



Integrating SharePoint with File Access Manager

Version: 8.3 Revised: March 30, 2022

This document and the information contained herein is SailPoint Confidential Information

Copyright and Trademark Notices.

Copyright © 2022 SailPoint Technologies, Inc. All Rights Reserved.

All logos, text, content, including underlying HTML code, designs, and graphics used and/or depicted on these written materials or in this Internet website are protected under United States and international copyright and trademark laws and treaties, and may not be used or reproduced without the prior express written permission of SailPoint Technologies, Inc.

“SailPoint,” “SailPoint & Design,” “SailPoint Technologies & Design,” “Identity Cube,” “Identity IQ,” “IdentityAI,” “IdentityNow,” “SailPoint Predictive Identity” and “SecurityIQ” are registered trademarks of SailPoint Technologies, Inc. None of the foregoing marks may be used without the prior express written permission of SailPoint Technologies, Inc. All other trademarks shown herein are owned by the respective companies or persons indicated.

SailPoint Technologies, Inc. makes no warranty of any kind with regard to this manual or the information included therein, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. SailPoint Technologies shall not be liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Patents Notice. <https://www.sailpoint.com/patents>

Restricted Rights Legend. All rights are reserved. No part of this document may be published, distributed, reproduced, publicly displayed, used to create derivative works, or translated to another language, without the prior written consent of SailPoint Technologies. The information contained in this document is subject to change without notice.

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c)(1) and (c)(2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

Regulatory/Export Compliance. The export and re-export of this software is controlled for export purposes by the U.S. Government. By accepting this software and/or documentation, licensee agrees to comply with all U.S. and foreign export laws and regulations as they relate to software and related documentation. Licensee will not export or re-export outside the United States software or documentation, whether directly or indirectly, to any Prohibited Party and will not cause, approve or otherwise intentionally facilitate others in so doing. A Prohibited Party includes: a party in a U.S. embargoed country or country the United States has named as a supporter of international terrorism; a party involved in proliferation; a party identified by the U.S. Government as a Denied Party; a party named on the U.S. Department of Commerce’s Entity List in Supplement No. 4 to 15 C.F.R. § 744; a party prohibited from participation in export or re-export transactions by a U.S. Government General Order; a party listed by the U.S. Government’s Office of Foreign Assets Control as ineligible to participate in transactions subject to U.S. jurisdiction; or any party that licensee knows or has reason to know has violated or plans to violate U.S. or foreign export laws or regulations. Licensee shall ensure that each of its software users complies with U.S. and foreign export laws and regulations as they relate to software and related documentation.

Contents

Contents	iii
Capabilities	5
Supported Versions	5
Connector Overview	6
Activity Monitor Operation Principles	6
Permissions Collector Operation Principle	6
Prerequisites	7
Software Requirements	7
Permissions	7
Configure View Activities Monitoring (Manual Mode Only)	7
Add the “IIS Management Console” Role for Activity Monitoring	9
Communications Requirements	11
SharePoint Installation Flow Overview	12
Collecting Data Stored in an External Application	13
Adding a SharePoint Application	15
Select Wizard Type	15
General Details	15
Connection Details	16
Configuring and Scheduling the Permissions Collection	17
Selecting and Scheduling the Data Classification Settings	23
Data Privacy	24
Configuring Activity Monitoring	24
Configuring Data Enrichment Connectors	25
Enabling Access Fulfillment for an Application	25
Installing Services: Activity Monitor and Collectors	27
Verifying the SharePoint Connector Installation	30
Installed Services	30
Log Files	30

Contents

Monitored Activities 30

Permissions Collection 30

Troubleshooting 31

Collector Installation 31

Crawler Fails With "Unable to Connect to Content Databases" 31

Capabilities

This connector enables you to use File Access Manager to access and analyze data stored in SharePoint and do the following:

- Analyze the structure of your stored data.
- Monitor user activity in the resources.
- Classify the data being stored.
- Verify user permissions on the resources, and compare them against requirements.
- Manage access fulfillment - automated granting and revoking of access - according to rules set in File Access Manager.

See the File Access Manager documentation for a full description.

Supported Versions

- SharePoint Server 2013, 2016, and 2019
- 32-bit and 64-bit

Connector Overview

Activity Monitor Operation Principles

Monitored activities can include activities from all Site Collections, Crawled Site Collections or from selected Site Collections, as described in Chapter [Adding a SharePoint Application](#).

File Access Manager Activity Monitor for SharePoint uses two separate mechanisms to audit user activities.

1. Fetch audits from SharePoint's audit facilities.
2. The SharePoint audit audits all events, except View. Since monitoring View events via the SharePoint audit may result in an extremely heavy load on the SharePoint content database, a different approach is needed. View activities are audited by reading and analyzing the IIS log files on the SharePoint front-end servers. Each Web Application in the farm has its own log file folder and can span across multiple front-end servers. The Activity Monitor can find IIS log file folders automatically or manually.

Automatic Mode

In this mode, the Activity Monitor performs the following discovery sequence:

- Read the list of front-end servers in the farm by using direct access to SharePoint databases.
- Read the Web Applications configured on each Front-end server.
- Configure the Web Application's IIS log fields by using the IIS Remote Management API.
- Locate the Web Applications IIS log file folder in each front-end server and access it through the administrative share remotely to read the IIS log files. Unless the default IIS log folder was changed, the administrative share will be `\\frontend_server\c$`.

Manual Mode

In this mode, each Web Application IIS logging configuration on each SharePoint front-end server must be configured to include specific fields. The IIS log path folders also must be manually configured in the Application Configuration Wizard in the form of a remote UNC share. Use of Manual Mode is **not** recommended since it requires more manual work, which makes it more susceptible to mistakes. **Only use this mode if the user running the Activity Monitor is not to be set as an administrator on all the front-end servers.**

See [Configure View Activities Monitoring \(Manual Mode Only\)](#) and the *IIS Log Configuration* field description in chapter [Adding a SharePoint Application](#) for information on configuring Manual Mode.

Permissions Collector Operation Principle

File Access Manager connects to SharePoint databases directly and analyzes the permissions for local and domain users and groups, including Site Collection administrators and Web Application Policy Rules.

By default, permissions are analyzed to the folder level, but they can also be analyzed on the file level. If permissions are analyzed on the file level, the system will only display uniquely managed files in the Business Resource Tree. Chapter [Adding a SharePoint Application](#) describes how to analyze file level permissions.

Prerequisites

Make sure your system fits the descriptions below before starting the installation.

Software Requirements

File Access Manager requires the latest ASP.NET Core 3.1.x Hosting Bundle. This bundle consists of .NET Runtime and ASP .NET Core Runtime. You can download the latest 3.1.x Hosting Bundle version from [here](#).

Permissions

You will need users with the following permissions to interact with SharePoint:

1. Create a designated domain user in the domain in which SharePoint works (for example, siq_wss).
 - For Access Fulfillment support, assign that user as a “Site Collection Administrator” for all Site Collections, using the Web Application Policy Rule to assign these permissions.
 - If the IIS log file configuration is set to Automatic, the user must be an Administrator on all the front-end servers to access the IIS remote management API and the administrative shares. If the IIS log file configuration is set to Manual, assign the user Read permissions to access all IIS Logs on all front-end servers through the dedicated UNC share. See [Configure View Activities Monitoring \(Manual Mode Only\)](#) for further details.
2. In the installation package you can find the script called **SIQGrantSharePointDBPermissions.sql** under Collectors\scripts. This script can be used to generate a new user login with the required database permissions. To run the script:
 - Open the Collectors\scripts folder in the installation package.
 - Copy the script to one of the SharePoint servers.
 - Follow the instructions at the top and run the script in the SharePoint SQL Server.
3. Verify that the permissions were granted successfully
The script should have the following messages:
 - “Successfully granted permissions to [Configuration DB]”
 - For each content database, a message “Successfully granted permissions to content db [Content DB Name]”
 - “Script execution completed successfully”

Configure View Activities Monitoring (Manual Mode Only)

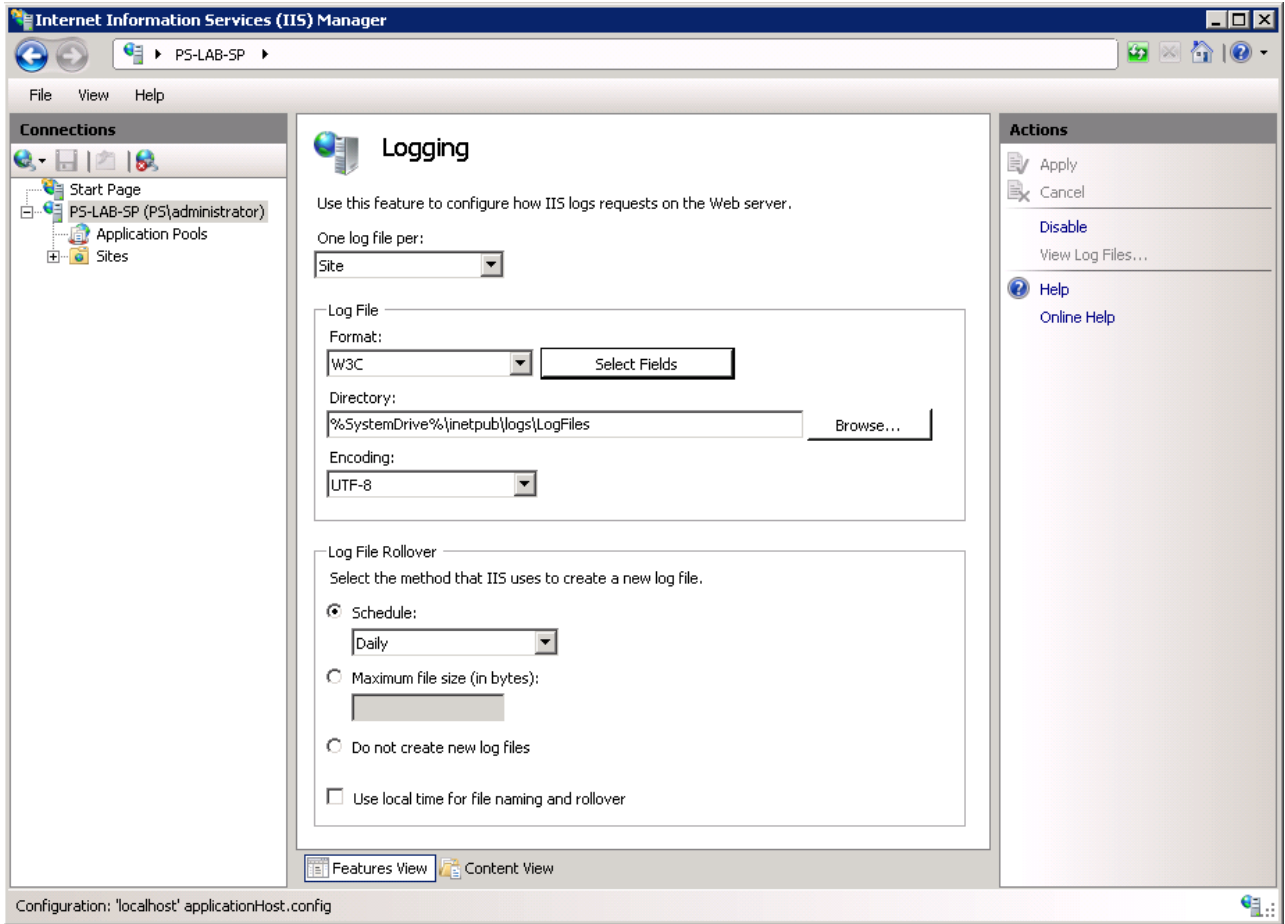
The following step can be skipped when automatic IIS log configuration is enabled in the Add New Application Wizard.

Enable Host field logging on all Front-end IIS servers. For each Web Application in each Front-end server:

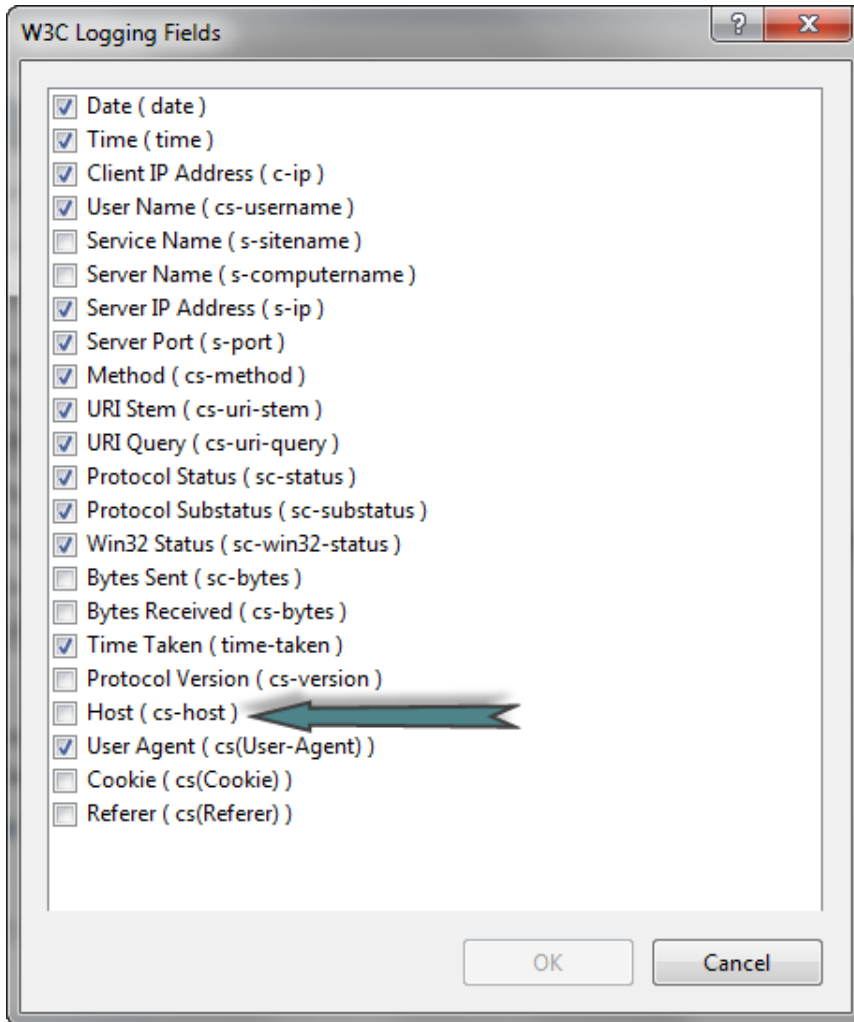
1. Open the IIS management console.
2. Locate the SharePoint Web Application site in the IIS.

Prerequisites

3. Open the "Logging" options on the IIS management console.
4. Click **Select Fields** to open the Logging sub-window



5. Select **cs-host** to select the field.



6. Click **Apply** under **Action** so the changes will take effect.

If the CS-host field was not defined for logging before, View events might take a few hours to start collecting. To make the connector start collecting new view events, stop the IIS, delete the last IIS log file and start the IIS again.

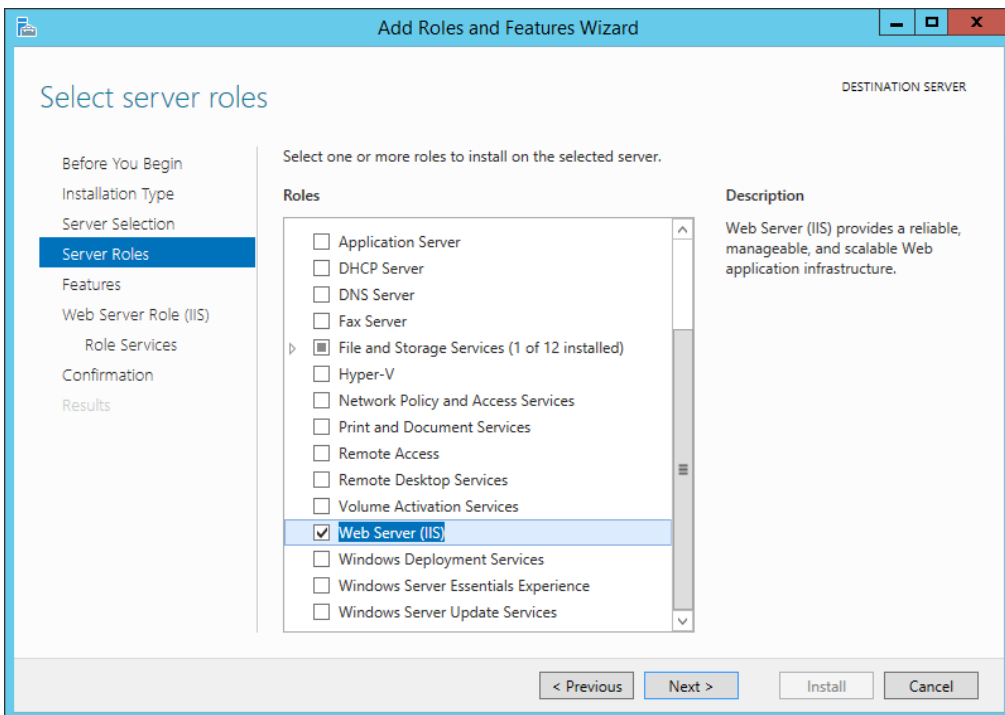
When running in a SharePoint farm with multiple Front-end servers, create a dedicated share on each Front-end for each Web Application IIS log directory, and give Read permissions to the user defined in the Permissions section above to access the share. These shares must be configured manually in the Application Configuration Wizard, as described in chapter [Adding a SharePoint Application](#) .

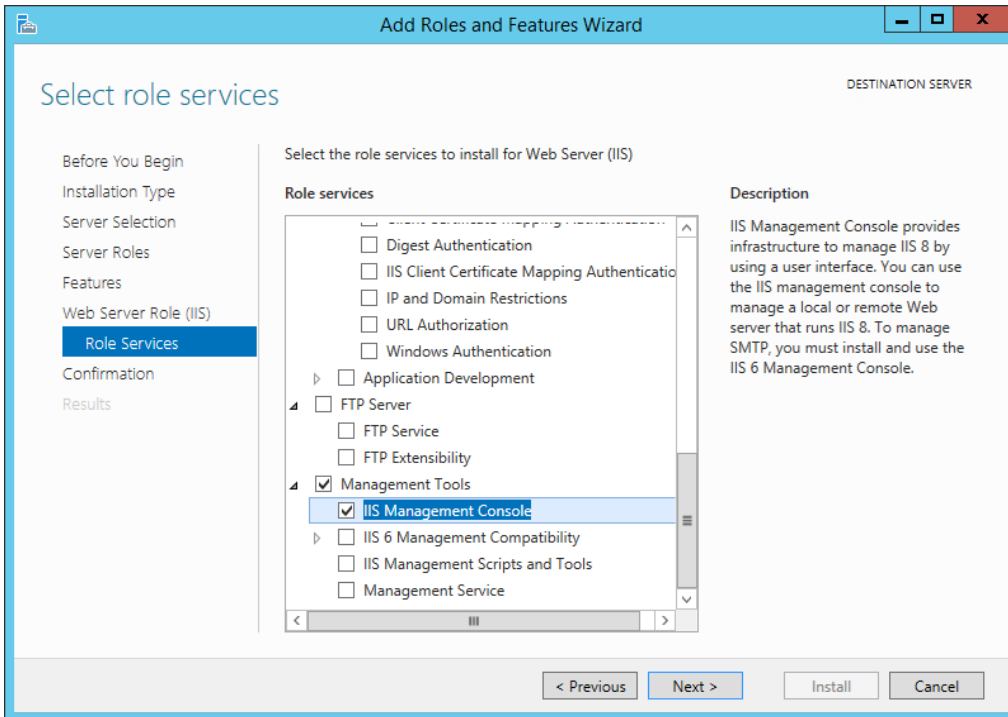
Add the “IIS Management Console” Role for Activity Monitoring

The SharePoint Activity Monitoring agent requires the “**IIS Management Console**” role to gather all view logs paths.

Enable the role on the server where the Activity Monitor service is installed:

1. Open the **Server Manager**.
2. Click **Manage** and then **Add roles and features**.
3. Click **Next** until reaching the **Server Roles** screen.
4. Select **Web Server (IIS)** and then click **Add Features** on the confirmation dialog.
5. Click **Next** until reaching the **Role Services** window of **Web Server Role (IIS)**.
6. Scroll to the bottom and under **Management Tools** make sure the required **IIS Management Console** role is selected.
7. Click **Next** and then click **Install** on the **Confirmation** window.





Communications Requirements

Requirement	Source	Destination	Port
Database Access	Permissions Collector	File Access Manager DB	According to the specific DB definitions
File Access Manager Access	Activity Monitor/Permission Collector server	File Access Manager Servers	8000-8008
SharePoint Database Access	Activity Monitor/Permission Collector service	SharePoint Databases	According to the specific DB definitions
Data Classification	Data Classification Server	SharePoint Farm	http & https as required
Access to IIS Logs	Activity Monitor	All SharePoint Front-end servers	139/445

SharePoint Installation Flow Overview

To install the SharePoint connector:

1. Configure all the prerequisites.
2. Add a new SharePoint application in the Business Website.
3. Install the relevant services:
 - Activity Monitor - This is the activity collection engine, used by all connectors that support activity monitoring.
 - Permissions Collector
 - Data Classification Collector

Installing the permissions collector and data classification services is optional and should only be installed by someone with a full understanding of File Access Manager deployment architecture. The File Access Manager Administrator Guide has additional information on the architecture.

Collecting Data Stored in an External Application

Terminology:

Connector

The collection of features, components and capabilities that comprise File Access Manager support for an endpoint.

Collector

The “Agent” component or service in a Data Classification and or Permission Collection architecture.

Engine

The core service counterpart of this architecture.

Identity Collector

A 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.

The identity collector has no “physical” manifest.

- The actual work is done by the Collector Synchronizer.

The list below describes the high level installation process required to collect and analyze data from an external application. Most of these should already be set up in your File Access Manager installation. See the server Installation guide for further details.

Install a Data Classification central engine

One or more central engines, installed using the server installer

Install a Permission Collection central engine

One or more central engines, installed using the server installer

Create an Application in File Access Manager

From the Business Website. The application is linked to central engines listed above.

Add an Activity Monitor

To collect activities for this application - run the Collector Installation Manager and add an application under Activity Monitoring.

Install Permission Collectors and / or Data Classification Collector (optional)

Optionally, you can install collectors that will run on a separate server and take some of the work from the central PC and DC engines (Where supported). When installing a collector, you attach it to an engine. If no collectors are installed, the central services act as both the engine and the collector.

To install a collector, you must have the **RabbitMQ** service installed for communication between the central engines and the collectors. RabbitMQ is installed

For further details, see section **Application > Central Service > Collector Relations** in the File Access Manager Administrator Guide

Adding a SharePoint Application

In order to integrate with SharePoint, we must first create an application entry in File Access Manager. This entry includes the identification, connection details, and other parameters necessary to create the link.

To add an application, use the **New Application Wizard**.

1. Navigate to *Admin > Applications*
2. Click **Add New** to open the wizard.

Select Wizard Type

1. Click **Standard Application**
2. Click **Next** to open the **General Details** page.

General Details

Application Type

SharePoint

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 Manager File Access Manager Administrator Guide for further details.

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

Click **Next**. to open the Connection Details page.

Connection Details

Database Server

The address of the SharePoint server containing the configuration database

- If you're using a non-default port number, add it, separated by a comma - *[Server Name],[Port]*

The default port number is 1433

- If the database has an instance name the address should be in a format of “[Server Name]\[Instance Name]”
- To enter a database with an instance name on a server with a non-default port number, use the format “[Server Name]\[Instance Name],[port]”

There are cases in which you will have configure an alias for Windows to support this non-default database name format. See the Troubleshooting section below

Domain Name / Username

The user defined in the prerequisites. This field is used by the Data Classification service. The Permissions Collector and Activity Monitor services will use it for impersonation to allow a connection via windows authentication to the SharePoint database

Password

The user defined in the prerequisites

Leave Audit On

Whether to leave the SharePoint audit on when the service is off

Analyze permissions on files

Check this box to display files that break permissions inheritance. Analyze the permissions of those files.

Purge Old Audit Events / Days to Keep Events

Deletes audits older than a given number of days from the SharePoint Content database, using the SharePoint API

IIS Log Configuration

Determines whether to specify IIS log folders manually or automatically, as explained in [Connector Overview](#) and [Add the “IIS Management Console” Role for Activity Monitoring](#).

- **Manual:** Configure access to the IIS log folders manually through UNC shares. This is defined in [Add the “IIS Management Console” Role for Activity Monitoring](#).

Fill in the IIS Log Folder Paths list with the UNC path for each Web Application on each Front-end server.

- **Automatic:** Let the monitor identify all front-end servers, web applications, and IIS log folder locations. (This is the default setting).

This mode also sets the IIS Host field logging for each Web application in each front-end server if it was not previously set.

Servers to Exclude: *If there are front-end servers that do not require monitoring, fill in this list.*

Each entry may be a server name or address.

Type in a server name to exclude, and click **+** to add it to the list.

To remove an item from the list, click the **x** icon on the item row.

Specify configuration database name?

Determines whether to specify a name for the configuration database in case it differs from the default "SharePoint_Config" name.

Click **Next**.

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 "IdentityIQ FAM 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.

Skip Identities Sync during Permission Collection

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

This option is checked by 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**.

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.

Calculate Resource Size

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)

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  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 Example

The following are examples of crawler Regex exclusions:

Exclude all resources which start with one or more resource names:

Example: Starting with `https://www.mysharepoint.com/resourceName`

Regex: `https:\\www.mysharepoint.com\\resourceName$`

Example: Starting with `https://www.mysharepoint.com\\resourceName` or `//www.my-`

sharepoint.com/OtherResourceName

Regex: `https:\\\\www.mysharepoint.com\\(resourceName|OtherResourceName)$`

Example: SharePoint resources starting with `https://www.mysharepoint.com/sites/mySiteCollection`

Regex: `https:\\\\www.mysharepoint.com\\sites\\mySiteCollection$`

Example: SharePoint resources starting with

`http://www.mysharepoint.com/sites/mySiteCollection` or
`http://www.mysharepoint.com/other site/Different Site`

Regex: `https:\\\\www.mysharepoint.com\\(sites\\mySiteCollection|other_site\\Different_Site)$`

Include ONLY resources which start with one or more resources names:

Example: Starting with `https://www.mysharepoint.com/resourceName`

Regex: `^(?!https:\\\\www.mysharepoint.com\\resourceName($|\\.*)).*`

Example: Starting with `https://www.mysharepoint.com/resourceName` or `https://www.mysharepoint.com/OtherResourceName`

Regex: `^(?!https:\\\\www.mysharepoint.com\\(resourceName|OtherResourceName)($|\\.*)).*`

Example: SharePoint resources starting with `https://www.mysharepoint.com/sites/mySiteCollection`

Regex: `^(?!https:\\\\www.mysharepoint.com\\sites\\mySiteCollection($|\\.*)).*`

Example: SharePoint resources starting with

`https://www.mysharepoint.com/sites/mySiteCollection` or
`https://www.mysharepoint.com/other site/Different_Site`

Regex: `^(?!https:\\\\www.mysharepoint.com\\(sites\\mySiteCollection|other_site\\Different_Site)($|\\.*)).*`

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 you 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.

Top Level Resources Exclusion

WFS-DC testing

Last Successful Run 06-22-2021 4:57:27 PM

[Run Task](#) [View Task Status](#)

Note: Refresh the list to view recently discovered resources [Refresh](#)

Top Level Resources Exclusion List 0 Selected | Clear Selection

Top Level Resources Exclusion List

- \\si-...-5\C\$
- \\si-...-5\MSSQLSERVER
- \\si-...-5\print\$

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 earlier

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.

Selecting and Scheduling the Data Classification Settings

To associate an application with a data classification service, and set the schedule

- 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 **Data Classification** settings page.

The actual entry fields vary according to the application type

Central Data Classification Service

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

If the “Central Data Classification” wasn’t installed during the installation of the server, this field is disabled.

Disabling Data Classification

To disable data classification, delete the entry from the central data classification field.

Disabling data classification can also be achieved by setting the scheduler to be inactive (which is the default setting for data classification).

Create a Schedule

This option is enabled only if a central data classification service is selected.

See [Scheduling a Task](#)

See the chapter “Data Classification” in the File Access Manager Administrator Guide for more information

Click **Next** or **Finish**.

Data Privacy

A user can associate the application with a Central Data Classification Engine Service. This engine will be responsible for executed Data Privacy tasks.

Though using different processes for each, the Data Classification engine service is in charge for both Data Privacy and Data Classification discovery tasks.

You may choose the same service for both, or use a different one for each, to run them in parallel.

The fields on the Data Privacy step are the same as the Data Classification step.

Configuring Activity Monitoring

Configure the activity monitoring processes frequency.

Polling Interval (sec)

Activity fetching interval [in seconds]. Default is set to 60 seconds,

Report Interval (sec)

Activity Monitor Health reporting interval [in seconds]. Default is set to 60 seconds.

Local Buffer Size (MB)

Local buffer size for activities [in MB]). Default is set to 200MB.

This cyclic buffer is used to store activities on the Application Monitor's machine in case of network errors that prevent the activities from being sent.

Configuring Data Enrichment Connectors

The Data Enrichment Connectors (DEC) configuration enables us to select data enrichment sources. These can be used to add information from other sources about identities.

An enrichment source could be a local HR database that is used to combine users' job descriptions or departments to the information stored in the identity store.

Select the data enrichment connectors to enrich monitored activities from the Available DEC's text box.

Use the > or >> arrows to move the selected DEC's to the Current DEC's text box.

The user can select multiple DEC's. Simply select each desired DEC.

You can create a new DEC in the Administrative Client (Applications>Configuration>ActivityMonitoring>DataEnrichmentConnectors).


After creating a new DEC, click **Refresh** to refresh the dropdown list.

The chapter Connectors of the File Access Manager Administrator Guide provides more information on Data Enrichment Connectors, including what they are, how to configure them, and how they fit in the Activity Flow.

Enabling Access Fulfillment for an Application

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 [Create/Edit 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 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:

- 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.

Installing Services: Activity Monitor and Collectors

The Collector Installation Manager is part of the File Access Manager installation package. This tool is used to install the activity monitor, permission collector, and data classification collector.

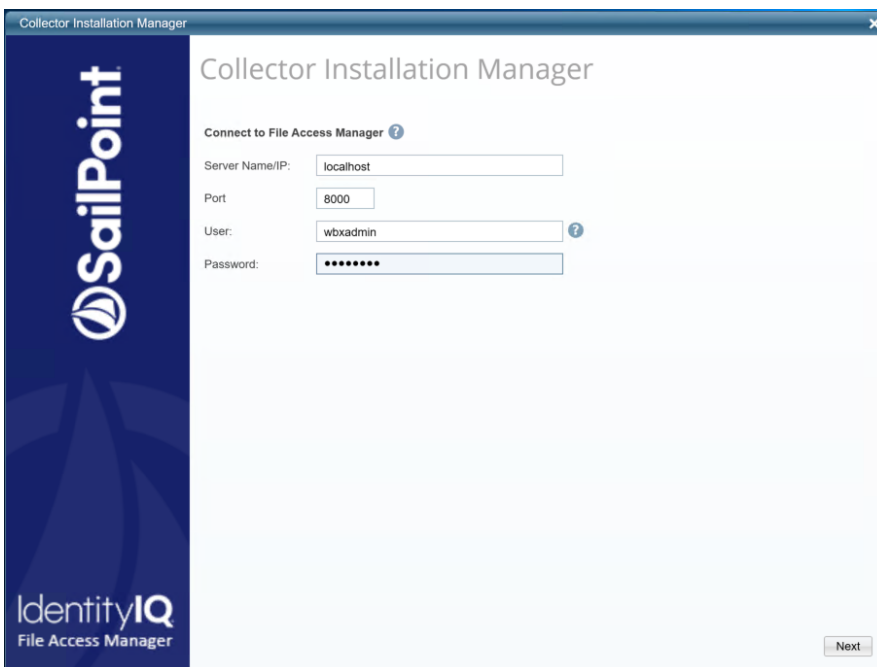
Activity Monitor

The activity monitor is installed per application, and collects SharePoint Audit entries and IIS activity logs.

When asked for user credentials for the activity monitor, select a user with permission to access these activity logs, who has local administrator privileges on the server hosting the File Access Manager activity monitor.

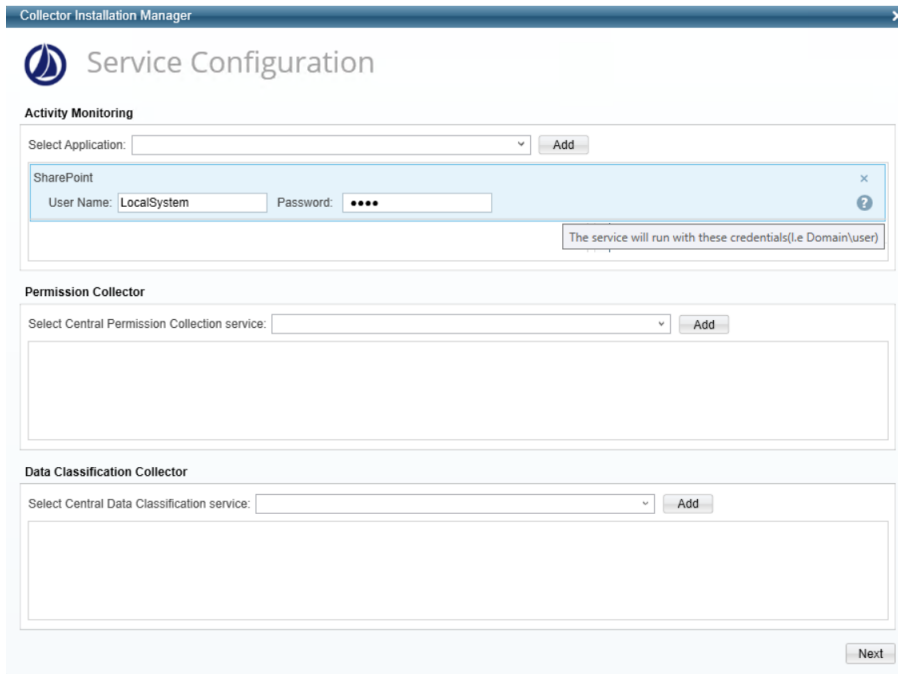
1. Run the **Collector Installation Manager** as an Administrator.
The installation files are in the installation package under the folder **Collectors**.

The Collector Installation Manager window displays.



2. Enter the credentials to connect to File Access Manager.
 - a. ServerName/IP should be pointed to the Agent Configuration Manager service server.
 - b. An File Access Manager user with Collector Manager permission (permission to install collectors). For Active Directory authentication, use the format domain\username.
3. Click **Next**.

The Service Configuration window displays.



4. If you are installing the Activity Monitor, select the application, and click **Add**.
5. When installing a SharePoint Activity Monitor, you will be prompted for service account credentials. This service account will be used by the Activity Monitor service to run the service and authenticate against the SharePoint IIS servers to fetch the logs (“Log on as”). Make sure the service account provided has local administrator privileges on the local server (hosting the Activity Monitor service) and can access the activity logs on the IIS servers.
6. If you are installing the Permission Collector, select the Central Permission Collector to which to connect this service, and click **Add**
7. If you are installing the Data Classification, select the Central Classification Collector to which to connect this service, and click **Add**
8. Click **Next**.

The Installation Folder window displays.

If this is the first time you are installing collectors on this machine, you will be prompted to select an installation folder, in which all future collectors will also be installed.

9. Browse and select the location of the target folder for installation.
10. Browse and select the location of the folder for system logs.
11. Click **Next**.
12. The system begins installing the selected components.
13. Click **Finish**

The Finish button is displayed after all the selected components have been installed.

The *File Access Manager Administrator Guide* provides more information on the collector services.

Verifying the SharePoint Connector Installation

Installed Services

Verify that the services installed for the connector are available and active. Using windows Service manager, or other tool, look for the File Access Manager services, and see that they are running.

for example:

- File Access Manager Central Activity Monitor - <Service Name>
- File Access Manager Central Permissions Collection - <Service Name>
- File Access Manager Central Data Classification - <Service Name>

Log Files

Check the log files listed below for errors

- "%SAILPOINT_HOME_LOGS%\PermissionCollection_<Service_Name>.log"
- "%SAILPOINT_HOME_LOGS%\DataClassification_<Service_Name>.log"
- "%SAILPOINT_HOME_LOGS%\WSSBAM-<Application_Name>.log"

Monitored Activities

1. Simulate activities on SharePoint.
2. Wait a minute (approximately).
3. Verify that the activities display in the File Access Manager website under

Forensics > Activities

Permissions Collection

1. Run the Crawler and Permissions Collector tasks (*Settings > Task Management > Scheduled Tasks*)
2. Verify that:
 - The tasks completed successfully
 - Business resources were created in the resource explorer (*Admin > Applications > [application column] > Manage Resources*)
 - Permissions display in the Permission Forensics page (*Forensics > Permissions*)

Troubleshooting

Check the issues below for common problems and suggested ways of handling them.

Collector Installation

File Access Manager does not verify the credentials provided in the collector installation stage. If incorrect credentials are provided, the permission collector installation will fail, and an error message displays in the [Application_Name].RA.install file under the **log** directory:

Error 1920. "Service SecurityIQ Permissions Collection – SharePoint" (SIQSPRA_SharePoint) failed to start. Verify that you have sufficient privileges to start system services.

Crawler Fails With "Unable to Connect to Content Databases

When using a non-default port, there are cases in which File Access Manager fails to connect to the SharePoint databases using the existing configuration.

In the log file, you can see that the Crawler connected to the SharePoint_config DB using the server,port address:

```
DEBUG, WBX.Com-
mon.SharepointDataAccess.DataAccessCore, executeStoredProcedure, connectionString =
Data Source=[Server Name]\[Instance Name],3123;Initial Catalog=PR_SharePoint_Con-
fig;Integrated Security=True
```

, but fails to connect to the SharePoint content DB, and the log shows that the connection is attempted without using the port

```
DEBUG, WBX.Com-
mon.SharepointDataAccess.DataAccessCore, executeStoredProcedure, connectionString =
Data Source=[Server Name];Initial Catalog=WSS_Content[_DBNAME];Integrated Secur-
ity=True
```

Error message:

```
2019-08-01 09:17:15, 851, 18, ERROR, WBX.Com-
mon.SharepointDataAccess.DataAccessCore, executeStoredProcedure, Execution of
'proc_GetTpWebMetaDataAndListMetaData' failed
```

```
System.Data.SqlClient.SqlException (0x80131904): A network-related or instance-spe-
cific error occurred while establishing a connection to SQL Server. The server was
not found or was not accessible. Verify that the instance name is correct and that
SQL Server is configured to allow remote connections. (provider: Named Pipes Pro-
vider, error: 40 - Could not open a connection to SQL Server) ---> Sys-
tem.ComponentModel.Win32Exception (0x80004005): The system cannot find the file
specified
```

Suggestion:

Using the Windows SQL Server Client Network Utility, create aliases for each SharePoint database server, to point to the server address including the port, in the format

```
[Server name], [port]
```

To set the aliases:

1. Open the Windows CMD as administrator
2. Cliconfg.exe
3. Click the *Alias* tab
4. Click **Add** to create a new alias
5. Select TCP/IP

Set the parameters:

Server Alias

The SharePoint database sever name

Server Name

If the database has an instance name, the address should be in the format “[Server Name]\[Instance Name]”

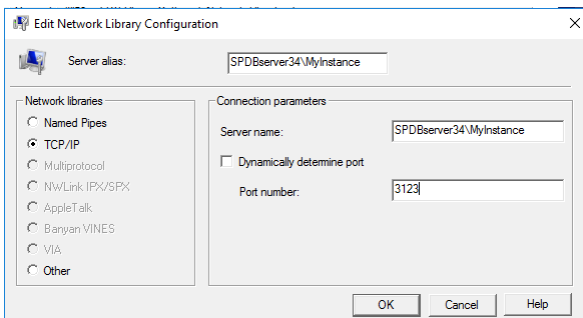
Dynamically Determine Port

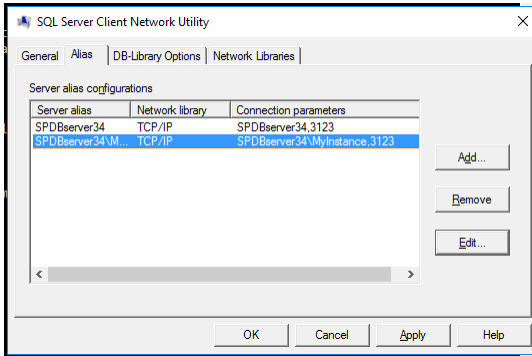
If not using the default port, unselect this option, and enter the port number.

If the port is non-default, and this isn't the default instance of the database, then you should create two aliases:

Server/Instance, port

Server,port





- Restart the server, and retry the Crawl.