File Access Manager Installation Guide

Version: 8.3 SP5

Revised: June 30th, 2023

This document and the information contained herein is SailPoint Confidential Information

Copyright and Trademark Notices

Copyright © 2023 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

File Access Manager General Information

When installing File Access Manager, the following is some information that could help in understanding the product and the process of installing.

File Access Manager Architecture

File Access Manager architecture usually requires a central installation with some remote gateways. Most File Access Manager connectors do not require any footprint on the monitored/analyzed system and therefore are installed on File Access Manager servers.

In some cases, due to 3rd party vendors (mostly NAS vendors), it is imperative to have a local server at the same physical site where the monitored system is located.

For more information on File Access Manager architecture see “Capabilities and Architecture” in the *File Access Manager Administrator Guide*.

File Access Manager Connector Services

Each type of connector has its own prerequisites and its own configuration. See the relevant Connector Installation guide for more information about the connector.

Sizing Considerations

File Access Manager is a scalable solution that enables the distribution of its services and also works in an all-in-one mode. The *Administrator Guide* has a complete description of the File Access Manager architecture configuration.

One of the critical sizing considerations is the amount of disk space required to store activities over time. The table below describes the guidelines.

> Note: For more details on sizing, refer to the *File Access Manager Hardware Sizing Guide* article on Compass.

Service	CPU	Memory	Disk
Elasticsearch	Minimum of 4 cores, Recommended 8	Minimum of 8Gb, Recommended 16Gb	0.5kb per event

Additional factors that affect the required hardware are:

- Disaster recovery environment
- High Availability solution

It is highly recommended to consult with your SailPoint File Access Manager representative to obtain the correct configuration to support your requirements.

Installation Prerequisites

File Access Manager Server Support Information

System	Supported Versions
File Access Manager Servers	Windows 2016 / 2019 / 2022
Workstation	Windows 7 and above
Browser	Edge, Safari, Chrome, Firefox
Database	MS SQL Server 2014 / 2016 / 2017 / 2019 / 2022

Database Configuration

Dedicated Instance

We recommend installing File Access Manager on a dedicated instance. This configuration enables independence of configuration and assures resource allocation for the instance.

We realize, however, that a dedicated instance is a costly solution and therefore might be chosen at a later stage.

Some of the File Access Manager requirements can be defined at the instance level and can work in such a way that avoids the definition of specific requirements for shared databases.

> Note: This decision should be part of the sizing process led by your SailPoint File Access Manager representative.

Required Features

File Access Manager uses MS SQL Standard Edition that utilizes the database engine only. No other feature is required. File Access Manager thus enables the use of MS SQL native features for high availability and encryption without any interruption.

Required Settings

The following settings must be chosen for the installation instance.

- FILESTREAM using "Full Access Enabled"
    a. Find the SQL Server Configuration Manager. Navigate to the properties of the service and select FileStream. Check all three boxes.
- CLR enabled (Running .NET code in the database in Safe mode)
- SQL Mixed Authentication

Hyper-Threading

It is recommended that hyper-threading on physical servers be disabled.

Storage

For a database server running as a virtual machine (of any kind), verify that the drives connected for the database storage are physical disks (dedicated for the virtual machine).

- The drives must be separated for Data and Logs.
- Format the drives with a 64K allocation unit.

Backup & Recovery

It is recommended that you use a Simple database recovery plan.
Choosing any other recovery plan requires scheduled log backups to prevent the log file from overflowing. Data performance may be affected during log backups since File Access Manager is very write I/O intensive.

Temp Database

> Note: Depending on your database configuration, you might require additional storage allocated for a temp database. Please discuss this with your DBA.

Ensure that the database is:

- Defined on a separate drive
- Physical and formatted to a 64K allocation unit
- Allocated a temp database file for each core on the system
- One that limits the temp database files and logs so they do not overgrow the size of the disk

Recommended Performance

Metric	Requirement
Disk I/O Throughput (IOPS)	12K IOPS
Disk I/O Throughput Rate	10500 Mb/s
Throughput in Transactions/sec	6000 TPS
Disk I/O latencies for Read	< 8 ms
Disk I/O latencies for Write	< 1 ms

Preparing for Installation

Before starting the installation, gather the required data, open the required ports, and set up the servers, as described.

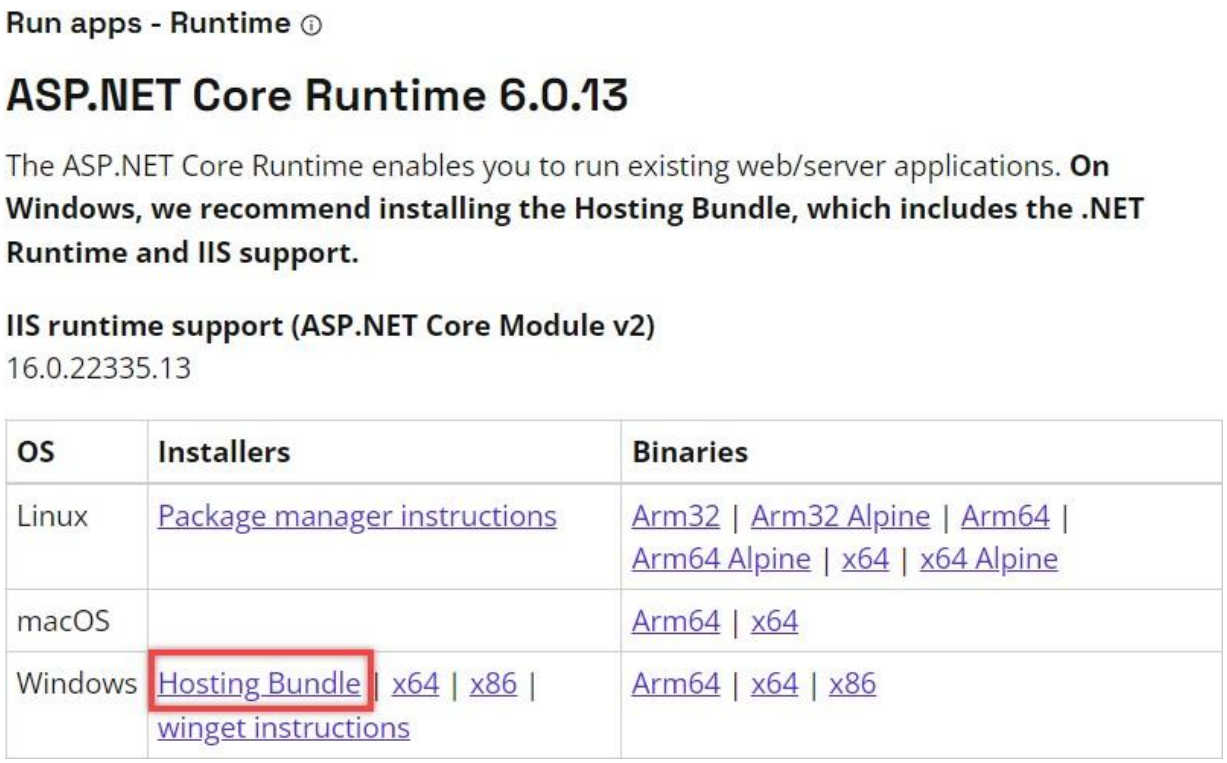
Communication Requirements

File Access Manager is a service-oriented solution, and as such, enables the distribution of its services on multiple servers. The model is flexible, and services can be shifted between servers to boost performance.

.NET

File Access Manager requires the latest ASP.NET Core 6.0.x Hosting Bundle. This bundle consists of .NET Runtime and ASP .NET Core Runtime.

You can download the latest 6.0.x Hosting Bundle version from here.



Run apps - Runtime

ASP.NET Core Runtime 6.0.13

The ASP.NET Core Runtime enables you to run existing web/server applications. **On Windows, we recommend installing the Hosting Bundle, which includes the .NET Runtime and IIS support.**

IIS runtime support (ASP.NET Core Module v2)
16.0.22335.13

OS	Installers	Binaries
Linux	Package manager instructions	Arm32 | Arm32 Alpine | Arm64 | Arm64 Alpine | x64 | x64 Alpine
macOS		Arm64 | x64
Windows	Hosting Bundle | x64 | x86 | winget instructions	Arm64 | x64 | x86

Caution: Without completing this step, the installation will fail.

a. All servers hosting File Access Manager services, including all Activity Monitors must, have .NET Core 6.0.x installed as a prerequisite for the installation.

b. The administrative client computer and Business Website service server must contain .NET Framework 4.7.2

> Note: .NET Core and .NET Framework 4.7.2 can be installed on the same server.

Verifying .NET Core Settings

Complete the following steps to verify the version of .NET Core:

1. Open a CMD window.
2. Execute the following command:
    a. dotnet --list-runtimes

The output should consist of at least these two:

- Microsoft.AspNetCore.App 6.0.x
- Microsoft.NETCore.App 6.0.x

If the command did not execute or the two runtimes mentioned above are not in the output list, reinstall or repair the hosting bundle.

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 Event Manager Central Data Classification Central Permissions Collector Data Classification Collector	8000

Service	Clients	Default Port
	Permissions Collector Collector Installation Manager	
Event Manager	User Interface Central Data Classification Scheduled Task Handler Central Permissions Collection Web Server	8001
Reporting Service	User Interface	8006
User Interface	File Access Manager Administrative Client	8005
Workflow	User Interface	8008
Elasticsearch	Event Manager Reporting Service Scheduled Task Handler User Interface Web Server Activity Analytics	9200
Elasticsearch	Elasticsearch	9300
RabbitMQ	Central Permissions Collector Central Data Classification Permissions Collector Data Classification Collector Activity Monitor Event Manager	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.

Ensuring HTTP/2 Support

Services will only accept http/2 connections (version 8.3 uses gRPC as the communication protocol, the requires http2).

Once fully installed, 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 installation to halt. As a pre-installation step, ensure all servers and communication middleware components are configured to support http/2.

File Access Manager Installation

The File Access Manager installation consists of the following phases:

1. File Access Manager Server Installer installation
2. Database creation
3. Configuration creation
4. Service installation on each File Access Manager Server

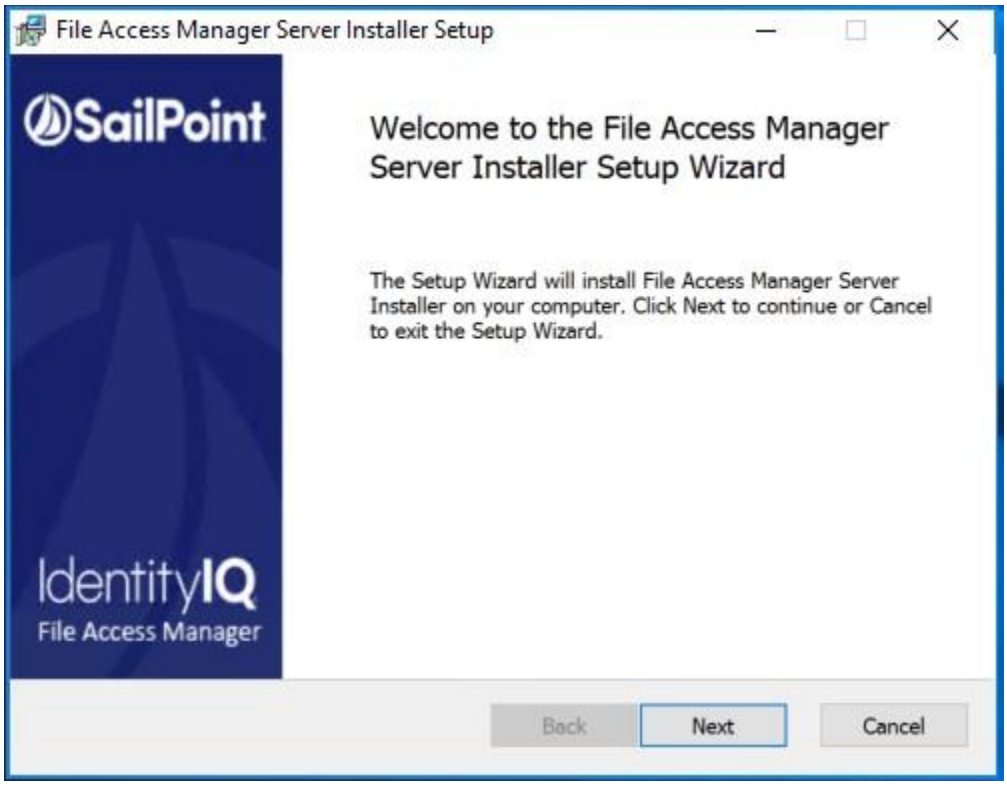
> Note: The installation process is logged to the installation logs. Any errors in the installation process or for any references to the logs in error messages, refer to the logs in this folder (according to the installation directory):
> C:\Program Files\SailPoint\FileAccessManager\Server Installer\Server\Logs

Server Installer

The Server Installer manages the configuration of the File Access Manager central servers and the installation process.

> Note: After the configuration, the installation process will need to be run for every server.

1. After downloading the appropriate version of File Access Manager from Compass, navigate to your downloads folder within File Explorer to locate the Server Installer.
2. Run the ServerInstaller.msi file.
   The "Welcome to File Access Manager Server Installer Setup Wizard" window displays.



3. Click **Next.**
4. Select the destination folder and click **Next**.
5. Click **Install** to start the installation, or **Back** to change the installation folder.
6. After the installation processes are complete, the “Completed the File Access Manager Server Installer Setup Wizard” window displays.
7. Verify the **Launch the File Access Manager server installer** check box is selected. This launches the Install Wizard of the Server Services.

   Note: If the Server Installer does not automatically launch, this is due to UAC. Please navigate to the directory you installed to, usually "Program_Files\SailPoint\FileAccessManager. Click **OK** on the UAC prompt and now the shortcuts and auto launch will work.

8. Click **Finish**.
   The File Access Manager Installation window displays.
9. Click **Next.**

Creating a Database Using the Installer

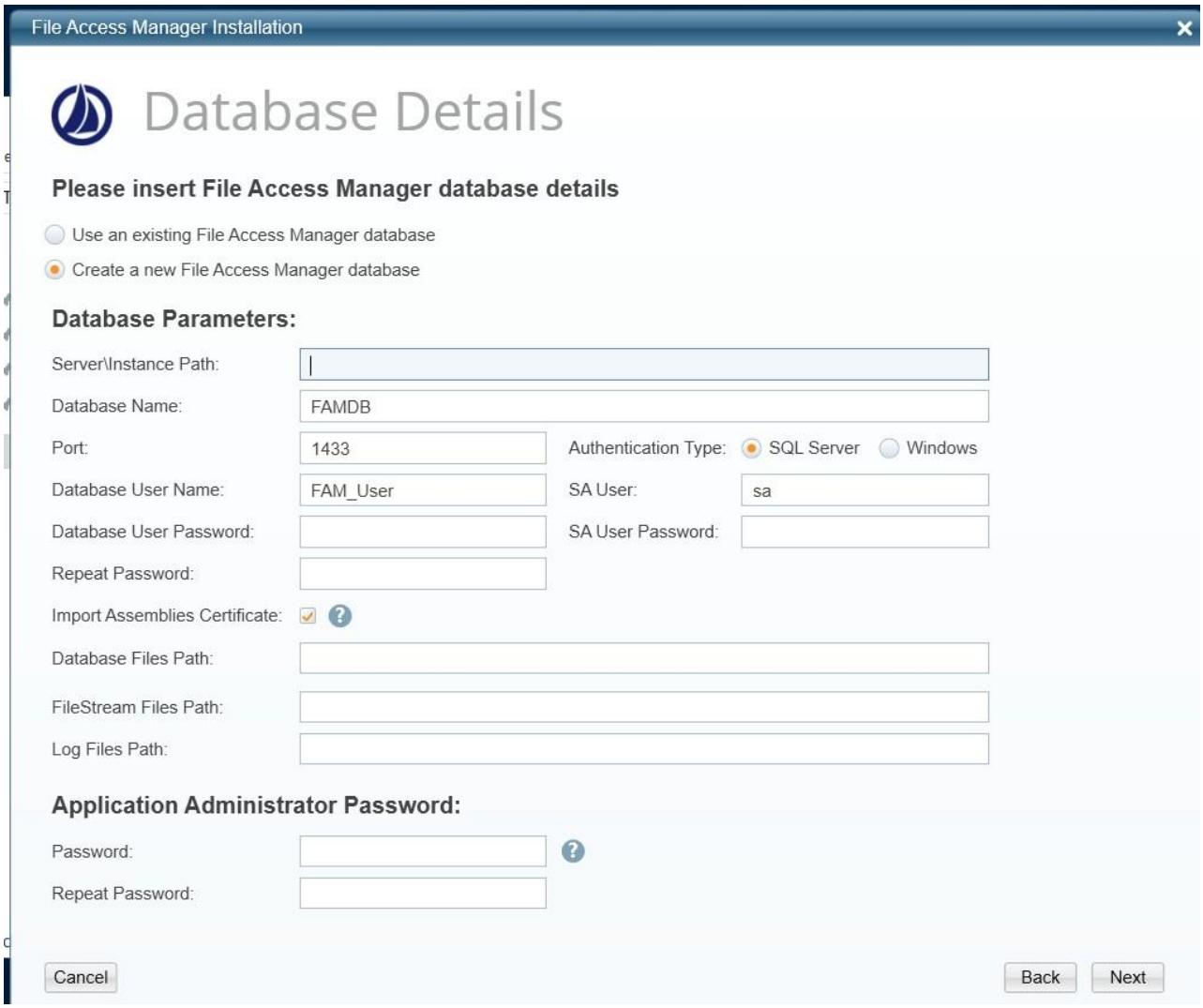
To create the database, perform the following steps:

1. Start the installer by opening the `SailPoint\Server Installer` shortcut.

   > Note: Run in Administrator mode.

2. Click **Next**.
   The End User License Agreement (EULA) window displays.

3. When you have read and accepted the End User License Agreement, select the **I have read and accepted the agreement** option and click **Next**.
   The Database Details window displays.



4. If you are installing File Access Manager for the first time:
    a. Select **Create a New File Access Manager Database**.
    b. Enter the following information:
        - Server\Instance Path – typically a server
        - Database Name – default is FAMBD
        - Port Number – default is 1433. When using a dynamic port, input 0
        - Database User Name – default is FAM_User
    c. Enter the Database User Password twice in the appropriate fields.
    d. Import Assemblies Certificate checkbox: Check this option if the CLR Strict Security Mode is enabled in the database. Using this option will import a certificate into the Master database. This option is relevant only for SQL Server 2017 and above.
    e. Enter the database files path. This folder must exist on the database server.
    f. Enter the file stream files path.
    g. Enter the log files path. This folder must already exist on the database server.
    h. Select the **Authentication Type** from the SQL Server or Windows options. This is the authentication used to log in to the database for the creation of the File Access Manager database.
        - For **SQL**, type in the SA User Field and password for the system administrator.
        - For **Windows**, the Server Installer will use the logged-in user to connect to the database.
    i. Enter a password (only for the WBXadmin user) for the administrative client user and repeat the password. The password needs to meet the following parameters:

- Minimum Length: 12 characters
- At least one uppercase and lowercase letter
- At least 1 special character

5. If you are installing additional services to an existing File Access Manager installation, select **Use an existing File Access Manager Database**.
    a. Enter the Server\Instance Path.
    b. The Database Name, Port, and Database User Name fields are automatically populated.
    c. Enter the Database User Password.
6. Click **Next**.
   The Action Select window displays.
7. Select **Create / Edit Installation Configuration** and click **Next.**

Creating the Configuration

The create / edit installation configuration will be the only option available if this is the first time running the Server Installer. After the first configuration is set, the rest of the options will be available for editing the configuration or uninstalling services.

The configuration steps are:

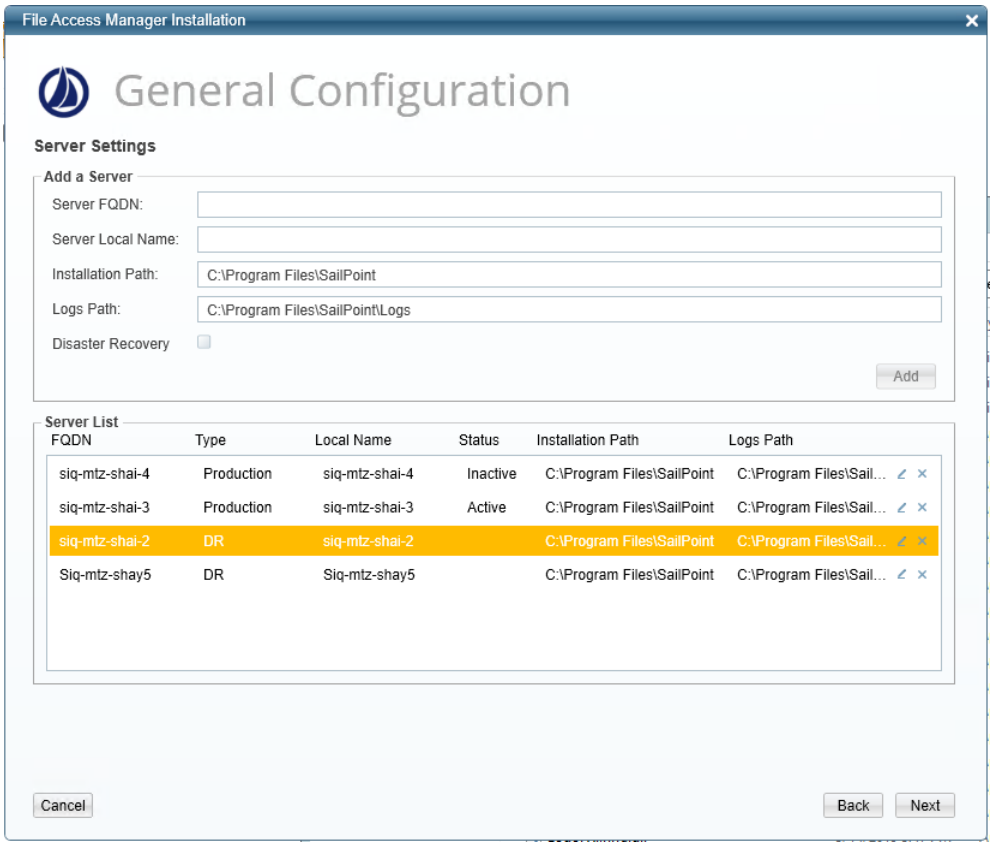
1. Adding and defining the servers as Production (default) or Disaster Recovery
2. Assigning File Access Manager services to Production and Disaster Recovery servers
3. Storing the installation configuration and installation commands file
4. Installing in one of two methods:
    a. On the current server using the installation GUI
    b. Using the preconfigured command file

Adding a Server

To create the configuration for a new server:

1. In the General Configuration window, define all the servers which the File Access Manager services will be installed on and whether the installed server is a production server (Prod) or a disaster recovery server (DR).

These servers should include DR servers and High Availability duplicate servers, if required. This does not include the Windows file server activity monitors; they are added automatically in the installation process and are not displayed.



2. For each server:

    a. In the **Server FQDN** field, enter the server's Fully Qualified Domain Name (FQDN).

    b. In the **Server Local Name** field, enter the server's short name (NetBIOS host name).

    c. In the **Installation Path** field, enter the installation path. This becomes the SAILPOINT_HOME environment variable on the installation server. This is the path in which the **File Access Manager** services will be installed.

    d. In the **Logs Path** field, enter the logs path. This becomes the SAILPOINT_HOME_LOGS environment variable on the installation server. This is the central folder, in which all **File Access Manager** logs will be written.

e. If this server is designated as a disaster recovery server, select the **Disaster Recovery** check box. For more information about Disaster Recovery servers, read the File Access Manager Disaster Recovery guide.

3. Click **Add**. The server configuration that you specified copies to the Server List.

> Note: File Access Manager services use SSL communication.

4. Within the Server List, a user can edit an existing server. Only the Sever FQDN and the Server Local Name are editable.

5. Click **Next**.

Service Configuration

There are two Service Configuration screens: one for the production environment and one for the disaster recovery environment.

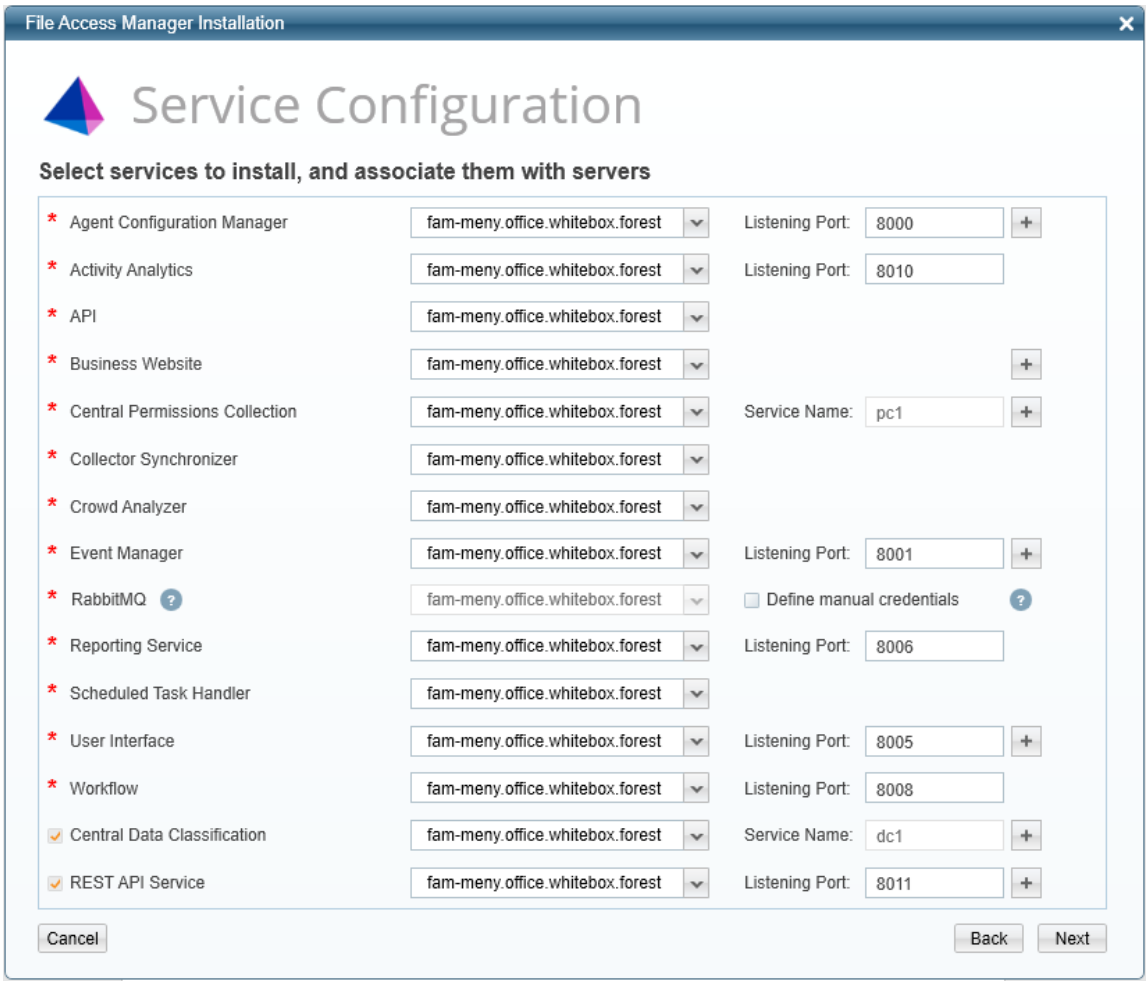
> Important: The services distribution should be planned before installation. SailPoint installation experts are available to discuss these options with you.

For each environment, this screen is used for associating services with the relevant servers defined in the Services Configuration window.

To configure services, perform the following steps:

1. In the **Action Select** window, select the **Create / Edit** configuration installation option.

2. Click **Next** to display the Service Configuration window.
Use the scroll bar to see all the configuration input fields.



3. Select the server to use in the production environment for each service. The dropdown list of available servers only includes production servers.

> Note: When allocating services to servers, make sure any servers dedicated to high availability are not used for the first instance of any services.

Service Ports

Enter the relevant port information. Make sure to adjust firewall rules, if required.

When installing High Availability, adjust the service port number to the port number of the load balancer.

Agent Configuration Manager

The Agent Configuration Manager service is a prerequisite for installing all other services, therefore the server configured for the Agent Configuration Manager must be installed first.

RabbitMQ

File Access Manager uses an open source message broker, RabbitMQ, to distribute operations across multiple services. The *File Access Manager Administrator Guide* has more information on horizontal scaling in this service.

The connection between the message broker and File Access Manager services is secured with SSL.

An account is required to handle internal processes between the message broker and File Access Manager server. Credentials can be created automatically or inserted manually.

> Important: When installed in a High-availability 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.

> Note: When installing RabbitMQ, the user completing the installation must have a valid %homepath% variable. During the installation the erlang.cookie will be copied over using this variable, which will cause the failure of the installation if not set.

Event Manager

The Event Manager Service can be duplicated and installed on multiple servers.

Click the **+** next to the port and select the correct destination server for the newly created service.

Central Data Classification

File Access Manager allows multiple instances of installed Central Data Classification services. The Architecture section of the *File Access Manager Administrator Guide* has additional information on installation planning.

- Click the **+** next to the port to add instances.
- Click the **x** to remove instances.

Central Permissions Collection

File Access Manager allows multiple instances of installed Central Permissions Collection services. The Architecture section of the *File Access Manager Administrator Guide* has additional information on installation planning.

- Provide a unique name for each service. This name will be displayed during the application configuration wizard when defining a new application in the File Access Manager Administrative Client.

File Access Manager supports installing a non-dedicated Permissions Collector service to handle multiple applications on the same service. You can also install a dedicated Permissions Collector service for an application. The *Collector Installation Guide* has additional information.

> Note: Requires a distinguished name.

> Caution: Removing a Central Permission Collector may orphan associated collectors. Any orphaned collectors should be uninstalled through the Collector Installation Manager.

Business Website

The Business Website installs IIS if it is not yet installed.

Configuring High Availability Services

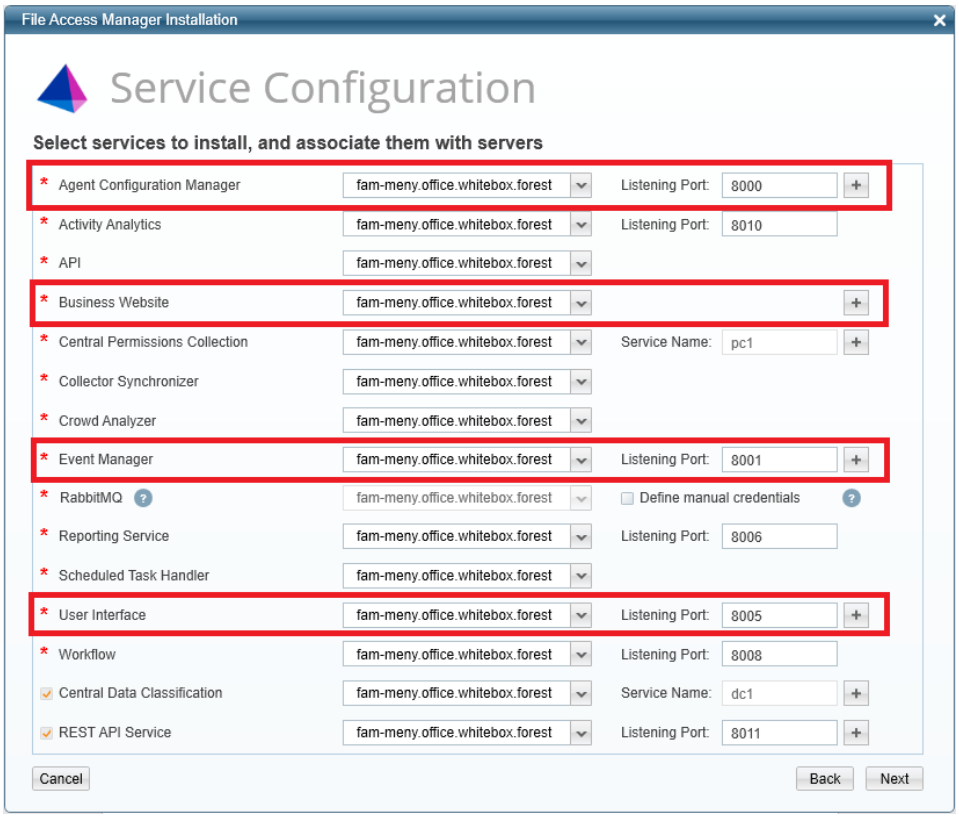
Perform the following:

- Add an additional instance of the service, by clicking the **+** icon next to the service on the configuration panel.
- Configure the installer to install the service on a parallel server allocated for high availability.
- Run your load balancer on the second server (or servers).
- Configure your load balancer to select between these instances.

> Important: The load balancer should be configured for SSL passthrough. It should not terminate the client TLS connection and create a new one between the load balancer and the server. This will cause an authentication error since each client has its own client certificate.

Duplicated Services to Allocate to a Parallel Server

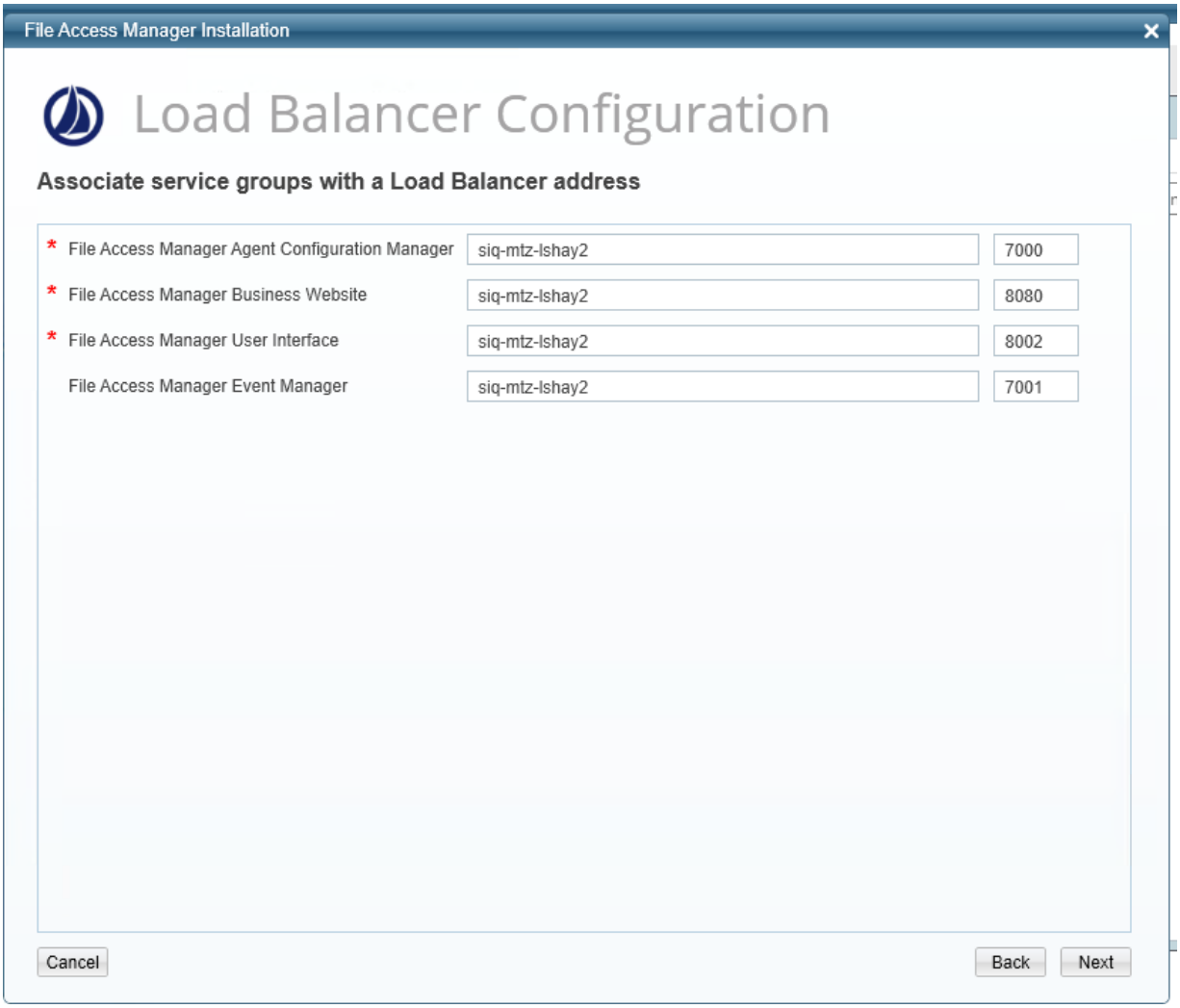
Service	Listening port
Agent Configuration Manager	8000
Business Website	80 / 443
Event Manager	8001
User Interface	8005


File Access Manager Installation
Service Configuration
Select services to install, and associate them with servers
* Agent Configuration Manager
fam-meny.office.whitebox.forest
Listening Port: 8000
* Activity Analytics
fam-meny.office.whitebox.forest
Listening Port: 8010
* API
fam-meny.office.whitebox.forest
* Business Website
fam-meny.office.whitebox.forest
* Central Permissions Collection
fam-meny.office.whitebox.forest
Service Name: pc1
* Collector Synchronizer
fam-meny.office.whitebox.forest
* Crowd Analyzer
fam-meny.office.whitebox.forest
* Event Manager
fam-meny.office.whitebox.forest
Listening Port: 8001
* RabbitMQ
fam-meny.office.whitebox.forest
Define manual credentials
* Reporting Service
fam-meny.office.whitebox.forest
Listening Port: 8006
* Scheduled Task Handler
fam-meny.office.whitebox.forest
* User Interface
fam-meny.office.whitebox.forest
Listening Port: 8005
* Workflow
fam-meny.office.whitebox.forest
Listening Port: 8008
Central Data Classification
fam-meny.office.whitebox.forest
Service Name: dc1
REST API Service
fam-meny.office.whitebox.forest
Listening Port: 8011
Cancel
Back
Next

Load Balancer Configuration

The Load Balancer Configuration screen lists all the services that support high availability. Services that have not been defined with multiple instances in the previous stage will be grayed out.

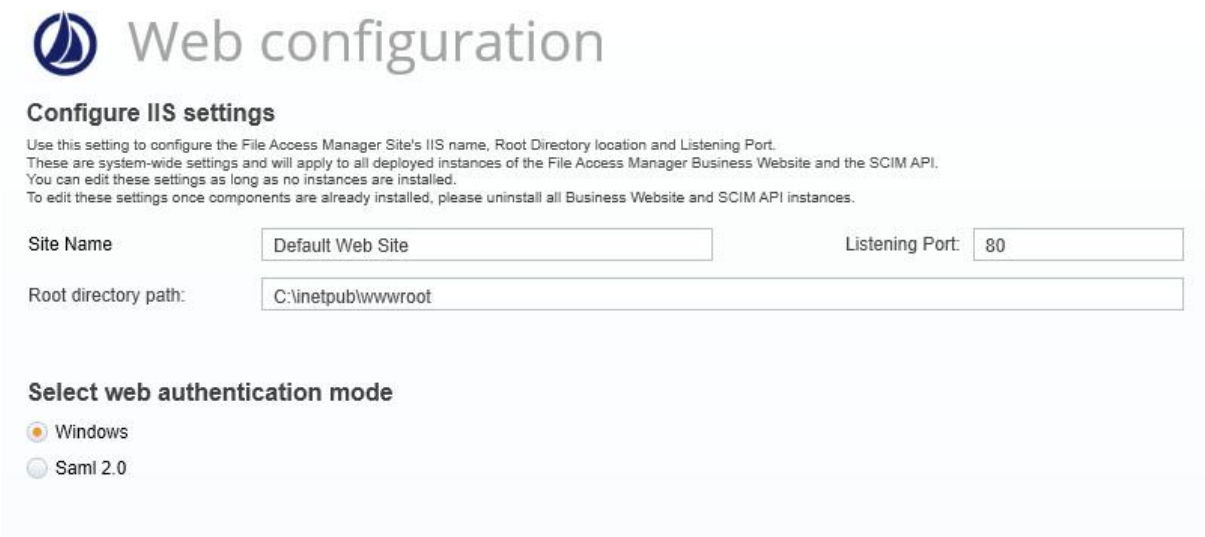
- Server Address: The server address of the high availability server allocated for this service.
- Port: The port should be unique



Note: The Load Balancer ports will be different from the ones described in Inter-service Communication.

Website Configuration

After configuring the services, the Web configuration screen will display.



IIS Settings

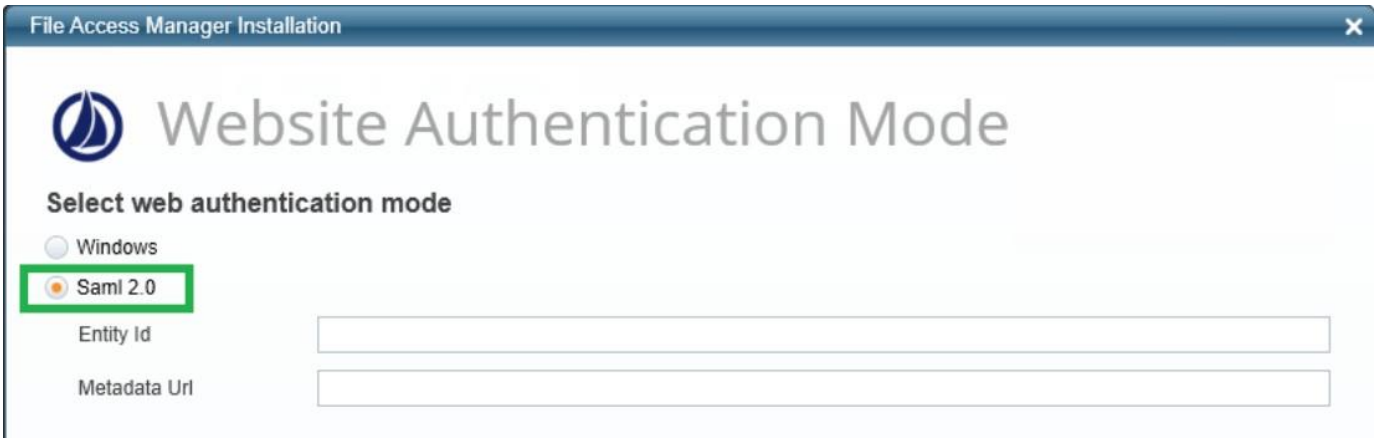
These settings allow for a non-default IIS installation.

Change the site name and physical path. File Access Manager will install its websites on the specified location.

> Note: Both site name and directory path must be changed for a non-default installation.

Website Authentication Mode

Now you can decide the type of authentication mode.



Windows

Using an Active Directory identity store

SAML 2.0

> Note: Refer to the SAML and SSO Installation guide for more information.

Using a 3rd party authentication store, such as Okta, ADFS or Azure.

Selecting SAML 2.0 on the Website Authentication Mode opens the SSO provider identification fields

- ***Entity ID***

  The application name of the relevant SSO provider

- ***Metadata URL***

  The URL to the relevant SSO provider

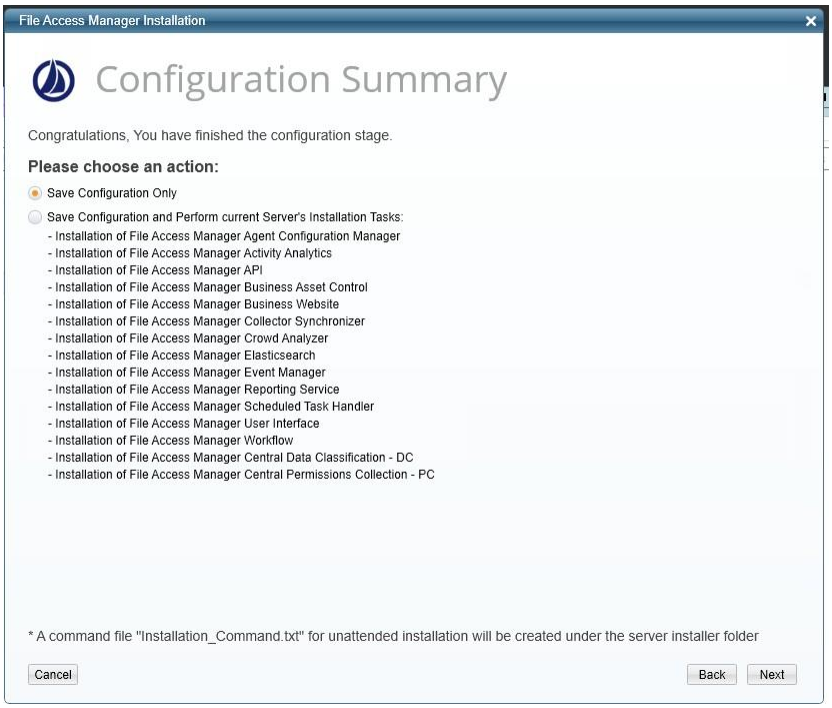
These fields are defined when creating an application in the relevant SSO provider. If you haven't created them yet, see the relevant section within the SAML and SSO Installation Guide.

- Creating an ADFS Application
- Creating an Azure Application
- Creating an Okta Application

Continue with the installation, without creating an authentication store.

Configuration Summary

1. Select the **Save Configuration Only** option.
2. Click **Next**.



Storing the Configuration

The installation process using the server installer creates a text file containing the commands for installation of the services on any server defined in the configuration.

The configuration itself is stored in the database.

Depending on the method of installation, select the next action. (See Performing the Installation

- Select **Save Configuration Only** to save the configuration without installing on this server.
- Select **Save Configuration and Perform current Server's Installation Tasks** option to start the installation of the services on the current server.

Click **Next** to install the services on the current server.

If the services installed require a system restart, the installer will open a popup message requesting a restart. Following the restart, run the installer again to continue the installation process.

Performing the Installation

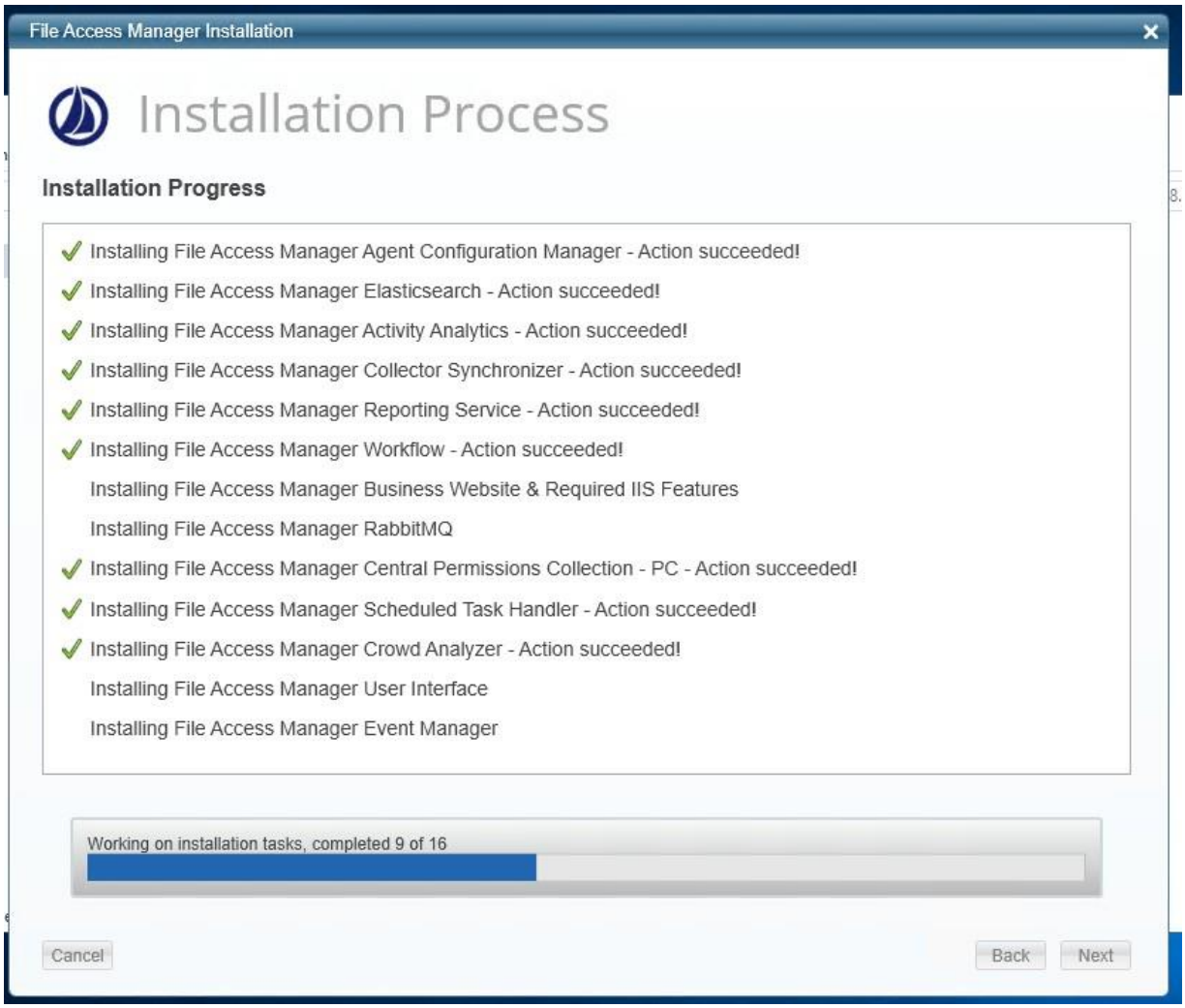
You can install using either the Server Installer or Unattended Installation, mostly for installing a system with many servers.

Installation Using the Server Installer

Some notes to consider when installing:

- The installation process runs service installers in groups.
- When a service starts the installation process, it is listed on the installation window.
- When a service is installed correctly, the application adds a checkmark next to the service name, and a comment "Action succeeded."
- If an installation of a service fails, the application adds a warning symbol on the installation line. Check the log file for further details and analysis.

> Note: The installation process at this point can take several minutes.



1. Open the Server Installer if it is not already open.
2. If you changed the configuration with the Server Installer, select **Save Configuration and Perform current Server's Installation Tasks** to start the installation.
3. If you are using an existing configuration, select **Perform Current Server's Installation tasks** to start the configured installation tasks for this server.
4. When the progress bar shows "Finished," click **Next**.
5. Check the **Open Installation Log** checkbox and click **Finish**.
6. Verify that no errors occurred during the install progress by searching the log for the word ERROR (note the capital letters).

Service Migration

This section relates to moving installed services from their original server and installing them on another server.

Services must be uninstalled prior to migrating them to a different server.

To migrate services, follow the instructions for each service on the server where the service to be migrated is installed:

> Important: You cannot use the Installation Wizard to move the Elasticsearch database from one server to another. For help with moving the Elasticsearch database, contact the File Access Manager Support Center.

Source Server – Database Connection

To connect to an existing database:

1. Start the installer in `C:\Program Files\SailPoint\FileAccessManager\Server Installer-\Server\ServerInstaller`

   > Note: Run in Administrator mode.

2. Click **Next**.
   The End User License Agreement (EULA) window displays.
3. When you have read and accepted the End User License Agreement, select the **I have read and accepted the agreement** option and click **Next**.
   The Database Details window displays the database connection details and the Database User Password filled out.

4. In the Database User Password field, enter the database user password.
5. Click **Next**.

Source Server – Configuration Modification

> Note: A service migration requires configuring another server to migrate to.

To modify the configuration:

1. In the Action Select window, select the **Create/Edit installation configuration** option.
2. Click **Next**.
   The General Configuration window displays.
3. Add new servers if necessary, as described in the section Adding a Server.
4. The General Configuration window displays.
5. Click **Next**.
6. Change the server of each of the services to be migrated as described in Service Configuration.
   The Service Configuration window displays.
7. Click **Next** to open the Configuration Summary window.

Source Server – Configuration Summary

1. Select the **Save Configuration and Perform current Server's Installation Tasks** option.
2. Click **Next** to uninstall the services to begin migration from the current server.

Source Server – Uninstallation Process

- The uninstallation process uninstalls services on this server in groups.
- When a service starts the uninstall process, it is listed on the uninstall window.
- When a service is uninstalled, the application adds a checkmark next to the service name and a comment "Action succeeded."

1. When the progress bar shows **Finished**, click **Next**.
   The Installation Summary window displays.
2. Check the **Open Installation Log** checkbox and click **Finish**.
   The Installation log displays automatically.
3. Verify that no errors occurred during the uninstall progress by searching the log for the word `ERROR` (note the capital letters).

Target Server – Database Connection

1. Connect to the database on the server that will host the migrating service(s) and run the Server Installer.
2. Follow the instructions in Source Server – Database Connection.
3. Click **Next**.

Target Server – Install Migrating Service(s)

To modify the configuration, perform the following steps:

1. In the Action Select window, select the **Perform current server's installation tasks configuration** option.
2. Click **Next**.
   The Configuration Summary window displays, listing the services to be installed.
3. Proceed with the installation by following the instructions at Preparing for Installation.

Administrative Client Installation

The Administrative Client can be installed locally on one of the File Access Manager servers or on any remote station with access to the User Interface service.

To run the Administrative Client installation, perform the following steps:

1. Open the Administrative Client Installation folder. This is in the File Access Manager distribution package.
2. Run ClientInstaller_x64.msi.
   The Welcome to the File Access Manager Administrative Client Setup Wizard screen displays.
3. Click **Next** to open the Connection Properties window.
4. In the UI Server field, enter the FQDN of the server that hosts the User Interface service.
5. In the Service Port field, enter the relevant port.
   The default port is 8005.
6. Click Next to open the Destination Folder window.
7. Enter the destination folder where you want to install the Administrative Client binaries.
8. Click **Next** to open the Ready to install File Access Manager administrative client window.
9. Click **Install to start the installation process.**
10. Once the installation completes, a confirmation message will appear on the screen.
11. Check the **Launch File Access Manager Client** checkbox to open the Administrative Client.
12. The first time you open the File Access Manager administrative client, you will see the following notification to confirm that the SSL certificate has been applied.

13. Click **Yes** if the certificate should be trusted.
    The *File Access Manager Administrator Guide* has additional information on changing the File Access

Manager security certificate.

14. Click **Finish**.
15. The SailPoint File Access Manager logon window displays.
16. When logging into the File Access Manager administrative client for the first time, use the following database user and the password entered in for the administrative client:
    User: wbxadmin
17. After you have logged in successfully, follow the instructions to change the admin password.
    The *File Access Manager Administrator Guide* has additional information on managing users.

With File Access Manager now fully installed, the user may now set up Identity Collectors, set up Data Enrichment Collector, add new applications, and more.

To set these up:

1. Login into the website with WBXAdmin and create an Identity Collector.
2. Login into the Admin Client with WBXAdmin and add a user as the admin.
3. Create a Data Enrichment Connector.

Endpoint Support Information

See the File Access Manager Connectors support document in Compass.

Each connector has a separate installation guide with more information on supported versions and prerequisites.

Recommended Secured Deployment

File Access Manager uses self-signed certificates, and SSL for internal communication.

If you require a higher security configuration, follow these configuration guidelines:

- Required Environment
- Installation Considerations and Constraints
- Post Installation Configuration
- Configuring the Process Exploit Mitigation for File Access Manager Services
- Enabling New Version Notifications

Required Environment

Windows operating system version:

File Access Manager must be installed on a Windows Server 2019 Datacenter edition, version 1809.

File Access Manager version:

For a secured deployment use File Access Manager version 8.1.0.1 or higher.

Installation Considerations and Constraints

- File Access Manager should be installed in the default directories (e.g. C:\Program Files\SailPoint). These include:
    - Server Installer
    - All Services (Core and Collectors)
    - Administrative Client
- The File Access Manager database should be created on an SQL Server that is setup with a certificate and enforces encryption.

Post Installation Configuration

Complete the following:

1. Replace all File Access Manager self-signed certificates with trusted certificates that you must provide. See section Configuring File Access Manager to Use Local Certificates, within the *Certifications and SSL Installation Guide*.
2. Setup the recommended Process Exploit Mitigation for File Access Manager services (Windows Defender settings). See Configuring the Process Exploit Mitigation for File Access Manager Services.
3. Change the IIS (on which our web components are installed on) settings to require SSL. See the File Access Manager Website SSL section within the Certifications and SSL Installation guide.
4. Set all Active Directory connections to use LDAPS (Identity Collectors / Data Enrichment Connectors).
5. Enable the File Access Manager New Version Notifications feature. See Enabling New Version Notifications.
6. For all these steps to take effect, restart all the services, or restart the server.

Configuring the Process Exploit Mitigation for File Access Manager Services

Part of the higher security settings involve configuring the Process Exploit Mitigation settings in Windows Defender for the File Access Manager Services, with the following settings enabled:

Component	Setting	Location
Control Flow Guard (CFG)	on (default)	System setting
DEP	on (default)	System setting
Randomize memory allocations (Bottom-Up ASLR)	on (default)	System setting
Export Address Filtering (EAF)	on (This requires manual configuration per service)	Program settings
Import Address Filtering (IAF)	on (This requires manual configuration per service)	Program settings

The *system settings* should be kept in the default values. Please verify that these settings above are in fact set in the Windows Exploit Protection Settings under the system tab.

The *program settings* can be updated using a script which is part of the File Access Manager deployment package, or manually in the Process Exploit Mitigation tool. Both methods are described below,

Configuring the Program Settings Using FAM.Exploit.protection.Settings.xml Script

You can enable the recommended security settings for File Access Manager using the file **FAM.Exploit.protection.Settings.xml from** in the installation folder.

To apply the settings, run the command below in an elevated PowerShell window:

```
Set-ProcessMitigation -PolicyFilePath "Full path to FAM.Exploit.protection.Settings.xml "
```

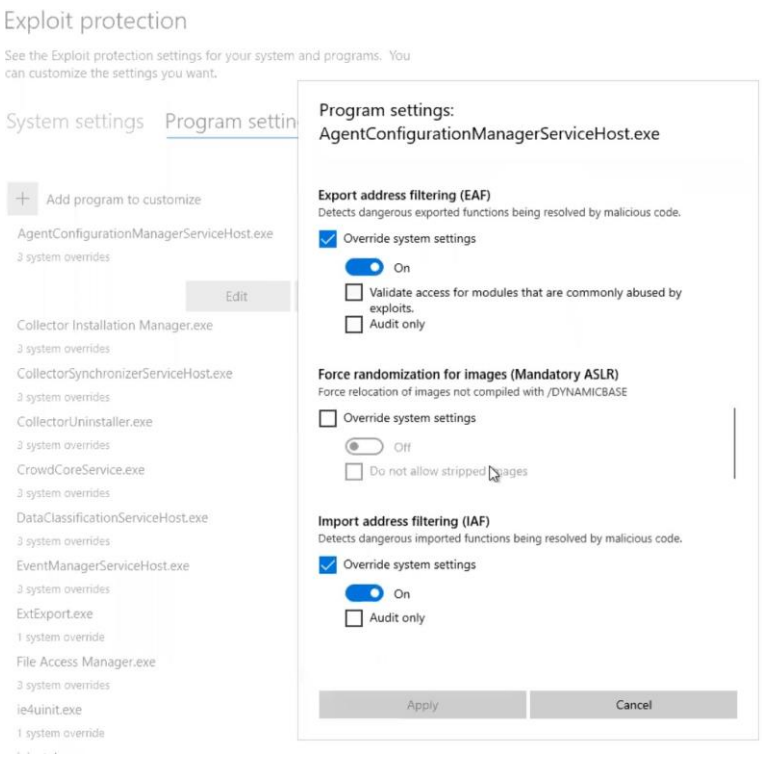
This script lists the File Access Manager to update, and configures the permissions per service.

For these settings to take effect, the services have to be restarted.

Configuring the Program Settings Using the Windows Defender Settings Tool

If you can't run the script described above, or want to see what's happening under the hood - the recommended security settings for File Access Manager can be changed manually in the Windows Defender Settings tool, as described below:

1. On the Windows server, open the *Windows Defender Settings.*
2. Click **App & Browser Control**.
3. Click **Exploit Protection Settings**.
4. Click **Program Settings** tab.
5. For each of the File Access Manager services:
    a. Click **+ Add program to customize** to open the parameters panel.
    b. Set the **EAF** and **IAF** to **on**.



6. Click **Apply** to save the changes.

7. Restart all the services modified, or reboot the server.

Enabling New Version Notifications

SailPoint publishes updates to the File Access Manager from time to time, such as new releases, minor releases, and soft- ware patches.

When updates are available, the application can send an email to the File Access Manager 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 to this address when a newer version is available to download from Compass.

Removing Unnecessary Banner Information on Web Responses

Microsoft's Internet Information Server (IIS) includes a header with every response that includes the originating server and webserver version.

To remove this information, you should configure the IIS to remove the 'Server' header. The method depends on the installed IIS version, as described below:

For IIS before version 10:

In Windows IIS Manager, you can use the URL Rewrite module to create a rule to rewrite all outgoing messages, replacing the server value in the header with an empty string. A detailed description can be found on MS IIS Support blog below, in the third method "**3. Using URLReqrite**":

https://techcommunity.microsoft.com/t5/iis-support-blog/remove-unwanted-http-response-headers/ba-p/369710

For IIS version above 10

Update the SiqWeb web.cofig file

C:\inetpub\wwwroot\siqApi\web.config

```
 <?xml version="1.0" encoding="UTF-8"?>
<configuration>
  <system.webServer>
    <security>
      <requestFiltering removeServerHeader="true" />
    </security>
  </system.webServer>
</configuration>
```

Advanced Installation

Disaster Recovery

File Access Manager supports disaster recovery, based on building a parallel backup system as described below. This setup will lower any downtime incurred by physical servers going down.

The fail-over between systems is a combination of automatic and manual processes and procedures.

For a full description of the disaster recovery procedure, see the *Disaster Recovery Plan* document or contact Professional Services.

High Availability

File Access Manager supports a high availability configuration. The solution involves configuring duplicate services on additional servers, and having a customer deploy a load balancer to manage the services traffic. When a production service, or entire server stops for any reason, the load balancer will route the traffic to another service on a different server.

The services configuration is performed in the installation phase, as described in this guide.

High Security Deployment

If you require a higher security deployment, refer to the chapter Recommended Secured Deployment.

Authentication Method

The File Access Manager login process can use Active Directory, or be integrated with any identity provider (IdP) supporting SAML 2.0-based authentication.

Detailed integration steps are available for the following providers:

- Azure
- Okta
- ADFS

Unattended Installation

The installation configuration process stores the configuration in the database, and creates a file with the commands for installation of the services in the required servers.

These commands can be configured to fit the installation on multiple servers using a distribution tool.

The script is described below.

- File name: `Installation_Command.txt`
- File path: Server installer folder (C:\Program Files\SailPoint\FileAccessManager\Server Installer\Server)

Installation Command Script

The installation command file contains three commands:

- Install the server installer
- Install the services required for the current server
- Return the last error code

Install the Server Installer

This is an msi installation file that installs the server installer on this server.

Command:

```
start /wait msiexec /i "[INSTALLER_PATH]\ServerInstaller.msi" /l*v "C:\FAMIn-
staller.log" /quiet /norestart TARGETDIR="[TARGETDIR]"
```

Parameters:

`INSTALLER_PATH`: The path of the msi file

`TARGETDIR`:Target directory of the application. E.g. : c:\Program Files\SailPoint\

Run the Unattended Installer with Database Connection Parameters

The script is created without the password. You will have to add it in to the command when you copy it across.

Command:

```
start /wait /d "[TARGETDIR]\FileAccessManager\Server Installer\Server" Unat-
tendedInstaller.exe --server "database server name" --database "Database name" --
```

```
port "1433" --user "database user" --password "[PASSWORD]"
```

Parameters:

`TARGETDIR`: This should be identical to the targetdir of the previous command
server - database server name

`port`: database server port number

`database`: database name

`user`: database user name

`password`: database password

Return the last resulting error code

`0` – successful installation

For further details, check the installation log in C:\Program Files\SailPoint\FileAccessManager\Server Installer-\Server\Logs

> Note: File Access Manager identifies which installation tasks are meant for this server, according to the configuration.

Error codes:

Code	Description
0	Success
1	Unknown error
2	Unable to perform prerequisites
3	Error in verifying the installation
4	Some services failed to install
5	There is a pending reboot on this machine. Please reboot and re-run the File Access Manager Server Installer
6	Bad arguments were passed to executable
7	Database version not compatible with server installer version
8	Database connection failed
9	Server address resolution failed

Uninstalling File Access Manager

To uninstall the File Access Manager completely (High level):

> Note: You will uninstall the services when migrating the services to another server. Contact your Product Services support contact for assistance when uninstalling services.

Feature to Uninstall / Remove	Uninstall Method
File Access Manager Administrative Client	Windows Programs and Features
Collectors (Permission, Data Classification, Activity Monitor)	SailPoint Collector Installation Manager.
Elasticsearch	SailPoint script and manual steps
Java	Windows Programs and Features
Other File Access Manager Services (including the website)	SailPoint Server Installer
Folders of application and data created by the installation	File Explorer
Registry keys created by the installation	Regedit (or similar)

Uninstalling the File Access Manager Administrative Client

To completely remove the Administrative Client:

1. If the Administrative Client is running, close it.
2. Open the window Programs and Features (Control **Panel > Programs > Programs and Features**)
3. Right click **File Access Manager Client** and choose **uninstall**.
4. Delete the folder %SECURITYIQ_HOME%\Client – this is the folder on which the administrative client was installed.
5. Delete the environment variables SECURITYIQ_HOME and SECURITYIQ_HOME_LOGS.

Uninstalling the Collectors

The collectors are services that collect information from the connected applications, for the File Access Manager to analyze. The collectors consist of the following:

- Permission collector
- Data Classification collector
- Activity Monitor collector

To uninstall the collectors:

1. Open the Collector Installation Manager.
2. Click uninstall for each of the collectors.

   The collectors can be uninstalled in any order.

   When the last collector has been uninstalled, if there are no other File Access Manager services running, the Connector Installation Manager will uninstall the Watchdog service.

Remove folders:

Delete the folder **Collectors** – this is an installation folder that you created when downloading the collector installation manager from the SailPoint source.

Remove registry keys:

Using a Windows registry editor, remove the folder **HKEY_LOCAL_MACHINE > Software > whiteboxsecurity > WhiteOPS > Components**.

If this server has no other services installed, you can remove the entire folder **whiteboxsecurity**.

Uninstalling the File Access Manager Services

To uninstall the File Access Manager services:

- Uninstall all the remaining services
- Cleanup the remaining folders and registry keys

Server Stop/Start Process

File Access Manager servers need to be shut down and restarted in a specific order to ensure proper connectivity between services after the restart.

Shutdown

These services may be running individually on their own dedicated File Access Manager servers, or may be on servers with shared services. These services or servers running these services must be shut down in the order shown below.

> Note: Disregard services that are not found in your environment, and proceed to the next service in the order shown here.

1. Activity Monitors
2. Permission Collectors and Data Classification Collectors
3. Central Permission Collection and Central Data Classification
4. RabbitMQ
5. Event Manager and IIS
6. Core and UI Services
7. Elasticsearch
8. Agent Configuration Manager (ACM)
9. Scheduled Task Handler
10. Microsoft SQL Server database

Startup

Services or servers that were shut down in the order shown above must be restarted in this order.

> Note: Disregard services that are not found in your environment, and proceed to the next service in the order shown here.

1. Microsoft SQL Server database
2. Scheduled Task Handler
3. Agent Configuration Manager (ACM)

4. Elasticsearch
5. Core and UI Services
6. Event Manager and IIS
7. RabbitMQ
8. Central Permission Collection and Central Data Classification
9. Permission Collectors and Data Classification Collectors
10. Activity Monitors

Validation Steps

Follow these steps after restarting the services/servers, to ensure that your environment is active and running normally.

1. Open the File Access Manager Administrative Client and click on the **Health Center**. The Health Center should show GREEN on all the tabs.
2. Refer to the appropriate application logs to ensure that the services were started without any errors.
3. If the logs show any errors related to connectivity, restart that service through the services.msc window.
4. If you still have difficulty in bringing any services up, contact SailPoint for further assistance.

Uninstalling Elasticsearch

The ElasticSearch could be installed either on a dedicated server, or on the main File Access Manager server.

You must use the Installation wizard if you want to move the Elasticsearch database from one server to another. Contact the File Access Manager Support Center if the Elasticsearch database must be moved after installation.

To uninstall the Elasticsearch:

1. Open an elevated command line in Windows and run the following commands. After running the commands, close the cmd windows:
    a. "%SAILPOINT_HOME%\elasticsearch-5.1.1\bin\elasticsearch-service.bat" remove
    b. setx JAVA_HOME "" -m

Note: There is no need to stop the Elasticsearch service before removing it.

Note: In some instances, the service will still be listed in the Windows services even though it has actually been removed. A refresh, waiting a few minutes, or a reboot (in extreme cases) will update the services list. We can trust that it has indeed been deleted.

2. From windows Programs and Features, uninstall the Java 8. This program was installed by the installer to support the Elasticsearch.
3. Delete the folder "%SAILPOINT_HOME%\elasticsearch-5.1.1". This folder stores the Elasticsearch program and configuration files, but not the actual stored data.
4. Execute the following update in the DB, to mark that the Elasticsearch database is uninstalled:

```
declare @server_name nvarchar(100) = N'ELASTICSEARCH SERVER FQDN'
delete
FROM   [whiteops].[installed_service]
WHERE  install_service_id = 20
and    server_id = (select id from [whiteops].[install_server] where name =
@server_name)
```

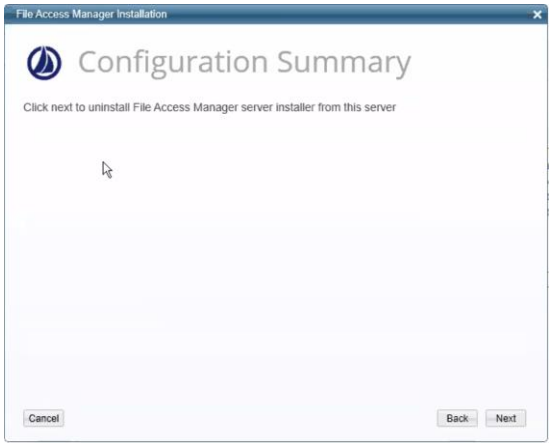
ELASTICSEARCH SERVER FQDN

This value must be replaced with the FQDN of the server from which we wish to uninstall the Elastic- search.

5. Delete the Elasticsearch data folder. Deleting this folder will delete all the activities it stores, so make sure you want to delete it. If you wish to reinstall Elasticsearch at a later time and use these data, do not delete this folder.
6. If this instance of the Elasticsearch is on a dedicated server - Uninstall the Watchdog service from this server
    a. Open the Server Installer
    b. **Next** till the Action Select page
    c. Click **Uninstall File Access Manager Features from the current server**

> Important: This procedure removes all services from this server, including the Server Installer itself.

This will open the configuration summary page. In this case, the list of services will be empty. This is normal, since no services besides the watchdog are to be uninstalled.



7. Click **Next** to start the uninstall process.

To reinstall Elasticsearch:

1. Install Elasticsearch using the Server Installer.
2. Restart the Event Manager services.

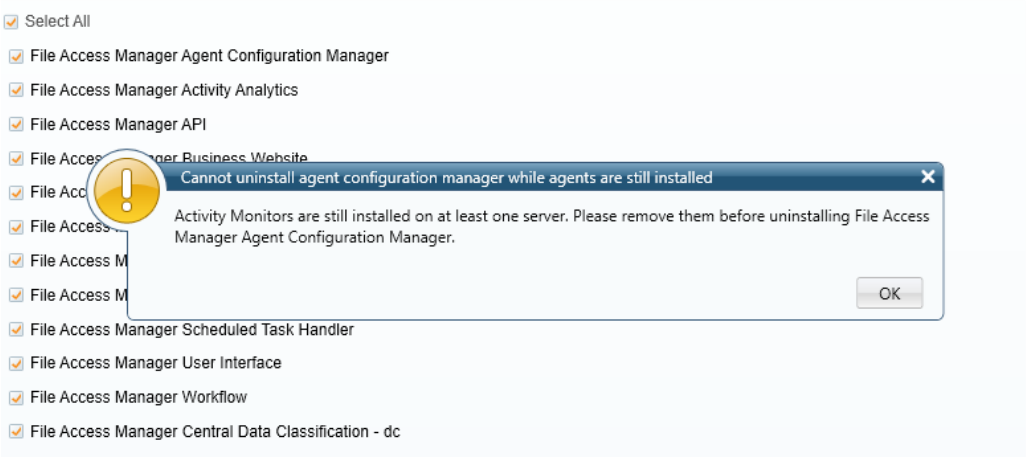
> Note: If you do not delete the Elasticsearch data folder (described below), reinstalling the Elasticsearch will maintain all the data in the website as it was before Uninstalling.

Uninstall all the Remaining Services

This procedure removes all services from this server, including the File Access Manager website and Server Installer itself.

1. Open the Server Installer
2. **Next** till the Action Select page
3. Click **Uninstall File Access Manager Features from the current server**
4. Click **Next** to start the uninstall process.

> Important: The service File Access Manager Agent Configuration Manager must be the last service to be removed, and must be removed after removing the collectors. If collectors or other services are still installed, the server installer will display an error message to that effect.



Cleanup After Uninstalling File Access Manager

1. Delete the SailPoint folder %SAILPOINT_HOME% – by default this is C:\Program Files\SailPoint.

   > Note: If this SailPoint environment variable was removed by the uninstall process, go directly to the installation folder.

2. Delete the registry keys created by the File Access Manager installation:

   a. Run RegEdit (or your favorite registry management software)

   b. Delete the folder HKEY_LOCAL_MACHINE > Software > whiteboxsecurity

3. Remove the SailPoint environment variables

   ```
   SAILPOINT_HOME
   ```

   ```
   SAILPOINT_HOME_LOGS
   ```

   ```
   SAILPOINT_APP_NAME
   ```

   > Note: In some configurations these variables are removed by the uninstall process.

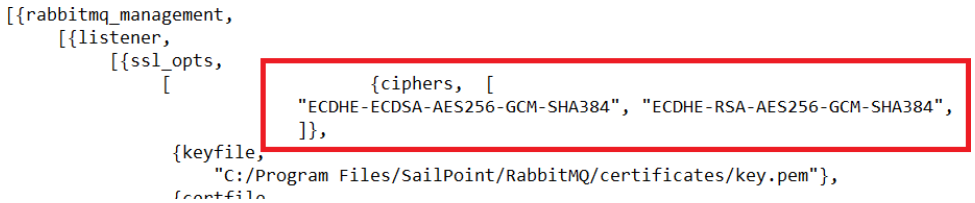
RabbitMQ Ciphers

The cipher algorithms that are utilized by RabbitMQ can be configured to meet customer requirements using the following steps:

1. Navigate to the server which is hosting the RabbitMQ service and stop the service.
2. Navigate to the Rabbit configuration location, generally located at:
   a. C:\Program Files\SailPoint\RabbitMQ\data\rabbitmq.config
3. With the desired cipher, update the current configuration to include the cipher section to the existing config file in both sections.

   OR

   Use the following example script to replace the current config file after updating the cipher section with the desired ciphers.



Here is an example script:

```
[{rabbitmq_management,
    [{listener,
        [{ssl_opts,
            [           {ciphers,  [
                         "ECDHE-ECDSA-AES256-GCM-SHA384", "ECDHE-RSA-AES256-GCM-
SHA384",
                         ]},
       {keyfile,
                    "C:/Program Files/SailPoint/RabbitMQ/certificates/key.pem"},
              {certfile,
                  "C:/Program Files/SailPoint/Rab-
bitMQ/certificates/rabbitmq.cer"},
              {cacertfile,
                   "C:/Program Files/SailPoint/RabbitMQ/certificates/ca.cer"}]},
         {ssl,true},
         {port,15671}]}]},
```

```
          {ssl, [{versions, ['tlsv1.2', 'tlsv1.1', tlsv1]}]},
 {rabbit,
     [
     {tcp_listeners, []},
     {log,[{file,[{level,error}]}]},
      {ssl_options,
          [
           {versions, ['tlsv1.2']},
           {ciphers,  [
                           "ECDHE-ECDSA-AES256-GCM-SHA384", "ECDHE-RSA-AES256-GCM-
SHA384",
                           ]},
           {keyfile,
               "C:/Program Files/SailPoint/RabbitMQ/certificates/key.pem"},
           {certfile,
               "C:/Program Files/SailPoint/RabbitMQ/certificates/rabbitmq.cer"},
           {cacertfile,
               "C:/Program Files/SailPoint/RabbitMQ/certificates/ca.cer"},
           {fail_if_no_peer_cert,false},
           {verify,verify_peer}]},
      {ssl_listeners,[5671]}]}].
```

Note: To find which ciphers are available, run a PowerShell command Get-TlsCipherSuite on the RabbitMQ machine. This will populate a list with a set of IANA names which can be used to search the site Ciphersuite Info to locate the OpenSSL name, which is what RabbitMQ configuration supports.

4. Restart the RabbitMQ service.

   Note: If the configuration file is not properly updated, the service will fail to start.

5. Wait a few minutes and then login to the Admin Client.

6. Navigate to the **Health Center > Infrastructure** tab and verify RabbitMQ is green.

Troubleshooting

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

Users Cannot Log into the Website After First Installation

When installing File Access Manager for the first time, the Identity Sync task has to complete its operation in order to get a list of users who can log into the web application. You can follow the progress of this task on the Health Center in the administrative client. The task status is generally displayed in the web application which you cannot access before this task has completed.

3rd Party SSO Login Users Cannot Access the Website

1. Verify that the correct connectivity values were stored in the database.

   Table: system_configuration_value

   Record: WebSamlConfiguration

   The JSON should be similar to the sample below, depending on the SSO provider.

   EntityId

   The File Access Manager application created in the SSO provider

   MetadataUrl

   Generated in the process of creating the application above

   ```
   {
   "EntityId": "FAM_SAML_LogIn",
   "MetadataUrl": "https://dev-39214733.okta.-
   com/app/exka5w2f1LvL5gpI05d6/sso/saml/metadata",
   "SignatureAlgorithm": "http://www.w3.org/2001/04/xmldsig-more#rsa-sha256",
   "CertificateValidationMode": "0",
   "RevocationMode": "0"
   }
   ```

2. Verify that all the users from the SSO provider were added correctly to the File Access Manager database.

   The identity collector should upload the users listed in the data source into the following tables:

   - whiteops.ra_user
   - crowdSource.[user]

Connection Errors

Following a successful upgrade to version 8.3, services will only accept http2 connections (version 8.3 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=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.

Firewall Verification

If an installation problem occurs when installing File Access Manager on multiple servers, verify the firewall is not blocking the installation process.

Access Denied to Business Website

If access is denied to the File Access Manager business website, it may be caused by not having proper configuration in IIS. .NET Trust Level in IIS needs to be set to Full to allow for consistent access.

Use the IIS Manager to set the .NET Trust Level to Full. This can be found by navigating to Default Web Site > .NET Trust Levels. Select **Full (internal)** from the dropdown. Select **Apply**.

Failed Installation of IIS

If File Access Manager did not install the IIS, verify the Request Filtering is turned off. If Request Filtering is on, the File Access Manager business website may fail to load.

Communication Issues Between Collectors or Activity Monitors and the Agent Configuration Manager

The Agent Configuration Manager and the Collectors or Activity Monitors might have trouble communicating with each other. This would result in no activities being collected or failed Crawl / Permission Collection / Data Classification tasks.

This could be caused by a registry value interfering with the SSL handshake that usually occurs between those services. This would introduce an extra criterion for the certificate to comply with that isn't normally part of the procedure, preventing the service from properly identifying itself.

This registry value is called SendTrustedIssuerList and it's located under the following path: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL.

If this registry value exists and is set to 1 (true), set it to 0 (false).

If it doesn't exist or is set to 0 (false), then this is not the cause of the issue.

More information about this registry value can be found here: https://learn.microsoft.com/en-us/windows-server-/security/tls/what-s-new-in-tls-ssl-schannel-ssp-overview#BKMK_TrustedIssuers

Further Information

For further configuration, and installation of the File Access Manager website, see chapter File Access Manager Initial Configuration in the *File Access Manager Administrator Guide*.