers, which function as separate entities, and permission scopes. Different Site Collections may have different users, groups, and permission types.<br><br>One or more users in a Site Collection may be defined as a Site Collection Administrator. The Administrator has full control of the resources in the Site Collection's inner structure.<br><br>The SharePoint Site Collection Administrator applies to:<br><br>• Microsoft SharePoint<br><br>• Microsoft SharePoint Online<br><br>• Microsoft OneDrive |
| Cloud Storage Providers | Typically, cloud storage providers include a permission type named "Owner" which grants full access rights to the resource (file, folder etc.).<br><br>The generic "Owner" permission is employed in:<br><br>• Box.com<br><br>• Dropbox<br><br>• Google Drive |

## Access Requests

With Access Requests, users can:

- Request permission to perform operations on an application (consisting of a business resource and a permission type)

- Join Identity Collector groups

Administrators use access requests (which are part of the access certification process) to revoke access to, or change permissions for, BRs.

When reviewers revoke a permission as part of an access certification campaign, an access request can be created to determine whether revoked permissions should be removed. Reviewers follow the same process as they do for an Access Certification.

File Access Manager can also fulfill access requests automatically.

At the end of the access request process, the system sends an email to the original requester to notify him or her of the final status of the request.

> Even if the request was created on behalf of a different user, the originator will receive the email notification.

See Chapter Review Process for additional information on the review process as it affects Access Requests.

### New Access Request Wizard

Users can initiate an access request using the New Access Request Wizard. This wizard is available using the **New Access Request** button, which is accessible from any screen in the web application. See the chapter *New Access Request Wizard* in the *User Guide*.

If required, this functionality can be disabled for all users, as part of the setup process.

### The Access Request Template

An administrator must create a review process for the application or identity collector to which a user requested access. This can be a multiple level process, with one or more reviewers at each level. Afterwards, the administrator creates an access request template to indicate which request process to use in granting permissions. For each review process, the administrator configures the capabilities and fields available to requesters and reviewers in the review process.

### Creating an Access Request Template

To create an Access Request template, perform the following steps:

1. In the administrative client, navigate to **Permissions > Access Requests > Configuration > Manage Access Requests Templates**.

2. Click **New**.

   The Access Request Template displays.

3. Type a unique name in the **Name** field.

4. Select a review process from the **Review Process** dropdown menu.

5. Select the applications/identity collectors in the available fields list to be moved to the Chosen list, using **>** or **>**.

> The available objects depend upon the selected review process. A static identity collector review process will display all applications/identity collectors, while a dynamic one will display the identity collector, itself, or will only display applications associated with the review process identity collector. A dynamic application review process will display only the selected application.
> This section includes the list of applications and identity collectors included in this template (updated according to the selected review process).

> Application and Identity Collectors can only be associated with one access request template.

> Applications and identity collectors that are already associated with an access request templates do not display in the list of available objects.

### *Maximum Duration*

is the maximum time for management of an access request, after which the system highlights the request to indicate an expired duration.

### *Fulfillment*

adds a fulfillment step for the permissions to the access request. Section *Access Fulfillment* has additional information on access fulfillment.

Select the fulfillment method:

### *None*

The access request will end after the last reviewer in the review process has reviewed all the request permissions, without a fulfillment step.

### *Fulfill Access Requests*

The review step will be followed by a fulfillment step, depending on the business resource type and manual fulfillment type selected:

- *Managed BRs*

    Fulfillment is handled automatically by  File Access Manager.

- *Unmanaged BRs*

    Selecting **File Access Requests** will open a drop down list to select the **Manual Fulfillment Review Process** – a one-step review process defining the user or group who will be responsible for the fulfillment process.

    > If selecting Fulfillment, **Bypass review process when a Data Owner issues a Revoke request** will display. If this option is selected, an additional review process will not be triggered if a data owner directly revokes access from a user on this resource.

### *Custom Script*

The review step will be followed by a fulfillment step, depending on the business resource type and manual fulfillment type selected:

- *Managed BRs*

  Fulfillment is handled automatically by File Access Manager.

- *Unmanaged BRs*

  Fulfillment is handled by a script prepared by the user. See Access Fulfillment for Unmanaged BRs for a full description of fulfillment using a user script.

  The system only displays single-level review processes.

6. Click **Next**.

   The *Review Data Fields* window displays.

   The Reviewer Data Fields display what the reviewer will see when reviewing permissions. All built-in fields display, and the relevant Identity Collector fields do not display if you selected an Identity Collector.

7. Select the fields in the Available Date Fields to be moved to the Review Data Fields list, using **>** or **>**.

8. Select a field, and use the up and down arrow keys above the Review Data Fields list to change the order of the Reviewer Data fields.

   The fields will display to the user in the order selected in the Reviewer Data Fields list.

9. Check the **Display the same fields in the File Access Manager client**check box to display the same fields in the administrative client as display in the Web interface.

   The administrator may want to provide the user of the Web interface with fewer fields if it is not necessary for the user to view all the fields.

10. Click **Finish** (only if you checked the check box). This will appear in the web client at **My Tasks > Access Request** on the web application.

11. If you do not check **Display the same fields in the File Access Manager client**, the *Administrators Data Fields* window displays, so the administrator can select a list of data fields that differ from the list of the Reviewer Data Fields.

12. Click **Finish**.

## *Managing Requestable Permission Types*

This feature allows an Administrator to determine which permission types will be available to users who request access to specific application types.

The list of available permission types for managed resources cannot be modified. If you add requestable permission types for a resource type, it will take affect only for non-managed resources i.e. only resources that take the manual fulfillment path.

***To manage requestable resources:***

1. In the administrative client, navigate to **Access Requests > Configuration > Manage Requestable Permission Types**.

   The Manage Requestable Permission Types window displays.

2. Select an application.

3. Click **Edit**.

   The Edit Requestable Permission Types window displays.

4. Select permission types from the Available (left) pane, and use the arrows to place them in the Chosen (right) pane.

   > You can also move the default Chosen permission types to the Available pane so that they are not displayed to users.

5. Click **Save**.

6. Expand the resource tree.

7. Select a resource.

8. Click **Add**.

   The selected resource is displayed in the right pane.

   > The right pane displays a Path column, which displays the full path of the selected resource, an Include Sub-Resources column with a checkbox to include (or not) the sub-resources of the selected resource, and an Action column with an option to remove the resource.

   > There is an option to add a label to easily identify the right resource to request.

9. Select a business resource from the Available (left) pane, and use the arrows to move them to the right pane, where you can decide whether to include their sub-resources or remove them.

10. Click **Save**.

    > If you select New to create a new requestable resource, any saved applications will no longer be available in the Application selection, but will be available for editing.

11. Click **Edit** to edit the resources within the displayed applications or **Delete** to delete the application's requestable business resources. When an application is deleted, all its business resources will be available for a user making an access request.

## *Managing Requestable Resources*

This feature allows an Administrator to determine which resources will be viewable by users who request access to resources.

***To manage requestable resources:***

1. In the administrative client, navigate to **Access Requests > Configuration > Manage Requestable Resources**.

   The Manage Requestable Resources window displays.

2. Click **New** or select an application, and click**Edit**.

   The Requestable Resources for Application window displays.

3. Select an application.

4. Expand the resource tree.

5. Select a resource.

6. Click **Add**.

7. The selected resource is displayed in the right pane.

   > The right pane displays a Path column, which displays the full path of the selected resource, an Include Sub-Resources column with a checkbox to include (or not) the sub-resources of the selected resource, and an Action column with an option to remove the resource.

   > There is an option to add a label to easily identify the right resource to request.

8. Select a business resource from the Available (left) pane, and use the arrows to move them to the right pane, where you can decide whether to include their sub-resources or remove them.

9. Click **Save**.

   > If you select New to create a new requestable resource, any saved applications will no longer be available in the Application selection, but will be available for editing.

10. Select **Edit** to edit the resources within the displayed applications or **Delete** to delete the application's requestable business resources. When an application is deleted, all its business resources will be available for a user making an access request.

## *Configuring Reminders*

### *To set reminders for access requests:*

1. In the administrative client, navigate to **Access Requests > Configuration > Configure Reminders**

The Access Requests Template Reminder displays.

> The Access Requests template reminder sends bulk emails to reviewers regarding all access requests pending their review.

2. Check the **Send Reminder Mail** check box.

   An empty email template displays.

3. Write free text in the email template and transfer information from the fields displayed in the Fields box to the right of the email template.

4. You can use the following fields either in the subject or in the body of the email, or in both locations:

   - Pending Requests – These pending requests are per reviewer.

   - Reviewer Display Name – This is the display name, and <u>not</u> the unique user name.

   - Reviewer Account – This is the unique user name.
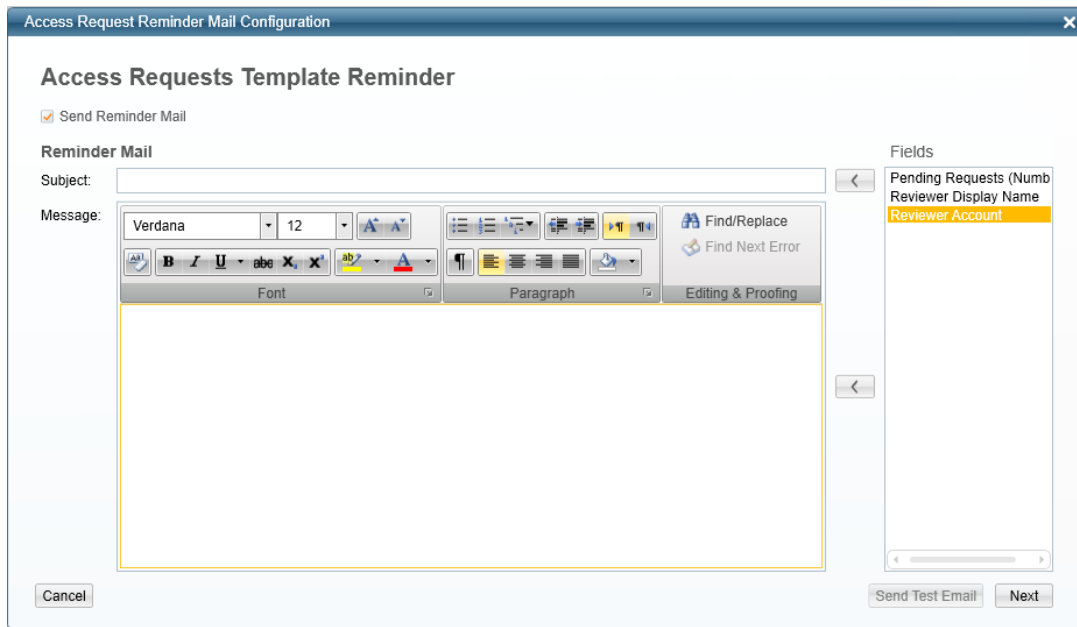


5. Click **Next**.
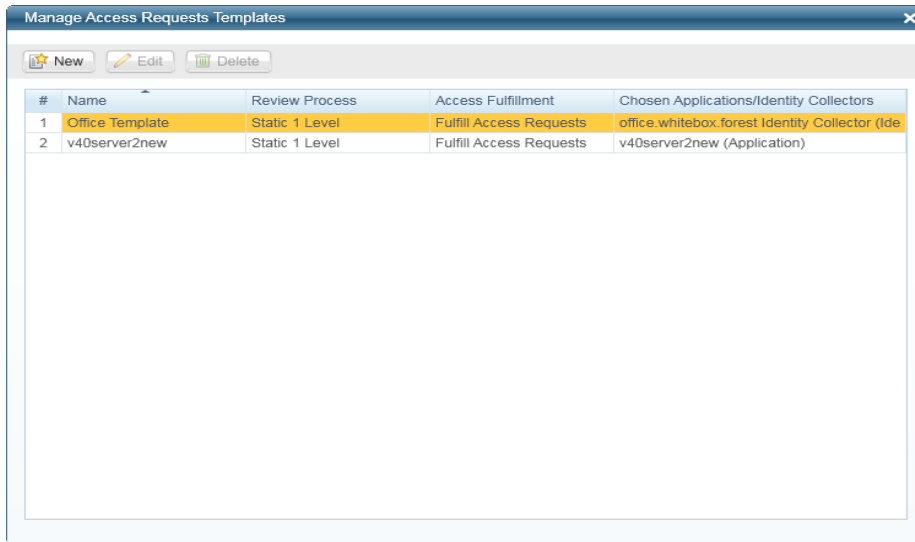
   The Reminder Email Scheduler displays.

6. Check the **Create a Schedule** check box to create a schedule.

7. Fill in the Name, Schedule, On (date), and At (time) fields with the relevant information.

8. Click **Finish**.

## *List Access Request Templates*

To view a list of Access Request templates, perform the following steps:

1. In the administrative client, navigate to **Access Requests > Configuration > Manage Access Requests Templates**.

2. Right click any of the Access Request templates to open an editing option menu:
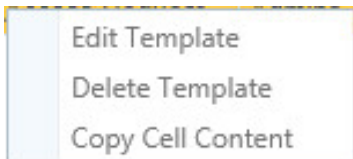


Access Request Template Editing Options

Menu options include:

- Edit template

- Delete template

## *Overview of Access Requests*

The *Access Requests* screen centralizes all access requests in the system.

It contains a filter mechanism, a main data grid (with displayed access requests) and a toolbar for the Actions, Reports, and Configurations menus.

This section describes how to list, view, and reassign access requests.

The main access request data grid contains the following information for each access request:

The main access request data grid contains the following information for each request:

- # (assigned by the system)

- ID

- Type

- Status

- Application

- Origin

- Issued By

- Review Conclusion

- Progress

- Fulfillment Status

- Issued At

- Due Date

- See More

1. To access the Access Requests panel, navigate to **Permissions > Access Requests**.

The default view of the navigation filter displays pending access requests, issued in the past seven days.

Filter the list of access requests first, and then select one or more access requests from which to drill down to more information.

To filter the access requests, perform the following steps:

> Not all fields are mandatory.

2. Select an ID for the Access Request.

3. Select one of the following campaign statuses to display from the **Status Field** dropdown menu:

    - *Pending Creation* – Access request has not been created

    - *Pending* – Access request is pending

    - *Closed* - All access review processes have finished

    - *All* - All access requests

4. Fill in the following Access Requests fields:

    - Due Date

    - Application

    - Origin (the campaign in which the permission was revoked)

    - Issued By

    - Issue Date

    > These fields are static and filter revoked permissions.

5. Fill in the following Advanced fields:

    - Resource

    - User

- Permission

- Group

> These fields are dynamic and the fields displayed may differ from those listed above.

6. Click **Apply** to apply the selected filters or click **Clear Filter** select different filters.

7. The filtered access requests display in the main **Access Requests** screen.

8. Select the **In Summary** expander to view summary charts of all the access requests (which are the same regardless of the selected filters).

9. Three separate access request summaries display:

   - The summary on the left is a bar graph that shows Open Requests by Due Date.

   - The summary in the middle lists Pending Access Requests by Reviewer (top 10), as well as the number of review items for each reviewer.

   - The summary on the right is a pie graph that displays In Process Access Requests by Application.

10. The section under the **In Summary** section lists the selected filtered status.

11. Double click on a selected access request to view its details.

## *Inside Access Requests*

Filter access requests by:

- Pending Permissions by Reviewer (which lists pending permissions by reviewer)

- All Permissions (which provides full filtering of all permissions)

In addition, it is also possible to reassign permissions or revert the permission review process.

The following subsections describe permission filtering, reassignment, and reversion of the permissions review process.

### Pending Permissions by Reviewer

To view pending permissions by reviewer, perform the following steps:

1. To view pending permissions by reviewer, click **Pending Permissions by Reviewer** as the filter view. The reviewers list will be displayed on the right with the number of permissions waiting for them to review.

2. Click **In Summary** expander to see a summary of the campaign's permissions.

> Since the charts in the In Summary view reflect all the permissions, they will remain the same, regardless of any filter applied.

3. The information on the left displays permissions by review process levels. The pie chart on the right displays permissions by review status (approved, rejected, or pending).

4. You can click **Refresh** to refresh the summary view.
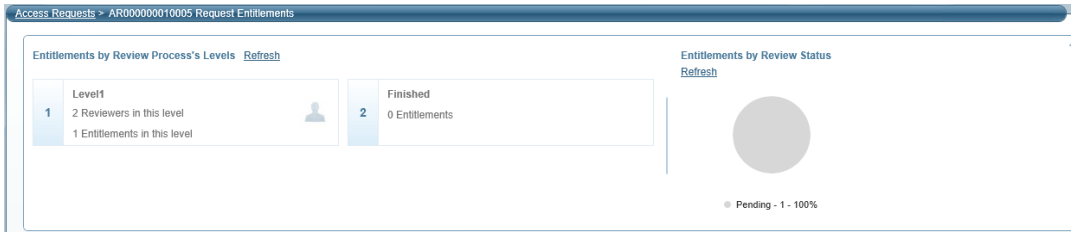


## All Permissions

All Permissions fall into the following filtering categories:

***Permissions—Standard (fixed) search fields, including:***

*Resource* - Business resource

*User* - User name

*Permission* - Permission level

*Group* - User group

*Rev. Conclusion* – Select from All, Rejected, Approved, Pending Conclusion, or Not Relevant.

*Fulfillment Type* – Select from All, Automatic, Manual, or None.

*Fulfillment Status* – Select from All, Not Relevant (Rejected by Reviewer), Not Fulfilled, Fulfilled, Pending Conclusion, and Not Relevant.

*Level Name* – Name of the level

***Dynamic Fields — Use these customizable fields for additional searching, for example:***

Business Resource Name

Department

To view all permissions:

1. Select **All Permissions** as the filter view.

2. Click in each of the Permissions fields, and select an option from the options displayed in the popup window.

3. Click **Apply**.

The filtered permissions displays in the Access Request list to the right.

1. Double click one or more of the entries from the list.

2. Review Process details display, with the following information on that permission:

    - Level ID

    - Level Status

    - Level Name

    - Reviewer

    - Response

    - Time

- Comment



## Reassign Permissions

An administrator can reassign a permission review from one reviewer to another reviewer (for any reason).

*To reassign permission permissions:*

1. Right click on a permission line from **Reassign Permissions**.

2. Select a user for reassignment of permissions and type a reason (mandatory).

3. Enter the new reassignment destination and click **Reassign**.

*To reassign all permissions:*

4. Navigate to **Actions > Reassign Permission Review > All Permissions**, and type a reason (mandatory).

The Permissions Reassignment window displays.
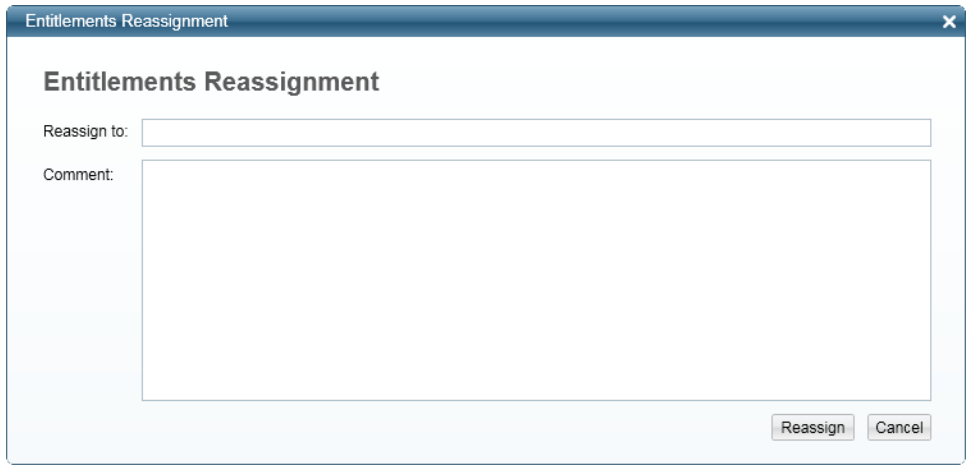
5. Enter the new reassignment destination and click **Reassign**.

   To reassign multiple permissions, perform the following steps:

6. Press and hold the shift key and select the permissions to reassign.

7. Right click outside of the highlighted area (on the grid), and then click **Reassign Permissions**.

8. Enter a reason for this action (mandatory).

9. The Permissions Reassignment window displays.

10. Enter the new reassignment destination and click **Reassign**.

### Revert Permissions

An administrator (not a reviewer) can revert permissions to a previous review level.

To revert permissions, perform the following steps:

1. Press and hold the shift key and select the permissions to reassign.

2. Right click and then select **Revert Review Process**.

3. Select the level (for example, Level 1) to which to revert.

4. The Confirmation popup below displays, noting the consequences of resetting the review process to a previous level.
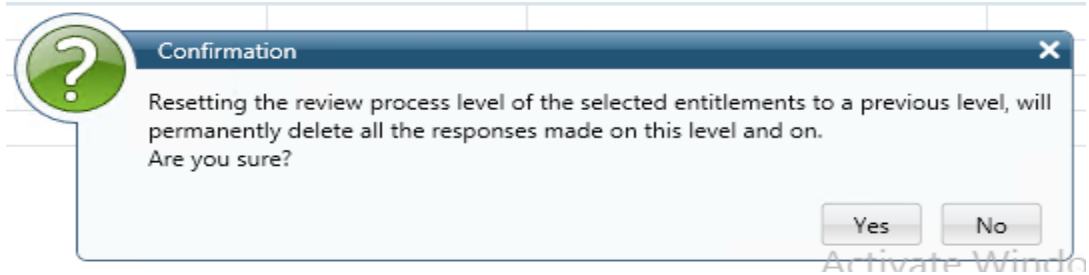


5. Click **Yes** to revert, or **No** to return to the previous screen.

## Access Fulfillment

The Access Fulfillment module assists organizations in managing permissions automatically on managed business resources (BRs).

The main steps of the access fulfillment process are:

1. A user initiates an access request to receive permissions to a BR.

2. The administrator assigned the relevant approval tasks to all required reviewers.

3. All required reviewers review and approve or deny the access request.

4. File Access Manager automatically fulfills the access request through the relevant Identity Collectors and the Collector Synchronizer service.

See section Review Process for further information about the review process as it affects Access Fulfillment.

### *Fulfillment for Managed and Unmanaged BRs*

Access fulfillment can be initiated by a user's access request, or as the outcome of a campaign, whereby the systems recommends revoking a user's access permission.

There are several methods for access fulfillment:

- Automatic fulfillment using File Access Manager functions. This process works on managed BRs – BRs that underwent a normalization process, as described in the sections below.

- Automatic fulfillment using a customer supplied script. This process works on unmanaged BRs only.

- Manual fulfillment – the user responsible for the fulfillment will receive a fulfillment task.

- The type of fulfillment is determined by the business resource type, and the setting of the Fulfillment type.

| Fulfillment field | Managed BRs | Unmanaged BRs |
|---|---|---|
| None | No action | No action |
| Fulfill Access Request / Manual Fulfillment Review Process | Fulfillment processed automatically by the system | Manual fulfillment process. The user performing the fulfillment must mark the task as done. |
| Execute Custom Script | Fulfillment processed automatically by the system | Fulfillment processed automatically, calling the custom script for each BR. |

### *Supported Applications*

The system supports Access fulfillment for the following applications:

| Target System | Products and Supported Versions |
|---|---|
| Base Product | Microsoft Active Directory |

| Target System | Products and Supported Versions |
|---|---|
| On-premises File Storage | Microsoft Windows |
| | Microsoft SharePoint |
| NAS File Storage | NetApp for CIFS |
| | EMC Celerra/VNX/Unity for CIFS |
| | EMC Isilon for CIFS |
| | Hitachi HNAS |
| | DFS for CIFS |

# General Flow of Access Fulfillment
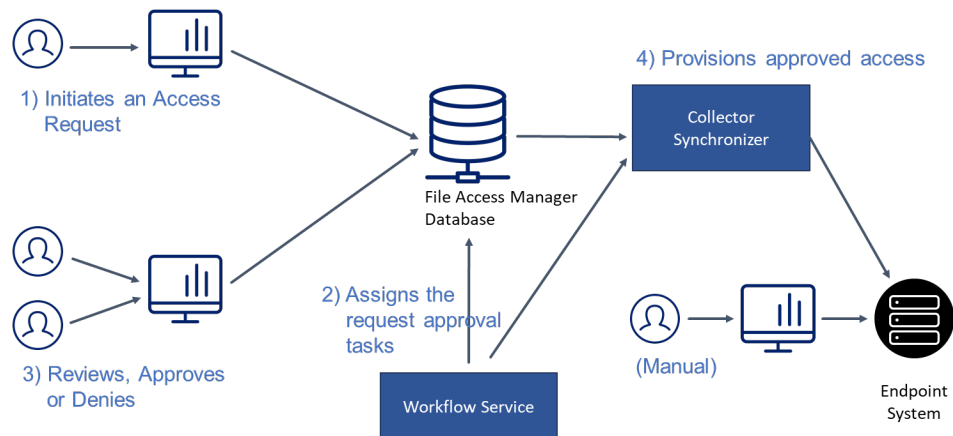


## The Normalization Process

The normalization process reconfigures permissions into dedicated groups. Once a resource is normalized, we can automatically fulfill access certification campaigns and requests.

Normalized resources are enabled and relevant only for applications that support fulfillment.

Every resource managed by File Access Manager (except for AD groups) must go through a normalization process.

- The system creates and sets managed permission groups with the correct permissions on the resource.

- The system distributes Users with permissions on a resource among the managed permission groups, based on their current access levels. (It is possible to customize the action applicable to an inexact permission match).

- The resource inheritance of permissions is set to **false**.

After successful normalization, it is possible to change resource permissions by:

### Access Request

> Whether self-issued, or as the result of an access certification campaign (Access Revoked).

### An approved What-If simulation

> One that a logged-in user has been requested to fulfill.

## Manage Normalized Resources

Normalized resources are enabled and relevant in the following conditions:

1. Applications that support fulfillment
2. Enabling Access Fulfillment for an Application

To access the Manage Normalized Resources page

1. Go to *Admin > Applications*
2. Locate the required application to which you want to add resources.
3. Click on the dropdown menu on the application row, and select **Manage Normalized Resources**

   This will open the Manage Normalized Resources page

4. The Normalized Resources page lists resources in this application that are normalized, or pending normalization.

### Name

> Name of the managed resource.

### Full Path

> Path name

### Status

> Provides the status of the uploaded resources.

### Actions

> The Actions column provides the Manage gear which gives the option to manage the normalization.

### Search by name or full path

> User can search by the resource name or the full path.

> The normalization process is still done within the Admin Client. There is another option to set a resource for a normalization using the Manage Resources screen.

### Global Options menu

- *Bulk Set*

   Allows the user to upload a list of resources to be normalized and become managed by File Access Manager. These resources will then be queued and the Normalization engine in the Permission Collection Engine will pick them up one by one, normalize their permissions and mark them as managed.

   See Adding or Removing Resources in Bulk

- *Bulk Remove*

   Removes the managed state from a list of resources. They are no longer considered normalized.

   See Adding or Removing Resources in Bulk

- *Generate Report*

   Run or schedule a report that lists all managed resources.

**Editing Normalized Resources**

Normalized resources are enabled and relevant only for applications that support fulfillment.

In the Manage Normalized Resources page you can change the following properties for resources:

- Disable normalization for this resource
- Determine the method of handling inexact permissions matches during a normalization process

*Editing the properties of Normalized Resources*

1. Go to *Admin > Applications*

2. Locate the required application to which you want to add resources.

3. Click on the dropdown menu on the application row, and select **Manage Normalized Resources**

   This will open the Manage Normalized Resources page

2. Locate the resource to edit, and press the Actions menu on the resource row

   This will open the "**Enable Normalization for this Resource**" panel

*Disabling normalization for this resource*

   Uncheck **Enable Normalization for this Resource**.

   This will remove normalization from the source, and remove the resource from the **Manage Normalized Resources** page.

   To enable normalization for this resource once it has been removed, you can use one of the following methods:

- Add it to a CSV file, and upload it using Bulk Set Normalized Resources (See Adding or Removing Resources in Bulk)

- Set the resource to Enable Normalization for this Resource in the **Manage Resources** page

*Setting the methods of handling inexact permissions matches during a normalization process*

As a part of the normalization process for a resource to be managed, File Access Manager attempts to match every existing permission to one of the managed permissions types. This attribute decides what to do in the case that a granted permission is not an exact match to one of the managed ones

Select one of the following methods of handling inexact permissions matches during a normalization process:

- Fail the normalization process - This is the default behavior

- Elevate to the nearest permission match

- Revoke the permission

**Adding or Removing Resources in Bulk**

Normalized resources are enabled and relevant only for applications that support fulfillment.

You can add or remove resources to normalize one at a time, or provide a csv file with a list of resources to normalize or remove from the normalization process.

1. Create a list of resources with a header, and save it as a csv file.

    *Format:*

    Resource Full Path

    \\fileServer\share

    \\fileServer\share1

    > The csv file should be in UTF-8 encoding

2. Go to *Admin > Applications*

2. Locate the required application to which you want to add resources.

3. Click on the dropdown menu on the application row, and select **Manage Normalized Resources**

    This will open the Manage Normalized Resources page

3. On the **Global Options menu**, select **Bulk Set** or **Bulk Remove**

    This will open the Bulk Set / Remove Resources to Normalize page

4. Click **Chose a file** to select the CSV file from your computer, or drag it onto the input panel.

5. Click **Upload**.

    > The CSV file for the Administrative Client should be in UTF-8 encoding.

    A popup will open listing errors in the input file.

    The files added for normalization will be listed in the normalized resources page as "Pending Normalization" until the normalization task is completed successfully.

## *Normalization and Access Fulfillment*

The following subsections discuss various aspects of normalization and management in Access Fulfillment activities.

## Normalization Process Concepts

Normalization is the process by which File Access Manager controls business resource permissions. An unmanaged business resource is made into a "managed" one by assigning a business resource with dedicated Domain Local AD Groups, to manage the access rights to that resource, using the following permission types:

- [Group] - Full Control

- [Group] - Modify

- [Group] - Read and Execute

- [Group] - List Folder Contents

The Local Users and Special groups listed below are excluded from the normalization process and will maintain their permissions on the normalized business resource:

- Local Users

- Domain Users (a domain group)

- Local Groups

    - Everyone (includes Domain, Local, and Guest)

    - Authenticated Users (includes Domain and Local)

## Normalization Process Steps

The Normalization Process consists of the following steps:

- Use the identity collection and permissions analysis capabilities to gather (read) information about the current identities access rights to the resource being normalized.

- Expand groups and nested groups.

- Calculate effective permissions.

- Create managed groups and associate users with managed groups.

- Assign BR permissions to managed groups.

## Normalization Process Examples

*Example 1:*

The Finance Group within C:\Finance has Full Control permissions, and User A has requested access to read permissions on C:\Finance.

An Administrator can grant User A the requested access either by:

- Granting User A Read permissions or

- Joining User A to the Finance Group

*Analysis:*

There are disadvantages to both methods, neither of which are good business practices. If User A has Read rights, to a BR, those rights will not be manageable, and as such, will not be eligible for the Normalization process. On the other hand, joining User A to the Finance Group will automatically give User A all the permissions available to the members

---

of the Finance Group. In both scenarios, User A will have rights over which File Access Manager will not have complete control.

*Example 2:*

The Finance Group includes User A, User B, and User C, each of whom has Full Control permissions.

The C-Level Executive Group includes User A, User D, and User E, each of whom has Read permissions.

*Analysis:*

User A has both Full Control permissions in the Finance Group and Read permissions in the C-Level Executive Group, since User A (and the other users) retains the same permissions before and after the Normalization process. The system can now manage Full Control Permissions in the Finance Group and Read permissions in the C-Level Executive Group for other users requesting access to those types of permissions in each group.

## Normalization Process Challenges

*Expand Groups and Nested Groups:*

The Identity Application represents either a single domain or multiple domains that are in a trust relationship. If these domains are not synchronized through the Identity Collector, it will not be possible to expand nested groups, and the Normalization process will fail.

*Calculate Effective Permissions:*

The calculation of effective permissions may become complicated when users are members of more than one group with permissions allowed in one group, but denied in another group.

*Scenario 1:*

Group A has Full Control permissions allowed to a BR and Group B has Modify permissions denied to that BR, and assume that User A belongs to both Group A and Group B.

Due to the permissions conflict created by User A's membership in both Group A and Group B, will have Full Control permissions except for Modify permissions, which leaves User A with only Read and Execute permissions.

*Scenario 2:*

User B requests access to Read and Execute permissions and to Delete permissions. Remember that Modify permissions include Read and Execute permissions. An administrator can either fail the normalization process, elevate to the nearest permission match, or revoke the permission.

The table below summarizes the results of each action involving the calculation of effective permissions.

| Action | Result |
|---|---|
| Fail the normalization process | User B has no permissions. |
| Elevate to the nearest permission match | User B has Modify permissions (Read and Execute, Write, and Delete). |
| Revoke the permission | User B has only Read and Execute permissions. |

## Normalization Process Results

User C submits an access request to have Read and Execute permissions to the Finance Group. All relevant reviewers reviewed and approved User C's request. If Read and Execute permissions to the Finance Group are a managed business resource, the system automatically executes access fulfillment, and User C will belong to the Finance - Read and Execute Group.

### Managed Resource

File Access Manager manages the access permissions of managed resources.

### Managed Permissions Group

This Active Directory (Domain Local) group includes users granted a specific permission type on a managed resource. It is possible to create Managed Permission Groups per managed permission type or per managed resource.

## *Enabling Access Fulfillment*

Access Fulfillment is supported by the following applications:

- Active Directory

- Windows File Server

- SharePoint

- NetApp CIFS

- EMC Celerra CIFS

- EMC Isilon CIFS

- Hitachi HNAS

- Windows DFS CIFS

To enable access fulfillment, the application has to be enabled for fulfillment (See Enabling Access Fulfillment for an Application), and the business resources under the application have to be normalized (See Manage Normalized Resources).

> Access fulfillment can be used on non-normalized resources for removal of direct permissions. see Access Fulfillment for Removal of Explicit Permissions

### Enabling Fulfillment for an Application

For applications that support Access Fulfillment only

Configured on the application configuration page. (Admin > Applications. Find application. Click Edit button. Change configuration)

See Enabling Access Fulfillment for an Application for a full description.

### Normalizing a Business Resource

To normalize a resource, open the Manage Resources page (Admin > Applications. Find application. Open the options menu and select Manage Resources)

Select the resource to normalize

Click *Manage Normalization > Enable Normalization* for this resource

Define *How to Handle Inexact Permissions Matches*

### Normalizing a List of Business Resources

To normalize a list of resources, use the *Bulk Set* option on the *Manage Normalized Resources* page (See Adding or Removing Resources in Bulk)

Open the *Manage Normalized Resources* page ( Admin > Applications. Find application. Open the options menu and select Manage Normalized Resources)

Open the *Global Options* menu and select *Bulk Set*

Upload a list of resources to normalize

### Disabling Normalization for a Resource

Select a resource on the *Manage Resources* page, and disable the normalization from the action menu

or open the *Manage Normalized Resources* page, and disable the normalization (See Editing Normalized Resources)

### Disabling Normalization for a List of Resource

For a list of resources use the *Bulk Remove* option on the *Manage Normalized Resources* page.

Create a file with a list of resources to disable, and upload them using Adding or Removing Resources in Bulk

## Enabling Access Fulfillment for an Application

> Standard Automatic Fulfillment (non-custom) is applicable to SharePoint Server and CIFS-based Applications (e.g. Windows Servers, and NetApp and EMC NAS devices supporting the CIFS protocol)

Access fulfillment is enabled per application in the application setting screen, for applications that support fulfillment (See the compatibility table in Compass for the full list)

### To enable Access Fulfillment for an application:

1. Open the configuration screen of the required application

    a. Navigate to *Admin > Applications*

    b. Scroll through the list, or use the filter to find the application

    c. Click the edit icon 📝 on the line of the application

2. Press **Next** till you reach the **Access Fulfillment** settings page.

    > The setting pages and entry fields vary according to the application type

3. For non-normalized resources, you can click **Enable Access Fulfillment for Revoking Explicit Permissions** . See Access Fulfillment for Removal of Explicit Permissions

4. Click **Enable Access Fulfillment for Normalized Groups**

    ### Identity Collector

    Fulfillment requires an identity collector in order to run. If you did not select an identity collector in the General Details configuration page, you can select one from the drop down list now.

    If there is no identity collector defined for this application, or if you want to use a different identity collector than the ones in the dropdown list, you can create a new identity collector in the Administrative Client (*Applications > Configuration > Permissions Management > Identity Collectors*).

    See Creating or Editing an Active Directory Identity Collector for more details on creating an identity collector.

    ### Managed Group OU (DN)

    The organizational unit in which the managed permission groups will be created. Make sure that the chosen identity collector's user has permissions to create groups under this location (e.g. OU=FileAccessManagerManaged, DC=SailPoint, DC=COM)

OU refers to an Organizational Unit, and DN refers to a Distinguished Name.

### *How to Handle 'List Folder Contents' Permissions*

Not relevant for SharePoint

- Create and manage a dedicated permissions group for it - this is the default value

- Revoke these permissions

### *How to Handle Inexact Permissions Matches*

During the normalization process, the application has to decide what to do with permissions that do not match the normalized permissions.

- Fail the normalization process

- Elevate to the nearest permission match

- Revoke the permission

5. Open the Advanced Settings panel for additional settings:

### *Group Cache Sync Interval(sec)*

This setting will add a pause to the process of setting normalize permissions on the resource. This will allow the endpoint's local AD groups cache to sync the newly created managed groups.

The default Is 0 - signifying the process will not pause by default.

### *Use Template Permission Group*

Template groups are created per application and added as a template to every managed resource. These groups are not managed by File Access Manager, and are usually used to ensure that users who need application-wide access such as backup or archiving users have access.

Select for each permission group whether File Access Manager should create a group or whether to use an existing group, for the following groups:

**Groups for SharePoint**

- Design

- Contribute

- Read

- Edit

- Full Control

**Groups for all other applications**

- List Folder Contents

- Read & Execute

- Modify

- Full Control

If you select **Use an Existing Group**, select the required group to use from the dropdown list.

Once an application is enabled for access fulfillment, you can set specific resources to be normalized using the Manage Normalized Resources page.

**Enabling Access Fulfillment for Identity Collectors**

*To enable Access Fulfillment for an identity collector (Active Directory Groups):*

1. In the administrative client, navigate to **Applications > Configuration > Permissions Management > Identity Collectors**.

   An Identity Collectors window displays.
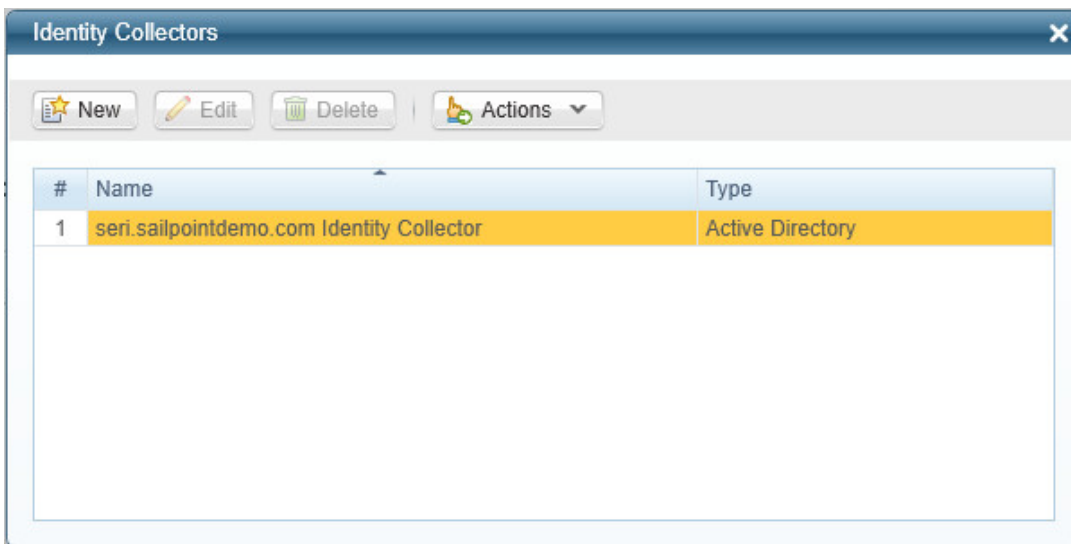


2. Select an Identity collector, and click **Edit to open the** Identity Collector Configuration Wizard.
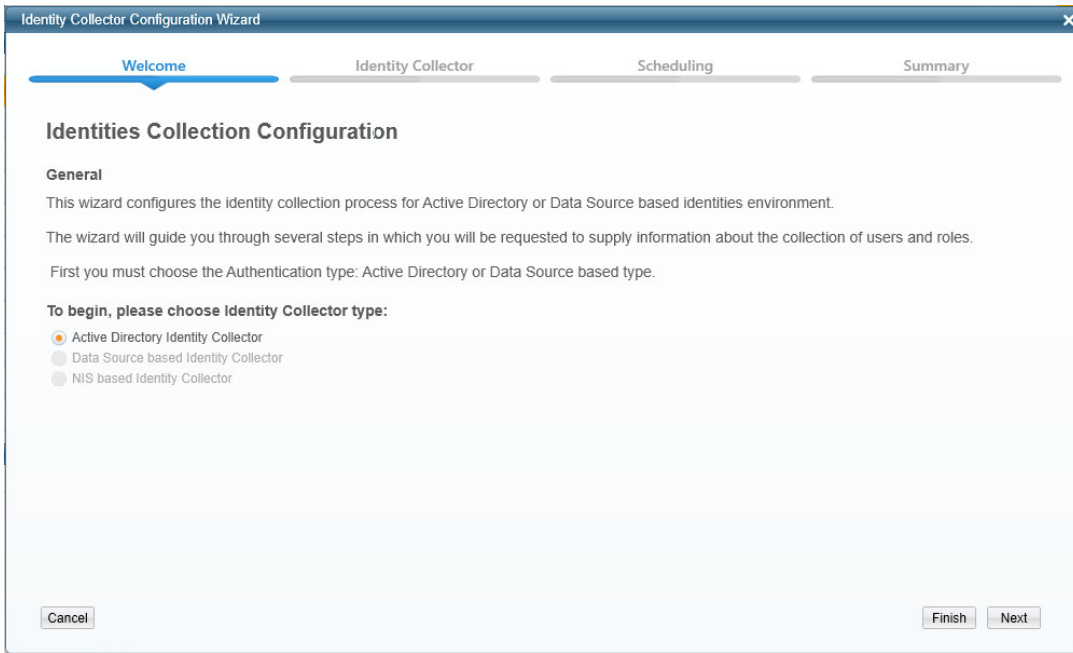
3. Click **Next**.

   The Identities Collection window displays.
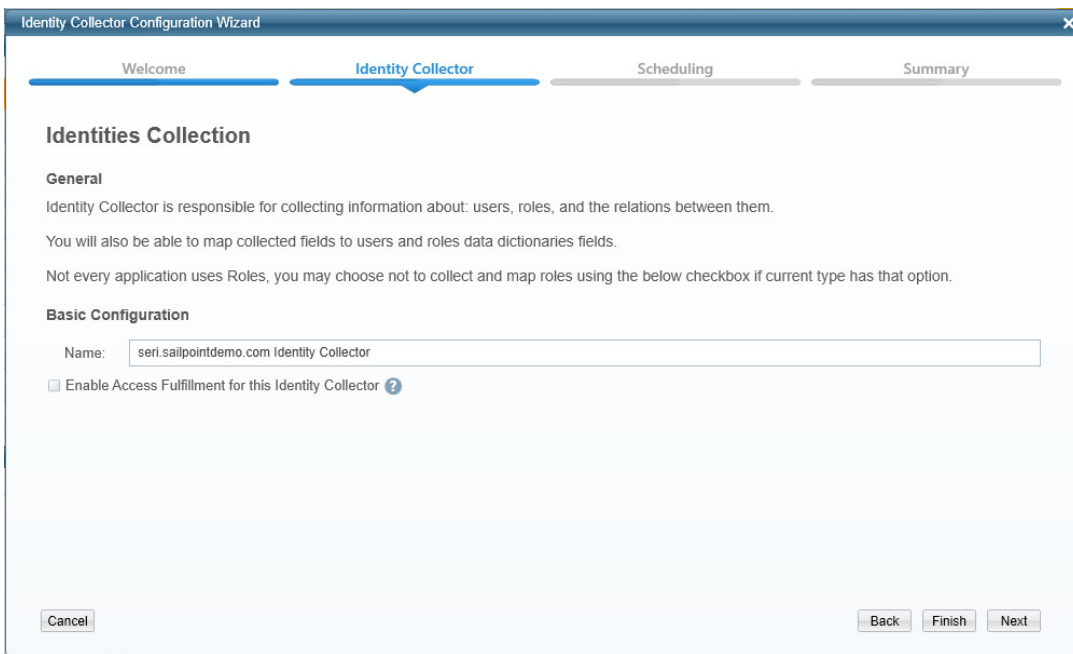


4. Select the **Enable Access Fulfillment for this Identity Collector** check box.

5. Click **Finish**.

**Enabling Access Fulfillment for Business Resources**

To enable access fulfillment for a resource, it has to meet the following conditions:

- The application has to support access fulfillment (See the compatibility matrix in Compass for a full list for this release)

- The Application has to be enabled for access fulfillment . This setting is in the application configuration pages.

- The business resource has to be normalized

> Access fulfillment can be used on non-normalized resources for removal of direct permissions. see Access Fulfillment for Removal of Explicit Permissions

**Enabling Normalization for a Resource**

> For a list of resources: Create a file with a list of resources to enable, and upload them using Adding or Removing Resources in Bulk

1. Open the Manager Resources page

   *Admin > Applications*. Find application. Open the options menu and select ***Manage Resources***

2. Select a resource and Click *Manage Normalization > Enable Normalization for this Resource*

3. Determine *How to Handle Inexact Permissions Matches*

   During the normalization process, the application has to decide what to do with permissions that do not match the normalized permissions.

   - Fail the normalization process

   - Elevate to the nearest permission match

   - Revoke the permission

**Disabling Normalization for a Resource**

> For a list of resources: Create a file with a list of resources to disable, and upload them using Adding or Removing Resources in Bulk

- Through the **Manage Resources** page

   a. Open the Manager Resources page

      *Admin > Applications*. Find application. Open the options menu and select ***Manage Resources***

   b. Select a resource and Click *Manage Normalization*

   c. Deselect *Enable Normalization for this Resource*

- Through the **Manage Normalized Resources** page

   a. Open the Manager Normalized Resources page

      *Admin > Applications*. Find application. Open the options menu and select ***Manage Normalized Resources***

    b.  Select a resource and Click *Actions*

    c.  Deselect *Enable Normalization for this Resource*

        The resource will be remved from the Manage Normalized Resources page.

## *Access Fulfillment Configuration*

The following subsections describe the available actions associated with the Access Fulfillment configuration.

### Configure Access Fulfillment Requests Commit Schedule

Commit schedule defines when to run pending normalization requests (which can be during non-working hours so it will not affect end users).

To define the Access Fulfillment Requests Schedule, perform the following steps:

1. In the administrative client, navigate to **Access Fulfillment > Configuration > Configure Access Fulfillment Requests Commit Schedules**.

The Access Fulfillment Requests Commit Schedules window displays.
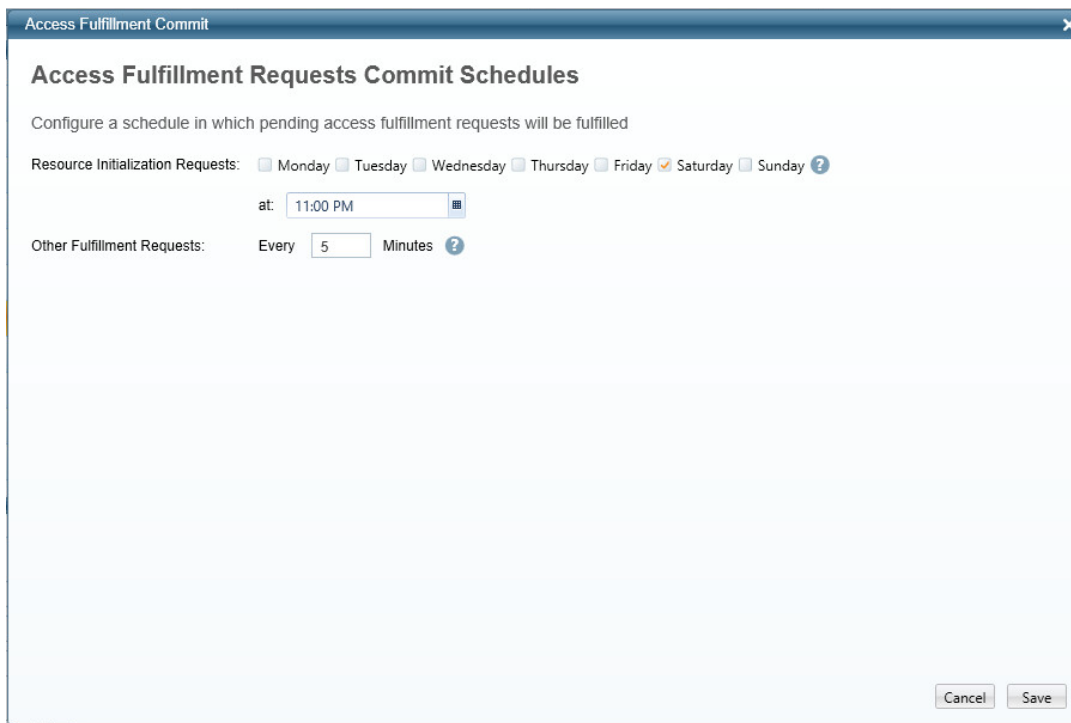


2. In the **Resource Normalization Requests** field, select the day and time for this schedule.
It is better to schedule normalization of new managed resources for off-peak hours; otherwise, it may overload the system.

3. In the **Other Fulfillment Requests** field, type the time cycle in minutes for this schedule.

4. Click **Save**.

### Configure Access Fulfillment Groups Naming Convention

This activity configures the naming convention for groups created during the normalization process of a business resource

To configure Access Fulfillment Groups Naming Convention, perform the following steps:

1. In the administrative client, navigate to **Access Fulfillment > Configuration > Configure Access Fulfillment Groups Naming Convention**.

The Access Fulfillment Groups Naming Convention window displays.



2. Enter the relevant data in the following fields:

- Resource Group Name

- Resource Group Description

- Template Group Name

- Template Group Description

> The name must contain the variables %Seq% and %PermType%.

> Template group names cannot contain the variables %ResName% or %ResPath%.

3. Click **Save**.

## *Access Fulfillment for Removal of Explicit Permissions*

Explicit permissions can be removed from a Business Resource (BR) without the necessity of running the normalization process on it.

> This option is only available for BRs that support fulfillment. BRs that do not support fulfillment will not have a Fulfillment tab on the Application Wizard.

The following guidelines apply to the removal of explicit permissions:

- The application should be configured to support the removal of explicit permissions.

- Only explicit permissions (ACEs) can be removed. An ACE is a permission set directly on a resource, which can include any domain user/group, local user/group, special groups, such as Everyone/Authenticated Users, or orphan accounts. Permissions inherited from a parent resource, or granted to a specific user through a group, **cannot be removed**.

- Explicit permissions of normalized groups, created and managed by File Access Manager, cannot be removed.

- Only Active Directory users with the Administrator capability can remove explicit permissions.

The following subsections describe how to configure applications and remove explicit permissions.

### Supported Applications

Access fulfillment for Removal of explicit Permissions is supported for the following CIFS applications: Windows, NetApps, EMC Celerra CIFS, Isilon, and HDS.

### Configuration

***To enable removal of explicit (direct) permissions on a specific application:***

1. Open the configuration screen of the required application

    a. Navigate to *Admin > Applications*

    b. Scroll through the list, or use the filter to find the application

    c. Click the edit icon   on the line of the application

2. Press **Next** till you reach the **Access Fulfillment** settings page.

    > The setting pages and entry fields vary according to the application type

3. Click **Enable Access Fulfillment for Revoking Explicit Permissions**

4. Click **Next** or **Done** to leave the configuration page.

### Removing Explicit Permissions

It is possible to remove explicit permissions in the *Permissions Forensics* page and in campaigns.

See "Remove Explicit Permissions" in Owner Permission Field and Remove Direct Permissions in Campaigns for more details .

## *Remove Direct Permissions in Campaigns*

1. Create and save a Permissions Query in the **Forensics > Permissions** screen.

2. Navigate to **Compliance > Access Certification**:

a. Create a campaign using the Permission Query.

b. From **Summary > Fulfillment Process**, click **Edit**.

c. Click **Fulfill Permissions Revoke Requests**.

d. Click **Save and Run the Campaign**.

Access Requests for permission removal are the results of campaign reviewers' reject decisions.

Once the review process for Access Requests is finished, the system removes all direct permissions on supported applications from the relevant BRs.

### Monitoring the Progress of Permission Removal

Access Fulfillment is created for each direct permission marked for removal. To monitor progress, in the administrative client, navigate to Access Fulfillment and filter the Fulfillment Requests by Action "Remove Permission".

## Access Fulfillment Advanced Forensics Control (AFC) Filter

To operate the AFC for access fulfillment, perform the following steps:

1. In the administrative client, navigate to Access Fulfillment.



2. Select the relevant data from the following dropdown menus in the Fulfillment Request section:

- *Action* (default is "All")

- *Status* (default is "Not Completed")

- Issued By

- *Issue Date* (Preset or Period)

- *Request ID*

3. Double click on the field next to each of the field types in the Fulfilled Permission section, and select the relevant data:

- Application

- Resource

- Group

- User

- Permission

The selections that open when you double click on each field display the number of each item, and provide a dropdown menu, in which you can select the number of items to display for each field type.

4. Click **Close** after you have selected each field selection.

5. Click **Apply** to activate the filters or click **Clear Filter** to clear the filter parameters.

**Access Fulfillment Actions**

Access Fulfillment actions involves the viewing of fulfillment requests and their statuses.

To specify Access Fulfillment Actions, perform the following steps:

1. In the administrative client, navigate to **Access Fulfillment > Actions**.

2. Double click on a business resource to view a detailed log of the resource, and to determine (if possible) where an error has occurred.

A configured user must have Full Control of a business resource to perform normalization on it.

3. Select one of the following actions:

- **Retry** - Retry a failed Access Fulfillment Request.

- **Fulfill Now** - Ignore the regular schedule, and fulfill now.

- **Cancel Fulfillment** - Cancel the fulfillment.

- **Rollback** - Undo changes caused by a successfully fulfilled access fulfillment request.

- **Rollback Now** - Ignore the regular schedule and rollback now.

## What-If Scenarios

The What-If scenarios in File Access Manager use simulations to help predict the effect on a user's permissions when the user is added to, or removed from, a group (for example, an Active Directory group).

## *What-If Simulation*

To run a What-If simulation, perform the following steps:

1.  Open the What-If window in the Administrative Client .

2.  In the What-If simulation panel on the left of the screen, select either:

    a.  Adding a user to a group

    b.  Removing a user from a group

3.  Under Scope, select one of the following:

    a.  *All applications* – Check the effect of the action on all existing applications.

    b.  *Only Application of Type* – Select the type of Application to simulate, which will show the results of the simulation for all Applications of the selected type.

    c.  *Specific Applications Only* – Select only one specific application to be included in the simulation.

4.  Under Parameters, select one of the following:

    a.  Select the group to add or remove under Group.

    b.  Select the user to add or remove under User.

5.  Click **Apply**.



6.  The What-If main window displays an Added Permissions Grid in table format for the selected user.

**Table View**

The table view displays only resources where permission changes occur, and not resources that change by permission inheritance. For example, if adding a user to a group results in giving that user permissions to a specific folder, File Access Manager only displays the folder in which the change occurs, and not all the child folders affected by this change.

1. Click the **>** next to Affected Resources on the left of the Added Permissions Grid to see a tree of the Affected Resources.

**Tree View**

The tree view displays resources in a color-coded format to help identify where changes occur, since those changes can sometimes be in a deep level of the tree. For example, if you simulate adding a user to a group, which results in giving the user permissions to a top-level folder, File Access Manager only displays the folder in which the change occurs, and not all the child folders affected by their inheriting this change.

The color-coding scheme is as follows:

- Dark Green indicates the direct addition of permission to a resource.

- Light Green indicates the addition of a permission somewhere in the tree below this resource. Follow all light green folders until they lead to a dark green folder, which indicates the direct addition of a permission.

- Dark Red indicates the direct removal of permission from a resource.

- Light Red indicates the removal of a permission somewhere in the tree below this resource. Follow all light red folders until they lead to a dark red folder, which indicates the direct removal of a permission.

> The Added Permissions Grid and the Affected Resources tree views complement one another with the same information in slightly different format.

> In the above figures, both views highlight Vss. In the tree view, Vss is dark green (indicating an added permission), and in the grid view, Vss has been added with full control permission.

## *Create Access Request*

After performing a simulation, you can create an access request to fulfill a change, but the request must pass all standard reviews before it is possible to fulfill it.

> See section Access Requests for additional information on Access Requests.

## *Fulfill Now (Bypass Review)*

The **Fulfill Now (Bypass Review)** option displays to users with a *Bypass review process for access requests* group. This option sends a request that is auto-approved and fulfilled.

Section Access Fulfillment  has additional information on Access Fulfillment.

# Forensics

The forensics' screens allow the administrators to view analysis screens of data collected by the File Access Manager services. The tables can be filtered to fit specific needs, and filters can be saved, and shared with others as well.

The File Access Manager website has the following forensics' screens:

- Activity forensics
- Permissions' forensics
- Identities' forensics
- Data Classification forensics

Forensic queries can be used to answer questions such as:

a. Who has accessed files classified as Credit Cards?

b. Who can access folders classified as SSN?

c. Are there users without a password in the system, or users who haven't logged in for the past six months?

## Forensic Screen Components

As we transition to the new graphic interface, the sections below describe the components of the **Permission** Forensics and **Identity** forensics screens.

### Filters: Creating and Editing a Forensics Query

Below is an image of the Permission Forensics filter menu.



A query is a collection of one or more filters that let you select from a list of parameters to select user types, permissions, user scenarios or permission scenarios to analyze.

> When creating a filter using Business Resource Name or Business Resource Full Path, those two fields only support Equals or Any of. This filter is not auto-complete capable.

1. Click **Clear All** to clear the current filters, and clear the grid.

2. Click **+** to add a filter to the query.

3. Select a field to filter by from the **Select Field** dropdown menu, and the filter criteria, according to the filed type and parameters.

4. Click **Save** to add the filter line to the query, or **Cancel** to start over.

5. Add more filter lines by repeating these steps as required.

*For example:*

> "Last login date older than 100 days
>
> and
>
> Password not required equals True"

6. Click **Apply** to run the query.

> For Permission Forensics, the data retrieved depend on the user scope of the user running the query. The data returned will only be within the applications and resources within each application to which the user running the query has access.

## Searching for Resources Using a Resource Tree

You can add resources for the filter by navigating down the resource tree and selecting the requested branch.

1. Open a new filter line.

2. Select **Resource** from the **Select Field** drop down list.

3. Open the **Select Resource** drop down menu to view the resource tree.

## Saving and Sharing Queries

### Saving Queries

1. To save a query click **Save**. That will open a popup screen to enter the query name.

2. Click **Save** or **Cancel** to continue.

A Query can be deleted only by the user who created it.

### Using Saved Queries

> If you select a saved query, the contents of your current query will be overwritten.

To retrieve a saved query:

1. Click **Saved Queries**

2. Select a query from one of the saved query lists:

- *Recent* – a list of your recently used queries. These queries are named and ordered by the timestamp.

- *Saved* – a list of queries saved by the user.

- *Shared* – a list of queries shared with the user.

Clicking on a Query will load its filters and displayed columns. A Query object cannot be edited, and changes made after loading a Query do not impact the loaded Query object. However, these changes can be saved in a new Query.

**Sharing Queries with Other Users**

The forensics screens give you the option to share queries with other users.

Sharing a query will make the query available in the quarry list of other users in this forensics screen.

To share a forensics query:

1.  Create a query as described above.

2.  Click **Save**.

3.  Type in a name for the query.

4.  Type in the name or part of a name of the user to share the query with.

5.  Select the user from the dropdown list.

6.  Click **Save** to save the query to your list and the assigned user's query list.

The query will be stored in the other user's list under "**Shared**".

## Generating Reports

To generate a report from the last run query:

1.  Run a query as described above, or by selecting a saved query from the query list.

2.  Select **Global Options > Generate Report**.

3.  The report will be available in My Reports.

To schedule and save a report template:

1.  Run a query as described above, or by selecting a saved query from the query list.

2.  Select **Global Options > Generate Report**.

3.  Name the schedule, and fill in the scheduling parameters.

## Permission Forensics

The Permission Forensics screen lets the user monitor and analyze the user and group permissions. On this screen you can create queries to analyze the permissions of specific groups of users, save and share queries for selecting users and groups, generate reports, run permission scans, and revoke explicit permissions of users.

This page supports reports and campaigns.

This component answers questions, such as:

*   Which users have access to what resources?

*   Which users have not used permissions granted to them?

*   Which permissions were granted to each group?

*   Which groups are not being used?

The table displays the permissions, according to the level of granularity selected in the filter.

When creating a filter, you can define the granularity of the report using the **View by** field, and can mark stale permissions on the table, according to the unused time selected.

> The query will retrieve the first 100,000 results. Narrow the search to obtain a better fit.

***Reports***

See Generating Reports

***Filters***

See Filters: Creating and Editing a Forensics Query

## Viewing Permission Forensics

The Permission Forensics table displays the permissions retrieved by the query run.

The data displayed, by default, includes the following columns for each permission:

- What resource
    - Business resource full path
    - Application
- Who the user is
    - User name
    - User display name
    - Group name
    - User domain
    - Group domain
    - User entity type
    - Group entity type
- The permission type
    - Permission type
    - Classification Category
    - Is Inherited
    - Inherits Permissions
    - ACL Type Allowed?

To change the order of the columns, drag the column titles.

Additional columns available are:

Application group, Application type, Business Resource Logical Path, Business Resource Name, Business Resource Type, Creates Loop, Creation Timestamp, Cumulative Last Used, Department, Distinguished Name, Group Path, Is

Effective, Is Owner Permission, Is Riskiest, Is, SID History, Last Login Date, Last Used Date, Loop Path, Password Never Expires, Password Not Required, Permission Type Description, User Disabled, User Email, User Locked

To select columns to display:

1. Click the Column chooser icon on the table header bar.

2. Select the columns to display from the drop down list.

   - Click **Show All** / **Show Less** to display a full list of columns / only the default columns in the column chooser. This does not change the selection of columns to display in the table.

   - User the search field to narrow down the list of columns in the column chooser.

   - Click **Reset Columns** to reset to the default selection and order of the columns in the table.

### *View by*

You can change the granularity of the output by selecting the View By type. These options will determine whether to check a user's direct permissions , or permissions granted by groups the user belongs too, as described below:

- Groups & Users direct Permissions

This view displays direct Users' and Groups' permissions but does not display the Group members.

- Users direct & Group membership Permissions

This view displays user permissions based on direct permission, group membership, and nested group membership. This view doesn't list the users in the groups Everyone and Authenticated Users.

- Everyone Groups expanded, Users direct & Group membership Permissions

This view displays user permissions based on direct permission, group membership, and nested group membership, including listing the members of the Everyone and Authenticated Users groups.

> The default view is the Users and Groups view.

> In the permission forensic screen, the View By field can be changed after setting or restoring the filter

### *Mark Stale Permissions*

Select the time period for stale permissions. The user permissions which were not in use for X time (configurable) will be marked in red.

## Scope and Hierarchical Search

By default, when you select a business resource (BR) to scope its permissions, only the direct BR permissions (not the child BR permissions) displays.

## Special Groups - Group Entity Type

When creating a filter, you can select the group entity type from the **Field** field.

In Windows-based environments, the user groups are *Everyone*, *Authenticated Users*, and *Domain Users*.

### *Everyone*

Includes all users.

### *Authenticated Users*

Includes all users without a guest.

### *Domain Users*

Includes a group with all users in the domain. By default, any user created is a member of this group (but it is possible to remove that user).

## Owner Permission Field

File Access Manager permissions forensics allows identification and tracking of Owner permissions in the AFM interface:

- A proprietary column, called "Is Owner Permission" indicates whether a given permission is an Owner permission.

- A proprietary query attribute is dedicated for filtering Owner permissions (allowing queries and/or reports listing the owners of resources).

### Permission Scan for Business Resource

The Permission Scan collects the security information from the scanned BRs, and stores it in the File Access Manager database. This includes which users or groups have access to the BR, and whether the access is inherited. The permission scan stores access types such as read, write, full control, etc., depending on the application type.

When requesting a permission scan, you can set the resources to scan, and the number of levels below the requested BR to scan.

To perform a permission scan:
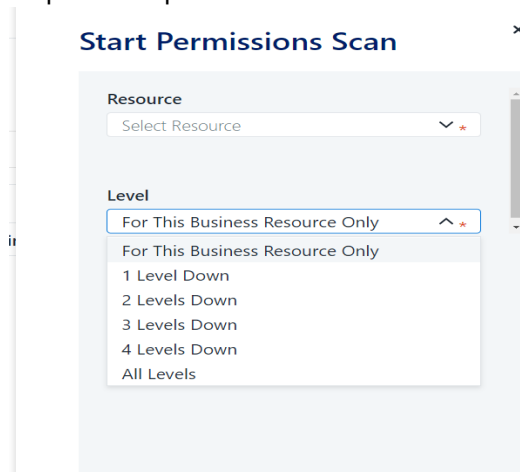


1. Open the Permission Forensics screen
   **Forensics > Permissions**

2. From the **Global Options** dropdown menu, select **Start Permission Scan.**

3. This will open the Permission Scan panelSelect the scan level:

- This Business Resource only

- This Business Resource and levels 'Level 1-4' and 'All Levels'

4. Click **Scan** to start the scan, or **Cancel** to return to the Permission Forensics screen.

## DFS Support

- For DFS resources, the Permission Forensics table will show the physical, as well as the logical path of resources.

- You can create a filter for DFS resources by logical path only. To select a logical path, select **Resource** on the **Select Field** drop down menu, then navigate to the required path on the resource tree on the **Select Resource** dropdown menu. (See Searching for Resources Using a Resource Tree).

## Removing Explicit Permissions Using the Permission Forensics Page

> This process will revoke explicit permissions from non-normalized resources that are configured for access fulfillment. Permissions that are inherited will not be removed.

1. Navigate to **Forensics > Permissions.**

2. Set a filter, as described in Filters: Creating and Editing a Forensics Query

3. Click **Apply** to run the filter.

4. Set the View to **Groups and Users direct permissions**.

5. In the permission results, select the permission rows to remove, by clicking the checkbox on the row.

   Before selecting which permissions to remove, be sure that:

   - The Application in which the BR resides is configured to support Access Fulfillment for Direct Permission Removal. Section Configuration in Access Fulfillment for Removal of Explicit Permissions has additional information on how to configure removal of explicit permissions.

   - The permission is defined directly on the BR (the value in the **Is Inherited** column is "False").

   - The selected permission is not a normalized group, created and managed by File Access Manager.

6. Click **Revoke Explicit Permissions**.



# Identities Forensics

To locate the Identity Forensics page, navigate to  **Forensics > Identities**.

The Identities Forensics screen displays users, groups and their relationship recorded by the system. Use filters to focus on specific data, The page supports reports and campaigns limited to 10,000 results.

*Filters*

> See Filters: Creating and Editing a Forensics Query

*Reports*

> See Generating Reports

## Viewing Identity Forensics Results

The Identity Forensics screen looks as follows:

## Tabs

Select the tab to display different data about users, groups and their relationship.

### Users' Membership in Groups

View of users and their group memberships;.

### Users

This tab displays users and their attributes, defined in the identity store.

### Groups

This tab displays groups and their attributes, defined in the identity store.

Identity queries involve identity stores connected to File Access Manager, regardless of the permissions attached to these identities.

Each tab has a separate filter and stored query list.

# Activity Forensics

To locate the Activity Forensics page, navigate to **Forensics > Activity**.

The Activity Forensics page can be used to track user activities in various areas of interest. For example:

## Filter

The activity forensics filter allows users to focus on set scenarios and areas of interest.

When you open the activity forensics page, it will load with the last query used.

The query is composed of one or more filters, combined with an **and** operator.



### Creating a Query

1. Create a filter.

   a. Select a field from the field dropdown list.

   b. Select an operator

c. Select or type in a value. For multiple values, start typing part of the value, and select items from the dropdown list by ticking the checkbox next to each item.

2. Click **Add** to add this filter to the query list

3. Repeat to add additional filter items to the query

4. Click **Apply** to run the query, and display the results

Common Activity Forensics filter fields

| Action type | |
|---|---|
| Application | From the applications connected and monitored by File Access Manager |
| Application type | |
| Category | As assigned by the data classification module |
| Object name | |
| Resource | Specific folder or folders to monitor |
| User | |

### Storing and Sharing Queries

The 10 last queries are stored for reuse, with the query timestamp as the name.

You can store queries for later use, with a meaningful name, with the option of sharing them with other users.


:
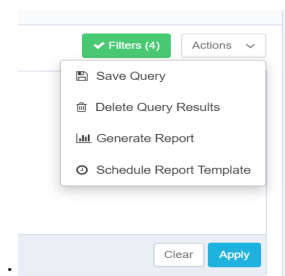
To store or share queries

1. Click the **Actions** dropdown menu on the top right corner.

2. Click **Save Query** to open the Save Query dialog box

3. Type in the query name, and , optionality, the name of a user(s) to share the query with.

a. Start typing the user name. To add a user to the share list, click the **+** button.

### Loading Stored Queries

To load a stored query, open the query list panel on the left side of the activity forensics page. You might have to click the restore button **>** , if this panel is minimized.

Click on a recent query, or a stored query to load the query, and apply it to the results.
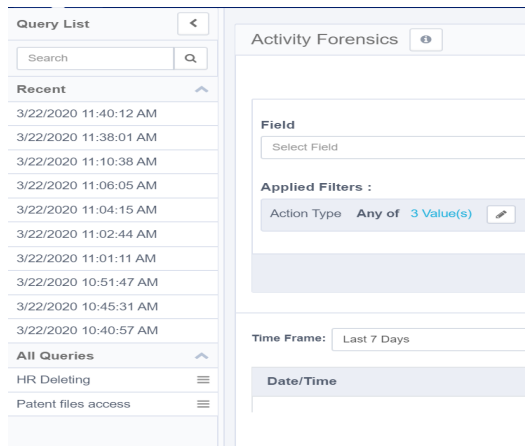
## Saving the Query to a Report

you can create a report out of an activity forensics query.

Select **Generate Report** from the **Activities** dropdown menu.

The report will be available in **Reports > My Reports**.

### Creating a Scheduled Report from a Query

You can also create a repeated report from the query.

Select **Schedule ReportTemplate** from the **Activities** dropdown menu to open the Schedule Report Template panel.

# Data Classification Forensics

The Data Classification Forensics screen can be found by navigating to **Forensics > Data Classification**. It displays data classification results, based on your active policies. Use filters to focus on specific data. You can sort the results by "Match Count". The returned records are limited to 10,000 results.

> The Data Classification Results table shows results of the data classification process running in File Access Manager, as well as any data classification results imported from an external source, using the Import Data Classification Results feature. This might lead to duplicate entries from the two sources.

## Reports

Data Classification reports can be found in the report templates, using the *Classified Data* tag to locate relevant reports.

## Using the Data Classification Forensics Table

Users can change one or more of the default columns by clicking on "Display Columns", and selecting one or more columns from the dropdown menu.
Currently, all columns display, including the following:

### *Application*

> This column displays all the system applications.

### *Application Type*

> This column displays all the system application types.

### *Last Updated*

> This is the timestamp of the last classification process, in which the file was classified into the specified category.

### *Result Type*

> This is the source of the classification result (Content, Behavioral, or Imported Classification).

> The default column headings, from left to right, are: Resource Full Path, File Name, Policy Name, Rule Name, Categories, and Match Count. You can clear any selections made in the Policy, Rule, and Category search fields by clicking "Clear Selection" on the top right of each field

1. Select a result type from the Result Type dropdown menu.

### *All*

> All possible result types

### *Behavioral*

> Only results from behavioral rules

### *Composite Classification*

> Results from composite rules (Combining the results of several classifications)

### *Content*

> Only results from content rules

### *Imported*

> Normally, the administrative client imports the results from a Data Loss Prevention (DLP) product that has already scanned the results to control what data end users can transfer, so there is no need to rescan those results.

2. Type a number in both the Match Count (Bigger than) and the Match Count (Smaller than) fields to restrict the number of Regular Expression (Regex, the general standard for textual search) results.

> Users can see the resources according to the user scope they have.

A result record represents the classification of a certain file by file, rule and policy. A single file can be classified into multiple rules/policies, resulting in a separate record in the result for each file-to-rule-to-policy relation.

The result record consists of default columns, which can be changed, based on the users' requirements:

### *Resource Full Path*

This is the full path of the resource in which the file resides.

### *File Name*

This is the name of the classified file.

### *Policy Name*

This is the name of the policy, by which the file is classified.

### *Rule Name*

This is the name of the rule, by which the file is classified.

### *Category*

This is the classification category name used by the rule.

### *Match Count*

This is the maximum number of matches under any rules requirements contained in the file . This is not an aggregative figure, and does not sum up the number of matches in each of the rule requirements for the file. Instead, it represents the highest match count yielded by any of the rule requirements, and should be viewed as a sensitivity score attributed to the file, in accordance with the applicable policy rules.

For example, if a policy rule contains two rule requirements – one matching credit card numbers with ten occurrences of credit card numbers within the same file, and another matching telephone numbers with eight occurrences of telephone numbers within the same file, the Match Count value of the file for that category (assigned by the rule) would be 10 (rather than 18, or 8), since it represents the maximum number of occurrences matching any of the rule requirements within that policy rule.
When the result displays a regular expression search, this field will be clickable and display the masked matches of the regular expression.

> The query will retrieve the first 10,000 results. Narrow the search to obtain a better fit.

## Filter

Complete the following steps to

---

1. To filter data classification forensics:

   a. Click the "Filters" button at the top right of the screen.

   b. The filter screen displays.



The forensics results can be filtered by:

- Policy Name

- Category

- Rule Name

- Result Type (All, Content, Behavior, Imported)

- Match Count (Bigger than/Smaller than)

- Filter by Scope

   a. Select a scope type (Application type, Application, or Resource) from the Scope Type dropdown menu.

   b. Select a corresponding resource from the Resources dropdown menu.
   You can clear a selection from this dropdown menu by clicking "Clear Selection" on the top right of the menu.

   c. Click Reset at the bottom left of the filtering screen to apply all the selected filters.

# Data Classification

The Data Classification categorizes and tags business resources based on the following:

- Content

- Behavior

- Imported designation

Classification is done by identifying resources with specific data, or resources accessed by specific user types, according to standard and user defined policies.

This section describes data classification module in File Access Manager and the operations available on the web application, **Compliance > Data Classification** tab.

## General

Data Classification:

- Content-based classification: Searching the files for specific content of interest, such as SSNs, credit card numbers, health records, etc.

- Behavioral-Based Classification: Analyzing BRs according to properties of users who access these data. For example, if members of the board of directors or members of the finance department regularly use these BRs

- Configuration of the classification process, using industry standard regulation compliance such as HIPAA and GDPR, as well as user configurable rules.

The Data Classification mechanism provides both a content-based and a behavioral-based analysis of files and BRs residing on the various applications, which facilitates their classification into categories, based on those analyses. Content-Based Classification parses and indexes the files' textual content and searches for specific patterns, according to predefined sets of rules consisting of sensitive keywords or keyword lists, complex regular expressions representing patterns such as Social Security Numbers (SSNs) and credit card numbers, and other user-defined formulae.

Behavioral-Based Classification analyzes the activity information gathered by File Access Manager, and can be used to classify BRs based on the type of users who access the files frequently.

The classification of both content and behavioral data depends upon user-configurable criteria. Classification results can serve as a data source on their own, and can form the basis of queries on the forensics screens (See the chapter on forensics. However, classification results also serve as an additional information layer, associated with activities and permission data.

The classification results layer connects all other layers with data.

The Data Classification module supports using external classification of files in one of the following methods:

- DC Import - importing a spreadsheet into File Access Manager listing files and directories assigned to categories

- Writing to file properties, and creating rules in File Access Manager, assigning categories to files that contain those properties.

These methods can even be used for encrypted files without File Access Manager reading the file content.

## Supported Applications

Data Classification supports the following applications:

| Target System | Products and Supported Versions |
|---|---|
| On-premises File Storage | Microsoft Windows |
| | Microsoft SharePoint |
| | NFS v3/v4 |
| NAS File Storage | NetApp for CIFS |
| | NetApp for NFS |
| | EMC Celerra/VNX/Unity for CIFS |
| | EMC Celerra/VNX for NFS |
| | EMC Isilon for CIFS |
| | Hitachi HNAS |
| | DFS for CIFS |
| | Generic CIFS |
| O365 File Storage | Microsoft OneDrive for Business |
| | Microsoft SharePoint Online (Office 365) |
| Cloud File Storage | Box |
| | Dropbox |
| | Google Drive |
| | Ctera |
| | Azure Files |

## Supported File Types

The privacy engine indexes data, based on a file's content and attributes. The system also supports file properties and custom properties for all supported file types. The privacy engine reads file content, based on the file extension.

Image files can be analyzed and searched for keywords using an optical character recognition (OCR) capability in . This is a resource heavy process, and is configured separately. See section Optical Character Recognition (OCR).

The Data Classification engine supports the following file types /extensions:

| File Extension | Expected file type |
|---|---|
| docx doc xls xlsx ppt pptx | Microsoft Office files |

| File Extension | Expected file type |
|---|---|
| txt csv | Plain Text (including Comma Separated Values files) |
| htm html xml | Web files |
| cs js sql | Code script files |
| pdf | |
| zip gzip tar rar 7zip | Archive files |
| Jpeg jpg tif tiff gif png wmf emf bmp pdf | Image files analyzed by the OCR module* |

The system downloads files from cloud-based content stores and non-CIFS application (for example, Box, DropBox, Google Drive, OneDrive, SharePoint and NFS) to a local directory on the server. Once the indexing process finishes, the system deletes the downloaded files from the indexing server.

## Optical Character Recognition (OCR)

File Access Manager can identify text from within image files either directly, or embedded in other files – such as a scanned driver's license image attached to an MS Word document, or a collection of scans stored in a zip file. Files less than 1000 pixels across will not be scanned, to avoid less reliable results from low resolution images.

The data privacy engine can analyze files containing sensitive data in image form.

> The optical character recognition process is resource intensive, and should be configured carefully taking the runtime into consideration. It is disabled by default.

OCR Capability can be added to the scope selected in the DSAR Scope screen.

### Enabling Optical Character Recognition

By default, optical character recognition is disabled on the entire scope of the DSAR. To enable optical character recognition on a resource, edit the application scope line.

1. Find the desired application from the DSAR Scope screen.

2. Click **Edit**.

3. Click **Optical Character Recognition (OCR)** to enable OCR analysis for this application.

## Classification Architecture and Flow Architecture

The Data Classification content indexing is performed by the Central Data Classification services and their associated Collectors. Architecture has additional information on the possible deployment models and how to scale the Data Classification Collectors to achieve greater speed and performance.

The Central Classification service reads the BRs eligible for indexing and sends them to the Collectors. The Collectors index the files in the received BRs according to the defined data classification policy, and send the results back to the Central Service to be saved in the database.

The Collectors no longer keep a persisted full text index on disk, since all the processing is done in-memory.

# Content Classification Process

The classification processes (run concurrently and independently) include:

- Classification Policy Management and Update

- Running a Content Indexing task

- Querying and Retrieving Results

## *Classification Policy Management and Updates*

Once a Content Indexing task is issued, the Data Classification Engine reads the most updated policy definition. That policy definition will persist through the duration of the Content Indexing task.Any changes made to the policy definition after the Content Indexing task has been started will not be reflected in the current classification process.

## *Indexing Flow*

The classification engine Content Indexing Task:

1. The central service retrieves the BRs to be indexed from the File Access Manager database but only when:

    a. This is the first indexing run of a business resource

    b. The last modified business resource date is more recent than the last business resource indexing date

    c. The business resource is included in the Scope of the Application

    d. The business resource is not contained in a de-duplicated share

    e. If the data classification policy was changed from the last indexing tasks, all the BRs will be re-indexed

2. The central service sends the BRs to the Collectors.

3. The Collector retrieves the list of files in each business resource.

4. Reads the content of each file.

5. Indexes and classifies the file content and sends the results to the Central Data Classification to be saved into the database.

## *Data Classification Deduplication Scan*

In CIFS systems it is possible for multiple shares to point to the same physical address (where they are considered "duplicate shares").

To minimize the running time of the Data Classification task, these duplicate shares are identified, and shared data is scanned only once.

When a user queries the Forensics tab of Data Classification, the classification results are reflected through all duplicate shares.

The following scenario involves four shares in a Windows server:

- Share1 points to D:\

- Share2 points to D:\folder1

- Share3 points to D:\

- Share4 points to E:\

The results of the deduplication scan will be:

- Share1 will be scanned completely.

- Share2 will be skipped, since Share1 contains Share2

- Share3 will be skipped, since Share1 is equal to Share3.

- Share4 will be scanned completely.

When a user queries the Forensics tab of Data Classification, the user will receive the results of all shares.

Limitations and Known Issues:

If the Crawler excludes BRs in contained shares, Data Classification will not classify those BRs.

## Re-Indexing Scenarios

Every data classification policy change will cause all the BRs to be re-indexed on the next indexing task. The assumption is that the policy remains static and unchanged after the implementation and testing phase are completed. File Access Manager provides different features to limit the scope of the indexed BRs to be able to test the policy changes faster, such as Scoping and Run a Specific Resource Classification task.

### *Enabling Optical Character Recognition*

In the case of OCR scanning, *enabling* will cause the next task to re-index the Data Classification. Disabling the OCR capability **will not** initiate re-indexing. This means that once files are marked as sensitive, we can turn off the resource intensive optical character recognition process without removing this indication, until any other filtering setting is changed.

## Classification Types

Data Classification types include:

- Content-Based Classification

- Behavior-Based Classification

### *Content-Based Classification*

The classification engine indexes data, based on file attributes and file contents (for text, office, and PDF files). The classification engine determines the file type by the file extension.

### Data Classification Process Overview

**Content-based**
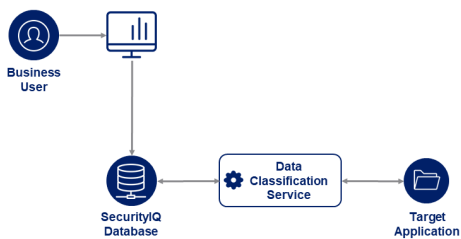
## Behavior-Based Classification

Behavior-Based classification classifies BRs, based on actual user activity.

An example of a Behavior-Based classification rule is:Classify BRs to "Finance" if more than 80% of the activities in the last month were issued by users whose Department is defined as Finance in the Active Directory.
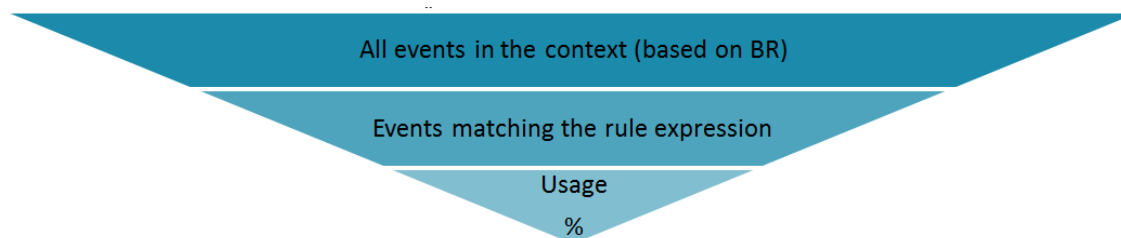


Activities Funnel Calculation

## Imported Classification

Imported classification involves the import of classification results from external data sources, for querying, reporting, and alerting purposes.

See Import Data Classification Results for further details.

## Composite Classification

In order to comply with complex regulations, it is sometimes required to use additional logic with data classification rules, combining the results of several classifications. The Composite Data Classification Rule is based on the File Access Manager categories already classified by the Content and Behavioral rules.

> A Data Classification Policy cannot have both Composite rules and other types of rules.

## File Access Manager Text Search

The Data Classification engine uses Lucene as its primary, text-based optimized database. The Lucene database provides term-based search capabilities, based on the textual content extracted and analyzed from indexed files.

---

To extract textual content from various file types and formats, the classification engine uses a proprietary text extraction library, which is able to extract the file content based on its type. Based on the extracted content, the Lucene indexing service parses and analyzes file content into an index of searchable terms. The full content of the files itself is not saved as part of the index, which allows the index to remain relatively small, highly efficient, and optimized for term-based textual searches.

When the system compares a Content Classification request with the textual index, it parses and translates the various policy rules into term-based search queries. Query results, representing files that correspond to the rules' requirements, consist of file names, extensions, and full path locations, along with other attributes. In certain cases, results may include an actual term or phrase that matches the rule-based query, rather than the full content of the file.

### Regular-Expressions

Regular-expression-based rules involves matching regular-expression patterns with a file during the process of reading the file content, and not comparing the pattern with a term-based index.

### Lucene's Indexing Process

While it parses and analyzes the content data, the Lucene index analyzer eliminates white spaces, certain punctuation characters, and "stop-words" from the content. Stop-words are a predetermined set of frequently used words with diminished semantic significance, such as pronouns and prepositions. Lucene filters stop-words to keep the index manageable, to eliminate "white noise", and to improve search heuristics. Lucene analyzes and tokenizes file content into searchable terms based on the white spaces and stop-words omitted from the original text. The tokenizing algorithm affects Data Classification policy rules.

### Multi-term Phrase-Based Rules

The Data Classification engine allows both single-term keyword searches and multi-term phrase searches. Lucene omits any "stop-word" contained in a multi-term search phrase. For example, a rule containing the phrase "It was the best of times, it was the worst of times", will classify the file containing the entire sentence, as well as any file containing a contiguous phrase, such as "best times worst times". To avoid possible false-positive classification, it is best to restrict multi-term phrase searches to meaningful, contiguous terms.

## Chinese and Logogrammatic Languages

Some scripts, such as Chinese, represent words by symbols (logograms), and a single word may consist of one or more logograms. Furthermore, while most languages use white spaces to separate words, Chinese , as well as other logogrammatic scripts often do not separate words by spaces. The combination of these two phenomena, along with Lucene's omission of white spaces, will cause phrase searches in Chinese (with multiple logograms, separated by spaces) to return positive matches for files containing the same sequence of logograms, regardless of the spaces between them. Thus, a rule containing the phrase *"莕 莚 處贅 �í 轑"*, will classify files containing phrases that consist of these logograms, regardless of spaces. Therefore, the phrases *"莕莚處贅�í轑"*, *"莆莚處贅�í轑"* or *"莆莚 處贅 �í 轑"*, and *"莕 莚 處贅 �í 轑"*, will all be classified by the rule defined above. However, single term keyword searches of words consisting of multiple logograms, and phrases not separated by spaces, will return correct, exact match results: a rule containing the term *"莆莚處"* will only classify files containing that exact term. If more complex phrases are required, a rule containing multiple phrases with the "Contains All" operator, will give the desired results.

# Data Classification Components
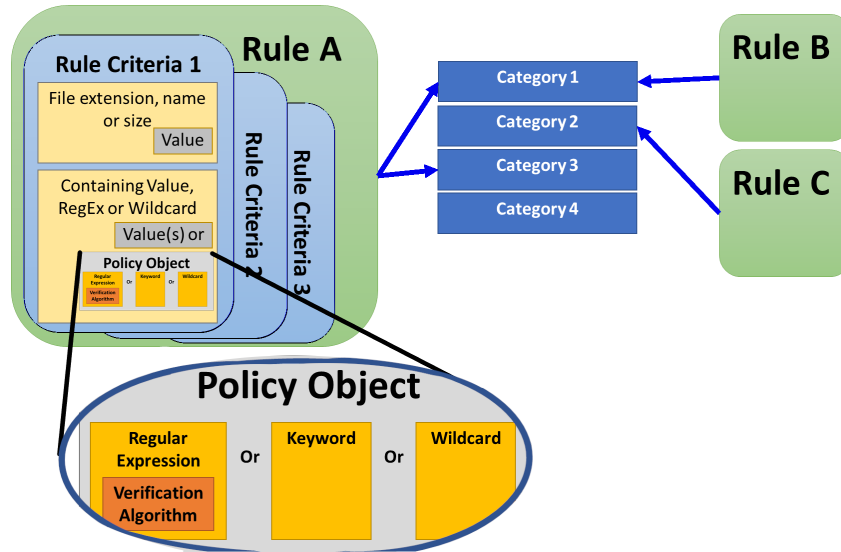
- The Data Classification process assigns **categories** to **business resources** according to **rules**.

  - Rules are composed of one or more rule criteria

Rule criteria consist of finding a match within files to one or more string or pattern.

The strings can be defined as free text, regular expressions, or one stored as a **policy object**.

A regular expression in a policy object may be accompanied by a verification algorithm to further narrow down the search.

> There are policy objects and verification algorithms out of the box for standard searches, or you can create your own to fit your needs.

The classification rule is the main data classification component. Rules also contain subcomponents that complete the rule structure, simplify the rule management task, and provide extended functions.

File properties can be used for classification of files that is performed by the customer manually or using a third party application. File Access Manager will read the metadata on the files, and can use them for data classification rules. This will include reading metadata from encrypted files.

## Data Categories

The data category (the basic component of data classification) is the tag used when a classification rule is satisfied.

To define a data category, open the **Manage Categories** panel from any of the Data Classification screens

For example:

1. Navigate to **Compliance > Data Classification > Policies > Actions > Manage Categories**
   or
   **Compliance > Data Classification > Rules > Actions > Manage Categories**.

2. In the Manage Categories window, type the category name in the "*Add New Category*: section

3. Click **Add**

The system adds a new data category to the "Current Categories" list.Users can edit and delete existing user-defined categories from the Current Categories list. Users can also search categories either by name or by checking the "Show user defined categories only" checkbox.

## Data Classification Policy

The Data Classification Policy is a logical container for data classification rules. For example, all the rules that belong to HIPAA should be located under the HIPAA policy. The system already contains several predefined policies, and users can create additional user-defined policies.

## Rules

Policies set the rules for detecting sensitive data to be protected by compliance regulation or by organizational procedure.

## File Properties

File Access Manager indexes standard attributes, including extension, size, and file name and also index attributes for office files. All the file properties are discovered and created during the indexing process.

1.  In the web client, navigate to **Compliance > Data Classification > Rules > Actions > Manage File Properties**
    or
    **Compliance > Data Classification > Policies > Actions > Manage File Properties** to open the Manage File Properties window.

2.  Type in the file property details.

3.  Check the **Custom Properties** checkbox, if relevant.

4.  Click **Add**.

## Encrypted files

In order to classify encrypted files without File Access Manager reading the file contents, you can tag the files locally according to your classification rules, and use these tags for classification rules (See Local Classification).

## Local Classification

You can use a local classification for files, tagging files with relevant tags. The metadata of the files are uploaded to the File Access Manager database as file properties in the scanning process. These properties can be used to create classification rules manually.

The file properties found will be added automatically to the list of available properties for filtering after the first iteration. In order to have these properties available in the initial run of the Data Classification, add the properties to the property list, as described in File Properties above.
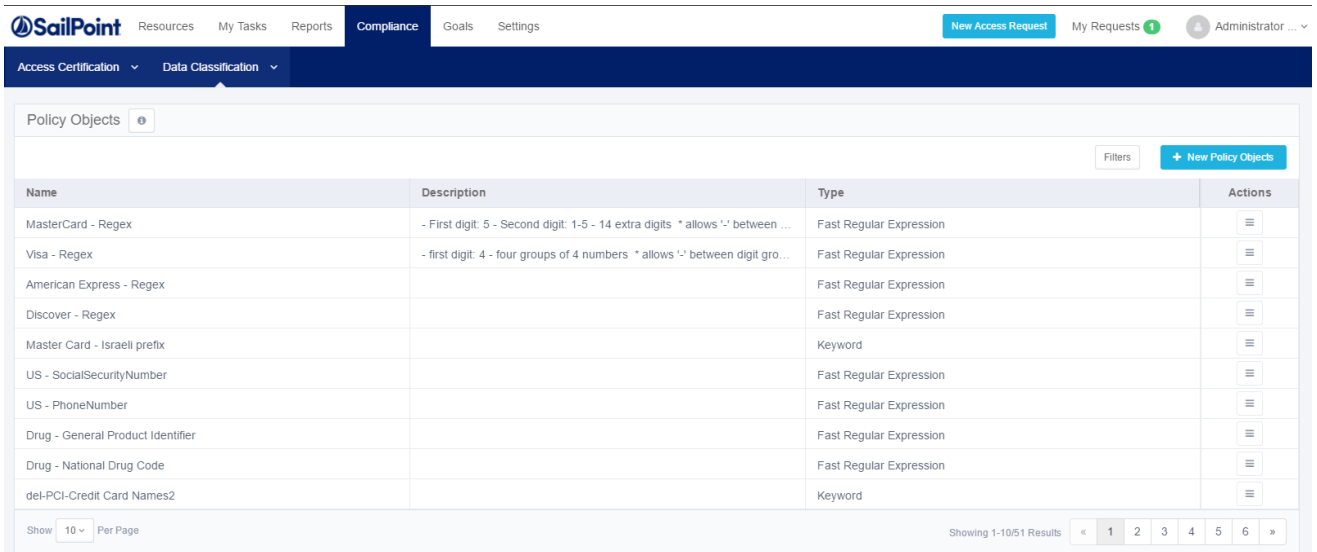
## Policy Objects

Policy objects are searches, saved for use in rules.

For example, predefined policy objects can search for credit cards.
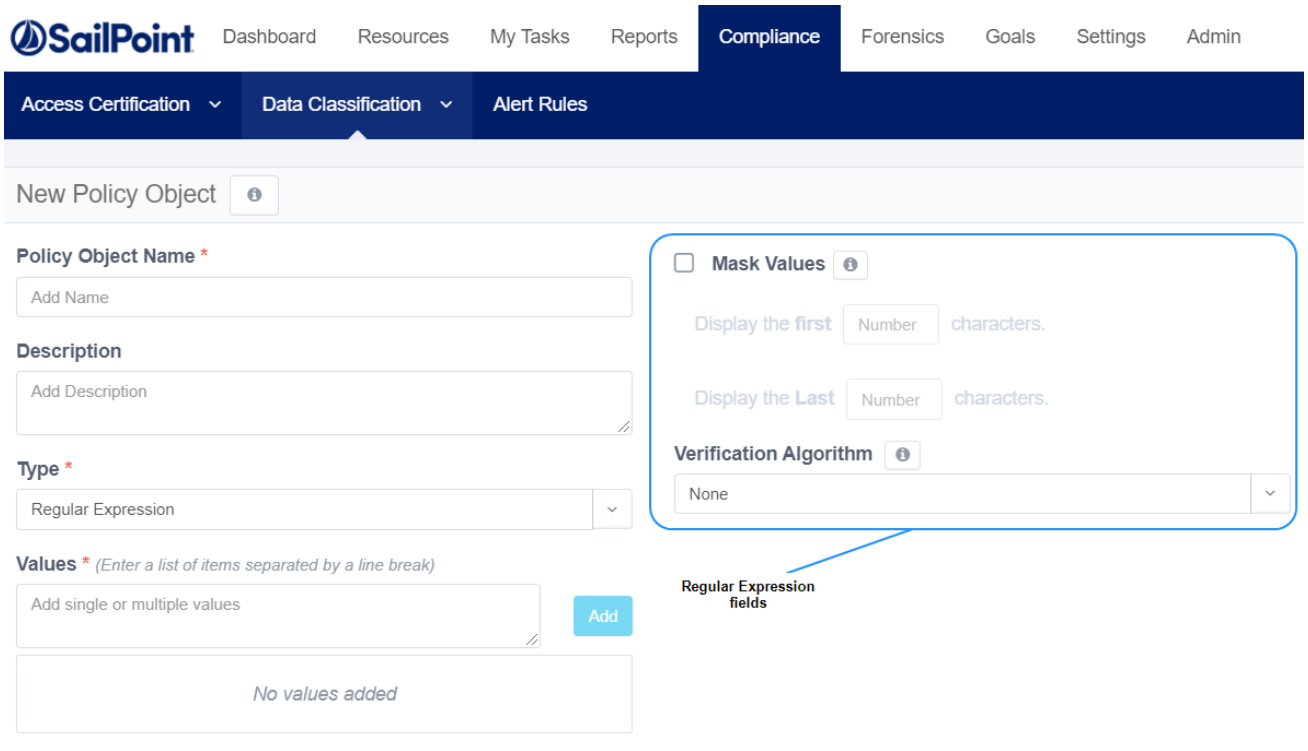
1. Navigate to **Compliance > Data Classification > Policy Objects.** to open the Data Classification – Policy Objects page.



2. Click **New Policy Object** to open the New Policy Object page.



Data classification policy object fields include:

*Policy Object Name*

      Name of the policy object

### Description

Free text.

### Type

The type of search the policy object performs:

#### Keyword

A keyword may be one or more words. If multiple words are involved, the entire phrase will be searched.

Note that stop words such as 'a' or 'and' are stripped from the search keywords. If you want to include stop keywords in the phrase, you can use a regex phrase instead. (For a nerd-level description of ignoring stop words, see https://www.elastic.co/guide/en/elasticsearch/guide/current/stopwords.html)

#### Wildcard

Supports the following special characters:
**\*** any number of characters

**?** only one character

#### Regular Expression

Using standard regex for defining policies

### Values

Values to search for:

- Single Value

- List - A list of matching values

### Mask Values (Regular Expression policy objects only)

Masking portions of matched values.

- **Display the first characters** - Number of characters from the left displayed in the matched value

- **Display the last characters** - Number of characters from the right displayed in the matched value

### Verification Algorithm

A code based algorithm to enable more complex filtering. See Data Classification Verification Algorithms for further details.

Policy objects are a good way to reuse searches containing complex definitions.

Click **Save** to end the New Policy Object process.

# Regular Expressions Within Policy Objects



Regular expressions form the basis for many content pattern searches. File Access Manager uses the *.net regular expression engine* as its underlying engine for regular expressions searches. All regular-expression definitions and searches must conform to the engine's restrictions, limitations, and standards.

When selecting a policy of type Regular Expression, the New Policy Object panel adds the following fields to the New Policy Object panel (See image above).

### Verification Algorithm

A standard, out of the box example, is the Luhn verification algorithm. This algorithm ensures that all phrases classified as credit cards are, indeed, valid credit card numbers (As far as an algorithm can validate without contacting the bank, of course). When selected, this verification will only be run on strings that conform with the credit card regular expression entered, for example:

"^3[47][0-9]{13}$"

See Data Classification Verification Algorithms for a full description on creating verification algorithms.

### Mask Values

By default, the regular-expression matches are saved as part of the results. It is recommended to mask the values of the matches to avoid exposing sensitive data in the File Access Manager database.



### Regex Matching and Case

Please note that regex matching is case sensitive by default. To make a regex ignore case, use the prefix "(?!)"
For example: "home" will find "home", but ignore "Home"
The regex "(?!)home" will find "Home", "HOME" and "HoMe"

### Identifying Line Breaks using Regex in File Access Manager

For parsed files, line breaks are represented by a single CR (\r), instead of (\r\n) or (\n), and therefore not identified by the regex line boundaries ^ and $.

if we take the following regex:

```
(?m)(^|\s)up($|\s)
```

And try to match it with the following text (assuming the line breaks are \r):

```
going

up

up

and away!
```

It will not match anything since the line breaks are not \n as expected by the regex.

In order to identify the start and end of a line, we have to check for the CR explicitly. The issue is that once we identify an end of line character, the cursor has moved past this character, and we can't use this to identify the start of the next line.

If we change the regex to look like this:

```
(\r|\s)up(\r|\s)
```

It's going to match only the first up, since the \r character will be part of the match and thus not part of the evaluation for the next "up".

We need to check the previous and next characters, without moving the cursor.

If we try the following regex:

```
(?<=(\r|\s))up(?=\r|\s)
```

Both "up" strings will be matched. This is because of two modifications:

***(?<=...) positive lookbehind,***

> When there's a match, it moves back to assert whether the regex that replaces "..." is matched, but then discards the match and moves forward to where it was to continue matching.

***(?=...) positive lookahead***

> When there's a match, it moves forward to assert whether the regex that replaces "..." is matched, but then discards the match and moves back to where it was to continue matching.

Combining those two means the match contains only "up" without the preceding or following \r, so they can be used for more matches.

These non-capturing matches are known as zero-length assertions. For more information on lookahead and lookbehind assertions (collectively called lookaround) see https://www.regular-expressions.info/lookaround.html.

***Examples***

> To look for rows starting with "John", you could use: `(?<=\r|^)John.*(?=\r|$)`

> To look for rows ending in "Doe", you could use: `(?<=\r|^).*Doe(?=\r|$)`

# Transferring Data Classification Policies Between Systems

File Access Manager provides an easy way to transfer data classification policies from one system to another, through a command line interface. Administrators can use the import/export tool to import/export custom policies from one server to another.

> Import / Export is only supported between systems running the same version of File Access Manager.

> You must be defined as an Administrator in the File Access Manager administrative client.

> You can only execute the import/export tool in its file working directory.

To run the Import/Export tool, perform the following steps:

1. In the Windows command line, type:

```
cd {path to the tool directory}
PolicyExporter.exe {options}
```

OR

```
PolicyImporter.exe {options}
```

> The tool argument can be a minus sign (-) followed by a letter in upper case, or two minus signs (--) followed by a word in lower case letters.

For example:

```
-U DOMAIN\USER
```

OR

```
--user DOMAIN\USER
```

2. Use the Windows command line to navigate to the following directory:

   % SAILPOINT_HOME%\FileAccessManager\Server Installer\Tools

The tool validates arguments before performing any action, and the system alerts the user if one or more arguments are missing or are invalid. If you do not provide arguments, a Help screen displays.

Each Data Classification Policy is assigned with a unique global ID (GUID). When new policies are imported, File Access Manager compares the GUID's on both policies to identify them uniquely.

> While the name of the tool is Import/Export, the procedural order is to export data classification policies first.

# Exporting Data Classification Policies

Data classification policies are exported with their rules, policy objects, categories, file properties, and rule criteria. The tool transfers an output file to the target server for import. The tool also creates a log file, which File Access Manager technical support team can use as a reference for troubleshooting.

If a policy object includes a verification algorithm created by the user, this dll file will be exported as well.

As noted in Transferring Data Classification Policies Between Systems , you must have administrative rights in File Access Manager and use the file working directory.

To export data classification policies, perform the following steps:

1. Run the tool with the following selected options:

   a. -O, --output (Default: output_policies.bin) (Output file location)

   > The output file is in binary format and cannot be edited.

   The file location can be both either absolute (c:\program files\Sailpoint\outputs) or relative (..\..\outputs).

   b. -A, --all

   c. The tool exports all policies available from current system.

   d. -L, --policies

   The tool exports specific policies (each policy specified by its policy name (not case sensitive) and with a comma separating the name of one policy from the other.

   Policy names that contain spaces ( ), should be in quotation marks (") Example: PolicyExporter.exe -U domain\user -L "policy1 – my policy","POLICY2 – HIS POLICY"

   > Select either -A or -L, since they are mutually exclusive.

   e. -U, --user (Required.)

2. This is the name of the user to whom data classification policies are exported, and should include both the user name and the domain name (if there is one).

   a. -P, --password

   b. The user password validates the export. The system will only prompt you three times to provide a password.

   c. --help

   d. The Help screen displays.

   e. –version
      The version information displays.

# Import Data Classification Policies

Data classification policies are exported with their rules, policy objects, categories, file properties, and rule criteria. The tool creates a file with a summary of what was imported and what was not imported. The tool also creates a log file, which File Access Manager technical support team can use as a reference for troubleshooting.

As noted in Transferring Data Classification Policies Between Systems , you must have administrative rights and use the file working directory.

To import data classification policies, perform the following steps:

1. Run the tool with the following selected options:

   a. -I, --input (Input file location)

   b. The exported output file path

      The file location can be either absolute (c:\program files\Sailpoint\outputs) or relative (..\..\outputs).

   c. -R, --override (Default: false)

      The system recognizes a policy by its unique ID, not by its policy name. Override refers to overriding existing data classification policies and policy rules.

   d. -C, --activate (Default: false)

      Activate refers to activation of all policies immediately after migration.

      > The option to activate supersedes the policy and policy rule association on the exported server - if the option to activate is specified will all be activated, otherwise will all be deactivated.

   e. -O, --output (Default: output_stats.txt)

The output summary file is in the selected location.

The file location can be absolute location (c:\program files\Sailpoint\outputs) or relative (..\..\outputs).

Examples:

--output ..\..\imported.log

-O c:\temp\stats.txt

-T, --test (Default: false)

Any changes made during this simulation of the importation of policies and policy rules are rolled back afterward, so you can see what has been changed without altering any policies or policy rules.

    f.  -M, --multi-output (Default: false)

    g.  The output summary is written in one or more files, with a time stamp appended to the file name.

Example: output_stats.180507091022.txt

> When this option is not used, append the content of the result to the same file, along with the time stamp.

    h.  U, --user (Required).

    i.  This is the name of the user to whom data classification policies are exported, and should include both the user name and the domain name (if there is one).

    j.  -P, --password

2. The user password validates the export. The system will only prompt you three times to provide a password.

    a.  --help

    b.  The Help screen displays.

    c.  –version
       The version information displays.

## Exporting Data Classification Policies

Data classification policies are exported with their rules, policy objects, categories, file properties, and rule criteria. The tool transfers an output file to the target server for import. The tool also creates a log file, which File Access Manager technical support team can use as a reference for troubleshooting.

If a policy object includes a verification algorithm created by the user, this dll file will be exported as well.

As noted in Transferring Data Classification Policies Between Systems , you must have administrative rights in File Access Manager and use the file working directory.

To export data classification policies, perform the following steps:

1. Run the tool with the following selected options:

    a.  -O, --output (Default: output_policies.bin) (Output file location)

> The output file is in binary format and cannot be edited.

       The file location can be both either absolute (c:\program files\Sailpoint\outputs) or relative (..\..\outputs).

    b.  -A, --all

    c.  The tool exports all policies available from current system.

    d.  -L, --policies

The tool exports specific policies (each policy specified by its policy name (not case sensitive) and with a comma separating the name of one policy from the other.

Policy names that contain spaces ( ), should be in quotation marks (") Example: PolicyExporter.exe -U domain\user -L "policy1 – my policy","POLICY2 – HIS POLICY"

> Select either -A or -L, since they are mutually exclusive.

    e.  -U, --user (Required.)

2. This is the name of the user to whom data classification policies are exported, and should include both the user name and the domain name (if there is one).

    a.  -P, --password

    b.  The user password validates the export. The system will only prompt you three times to provide a password.

    c.  --help

    d.  The Help screen displays.

    e.  –version
       The version information displays.

## Import Data Classification Policies

Data classification policies are exported with their rules, policy objects, categories, file properties, and rule criteria. The tool creates a file with a summary of what was imported and what was not imported. The tool also creates a log file, which File Access Manager technical support team can use as a reference for troubleshooting.

As noted inTransferring Data Classification Policies Between Systems, you must have administrative rights and use the file working directory.

To import data classification policies, perform the following steps:

1. Run the tool with the following selected options:

    a.  -I, --input (Input file location)

    b.  The exported output file path

       The file location can be either absolute (c:\program files\Sailpoint\outputs) or relative (..\..\outputs).

    c.  -R, --override (Default: false)

       The system recognizes a policy by its unique ID, not by its policy name. Override refers to overriding existing data classification policies and policy rules.

    d.  -C, --activate (Default: false)

       Activate refers to activation of all policies immediately after migration.

> The option to activate supersedes the policy and policy rule association on the exported server

> - if the option to activate is specified will all be activated, otherwise will all be deactivated.

   e.  -O, --output (Default: output_stats.txt)

The output summary file is in the selected location.

The file location can be absolute location (c:\program files\Sailpoint\outputs) or relative (..\..\outputs).

Examples:

--output ..\..\imported.log

-O c:\temp\stats.txt

-T, --test (Default: false)

Any changes made during this simulation of the importation of policies and policy rules are rolled back afterward, so you can see what has been changed without altering any policies or policy rules.

   f.  -M, --multi-output (Default: false)

   g.  The output summary is written in one or more files, with a time stamp appended to the file name.

Example: output_stats.180507091022.txt

> When this option is not used, append the content of the result to the same file, along with the time stamp.

   h.  U, --user (Required).

   i.  This is the name of the user to whom data classification policies are exported, and should include both the user name and the domain name (if there is one).

   j.  -P, --password

2.  The user password validates the export. The system will only prompt you three times to provide a password.

   a.  --help

   b.  The Help screen displays.

   c.  –version
       The version information displays.

# Creating a Data Classification Policy

Creating a data classification policy involves defining several policy details to make the policy unique. Any new policy can be used as a template and the basis for additional policies.

***To create a new policy:***

1.  In the web client, navigate to **Compliance > Data Classification > Policies > New Policy**.

    A New Policy window displays.

The available Classification Policy fields / buttons that display in this window include:

### Policy Name

Policy names are unique. It is best to create a naming convention that avoids using the same name twice.

### Activate/Deactivate Policy

Users can activate or deactivate a policy using this button

### Owner

The login user is the creator of the policy. (This field is read-only.)

### Description

Free text

2. Users can add existing rules or create a new rule for a policy.

   a. Add an existing rule, using the Add Rule search field.

   b. Click **+New Rule** to add a new rule.

   The rule you added displays in the Rules Assigned list

Users can perform the following actions on rules:

- Activate/deactivate

- Edit (only user-defined rules)

- Remove

3. Click **Save** to save the new policy.

4. The system adds the policy to the Policies list.

***To search for an existing policy:***

1. Navigate to: **Compliance > Data Classification > Policies**

   The Policy window displays.

2. Search for existing policies by typing a name or part of a name in the following search fields:

   - Policy Name

   - OwnerSearch by status by selecting an option from the Status dropdown menu.

3. Fine tune the search even further by selecting an option from the Scope Type dropdown menu or by typing a name or part of a name in the Application Type search field.

4. You can perform the following actions on a selected policy:

   - Activate/deactivate

   - Edit (only user-defined policies)

   - Duplicate

   - Delete (only user-defined policies)

# Content-Based Classification Rules

A Content-Based classification rule specifies file attributes, as well as data patterns within the files, that fit a particular type of data. For example, credit card numbers, driver's license numbers, text files created last month by user X@do-main.com. Each such rule is associated with a category.

## Creating a Content-based Classification Rule

In the process of creating a content-based classification rule, File Access Manager performs an AND operation between each expression. However, some operators act as an internal OR (for example, the IN operator).

To create a Content-Based rule, perform the following steps:

1. Open the rules page

   *Compliance > Data Classification > Rules*

2. Click **+ New Rule** >Content-Based Rule

   A New Content-Based Rule window displays.

   The available Content-Based Rule fields include:

   ***Rule Name (mandatory field)***

   > Rule names are unique. It is best to create a naming convention that avoids using the same name twice.

*Categories*

One or more categories to tag files that meet rule requirements.

To add a new category to the Categories list, click **Manage Categories** and add a new item.

3. In the web client, navigate to **Compliance > Data Classification > Rules > New Rule >** .

4. In the Rule Criteria section, add the general details to the Content-Based Classification rule.

Users can search for existing rules, using filters.

Users can perform the following actions on rules:

- Edit (only user-defined rules)

- Duplicate

- Delete (only user-defined rules)

5. Create an expression and click **Save**.

Users can edit or delete existing rule criteria.

6. Add additional rule requirements as needed.

7. Click **Save** to save the new content-based rule.

The system adds the rules to the Rules list.

# Composite Rule

A composite classification rule lets you combine several rules together to form a more complex criterion. This can include content and behavioral type rules, and is defined by category.

- The data classification matches content or behavioral patterns to rules, and assign categories to resources according to these rules.

- After running data classification, composite rules use combinations of categories to define complex combinations of simple rules

*Examples:*

You can combine Personal Identification Information (PII) in conjunction with health-related information (ICD), to define a rule to identify Personal Health Information (PHI).

or

You can create a rule to list files that have at least two out of one list of categories, and must contain another specific category.

or

Identify all resources that would be defined by rules that belong to category **X**.

To define a composite classification rule, select one or more categories, and the created rule will be triggered for any existing rules within the selected categories.

In the first example above, if we define a rule as follows:

```
Contain at least 2 of  PII, ICD
```

This will add all business resources that fill any of the rules in *PII category*, and any of the rules in *ICD category*.

- The value column allows selecting one or more categories from the category repository.

## Triggering the Composite Rules

- Composite rule tasks are trigger after each data classification task, and evaluate results from that application only.

- The Composite rule runs after of all content and behavioral rules, as it is based on their results.

- If you change a composite rule, this change will take effect only when a new classification task is executed, and triggers the composite rule.

- This task can not be scheduled.

## Creating a Composite Classification Rule

*To create a composite classification rule:*

1. Open the rules page

   *Compliance > Data Classification > Rules*

2. Click **+ New Rule** > Composite Classification Rule

   ***Rule Name***

   Rule names are unique. It is best to create a naming convention that avoids using the same name twice.

   ***Categories***

   Enter one or more categories for the rule

   To add a new category to the Categories list, click **Manage Categories** and add a new item

3. In the Rule Criteria section, add the desired combination of categories to trigger the rule.

   ***Operator***

   Enter the number of concurrence of categories in the business resource tested for this criterion.

   For example, if you went the rule to collect BRs that fit both criteria C1 and C2, set

   Operator: Contain at least 2 of

   Value: C1, C2

   ***Value***

   Enter one or more categories from the search box

4. Click **Save** to save the criterion.

5. Click **+ Add** to add another criterion. All criteria will be combined with an AND operator.

6. Click **Save** to save the new content-based rule.

7. The system adds the rules to the Rules list.

# Data Classification Verification Algorithms

You can use verification algorithms in a Data Classification policy object of type "Regular Expression" to filter the regular expression results. This will enforce additional restrictions and validations on matched phrases. The verification algorithm will take as an input each one of the data classification policy objects' regular expression match result strings, and will remove results that do not meet the criteria defined within the algorithm.

File Access Manager comes with a set of verification algorithms out of the box for standard verifications, such as Luhn, for credit card numbers, or SSN algorithms. In addition, you can write a verification algorithm, upload it to the File Access Manager website, and use it in data classification policy objects.

## Out of the Box Verification Algorithms

Verification algorithms for common rules are pre-loaded in File Access Manager:

- Luhn (Credit Card Number)

- US SSN

- Netherlands BSN

- Israeli ID

- IBAN

- South African ID

The dropdown list of verification algorithms in the Rule Criteria screen includes out of the box algorithms, as well as algorithms uploaded by the user.

## Creating a Verification Algorithm

### *Guidelines*

- The assembly must target .NET Standard 2.1 or .NET Core up to 3.1 These will be referred to as the supported .NET platforms.

- You may write only one implementation class of the IDataClassificationVerifier interface per assembly.

- It is only possible to upload one assembly per verification algorithm. In case your code requires usage of additional referenced assemblies, you must pack them all into one assembly.

> Verification algorithm assemblies written in previous versions of File Access Manager (in .NET Framework 4.5) must be removed, and re-written to target one of the supported .NET platforms as mentioned above, and uploaded again.

## *Walkthrough*

1. Create a new .NET Framework Class Library targeting a supported .NET platform.

2. In your project, add a reference to the assembly FAM.DataClassification.Verifiers.dll. This assembly is provided by SailPoint, and contains the IDataClassificationVerifier interface. This assembly can be downloaded from Compass .

3. Create a new class that implements the IDataClassificationVerifier interface.

4. This class must provide an implementation of the only public method defined in the interface named "Verify". This method takes as an argument a match result string and returns a boolean that denotes if the verification passed or failed.

5. Build your project, and upload the output assembly as described in Verification Algorithms screen

6. This uploaded verification algorithm will now be available in the verification algorithm dropdown list of the Policy Object screen, alongside the other built in or uploaded algorithms.

## *Examples*

Below is an example of code to create a verification dll that verifies that the number passed is even.

```
using FAM.DataClassification.Verifiers;

namespace VerificationAlgorithmExample

{

  public class EvenNumberVerificationAlgorithm : IDataClas-
sificationVerifier

  {

    /// <summary>

     /// Example for a custom verifier that verifies that the input is an
even number

    /// </summary>

    /// <param name="value">A regular expression match result</param>

    /// <returns>True if passed verification, False if failed</returns>

    public bool Verify(string value)

    {

        if (long.TryParse(value, out long parsedLong))

        {

            return parsedLong % 2 == 0;

        }

        return false;
```

```
      }

   }

}
```

# Verification Algorithms screen

### *Description*

The Verification Algorithms table shows the custom verification algorithms uploaded by the users, or as part of a policy upload from another File Access Manager system.
This table does not contain the standard out of the box verification algorithms.

### *Access*

File Access Manager website:

**Compliance --> Data Classification --> Verification Algorithms**

### *Permission*

By default, this page is accessible only to Administrators.



## *Table fields:*

### *Name:*

Verification algorithm name. This name will also appear in the dropdown list of verifications, along with the existing, out of the box verification algorithms.

### *Description:*

Added when the verification algorithm is uploaded

***File name:***

>   The verification algorithm dll file created by the user and uploaded to File Access Manager

***In use:***

>   This flag indicates whether this algorithm is part of a policy object, that is used in an active policy.

***Created by:***

>   The user uploading the algorithm. Verification algorithms that are uploaded to the system using the policy upload tool, will be listed in the verification algorithms list as Created By "Conversion".

See Transferring Data Classification Policies Between Systems for further details on imported policies.

This screen can be used to:

- View custom built verification algorithms.

- See whether an algorithm is in use

- Edit an algorithm details: Update the name, upload a new file or update the description.

- Upload new verification algorithms (See below how to create an algorithm dll),

- Delete verification algorithms.

## *Uploading a New Verification Algorithm*

A new verification algorithm must follow the guidelines below:

- Extension: .dll

- File size: Up to 5 MB

- The verifier name must be unique in the list of verification algorithms.

1. Open the Verification Algorithms panel.

2. Click **+ New Verification Algorithm**.

3. Select **File**.

4. Select a .dll file from your computer.

5. Enter the name and description of the verification algorithm (see description above).

    ***Name***

    >   Verification algorithm name. This name will appear in the dropdown list of verifications, along with the existing, out of the box verification algorithms

    ***Description***

    >   Free text description of the verification algorithm.

6. Click **Save** or **Cancel** to continue.

### *Deleting a Custom Verification Algorithm*

1. Open the Verification Algorithms panel.

2. Click the menu icon on the row of the verification algorithm you want to delete, to open the action menu.

3. Click **Delete**.

> If the algorithm is currently part of a policy object that is used in an active policy, a popup message will warn the user before deleting.

# Data Classification Scope

Use this screen to view and set the scope of applications and resources on which to apply Data Classification policies.

In the web client, navigate to **Compliance > Data Classification > Scope**.



The scope list includes only applications with installed Data Classification. It is only possible to install Data Classification on an application in the administrative client.

The column Optical Character Recognition (OCR) indicates whether the application has OCR activated on part or all part of its resources.

The scope definition directly affects the time required for Data classification indexing.

Activating optical character recognition on resources is a resource intensive process, and should be configured carefully.

For example, to reduce Data Classification indexing, an Administrator can:

- Exclude an application from Data Classification indexing (if "non-sensitive" data is saved by default on that application).

- Include a specific resource (one with very important data) for Data Classification indexing.

You can specify which resources to use (and which to exclude) from a selected application by clicking the Edit button to the right of the application.

While the data classification status (Active/Inactive) can only be changed from the administrative client, non-administrator users can view the status in the Web application.

The Scope definition only takes effect after the next run of the Data Classification task.

Only the business resources of an application selected for editing display on the list.

## Editing the Data Classification Scope

1. Click **Edit** to modify the scope (such as folders), and/or the OCR setting of the Data Classification per application.

2. Find the desired application from the Data Classification Scope screen

3. Click **Edit**.

This will open the Data Classification Scope Edit screen



To change the scope to include in the Data Classification process:

1. Select the scope type.

    - All – Run Data Classification on all the resources in the application

    - Resource – select from a list of resource to include

To exclude resources from the Data Classification process:

a. Click **Add Exclusion** to open the exclusion entry field

b. Select resources to exclude from the dropdown list

To remove the exclusion of resources from the Data Classification process:

a. Click **Remove Exclusion**.

To enable OCR

a. Click **Optical Character Recognition (OCR)** to enable / disable OCR analysis for this application.

b. Select the resources to exclude from the OCR analysis from the drop down resource tree.

> All resources selected in the Data Classification scope will include all subfolders (or parallel resources, per application) as well. The checkbox "Including subfolders" cannot be unselected.

> Changes to the scope or activating the OCR on an application will trigger a re-indexing in the next run of the Data Classification task.

> Deactivating OCR on an application will not trigger re-indexing.

Section Selecting Scope for Alert Rules has additional information on scope inclusion and exclusion.

Data Classification Verification Rules

# Run Resource Classification

Use this feature to run the Data Classification process on a specific business resource, rather than on an entire application. You can test the Data Classification process faster, since you will only be testing a single resource. In addition, you can run Data Classification faster on a single sensitive resource (for example, one on which many changes were made), than on multiple resources.

To run Resource Classification, perform the following step:

Navigate to **Compliance > Data Classification > Policies or Rules > Actions > Run Resource Classification**



# Creating a Behavioral-based Classification Rule

> You must enable the "Classify behavioral rules" task in order to run behavioral based rules

In the process of creating a content-based classification rule, File Access Manager performs an AND operation between the expressions. However, some operators act as an internal OR (for example, the IN operator).

***To create a Behavioral-based rule:***

1. Open the rules page

   *Compliance > Data Classification > Rules*

2. Click **+ New Rule** > Behavioral Based Rule

   ***Rule Name***

   > Rule names are unique. It is best to create a naming convention that avoids using the same name twice.

   ***Categories***

   > Enter one or more categories for the rule

   > To add a new category to the Categories list, click **Manage Categories** and add a new item

3. Behavioral Requirements for Rule specifies the threshold and timeframe for categorizing BRs according to the users accessing these files. An example of a threshold configuration is: "at least 25% of the users with activities on files in this folder are members of the Finance department."

   Behavioral requirements for rule

   This pattern should match **at least** | 15 | % of the activities over last | Day | ⌄ | *(Valid values for % of activities are whole*

4. Define the timeframe and required usage:

   - *Value* - Percentage required to meet the rule.

   - *Timeframe* - The timeframe during which to check the rule

5. In the Rule Criteria section, add the general details to the Behavioral Based Classification rule.



6. Select an Attribute, an Operator, and a Value (optional) from the dropdown menus.

7. Create an expression and click **Save**.

> Users can edit or delete existing rule criteria.

8. Add additional rule requirements as needed.

9. Click **Save** to save the new content-based rule.

10. The system adds the rules to the Rules list.



## Scheduling Classify Behavioral Rules Task

The Classify Behavioral Rules task is a global scheduled task. It is created out of the box, and is disabled by default. This task runs on all scope on supported applications.

All applications, besides the ones listed below, support the classify behavioral rules task.

| Application | Reason |
|---|---|
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

To schedule the Classify Behavioral Rules task:

1. Navigate to **Settings > Task Management > Scheduled Tasks**.

2. Select the task Classify Behavioral Rules on the Scheduled Tasks table on the tickbox on the task row. This will open the options buttons.

3. Click **Edit** to open the scheduling edit panel.

4. Set the task to active / inactive.

5. Change the scheduling parameters as required.


# Import Data Classification Results

To import external data classification results, select the data source that contains the results. This data source must have the following fields:

- Category
- Application name
- Full path
- File name

An additional field - **match count** - is optional.

> The final content of the data classification table might contain duplicate categories, if the import process, and data classification process contain identical categories. These are added as additional lines in the table.

To import data classification results from other data sources:

1. Open the File Access Manager website

2. Navigate to **Compliance > Data Classification > Policies**
   or
   **Compliance > Data Classification > Rules**

3. Click the **Actions** menu > **Import Data Classification results**

4. Configure the import fields by mapping the data source filed to the File Access Manager fields.

> The import task will import the match count from the external source, in addition to the fields of the categories. The match count field is imported as a number. If the field mapped to Match Count is empty, or is not a number, the process will load a null into this field.Set a schedule for refreshing the database from the external source.
> The schedule can be any of the following frequency types:

- Once

- Daily

- Weekly - default value

- Monthly

5. Click **Save** to store the field mapping and scheduling.

To follow the task progress, go to **Settings > Tasks Management > Tasks >** "Value from the Scheduled task name field" task.

To cancel the setup of the import, close the window.

# Data Classification Results

## Data Classification Results – Report

File Access Manager provides reports of data classification results. You can filter the results be various parameters, including a "match count" – having a certain sensitive category at either more than, or less than a given threshold.

To generate data classification report, perform the following steps:

1. In the web client, navigate to **Reports > Report Templates**.

2. Use the **Classified Data** tag to locate a specific report.

3. To apply a different filter than one of the existing templates:

    a. Create a duplicate template by selecting **Duplicate** from the template drop down menu

    b. Set the filter parameters, and **run now** or **Save** the template for future runs.

4. The report will be available in the **My Reports** screen.

# Data Remediation Policy

A Data Remediation policy is a set of policy rules, which govern actions that are run on the basis of the Data Classification process results.

Each File Access Manager deployment has a data remediation policy that spans all the deployment's applications.

Each Data Remediation rule consists of:

- Categories - the data classifications of a file that triggers the specific rule

- Scope - whether the rule should be triggered by application, by application type, or should not be limited by either [unlimited]

- Script path - The path to a script to be executed on the files that match this category.

> The script must be written in PowerShell and can accept both the filename and the category as parameters, and return an error message in case it fails.

A Data Remediation script is executed on a file that matches one of the Data Remediation rules. Each rule can run a single script.

The Data Remediation scripts are executed by the installed Application's Data Classification service. The service periodically queries the database for new scripts which are pending for execution, and in turn executes them and writes the execution results to the logs.

You can track the execution of the Data Remediation rules by generating log reports.

To set a Data Remediation Policy:

1. Navigate to **Compliance > Data Classification > Data Remediation**

**Data Remediation Rules** ⓘ                      Generate Report    **New Rule**

| Name | Description | Categories | Scope | Script | Run Once | Actions |
|------|-------------|------------|-------|--------|----------|---------|
| Remove unused HR... | Remove policies that rem... | Confidential | Win01 | \\Example.com\C$\... | Yes | ✎  🗑 |

2. The data remediation has the following options:

    a. **Generate Report**: Run or schedule a report based on the remediation rules, according to the requested time period.

    b. **New Rule**: Create a data remediation rule

    c. Each Data Remediation line has the options **Edit** and **Delete**.

## Create a Data Remediation Rule

To set a new Data Remediation rule:

1. Navigate to **Compliance > Data Classification > Data Remediation**

The New Data Remediation Rule screen displays.



2. Fill in the following fields:

- *Rule Name* (mandatory)

- *Description*

- *Categories* – Select at least one category from the dropdown list.

- *Script Path* - the path to the PowerShell script to run. Since the script is executed by the data classification service, the path must be relative to the server in which the data classification service is installed. If this action will be run by multiple data classification services serving different applications, all services must be able to access the path.

- *Scope Type*: Select the scope to apply to the rule by selecting one of the following:

    - All (default)

- Application Type

- By Application

- *Application*: Select one or more applications by marking the tickboxes in the dropdown list.

- *Application type*: Select one or more application types by marking the tickboxes in the dropdown list.

- *Frequency*: Select an execution interval.

- Run Now - one time run.

- Run now and Every X Hours - the default is 24 hours. Set an interval between 1-99 hours.

3. Click **Save & Run**, or **Cancel**.

## Edit a Data Remediation Rule

To edit a Data Remediation rule:

1. Navigate to **Compliance > Data Classification > Data Remediation** [Select policy] **Edit Rule icon**.

2. The Edit Data Remediation Rule screen displays. Follow the steps described above.

3. Click **Save & Run** or **Cancel**. If you click **Save & Run** at any stage of editing a data remediation rule, it will cause the assigned actions to execute immediately. This is true even if no changes were made.

## Delete a Data Remediation Rule

To delete a Data Remediation rule:

Navigate to **Compliance > Data Classification > Data Remediation** [Select policy] **Delete Rule icon**.

## Log Reports

You can track the execution of the Data Remediation rules and actions by generating log reports.

To view Data Remediation reports navigate to **Compliance > Data Classification > Data Remediation**.

1. Click the **Generate Report** menu option. This will open the report dialog box.
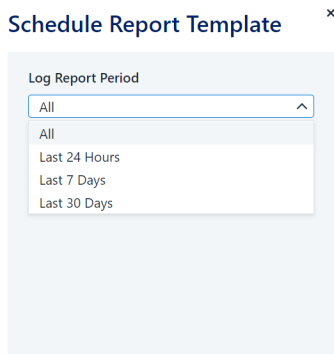


2. Click **Produce Now** to produce the report now, or click **Schedule a New Report** to schedule the report.

3. If you selected Schedule a New Report in the previous step, select one of the following scheduling options:

a.  Last Day

b.  Last 7 Days

c.  Last 30 Days

d.  All

## Writing a PowerShell Script for Data Remediation

The File Access Manager administrator must provide a path to a valid script to perform the desired action.

That script must be written in PowerShell and return either nothing (or an empty string) to indicate success, or a string message to specify an error in case of failure.

The script receives 2 parameters when its executed:

- A string which represents the full path of the file upon which the action should act

- A string which represents the category which caused the action to be executed

Any credentials needed for the script to operate must be provided within the script.

# Access Certification (Campaigns)

*Access Certification* is the process of verifying that the list of users and groups of users who currently have access to a particular resource should have access to that resource.

Access Certification is performed by means of running campaigns, which match resources with users who have access to these resources, and sending these to reviewers for approval.

Define the review in the File Access Manager Administrative Client

A user can create a new campaign to certify permissions or identities, create a new campaign template, or use an existing campaign template to create new campaign. It saves a user time and effort to use a campaign template for recurring or scheduled campaigns, or to make small changes to the general configuration of a campaign. A user can also create a campaign template from an existing campaign for reuse in another campaign.

Access Certification includes the following steps:

1. Determine the identities / permissions to be certified.

2. Determine the review process to use.

3. Create an Access Certification Campaign.

## Create Campaign

Compliance managers and administrators can create an Access Certification campaign, with or without an Access Certification template.

***Creating an Access Certification campaign without an Access Certification template***

1. In the web client, navigate to **Compliance > Access Certification > Campaign Management**.

2. Click **+ New Campaign**.

3. The Create Campaign screen displays, and includes the following steps:

    a. General Details

    b. Filter Selection

    c. Review Process

    d. Summary

e. Save
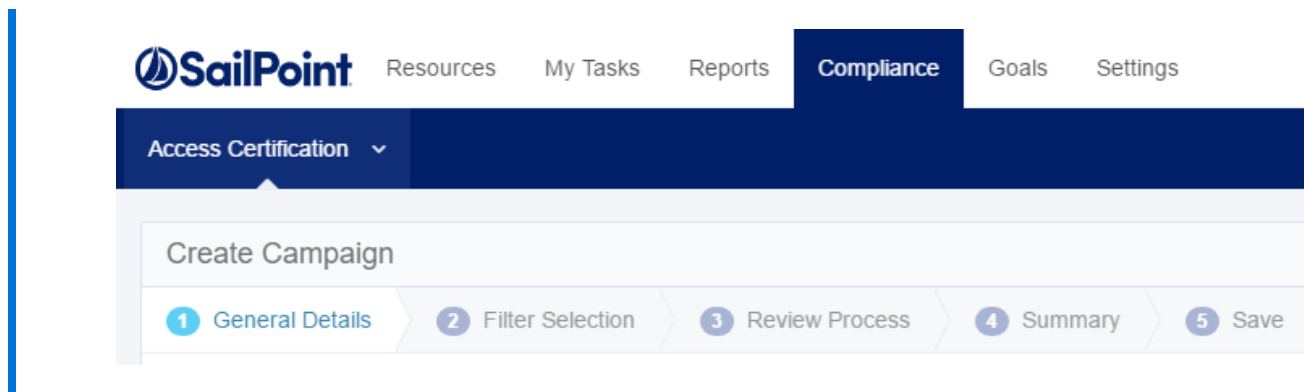


An asterisk after the name of a field marks it as mandatory.

4. In *General Details*, type or select the relevant data in the following fields:

### *Name*

Enter the name of the campaign. This is a mandatory field.

### *Description*

Enter a description of the campaign.

### *Instruction to Reviewers*

This instruction text will display to the reviewer in the approval screen. It can also be used in the campaign email templates.

### *Duration*

Select "Days", "Weeks", or "Months" from the dropdown menu, and type in the relevant number of days, weeks, or months. This is a mandatory field.
The system sets the due date of a campaign, based upon the campaign duration. The due date is the recommended end date of a campaign, although the campaign does not end automatically on that date.

> If the access certification / access revoke request was created from a filter defined with a classification category, the classification category column is displayed in the access certification / access revoke request .

5. Click **Next**

6. The *Filter Selection* tab is highlighted and the tab fields display.

7. In *Filter Selection*, type or select the relevant data in the following fields:

### *Filter Type*

Select a filter type (All, Permissions, or Identities) from the dropdown list.
You can update the filter selection in the administrative client (if you have permission to do so), and then click **Refresh**.

### Filter List

Select a filter from the dropdown list.

(Some of the filters are predefined, out-of-the-box Permissions and Identities filters.)

### Filter Definition

The displayed filter definition is based on the administrative client definitions.
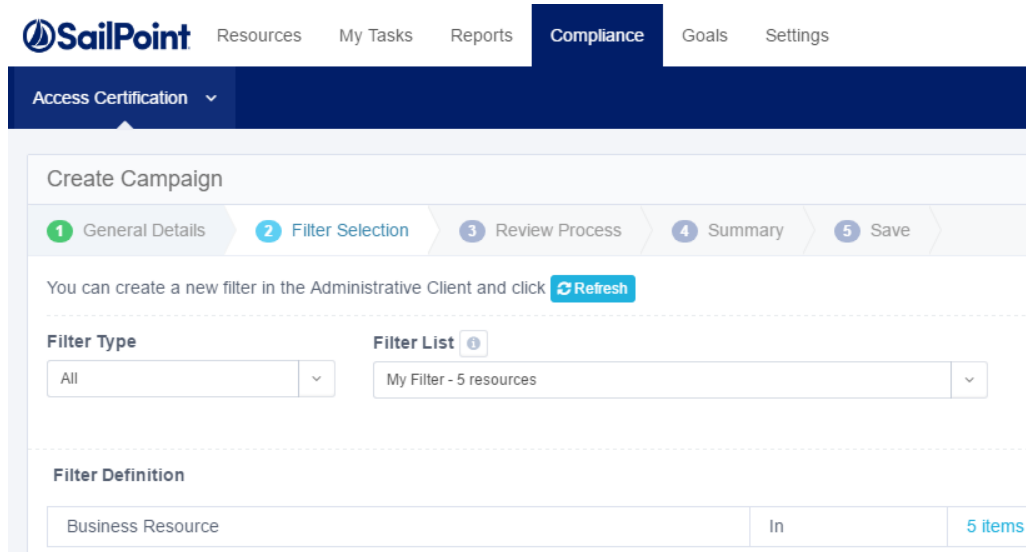


If there are several items included in the definition, click on the number of items (for example, "5 items".



8. Click **Next**

9. The *Review Process* tab is highlighted and the tab fields display.

The predefined review process sources are "By Data Owner" or "By Selected Reviewer(s)". If you select "By Data Owner", the review process is only available for Permission type filters.

10. In *Review Process*, type or select the relevant data in the following fields:

### Source

Select a source (All, Predefined, or Custom) from the dropdown list.

### Review Process

Select a review process from the dropdown list. (The processes available depend upon the Source you selected.)

You can update the review process list in the File Access Manager administrative client (if you have permission to do so), and then click **Refresh**.

### Type of Account

Select either "User Account" or "Group Account" from the dropdown list.

This option is only displayed if you chose the "By Data Owner" review process or the "By Selected Reviewer(s)" review process

### Default Reviewer(s)

This option is only displayed for the "By Data Owner" predefined review process, since default reviewers are the reviewers when no data owner was found.

-OR-

### Selected Reviewer(s)

This option is only displayed for the "By Selected Reviewer(s)" predefined review process to set a static list of reviewers. You can choose multiple users or groups.

11. .Click **Next**

The **Summary** tab is highlighted and its fields display.

12. In *Summary*, you can view a summary of your Create Campaign selections in the following fields:

- Campaign Name

- Campaign Duration

- Filter Selected

- Review Process

When a campaign is complete, no records will display. Only when a campaign is in progress, will a record display.

This view is available for a predefined review process. Click on the dropdown list to display the selected reviewer(s).

- Fulfillment Process – Click **Edit** to edit this selection. In the *Edit* screen, select:

    a. **None** or

    b. **Fulfill Permissions Revoke Requests**. This will open the fulfillment process panel.

An access revoke request is created at the end of the campaign if any records were rejected. This request contains all the permissions that the campaign reviewers revoked. To review the access revoke request, select "**Access revoke request should be reviewed**".

- Manual Fulfillment Review Process – If an access request involves non-managed resources and identifies, a one-step review process is assigned to be fulfilled manually.



- Display Columns – Click on the dropdown list to display the selected columns. Click "Edit" to edit this selection. The columns available are based on the filter selected in Step 2. Therefore, if the filter has changed, the columns will also change accordingly.

    a. To add columns in the *Edit* screen, type free text in the *Add Display Columns* field.

    b. To delete items in the *Edit* screen, click the "x" to the right of the name of a display column in the fields under *Current Display Columns*.

    c. To change the order of items in a column, drag and drop the items to the desired location

in the column.
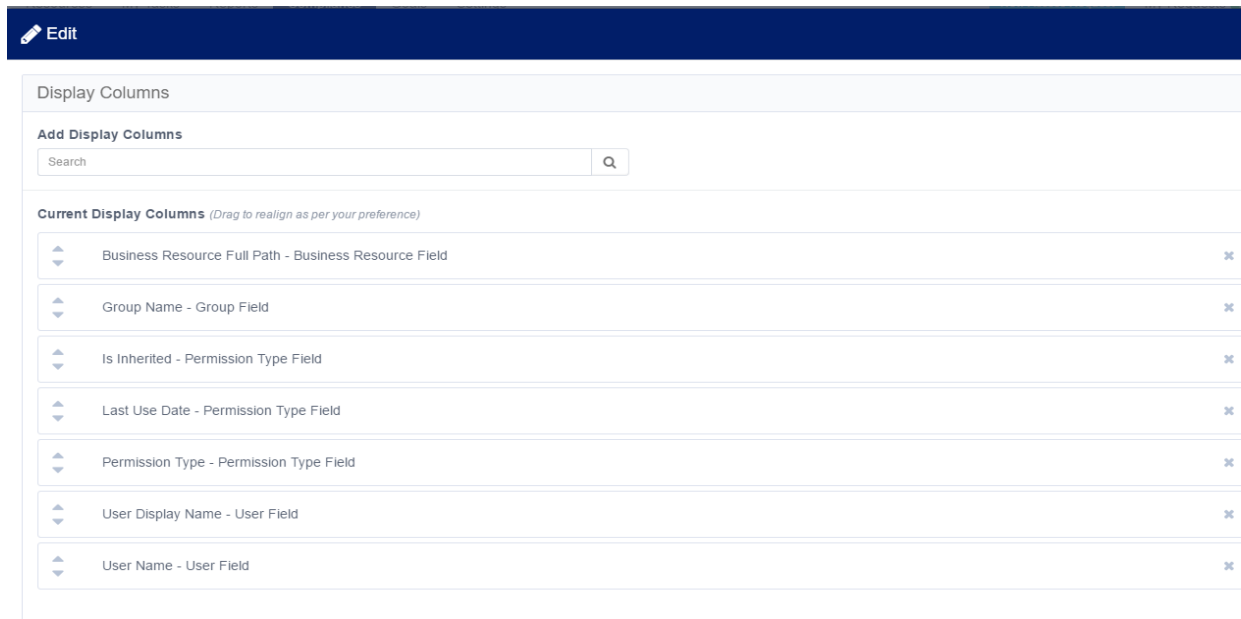


- Campaign Invitation – Click **Edit** to edit this selection.

In the Edit screen, click **Use email template from setting screens (recommended)** or **Custom Email** to create an email that differs from the default email.
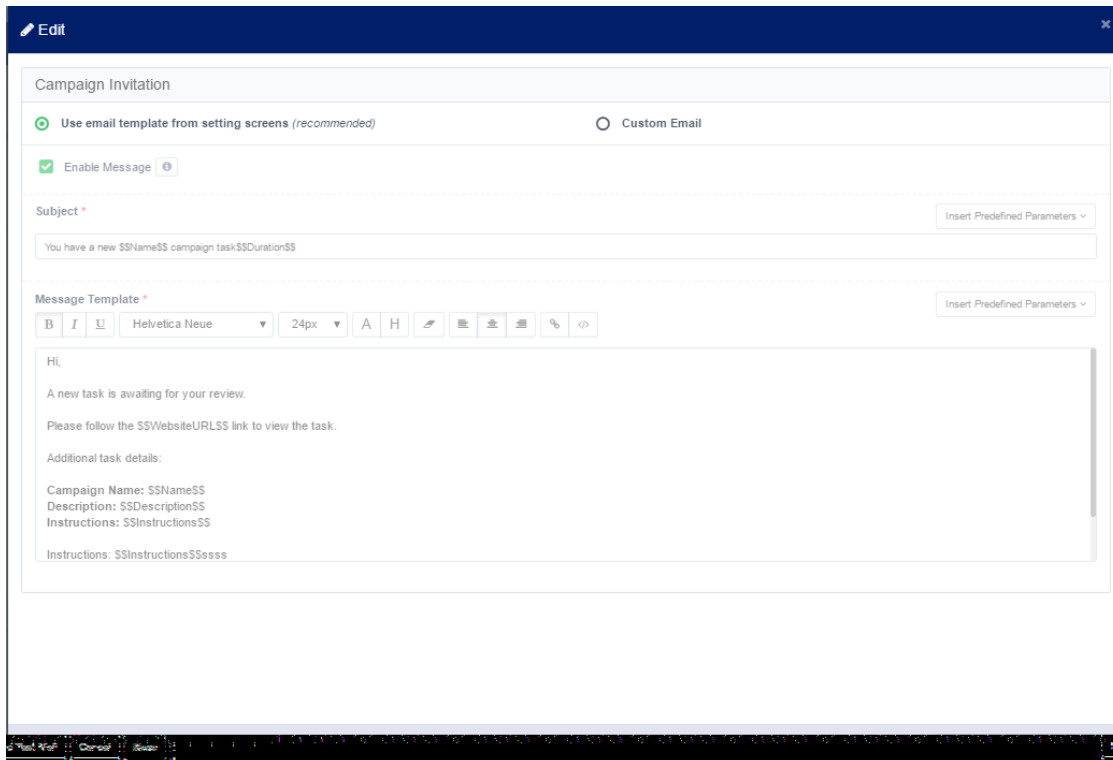
- Reminder Emails – Click **Edit** to edit this selection.
  In the *Edit* screen, click **Use email template from setting screens (recommended)** or **Custom Email** to create an email that differs from the default email.

- You must select the days and the time of day to send weekly reminders.
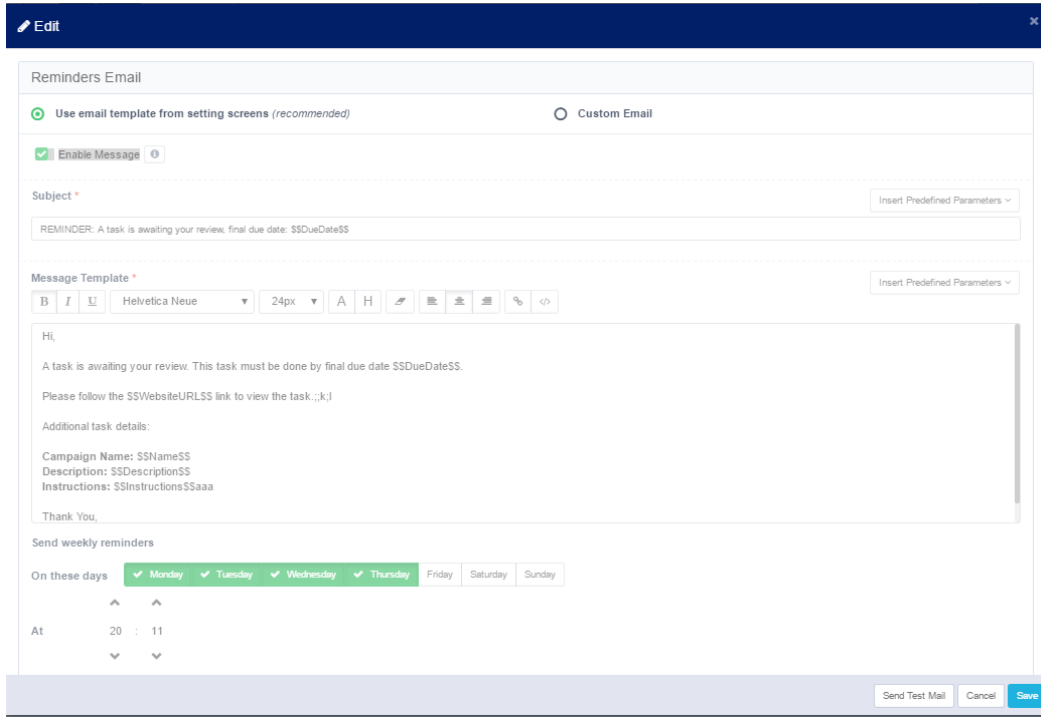


13. When you have completed all edits, click **Next**.

14. The *Save* tab is highlighted and the tab fields display.

Select one of the following options under **Scheduling Campaign**:

> ***Save & run manually***

> > Run the campaign when you choose after the campaign has been created and is ready to run, or

> ***Save & run automatically***

> > Run the campaign after it has been created and is ready to run.

If desired, check the "Save as template & add schedule recurrence" checkbox.

1. You may create a campaign template with or without a scheduler. Also, you may either run the template-created campaign automatically after creating the template, or you may run it manually in the future.

2. Click **Save**.

3. An Information pop-up window displays to indicate that the campaign has been saved successfully, and a task is created to create the campaign, itself. A "Campaign Management" link displays to redirect you to a screen to view the campaign. Alternatively, you can view the campaign by navigating to **Compliance > Access Certification > Campaign Management**.

4. Click **Close**.

# Campaign Templates

Compliance managers and administrators can manage campaign templates by selecting one of the following actions:

- Create a new template

- Edit an existing template

- Duplicate an existing template

- Delete an existing template

- Create a campaign, based on an existing template

The templates display from left to right, row by row, sorted chronologically by date of template creation.

| Campaign Templates | | |
|---|---|---|
| Filters | | + New Template |
| **aaa** ☰ | **GDPR Data Access Review Template** ☰ | **Sharon Test1** ☰ |
| Template Type: Permissions | Template Type: Permissions | Template Type: Permissions |
| Description: iiii | Description: GDPR Data Access | Description: Sharon Test1 |
| Owner: Me | Owner: isabella very long display name12132324243434534354545454... | Owner: isabella very long display name12132324243434534354545454... |
| Created on: 5/23/2017 | Created on: 5/22/2017 | Created on: 5/22/2017 |
| Create Campaign | Create Campaign | Create Campaign |
| **Test campaign - doc Template** ☰ | **office-users-password-never-expired** ☰ | **Copy of with temp Template** ☰ |
| Template Type: Permissions | Template Type: Identities | Template Type: Permissions |
| Description: | Description: | Description: qqq |
| Owner: Me | Owner: Me | Owner: isabella very long display name12132324243434534354545454... |
| Created on: 5/9/2017 | Created on: 4/30/2017 | Created on: 4/24/2017 |
| Create Campaign | Create Campaign | Create Campaign |

You can filter the display of current templates to find the templates more quickly.

To filter the available campaign templates, perform the following steps:

1. Click **Filters**.

2. Under *Filters*, type or select the relevant data in the following fields to narrow your search of campaign templates:

    ***Template Name***

    Type the first letter or letters of the template name, and then click "**Search**" next to that field.

    ***Owner***

    Type the first letter or letters of the owner (user), and then click "**Search**" next to that field.

    ***Type***

    Select "All", "Permissions", or "Identities" from the dropdown menu.

## Create a New Template

To create a new Access Certification template, perform the following steps:

1. In the web client, navigate to **Compliance > Access Certification > Campaign Templates**.

2. Click **+New Template**.

3. The Create Template screen displays, and includes the same steps (in order) as described in Create Campaign:

   ***General Details***

   > This step has the same fields as the Create Campaign step, except that the name field is for a template (not a campaign), and the description field is for a template (not a campaign).

   ***Filter Selection***

   > This step has the same fields as the Create Campaign step.

   ***Review Process***

   > This step has the same fields as the Create Campaign step.

   ***Summary***

   > This step has the same fields as the Create Campaign step.

   ***Save***

   > The Save fields displayed in the "Create Template" process differ from the Save fields displayed in the "Create Campaign" process.

4. Follow the process steps described in Create Campaign:, from *General Details* to *Save*.

5. When you reach the *Save* step, the *Save* tab is highlighted and the tab fields display.

6. You may save the template with or without a schedule.

   a. Save the new template without a schedule by leaving the "Enable Schedule" checkbox unchecked, or

   b. Save the new template with a schedule by checking the "Enable Schedule" checkbox, and then type or select the relevant data in the following fields:

   ***Frequency Type***

   > Select "Monthly" or "Yearly" from the dropdown menu.

   ***Starts On***

   > Click on the calendar icon to the right of this field and select a start date from the calendar that displays.

   ***Ends On***

   > Select either the **Never** or the **On** radio button.

   > If you want the selection to be available indefinitely, select **Never**, and the end date selection will not be enabled.

If you want the selection to be available for a set period, select **On**, then click on the calendar icon to the right of this field, and select an end date from the calendar that displays.

> The new campaign will be created from the "Starts on" date to the "Ends on" date, based on the selected frequency and interval in months or years.

*Interval Of*

Type the number of months or years (depending upon your "Frequency Type" selection above) to indicate how often you want to schedule the template.

*Summary*

This field is a display that summarizes the selections you made in the previous fields (for example, "every 2 months on [start date] until [end date]).

*Time*

Use the up and down arrows to select a schedule time, based on the 24-hour clock (for example, 1:05 p.m. displays as 13:05).

   c. Run the campaign manually, and not per the schedule you just set, by leaving the "Campaign will run automatically on the set schedule" checkbox unchecked,

   or

   d. Run the campaign automatically on the set schedule by checking the "Campaign will run automatically on the set schedule" checkbox.

> All campaigns created from this template that are set to run automatically will continue to run until they are reset manually.

7. Click **Save**

8. An Information pop-up window displays to indicate that the template has been saved successfully, and a task is created to create the template. A "Template Management" link displays to redirect you to a screen from where you can view the template. Alternatively, you can view the campaign by navigating to *Compliance > Access Certification > Campaign Management*

## Edit an Existing Template

To make changes to an existing template - edit the template.

To make a new template, based on an existing template with some changes - duplicate the template.

*Editing an existing Access Certification template*

1. In the web client, navigate to **Compliance > Access Certification > Campaign Templates**.

2. Select a template from the displayed templates.

3. Click **Menu** on the top right of the selected template.

4. The Edit, Duplicate, and Delete options display.

5. Click **Edit**.

6. The Edit Template screen displays, and includes the same steps (in order) as the Create Template screen:

    a. General Details

    b. Filter Selection

    c. Review Process

    d. Summary

    e. Save

7. Review each step and make any relevant changes.

8. Click **Next** to proceed to the next step, or click **Previous** to return to the previous step.

9. When you click **Save**, an information pop-up window displays to indicate that the template has been saved successfully.

10. Click **Close**.

### Duplicating an Existing Template

To duplicate an existing Access Certification template:

1. Navigate to *Compliance > Access Certification > Campaign Templates*.

2. Select a template from the displayed templates.

3. Click **Menu** on the top right of the selected template.

4. The Edit, Duplicate, and Delete options display.

5. Click **Duplicate**.

6. The Duplicate Template screen displays, and includes the same steps (in order) as the Edit Template screen.

7. Review each step and make any relevant changes.

8. Click **Next** to proceed to the next step, or click **Previous** to return to the previous step.

9. When you click **Save**, an information pop-up window displays to indicate that the template has been saved successfully.

10. Click **Close**.

11. The duplicated template will be the newest template in the Campaign Templates display, and will have the same name as the original template, with "Copy of" before the name.

### Deleting an Existing Template

If you no longer need a template, you can delete it. Once deleted, it cannot be recovered.

***To delete an existing Access Certification template***

1. Navigate to *Compliance > Access Certification > Campaign Templates*.

2. Select a template from the displayed templates.

3. Click **Menu**" on the top right of the selected template.

4. The Edit, Duplicate, and Delete options display.

5. Click **Delete**.

6. A question pop-up window displays, asking if you are sure you want to delete the template.

7. Click **Yes** to delete the template, or click *No* to retain the template.

8. If you created campaigns using a template, you cannot delete that template without first deleting the campaigns from which it was created. If you attempt to delete the template, a notification will display those campaigns, requesting that you delete them before you delete the template.

## Create a Campaign

To create an Access Certification campaign, based upon an existing Access Certification template:

1. In the web client, navigate to **Compliance > Access Certification > Campaign Templates**.

2. Select a template from the displayed templates.

3. Click **Create Campaign** on the bottom left of the selected template.

4. The *Create Campaign* screen displays, with the General Details step displayed automatically.

5. In *General Details*, type or select the relevant data in the following fields:

   *Name*

   > Enter the name of the campaign. This is a mandatory field.

   *Description*

   > Enter a description of the campaign.

   *Instruction to Reviewers*

   > This instruction text displays to the reviewer in the approval screen. It can also be used in the campaign email templates.

   *Duration*

   > Select "Days", "Weeks", or "Months" from the dropdown menu, and type in the relevant number of days, weeks, or months. This is a mandatory field.
   > The system sets the due date of a campaign, based upon the campaign duration. The due date is the date on which it is recommended that a campaign should end, but the campaign does not end automatically on that date.

6. Click **Next**.

7. The *Save* step displays.

8. Under Scheduling Campaign, click one of the following options:

   *Save & run manually*

   > This option saves the campaign for you to run manually in the future.

   *Save & run automatically*

This option saves the campaign, and runs it automatically when the template was set to run (in the Create Template or Edit Template steps).

9.  Click **Save**.

10. An Information pop-up window displays to indicate that the campaign has been saved successfully, and a task is created to create the campaign. A "Campaign Management" link displays to redirect you to a screen to view the campaign.

You can see the campaigns and campaign statuses on the *Campaign Management* screen

# Campaign Management

*To manage existing campaigns*

Navigate to **Compliance > Access Certification > Campaign Management**.



The campaigns display from left to right, row by row, sorted chronologically by date of campaign creation.

You can filter the display of campaigns for easier viewing.

*To filter the available campaigns:*

1.  Click **Filters**.

2.  Under *Filters*, type or select the relevant data in the following fields to narrow your search of campaigns:

    *Campaign Name*

    Type the first letter or letters of the campaign name, and then click "**Search**" next to that field.

    *Owner*

Type the first letter or letters of the owner (user), and then click **Search** next to that field.

- *Status*

    The dropdown list contains the following options:

    - Created

    - In Process

    - Completed

    - Pending Re-initialization

    - Pending Deletion

    - Pending Creation

    - Deletion Failed

    - Pending Review In Process

    - Pending Completion

    - Creation Failed

*Type*

Select "All", "Permissions", or "Identities" from the dropdown menu.

*Due Date*

Select "All", "Overdue", "Due Today", "Due in 7 Days", or "Define Range" from the dropdown menu.

| Campaign Management | | | | | |
|---|---|---|---|---|---|
| Filters | | | | | |
| **Campaign Name** | **Owner** | **Status** | **Type** | **Due Date** | |
| Select Campaign Name 🔍 | Search for a user 🔍 | All ⌄ | All ⌄ | All | |
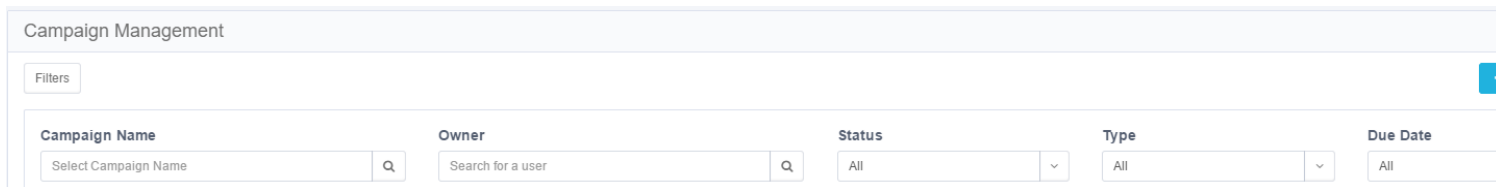
If you select *Define Range* from the dropdown menu, a calendar displays for you to select a date range.

Each displayed campaign lists the following information:

*Template*

The template name displays as a link, which the user can click to edit the template. Any changes that the user makes to the template will only affect future campaigns. If the campaign was created without a template, "No Template" will display (but not as a link).

*Description*

The template description displays.

*Owner*

The template owner displays.

*Due Date*

The due date displays. If the status is *Pending Creation* ("Creation in Progress") or *Created* ("Created & ready to run"), then "Due date to be calculated during initial run" displays.

### *Color Code*

**Yellow**

Status is "Pending Review in Progress", 0-7 days before the date.

**Red**

Status is "Pending Review in Progress", due date has past.

### *Refresh*

This button refreshes the current campaign status, and is located on the bottom left of the displayed campaign.

### *Run Now*

This button only displays for a campaign whose status is *Created* ("Create & ready to run").
When you select this tab, it creates a task that:

- Runs the campaign

- Sets a campaign due date

- Sets the campaign reviewers

- Sends email notification to the reviewers, requesting them to approve or reject suggested user accesses.

### *Menu options*

The menu button, on the top right of each campaign display, contains various options, depending upon the campaign status. All options are available when the campaign status is "Review in Progress", and include:

### *Edit*

Edit the campaign.

### *Save as Template*

Save the campaign as a template.

### *Refresh*

Refresh the user's view of the campaign status.

### *Reinitialize*

Create a task that reinitializes the campaign.

### *Delete*

Delete the campaign.

### *Send Reminders*

Send reminder emails to reviewers to complete the campaign.

### *Generate Report*

After you select this option, you can view the generated reports by navigating to **Reports > My Reports**.

## Campaign Management Reports

A user can generate a report from the *Campaign Management* screen. This report contains a detailed list of all records, including their process levels and a summary of their statuses.

# Campaign Details

The **Show Details** tab provides a variety of functions.

1. Click on the Show Details tab to display campaign details, including the campaign name, template, owner, type, status, and other information.

2. Click **End Campaign** to end a campaign, or **Hide Details** to hide certain details.

### *End Campaign*

Click this if you want to end a campaign in progress before all the reviewers have finished their tasks. The campaign will end automatically, and will remove all uncompleted tasks from the reviewers' My Tasks lists. Once you end a campaign, all access requests that have not been rejected will be accepted, and the reviewers can no longer work on that campaign. In addition, it will create revoke requests for any records rejected during the campaign if the campaign was set to create those revoke requests.

### *Hide Details*

Click this to hide the first three rows displayed.

Select various tabs, located directly below the displayed details, to perform additional functions.

### *Pending Records Per Reviewers*

This tab is activated by default. It is displayed with white letters on a blue background, and lists only the relevant campaign's pending records by reviewer.

### *Reassign Records*

Reassign pending records to different reviewer(s).

### *Send Reminders*

Send reminders to reviewers regarding actions on pending records.

### *Bulk Actions*

Reassign records in bulk or to send reminders in bulk.

### *Filter*

Filter pending records by Reviewer or Level Name.

### *All Records*

Display all a campaign's records.

You can reassign records, revert the review process, or show the review process if the campaign is in the "In Progress" status.

- Reassign Records reassigns pending records to different reviewer(s).

- Revert Review Process reverts the review process to a previous state.

- Show Review Process shows all review process details at all levels.

There is no "**Show Details**" button for a campaign whose status is "Creation in Progress".

# Campaign Invitation

This message is global to all campaigns but can be overridden for a specific campaign. It is sent to the reviewer with every new campaign pending that reviewer's decision.

To send a Campaign Invitation message, perform the following steps:

1. In the web client, navigate to **Settings > Message Templates > Access Certification > Campaign Invitation**.

2. Check **Enable Message**.

3. The check box turns green with a white check mark in it, and the fields under Subject and Message Template are enabled.

# Remove Direct Permissions in Campaigns

When campaign reviewers reject access, this generates an access requests for permission removal.

For additional information on access fulfillment and certification, see the Permissions chapter, and particularly Access Fulfillment .

1. Create and save a Permissions Query, as described in Filters: Creating and Editing a Forensics Query

2. In the web client, navigate to **Compliance> Access Certification**:

    a. Create a campaign using the Permission Query.

    b. From **Summary > Fulfillment Process**, click **Edit**.

    c. Click **Fulfill Permissions Revoke Requests**.

    d. Click **Save and Run the Campaign**.

3. Once the review process for Access Requests is finished, the system removes all direct permissions on sup-ported applications from the relevant BRs.

## Monitoring the Progress of Permission Removal

Access Fulfillment is created for each direct permission marked for removal. To monitor progress, in the administrative client, navigate to Access Fulfillment in the administrative client and filter the Fulfillment Requests by Action "Remove Permission".

# Data Source Types and Usages

A data source In File Access Manager is a table containing data from various sources, including internal File Access Manager reports, for use in various system locations. An Administrator can join data sources to form a superset of data, which follows the same logic as a "left join" in an RDBMS database.

> For some data source types, the files should be located on the same server where the IIS is running. To run reports on these data types, the Reporting service has to be installed on the same server as well. Please check in the description of the relevant type below.

## Available Data Sources

***SQL Server Database***

    Access to SQL server database

***Flat File***

    Query a delimited file

***Excel***

    Read data from an MS Excel document

***User Exit***

    Run a user script to return data

***Active Directory***

    Access to the Active Directory

    The files should be located on the same server as the IIS. In order to run reports, the Reporting service should be installed on the same server as well.

***LDAP***

    Query LDAP for object types and properties

***ODBC***

    Access to any ODCB source (such as, DB2 and AS400)

    The files should be located on the same server as the IIS. In order to run reports, the Reporting service should be installed on the same server as well.

***Oracle Database***

    Access to an Oracle database

***Static Table***

    Define an ad-hoc source by creating and populating a table on screen

The files should be located on the same server as the IIS. In order to run reports, the Reporting service should be installed on the same server as well.

*XML*

Analyze and import data from XML

The files should be located on the same server as the IIS. In order to run reports, the Reporting service should be installed on the same server as well.

# Viewing and Editing Data Sources

The Data Source page displays a list of data sourced defined in File Access Manager.

*To Create a data source*

Click New Data Source

See Creating Data Sources

*Actions available on data sources*

- Edit

- Delete

- Generate Report - Opens a scheduling panel to run a report once, or create a scheduled report from this data.

# Join Data Sources

The Join Data Source works like a *Left Join* in an RDBMS, where the configured data source is the left table, and the joined data source is the right table.
The join will produce a complete set of records by matching data from the configured Data Source, with data in the joined Data Source (if available). If there is no matching data, the right columns will be empty (null values).

A joined data source depends on a match between the Local Key (in the configured Data Source column) and the Remote Key (in the joined Data Source column).

In the following example:

Data Source A (configured) has the following columns:

> A User Name is a unique entity, while a User Display Name may have more than one associated user.

Data Source A

| User Name | User Display Name |
|-----------|-------------------|
| John | John Doe |
| Mike | Mike Miller |
| Lisa | Lisa B |

Data Source B (the joined data source) has the following columns:

Data Source B

| User Name Joined | Department |
|---|---|
| John | Engineering |
| Mike | Product |
| Other User | Finance |

The joined data source below results from joining Data Source A and Data Source B, Local Key = User Name and Remote Key = User Name Joined:

Joined Data Source

| User Name | User Display Name | Department |
|---|---|---|
| John | John Doe | Engineering |
| Mike | Mike Miller | Product |
| Lisa | Lisa B | |

The Department value for Lisa is null in Data Source B. Other User is not in Data Source A, and is therefore, not in the joined Data Source.

## Creating Data Sources

To create a new Data Source:

1. Navigate to **Admin > Data Sources > New Data Source** to open the New Data Source wizard.

2. Select the data source type from the dropdown list, and enter a name and description.

3. Click **Next** to open the configuration page.

   The parameters Data Source Wizard screen displays. This screen is different for each data source type.

   For a detailed description of the fields for each data source type, see the next sections.

   | | | |
   |---|---|---|
   | Active Directory Data Source | LDAP Data Source | SQL Server Database Data Source |
   | Excel Data Source | ODBC Data Source | Static Table Data Source |
   | Flat File Data Source | Oracle Database Data Source | User Exit Data Source |
   | XML Data Source | | |

4. Fill in the configuration fields for the data source.

5. Click **Test**.

   If the configuration is correct, the Test will run the data source with the values entered in the configuration fields, and display the first ten results.

   If there is an error the test will fail.

6. Joining with additional data sources (Optional)

The Join Data Source works like a *Left Join* in an RDBMS, where the configured data source is the left table, and the joined data source is the right table. See Join Data Sources for further details.

Click the box "**Do you want to join this data source with another one?**" to configure joining this data source with other predefined data sources.

Select the data source, and the key to link by from the dropdown lists. Press the **+** to add additional data sources.

7. Click **Done** to create the data source.

# Active Directory Data Source

The Active Directory data source allows the creation of an LDAP query to the Active Directory to obtain specific objects and their properties.

An Active Directory data source can be added as a previously configured DEC, or using specific parameters to access the Active Directory.

## Configuring an Active Directory Source by DEC

### *DEC*

The Data Enrichment Application. Select from a list of Active Directory DECs

### *Filter*

An Active Directory path by which to filter. For example: `OU=NewUsers,DC=Example,DC=Com`

### *Search Scope*

Where to search objects. Select from

- Base

- One Level

- Subtree

### *Properties to Fetch*

More properties to fetch in addition to the default (Active Directory properties names). For example:

description, objectClass, sAMAccountName etc.

## Configuring an Active Directory Source by Properties

### *Domain NetBios Name*

The Active Directory domain NetBios name

Example: CONTOSO

### *Domain DNS Name*

The Active Directory domain DNS name

Example: www. Example.com

### *User / Password*

A user from the Active Directory domain with Administrative Rights

**Port**

The connection port. The default is default is 389

Must be 389 or 636 if SSL is selected

**SSL**

Check this box to use SSL

**Specific Server**

Should use a specific server connection

**Base DN**

Domain's Base DN (if unsure, leave empty)

**Filter**

An Active Directory path by which to filter

Example: OU=NewUsers,DC=Example,DC=Com

**Search Scope**

Where to search objects: Subtree, Base or One Level.

**Properties to Fetch**

More properties to fetch in addition to the default (Active Directory properties names)

For example: description, objectClass, sAMAccountName etc.

# Excel Data Source

You can create an Excel data source from an existing Excel file.

***Properties of the Excel data source:***

**File UNC Path**

The file location. This must be a relative UNC since it can be accessed from multiple File Access Manager servers

Example: \\file-server\share1\file.xlsx

**Domain**

The domain of the user that has access to the file

**User / Password**

The user that has access to the file

**Worksheet**

The name of the worksheet in the Excel file to query

Example: Sheet1

***Custom Columns Letters***

The columns to query, comma delimited

Example: A,B,E,Z.

Enter a column letter, then click **+** for each additional column

***First Row***

The first row number to query

***First-row columns are headers***

Click to read the headers from the Excel sheet

# Flat File Data Source

You can create a table from a flat file data source (such as *.csv).

***Properties of the Flat File data source:***


***Source File Path***

The file location

Example: \\file-server\share1\file.xlsx

***Headers Row Structure***

The Row Header (the name of the new table)

according to the structure of the file, for example: Users, Roles, Data

***Delimiter Character***

The delimiter separating entries

***First row specifies a column name***

Click to read the headers from the Excel sheet

# LDAP Data Source

You can create a table from an LDAP query.

***Properties of the LDAP data source:***

***Query***

The LDAP query that defines the data source

Example: objectClass=user

***User / Password***

The user that has permissions to run the query

### *Server*

The server to run the LDAP query

### *Port*

The port (default 389)

### *SSL*

Should use SSL

### *Expand Multi-value Attributes*

If set, will create a row in the data source for each value in a multi-value attribute

### *Search Scope*

Where to search objects: Subtree, Base, or One Level.

### *Base DN*

The Base DN from which the query should run

Example: DC=Example,DC=COM

### *Properties to Fetch*

Type in the name of the property, and click **+** to add it to the list.

Click the delete icon on any item to remove it from the list.

# ODBC Data Source

You can create a table from an ODBC data source.

### *Properties of the ODBC data source:*

### *System DSN*

The ODBC file data source name as it is stored in the server

### *Timeout (min)*

The ODBC query timeout, in minutes (default is 0)

### *User / Password*

Credentials of the user with permissions to run the ODBC query

### *Query*

The query to retrieve the required data

# Oracle Database Data Source

You can create a table from an Oracle Database query.

### *Properties of the Oracle Database data source:*

### SID

The oracle site identifier

This field is compulsory if 'By Properties' radio button is checked

### User / Password

The user with permission to run the query

This field is compulsory if 'By Properties' radio button is checked

### Timeout

The query timeout in minutes

This field is compulsory if 'By Properties' radio button is checked

### Query

The query that defines the data to retrieve

# SQL Server Database Data Source

You can create a table from an SQL Server Database query.

### Properties of the SQL Server Database data source:

### WPC

The Data Enrichment Application from which to take the parameters (only SQL DECs)

This field is compulsory if '**BY DEC**' radio button is checked

### Server Name / Port / Database

SQL Server Database access

These fields are compulsory if '**By Properties**' radio button is checked

### User / Password

The user with permission to run the query

This field is compulsory if 'By Properties' radio button is checked

### Timeout (min)

The query timeout (default is 0)

This field is compulsory if '**By Properties**' radio button is checked

### Query

The SQL query that defines the data to retrieve

# Static Table Data Source

Create a static custom table by adding or deleting columns and inserting / editing written text in the data grid on the screen.

Edit the headers and content directly in the New Data Source page.

Use the **Add Row** / **Column** buttons and the delete buttons to manage the table dimentions.

# User Exit Data Source

The User Exit data source executes an external script / executable file, which prints a *.csv-formatted table of data to the Standard Output stream.

*Properties of the User Exit data source:*

### *File Name*

The full path to the file being executed

Examples: c:\temp\UserExitScript.bat

\\remotehost\shared_dir\ UserExitScript.exe

### *Arguments passed to the file*

List of arguments

### *User Name / Password /User Domain*

The user running the file execution process

### *Timeout (ms)*

The amount of time, in milliseconds, to wait for the process to exit. The maximum is the largest possible value of a 32-bit integer. If the timeout passes, the process terminates.

### *First-row columns are headers*

Click to indicate that the csv output contains headers in the first row

### *Values Delimiter Character*

The delimiter of the values in each row

Examples: , (comma  sign)

|(pipe sign)

# XML Data Source

Create a table from an XML data source file.

*Properties of the XML connection details:*

- *XML Namespace*

    The connection details screen contains a list of namespaces.

    Add or remove rows pressing the Add Row button, or the delete icon respectively.

### Prefix

    If the source xml has XML namespaces, this is the namespace's prefix

    This field is compulsory if the source xml has XML namespaces

    Example: If the namespace is: `xmlns:sp=http://some.namespace.uri` then the prefix is sp.

### URI

    If the source xml has XML name spaces, this is the namespace's URI.

    This field is compulsory if the source xml has XML namespaces

    Example: If the namespace is: `xmlns:sp=http://some.namespace.uri` then the URI is: http://-some.namespace.uri

- *Fields*

    Define the fields within the XML source

    Add or remove rows pressing the Add Row button, or the delete icon respectively.

### Name

    Example: The name in this record would be "Job"

    ```
    <record><job>fireman</job></record>
    ```

### XPath

    Example: the XPath for this record would be "Job/text()"

    ```
    <record><job>fireman</job></record>
    ```

### Type

    Example: `System.DateTime, System.Int32`

### Format

    If the columns is of a Date type, can set the date format

    Example: DD'/'MM'/'yyyy

- *Source XML File Path*

    The path to the source Xml file. This is a local path, from which the "File Access Manager User Interface" service is installed

- *Record Base XPath*

This XPath query defines the reoccurring element to use as a base record. The different field definition query from inside this base record.

For example, if the xm is:

```
<someData xmlns:sp="http://some.namespace.uri"><record><name id="1">john smith</-
name></record><record><name id="2">john doe</name></record></someData>
```

Then the record base xpath is .someData/record

# Configuring the File Access Manager Website

This chapter describes the Settings tab of the File Access Manager website .

The *Settings* tab include the following sub tabs (displayed from left to right):

***Message Templates***

- Access Certification
    - Campaign Invitation
    - Scheduled Reminders
- Access Request
- Data Owners Election
    - Welcome Message
    - New Task
    - Pending Activities
    - Scheduled Reminder
    - Review Task
    - Owner's Appointment
    - Company Information
- System Notifications
    - Service Monitoring

***Capabilities***

- Import User Scope

***Account Exclusions***

- Goal Exclusions
- Sensitive Account Exclusions
- Alert Exclusions

***Discard Rules***

***Task Management***

- Tasks
- Scheduled Tasks
- Task Auto Retry

***General***

- Overexposed Resources

- API Authentication

- SMTP Account

# Message Templates

The message templates are used to send alerts and messages to users in various scenarios. For example, if while creating an Access Certification template, an administrator checks the check box to send a reminder, the system will send the reminder automatically, according to the format and parameters of the Scheduled Reminders template. The templates use variables to be replaced by the actual relevant data when sending the message.

The available templates are listed above. Edit the templates to fit your company culture and language.

To edit a message template, perform the following steps:

1. Open the relevant template

2. Navigate to *Settings > Message Templates >* template submenu (see list above)

3. Check **Enable Message** – to toggle the checkbox and enabling the subject and message input fields

4. To add variables to the heading or message text, click **Insert Predefined Parameters**, and select one or more fields in the dropdown list. The values in the lists vary according to the context.

> The system will replace the values in the dynamic fields with real values when the messages are sent.
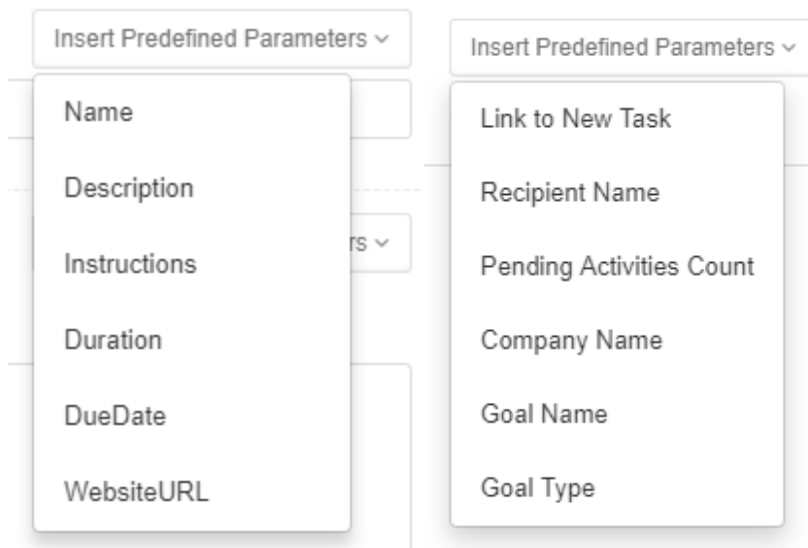


5. Click **Send Test Mail** to send a test Email to yourself to check that the information in the Message Template is correct.

6. For templates for scheduled reminders, set the weekday(s) and time for a scheduled reminder in the *Send Weekly Reminders* section at the bottom of the *Scheduled Reminders* screen. The default is Wednesday at 13:00.

7.  Click **Save** or **Discard** to save (or discard) the template

The system saves this template to the web client server to create messages when required

## Access Certification

These are automated emails referring to the access certification process

### *Campaign Invitation*

This message is global to all campaigns, but can be overridden for a specific campaign. It is sent to the reviewer with every new campaign pending that reviewer's decision.

### *Schedule Reminders*

This reminder is global to all campaigns, but can be overridden for a specific campaign. It is sent to all pending reviewers, per the weekly schedule.

### *Access Requests*

This email is sent to a user who created an access request, when the request is finalized.

In any of the stages:

- Approved
- Rejected
- Fulfilled

## Data Owners Election

### *Welcome Message*

A Welcome Email message is sent to users when they get their first task, explaining the need for data owners and owner election, and their part in the process.

### *New Task*

A New Task message is sent to users whenever they receive a new task.

### *Pending Activities*

A Pending Activities message is initiated (on-demand) by the administrator and is sent to users who do not fulfill their tasks.

### *Scheduled Reminder*

A Scheduled Reminders message is sent, according to the set schedule, to all users with pending tasks.

### *Review Task*

A Review Task message is sent to relevant reviewers after a data owner's election process has concluded.

To send a Review Task message, perform the following steps:

1. Navigate to **Settings > Message Templates > Data Owners Election > Review Task**

2. Check Enable Message.

3. The check box it is ticked, and the fields under Subject and Message Template are enabled.

> The system sends this message to the Data Owners election reviewers in the goal Appointment portion of this process. The review task will appear in My Tasks **>** Owners Election

4. Continue as described above.

### *Owner's Appointment*

Navigate to **Settings > Message Templates > Data Owners Election > Owner's Appointment**

An Owner's Appointment message is sent once to each of the appointed owners of a resource.

The message is supposed to explain the data owner role as access request approver.
Something along the lines of:

Your colleagues have elected you as the Data Owner for the following resource under the $$APPLICATION_
NAME$$ application: $$RESOURCE_PATH$$

As a Data Owner you are required to take an active role in protecting the sensitive information within your resource. The processes in which your participation is needed may include reviewing suspicious activity on your resource, reviewing new access requests, and certifying the currently granted permissions.

We will approach you once your input is required.

> The system sends this message to users who have been appointed as data owners.

### *Company Information*

The Company Information template contains the name and logo to be included in every email message.

To set the details in a Company Information message (sent in emails), perform the following steps:

1. Navigate to **Settings > Message Templates > Data Owners Election > Company Information**

2. Enter the company name

3. Click **Select File** to select a logo image from your drive. The file size cannot exceed 300 x 140 pixels

4. The logo displays in the Company Logo graphic box

5. **Click Remove** to remove the logo

6. Click **Save** to save the Company Information or **Discard** to discard it

### System Notifications

To see System Notification, navigate to **Settings > Message Templates > System Notifications**.

System notifications alert users when a service goes down.

While a default message can be used as a notification, users can also change the default message to conform to their company's particular needs.

The following predefined parameters are available:

- ServiceName

- Server

- ServiceType

# Capabilities

Use this screen to view, add or remove user accounts to or from the capabilities list. Adding a capability to a user will grant the capability rights to this user.

See section Capabilities (Web Client) for more details.

## Excluding Accounts from File Access Manager Processes

Administrators use the Account Exclusions setting to exclude specific accounts from appearing in various reports or activities. This might include bots that access resources often,. But should not be considered for data ownership, or sensitive accounts, that we might not want appearing on activity reports.

There are three types of exclusions, as described below: goal exclusion, sensitive account exclusion, alert exclusion.

To open the exclusion screen, navigate to *Settings > Account Exclusions*

### To add a single account

1. Click **+Add Account**

2. Search for a user from the combo box

3. Click **Add**

### To remove accounts from the exclusion list

1. Filter the list of accounts using the filter field

2. For a single account

    a. Select **Delete** from the Actions menu on the row of the account to delete

3. For multiple accounts

    a. Select the required accounts by clicking the checkbox on the account row

    b. Click the **Delete** icon

### To add a list of accounts to exclude

See Uploading Bulk Account Exclusions below.

## Types of Exclusions

There are three types of exclusions :

### Goal Exclusions

Exclude specific accounts from the data owner's election process. The excluded users will not participate in the Data Owner Election, neither as candidates nor as voters.

### Sensitive Account Exclusions

The permissions and activities of the excluded accounts will be visible to Administrators only. Select User / Group accounts, or use a prefix. All the direct members of an excluded group will be excluded.

Once an account is on the exclusion list, data owners will not be able to see those accounts in the following screens:

- *Resources > Activities >Access Frequency*

- *Resources > Permissions > Simple View*

- *Resources > Permissions > Excess View*

- *Resources > Permissions > Tree*

- *Resources > Owners*

   *Forensics*

### Alert Exclusions

Alert Rules will ignore all Activities performed by the excluded users.

## Uploading Bulk Account Exclusions

1. Navigate to *Settings > Account Exclusions > [X] Exclusions*, and select *Bulk Upload*
   For example: Settings > Account Exclusions > Goal Exclusions

   A Bulk Actions dialog box displays.

2. to download a sample CSV file, Click **Download Sample File**.

3. In the CSV file, fill in the relevant fields Domain Name, Username, account type (if required) , as relevant

4. Save and upload the file.

5. A status popup appears with the upload status.

6. The Exclusions grid refreshes automatically with the uploaded accounts.

### Searching for users or accounts to exclude

1. Type the user or account name, or the first few characters of the name, in the Search box. You can select the account type – Group or User, where these filters are present. If this option is not available, the default is user account.

2. Click **Add** to add the exclusion or **Clear** to delete the exclusion selected.

3. To search for a current excluded account, type the excluded account name, or the first few characters of the name, in the Search box at the top right of the screen.

### Starts With

If you are using the "starts with" operator (where supported), the application will not display a list of candidates. Type in one or more letters of the prefix of the accounts to exclude from this list. All the accounts in the system that start with the string provided will be excluded.

The free text that you type in the "Account to be Excluded" field when you select the "Starts with" operator can only be a user/group name, and cannot include a domain name.

### *Deleting Accounts / Groups:*

Click the drop-down menu to the left of a username, and click **Delete**.

To delete more than one account, select the accounts to delete, and click the Delete icon.

# Task Management Menu

In the web client, navigate to **Settings > Task Management**.

- Tasks

- Scheduled Tasks

- Task AutoRetry

## General

File Access Manager is a task-oriented system, with both interactive tasks (such as querying events) and background tasks (producing reports).

Scheduling tasks with parameters allows them to comply with various requirements.

File Access Manager has long-running processes, including crawling, permissions collection, and reports. The system executes and tracks these processes using tasks, and runs them in batches. It is thus possible to work in the administrative client while tracking the progress of various processes.
Most reports throughout the system have a button or menu item to create a scheduled task, or produce now. Click Produce Now to create ad-hoc tasks in the administrative client to run the report. You can track the tasks in the File Access Manager web application, under **Settings > Task Management > Tasks**.

When the system creates a task, the following Information popup displays.

An File Access Manager service runs this task, and polls the File Access Manager Database periodically to search for new pending tasks. Each service polls the specific types of Tasks for which it is responsible. For example, the Reporting Service polls and handles Report Tasks. User-created tasks and scheduled tasks display in the *Tasks* screen.

> The permission "Show Tasks from All Users" is required to view all system tasks. This permission is granted by default to the administrator role. Without this permission, the system only displays user-created tasks.

## *Navigation and menus*

- Checkbox on the left of a task – select task.

- Checkbox on the top of the table – select all tasks on this page.

- Select all x items on the top menu – Select all tasks on all pages according to the filter.

- Unselect all items – unselect all items on other pages except for the current one.

- Filter icon on the top right corner – open the filter.

- Rows per page on the bottom of the table – select the number of entries per page.

# Tasks

This screen shows table with the tasks selected according to the user's permissions and the filter. The data are updated in real time. On this screen you can cancel, rerun or delete task instances. The filter allows selecting tasks by various parameters, including status, type and date.

Selecting a task opens the Task Details panel listing with details detailed description of the task details and status of



submitted tasks.

## Task fields

### Name, Type

Task Name, Task type

### Service

The service related to this task.

### Server

The server this task is running on.

### Status

This field shows the current status of the task, including a progress bar.

The field statuses are shown below:

| Status | Icon | Description |
|---|---|---|
| Completed |  | |
| Completed with warnings |  | |

| Status | Icon | Description |
|--------|------|-------------|
| Failed | | |
| Canceled | | |
| In Progress | 90% | Shows a progress bar of the task completion. |
| Pending | | Task has been created, but is not running yet. |

Start / end date

Create By

Parameters

### Task filter

The task screen includes a filter to narrow down the selection of tasks. click the filter button on the top right corner of the Task screen to open the filter.

> The filter is not visible if there are tasks selected
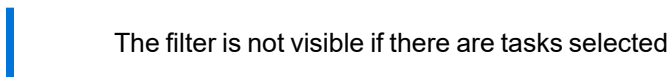
*Filter fields:*

Name, Type, Service, Status, Task that ended before (date field), Created by me only

The **service** filter dropdown lists services that have tasks.

Click **Apply** to set the filter

### Task screen actions

Select one or more tasks using the checkbox to the left of each task. Selecting a task will open the top option menu:

- *Re-run*: rerun the task(s) selected. Selected tasks that cannot be run will not run. Selected tasks that depend on other tasks to complete before running will run after the prerequisite task runs.

- *Cancel*: Cancel the running tasks out of the list selected.

- *Delete*: Delete

### Task Details screen

Clicking on a task opens the Task Details screen, with a description of the task stages.

To close the detail screen, click outside the details screen, or click the **X** in the upper corner.

**Task Details**
Database Clean Up

| Severity | Date | Service | Description |
|---|---|---|---|
| Information | 9/20/19 7:01:15 AM | File Access Manager Scheduled T... | Database Clean Up Task: Database clean up task completed |
| Information | 9/20/19 7:01:15 AM | File Access Manager Scheduled T... | Database Clean Up Task: Cleaning old reports skipped |
| Information | 9/20/19 7:01:15 AM | File Access Manager Scheduled T... | Database Clean Up Task: Cleaning old reports |
| Information | 9/20/19 7:00:19 AM | File Access Manager Scheduled T... | Database Clean Up Task: Database clean up task is rebuilding the DB indexes ... |
| Information | 9/20/19 7:00:19 AM | File Access Manager Scheduled T... | Database Clean Up Task: Finished deleting stale Data Remediation entries |
| Information | 9/20/19 7:00:19 AM | File Access Manager Scheduled T... | Database Clean Up Task: Deleting stale Data Remediation entires |
| Information | 9/20/19 7:00:18 AM | File Access Manager Scheduled T... | Database Clean Up Task: Finished cleaning temporary tables |
| Information | 9/20/19 7:00:18 AM | File Access Manager Scheduled T... | Database Clean Up Task: Cleaning temporary tables |
| Information | 9/20/19 7:00:18 AM | File Access Manager Scheduled T... | Database Clean Up Task: Finished SQL [event] table maintenance |
| Information | 9/20/19 7:00:18 AM | File Access Manager Scheduled T... | Database Clean Up Task: SQL [event] table maintenance |

## Scheduled Tasks

A Scheduled Task tells File Access Manager when, and how often, to execute a specific Task repeatedly. For example, a weekly scheduled task can run a weekly Activities Report.

The wizards in the File Access Manager administrative client help create Scheduled Tasks. Every wizard with a scheduling screen has a checkbox for creating a scheduled task in the background. While deselecting a checkbox deletes a scheduled task, an attempt to delete a Scheduled Task via the *Scheduled Tasks* screen results in the display of a warning popup, indicating that another object or process is dependent on this Scheduled Task.

The Schedule Task Handler service creates and processes Scheduled Tasks for the relevant services to handle.

Except for a few types of scheduled tasks, it is only possible to edit task scheduling (not parameters) from within the *Scheduled Tasks* screen.

### Scheduled tasks filter

The Scheduled tasks screen includes a filter to narrow down the selection of scheduled tasks. Click the filter button on the top right corner of the Task screen to open the filter.

> The filter icon is not visible if there are tasks selected

Filter fields:

*Name*

> The scheduled task name

*Type*

> a drop down list of scheduled task types

*Status*

> All, Active, Inactive

Click **Apply** to set the filter

### *Scheduled Tasks' fields*

- Name

- Task Name

- Type

- The type of a Scheduled Task indicates the task actions.

The table below lists and describes the task types:

| Type | Description and task source |
|---|---|
| Access Certification Campaign | Tasks related to Access Certification Campaigns, created from the Access Certification screen |
| Access Certification Campaign Reminder Emails | Reminder emails for a campaign. This task is created for each new campaign that is configured to send reminders. The task is controlled through the Edit Campaign wizard |
| Access Requests Reminder Emails | Controlled through the Access Request screen |
| Application Deletion | One-time task created when deleting an Application<br><br>You cannot schedule this task type. |
| Archive Events by Filter | Created from the Activities to Archive events |
| Built-in Application Permissions Only Collection | Created from the Permissions Collector or the Edit Application wizard |
| Built-in Business Resource Permissions Only Collection | Created by right clicking a business resource in the Permissions/Permissions and Identities Forensics screen and starting a specific business resource permissions' collection<br><br>You cannot schedule this task type. |
| Business Resource Deletion | One-time task created when deleting a Business Resource<br><br>You cannot schedule this task type. |
| Classify Behavioral Rules | A Scheduled Task that classifies data, based on behavioral rules.<br><br>This task can be scheduled from the File Access Manager Administrative Client under *Policies > Data Remediation Policy > Configuration > Schedule Classify Behavioral Rules* |
| Crawler | Controlled through the Edit Application Wizard |
| Daily Statistics Calculation | An internal, built-in, system-scheduled task that calculates daily statistics on collected activities |
| Data Classification | Different Data Classification tasks |

| Type | Description and task source |
| --- | --- |
| Database Clean Up | An internal built-in, system-scheduled task that maintains the File Access Managerdatabase |
| Homegrown Application Identities and Permissions Collection | Controlled through the Permissions Collector wizard of a Homegrown Application |
| Identity Collector Synchronization | Controlled through the Edit Identity Collector wizard |
| Reassign Review Process | A one-time task, created when a review process is reassigned to Access Certification, or Access Request<br><br>You cannot schedule this task type. |
| Report | Created during report creation or in the Edit report wizard |
| Revert Review Process | A one-time task, created when a review process is reverted in Access Certification, or Access RequestYou cannot schedule this task type. |
| Scheduled Events Deletion | Created in Activities to delete events periodically |
| Service Log Level Update | A one-time task that changes the log level of a service created in the Health Center when performing a service drill down<br><br>You cannot schedule this task type. |
| Users Logical Drives Mappings | Controlled using Access Fulfillment configuration |

*Status*

This field shows the current status of the task, including a progress bar.

A scheduled task can be either active, or inactive.

*Schedule Type*

The schedule type describes the frequency of running the tasks.

- *Schedule Types and Intervals*

  *Once*

  Single execution task runs.

  *Run After*

  Create dependency of tasks. The task starts running only upon successful completion of the first task.

  *Hourly*

Set the start time.

*Daily*

Set the start date and time.

*Weekly*

Set the day(s) of the week on which to run.

*Monthly*

The start date defines the day of the month on which to run a task.

*Quarterly*

A monthly schedule with an interval of 3 months.

*Half Yearly*

A monthly schedule with an interval of 6 months.

*Yearly*

A monthly schedule with an interval of 12 months.

*Last run*

The last time the task ran. Whether successful or not.

*Next run*

For scheduled tasks that have future runs scheduled

*Parameters*

The run parameters of the scheduled task.

## *Edit Schedule / Edit Schedule of x selected tasks*

To edit the schedule of one or more scheduled tasks, select the scheduled task from the Scheduled Task screen, and click **Edit**.

This will open the Edit Schedule panel. Scroll down the panel to see all the input fields.

Frequency type – see above

Run After

If selecting Run After, select the task after which this task should run.

> When editing more than one task at the same time, you cannot select Run After.

Start date

All tasks, except for *Once & Run After*, have a Start Date. That date defines the baseline date for all calculations.

For example, daily tasks with two-day intervals run first on the start date. The next run will be two days after the start date (not two days after the scheduling date).

End Date (Ends)

- *Never* –tasks without an end date.

- *On* – select an end date.

If set, the system does not schedule new tasks beyond the End Date.

### *Related Tasks*

Clicking a task will open the *Related Tasks* panel, listing the instances of the scheduled task that were run, the run dates, task status, and running user. Click outside the panel, or click the **X** on the top right corner of the panel to return

to the previous screen.

## *Running Tasks*

To run a task, perform the following steps:

1. In the web client, navigate to **Task Management > Scheduled Tasks**.

2. Select a task or tasks from the list of tasks.

   - Using the filter to narrow down the list of tasks

   - Marking the boxes at the left of each task to select it

   - Using the "select all" checkbox at the top of the list – This selects all the tasks on the page.

3. This will open the task menu bar at the top of the Task table.

   - *Edit:* Edit the task scheduling parameters.

   - *Run Now:* rerun the task(s) selected. Selected tasks that cannot be run will not run. Selected tasks that depend on other tasks to complete before running will run after the prerequisite task runs.

   - After running a task or tasks, a popup message opens, with a link to the Tasks screen to view the task progress.

   - *Activate*: Turn on the Activate flag for all schedule tasks selected. This will enable the scheduling to run, as it is configured.

   - *Deactivate*: Turn off the activation flag for all scheduled tasks selected.

If you deactivate scheduled task, the next run field for these tasks will remain empty.

> The options displayed after right clicking are Run Now, Edit, and Delete.

## Task Auto Retry

File Access Manager can set an auto-retry on task, whereby tasks will be automatically run again a preconfigured number of times in case of failure. The tasks that can be retried are configured by task type.

By default, most task types are set to auto retry twice. See list below for task types set to auto retry:

| |
|---|
| Access Certification Campaign Reminder Emails |
| Access Requests Reminder Emails |
| Application Deletion |
| Built-in Application Permissions Only Collection |
| Business Resource Deletion |
| Classify Behavioral Rules |
| Classify Composite Rules |

| |
|---|
| Crawler |
| Dashboard Widgets Calculation |
| Data Classification |
| Global Campaign Reminder |
| Identity Collector Synchronization |
| Import Data Classification Results |
| Import User Scope |
| eMail Reminder |
| Report |
| Report Template |
| Scheduled Alerts Deletion |
| Users Logical Drives Mappings |

Access to this panel is controlled by the permission "**Settings > Task Management > Task Auto Retry**".
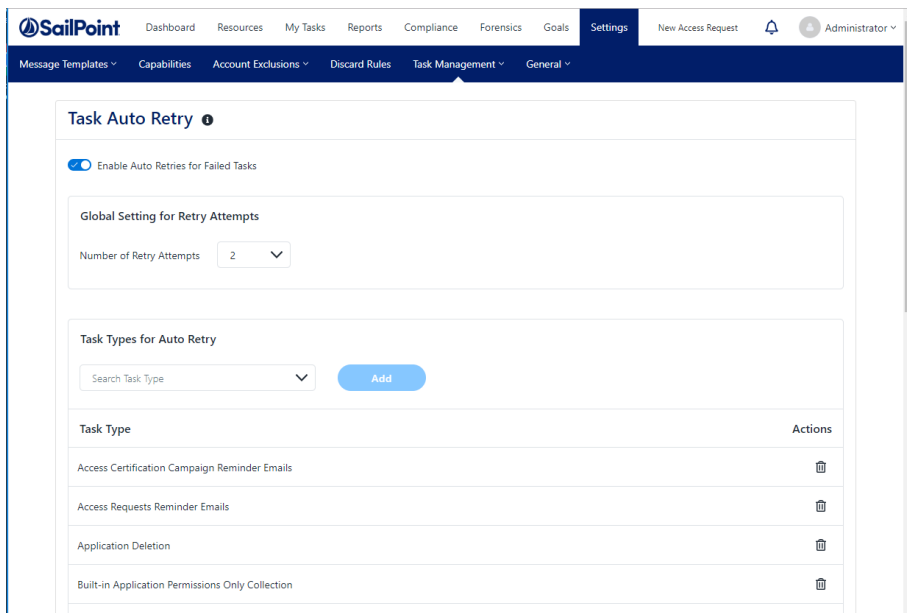


To enable auto retry for tasks for File Access Manager

1. In the web client, navigate to **Settings > Task Management > Task Auto Retry**.

2. Click **Enable Auto Retries for Failed Tasks**.

3. Set the *number of retry attempts* – the number of additional tries the system will run the task.

To set the task types that will be retried, complete the following:

1. Select task types from the drop-down menu

   The drop down list includes all available task types that are not already selected for auto-retry. If all the task types are enabled, the Add Task Type field is disabled.

2. Click **Add** to add the task type to the list.

To delete a task type from the list of task types to retry, complete the following:

1. Locate the task type from the task type list

2. Click the trash icon on the row of the task type to delete.

3. Click **Save** or **Discard** to save or discard the changes made on this panel.

## My Tasks

### Tracking Tasks (Task Progress in the Task Detail Pane )

To track a task, perform the following steps:

1. Navigate to **My Tasks**.

2. Select the task type from the menu bar:

- Access Certification

- Access Request

- Owners Election – suggest owners for a given resource

- My Requests

Each menu will open a list of active tasks assigned to the current user.

Click the selection from the actions column to view or perform the assigned task.

## General Menu

To get to the general menu, navigate to **Settings > General**.

General settings affect the entire system.

### Path Display

An administrator can define the mapping of application paths throughout the business user interface.

To define the mapping of application paths, perform the following steps:

1. Define the path in the administrative client.

2. Check the "Translate physical path to logical drive mapping wherever applicable" checkbox if applicable.

3. To exclude administrators, check the "Exclude Administrators" checkbox.

> If there is a preference to see the physical name of the administrator, rather than the logical name, the "Exclude Administrators" checkbox should be checked.

4. To display the physical path, check the "Allow physical path to be viewed" checkbox.

> If the preference is to see only the logical path (to avoid confusion caused by the display of multiple names) this checkbox should remain unchecked.

5. Click **Save** to save the selection, or **Discard** to discard it.

6. After making and saving changes, delete the cache.

## Overexposed Resources

Overexposed resources are resources accessed by groups with "too many" members. The system determines large groups based on basic parameters, and administrators can change those parameters. "Everyone" and "Authenticated Users" groups are included by default, but it is possible to further filter (define) overexposed resources by group.

To define overexposed resources, perform the following steps:

Navigate to **Settings > General > Overexposed Resources**

1. Check the "Groups containing at least ____% of user accounts" checkbox to define groups by the percentage of user accounts. (This checkbox is checked by default.)

2. Check the "Groups containing at least ____ user accounts" checkbox to define groups by the number of user accounts. (This checkbox is checked by default.)

3. Check the "Include Share permissions (on CIFS-based applications)" checkbox to include those share per-missions. (This checkbox is checked by default.)

4. To exclude group accounts from the overexposed group, type the account name, or the first few characters of the account name, in the "Exclude Group Account" search box.

5. Click **Save** to save the selection, or **Discard** to discard it.

6. To remove a group from the list, click the "**x**" next to the group name.

## API Authentication

This screen enables administrators to view the API authentication.

The screen does not display the client secret, but it enables the users to copy the secret to the clipboard

To generate a new client secret, click the **Generate Secret** button.

## Configuring the SMTP Account

File Access Manager SMTP Account is used for configuration of the connection to the organization email server to send notifications, reports, and reminders.

***To configure the SMTP account:***

1. Open the SMTP Account configuration screen.

   *Settings > General > SMTP Account*

2. Configure the account details.

   *Server Host/IP*

   > The server host details

   *Port*

   > For the SMTP service connection

   *Username, Password*

   > Connection credentials

   *From*

   > This is a unified From field from all Email responses.

   *Timeout (MS)*

   > The timeout, in milliseconds

   *SSL*

   > If SSL is required, check this box

   *Recipient Email*

   > An email address to send the test email to, when clicking the test button.

   > Use a non SailPoint email address. Or, configure your own email during deployment.

3. Click **Send Test Email** to test the configuration by sending a test email to your mailbox and verifying receipt.

4. Click **Save** or **Cancel** to exit.

# Running and Viewing Reports

File Access Manager provides advanced report generation capabilities. Reports can be generated using report templates in the File Access Manager website, or initiating reports off tables in the File Access Manager website.

Regardless of where reports are generated, all reports can be retrieved in the File Access Manager website.

## Editing Scheduled Reports in the Administrative Client

Scheduled reports that are created in the Administrative Client can be edited in the Reports table.

The following fields can be modified:

*Name*

*Description*

*Viewable by*

*Scheduling*

> Available to users who have the permission `Report Templates Administrator`

*Sharing*

> Available to users who have the permission `Report Templates Administrator`

*Displayed column*

> Available on certain types of reports

Reports make processed data available to the appropriate data owners.

## Using and Accessing Report Templates

Report templates are templates for built-in reports, based on the user who accesses them. For example, administrators and users who have the permission `Report Templates Administrator` see all report templates, while data owners see only templates that are shared with data owners, and other users (non-administrators and non-data owners) do not see any report templates.

In the web client, navigate to the **Reports > Report Templates** screen on the web application to use the built-in report templates for standard and customized reports.

### Filter by Tags

You can assign one or more tags per report to help find them later.

**The Filter by Tags** panel on the left can be used to filter out relevant report templates:

**Search field**:

1. Type in the report tag. Available tags will be filtered out as you type.

2. Select one of the available tags to filter out the report templates displayed.

**Created by me**: Select this checkbox to filter out your own report templates



## *Managing Tags*

1. Click **Manage Tags** to open the tag management screen.

   This option is available by default to the Administrator capability only.


   Available options are:

   - Hide system-defined tags (by checking the check box)

   - Search for tags

   - Edit tags

   - Add customized tags

   The Delete option - a trashcan icon - is disabled for system tags; they cannot be deleted.

2. Click the Edit option (a pencil icon) next to a non-system tag to edit that tag.


   You cannot use a name that already exists or use a blank tag.

3. Click **Save** to the right of the edited tag to save it.

4. Click **Save** at the bottom of the Manage Tags screen to save all changes.
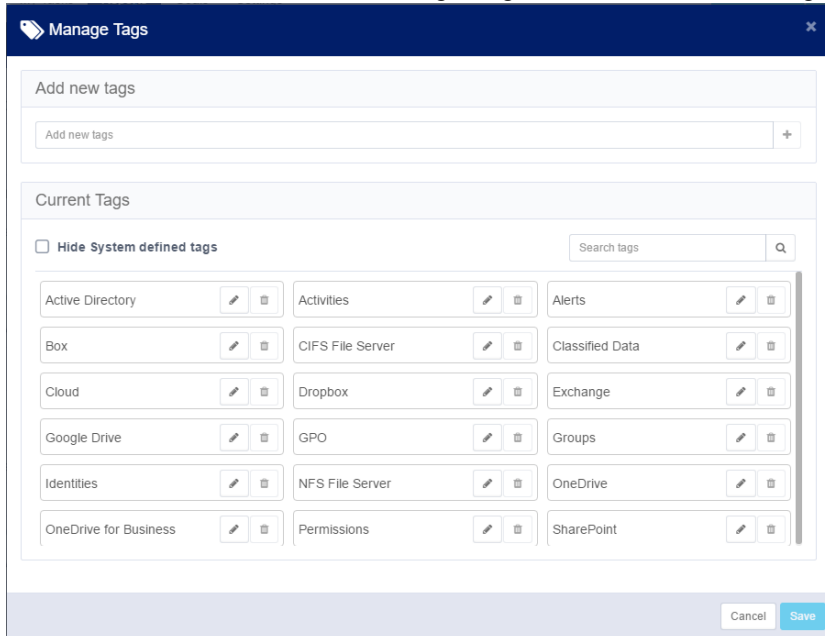


## Running a Report

1. To run the report with settings other than the default parameters, select **Duplicate** from the template menu.

   This will open the **Duplicate Template** panel.

2. Set the desired report parameters, scheduling times, and other setup fields

3. Click **Run Now** to run the report now

4. Click **Save** to save the template for future use of this template
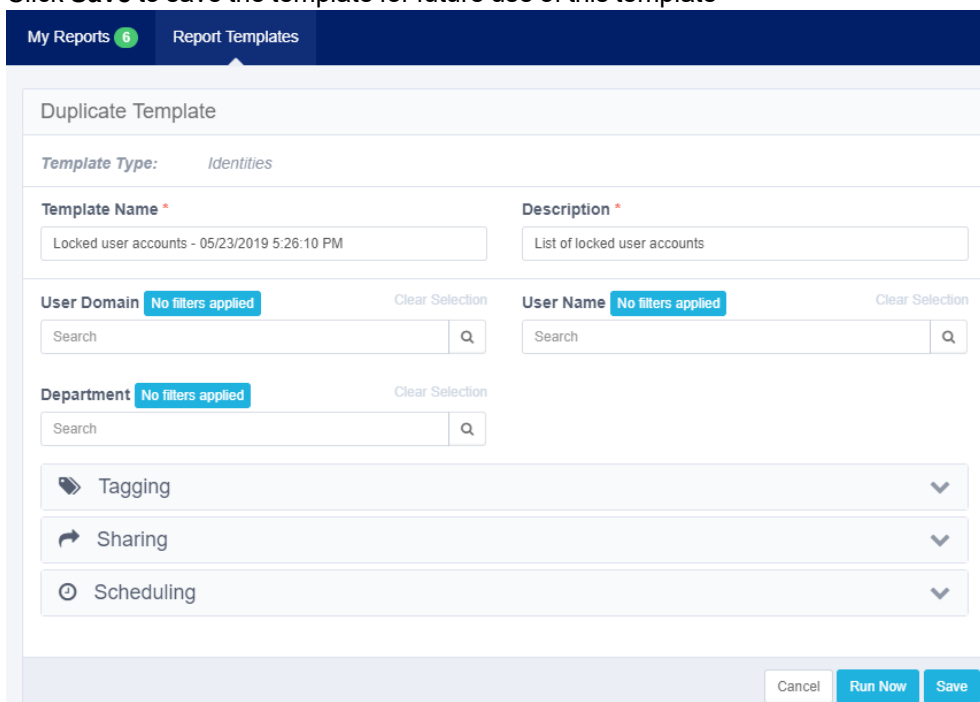
# Report Mechanism

File Access Manager sends reports to the recipients defined in the **Viewable by** section of the report.

The system sends an email with a link to the report only to recipients with permission to download the report. If a recipient forwards that link to a user without permission to download a report, the recipient will not be able to download the report.

# Report Operations

This section describes the operations you can perform on reports.

To open the report management screen in the Administrative Client, navigate to **Reports**.

1. Double click on a report to display report details. The Report Details window will display under the Reports window

2. Click **Refresh** to refresh the Reports list

3. Click **Delete** to delete a selected report

   This option is available only to users with the permission "System>Reports>Delete"

## Editing Reports

The following fields are available to edit a customized report:

- Custom fields to display (where supported)

- Recipients list

- Name

- Description

- Scheduling

   It is not possible to change the query filter of a saved customized report.

To edit report parameters in the Administrative Client, navigate to **Reports**.

1. Select a scheduled report from the list to edit

2. Click **Edit**

3. The Welcome to the Schedule Report Wizard Screen displays

4. Click **Next** on the *Schedule Report Wizard Welcome* page.

5. The **Report Configuration** screen of the Schedule Report Wizard already displays the name in the **Name** field.

1. Type a description in the **Description** field.

2. Double click in the Viewable By field to view a list of users who can view the report.

3. Click on a user's name and click the **+** sign.

4. The user's name appears in the box under the **Viewable By** field.

5. Check the **Send to Data Owners** check box to send the report to data owners.

6. Relevant queries appear in the **Query** section of the **Report Configuration** screen.

7. Click **Finish** to send the configuration to the system without configuring a report schedule.

8. If you click **Finish**, the following Confirmation popup displays: "You are creating a report without a scheduler. Do you wish to continue?"

9. Click **Yes** to save the report without configuring a report schedule, or **No** to return to the **Report Configuration** screen.

10. If you click **Yes**, and the following Warning popup displays: "This action can only run by a File Access Manager user that is associated with a user from the authentication store. The action will not be executed". This means that you logged into the client with a local File Access Manager user, rather than with an Active Directory user from the Authentication Store. Only Active Directory users can create reports, since File Access Manager needs the email address of the user and the user's identity to generate the report.

Otherwise:

11. Click **Next**.

12. The Report Configuration screen displays.

13. Check the **Create a Schedule** check box to create a schedule, or click **Finish** to send the report configuration to the system without a schedule.

14. If you click **Finish**, the following Confirmation popup displays: "You are creating a report without a scheduler. Do you wish to continue?"

15. Click **Yes** to send the configuration to the system without configuring a report schedule, or **No** to return to the **Report Configuration** screen.

16. If you click **Yes**, the following Warning popup displays: "This action can only run by a File Access Manager user that is associated with a user from the authentication store. The action will not be executed."

## Report Actions

### *(Right click) Run Now*

Run the report and send it to all recipients.

### *(Right click) Run now and send only to me*

Run the report and send it to the current user who is active in the Administrative Client.

It is not possible to delete a scheduled report.

# System Usage Report

The system usage report aggregates information captured by the File Access Manager website audit mechanism in order to highlight usage statistics and highlight areas in the website that are the most and least used. It also has the ability learn about the usage habits of our customers - what flows are working better, where do we see flows taking longer or receive less traction.

To ensure the privacy and anonymity of our users and customers, all private identifiable information is redacted and all particular user activity is abstracted or obscured. Usage statistics are aggregated to calculate averages and ranges, and never information about particular users.

# Administrator Tasks - Website

As an administrator in charge of the File Access Manager configuration and ongoing operation, the dashboard and gives an overall view of the state of the system.

In the web client, navigate to **Dashboard > Administrator**.

The Administrator Dashboard features a graphic overview to assist monitoring the system. Its widgets show various system statistics for detailed analysis, including reports and drill-downs to forensics screens. You can update the widgets on the Administrator Dashboard either automatically or manually.

When the Update Now task finishes, the system generates a notification and displays it as a new unread notification which refreshes the dashboard.

The Administrator tab of the dashboard consists of the following widgets:

- Data Ownership

- Sensitive Data Exposure

- System Health Check

- Activity Statistics

- Alerts in Last 7 Days

- Active Data Classification Policies

- Active Campaigns

- Top Sensitive Resources by Activity

- Top Users with Pending Tasks

- Click the **Update Now** button to update all the widgets in the Administrator tab. Clicking Update Now starts a task that updates tables with information (in the background) for widgets, either automatically (daily) or manually. The Last Updated date to the left of the Update Now button is updated accordingly.

- Click the bell icon to open the Most Recent notifications.

- Click the most recent notification (at the top of the list) to update all information displayed in all widgets.
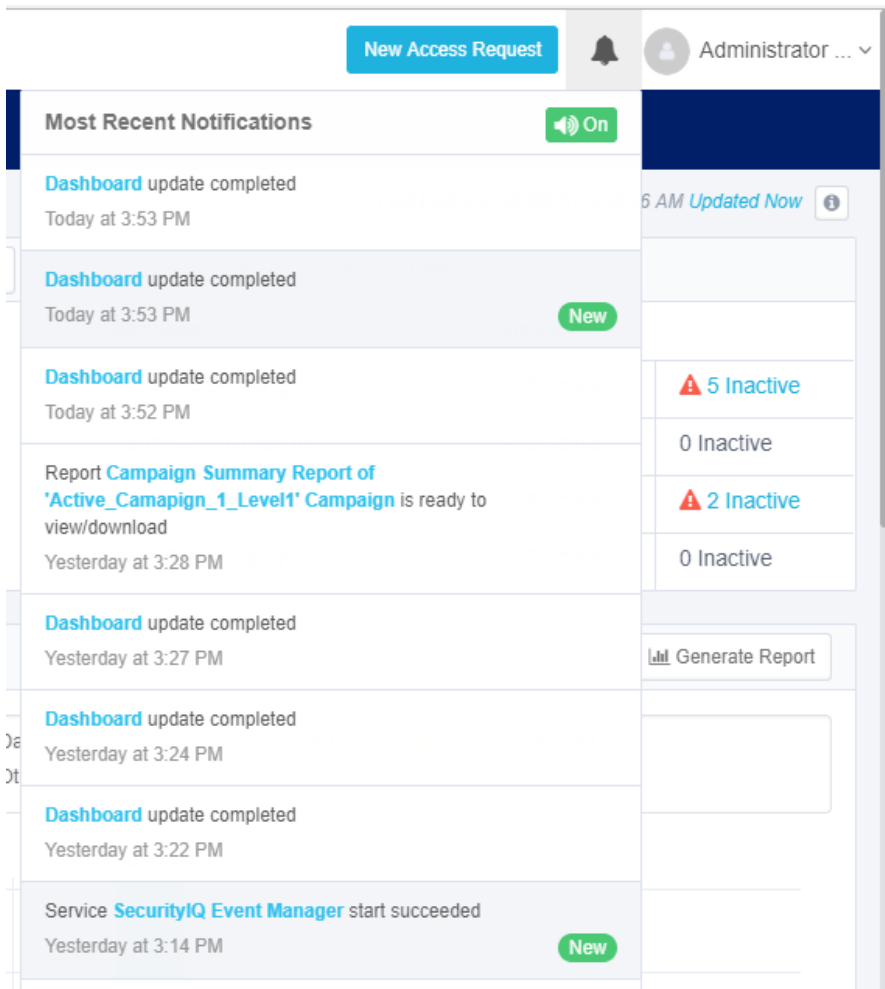
# Data Ownership

The Data Ownership widget displays the number of resources with classified data that are missing an assigned data owner. This widget display the overall compliance score.

***Data Owner***

A user who is responsible for reviewing and approving the access of users to resources.

***Score***

The score consists of a number and an associated color, as follows:

- A score of 0 to 5 displays in red, and indicates a high risk

- A score of 5.1 to 7.5 displays in yellow, and indicates a medium risk

- A score of 7.6 to 10 displays in green, and indicates a low risk

***Counter***

The counter displays the number of sensitive resources missing owners.

> If the number of resources is one thousand or more, it is expressed in K (for example, 10,000 displays as 10K).
> If the number of resources is one million or more, it is expressed in M (for example, 10,000,000 displays as 10M).
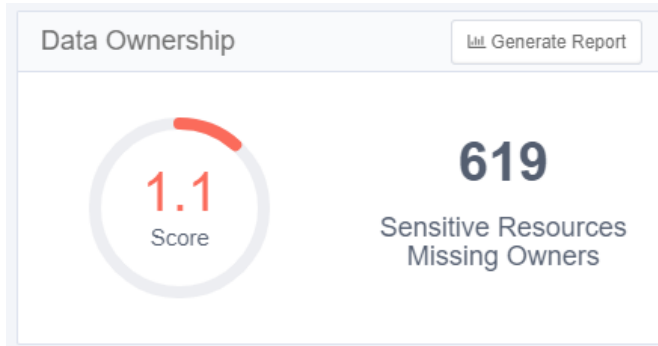


*Report*

Click **Generate Report** to create a detailed resources report. When the report is generated it can be accessed in **Reports > My Reports**.

*Update frequency*

The data is updated daily, by default.

# Sensitive Data Exposure

The Sensitive Data Exposure widget displays the number of overexposed resources, and the overall compliance score.

The structure of this widget is similar to that of Data Ownership.

*Overexposed resources*

Resources containing classified data which can be accessed by a large number of users.

You can configure the definition of "large number of users" in **Settings > General > Overexposed Resources**
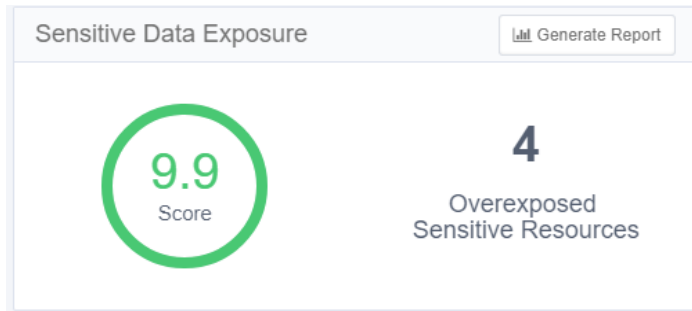
*Report*

Click **Generate Report** to create a detailed report listing resources and groups.

When the report is generated it can be accessed in **Reports > My Reports**.

*Update frequency*

The data are updated daily, by default.

## System Health Check

The System Health Check widget displays the status of system services. This widget displays a list of active and inactive services by service and status, some of which may be restarted.

The widget displays services by category, and the status indicates the total number of active and inactive services. The status of a service can be either active or inactive, where an inactive service is one which might have a problem.

**To view a list of all inactive services and the reasons they are inactive**

1. Click on a blue "**Inactive**" link.
   *An Inactive Services screen displays a table with the following columns:*



| Status | Not Responding, Broken |
|---|---|
| Service | Service name |
| Server Name | The name of the server on which the service resides. Since the System Health Check screen shows the current active servers, this can be used to tell the user which server is active, in a configuration of Disaster Recovery / Production / high availability. |
| Action | Start [Enabled]<br><br>Start [Disabled]<br><br>empty - no screen action available |

2. Click **Start** in a row on the table to start the service in that row.

3. Click **Close** to close the Activity Monitoring Inactive Services screen.

Activity Monitoring Inactive Services

***Report***

This widget does not have a report

***Update frequency***

The data are updated continuously.

### Disaster Recovery Considerations

When you have a Disaster Recovery environment configured, all the services are duplicated – one set in Standby mode, one set in Active mode. The System Health Check widget shows only the active server services.

The System Health Check widget always shows the current active services, regardless of the physical environment being used (Disaster recovery, or Production).

> Services marked as "inactive" are services that are on the active servers (in terms of Disaster Recovery), but are inactive.

The Activity Monitoring Inactive Services panel (see above) displays the active server name.

## Activity Statistics

The Activity Statistics widget displays a trend graph of activities per application. The chart displays one application per tab, for a maximum of five tabs. You can select which applications to monitor by adding or removing tabs.

## *Timeline*

Set the time in which to aggregate the data. This will affect the report output as well.

Valid values are:

- Last 24 Hours

- Last 72 Hours

- Last 7 Days

- Last 30 Days

## *Activity Statistics graph*

Hover the mouse over any point on the graph to display the number of activities on a given date and time.

Click on the graph to drill down to the activity forensics screen with a list of activities per resource. (In the web client, you can also reach this screen by navigating to *Forensics > Activities*.)
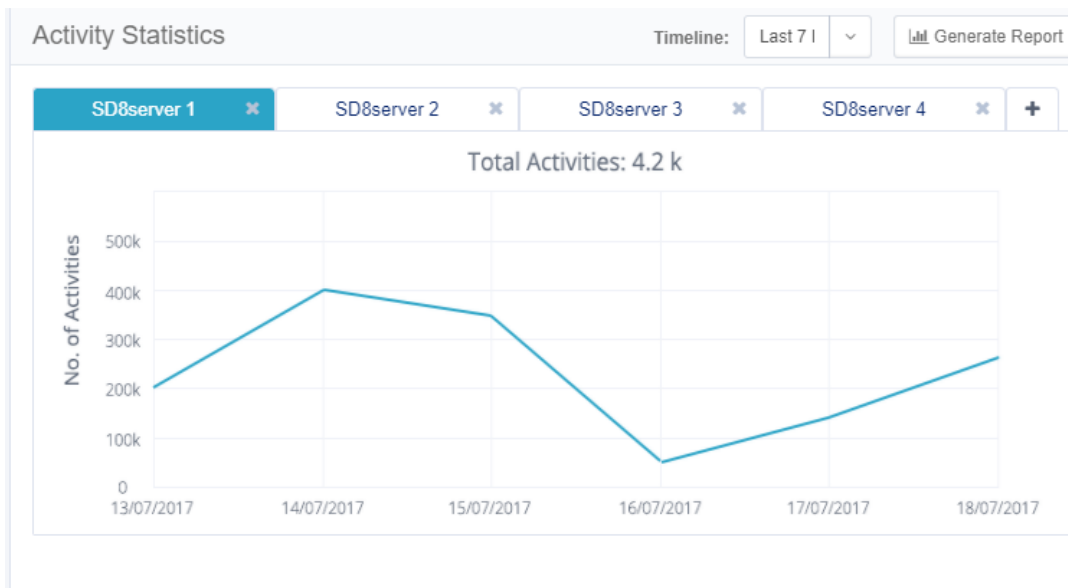


##  *Activity Statistics Widget*

**To add a tab:**

- Click the **+** to the right of the tabs.

- Type in an application name to add. This is an autocomplete field.

**To remove a tab:**

Click the **X** on the tab title.

**Report:**

Click **Generate Report** to create a detailed activities report, according to the timeline and applications selected.

When the report is generated it can be accessed in *Reports > My Reports*.
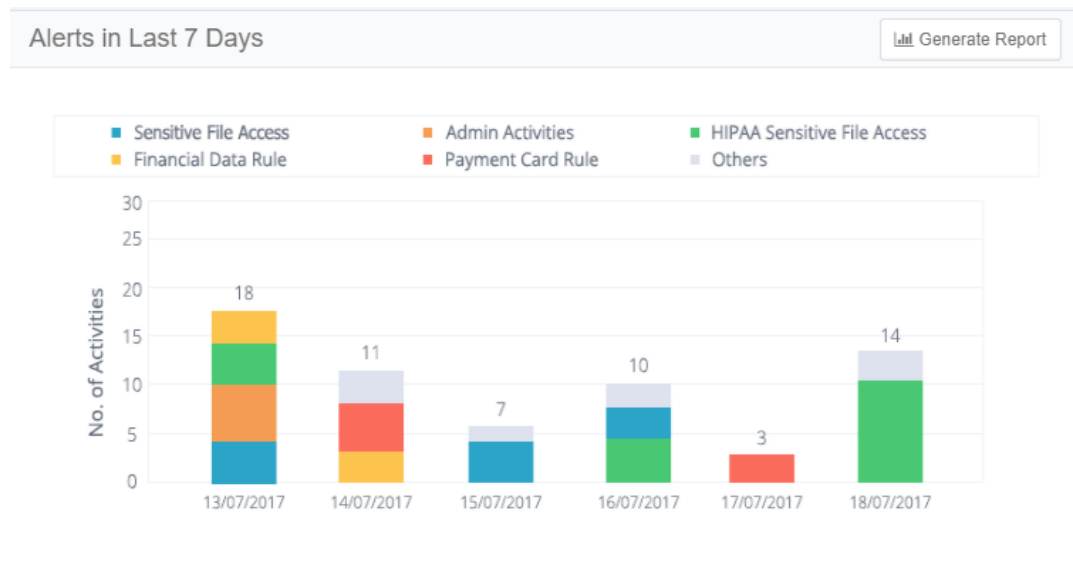
**Update frequency:**

The data on this widget are updated continuously.

# Alerts in Last 7 Days

The Alerts in Last 7 Days widget displays the number of alerts created within the last seven days.

### *Alerts in Last 7 Days graph*

Hover the mouse over any portion of a bar graph to display a tool tip with information on the number of alerts of a specific type, the alert date, and the group for whom the alert was issued.



**Report:**

Click **Generate Report** to create a detailed alerts report.

When the report is generated it can be accessed in *Reports > My Reports*.

**Update frequency:**

The data on this widget are updated continuously.

# Active Data Classification Policies

The Active Data Classification Policies widget displays the active data classification policies in a separate graph for each policy. Each graph displays the five applications with the most policy-classified resources.

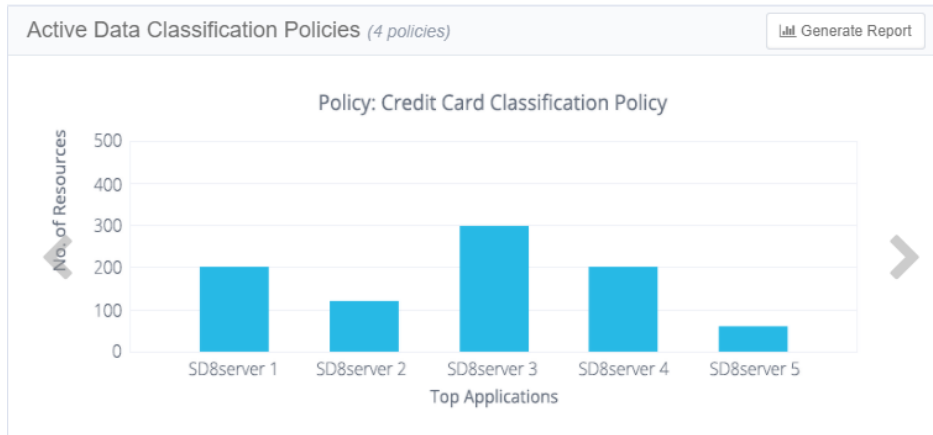The main portions of the Activities Statistics widget are:

- Number of Policies – The number is in parentheses after the widget name. Only one policy bar graph displays at a time. Click the arrows to the right or left of the graph to display graphs for other policies.

- Generate Report

- Active Data Classification Policy graph

This graph shows the number of resources for each of the five top applications for a given policy.

Click on a bar on the graph to display the list of classified resources in the selected application.

This widget is updated once a day (default).



## Active Campaigns

The Active Campaigns widget displays a graph showing the progress of active campaigns, with a separate screen for each campaign.

The main portions of the Active Campaigns widget are:

- Number of Active/In Progress Campaigns – The number is in parentheses after the widget name. Only one campaign circle graph displays at a time. Click the arrows to the right (to display the next graph) or left (to display the previous graph) of the graph to display the graphs of other campaigns.

- Generate Report

- Active Campaign graph

This circle graph shows the percentage of records for each active campaign, as well as the campaign status (approved is green, rejected is red, and pending is gray).

Click on a segment in the graph to drill down to a screen with a list of pending records per reviewer in a selected campaign. (You can also display this screen by navigating to **Compliance > Access Certification**.)

This widget is updated once a day (by default).

## Top Sensitive Resources by Activity

The Top Sensitive Resources widget displays a table of the sensitive resources with classified data, with the most activities within a selected timeframe. The table includes columns for the number of categories and number of activities for each resource listed.

Click on the **No. of Categories** value in a resource to display the names of the categories.

This widget is updated continuously.

## Top Users with Pending Tasks

The Top Users with Pending Tasks widget displays a table of users with the most pending tasks. Examples of tasks are access certifications and access requests.

The table includes columns for the name of the user, the number of the user's pending tasks, and a button for sending a reminder to the user.

Click **Send Reminder** in the row of the user to send the user a reminder of the tasks still pending.

The following alert displays: "Email reminder to [User FullName] is being sent. Notification will be provided upon completion."

This widget is updated continuously (by default).

# Administrator Tasks - Admin Client

This section describes general File Access Manager system administration capabilities, which assist in File Access Manager management and self-monitoring and include:

- Health Center
- Event Viewer
- Tasks and Scheduled Tasks

## Checking the System Health

The **Health Center** provided in the administrative console displays a list of all File Access Manager services.

File Access Manager is a distributed system with components in multiple locations.

Each tab in the service status display represents the service types, arranged by subject.

The panel is split into two tabs, for the environment the services are in: Production or Disaster Recovery. If the system does not have a disaster recovery environment configured, the Disaster Recover tab is disabled.

The spotlight on each service represents its status as follows:

*Green*

> Service is in "good health"

*Yellow*

> Warning – Service is "in need of a checkup"

*Red*

> Service is in "poor health"

*Gray*

> Service exists, but is not installed

To display a service's health status in the Administrative Client, navigate to **Health Center** and click on a service.

The following information displays:

*Physical Status*

> Service started / stopped / stating
>
> The Watchdog Service operates the physical statuses.

*Log Level*

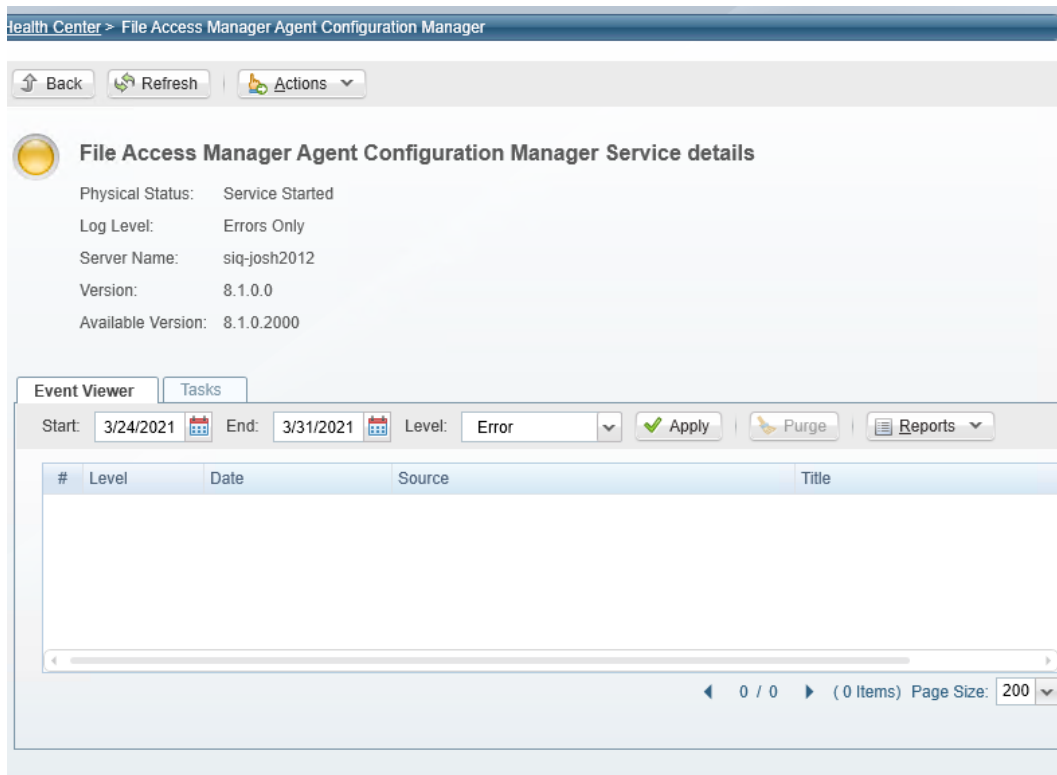> Current (running value) log level (DEBUG/INFO/ERROR)

*Server Name*

> The server on which the service is running

*Version*

The File Access Manager version that is running (as well as any pending versions)



1. Click **Refresh** to refresh the service health status.

2. Click **Actions** to perform one of the following actions on this service:

   - Change Log Level – It is not necessary to restart the service to change the log level. Changing the log level through the administrative client creates a task for a specific service to handle, and changes the log level in runtime. If you restart the service, the log level will be reverted to the original state (Error) by default until the next service restarts.

   - Restart Service

   - Start Service

   - Stop Service

The File Access Manager Watchdog Service performs the start, stop, and restart service actions. If you stop the Watchdog Service, there are no stop/start/restart service actions for services on that server.

It is not possible to stop, start, restart, or change the log levels of applications from the Health Center. You must perform a manual log collection, start, stop, or restart on:

The Watchdog Service

Any service with installed applications

*To gather system logs, in the Administrative Client, navigate to Health Center.*

1. Click **Actions**, and then select **Gather System Logs** (the only action available).

2. The system creates a task to handle log collection from the physical servers with File Access Manager installed. The task gathers all the logs, compresses them into a zipped file, and sends the link to the user (just as it sends a report to the user). You can view the logs (collected per physical server) in the Reports page of the File Access Manager web application.

*To view Health Center events:*

1. Click the **Event Viewer** tab to view events on the selected service.

2. Select a start date and an end date by clicking on the calendars next to the *Start* and *End* fields.

3. Select a level (Information, Error, Warning, All) from the **Level Field** dropdown menu.

4. Click **Apply** to apply the date and level filters.

5. Click **Reports**, and navigate to **Reports > Applied Filter Events > Produce Now** to produce reports on the selected service, based on the selected service.

*To view Health Center tasks:*

1. Click the **Tasks** tab to see a list of tasks related to the select service.

2. Check the **Show Tasks from all users** check box to show tasks related to the selected service from all users.

3. Click **Refresh** to refresh the list of tasks.

4. Click **Clear All** to clear the entire list of tasks.

## Viewing and Scheduling Health Center Reports

To produce or schedule the health center reports in the Administrative Client, navigate to the Health Center.

1. Select the report from the dropdown list

2. Select to run now, or create a schedule for a scheduled report.

3. To view the reports in the web client, navigate to **Reports > My Reports**.

You can produce the following system health reports from within the Health Center:

### *System Services Versions Report*

This report lists the current version of the installed services, and the service types

### *Services Health Report*

This reports lists the current status of the installed services.

*Service Status types:*

- Service Not Installed

- Service Running

- Service Down

- StandBy - This status refers to services that are in the inactive environment of a Disaster Recovery setup

### *Task Status Report*

This report lists all tasks from the last 24 hours.

### *Activity Summary Report*

This report shows the number of activities captured per application in the last 24 hours.

# Viewing System Messages on the Event Viewer

File Access Manager services forward important messages to the administrative console. These messages can be viewed in the Event Viewer on the administrative client.

To select event sources to view within the Administrative Client, navigate to **Event Viewer**.

1. Select the **Source: [x] Selected** button on the menu to open the source picker.

   The source picker button displays the number of sources selected previously.

2. Select a category from the **Categories Field** dropdown list.
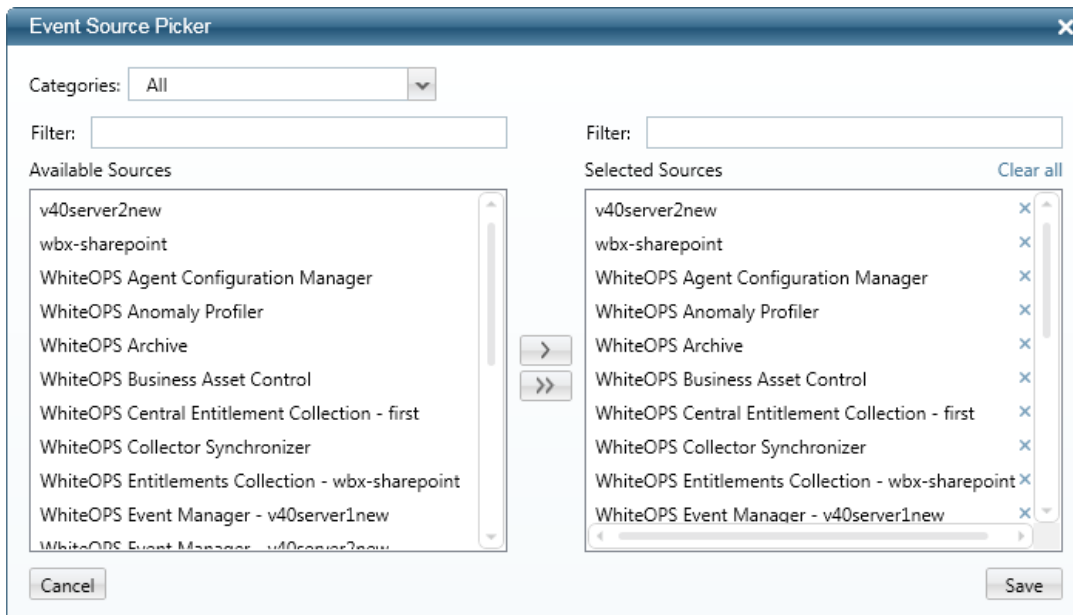


3. Type text in the *Filter* field (above either the Available Sources or the Selected Sources box) to search for sources listed in those boxes.

4. Select a source in the Available Sources box, and click **>** to copy it to the Selected Sources box, or click **>** to copy all the Available Resources to Selected Resources.

5. to delete a source, click the **X** next to it, or click **Clear All** at the top of the Selected Resources box to clear all the selected sources.

6. Click **Save** to save your selections.

7. Click √ **Apply** to refresh the screen with the selection.

8. The table displays a list of events from the selected sources.

***To filter events:***

1. Select a start date and an end date by clicking on the calendars next to the **Start** and **End** fields.

2. Select a level from the levels (Information, Error, Warning, All) available in the **Level Field** dropdown menu.

3. Click **Apply** to apply the date and level filters.

4. Click **Reports**, and navigate to *Reports > Applied Filter Events > Produce Now* to produce reports on the selected service, based on the selected service to delete events:

5. Define a filter defining the events to delete.

6. Click **Purge** to delete all displayed events that match the filtering criteria.

7. The following confirmation window displays: "Are you sure you want to delete all shown events?"

8. Click **Yes** to delete the event, or **No** to return to the Event Viewer window.

> File Access Manager saves events for 30 days, and automatically deletes them after that period.

## Licensing Model

File Access Manager uses an honor-based licensing method. The application does not manage or enforce these licenses.

## Impersonating Another System User

User Impersonation allows an Administrator to impersonate another system user for troubleshooting.

Authorized users gain access to the *User Impersonation* screen by clicking on a URL hyperlink, which is only available to administrators who are also Active Directory users with "Web User Impersonation" permission in the File Access Manager administrative client. This permission should be given to a role of which the user is a member.

If an unauthorized user attempts to activate user impersonation, an error message displays.
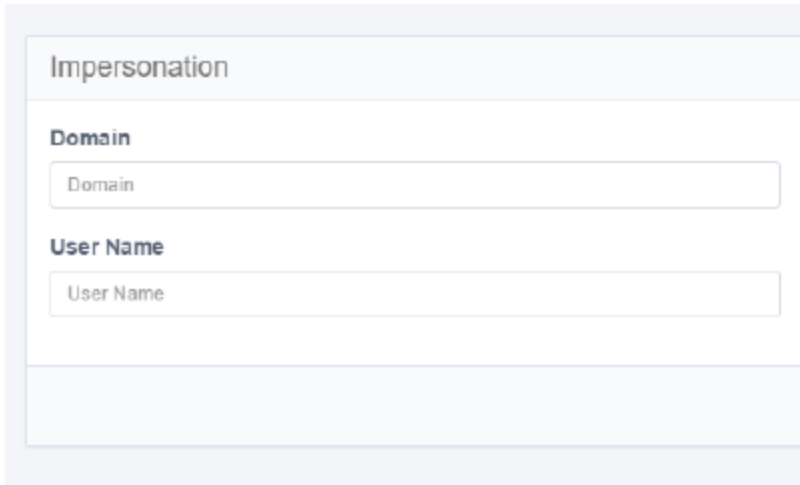
**To access user impersonation:**

1. Type the following URL to gain initial access:

   http://ServerName/SiteName/v1/#/impersonation

   For example: *http://server.example.domain/IdentityIQFAM/v1/#/Impersonation*



2. Type the User Name and Domain of the user to be impersonated, and click **Save**.

3. When the impersonation process finishes, a page with the new (impersonated) user credentials displays.

4. Click "Reset Impersonation" to cancel the impersonation.

5. If an unauthorized user clicks "**Reset Impersonation**", the page reloads with the same credentials.

   The system automatically cancels the impersonation when the server session expires. If left without action, the session will expire within approximately 20 minutes.

6. Click "**Discard**" to clear all fields.

# Updating File Access Manager Software

SailPoint publishes updates to the File Access Manager from time to time, as new releases, minor releases, and software patches.

When updates are available, the application can sends an email to the administrator to notify you of the update. This feature is disabled by default.

To enable this feature:

1. Update the database with the email address which the notification mail will be sent to, by running the following update statement:

   ```
   update [whiteops].[system_configuration_value] set [value] = N'[ENTER DESIRED
   eMAIL HERE]' where [name] = N'New Version Message To'
   ```

2. From the "*Scheduled Task Handler*" service server, edit the file "%SAILPOINT_HOME%\FileAccessManager\ScheduledTaskHandler\ScheduledTaskHandlerServiceHost.exe.config"

3.  In the "**appSettings**" section, change the "*newVersionCheckIntervalInMinutes*", from -1 (which means, do not check for new versions) to a desired check interval (in minutes).

    Save the file and close it.

4.  Restart the "*Scheduled Task Handler*" service.

After the service restart, an email will be sent if a newer version is available for download from Compass.

Please contact your SailPoint representative for further details, and to discuss the options for upgrade.

This feature requires there to be Internet access from the server.

# Audit Log

File Access Manager creates audit records for all activities performed in the web application. The audit log can be exported for use by external auditing tools.

## Audit Log Format

The audit log stores the following information per record:

*id*

> request_timestamp

*client_ip*

> request_params

*authorization*

> body_params

*endpoint*

> http_status_code

*authentication_method*

> user_roles

*request_uri*

> action_type

*http_method*

> action_description

The actions are mapped to the following action types:

- Delete
- Update
- Create

- Execute

- Read

## Audit Log Report

The administrator (or anyone with the right **Reports > Report Templates > Report Templates Administrator**) can configure a report to download as a subset of the audit log as an Excel report for a one-time report, or a scheduled report.

To configure an audit log report:

1. Navigate to **Reports > Report Templates**.

2. Type (or start typing) **Audit** into the filter and select Audit, to filter out all the available audit report templates.

3. If there is no report template that fits your needs, create a custom report by selecting duplicate from the **Audit Log Report menu**.

This will open the Duplicate Template panel Fill in the required fields, and either **Run Now**, or set a schedule.

- Time period - Time period to scan for activities. Last 7\30\90\365 days. The default is 'last 7 days'.

- Action type – Which action to report on, Or all actions. The default is 'All'.

- By default the template displayed only for user with "Administrator" role

- This report is limited to 1M rows.
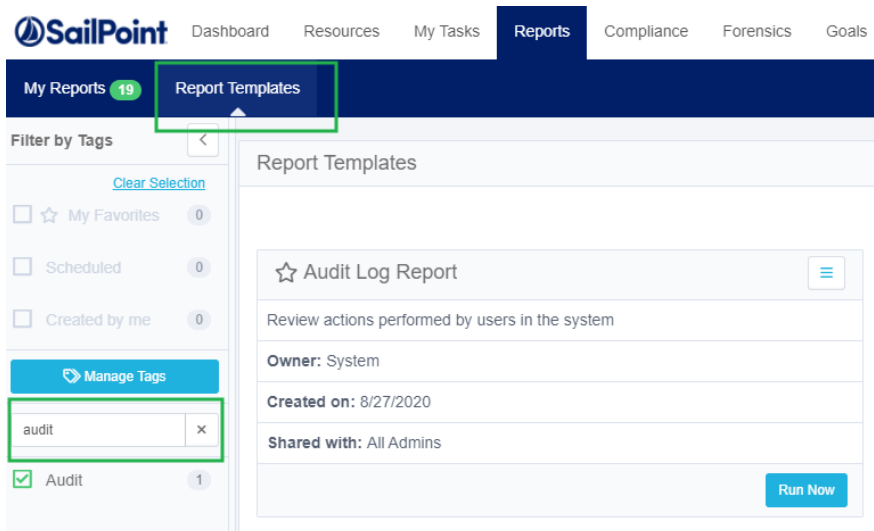


### *The Audit Log Report Fields*

The audit log report is a subset of the full audit log stored in the database. The report contains the following fields:

- User

- Role

- Host IP address

- Timestamp (UT)

- Action

- Action Description

# Managing the Data Dictionary

Data dictionary fields are attributes that define data types. You can modify this list to fit your organization and needs. Each data type has a separate list of data fields.

The list of data fields contains the fields for all data types. You can filter the list to display either all or a single data type.

> You can also create relevant data dictionary fields in the administrative client in the identity collector wizard and application wizard for home grown applications.

These Fields can be seen in the following features and pages:

- Enrichment

- Access request Template wizard

- Permissions \ Identities page.

When data dictionary fields are used in the Permissions \ Identities screens, and the user saves the queries, these queries can be used in campaigns.

These data dictionary fields can also be displayed in the scheduled report templates that were created from the filters set in the Permissions \ Identities page

- Access Request

- Access Certification

- Permissions

- Identities

Navigation:

**Admin > Permissions Management > Data Dictionary Fields**

Permissions:

This screen is accessible by default for users with administrator capability.

**Data Dictionary Fields**

New Data Dictionary Field

| Name | Field Type | Data Dictionary Type | Is Mandatory | | Actions |
|------|-----------|---------------------|--------------|--|---------|
| AA-New-HG-PT... | String | Permission Types | No | | ✏ 🗑 |
| AA-New-HG-Us... | String | Users | No | | ✏ 🗑 |
| AA-New-HG-Us... | String | Users | No | | ✏ 🗑 |
| abcdefghijklmn... | String | Business Resources | No | | ✏ 🗑 |
| ACL Type Allow? | Boolean | Permission Types | Yes | | ✏ 🗑 |
| adasdcqwe23 | String | Groups | No | | ✏ 🗑 |
| Application Gro... | String | Business Resources | No | | ✏ 🗑 |
| Application Type | String | Business Resources | No | | ✏ 🗑 |
| A-Test-For-Edit ... | String | Users | No | | ✏ 🗑 |
| Business Resour... | String | Business Resources | Yes | | ✏ 🗑 |

Rows per page  10 ⌄   11 - 20 of 110          Page  2  of 11  ‹ ›

# Data Types

The system supports managing the attributes for the following data types:

- Users
- Groups
- Business Resources
- Permission Types

# Filters

Pressing the filter icon will open the Filter panel. Type in and / or select the filter

The *Name* field filters the data dictionary fields using a "contains" operator.

**Apply**

Apply the filter and fill the grid accordingly

**Clear All**

Clear the filter, and fill the grid with all data

**X**

Close the filter panel without changing the grid output

# Data Dictionary Fields

Data dictionary fields are attributes that define data types. You can modify this list to fit your organization and needs. Each data type has a separate list of data fields.

**Name**

Field name

**Field Type**

The type of the attribute. For all user created attributes, the field type is "String"

### Data Type

The data type to which this attribute is associated. See the list of Data Types.

### Is Mandatory (Out of the box)/ system?

Yes / No. Fields that are mandatory cannot be edited or deleted.

## Actions

Each data dictionary field has the following Actions:

### Edit

Opens the Edit panel. Only the data dictionary field name can be changed.

This action button is disabled for mandatory fields.

### Delete

Delete the data dictionary filed.

This action button is disabled for mandatory fields.

A data dictionary field that is used cannot be deleted. Clicking the delete button, and clicking **Accept** will open a message showing the dependency

## New Data Dictionary Field

To create a new dictionary field:

1. Open the Dictionary fields page **Admin > Permissions Management > Data Dictionary Fields**.

2. Click **New Data Dictionary Filed**

3. Fill in the following parameters:

   ### Name

   The name of the data dictionary field. The name of the data dictionary field must be uniqe, even if it has a different data type.

   ### Data type

   The data type this attribute is associated with.

   New data dictionary fields created will be non mandatory, and of field type "String"

4. Click **Save** or **Cancel**.

# Managing File Access Manager Users

All the users of the business resources you want to monitor are potential File Access Manager users.

You will need **administrators** configuring and monitoring the system, **data owners** of particular areas of the business resources , verifying that the users (employees, bots, and other entities) that require access to resources in their control have the appropriate access, and other users do not.

In order to Users in File Access Manager

This chapter describes how to create, delete, manage, and authorize users in File Access Manager. It also discusses several processes available under the System tab.

- User access terminology
- Creating or importing users
- Assigning permissions to users
- Assigning scope to users
- Data Ownership

## User Access Terminology

File Access Manager users have two main characteristics that determine their abilities in the system:

***Permissions***

> Determine **what** a user has rights to – mainly in terms of screens the user can access, and actions the user can perform on each screen.
>
> Naming convention: The name is in most cases the path to the screen or button being permitted
>
> *Permission* name – the path in the File Access Manager Administrative Client
>
> *Right* name – the path in the File Access Manager website

***Scope***

> Determining which application, and **which business resources** within each applications a user has a right to perform these actions **on** - Business Resources that the user is allowed to see on the screens, run reports on, or any other activity enabled by the user's permissions.
> For example, an Auditor has the **right** to run all reports, but only on the data limited by the **scope** assigned to him or her.

As stated previously, these access parameters are configured separately for the File Access Manager Administrative Client and the File Access Manager website, The terms below are used in each user interface:

| `` | Allowed screens and actions | Allowed resources |
|---|---|---|
| Admin Client File Access Manager Administrative Client | Role<br><br>(and permissions within | Data Role |

| ` | Allowed screens and actions | Allowed resources |
|---|---|---|
| | roles) | |
| File Access Manager website | Capability<br><br>(and rights within capabilities) | User Scope |

***Permission***

>   Defines a page or activity on a screen in the application that user can access

***Capability***

>   An aggregation of permissions

***Users***

>   Are assigned to one or more capabilities

## User

The user is an object that represents an account associated with a permission.

Standard user attributes include:

***User type***

>   User, orphan, or local

***User disabled / enabled***


***User domain***

>   The security domain in the identity store in which the user is defined. For example, you can define the identity store as an Active Directory forest, in which you define the User in one of the domains of the forest.

User data is commonly part of an identity collector connected to a relevant identity store.

For example:

- **Identity Store** = Organization's Active Directory.

- Extended Attributes:

    ◦ Department

    ◦ Manager

## Capability

A capability is a set of rights. Assigning a capability to a user grants him or her these rights.

A right allows a user to perform an action in the File Access Manager Administrator Guide, such as pressing a button or opening a page, or in the File Access Manager website, such as using the navigation menu. If the user lacks a right, the relevant page or button will be either unavailable or grayed out.

Since a user can be associated with multiple capabilities, the user's rights will be the total of all the user's rights in all the user's capabilities.

> Administrators in the administrative client are admins in the File Access Manager website as well. Administrators in File Access Manager website, on the other hand are not automatically administrators in the administrative client.

## Role-Based Access Control

Capabilities can be created and configured to fit your needs. This is best done during the File Access Manager installation phase.

> Except as stated above, capabilities apply only to the interface in which they are assigned.

At least one super user (a user with the capability of Administrator) should be defined as an Administrator, with access to both the File Access Manager Administrative Client and File Access Manager website systems. . You must first define an Administrator with the assigned capability of Administrator in the File Access Manager Administrative Client before that Administrator can access File Access Manager website.

After logging into the File Access Manager website, an Administrator can assign different capabilities to users in the File Access Manager website.

| Admin Client | File Access Manager website | File Access Manager DB |
|---|---|---|
| 1. Log in as the system user<br>2. Create administrator user (s).<br>3. Log in as administrator user<br>4. Change the system password | | Optional: Create custom capabilities |
| | Log in as administrator user | |
| | Assign user access within the web client | |
| | Capabilities (Assigning functionality and screen access) | |
| | User scope (applications and directories a user is allowed to access) | |

| Admin Client | File Access Manager web-site | 🖳File Access Manager DB |
|---|---|---|
| Optional: Assign user access within the administrative client<br><br>- Roles (assigning functionality)\<br><br>- Data roles (defining valid applic-ations) | | |

## Security Objects

The File Access Manager security objects include:

- User

- Role

- Data Role

# Creating and Deleting Users

Users in File Access Manager This section describes the process of managing users who are assigned administrative roles either in the administrative client or in the web client. User management includes the following:

- Listing users

- Creating or modifying users

- Deleting users

## Listing Users

The Users section in the File Access Manager Administrator Guide is under the Applications > Configuration menu.

1. <span style="background:#13357a;color:white;border-radius:12px;padding:2px 8px">Admin Client</span> Navigate to *Applications > Configuration > Manage File Access Manager Permissions > Users*

2. Double click on a user (or click **Edit**) to view that user's details.

3. A window with the user's details displays with the following data fields:

   ***Username***

   > A unique user ID

   > For users who must authenticate to AD, this must be identical to the AD user name in the authen-tication store.

   ***Full Name***

   > The user's full name

   ***Description***

   > The user's description

### *Log in Timeout*

Inactivity logoff timeout

### *Suspended*

A flag to internally suspend the user

### *Password*

This is required to identify internal users

### *Is AD User?*

Checking this check box grays out the password fields and marks the user for AD authentication

### *Connected AD User*

Internal users must be associated with an AD account to be able to generate reports and access the business user portal. When the account name is set here, the internal user is associated with the AD account permissions and email address.

In addition to these fields, roles (functions) can be associated with users and data roles so those users can view information on applications.

By default, users are associated with the "All" data role, which grants access to all applications

4. Type any changes in the relevant fields

5. Click **Save** to save the changes or **Cancel** to retain the user's details before making changes

6. The Users' window displays

## Creating Users

### *To create users in File Access Manager:*

1. <span style="background-color:navy;color:white;"> Admin Client </span> Navigate to *Applications > Configuration > Manage File Access Manager Permissions > Users*

2. Click **New** to add a new user

3. An empty user details window displays

4. Type the information for each field listed in the List Users Section

5. Click **Save** to save the information and return to the Users window, or click **Cancel** to return to the previous window

User Data Window

## Deleting Users

Complete the following steps to delete a user:

1. To delete users, perform the following steps:

2. In the Administrative Client, navigate to **Applications > Configuration > Manage File Access Manager Permissions > Users** to open the Users window.

3. Select a user to delete.

4. Click **Delete**.

5. A Confirmation window displays, asking if you are sure you want to delete the user.

6. Click **Yes** to delete or **No** to cancel the deletion.

> This action is irreversible.

# Managing Roles

Roles are a way to assign permissions to users in the File Access Manager Administrative Client. Role management includes the following tasks:

- Listing roles

- Creating and modifying roles

- Deleting roles

- Assigning users to roles

***To open the roles screen:***

In the Administrative Client, navigate to **Applications > Configuration > Manage File Access Manager Permissions > Roles**

A Roles window displays, listing the role names and descriptions.

> "roles" are called "capabilities" in the File Access Manager website , and are managed separately.

## Creating or Modifying Roles

To create or modify roles, complete the following steps:

1. In the Administrative Client, navigate to **Applications > Configuration > Manage File Access Manager Permissions > Roles** to open the Roles window.

2. Click **New** or Select a role, and click **Edit**.

   This will open the role data window.

Fill in the relevant fields, moving permissions between the Available Permissions list and Role Permissions list as desired, using the move buttons > < >> << .

***Role Name***

> The role unique identifier

***Description***

> The role description

***Role Users***

> Add or remove users from the role

***Permissions***

> Add or remove permissions from the role

Every permission can be associated with one or more roles

3. Click **Save** to save the changes

   or

   **Cancel** to retain the role details before making changes.

## Adding roles to a user (Administrative Client)

To add or remove a role from a user, complete the following steps:

1. Open the Edit User panel.
   In the Administrative Client, navigate to **Applications > Configuration > Manage File Access Manager Permissions > Users**.

1. Select and click on the user to update.

2. Drag roles between the Available Roles list and the User Roles list .

3. Click **Save** or **Cancel** .

## Adding a Permission to a User (Administrative Client)

Permissions are listed as the path within the File Access Manager Administrative Client To add a permission to a user, you must first identify the permission in the list of available permissions.

### *Example: Grant a User the Permission to Configure responses for activities*

As an example, we will try to grant a user permission to configure responses for activities.

1. First you must identify the permission path for this screen within the File Access Manager Administrative Client. The path for accessing this screen is:

   Admin Client   *Applications > Configuration > Activity Monitoring > Responses> Manage Responses*
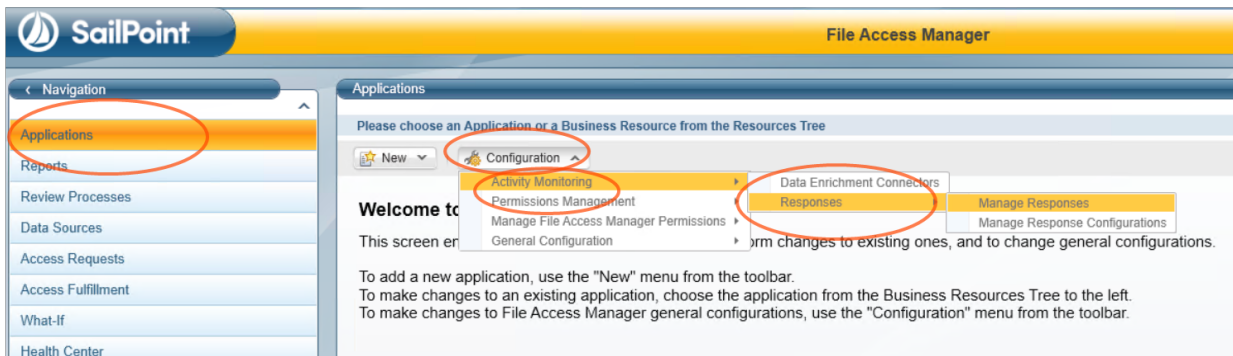


2. Next you should identify this permission in the list of permissions, by drilling into the detail of a role (any role) in
   **Applications > Configuration > Manage File Access Manager Permissions > Roles**,and checking the
   **Role Permissions** list. This is the list of permissions that are assigned to the selected role. Note that the permission window can scroll to show longer permission paths.

   In this case, the closest permission is:

   **Applications > Configuration > Activity Monitoring > Responses**

3. Once identified, you can add this permission to a user in one of three ways:

   - Find a role that already has this permission, and assign the user to this role

   - Add this permission to an existing role, and verify that the user has this role. (Note that this permission will be added to users with this role.)

- Create a new role that includes this permission, and add it to the user
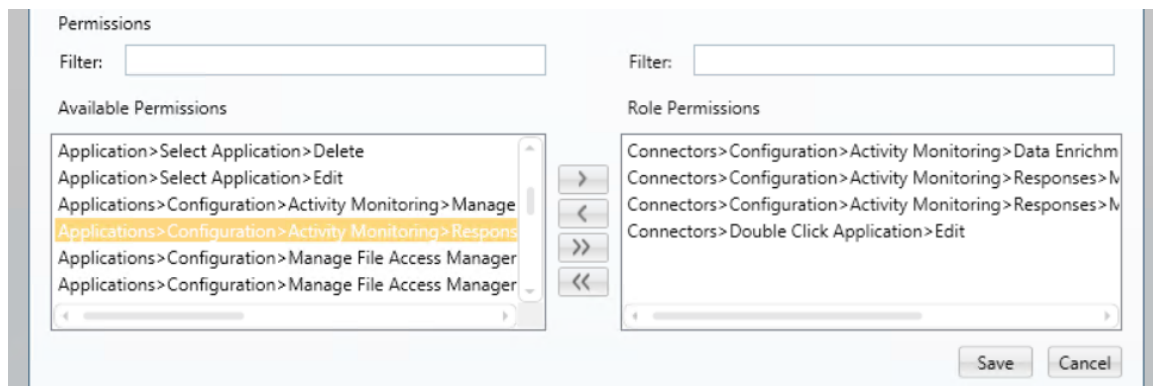


## Deleting Roles

To delete roles, perform the following steps:

1. In the Administrative Client, navigate to **Applications > Configuration > Manage File Access Manager Permissions > Roles**.

2. A Roles window opens.

3. Select a role to delete.

4. Click **Delete**. A Confirmation window displays.

5. Click **Yes** to delete or **No** to cancel the deletion.

> This action is irreversible.

# Capabilities (Web Client)

Capabilities in the File Access Manager websitedetermine what pages and actions the users can access in File Access Manager. Capabilities are groups of rights, where a right grants access to an action or a particular page. By assigning a capability to a user, the user is given these rights.

File Access Manager comes with several capabilities configured out of the box (see System Capabilities), and more can be configured together with SailPoint professional services to meet your needs.

## Basic Rights Granted to all Users

There are a set of basic rights granted to all users. These rights cannot be revoked.

- Make access requests (This right can be turned off in the settings)

- Access reports that have been generated for them

- Respond to certifications, access request approvals, and manual fulfillment tasks assigned to them

## System Capabilities

The capabilities below are system capabilities, shipped with the default configuration of File Access Manager. You can create custom capabilities to fit your needs.

> Warning: The system capabilities described below should not be removed or modified

## *Auditor*

The auditor capability is designed for users who perform internal audits, and assist in external audits, on user access information within the organization.

***Rights***

- See and manage all reports

- See and run the forensic screens

- Delete report templates

- The Auditor capability is assigned **Full Scope** by default (See Scope section below). This allows users in this capability to see and run reports on all resources. It does not allow the auditor users actions that require specific resources assigned to them.

  This capability does not have permission to delete query results from the Activity Forensics screen.

## *Data Owner*

This is a capability automatically associated with anyone assigned as an owner of any business resource. Users who are assigned this role will be the data owners of all the resources in their scope.

***Rights***

- See and manage user access information around business resources in their scope

## *Compliance Manager*

***Rights***

- Configure and manage certification templates and campaigns

- Configure data classification policies, rules, and policy objects

- View data classification forensics. (This does not include the Activities)

- See and run most reports. (This role does not have the right "`Report Templates Administrator`". See Special Rights.)

- The Compliance Manager capability is assigned **Full Scope** by default (See Scope section below). This allows users in this capability to see and run reports on all resources. It does not allow the compliance manager users actions that require specific resources assigned to them.

## *Administrator*

The administrator has all the rights in File Access Manager enabled, except for **Reviewer**. See Special Rights section below.).

***Rights***

- The administrator dashboard view and statistics

- See and manage user access information around all business resources

- Configure and run data owner election processes

- Configure settings for the File Access Manager website

- Access rights granted to anyone with Administrator capability in the File Access Manager website or File Access Manager Administrative Client

- The `Report Templates Administrator` right. (See Special Rights section below)

- The Administrator capability is assigned **Full Scope** by default (See Scope section below). This allows users in this capability to see and run reports on all resources. It does not allow the administrator users actions that require specific resources assigned to them.

The default capabilities are set with the rights to access the following screens (High level description):

| Capability <br><br> Screens | Administrator | Compliance Manager | Data Owner | Auditor |
|---|---|---|---|---|
| Dashboard | ✓ | | ✓a | |
| Resource | ✓ | | ✓ | |
| My Tasks | ✓ | ✓ | ✓ | ✓ |
| Reports | ✓ | ✓ | ✓ | ✓ |
| Compliance | ✓ | ✓ b | | |
| Forensics | ✓ | ✓ c | ✓ | ✓ |
| Goals | ✓ | | | |
| Settings | ✓ | ✓d | | |

Notes:

a. Data Owners see a limited version of the dashboards that is relevant to the capability.

b. The Compliance Manager cannot access the **Alert Rules** under the **compliance** menu.

c. Compliance Managers have access to the Data Classification Forensics page only.

d. Compliance Managers' access to the Settings screen is limited to the Access Certification Message Template.

For a full description of the rights set per capability, see the `web_permission` table in the File Access Manager database.

The capabilities in your system can be modified, and new capabilities added by the administrators and implementation teams, and might differ from the table above.

## Special Rights

### *Report Templates Administrator*

The right **Reports > Report Templates > Report Templates Administrator** is an administrator level right. A user with this right can do the following:

- View all report templates

- Delete report templates

- Share report templates

### *Reviewer*

The reviewer is a central part of the review process involving Access Certification and Access Requests.

The reviewer right enables the user to approve access requests for resources that are in his or her scope, and the responsibility to review and approve the access certification process.

This right is not included by default in the Administrator capability.

The *Data Owner* and *Reviewer* are not necessarily the same entity. The *Data Owner* capability has the *Reviewer* right by default, but you could define a separate capability with the *Reviewer* right that is not a *Data Owner*.

## Viewing Capabilities

To view the existing capabilities, navigate to **Settings > Capabilities > Current Capabilities** panel

This will open a list of all the capabilities, with users and user groups associated with each capability. These will include the system out of the box capabilities, and any custom capabilities created by the users.

- To filter a single capability - Select a capability from the dropdown box

- Filter a user or user group using the filter, by typing a letter (not necessarily the first letter) in the name of a prospective user/group. The filtering of the output on the screen is automatic, as you type. This will filter out the users within the list of each capability.

Additional custom permission changes can be added with the assistance of SailPoint Professional Services or Partners.

## Adding or Deleting Capabilities to a User or Group (Web Client)

### *To add a user account to a capabilities list:*

1. Navigate to **Settings > Capabilities > Capabilities panel**.

2. Select the type of account: **Group** or **User account**.

3. Search for a user / group in the Account search box.

4. Select a capability from Capability dropdown box.

5. Click **Add** to add a selected user to a selected capability or click **Clear** to clear the selections.

6. Click **Add** to add the user-capability selection to the capabilities list.

When you have added user(s) to the list successfully, the system displays "User(s) added to the list." In green for five seconds. When you have removed user(s) from the list successfully, the system displays "User(s) removed from the list." In blue for five seconds.

***To remove a user account from a capabilities list:***

1. Navigate to **Settings > Capabilities > Capabilities panel**.

2. Find the account to remove, and click the **x** icon on the Actions column.

3. Confirm / cancel the deletion.

## Adding a Right to a User (Web Client)

Adding a right to users is similar in concept to adding permissions to users in the File Access Manager Administrative Client.

> Capability management activities such as listing rights in each capability, adding rights to capabilities, and creating new capabilities are performed in the database. These permission changes can be added with the assistance of SailPoint Professional Services or Partners.

1. Identify the right according to the path within the application to the screen, panel, button and / or functionality to which we want to define the right.

2. Add a capability that has this right to the user, in one of the following methods. The steps are divided to activities done in the database, and in File Access Manager website:

| **Database** | | Web Client |
|---|---|---|
| Find a capability that has this right | | Assign the capability to the user |

This will add all the other rights in this capability to the user as well

or

| | | |
|---|---|---|
| Add this right to an existing capability | | Add this capability to the user (if necessary) |

This added permission will be granted to all users that have this capability

or

| | | |
|---|---|---|
| Create a new capability that includes this right | | Add it to the user |

## Scope

The scope determines what applications and resources a File Access Manager user can access and run reports on within the application.

## Assigning Scope to Users

**Admin Client** Scope is assigned to users in the administrative client by assigning a **data role** to them.

Data roles can be defined in terms of applications that the user has access to. See details below.

**Web Client** User scope can be assigned to users in the web client. Data scope can be defined in terms of folders within an application that the user can access. See User Scope (Web Client scope) below.

## Data Role - Administrative Client Scope

A data role lists the applications that a user can access in the File Access Manager Administrative Client.

### Managing Data Roles

A user can be associated with one or more data roles, and will be able to access all the applications in every data role with which that user is associated.

***User access to data roles:***

The user's ability to query applications, such as Activities or Permissions, visible in the resource tree

### Listing and Deleting Data Roles

To list data roles, perform the following steps:

1. In the administrative client navigate to **Applications > Configuration > Manage IdentityIQ FAM Permissions > Data Roles**.

2. The Data Roles window displays.

3. To delete a data role, select a data role, and click **Delete**.

### Creating / Modifying Data Roles

***To create/modify data roles:***

1. In Administrative Client, navigate to **Applications > Configuration > Manage IdentityIQ FAM Permissions > Data Roles**.A Data Roles window displays.

2. Click **New** to create a new data role.

3. Click **Edit** to edit an existing data role.
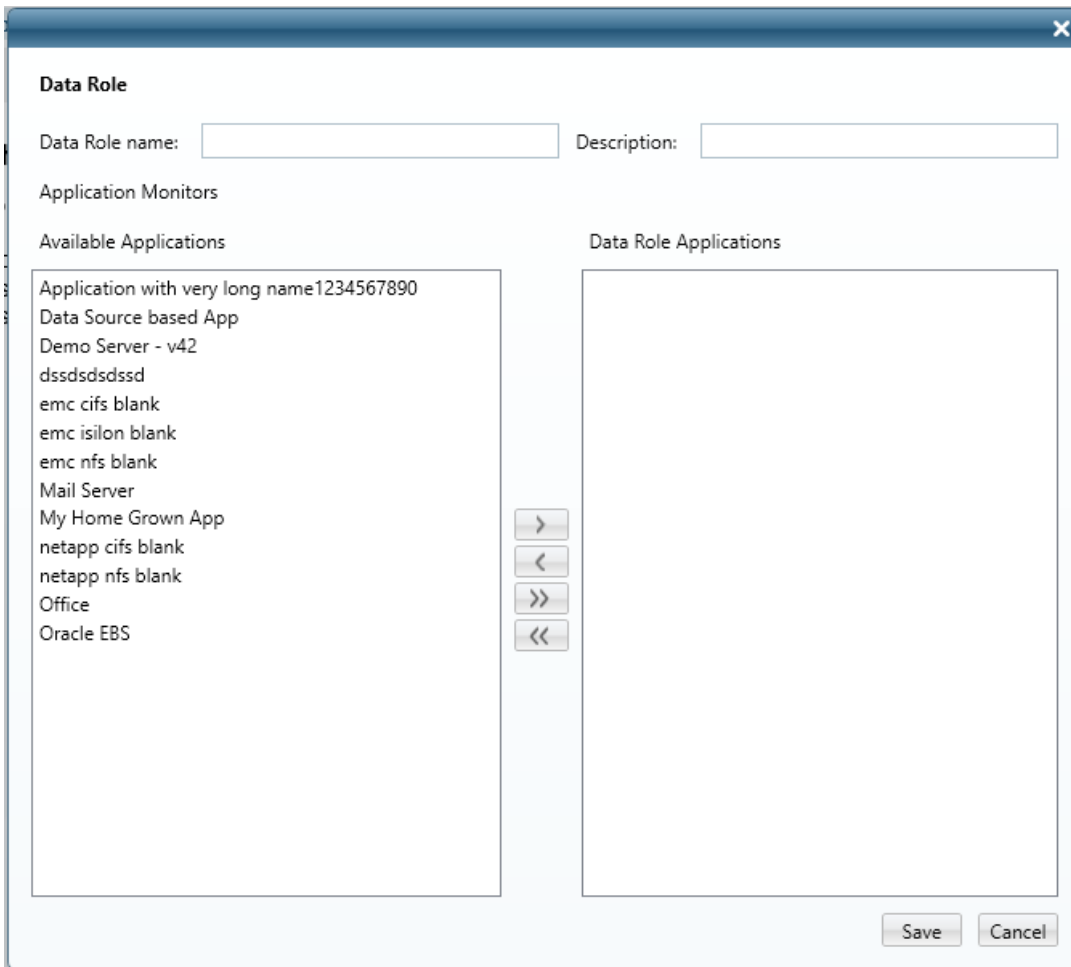


4. Fill in a name and description for the data role

5. Create a list of applications that this data role will be allowed to access by selecting applications from the **Available Applications** column and moving them to the **Data Role Applications** column.

## User Scope (Web Client scope)

### *Assigning User Scope to Users*

There are several ways of assigning scope to users in the File Access Manager.

- Administrators are assigned the *Full Scope* resource allocation (see below) automatically when they are assigned the capability *Administrator*.

- Bulk assigning of user scope, using *Import User Scope* (see below)

### *The "Full Scope" Resource Allocation*

- The resource allocation Full Scope is an administrator level allocation, to allow broad view and general system-wide statistics of the business resources.

- Full Scope is added automatically to Administrator users. It can also be added through the user scope import **Settings > Capabilities > Import User Scope**.

- You cannot remove the Full Scope from users of capability Administrator, even by using Import User Scope. To create an administrator that has less access than Full Scope, create a clone capability of Administrator, and upload the required coverage using User Scope Import.

### *What it allows*

Access to all resources in the dashboard and reports.

### *What it does not allow*

- Users with Full Scope, who are assigned with the capability Data Owner <u>will not be</u> data owners of the entire scope, but only of any user scope that is allocated to them specifically. This includes approving data owner request, approving access requests, etc. see Chapter Business Resource Owners for additional details.

- Drilling down from statistics in the Data Owner Dashboard will allow viewing only the resources to which this user has direct allocation. This means that in some cases, drilling down from a chart on the dashboard will display detailed charts (of partial scope) that do not add up to the totals that were on the dashboard charts (all scope).
  If an admin user has no directly allocated resources, the user will receive an error message, and an empty chart.

## *Import User Scope*

Users can be assigned resources in bulk, using a one time, or scheduled import process.

The list of users and scopes assigned to them are input when configuring the Data Source within the website under **Admin > Data Sources**. The data source could be any of the supported data sources, such as an Excel file or database table. The upload process setup includes mapping the source data fields to the File Access Manager user scope fields.

> The Import User Scope functionality supports changes and adjustments to existing scopes. New imports will not override existing scopes and manually-set data owners, but will retain or adjust the existing scope assignments based on the specified action. There is an Action field that will display one of four possible values:
>
> - Add – will add the resource to the User's Scope. This action can either have a full scope or a resource. If a resources is specified, the full scope is ignored. If a resource is empty, the full scope field must be true.
>
> - Remove – will remove the resource from the User's Scope. This action can either have a full scope or a resource. If a resources is already specified, the full scope is ignored. If a resource is empty, the full scope field must be true.
>
> - Clear – Will remove all resources from the user's scope. This command does not need any data specified in the "Application" or "Resource Full Path" columns. This operation will remove all resources from the users scope. This action can only have Full Scope set to true.

- Data Owner – Will function in the same way as "Add", but will also add the Data Owner capability to the user if it does not have it already. If the user already has the Data Owner capability - the "Data Owner" action will function just as "Add". This action cannot have a full scope. It must have a resource. Full scope is ignored and if the resource is empty, the line will be ignored as well.

*To import user scope:*

In the File Access Manager website, create a data source that contains the users and scope fields. See Creating Data Sources for a description on creating data sources.

Mapping the input fields is done at a later stage. The names of the fields, and any additional fields in the input data source won't affect the input process.

When setting the **Full Scope** parameter to TRUE, the record cannot contain other parts of resources, such as Application Name and Full Path, since it already contains all paths and applications.

The input source should contain the following information:

| Input field | Description |
| --- | --- |
| Application Name | Name of the application as it appears in File Access Manager |
| Full Path | Full path of the resource |
| Full Scope | TRUE / FALSE – granting the user full scope – all resources in File Access Manager |
| User Domain, User Name | Of the user to which to grant this access |
| Action | Possible actions related to resources include: Add, Remove, Clear, Data Owner |

*To set up the import process:*

1. In the File Access Manager website Navigate to **Settings > Capabilities > Import User Scope** to open the **Import User Scope** page.

    There is an Excel template file within the website that is there to serve as a basis for the datasource. There are explanations about the different actions within the template file. Click the provided link within the Import User Scope display for this preferred method.

1. Select the data source from the dropdown list. This list will contain data sources created in the administrative client.

2. Map the fields in your file to the File Access Manager fields listed on the panel.

3. Set the frequency of running the upload process.

4. Once / Periodically (set the recurrence parameters).

5. Click **Save** / **Cancel** to exit.

Adding or removing of the full scope will take affect the next time the user logs in. To force a user login, close the application, and wait ten minutes for the system to time out and log the user out.

# Review Process

The review process involves a review of permissions, access certification, access requests, or access fulfillments.

A review process consists of one or more levels, each level containing one or more reviewers. The reviewed permissions / violations go from the first to the last level in the process.

Each reviewer decides whether to approve or revoke a given permission or violation.

If there are multiple reviewers on a given level, the administrator can configure that level to require the approval of only one, or all, of the reviewers.

There are two types of review Processes:

***Static***

>Defining all reviewers at each level statically, disregarding the groups to which they belong

***Dynamic***

>Defining all reviewers at each level dynamically, based on the content of a permission field.

Reviewers can review many permissions during the review process. Each permission consists of several entities, consisting of these and other details:

- User
- Group
- Business Resource
- Permission Types

The permissions in the table below can serve as a simple illustration of a review process.

| User | Group | Business Resource | Permission Type |
|------|-------|-------------------|-----------------|
| John | Engineering | C:\R&D | Read |
| Mike | Accounting | C:\Finance | Full Control |
| Tom | Legal | C:\Legal | Read/Write |

The determination of the identity of the reviewer for the permissions to review, based on the values in the Group Column, with the following logic:

- Dave will review the Engineering group
- Marie will review the Accounting group
- Chris will review the Legal group

To accomplish this, we must provide File Access Manager with a Data Source having these conditions, mapped in a specific format.

Mapping identifies:

- Reviewer: User or Group?

- Reviewer Name

- Reviewer Domain7

The Data Source must contain a list of conditions that map a value to one or more reviewers.

A permission can consist of multiple fields, such as User Domain, User Type, Group Domain, Group Type, Permission Type, and the enriched fields of each basic entity.

Dynamic review processes types include:

### *Dynamic Applications*

With permission entity fields (User, Group, business resource, and Permission Type) used in review decisions. These review processes are relevant to campaigns in which the scope contains either an Application or a BR of a single application.

### *Dynamic Identity Collector*

With User/Group entity fields used in review decision. These review processes are relevant to campaigns in which the scope contains multiple Applications or BRs that share the same Identity Collector.

Review process activities include:
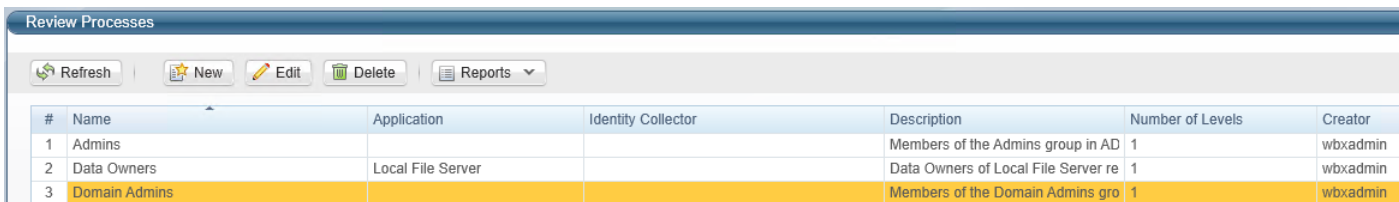
- Create a review process

- Edit a review process

- Delete a review process

# Create a Review Process

To create a review process, perform the following steps:

1. In the administrative client, navigate to **Review Processes**.

   This will open the Review Processes window.

   | # | Name | Application | Identity Collector | Description | Number of Levels | Creator |
   |---|------|-------------|--------------------|-------------|------------------|---------|
   | 1 | Admins | | | Members of the Admins group in AD | 1 | wbxadmin |
   | 2 | Data Owners | Local File Server | | Data Owners of Local File Server re | 1 | wbxadmin |
   | 3 | Domain Admins | | | Members of the Domain Admins gro | 1 | wbxadmin |

2. Click **New** to open the New Review Process Wizard.

3. Fill in a review name and description

4. Select the source type.

   - Application

   - Identity Collector

   - Static Levels Only

If multiple levels are involved, the levels can be a mixture of static and dynamic levels.

***Application***

Select the application to review from the *Application Data Field* dropdown menu.

***Identity Collector***

Select the identity collector to be reviewed from the *Identity Collector Data Field* dropdown menu.

If you want to change the source type after passing this screen, click **Cancel**, and start the wizard again.

5. Click **Next** to open the Levels Definition window (See below)

## New Review Process – Levels' Definition

The review process is composed of one or more approval levels. Each subsequent approver will receive the approval request only if the previous level approver(s) has approved the request. As part of the configuration you can set the number of required approves for a decision.

Each approval level defines the user, users or group who will be selected as an approver of the request at this level, according to the following logic:

***Dynamic Field***

Approvers are selected according to various requestor parameters.

***Static List of Users***

A constant list of approvers.

***Data Owners***

The data owners of the resource being applied.
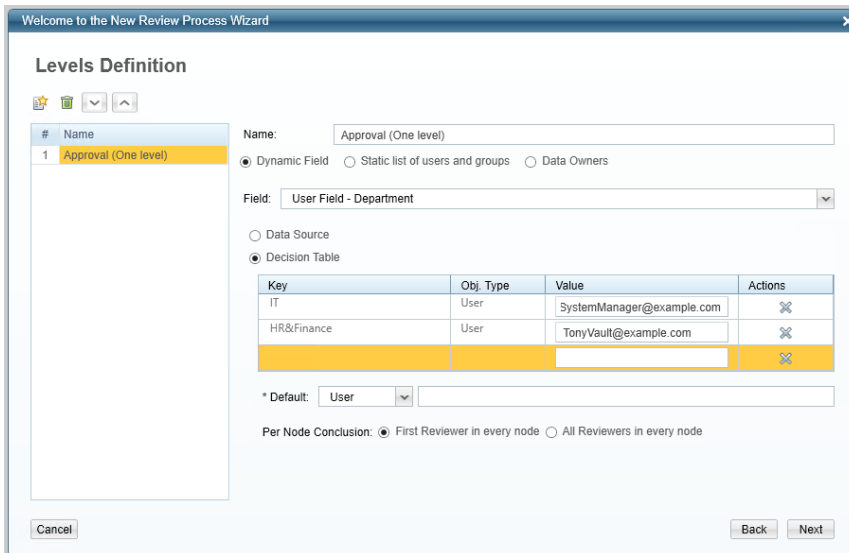
1. Click on [icon] to open a new level. The default name is "Level 1".

   Each level receives an automatic sequenced name: Level 1, Level 2, and so on.

2. Select one of the following, depending upon the type of field desired for Level 1: *Dynamic Field*, *Static list of users and groups*, or *Data Owners*.

   **Dynamic Field**

   If you select the dynamic field, then select Data Source or Decision Table.

   A Data Source gathers data from a source outside of the system, while a Decision Table gathers data from within the system.

   **Data Source**

   If you select Data Source, fill in the following fields:

   **Data Source Name**- *Select a data source name from the dropdown menu, to find the reviewer, and the following fields will be mapped with the data source:*

| | |
|---|---|
| Key Column | This field matches the data source with the relevant permission. Select a key column from the dropdown menu, and type a name for that key column. |
| Object Domain Column | This entity conducts the review. Select an object domain column from the dropdown menu or type a name for that object domain column.<br><br>This corresponds to the Reviewer Domain Name (ACME) in the Data Source Wizard. |
| Object Name Column | This column contains the name of the User or Group. Select an object name column from the dropdown menu or type a name for that object name column.<br>This corresponds to the Reviewer User/Group Name (Dave, Cam, Chris) in the Data Source Wizard. |
| Object Type Column | This column defines the type of reviewer (user or group). (This corresponds to the Reviewer Type (User) in the Data Source Wizard. |
| Default | This is the default data source. Select either User or Group from the dropdown menu, and then type in the name of the default User or default Group. The default User or Group can be the same as the entity in the Key Column of the Data Source. While the default entity may also be one of the entities listed in Key or Value, the system selects the default entity if no other entity is available. |

   **Decision Table**

   If you select Decision Table, the following columns of the Decision table must be filled in:

| | |
|---|---|
| Key | What to look for in the *Field* field above |
| Obj. Type | The User or Group of reviewers |
| Value | The user or group to which to send the review |

| | |
|---|---|
| Actions | Click on the X in this column to delete the corresponding row of the Decision Table. |
| Default | This is the default reviewer. Select either User or Group from the dropdown menu, and then type in the name of the default User or default Group. The default User or Group can be the same as the entity in the Key column of the Decision Table. While the default entity may also be one of the entities listed in Key or Value, the system selects the default entity from the authentication store if no other entity is available.<br><br>For more information on the authentication store, see File Access Manager Initial Configuration Wizard |
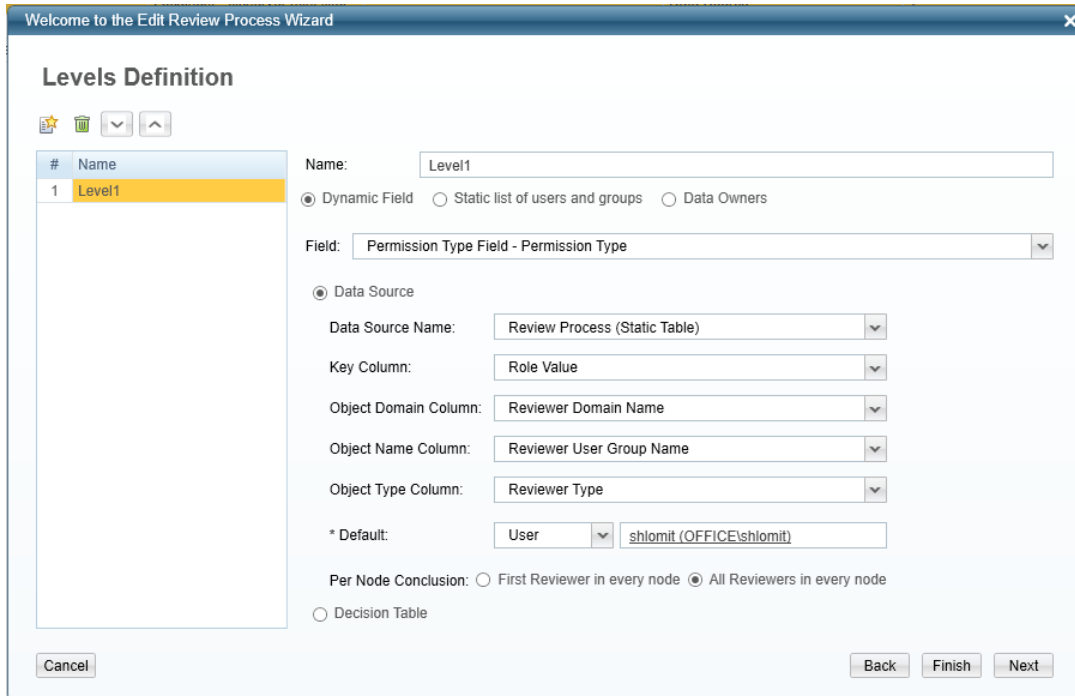


3. After completing the necessary values for either the Data Source, the Decision Table, under Per Node Conclusion, select either First Reviewer in every node or All Reviewers in every node.

***First Reviewer in Every Node***

> The first reviewer's approval of the review is sufficient.

***All Reviewers in Every Node***

> The approval must be unanimous. If one reviewer revokes, the entire review is revoked.

> The choice of first review or all reviewers may differ at each level.

a. If you select **Static list of users and groups** :

- Click inside the *Reviewers* field

- Select each entity to serve as a reviewer

- Click the **+** at the right of the field to add that reviewer

  b. If you select **Data Owner**

4. Click **Next**. The Review Process Permissions window opens.
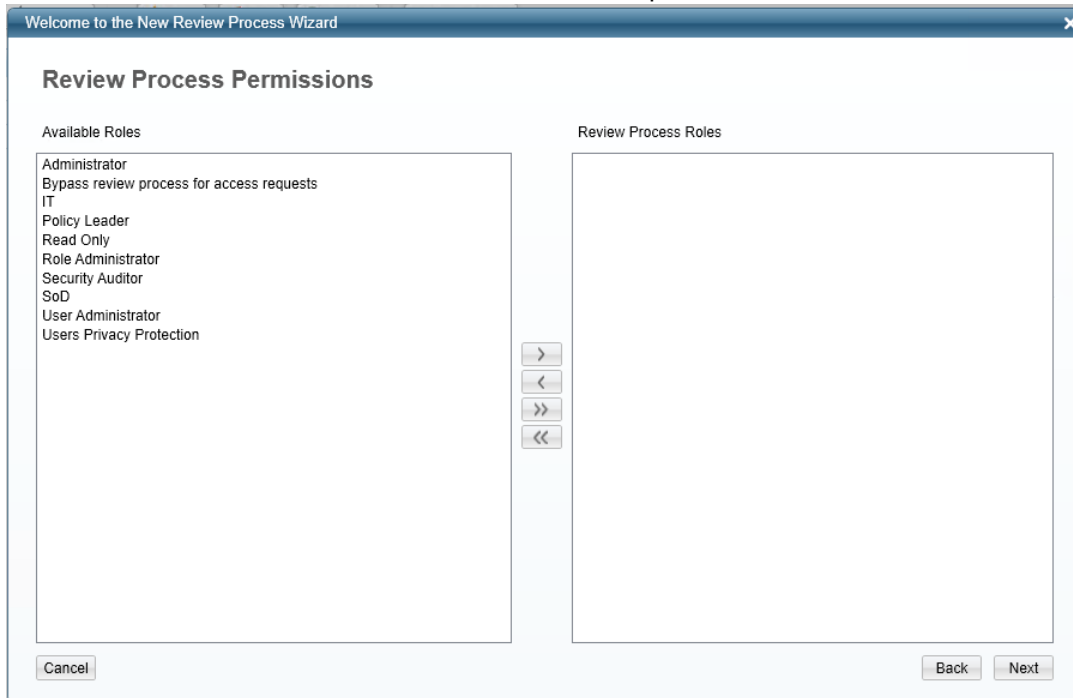


5. Click **>** or **>** to associate available roles to review process roles.

   The Review Process must be associated with at least one role. If not, a warning popup window displays.

6. Click **Next** to open the Review Process Summary Report window.

7. Click **Finish**.

8. The Review Processes window displays with a list of all the review processes.

# Business Resource Owners

Business resources in File Access Manager are assigned to users so they can see the resources in the various screens they are permitted to access. The BRs assigned to a user are defined as the user's **scope**. A business resources owner (Data Owner) is defined in the system as a user with user scope assigned to him or her, who has the capability "**Data Owner**". The Data Owner is the owner all the business resources that are assigned to him or her.

## Assigning Data Owners

You can select business resource owners through any of the following methods:

***manually - using the Data Owners page***

> Location: **Resources > Owners**
>
> See Assigning a Data Owner Manually

***Creating Goals - using crowd sourcing election.***

> Location: **Goals > Set New Goal**
>
> See Creating Goals

***Bulk upload – using the Import User Scope***

> (See section Import User Scope )

> This process only updates the user scope. You must add the capability **Data Owner** in order to make the user a data owner of this scope.

> The bulk assignment of data ownership overrides data ownership previously assigned to an individual business resource.

### Assigning a Data Owner Manually

By default, data owners will own the entire tree below the business resource they are assigned to, via data owner hierarchy.

To assign a data owner to a resource manually, we must first break the hierarchy.

***To add a data owner to a resource***

1. Navigate to **Resources > Owners**.

2. Select a resource from the resources tree on the panel on the left.

3. If there is a current owner inherited from a higher hierarchy, uncheck **Inherit data owners from [application] [business resource]** . There are two options for breaking the hierarchy:

   ***Yes***

   > Break the inheritance and remove the current owner(s).

   ***Yes – Copy the current owners***

Break the inheritance, and add a new owner in addition to the current owner(s).

4. Click **+ Add New Owner**.

5. Select the requested user, by tying part of the name, and selecting from the dropdown list.

6. Click **Save.**

# Data Owner Inheritance

The owner of a business resource is also the owner of the child business resource, unless you assign a different data owner to a specific child business resource.

If the business resource has an owner through *data owner inheritance*, there won't be a button to add an owner. Breaking the inheritance will allow assigning additional data owners at this level, and below.
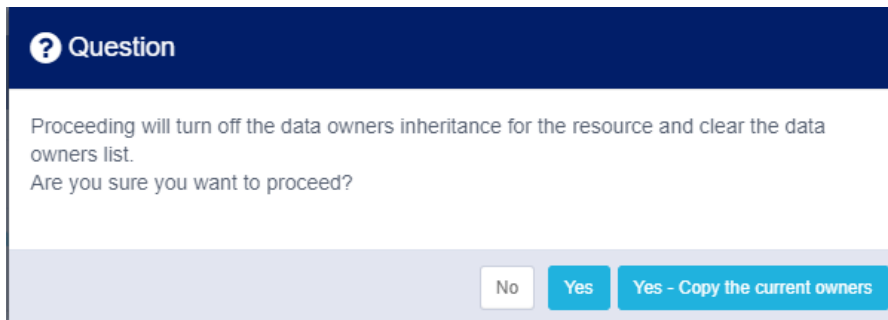


If you break the data owner inheritance, but do not assign a new owner, the data owner inheritance will be switched back on.

The new owner assigned to the business resource will be the owner of the current, and all downstream resources.

## Breaking Data Ownership Inheritance

In this example, Data_Admin is the owner of folder **C$\Data**.

You want to assign the folder **C$\Data\HR** to *Admin_HR*, and the folder **C$\Data\System** to the users *Data_Admin* and *Example_Ops*.

1. Navigate to **Resources > Owners**.

2. Assign a unique owner for HR:

   a. Select the folder C$\Data\HR on the Resource Tree.

   b. On the Current Owners panel, uncheck **Inherit data owners from [application]C$.**

   c. Click **Yes** to indicate that you want to break the inheritance, and not continue *Data_Admin* as the local owner from this branch down.

   d. Click **+ Add New Owner**.

   e. Select the user *Admin_HR* (you can starting typing the name, and select from the dropdown list).

   f. Click **Save.**

3. Assign additional owner for System:

a. Select the folder C$\Data\System.

b. On the Current Owners panel, uncheck *Inherit data owners from [application]C$* .

c. Click **Yes – Copy the current owners** to indicate that you want to break the inheritance, and add a new owner in addition to *Data_Admin* for this resource.

d. Click **+ Add New Owner**.

e. Select the user Example_Ops (you can starting typing the name, and select from the dropdown list).

f. The names Data_Admin and Example_Ops will be listed as current owners for this, and all downstream folders.

g. Click **Save**.

# Goals

Data Owners are responsible for protecting the data within a specific resource. Administrators use the **Goals process** so that those who are the most knowledgeable regarding the use of a specific resource can elect the most suitable data owners for a specific resource. This process uses a crowd sourcing process.

In the default configuration, only administrators can access and view the Goals tab.

*Activity*

Each selection of a data owner for a particular resource in a crowd sourcing process.

*Goal*

A collection of all the selections of data owners for a particular resource in a crowd sourcing process.

Therefore, a "goal" is a collection of "activities".

For example, if the goal is to determine the identity of the data owners for five business resources in a file server application, that goal consists of five activities – one for each resource.

## Goal Lifecycle Stages

*Creation*

First, an administrator creates goal activities, specifying the goal type, application, scope, and settings.

*Pending for Execution*

After goal creation, but before the system sends emails to participants, an administrator checks the goal status, including the goal participants selected, and the data owner candidates selected, to validate successful goal creation.

*Election*

After goal execution, participants (who were decided upon in the creation process) vote for data owners.

Appointment – Reviewers review the selected data owners (unless the administrator choses the automatic selection of data owners.

*Finished*

A goal is completed when all the goal activities have been completed (for example, all data owners have been assigned).

You can block users from being eligible for elected as data owners, using the Goals Exclusion setting. See section Excluding Accounts from File Access Manager Processes.

## Creating Goals

The Set New Goal process consists of the following steps:

- Goal Type
- Application
- Scope
- Settings
- Summary

To set a new goal:

1. Navigate to **Goals > Set New Goal**.

2. Select the relevant goal type from the available types.
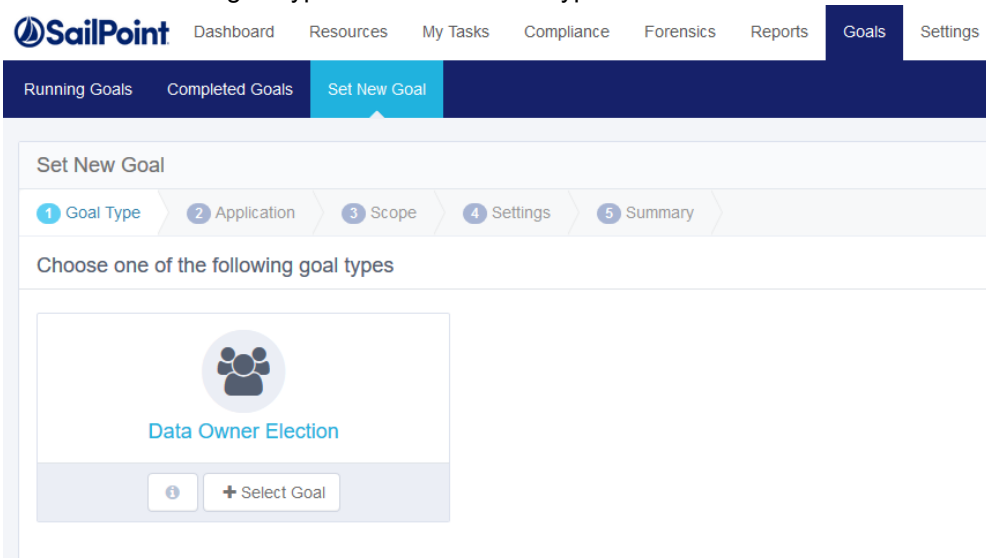


3. Click **Next** to select the Application .
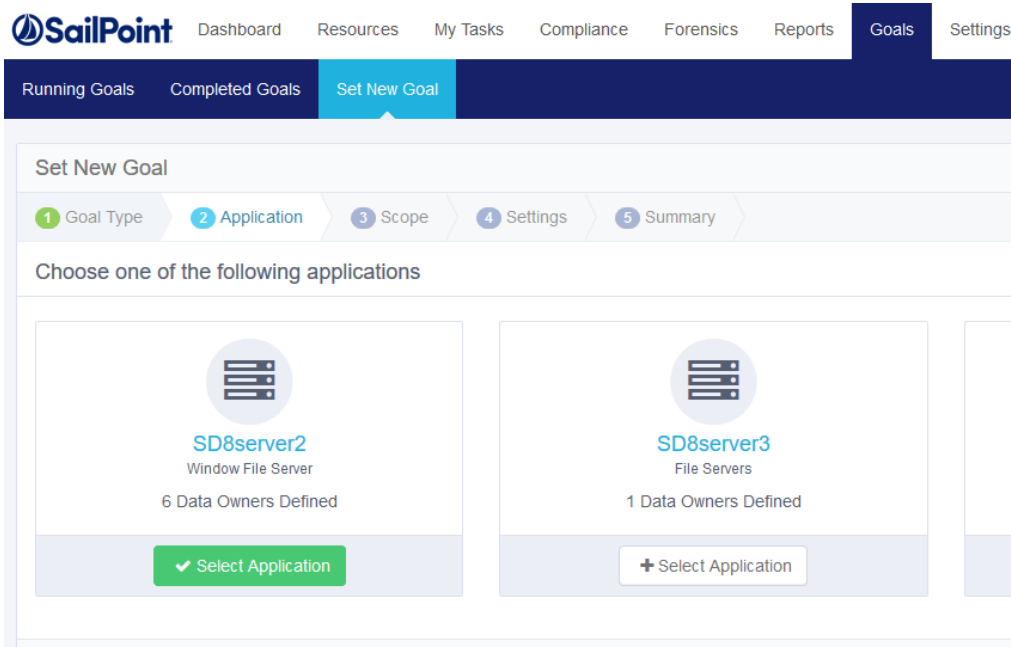
4. Select one of the applications displayed. The resources for this goal will be from the selected application.

5. Click **Next** to set the scope.
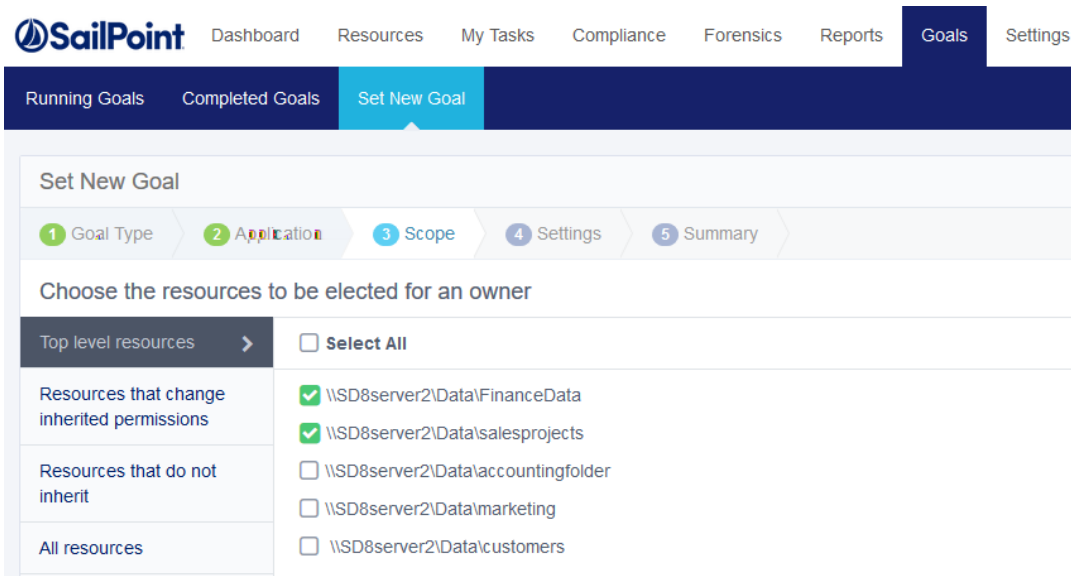


6. Select resources (one or more) from any of the categories, including:

   • Top level resources – Resources for a specific application from the top level of the resource tree

   • Resources that change inherited permissions – Resources that inherit permissions, with permissions added to those inherited permissions

- Resources that do not inherit – Resources that break an inheritance

- All resources – Resources from the entire resource tree

7. Check the check box next one or more resources to select that resource, then click **Add** under the resource list to add the resource as a new activity in the current goal.

   Check the **Select All** check box to select all the resources listed under each category.

   The number of resources selected displays in parentheses in "Resources Added", and the added resources are unchecked in the original resource list.

8. Click **Resources Added** to display a list of Selected Resources.

9. Click the blue **X** to the right of any selected resource in the list of resources to deselect that resource.

10. Click **Save** to save the revised selection of resources.
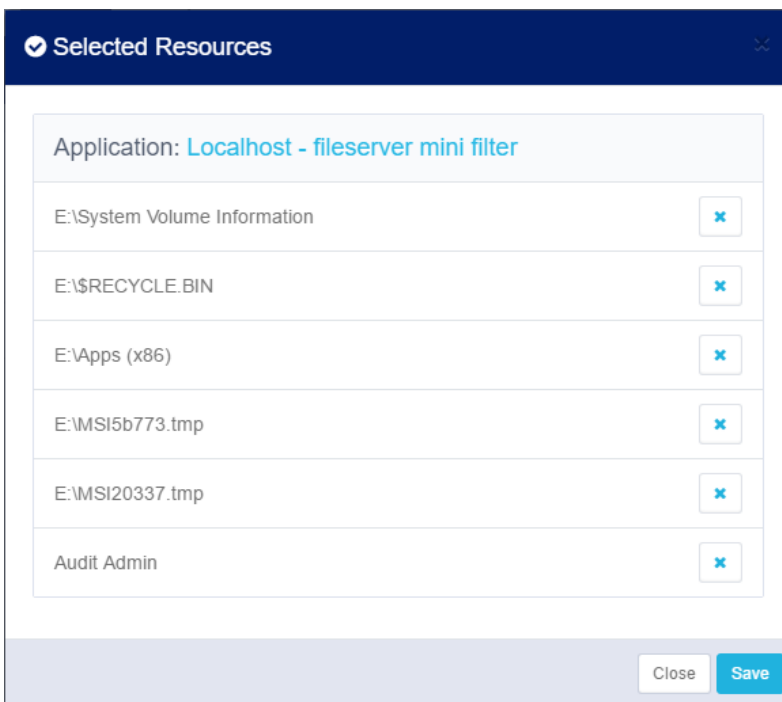


11. Click **Next** to open the Settings screen.

12. In the **Goal Name** text box, type an appropriate name for the goal.

13. There are two methods of finalizing data owners:
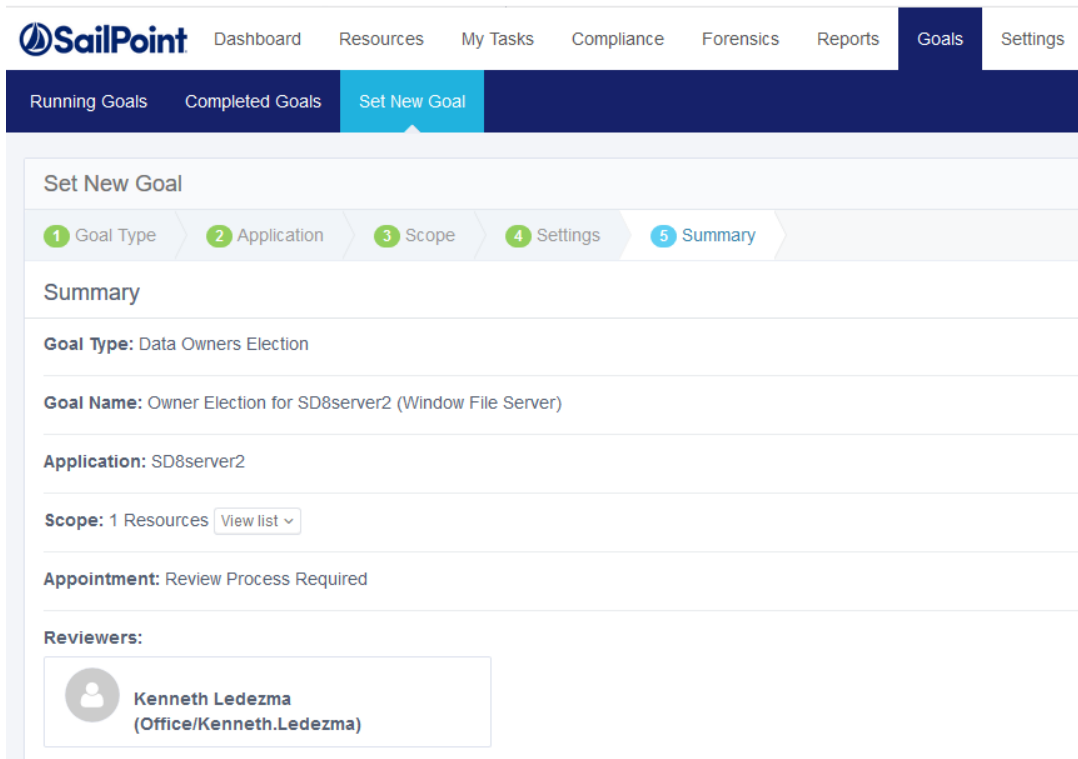
    *Review Process Required*

       A reviewer has to either approve or reject the selected data owners who were voted for, before their final appointment.

    *Automatic*

       Appoint selected data owners without a review based on the votes of the participants

14. If you select "Review Process Required":

    a. Select a reviewer by starting to type in the **Reviewers** text box.

    b. Select the blue x to the right of any selected reviewer in the reviewer list to deselect a reviewer.

15. Click **Next** to open the Summary screen.

The goal **Summary** screen lists the following information:

***Goal Type***

> The goal type, for example, Data Owners Election

***Goal Name***

> The name selected for the goal

***Application***

> The application for which a data owner is to be selected

***Scope***

> Number of resources

***Appointment Method***

> Either "Review Process Required" or "Automatic"

***Reviewers***

> Names of reviewers if the appointment method is "Review Process Required"

Click "View List" in Scope to view the selected resources.

16. Click **Create Goal** at the bottom right of the *Summary* screen.

17. A Success dialog displays, indicating that the goal was created successfully, and requesting that you execute the goal in "Running Goals".

18. Click **OK**.

## Goal Status

Administrators can manage goals more efficiently, by viewing the status of the goals before executing them.

To view status details for a newly created goal, perform the following steps:

1. Navigate to **Goals > Running Goals**.

   The Running Goals screen displays.
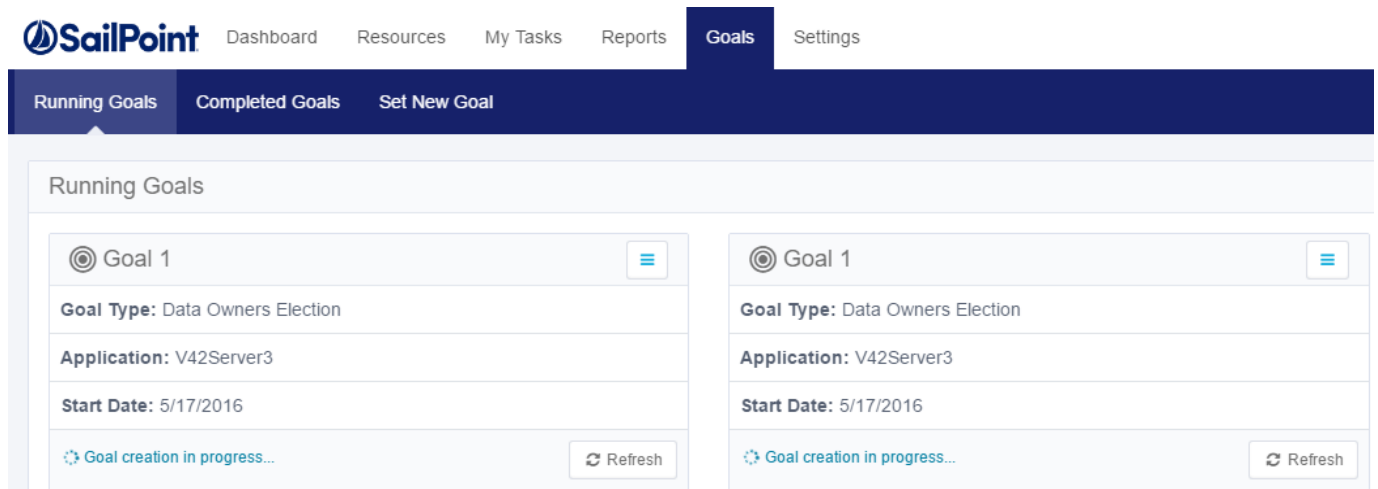


   If the goal is ready for execution, "Ready for execution …" displays in <span style="color:green">green</span> at the bottom left of the New Goal box.

2. Click **Show Status** at the bottom right of the Running Goals box.

   The status of the running goals displays, based on one of the following filtered statuses (the default being "All"):

   - All – Displays all the resources in this goal

   - Election – Displays resources in the Election state (pending completion of voting)

   - Appointment – Displays resources in the Appointment state (pending review)

   - Finished – Displays all the resources for which the Election and Appointment processes have been completed.

If no candidates were selected as data owners for a given resource, the message "There were no eligible candidates for the selected resource" displays to the right of the list of resource statuses.

3. Click **Menu** on the right top of the Running Goals window to display a dropdown menu of status activities.

The Running Goals status actions include:

***View Details***

Displays all the goal details

***Refresh***

Updates the goal status

***Reinitialize***

Starts the goal creation process from the beginning. The status will be "Ready for Execution" and the system will delete all votes. This action cannot be undone.

A Question dialog displays, asking if you are sure you want to reinitialize the goal. Click **Yes** to reinitialize, or **No** to return to the Running Goals screen.

***Delete***

Deletes the goal. This action cannot be undone.

A confirmation dialogue displays. Click **Yes** to delete, or **No** to return to the Running Goals screen.
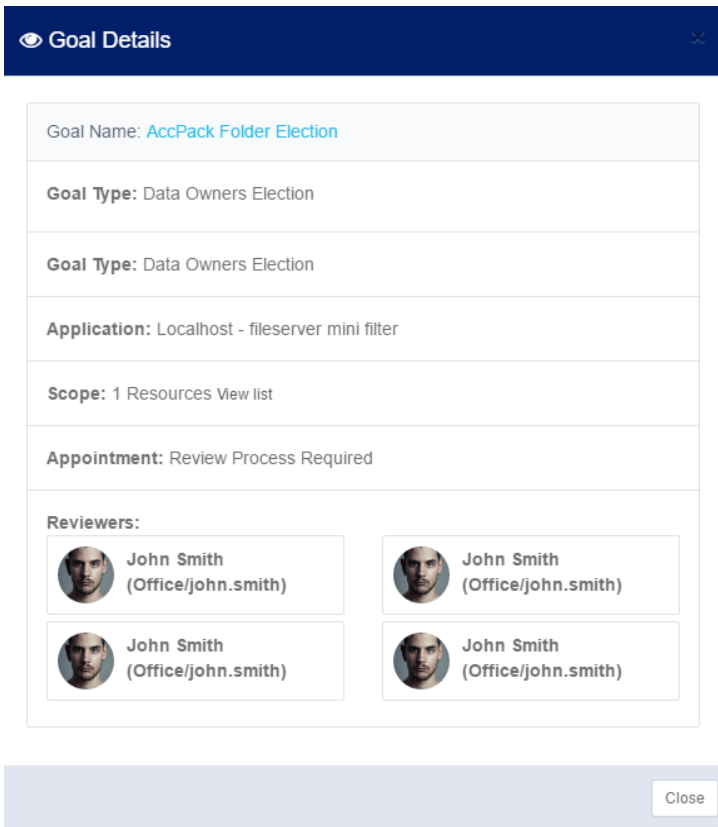


4. Click **Execute Now** at the bottom of the Running Goals box to execute pending running goals.
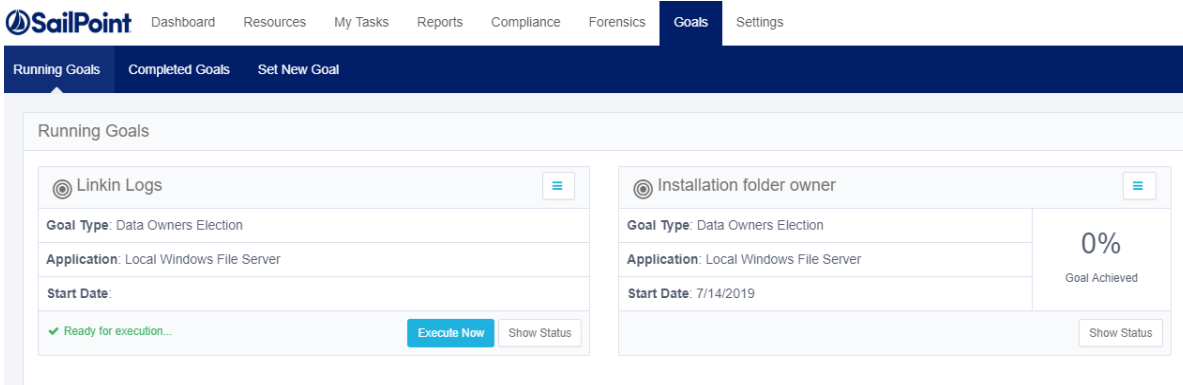


## *Completed Goals*

1. Click **Completed Goals**.

   A summary of the completed goals displays, including the following information:

   - Goal Type
   - Application

- Start Date

- End Date

- Percentage of Goal Completed

2. Click **Menu** on the right top of the *Completed Goals* window to display a dropdown menu of status activities.

The Completed Goals status actions include:

***View Details***

> Displays all the goal details.

***Reinitialize***

> Starts the goal creation process from the beginning. The status will be "Ready for Execution" and the system will delete all votes. This action cannot be undone.

> A confirmation dialog displays, reminding you that proceeding will result in the permanent loss of all the data for that goal.

> Click **Yes** to reinitialize, or **No** to return to the Running Goals screen.

***Delete***

> Deletes the goal. This action cannot be undone.

> A confirmation dialog displays.

> Click **Yes** to delete, **or** No to return to the Running Goals screen.
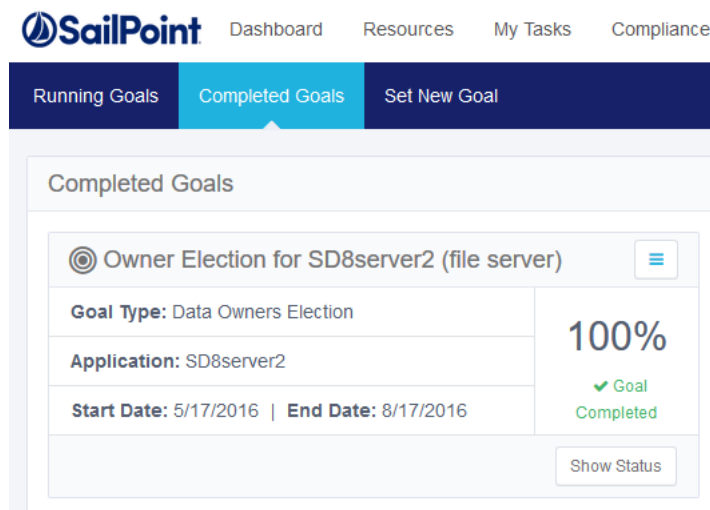


3. Click **Show Status** at the bottom right of the Completed Goals box.

After a user (for whom a review process was required) has voted, the system will add a review task to the reviewer's task list.

One user can be both a final candidate and a reviewer.

If a goal is ready for execution, it is possible to see the status of that goal before executing it, by clicking "Show Status" (to the right of "**Execute Now**" at the bottom right of each goal marked "**Ready for Execution**".)

If goal creation is in progress, "**Execute Now**" and "**Show Status**" are not available. The only available option is "Refresh".

To view status details for a newly created goal, Click **Show Status**



The Resources (left) section of the **Show Status** screen displays the number of total activities (resources) for the displayed goal have been finished.

In the Status dropdown menu under Resources, the following options are available:

- All – Displays all the resources in this goal

- Election – Displays activities in the Election state (pending completion of voting)

- Appointment – Displays resources in the Appointment state (pending review)

- Finished – Displays all the resources for which the Election and Appointment processes have been completed.

The bottom right of the Resources section displays the previous (Prev) or next (Next) screen, and the number of the total number of screens displayed (for example, 1/2 indicates that the first of two screens displays).

The Election section of the **Show Status** screen displays the "Current Results", which is the number of participants (out of the total number of participants) who have voted. Up to five data owner candidates may be displayed, with their names, place, and percentage of votes received. However, the first and second place data owner candidates are given prominence.



Election Section of the Show Status Screen

1. Click "All Participants" in the top right of the Election Participants section.

2. A summary of the election participants displays.

3. The viewing options are:

- All Participants

- Voted – The number of all participants who have already voted.

- Pending – The number of all participants whose vote is still pending.

Navigation in the "All Participants" view of Election section of the Show Status screen is the same as in the Resources section of the Show Status screen.

1. Click **Remind** next to a user who has not yet voted to remind the user to vote.

2. Click **Votes** next to a user who has voted to see a list of the people for whom that use voted.

1. Click **See Summary** in the top right of the Election section to return to the Summary view.

2. Click **End Election Process** in the top right of the Election section to end the election process even if it does not include 100% of the votes.

3. A Question dialog displays, asking whether you want to end the election process.

4. Click **Yes** to end the election process or **No** to return to the previous screen.

## Completed Goals

Navigate to **Goals > Completed Goals**.



A summary of the completed goals displays, including the following information:

- Goal Type

- Application

- Start Date

- End Date

- Percentage of Goal Completed

## *Status Activities*

Click **Menu** to display a list of status activities.

The Completed Goals status actions include:

### *View Details*

Displays all the goal details, as shown below.

### *Reinitialize*

Starts the goal creation process from the beginning. The status will be "Ready for Execution" and the system will delete all votes. This action cannot be undone.

A confirmation dialog displays, reminding you that proceeding will result in the permanent loss of all the data for that goal.

Click **Yes** to reinitialize, or **No** to return to the Running Goals screen.

### *Delete*

Deletes the goal. This action cannot be undone.

A confirmation dialog displays.

Click **Yes** to delete, **or** No to return to the Running Goals screen.

## *Show Status*

Click **Show Status** at the bottom right of the Completed Goals box

A panel will open with the results of the Goal, and the users selected.

There are two final candidates pending the review of one reviewer. After a user (for whom a review process was required) has voted, the system will add a review task to the reviewer's task list.

One user can be both a final candidate and a reviewer.

If a goal is ready for execution, it is possible to see the status of that goal before executing it, by clicking "Show Status" (to the right of "**Execute Now**" at the bottom right of each goal marked "**Ready for Execution**".)

If goal creation is in progress, "**Execute Now**" and "**Show Status**" are not available. The only available option is "Refresh".

To view status details for a newly created goal, perform the following steps:

1. Click **Show Status**.

2. The Data Owners Election displays.
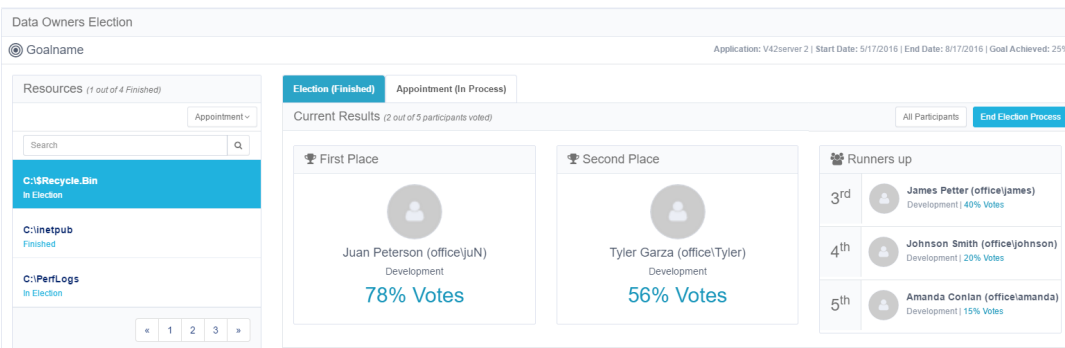
The Resources (left) section of the **Show Status** screen displays the number of total activities (resources) for the displayed goal that have been finished.

In the Status dropdown menu under Resources, the following options are available:

- All – Displays all the resources in this goal

- Election – Displays activities in the Election state (pending completion of voting)

- Appointment – Displays resources in the Appointment state (pending review)

- Finished – Displays all the resources for which the Election and Appointment processes have been completed.



The bottom right of the Resources section displays the previous (Prev) or next (Next) screen, and the number of the total number of screens displayed (for example, 1/2 indicates that the first of two screens displays).



The Election section of the **Show Status** screen displays the "Current Results", which is the number of participants (out of the total number of participants) who have voted. Up to five data owner candidates may be displayed, with their names, place, and percentage of votes received. However, the first and second place data owner candidates are given prominence.



Election Section of the Show Status Screen

1. Click "All Participants" in the top right of the Election Participants section.

2. A summary of the election participants displays.

3. The viewing options are:

   - All Participants

   - Voted – The number of all participants who have already voted.

   - Pending – The number of all participants whose vote is still pending.

Navigation in the "All Participants" view of Election section of the Show Status screen is the same as in the Resources section of the Show Status screen.



## All Participants View

1. Click **Remind** next to a user who has not yet voted to remind the user to vote.

2. Click **Votes** next to a user who has voted to see a list of the people for whom that user voted.
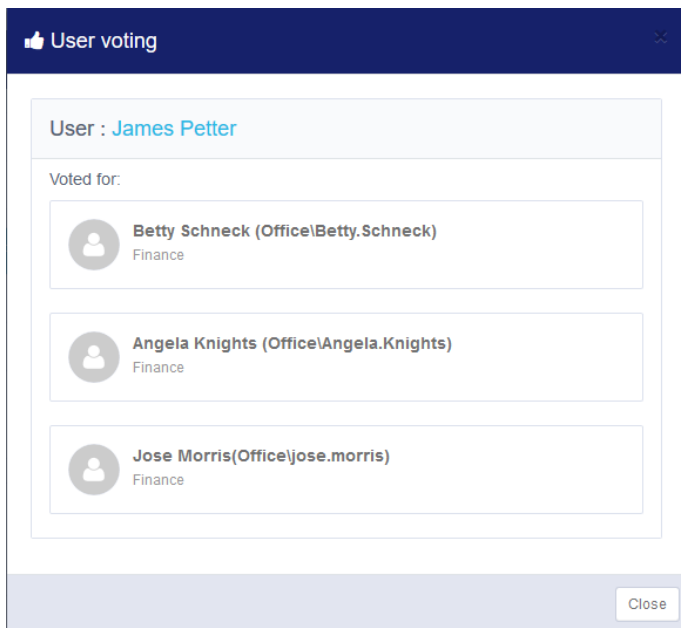
1. Click **See Summary** in the top right of the Election section to return to the Summary view.

2. Click **End Election Process** in the top right of the Election section to end the election process even if it does not include 100% of the votes.

3. A Question dialog displays, asking whether you want to end the election process.

4. Click **Yes** to end the election process or **No** to return to the previous screen.

## Appointment

Appointment is the second step, following election, in the process of assigning data owners to resources.

If a goal has an appointment, the goal will not proceed directly to the "Finish" status.

To continue with the appointment process after the election process has completed, perform the following steps:

1. On the File Access Manager websiteNavigate to **Goals**

2. Select a goal, and click **Show Status**.

3. The **Show Status** screen displays.

4. Click **Appointment (In Process)**.

5. A list of final candidates and reviewers displays.

6. Click the Remind icon next to a reviewer's name to send an email reminder to that reviewer.

7. A Question dialog displays, asking whether you want to send the reminder email.

8. Click **Yes** to send the email reminder or **No** to return to the *Show Status* screen.

After the appointment process has finished, the system displays the names of the final candidates and the names of all reviewers, together with information on whether a candidate's reviewer approved or disapproved of that candidate.



## Data Owners Election (Goal Creation)

Data owner election is managed from the Goals process. For a full list of emails sent to data owners and other members of the goals process, see section Message Templates.

## Data Owner Exclusion (Goals Exclusion)

You can block users from being eligible for election as data owners, using the Goals Exclusion setting

In the File Access Manager website navigate to **Settings > Account Exclusions > Goal Exclusions**.

See section Excluding Accounts from File Access Manager Processes.

# Web Localization- Editing Localization Files

The localization files are JSON files, used to set an organization's Website text for each language.

The row of each file contains both a key and a value, with the value containing text in the desired language.

Simply edit the value portion of a localization file to change a word, phrase, or message on the website.

***To edit localization files:***

1. Identify the server on which the File Access Manager website is installed.

2. Open the following localization file folder: C:\inetpub\wwwroot\cdn\i18n

3. The translation files name is according to the language – local code

| | |
|---|---|
| Chinese (Simplified) | zh_CN.json |
| Chinese (Tra-ditional) | zh_TW.json |
| Danish | da_DA.json |
| Dutch | nl_NL.json |
| English | en_US.json |
| French (Canada) | fr_FR.json |
| French (France) | fr_CA.json |
| German | de_DE.json |
| Hebrew | he_IL.json |
| Italian | it_IT.json |
| Japanese | ja_JA.json |
| Portuguese (Brazil) | pt_BR.json |
| Spanish | es_ES.json |
| Swedish | sv_SE.json |

4. Edit the file with Notepad++, Textpad, or any online JSON viewer.

5. Each file row contains a key (the technical name of the word or expression) and a value (the actual text to be displayed on the Website)

6. Edit the text, being careful to change only the value (**<u>not</u>** the key).

7. Save the file.

8. Refresh the Website to view the edited text.

Any changes to the localization files will be overwritten by the next installation of File Access Manager It is recommended to keep a backup of any updated translation file(s), and add in the corrections carefully after installation. In cases of errors in the translation, please notify your representative so we can correct our files as well.