



File Access Manager Upgrade Guide

Version: 8.2 Revised: November 22, 2021

This document and the information contained herein is SailPoint Confidential Information

Copyright and Trademark Notices.

Copyright © 2021 SailPoint Technologies, Inc. All Rights Reserved.

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

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

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

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

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

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

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

Contents

Contents	ii
Planning Your Upgrade	4
Support Matrix	5
File Access Manager Server Support Information	5
Endpoint Support Information	5
Changes Performed During the Upgrade	6
Activity Monitor Configuration	6
From Field Added to SMTP Response	6
Pre-upgrade Steps	7
.NET	8
Verifying .NET Core Settings	9
Verify that the Unique Hash Fix has Completed - Script	9
HTTP/2.0 Settings	11
Ensuring HTTP/2 Support	11
Upgrading to Version 8.2	12
Verification During the Upgrade Process	12
Post Upgrade Actions	15
Upgrading the File Access Manager Server Installer	15
Upgrading File Access Manager Client	15
Validating the Upgrade	15
Updating the IIS Binding Port	15
Updating Data Classification Verification Algorithms	16
O365 Application Access Tokens	16
Configuring Exchange Online to Support Version 8.2	17
Creating an Azure Application for Exchange Online	18
Creating and Configuring the Application Automatically	18
Creating and Configuring the Application Manually	19
Step 1: Register the Application in Azure AD	19

Step 2: Assign API Permissions to the Application	19
Step 3: Generate a self-signed certificate	20
Step 4: Attach the Certificate to the Azure AD Application	21
Step 5: Assign Azure AD role to the application	21
Troubleshooting	22
Watchdog Failed During the Upgrade	22
"Access Denied" Message While Logging Into the Business Website	22
.NET Core Installation Issue	22
Website Folder Structure Issues	23
Suspended due to Database Upgrade Error	24
Upgrade Checklist	24
Signature is Not Valid Error	26
Connection Errors Following an Upgrade	27

Planning Your Upgrade

Upgrade Path

File Access Manager version 8.2 can be upgraded from version 8.1sp3 and above Only.

For earlier versions of File Access Manager, or SecurityIQ, first upgrade to File Access Manager 8.1 and then install service pack 3 before starting the 8.2 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.

Exchange Online Note to Support OAuth 2.0 Authentication

If you have an Exchange Online application, you'll have to configure the application, as described in section [Configuring Exchange Online to Support Version 8.2](#).

Support Matrix

File Access Manager Server Support Information

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

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.

Changes Performed During the Upgrade

Some of the changes included in this upgrade require changes to settings and the database.

Activity Monitor Configuration

When an activity from an unknown resource is detected, there is no longer the option to discard the activity ("No auto learning mode")

During the upgrade process, activity monitors that had this setting will be set to Store the Activity (Full learning mode)

When upgrading, a change in behavior will occur on the Permission Forensics page. Any filters previously created with **business resource name** or **business resource full path** will have the operator and value deleted during the upgrade. These filters have to be rewritten after the upgrade with one of the valid values.

From Field Added to SMTP Response

The upgrade process will take the report response From field as the unified email From value. This value can be set in the SMTP Account Configuration screen.

Pre-upgrade Steps

Please read these steps carefully when planning the upgrade. Some of these tasks, such as the hash recalculation task might take a long time to run.

Before the upgrade, perform the following steps:

1. Back up the database.
2. **Remove deprecated connectors**

The following connectors were deprecated in version 8.2. If you have applications using these versions, uninstall the activity monitors:

- a. Windows File Server (Agent) 2008/2012

Windows File Server 2012R2 is still supported.

- b. Exchange 2010
- c. SharePoint 2010

3. Make sure you ran the Isilon Unique Hash Revert Fix For 8.1 SP3.

These scripts make backend changes which will restart the recalculation of the hashes in preparation for the upgrade.

This is a fix that should be run on v8.1 SP3. The fix is described in Compass [here](#)

<https://community.sailpoint.com/t5/File-Access-Manager-Blog/Prerequisite-Scripts-in-Preparation-for-8-2-Encouraged-to-Run/ba-p/189470>

This process takes a long time to complete, depending on the database size. Make sure to take this into consideration when planning the upgrade.

To verify that the process has completed, you can run the script below on the database (Copy from [Verify that the Unique Hash Fix has Completed - Script](#)) and check the results.

When Upgrading from Versions Before 8.1

Data Remediation Rules

Before upgrading to version 8.1, verify that you don't have any data remediation rules with more than one action.

Rules that contain more than one action will be deleted by the upgrade process.

Regex Matching is Now Case Sensitive in Data Classification

Starting from version 8.1 regex matching in the data classification module will be case sensitive by default. To make a regex ignore case, use the prefix "(?!)"

For example: "home" will find "home", but ignore "Home"

The regex "(?!)home" will find "Home", "HOME" and "HoMe"

Classify Behavioral Rules Tasks

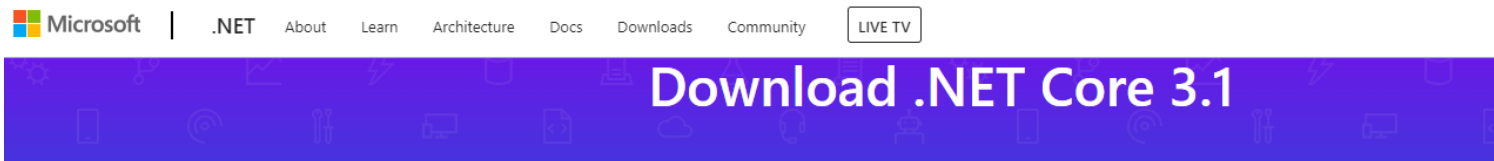
As part of the upgrade to V8.1, any existing scheduled Classify Behavioral tasks are removed.

There is a single, system generated scheduled classify behavioral rules task, that covers all applications. This task is created disabled.

.NET

File Access Manager requires the latest ASP.NET Core 3.1.x Hosting Bundle. This bundle consists of .NET Runtime and ASP .NET Core Runtime.

You can download the latest 3.1.x Hosting Bundle version from [here](#)



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

Release information	Build apps - SDK	Run apps - Runtime																												
<p>v3.1.16</p> <p>Security patch</p> <p>Release notes</p> <p>Released June 08, 2021</p>	<p>This release contains multiple SDKs. If you're using Visual Studio, look for the SDK that supports the version you're using. If you're not using Visual Studio, install the first SDK listed.</p> <p>SDK 3.1.410</p> <p>Visual Studio support Visual Studio 2019 (v16.7) Visual Studio 2019 for Mac (v8.10)</p> <p>Included in Visual Studio 16.4.23, 16.7.16, 16.9.7</p> <p>Included runtimes .NET Runtime 3.1.16 ASP.NET Core Runtime 3.1.16 .NET Desktop Runtime 3.1.16</p> <p>Language support C# 8.0 F# 4.7 Visual Basic 15.9</p> <table border="1"><thead><tr><th>OS</th><th>Installers</th><th>Binaries</th></tr></thead><tbody><tr><td>Linux</td><td>Package manager instructions</td><td>Arm32 Arm64 Alpine</td></tr><tr><td>macOS</td><td></td><td>x64</td></tr><tr><td>Windows</td><td>Hosting Bundle x64 x86</td><td>Arm32 Arm64</td></tr></tbody></table>	OS	Installers	Binaries	Linux	Package manager instructions	Arm32 Arm64 Alpine	macOS		x64	Windows	Hosting Bundle x64 x86	Arm32 Arm64	<p>ASP.NET Core Runtime 3.1.16</p> <p>The ASP.NET Core Runtime enables you to run existing applications. On Windows, we recommend installing the Hosting Bundle, which includes the .NET Runtime and IIS support.</p> <p>IIS runtime support (ASP.NET Core Module v2) 13.1.21133.16</p> <table border="1"><thead><tr><th>OS</th><th>Installers</th><th>Binaries</th></tr></thead><tbody><tr><td>Linux</td><td>Package manager instructions</td><td>Arm32 Arm64 Alpine</td></tr><tr><td>macOS</td><td></td><td>x64</td></tr><tr><td>Windows</td><td>Hosting Bundle x64 x86</td><td>Arm32 Arm64</td></tr></tbody></table> <p>.NET Desktop Runtime 3.1.16</p> <p>The .NET Desktop Runtime enables you to run existing applications. This release includes the .NET Runtime, so you don't need to install it separately.</p> <table border="1"><thead><tr><th>OS</th><th>Installers</th></tr></thead><tbody><tr><td>Windows</td><td>Hosting Bundle x64 x86</td></tr></tbody></table>	OS	Installers	Binaries	Linux	Package manager instructions	Arm32 Arm64 Alpine	macOS		x64	Windows	Hosting Bundle x64 x86	Arm32 Arm64	OS	Installers	Windows	Hosting Bundle x64 x86
OS	Installers	Binaries																												
Linux	Package manager instructions	Arm32 Arm64 Alpine																												
macOS		x64																												
Windows	Hosting Bundle x64 x86	Arm32 Arm64																												
OS	Installers	Binaries																												
Linux	Package manager instructions	Arm32 Arm64 Alpine																												
macOS		x64																												
Windows	Hosting Bundle x64 x86	Arm32 Arm64																												
OS	Installers																													
Windows	Hosting Bundle x64 x86																													

Without completing this step, the upgrade will fail.

- a. All servers hosting File Access Manager services, including all Activity Monitors must, have .NET Core 3.1.x installed as a prerequisite for the upgrade.
- b. The administrative client computer must contain .NET Framework 4.7.2

- c. The User Interface service server must contain .NET Framework 4.7.2

■ .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 3.1.x
- Microsoft.NETCore.App 3.1.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.

Verify that the Unique Hash Fix has Completed - Script

Copy the script to your File Access Manager database, and run it.

The results can be one of the following:

Failure messages

Please make sure you are running File Access Manager version 8.1 with Service Pack 3 or newer.

Please make sure you have deployed E-Fix SIQETN-2945 - "Isilon Unique Hash Revert Fix For 8.1 SP3

There are still @num_of_brs_to_calculate resources left to calculate. Please run the "New Unique Path Hash Calculation" task, wait for it to complete and then try again.

Success messages

SUCCESS – The "New Unique Path Hash Calculation" task only has @num_of_brs_to_calculate resources left to calculate, which is lower than the failure threshold. (The upgrade will auto complete these on upgrade)

SUCCESS – The "New Unique Path Hash Calculation" task has completed successfully.

```
-- =====  
-- Author:          Tom Gez  
-- Create date:    2021-05-24  
-- Description:    Make sure that:  
--                1. Service Pack 3 is deployed.  
--                2. SIQETN-2945 is applied.  
--                3. The new unique path hash column in  
--                   business_service is filled with hash values.  
-- =====
```

```

BEGIN TRY

    SET NOCOUNT ON;

    DECLARE @curr_br_id BIGINT;
    DECLARE @should_rebuild BIT;
    DECLARE @max_num_of_brs_to_calculate BIGINT = 1000000;
    DECLARE @num_of_brs_to_calculate BIGINT;
    DECLARE @message NVARCHAR(MAX);

    IF NOT EXISTS (SELECT 1 FROM sys.columns WHERE object_id = OBJECT_ID(N'[whiteops].[business_service]') AND name = 'unique_path_hash_new')
        RAISERROR('Column ''unique_path_hash_new'' is missing from table ''whiteops.business_service''. Please make sure you are running File Access Manager version 8.1 with Service Pack 3 or newer.', 16, 1);

    IF OBJECT_ID('[whiteops].[business_service_new_path_hash_tracking]') IS NULL
        RAISERROR('Table ''whiteops.business_service_new_path_hash_tracking'' is missing. Please make sure you are running File Access Manager version 8.1 with Service Pack 3 or newer.', 16, 1);

    IF NOT EXISTS (SELECT 1 FROM sys.columns WHERE object_id = OBJECT_ID(N'[whiteops].[business_service_new_path_hash_tracking]') AND name = 'isilon_fix')
        RAISERROR('Column ''isilon_fix'' is missing from table ''whiteops.business_service_new_path_hash_tracking''. Please make sure you have deployed E-Fix SIQETN-2945 - ''Isilon Unique Hash Revert Fix For 8.1 SP3''.', 16, 1);

    -- Get the latest resource ID to calculate hash for and whether the table rebuild has occurred
    SELECT TOP 1
        @curr_br_id = [curr_id],
        @should_rebuild = [should_rebuild_table]
    FROM [whiteops].[business_service_new_path_hash_tracking];

    IF @curr_br_id IS NULL
        RAISERROR('Table ''whiteops.business_service_new_path_hash_tracking'' is not supposed to be empty. Please contact support for information on how to proceed.', 16, 1);

    IF @should_rebuild = 1
        RAISERROR('Table ''whiteops.business_service'' must be rebuilt by the ''New Unique Path Hash Calculation'' task. Please run the task, wait for it to complete and then try again.', 16, 1);

    -- Check how many resource hashes are left to calculate
    SELECT TOP (@max_num_of_brs_to_calculate + 1) @num_of_brs_to_calculate = COUNT(1)
    FROM [whiteops].[business_service]
    WHERE [id] >= @curr_br_id;

    IF @num_of_brs_to_calculate > @max_num_of_brs_to_calculate
    BEGIN
        SET @message = 'There are still ' + CONVERT(NVARCHAR(MAX), @num_of_brs_to_calculate) + ' resources left to calculate. Please run the ''New Unique Path Hash Calculation'' task, wait for it to complete and then try again.';
        RAISERROR(@message, 16, 1);
    END
END

```

```
        ELSE IF @num_of_brs_to_calculate > 0
            SET @message = 'SUCCESS - The ''New Unique Path Hash Calculation'' task only has
' + CONVERT(NVARCHAR(MAX), @num_of_brs_to_calculate) + ' resources left to calculate,
which is lower than the failure threshold.';
        ELSE
            SET @message = 'SUCCESS - The ''New Unique Path Hash Calculation'' task has com-
pleted successfully.';

        PRINT(@message);

END TRY
BEGIN CATCH

    DECLARE @ErrorMessage NVARCHAR(4000);
    DECLARE @ErrorSeverity INT;
    DECLARE @ErrorState INT;

    SELECT
        @ErrorMessage = ERROR_MESSAGE(),
        @ErrorSeverity = ERROR_SEVERITY(),
        @ErrorState = ERROR_STATE();

    RAISERROR (
        @ErrorMessage,
        @ErrorSeverity,
        @ErrorState
    );
END CATCH
```

HTTP/2.0 Settings

In order to communicate properly and securely, all servers hosting File Access Manager services, must support HTTP/2.0. This requirement includes all load-balancers included in the File Access Manager architecture.

Make sure HTTP/2.0 is supported and enabled on all servers and load-balancers, before starting the upgrade, in order for it to complete successfully. If HTTP/2.0 is not supported, the upgrade will not complete.

Ensuring HTTP/2 Support

Following a successful upgrade to version 8.2, services will only accept http/2 connections (version 8.2 uses gRPC as the communication protocol, the requires http2).

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

Upgrading to Version 8.2

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

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

In case of update failure, **do not use** "Resume Database Upgrade" in the following cases:

- 01_SIQETN-2786-Prerequisite - Unique Hash Stage 1.sql
 - 02_SIQETN-2786-Prerequisite - Unique Hash Stage 2
- If this script fails, see [Upgrade Checklist](#)
- 03_SIQETN-2786-Prerequisite - Unique Hash Stage 3.sql
 - 28_SIQETN-2786-New Unique Hash Finalization.sql

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

The screenshot shows the 'Upgrades & Patches' section of the administrative interface. It includes buttons for 'Refresh', 'Load New Package', and a 'Reports' dropdown menu. Below these is a table with the following data:

#	Type	Name	Description
1	Upgrade	File Access Manager v8.2.0.0	Upgrades File Access Manager to v8.2.0.0

Verification During the Upgrade Process

During the Upgrade process, some services are upgraded and require a server restart.


All watchdogs, including all Activity Monitors watchdogs, must be successfully upgraded before upgrading the other services. The user does not need to perform any additional actions.

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.

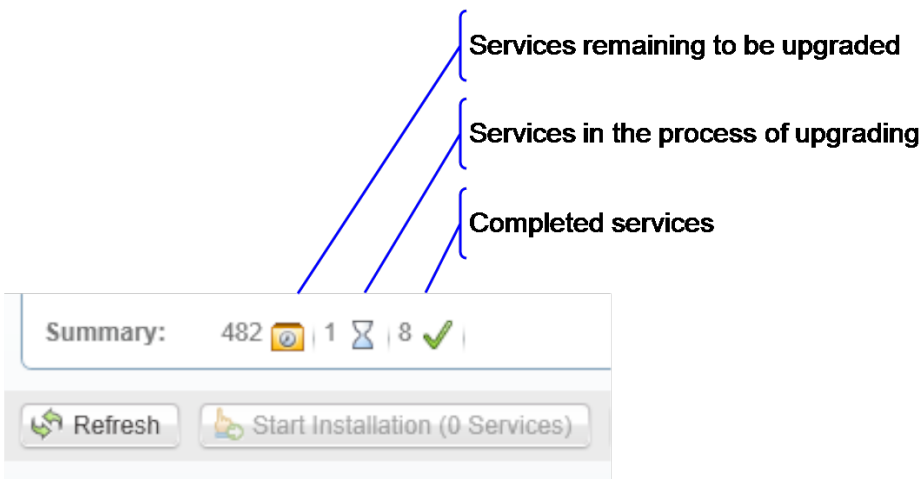
Description: Upgrades File Access Manager to v8.2.0.0

Issued At: 04/06/2019 13:58:36 [\(View Release Notes\)](#)

Status: In progress - upgrading database

Summary: 491 




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

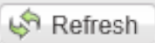
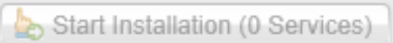


Services remaining to be upgraded

Services in the process of upgrading

Completed services

Summary: 482  | 1  | 8 

 Refresh  Start Installation (0 Services)


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/DB	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](#).

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

Description:	Upgrades File Access Manager to v8.2.0.0
Status:	Finished
Summary:	473 

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:

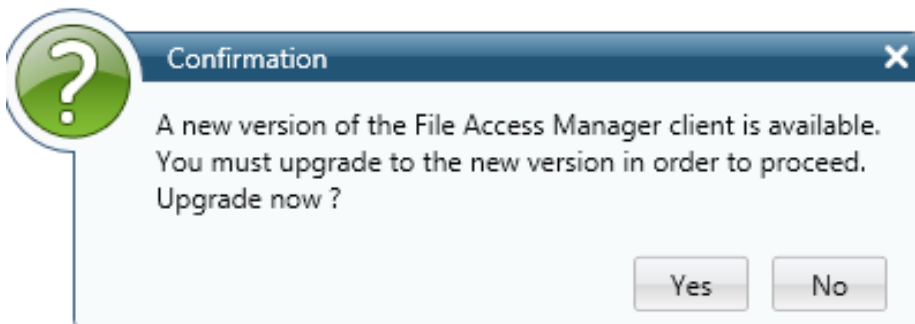
1. Copy "ServerInstaller.msi" from the "v8.2 Full Installers" folder to the server.
2. Run "ServerInstaller.msi".
3. Follow the instructions on the screen to complete the upgrade process.

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.

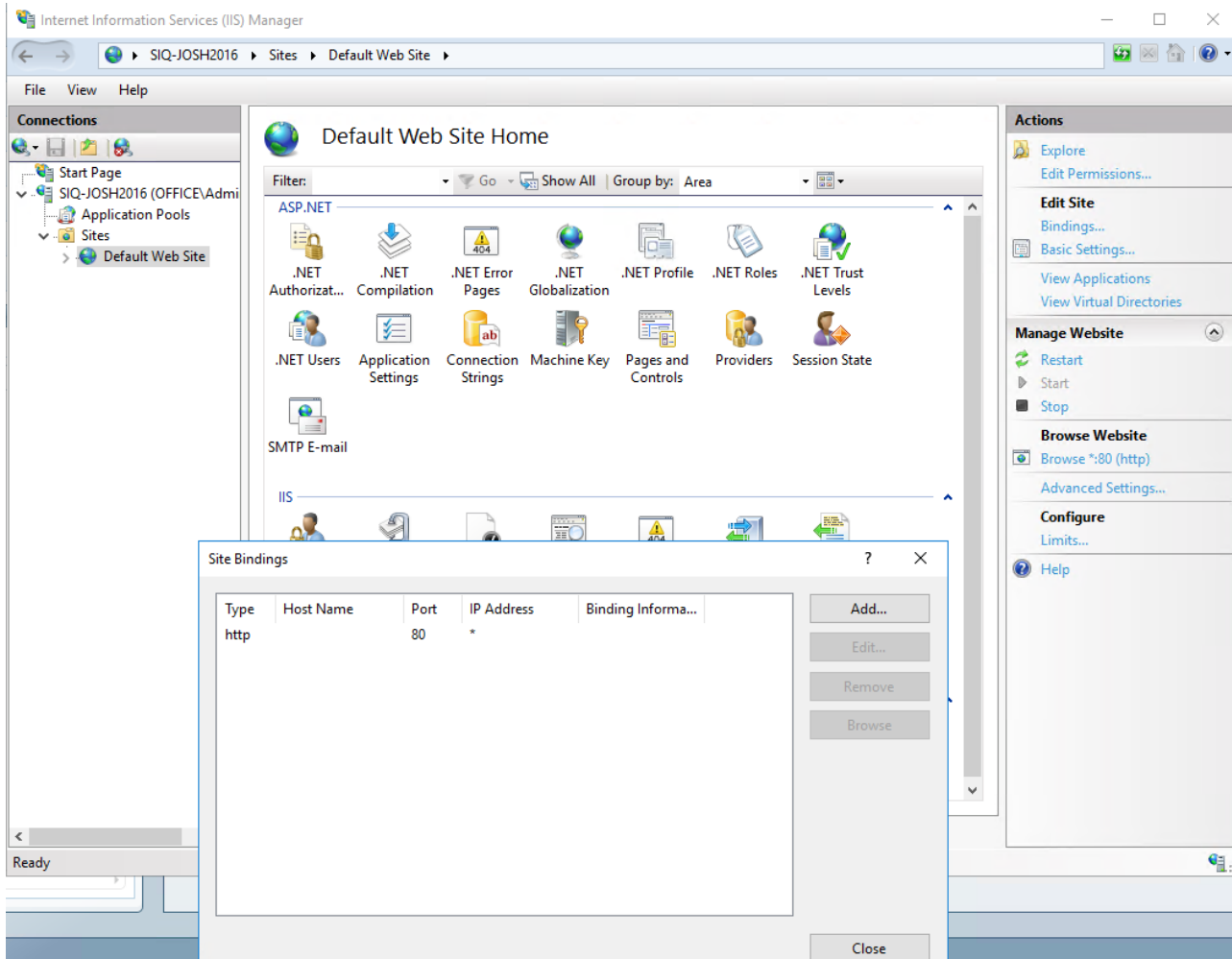
The versions of the File Access Manager components should be listed as "8.2.0.0".

Updating the IIS Binding Port

If you set up IIS on a port other than the default port (80), you will have to manually remove the port 80 binding from the Default Web Site and create a binding to the desired custom port.

On the Windows Administrative tools, open the IIS manager. Select the Default Web Site.

Open the Bindings menu to delete and add site binding protocols and ports.



Updating Data Classification Verification Algorithms

Verification algorithm assemblies written before version 8.2 (in .NET Framework 4.5) must be removed, and re-written to target .NET Standard 2.1, or .NET Core up to 3.1. These algorithms should then be uploaded into the Data Classification page in File Access Manager again.

When upgrading, a change in behavior will occur on the Permission Forensics page. Any filters previously created will have the operator and value deleted during the upgrade. These filters have to be rewritten after the upgrade with one of the valid values.

O365 Application Access Tokens

The File Access Manager 8.2 release included some updates to the way connections are made to Microsoft O365 Applications, for better performance and security.

For more information about these changes, please refer to the File Access Manager 8.2 Release Notes, and the individual deployment guides for AzureAD, OneDrive, SharePoint Online and Exchange Online.

To avoid any issue with connectivity to the Azure AD Identity Collector, please update the connection details by adjusting the configuration settings through the Identity Collector Configuration Wizard in the Administrative Client, to acquire new Access Tokens.

To avoid any issue with connectivity to these endpoints, please update the connection details for these O365 Applications by adjusting the configuration settings through the Application Configuration Wizard - to acquire new tokens.

The Application Configuration Wizard has migrated to the Business Website and is now available under the **Admin > Applications** menu.

Detailed instructions regarding additional prep work required specifically for the Exchange Online application are detailed below.

Configuring Exchange Online to Support Version 8.2

File Access Manager now offers full support of standard OAuth 2.0 Authentication for the Exchange Online connector. The new authorization sequence will use the client credentials workflow in which the user creates and configures an Azure Enterprise Application. When making Exchange Online API calls, Microsoft will enforce that the application is authorized to perform the action.

Configured user accounts are no longer necessary.

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

- The Exchange Online Connector now uses only fully modern authentication methods, and does not require Legacy Authentication methods be enabled, tenant-wide, or otherwise.
- The Exchange Online Connector now uses a designated Azure Application to authenticate against. This authentication will happen on-demand automatically when making API calls.
- Access tokens are no longer stored and renewed. We only store the Azure application ID and the certificate which is used for authentication to generate access tokens.

After performing the upgrade to File Access Manager v8.2, the following additional steps will be required for any existing Exchange Online applications.

This will not recreate the application, and current Exchange Online information will remain intact.

1. Create and configure a new Azure Application for Exchange Online. See [Creating an Azure Application for Exchange Online](#).

Make sure you have access to Microsoft Azure

2. Edit the Exchange Online application in the File Access Manager website and
 - Fill in the application ID
 - Upload the certificate associated with the new Azure application

- Set the certificate password.
- Save the changes

Creating an Azure Application for Exchange Online

A new Azure application must be created and configured to support the File Access Manager Exchange Online functionality.

This configuration can be performed either by running the automated powershell script supplied with the SailPoint distribution pack, or by creating and configuring the application through the Azure portal.

Creating and Configuring the Application Automatically

There is a powershell script named **CreateExchangeOnlineApp.ps1** provided in the **Collectors.zip** under the extracted scripts sub-folder. This script will perform all the Azure application creation and configuration steps required for Exchange Online.

To run this script the Azure AD powershell module must be installed.

```
Install-Module -Name AzureAD
```

Before running the script open the file in a text editor to review the default parameters. The parameters can be edited in the file or passed as parameters when running the script.

To run the script with the default parameters:

```
.\CreateExchangeOnlineApp.ps1
```

To run the script while overriding some of the default parameters:

```
.\CreateExchangeOnlineApp.ps1 -AppName "Exchange Online FAM App" -DirectoryRole "Exchange Administrator" -CertDnsName "contoso.com" -CertYearsValid 15
```

When prompted, log in with administrator credentials to create and configure Azure applications. The last step of the script will launch a URL to grant admin consent for the Application. After granting consent the page will redirect to a missing localhost URL. This can be ignored.

If you experience an **access denied** error or other error in the web browser when granting admin consent, this might be a timing issue. This can be resolved by either manually granting admin consent through the Azure portal (see section [Grant admin consent manually](#)), or by copying and pasting the consent URL (the last line of output from the script output that contains text “adminconsent”) into your browser.

The following output should be gathered or noted when running the script. This information will be used to configure the Exchange Online application in File Access Manager.

1. The App ID value in the console output.
2. The created certificate file <AppName>.pfx located in your working directory.
3. The certificate password that was entered when prompted.

Creating and Configuring the Application Manually

The following steps will create and configure an Azure application for Exchange Online authentication through the Azure portal.

These steps are adapted from the following online Microsoft documentation:

<https://docs.microsoft.com/en-us/powershell/exchange/app-only-auth-powershell-v2?view=exchange-ps#set-up-app-only-authentication>

Step 1: Register the Application in Azure AD

1. Open the Azure AD portal at <https://portal.azure.com/>
2. Under **Manage Azure Active Directory**, click **View**.
3. On the **Overview** page that opens, under **Manage**, select **App registrations**.
4. On the **App registrations** page that opens, click **New registration**.
5. On the Register an application page that opens, configure the following settings:

Name

Enter something descriptive. For example, Exchange Online FAM App

Supported account types

Verify that Accounts in this organizational directory only (<YourOrganizationName> only - Single tenant) is selected.

Redirect URI (optional)

Leave empty.

6. When you're finished, click **Register**.

Leave the app page open. You'll use it in the next step.

Step 2: Assign API Permissions to the Application

1. On the app page under Manage, select Manifest.
2. On the Manifest page that opens, find the *requiredResourceAccess* entry (on or about line 44).
3. Modify the **resourceAppId**, **resourceAccess**, **id**, and **type** values as shown below:

```
"requiredResourceAccess": [  
  {
```

```
"resourceAppId": "00000002-0000-0ff1-ce00-000000000000",
"resourceAccess": [
  {
    "id": "dc50a0fb-09a3-484d-be87-e023b12c6440",
    "type": "Role"
  }
],
}
```

4. Click **Save**.
5. On the **Manifest** page, under **Manage**, select **API permissions**.
6. **Grant admin consent manually**

On the **API permissions** page that opens, do the following:

API / Permissions name

Verify the value **Exchange.ManageAsApp** is shown.

Status

The initial value is Not granted for <Organization>.

Select **Grant admin consent for <Organization>**, read the confirmation dialog that opens.

Click **Yes**.

The Status value should now be **Granted for <Organization>**.

7. Close the current API permissions page (not the browser tab) to return to the App registrations page. You'll use it in an upcoming step.

Step 3: Generate a self-signed certificate

Create a self-signed x.509 certificate using the following powershell commands.

Edit parameters such as **DnsName**, **Certificate expiration**, and **password** as appropriate.

Create certificate

```
$mycert = New-SelfSignedCertificate -DnsName "contoso.org" -CertStoreLocation "cert:\LocalMachine\My" -
NotAfter (Get-Date).AddYears(15) -KeySpec KeyExchange
```

Export certificate to .pfx file

```
$mycert | Export-PfxCertificate -FilePath mycert.pfx -Password $(ConvertTo-SecureString -String "P@ss-
w0Rd1234" -AsPlainText -Force)
```

Export certificate to .cer file

```
$mycert | Export-Certificate -FilePath mycert.cer
```

Step 4: Attach the Certificate to the Azure AD Application

After you register the certificate with your application, you can use the private key (.pfx file) for authentication.

1. On the Apps registration page from the end of Step 2, select your application.

If you need to get back to Apps registration page

- a. Open the Azure AD portal at <https://portal.azure.com/>
 - b. Under **Manage Azure Active Directory**, click **View**.
 - c. On the **Overview** page that opens, under **Manage**, select **App registrations**.
2. On the application page that opens, under **Manage**, select **Certificates & secrets**.
 3. Click **Upload Certificate**.
 4. Browse to the self-signed certificate (.cer file) that you created in Step 3.
 5. Click **Add**.

The certificate is now shown in the Certificates section.

6. Close the current Certificates & secrets page, and then the App registrations page to return to the main <https://portal.azure.com/> page. You'll use it in the next step.

Step 5: Assign Azure AD role to the application

The following admin roles are available. Each of these roles has the necessary permissions for File Access Manager functionality. Choose a role and assign the new Azure Application to it to complete the configuration.

- Global administrator
 - Compliance administrator
 - Exchange administrator
1. Open the Azure AD portal at <https://portal.azure.com/>
 2. Under **Manage Azure Active Directory**, click **View**.
 3. On the **Overview** page that opens, under **Manage**, select **Roles and administrators**.
 4. Find and select one of the supported roles by clicking on the name of the role (not the check box) in the results.
 5. On the Assignments page that opens, click **Add assignments**.
 6. In the **Add assignments** flyout that opens, find and select the app that you created in Step 1.
 7. Click **Add**.
 8. Back on the Assignments page, verify that the app has been assigned to the role.

Troubleshooting

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

Watchdog Failed During the Upgrade

Problem: The Watchdog service(s) failed during the upgrade process.

The screenshot shows a software upgrade progress window. At the top, it displays:

- Description: Upgrades File Access Manager to v8.2.0.0
- Status: In progress - upgrading services
- Summary: 51 [eye icon] 446 [check icon] | 3 [warning icon]

 Below this are several action buttons: Refresh, Start Installation (0 Services), Save Log File, Retry Installation, Resume Database Upgrade, and Back.

 The main part of the window is a table with the following columns: #, Upgrade?, Service, Server, Type, and Status.

#	Upgrade?	Service	Server	Type	Status
1	<input type="checkbox"/>	File Access Manager WatchDog - siq-mtz-lsh:	siq-mtz-lshay3	Infrastructure	Failed
2	<input type="checkbox"/>	File Access Manager WatchDog - siq-mtz-lsh:	siq-mtz-lshay4	Infrastructure	Failed
3	<input type="checkbox"/>	File Access Manager WatchDog - siq-mtz-lsh:	siq-mtz-lshay2	Infrastructure	Failed
4	<input checked="" type="checkbox"/>	File Access Manager Reporting Service	siq-mtz-lshay3	Infrastructure	Pending

Suggested solution:

1. Check the log file **SelfUpgradeLegacy**

`%SAILPOINT_HOME_LOGS%\SelfUpgradeLegacy`

(Usually Program Files\SailPoint\Loggs)

Message: "Cannot upgrade Watchdog because .NET Core is not installed"

2. Make sure .NET is installed correctly in the server and try again.
3. After trying again, the Watchdog service might remain in Pending status for about 10 minutes before trying the upgrade again. If you wish to not wait, you may restart the Watchdog service manually.

“Access Denied” Message While Logging Into the Business Website

Problem: You encounter an “Access Denied” error message while logging in to the Business Website after the upgrade.

Suggested solutions:

.NET Core Installation Issue

Try to repair the .NET core, and try again.

There is no need to restart after the repair process.

Website Folder Structure Issues

1. Verify the structure website folder:
 - a. Navigate to the wwwroot folder on the server hosting the Website at C:\inetpub\wwwroot.
 - b. Verify that the following folders appear in the wwwroot folder:
 - cdn
 - FAM
 - FAMAPI
 - SecurtyIQBiz
 - SiqApi

If these folders are in the wwwroot folder, but there are still problems with the Business Website, contact SailPoint Customer Support.

2. If these folders are not in the wwwroot folder, perform the following steps:
 - a. Open the Internet Information Service (IIS) manager
`Server Manager > Tools > Internet Information Service (IIS) manager.`
 - b. Select the Application Pools node.
 - c. Verify that the FamV1_ApplicationPool, FamV2_ApplicationPool, ScimApi_ApplicationPool, SecurityIQ_ApplicationPool, SiqApi_ApplicationPool and SiqCdn_ApplicationPool are missing from the Application Pools node.
 - d. Create all missing application pools, with the following parameters:
 - .Net CLR Version**
.Net CLR Version v4.0.30319
 - Managed pipeline mode**
Integrated
 - e. Check the “**Start application pool immediately**” checkbox.
 - f. For each application pool, navigate to Advanced Settings
`Right-click > Advanced Settings`
 - g. Under Process Model, set the “Identity” parameter to LocalSystem.
 - h. Under Recycling set the “Regular Time Interval (minutes)” to 720.
 - i. From the Site panel (on the left), navigate to fam->v1, and click on it.
 - j. Click “**Basic Settings**” on the right. If this option is not available, right click identityiqfam->v1, (on the left) and select “**Convert to Application**”.

- k. On the newly opened screen
 - Click **Select**
 - Select the FamV1_ApplicationPool you created earlier
 - Click **OK** twice.
 - l. Double click "**Authentication**".
 - m. Enable "Windows Authentication" and disable all other authentication methods.
3. Repeat the steps under #2 for the following :
- IdentityIQFAM->v2
 - SiqApi
 - SecurityIQBiz
 - FAMAPI sites and application pools.
4. Reset the IIS using the iisreset command.

Suspended due to Database Upgrade Error

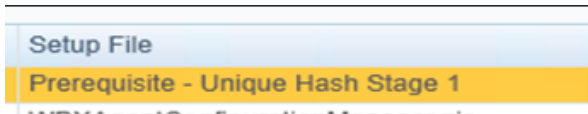
Stage

Prerequisite - Unique Hash Stage 1

Error Information

Suspended due to Database upgrade error

"Prerequisite - Unique Hash Stage 1" is in status **failed**



Suggested solution

Make sure you have deployed E-Fix SIQETN-2945 (Isilon Unique Hash Revert Fix for 8.1 SP3) . The scripts for this fix can be found in the upgrade folder.

Upgrade Checklist

Use the following checklist to verify all steps were completed in the upgrade of File Access Manager.

Category	Description	Comments
Pre-Upgrade	Current File Access Manager version is at least 8.1 Service Pack 3	Only File Access Manager versions 8.1 SP3 & 8.1 SP4 can be upgraded to 8.2
Pre-Upgrade	Microsoft .NET version	This is required on servers running FAM services.

Category	Description	Comments
	4.7.2 is installed	
Pre-Upgrade	"New Unique Path Hash Calculation" task is completed successfully in the customer environment	
Pre-Upgrade	Mandatory pre-requisite (SIQETN-2945) is applied.	SIQETN-2945 Documentation
Pre-Upgrade	.NET Core 3.1.X is installed on all servers running File Access Manager services (Core servers, collectors, BAMS including WFS)	https://dotnet.microsoft.com/download/dotnet/3.1
Pre-Upgrade	Verify Unique path hash calculation completion. Refer to the link in the comments section. This verification script should return one of the SUCCESS messages.	FAM KB Article: 8.2 Prerequisite Database Scripts
Pre-Upgrade	HTTP/2 communication. Ensure that all the servers on which File Access Manager services are running support HTTP/2 protocol.	By default most of the servers hosting FAM services would support this.
Pre-Upgrade	Load Balancer for File Access Manager services. If the File Access Manager environment has a load balancer in front of ACM/EM/UI services, ensure that the load balancer supports HTTP/2.	If HTTP/2 is not enabled, the services tend to drop the connection to HTTP/1.1 which will cause communication problems.
Upgrade	Load the 8.2 upgrade package and start the install.	Refer to the upgrade guide for expected behavior.
Upgrade	Order in which the upgradable items are executed: Database scripts WatchDog services	The 8.2 Upgrade halts upgrading other services until all the WatchDog services are upgraded. Make sure all the WatchDog services are on version 8.2.0.0. You can run the below query to

Category	Description	Comments
	Core services Collectors & BAMs	<p>get the list of WD services and their current versions. If there are any rogue servers on which the WatchDog service is present, get rid off them.</p> <pre>SELECT a.version,* from [whiteops].[installed_service] a inner join [whiteops].[install_service] b on a.install_service_id = b.id where b.static_group_enum_id = 100 and installed_server_id is not null</pre>
Upgrade	<p>If any of the services in the Upgrades & Patches screen seems to be halted for a long time, do the following.</p> <ol style="list-style-type: none"> 1. WatchDog service is on version 8.2.0.0 2. WatchDog service is running. 3. WatchDog service doesn't have any communication errors with the ACM service. 4. If need be, restart the WatchDog service. This should pick the upgrade for other services running on the server. 	

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.

Connection Errors Following an Upgrade

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

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

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

```
Unable to connect to test.domain.com with user_name Grpc.Core.RpcException: Status(StatusCode=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.