SailPoint IdentityIQ

Version: 8.0

File Access Manager Server Installation Guide

Table of Contents

List of Figures

List of Tables

Table of Revisions

Ver. #	Description	Author	Date
5.0	Final Version	Jonathan Rappeport	10 Jan 2017
5.1	First Draft	Jonathan Rappeport	08 Feb 2017
5.1	Second Draft	Jonathan Rappeport	13 Jun 2017
5.1	Third Draft	Jonathan Rappeport	26 Sep 2017
6.0	First Draft	Jonathan Rappeport	10 May 2018
6.1	• Updated installation screens • Document reformatted	Josh Lewin	29 Nov 2018
8.0	• SIQDEV-5232 - SSL is mandatory, not an option • Rebranding product to IdentityIQ File Access Manager • Support for **CLR Strict Security Mode**". Using this option will import a certificate into the Master database • Disaster recovery support • Rebranding – renaming to IdentityIQ File Access Manager.	Josh Lewin	5 Feb 2019
8.0 - GA	Formatting and clarification	Josh Lewin	30 Jul 2018

Chapter 1: Planning Your Installation

General

IdentityIQ File Access Manager Architecture

IdentityIQ File Access Manager architecture usually requires a central installation with some remote gateways. Most IdentityIQ File Access Manager connectors do not require any footprint on the monitored/analyzed system and therefore are installed on IdentityIQ 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 IdentityIQ File Access Manager architecture see ***Capabilities and Architecture*** in the ***IdentityIQ File Access Manager Administrator Guide***.

Disaster Recovery

IdentityIQ 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.

IdentityIQ File Access Manager Connector Services

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

Sizing Considerations

IdentityIQ 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 IdentityIQ 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

Service	CPU	Memory	Disk
Elasticsearch	Minimum of 4 cores, Recommended 8	Minimum of 8Gb, Recommended 16Gb	0.5kb per event
SQL Database	See Chapter 3: ***Database Configuration***		3.5kb per event

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

Chapter 2: Support Matrix

IdentityIQ File Access Manager Server Support Information

Table 1. Server Support Information

System	Supported Versions
IdentityIQ File Access Manager Servers	Windows 2012/2012R2/2016/2019
Workstation	Windows 7 and above
Browser	IE11, Edge, Safari, Chrome, Firefox
Database	MS SQL Server 2008R2/2012/2014/2016 64 bit 2017

Endpoint Support Information

See the relevant Connector Installation guide for more information on supported versions and prerequisites.

Chapter 3: Database Configuration

General

Dedicated Instance

We recommend installing IdentityIQ 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 IdentityIQ 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 IdentityIQ File Access Manager representative.

Required Features

IdentityIQ File Access Manager uses MS SQL Standard Edition that utilizes the database engine only. No other feature is required. IdentityIQ 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"
- 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 REAL 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 IdentityIQ File Access Manager is very write I/O intensive.

Temp Database

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

Ensure that the database is:

- defined on a separate drive
- real and formatted to a 64K allocation unit
- allocated a Temp database file for each real 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

Table 2. 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

Chapter 4: Server Services Installation

Preparing for Installation

Collecting the Required Data

the table below describes the pre-installation checklist.

Table 3. Pre-Installation Checklist

Item	Verification / information to list
Database server	Verify connectivity to the DB server.
Database instance	Database name for IdentityIQ File Access Manager
Static/Dynamic ports	Static port – port number Dynamic port – use 0
(optional) SysAdmin (SA) user + password	SA user (or equivalent).
Data files location	Full path for database data files.
FileStream files location	Full path for database FileStream files.
Log files location	Full path for database log files.
Servers names	Verify connectivity and name resolution (NetBIOS name and DNS name).
Services distribution	The location of the various server services to be used in the installation.

Communication Requirements

IdentityIQ 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.

See Section 2: ***Capabilities and Architecture*** in the ***IdentityIQ File Access Manager Administrator Guide*** for a detailed description of the different IdentityIQ File Access Manager Services, architecture and the required ports.

Preparing the Servers

Each server used in the IdentityIQ File Access Manager environment must have the following:

- .NET 4.5 (any service pack is acceptable)

  Note: The current .NET framework version can be seen in the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4\Full (or until NDP for .NET versions before 4.0)

- .NET 4.7.2 is required on the server in which the API is installed
- Server installation binaries:
  - Access the server installation either from a network share or locally

Chapter 5: IdentityIQ File Access Manager Installation

General Information

The IdentityIQ File Access Manager installation consists of the following phases:

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

Installation log file

The installation process is logged to the installation logs. Any errors in the installation process, and 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 Installation

The first step of every IdentityIQ File Access Manager server is to run the Server installer.

The Server installer is the product responsible for managing the configuration of the IdentityIQ File Access Manager central servers, and the installation process.

To start the Server installation, perform the following steps:

1. Run the ServerInstaller.msi file.

   The "Welcome to File Access Manager Server Installer Setup Wizard" window displays.

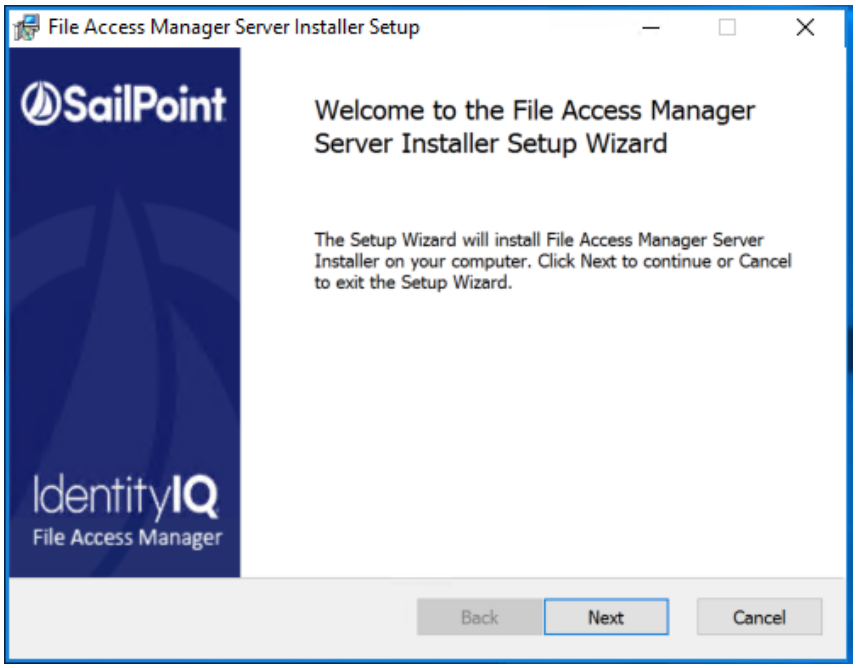


Figure 1. Welcome Window – Installer Setup

2. Click **Next.**
3. Select the destination folder and click **Next**.
4. Click **Install** to start the installation, or **Back** to change the installation folder.
5. After the installation processes are complete, the "Completed the IdentityIQ File Access Manager Server Installer Setup Wizard" window displays.
6. Check the **Launch the IdentityIQ File Access Manager server installer** check box, which launches the Install Wizard of the Server Services.

   Note: Opting for manual database creation requires the creation to be done before launching the installer.

7. Click **Finish**.

The “File Access Manager Installation” window displays.

Figure 2. File Access Manager Installation window

8. Click **Next**

Creating a Database (through 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**

3. The “End User License Agreement” (EULA) window displays. 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.

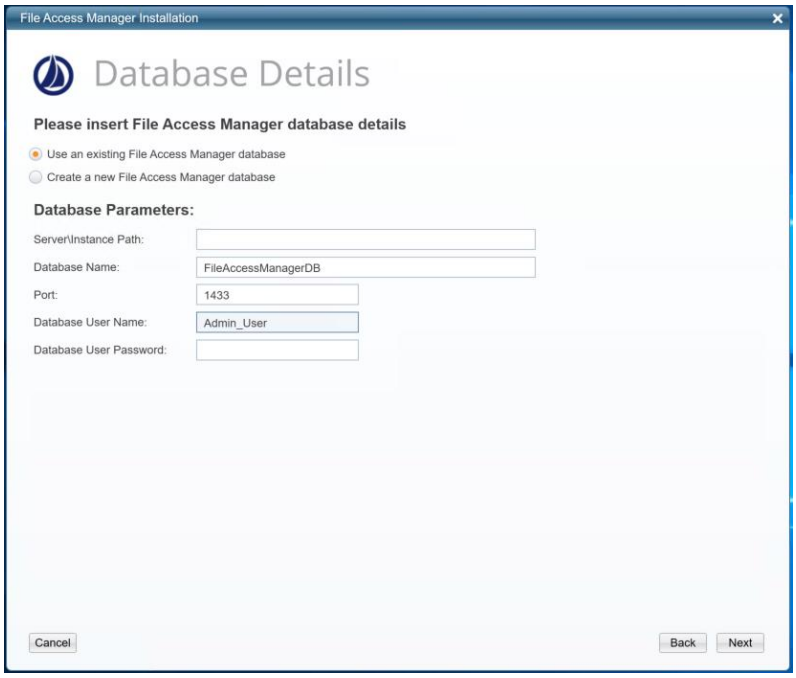


Figure 3. Database Details

4. Identify the installation type:

    a. If you are installing IdentityIQ File Access Manager for the first time
        - Select “**Create a New** IdentityIQ File Access Manager **Database**”
        - Enter the server\instance path, database name and port number required in order to connect the database. (Write 0 for dynamic ports)
        - Enter the database username and password to create.
        - **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.
        - Enter the database files path. This folder must exist on the database server
        - Enter the file stream files path
        - Enter the log files path. This folder must already exist on the database server.
        - Enter a password for the admin client user and repeat the password
        - 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 IdentityIQ File Access Manager database.
            i. For SQL, type in the SA User Field and password for the system administrator
            ii. For Windows, the Server Installer will use the logged-in user to connect to the database.

    b. If you are installing additional services to an existing File Access Manager installation
        - Select “Use an existing IdentityIQ File Access Manager Database”

5. Click **Next**

6. The “Action Select” window displays. 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. Defining the servers as Production (default) or Disaster Recovery
2. Assigning IdentityIQ File Access Manager services to Production servers
3. Assigning IdentityIQ File Access Manager services to Disaster Recovery servers
4. Installing

Adding a Server

To create the configuration for a new server, perform the following steps:

1. Open the "General Configuration" window.

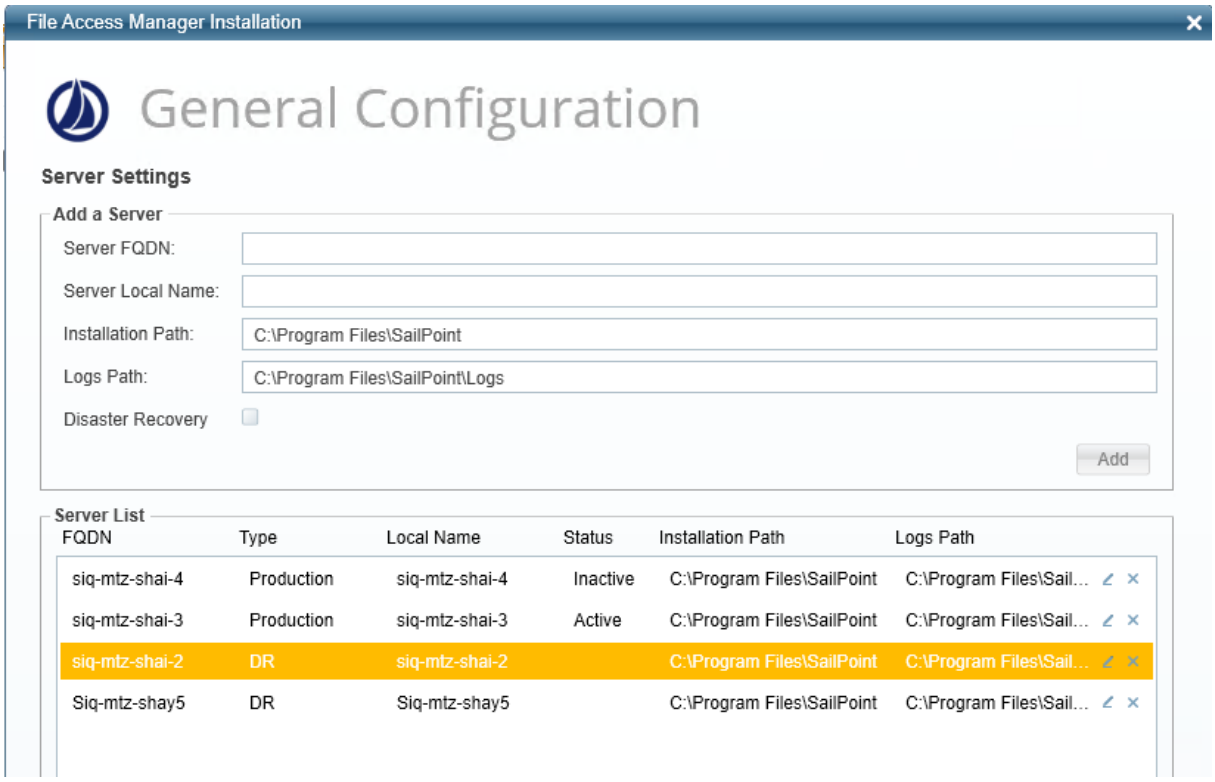


Figure 4. General Configuration

Notes:

- **Use this screen to define all the servers on which the IdentityIQ File Access Manager services will be installed and whether the installed server is a production server (Prod), or a disaster recovery server (DR).**
- **This does not include the Windows file server activity monitors**

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 **IdentityIQ 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 **IdentityIQ File Access Manager** logs will be written.

e. If this server is designated as a disaster recovery server, select the **Disaster Recovery** checkbox.

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

Note: IdentityIQ File Access Manager services use SSL communication.

4. Click **Next**.

Disaster recovery configuration: Setting the active servers

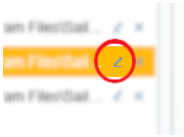
You can set the servers to be active or inactive in the Server Installer. If a Production server is set to be Active, the corresponding Disaster Recovery Server will be in idle mode, and vice versa.

The user can set the server as active and inactive from any machine.

To toggle a production server to Active\Inactive

1. Open the Server Installer and connect to an existing DB.

2. Select the Production server which will be Toggled Up\Down and click the Edit button to open the server detail panel



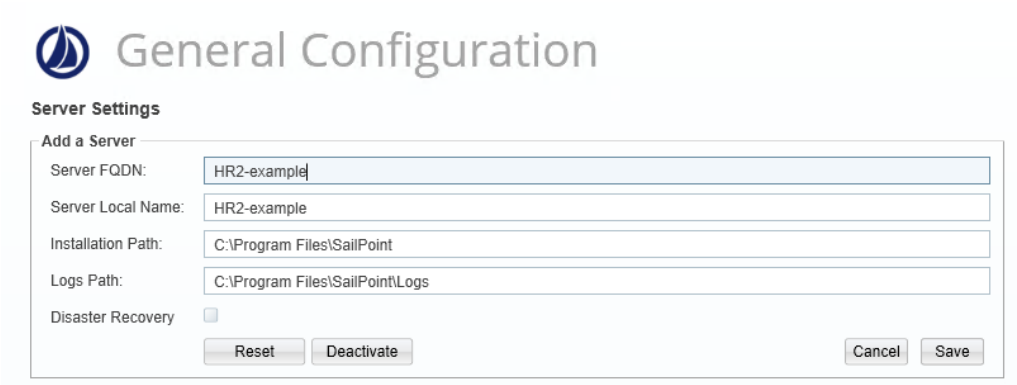


Figure 5. Server detail panel

3. Click **Activate** / **Deactivate** to change the server state.

4. Click **Save**

Services Configuration

There are two Service Configuration screens: one for the Production environment, and one for the Disaster Recovery environment.

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 Services Configuration window

Note: Use the scroll bar to see all the configuration input fields.

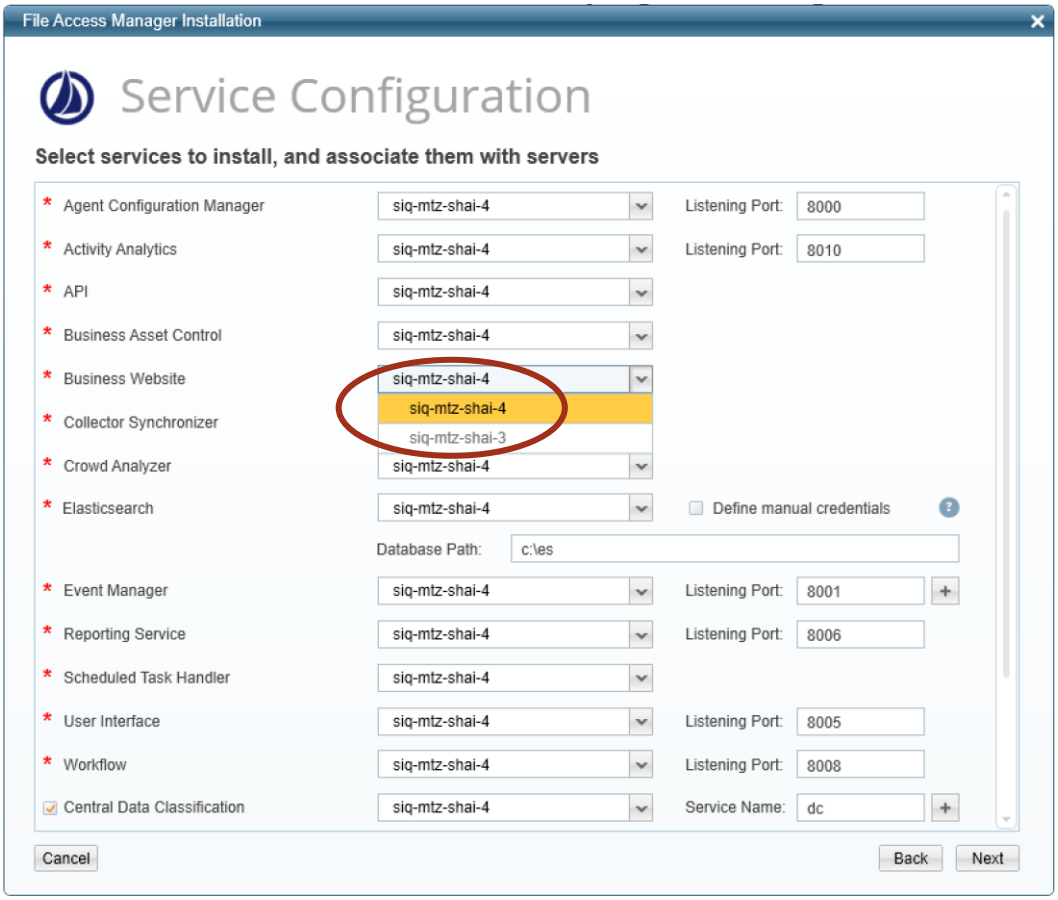


Figure 6. Service Configuration

Services Distribution

3. Select the server to use in the Production environment for each service. The services distribution should be planned before installation. Preferably with SailPoint installation experts. Note the dropdown list of available servers will include only Production servers (See image above).

Services Ports

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

Elasticsearch

5. If this is the first time you are installing IdentityIQ File Access Manager, specify the name of the server on which to install the Elasticsearch database, as well as the full database path.

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

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

RabbitMQ

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

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

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

Agent Configuration Manager

Note: 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.

Event Manager

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

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

Central Data Classification

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

11. Click the **+** next to the port to add instances.

12. Click the **x** to remove instances.

Central Permissions Collection

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

13. Provide a unique name for each service. This name will be displayed during the Application configuration wizard when defining a new Application in the IdentityIQ File Access Manager Admin Client.

14. Click **Next** to repeat this configuration for the Disaster Recovery environment. The list of servers in the next panel will be servers defined previously as Disaster Recovery servers.

Note: IdentityIQ 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.

Business Website

Note: The Business Website installs IIS if it's not installed yet.

Service Installation

Configuration Summary

1. In the “Action Select” window, select the Configuration Summary option.
2. Click **Next**.

   The “Configuration Summary” window displays.

   Note: IdentityIQ File Access Manager identifies which installation tasks are meant for this server, according to the configuration.
3. Select the “Save Configuration and Perform current Server’s Installation Tasks” option to start the installation of the services on the current server.
4. Click **Next** to install the services on the current server.

Installation Process

Notes

- **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.**

5. When the progress bar shows “Finished”, click **Next**. This opens the “Installation Summary” window
6. Check the “Open Installation Log” check box and click **Finish**. The Installation log displays automatically.
7. 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.

To migrate services, perform the following steps on the server where the service to be migrated is installed:

Note: 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 IdentityIQ File Access Manager Support Center.

Source Server – Database Connection

To connect to an existing database, perform the following steps:

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**.

4. The "Database Details" window displays with the database connection details and the Database User Password filled out.

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

6. Click **Next**.

Source Server – Configuration Modification

To modify the configuration, perform the following steps:

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

2. Click **Next** to open the "General Configuration" window

3. Add new servers if necessary, as described in the section ***Adding a Server*** above.

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

   The "General Configuration" window displays.

4. Click **Next**

5. Change the server of each of the services to be migrated as described in ***Services Configuration*** above.

   The Services Configuration window displays.

6. 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

Notes:

- **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**.
2. The "Installation Summary" window displays.
3. Check the "Open Installation Log" check box and click **Finish**. The Installation log displays automatically.
4. 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 at 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 Service Installation.

Chapter 6: Administrative Client Installation

The administrative Client can be installed locally on one of the IdentityIQ 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 IdentityIQ File Access Manager Admin 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 IdentityIQ File Access Manager Admin 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” check box to open the Administrative Client.
12. The first time you open the IdentityIQ File Access Manager Admin Client, you will see the following notification to confirm that the SSL certificate has been applied.

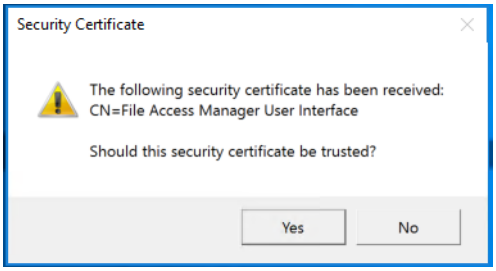


Figure 7. Security certificate confirmation

13. Click “Yes” if the certificate should be trusted.
    The IdentityIQ File Access Manager Administrator Guide has additional information on changing the IdentityIQ File Access Manager security certificate.
14. Click **Finish**

    The SailPoint IdentityIQ File Access Manager logon window displays.
15. When logging into the IdentityIQ File Access Manager Admin Client for the first time, use the following database user and the password entered in for the Admin Client:

    User: wbxadmin

16. After you have logged in successfully, follow the instructions to change the admin password.
    The IdentityIQ File Access Manager Administrator Guide has additional information on managing users.