



File Access Manager Upgrade Guide

Version: 8.4

Revised: March 27, 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

- Planning Your Upgrade** **3**
- Installation Prerequisites** **4**
 - File Access Manager Server Support Information 4
 - Pre-upgrade Steps 4
- Upgrading to Version 8.4** **10**
 - Verification During the Upgrade Process 11
- Post Upgrade Actions** **13**
 - Upgrading the File Access Manager Server Installer 13
 - Upgrading File Access Manager Client 13
 - Validating the Upgrade 13
- Troubleshooting** **14**
 - Signature is Not Valid Error 14
 - Watchdog Failed During the Upgrade 14
 - Elasticsearch Prerequisite Script Failed 15
 - Verify RabbitMQ Service Install Prerequisite Script Failed 15
 - Installing Elasticsearch Prior to RabbitMQ Install 16

Planning Your Upgrade

Caution: File Access Manager version 8.4 can only be upgraded from version 8.3 and above. Before the upgrade, back up the database.

Upgrade Path

File Access Manager version 8.4 can be upgraded from version 8.3 and above only.

For earlier versions of File Access Manager, or SecurityIQ, first upgrade to File Access Manager 8.3 before starting the 8.4 upgrade process.

Please read this upgrade guide in its entirety before starting the upgrade process.

Version Numbers

The version number is displayed on the bottom right corner of the File Access Manager Administrative Client screen.

If the version number is not displayed in the Administrative Client, refer to the SecurityIQ 5.1 Upgrade guide to upgrade from an older version.

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

Pre-upgrade Steps

Before the upgrade, back up the database. All of the following should be installed prior to the upgrade.

RabbitMQ

RabbitMQ is now a mandatory service, therefore RabbitMQ must be installed using the 8.3.x installer prior to the 8.4 upgrade. Without installing RabbitMQ, the upgrade process will not be completed.

Note: In case File Access Manager is installed on both Production and Disaster Recovery servers, RabbitMQ must be installed on both servers prior to the upgrade process.

.NET 6.0

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. .Net 6.0 must be installed before the upgrade.

You can download the latest 6.0.x Hosting Bundle version from [here](#).

Note: Without completing this step, the upgrade will fail.

Download .NET 6.0

Not sure what to download? [See recommended downloads for the latest version of .NET.](#)

6.0.13 Security patch

[Release notes](#) Latest release date January 10, 2023

Build apps - SDK

SDK 6.0.405

OS	Installers	Binaries
Linux	Package manager instructions	Arm32 Arm32 Alpine Arm64 Arm64 Alpine x64 x64 Alpine
macOS	Arm64 x64	Arm64 x64
Windows	Arm64 x64 x86 winget instructions	Arm64 x64 x86
All	dotnet-install scripts	

Included runtimes

.NET Runtime 6.0.13
 ASP.NET Core Runtime 6.0.13
 .NET Desktop Runtime 6.0.13

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

- All servers hosting File Access Manager services, including all Activity Monitors, must have .NET Core 6.0.x installed as a prerequisite for the upgrade.
- The administrative client computer must contain .NET Framework 4.7.2.
- The User Interface service server must contain .NET Framework 4.7.2.
 .NET 6 and .NET Framework 4.7.2 can be installed on the same server.

Verifying .NET Settings

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

1. Open a CMD window.
2. Execute the following command:

```
dotnet --list-runtimes
```

The output should consist of at least the following:

```
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.

Elasticsearch 8.2.2

File Access Manager 8.4 requires Elasticsearch version 8.2.2 to be installed prior to the upgrade procedure. Without installing Elasticsearch, the upgrade operation will not be completed.

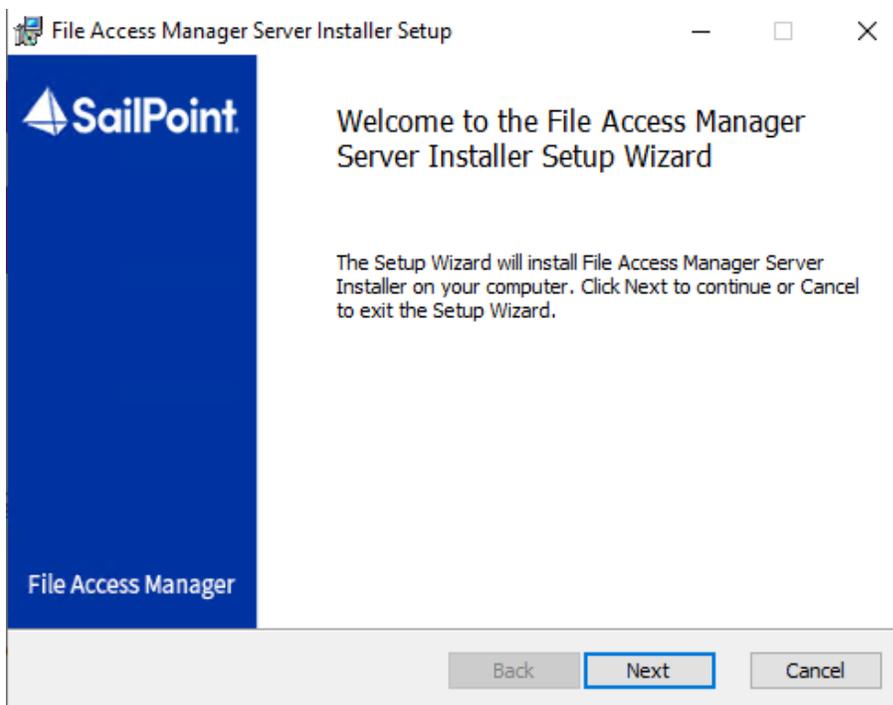
If File Access Manager is deployed in Production and Disaster Recovery mode, install the new Elasticsearch in both the Production environment and Disaster recovery environment.

Note: New Elasticsearch cannot be installed on a server which contains an already existing Elasticsearch installation. It must be on a server without an Elasticsearch installation.

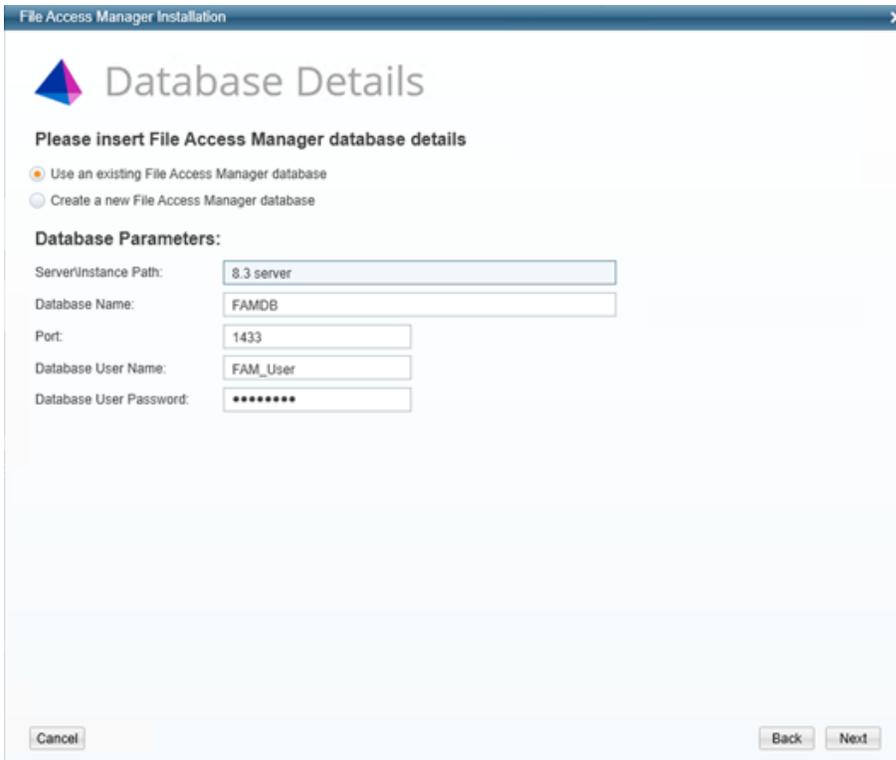
Note: If a user is upgrading to File Access Manager 8.4 from an older version, the user must keep the legacy Elasticsearch running in order to avoid loading failures.

To Install New Elasticsearch 8.2.2 perform the following steps:

1. Copy "ServerInstaller.msi" from the File Access Manager 8.4 installation package into the new File Access Manager server and perform the installation.



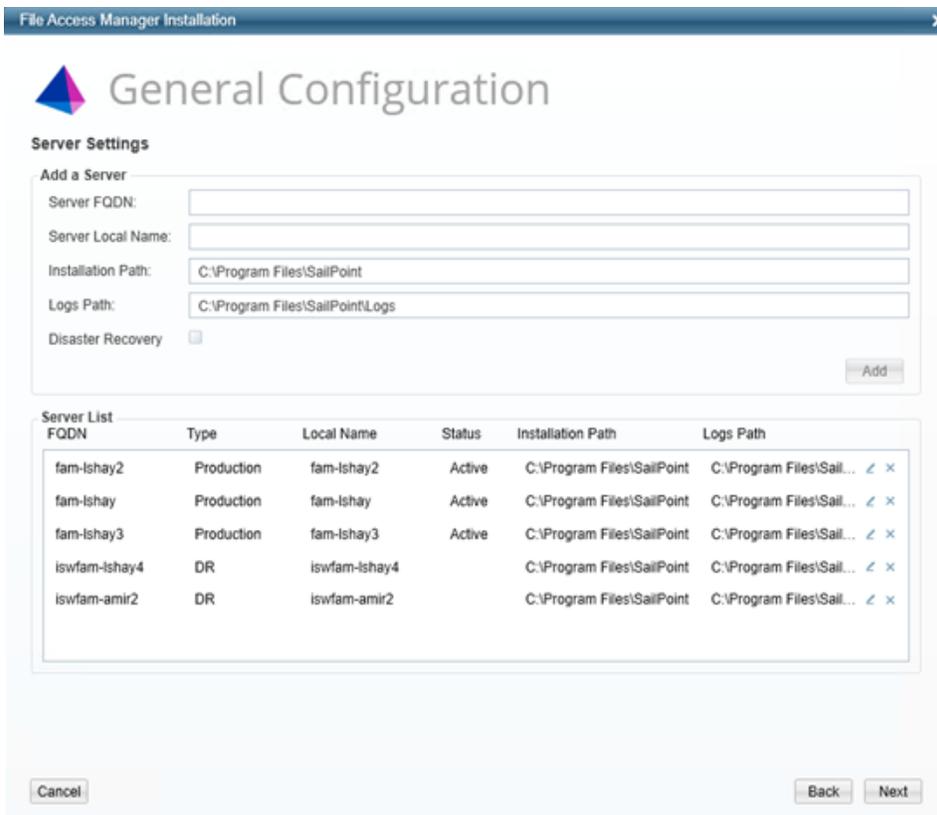
2. Open the server installer as an administrator and choose the Use Existing File Access Manager Database option.
3. Insert valid database information and select **Next**.



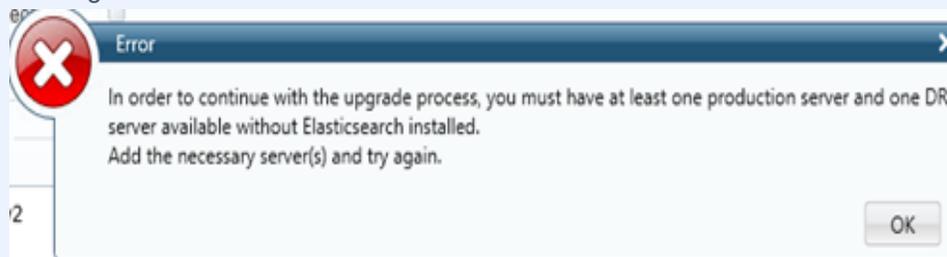
4. Select Create/Edit Installation Configuration and click **Next**.



5. In the General Configuration screen, insert the new File Access Manager server(s) that will be used to install the new Elasticsearch and select **Next** to continue.

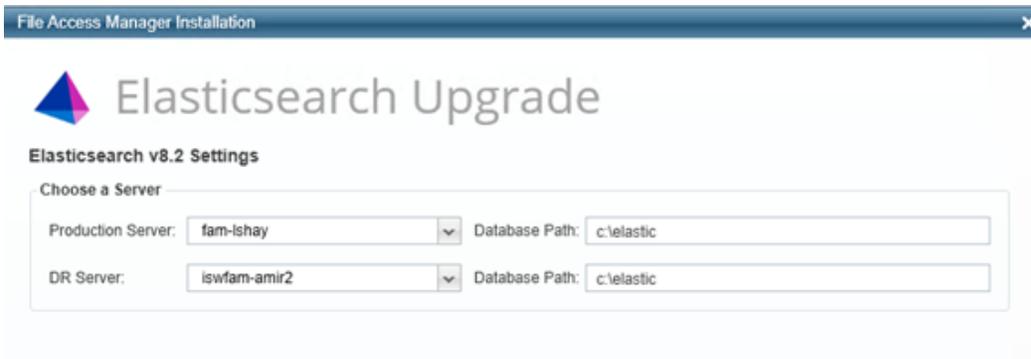


Note: If File Access Manager is installed in Production and Disaster Recovery, make sure to insert both Production and Disaster Recovery server addresses. Without inserting them both, you will not be able to proceed into the next step and you will get the following error message.



- Choose the server that the new Elasticsearch will be installed on and insert the database path.

Note: The database path is generated during the installation. Make sure that the path is valid



7. Choose the Save Configuration and Perform current Server's Installation Tasks button and select **Next**.
The installation process will begin.



8. Once the Installation process is completed, close the Server Installer Wizard.

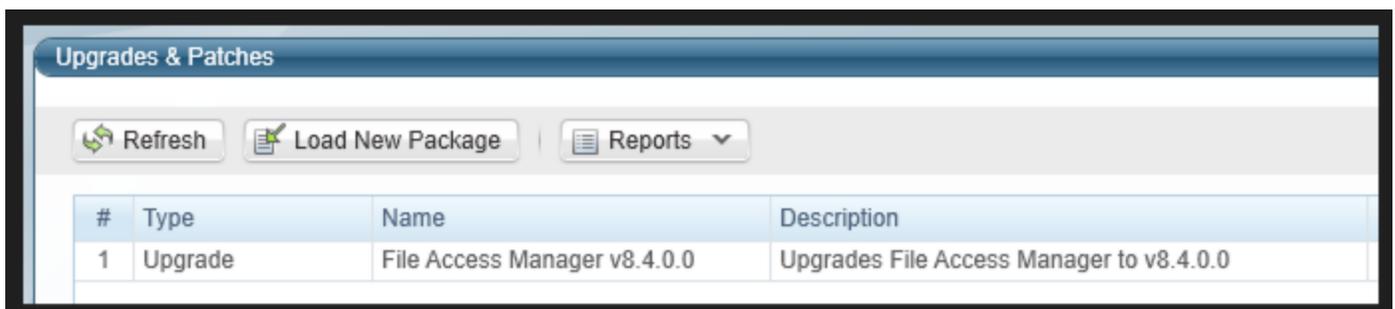
Upgrading to Version 8.4

Caution: File Access Manager version 8.4 can only be upgraded from version 8.3 and above. Before the upgrade, backup the database.

1. Extract the “File Access Manager v8.4.zip” installation package.
2. Navigate to the folder “v8.4 Upgrade”.
3. Open the File Access Manager Administrative Client.
4. Navigate to **Upgrades & Patches > Load New Package**.
5. Load “File Access Manager v8.4.wbxpkg” from the upgrade folder.
 - a. Click **Browse** and load the file from the upgrade folder.
 - b. Click **Upload Package**.
 - c. Click **Save**.
 - d. Right-click the upgrade package and select *See More > Start Installation*.
 - e. Click **Confirm** to start the installation.

Note: In any case of failure, right click the failed script and select "**save log file**."

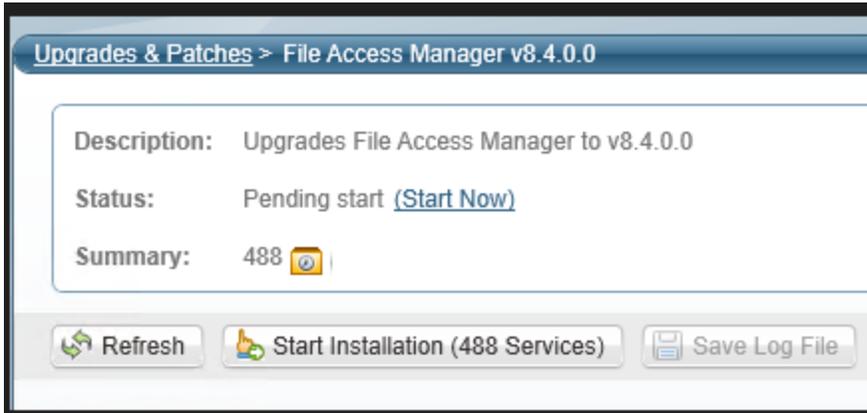
Note: If the package has already been uploaded into File Access Manager, the system will give a warning message, and block uploading the package again.



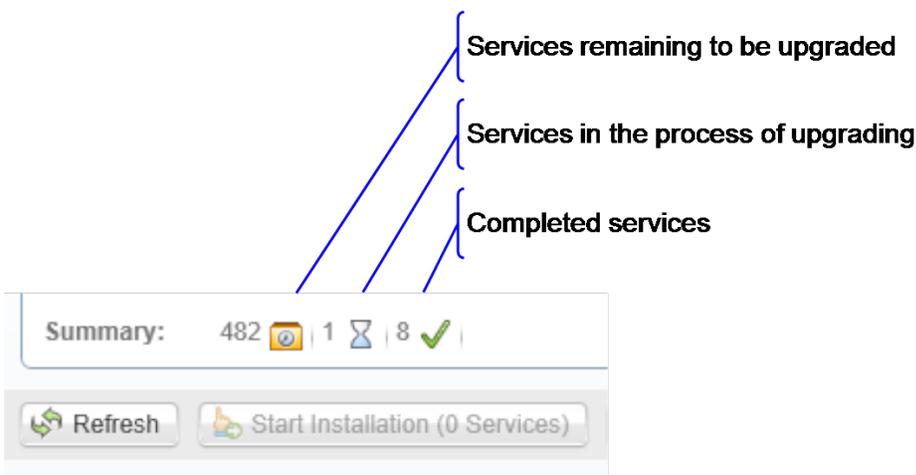
Verification During the Upgrade Process

During the Upgrade process, services are upgraded. Some servers may require a restart to complete the upgrade.

1. When the upgrade starts, you will see a window with the total number of services that need to be upgraded on the top left side of the upgrade window.



2. When you click Refresh you can see the number of upgraded services and the remaining services to be upgraded.



3. Click **Refresh** until you see that there are no services left to upgrade.
4. Some services, such as WebSite and FamAPI, might require a Restart of the server they are running on, in order to complete the upgrade process.
5. To check which services require a server restart:

- a. Click the Status pane in the Services grid

#	<input type="checkbox"/> Upgrade?	Service	Server	Type	Status
1	<input type="checkbox"/>	File Access Manager API	v51-v52-i	Infrastructure	PendingRestart
2	<input type="checkbox"/>	Database		Security/IDB	Completed

- b. If a service has the status “Pending Restart,” you will need to perform a server restart in order to complete the upgrade process for this specific service. The installed server is listed in the table.
 - c. Once the server is restarted, the upgrade operation will be able to proceed.
6. Once all the services have been upgraded successfully, with a status of “Finished”, you can proceed to the next step—[Post Upgrade Actions](#).

Note: The Summary number may vary across installations, depending on the specific configuration, such as the number of Permission Collector services, or other configuration changes.

Upgrades & Patches > File Access Manager v8.4.0.0

Description: Upgrades File Access Manager to v8.4.0.0

Status: Finished

Summary: 490

Post Upgrade Actions

Following the upgrade, follow the configuration steps below.

Upgrading the File Access Manager Server Installer

The Server Installer must be upgraded on each of the File Access Manager central servers.

To upgrade the Server Installer on each central server, perform the following steps:

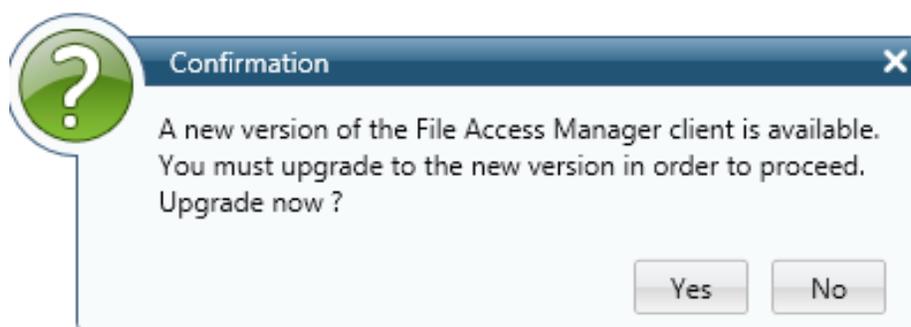
1. Copy "ServerInstaller.msi" from the "v8.4 Full Installers" folder to the server.
2. Run "ServerInstaller.msi".
3. Follow the instructions on the screen to complete the upgrade process.

Note: The server installer can be run in "unattended mode."

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

Upgrading File Access Manager Client

On the first run of the File Access Manager Administrative Client after an upgrade, a popup message displays, requesting that you upgrade the client. During the upgrade, you will be required to reenter the server on which the User Interface Service is installed and choose the installation folder.



Validating the Upgrade

To validate the installation, and verify that the correct versions were installed, check in the Windows Add/Remove programs in the control panel.

The versions of the File Access Manager components should be listed as 8.4.0.0.

Troubleshooting

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

Signature is Not Valid Error

Problem: During the package upgrade step, you receive a warning with the message:

Loading the package failed due to the following error: Signature is not valid.

The problem is likely that the machine hosting the User Interface service does not have the necessary Root Certificate (or is missing part of the Certification Chains leading up to the root) to validate the signature of the upgrade package.

Suggested solution:

1. To resolve the issue you should check that the machine hosting the User Interface service contains the root certificate named "DigiCert Assured ID Root CA," which has a serial # 0C:E7:E0:E5:17:D8:46:FE:8F:E5:60:FC:1B:F0:30:39.

If this root certificate is missing, it can be downloaded from <https://www.digicert.com/digicert-root-certificates.htm> and installed as a trusted root certificate manually.

2. Another reason for this error would be that the machine hosting the User Interface service has been configured so that updating root certificates is disabled. To fix this, set the registry value HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\SystemCertificates\AuthRoot\DisableRootAutoUpdate to 0, and retry uploading the upgrade package.

This will allow Microsoft to restore the missing root certificate during validation.

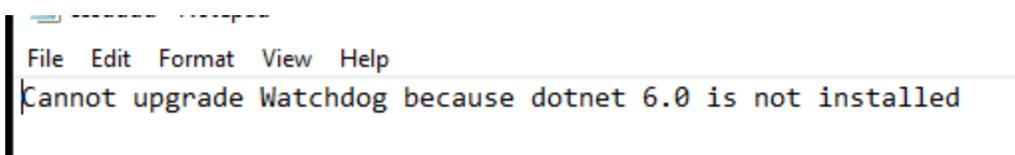
Watchdog Failed During the Upgrade

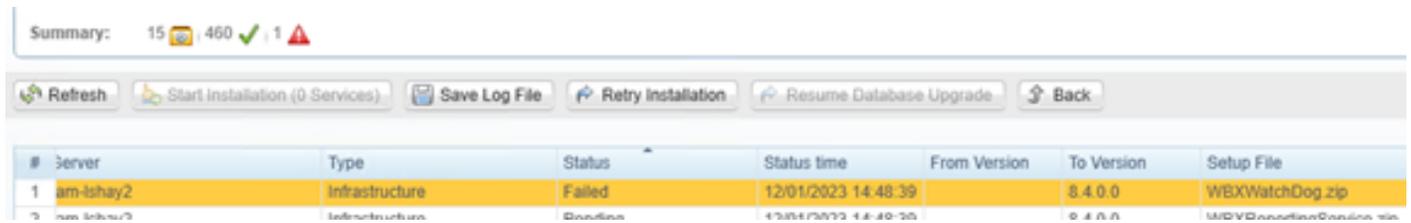
Problem: During File Access Manager V8.4, the watchdog upgrade failed and the upgrade operation has been suspended.

To check the error, perform the following steps:

1. Right click the failed row and select **Save Log File**.
2. Open the saved log file.

The error below (screenshot) indicates that .NET 6.0 is not installed on the File Access Manager server.





Suggested solution:

Perform the .NET 6.0 install in the [Pre-upgrade Steps](#) section and rerun the failed upgrade step.

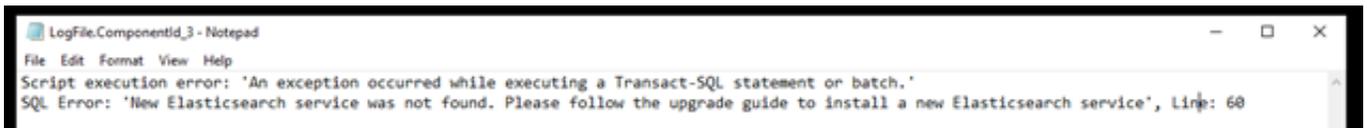
Elasticsearch Prerequisite Script Failed

Problem: The pre-requisite script (Elasticsearch Upgrade) failed and the upgrade operation has been suspended.

To check the error, perform the following steps:

1. Right click the failed row and select **Save Log File**.
2. Open the saved log file.

The error indicates that Elasticsearch was not installed prior to the upgrade operation.



Suggested solution:

Perform the Elasticsearch 8.2.2 install in the [Pre-upgrade Steps](#) and rerun the failed script.

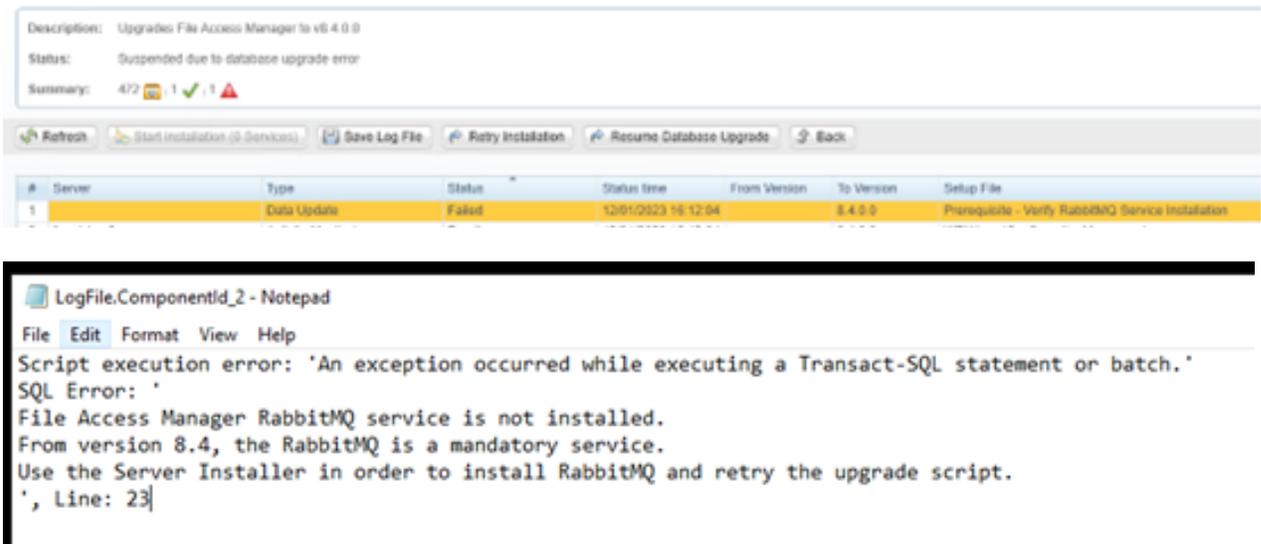
Verify RabbitMQ Service Install Prerequisite Script Failed

Problem: The script failed and the upgrade operation has been suspended.

To check the error, perform the following steps:

1. Right click the failed row and select **Save Log File**.
2. Open the saved log file.

This error indicates File Access Manager RabbitMQ service is not installed.

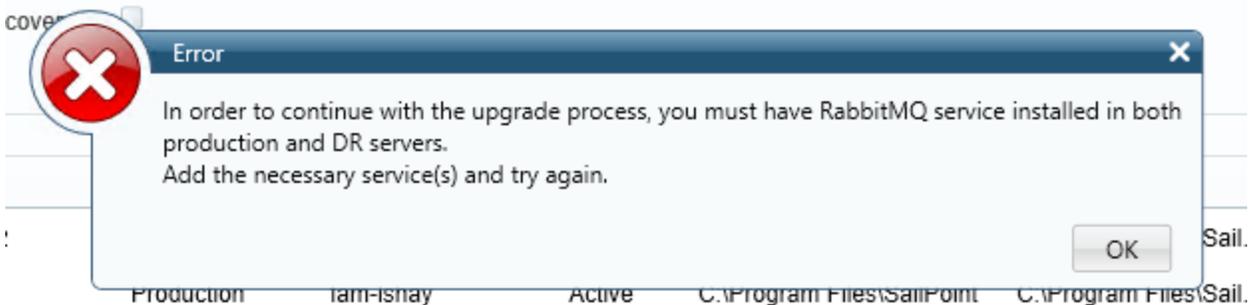


Suggested solution:

Perform the RabbitMQ install in the [Pre-upgrade Steps](#) and rerun the failed script.

Installing Elasticsearch Prior to RabbitMQ Install

Problem: Installing Elasticsearch prior to installing RabbitMQ will show the following error inside the Server Installer:



Suggested solution:

Perform the RabbitMQ install in the [Pre-upgrade Steps](#) After the install of RabbitMQ, install the new Elasticsearch DB.