AVEVA™ PI Audit Reporter

User & Administration Guide (UAG)

1.0

April 2026

Contents

CHAPTER 1

Introduction

Purpose

This document serves as the User and Administration Guide (UAG) for the AVEVA PI Audit Reporter application, developed by Cognizant Life Sciences Manufacturing Group (LSMG).

Intended Purpose

This guide is intended for system administrators and users responsible for configuring and managing the AVEVA PI Audit Reporter application. It assumes that readers are already familiar with the application's basic functionality, as well as several topics related to computer networking.

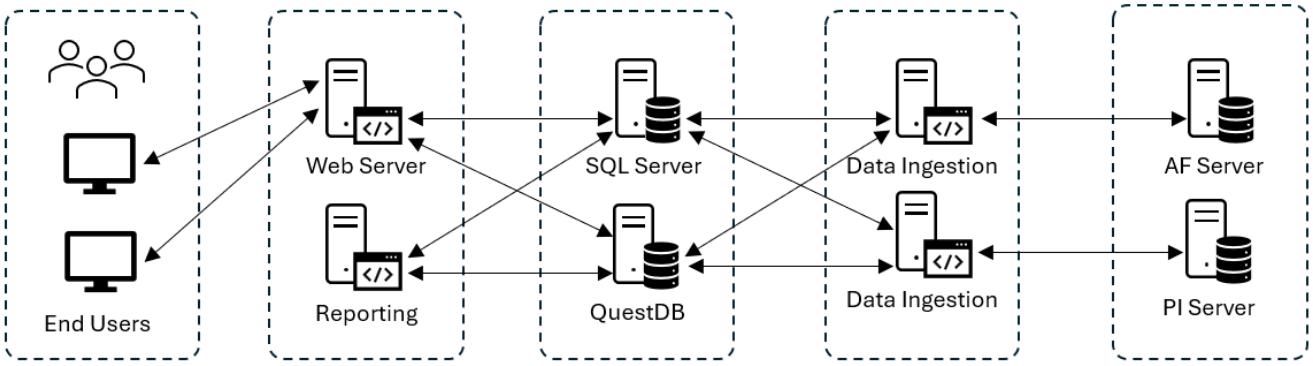
AVEVA™ PI Audit Reporter Scope

This manual offers a comprehensive overview of the AVEVA PI Audit Reporter application, to equip system administrators with the knowledge and tools needed to understand, configure and manage the application for effective use and administration.

CHAPTER 2

Architecture

The system architecture is based on a microservices model, which inherently supports greater scalability and flexibility. In this design, the application is composed of multiple loosely coupled, independently deployable services that work together to deliver the overall functionality. This is shown below, which shows how the microservices interact within the overall architecture.



Key features of the AVEVA PI Audit Reporter application

The AVEVA PI Audit Reporter application delivers a robust, scalable, and integration-ready solution with the following core features:

a. Clear search functionality
   - Enables users to filter, locate, and retrieve audit trail records based on defined criteria to improve traceability and efficiency.

b. Comments
   - Supports the addition of comments to audit trail records, allowing users to document the rationale behind changes, ensuring accountability.

c. Out-of-the-box reports
   - Provides preconfigured reports that are ready to use immediately after installation, to require minimal customization. These reports are designed to meet standard compliance requirements and are FDA 21 CFR Part 11 ready.

d. Centralized workspace

- Uses distributed data ingestion services to connect multiple AVEVA PI Systems and forward audit trail records to a centralized application. This enables centralized management, while leveraging existing PI Data Historians and Asset Framework servers. Changes and audit events are captured and forwarded in near real-time, enabling immediate visibility into system changes and faster incident response and root cause analysis.

e. Integration-friendly architecture

- Microservices-based architecture is built to easily connect and communicate with other enterprise systems, making it a flexible and scalable solution for organizations with complex IT ecosystems and supporting Information Technology Service Management (ITSM), Change Control, or other change management platforms. This enables faster delivery changes and more comprehensive auditing.

f. Scalable solution

- Engineered to efficiently handle high volumes of data, to support millions of audit trail records without compromise on the performance, distributed architecture, each component (data ingestion, storage, reporting) can be scaled independently (these settings can be found in Chapter 5 – Core Modules), efficient storage management.

CHAPTER 3

Installation Requirements

Recommended Infrastructure

The AVEVA PI Audit Reporter application supports the installation of all components on a single virtual machine (VM), but it is recommended to distribute components across three VMs to ensure optimal performance, scalability, and maintainability; one VM to host data ingestion services, one VM to host the data visualization components and the last one to host the databases used.

Data Ingestion Group

The group of data ingestion components responsible for collecting, processing and storing audit data. It includes the following services:

a. AVEVA PI Audit Reporter PI Data Ingress Service

b. AVEVA PI Audit Reporter AF Data Ingress Service

Data Visualization Group

The group of core modules responsible for accessing processed audit trail records and generating reports for management, compliance, and regulatory purposes. This group includes the following:

a. AVEVA PI Audit Reporter Reporting Service

b. AVEVA PI Audit Reporter Web Application

Databases Group

The group of databases used to store audit data and application-related configuration data as settings. It includes the following databases:

a. Microsoft SQL Server

b. QuestDB

Distributing components across dedicated virtual machines ensures that each group has access to the necessary resources, significantly enhancing the performance, scalability, and stability of the AVEVA PI Audit Reporter Application. The table below outlines the minimum hardware requirements for deploying each component. It is recommended to use a dedicated disk for storing application data. If the application shares the same disk as the operating system, the disk should have a minimum capacity of 256 GB with at least 128 GB of free space available to ensure reliable performance.

For both QuestDB and MS SQL server, it is strongly recommended to use a dedicated hard disk to optimize I/O performance operation and storage.

Component	Hardware Minimum System requirements		
	CPU	RAM	Hard Disc
PI Data Ingress Service	Core 2 Quad Q6600 at 2.4 GHz or AMD Phenom 9850 at 2.5 GHz	*16 GB RAM	*128 GB
AF Data Ingress Service			
Reporting Service			
Web Application			
MS SQL Server			*256 GB
QuestDB			

While we provide a recommended minimum configuration for virtual machines (VM), it is important to understand that actual requirements may vary depending on how specific components are used. In some cases, the user may need to increase the VM capacity or deploy a component on a dedicated VM. This approach enables more accurate monitoring of usage peaks and helps determine resource needs more effectively.

One of the key advantages of microservices architecture is its ability to support gradual and targeted scaling of hardware infrastructure. Rather than scaling an entire monolithic application, the user can allocate resources based on the demands of individual components. This flexibility can lead to improved performance and cost efficiency.

The minimum requirements listed for product installation are based on official supplier documentation. Depending on the usage patterns and storage needs, additional capacity may be necessary. Consult the supplier's official documentation for detailed guidance.

To assist with planning and decision-making, the table below presents sample data ingestion scenarios, including information such as processed intervals, ingestion duration and memory usage.

Scenario #	Processed Interval (days)	Ingestion Duration (seconds)	Validation Duration (seconds)	Audit trail Records Processed	Ingestion Memory Usage (Mb)	Validation Memory Usage (Mb)
01	60.00	33.00	27.00	2125.00	89.16	114.57
02	60.00	36.00	29.00	2128.00	74.30	120.25
03	60.00	37.00	28.00	2160.00	149.96	122.00
04	60.00	38.00	28.00	2157.00	78.07	121.89
05	60.00	39.00	26.00	2084.00	77.36	118.41
06	60.00	35.00	26.00	2124.00	135.86	120.10
07	60.00	35.00	23.00	2080.00	134.04	117.92
08	10.00	13.00	7.00	375.00	58.21	51.11
09	10.00	12.00	6.00	350.00	52.82	50.24

Scenario #	Processed Interval (days)	Ingestion Duration (seconds)	Validation Duration (seconds)	Audit trail Records Processed	Ingestion Memory Usage (Mb)	Validation Memory Usage (Mb)
10	10.00	13.00	7.00	366.00	55.14	19.99
11	10.00	12.00	7.00	358.00	53.11	50.86
12	10.00	14.00	6.00	393.00	55.86	33.52
13	10.00	14.00	9.00	365.00	53.27	40.22
14	10.00	12.00	6.00	339.00	52.53	36.67
15	10.00	13.00	6.00	359.00	40.92	20.00
16	10.00	11.00	5.00	342.00	52.79	35.55
17	10.00	12.00	5.00	353.00	53.12	40.13
-	**Maximum**	**39.00**	**29.00**	**2160.00**	**149.96**	**122.00**
-	**Minimum**	**11.00**	**5.00**	**339.00**	**40.92**	**19.99**
-	**Average**	**22.29**	**14.76**	**1085.76**	**74.50**	**71.38**

Prerequisites

The following are the minimum system requirements for installing the AVEVA PI Audit Reporter components:

a. AVEVA PI Audit Reporter Web Application
   - Internet Information Service (IIS) Version 10 or greater.
   - QuestDB version 9.2.1 or greater.
   - psqlODBC_x64 version 17.00.x or greater.
   - Microsoft SQL Native Client 11.0.x or greater.
   - ASP.NET Core Runtime - 8.0.x or greater.
   - Microsoft .NET Hosting Bundle version v8.0.7 or greater but not greater or equal to 9.0.
   - MS SQL Server version 15 (2019) or greater.

b. AVEVA PI Audit Reporter Reporting Service
   - Microsoft SQL Native Client 11.0 or greater.
   - Microsoft .NET version 8.0.0 or greater.
   - psqlODBC_x64 version 17.00.x or greater.
   - QuestDB version 9.2.1 or greater.

c. AVEVA PI Audit Reporter PI Data Ingress Service
   - QuestDB version 9.2.1 or greater.
   - Microsoft SQL Native Client 11.0 or greater.
   - Microsoft .NET framework version 4.6.2 or greater.

- Microsoft .NET version 8.0.0 or greater.
- AVEVA AF-SDK version 2.10.x.x or greater.
- AVEVA PI-SDK version 1.4.x.x or greater.
- psqlODBC_x64 version 17.00.x or greater.

d. AVEVA PI Audit Reporter AF Data Ingress Service
   - QuestDB version 9.2.1 or greater.
   - Microsoft SQL Native Client 11.0 or greater.
   - Microsoft .NET framework version 4.6.2 or greater.
   - Microsoft .NET version 8.0.0 or greater.
   - AVEVA AF-SDK version 2.10.x.x or greater.
   - AVEVA PI-SDK version 1.4.x.x or greater.
   - psqlODBC_x64 version 17.00.x or greater.

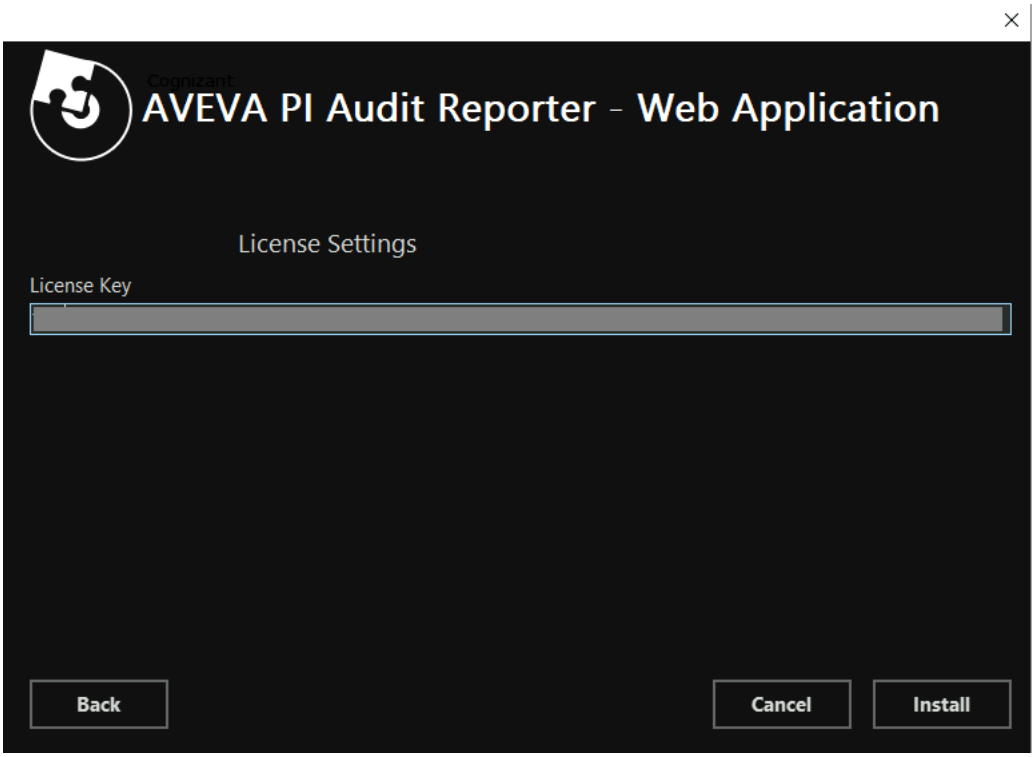
License Configuration

The licensing of PI Audit Reporter application is based on a license key, and it is managed by Cognizant Life Sciences Manufacturing Group (LSMG) using an in-house generation tool.

License key generation process

The license key generation tool uses inputs like license start date and end date, client, site, product and product version etc. The generated license key is in an encrypted form. Information about the license can later be derived using the decryption feature available within the license generation tool. The decrypted license key provides the start date and end date, client, site, product and product version etc.

The license key generated and provided to the users must be informed during the installation of the AVEVA PI Audit Reporter Web Application. This component will be responsible for storing and applying the license key through the other components, like the ingestion and reporting services.



Upon a license renewal request, the Cognizant Life Sciences Manufacturing Group (LSMG) generates a fresh license key and provides the client with an encrypted license key which can be used for the system.

License key generation tool

The license key generation tool is a standalone executable file that runs from a command prompt. And there are two functionalities: Encrypt a new license key based on some parameters and decrypt an existent license key to retrieve licensing information.

Generating a new license key

For license generation it is required to create and inform a set of parameters to be used, as described below:

- Tool file path: The path of the license key generation tool.
- Client Name: The name of the customer that will use the PI Audit Reporter.
- Site Name: The end customer site that will use the PI Audit Reporter.
- Client ID: A unique identifier for that customer.
- Product Name: The full name of the product.
- Version Number: The version of the PI Audit Reporter.
- Start Date: The start date when the license becomes valid (format is YYYY-MM-DD).
- End Date: The end date when the license becomes expired (format is YYYY-MM-DD).

Once ready with the parameters, open the command prompt and run the following command, replacing the parameters:

```
<Tool file path>.exe generatekey client=<Client Name> site=<Site Name> id=<Client ID>
product=<Product Name> version=<Version Number> start=<Start Date> end=<End Date>
```

It generates an encrypted license key to be shared with the customers.

To decrypt an existent license key to retrieve licensing information, run the following parameter replacing the parameter <Encrypted License Key> with the license key previously generated and used by the customers.

```
<Tool file path>.exe getkeyinfo licensekey=<Encrypted License key>
```

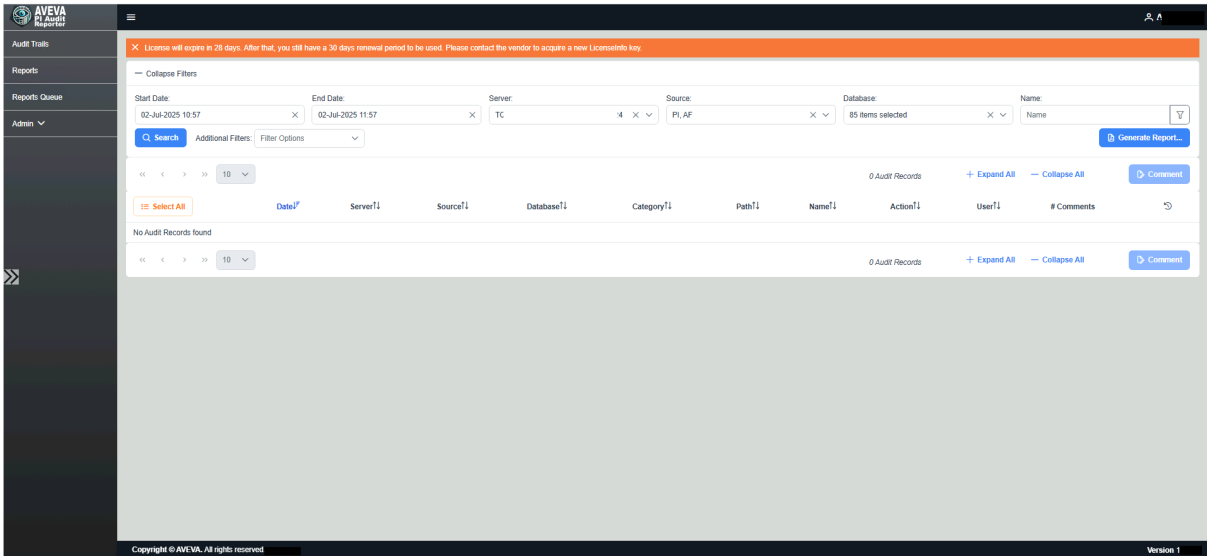
It generates a decrypted license information in plain text to be checked.

License key alert notifications

PI Audit Reporter application contains 3 levels of license notification.

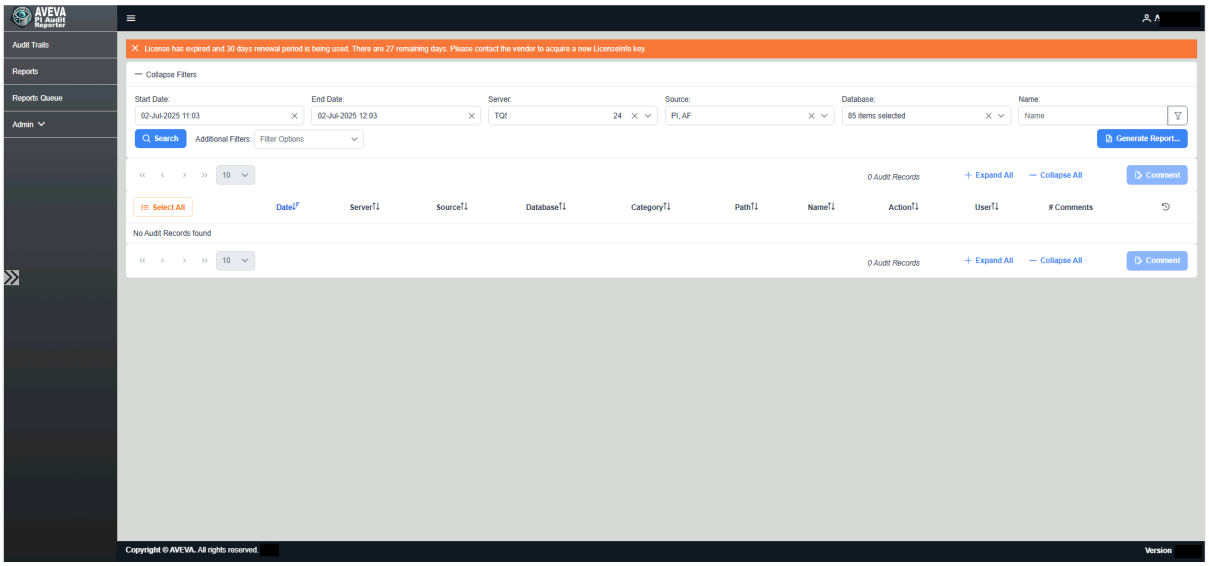
License key expiry advance warning message – Level 1

The first level of license notification happens when the license is about to expire. A license expiry warning message is displayed on the AVEVA PI Audit Reporter User Interface (UI), 30 days before the license expiration date, as illustrated in the screenshot below:



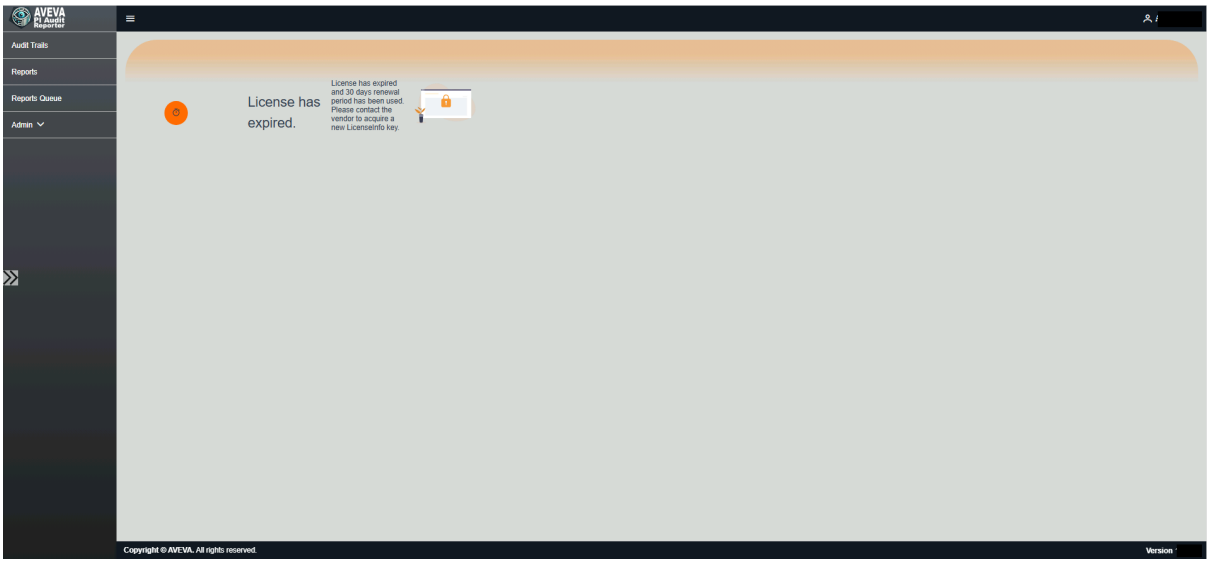
License key renewal alert – Level 2

The second level of license notification happens when the license has expired, but users still have a valid period to use the system meanwhile the license renewal is in progress. A license key renewal alert is displayed on the AVEVA PI Audit Reporter User Interface (UI), starting from the license expiry date and continuing up to 30 days, or until a new license key is activated. Refer to the screenshot below for the license key renewal alert.

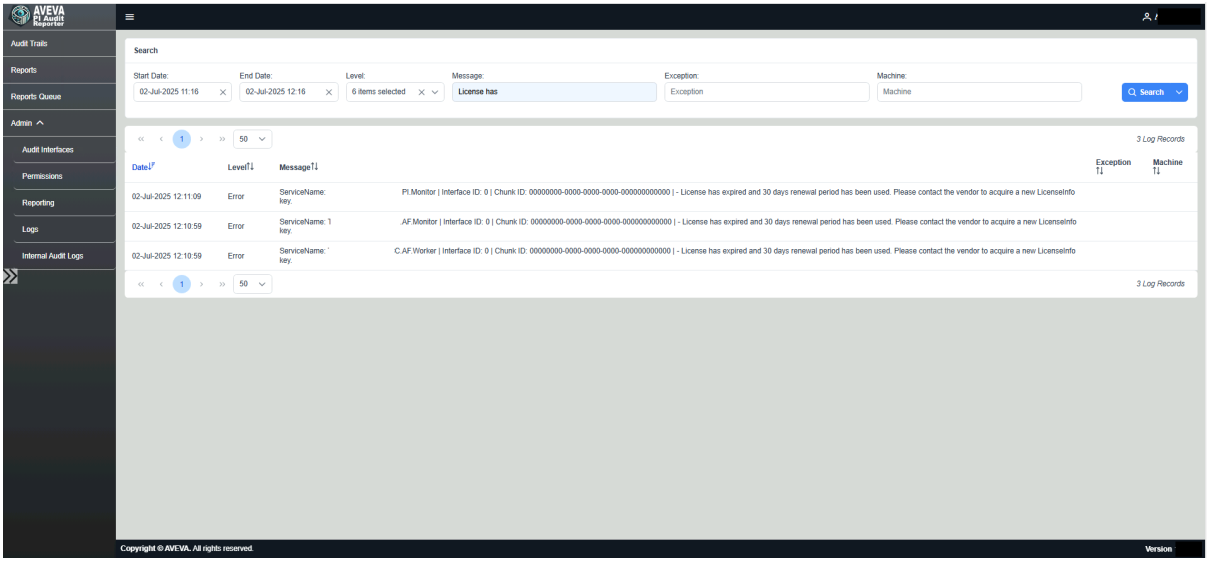


License key expiry message – Level 3

The third and last level of license notification happens when the license has expired. If the license key activation exceeds the 30 days period of license renewal alert, a message is displayed on the AVEVA PI Audit Reporter User Interface (UI), notifying license expiry beyond which certain features of the applications are made unavailable for the user as part of license enforcement. Refer to the screenshot below for the license key expiry message.



Additionally, license messages are captured in the admin-logs section as shown below. Refer to Logs.



Installation

Before the AVEVA PI Audit Reporter application installation, ensure that all required software tools are properly installed and configured in Prerequisites.

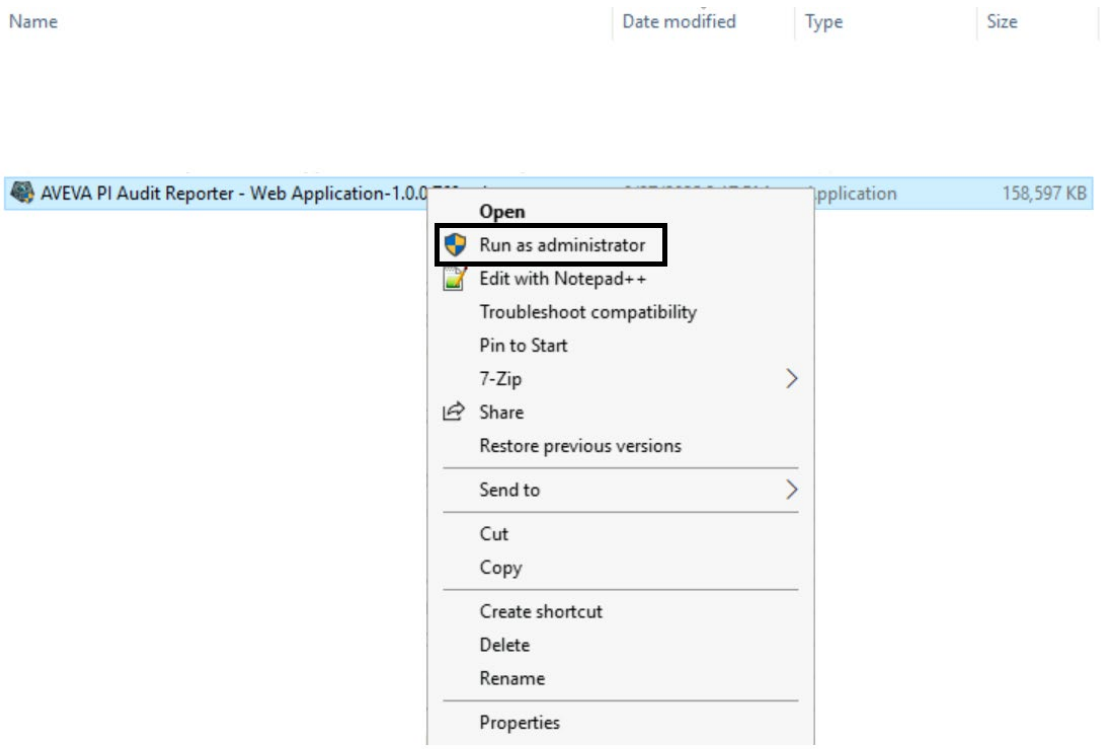
Deploy the AVEVA PI Audit Reporter application using dedicated component installers, which are detailed in the following sections. Each installer corresponds to a specific component.

Begin by installing the AVEVA PI Audit Reporter Web Application before proceeding with the installation of any additional services.

Install AVEVA PI Audit Reporter - Web Application

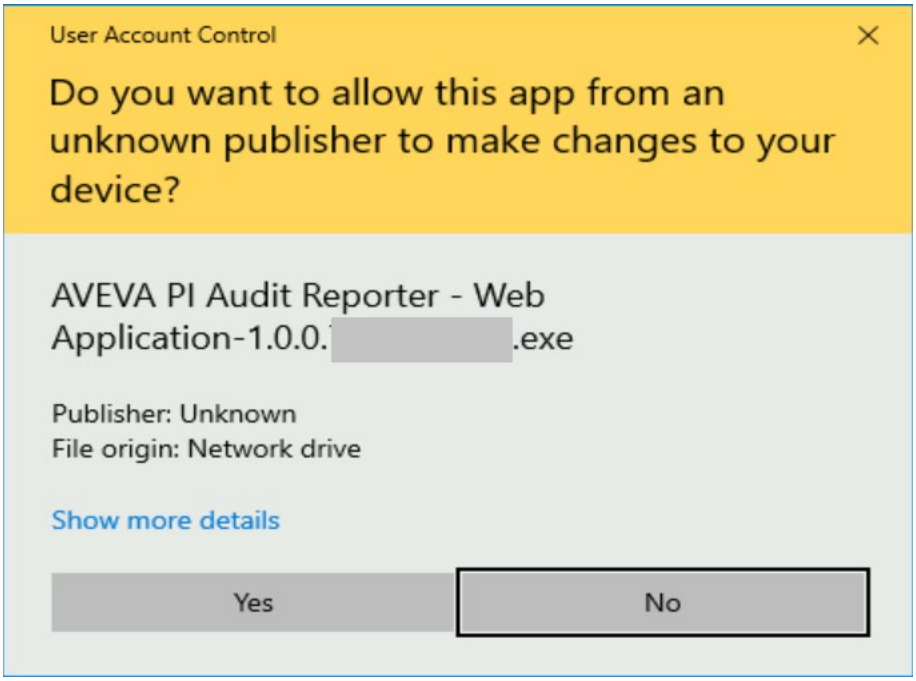
To install the AVEVA PI Audit Reporter - Web Application, follow the steps below:

1. Locate the provided installer file, named: AVEVA PI Audit Reporter - Web Application-1.0.0.xxx_release.exe
2. Right-click the file.
3. Select “Run as administrator (required)” from the context menu as shown below.



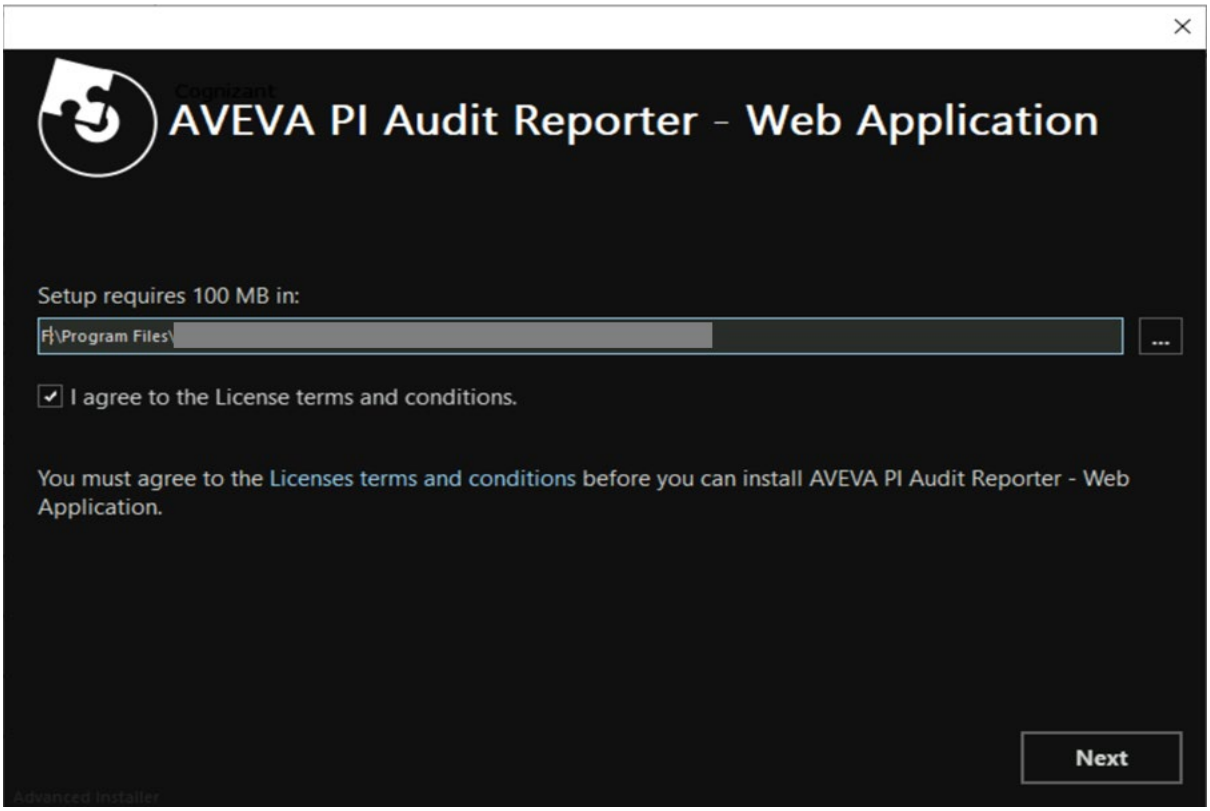
When the installer is launched, a User Account Control (UAC) prompt as shown below will appear with the following message: “Do you want to allow this app from an unknown publisher to make changes to your device?”

4. Select “Yes” to proceed with the installation.



After accepting the User Account Control prompt, the installer proceeds to the File Location Setup screen as shown below.

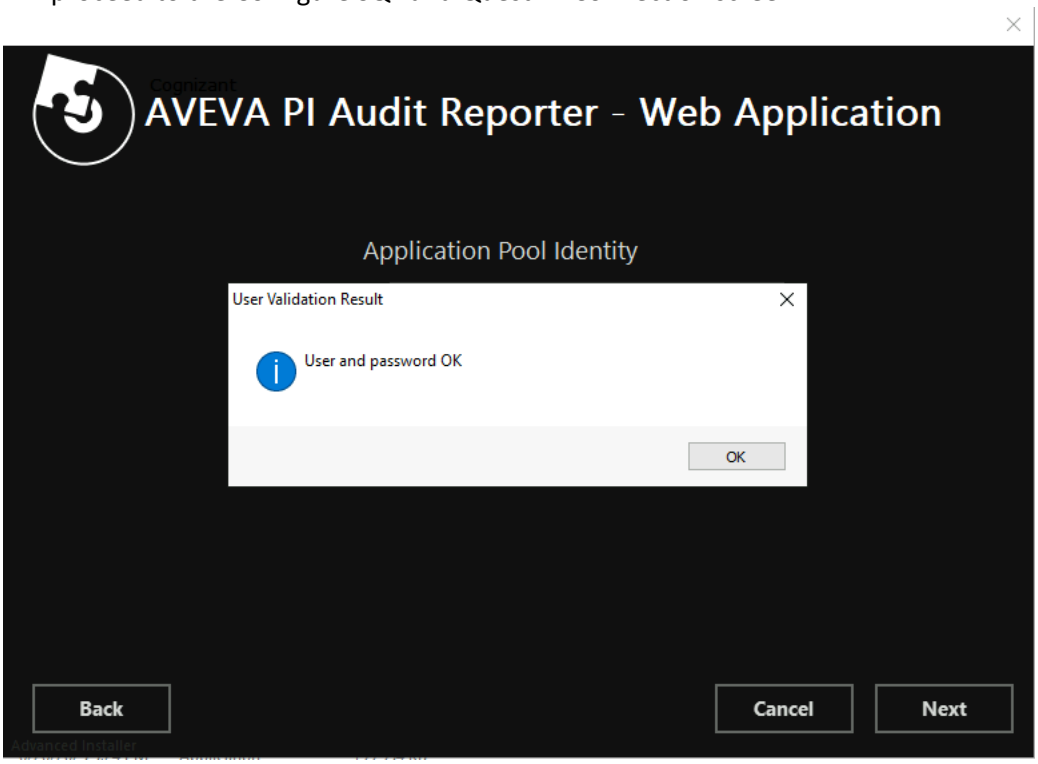
5. Select the ellipsis button ([...]) to open the folder browser.
6. Select the desired directory where the user wants to install the AVEVA PI Audit Reporter - Web Application.
7. Once the installation path is entered, select the check box labeled:
   "I agree to the License terms and conditions."
8. The Next button will become active. Select Next to proceed to the Application Pool Identity screen.



The next screen in the setup process is the "Application Pool Identity" configuration as shown below.

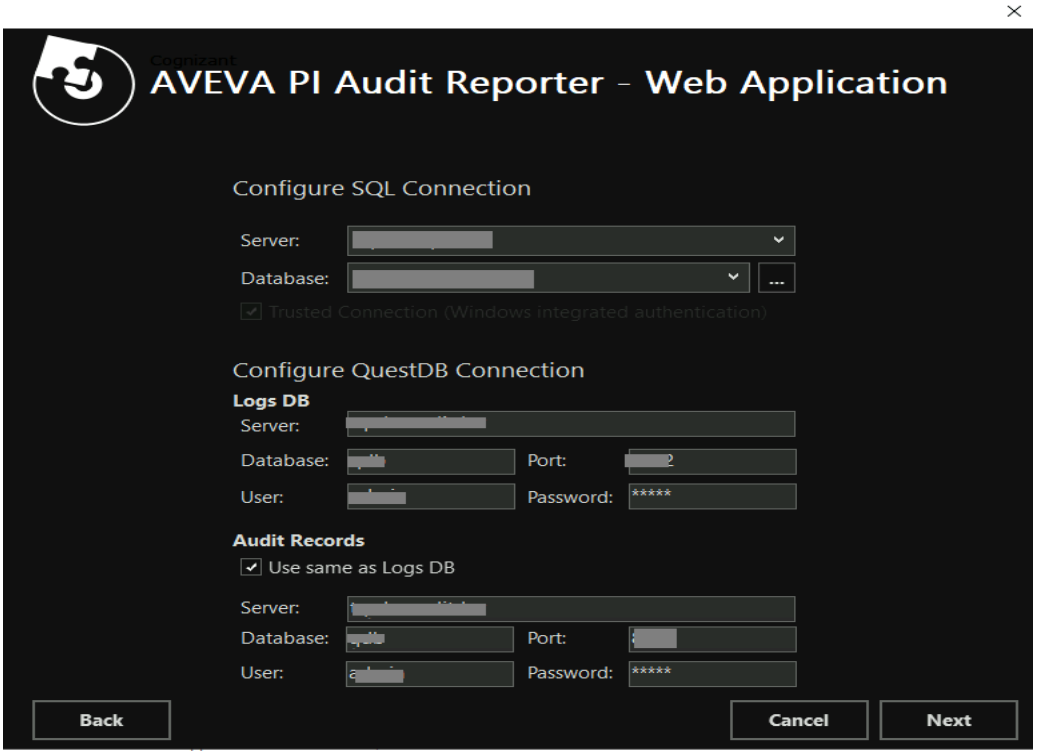
9. Enter the following credentials required for the Audit Trail settings: Username, Domain and Password.
10. After entering the above details, Select the "Validate" button to confirm the configuration.

11. If the credentials are correct, a confirmation popup will appear with the message: "User and password OK".
12. Select "Back" button (in the above figure) to return to the File location setup screen. Select "Next" button to proceed to the Configure SQL and QuestDB Connection screen.



The next screen in the setup process is "Configure SQL and QuestDB Connection".

13. Enter the SQL Server Name and select the appropriate Database options.
14. Proceed to the Configure QuestDB Connection section:
    a. Provide the following details for both the Logs DB and Audit Trail DB: Server, Database, Port, User and Password.
15. If the Audit Trail DB requires the same configuration as the Logs DB, check the box labeled: “Use same as Logs DB”. This user account must have appropriate access to the database to allow record insertion and updates.
16. Once all fields are completed, Select Next to proceed with Setup Administrator screen. Select “Back” button to return to the Application Pool Identity screen.

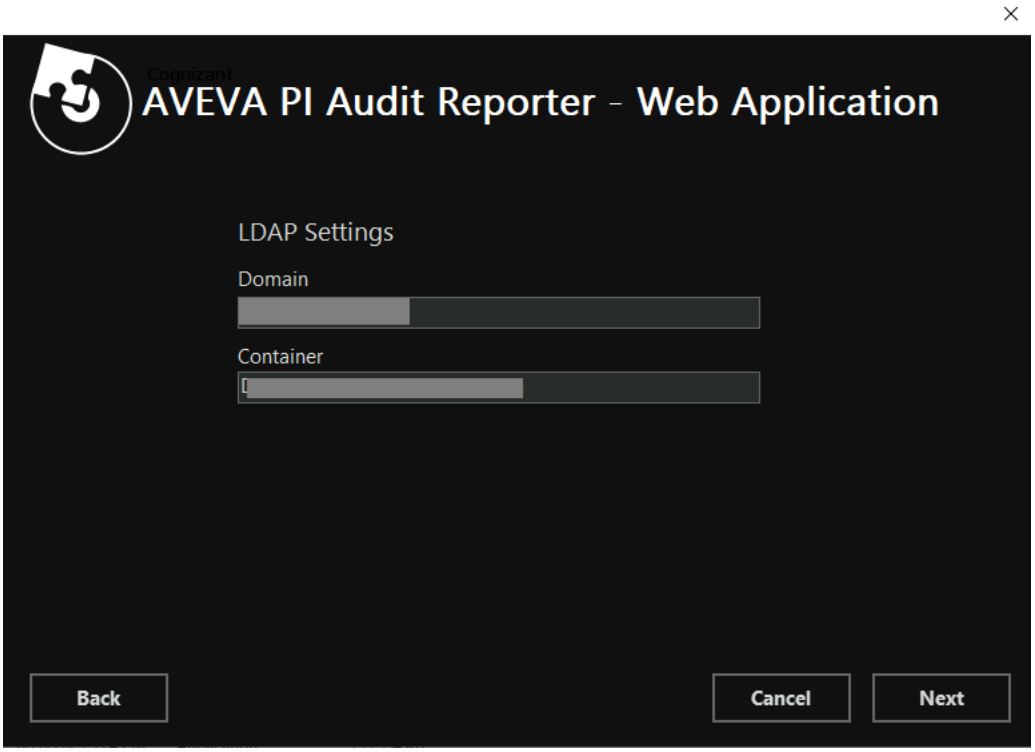


The next screen in the installation process is “Setup Administrator”.

17. Enter the following administrator’s account details: Account Name, First Name, Last Name and Email Address.
18. After filling in all required fields, select “Next” button to proceed with LDAP Settings screen. Select “Back” button to return to the Configure SQL and QuestDB Connection screen.

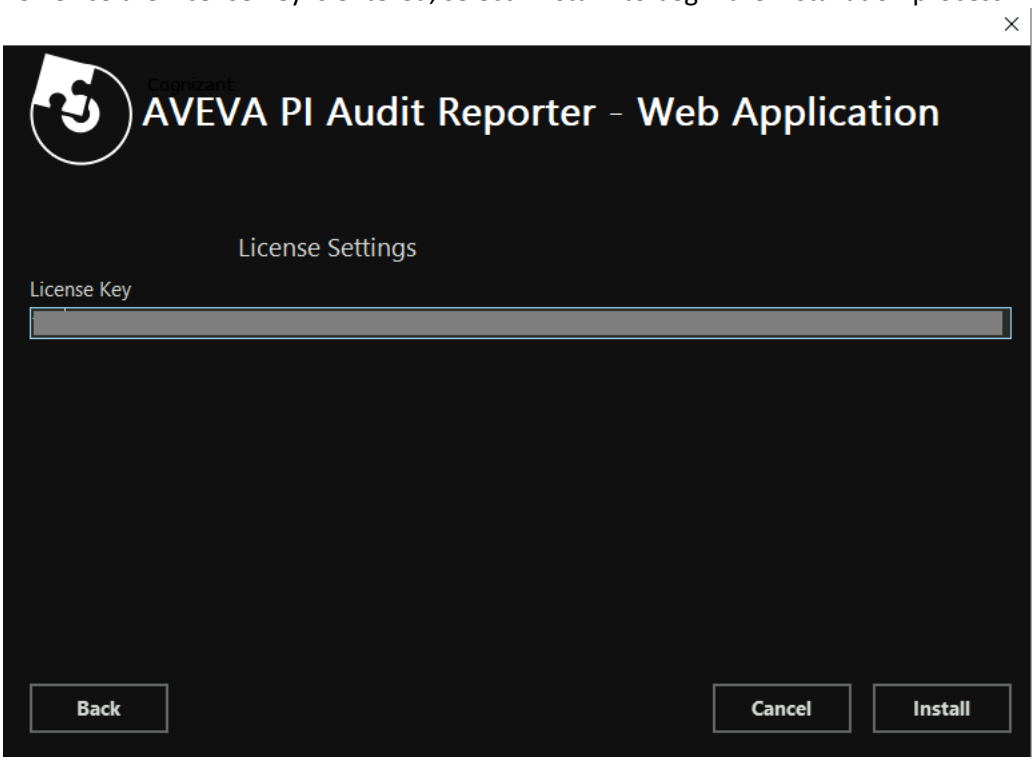
The next screen in the setup process is “LDAP Settings”.

19. Enter the following details: Domain, Container.
20. Once the required fields are completed, Select the “Next” button to proceed with License settings screen. Select “Back” button to return to the Setup Administrator screen.

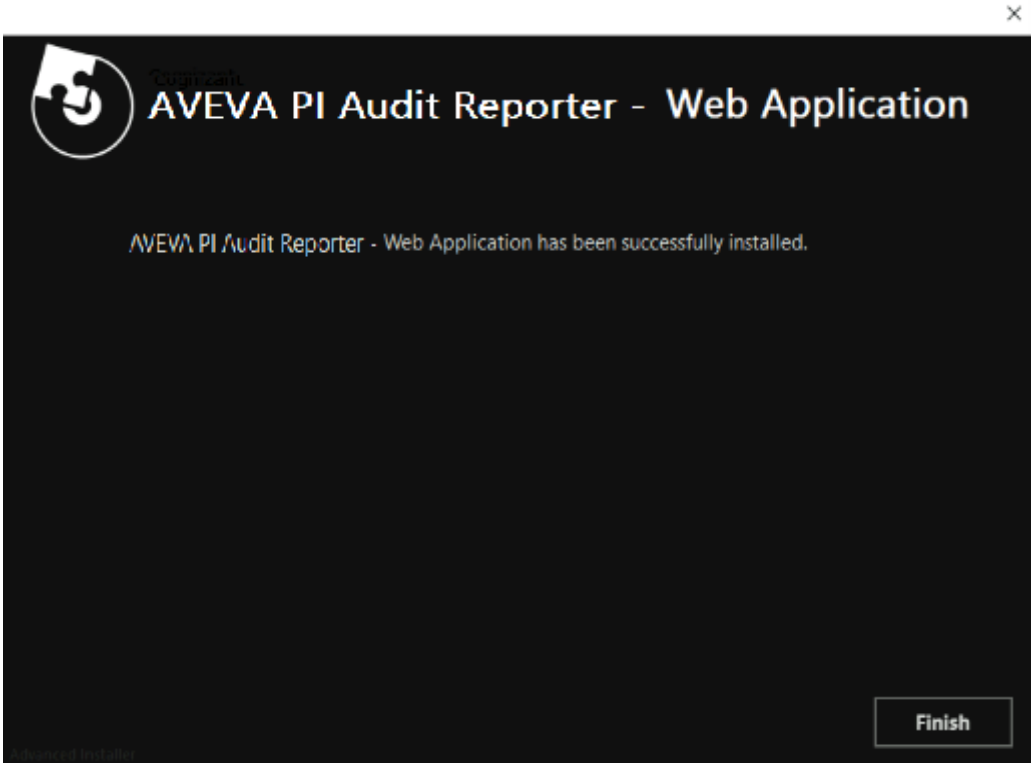


Installer will prompt the user to enter the License Key for the AVEVA PI Audit Reporter application.

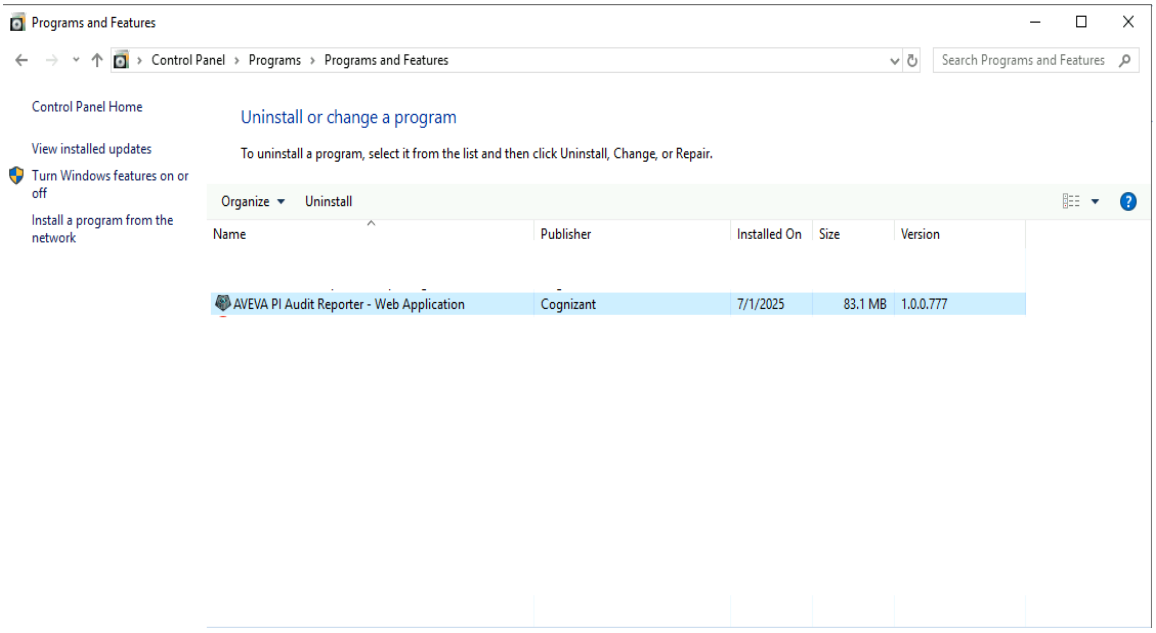
21. Enter the valid License Key in the provided field.
22. If required, the User can Select the “Back” button to return to the LDAP Settings screen and make any changes.
23. Once the License Key is entered, select “Install” to begin the installation process.



Once the installation process is complete, a confirmation message will appear: “AVEVA PI Audit Reporter - Web Application has been successfully installed.” This indicates that the application has been installed correctly and is ready for use. Select the “Finish” button to exit the installer.

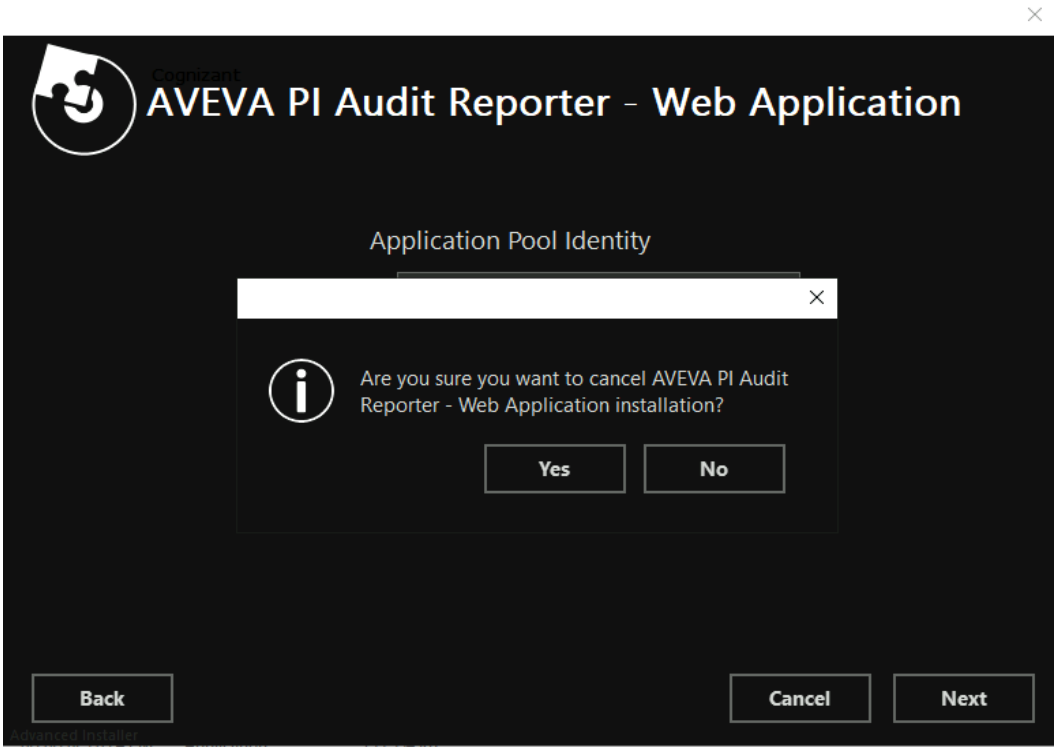


After successful installation, the AVEVA PI Audit Reporter - Web Application will be listed under Programs and Features in the Windows Control Panel.



How to cancel the Installation process

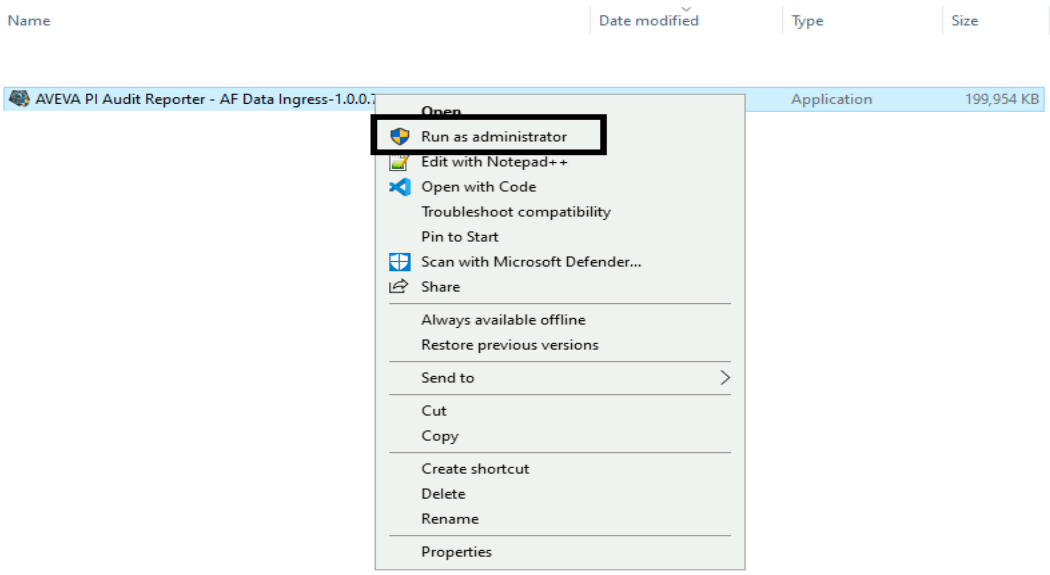
To cancel installation, select the (×) button in the upper-right corner or select cancel button. A confirmation dialog will appear, prompting the user to confirm or abort the cancellation. Refer to the screenshot below to verify the settings.



Install AVEVA PI Audit Reporter - AF Data Ingress

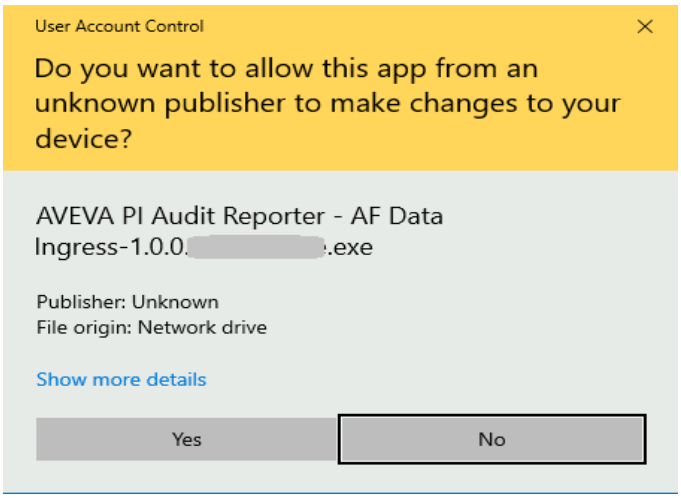
To install the AVEVA PI Audit Reporter - AF Data Ingress service, follow the steps below:

1. Locate the provided installer file, named: AVEVA PI Audit Reporter - AF Data Ingress-1.0.0.xxx_release.exe
2. Right-click the file.
3. Select “Run as administrator (required)” from the context menu as shown below.



When the installer is launched, a User Account Control (UAC) prompt as shown below will appear with the following message: “Do you want to allow this app from an unknown publisher to make changes to your device?”.

4. Select “Yes” to proceed with the installation.



After accepting the User Account Control prompt, the installer proceeds to the File Location Setup screen as shown below.

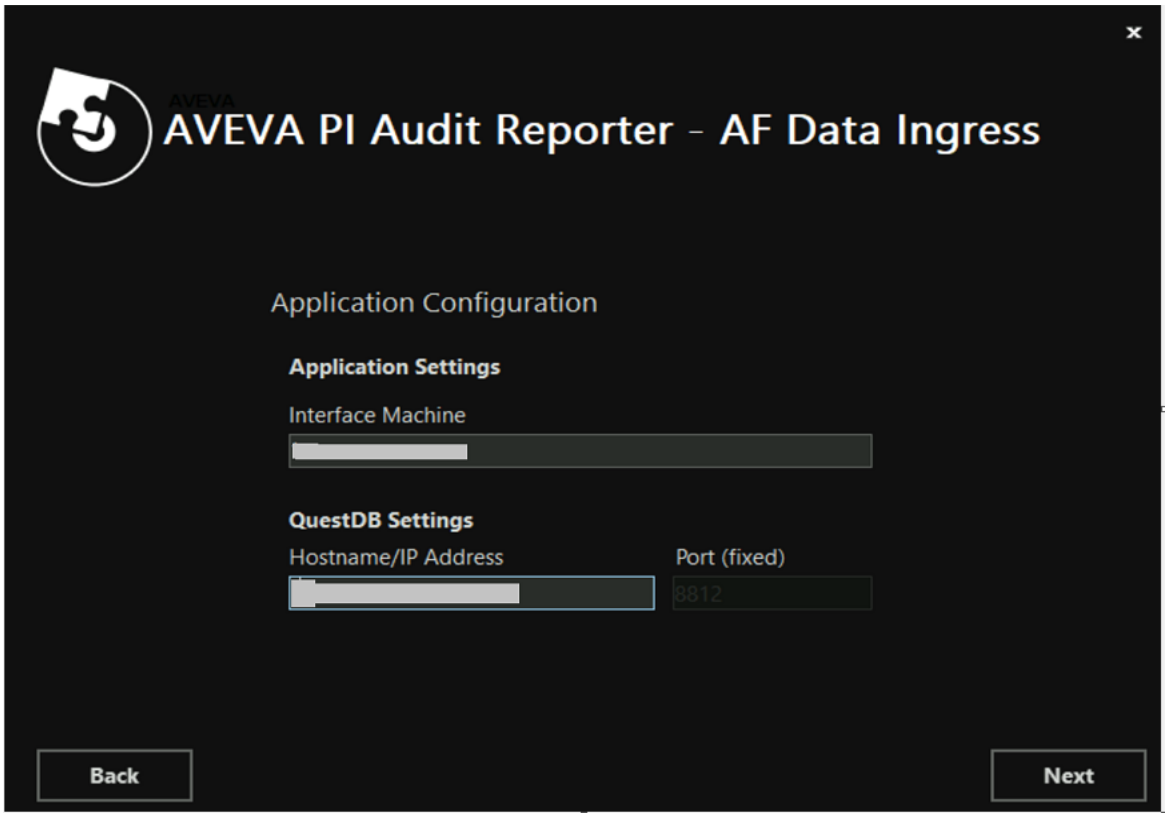
5. Select the ellipsis button ([…]) to open the folder browser.
6. Select the desired directory where the user wants to install the AVEVA PI Audit Reporter - AF Data Ingress.
7. Once the installation path is entered, select the check box labeled:
   “I agree to the License terms and conditions.”
8. Select Next to continue with the installation.

The next screen in the setup process is the “Application Configuration” screen as shown below.

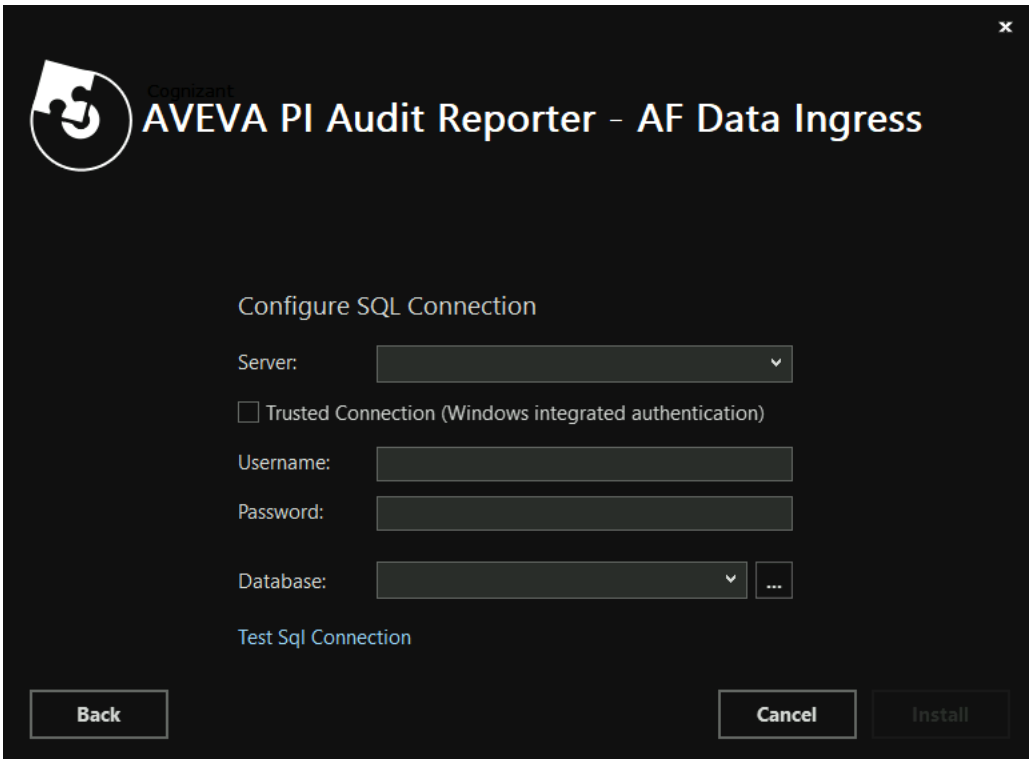
9. Enter the following configuration details: Interface Machine Name, QuestDB Settings (Hostname or IP Address), Port (fixed).

Note: All fields are mandatory. The installation will not proceed unless this information is provided.

10. Select the “Next” button to proceed to the Configure SQL Connection screen.



11. Enter the SQL Server Name and select the appropriate Database options from the Configure SQL Connection window.
12. It is strongly recommended to use a Trusted Connection, as all services will be configured to run under a single service account. This user account must have appropriate access to the database to allow record insertion and updates. If the user prefers to use SQL Authentication (Username/Password), the following configuration is required:
    a. Uncheck the “Trusted Connection” checkbox.
13. Enter the Username and Password.

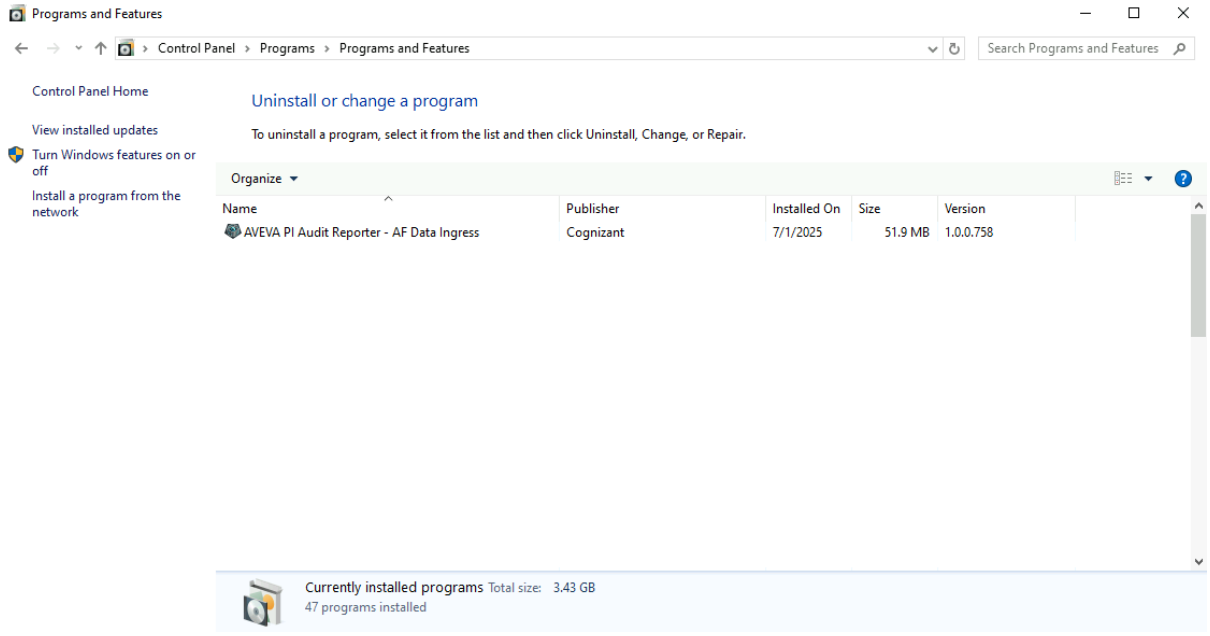


14. When the user selects a Test SQL Connection, a “Connection successful” message displays if the configuration is correct.
15. Once all fields are completed, select the “Install” button to begin the installation process.

Once the installation process is complete, a confirmation message appears: “AVEVA PI Audit Reporter - AF Data Ingress has been successfully installed.” This indicates that the application has been installed correctly and is ready for use.

16. Select Finish to exit the installer.

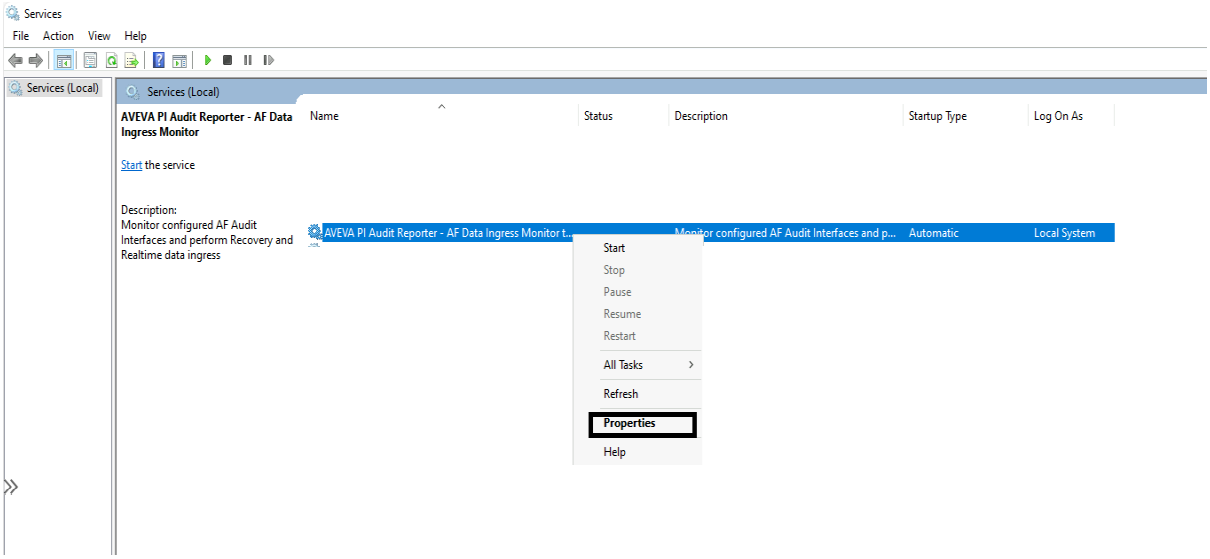
After a successful installation, the AVEVA PI Audit Reporter - AF Data Ingress will be listed under Programs and Features in the Windows Control Panel.



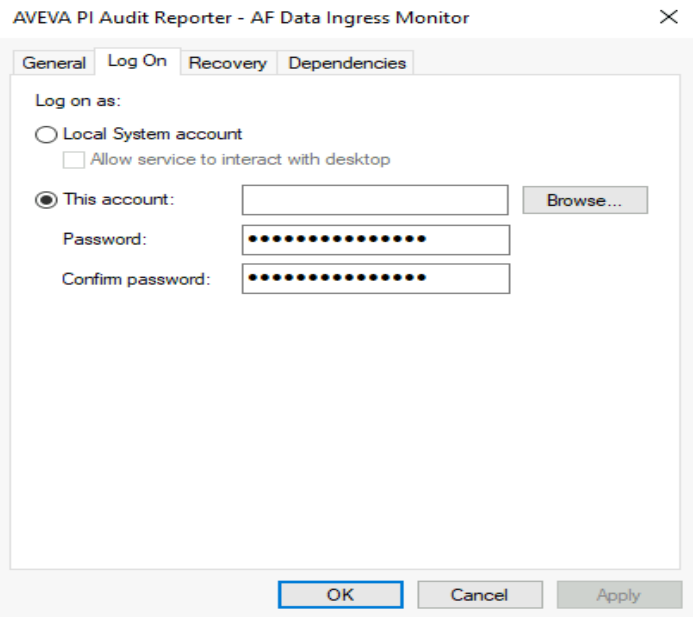
Set the Service Account

To set up a custom service account for running the installed service, update the service Log On tab as follows:

1. Open Services from the Start menu and scroll down to find the AVEVA PI Audit Reporter - AF Data Ingress service.
2. Right-click the service and select properties. The services Log On screen displays.

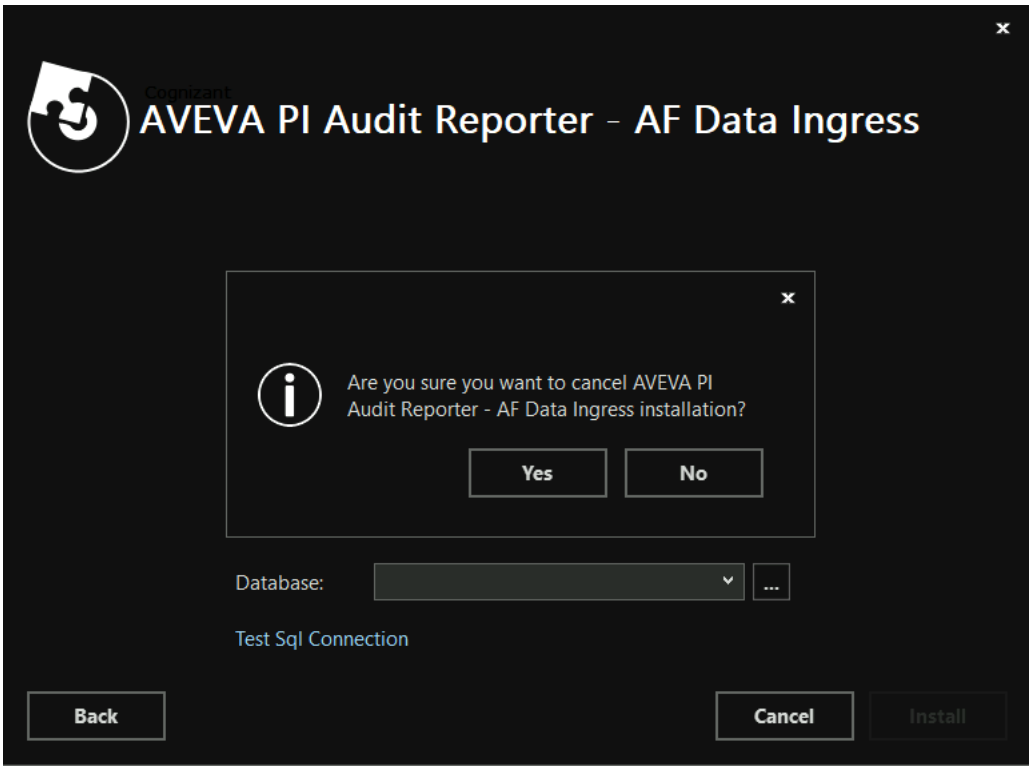


3. In the Properties window of the service, select the Log On tab.
4. Select the option “This account”. Use the “Browse..." button to select a user account from the directory.
5. Enter the password and confirm the password for the service account.
6. Select Apply to save the changes.
7. Select OK to close the window.



How to cancel the installation

To cancel the installation, select the (×) in the upper-right corner or Select cancel button. A confirmation dialog appears, prompting the user to confirm or abort the cancellation. Select Yes to confirm. Refer to the screenshot below to verify the settings.



Add a new AF service instance to the AVEVA PI Audit Reporter application on existing server

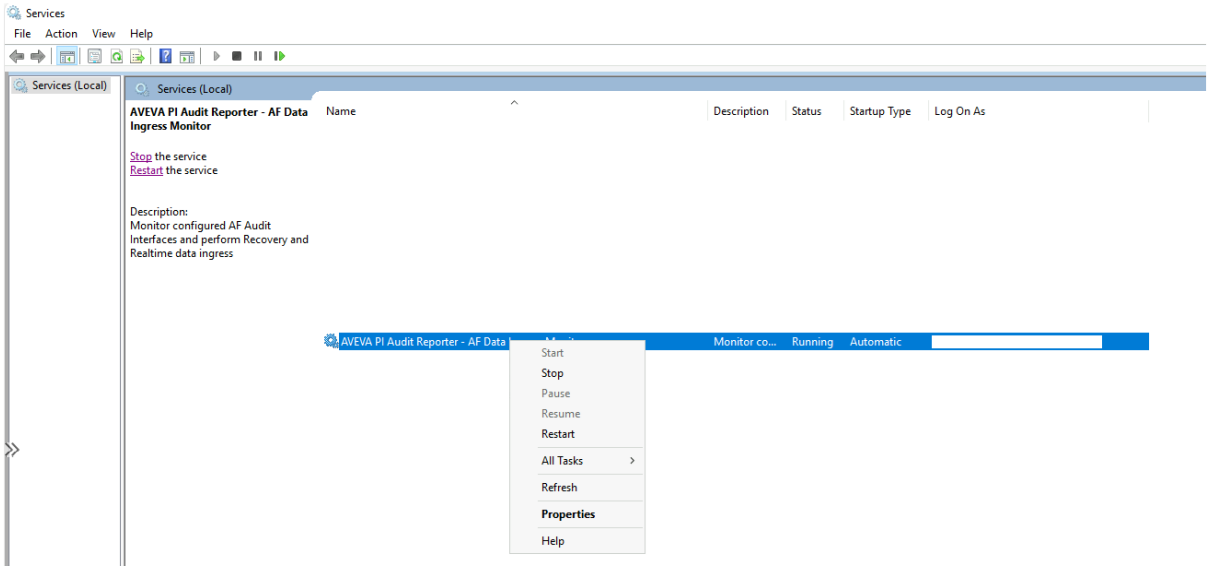
Some mandatory steps are required to add a new AF service instance to the AVEVA PI Audit Reporter application on existing server.

Duplicate installation files and replace settings

To duplicate installation files and replace settings, perform the following:

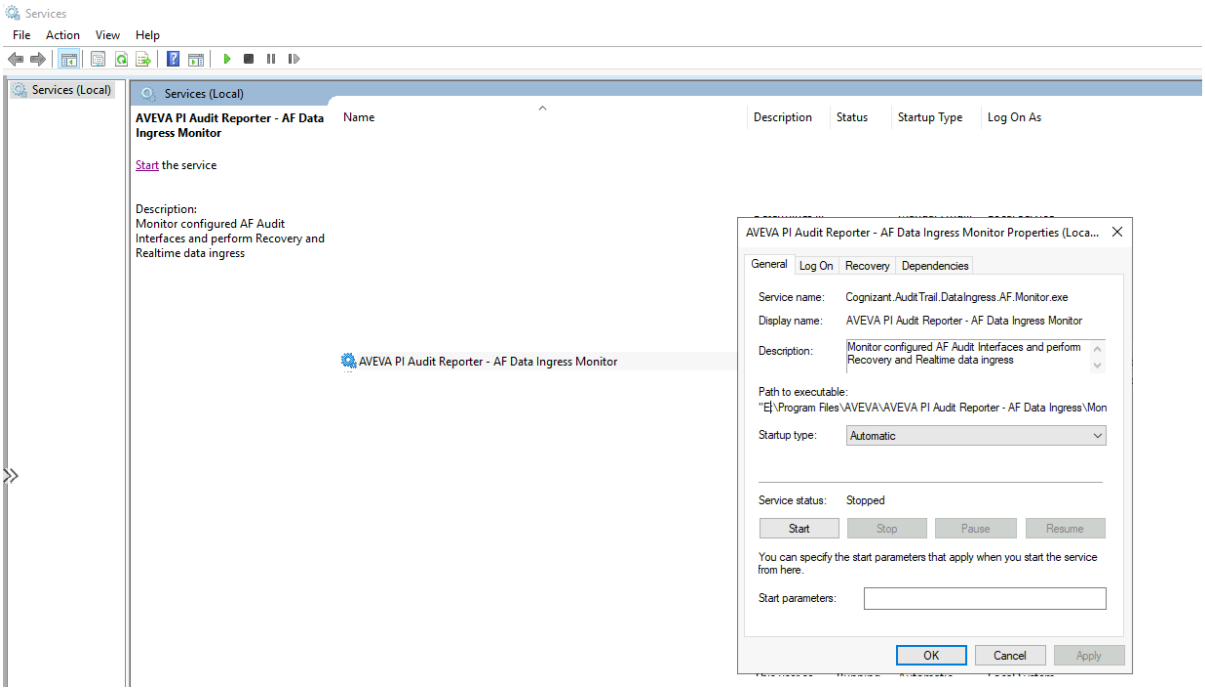
1. Open the Windows Services Management Console.
    a. Press Win + R, type services.msc, and press Enter.
2. Locate the service named: AVEVA PI Audit Reporter - AF Data Ingress Monitor.
3. Right-click the service and select Stop from the context menu.

Note: Ensure the user has the necessary administrative privileges to perform this action. Stopping this service may interrupt data ingestion processes associated with the AVEVA PI Audit Reporter.



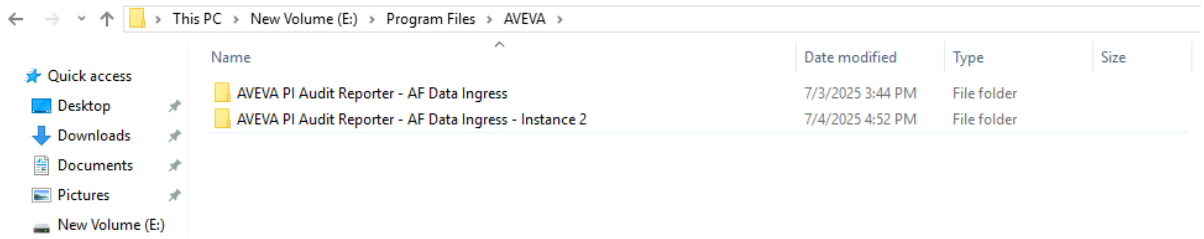
4. Right-click the same service entry in the Services Management Console.
5. Select Properties from the context menu.
6. In the General tab of the Properties window, locate the field labeled Path to executable.

This field displays the full file system path to the services executable file, indicating the directory where the service is installed.



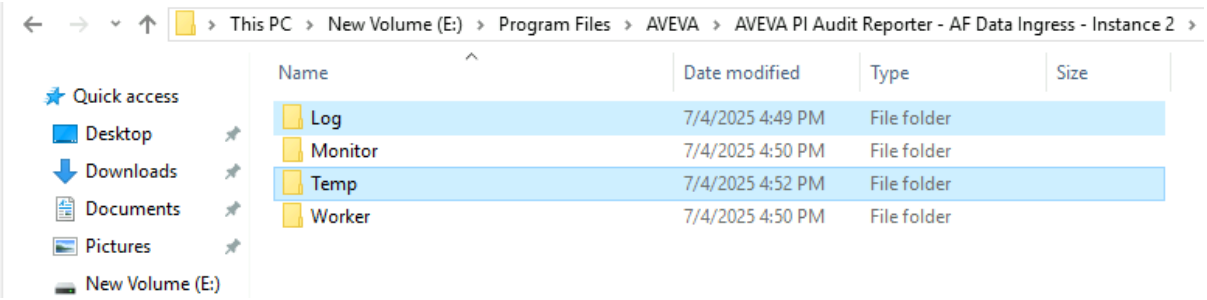
7. Using the Path to executable identified in the previous step, navigate to the corresponding directory in File Explorer.
8. Locate the folder named: AVEVA PI Audit Reporter - AF Data Ingress
9. Right-click the folder and select Copy.
10. Paste the copied folder in the same directory or a designated location.
11. Rename the duplicated folder to: AVEVA PI Audit Reporter - AF Data Ingress - Instance 2.

Note: Ensure the copied folder retains all subdirectories and files. This duplicate may be used for configuring a secondary instance or for backup purposes.



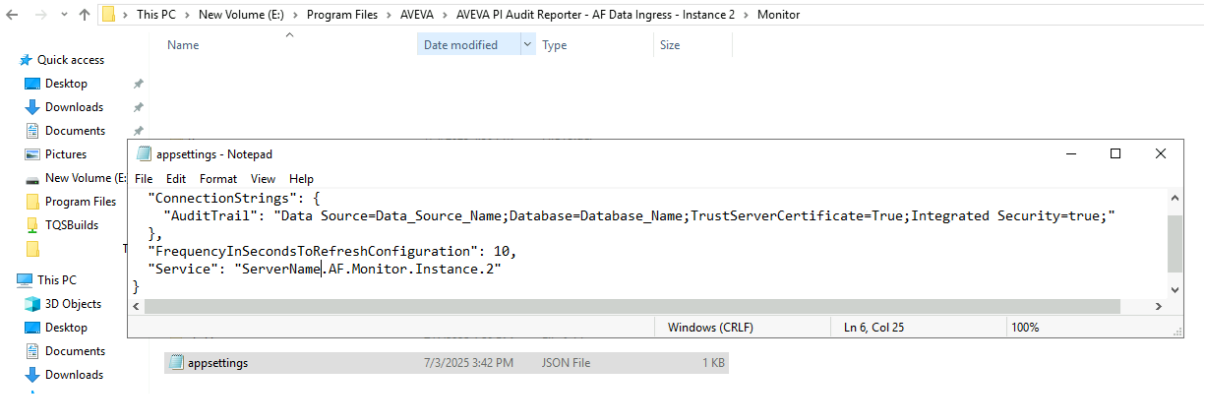
12. Navigate to the duplicated folder: AVEVA PI Audit Reporter - AF Data Ingress - Instance 2 and delete folders Log and Temp.

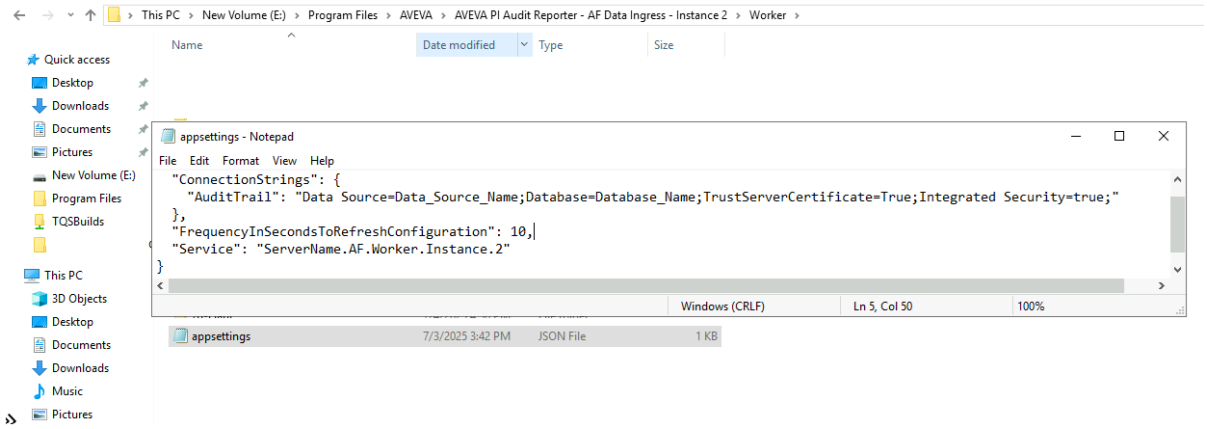
Note: These folders typically contain runtime logs and temporary files that are not required for initializing a new instance. Removing them ensures a clean environment for configuration.



13. Navigate to the duplicated folder: AVEVA PI Audit Reporter - AF Data Ingress - Instance 2 and delete folders Log and Temp.
14. Within the duplicated folder: AVEVA PI Audit Reporter - AF Data Ingress - Instance 2, navigate to the subdirectories Worker and Monitor and locate the file named: appsettings.json.
15. Open each appsettings.json file using a text editor (e.g., Notepad, Notepad++, Visual Studio Code).
16. Locate the entry corresponding to the service name. This may appear under a key such as "ServiceName" or similar.
17. Update the value to reflect the new instance name. For example: "ServiceName": "AVEVA PI Audit Reporter - AF Data Ingress - Instance 2".
18. Save and close the files after making the changes.

Note: Ensure the JSON structure remains valid after editing. Incorrect formatting may prevent the service from starting correctly.

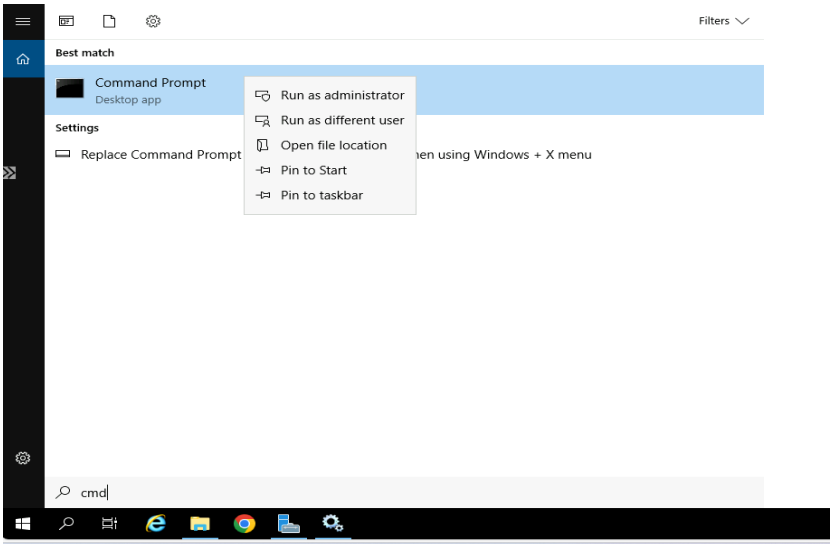




Register a new windows service for the duplicated instance

To create a new service for the duplicated AVEVA PI Audit Reporter - AF Data Ingress instance, follow the steps below:

1. Open Command Prompt as Administrator, selecting Start, type cmd, right-click Command Prompt, and select Run as administrator.



2. Create the register command using the following syntax:

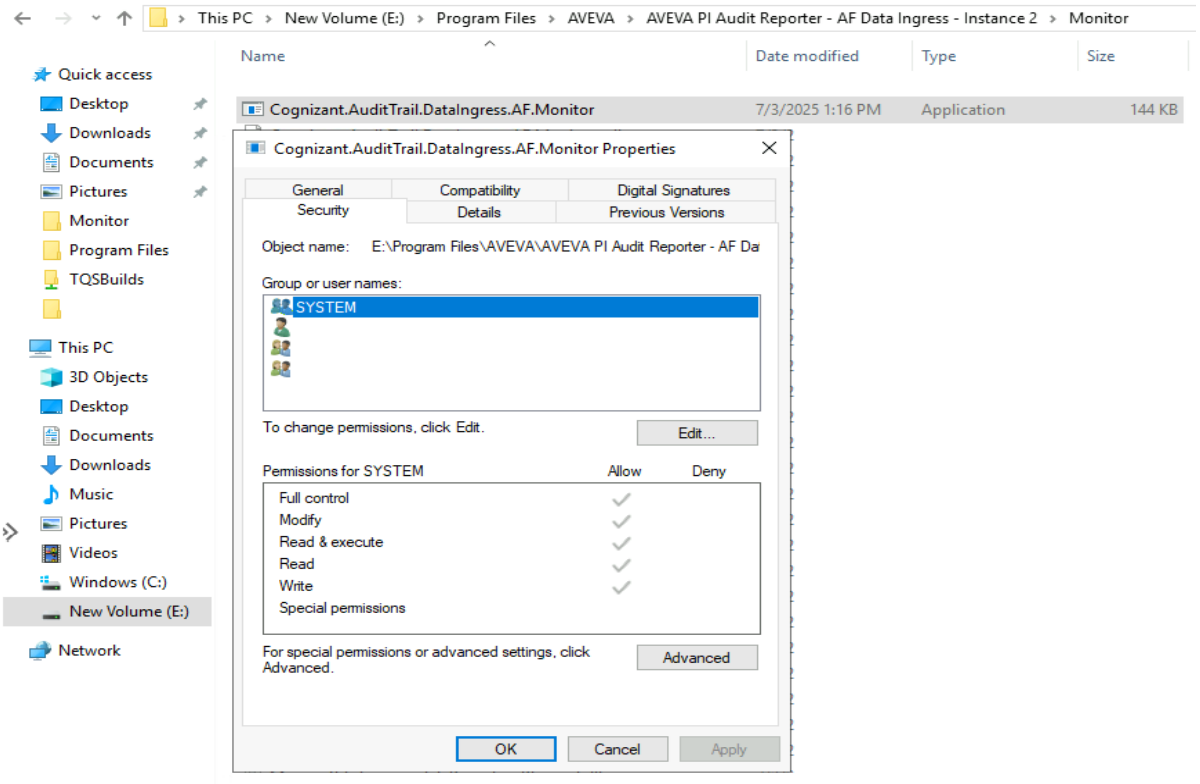
```
sc create "Service_Name_for_Instance_2" displayName=
"Display_Name_For_Service_Instance_2" binPath= "Full_Path_To_Monitor_Executable"
```

   a. Replace "Service_Name_for_Instance_2" with a unique internal name for the service (e.g., Cognizant.AuditTrail.DataIngress.AF.Monitor.Instance.2).

   b. Replace "Display_Name_For_Service_Instance_2" with a user-friendly name that will appear in the Services console (e.g., AVEVA PI Audit Reporter - AF Data Ingress Monitor - Instance 2).

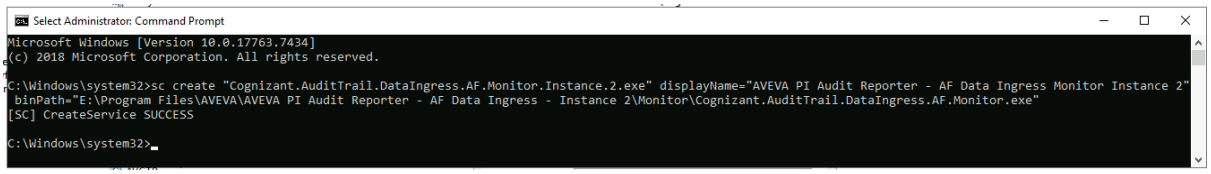
   c. Replace "Full_Path_To_Monitor_Executable" with the full path to the Monitor.exe file inside the duplicated folder.

d. Full path of monitor executable file ‘Cognizant.AuditTrail.DataIngress.AF.Monitor’ can be found in Object name field in “Security” tab under file properties



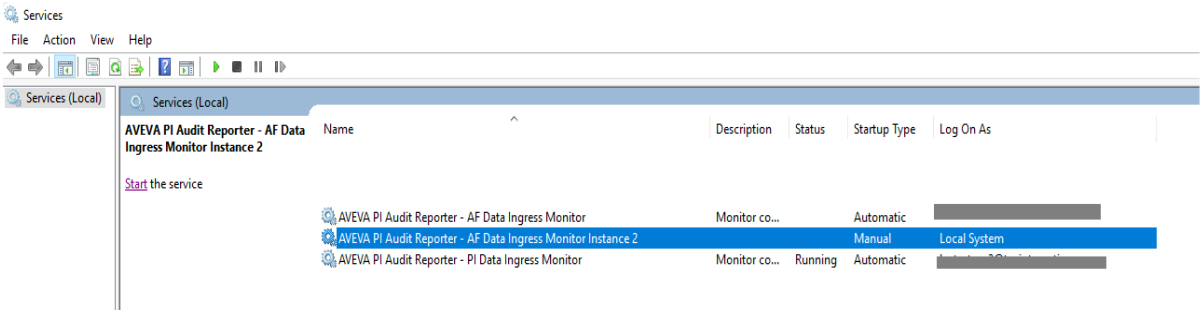
3. Run the sc create Command using the following syntax to register the new service:

```
sc create "Cognizant.AuditTrail.DataIngress.AF.Monitor.Instance.2.exe"
displayName="AVEVA PI Audit Reporter - AF Data Ingress Monitor Instance 2"
binPath="E:\Program Files\AVEVA\AVEVA PI Audit Reporter - AF Data Ingress -
Instance2\Monitor\Cognizant.AuditTrail.DataIngress.AF.Monitor.exe"
```

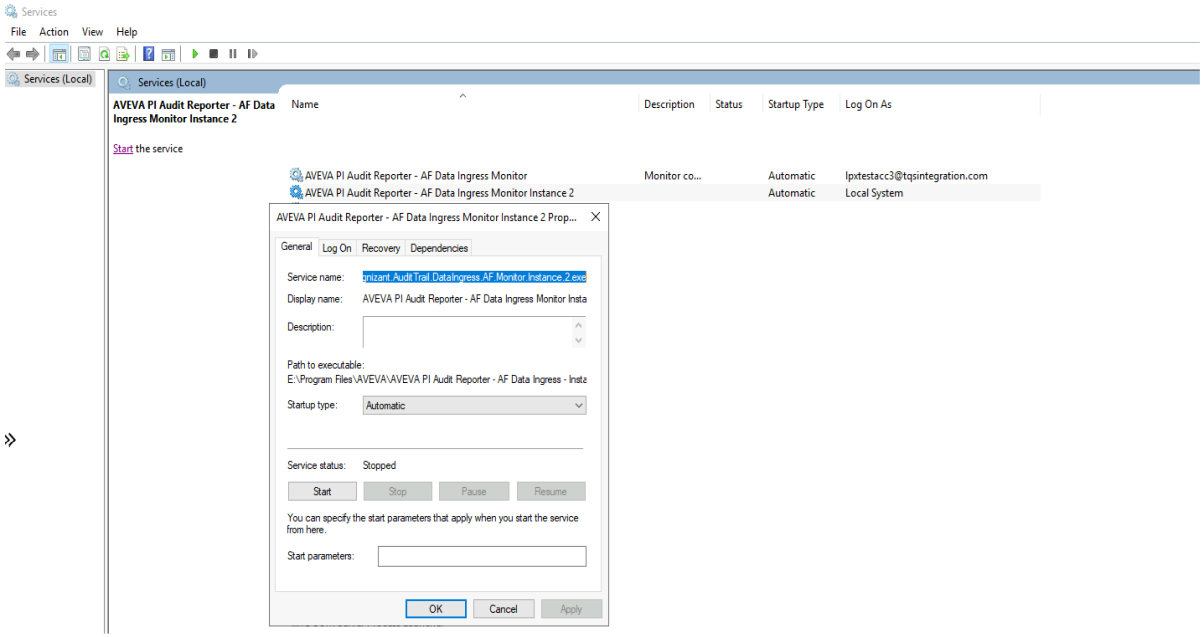


Note: Ensure the command parameters are matching with the environment where it is installed.

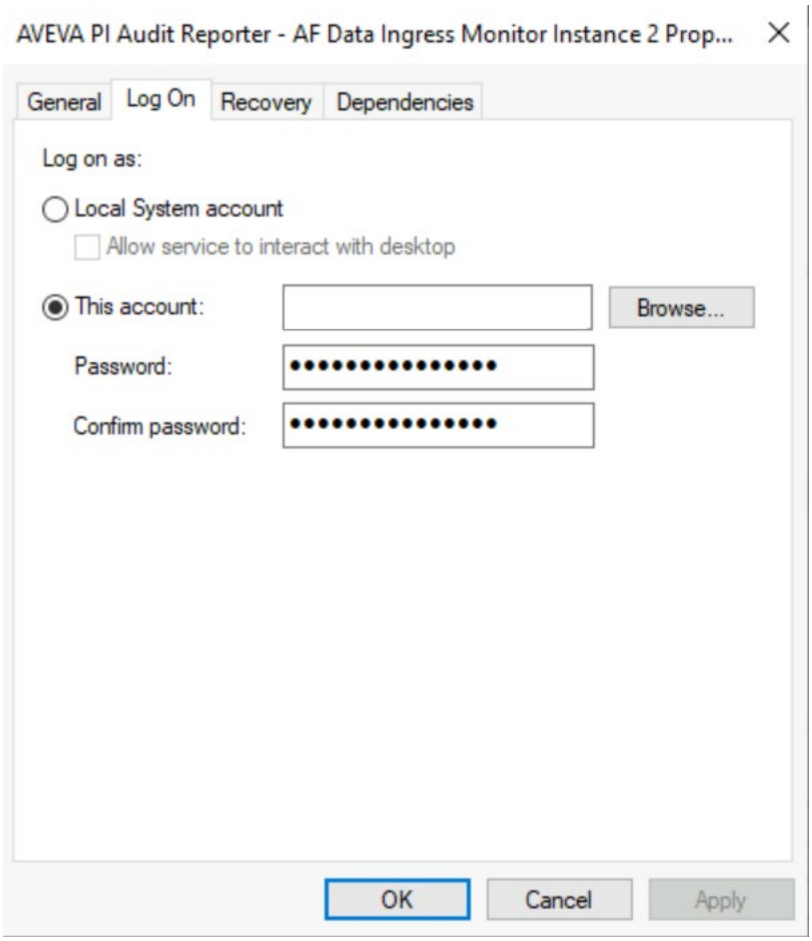
4. In the Windows Services list, scroll through or use the search function to locate the newly created service: AVEVA PI Audit Reporter - AF Data Ingress Monitor - Instance 2. Confirm that the service appears in the list and is available for manual start or automatic startup configuration.



5. Right-click the service and a context menu appears.
6. Select properties and on general screen change “Startup type” to “Automatic”.



7. Select the Log On tab to set up a custom service account for running the installed service.
8. Select the option This account. Use the "Browse..." button to select a user account from the directory.
9. Enter the password and confirm the password for the service account.
10. Select Apply to save the changes.
11. Select OK to close the window. Refer to the screenshot below to verify the settings.



Configure AF Interface in SQL Server

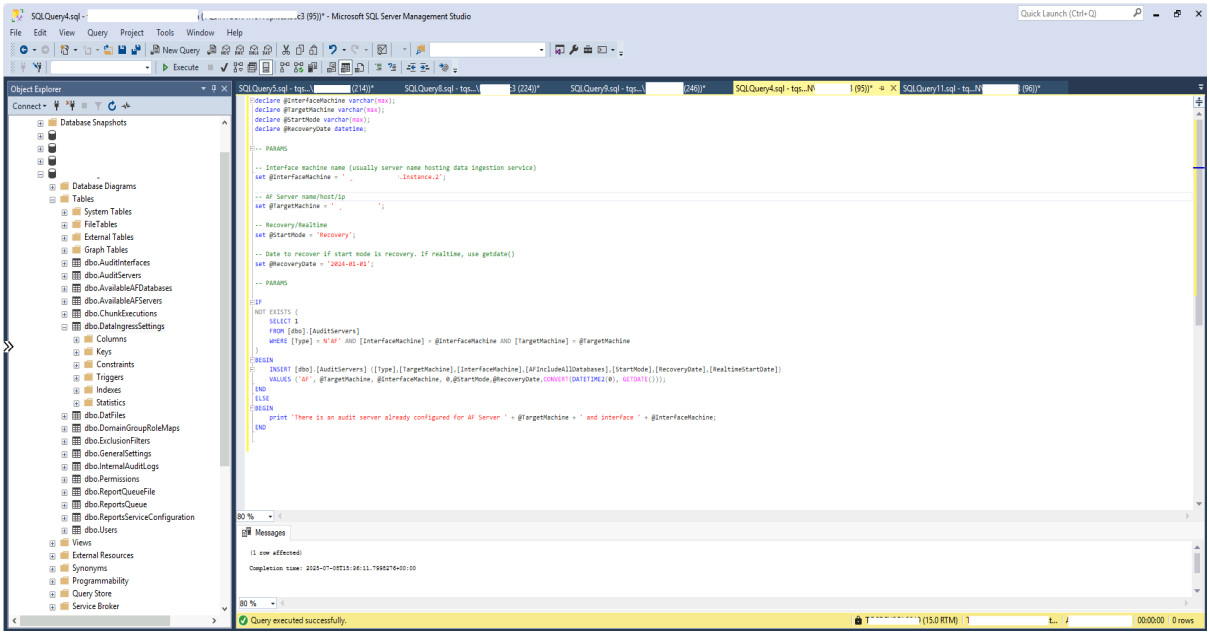
To complete the configuration for the AF interface, follow these steps using SQL Server Management Studio (SSMS).

1. Launch SQL Server Management Studio and connect to the appropriate SQL Server instance.
2. In the Object Explorer, expand the Databases node and select the database currently used by the application.
3. Select New Query in the toolbar to open a new SQL query window.
4. Execute the following SQL script to include the AF interface:

```
declare @InterfaceMachine varchar(max);
declare @TargetMachine varchar(max);
declare @StartMode varchar(max);
declare @RecoveryDate datetime;
-- PARAMS
-- Interface machine name (usually server name hosting data ingestion service)
set @InterfaceMachine = 'Interface_Machine_Name.Instance.2';
-- AF Server name/host/ip
set @TargetMachine = 'Target_Machine_Name';
-- Recovery/Realtime
set @StartMode = 'Recovery';
```

```
-- Date to recover if start mode is recovery. If realtime, use getdate()
set @RecoveryDate = '2025-01-01';
-- PARAMS
IF
NOT EXISTS (
    SELECT 1
    FROM [dbo].[AuditServers]
    WHERE [Type] = N'AF' AND [InterfaceMachine] = @InterfaceMachine AND [TargetMachine]
= @TargetMachine
)
BEGIN
      INSERT [dbo].[AuditServers]
([Type],[TargetMachine],[InterfaceMachine],[AFIncludeAllDatabases],[StartMode],[Rec
overyDate],[RealtimeStartDate])
      VALUES ('AF', @TargetMachine, @InterfaceMachine,
0,@StartMode,@RecoveryDate,CONVERT(DATETIME2(0), GETDATE()));
END
ELSE
BEGIN
      print 'There is an audit server already configured for AF Server ' + @TargetMachine
+ ' and interface ' + @InterfaceMachine;
END
```

5. Refer to the screenshot below to verify the query in MSSQL.



6. Select New Query in the toolbar to open a new SQL query window to replicate data ingress settings for new interface service.

7. Execute the following SQL query, updating the placeholder values as needed to reflect the new instance configuration:

```
insert into [Database_Name].[dbo].[DataIngressSettings]
SELECT 'Interface_Name.AF.Monitor.Instance.2' as [Service], [Key], replace([Value],
'AVEVA PI Audit Reporter - AF Data Ingress', 'AVEVA PI Audit Reporter - AF Data Ingress
- Instance 2') as [Value]
```

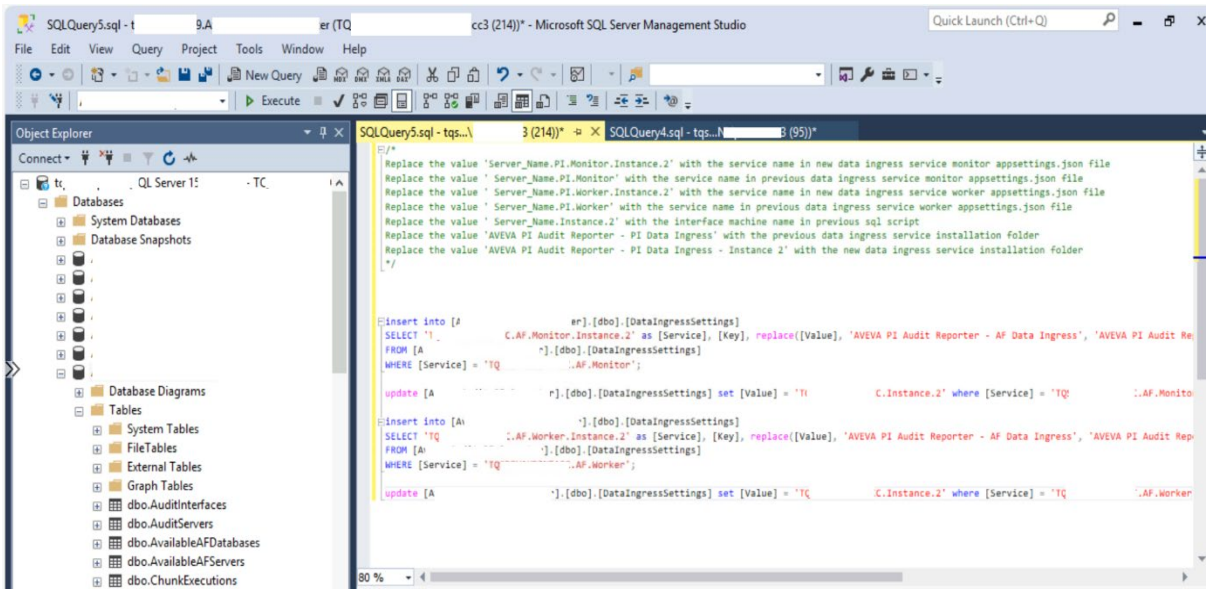
```
FROM [Database_Name].[dbo].[DataIngressSettings]
WHERE [Service] = ' Interface_Name.AF.Monitor';

update [Database_Name].[dbo].[DataIngressSettings] set [Value] = '
Interface_Name.AF.Monitor' where [Service] = ' Interface_Name.AF.Monitor.Instance.2'
and [Key] = 'AppSettings:InterfaceMachine';

insert into [Database_Name].[dbo].[DataIngressSettings]
SELECT ' Interface_Name.AF.Worker.Instance.2' as [Service], [Key], replace([Value],
'AVEVA PI Audit Reporter - AF Data Ingress', 'AVEVA PI Audit Reporter - AF Data Ingress
- Instance 2') as [Value]
FROM [Database_Name].[dbo].[DataIngressSettings]
WHERE [Service] = ' Interface_Name.AF.Worker';

update [Database_Name].[dbo].[DataIngressSettings] set [Value] = '
Interface_Name.AF.Worker' where [Service] = ' Interface_Name.AF.Worker.Instance.2' and
[Key] = 'AppSettings:InterfaceMachine';
```

8. Refer to the screenshot below to verify the query in MSSQL.

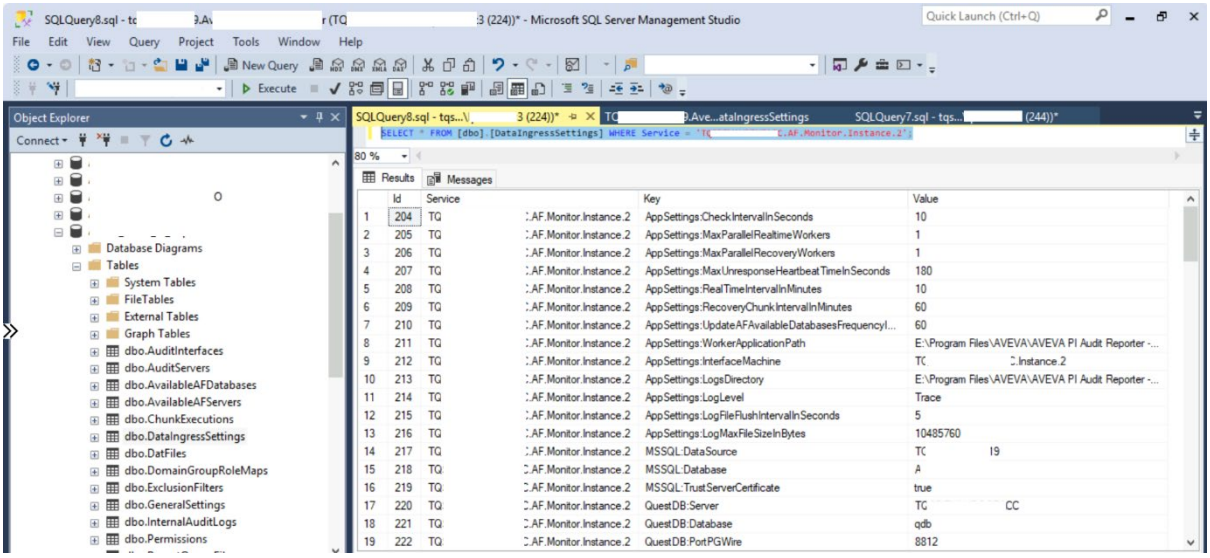


9. Verify Replicated Settings in the DataIngressSettings table by running following sql query (for example):

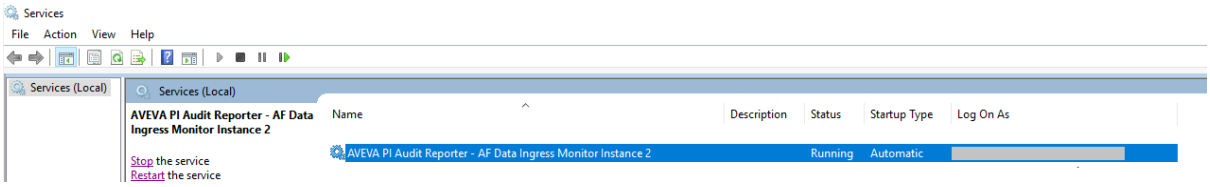
```
SELECT * FROM [dbo].[DataIngressSettings] WHERE Service =
'Interface_machine_name.AF.Monitor.Instance.2';
```

10. Review the results to ensure that all expected configuration parameters for the new interface instance are present and correctly populated.

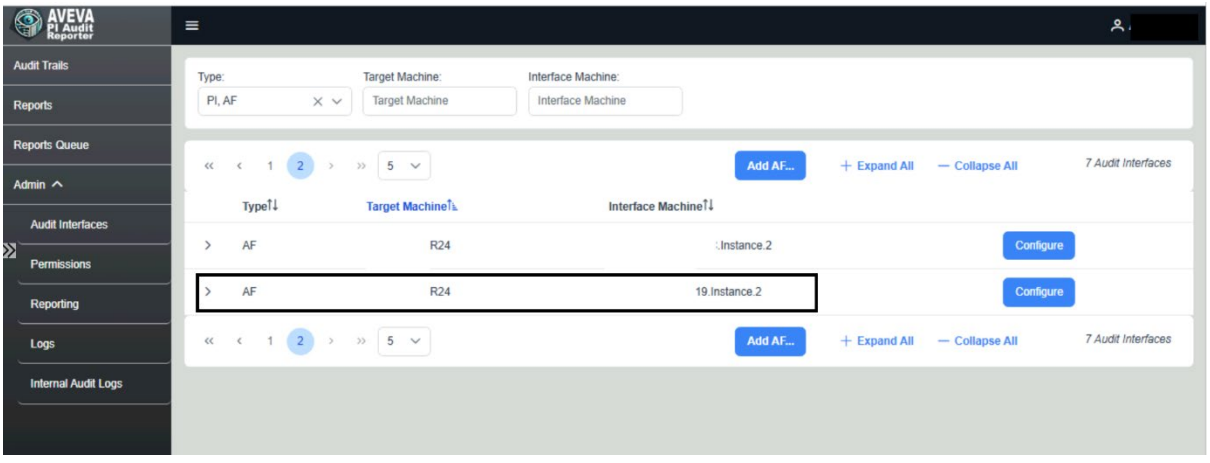
Note: All existent settings from original service instance must be in the duplicated one. Please refer to the configuration settings in Chapter 5.



11. Once the service has been successfully created and its configuration settings replicated:
12. Locate the newly created service: AVEVA PI Audit Reporter - AF Data Ingress Monitor - Instance 2.
13. Right-click the service and select Start.
14. Monitor the service status to ensure it transitions to running without errors.



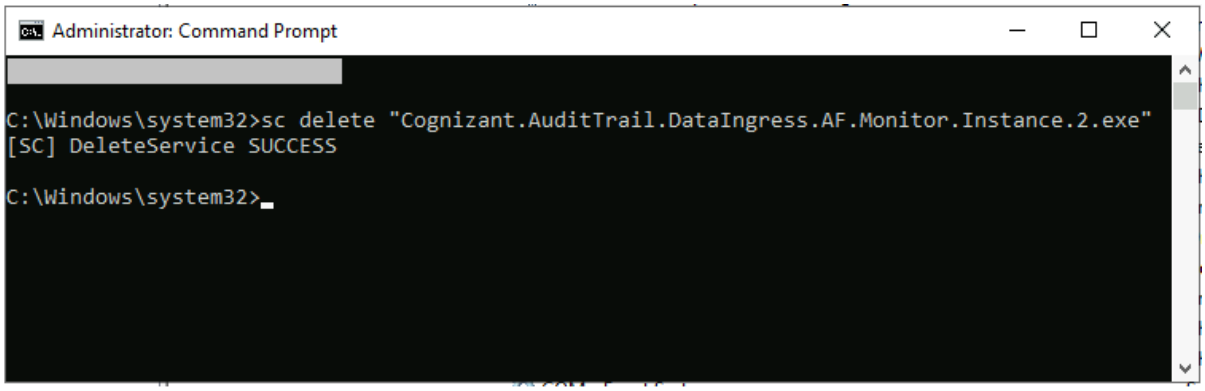
15. Confirm New AF Interface added in the AVEVA PI Audit Reporter. Select Admin, Audit Interfaces.



Delete a service instance from the System

To remove the previously created service from the system:

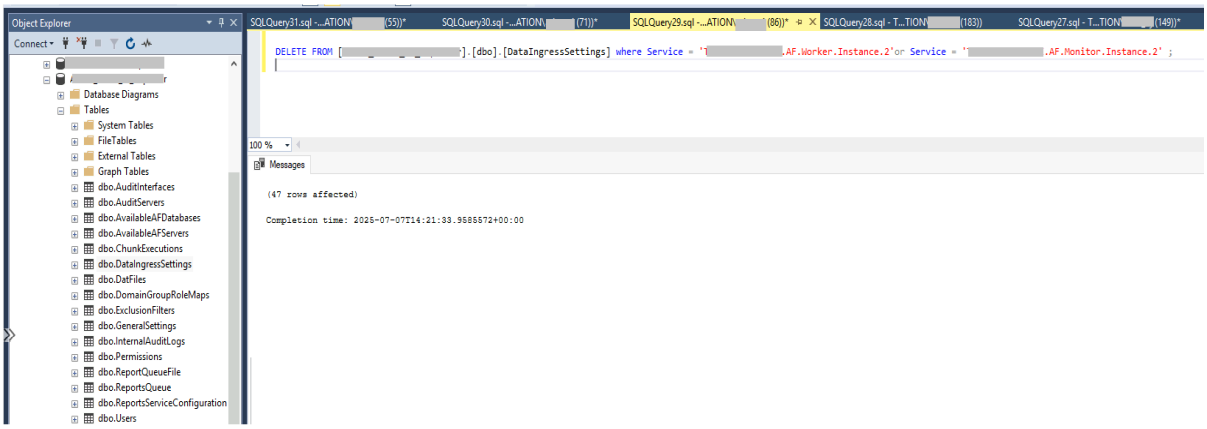
1. Stop the Service:
    a. Open the Services Management Console (services.msc).
    b. Locate the service (e.g., AVEVA PI Audit Reporter - AF Data Ingress Monitor - Instance 2).
    c. Right-click the service and select Stop.
2. Open Command Prompt as Administrator:
    a. Select Start, type cmd, right-click Command Prompt, and select Run as administrator.
3. Run the Following Commands to Delete the Service:
    a. sc delete "Service_Name".
    b. Replace "Service_Name" with the actual internal name of the service (e.g., sc delete "Cognizant.AuditTrail.DataIngress.AF.Monitor.Instance.2.exe").



Note: After deleting the Windows service, remove all associated configuration records from the database to ensure clean decommissioning of the interface.

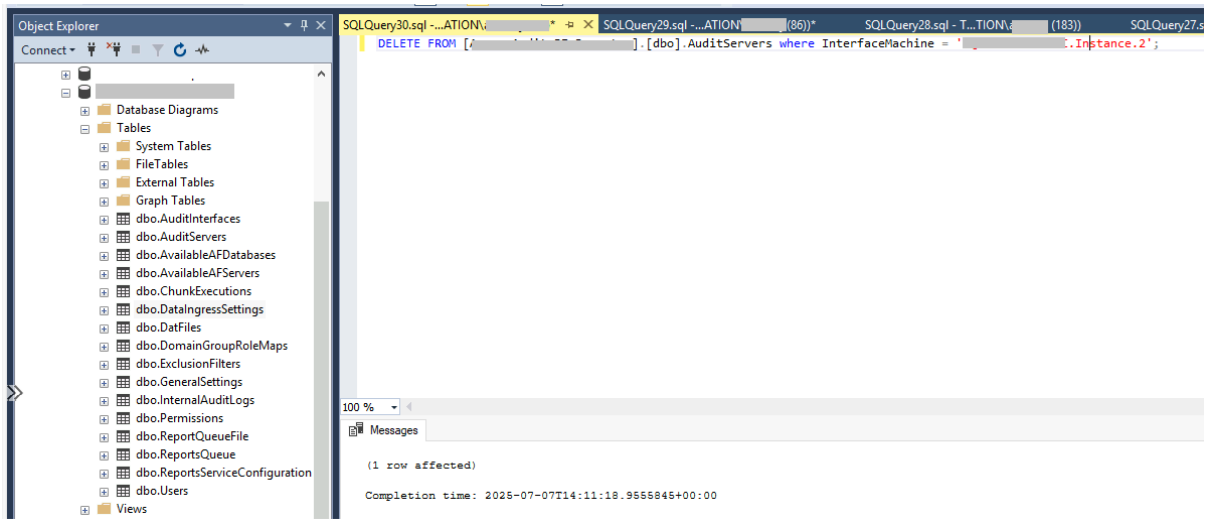
4. Delete DataIngresSettings table for newly added interface with below command:

```
DELETE FROM [Database_Name].[dbo].[DataIngressSettings] where Service =
'Interface_Server.AF.Worker.Instance.2' or Service =
'Interface_server.AF.Monitor.Instance.2'
```



5. Delete audit servers for newly added interface with below command:

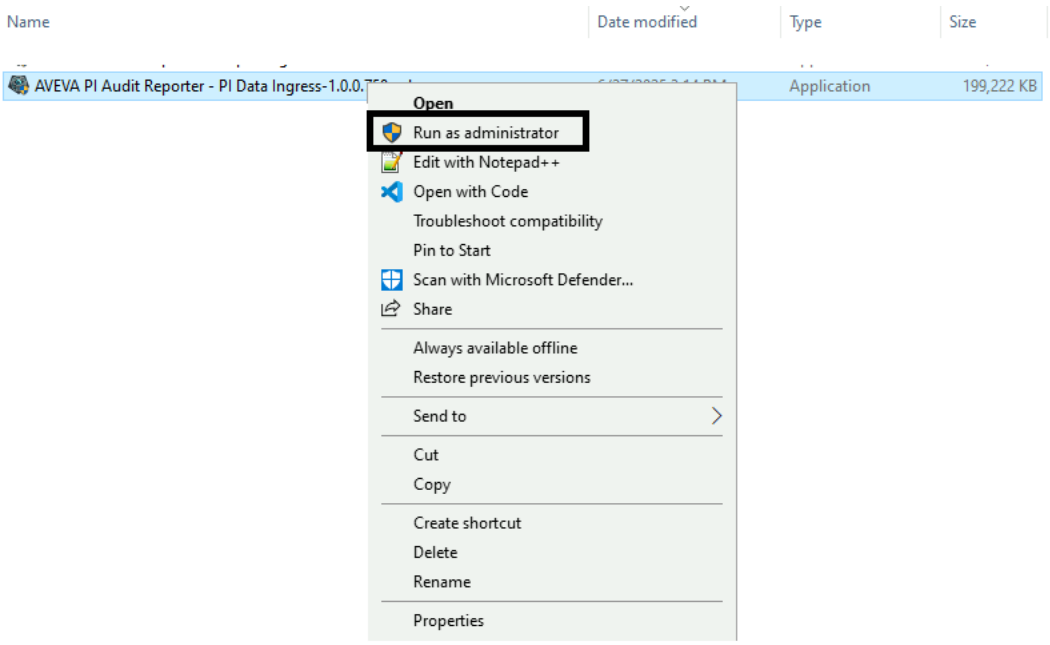
```
DELETE FROM [Database_Table].[dbo].AuditServers where InterfaceMachine =
Interface_server.Instance.2'
```



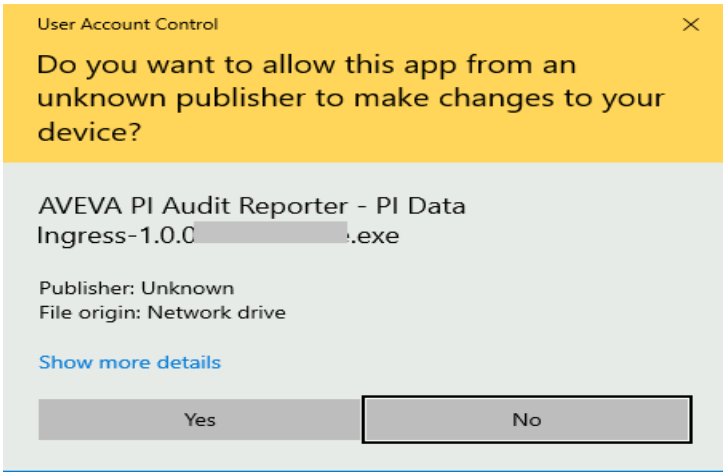
Install AVEVA PI Audit Reporter - PI Data Ingress

To install the AVEVA PI Audit Reporter - PI Data Ingress service, follow the steps below:

1. Locate and right-click the provided installer file AVEVA PI Audit Reporter - PI Data Ingress-1.0.0.xxx_release.exe
2. Select “Run as administrator” (required) from the context menu as shown below.



3. When the installer is launched, a User Account Control (UAC) prompt as shown below will appear with the following message: “Do you want to allow this app from an unknown publisher to make changes to your device?”. Select “Yes” to proceed with the installation.



4. After accepting the User Account Control prompt, the installer proceeds to the File Location Setup screen.
5. Select the ellipsis button ([…]) to open the folder browser.
6. Select the desired directory where the user wants to install the AVEVA PI Audit Reporter - PI Data Ingress.
7. Once the installation path is selected, check the box labeled: “I agree to the License terms and conditions.”
8. Select Next to continue with the installation.

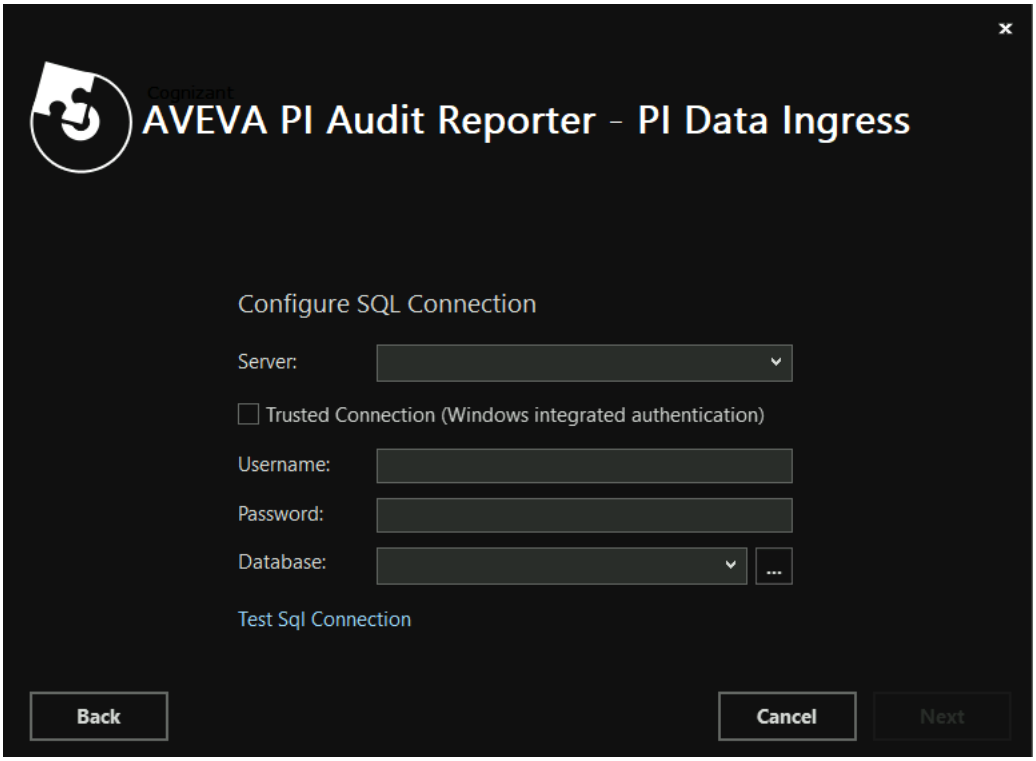
9. The next screen in the setup process is the “Application Configuration” screen.

10. Enter the following configuration details: Interface Machine Name, Local PI Administration folder/directory of the AVEVA PI SDK installation, PI Server Address, QuestDB Settings (Hostname or IP Address) and Port(fixed).

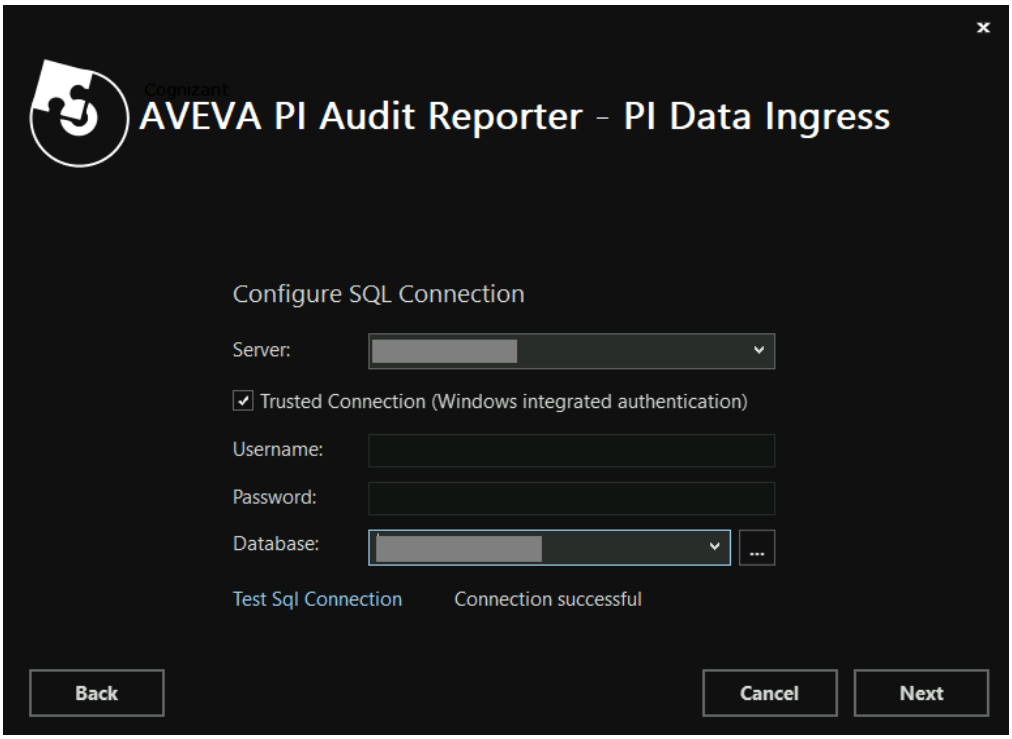
Note: All fields are mandatory. The installation will not proceed unless this information is provided.

11. Select “Next” to navigate to the “Configure SQL Connection” screen.

12. Enter the SQL Server Name in the Configure SQL Connection screen and select the appropriate Database options.
13. It is strongly recommended to use a Trusted Connection, as all services will be configured to run under a single service account. This account must have the appropriate access to the database to allow insertions and updates. If the users prefer to use SQL Authentication (Username/Password), the following configuration is required:
    a. Uncheck the “Trusted Connection” checkbox.
    b. Enter the Username and Password.



14. When the user Selects on Test SQL Connection to verify connectivity, a “Connection successful” message display if the configuration is correct.
15. Once all fields are completed, select “Next”.

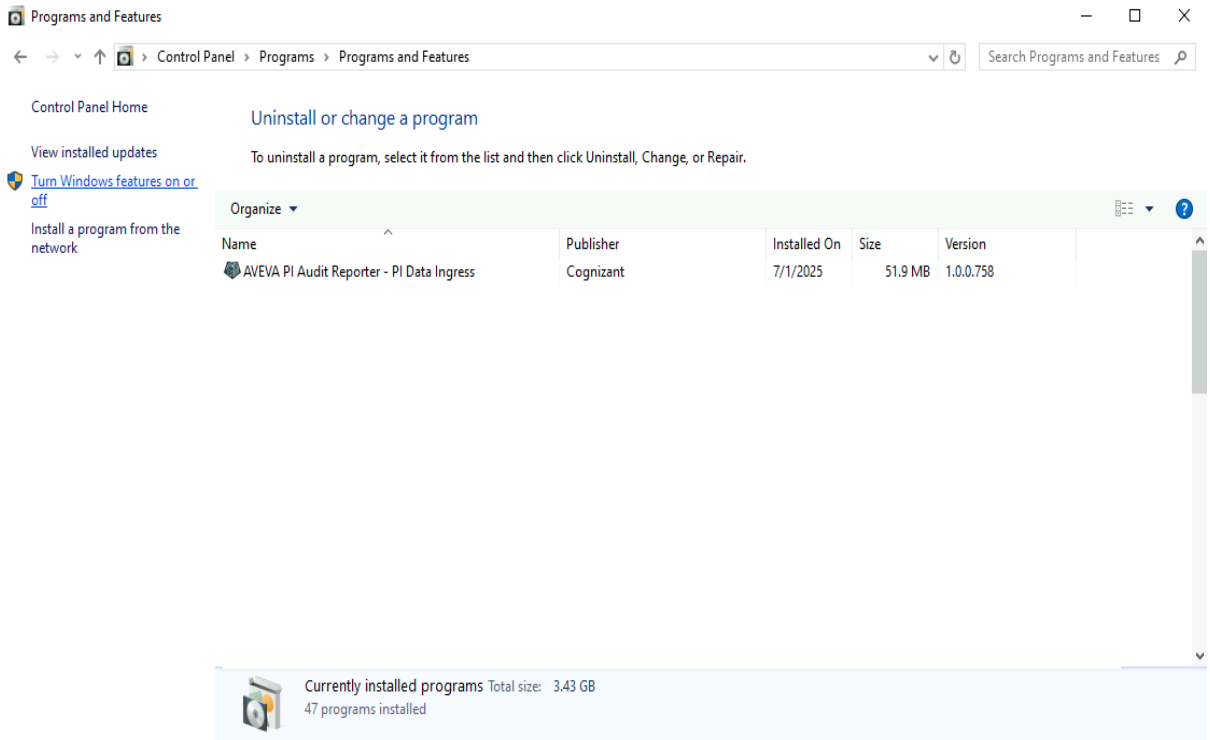


16. The next screen in the setup process is “Interface Configuration”.

17. The user can choose the appropriate start mode for the data ingress process. If Recovery Mode is selected, the user must specify the Recovery Date.
18. Enter the paths to the directories containing the .dat files to be processed. Select the PI Subsystems that will be processed during data ingestion.
19. Once all fields are completed, select “Install” to begin the installation process.

20. Once complete, a confirmation message appears: “AVEVA PI Audit Reporter - PI Data Ingress has been successfully installed.” This indicates that the application has been installed correctly and is ready for use. Select Finish to exit the installer.

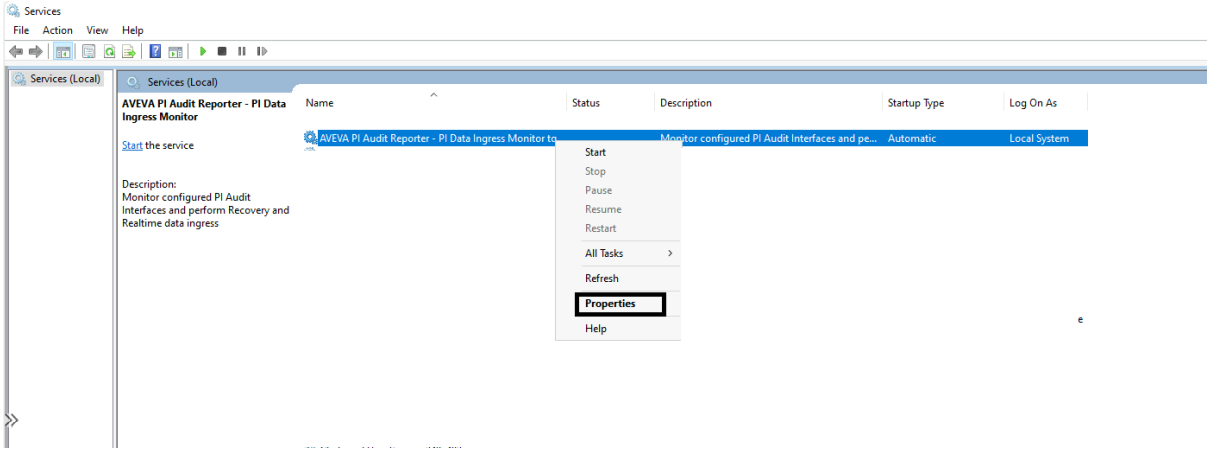
After successful installation, the AVEVA PI Audit Reporter - PI Data Ingress will be listed under Programs and Features in the Windows Control Panel.



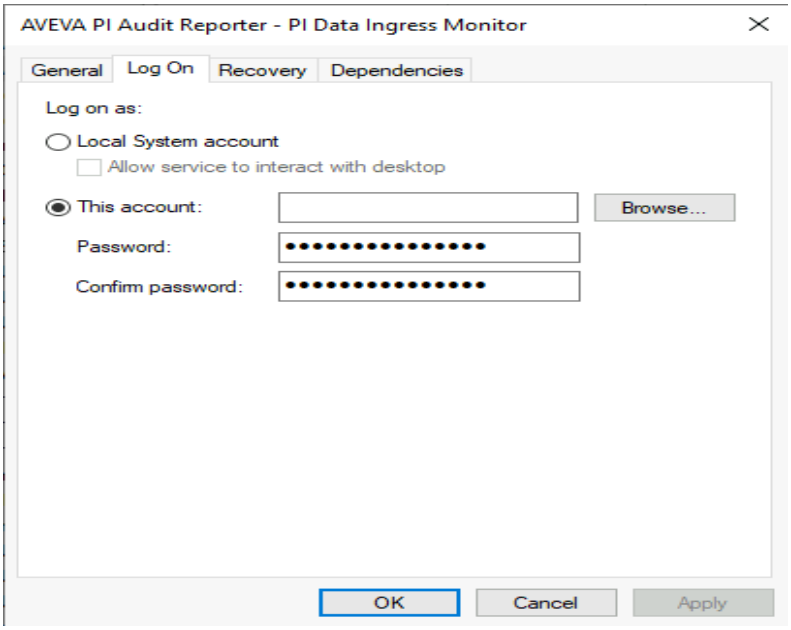
Set the Service Account

To set up a custom service account for running the installed service, update the service Log On tab as follows:

1. Open Services from the Start menu and scroll down to find the AVEVA PI Audit Reporter - AF Data Ingress service.

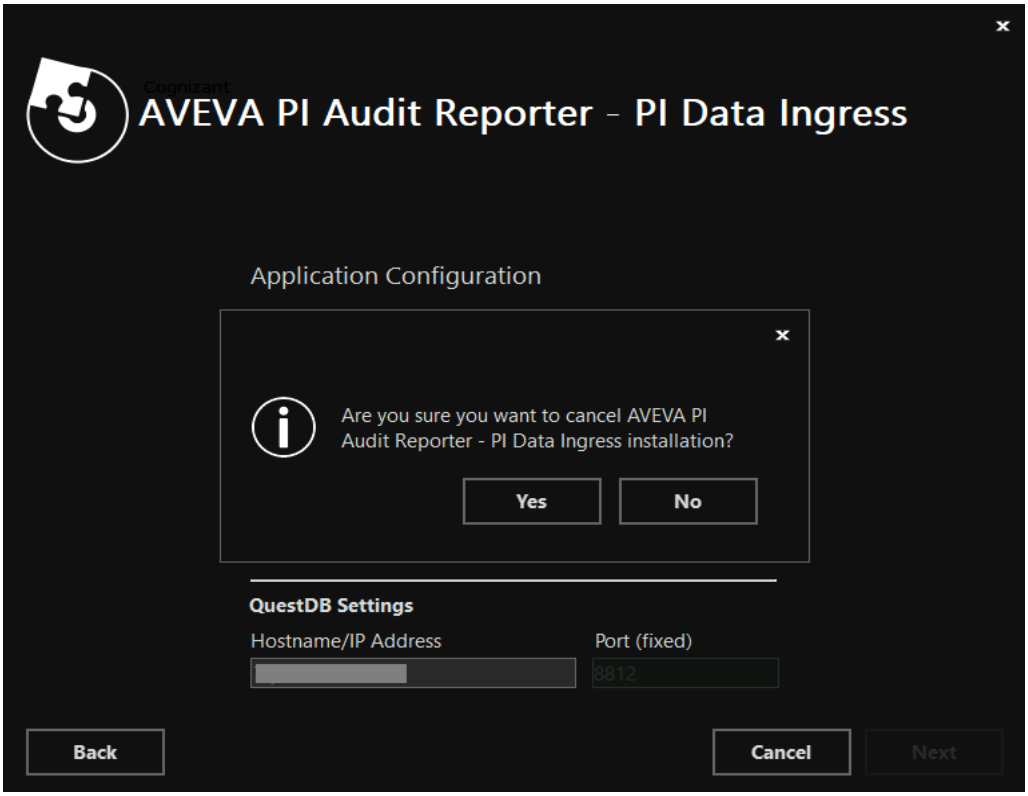


2. Right-click the service and select properties.
3. In the Properties window of the service, select the Log On tab.
4. Select the option “This account”, select "Browse..." button to select a user account from the directory.
5. Enter the password and confirm the password for the service account.
6. Select Apply to save the changes.
7. Select OK to close the window. Refer to the screenshot below to verify the settings.



How to cancel the installation

To cancel the installation, select the (×) in the upper-right corner or Select cancel button. A confirmation dialog appears, prompting the user to confirm or abort the cancellation. Select Yes to confirm. Refer to the screenshot below to verify the settings.



Adding a new PI Interface to the AVEVA PI Audit Reporter application on existing service instance

To integrate a new PI Interface into the application, users must execute a specific SQL query on the database. This operation registers the new Interface and enables data ingestion from the specified PI source. Before executing the SQL query, ensure the following fields are correctly configured:

- Interface_Machine: The hostname or identifier of the machine where the PI interface is running.
- Target_Machine: The destination system where processed data is intended to be delivered or consumed.
- PI_Server_Name/Host/IP: The name or IP address of the PI server to connect to.
- Recovery_Start_Date: The date from which historical data recovery should begin.
- Dat_File_Backup_Directory: The directory path where backup .dat files will be stored.
- Dat_File_Directory: The directory path where incoming .dat files will be read from.

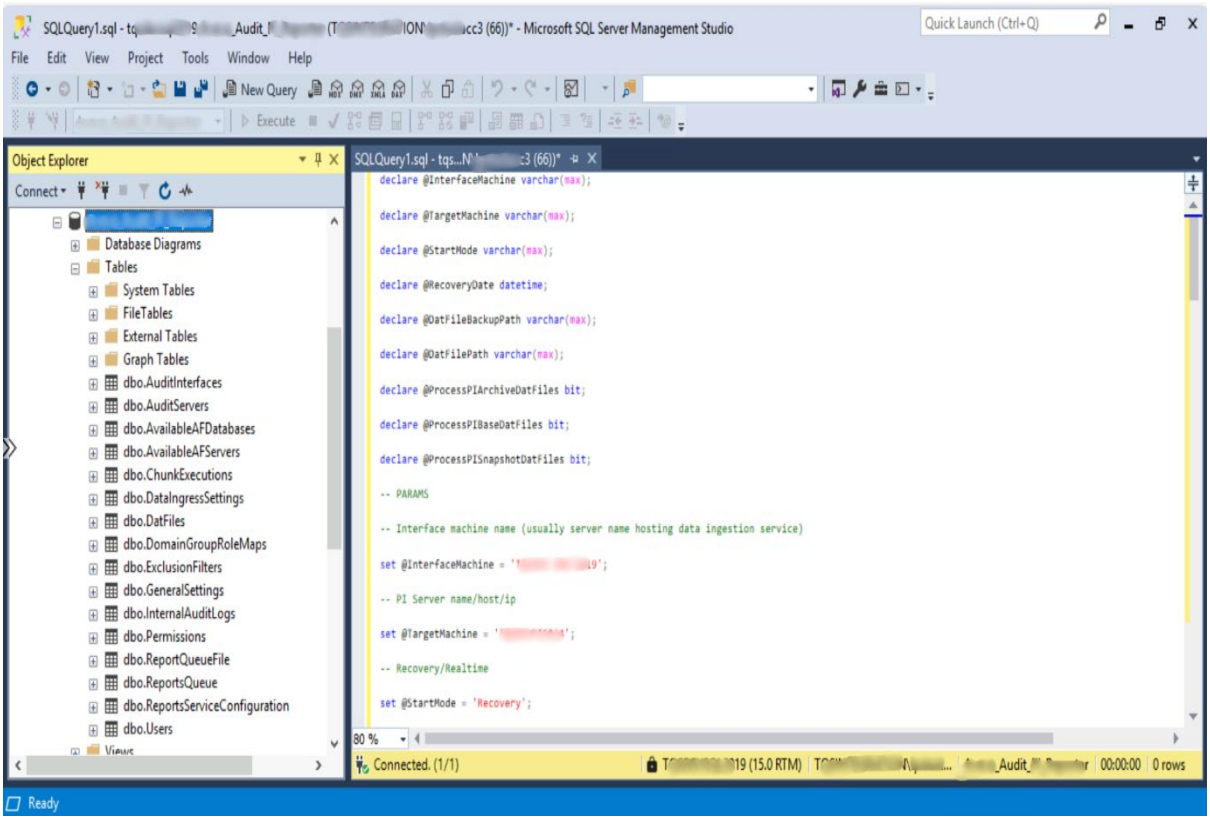
Once the above fields are configured, perform the following steps to run the query:

1. Launch SQL Server Management Studio and connect to the appropriate SQL Server instance.
2. In the Object Explorer, expand the Databases node and select the database currently used by the application.
3. Select New Query in the toolbar to open a new SQL query window.
4. Execute the following SQL script to include the PI interface:

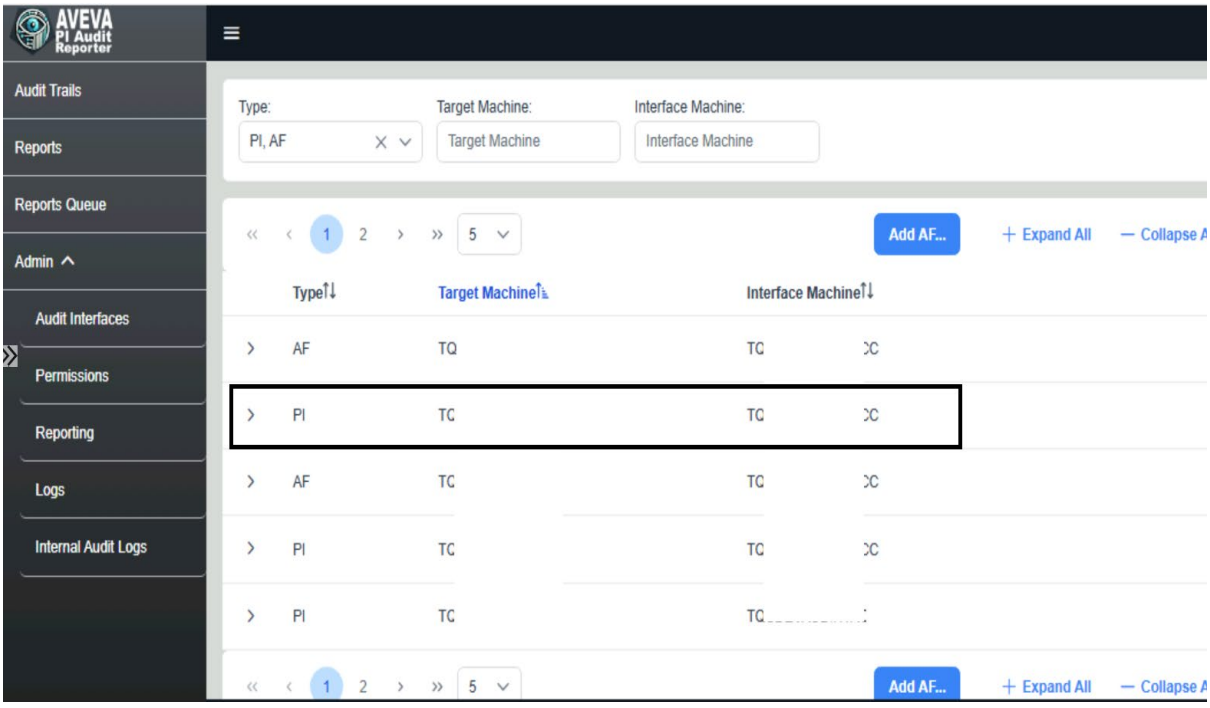
```
declare @InterfaceMachine varchar(max);
declare @TargetMachine varchar(max);
declare @StartMode varchar(max);
declare @RecoveryDate datetime;
declare @DatFileBackupPath varchar(max);
declare @DatFilePath varchar(max);
declare @ProcessPIArchiveDatFiles bit;
declare @ProcessPIBaseDatFiles bit;
declare @ProcessPISnapshotDatFiles bit;
-- PARAMS
-- Interface machine name (usually server name hosting data ingestion service)
set @InterfaceMachine = 'Interface_Machine_Name';
-- PI Server name/host/ip
set @TargetMachine = ' PI_Server_Name/Host/Ip';
-- Recovery/Realtime
set @StartMode = 'Recovery';
-- Date to recover if start mode is recovery. If realtime, use getdate()
set @RecoveryDate = 'Recovery_Start_Date';
-- Dat file backup directory. Empty if does not exist
set @DatFileBackupPath = 'Dat_File_Backup_Directory'
-- Dat file directory
set @DatFilePath = ' Dat_File_Directory'
-- Flag that indicates if interface will process pi archive audit database files (.dat)
set @ProcessPIArchiveDatFiles = 1;
-- Flag that indicates if interface will process pi base audit database files (.dat)
set @ProcessPIBaseDatFiles = 1;
-- Flag that indicates if interface will process pi snapshot audit database files (.dat)
set @ProcessPISnapshotDatFiles = 1;
-- PARAMS
IF
NOT EXISTS (
    SELECT 1
    FROM [dbo].[AuditServers]
    WHERE [Type] = N'PI' AND [InterfaceMachine] = @InterfaceMachine AND [TargetMachine]
= @TargetMachine
)
BEGIN
      INSERT [dbo].[AuditServers]
([Type],[TargetMachine],[InterfaceMachine],[AFIncludeAllDatabases],[StartMode],[Rec
overyDate],[RealtimeStartDate])
      VALUES ('PI', @TargetMachine, @InterfaceMachine,
0,@StartMode,@RecoveryDate,CONVERT(DATETIME2(0), GETDATE()));
END
ELSE
BEGIN
      print 'There is an audit server already configured for PI Server ' + @TargetMachine
+ ' and interface ' + @InterfaceMachine;
END
```

```
IF NOT EXISTS (
    SELECT 1
    FROM [dbo].[AuditInterfaces]
    WHERE [Type] = N'PI' AND [InterfaceMachine] = @InterfaceMachine AND [TargetMachine]
= @TargetMachine
)
BEGIN
    INSERT [dbo].[AuditInterfaces]
      ([AuditServerID],
       [Type],                                [InterfaceMachine],
[TargetMachine],
       [TargetDatabase],                      [TargetDatabaseGUID],
[DatabaseEnabled],
       [StartMode],                           [RecoveryDate],
[RealtimeStartDate],
       [ProcessedRecoveryCount],              [ProcessedRecoveryMaxDate],
[ProcessedRealtimeCount],
       [ProcessedRealtimeMaxDate],            [TotalRecords],
[BackupFilesDirectory],
       [AuditDatFilesDirectory],              [ProcessArchiveAuditSubsystem],
[ProcessSnapshotAuditSubsystem],
       [ProcessBaseAuditSubsystem],           [CurrentDatFile],
[ExclusionFilterStatus],
       [BackupFilesCopied],                   [Summary])
 VALUES
      ((SELECT ID FROM [dbo].[AuditServers] WHERE [Type] = N'PI' AND [InterfaceMachine]
= @InterfaceMachine AND [TargetMachine] = @TargetMachine),
      'PI',                                                  @InterfaceMachine,
                      @TargetMachine,
       NULL,                                                       NULL,
                             1,
       @StartMode,                                           @RecoveryDate,
                      CONVERT(DATETIME2(0), GETDATE()),
       0,                                                    CONVERT(DATETIME2(0),
GETDATE()), 0,
       CONVERT(DATETIME2(0), GETDATE()),      0,
                  @DatFileBackupPath,
       @DatFilePath,
      @ProcessPIArchiveDatFiles,          @ProcessPISnapshotDatFiles,
       @ProcessPIBaseDatFiles,                NULL,
            NULL,
       0,                                     NULL);
END
ELSE
BEGIN
      print 'There is an audit interface already configured for PI Server ' +
@TargetMachine + ' and interface ' + @InterfaceMachine;
END
```

Refer to the screenshot below to verify the query in MSSQL.



To Confirm New PI Interface added in the AVEVA PI Audit Reporter, select Admin, Audit Interfaces, as shown below.



Add a new PI service instance to the AVEVA PI Audit Reporter application on existing server

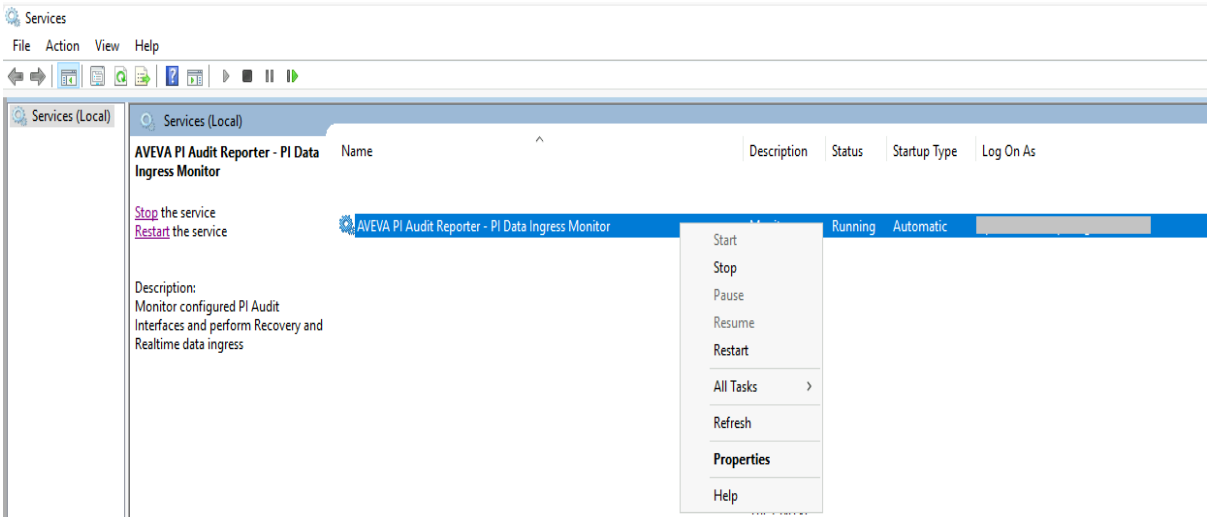
Some mandatory steps are required to add a new PI service instance to the AVEVA PI Audit Reporter application on existing server.

Duplicate installation files and replace settings

To duplicate installation files and replace settings, perform the following:

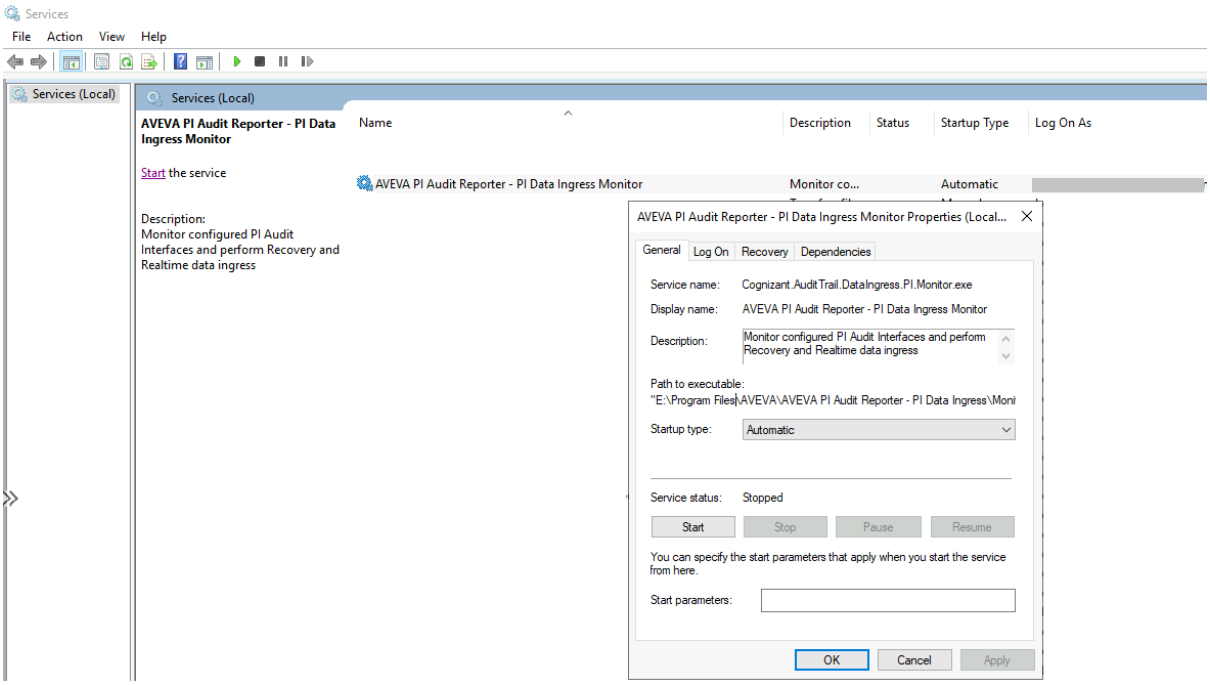
1. Open the Windows Services Management Console.
   a. Press Win + R, type services.msc, and press Enter.
2. Locate the service named: AVEVA PI Audit Reporter - AF Data Ingress Monitor.
3. Right-click the service and select Stop from the context menu.

Note: Ensure the user has the necessary administrative privileges to perform this action. Stopping this service may interrupt data ingestion processes associated with the AVEVA PI Audit Reporter.



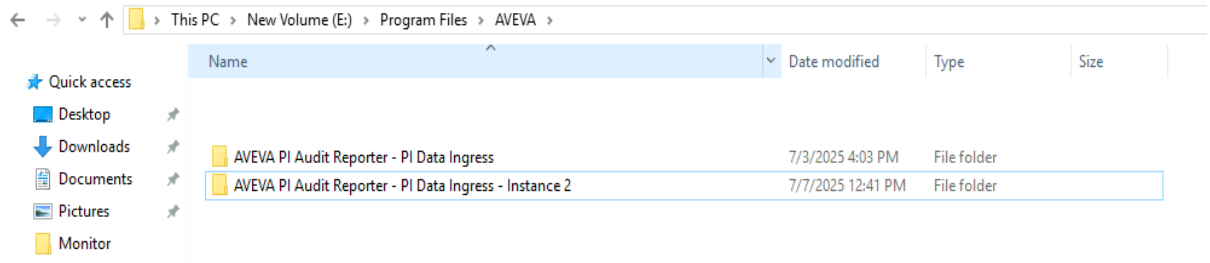
4. Once the 'AVEVA PI Audit Reporter - PI Data Ingress Monitor' service has been successfully stopped:
5. Right-click the same service entry in the Services Management Console.
6. Select Properties from the context menu.

In the General tab of the Properties window, locate the field labeled Path to executable. This field displays the full file system path to the services executable file, indicating the directory where the service is installed.



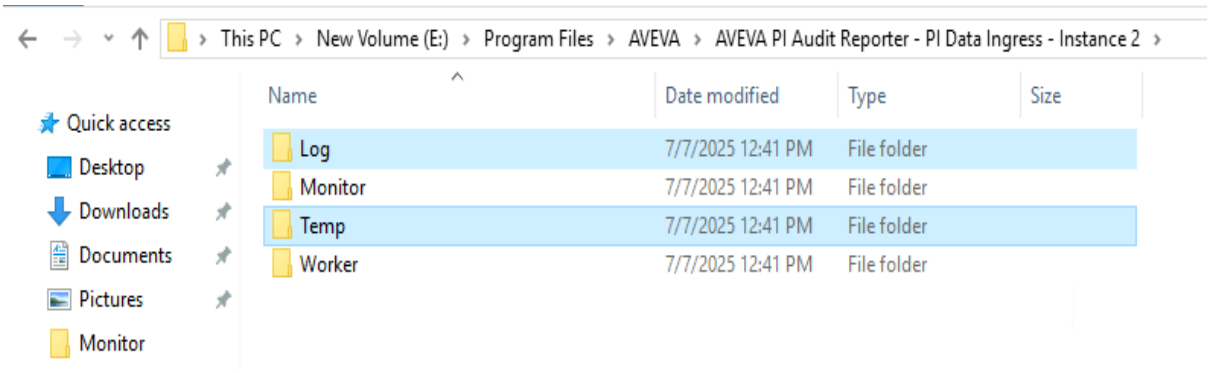
7. Using the Path to executable identified in the previous step, navigate to the corresponding directory in File Explorer.
8. Locate the folder named: AVEVA PI Audit Reporter - PI Data Ingress
9. Right-click the folder and select Copy.
10. Paste the copied folder in the same directory or a designated location.
11. Rename the duplicated folder to: AVEVA PI Audit Reporter - PI Data Ingress - Instance 2.

Note: Ensure the copied folder retains all subdirectories and files. This duplicate may be used for configuring a secondary instance or for backup purposes.



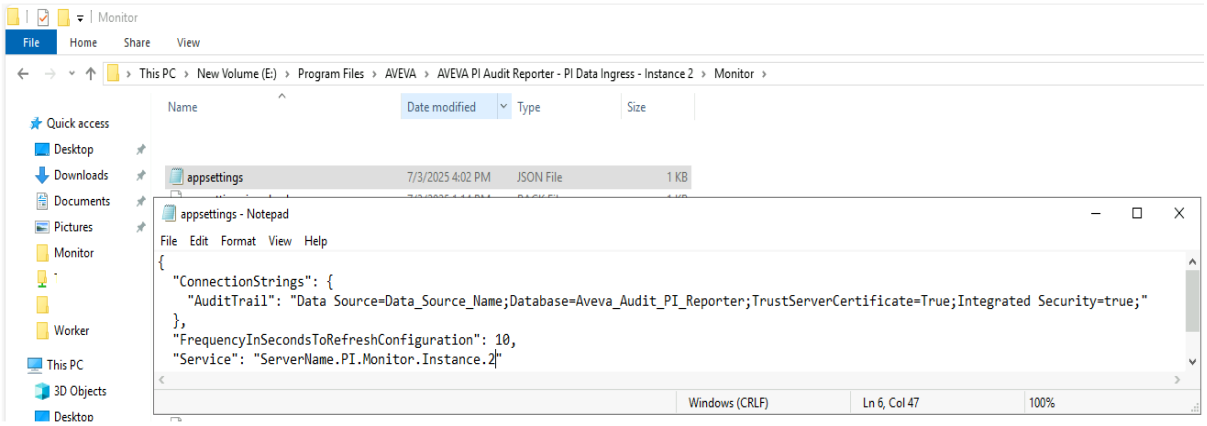
12. Navigate to the duplicated folder: AVEVA PI Audit Reporter - AF Data Ingress - Instance 2 and delete folders Log and Temp.

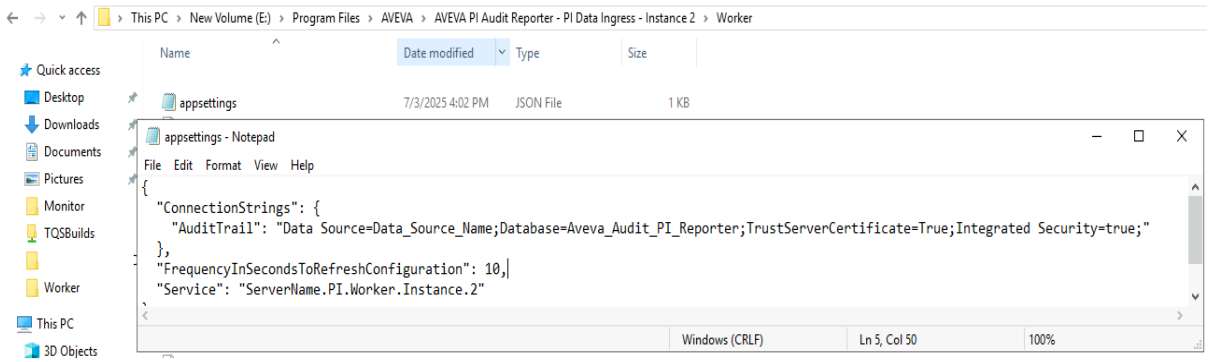
Note: These folders typically contain runtime logs and temporary files that are not required for initializing a new instance. Removing them ensures a clean environment for configuration.



13. Navigate to the duplicated folder: AVEVA PI Audit Reporter - PI Data Ingress - Instance 2 and delete folders Log and Temp.
14. Within the duplicated folder: AVEVA PI Audit Reporter - PI Data Ingress - Instance 2, navigate to the subdirectories Worker and Monitor and locate the file named: appsettings.json.
15. Open each appsettings.json file using a text editor (e.g., Notepad, Notepad++, Visual Studio Code).
16. Locate the entry corresponding to the service name. This may appear under a key such as "ServiceName" or similar.
17. Update the value to reflect the new instance name. For example: "ServiceName": "AVEVA PI Audit Reporter - PI Data Ingress - Instance 2".
18. Save and close the files after making the changes.

Note: Ensure the JSON structure remains valid after editing. Incorrect formatting may prevent the service from starting correctly.

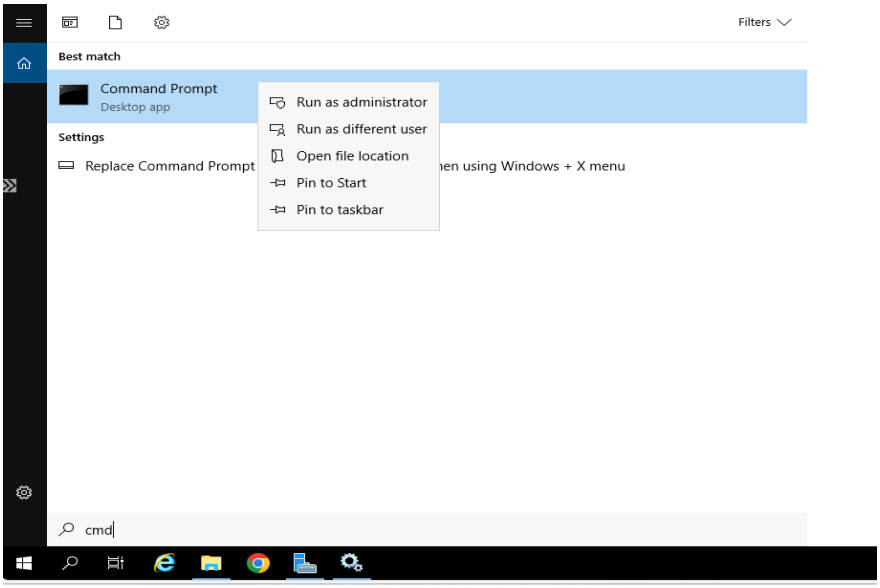




Register a new windows service for the duplicated instance

To create a new service for the duplicated AVEVA PI Audit Reporter - PI Data Ingress instance, follow the steps below:

1. Open Command Prompt as Administrator, selecting Start, type cmd, right-click Command Prompt, and select Run as administrator.



2. Create the register command using the following syntax:

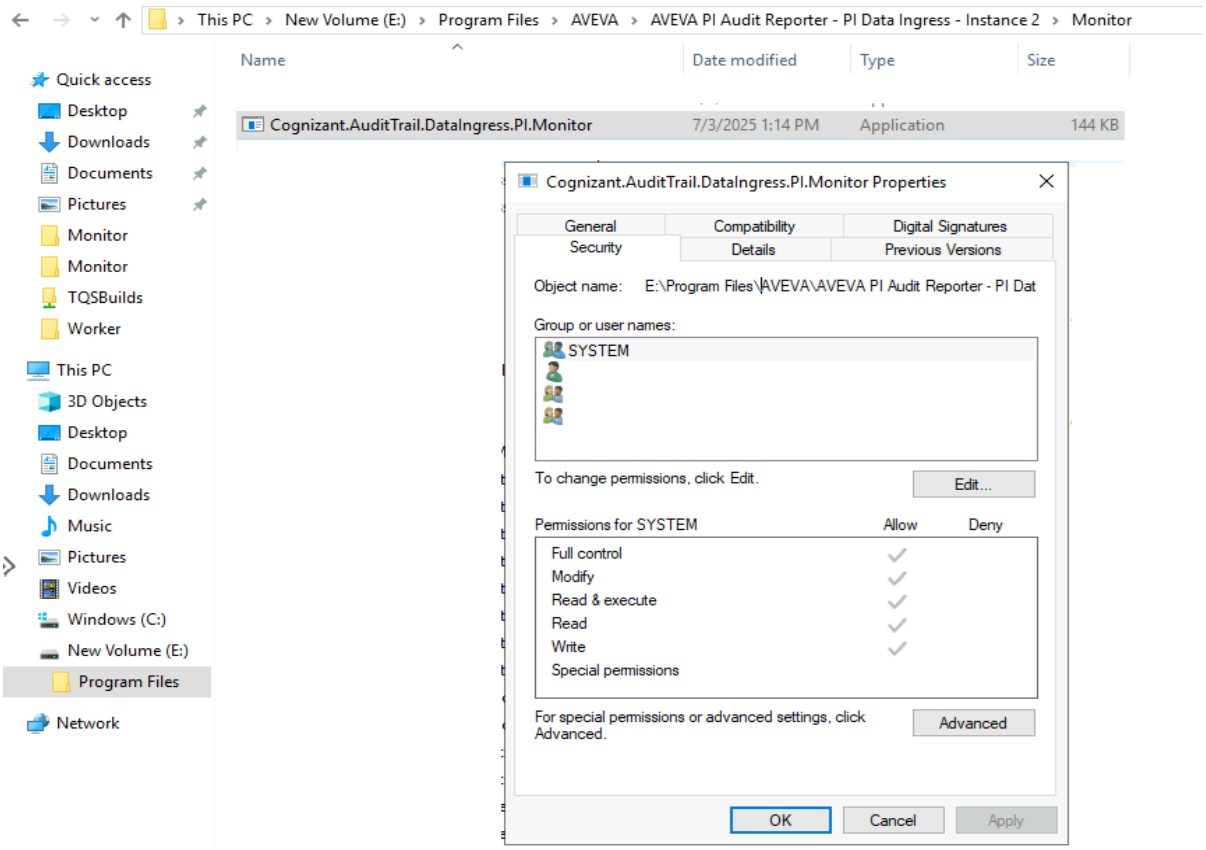
```
sc create "Service_Name_for_Instance_2" displayName=
"Display_Name_For_Service_Instance_2" binPath= "Full_Path_To_Monitor_Executable"
```

   a. Replace "Service_Name_for_Instance_2" with a unique internal name for the service (e.g., Cognizant.AuditTrail.DataIngress.PI.Monitor.Instance.2).

   b. Replace "Display_Name_For_Service_Instance_2" with a user-friendly name that will appear in the Services console (e.g., AVEVA PI Audit Reporter - PI Data Ingress Monitor - Instance 2).

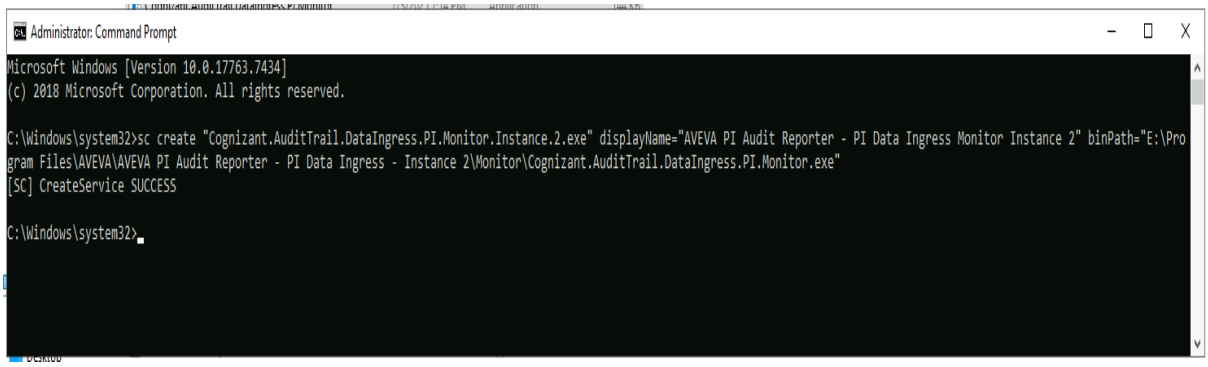
   c. Replace "Full_Path_To_Monitor_Executable" with the full path to the Monitor.exe file inside the duplicated folder.

   d. Full path of monitor executable file ‘Cognizant.AuditTrail.DataIngress.PI.Monitor’ can be found in Object name field in “Security” tab under file properties



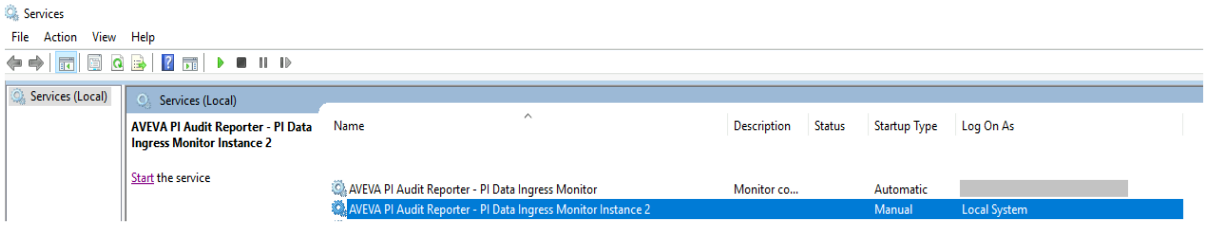
3. Run the sc create Command using the following syntax to register the new service:

```
sc create "Cognizant.AuditTrail.DataIngress.PI.Monitor.Instance.2.exe"
displayName="AVEVA PI Audit Reporter - PI Data Ingress Monitor Instance 2"
binPath="E:\Program Files\AVEVA\AVEVA PI Audit Reporter - PI Data Ingress -
Instance2\Monitor\Cognizant.AuditTrail.DataIngress.PI.Monitor.exe"
```

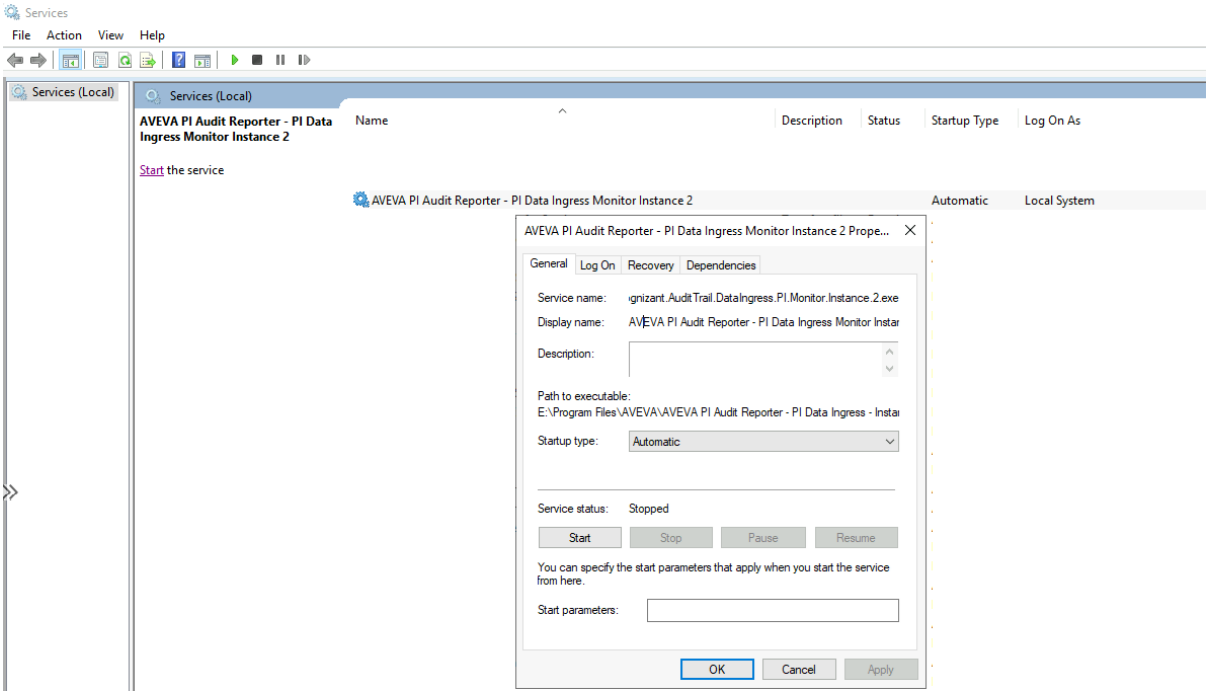


Note: Ensure the command parameters are matching with the environment where it is installed.

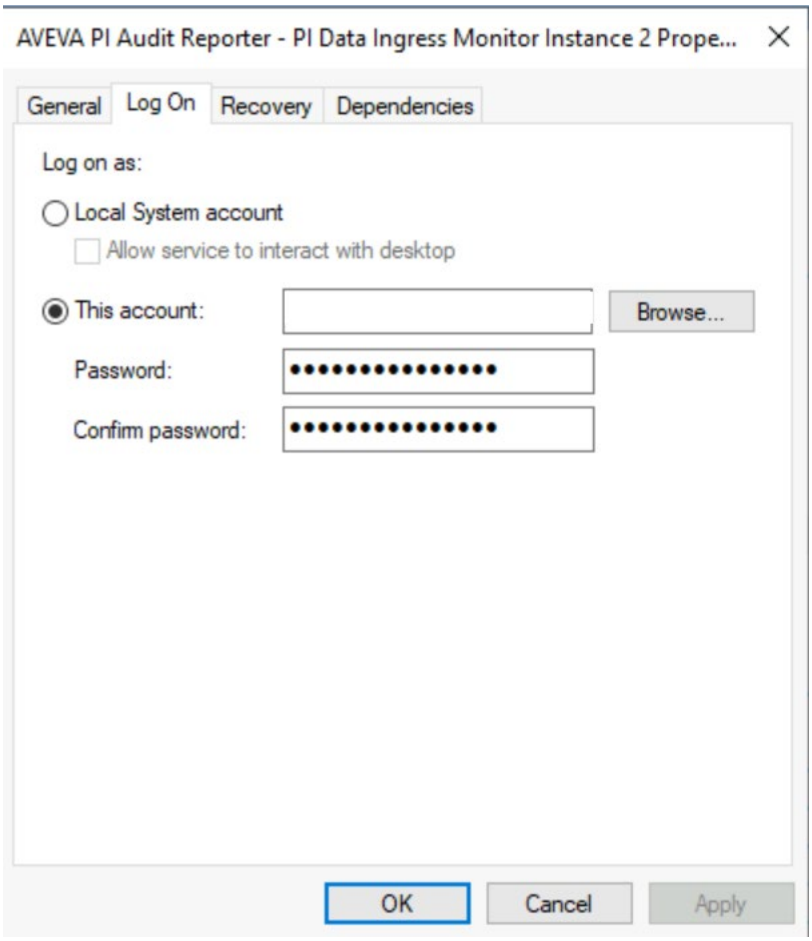
4. In the Windows Services list, scroll through or use the search function to locate the newly created service: AVEVA PI Audit Reporter - AF Data Ingress Monitor - Instance 2. Confirm that the service appears in the list and is available for manual start or automatic startup configuration.



5. Right-click the service and a context menu appears.
6. Select properties and on general screen change “Startup type” to “Automatic”.



7. Select the Log On tab to set up a custom service account for running the installed service.
8. Select the option This account. Use the "Browse..." button to select a user account from the directory.
9. Enter the password and confirm the password for the service account.
10. Select Apply to save the changes.
11. Select OK to close the window. Refer to the screenshot below to verify the settings.



Configure PI Interface in SQL Server

To complete the configuration for the PI interface, follow these steps using SQL Server Management Studio (SSMS).

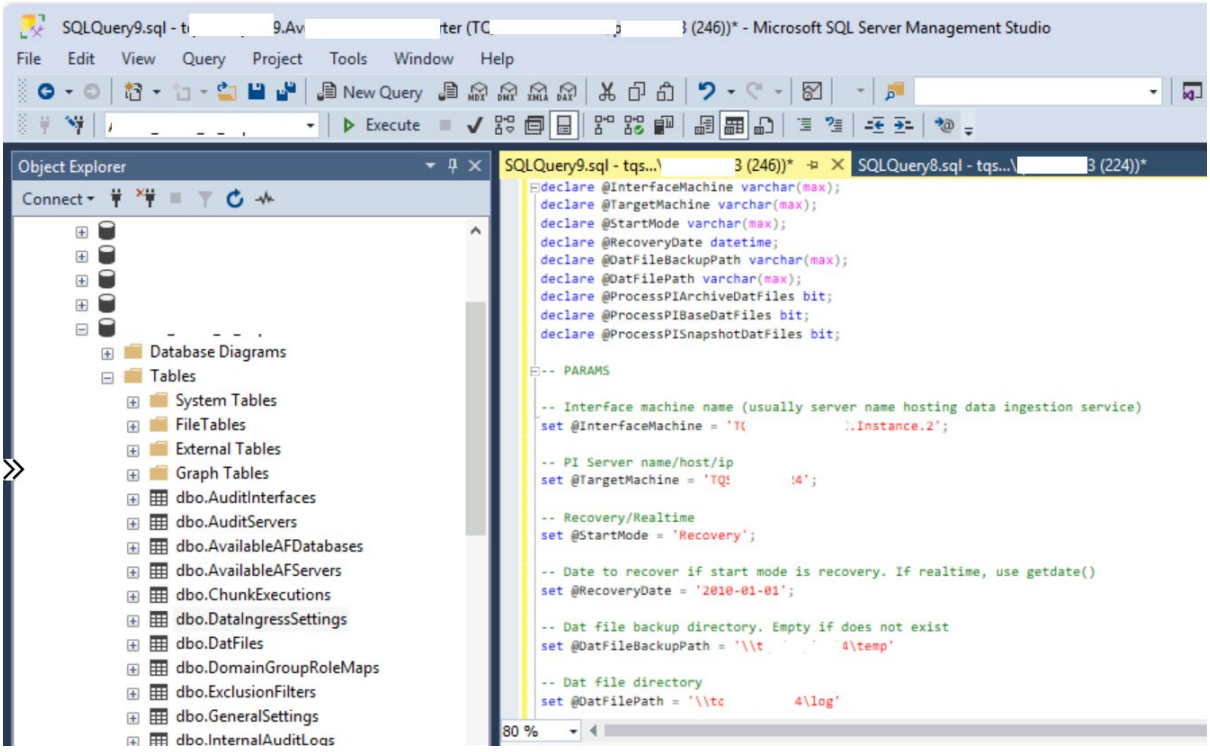
1. Launch SQL Server Management Studio and connect to the appropriate SQL Server instance.
2. In the Object Explorer, expand the Databases node and select the database currently used by the application.
3. Select New Query in the toolbar to open a new SQL query window.
4. Execute the following SQL script to include the PI interface:

```
declare @InterfaceMachine varchar(max);
declare @TargetMachine varchar(max);
declare @StartMode varchar(max);
declare @RecoveryDate datetime;
declare @DatFileBackupPath varchar(max);
declare @DatFilePath varchar(max);
declare @ProcessPIArchiveDatFiles bit;
declare @ProcessPIBaseDatFiles bit;
declare @ProcessPISnapshotDatFiles bit;
-- PARAMS
-- Interface machine name (usually server name hosting data ingestion service)
```

```
set @InterfaceMachine = 'Interface_Machine_Name.Interface.2';
-- PI Server name/host/ip
set @TargetMachine = 'Target_Machine';
-- Recovery/Realtime
set @StartMode = 'Recovery';
-- Date to recover if start mode is recovery. If realtime, use getdate()
set @RecoveryDate = 'Recovery_Start_Date';
-- Dat file backup directory. Empty if does not exist
set @DatFileBackupPath = 'Dat_File_Backup_Directory'
-- Dat file directory
set @DatFilePath = 'Dat_File_Directory'
-- Flag that indicates if interface will process pi archive audit database files (.dat)
set @ProcessPIArchiveDatFiles = 1;
-- Flag that indicates if interface will process pi base audit database files (.dat)
set @ProcessPIBaseDatFiles = 1;
-- Flag that indicates if interface will process pi snapshot audit database files (.dat)
set @ProcessPISnapshotDatFiles = 1;
-- PARAMS
IF
NOT EXISTS (
    SELECT 1
    FROM [dbo].[AuditServers]
    WHERE [Type] = N'PI' AND [InterfaceMachine] = @InterfaceMachine AND [TargetMachine]
= @TargetMachine
)
BEGIN
      INSERT [dbo].[AuditServers]
([Type],[TargetMachine],[InterfaceMachine],[AFIncludeAllDatabases],[StartMode],[Rec
overyDate],[RealtimeStartDate])
      VALUES ('PI', @TargetMachine, @InterfaceMachine,
0,@StartMode,@RecoveryDate,CONVERT(DATETIME2(0), GETDATE()));
END
ELSE
BEGIN
      print 'There is an audit server already configured for PI Server ' + @TargetMachine
+ ' and interface ' + @InterfaceMachine;
END
IF NOT EXISTS (
    SELECT 1
    FROM [dbo].[AuditInterfaces]
    WHERE [Type] = N'PI' AND [InterfaceMachine] = @InterfaceMachine AND [TargetMachine]
= @TargetMachine
)
BEGIN
    INSERT [dbo].[AuditInterfaces]
      ([AuditServerID],
       [Type],                                [InterfaceMachine],
[TargetMachine],
       [TargetDatabase],                      [TargetDatabaseGUID],
[DatabaseEnabled],
       [StartMode],                           [RecoveryDate],
[RealtimeStartDate],
       [ProcessedRecoveryCount],              [ProcessedRecoveryMaxDate],
[ProcessedRealtimeCount],
       [ProcessedRealtimeMaxDate],            [TotalRecords],
[BackupFilesDirectory],
```

```
       [AuditDatFilesDirectory],                [ProcessArchiveAuditSubsystem],
[ProcessSnapshotAuditSubsystem],
       [ProcessBaseAuditSubsystem],             [CurrentDatFile],
[ExclusionFilterStatus],
       [BackupFilesCopied],                     [Summary])
 VALUES
      ((SELECT ID FROM [dbo].[AuditServers] WHERE [Type] = N'PI' AND [InterfaceMachine]
= @InterfaceMachine AND [TargetMachine] = @TargetMachine),
      'PI',                                                  @InterfaceMachine,
                        @TargetMachine,
       NULL,                                                       NULL,
                              1,
       @StartMode,                                            @RecoveryDate,
                        CONVERT(DATETIME2(0), GETDATE()),
       0,                                                     CONVERT(DATETIME2(0),
GETDATE()), 0,
       CONVERT(DATETIME2(0), GETDATE()),       0,
                  @DatFileBackupPath,
       @DatFilePath,
      @ProcessPIArchiveDatFiles,          @ProcessPISnapshotDatFiles,
       @ProcessPIBaseDatFiles,                NULL,
            NULL,
       0,                                          NULL);
END
ELSE
BEGIN
      print 'There is an audit interface already configured for PI Server ' +
@TargetMachine + ' and interface ' + @InterfaceMachine;
END
```

5. Refer to the screenshot below to verify the query in MSSQL.



6. Select New Query in the toolbar to open a new SQL query window to replicate data ingress settings for new interface service.

7. Execute the following SQL query, updating the placeholder values as needed to reflect the new instance configuration:

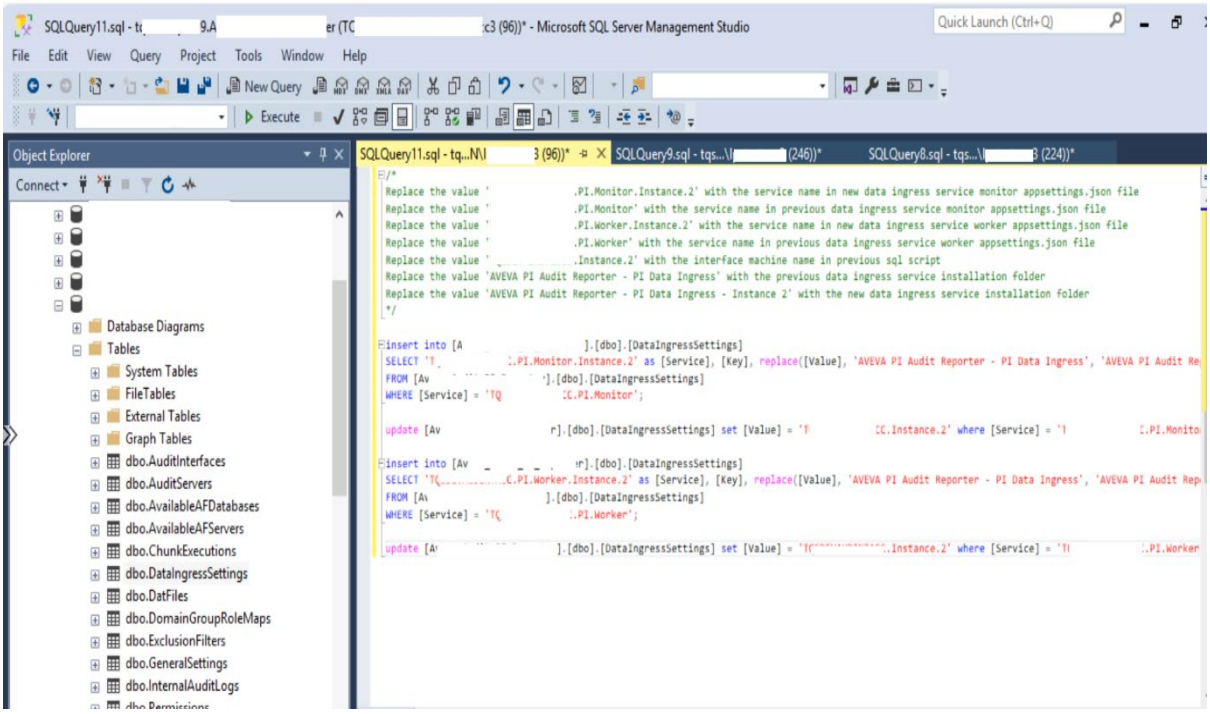
```
insert into [Database_Name].[dbo].[DataIngressSettings]
SELECT 'Interface_Name.PI.Monitor.Instance.2' as [Service], [Key], replace([Value],
'AVEVA PI Audit Reporter - PI Data Ingress', 'AVEVA PI Audit Reporter - PI Data Ingress
- Instance 2') as [Value]
FROM [Database_Name].[dbo].[DataIngressSettings]
WHERE [Service] = ' Interface_Name.PI.Monitor';

update [Database_Name].[dbo].[DataIngressSettings] set [Value] = '
Interface_Name.PI.Monitor' where [Service] = ' Interface_Name.PI.Monitor.Instance.2'
and [Key] = 'AppSettings:InterfaceMachine';

insert into [Database_Name].[dbo].[DataIngressSettings]
SELECT ' Interface_Name.PI.Worker.Instance.2' as [Service], [Key], replace([Value],
'AVEVA PI Audit Reporter - PI Data Ingress', 'AVEVA PI Audit Reporter - PI Data Ingress
- Instance 2') as [Value]
FROM [Database_Name].[dbo].[DataIngressSettings]
WHERE [Service] = ' Interface_Name.PI.Worker';

update [Database_Name].[dbo].[DataIngressSettings] set [Value] = '
Interface_Name.PI.Worker' where [Service] = ' Interface_Name.PI.Worker.Instance.2' and
[Key] = 'AppSettings:InterfaceMachine';
```

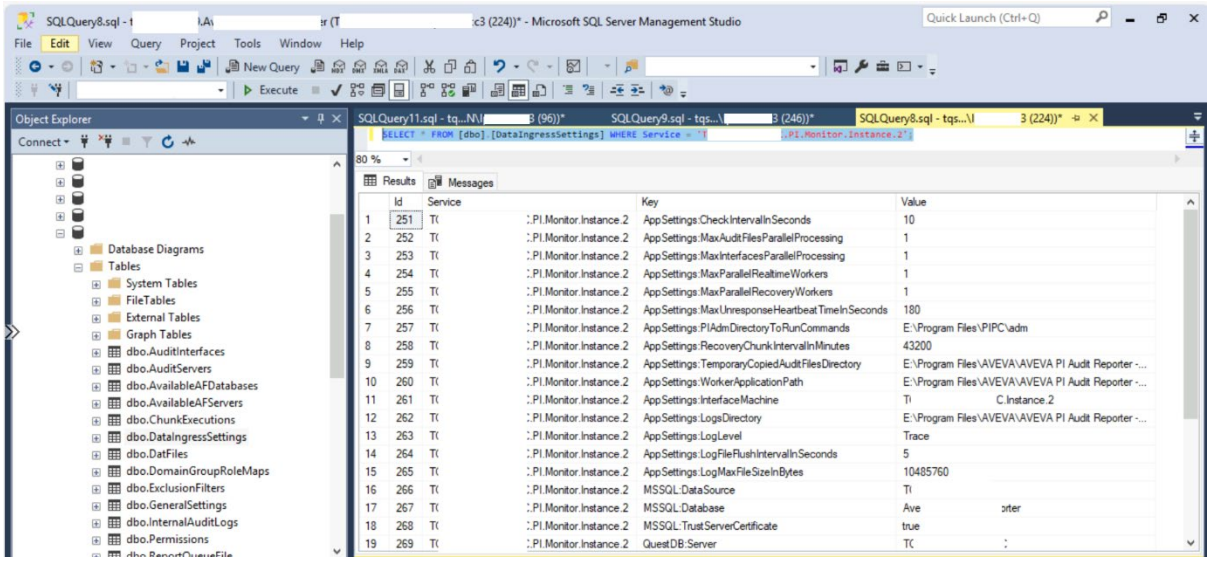
8. Refer to the screenshot below to verify the query in MSSQL.



9. Verify Replicated Settings in the DataIngressSettings table by running following sql query (for example):

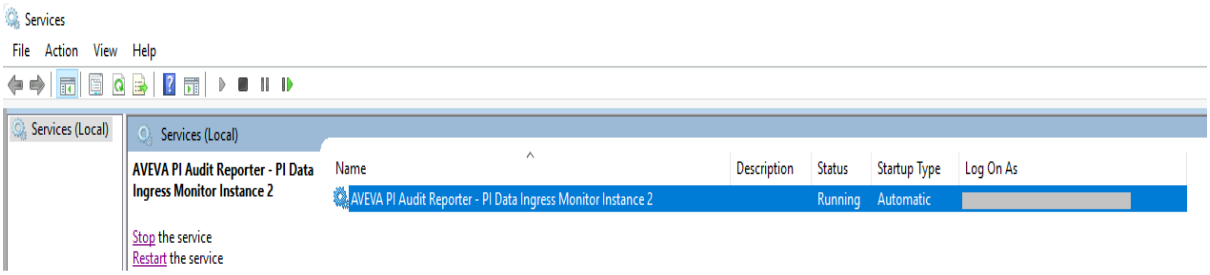
```
SELECT * FROM [dbo].[DataIngressSettings] WHERE Service =
'Interface_machine_name.PI.Monitor.Instance.2';
```

10. Review the results to ensure that all expected configuration parameters for the new interface instance are present and correctly populated.

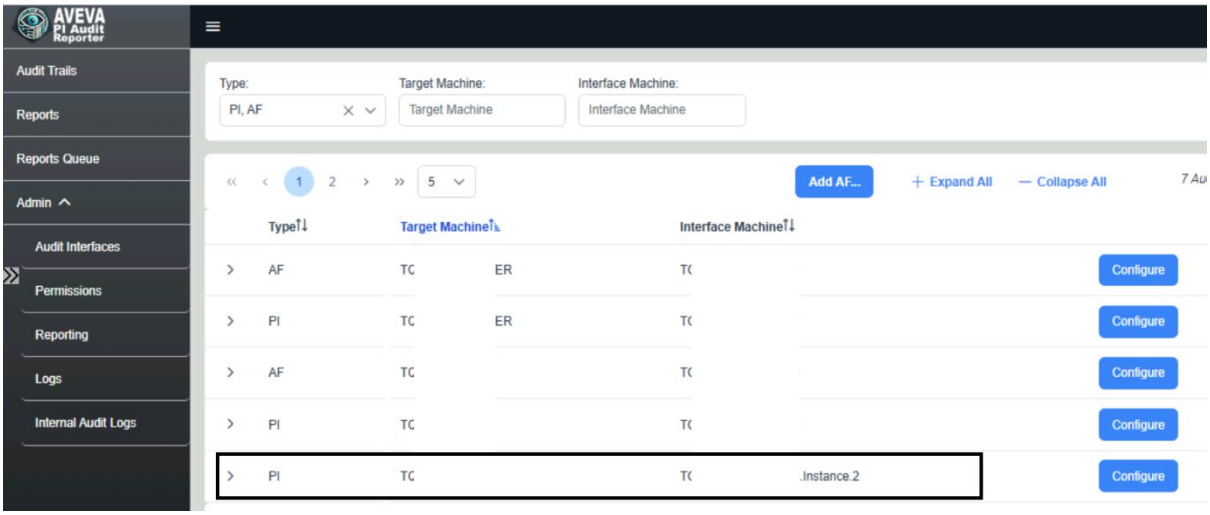


Note: All existent settings from original service instance must be in the duplicated one. Please refer to the configuration settings in Chapter 5.

11. Once the service has been successfully created and its configuration settings replicated:
12. Locate the newly created service: AVEVA PI Audit Reporter - PI Data Ingress Monitor - Instance 2.
13. Right-click the service and select Start.
14. Monitor the service status to ensure it transitions to running without errors.



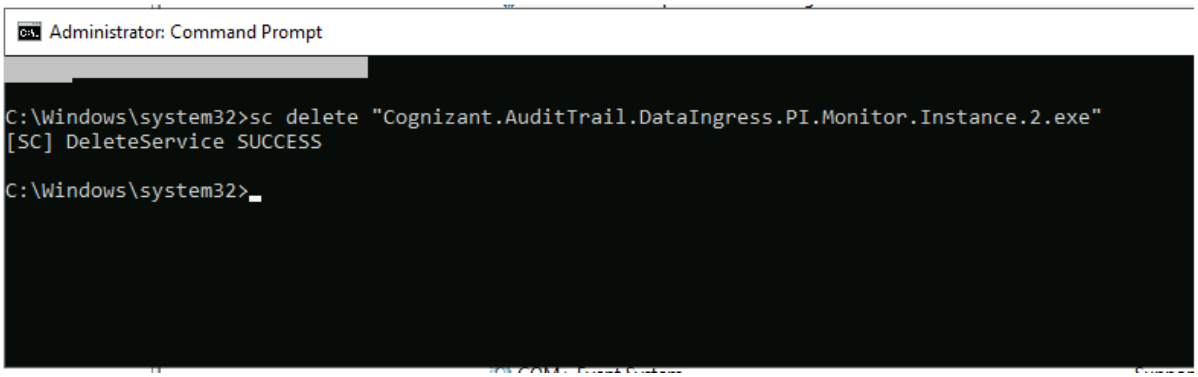
15. To Confirm New PI Interface added in the AVEVA PI Audit Reporter, select Admin, Audit Interfaces.



Delete a service instance from the System

To remove the previously created service from the system:

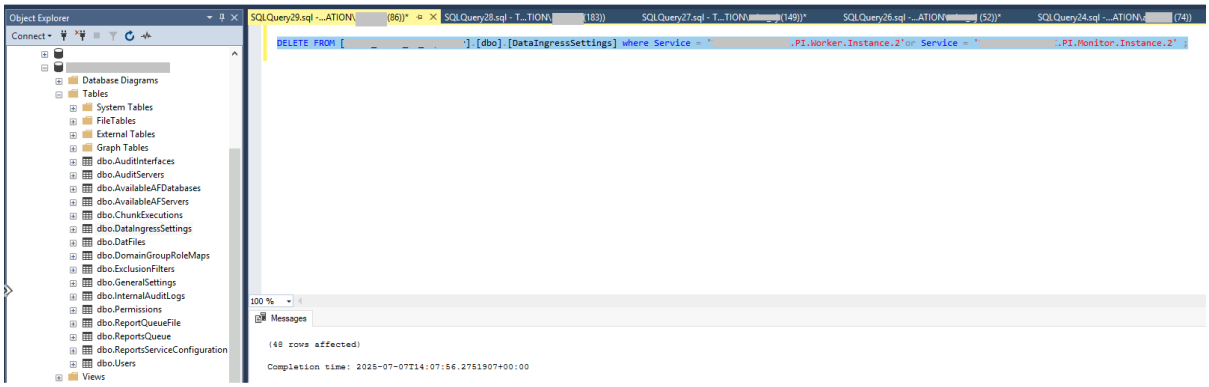
1. Stop the Service:
    a. Open the Services Management Console (services.msc).
    b. Locate the service (e.g., AVEVA PI Audit Reporter - PI Data Ingress Monitor - Instance 2).
    c. Right-click the service and select Stop.
2. Open Command Prompt as Administrator:
    a. Select Start, type cmd, right-click Command Prompt, and select Run as administrator.
3. Run the Following Commands to Delete the Service:
    a. sc delete "Service_Name".
    b. Replace "Service_Name" with the actual internal name of the service (e.g., sc delete "Cognizant.AuditTrail.DataIngress.PI.Monitor.Instance.2.exe").



Note: After deleting the Windows service, remove all associated configuration records from the database to ensure clean decommissioning of the interface.

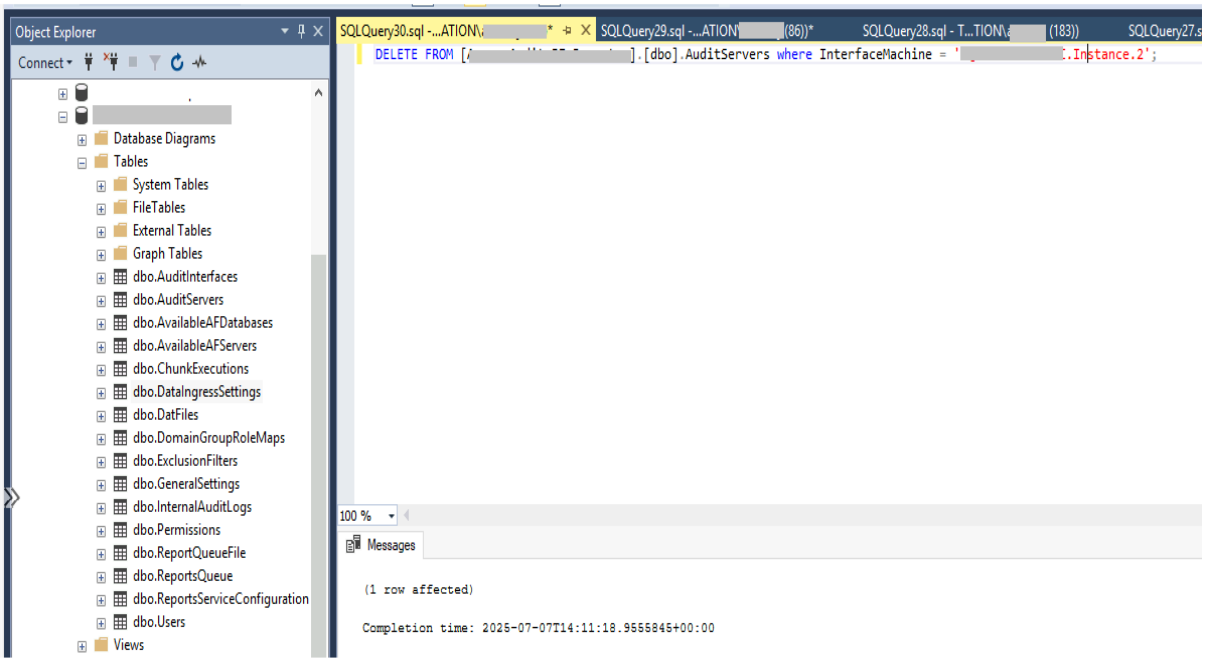
4. Delete DataIngresSettings table for newly added interface with below command:

```
DELETE FROM [Database_Name].[dbo].[DataIngressSettings] where Service =
'Interface_Server.PI.Worker.Instance.2' or Service =
'Interface_server.PI.Monitor.Instance.2'
```



5. Delete audit servers for newly added interface with below command:

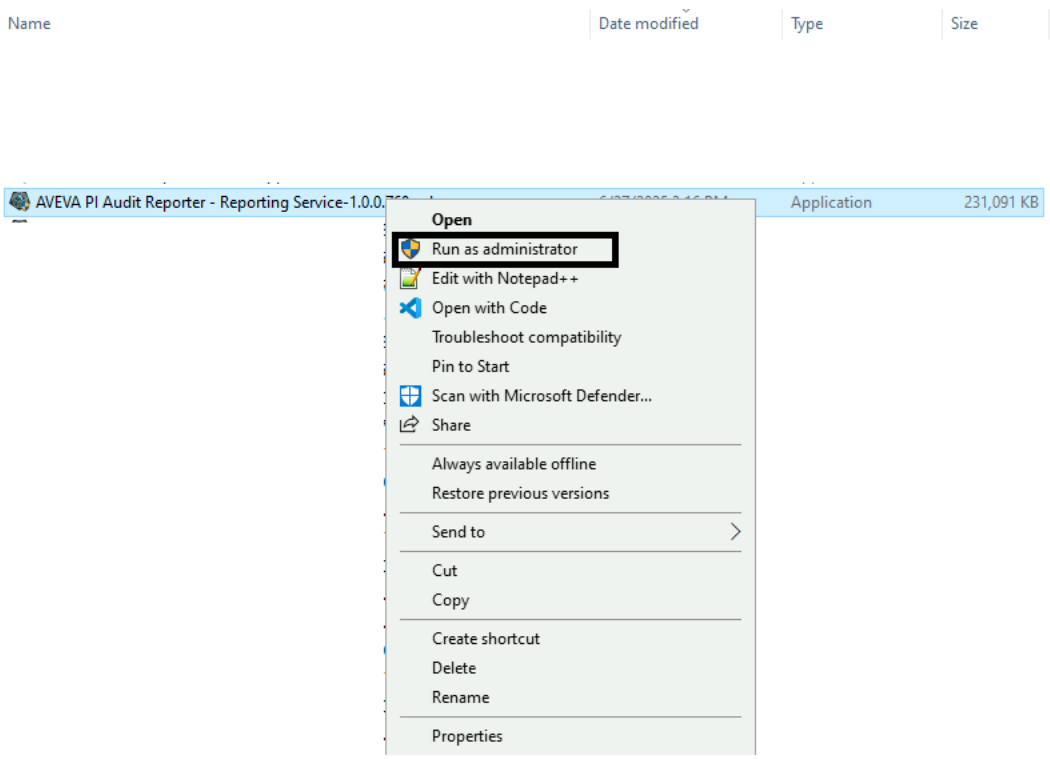
```
DELETE FROM [Database_Table].[dbo].AuditServers where InterfaceMachine =
Interface_server.Instance.2'
```



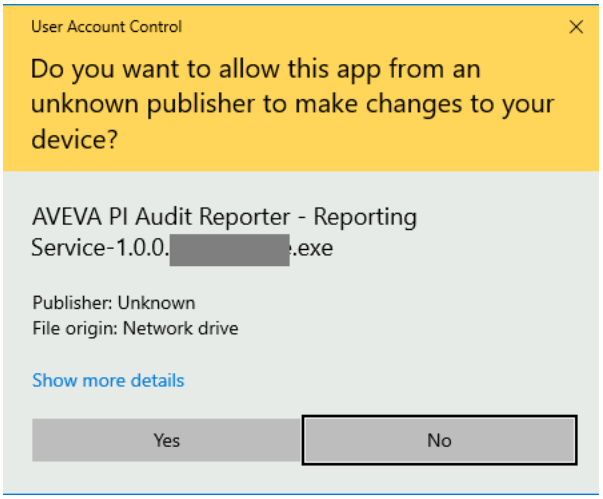
Install AVEVA PI Audit Reporter - Reporting Services

To install the AVEVA PI Audit Reporter - Reporting Service, follow the steps below:

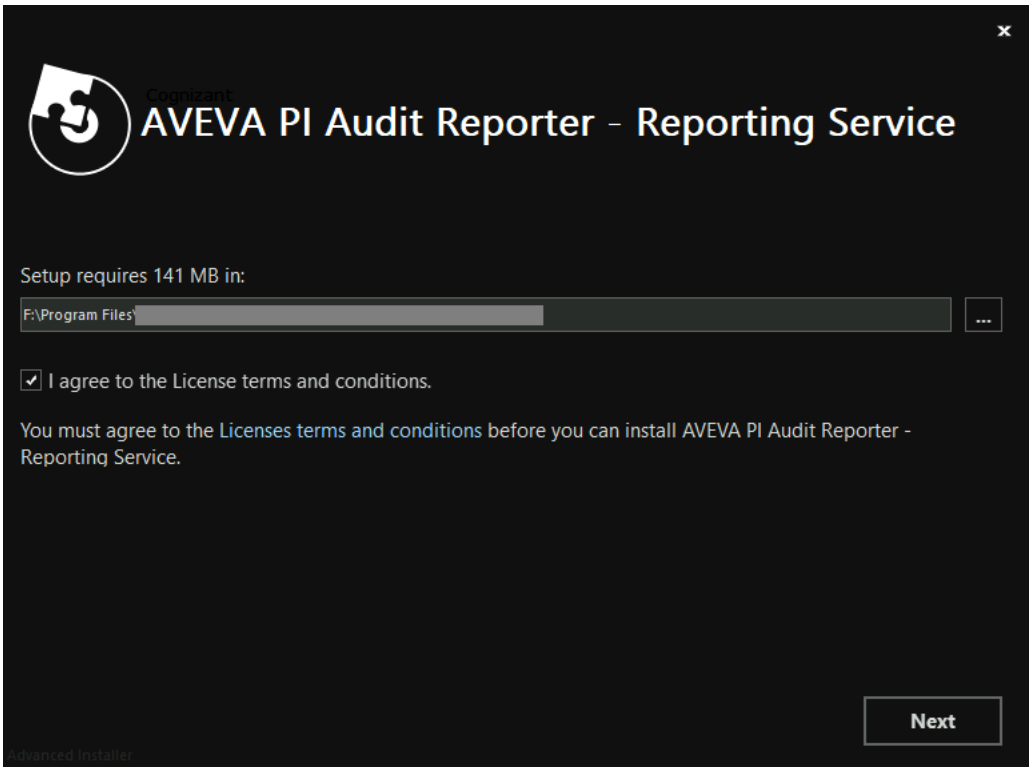
1. Locate and right-click the provided installer file AVEVA PI Audit Reporter - PI Data Ingress-1.0.0.xxx_release.exe.
2. Select “Run as administrator” (required) from the context menu as shown below.



3. When the installer is launched, a User Account Control (UAC) prompt as shown below will appear with the following message: “Do you want to allow this app from an unknown publisher to make changes to your device?”. Select “Yes” to proceed with the installation.



4. After accepting the User Account Control prompt, the installer proceeds to the File Location Setup screen as shown below. Select the ellipsis button ([...]) to open the folder browser.
5. Select the desired directory where the user wants to install the AVEVA PI Audit Reporter - Reporting Service.
6. Once the installation path is selected, check the box labeled: “I agree to the License terms and conditions”.
7. Select Next to continue with the installation.



8. The next screen in the setup process is “Configure SQL Connection”.
9. Enter the SQL Server Name and select the appropriate Database options.
10. It is strongly recommended to use a Trusted Connection, as all services will be configured to run under a single service account.

11. Once all fields are completed, if the user Selects “Test SQL Connection” to verify connectivity, a “Connection successful” message will be displayed if the configuration is correct.
12. Once all fields are completed, select Install to begin the installation process.

13. Once complete, a confirmation message displays: “AVEVA PI Audit Reporter - Reporting Service has been successfully installed.” This indicates that the application has been installed correctly and is ready for use. Select Finish to exit the installer.

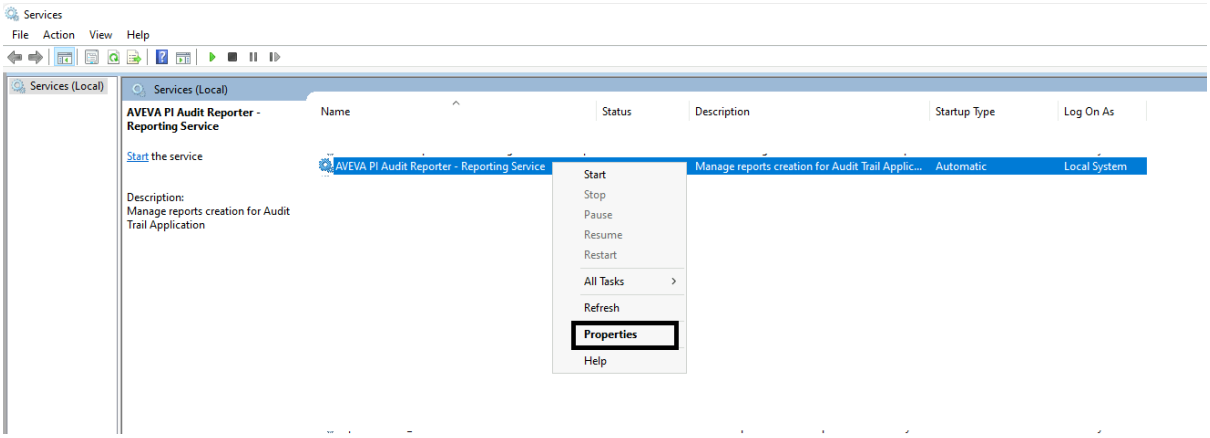
How to cancel the installation

To cancel the installation, select the (×) in the upper-right corner or Select cancel button. A confirmation dialog appears, prompting the user to confirm or abort the cancellation. Select Yes to confirm. Refer to the screenshot below to verify the settings.

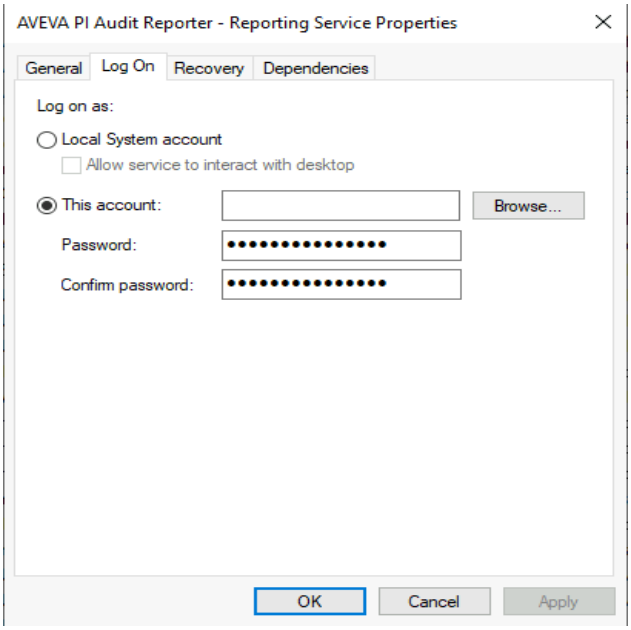
Set the Service Account

To set up a custom service account for running the installed service, update the service Log On tab as follows:

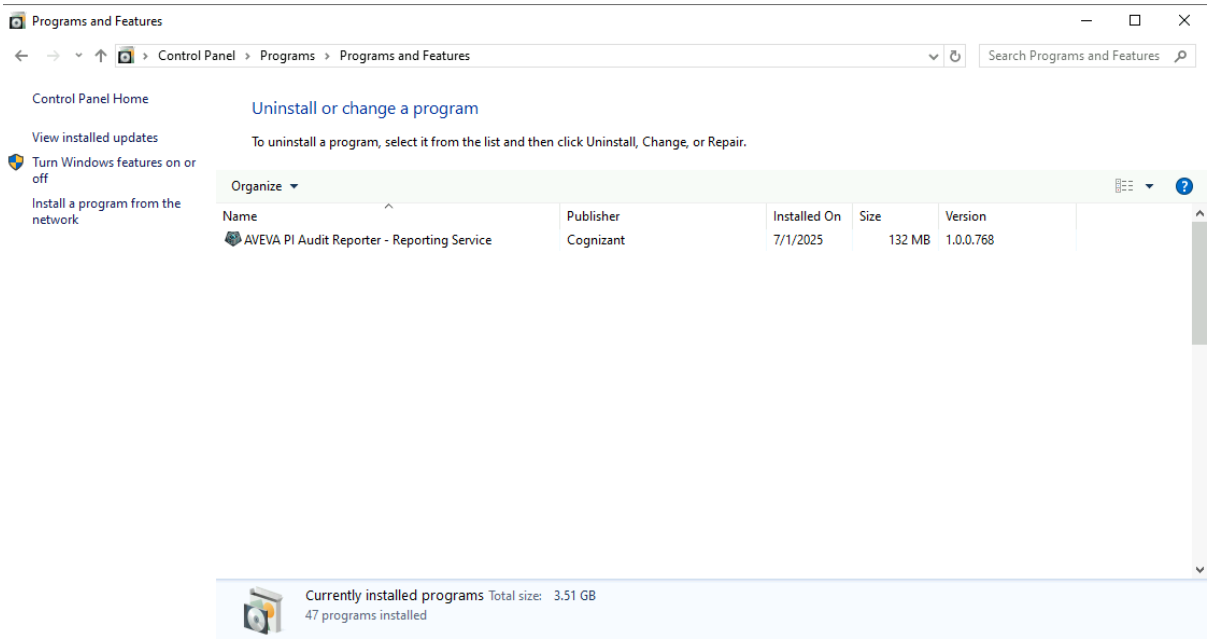
1. Open Services from the Start menu and scroll down to find the AVEVA PI Audit Reporter - Reporting service.



2. Right-click the service and select properties.
3. In the Properties window of the service, select the Log On tab.
4. Select the option “This account” and then "Browse..." to select a user account from the directory.
5. Enter the password and confirm the password for the service account.
6. Select Apply to save the changes.
7. Select OK to close the window. Refer to the screenshot below to verify the settings.



8. After a successful installation, the AVEVA PI Audit Reporter - Reporting Service will be listed under Programs and Features in the Windows Control Panel.



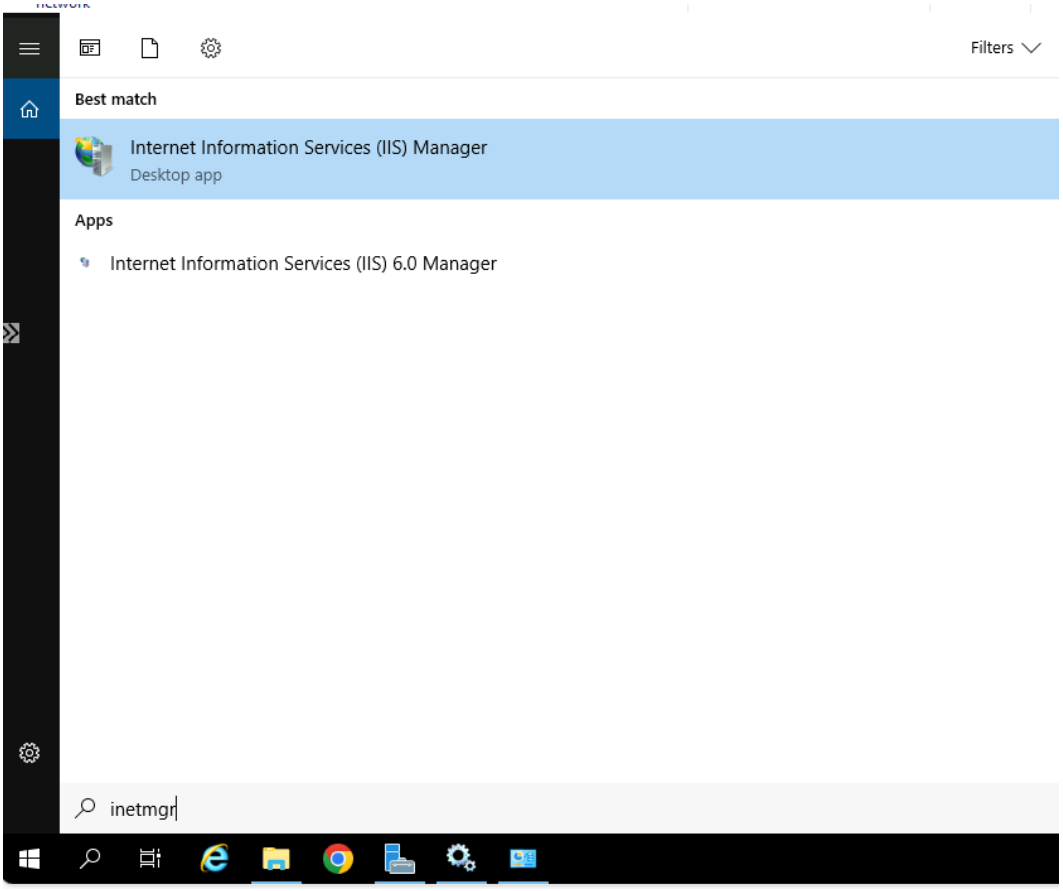
Internet Information Services (IIS) manager

On the Internet Information Services (IIS) Manager screen, users can view both Application Pools and Sites, which display hosted websites and related web content. To make any configuration changes within IIS, administrator privileges are required.

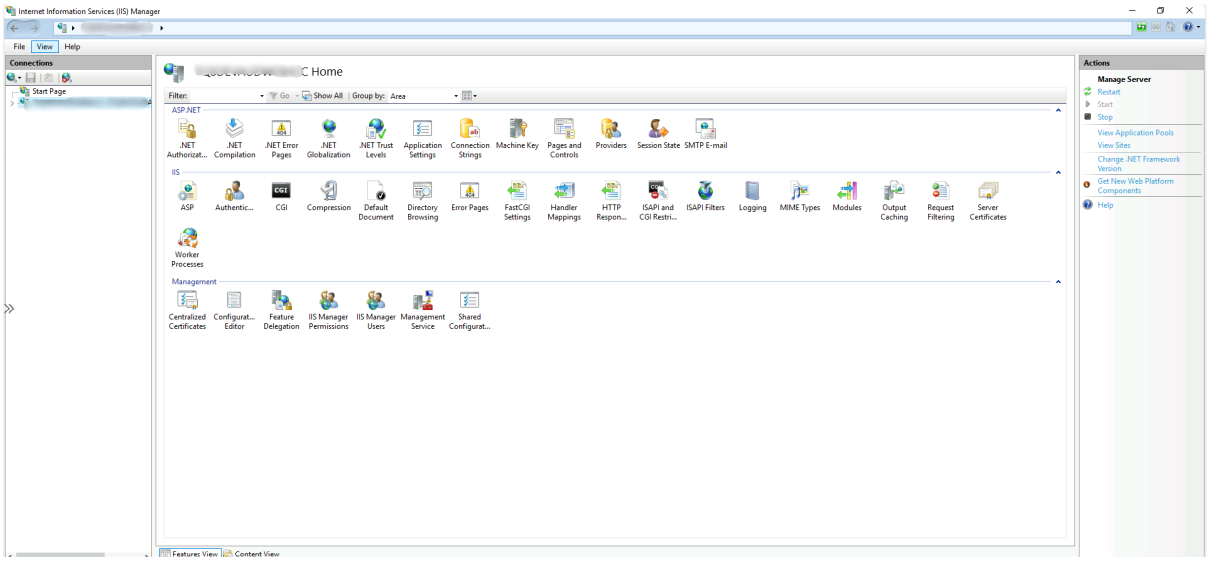
Authentication

To configure the IIS server to use Windows Authentication exclusively—disabling all other authentication methods—follow the steps outlined below:

1. Open IIS Manager by going to the Start menu and type “inetmgr” in the search bar. Press Enter, and the Internet Information Services (IIS) Manager window will open.

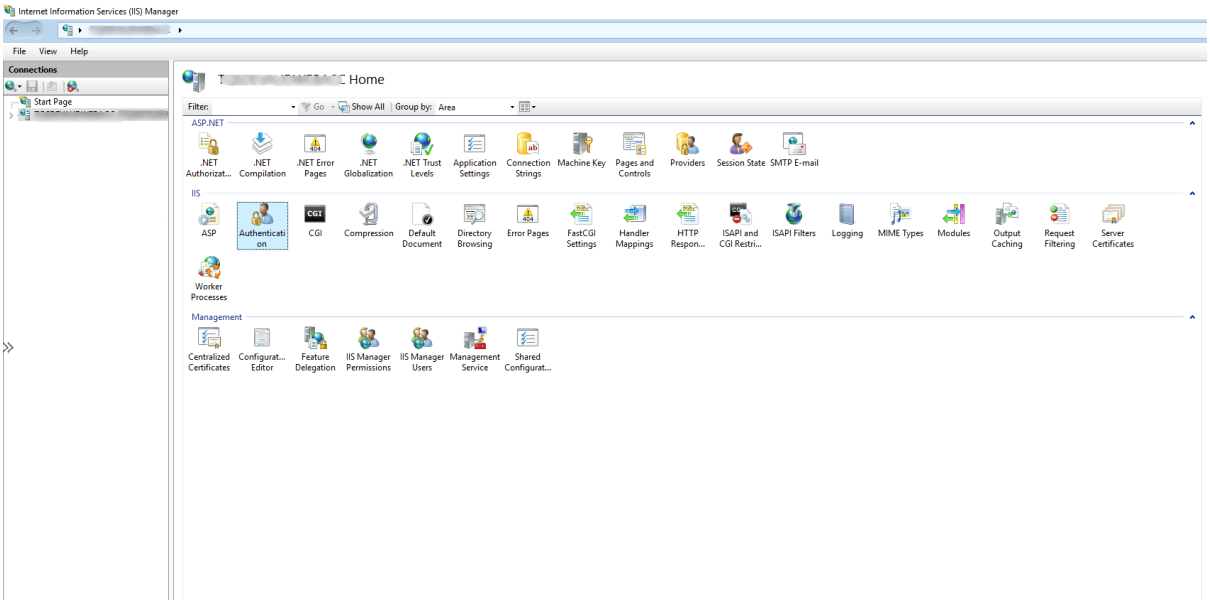


Select the server’s name listed in the left-hand Connections panel—it appears directly beneath Start Page. This opens the server-level configuration options in IIS Manager.

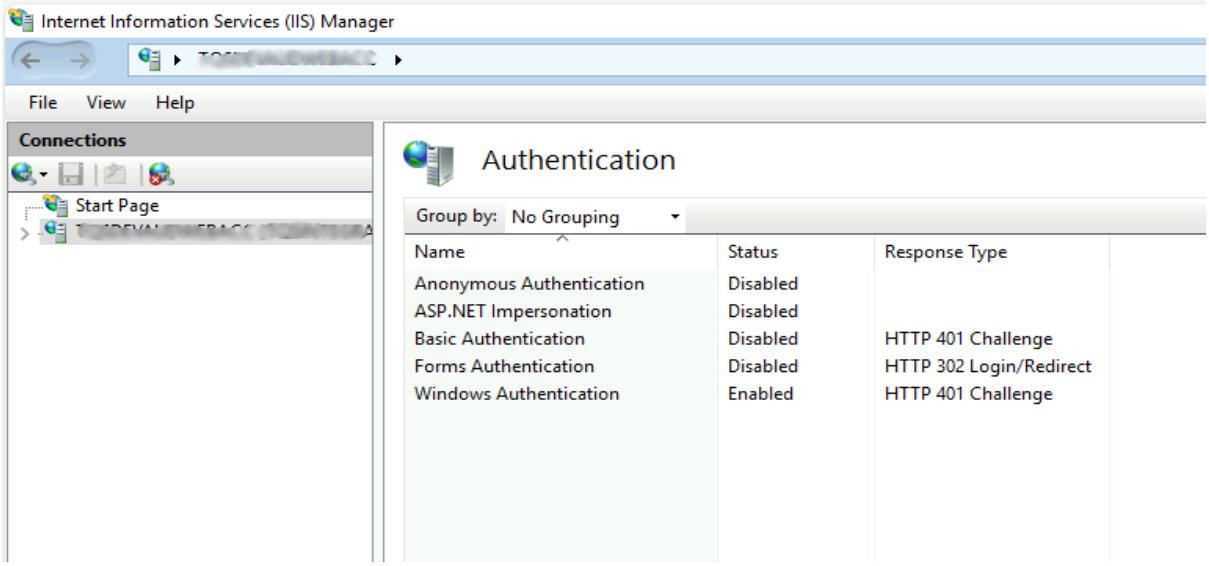


In the right-hand panel of IIS Manager, locate the IIS section and double-click Authentication. This opens a screen displaying all available authentication methods for the IIS Web Server.

To configure authentication for the AVEVA PI Audit Reporter website right-click Windows Authentication and enable.



Disable all other authentication methods with a right-click. This ensures that the AVEVA PI Audit Reporter website uses Windows Authentication exclusively.

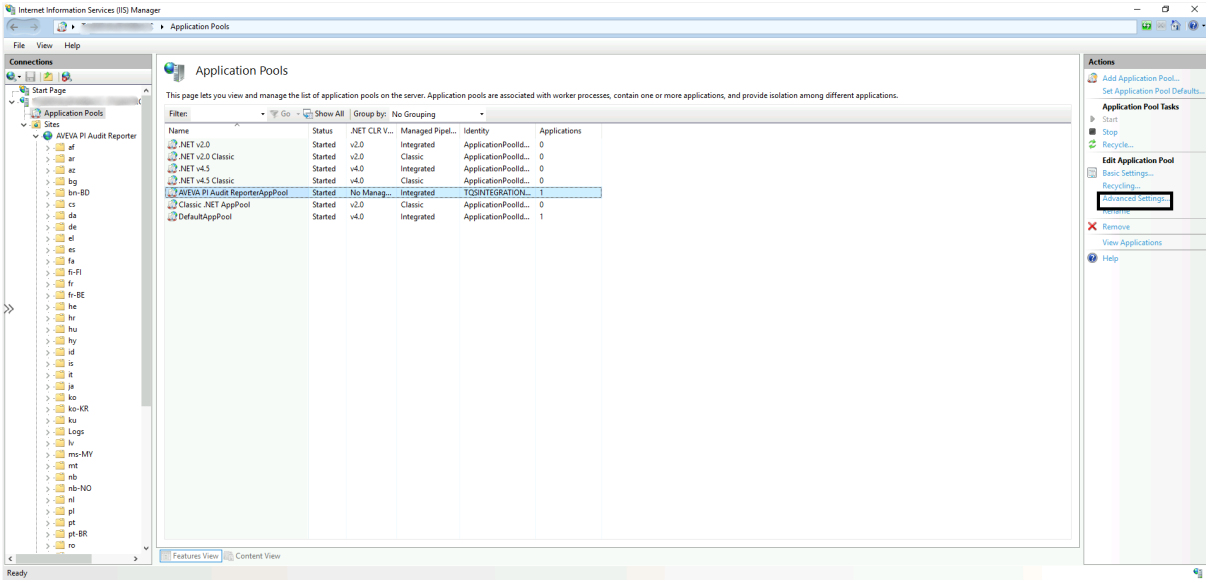


Note: If Administrator is unable to modify authentication settings at the server level, administrator user can configure them directly within the AVEVA PI Audit Reporter website settings. However, in this case, Windows Authentication must be manually enabled after each installation of the web application.

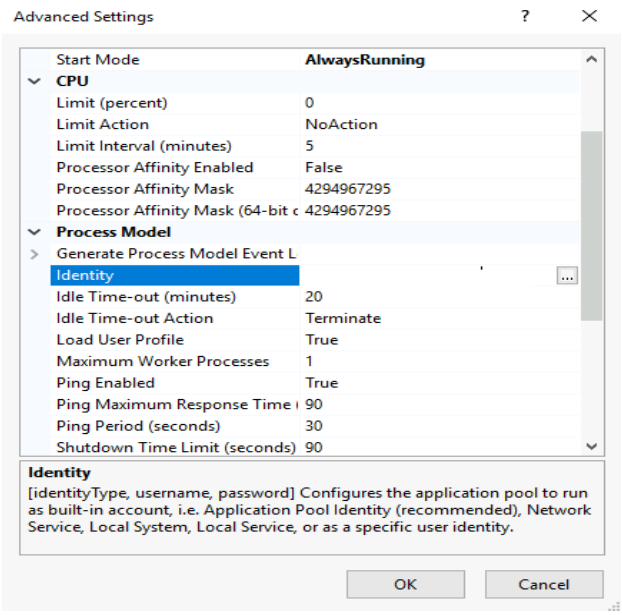
Application Pool

To configure the application pool to run under a domain account follow these steps:

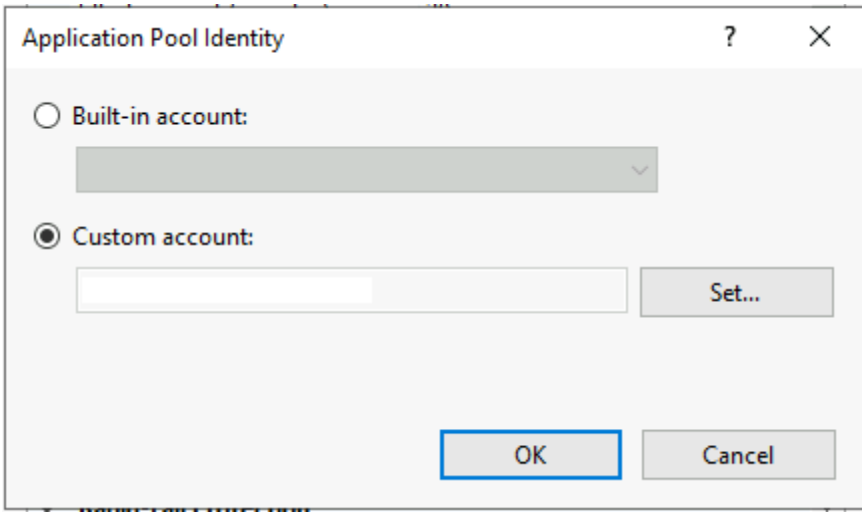
1. In the left-hand Connections panel, select Application Pools under the server's name.
2. The list of application pools will appear in the center pane.
3. Locate and select the AVEVA PI Audit Reporter application pool.
4. In the Actions pane on the right, select Advanced Settings as shown below.



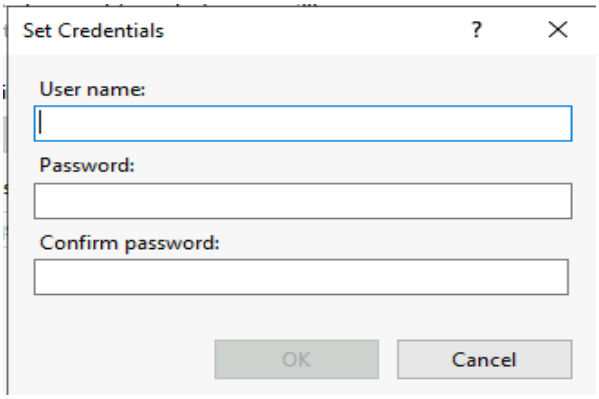
5. In the Advanced Settings window, find the “Identity” property under the Process Model section. Select the ellipsis (…) button next to Identity, then choose Custom account as shown below.



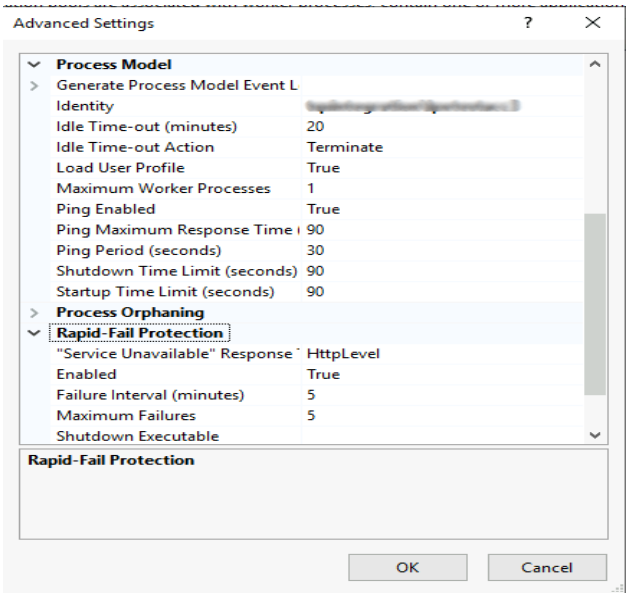
6. Select “Set” and enter the domain username, password and confirm password for the account under which the application pool will run.



7. Select OK to apply the changes.



8. In the same advanced settings screen, use the configuration settings below.



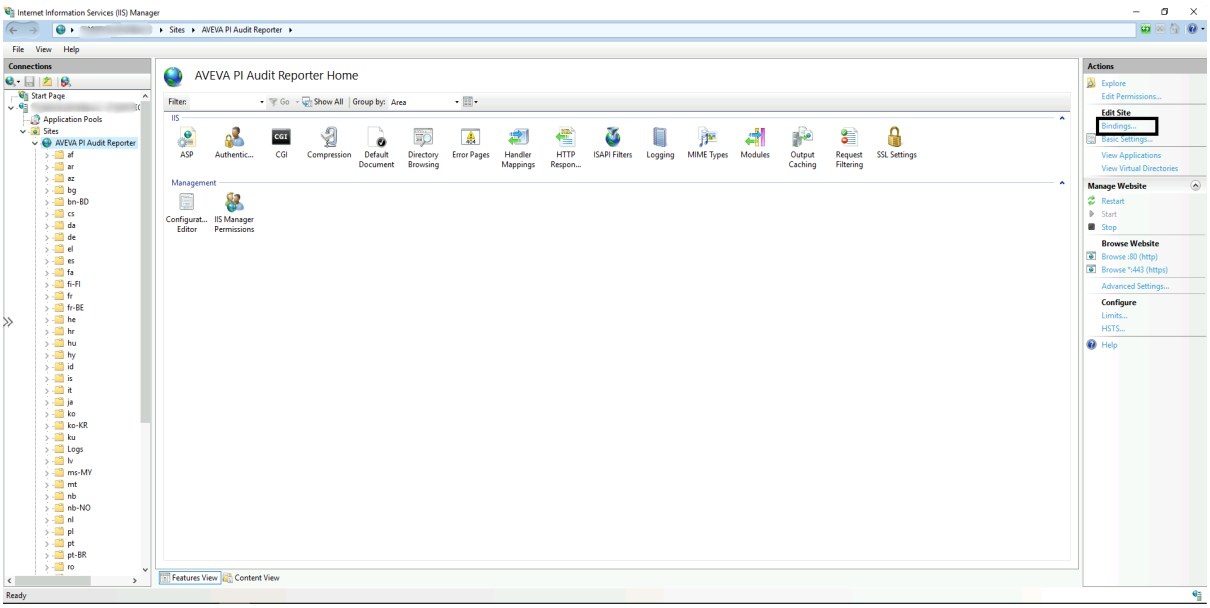
SSL – Secure Sockets Layer

The AVEVA PI Audit Reporter application employs SSL (Secure Sockets Layer) to protect communication between its microservices and the web application. This security layer offers several important advantages:

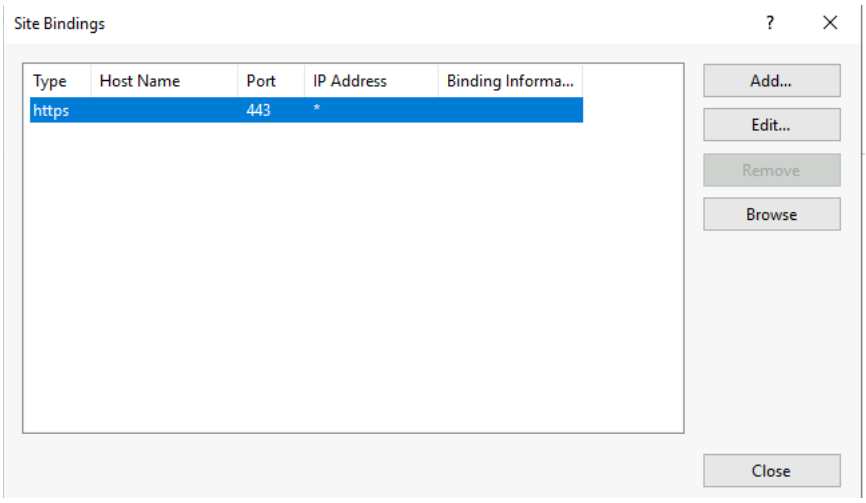
- Encrypted Communication
  SSL encrypts data in transit, ensuring that sensitive information remains confidential and protected from unauthorized access or interception.
- Data Integrity
  It safeguards the accuracy and consistency of data by preventing tampering or corruption during transmission.
- Authentication
  SSL verifies the identity of connected parties, helping to establish trust and prevent impersonation or man-in-the-middle attacks.
- Secure and Trusted Connections
  By enabling SSL, the system ensures that all communications occur over a secure and verified channel, enhancing overall system security and compliance.

To bind the SSL Certificate for the AVEVA PI Audit Reporter site in the IIS, perform the following steps:

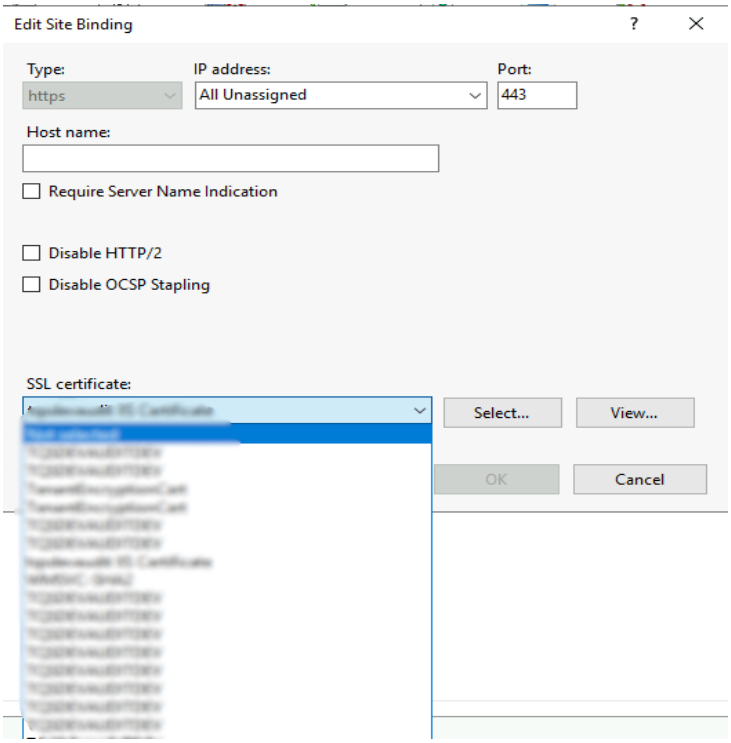
1. Select the Sites -> AVEVA PI Audit Reporter and in the right panel select on “Bindings”.



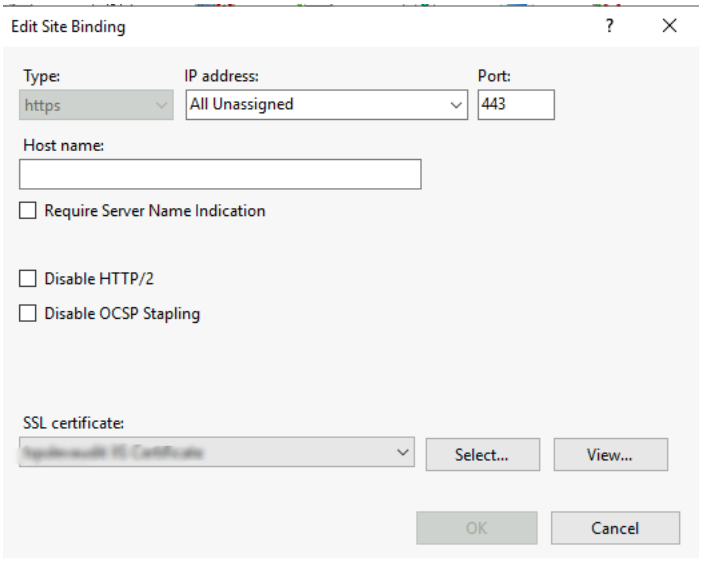
2. Select the existing Site binding and select ‘Edit’ Button.



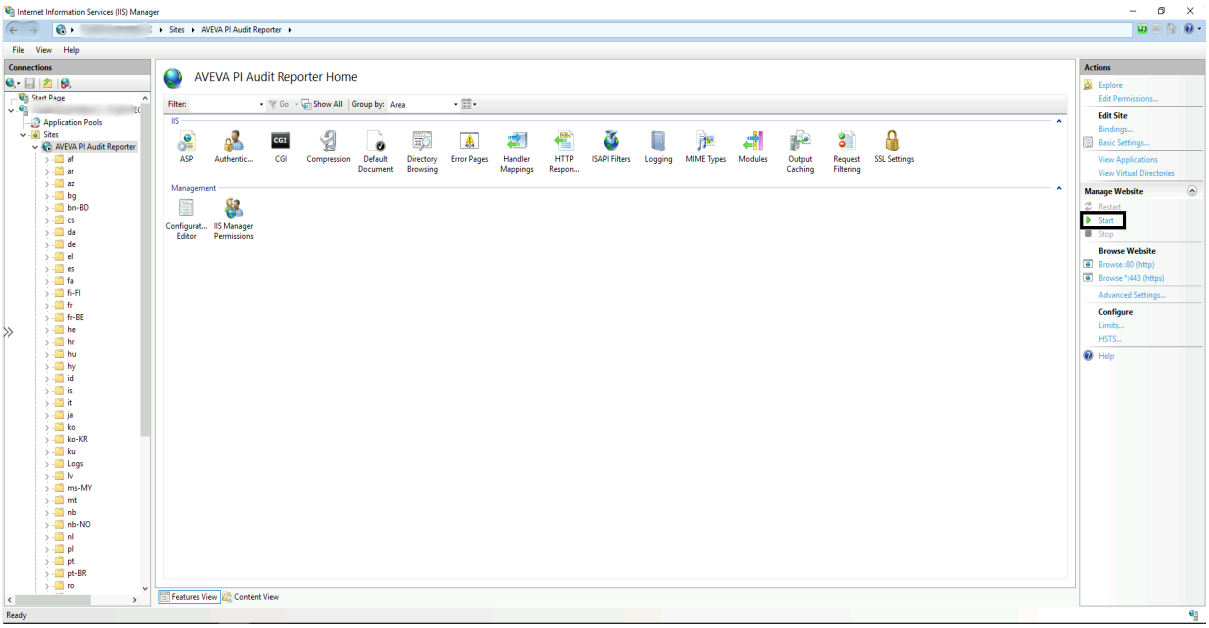
3. Select the appropriate SSL certificate from the list.



4. Select OK to apply the changes.



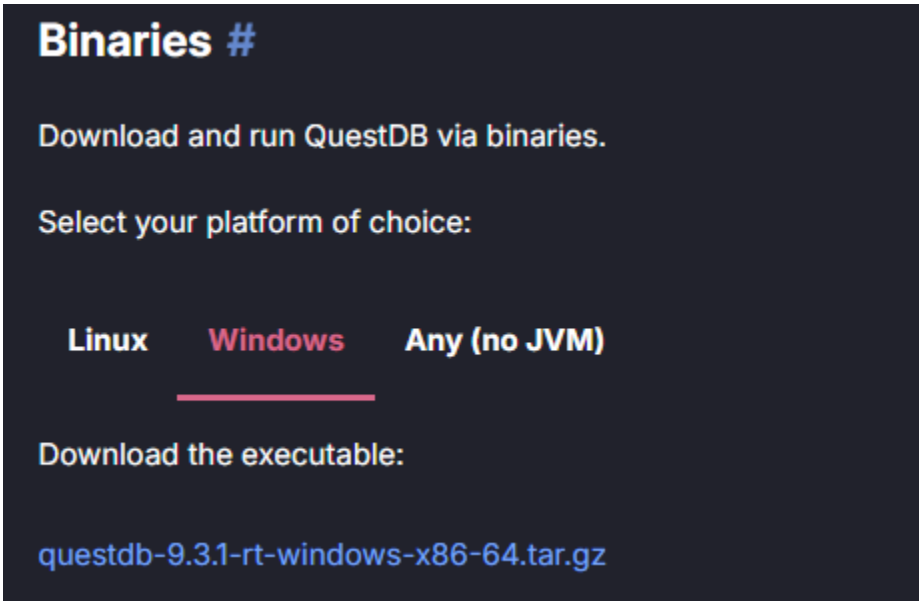
5. Select ‘Start’ located in the right-hand panel to initiate the website.



QuestDB

To install QuestDB application, the user must follow the steps.

1. Download the binaries for the platform of choice (in this case, Windows), which are available at the following address: https://questdb.io/docs/quick-start/#binaries.



Note: The term binaries mean the set of files used to configure and run applications. The binaries for QuestDB are compressed into a .gz file as shown.

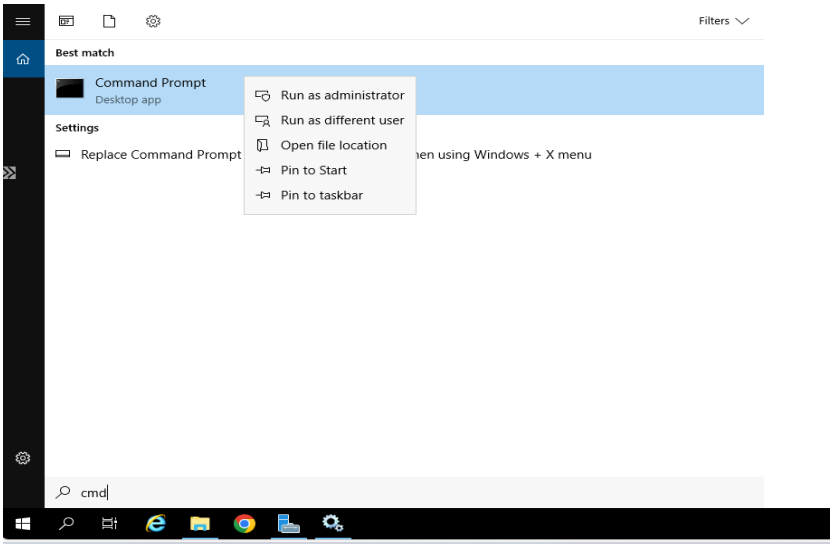
2. After downloading the binaries, extract the content to any directory, but suggest the following: <drive>\questdb\<questdb-version>. This will be the QuestDB installation directory, so it cannot be removed after installation.

Note: Binaries can be delivered in an unusual format for Windows applications. You can use 7-Zip or WinRAR to extract the files.

---

3. Define the data directory during the QuestDB installation. We suggest <drive>\questdb\audit-data.

4. Open the Command Prompt as an Administrator by selecting Start, type cmd, right-click Command Prompt, and select Run as administrator.

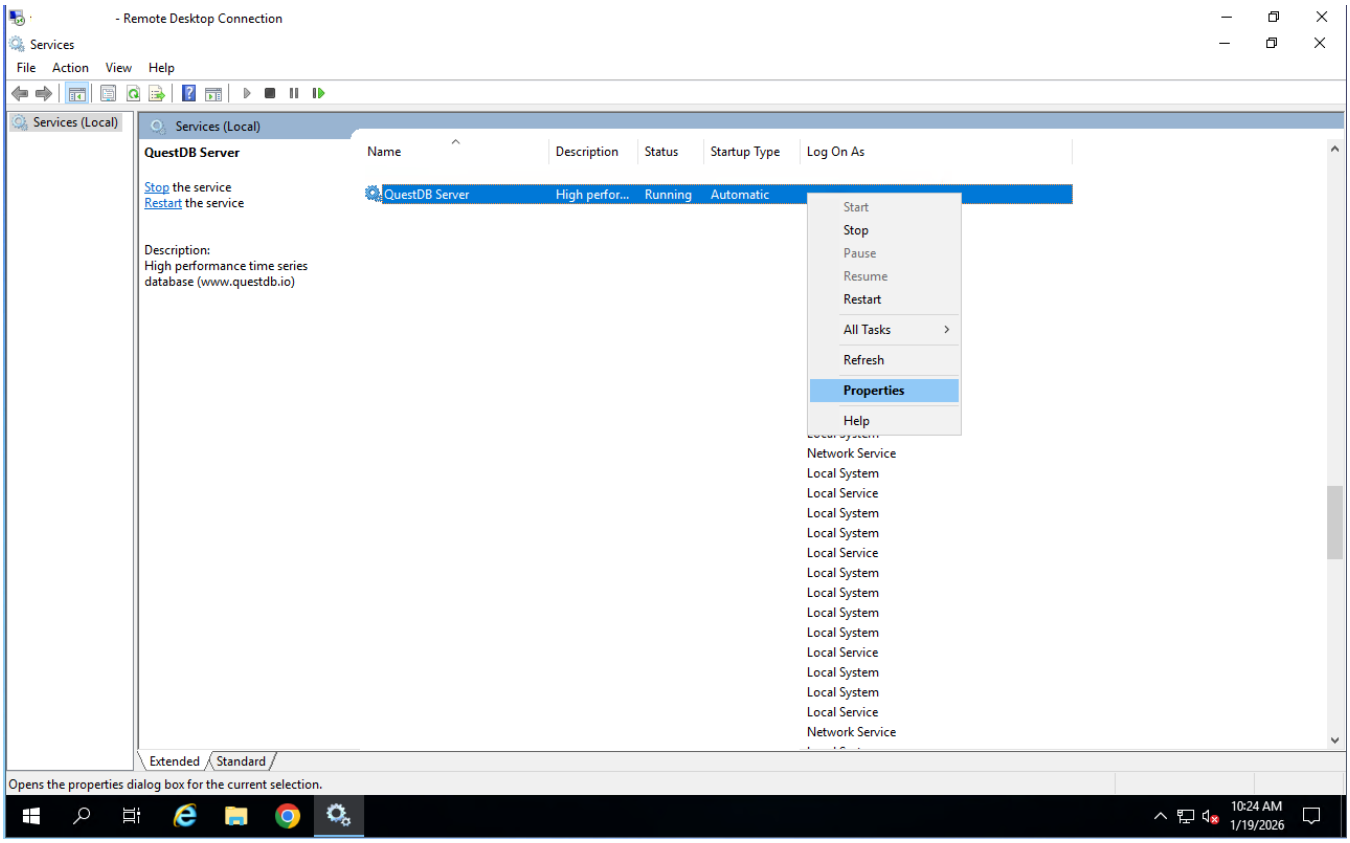


5. Use the following command line in the Command Prompt window to launch questDB to run install QuestDB as a service:

```
<selected questdb installation directory>\questdb.exe install -d <selected data directory>
```

6. Open Services from the Start menu and scroll down to find the QuestDB service.

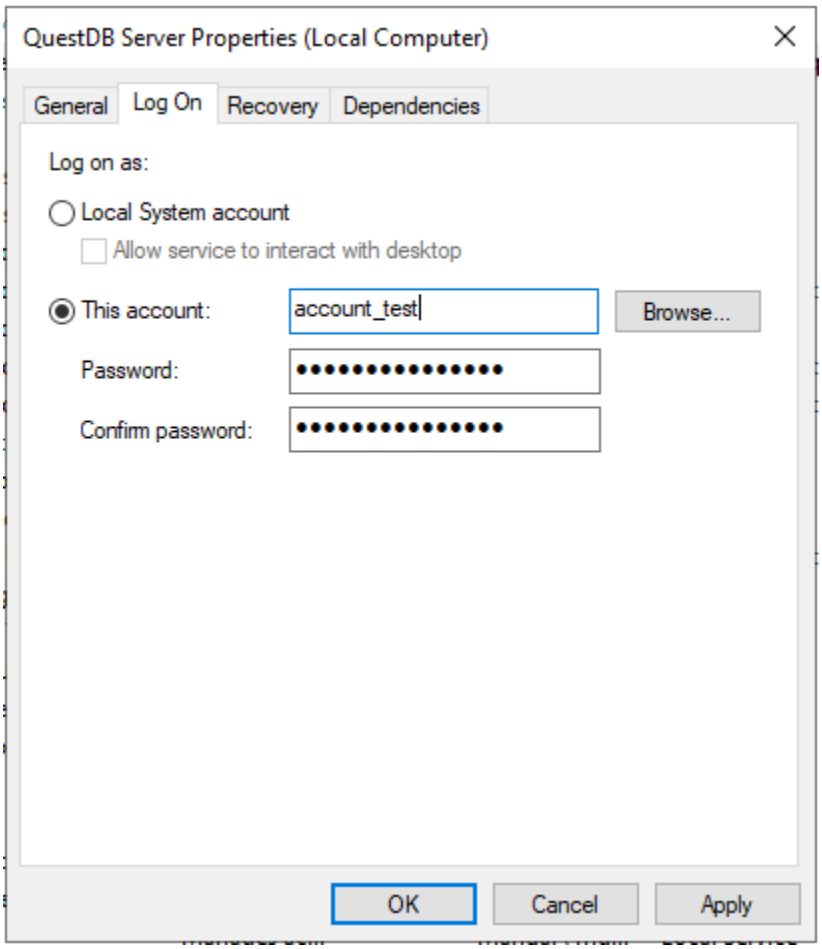
7. Right-click the QuestDB Server service and select Properties.



8. In the Properties window of the service, select the Log On tab.

9. Select the option “This account”. Use the “Browse..." button to select a user account from the directory.

10. Enter the password and confirm the password for the service account.



11. Select Apply to save the changes.

12. Select OK to close the window.

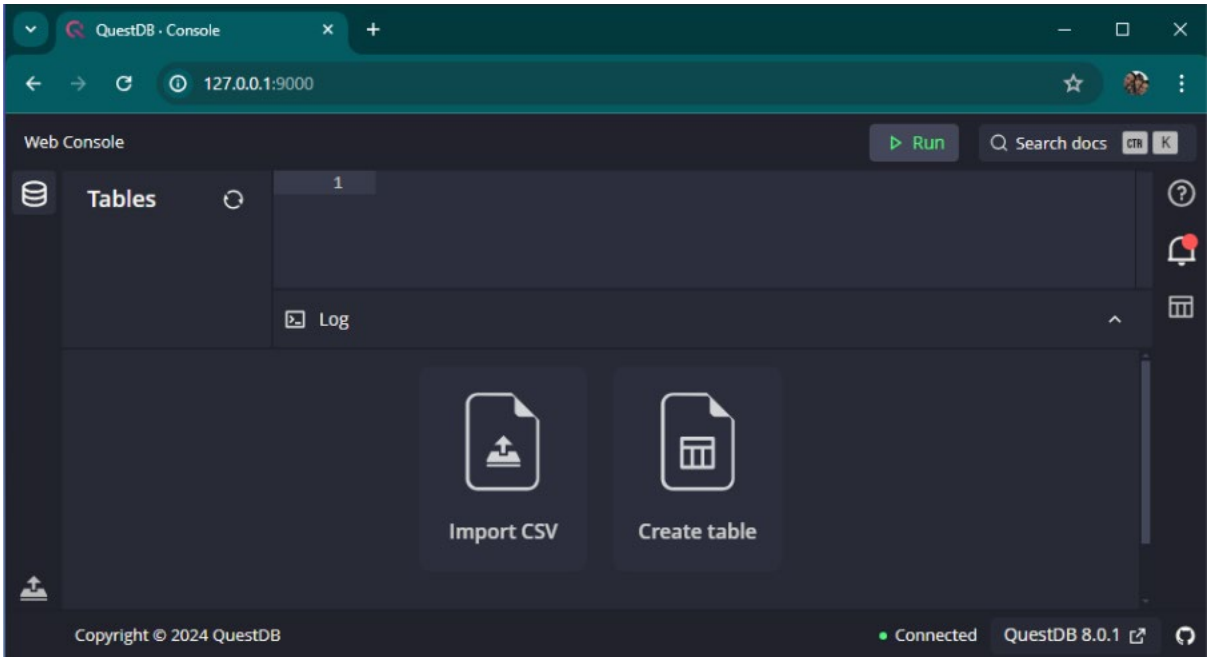
13. QuestDB Server windows service will be created after the installation. Remember to start the windows service to complete the verification step detailed above.

In order for PI Audit Report to connect and execute queries, QuestDB must be running and the following ports must be available for connections:

- 9000 – REST Api and web console (web console)
- 9000 – InfluxDB Line Protocol (internal use)
- 8812 – Postgress Wire Protocol (used for queries)
- 9003 – Min Health Server

Note: IT support will be able to ensure the above ports are open and accessible among servers used to host the PI Audit Reporter application.

14. Once installation is complete, User may verify QuestDB by visiting the address shown below.



All extra QuestDB configurations are saved in one file with the name server.conf, placed on the <installation dir>\Conf. To change user and password, for example, users can search the file for the configuration '#pg.user', like the screenshot below:

```
684
685  #pg.character.store.capacity=4096
686  #pg.character.store.pool.capacity=64
687  #pg.connection.pool.capacity=64
688  #pg.password=quest
689  #pg.user=admin
690  # Enables read-only mode for the pg wire protocol. In this mode data mutation queries are rejected.
691  #pg.security.readonly=false
692  #pg.readonly.password=quest
693  #pg.readonly.user=user
694  # Enables separate read-only user for the pg wire server. Data mutation queries are rejected for all cor
```

Note: As a best practice, the recommendation is to change the user and password avoiding using the default values. For more information about the QuestDB settings, please visit the support website at https://questdb.com/docs/configuration/overview/.

CHAPTER 4

Security

PI and AF Data

The AVEVA PI Audit Reporter application uses Windows security for secure connections to PI and AF. Historical and real-time audit trail records from both PI and AF are unified within the AVEVA PI Audit Reporter application.

MS SQL Server

The AVEVA PI Audit Reporter application uses Windows security for secure connection to the SQL Server.

Microsoft SQL is used to create database objects, insert, update, and delete records in MS SQL Server. Domain service account is required to be provided by the customer IT department and that service account granted permission on the db as follows:

- db_datawriter: Allows the user to add, delete, or modify data in the tables.
- db_ddladmin: Allows the user to create, drop, or modify any objects within a database.
- Execute: Allows the user to execute a stored procedure.
- db_datareader: Allows the user to read all data from all user tables and views in the database.

Note: For more information about the SQL Server permissions and roles, please visit the support website here.

Failover Mechanisms

SQL Server supports always on availability groups and Failover Cluster Instances (FCIs) for high availability.

Also, Failover Cluster Instances (FCIs) rely on Windows Server Failover Clustering (WSFC) to manage automatic failovers between nodes. The common issues during failover include:

- Replica stuck in RESOLVING state.
- Databases in NOT SYNCHRONIZING state.
- Failures due to exceeded failover thresholds or network issues.
- Data ingestion to the AVEVA PI Audit Reporter application will pause when MS SQL is unavailable and will automatically resume once MS SQL is running again.

As best practices, we have the following:

- Monitor cluster logs and SQL Server logs.
- Configure proper quorum settings and preferred owners in WSFC.

PI Audit Reporter tables

The following tables reside in the SQL database:

Name	Description
AuditInterfaces	Contains interfaces configured to extract audit data
AuditServers	Contains available Servers details.
AvailableAFDatabases	Contains available AF Databases to monitor
AvailableAFServers	Contains available AF Servers to monitor
ChunkExecutions	Contains chunks processed and to be processed by data ingress services
DataIngressSettings	Contains settings specific for data ingress services
DatFiles	Contains PI Audit database files and its details
DomainGroupRoleMaps	Contains relationships between domain groups and internal roles in web application
ExclusionFilters	Contains filters used to exclude some audit events from database
GeneralSettings	Contains general settings used by the web application to adjust behavior
InternalAuditLogs	Contains audit records for changes applied to AVEVA PI Audit Trail Application Management
Permissions	Contains the list of roles and permissions for web application
ReportQueueFile	Contains the files of reports generated
ReportsQueue	Contains metadata about report files generated
ReportsServiceConfiguration	Contains settings specific for reporting services
Users	Contains the list of web application users

PI Audit Reporter tables definition

Listed below is the definition of each database table:

AuditInterfaces

Constraints (PK/FK)	Column name	Data Type	Column Length	Nullable	Description
PK	ID	int	4	no	Sequential Number
N/A	AuditServerID	int	4	no	Server responsible for generating or storing audit records
N/A	Type	nvarchar	4	no	Type of audit interface, PI or AF
N/A	InterfaceMachine	nvarchar	200	no	Address/Hostname of server interface will retrieve audit events

Constraints (PK/FK)	Column name	Data Type	Column Length	Nullable	Description
N/A	TargetMachine	nvarchar	200	no	Name of machine is running the data ingestion service
N/A	TargetDatabase	nvarchar	2000	yes	Name of database will be processed for the specified AF server in TargetMachine column
N/A	TargetDatabaseGUID	uniqueidentifier	16	yes	Unique identifier of database will be processed for the specified AF server in TargetMachine column. (Applicable only for AF)
N/A	DatabaseEnabled	bit	1	yes	Flag to inform if this database is enabled for audit events retrieval. (Applicable only for AF)
N/A	StartMode	nvarchar	100	yes	Defines how data ingress will work for that specific interface, in recovery or real time mode
N/A	RecoveryDate	datetime	8	yes	Date and time to be used to recover past audit events
N/A	RealtimeStartDate	datetime	8	yes	Date and time to be used to start the real time audit events processing
N/A	ProcessedRecoveryCount	bigint	8	yes	Counter of total records processed in recovery mode
N/A	ProcessedRecoveryMaxDate	datetime	8	yes	Last date already processed by interface in recovery mode
N/A	ProcessedRealtimeCount	bigint	8	yes	Counter of total records processed in real time mode
N/A	ProcessedRealtimeMaxDate	datetime	8	yes	Last date already processed by interface in real time mode
N/A	TotalRecords	bigint	8	yes	Counter of total records processed by interface in rea time and recovery modes
N/A	BackupFilesDirectory	nvarchar	1024	yes	Directory that contains audit databases backup files that must be imported to the database. (Applicable only for PI)
N/A	AuditDatFilesDirectory	nvarchar	1024	yes	Directory that contains the current audit database files in PI Server. (Applicable only for PI)

Constraints (PK/FK)	Column name	Data Type	Column Length	Nullable	Description
N/A	ProcessArchiveAuditSubsystem	bit	1	yes	Flag that informs if archive subsystem database file will be processed by this interface. (Applicable only for PI)
N/A	ProcessSnapshotAuditSubsystem	bit	1	yes	Flag that informs if snapshot subsystem. database file will be processed by this interface. (Applicable only for PI)
N/A	ProcessBaseAuditSubsystem	bit	1	yes	Flag that informs if base subsystem database file will be processed by this interface. (Applicable only for PI)
N/A	CurrentDatFile	nvarchar	100	yes	Current audit database file being processed. Notice that it can change more frequently if parallel processing is enabled. (Applicable only for PI)
N/A	ExclusionFilterStatus	nvarchar	40	yes	Status of exclusion filters application once it is changed manually by user through administrator panel in web application
N/A	BackupFilesCopied	bit	1	yes	Flag that informs if backup files have been copied to avoid multiple copies of same files during data ingestion. (Applicable only for PI)
N/A	Summary	nvarchar	100	yes	Simple field that indicates if data ingress has some kind of error during data ingestion. Possible values are “OK” or “Error”.

AuditServers

Constraints (PK/FK)	Column name	Data Type	Column Length	Nullable	Description
PK	ID	int	4	no	Sequential Number
N/A	Type	nvarchar	4	no	Type of audit interface, PI or AF
N/A	TargetMachine	nvarchar	200	no	Address/Hostname of server interface will retrieve audit events
N/A	InterfaceMachine	nvarchar	200	no	Name of machine is running the data ingestion service

Constraints (PK/FK)	Column name	Data Type	Column Length	Nullable	Description
N/A	AFIncludeAllDatabases	bit	1	no	A flag to inform if all AF databases must be included on creation
N/A	StartMode	nvarchar	100	yes	Defines how data ingress will work for that specific interface, in recovery or real time mode
N/A	RecoveryDate	datetime	8	yes	Date and time to be used to recover past audit events
N/A	RealtimeStartDate	datetime	8	yes	Date and time to be used to start the real time audit events processing

AvailableAFDatabases

Constraints (PK/FK)	Column name	Data Type	Column Length	Nullable	Description
PK	ID	int	4	no	Sequential Number
FK	AvailableAFServerID	int	4	no	AF Server ID reference
N/A	DatabaseName	nvarchar	2000	no	AF Database name available.
N/A	DatabaseGUID	uniqueidentifier	16	no	Database unique identifier available

AvailableAFServers

Constraints (PK/FK)	Column name	Data Type	Column Length	Nullable	Description
PK	ID	int	4	no	Sequential Number
N/A	AFServerName	nvarchar	200	no	AF server name available
N/A	InterfaceMachine	nvarchar	200	no	Interface machina name available

ChunkExecutions

Constraints (PK/FK)	Column name	Data Type	Column Length	Nullable	Description
N/A	ChunkExecutionGUID	uniqueidentifier	16	no	Unique identifier of chunks
N/A	InterfaceID	int	4	no	Reference of interface this chunks belongs to

Constraints (PK/FK)	Column name	Data Type	Column Length	Nullable	Description
N/A	InterfaceMachine	nvarchar	200	no	Name of interface is processing this chunk
N/A	TargetMachine	nvarchar	200	no	Name of server is being processed by this chunk
N/A	Source	nvarchar	200	no	Source type (AF or PI)
N/A	TargetDatabase	nvarchar	200	yes	Name of database will be processed for the specified AF server in TargetMachine column
N/A	TargetDatabaseGUID	uniqueidentifier	16	yes	Unique identifier of database will be processed for the specified AF server in TargetMachine column
N/A	StartMode	nvarchar	100	no	Defines how data ingress will work for that specific interface, in recovery or real time mode
N/A	StartTime	datetime2	8	no	Start time of the interval to process audit events
N/A	EndTime	datetime2	8	no	End time of the interval to process audit events
N/A	ExecutionStartTime	datetime2	8	yes	Moment of data audit events processing started
N/A	ExecutionEndTime	datetime2	8	yes	Moment of data audit events processing finished
N/A	DurationInSeconds	int	4	yes	Duration in seconds of audit events processing
N/A	GetAuditRecordDurationInSeconds	int	4	yes	Duration in seconds of audit events retrieval
N/A	GetDetailsDurationInSeconds	int	4	yes	Duration in seconds of audit events details retrieval
N/A	SerializeDataDurationInSeconds	int	4	yes	Duration in seconds of audit events serialization
N/A	PersistDataDurationInSeconds	int	4	yes	Duration in seconds of audit events storing
N/A	ValidationDurationInSeconds	int	4	yes	Duration in seconds of audit events validation

Constraints (PK/FK)	Column name	Data Type	Column Length	Nullable	Description
N/A	TotalRecords	int	4	yes	Counter of total records processed by this chunk
N/A	Summary	nvarchar	max	yes	Simple field that indicates if data ingress has some kind of error during data ingestion. Possible values are “OK” or “Error”
N/A	DatFileId	int	4	yes	ID of dat file being processed by this chunk
N/A	DatFile	nvarchar	max	yes	Local path of dat file is being processed by this chunk
N/A	IngestionHash	nvarchar	1024	yes	Hash created from audit events retrieved and saved in ingestion process
N/A	ValidationHash	nvarchar	1024	yes	Hash created from audit events retrieved in validation process
N/A	ValidationStartTime	datetime2	8	yes	Date and time of the moment the chunk started to be validated
N/A	ValidationEndTime	datetime2	8	yes	Date and time of the moment the chunk finshed to be validated
N/A	ReprocessingDate	datetime2	8	yes	Date and time of the moment chunk is marked as invalid to be reprocessed
N/A	ReprocessingReason	nvarchar	510	yes	Reason why this chunk is marked as invalid to be reprocessed
N/A	LastHeartbeatDate	datetime2	8	yes	A field used to ensure this chunk is being processed or it is unresponsive
N/A	ParentChunkExecutionGUID	uniqueidentifier	16	yes	Unique identifier of an invalid parent chunk that created this chunk.
N/A	AttemptNumber	int	4	no	Number of current attempt of this chunk to be processed.

DataIngressSettings

Constraints (PK/FK)	Column name	Data Type	Column Length	Nullable	Description
PK	Id	int	4	no	Sequential Number
N/A	Service	nvarchar	510	no	Name of service is running and retrieving this configuration
N/A	Key	nvarchar	510	no	Key name of configuration
N/A	Value	nvarchar	510	no	Value of configuration

DatFiles

Constraints (PK/FK)	Column name	Data Type	Column Length	Nullable	Description
PK	ID	int	4	no	Sequential Number
N/A	AuditInterfaceID	int	4	yes	Reference of interface this dat file belongs to
N/A	SubSystem	nvarchar	100	yes	Name of subsystem this dat file refers to
N/A	RemotePath	nvarchar	1000	yes	Remote path of this dat file
N/A	LocalPath	nvarchar	1000	yes	Local path of this dat file
N/A	MajorVersion	int	4	yes	Major version of dat file
N/A	MinorVersion	int	4	yes	Minor version of dat file
N/A	ByteAlignment	bigint	8	yes	Byte alignment of dat file
N/A	DirectoryLocation	bigint	8	yes	Directory location of dat file
N/A	DirectorySize	bigint	8	yes	Directory size of dat file
N/A	RecordCount	bigint	8	yes	Number of records stored in dat file
N/A	LastRecno	bigint	8	yes	Last record number for this dat file
N/A	MaximumRecno	bigint	8	yes	Maximum record number of this dat file
N/A	UserBlockSize	bigint	8	yes	User block size in bytes of dat file
N/A	DataLocation	bigint	8	yes	Data location of dat file
N/A	DataSize	bigint	8	yes	Data size in bytes of dat file

Constraints (PK/FK)	Column name	Data Type	Column Length	Nullable	Description
N/A	AutoCompactPct	int	4	yes	Percent of auto compact
N/A	LastModified	datetime	8	yes	Last date and time this dat file was modified
N/A	BackupTime	datetime	8	yes	Date and time of backup for this dat file
N/A	Processed	bit	1	yes	Flag informing if this dat file is processed or not
N/A	ProcessedRecoveryMaxDate	datetime	8	yes	Last date already processed by interface in recovery mode
N/A	ProcessedRecoveryCount	bigint	8	yes	Counter of total records processed in recovery mode
N/A	ProcessedRealtimeMaxDate	datetime	8	yes	Last date already processed by interface in recovery mode
N/A	ProcessedRealtimeCount	bigint	8	yes	Counter of total records processed in real time mode
N/A	Summary	nchar	100	yes	Simple field that indicates if data ingress has some kind of error during data ingestion. Possible values are “OK” or “Error”.
N/A	IngestedPercent	real	4	yes	Percent of chunks ingested for this dat file
N/A	ValidatedPercent	real	4	yes	Percent of chunks validated for this dat file

DomainGroupRoleMaps

Constraints (PK/FK)	Column name	Data Type	Column Length	Nullable	Description
PK	ID	int	4	no	Sequential Number
N/A	group	nvarchar	255	no	Domain Group name
N/A	role	nvarchar	255	no	Role in the Application
N/A	createdBy	nvarchar	512	not	User that created the record
N/A	createdTime	Bigint	n/a	no	Timestamp of creation
N/A	updatedBy	nvarchar	512	yes	Most recent user that updated the record

Constraints (PK/FK)	Column name	Data Type	Column Length	Nullable	Description
N/A	updatedTime	bigint	n/a	yes	Most recent timestamp of update

ExclusionFilters

Constraints (PK/FK)	Column name	Data Type	Column Length	Nullable	Description
PK	ID	int	4	no	Sequential Number
N/A	AuditInterfaceID	int	4	yes	Reference of interface this dat file belongs to
N/A	Field	nvarchar	200	yes	Field where filter is applied.
N/A	Operator	nvarchar	40	yes	Operator to use when comparing values
N/A	ExclusionValues	nvarchar	-1	yes	Values to search against the field

GeneralSettings

Constraints (PK/FK)	Column name	Data Type	Column Length	Nullable	Description
PK	ID	int	4	no	Sequential Number
N/A	ReportHeaderText	nvarchar	200	yes	Report header text to Title into Report Cover page
N/A	LicenseKey	nvarchar	-1	no	This key is required to activate and authorize the application for use.
N/A	ReportLogo	nvarchar	-1	yes	Base64 string if the logo image to be used in Cover page for reports

InternalAuditLogs

Constraints (PK/FK)	Column name	Data Type	Column Length	Nullable	Description
PK	ID	int	4	no	Sequential Number
N/A	username	nvarchar	1024	no	User that is performing the operation that is being recorded
N/A	timestamp	bigint	8	no	Timestamp the operation that is being recorded

Constraints (PK/FK)	Column name	Data Type	Column Length	Nullable	Description
N/A	origin	nvarchar	1024	yes	From where is the operation that is being recorded
N/A	action	nvarchar	2048	yes	Action (Insert, Update, Delete) of the operation that is being recorded
N/A	message	nvarchar	-1	yes	Additional message of the operation that is being recorded
N/A	before	nvarchar	-1	yes	Value of the object or original value before changes of the operation that is being recorded
N/A	after	nvarchar	-1	yes	Value of the object or updated value after changes of the operation that is being recorded

Permissions

Constraints (PK/FK)	Column name	Data Type	Column Length	Nullable	Description
PK	ID	int	4	no	Sequential Number
N/A	role	nvarchar	510	no	Role into the system that the permissions are recorded
N/A	functionality	nvarchar	1024	no	Functionality that the permission will be set
N/A	key	nvarchar	1024	no	Key for internal checking when validating the permission by user's role
N/A	allowed	bit	1	no	True or False to indicate the allowed or not allowed permission x functionality
N/A	createdBy	nvarchar	1024	no	User that created the record
N/A	createdTime	bigint	8	no	Timestamp of creation
N/A	updatedBy	nvarchar	1024	yes	Most recent user that updated the record
N/A	updatedTime	bigint	8	yes	Most recent timestamp of update
N/A	defaultallowed	bit	1	yes	Default or original permission for reseting purposes only.

ReportQueueFile

Constraints (PK/FK)	Column name	Data Type	Column Length	Nullable	Description
N/A	ID	uniqueidentifier	16	no	Sequential Number
N/A	ReportQueueId	uniqueidentifier	16	no	Id of the request reporting for generation, this links the files with the report requested.
N/A	Index	int	4	no	The index of the file chunk to be downloaded by clients in the web application
N/A	File	varbinary	-1	no	The byte array for the chunk of the file

ReportsQueue

Constraints (PK/FK)	Column name	Data Type	Column Length	Nullable	Description
N/A	ID	uniqueidentifier	16	no	Sequential Number
N/A	Timestamp	datetime	8	yes	Timestamp of the request report generation
N/A	User	nvarchar	1024	no	User that is requesting the report generation
N/A	UserData	nvarchar	-1	no	Full user data in JSON that is requesting report generation
N/A	Predicate	nvarchar	-1	no	Predicate (filters) parameters to retrieve the database data and processing the report generation
N/A	TotalAuditRecords	int	4	yes	Total of Audit Records that is expected to be processed in a report generation
N/A	TotalAuditRecordItems	Int	4	Yes	Total of Audit Records Items/Events that is expected to be processed in a report generation
N/A	TotalProcessing	int	4	yes	Total of records that is being processed in that point of the time
N/A	FileChunks PercentageComplete	Decimal(5,2)	18	yes	Total of Items/Events processed when processing the Report

Constraints (PK/FK)	Column name	Data Type	Column Length	Nullable	Description
					Request
N/A	RetryCount	Int	4	Yes	Number of reprocessing attempts to the report request.
N/A	Status	nvarchar	256	yes	Status of the report generation that could be Enqueued, Requested, Processed, Completed, Failed or any other status that could be used for controlling report generation status.
N/A	FileSize	int	4	yes	Whole size of the file to be downloaded in Bytes.

ReportsServiceConfiguration

Constraints (PK/FK)	Column name	Data Type	Column Length	Nullable	Description
PK	ID	int	4	no	Sequential Number
N/A	configuration	nvarchar	1024	no	Name of the configuration used to control aspects of the reporting generation, see ReportsServiceConfiguration for reference.
N/A	value	nvarchar	1024	no	Value of the configuration.
N/A	updatedBy	nvarchar	1024	yes	User who has updated the record.
N/A	updatedTime	bigint	8	yes	Timestamp that the record is being updated in the database.

Users

Constraints (PK/FK)	Column name	Data Type	Column Length	Nullable	Description
PK	uid	uniqueidentifier	16	no	Unique ID for the user
N/A	enabled	bit	1	yes	Indicative if this user is enabled or not into this application
N/A	username	nvarchar	1024	no	Username from domain

Constraints (PK/FK)	Column name	Data Type	Column Length	Nullable	Description
N/A	firstname	nvarchar	1024	No	Firstname of the user from domain
N/A	lastname	nvarchar	1024	no	Lastname of the user from domain
N/A	email	nvarchar	1024	no	Email of the user from domain
N/A	role	nvarchar	510	no	Role of the user based on Domain Group x Role mapping.
N/A	createdBy	nvarchar	1024	no	User that is adding this record into the application
N/A	createdTime	bigint	8	no	Timestamp that this record is being created.
N/A	updatedBy	nvarchar	1024	yes	User that is updating the record
N/A	updatedTime	bigint	8	yes	Timestamp of the record update

QuestDB

QuestDB is a database used for specific workloads when in read-heavy scenarios where failover is less critical.

Failover Mechanisms

QuestDB is designed for high-performance time-series data, but it does not natively support automatic failovers like traditional RDBMS systems. It focuses on write-ahead logging and durability for crash recovery.

Data ingestion to the AVEVA PI Audit Reporter application will pause when QuestDB is unavailable and will automatically resume once QuestDB is running again.

As a best practice it is recommended to regularly back up data and test recovery procedures.

PI Audit Reporter tables

The following tables reside in the SQL database:

Name	Description
AuditRecords	Contains the list of audit records retrieved from data sources PI DA and PI AF
commentEntries	Contains the records for data audits when users are adding comments in the web application.
Log	Contains the log for web application and for data ingress events like runs, errors, etc.

PI Audit Reporter tables definition

Listed below is the definition of each QuestDB table:

AuditRecords

Constraints (PK/FK)	Column Name	Data Type	Symbol Capacity	Index Capacity	Description
N/A	uid	uniqueidentifier	N/A	N/A	Unique ID for the record in database
N/A	server	symbol	64	256	Server where the data is to be retrieved
N/A	source	symbol	2	16	PI or AF
N/A	date	timestamp	N/A	N/A	Date of audit record
N/A	ingestionDate	timestamp	N/A	N/A	Date of when audit record was saved
N/A	action	symbol	4	32	Change type, New, Modified, Excluded
N/A	category	symbol	32	64	Object changed
N/A	database	symbol	256	256	Database
N/A	id	varchar	N/A	N/A	Unique Id of the object
N/A	name	varchar	N/A	N/A	Name of the item changed
N/A	user	varchar	N/A	N/A	User that made change
N/A	userid	varchar	N/A	N/A	User ID that made change
N/A	path	varchar	N/A	N/A	Root path of item changed
N/A	details	varchar	N/A	N/A	JSON with the nested child items related to the data modifications that contains the audit record
N/A	reviews	varchar	N/A	N/A	Reviews made by users through web application
N/A	reason	varchar	N/A	N/A	Reason inserted by user for that audit event
N/A	changeNo	varchar	N/A	N/A	Number of changes made
N/A	userComment	varchar	N/A	N/A	Comments added by user for that audit event
N/A	targetDatabaseGuid	uniqueidentifier	N/A	N/A	Unique identifier of source database for the audit event
N/A	excluded	boolean	N/A	N/A	Marks if audit record is shown or not in web application and reports based on Exclusion Filters
N/A	hash	varchar	N/A	N/A	Hash of audit record
N/A	chunkExecutionGUID	varchar	N/A	N/A	Unique identifier of chunk that generated the record in QuestDB table

Constraints (PK/FK)	Column Name	Data Type	Symbol Capacity	Index Capacity	Description
N/A	deleted	boolean	N/A	N/A	Marks if the record was deleted
N/A	itemDescription	varchar	N/A	N/A	The list of items descriptions concatenated with “\u001f”
N/A	itemName	varchar	N/A	N/A	The list of items names concatenated with “\u001f”
N/A	itemId	varchar	N/A	N/A	The list of items ids concatenated with “\u001f”
N/A	itemProperty	varchar	N/A	N/A	The list of items properties concatenated with “\u001f”
N/A	itemOldvalue	varchar	N/A	N/A	The list of items old values concatenated with “\u001f”
N/A	itemOldtype	varchar	N/A	N/A	The list of items old types concatenated with “\u001f”
N/A	itemNewvalue	varchar	N/A	N/A	The list of items new values concatenated with “\u001f”
N/A	itemNewtype	varchar	N/A	N/A	The list of items new types concatenated with “\u001f”

CommentEntries

Constraints (PK/FK)	Column Name	Data Type	Symbol Capacity	Index Capacity	Description
N/A	uid	uniqueidentifier	N/A	N/A	Unique ID for the record in database
N/A	auditrecord_uid	uniqueidentifier	N/A	N/A	Unique ID for the audit record in database
N/A	date	timestamp	N/A	N/A	Date of audit record
N/A	changeNo	varchar	N/A	N/A	Number of changes made
N/A	username	varchar	N/A	N/A	User that made change
N/A	comment	varchar	N/A	N/A	Comment added by the user.

Log

Constraints (PK/FK)	Column Name	Data Type	Symbol Capacity	Index Capacity	Description
N/A	exception	string	N/A	N/A	Exception message and stack trace raised by the application. Null if log is not an error.
N/A	level	string	N/A	N/A	Level of that log message (error, information, debug, warning)
N/A	machine_name	string	N/A	N/A	Name of machine is hosting the application that wrote this log records
N/A	message	string	N/A	N/A	Main message of log record
N/A	message_template	string	N/A	N/A	Message template used to build the log message in this record
N/A	raise_date	timestamp	N/A	N/A	Date and time of when this log record was created.

CHAPTER 5

AVEVA™ PI Audit Reporter Modules and Components

Application Overview

The AVEVA PI Audit Reporter is a purpose-built application for auditing audit trail records provided by the AVEVA PI System that conform to accepted standards with compliant reports. It enhances audit capabilities by offering greater flexibility, performance, and compliance support. Refer to AVEVA PI Audit Reporter Architecture to explain the role of the application in the context of the complete PI system.

The application features a distributed architecture, with a web-based user interface serving as the primary access point. Supporting components include remote agents deployed to existing PI Data Historian and Asset Framework servers. These agents are responsible for collecting and transmitting audit data to a centralized application, enabling seamless enterprise-wide integration.

The application can immediately identify changes that require comments or electronic signatures, eliminating delays caused by slow search or query performance. The application is designed to handle millions of audit trail records efficiently, ensuring robust performance even in large-scale environments. Only minimal agent components need to be installed on existing infrastructure, simplifying adoption and reducing deployment overhead.

Core Modules

While the AVEVA PI Audit Reporter application is built on a microservices architecture, it is important to note that AF data interface, PI data interface, web application, reporting service modules form part of the Core system. These core services are essential for the basic functionality of the application. Without them, the system cannot operate, regardless of the modular and distributed nature of the architecture.

This design ensures flexibility and scalability, while maintaining a reliable foundation for critical operations such as authentication, data ingestion, and audit processing.

AF Data Interface

The AF Data Interface is a core module of the AVEVA PI Audit Reporter application. Implemented as a Windows service, this component is responsible for retrieving audit events from the AVEVA AF Audit Database. Once retrieved, the data is processed and transformed into a normalized format, which is then stored in a QuestDB table for efficient querying and reporting.

This module plays a critical role in ensuring that audit data is consistently structured, searchable, and ready for downstream analysis and compliance reporting.

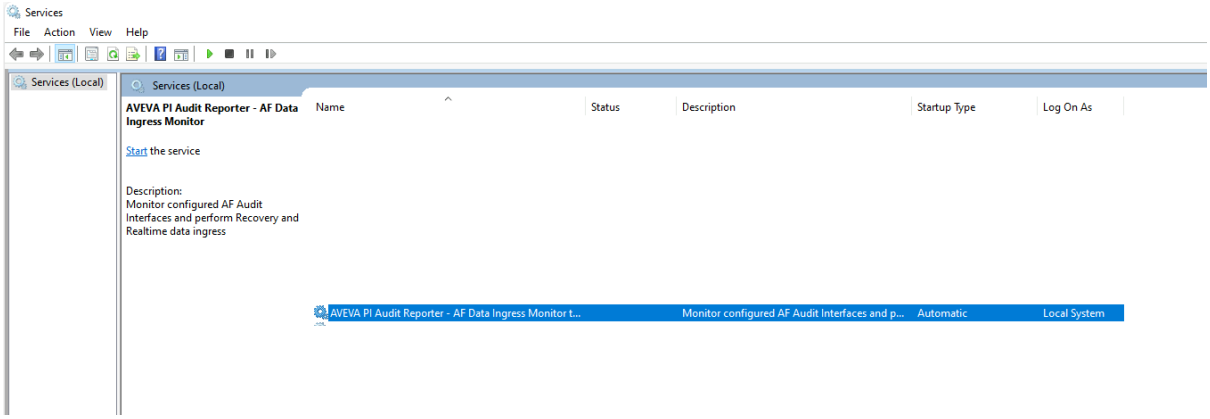
This service works with two main components with specific functionalities called Monitor and Worker. Monitor manages the overall control and coordination of data retrieval. Monitor's key responsibilities include, defining and enforcing the processing intervals, managing the retrieval period for audit data, checking for new or updated files and databases, controlling the chunk size for data processing, updating status and summary information and overseeing the execution flow of the service.

Monitor acts as the orchestrator of the data ingress process and runs continuously in the background. When required, the Worker component is triggered by Monitor and passes a set of the above parameters to process audit data.

Worker components are responsible for the collection, processing, and storage of audit data within the AVEVA PI Audit Reporter application. Unlike continuously running services, workers are on-demand executables that operate based on specific instructions. Workers are not active agents. They are invoked by the Monitor component to process a defined time range from a specific database. Each execution is guided by parameters such as time period to process, target database and Data chunk size or limits.

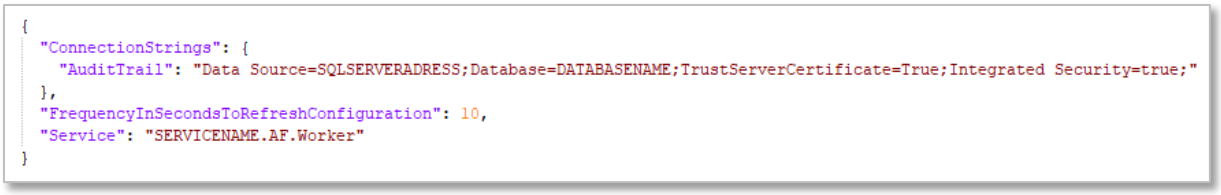
Install and Configure AVEVA PI Audit Reporter AF Data Ingress service

The AVEVA PI Audit Reporter AF Data Ingress service must be installed and configured with a user account with elevated privileges and access to an AF Server. The AVEVA PI Audit Reporter AF Data Ingress service must have an "automatic" startup type. It is possible to check the service status by opening Start > Windows Service and view the Services installation as per example below:



Once the Windows Service is installed and properly configured by the administrator user, the next step is to check the configuration file in the root folder of Service. File name is "appsettings.json", and it has connection settings that will allow the AF Data Ingress service to communicate with SQL Server database and retrieve the full list of settings and start processing. The configuration file must contain the following configured parameters:

- ConnectionStrings.AuditTrail: Represents the secure connection string to access the SQL Server database and retrieve information about settings and servers, which is used to integrate audit trail records.
- FrequencyInSecondsToRefreshConfiguration: Represents the interval, in seconds, AF Data Ingress service will look for updates in data ingress settings. DataIngressSettings table configurations can be changed while the service is still running.
- Service: Represents the name of the service installed. The screenshot below shows the required configuration.



Two separate appsettings.json files need to be configured, one for the Monitor component and one for Worker component, both part of the same installation.

Next step is to configure the AVEVA PI Audit Reporter AF data ingress settings table. This table stores general configuration settings for the data ingress services of both Monitor and Worker components. These settings include parameters i.e. execution interval, database information, logging, parallelization levels, and other related configurations, which are described in the following sections.

AF Configuration Settings

Service	Key	Default Value	Description
AF Monitor	AppSettings: CheckIntervalInSeconds	2	The interval, specified in seconds, determines how frequently the data ingress service runs to check for new data chunks to process
AF Monitor	AppSettings:MaxParallelRealtimeWorkers	2	Defines the maximum number of workers that can concurrently validate audit data recovery tasks for Realtime data
AF Monitor	AppSettings:MaxParallelRecoveryWorkers	2	Defines the maximum number of workers that can concurrently validate audit data recovery tasks for Recovery data
AF Monitor	AppSettings:RealtimeIntervalInMinutes	10	Defines the interval at which the data ingress service creates chunks for processing real-time audit data (e.g., every “X” minutes).
AF Monitor	AppSettings:RecoveryChunkIntervalInMinutes	30	Defines the interval at which the data ingress service creates chunks for processing recovery audit data (e.g., every “X” minutes)
AF Monitor	AppSettings:UpdateAFAvailableDatabasesFrequencyInSeconds	60	Defines how frequently the data ingress service updates the list of available AF Servers and databases in seconds.
AF Monitor	AppSettings:WorkerApplicationPath	<installationpath>¥AF Worker¥Cognizant.AuditTrail.DataIngress.AF.Worker.exe	Defines the complete system path to the installed worker executable file location.
AF Monitor	AppSettings: InterfaceMachine	localhost	Defines the hostname of the server where the data ingress service is installed.

Service	Key	Default Value	Description
AF Monitor	AppSettings:LogDirectory	File directory	Defines the directory used to store file system logs. By default, it is recommended not to use the C drive to prevent potential performance or disk space issues.
AF Monitor	AppSettings:LogLevel	Trace	Log level of the application. Default level is “Trace”. The following are the available options: Trace - 0: Logs that contain the most detailed messages. Debug - 1: Logs that are used for interactive investigation during troubleshooting. Information - 2: Logs that track the general flow of the application. Warning - 3: Logs that highlight an abnormal or unexpected event in the application flow. It does not represent an error, but an event that may require attention. Error - 4: Logs that highlight when the current flow of execution is stopped due to a failure. These should indicate a failure in the current activity, not an application-wide failure. Critical - 5: Logs that describe an unrecoverable application or system crash, or a catastrophic failure that requires immediate attention.
AF Monitor	AppSettings:LogFileFlushIntervalInSeconds	5	Defines the interval at which the logging mechanism writes information to the file system, measured in seconds.
AF Monitor	AppSettings:LogMaxFileSizeInBytes	10485760	Defines the maximum size/upper limit of log files in bytes. When a file reaches the maximum size/upper limit, a new log file is automatically created.
AF Monitor	MSSQL:DataSource	Server_name	Defines the name of the SQL Server instance used to store data ingress settings.
AF Monitor	MSSQL:Database	Database_name	Defines the name of the SQL Server database used to store data ingress configuration settings.
AF Monitor	MSSQL:TrustServerCertificate	true	Determines whether client applications should trust the SSL certificate presented by the SQL Server. When set to true (default), the client bypasses certificate validation, allowing

Service	Key	Default Value	Description
			encrypted connections without verifying the certificate's authenticity.
AF Monitor	QuestDB:Server	Server_name	Defines the hostname or IP address of the server where QuestDB is installed.
AF Monitor	QuestDB:Database	Database_name	Defines the name of the QuestDB database used to store logs and audit records.
AF Monitor	QuestDB:PortPGWire	8812	Defines the port number used to connect to QuestDB and transmit data.
AF Monitor	QuestDB:SslMode	prefer	Determines whether a secure connection (SSL) is used when connecting to QuestDB. Available options: Prefer: SSL is preferred; if unavailable, the connection will proceed without SSL. Require: SSL is mandatory; if unavailable, the connection will be rejected.
AF Monitor	QuestDB:User	User_name	Defines the username for the account used to connect to the QuestDB database.
AF Monitor	QuestDB:Password	Password encrypted	Defines the password for the account used to connect to the QuestDB database.
AF Monitor	AppSettings:MaxParallelValidationRecoveryWorkers	1	Defines the maximum number of workers that can validate audit data recovery tasks in parallel for recovery tasks.
AF Monitor	AppSettings:MaxParallelValidationRealtimeWorkers	1	Defines the maximum number of workers that can validate audit data recovery tasks in parallel for realtime tasks.
AF Monitor	MSSQL:ConnectionTimeout	30	Defines the maximum time, in seconds, that a server will attempt to connect to a Microsoft SQL Server instance before timing out and returning an error.
AF Monitor	MSSQL:CommandTimeout	120	Defines the maximum time, in seconds, that a SQL command is allowed to execute before being automatically terminated by the server.
AF Monitor	AppSettings:MinutesToWaitBeforeValidating	5	Defines the number of minutes the application should wait before starting a validation process.
AF Monitor	AppSettings:WorkerTimeoutInSeconds	600	Defines the maximum duration (in seconds) that a background worker is allowed to run before being forcefully timed out or cancelled.
AF Monitor	QuestDB:ILPPort	9009	The port number QuestDB uses to receive data via the Influx Line Protocol (ILP).

Service	Key	Default Value	Description
AF Monitor	QuestDB:PortInLine	9009	The port number QuestDB uses to accept SQL queries directly (inline execution).
AF Worker	AppSettings:HeartbeatIntervalInSeconds	10	Defines the interval, in seconds, at which the heartbeat mechanism updates chunk execution status. The interval is used to determine whether a chunk is still running.
AF Worker	AppSettings:InterfaceMachine	localhost	Defines the hostname of the server where the data ingress service is installed.
AF Worker	AppSettings:LogsDirectory	File directory	Defines the directory path where file system logs will be saved. By default, it is recommended not to use the C drive to prevent potential performance or disk space issues.
AF Worker	AppSettings:LogLevel	trace	Log level of the application. Default level is “Trace”. The following are the available options: Trace - 0: Logs that contain the most detailed messages. Debug - 1: Logs that are used for interactive investigation during troubleshooting. Information - 2: Logs that track the general flow of the application. Warning - 3: Logs that highlight an abnormal or unexpected event in the application flow. It does not represent an error, but an event that may require attention. Error - 4: Logs that highlight when the current flow of execution is stopped due to a failure. These should indicate a failure in the current activity, not an application-wide failure. Critical - 5: Logs that describe an unrecoverable application or system crash, or a catastrophic failure that requires immediate attention.
AF Worker	AppSettings:LogFileFlushIntervalInSeconds	5	Defines the interval in seconds, at which the application flushes log data to the file system.
AF Worker	AppSettings:LogMaxFileSizeInBytes	10485760	Defines the maximum size/upper limit of log files in bytes. When a file reaches this maximum size/upper limit, a new log file is automatically created.

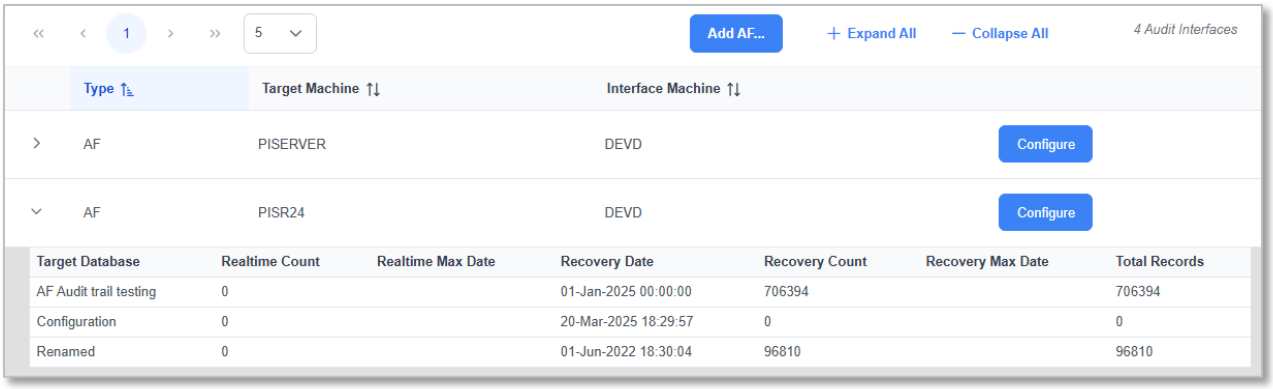
Service	Key	Default Value	Description
AF Worker	MSSQL:DataSource	Server_name	Defines the name of the SQL Server database used to store data ingress configuration settings.
AF Worker	MSSQL:Database	Database_name	Defines the name of the SQL Server instance used to store data ingress settings.
AF Worker	MSSQL:TrustServerCertificate	true	Determines whether client applications should trust the SSL certificate presented by the SQL Server. When set to true (default), the client bypasses certificate validation, allowing encrypted connections without verifying the certificate's authenticity.
AF Worker	QuestDB:Server	Server_name	Defines the hostname or IP address of the server where QuestDB is installed.
AF Worker	QuestDB:Database	Database_name	Defines the name of the QuestDB database used to store logs and audit records.
AF Worker	QuestDB:PortInLine	9009	Defines the port number used for inline data transmission to QuestDB.
AF Worker	QuestDB:PortPGWire	8812	Defines the port number used to connect to QuestDB and transmit data.
AF Worker	QuestDB:SslMode	prefer	Determines whether a secure connection (SSL) is used when connecting to QuestDB. Available options: Prefer: SSL is preferred; if unavailable, the connection will proceed without SSL. Require: SSL is mandatory; if unavailable, the connection will be rejected.
AF Worker	QuestDB:User	user_name	Defines the username for the account used to connect to the QuestDB database.
AF Worker	QuestDB:Password	Password Encrypted	Defines the password for the account used to connect to the QuestDB database.
AF Worker	MSSQL:ConnectionTimeout	30	Defines the maximum time, in seconds, that a server will attempt to connect to a Microsoft SQL Server instance before timing out and returning an error.
AF Worker	MSSQL:CommandTimeout	120	Defines the maximum time, in seconds, that a SQL command is allowed to be executed before being automatically terminated by the server.

Service	Key	Default Value	Description
AF Worker	AppSettings:MaxRecoveryChunksPerInterfaceAtTime	5	Defines the maximum number of recovery chunks handled per interface in a single operation.
AF Worker	AppSettings:ParentRecordsPageSize	500	Specifies the page size, the maximum count of parent record per page.
AF Worker	AppSettings:ParentRecordsPagesLimit	10	Defines the maximum number of pages of parent records that can be retrieved, displayed, or processed within the application at one time.
AF Worker	QuestDB:ILPPort	9009	The port number QuestDB uses to receive data via the Influx Line Protocol (ILP).
AF Worker	AppSettings:MaxRealTimeChunksPerInterfaceAtTime	5	Limits how many data chunks can be processed at once per interface in QuestDB
AF Worker	AppSettings:RecoveryChunkIntervalInMinutes	30	Defines the interval at which the data ingress service creates chunks for processing recovery audit data (e.g., every “X” minutes)
AF Worker	AppSettings:MaxParallelRealtimeWorkers	1	Defines the maximum number of workers that can concurrently validate audit data recovery tasks for Realtime data.
AF Worker	AppSettings:MaxParallelRecoveryWorkers	3	Defines the maximum number of workers that can concurrently validate audit data recovery tasks for Recovery data.
License	LicenseKey	License Key Encrypted	The license key provided by the vendor must be entered during the installation of the Web Application. This key is required to activate and authorize the application for use.

Once the above mandatory configurations for the AVEVA PI Audit Reporter AF Data Ingress are completed, the service can be started. After the service is running, AF audit data ingestion can be configured through the administrator panel of the web application.

For detailed instructions on configuring the AF interface, refer to Audit Interfaces view and Admin.

Once configuration is complete, the interfaces will appear as shown in the image below.



PI Data Interface

The PI Data Interface is a core module of the AVEVA PI Audit Reporter Application. Implemented as a Windows service, this component is responsible for retrieving audit events from the AVEVA PI Audit Database. Once retrieved, the data is processed, and transformed into a normalized format, which is then stored within a QuestDB table for efficient querying and reporting.

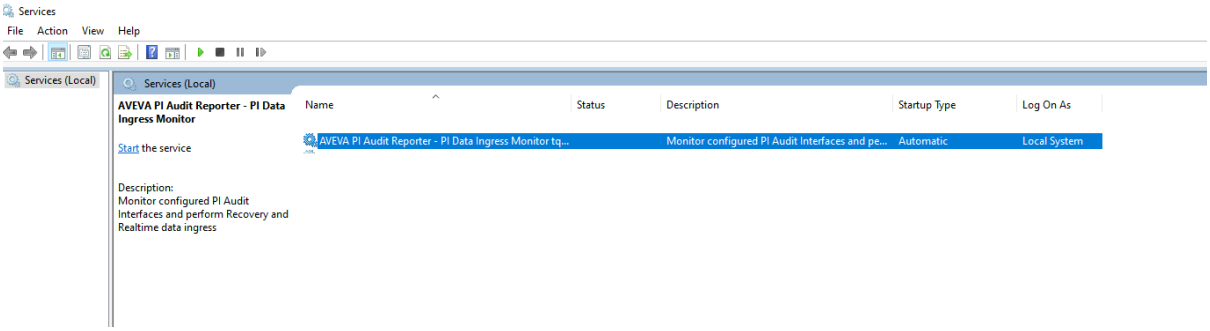
This module plays a critical role in ensuring that audit data is consistently structured, searchable, and ready for downstream analysis and compliance reporting.

This service works with two main components with specific functionalities called Monitor and Worker. Monitor components manage the overall control and coordination of data retrieval. Its key responsibilities are defining and enforcing the processing interval, managing the retrieval period for audit data, checking for new or updated files and databases controlling the chunk size for data processing, updating status and summary information, and overseeing the execution flow of the service.

The Monitor acts as the orchestrator of the data ingress process and runs continuously in the background. The Worker component is triggered by Monitor when required, passing a set of parameters to process audit data.

Worker components are responsible for the collection, processing, and storage of audit data within the AVEVA PI Audit Reporter application. Unlike continuously running services, Workers are on-demand executables that operate based on specific instructions. Workers are not active agents. They are invoked by the Monitor component to process a defined time range from a specific database. Each execution is guided by parameters such as time period to process, target database and Data chunk size or limits.

The AVEVA PI Audit Reporter PI Data Ingress service must be installed and configured with a user account with elevated privileges. The user must have access to both the PI Server and the folder which contains .dat files, in order to restart subsystems using the piartool AVEVA PI Audit Trail utility. The AVEVA PI Audit Reporter PI Data Ingress service must have “Automatic” startup type. To check service status, open Start > Windows Service and view Service installation as per example below:



Once Windows service is installed and properly configured, the next step is to check the configuration file in the root folder of service. File name is “appsettings.json” and has connection settings that will allow the AVEVA PI Audit Reporter PI Data Ingress service to communicate with SQL Server database and retrieve the full list of settings and start processing. The configuration file must contain the following configured parameters:

- ConnectionStrings.AuditTrail: Represents the secure connection string to access the SQL Server database and retrieve information about settings and servers, which is used to integrate audit trail records.
- FrequencyInSecondsToRefreshConfiguration: Represents the interval, in seconds, that windows service will look for updates in data ingress settings. DataIngressSettings table configurations can be changed while the service is still running.
- Service represents the name of the service installed. The screenshot below shows the required configuration.

```
{
  "ConnectionStrings": {
    "AuditTrail": "Data Source=SQLSERVERADRESS;Database=DATABASENAME;TrustServerCertificate=True;Integrated Security=true;"
  },
  "FrequencyInSecondsToRefreshConfiguration": 10,
  "Service": "SERVICENAME.AF.Worker"
}
```

Two separate appsettings.json files need to be configured, one for the Monitor component and one for Worker component, both part of the same installation.

Next step is to configure the AVEVA PI Audit Reporter PI data ingress settings table. This table stores general configuration settings for the data ingress services of both Monitor and Worker components. These settings include parameters i.e. execution interval, database information, logging, parallelization levels, and other related configurations, which are described in the following sections.

PI Configuration Settings

Service	Key	Default Value	Description
PI Monitor	AppSettings: CheckIntervalInSeconds	10	The interval, specified in seconds, determines how frequently the data ingress service runs to check for new data chunks to process
PI Monitor	AppSettings:MaxAuditFilesParallelProcessing	5	Defines the maximum number of audit database files that can be processed in parallel.

Service	Key	Default Value	Description
PI Monitor	AppSettings:MaxInterfacesParallelProcessing	5	Defines the maximum number of interfaces that can be processed in parallel.
PI Monitor	AppSettings:MaxParallelRealtimeWorkers	1	Defines the maximum number of workers that can process real-time audit data concurrently.
PI Monitor	AppSettings:MaxParallelRecoveryWorkers	3	Defines the maximum number of workers that can process data recovery tasks in parallel.
PI Monitor	AppSettings:PIAdmDirectoryToRunCommands	<drive>¥Program Files¥PIPC¥adm	Defines the directory path where the default install location for administrative and utility tools used with the PI System. (i.e.pidiag,piartool,piconfig,pigetmsg)
PI Monitor	AppSettings:RecoveryChunkIntervalInMinutes	21600	Defines the interval at which the data ingress service creates chunks for processing recovery audit data (e.g., every “X” minutes)
PI Monitor	AppSettings:TemporaryCopiedAuditFilesDirectory	File directory	Defines the complete path where the temporary audit file directory is stored.
PI Monitor	AppSettings:WorkerapplicationPath	<installationpath>¥PI Worker¥Cognizant.AuditTrail.DataIngress.PI.Worker.exe	Defines the complete system path to the installed worker executable file location.
PI Monitor	AppSettings:InterfaceMachine	localhost	Defines the hostname of the server where the data ingress service is installed.
PI Monitor	AppSettings:LogsDirectory	File directory	Defines the directory used to store file system logs. By default, it is recommended not to use the C drive to prevent potential performance or disk space issues.

Service	Key	Default Value	Description
PI Monitor	AppSettings:LogLevel	Trace	Log level of the application. Default level is “Trace”, and these are the available options: Trace - 0: Logs that contain the most detailed messages. Debug - 1: Logs that are used for interactive investigation during troubleshooting. Information - 2: Logs that track the general flow of the application. Warning - 3: Logs that highlight an abnormal or unexpected event in the application flow. It does not represent an error, but an event that may require attention. Error - 4: Logs that highlight when the current flow of execution is stopped due to a failure. These should indicate a failure in the current activity, not an application-wide failure. Critical - 5: Logs that describe an unrecoverable application or system crash, or a catastrophic failure that requires immediate attention.
PI Monitor	AppSettings:LogFileFlushIntervalInSeconds	5	Defines the interval at which the logging mechanism writes information to the file system, measured in seconds.
PI Monitor	AppSettings:LogMaxFileSizeInBytes	10485760	Defines the maximum size/upper limit of log files in bytes. When a file reaches the maximum size/upper limit a new log file is automatically created.
PI Monitor	MSSQL:DataSource	Server_name	Defines the name of the SQL Server instance used to store data ingress settings.
PI Monitor	MSSQL:Database	Database_name	Defines the name of the SQL Server database used to store data ingress configuration settings.
PI Monitor	MSSQL:TrustServerCertificate	true	Determines whether client applications should trust the SSL certificate presented by the SQL Server. When set to true (default), the client bypasses certificate validation, allowing encrypted connections without verifying the certificate's authenticity.
PI Monitor	QuestDB:Server	Server_name	Defines the hostname or IP address of the server where QuestDB is installed.

Service	Key	Default Value	Description
PI Monitor	QuestDB:Database	Database_name	Defines the name of the QuestDB database used to store logs and audit records.
PI Monitor	QuestDB:PortPGWire	8812	Defines the port number used to connect to QuestDB and transmit data.
PI Monitor	QuestDB:SslMode	prefer	Determines whether a secure connection (SSL) is used when connecting to QuestDB. Available options: Prefer: SSL is preferred; if unavailable, the connection will proceed without SSL. Require: SSL is mandatory; if unavailable, the connection will be rejected.
PI Monitor	QuestDB:User	User_name	Defines the username for the account used to connect to the QuestDB database.
PI Monitor	QuestDB:Password	Password Encrypted	Defines the password for the account used to connect to the QuestDB database.
PI Monitor	AppSettings:MaxParallelValidationRecoveryWorkers	1	Defines the maximum number of workers that can concurrently validate audit data recovery tasks for Recovery data.
PI Monitor	AppSettings:MaxParallelValidationRealtimeWorkers	1	Defines the maximum number of workers that can concurrently validate audit data recovery tasks for Realtime data.
PI Monitor	MSSQL:ConnectionTimeout	30	Defines the maximum time, in seconds, that a server will attempt to connect to a Microsoft SQL Server instance before timing out and returning an error.
PI Monitor	MSSQL:CommandTimeout	120	Defines the maximum time, in seconds, that a SQL command is allowed to be executed before being automatically terminated by the server.
PI Monitor	AppSettings:MinutesToWaitBeforeValidating	5	Defines the number of minutes the application should wait before starting a validation process.
PI Monitor	QuestDB:PortInLine	9009	Defines the port number used for inline data transmission to QuestDB.
PI Worker	AppSettings:PIAdmDirectoryToRunCommands	<drive>¥Program Files¥PIPC¥adm	Defines the directory path where the default install location for administrative and utility tools used with the PI System. (i.e.pidiag,piartool,piconfig,pigetmsg)

Service	Key	Default Value	Description
PI Worker	AppSettings:HeartbeatIntervalInSeconds	10	Defines the interval, in seconds, at which the heartbeat mechanism updates the chunk execution status. Used to determine whether a chunk is still running.
PI Worker	AppSettings:InterfaceMachine	localhost	Defines the hostname of the server where the data ingress service is installed.
PI Worker	AppSettings:LogsDirectory	File directory	Defines the directory path where file system logs will be saved. By default, it is recommended not to use the C drive to prevent potential performance or disk space issues.
PI Worker	AppSettings:LogLevel	trace	Log level of the application. Default level is “Trace”. The following are the available options: Trace - 0: Logs that contain the most detailed messages. Debug - 1: Logs that are used for interactive investigation during troubleshooting. Information - 2: Logs that track the general flow of the application. Warning - 3: Logs that highlight an abnormal or unexpected event in the application flow. It does not represent an error, but an event that must be checked. Error - 4: Logs that highlight when the current flow of execution is stopped due to a failure. These should indicate a failure in the current activity, not an application-wide failure. Critical - 5: Logs that describe an unrecoverable application or system crash, or a catastrophic failure that require immediate attention.
PI Worker	AppSettings:LogFileFlushIntervalInSeconds	5	Defines the interval, in seconds, at which the application flushes log data to the file system
PI Worker	AppSettings:LogMaxFileSizeInBytes	10485760	Defines the maximum size of log files in bytes. When a file reaches this size, a new log file is automatically created.
PI Worker	MSSQL:DataSource	Server_name	Defines the name of the SQL Server database used to store data ingress configuration settings.

Service	Key	Default Value	Description
PI Worker	MSSQL:Database	Database_name	Defines the name of the SQL Server instance used to store data ingress settings.
PI Worker	MSSQL:TrustServerCertificate	true	Determines whether client applications should trust the SSL certificate presented by the SQL Server. When set to true (default), the client bypasses certificate validation, allowing encrypted connections without verifying the certificate's authenticity.
PI Worker	QuestDB:Server	Server_name	Defines the hostname or IP address of the server where QuestDB is installed.
PI Worker	QuestDB:Database	Database_name	Defines the name of the QuestDB database used to store logs and audit records.
PI Worker	QuestDB:PortInLine	9009	Defines the port number used for inline data transmission to QuestDB.
PI Worker	QuestDB:PortPGWire	8812	The port number used to connect to QuestDB and transmit data.
PI Worker	QuestDB:SslMode	prefer	Determines whether a secure connection (SSL) is used when connecting to QuestDB. Available options: Prefer: SSL is preferred; if unavailable, the connection will proceed without SSL. Require: SSL is mandatory; if unavailable, the connection will be rejected.
PI Worker	QuestDB:User	User_name	Defines username for the account used to connect to the QuestDB database.
PI Worker	QuestDB:Password	Password Encrypted	Defines the password for the account used to connect to the QuestDB database.
PI Worker	MSSQL:ConnectionTimeout	30	Defines the maximum time, in seconds, that a server will attempt to connect to a Microsoft SQL Server instance before timing out and returning an error.
PI Worker	MSSQL:CommandTimeout	120	Defines the maximum time, in seconds, that a SQL command is allowed to be executed before being automatically terminated by the server.
PI Worker	AppSettings:WorkerTimeoutInSeconds	300	Defines the maximum duration (in seconds) that a background worker is allowed to run before being forcefully timed out or cancelled.

Service	Key	Default Value	Description
PI Worker	AppSettings:RealTimeIntervalInMinutes	10	Defines the interval at which the data ingress service creates chunks for processing real time audit data (e.g., every “X” minutes)
PI Worker	AppSettings:RealTimeIntervalInMinutes	10	Defines the interval at which the data ingress service creates chunks for processing real time audit data (e.g., every “X” minutes)
PI Worker	AppSettings:TemporaryCopiedAuditFilesDirectory	File directory	Defines the complete path where the temporary audit file directory is stored.
PI Worker	AppSettings:ParentRecordsPageSize	500	Specifies the page size, the maximum count of parent record per page.
PI Worker	AppSettings:ParentRecordsPagesLimit	10	Defines the maximum number of pages of parent records that can be retrieved, displayed, or processed within the application at one time.
PI Worker	AppSettings:RecoveryChunkIntervalInMinutes	21600	Defines the interval at which the data ingress service creates chunks for processing recovery audit data (e.g., every “X” minutes)
PI Worker	AppSettings:MaxParallelRealtimeWorkers	1	Defines the maximum number of workers that can concurrently validate audit data recovery tasks for Realtime data
PI Worker	AppSettings:MaxParallelRecoveryWorkers	3	Defines the maximum number of workers that can concurrently validate audit data recovery tasks for Recovery data
License	LicenseKey	License Key Encrypted	The license key provided by the vendor must be entered during the installation of the Web Application. This key is required to activate and authorize the application for use.

Once the above mandatory configurations are completed, the AVEVA PI Audit Reporter PI Data Ingress Service instance can run without issues. To set up a new interface representing a new AVEVA PI Server for audit data collection, the final step is to add a new record to the AuditInterfaces table. This record defines the connection and configuration details required for the service to begin ingesting audit data from the specified AVEVA PI Server.

The AuditInterfaces table is responsible for managing all audit interfaces integrated into the AVEVA PI Audit Reporter Application. For AVEVA PI Audit Reporter PI Data Ingress, each record in this table represents an AVEVA PI Server whose audit events are collected, processed, and stored in the QuestDB database. An audit interface entry is typically created during the installation of the Windows service, but it can also be added manually using an SQL INSERT script on the SQL Server.

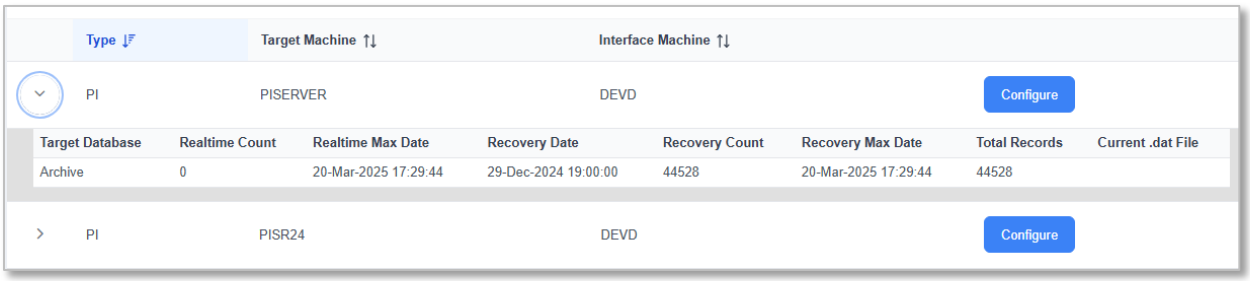
Below is a detailed explanation of each column in the AuditInterfaces table:

Column	Description
ID	Unique identifier for the audit interface. Auto incremented; not required to be added manually.
Type	Identifies the interface type. Possible values: "PI" or "AF".
InterfaceMachine	Hostname of the server where the data ingress service is installed. Default: "localhost".
TargetDatabase	Refers to the destination database where data is intended to be written or stored during data ingestion. Not used for PI interfaces. Must be ignored.
TargetDatabaseGUID	Refers to a Globally Unique Identifier (GUID) associated with a target database. Not used for PI interfaces. Must be ignored.
DatabaseEnabled	Referring to a configuration setting indicates whether a database-related feature is active or in use. Not used for PI interfaces. Must be ignored.
StartMode	Defines how data ingress operates for the interface. Default value is “Realtime”. The following options are available: Realtime: processes only real-time events starting from the moment of configuration. Recovery: process real time audit events starting from the moment of configuration and recovers past events from the RecoveryDate configured in column “RecoveryDate”.
RecoveryDate	Start date for recovery mode processing.
RealtimeStartDate	Start date for real-time processing.
ProcessedRecoveryCount	Total number of records processed in recovery mode.
ProcessedRecoveryMaxDate	Latest date processed in recovery mode.
ProcessedRealtimeCount	Total number of records processed in real-time mode.
ProcessedRealtimeMaxDate	Latest date processed in real-time mode.
TotalRecords	Total number of records processed (real-time + recovery).
BackupFilesDirectory	Directory containing backup audit database files to be imported.
AuditDatFilesDirectory	Directory containing current audit database files on the AVEVA PI Server. Default: "<PI Server installation drive>¥¥Program Files¥¥PI¥¥log".
ProcessArchiveAuditSubsystem	Flag indicating whether the archive subsystem database file should be processed. ☑ Yes (Checked) – The interface will process the archive subsystem database file. ☐ No (Unchecked) – The interface will skip processing the archive subsystem database file.

Column	Description
ProcessSnapshotAuditSubsystem	Flag indicating whether the snapshot subsystem database file should be processed.
ProcessBaseAuditSubsystem	Flag indicates whether the base subsystem database file should be processed.
CurrentDatFile	This setting identifies the specific audit database file that is currently being processed by the system. May change frequently if parallel processing is enabled.
ExclusionFilterStatus	Status of exclusion filters, updated manually via the web application's admin panel.
BackupFilesCopied	Flag indicating whether backup files have already been copied to prevent duplication.
Summary	It indicates the status of data ingestion. Possible values: "OK" or "Error".

For detailed instructions on configuring the PI interface, refer to Audit Interfaces view and Admin.

Once configuration is complete, the interfaces will appear as shown in the image below.



Web Application

The Web Application serves as the user interface of the application, enabling users to view audit trail records, generate reports, view logs, add users and add comments to records. The next step is to configure the Cognizant® PI Audit Trail Data Ingress Settings table, which defines the general configuration parameters used by the data ingress services within the Web application.

Web Application Configuration Settings

Service	Key	Default Value	Description
WebApplication:LogsQDB	Host	Server_name	Defines the hostname of the server where the data ingress service is installed.

Service	Key	Default Value	Description
WebApplication:LogsQDB	Database	Database_name	Defines the name of the database used to store data ingress configuration settings.
WebApplication:LogsQDB	PortPGWire	8812	Defines the port number used to connect to web application and transmit data.
WebApplication:LogsQDB	SslMode	prefer	Determines whether a secure connection (SSL) is used when connecting to web application. Available options: Prefer: SSL is preferred; if unavailable, the connection will proceed without SSL. Require: SSL is mandatory; if unavailable, the connection will be rejected.
WebApplication:LogsQDB	User	User_name	Defines the username for the account used to connect to the database.
WebApplication:LogsQDB	Password	Password Encrypted	Defines the password for the account used to connect to the database.
WebApplication:AuditTrailQDB	Host	Server_name	Defines the hostname of the server where the data ingress service is installed.
WebApplication:AuditTrailQDB	Database	Database_name	Defines the name of the database used to store data ingress configuration settings.
WebApplication:AuditTrailQDB	PortPGWire	8812	Defines the port number used to connect to web application and transmit data.
WebApplication:AuditTrailQDB	SslMode	prefer	Determines whether a secure connection (SSL) is used when connecting to web application. Available options: Prefer: SSL is preferred; if unavailable, the connection will proceed without SSL. Require: SSL is mandatory; if unavailable, the connection will be rejected.
WebApplication:AuditTrailQDB	User	User_name	Defines the username for the account used to connect to the database.

Service	Key	Default Value	Description
WebApplication:AuditTrailQDB	Password	Password Encrypted	Defines the password for the account used to connect to the database.
WebApplication	AppSettings:MaxAuditRecordsPerCall	10000000	Defines the maximum number of audit records that can be retrieved, processed, or returned per single call.
License	LicenseKey	License Key Encrypted	The license key provided by the vendor must be entered during the installation of the Web Application. This key is required to activate and authorize the application for use.
WebApplication	AppSettings:CryptoKey	No Default Value Provided	A text value used to encrypt and decrypt sensitive information like username, passwords and connection strings in Data Ingress Settings table. Please provide a 32 characters string text composed by letters, and numbers if you want to use your own key. If you enter or modify the key, all service must be stopped and all sensitive information must be set again to be encrypted using the new key.
WebApplication	AppSettings:CryptoPassword	No Default Value Provided	A text value used in the encryption and decryption process to secure data communication between client and server. Please provide a 32 characters string text composed by letters, numbers, signals, and special characters if you want to use your own password.
WebApplication	AppSettings:CryptoSalt	No Default Value Provided	A text value used in the encryption process to increase security and avoid predictable patterns like duplicated encrypted values. Please provide a 44 characters string text composed by letters, numbers, signals, and special characters if you want to use your own salt.

Reporting Service

The Reporting Service is a background windows service responsible for generating reports on demand. It can be run on the same server as the web application or on a separate web server.

This service handles both the reprocessing of failed reports and the recovery of in-progress report generations in the event of a failure. To maintain the health and consistency of the reporting service, a background routine runs at regular intervals - every 15 seconds by default, or as specified in the settings. These timed routines are responsible for reprocessing failed reports and processing requests that did not start properly. A routine removes cancelled reports and expired reports after the request, based on the expiration time specified in settings or 24 hours after the request, which is the default setting. These settings can be found under ReportsServiceConfiguration table in the Generate Report section.

How to initialize the AVEVA PI Audit Reporter application

When the Administrator user is installing and running the AVEVA PI Audit Reporter application for the first time, they must define the Domain Settings and set up the AVEVA PI Audit Reporter administrator account to log in to the AVEVA PI Audit Reporter Web application and create new users.

For detailed instructions, refer to AVEVA PI Audit Reporter Web Application documentation.

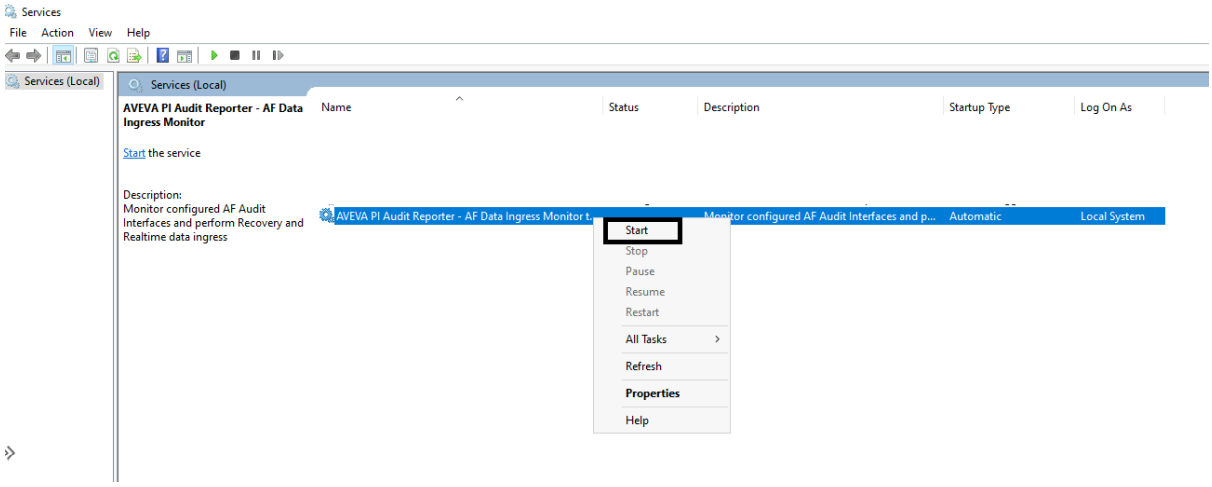
The AVEVA PI Audit Reporter version has been developed as per Architecture and some services must be started in the following sequence.

1. AVEVA PI Audit Reporter Web application – to start the user interface.
2. AVEVA PI Audit Reporter AF Data Ingress - to start reading and ingesting data from sources.
3. AVEVA PI Audit Reporter PI Data Ingress - to start reading and ingesting data from sources.
4. AVEVA PI Audit Reporter Reporting Service - to generate reports by using services.

Not following this order may cause start errors and require restarting the service.

To start AVEVA PI Audit Reporter Services, open the “Services” application in Windows and navigate to the AVEVA PI Audit Reporter services. In the screenshot below, the user sees all the services in the same server.

Select the Start option for each service, following the sequence mentioned above.

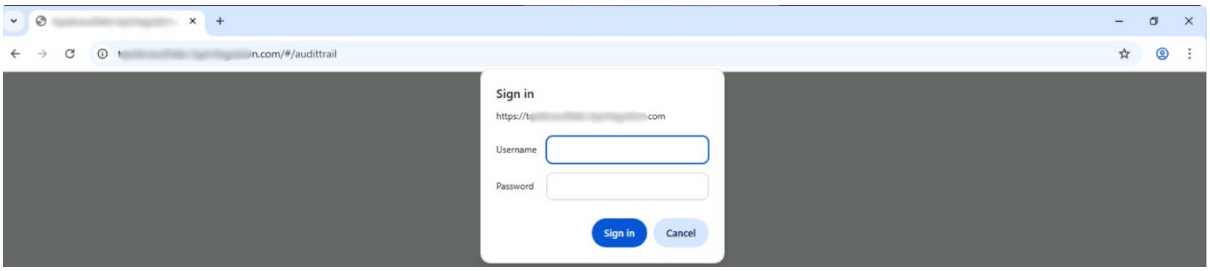


Sign In

The AVEVA PI Audit Reporter authentication functionality is integrated with Windows Active Directory using Windows Authentication. This ensures secure, centralized user management and seamless access control aligned with enterprise IT policies. The AVEVA PI Audit Reporter is compatible with Windows Active Directory (AD) environments from Windows Server 2012 onwards.

Windows Authentication Integration Overview

In the screenshot below, when accessing the AVEVA PI Audit Reporter application for the first time, after a period of inactivity (based on application pool idle timeout) or a server-side refresh of authentication settings, users will be prompted to re-enter their credentials. This ensures secure access and alignment with enterprise authentication policies. Password policies, account lockout, and multi-factor authentication (MFA) can be enforced centrally through Active Directory.



Note: Application pool idle timeout can be configured under application pool advanced settings as per step 8 of IIS installation procedure.

Security Implications

Listed below are some security implications for the PI Audit Reporter application:

- If Active Directory is compromised or unavailable, authentication may fail unless.
- Misconfigurations during user creation can lead to vulnerabilities or authentication failures.

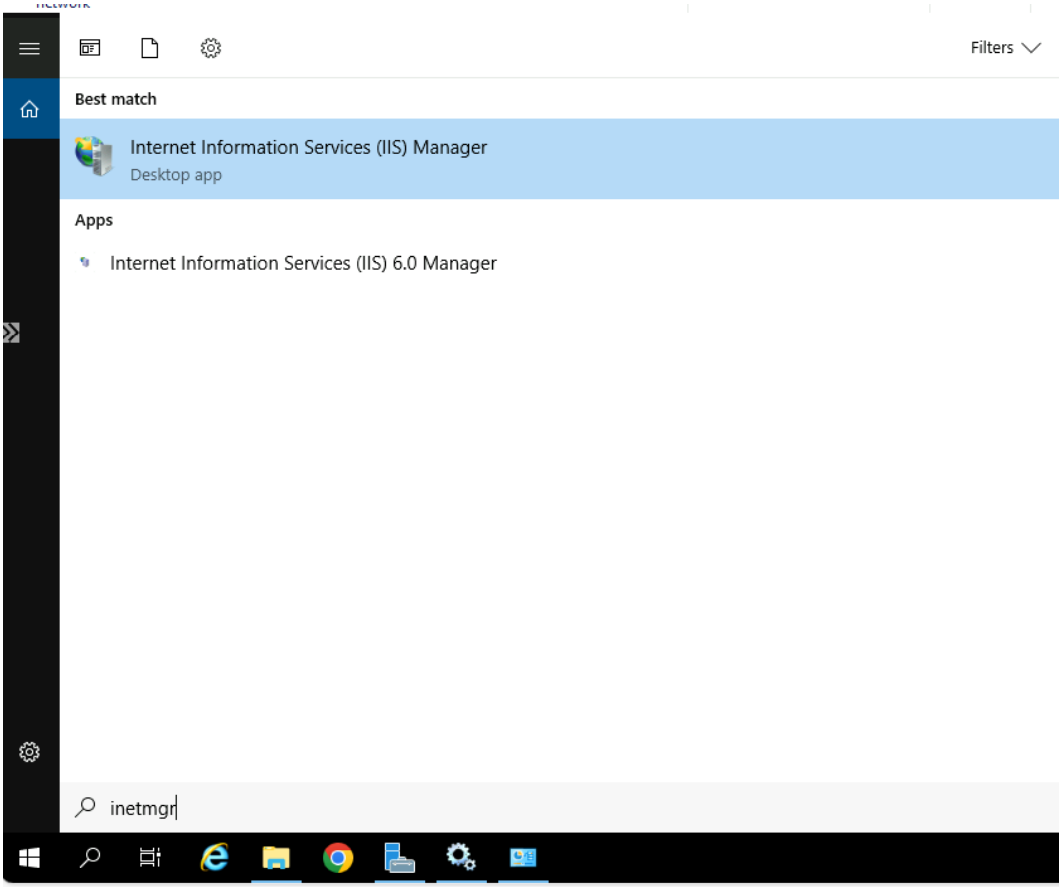
Application upgrade for AVEVA PI Audit Reporter

To upgrade the PI Audit Reporter, the recommendation is to uninstall the previous version before installing the new one. The existent version of AVEVA PI Audit Reporter database can be used with the new application version that will be installed. To perform this, some mandatory procedures are required as described in next sections.

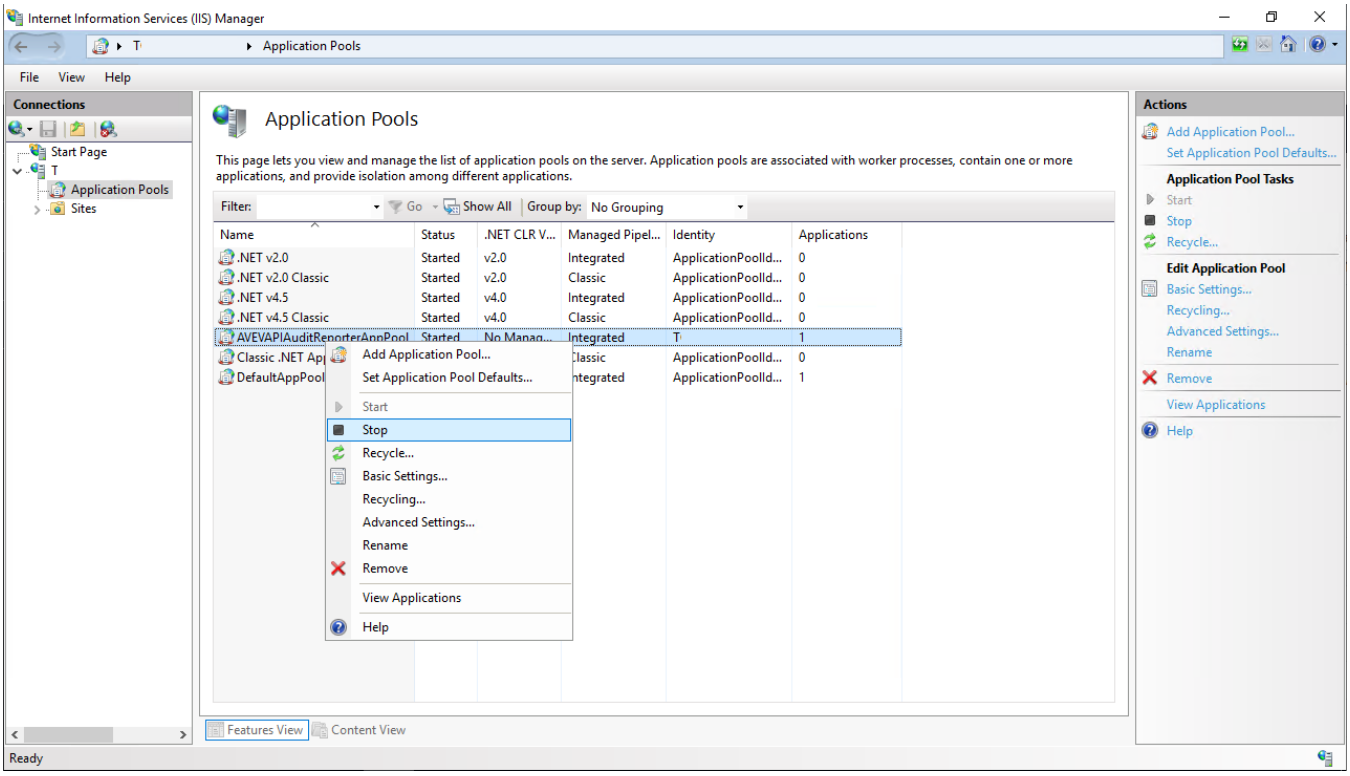
Create a backup of existing version

The backup of existing version of the application is essential to roll back the upgrade for any reason. Follow these steps to perform this:

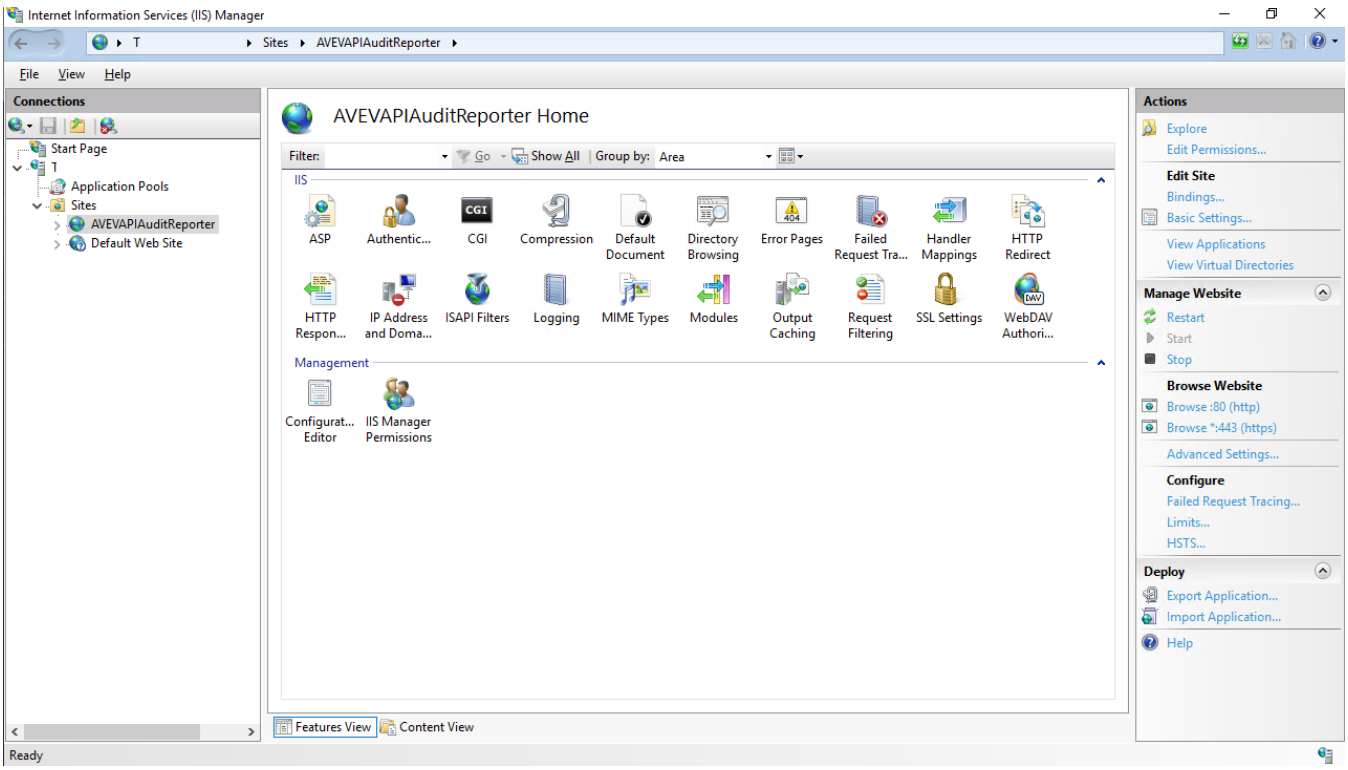
1. Open IIS Manager, go to the Start menu and type “inetmgr” in the search bar. Press Enter, and the Internet Information Services (IIS) Manager window will open.



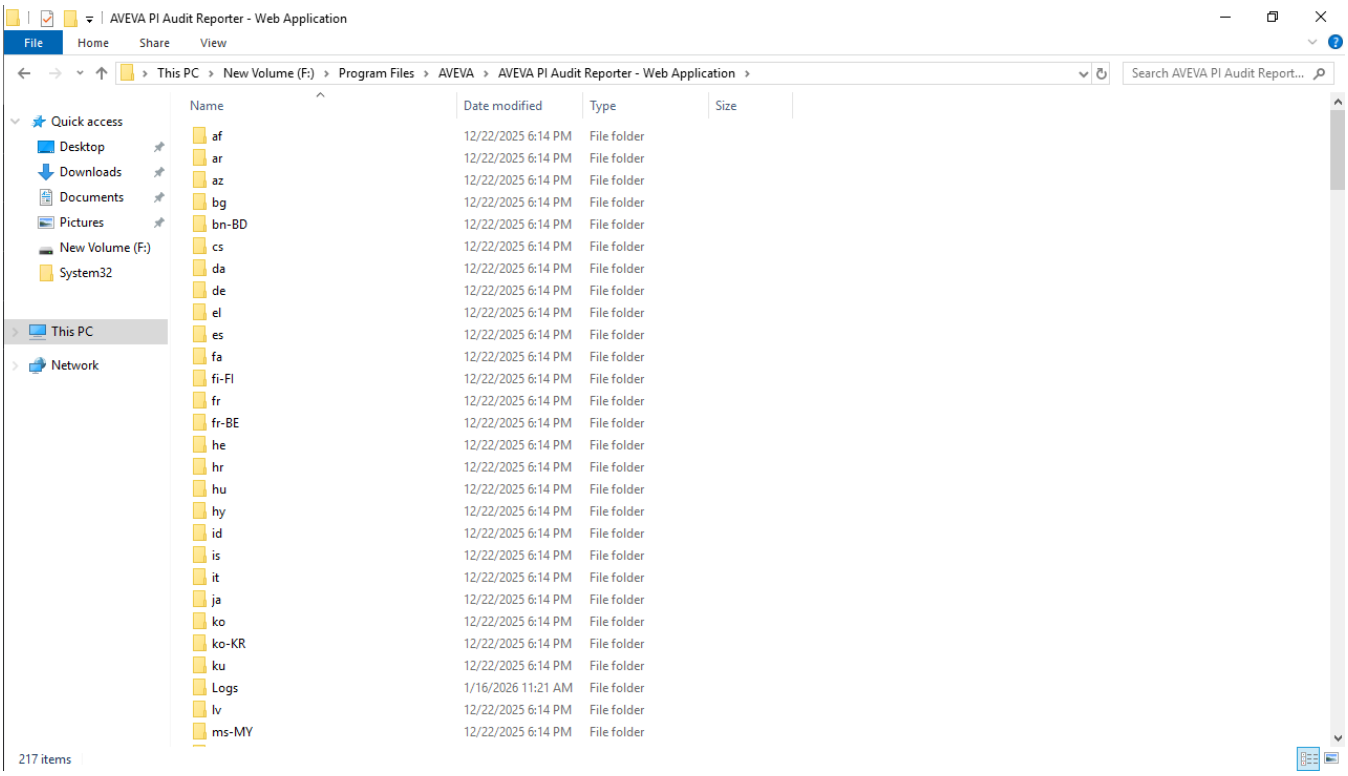
2. Expand the server’s name listed in the left-hand Connections panel, select the Application Pools item and locate the AvevaPIAuditReporterAppPool.
3. Right-click in the located application pool and stop.



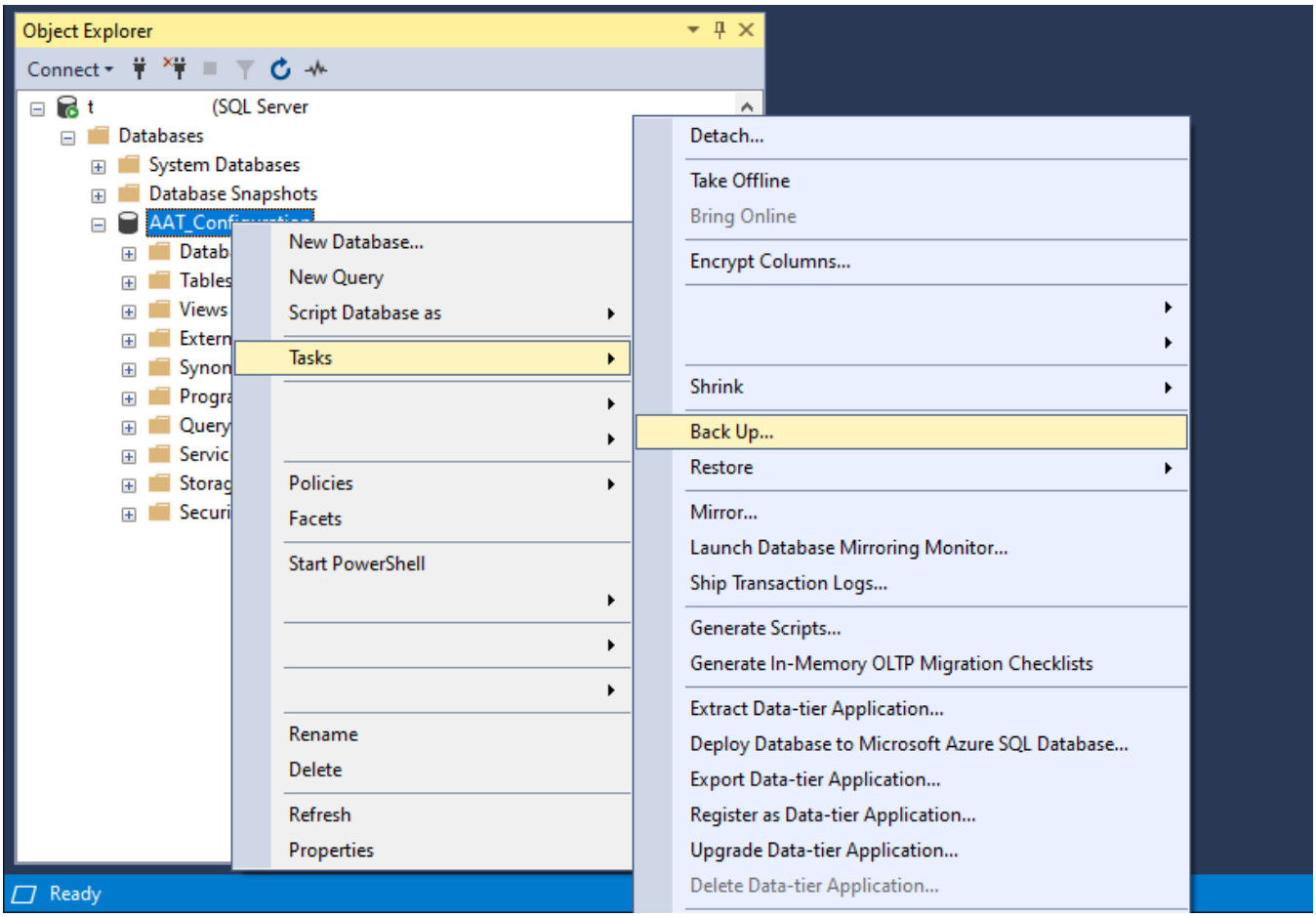
4. Expand the Sites list, locate the AvevaPIAuditReporter site and select Stop in right panel.



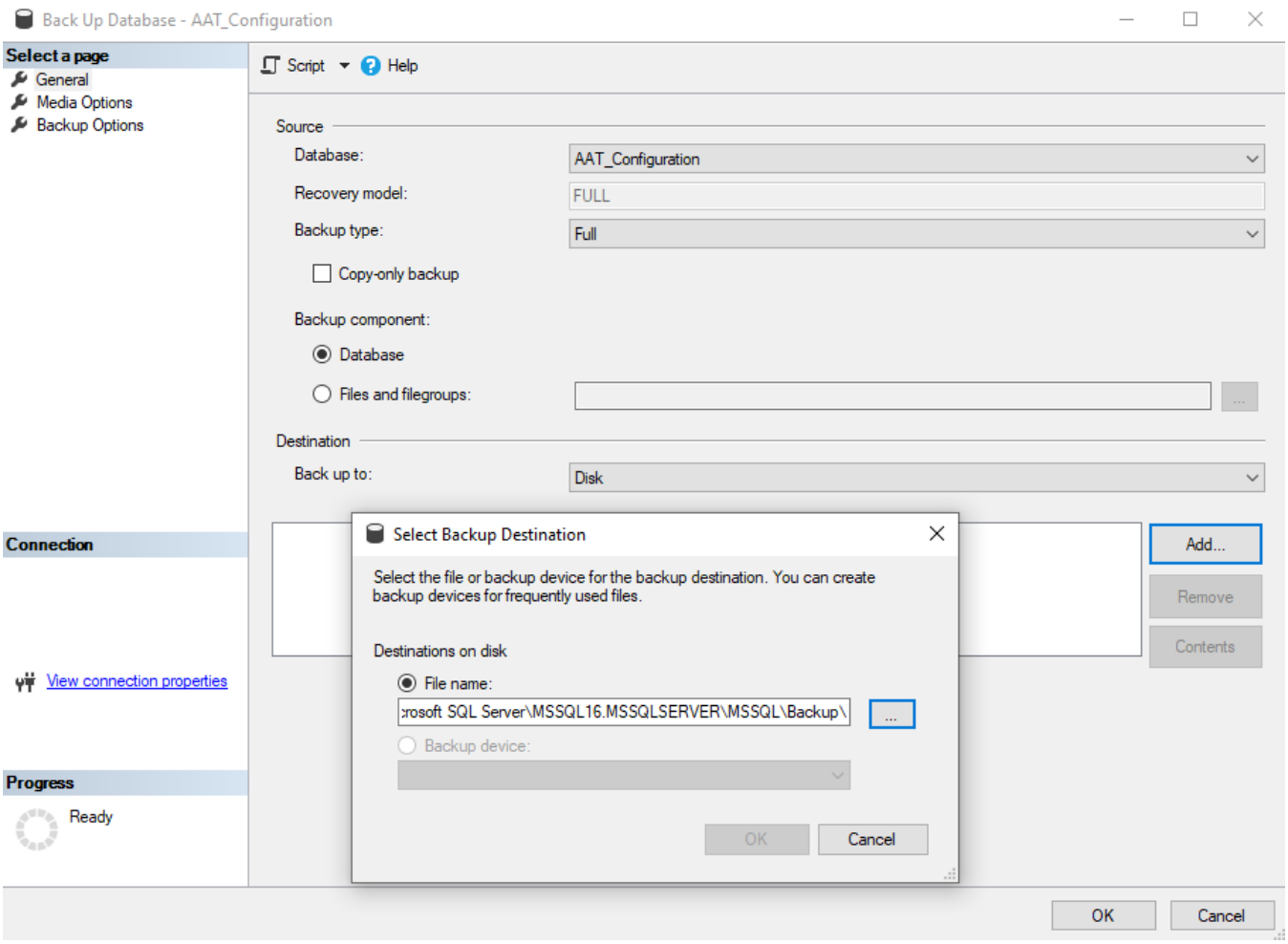
5. Once stopped, select the action Explore in right panel. It will show the Windows Explorer with all installation files.



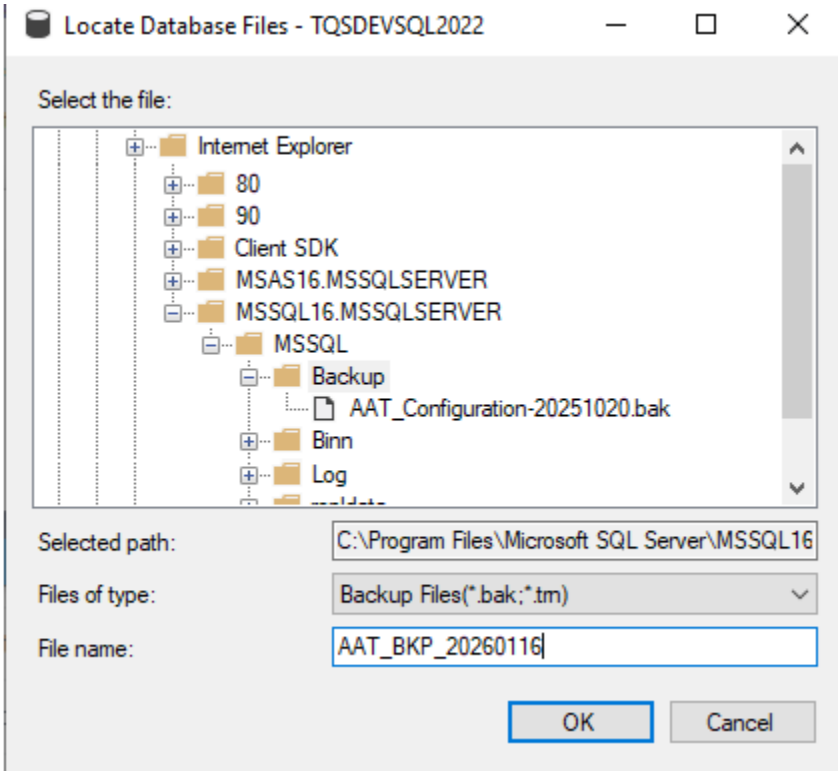
6. Copy these files to another directory (a different disk, if possible).
7. Launch SQL Server Management Studio and connect to the appropriate SQL Server instance.
8. In the Object Explorer, expand the Databases node and select the database currently used by the application.
9. Right-click in the selected database, Tasks, and select Backup.



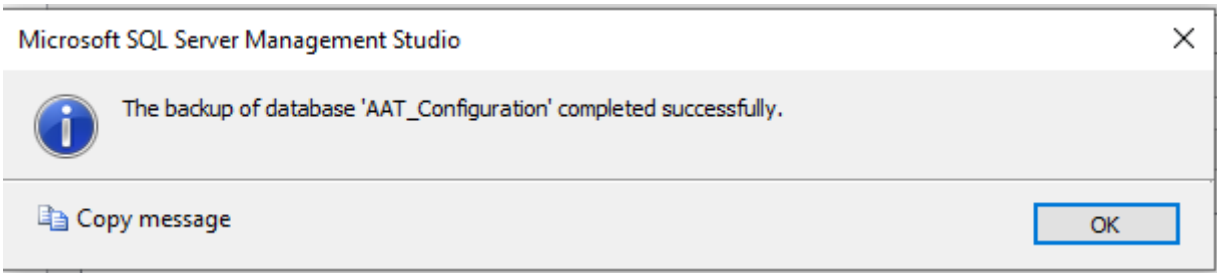
10. Click Add to select a backup destination.



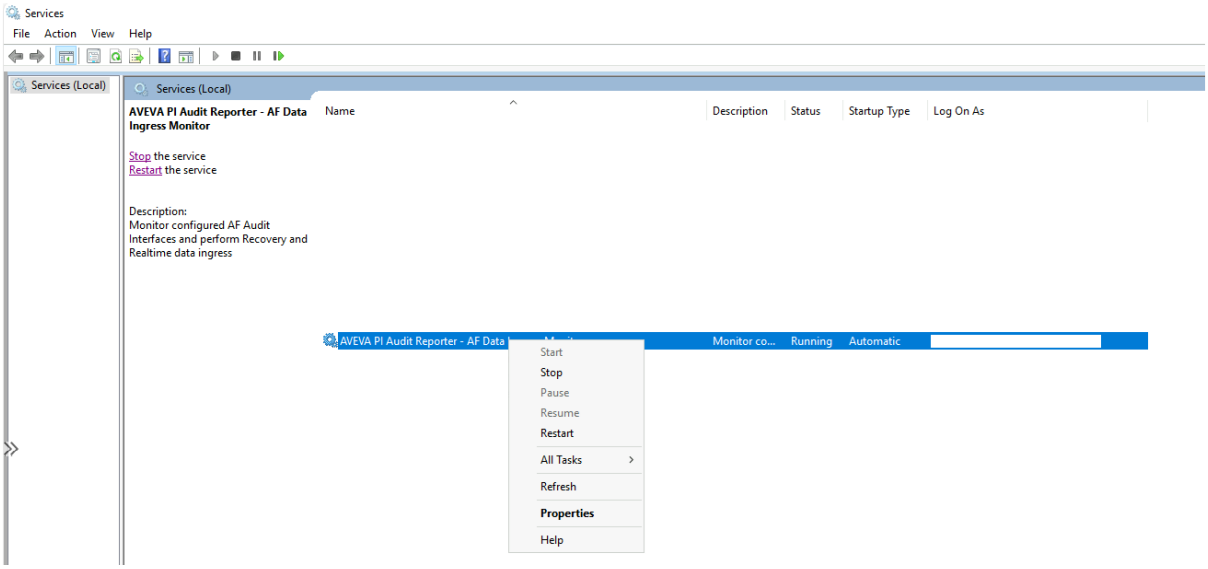
11. Select the ellipsis ([…]) to inform the file name.



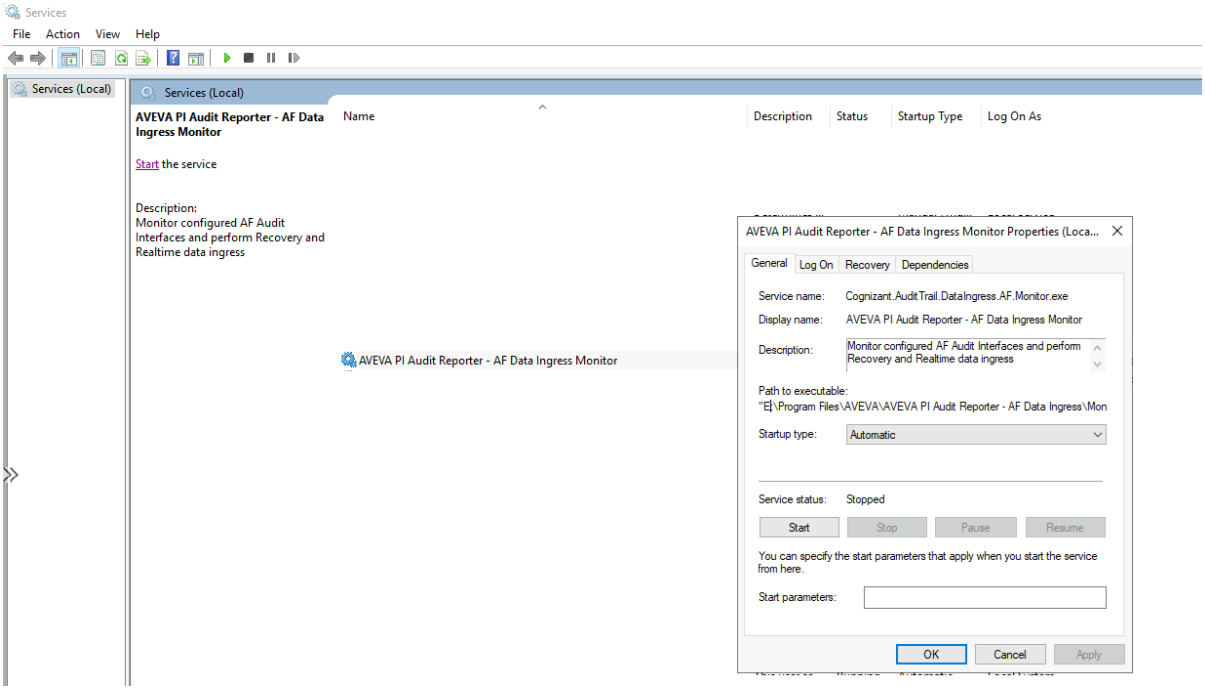
12. Click OK to confirm the database file name, then OK again to confirm the Backup settings and OK again to create the Backup.
13. A message appears once SQL database backup is complete.



14. Open the Windows Services Management Console.
    a. Press Win + R, type services.msc, and press Enter.
15. Locate the service named: AVEVA PI Audit Reporter - AF Data Ingress Monitor.
16. Right-click the service and select Stop from the context menu.



17. Right-click the same service entry in the Services Management Console.
18. Select Properties from the context menu.
19. In the General tab of the Properties window, locate the field labeled Path to executable.
20. This field displays the full file system path to the services executable file, indicating the directory where the service is installed.



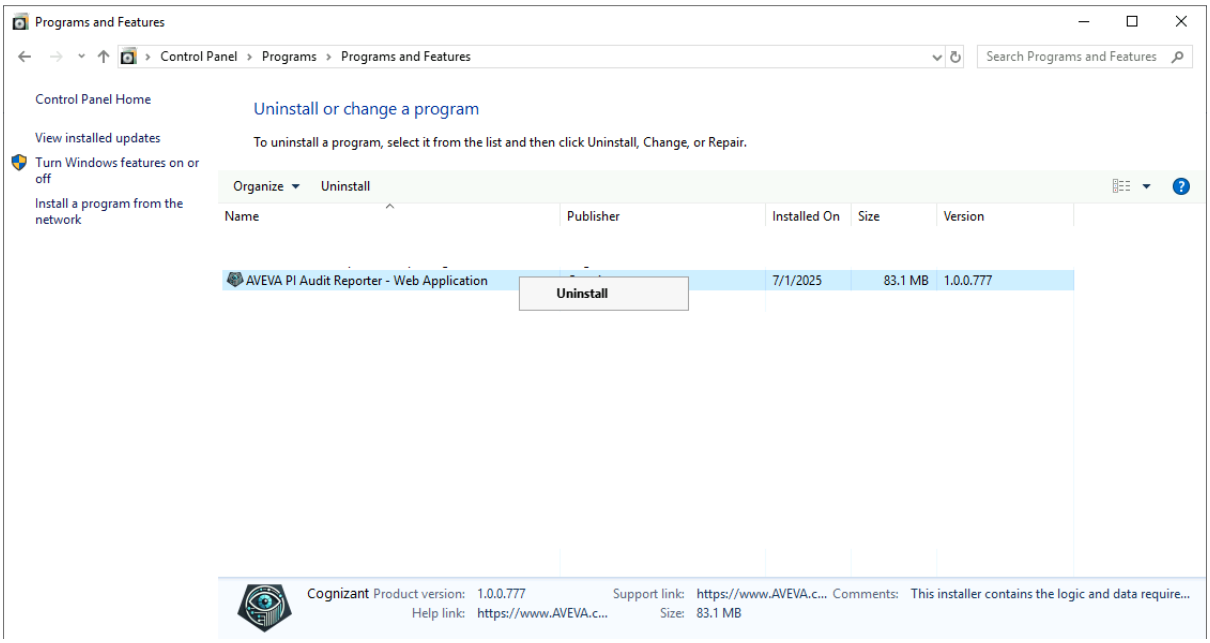
21. Using the Path to executable identified in the previous step, navigate to the corresponding directory in File Explorer.
22. Locate the folder named: AVEVA PI Audit Reporter - AF Data Ingress

23. Right-click the folder and select Copy.
24. Paste the copied folder in a different directory (a different disk, if possible).
25. Repeat the steps from step 14 to step 24 to create a backup for AVEVA PI Audit Reporter – PI Data Ingress and for AVEVA PI Audit Reporter – Reporting Services.

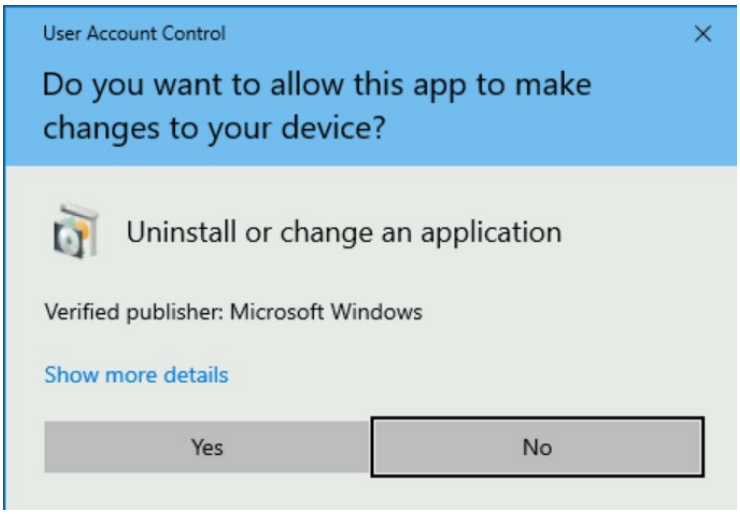
Uninstalling existing version

To uninstall AVEVA PI Audit Reporter application, the user must follow the following steps:

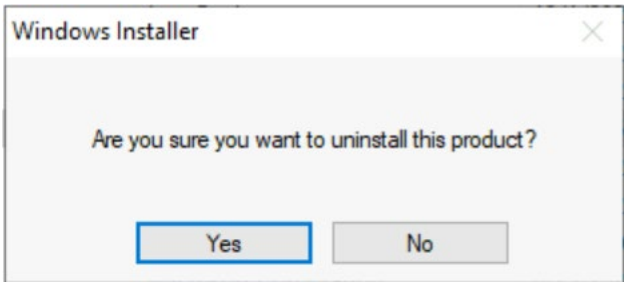
1. Navigate to: Control panel > Programs > Programs and Features.
2. Then select the program 'AVEVA PI Audit Reporter Web application', right-click and then Select uninstall.



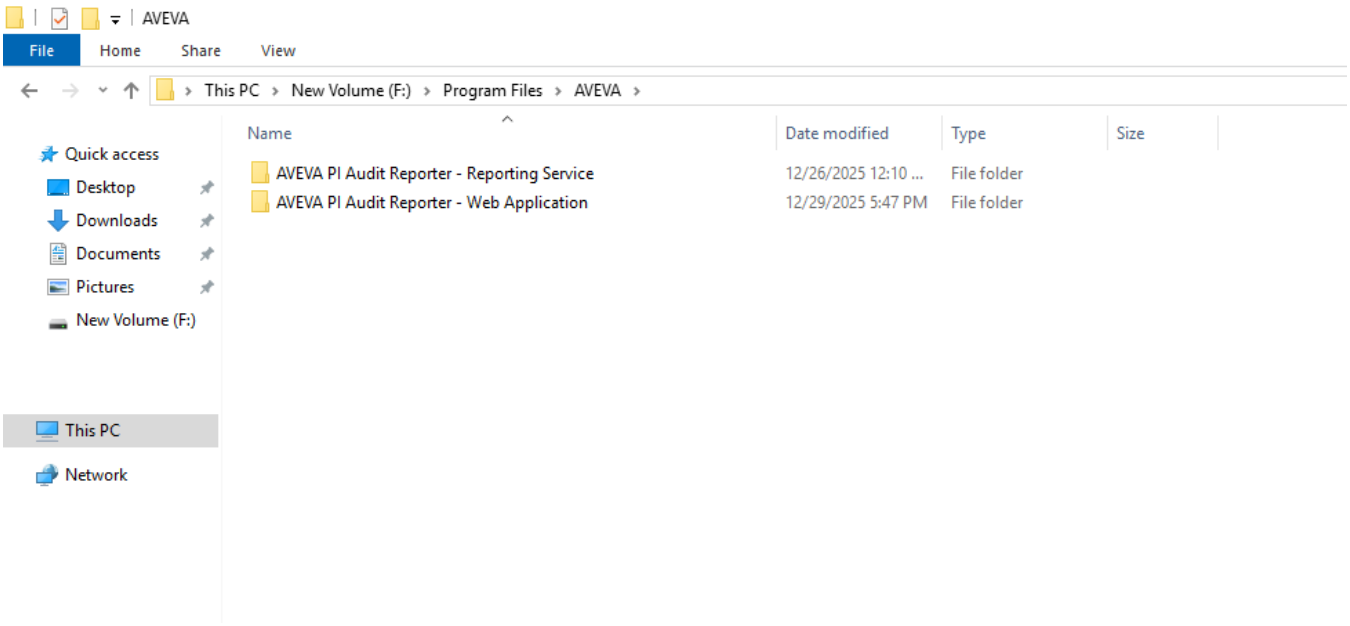
3. After selecting the uninstall option, the "User Access Control" screen will then be displayed. Select 'Yes' option to uninstall the application as shown below.



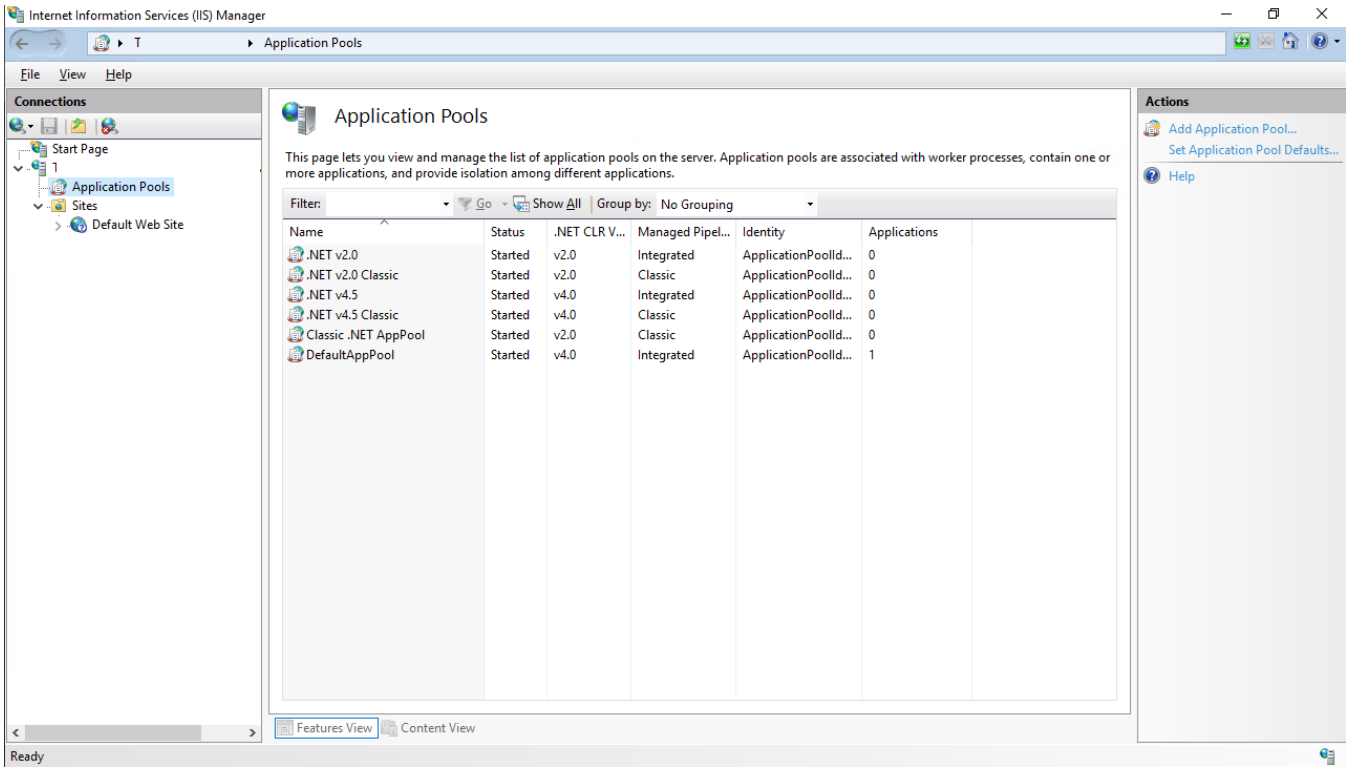
4. Select ‘Yes’ in Windows Installer screen to Uninstall AVEVA PI Audit Reporter Web application. AVEVA PI Audit Reporter Web application will be removed from Control panel > Programs > Programs and Features.



5. Delete remaining folders and files from installation directory.



6. AVEVA PI Audit Reporter Site and AVEVA PI Audit Reporter application pool were deleted in the IIS Manager by the uninstalling process.



7. Repeat steps from step 1 to step 5 to uninstall of AVEVA PI Audit Reporter AF Data Ingress, AVEVA PI Audit Reporter PI Data Ingress and AVEVA PI Audit Reporter Reporting service.

Installing existing version

After the completion of the steps above, run the new AVEVA PI Audit Reporter services with admin privileges as the user needs write-permission to the file system. Refer to Prerequisites for installation requirements followed by the Installation procedure. Do not start any AVEVA PI Audit Reporter services.

Check the database version compatibility running this SQL Query in the server:

```
SELECT compatibility_level from sys.databases  where name = 'Database_name';
```

If the result is lower than 130, run the following command. If not, there is no need to update the compatibility level because it is correct.

```
ALTER DATABASE (Database_name) SET COMPATIBILITY_LEVEL = 130;
```

Note: For more details about the SQL Server compatibility level, please refer to Microsoft portal

Execute the following steps to complete the AVEVA PI Audit Reporter upgrade:

- Start AVEVA PI Audit Reporter AF Data Ingress service.

Start AVEVA PI Audit Reporter PI Data Ingress service.

Start AVEVA PI Audit Reporter Reporting service.

Start the AVEVA PI Audit Reporter Application Pool in IIS Manager.

Open the web browser and navigate to the AVEVA PI Audit Reporter website. Check that the user can login with credentials.

Audit trail record data structure

The Normalized Audit trail record will have the following structure in QuestDB table:

Field	Type	Description
Uid	Uniqueidentifier	Unique ID for the record in database
Server	String	Server where the data is to be retrieved
Source	String	PI or AF
Date	Datetime	Date and time of audit trail record
Action	String	Change type, New, Modified, Excluded
Category	String	Object changed
Database	String	Database
Id	String	Unique Id of the object
Name	String	Name of the item changed
User	String	User that made change
UserID	String	User ID that made change
Path	String	Root path of item changed
Details	Array of Detail item	JSON with the nested child items related to the data modifications that contains the audit trail record
Reviews	String	Reviews made by users through web application
Reason	String	Reason inserted by user for that audit event
ChangeNo	String	Number of changes made
UserComment	String	Comments added by user for that audit event
TargetDatabaseGuid	Uniqueidentifier	Unique identifier of source database for the audit event
Excluded	Boolean	Marks if audit trail record is shown or not in the web application and reports based on Exclusion Filters
Hash	String	Hash of audit trail record
ChunkExecutionGUID	String	Unique identifier of chunk that generated the record in QuestDB table
Deleted	Boolean	Marks if the record was deleted
itemDescription	String	The list of items descriptions concatenated with “\u001f”
itemName	String	The list of items names concatenated with “\u001f”

Field	Type	Description
itemId	String	The list of items ids concatenated with “\u001f”
itemProperty	String	The list of items properties concatenated with “\u001f”
itemOldValue	String	The list of items old values concatenated with “\u001f”
itemOldType	String	The list of items old types concatenated with “\u001f”
itemNewValue	String	The list of items new values concatenated with “\u001f”
itemNewType	String	The list of items new types concatenated with “\u001f”

Mapping to PI/AF Audit trail records

PI and AF audit trail records will be displayed using the below mapping in the frontend application.

Proposed	Description	PI Audit field	AF Audit field
Server	PI/AF Server Name	N/A	N/A
Source	PI or AF – source of where this data comes from	N/A	N/A
Date	Date and Time of the Action	Action Time	Date
Action	Action executed	Audit Action	Action
Category	Category of the record	Category	Type
Database	PI or AF Database	PI Database	Database
ID	PI or AF record ID	DB RecordID	ID
Name	PI or AF record name	DB RecordName	Name
Path	Path to the record	PI Database \ DB RecordName	Path
User	User who performed the action	PI Username	User
UserID	User ID who performed the action	PI User ID	N/A
Details	Contains the audit trail record child items for modifications	Changes	Details

Roles & Responsibilities

The table below outlines the configuration of roles and responsibilities for the AVEVA PI Audit Reporter application. These configurations are established during the initial deployment phase and are maintained throughout the system's lifecycle.

Functionality	**Administrator**	**Reviewer**	**Viewer**
Administration			
Allow Access	Yes	No	No
Allow Access Domain Groups	Yes	No	No
Allow Manage Domain Groups	Yes	No	No
Allow Access Users	Yes	No	No
Allow Manage Users	Yes	No	No
Allow Access Roles	Yes	No	No
Allow Manage Roles	Yes	No	No
Allow Manage Report Settings	Yes	No	No
Audit Trails			
Allow Access	Yes	Yes	Yes
Allow Generate Reports	Yes	Yes	Yes
Allow Comments	Yes	Yes	Yes
Allow Read Comments	Yes	Yes	No
Reports			
Allow Access	Yes	Yes	Yes

CHAPTER 6

AVEVA™ PI Audit Reporter application

AVEVA PI Audit Reporter application has four main options in menu that are dynamically displayed based on the logged-in user's access permissions. If a user does not have the necessary privileges (see in Roles & Responsibilities section) to view a specific resource, the corresponding menu item will not be visible. Additionally, if the user attempts to access a restricted resource directly via URL, an "Authorization required" message will be presented.

The menu section includes the following options: Audit Trails, Reports, Reports Queue and Admin. All of them will be better described in the subsequent sections.

Audit trails

The Audit trails section provides instant and summarized information of PI and AF audit trail information from the AVEVA PI system. To access this section, users must select the Audit Trails tab to be directed to the <AVEVA PI AUDIT REPORTER SERVER NAME /audit-trails> Audit Trails Page.

Audit trails search

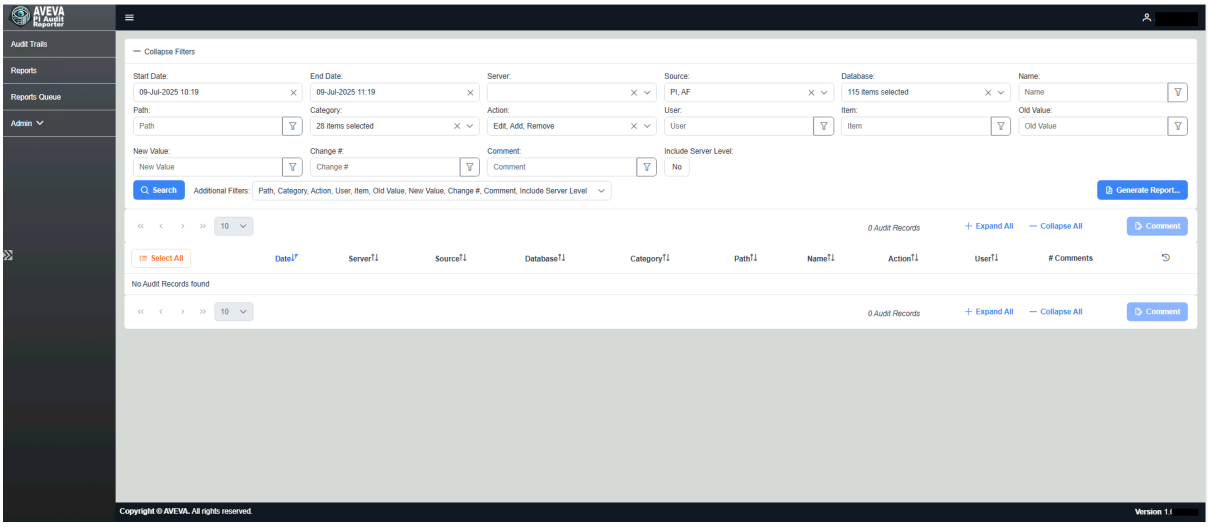
On the Audit trail page, users can utilize the available filters to search for audit records based on a specific criteria. The following are the default filters available to the user to refine and customize the audit trail records:

- Start Date: Defines the beginning of the reporting period.
- End Date: Defines the end of the reporting period.
- Server: Filters records by the PI or AF server name.
- Source: Defines the origin of the data. (PI or AF).
- Database: Filters by the associated PI or AF database.
- Name: Searches for specific tag names or element names.

These optional filters can be used as needed to further refine results:

- Path: Filters by the full hierarchy path like Starts with, ends with, Contains, Not Contains, Equals and Not Equals.
- Category: Filters by assigned category or classification.
- Action: Filters by the type of action. (e.g., Edit, Add, Remove).
- User: Filters by the user who performed the action.

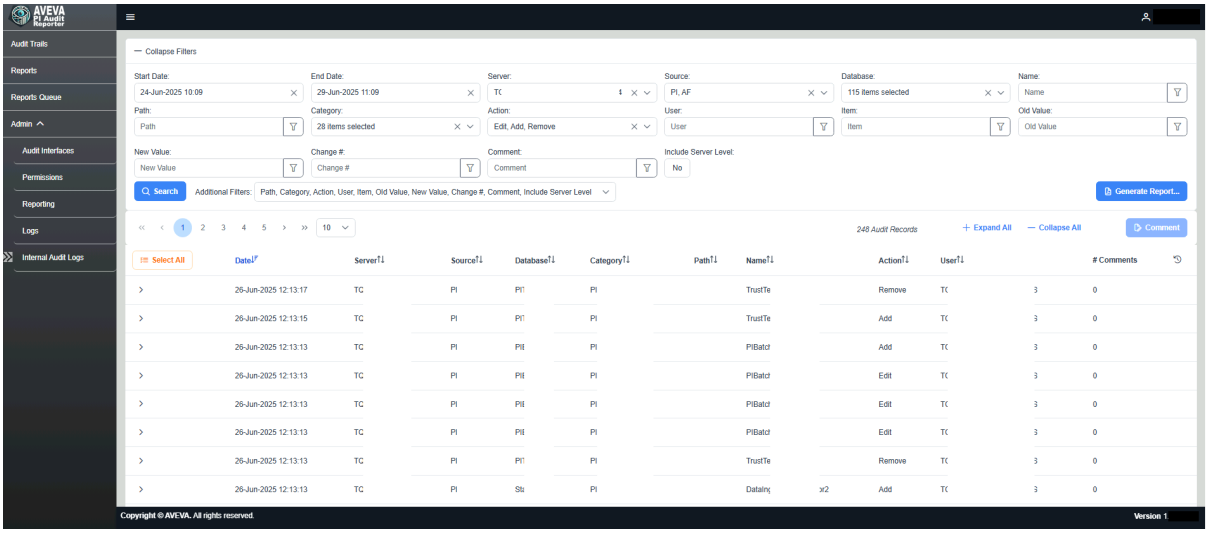
- Item: Filters by the specific item or object affected.
- Old Value: Filters based on the previous value before the change.
- New Value: Filters based on the updated value after the change.
- Change #: Filters by the unique change identifier.
- Comment: Filters by user-entered comments.
- Include Server Level: Option to include or exclude server-level changes in the results.



The results of the Audit trail records will include the fields below:

- Date
- Server
- Source
- Database
- Category
- Path
- Name
- Action
- User
- # Comments

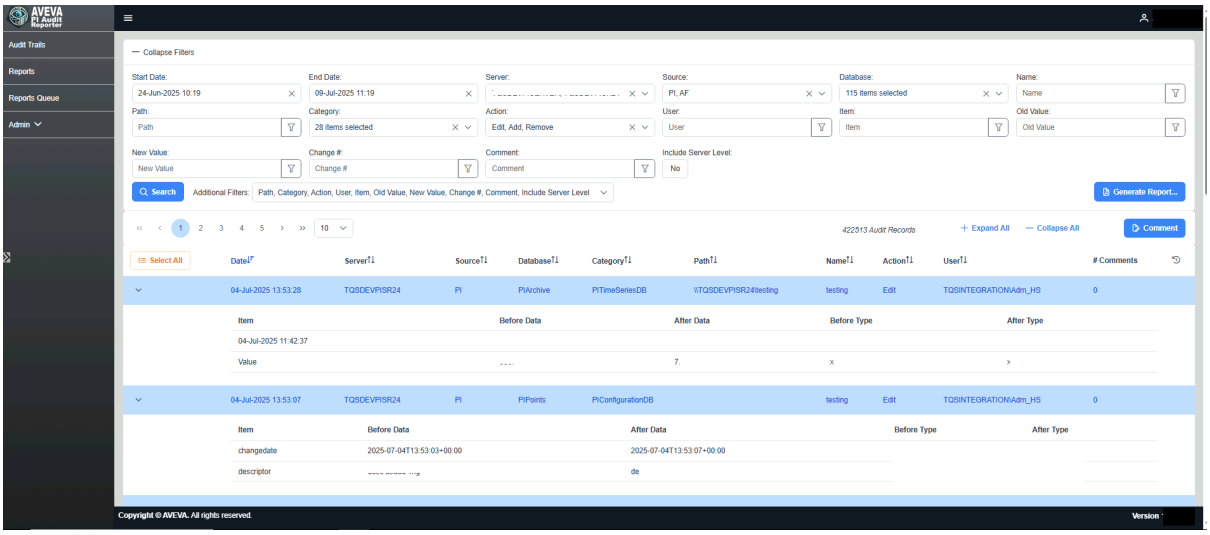
Refer to the screenshot below to verify Audit Trails Search results View



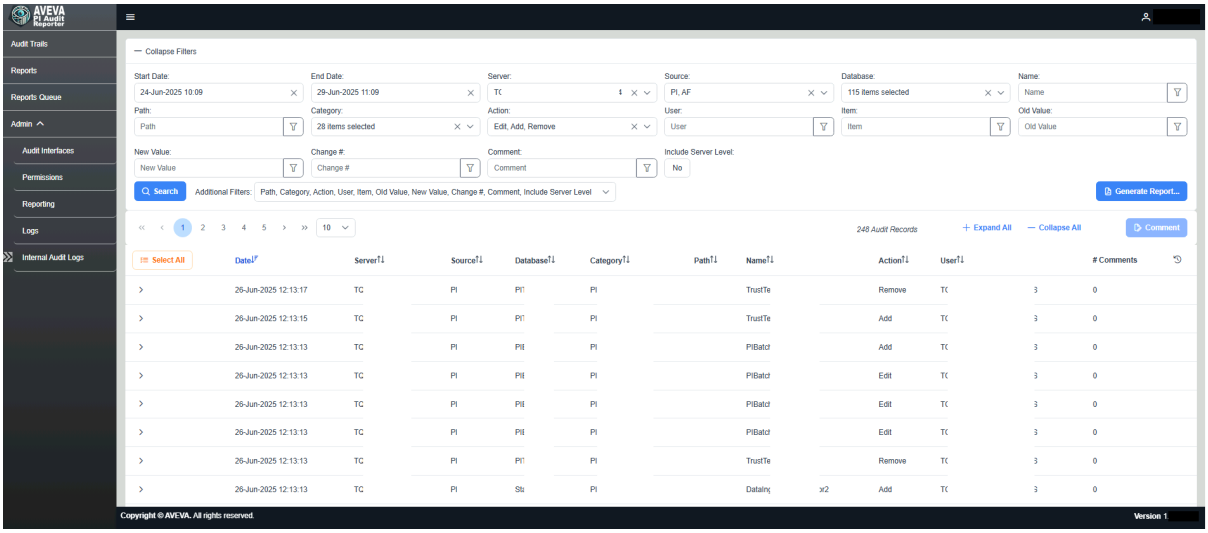
With the applied filters, users can generate audit trail records that display all relevant fields, as shown above. This allows for a comprehensive and customized view of the audit data, tailored to the selected criteria.

Expand All options

On the Audit trails page, the user can add all filter option and with “Expand all” option. These options allow users to view the complete list of audit trail records in a detailed and fully expanded format.



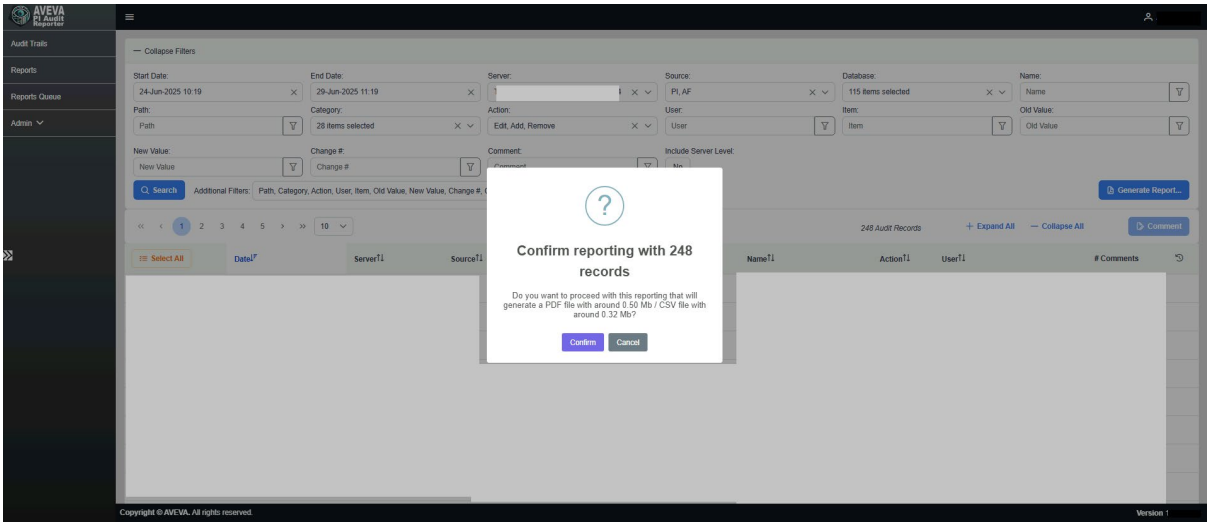
After expanding the details for all audit trail records, user can select the “Collapse All” option to hide all details.



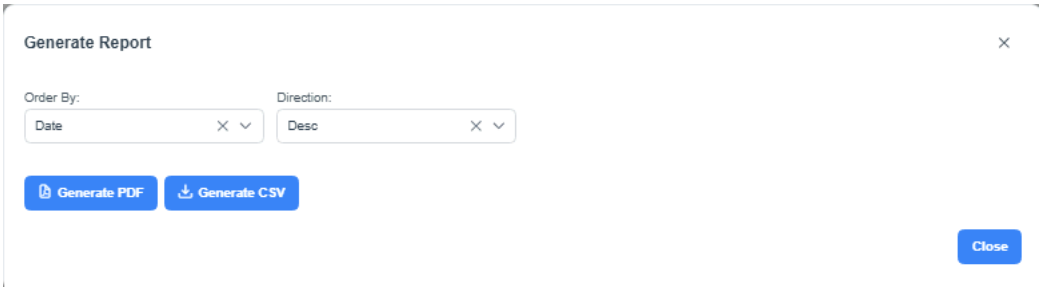
Generate report

Users can export audit trail reports in PDF and CSV formats using the following steps:

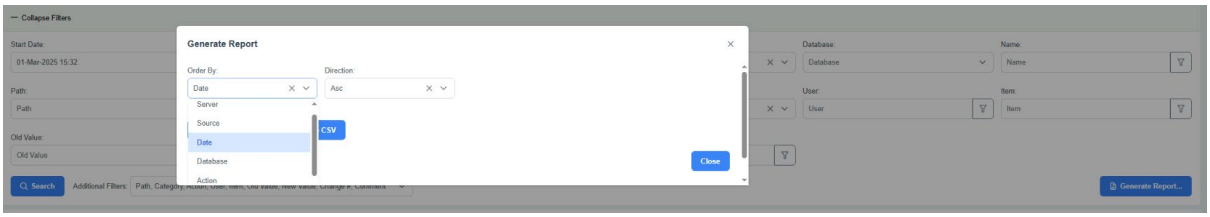
1. When the Generate Report option is selected, a confirmation popup window is displayed, prompting the user to confirm the report generation.



2. After selecting confirm in the Generate Report popup window, the user is prompted to select sorting options: “Order by” and “Direction” dropdown options.



3. Under the “Order by” dropdown, review the options such as Source, Type, Date, Database, Action, Category, Name and User.
4. Select options from the dropdown to generate reports based on the selected filter.



5. On the Generate Report popup, select the “Direction” options and generate reports in either Asc (Ascending) or Desc (Descending) order.
6. Once a PDF or CSV report format is selected, the file is queued in the Reports Queue section. Monitor its status and download the report once it is ready.

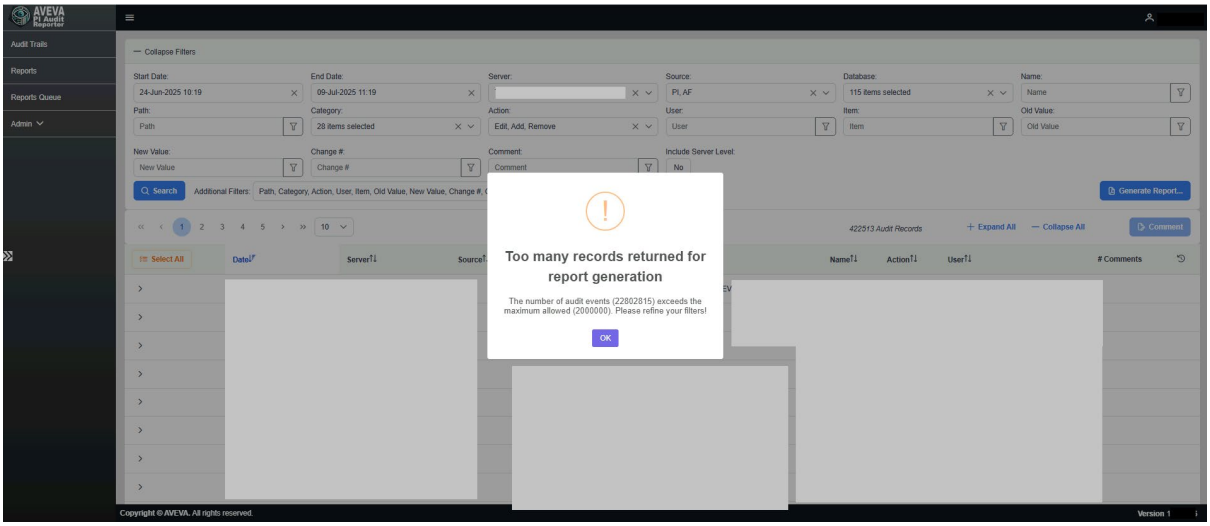
To ensure system stability and prevent interruptions or exceptions during report processing, the application enforces a maximum limit on the number of audit trail records that can be included in a report.

This limit is defined by a configurable parameter in the database of ReportsServiceConfiguration table:

Configuration key	Default value	Definition
MaxAuditRecordsItemsAllowed	2,000,000 (two million records)	Specifies the maximum number of audit record items that can be stored or processed. This helps control memory usage and performance in systems that track user or system activity.
ReportsExpirationTimeInHours	24	Determines how long generated reports remain available before they expire or are deleted. A value of 24 means reports is retained for 24 hours.

Configuration key	Default value	Definition
CheckReportsIntervalInSeconds	15	Sets the frequency (in seconds) at which the system checks for new or updated reports. A value of 15 means the system checks every 15 seconds.
LicenseKey	License Key Encrypted	The license key provided by the vendor must be entered during the installation of the Web Application. This key is required to activate and authorize the application for use.

If the number of audit trail records matching the selected filters exceeds this threshold, the system displays a warning message to the user and prevent the report generation request from proceeding. This safeguard helps maintain optimal performance and avoids overloading the reporting service.



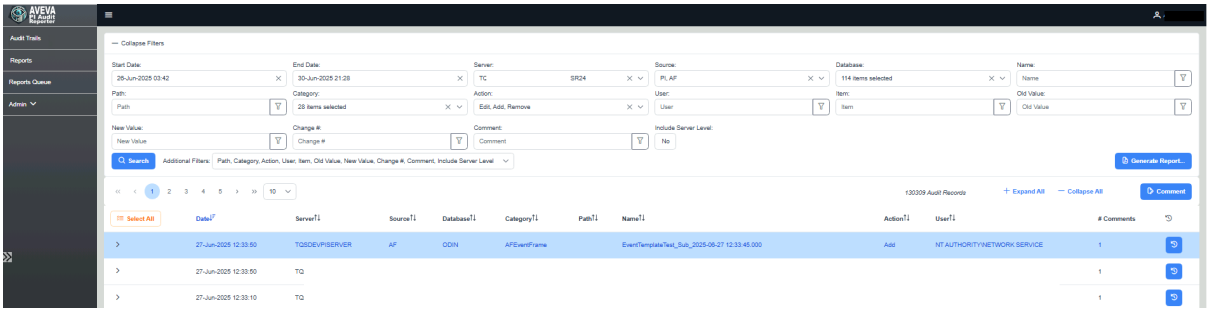
Add comments

Users can add comments on the audit trail records. The PI Audit Reporter allows users to add comments to a specific audit record or to add comments to a group of audit records.

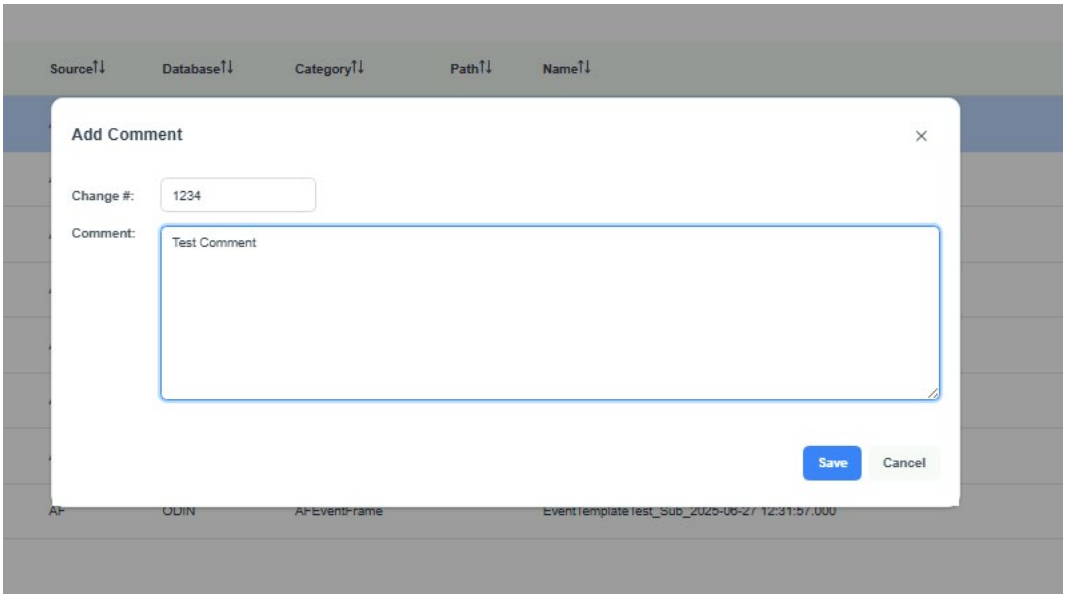
Add comments to a specific audit record

To add comments to a specific audit record, users must follow the steps below:

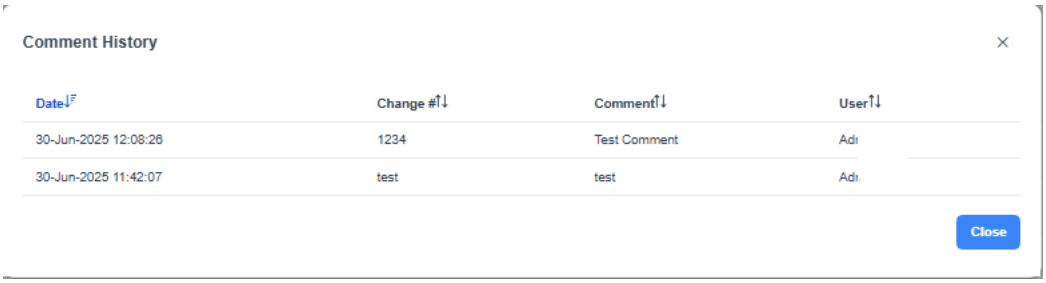
1. Choose a single audit trail record from list and then select the “Comment” option.



2. When selecting the “Comment” option after choosing single audit trail record, the “Add Comment” popup window is displayed.
3. Pop-up window displays “Change #” and “Comment” fields to add in a remark or relevant notes. Select “Save” to attach the comment to the selected audit trail record.



4. View all saved comments on audit trail records by using the comment history option.



Add comments to multiple audit records

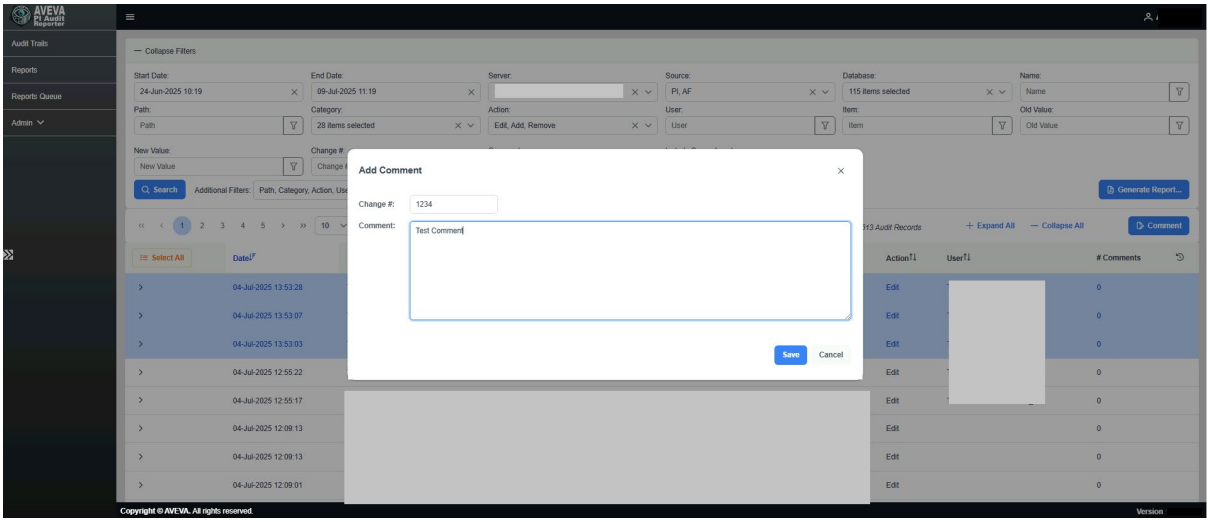
To add comments to multiple audit records simultaneously, users must follow the steps below:

1. Select multiple audit trail records from list and then select the “Comment” option.

Note: Mark “Select All”/ “Unselect All” option to select/unselect all the search results.

2. The “Add Comment” popup window appears and it shows the Change # associated with the audit trail records.
3. Add a comment by providing the comment details and selecting “Save” to attach the comment to the selected audit trail records.

CHAPTER 7



Reports

The Reports section allows users to generate reports about the audit trail records based on selected criteria. To access this section, users must select the Reports tab to be directed to the <AVEVA PI AUDIT REPORTER SERVER NAME /reports> Reports Page.

Reports Generation

On the Reports page, users can utilize the available filters to generate the reports based on a specific criteria. The following are the default filters available to the user to refine and customize the report:

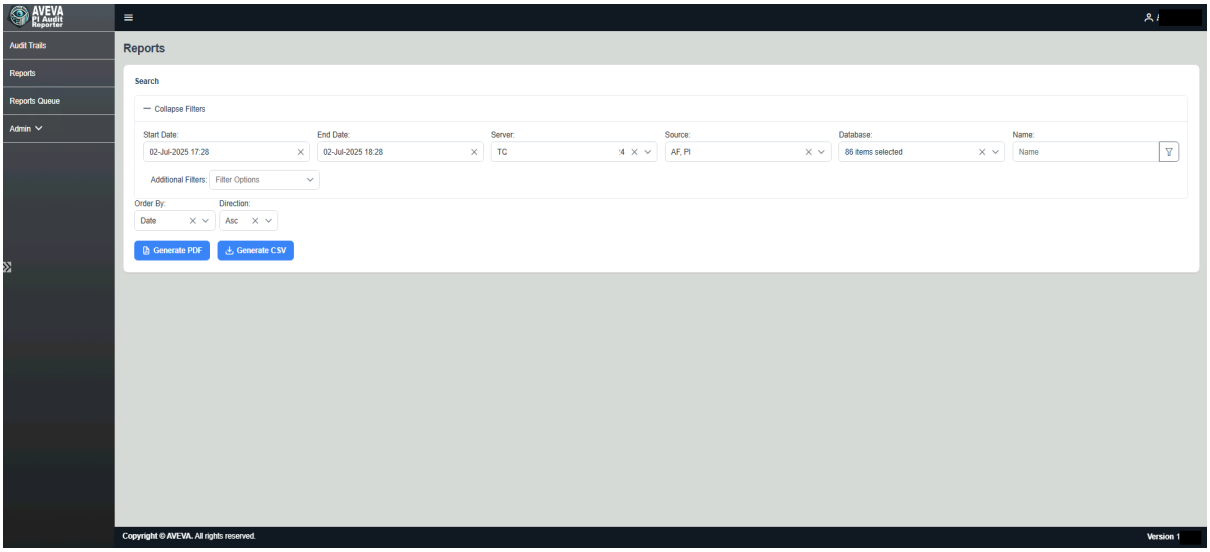
- Start Date: Defines the beginning of the reporting period.
- End Date: Defines the end of the reporting period.
- Server: Filters records by the PI or AF server name.
- Source: Defines the origin of the data (PI or AF).
- Database: Filters by the associated PI or AF database.
- Name: Searches for specific tag names or element names.

These optional filters can be used as needed to further refine results:

- Path: Filters by the full hierarchy path like Starts with, ends with, Contains, Not Contains, Equals and Not Equals.
- Category: Filters by assigned category or classification.
- Action: Filters by the type of action. (e.g., Edit, Add, Remove).
- User: Filters by the user who performed the action.

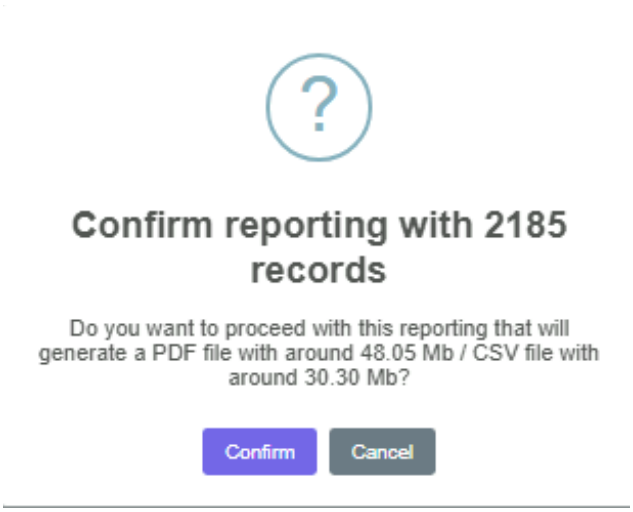
- Item: Filters by the specific item or object affected.
- Old Value: Filters based on the previous value before the change.
- New Value: Filters based on the updated value after the change.
- Change #: Filters by the unique change identifier.
- Comment: Filters by user-entered comments.
- Include Server Level: Option to include or exclude server-level changes in the results.

Users can use the above filters to generate reports as per their requirements.



To generate a report, the following steps are required:

1. Review the default filters that are automatically applied.
2. Add any extra filters if needed by selecting Additional Filters and choosing the options to apply.
3. Select the Order By field. Default value is by Date.
4. Select the Direction field. Default value is Asc (ascending).
5. Select Generate PDF (if a PDF file is required) or Generate CSV (if a CSV file is required).
6. A confirmation popup window is displayed, prompting the user to confirm the report generation which asks for user confirmation of the file size and then confirm the request.



7. Select Confirm to proceed.
8. The request is sent to the Reports Queue section.

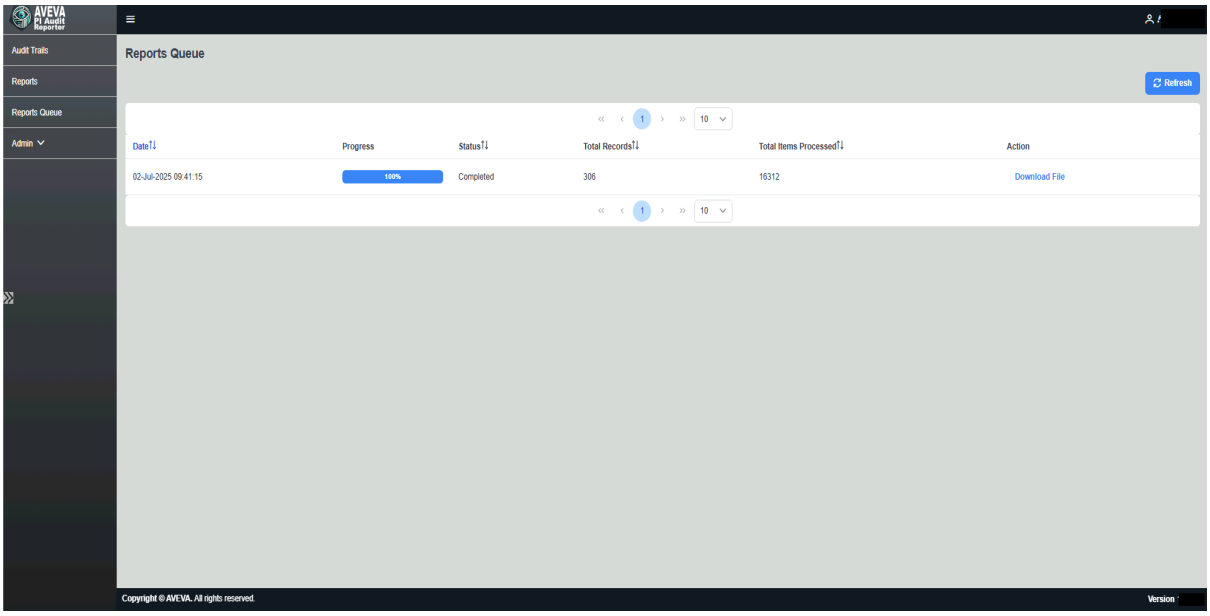
Note: For this feature, the same behavior as Audit trails page will occur, refer to Audit trails - Generate Report.

Reports Queue

The Reports Queue section displays all report generation requests - whether initiated from the Reports or Audit Trail section. This includes both PDF and CSV file formats. To access this section, users must select the Reports queue tab to be directed to the <AVEVA PI AUDIT REPORTER SERVER NAME/reports queue> Reports Queue Page. Report Queue display includes the following:

- Date: The timestamp when the report request was submitted. (This column can be sorted in ascending or descending order).
- Progress: Shows the percentage of records processed. (Provides a visual indicator of report generation progress).
- Status: Indicates the current state of the report (e.g., Queued, In Progress, Completed, Failed).
- Total Records: The total number of audit trail records included in the report.
- Total Items processed: The number of records processed.
- Actions: Cancel a report request that is currently being processed or select to download a file after completion.

This section helps users monitor the status of their report requests and manage them efficiently.



After completion, the user can select the Download file to view the file on their local system.

AVEVA PI Audit Reporter - Report

Date	Server	Source	Database	Action	Category	Name
01-Jul-2025 10:40:59	T	AF	AF Audit trail testing	Add	AFEventFrame	Analysis4 2025-07-01 09:40:54.000

Details:

Id	Name	Property	Description	Old Value	New Value
19331024	Analysis4 2025-07-01 09:40:54.000	rid			19331024
19331024	Analysis4 2025-07-01 09:40:54.000	id			7C2F8157-565F-11F0-83DA-6045BDDDDDBC
19331024	Analysis4 2025-07-01 09:40:54.000	fkdatabaseid			-2
19331024	Analysis4 2025-07-01 09:40:54.000	name			Analysis4 2025-07-01 09:40:54.000
19331024	Analysis4 2025-07-01 09:40:54.000	description			Description Changed
19331024	Analysis4 2025-07-01 09:40:54.000	fktemplateid			1
19331024	Analysis4 2025-07-01 09:40:54.000	parentid			NULL
19331024	Analysis4 2025-07-01 09:40:54.000	fkparentreferencetypeid			NULL
19331024	Analysis4 2025-07-01 09:40:54.000	parentid2			NULL
19331024	Analysis4 2025-07-01 09:40:54.000	fkparent2referencetypeid			NULL
19331024	Analysis4 2025-07-01 09:40:54.000	isroot			1
19331024	Analysis4 2025-07-01 09:40:54.000	fkdefaultattributeid			NULL
19331024	Analysis4 2025-07-01 09:40:54.000	starttime			Jul 1 2025 9:40AM
19331024	Analysis4 2025-07-01 09:40:54.000	endtime			Jul 1 2025 9:40AM
19331024	Analysis4 2025-07-01 09:40:54.000	changedby			NT SERVICE\PIAnalysis Manager

Comments:

Date	Change #	Username
01-Jul-2025 11:10:38	1	Adm_nj
TestNJ		

Generated By: A
User Signature.: b0c8e853-3b6f-4456-8620-3d527531d7cb **At.:** 02-Jul-2025 10:41:35

Page 2 of 1058

Generated Date: 02-Jul-2025 10:41:35

Admin

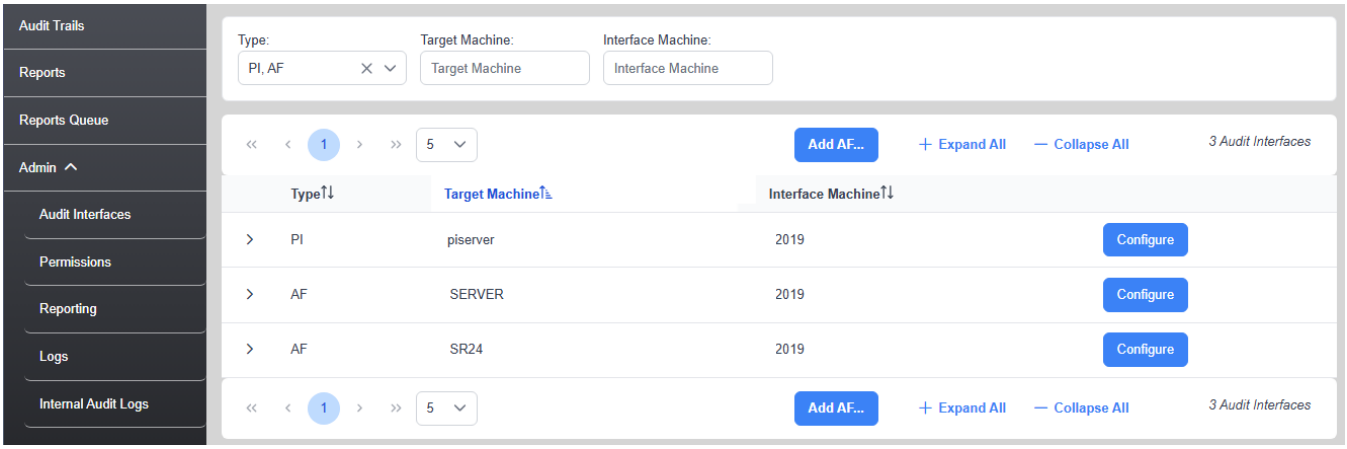
The Admin tab includes the following five key options: Audit Interfaces, Permissions, Reporting, Logs and Internal Audit Logs. Selecting the Admin tab to expand the options on <AVEVA PI AUDIT REPORTER SERVER NAME/admin>, the options are:

- Audit Interfaces open <AVEVA PI AUDIT REPORTER SERVER NAME/admin/list-interfaces>
- Permissions <AVEVA PI AUDIT REPORTER SERVER NAME/admin/permissions>
- Reporting <AVEVA PI AUDIT REPORTER SERVER NAME/admin/reporting>
- Logs <AVEVA PI AUDIT REPORTER SERVER NAME/admin/logs>
- Internal Audit Logs <AVEVA PI AUDIT REPORTER SERVER NAME/admin/internal-audit-logs>

Audit Interfaces

The Audit Interfaces section enables users to manage and configure the ingestion of audit trail records from AVEVA PI and AF system. This lists the currently configured Audit Interfaces. This section also includes filtering options, enabling users to apply the following filters:

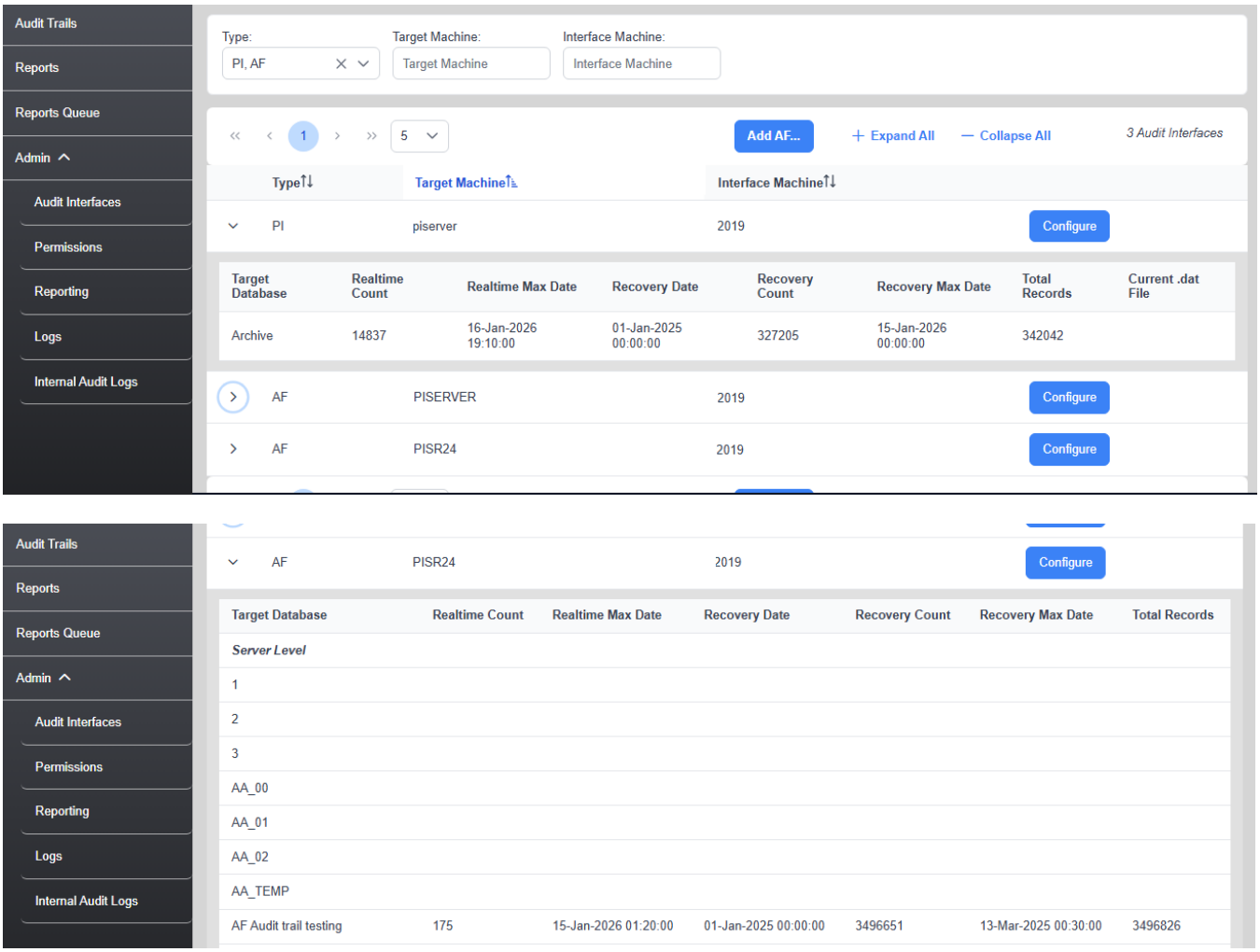
- Type: AF or PI
- Target Machine: PI or AF server name
- Interface Machine: Name of the server hosting the data ingestion service.



All configured audit interfaces are displayed in a structured table view within the Audit Interfaces section and it enables users to easily monitor and manage all audit data ingestion points from a single view. The following table provides a clear overview of each interface configuration and status.

Column	Description
Type	AF or PI.
Target Machine	The machine to ingest audit trail records from.
Interface Machine	The interface machine where the data ingress components are installed.
Configure	Button to access configuration view.

Further details can be shown by using the expansion icon on each row or using the “+ Expand All” option.



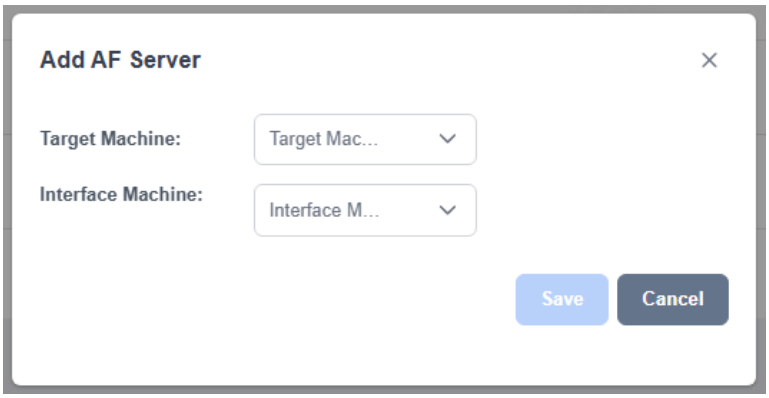
In addition to the features already mentioned, this is the list of other features available in the Admin, Audit interfaces section that will be better described in subsequent sub sections:

- Add a new AF Audit Interface for an existing interface machine.
- Enable or disable AF databases for real time and recovery data ingestion.
- Define the default behavior for future AF databases that are not mapped or created yet.
- Check details for data ingestion (chunk executions).
- Manage exclusion filters for data ingestion.
- Check details about PI Server .dat files processing.

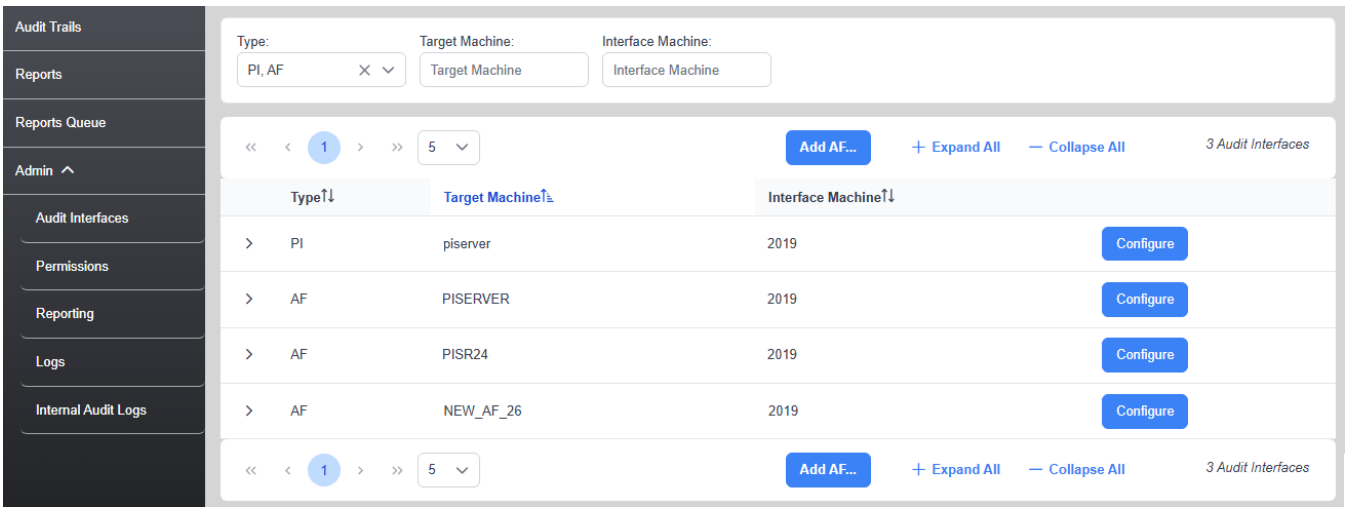
Add AF Server

This feature enables users to create a new Audit Interface to process the audit trail records from a new AF Server in an existing interface machine (server running the data ingestion service). The following steps are required to enable:

1. Access the Admin, Audit Interfaces section and select the “Add AF…” button.
2. A popup window shows 2 options, Target Machine (AF Server) and Interface machine.



3. Select the AF Server name (Target Machine) and the interface machine that will handle the data ingestion process.
4. Select Save.
5. Added AF server details will appear in Audit Interface view in the screenshot below.



Configure Audit Interface

The Configure Audit Interface dialog is used to set up and manage audit interfaces for both PI and AF data sources.

Alongside the Audit Interfaces view, users are presented with key summary information that offers a quick overview of the current configuration and system status.

Field	Description
Type	AF server or PI server.
Target Machine	The machine name of the AF or PI server.
Interface Machine	The machine name where the data ingress components are installed.

Configure Audit Interface for AF

In the AF Audit Interfaces Configure screen, a list of available databases is displayed, allowing users to manage audit data ingestion settings.

Column	Description
Enabled	Enable or disable AF database for ingestion.
Target Database	Name of the AF database.
Mode	Realtime (from current date) or Recovery (from a date in the past and new audit trail records).
Realtime Start Date	The date the real time ingestion was started.
Recovery Date	The date from which recovery should begin from.
Realtime Count	The count of audit trail records ingested via real-time.
Realtime Max Date	The date of the most recent audit data record ingested via real time.
Recovery Count	The count of audit trail records is ingested via recovery.
Recovery Max Date	The date of the most recent audit data record ingested via recovery.
Total Records	The total number of audit trail records ingested.
Integrity Check Status	The status of the integrity checks. Detailed integrity check information can be displayed by selecting the Details button – see data Integrity section.
Details	All information about the ingested database.
Excl. Filters	Exclusion filters can be viewed by selecting this button – see Exclusion Filters section.

Enable AF Database Audit Data Ingestion

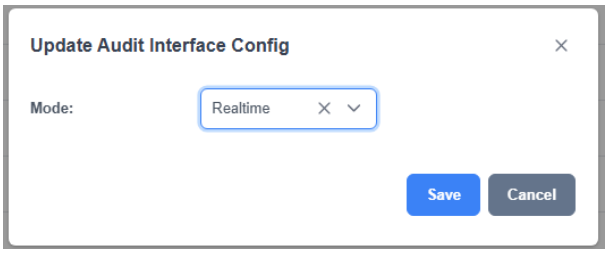
For AF Audit Interfaces, users can enable or disable the processing of AF Databases. It means there is the option to turn off the data ingestion and the option to turn on the data ingestion informing the start mode as real time or as recovery, that will be better described in subsequent sections.

To enable a single database, the following steps are required:

1. Locate the desired database in the table. In the “Enabled” column of the corresponding row, select the checkbox to activate ingestion.
2. A popup window shows an option to inform the start mode for that database.
3. There are two modes of operation: Real time and Recovery.

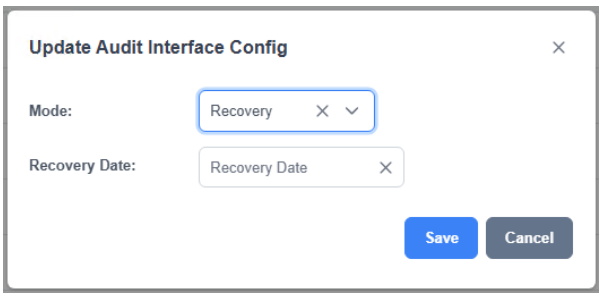
    a. Real time

When a database is enabled for audit data ingestion in real-time mode, only new audit trail data generated after the time of activation will be considered. Historical audit trail records created before the database was enabled for audit data ingestion in real-time mode, are not included. This ensures that only current and forward-moving changes are tracked in real-time.



    b. Recovery mode

When a database is enabled for audit data ingestion in recovery mode, the historical audit trail data generated after the recovery date informed will be considered. This mode is useful for backfilling audit trail records from a specific point in the past, while continuing to capture new changes in real time.



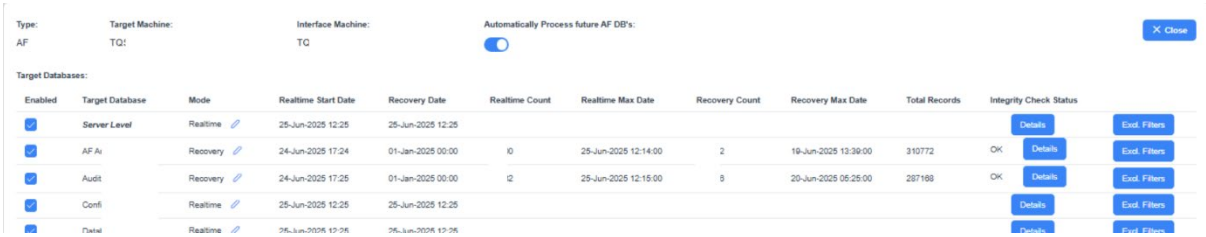
4. Select Save to confirm the new AF database data ingestion.

Automatically Process future AF DBs

In addition to enable a single AF database for data ingestion, there is the feature "Automatically Process future AF DBs". When this option is selected, all current databases on the AF Server are enabled for processing by the ingestion services. Additionally, any new databases created in the future will be automatically included.

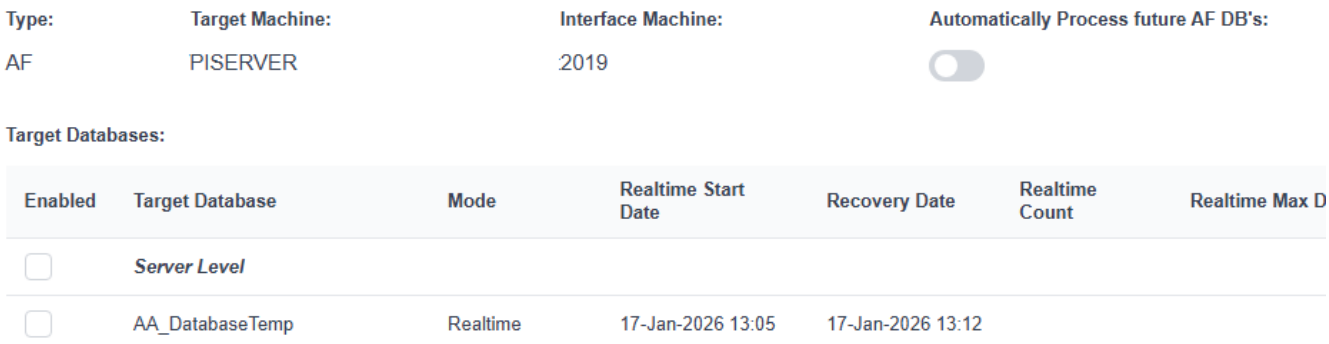
If the "Automatically Process future AF DBs" option is not selected, newly created databases will not be automatically enabled for processing – they must be enabled manually according to previous section Enabling AF Database Audit Data Ingestion.

Existing databases that are already enabled remain unaffected unless the user disables them individually.



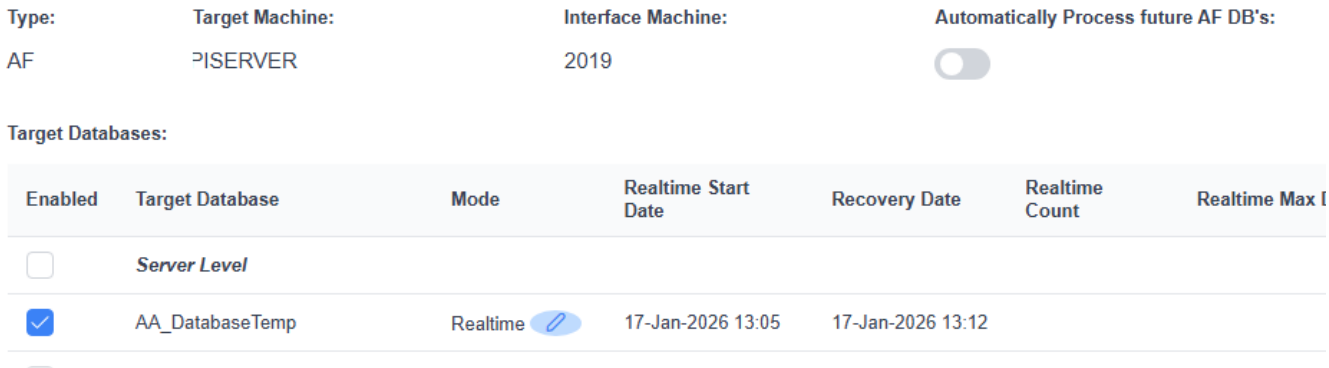
Disable AF Database Audit Data ingestion

To disable an AF database from audit data ingestion, uncheck the enabled column in the relevant row.



Modify AF Database Audit Data ingestion

To modify a database ingestion configuration, select the pencil icon next to the mode on the relevant row. The user can select mode whether recovery or real time mode according to step 3 in section Enabling AF Database Audit Data Ingestion.



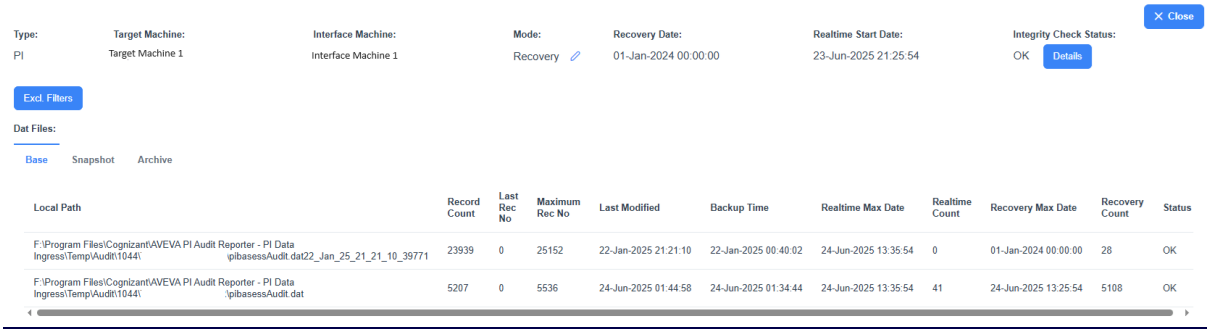
Configure Audit Interface for PI

The following additional fields are shown at the top of the view:

Field	Description
Mode	Realtime or Recovery.
Recovery Date	If Recovery mode is selected, the Recovery Date is displayed.
Realtime Start Date	The date at which Realtime recovery was started.
Integrity Check Status	The status of the integrity checks. Detailed integrity check information can be displayed by selecting the Details button – see Data Integrity section.
Excl. Filters	Exclusion filters can be viewed by selecting this button – see Exclusion Filters section.

The dat files for each AVEVA PI subsystem (Base, Snapshot, Archive) currently configured with Audit Data ingress are shown below and users can select the corresponding subsystem names to check the details about each dat file processing.

Column	Description
Local Path	The local path (on target server) of the dat file.
Record Count	The record counts in the dat file.
Last Rec No	The last record number in the dat file.
Maximum Rec No	The maximum record number in the dat file.
Last Modified	Date dat file was last modified.
Backup Time	Date dat file was backed up.
Realtime Max Date	The date of the most recent audit data record ingested via real time.
Realtime Count	The total number of audit data records ingested via real-time.
Recovery Max Date	The date of the most recent audit data record ingested via recovery.
Recovery Count	The total number of audit data records ingested via recovery.
Status	The data integrity status.

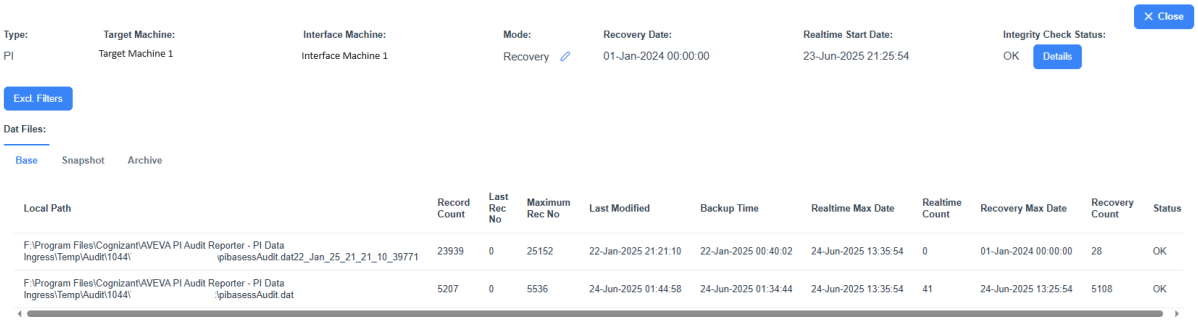


Data Integrity details

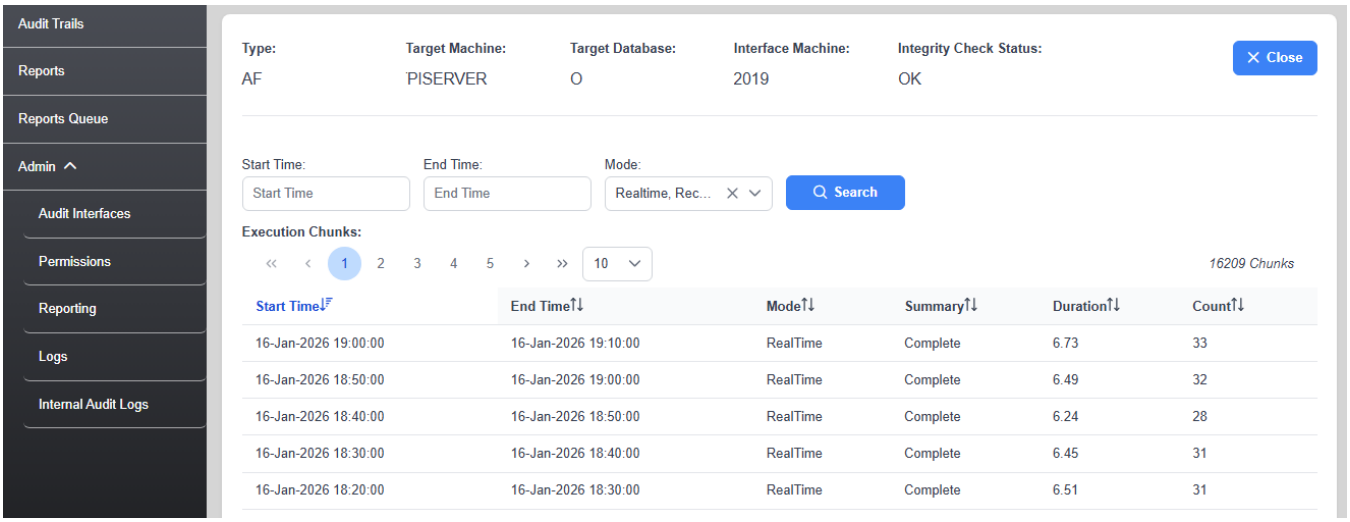
The Data Integrity details view allows a user to view detailed information about data integrity checks. To access this information, the users must select the option Details in the Audit Interface configuration screen next to Integrity Check Status, and it has a small difference between AF and PI interfaces.

For AF Audit Interfaces, the Integrity Check Status Details option is in the end of each AF database row.

For PI Audit Interfaces, the Integrity Check Status Details option is in the header of the page, on the upper right.



After accessing the Data Integrity Details screen, the information about the data processing can be filtered by Start Date, End Date and Mode – Realtime, Recovery.



Field	Description
Type	AF server or PI server.
Target Machine	The machine name of the AF or PI server.

Field	Description
Interface Machine	The machine name where the data ingress components are installed.
Data Integrity Status	Overall status of integrity checks.

The status of each audit data retrieval chunk is shown in a table.

Column	Description
Start Time	The start time of the period of audit data retrieval.
End Time	The end time of the period of audit data retrieval.
Mode	The mode of the audit data retrieval chunk.
Summary	The integrity status for the audit data retrieval chunk.
Duration	The time taken for each audit data retrieval chunk.
Count	Count of records retrieved via the audit data retrieval chunk.

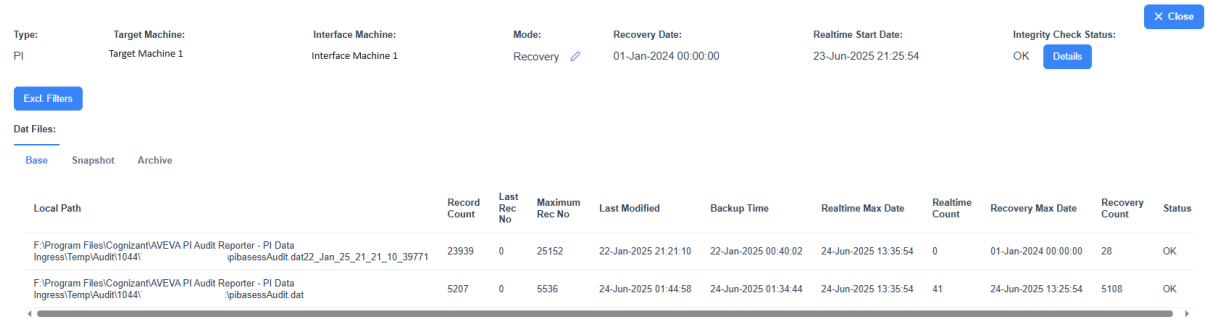
Exclusion filters

The Exclusion filters enable users to avoid the processing of useless audit trail records. They are recommended to be used when there is a known activity in PI or AF environments with changes that are not required to be stored. For example, for some users, the AF Event Frame automatic creation is not required in audit processing, only the manual operations are mandatory.

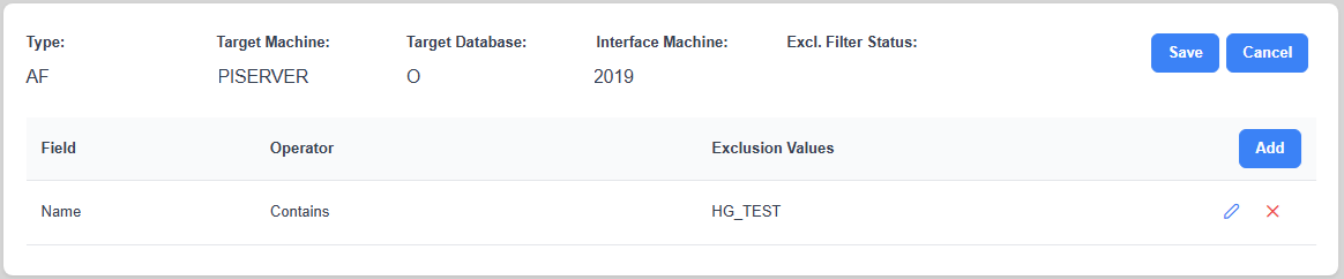
To access this information, the users must select the option Excl. Filters in the Audit Interface configuration screen, and it has a small difference between AF and PI interfaces.

For AF Audit Interfaces, the Exclusion Filters option is in the end of each AF database row.

For PI Audit Interfaces, the Exclusion Filters option is in the header of the page, on the upper left.



After accessing the Exclusion Filters screen, all the exclusion values are listed.



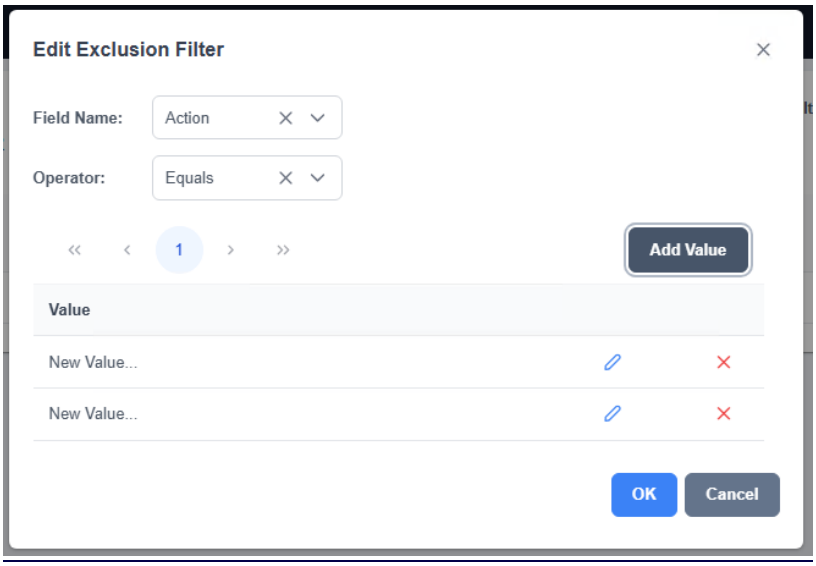
The following fields are shown at the top of the view.

Field	Description
Type	AF server or PI server.
Target Machine	The machine name of the AF or PI server.
Interface Machine	The machine name where the data ingress components are installed.
Excl. Filter Status	Applied, or applying the exclusion filters to the audit data.

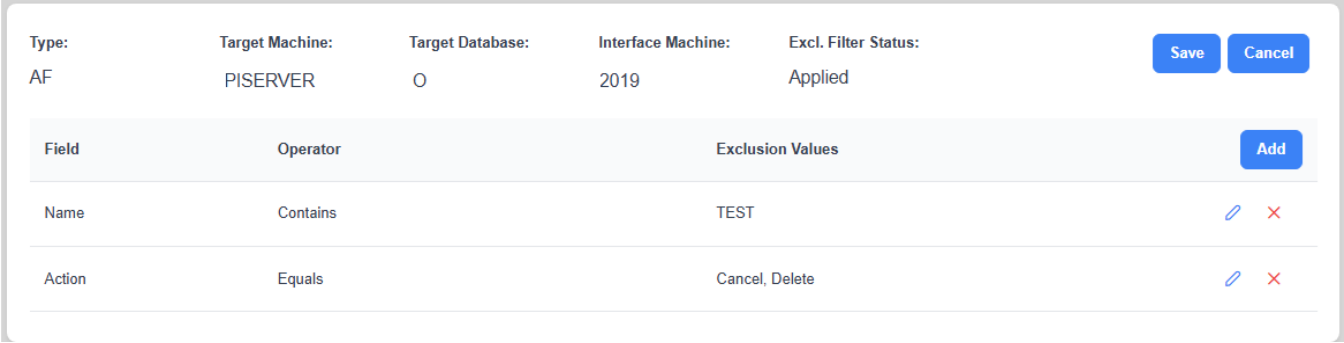
The current Exclusion fields are shown in a table:

Column	Description
Field	The specific field in the dataset to which the filter is applied.
Operator	The comparison method is used to evaluate the field against the provided values.
Exclusion Values	The values used in the filter condition include or exclude matching records.

1. To create a new Exclusion Filter, the following steps are required:
2. Navigate to the Exclusion Filters screen.
3. Select Add.
4. A window popup shows the fields to inform the exclusion filter criteria.



5. Inform the audit trail record field name to be filtered.
6. Inform the Operator (starts with, ends with, contains, equals, etc.)
7. Select Add Value.
8. A new row will be added to the list of values. Users must add more than one value if required.
9. Once values are informed, confirm the change by selecting ✓.
10. Select OK to confirm the values. They will be added to the list.
11. To apply the changes made, select Save. The status changes to “Applying” and once finished, to “Applied”.



Users must navigate to the same screen and select ✕ to delete an exclusion filter or value, and they must select ✎ to edit an exclusion filter or value.

Permissions

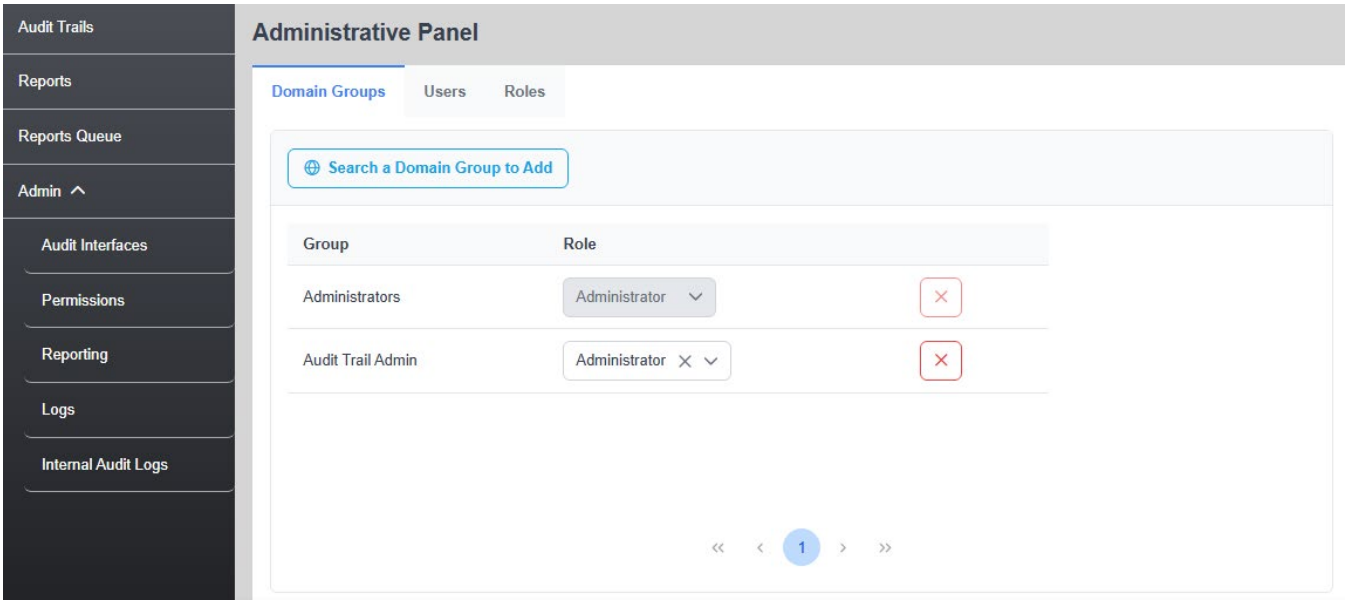
This tab enables access requirement configuration for users. Under the Administrator Panel, users have access to three key administrative management options: Domain groups, Users, Roles.

Domain groups

Domain groups are collections of user accounts, computer accounts, and other groups that are managed as a single unit. They are commonly used in enterprise environments to:

1. Assign permissions to resources (e.g., files, folders, applications)
2. Simplify administration by grouping users with similar access needs
3. Enforce security policies consistently

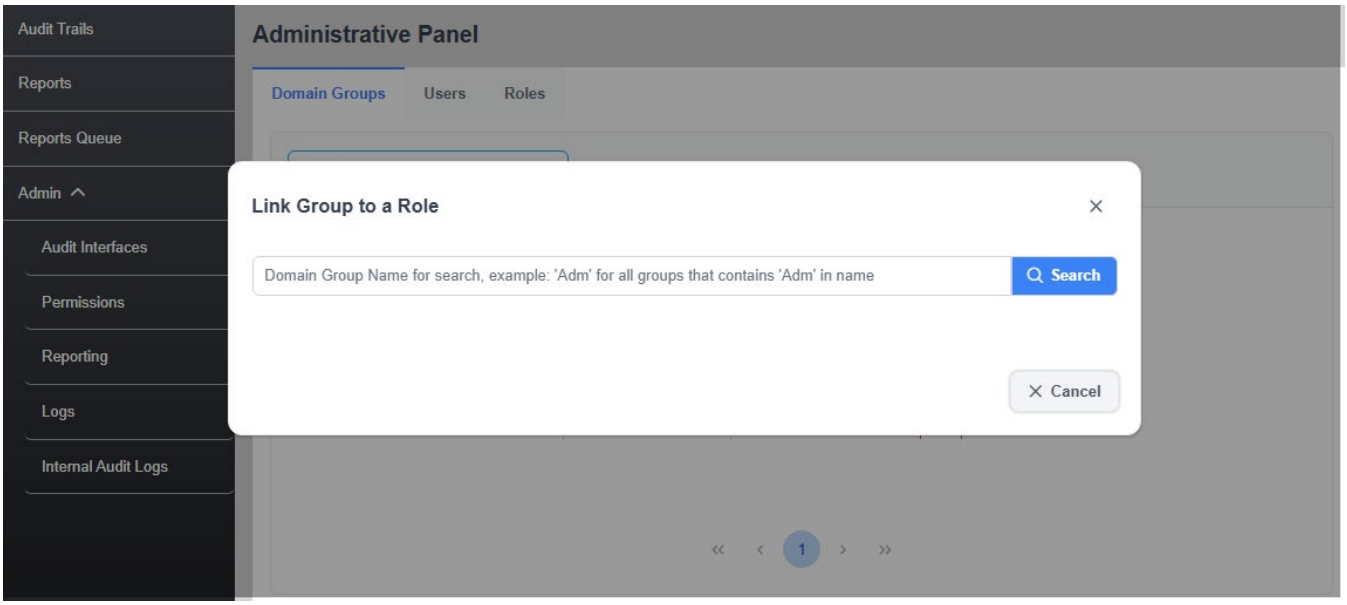
The Domain groups section allows administrators to manage user groups efficiently. It includes the following key features: Search Domain groups, Add Domain groups, view existing Domain groups with role.



Add a domain group

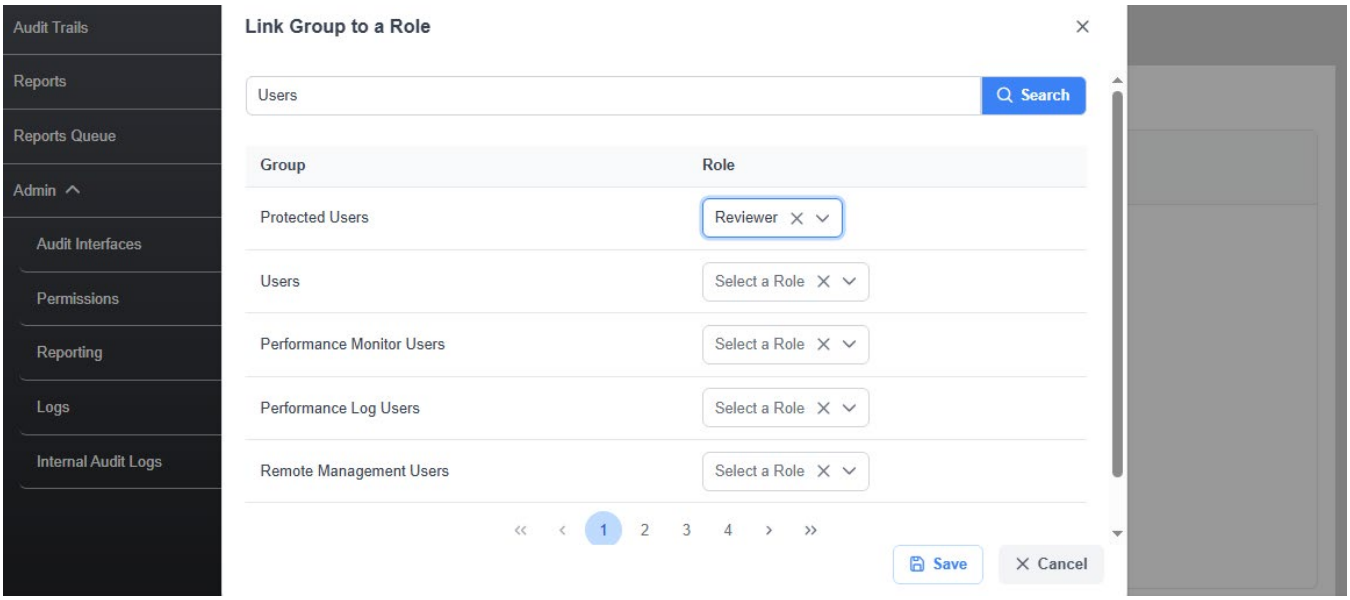
To add a domain group the following steps are required:

1. Select the Admin section in left panel and then in Permissions.
2. Select Search Domain Group to Add.

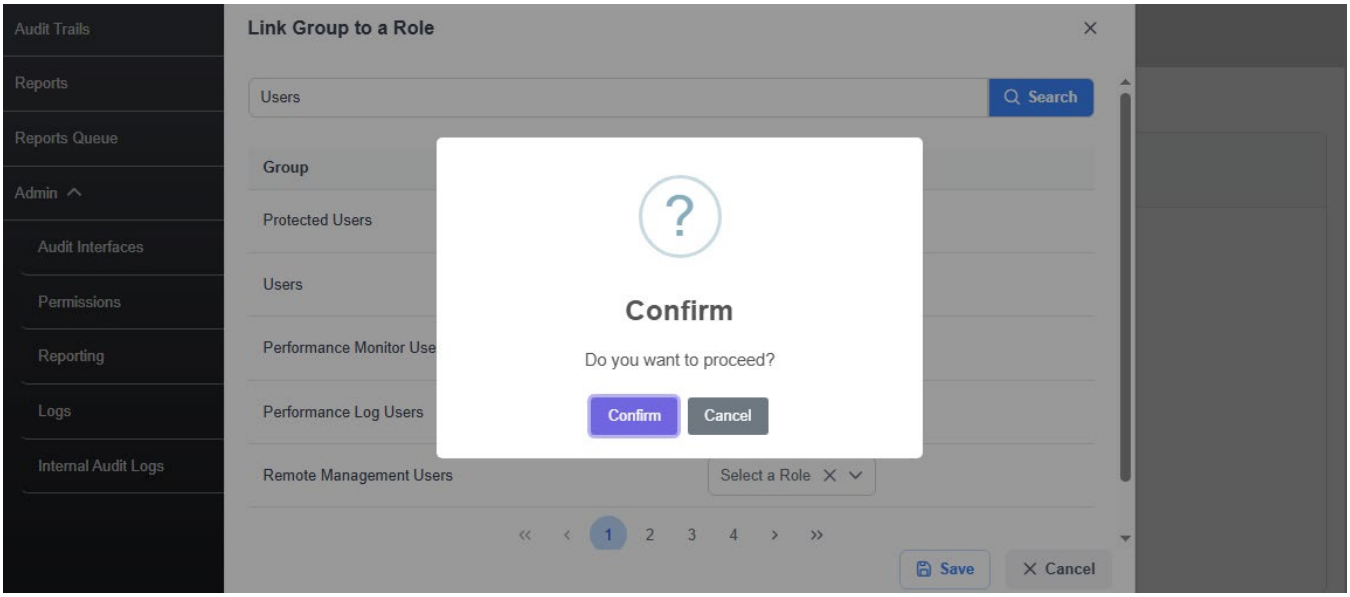


3. Type the name of part of the name of the domain group and select Search.

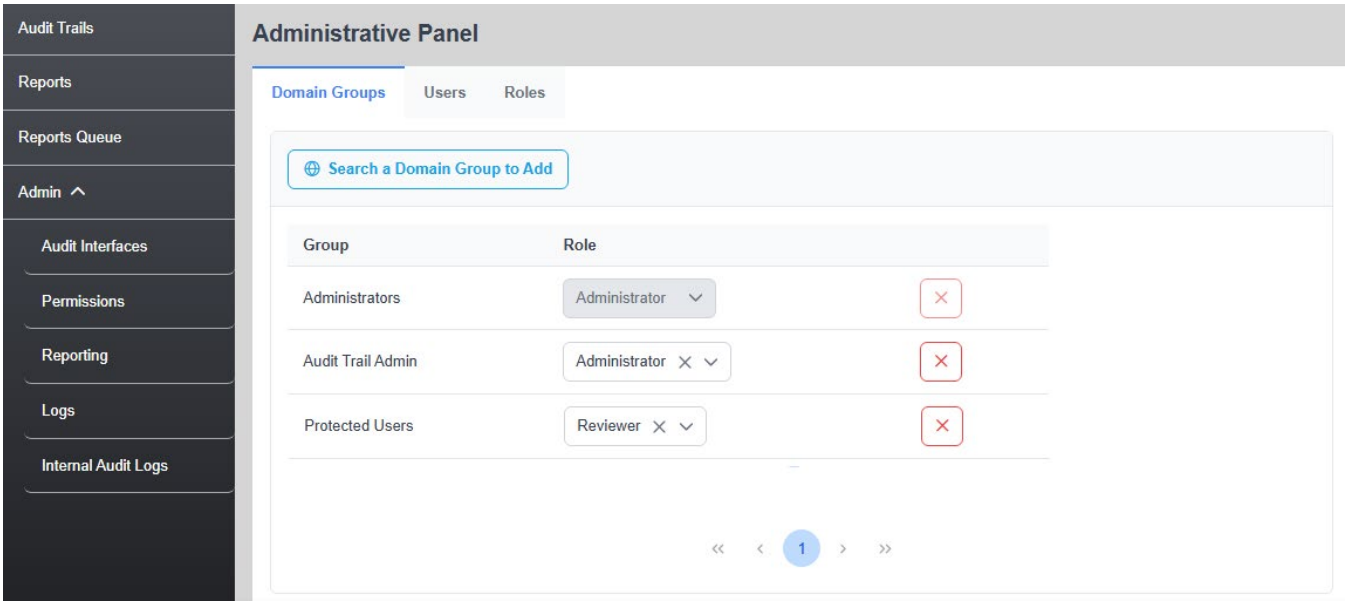
4. Locate the domain group to be added, choose a role and then Save.



5. Select Confirm in the window popup to proceed.



6. The new domain group is mapped to the selected Role.

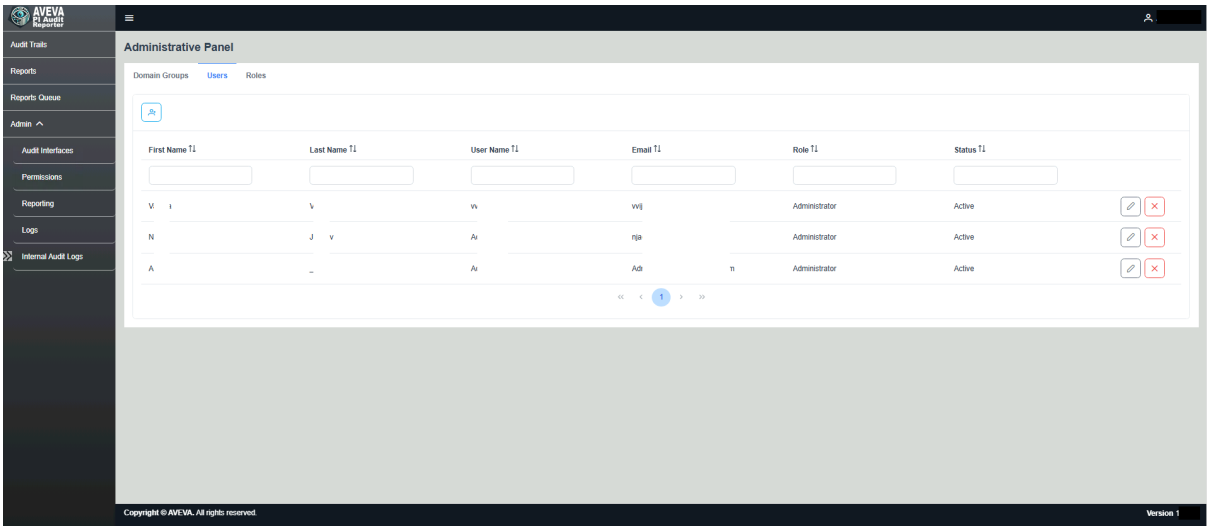


Note: In that same screen it is possible to change the domain group associated role and to remove the domain group association.

Users

The Users section provides a comprehensive list to manage all registered users within the system, configured by users with the "Allow Manage User" permission.

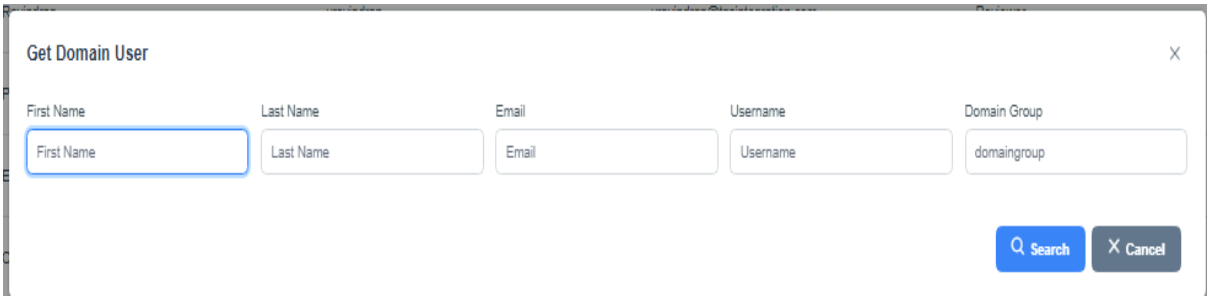
Each user entry includes the following Information: First Name, Last Name, Username, Email, Role, Status. Administrators can edit user information and Activate / Inactivate a User.



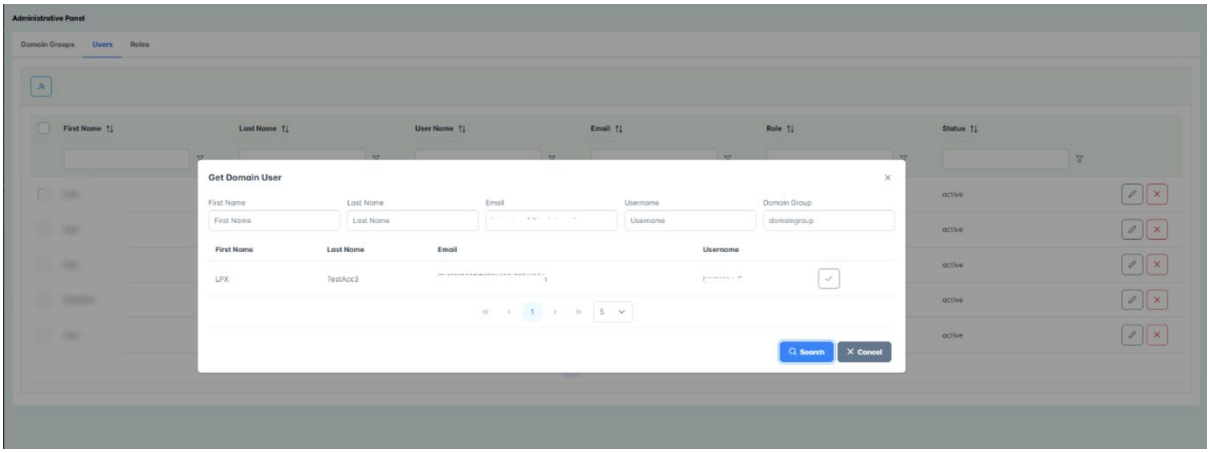
Add a new user

To add a new user to the application, the following steps are required:

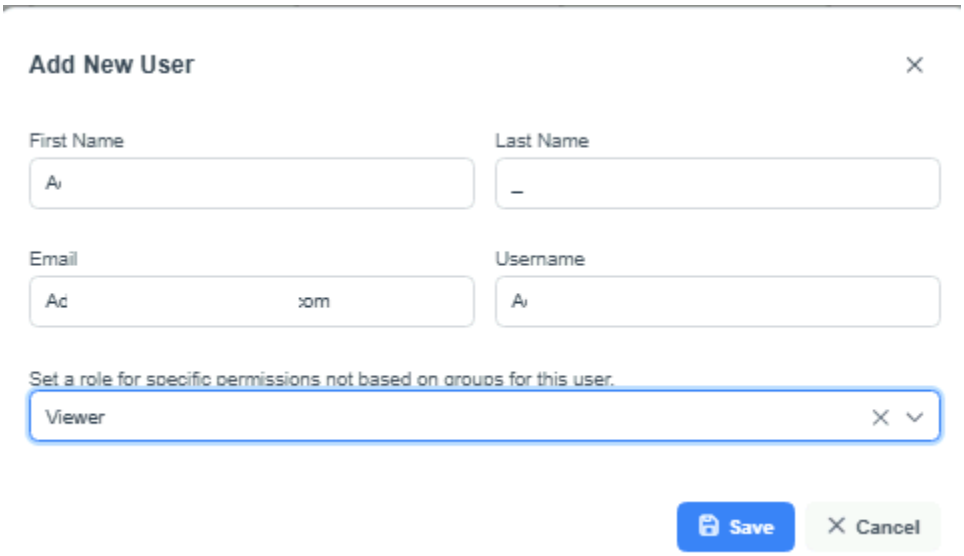
1. Select ‘Add User’ to open a popup window titled ‘Get Domain User’.
2. In the ‘Get Domain User’ popup, administrators can search for users using the following fields: First Name, Last Name, Email, Username and Domain Group.
3. A list of matching users from the domain appears based on the search criteria.



4. "Select User" adds the chosen user to the application.



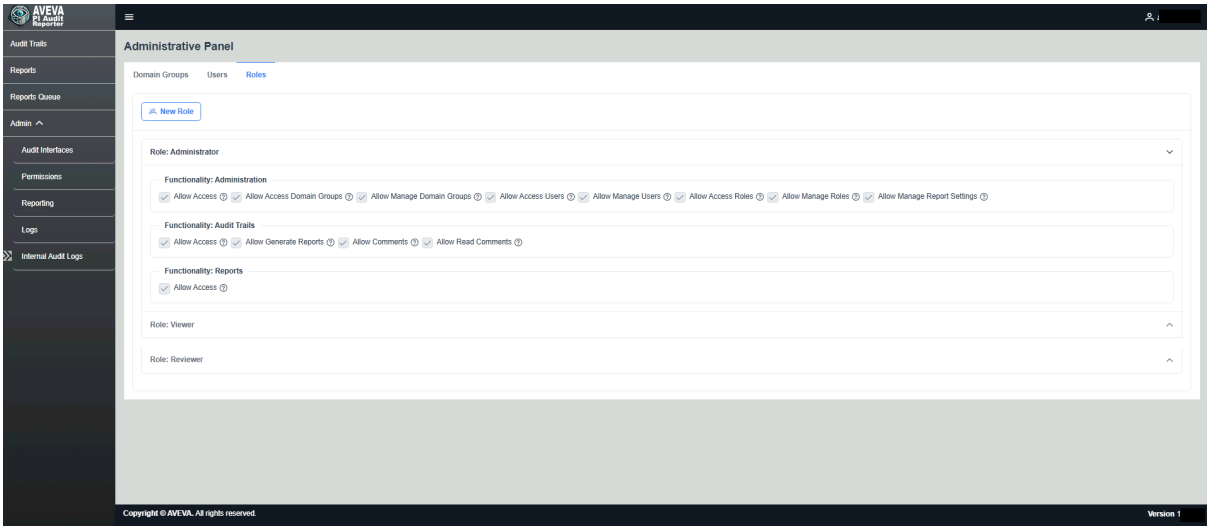
5. Assign a specific role to the user for permissions, independent of group membership, by selecting it from the dropdown menu.
6. Select 'Save'.



Roles

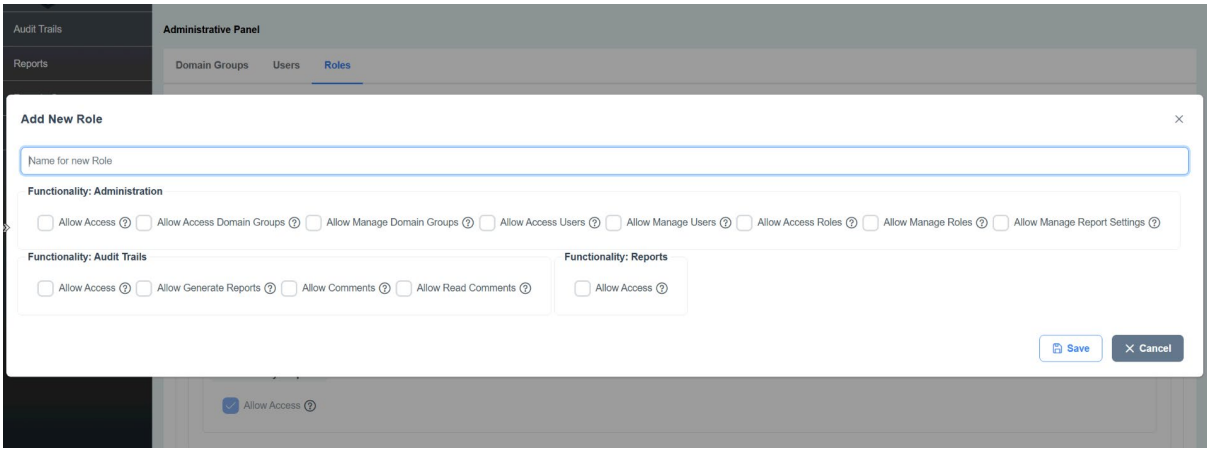
The Roles tab provides a centralized view of all the defined roles within the system, along with their associated permissions and functionalities.

1. In the Roles tab, view the roles and permissions assigned to each role. Permissions are categorized into three main functional areas: Administration, Audit Trails, and Reports.
2. Users with either 'Administrator Access' or ‘Allow Manage Roles' permission can assign or deactivate specific permissions within each role.



3. Administrators can define custom roles tailored to specific responsibilities and access levels within the system. Select the "New Role" option. In the "Add New Role" screen, enter the Role name, Permissions configurations within three functional areas: Administration, Audit Trails, and Reports.

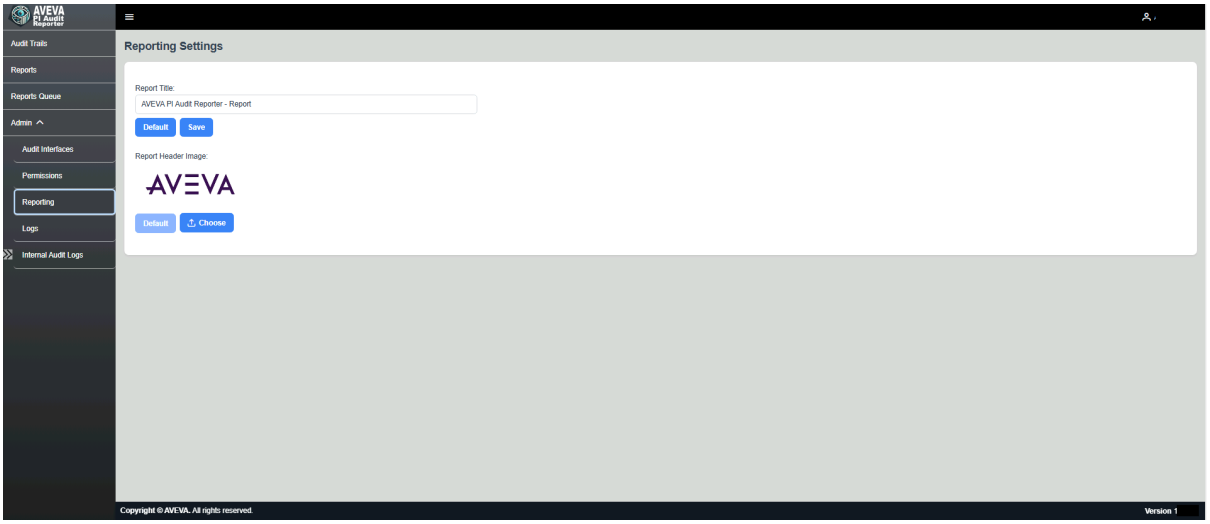
4. After configuring the permissions, select Save to make it available in the system.



Reporting

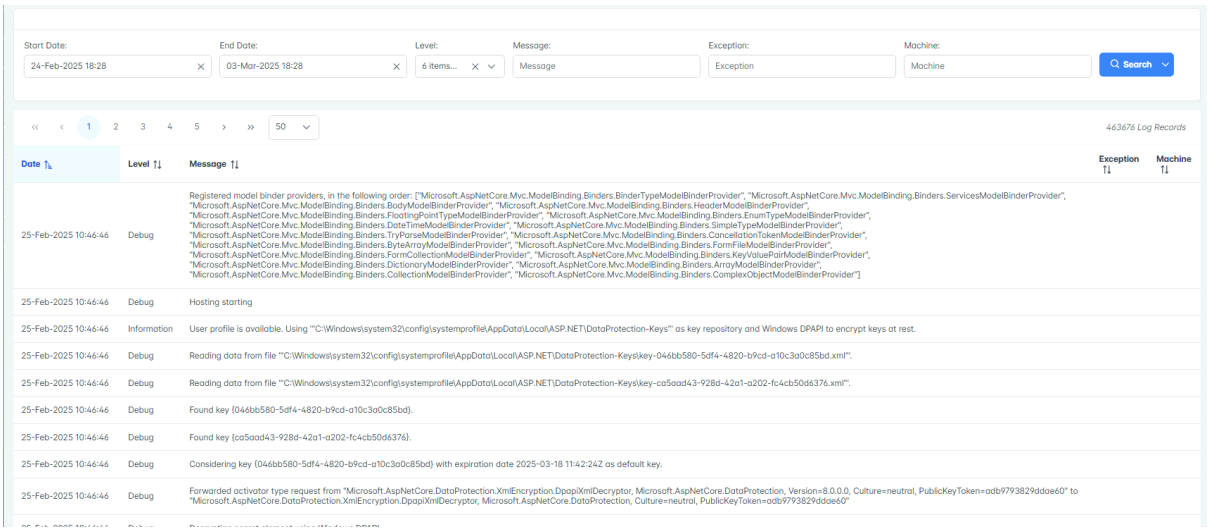
This section allows users to customize the appearance of all reports generated within the AVEVA PI Audit Reporter application.

- Report Title: The title entered will appear in all AVEVA PI Audit Reporter Reports.
- Report header image: Allows users to upload a custom image (e.g., company logo or branded banner). The selected image will be displayed as the header on all AVEVA PI Audit Reporter reports.

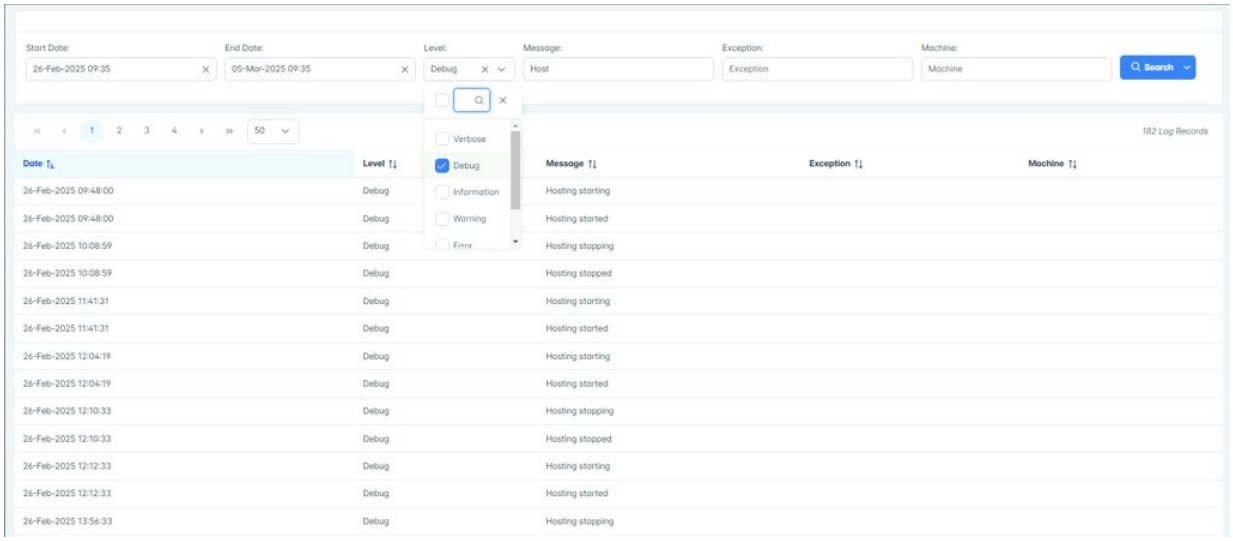


Logs

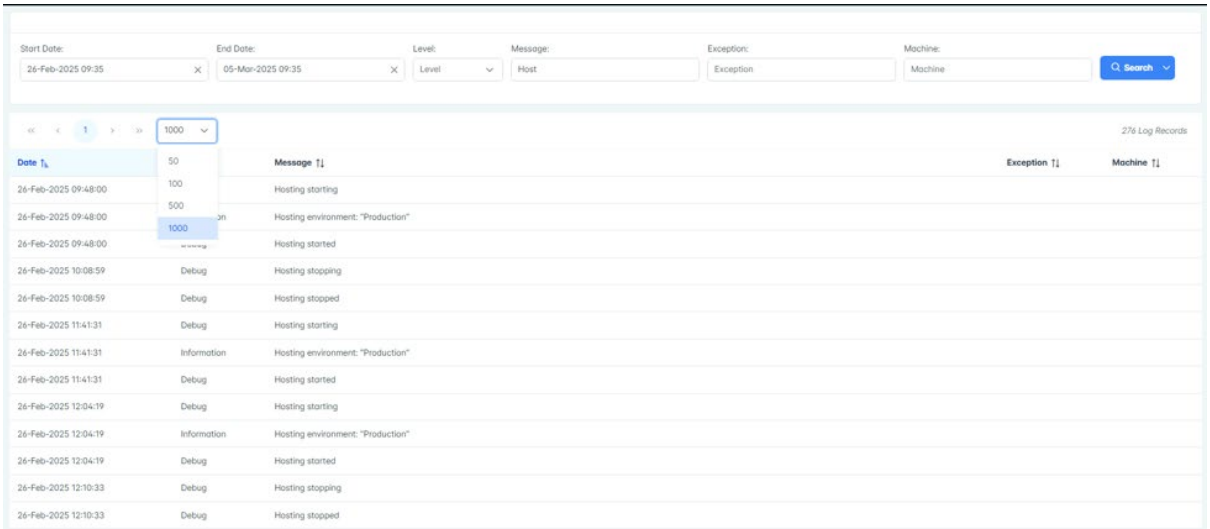
The Logs section records and displays detailed information about all backend actions performed within the system. This feature is essential for monitoring, debugging, and auditing system behavior. Each log entry includes the following key details: Start Date, End Date, Level, Message, Exception (if any) and Machine Information.



1. Search for any logs by providing required information in the available search fields - Start Date, End Date, Level, Message, Exception, Machine.
2. Sort logs based on any available column.



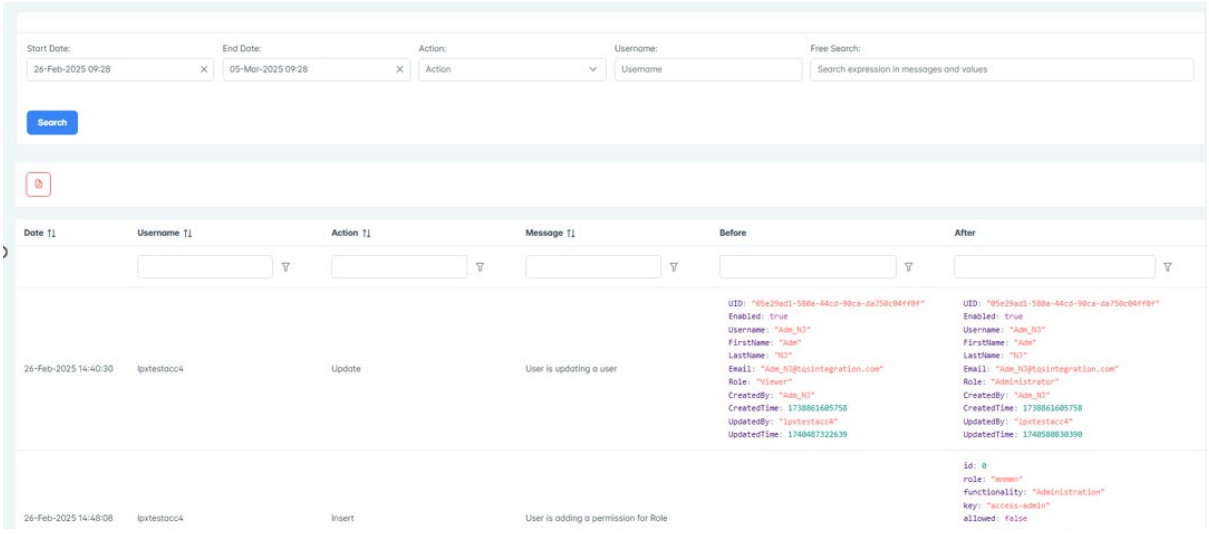
3. Select a number for log entries to be displayed on the page: 50,100,500 or 1000.



Internal Audit Logs

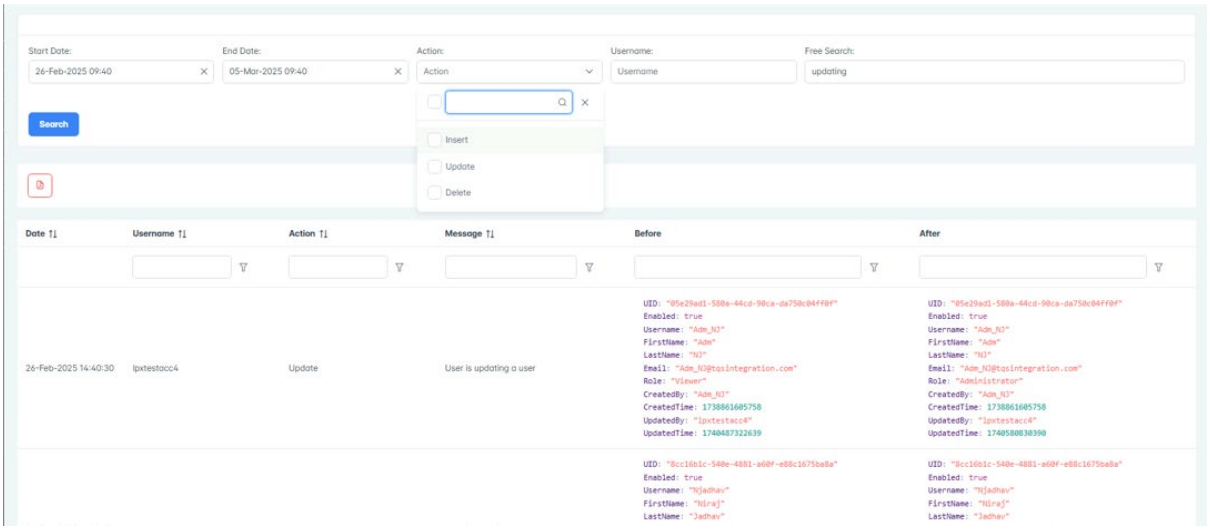
Internal Audit Logs capture all administrative actions performed within the application's admin panel. These actions include adding or deleting users, modifying user roles and permissions, updating exclusion filters, enabling or disabling databases, and configuring servers. To access the Audit Logs, follow the instructions:

1. Navigate to the Admin Panel of the application.
2. Select the Internal Audit Logs section.

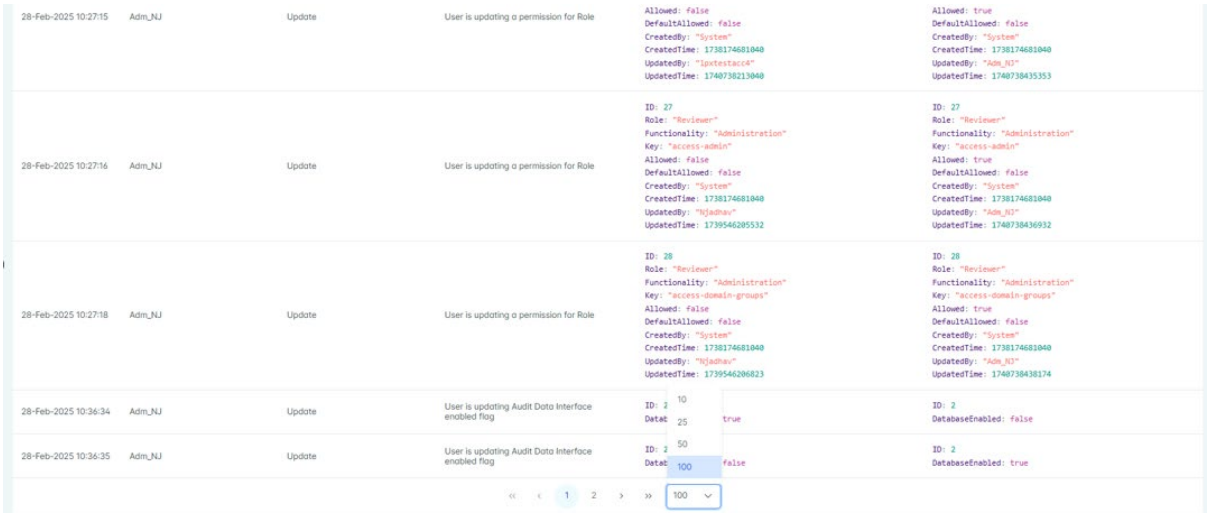


3. Filter and Search Logs by using the following filters to narrow down the logs:
   a. Start Date and End Date: Select the date range for the logs.
   b. Action: Choose specific actions (e.g., Add User, Edit Role).
   c. Username: Filter logs by the administrator or user who performed the action.

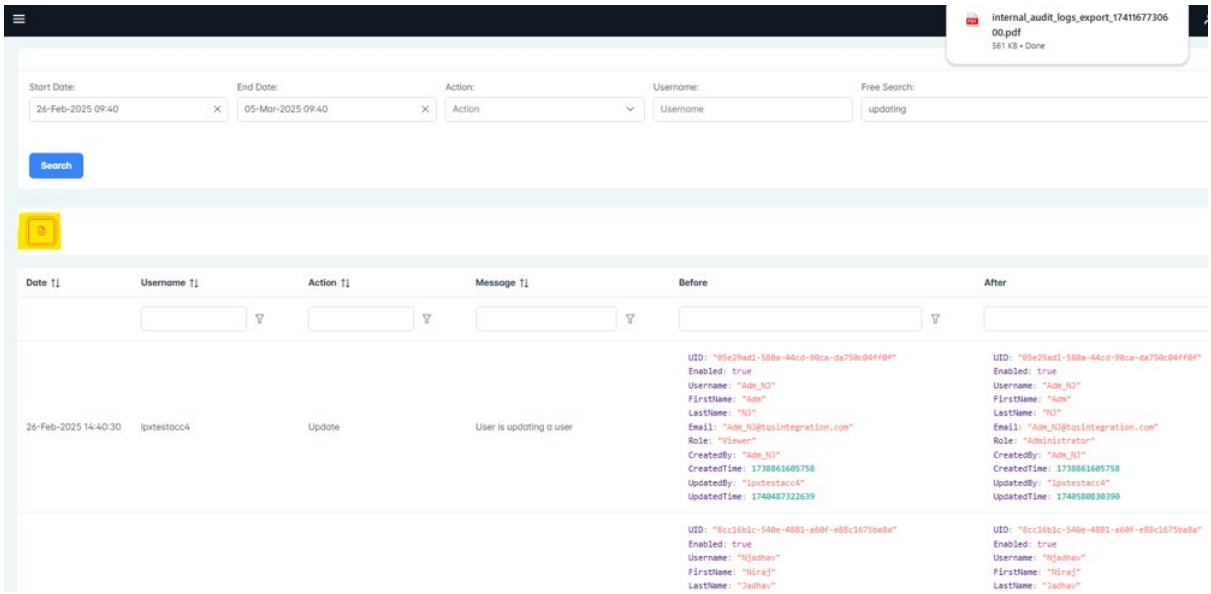
d. Use the Free Search field to enter keywords and search within log messages.



4. Select the number of entries to display per page. Options are 10, 25, 50, or 100 entries.
5. Scroll through the pages to view more logs.



6. If required, select the Export Logs option to save the internal audit logs to a PDF file.
7. Save or share the report as needed.



8. View Log Entries

Date	Username	Action	Message
17-Jan-2026 10:44:36	s	Update	AAT Web Application :: User is updating a user
Before			After
UID.: 1 9 Enabled.: false Username.: m FirstName.: s LastName.: o Email.: a .com Role.: A CreatedBy.: m CreatedTime.: 1766864982653 UpdatedBy.: s UpdatedTime.: 1768646674678			UID.: 1 9 Enabled.: false Username.: m FirstName.: s LastName.: o Email.: a .com Role.: A CreatedBy.: m CreatedTime.: 1766864982653 UpdatedBy.: s UpdatedTime.: 1768646676583

CHAPTER 7

FDA 21 CFR Part 11 Compliance

The relevant sections of the FDA 21 CFR Part 11 regulations are listed together with how AVEVA PI Audit Reporter can be used to comply with the regulation. The deployment of the AVEVA PI Audit Reporter application on site shall be done in conjunction with client-based requirements and shall adhere to their SDLC process in place.

21 CFR Part 11 Regulation		**AVEVA PI Audit Reporter Statement of Compliance**
Section	**Requirement**	**Response**
B/11.10	**Controls for Closed Systems**	
	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:	AVEVA PI Audit Reporter customers are responsible for the implementation of procedures that will ensure that the PI System and its application meet the requirements of the regulations. PI System has many security and audit functions that address these requirements.
(a)	Validation of systems to ensure accuracy, reliability, consistent intended performance and the ability to discern invalid or altered records.	Validation and verification is an overriding requirement for compliance. The deployment of AVEVA PI Audit Reporter application onsite shall always been done in conjunction with customer based SDLC and its requirements.
(b)	The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.	The system stores historical records, ensuring data integrity and availability. Records can be exported in both human-readable formats (such as PDF or CSV) suitable for inspection, review, and copying by regulatory agencies. AVEVA PI Audit Reporter Reports and Internal audit logs functionality are available for

21 CFR Part 11 Regulation		AVEVA PI Audit Reporter Statement of Compliance
Section	**Requirement**	**Response**
		generating accurate and complete copies. Audit trail logs and reports can be used to verify any changes. If the agency requires assistance during review, support is available to facilitate access.
(c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Electronic records are protected through secure logon and group permissions. Data integrity is ensured by the use of a comprehensive audit trail capability that detects and logs any change to original data values or system manipulation. Many years of PI data can be kept online and immediately accessible to users. The only limitation to the online retention period is the on-line storage capacity of the PI Server. Both data value and system configuration records are backed up to secure media and can be easily restored to the system if necessary.
(d)	Limiting system access to authorized individuals.	Access to the AVEVA PI Audit Reporter application is governed by its access control framework. Refer to Permissions for further details regarding system access.
(e)	Use of secure, computer-generated, time- stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	This does not apply to the AVEVA PI Audit Reporter application. Refer to the underlying data source, AVEVA PI, and its official documentation for relevant details
(f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	This does not apply to the AVEVA PI Audit Reporter application. Refer to the underlying data source, AVEVA PI, and its official documentation for relevant details.
(g)	Use of authority checks to ensure that only authorized individuals can use the system,	Access to the AVEVA PI Audit Reporter application is managed through its access

21 CFR Part 11 Regulation		AVEVA PI Audit Reporter Statement of Compliance
Section	**Requirement**	**Response**
	electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	control mechanism. Refer to Permissions for further details regarding system access.
(h)	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	Access to the AVEVA PI Audit Reporter application is managed through its access control mechanism. Refer to section Permissions for further details regarding system access.
(i)	Determination that person who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.	AVEVA PI Audit Reporter customers are responsible for ensuring that all personnel using and/or administering the system have taken the appropriate training. AVEVA employs experienced and qualified software professionals in the development and support of the AVEVA PI Audit Reporter.
(j)	The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification	AVEVA PI Audit Reporter customers are responsible for establishing and enforcing procedures that support the use of applications in any regulated environment. AVEVA employs experienced and qualified software professionals in the development and support of the AVEVA PI Audit Reporter.
(k)	Use of appropriate controls over systems documentation including:	
(1)	Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance	Access to the AVEVA PI Audit Reporter is managed through its access control mechanism. Refer to Permissions for further details regarding system access. AVEVA provides a User & Administration Guide (UAG) for AVEVA PI Audit Reporter.
(2)	Revision and change control procedures to maintain an audit trail that documents time- sequenced development and modification of systems documentation.	AVEVA PI Audit Reporter's engineering group tracks changes to the application or associated documentation using its internal Change Control procedures.
B/11.30	**Controls for open systems**	
	People who use open systems to create, modify, maintain, or transmit electronic records shall	AVEVA PI Audit Reporter customers are responsible for the development of

21 CFR Part 11 Regulation		AVEVA PI Audit Reporter Statement of Compliance
Section	**Requirement**	**Response**
	employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in §11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	procedures and controls associated with the use of the PI Audit Trail application in any regulated situation.
B/11.50	**Signature manifestations**	
(a)	Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:	The AVEVA PI Audit Reporter application does not provide electronic signature functionality.
(1)	The printed name of the signer.	The AVEVA PI Audit Reporter application does not provide electronic signature functionality.
(2)	The date and time when the signature was executed;	The AVEVA PI Audit Reporter application does not provide electronic signature functionality.
(3)	The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	The AVEVA PI Audit Reporter application does not provide electronic signature functionality.
(b)	The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).	The AVEVA PI Audit Reporter application does not provide electronic signature functionality.
B/11.70	**Signature/record linking**	
	Electronic signatures and hand-written signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.	The AVEVA PI Audit Reporter application does not provide electronic signature functionality.

CHAPTER 8

References

This section contains all references used during the development of this document, just like manuals, documents, operational procedures, definitions, abbreviations and so on.

Definitions, Acronyms and Abbreviations

Table below contains all the definitions, acronyms and abbreviations used in this document.

Term	Definition/ Description
API	Application Programming Interface
ATRAIL	AVEVA™ PI Audit Reporter application
AVEVA	AVEVA is a British multinational company that specializes in industrial software for engineering, design, and information management.
CSV	Comma-separated values
DB	Database
FCI	Failover Cluster Instances
IIS	Internet Information Services
IO	Input/Output
IT	Information Technology
ITSM	Information Technology Service Management
LDAP	Lightweight Directory Access Protocol
LSMG	Life Sciences Manufacturing group
Microservices	An organizational and architectural methodology for developing software that divides the program into discrete, independent services that interface with one other via explicit APIs.
WSFC	Windows Server Failover Clustering
OS	Operating System
PDF	Portable Document Format
RDBMS	Relational Database Management System
SQL	Structured Query Language

Term	Definition/ Description
SSL	Secure Sockets Layer
UAC	User Account Control
UI	User Interface
URL	Uniform Resource Locator
VM	Virtual Machine

Documents

Table below contains all the documents used in the development of this document.

Name	Version
AVEVA Template Book_Word Version.docx	Apr 2025
AVEVA PI Audit Reporter - Demo Script.pptx	Jan 2026
AVEVA Technical Writer's Handbook.pdf	Apr 2025