Aspect Workforce Engagement Management Quality Installation Guide

25

RELEASE DATE: 11/7/2025

Legal Notices

Contents

Revision History

The table below describes the revision history for Aspect Workforce Engagement Management Quality™ Installation Guide.

Date	Description	Section
11/7/2025	Rev A, initial Release.	Update front and back covers and Legal Notices page Updates for consistency
5/12/2026	Rev B	Added information about the content security key in section 6.4.

About this Guide

This document contains detailed instructions on how to install and configure Aspect Workforce™, Aspect Quality™, and Aspect Performance™ with Aspect Workforce Engagement Management™.

For information about Training, Technical Support, commenting on the documentation, and a list of additional documentation see the appropriate product Release Notes document on the Aspect web site at http://www.aspect.com.

Audience

The *Aspect Workforce Engagement Management Installation Guide* is for IT personnel and Aspect Administrators who set up the system. Contact center managers may also want to review this manual to obtain familiarity with what is involved in the system installation.

Specifically this guide is intended for use by anyone who participates in the installation and configuration of the Aspect Workforce Engagement Management™ , Aspect Workforce™ , Aspect Performance™ , and Aspect Quality™.

Knowledge of third-party applications including Microsoft Windows Server and Microsoft Internet Information Services (IIS) is a prerequisite for installation and deployment.

Organization of this Guide

This guide consists of these chapters:

- Chapter 1, Overview provides information on what prerequisites need to be performed prior to installing and configuring the software.
- Chapter 2, Pre-Installation Tasks provides pre-installation tasks that you must perform prior to installing and configuring Aspect Workforce Engagement Management.
- Chapter 3, Installing Aspect Workforce Engagement Management provides procedures on how to install and configure Aspect Workforce Engagement Management.
- Chapter 4, Configure Workforce Engagement Management provides information on how to configure Workforce Engagement Management, once you have the components installed.

- Chapter 5, Configure Aspect Workforce provides procedures on how to install and configure Aspect Workforce with Aspect Workforce Engagement Management.

- Chapter 6, Configure Aspect Quality provides procedures on how to install and configure Aspect Quality with Aspect Workforce Engagement Management.
- Chapter 7, Configure Aspect Performance provides procedures on how to install and configure Aspect Performance with Aspect Workforce Engagement Management.
- Chapter 8, Verifying the Installation provides procedures on how to verify that the installation of Aspect Quality, Aspect Performance, and Workforce Management are properly installed and configured with Workforce Engagement Management.
- Chapter 9, Dashboard Configuration provides information on how to configure a dashboard in Workforce Engagement Management if you prefer not to use the default dashboard.
- Appendix A, Troubleshooting provides troubleshooting guide for issues related to Aspect Workforce, Aspect Quality, and Aspect Performance, based on their integration with Aspect Workforce Engagement Management.
- Appendix B, Notes on the IIS Role Services for Windows contains a table that you can use to identify which IIS Role Services you can disable when you are using Server Manager to configure role services for IIS.
- Appendix C, Security and Authentication contains information on how to configure authentication with Workforce Engagement Management and Workforce, Quality, and Performance.

1. Overview

This chapter provides an overview of Aspect Workforce Engagement Management™ and the Aspect Workforce™, Aspect Performance™, and Aspect Quality™ components.

1.1 Terminology Note

Be sure to distinguish between the following terms throughout this guide:

- **Aspect Workforce Engagement Management™** refers to the umbrella application that houses the web user interface for Aspect Workforce, Aspect Performance, and Aspect Quality.
- **Aspect Workforce™** refers to the Workforce component of Aspect Workforce Engagement Management.
- **Aspect Performance™** refers to the Aspect Performance component of Aspect Workforce Engagement Management.
- **Aspect Quality™** refers to the Aspect Quality component of Aspect Workforce Engagement Management.

1.2 About Aspect Workforce Engagement Management

Aspect Workforce Engagement Management is a web application that consists of the following components:

- **Aspect Workforce** component enables contact center agents self-service functionality, such as viewing schedules, requesting time off, viewing account balances, and trading schedules. Plus optional features to send/receive notifications, and monitor Real-Time Adherence in the web.
- **Aspect Performance** component provides an analytical tool used to collect, correlate and display information tailored to the user's role and responsibilities, and enables employees to track their personal performance against assigned goal metrics across tasks and systems.
- **Aspect Quality** component enables contact centers to record and monitor agents. Agents and supervisors can search for and listen to these recordings, including searching by speech analytics, and can score an interaction, including downloading evaluation attachments, printing, and emailing evaluations, viewing non-recording tasks, retrieving archived interactions and evaluations, and downloading media files. Administrators can create, edit, and duplicate templates; create, edit, activate, and deactivate storage groups; and assign coaching.

1.2.1 About Aspect Workforce

By using Workforce, contact center employees can view scheduling information and request changes to schedules through a web browser. In addition to this core functionality, the web client gives employees the ability to:

- Request time off and similar schedule changes
- View the status of schedule change requests
- View productivity information
- Bid for schedules
- View personal accounts, group allowance accounts, and intra-day staffing balances, any of which can affect the approval of a schedule change request. Request schedule trades with other agents, or respond to other agents' trade requests
- Monitor Real-Time Adherence in the web.

Contact center supervisors and administrators can view and manage employee schedule information, facilitate schedule trades, and view agent productivity information. The web client gives supervisors and administrators the ability to perform the following functions including, but not limited to:

- Add, modify, and delete employee segments
- View personal accounts, group allowance accounts, and intra-day staffing balances
- Manually trade employee schedules
- Process agent requests
- Monitor Real-Time Adherence of employees in the web in one or more groups.

1.2.1.1 Aspect Workforce Mobile

The Workforce Engagement Management user interface includes Workforce capabilities designed for mobile phones. Enabling mobile phone capabilities is a licensed feature; contact *Aspect* for more information.

The desktop web capabilities of the Workforce Engagement Management UI can be accessed on mobile devices; simply choose the 'Logon to Desktop Version' link on the login screen.

Note: 1. The Workforce Engagement Management mobile device capabilities only applies to Workforce, and is not applicable to Aspect Performance or Aspect Quality.
2. The Workforce Engagement Management user interface for mobile, differs from the Mobile Notifications feature of Aspect Workforce. See the *Aspect Workforce Empower Installation Guide* for more information.

1.2.2 About Aspect Performance

Aspect Performance reports on data from data sources and provides a complete picture of contact center performance. Through data monitoring and analysis, you can use the product to accurately assess and improve performance across many Key Performance Indicators (KPIs), which are a metric with an associated goal used to measure performance.

By using Aspect Performance, contact centers can monitor performance and engage agents through the use of Coaching. Using the Workforce Engagement Management - Aspect Performance web client, users can:

- View a complete picture of contact center performance at any level through Metrics and Key Performance Indicators (KPIs).
- Assign goals for KPIs to measure Agent performance.
- Use a KPI status to quickly identify problem areas or find areas of the business that are excelling.
- View custom dashboards to focus users' attention to metrics and information that matters
- View custom scorecards to view metrics and KPIs that are important to users, along with an associated score.
- View custom reports that allow users to analyze multi-dimensional data of contact center performance.
- Create coaching actions to help train agents.
- View the impact of completed coaching actions to monitor how coacting affects KPIs, once completed.
- Create awards to motivate agents, and to reward good performance.
- Automatically monitor agents to suggest coaching or assign awards based on custom business rules.
- Use custom forms to automate and manage business process.
- Use Challenges to increase agent engagement, reinforce good behavior, allow supervisors to reward achievement, and use competition to increase agent performance.

1.2.3 About Aspect Quality

Using Aspect Quality, contact centers can record and monitor agents' customer contact. In the Workforce Engagement Management - Aspect Quality web client, users can:

- Search for Aspect Quality recordings for any amount of time with simple search and retrieval.
- Provide individual Agent feedback about the Agent performance on each call.
- Share Aspect Quality recordings across teams for training and quality purposes.

- Share Aspect Quality recordings with peers to provide individual feedback about the Agent performance on each call.
- Configure Aspect Quality to allow an Agent to decide if the Agent should record a call at any time during that call.
- Create Aspect Quality custom scoring templates that Agents can use to evaluate interactions. Agents provide quick feedback about the Agents' own performance; the feature is a great technique for a coaching session where a Supervisor can compare the Manager and Agent evaluations.
- (Optional) Capture Aspect Quality window activities that take place during any call that Quality records. After you search for a call to review, you can play back both the call and the Agent's desktop in multi-media fashion. You can use this feature to drive great process and performance improvements, as well for training purposes.

Note: Not all the features described preceding may be in use in the environment. The configurations may differ from site to site. Check with the Administrator or Supervisor regarding specific questions about the configuration.

1.3 Architecture

The Aspect Workforce Engagement Management application is browser-based and is distributed among the following systems:

- Aspect Workforce Engagement Management web server
- Aspect Workforce, Aspect Performance, or Aspect Quality Web Services web server(s)
- Aspect Workforce, Aspect Performance, or Aspect Quality database server(s)
- Browser-equipped PCs for agents

These systems reside on servers and workstations connected by a LAN and, if applicable, can be accessed using a WAN.

Figure 1-1 shows a typical Aspect Workforce Engagement Management configuration with Aspect Workforce, Aspect Performance, and Aspect Quality

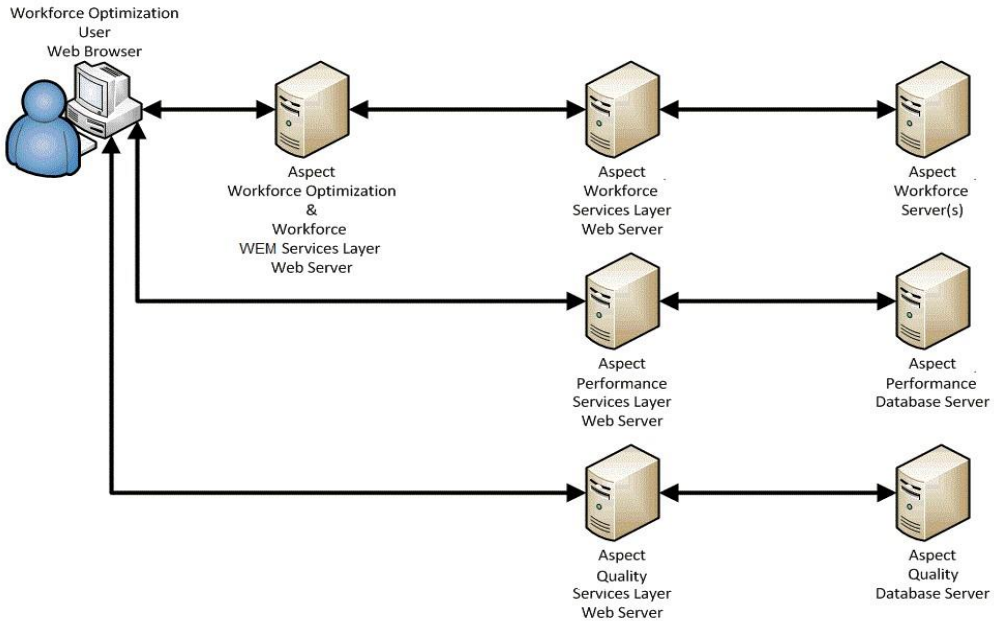


Figure 1-1 *Aspect Workforce Engagement Management Configuration with Aspect Workforce, Aspect Performance, and Aspect Quality*

Note: Your configuration might be different, depending on your business needs.

1.4 Order of Installation Tasks

When you install Aspect Workforce Engagement Management, you complete the following tasks:

1. Complete the installation checklist in Appendix B, Installation and Setup Checklists.
2. Complete the pre-installation tasks described in Chapter 2, Pre-Installation Tasks.
3. Install Aspect Workforce Engagement Management, as described in Chapter 3, Installing Aspect Workforce Engagement Management.
4. Configure Aspect Workforce Engagement Management, as described in Chapter 4, Configure Workforce Engagement Management.
5. Configure Aspect Workforce Engagement Management for the Aspect Workforce component by completing the post-installation tasks described in Chapter 5, Configure Aspect Workforce.
6. Configure Aspect Workforce Engagement Management for the Aspect Quality component by completing the post-installation tasks described in Chapter 6, Configure Aspect Quality.
7. Configure Aspect Workforce Engagement Management for the Aspect Performance component, by completing the post-installation tasks described in Chapter 7, Configure Aspect Performance.
8. Verify that the configuration of Aspect Workforce, Aspect Quality, and Aspect Performance are properly integrated with Aspect Workforce Engagement Management by completing the tasks described in Chapter 8, Verifying the Installation.

9. If you choose not to use the default Aspect Workforce Engagement Management dashboard layout, configure a new Aspect Workforce Engagement Management dashboard layout, as described in the Chapter 9, Dashboard Configuration.

2. Pre-Installation Tasks

This chapter describes how to prepare your system for installing Aspect Workforce Engagement Management™. It includes instructions for installing all prerequisite software.

2.1 Pre-Installation Considerations

Consider the following before installing Aspect Workforce Engagement Management:

- Before you begin the pre-installation tasks, ensure that your environment meets all requirements described in the following guides: • *Aspect Workforce™ Planning Guide*
- *Aspect Performance™ Planning Guide*
- *Aspect Quality™ Planning Guide*
- The Aspect Workforce Engagement Management web server must be a computer with a standard DNS name. In particular, the underscore character is not allowed.
- All applications that access Aspect Workforce, including Aspect Workforce Engagement Management, should be installed with user accounts that are:
- An Administrator User on the server where installing Workforce Engagement Management, *and*
- Domain accounts, *and*
- Local administrators on all Aspect Workforce servers in your deployment Work with your network administrator to set up these accounts.
- Aspect Workforce Engagement Management requires the use of three services:
- Aspect Message Routing (AMR)
- WFM Dispatcher
- WFM Web Services

For more information regarding the installation and configuration of these services, please refer to the *Aspect Web Services Installation Guide*.

- Aspect Workforce Engagement Management requires a domain user that also exists in Workforce as an administrator user in the Users module. For more information on configuring domain user access to your Workforce database, please see the *Aspect Workforce™ Installation Guide*, section 4.4.5 for MS SQL Server, or section 5.3.2 for Oracle.

2.1.1 Running Windows Server with UAC Enabled

In Windows Server 2022 and 2025, enabling User Account Control (UAC) provides a higher level of security but requires more user interaction when performing procedures. If you are running Windows Server with UAC enabled, special actions are required when running the setup program for Aspect Workforce Engagement Management and for related procedures.

Table 2-1 describes the actions required to perform common installation-related procedures in Aspect Workforce Engagement Management.

***Table 2-1** Effects of UAC on Installation-Related Procedures*

Procedure	Actions Required
Installing	Launch **Setup.exe** from the Aspect Workforce Engagement Management software CD. When installing with the command line, launch the command prompt with administrative privileges. Silent installation command would look like: [path]/WFO.msi -q -c CONFIG_FILE=#{Alvaria_wfo_config} MSI Arguments explained: -q => Quiet Mode means that no UI will be shown -c => Command allows for passing in additional command options WFO Arguments explained: CONFIG_FILE => This is the location to the configuration file that will be used to pass Workforce Engagement Management Parameters into it. Configuration File options INSTALLDIR => Path to where the installation files will be stored IIS_SITE_NAME => This is the display name of the web site as seen in the IIS Manager. This is only required if multiple web sites exist in IIS. Example Configuration File <?xml version="1.0" encoding="utf-8"?> <Install> <Options> <INSTALLDIR><%install_path%></INSTALLDIR> <IIS_SITE_NAME><%website_name%></IIS_SITE_NAME> </Options> </Install>

***Table 2-1** Effects of UAC on Installation-Related Procedures*

Procedure	Actions Required

Modifying Aspect Workforce Engagement Management components after initial installation	Launch **Setup.exe** from the Aspect Workforce Engagement Management software CD, and select **Modify** in the Program Maintenance dialog box. When installing with the command line, launch the command prompt with administrative privileges. You cannot make changes using **Control Panel > Programs > Programs And Features**.
Repairing	Launch **Setup.exe** from the Aspect Workforce Engagement Management software CD, and select **Repair** in the Program Maintenance dialog box. When installing with the command line, launch the command prompt with administrative privileges. You cannot repair using **Control Panel > Programs > Programs And Features**.
Uninstalling	Do either of the following: • Launch **Setup.exe** from the Aspect Workforce Engagement Management software CD, and select the **Remove** option. • In the Windows Control Panel, go to **Programs > Programs And Features**. In the list of programs, select **Workforce Engagement Management** and click **Uninstall**.
Modifying configuration files in the Program Files folder	Copy the file to your desktop, edit the desktop file, and copy the edited file to the Program Files folder by overwriting the existing file.

2.2 Installing Internet Information Server (IIS)

All deployments of Aspect Workforce Engagement Management require pre-installation of Internet Information Server (IIS) on the Aspect Workforce Engagement Management web server.

Microsoft Internet Information Server (IIS) is web server software that uses HTTP (Hypertext Transfer Protocol) to deliver data to the web service engine.

When installing IIS For Windows Server 2022 and 2025 it is necessary to select and configure specific roles that are appropriate for Aspect Workforce Engagement Management.

2.2.1 For Windows Server 2022 and 2025

To install IIS for Windows Server 2022 and 2025, perform the following steps.

1. On the Aspect Workforce Engagement Management web server, click the **Start** icon, and click the **Server Manager** icon.
2. On the Dashboard of Server Manager, click **Add Roles And Features**.
3. If the **Before You Begin** window is displayed, review the information, and click **Next**.
4. In the Select Installation Type window, select **Role-Based Or Feature-Based Installation,** and click **Next**.

5. In the Select Destination Server window, select the **Select A Server From The Server Pool** option.
6. Select the **Aspect Workforce Engagement Management** web server in the Server Pool list, and click **Next**.
7. In the Select Server Roles window, in the Roles list, select the **Web Server (IIS)** check box and click **Next**. The Add Roles and Features wizard opens.
8. To add the features required for Web Server (IIS), click **Add Features**.
9. On the Select Server Roles window, with the Web Server (IIS) check box selected, click **Next**.
10. On the Select Features window, click **Next**.
11. On the Web Server Role (IIS) window, click **Next**.
12. On the Select Roles Services window, leave the default Role Services selected, and select the following.
    - **Web Server > Security > Windows Authentication**
    - **For Windows Server 2022: Web Server > Application Development > ASP.NET 4.8**

    •For Windows server 2025: Web Server > Application Development > ASP.NET x.x •

    Web Server > Application Development > WebSocket Protocol

    Note: Several default selections are not required by Aspect Workforce Engagement Management and can be disabled. For a list of selections that can be disabled, see Appendix B, Notes on the IIS Role Services for Windows
13. Add the features required for ASP.NET 4.7/4.8 by clicking **Add Features**.
14. Click **Next**. The Confirm Installation Selections window opens.
15. Click **Install**. The Installation Progress window opens.
16. When the Installation Succeeded message opens, click **Close**.

Note: If a Reverse Proxy or Load Balancer is used, it should have **sticky sessions enabled.**

3. Installing Aspect Workforce Engagement Management

This chapter describes how to install Aspect Workforce Engagement Management.

The Aspect Workforce Engagement Management layer acts as the platform for a suite of Aspect products. It is required in order to be able to use Aspect Performance, Aspect Workforce, and Aspect Quality. Use the Aspect Workforce Engagement Management Install Wizard to install Aspect Workforce Engagement Management.

Note: Aspect Workforce Engagement Management can be installed on its own server, or side by side on one of the Performance Management servers, on the Workforce Web Services server, or on the Aspect Quality Web Services server. If you want to maximize scalability of Workforce Engagement Management - for example, with Aspect Quality - you should always install Workforce Engagement Management on a separate server.

Before you begin installing Aspect Workforce Engagement Management, verify the Prerequisites and Requirements.

3.1 Prerequisites and Requirements

You can install the following programs prior to running the Workforce Engagement Management installer. If you do not install these programs prior to running the Workforce

Engagement Management installer, the installer installs the missing prerequisites: •

Microsoft .NET 4.7.2

- Microsoft System CLR Types for Microsoft SQL Server 2014 SP2 or 2016 SP1
- Microsoft Report Viewer 2015 Runtime
- Microsoft .NET Core Hosting Bundle 6.0
- Microsoft URL Rewrite Module 2.1

You ***must*** install the following programs ***prior to*** running the Workforce Engagement Management installer:

•Windows Server 2022 or 2025.

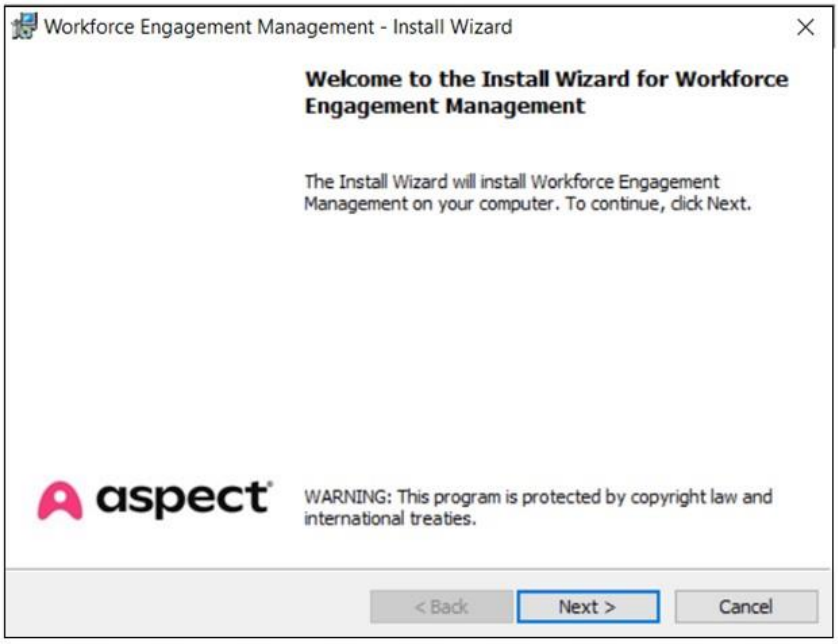
- IIS. See Installing Internet Information Server (IIS) on page 2-15.

You have administrator access to the machine you are using.

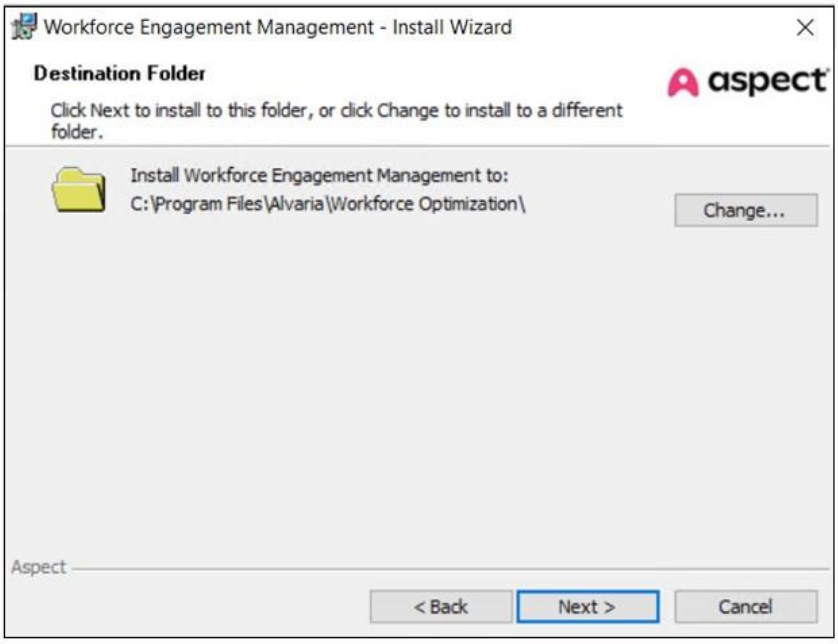
3.2 Installation Procedure

1. Log in to the machine on which you are installing Aspect Workforce Engagement Management.

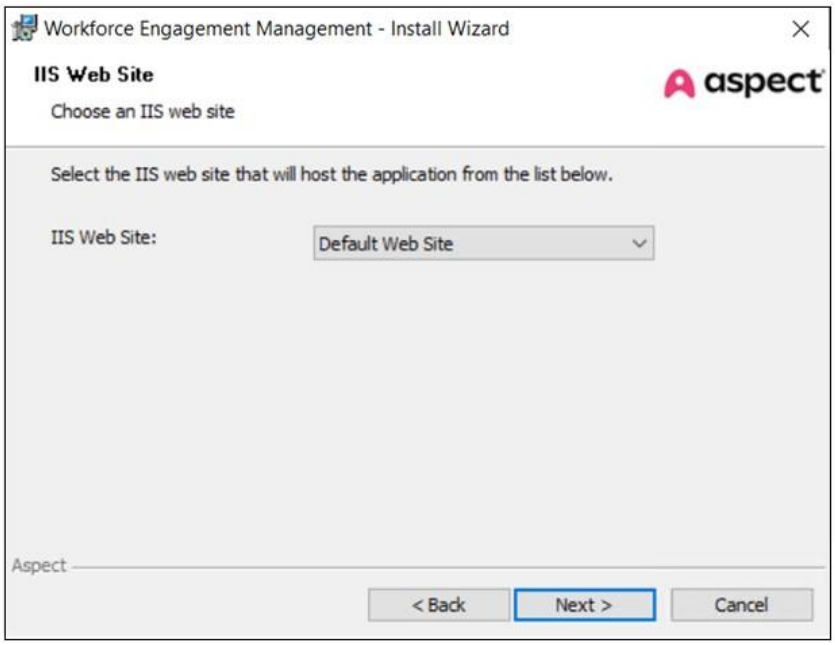
2. Depending on the installation media, install the product CD or double-click on the Setup.exe. The Workforce Engagement Management Install Wizard displays:



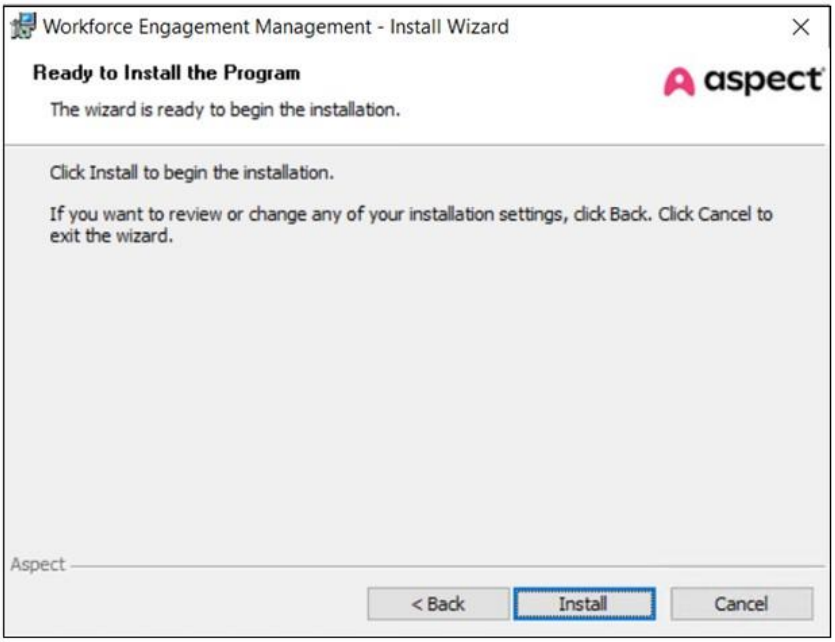
3. Click **Next**. The Destination Folder part of the Wizard displays:



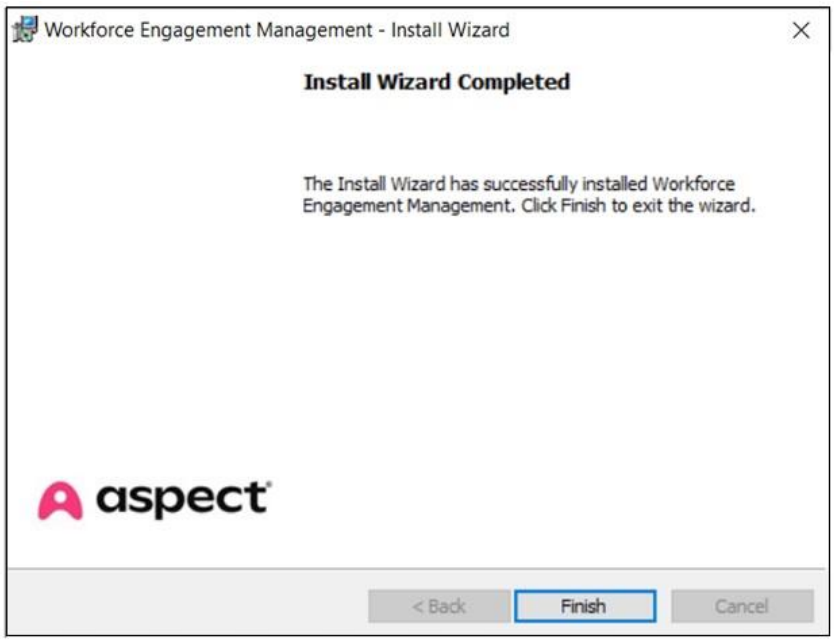
4. Either accept the default file path or change the path. Click **Next**.
5. Select the **IIS Web Site**. Click **Next**.



6. Click **Install** to complete the installation:



When the installation is completed, the **Install Wizard Completed** message displays.



7. Click **Finish** to exit the wizard.

   The Aspect Workforce Engagement Management directories and files are now on your server.

Note: As part of the Aspect Workforce Engagement Management installation, the Workforce Management Data Service is installed. It is visible under IIS. The service is not used by Aspect Performance or Aspect Quality.

To uninstall Aspect Workforce Engagement Management, see Uninstalling with the Setup Program or Uninstalling with Windows Control Panel.

3.2.1 Uninstalling with the Setup Program

To uninstall Aspect Workforce Engagement Management with the setup program:

1. Log in to the Aspect Workforce Engagement Management web server.
2. Launch **Setup.exe** from the Aspect Workforce Engagement Management ISO image. The Installation Wizard dialog box opens.
3. Click **Next**.
4. Select **Remove**, and then click **Next**. The Remove The Program window opens.
5. Click **Remove**. After the files are uninstalled successfully, the Install Wizard Completed window is displayed.
6. Click **Finish** to exit the wizard.

3.2.2 Uninstalling with Windows Control Panel

To uninstall Aspect Workforce Engagement Management with Windows Control Panel:

1. Log in to the Aspect Workforce Engagement Management web server.
2. In Windows Control Panel, browse to **Programs > Programs And Features**.
3. Select **Workforce Engagement Management** in the list of programs, and click **Uninstall**. Aspect Workforce Engagement Management is then uninstalled automatically, with no user interaction required.

3.3 Set Machine Key for CSRF Anti-Forgery Token

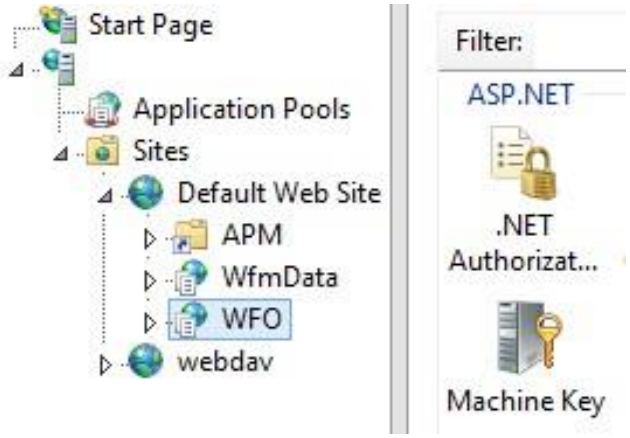
Workforce Engagement Management has support for stopping cross site request forgery (CSRF) attacks by implementing an anti-forgery token that is used in all communication with the client and Workforce Engagement Management and the connecting systems Web API layers; Performance, Quality and Workforce.

This option is enabled by default in all products, but requires a manual step to configure each product. This is done by setting a machine key in the web.config file of each product. The machine key must be the same across all products to ensure the anti-forgery token can be decrypted and read by the Web API to confirm the incoming request is valid. If this is not done, then HTTP POST, PUT and DELETE requests will fail with a 403 forbidden response code.

Note: This needs to be done on each Workforce Engagement Management server, and on each Application server of the systems connecting to Workforce Engagement Management.

To set the machine key attribute, perform the following steps.

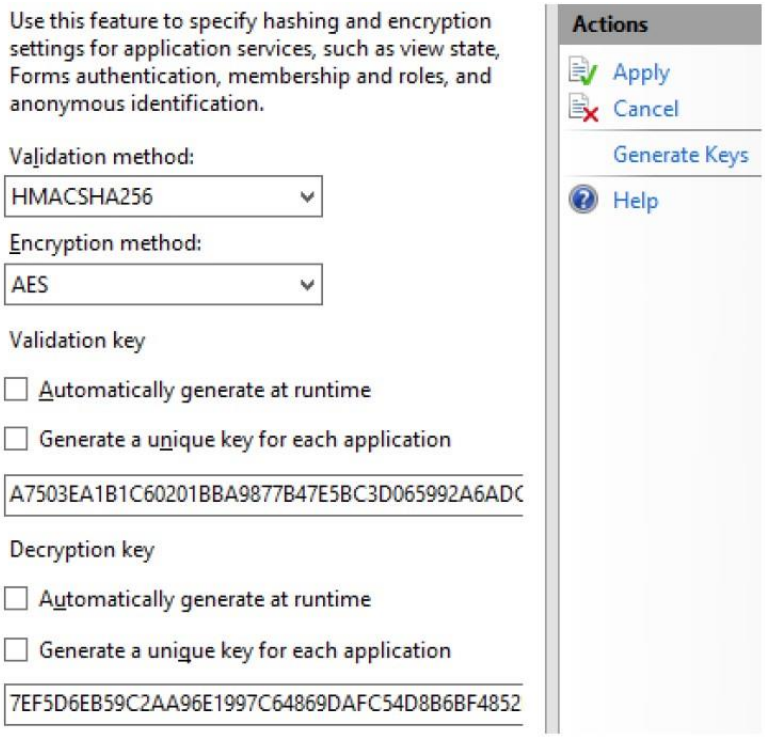
1. Log onto the Workforce Engagement Management server as an Administrator.
2. Open IIS, Start > Administrative Tools > Internet Information Services (IIS) Manager.
3. On the left-hand pane, navigate to the Workforce Engagement Management Application. Typically, under **Server > Sites > Default Web Site > WFO**
4. In the middle pane, double click **Machine Key**.



5. The Machine Key pane opens. Set the following properties:
   - **Validation method: HMACSHA256**
   - **Encryption method: AES**
   - **Validation Key - Automatically generate at runtime: Deselect the checkbox**
   - **Validation Key - Generate a unique key for each application: Deselect the checkbox**
   - **Decryption Key - Automatically generate at runtime: Deselect the checkbox**

- **Decryption Key - Generate a unique key for each application: Deselect the checkbox**

6. On the right-hand pane, click **Generate Keys**, then **Apply**, and exit IIS Manager.



Note: The machine key for CSRF anti-forgery token for Workforce Engagement Management **must match** the machine key in Workforce, Quality, and Performance.

These procedures are covered in the following chapters:

- Chapter 5, Configure Aspect Workforce
- Chapter 6, Configure Aspect Quality
- Chapter 7, Configure Aspect Performance

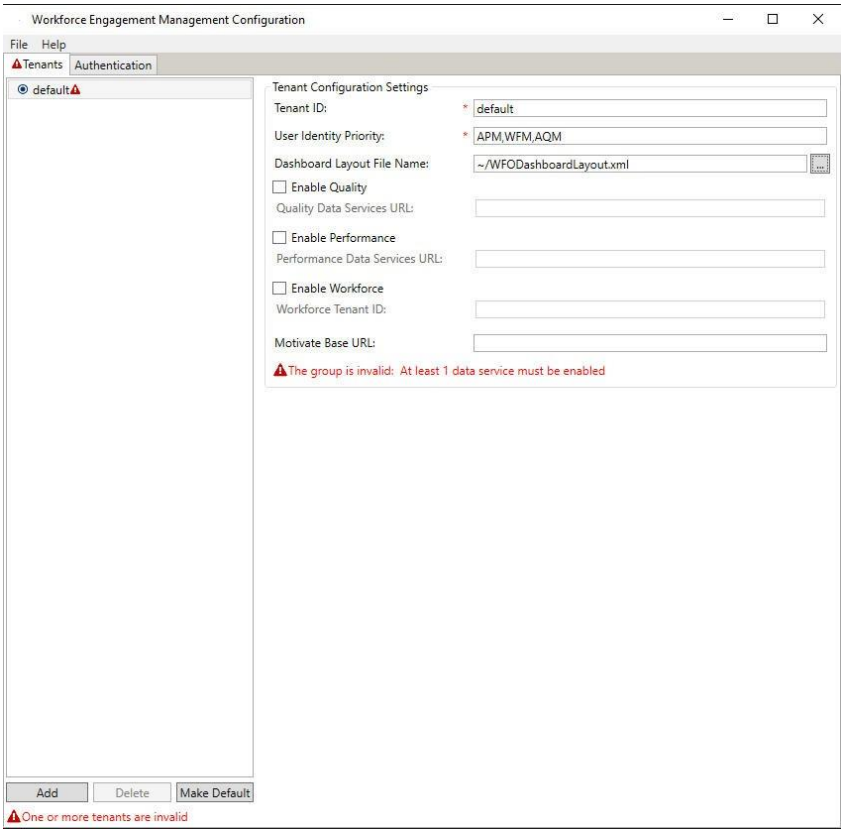
4. Configure Workforce Engagement Management

Installing Aspect Workforce Engagement Management also installs a tool for configuring Workforce Engagement Management™. You can access this tool on the Windows Start menu at the following path:
For Windows Server 2022 and 2025:
Start > Aspect > Workforce Engagement Management Configuration
This utility enables you to configure the Quality, Performance, and Workforce areas of the Aspect Workforce Engagement Management client.

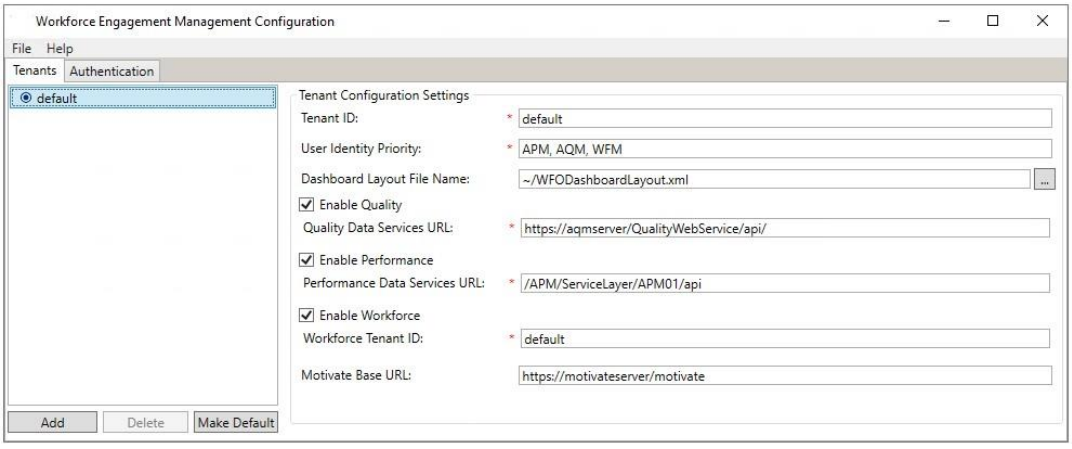
4.1 Configuration Utility Basic Features

The Aspect Workforce Engagement Management configuration utility is organized into multiple tabs. (Some tabs are displayed only when you have selected Advanced Mode, as described later in this chapter.) Each tab contains a collection of related configuration settings. Some settings are further organized into groups within the tab.

When a field is invalid, a red triangle warning icon will appear to next to the field. This icon provides a tool tip that explains the reason that the field is invalid. The following screen shot shows an example of the warning message, which is displayed in this case because neither the Performance, Quality, nor the Workforce check box has been selected.



Below is the image that includes the Motivate Base URL image:



If a group contains an invalid field, or is invalid for any other reason, then the same warning icon will appear at the bottom of the group. If any field or group is invalid on a tab, then a warning icon will also appear on the tab title. The configuration may be saved while invalid, but a warning message will be displayed.

The configuration tool will automatically open the correct configuration file if both the tool and configuration file have been delivered with the Aspect Workforce Engagement Management installer.

Use the **File > Open** command if the tool does not open the configuration file automatically, or if another configuration file is to be edited. By default, the correct configuration file is delivered to the following path:

\<ProgramFiles>\Alvaria\Workforce Engagement Management\Default\Web\WFO\web.config

To commit changes, use the **File > Save** or **File > Save As** command.

The **File > Advanced Mode** menu item toggles the visibility of advanced configuration settings that normally do not need to be changed. These advanced settings will be discussed later in this chapter.

4.2 Tenants Tab

The Tenants tab of the configuration tool enables the configuration of the Workforce, Quality, and Performance areas of the Aspect Workforce Engagement Management client. This tab enables the tenant configuration and also specifies the location of the configuration file that defines the layout of the Aspect Workforce Engagement Management dashboard.

At least one data service in the Data Services section must be enabled for Aspect Workforce Engagement Management to function.

4.2.1 Working with Tenants

The tenant feature of Workforce Engagement Management allows users to utilize multiple environments via a single instance. You can have multiple Workforce Management databases connected to one Workforce Engagement Management server. These databases can be managed by one or more Workforce Management main application servers.

4.2.1.1 Adding a Tenant

To add a tenant in Workforce Engagement Management, click the Add button on the lower-left corner of the Tenants tab. This displays a blank configuration screen that you must complete as described in the remainder of this chapter.

Since the Tenant ID is used as part of the URL to access Workforce Engagement Management, no special characters that would be rejected by a browser can be used.

If the new tenant name is not acceptable, a warning icon will be displayed.

4.2.1.2 Deleting a Tenant

To delete a tenant, highlight the tenant name in the list, and click the Delete button on the lower-left corner of the Tenants tab.

4.2.1.3 Designate a Default Tenant

Workforce Engagement Management is installed with a blank tenant named Default which is automatically designated as the default tenant. You can change the default tenant to a different tenant or change its name.

When a user navigates to http://server/WFO, the default tenant is assumed. To navigate to a non-default tenant, you must include the Tenant ID in the URL. An example of a non-default URL would be http://sever/WFO/TenantID.

To designate a default tenant, simply highlight the tenant name in the list and click the Make Default button.

4.2.2 Tenant ID

To change the name of the Tenant ID, complete this field. This field must meet the ID requirements as described above. If the requirements are not met, a warning icon will be displayed with a short message indicating why it was rejected.

4.2.3 User Identity Priority

If you are using the Workforce component with the Performance or Quality component, configure the User Identity Priority setting. This setting controls which system provides the user name that an Aspect Workforce Engagement Management user sees in the user interface.

The User Identity Priority setting is a comma-separated list of identifiers for each Aspect system to which Aspect Workforce Engagement Management is configured to connect. **WFM** indicates Aspect Workforce, **APM** indicates Aspect Performance, and **AQM** indicates Aspect Quality. The first system to which Workforce Engagement Management can connect *and* for which the current user is a valid user will contribute the user name. The systems are searched in the order dictated by the User Identity Priority setting.

4.2.4 Dashboard Layout File Name

The default value of the file name is empty, indicating that Aspect Workforce Engagement Management will not display any dashboards. To enable the display of dashboards in Aspect Workforce Engagement Management, click the ellipsis button and select **WFODashboardLayout.xml**. This file configures the system to use the default dashboard layout installed by the Aspect Workforce Engagement Management installation utility. For more information on the Aspect Workforce Engagement Management Dashboard Layout, see Chapter 9, Dashboard Configuration.

The dashboard layout file name setting designates which dashboard layout XML file should be used to select dashboards to show to Aspect Workforce Engagement Management users.

Note that this setting is a URL which begins with the tilde (~) to indicate the root of the Aspect

Workforce Engagement Management web site. The dashboard layout XML file may reside anywhere within subfolders of the Aspect Workforce Engagement Management web site.

Note: Depending on which Workforce Management module widgets are included in the Workforce Management dashboard, enabling the display of dashboards can increase server load on your Aspect Workforce Engagement Management system.

4.2.5 Enabling Workforce Management in Aspect Workforce Engagement Management

To enable Workforce Management features, select the Enable Workforce Management check box. You will need to enter the Workforce Management Tenant ID that matches the Tenant ID configured in the Workforce Management Data Services Configuration tool as described in Using the Workforce Management Data Services Configuration Utility on page 5-40.

4.2.6 Enabling Quality in Aspect Workforce Engagement Management

For information about enabling Quality in Aspect Workforce Engagement Management, see Chapter 6, Configure Aspect Quality.

4.2.7 Enabling Performance Management in Aspect Workforce Engagement Management

For information about enabling Performance Management in Aspect Workforce Engagement Management, see Chapter 7, Configure Aspect Performance.

4.3 Authentication Tab

This section describes the settings found on the Authentication tab.

4.3.1 Authentication Protocol

This drop-down list gives the options to choose Windows Authentication, Federation/Claimsbased Authentication, or OAuth 2.0/OpenID Connect Authentication.

If Windows Authentication is the desired method, no further settings need to be configured on this tab.

By default, Workforce Engagement Management authenticates to IIS using Windows Authentication. More information regarding Windows Authentication is discussed in About the Windows Credentials Dialog on page 8-79.

If you select Federation/Claims-based Authentication, the Federation Settings section is enabled and requires completion. This method is also dependent upon installation and configuration of a token server. Aspect officially supports only ADFS 4.0 on Windows Server 2022 and 2025 as a token server, although you can configure any token server that supports issuing SAML 1.1 and SAML 2.0 tokens using the WS-Federation to work with Workforce Engagement Management.

Aspect Customer Care only offers limited support for token servers other than ADFS 4.0.

For assistance in configuring ADFS 4.0 as the token server for Workforce Engagement Management, see Appendix C, Security and Authentication.

Note: Although OAuth 2.0/OpenID Connect can be selected, this option is unsupported and used only for Aspect Via (Aspect's Cloud offering). The settings for this option are not documented in this guide.

4.3.2 Federation/Claims-based Authentication

4.3.2.1 Token Server Realm/Audience

This field is used to configure how Workforce Engagement Management identifies itself to the security token server.

When Workforce Engagement Management communicates with the token server, it provides this value as the Relying Party ID. The token server must have a Relying Party Trust configured for the value specified in Token Server Realm before a claim token will be issued.

Typically this value is the fully qualified HTTPS URL for Workforce Engagement Management, but it can be any value and does not have to be a URL. For example, "https://wfm.Alvaria.com/ wfo/". This value must match exactly the Relying Party Identifier configured on the token server and is case sensitive.

See section Configure the ADFS Relying Parties on page C-104 for step by step instructions to configure your AD FS server.

4.3.2.2 Additional Audience

You do not need to configure this field for Workforce Engagement Management.

4.3.2.3 Token Server Issuer

This field is used to configure the HTTPS WS-Federation endpoint published by a token server which authenticates the user. This value will vary depending on the specific token server. Often this is referred to as the WS-Federation Passive Requestor Endpoint in token server documentation.

To find this value in AD FS 4.0, open the AD FS Management tool on the server and browse to **AD FS > Service > Certificates** in the navigation tree. Double click the Service communications certificate and make note of the "Issued to" value. Next browse to **AD FS >**

Service > Endpoints and make note of the URL Path for the endpoint of the type **"**SAML 1.1/ WS-Federation". The value to enter in the Token Server Issuer field is:

`https://<Certificate_Issued_To>/<URL_Path>`

where <Certificate_Issued_To> is the fully qualified host name from the Service communication certificate and <URL_Path> is the value from the endpoints screen. For example: `https://adfs.Alvaria.com/adfs/ls`

4.3.2.4 Token Server Signing Certificate Thumbprint

This field must be the thumbprint from the certificate used by the token server to sign the tokens it issues, usually referred to as the Token Signing Certificate in token server documentation.

In AD FS 4.0 this can be found by browsing to **AD FS > Service > Certificates** and locating the Token-signing certificate. If there are multiple token signing certificates installed then the one used when Configure the ADFS Relying Parties on page C-104 must be used. Double click this certificate and make note of the Thumbprint value on the Details tab. Enter this value in the "Token Server Signing Certificate Thumbprint" field in the Workforce Engagement Management configuration tool. Omit any spaces.

To eliminate the possibility of mistakes while typing this value, you may import the certificate with the Workforce Engagement Management configuration tool. First, when viewing the certificate properties in the AD FS Management tool, open certificate's Details tab and click the Copy to File button. Choose the X.509 .CER format and save to disk. Next, copy the exported
.CER file to the Workforce Engagement Management server. Open the Workforce Engagement Management configuration tool and chose **File > Load from Certificate**. Pick the .CER file and the thumbprint value will be imported into the configuration tool.

Note that this step must be performed for both the Workforce Engagement Management and Workforce Management Data Services for Workforce Engagement Management configuration tools.

4.3.2.5 Thumbprint Issuer Friendly Name

This is the name of the thumbprint. A good rule of thumb would be to name the thumbprint the server and the issuer of the trust.

4.4 Advanced Mode

To display the advanced settings tabs and fields, select **File > Advanced Mode** in the Aspect Workforce Engagement Management Configuration utility. When Advanced Mode is enabled, several advanced fields and tabs will become visible. These settings typically do not need to be changed and should be changed with caution, since changing them may result in undesired behaviors.

4.4.1 Advanced Settings Tab

This section describes the advanced settings that are configured on the Advanced Settings tab.

4.4.1.1 Enable Bundle Optimization

Enabling Bundle Optimization is an option used by Aspect Customer Care for troubleshooting purposes. If the check box is deselected, it unbundles the code, allowing it to be read. Do not disable this without first consulting with Aspect Customer Care.

4.4.1.2 Require HTTPS

If you are using the HTTPS protocol, the Require HTTPS setting causes Aspect Workforce Engagement Management to refuse non-encrypted connections. This setting is useful if enhanced security is required, but non-encrypted connections are still allowable on the web server hosting Aspect Workforce Engagement Management for other purposes.

4.4.1.3 Reporting Services

You can optionally enter a Domain, User, Password, and Password Confirmation of a user that you want to connect to Reporting Services. For more information, see the *Aspect Performance Installation Guide*.

4.4.1.4 Anti-forgery

This field is pre-populated with the default Claims Type identifier used by Workforce Engagement Management for anti-forgery protection in claims authentication mode. This identifier can be modified here if a different Claim Type is required (for example, if the ADFS configuration is outside of Workforce Engagement Management's control)

4.4.2 Supported Languages Tab

The Supported Languages tab allows an administrator to control what language is used if the user chooses a language which is not available for a feature. By default, any feature lacking a translation in the chosen language will use English.

The Supported Language tab is configurable. For assistance in changing the displayed configuration, contact Aspect Customer Care.

4.4.3 Authentication Tab

The Authentication tab displays some additional fields when the Show Advanced Settings is enabled.

4.4.3.1 Bonus Additional Audience

In a rare circumstance, where SAML tokens are trusted by Workforce Engagement Management that is issued for a third audience (in addition to the ones specified in Token Server Realm/Audience and Additional Audience), specify that audience here.

4.4.3.2 Alternative SAML Name Claim Type Schema Mapping

By default, WEM expects the name of the Workforce Engagement Management user to be transmitted within a SAML attribute named **name**, in the namespace http://schemas.xmlsoap.org/ws/2005/05/identity/claims. If the WEM user name is transmitted in a different SAML attribute, specify that attribute here in the format *<namespace>/<name>*. For example, the default **name** attribute would be specified as http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name.

4.4.3.3 Specifies if Federation Requires Communication over HTTPS (checkbox)

Deselect this option to allow communication with a SAML server over a non-secure connection. This option should always remain selected, otherwise, Workforce Engagement Management may accept SAML tokens over an unsecure HTTP connection that allows a 3rd party to see and steal the SAML token. This option is only offered to allow for diagnostics during initial setup, and many SAML token servers do not support unsecure connections.

4.4.3.4 Inactivity Timeout (Minutes)

If a 0 value is specified for this field, a user's Workforce Engagement Management session ends when the SAML token expires. If the Workforce Engagement Management user's session should be extended while the user remains active beyond the SAML token's expiration, then specify the number of minutes the user must remain inactive to be automatically logged out. The user's session is valid as long as the SAML token is valid, irrespective of the value specified.

4.4.3.5 Absolute Timeout (Minutes)

This value is only active when a non-zero **Inactivity Timeout (Minutes)** value is specified. If this value is non-zero, the user's session ends after the specified time even if the user remains active. This can prevent user sessions from being extended indefinitely when an inactivity timeout is specified.

4.4.3.6 Important Claims

This field can always be left blank. The Additional claims specified in the format discussed in Alternative SAML Name Claim Type Schema Mapping can be specified here as a commaseparated list if a Workforce Engagement Management customization requires the value of additional claims to be preserved.

4.5 Workforce Engagement Management with Firefox

By default, the Mozilla Firefox web browser does not allow the pass-through of the Windows domain user credentials when the web application being accessed is configured for Windows Authentication. In the case of Aspect Workforce Engagement Management, each time you access the application, Firefox challenges you to enter your user credentials.

Note: Aspect Quality with Aspect Workforce Engagement Management is compatible with Firefox version 3.0 or above on Microsoft Windows 7+.

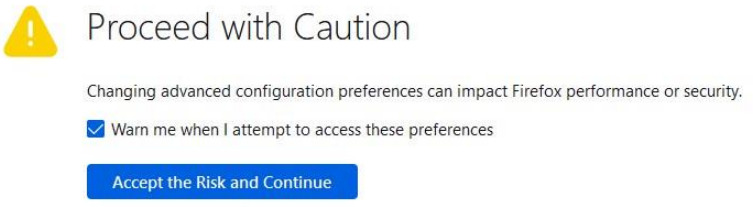
Also, Firefox does not utilize the common certificate repository in Windows which both Google Chrome and Microsoft Edge utilize. As such, if the Certificate Authority (CA) which issued the certificate for Workforce Engagement Management, or any of the connecting systems back end services cannot be verified back to a commonly-trusted root CA, then the certificate for the CA which issued the certificate must be installed in Firefox. If you do not configure the CA, Firefox prompts you with a security alert every time you access Workforce Engagement Management, or any of the connecting systems back end services.

Perform the following procedures to configure Firefox to allow the credentials pass-through for NTLM/Kerberos Windows authentication, and for root CA certificate installation.

- Credential Pass-Through Configuration
- CA Certificate Installation

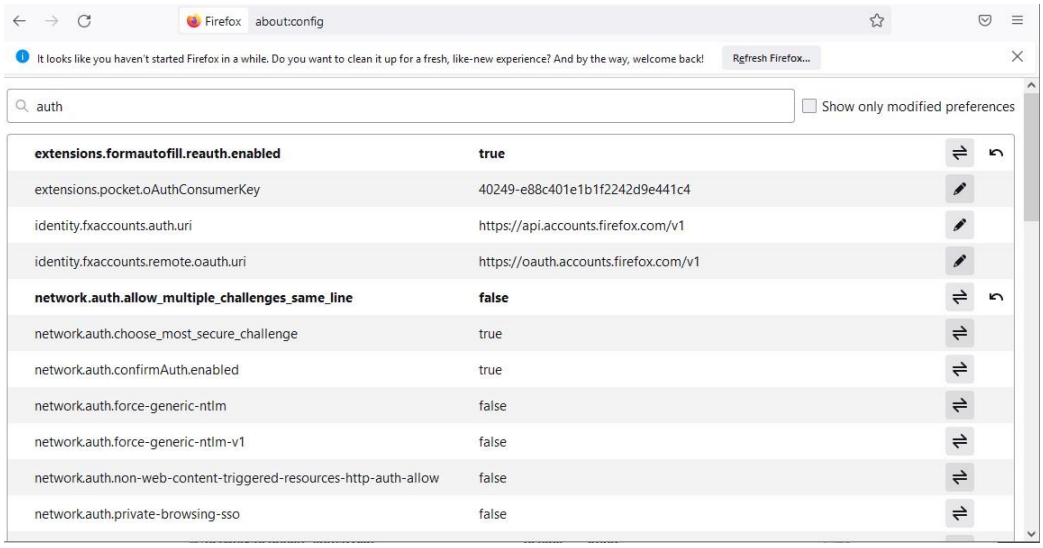
4.5.1 Credential Pass-Through Configuration

1. Launch Firefox.
2. From the address tool bar, browse to **about:config**. A Warning message opens.



3. Click **Accept the Risk and Contibue** Mozilla Firefox main window opens.
4. In the Search text box, type **auth**.
5. Press **Enter**. A Preference Name list displays.

6. Search for and double-click **network.automatic-ntlm-auth.trusted-uris**.



The Enter string value window opens.

7. In the text box, type the Uri for the Aspect Workforce Engagement Management web application root and the back end services delimited with a comma, followed by a space. For example: https://<WFOMachineName>/wfo

   https://<AQMBackEndServiceMachineName>/QualityWebService/api

   https://<APMBackEndServiceMachineName>/APM/ServiceLayer

8. Click **OK**.
9. Repeat steps 6-9 for the following configuration items:

   network.negotiate-auth.delegation-uris

   network.negotiate-auth.trusted-uris

10. Toggle the following entries to **true** by double-clicking each one.

    network.automatic-ntlm-auth.allow-non-fqdn

    network.negotiate-auth.allow-non-fqdn

11. Close all running instances of Firefox.

4.5.2 CA Certificate Installation

To install the CA certificate, see Install the Certificate for Mozilla Firefox Browsers on page 658.

4.6 Saving Your Settings

After configuring Workforce Engagement Management as required, save your settings by selecting **File > Save** in the main menu of the tool. After saving, close the tool by selecting **File > Exit**.

5. Configure Aspect Workforce

This section describes how to configure Aspect Workforce Engagement Management for the Workforce Management component after you have installed Aspect Workforce Engagement Management.

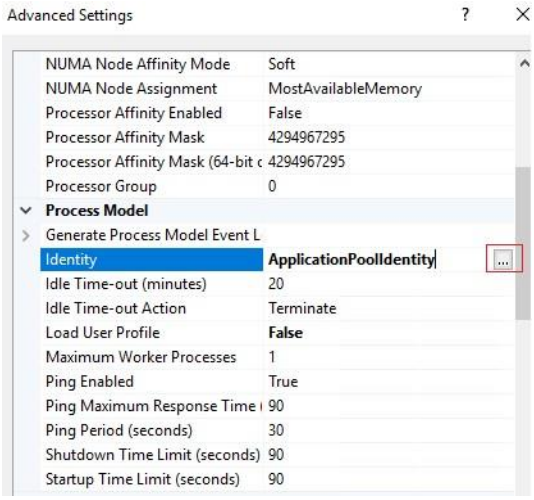
Before you begin, see the *Aspect Workforce Installation Guide* to install Workforce Management and to verify that it is running.

5.1 Configure User Credentials

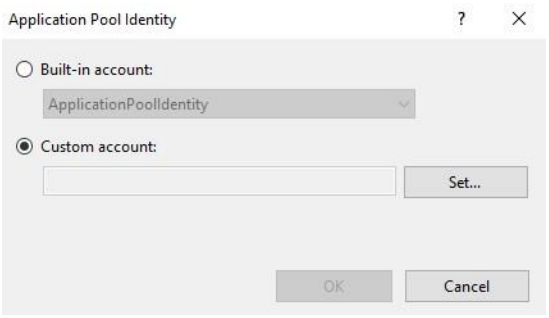
To allow Workforce Engagement Management access to your Workforce database, follow the steps below to configure the Application Pool Identity for the specified application pools.

1. Log onto the Workforce Engagement Management server as an Administrator.
2. Open IIS, Start > Administrative Tools > Internet Information Services (IIS) Manager.
3. Navigate to Application Pools
4. For the **Wem and WemData** application pools, do the following:
   a. Select the application pool, then click **Advanced Settings** in the right pane.

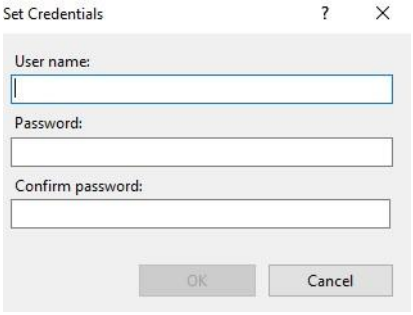
   b. Click ellipsis button next to the **Identity** under **Process Model**.



   c. Select the **Custom account** option in the **Application Pool Identity** dialog box, then click **Set**.



d. **Set Credentials** dialog appears, enter the credentials for the user who has been configured to have access to the Workforce database (MS SQL or Oracle).



Note: The Application Pool Identity custom account should be a domain user that also exists in Workforce as an administrator user in the Users module. For more information on configuring domain user access to your Workforce Management database, please see the *Aspect Workforce™ Installation Guide*, section 4.4.5 for MS SQL Server, or section 5.3.2 for Oracle.

5.2 Updating the Application Key in Aspect Workforce

To ensure security, an encrypted Application Key is used when Aspect Workforce Engagement Management communicates with Aspect Workforce. You enter the key for Aspect Workforce using the procedure shown below. Later, you will enter the same key for Aspect Workforce Engagement Management in the Workforce Management Data Services Configuration Utility, as described later in this chapter.

To update the application key:

1. On an Aspect Workforce server, log in to Aspect Workforce as an administrator.
2. Select **Administration > Access Control > Users**. The Users module opens.
3. In the main menu, select **Special > Update Application Key**. The Update Application Key window opens.
4. In the New Password and Confirm Password fields, type any **string**.

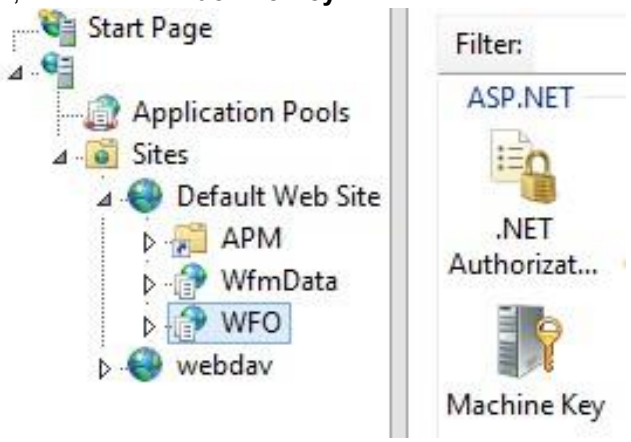
   Note: The string you use for the password does not have any length or complexity requirements.

5. Make a note of the string, since you will need to enter it in the Workforce Management Data Services Configuration Utility Application.
6. Click **OK**.

5.3 Set Machine Key for CSRF Anti-Forgery Token

Verify that you have set the machine key for CSRF anti-forgery token.

1. Based on the procedure that you completed in Set Machine Key for CSRF Anti-Forgery Token, log onto the Workforce Engagement Management server as an Administrator.
2. Open **IIS, Start > Administrative Tools > Internet Information Services (IIS) Manager**.
3. On the left-hand pane, navigate to the Workforce Engagement Management Application. Typically, under **Server > Sites > Default Web Site > WFO.**
4. In the middle pane, double click **Machine Key**.



The Machine Key pane opens.

5. Copy the **Validation Key** and **Decryption Key**.
6. Complete the following steps for all Workforce Management Data application servers (automatically installed with Workforce Engagement Management).
   a. Log onto the appropriate Workforce Engagement Management or application server as an Administrator.
   b. Open IIS, **Start > Administrative Tools > Internet Information Services (IIS) Manager**
   c. On the left-hand pane, navigate to Workforce Management: **Server > Sites > WfmData**.
   d. In the middle pane, double click **Machine Key**.
   e. Set the following properties:

i. - Validation method: HMACSHA256 ii. - Encryption method: AES iii. - Validation Key - Automatically generate at runtime: Deselect the checkbox iv. - Validation Key - Generate a unique key for each application: Deselect the checkbox

v. - Decryption Key - Automatically generate at runtime: Deselect the checkbox

vi.- Decryption Key - Generate a unique key for each application: Deselect the checkbox

f. Paste the **Validation Key** and **Decryption Key** from the Workforce Engagement Management application that you copied in step 5. ***These values must match across all Workforce Engagement Management and product application servers for CSRF protection to work.***

7. In the right-hand pane, click **Apply**, and exit IIS Manager.

5.4 Using the Workforce Management Data Services Configuration Utility

Installing Aspect Workforce Engagement Management also installs a tool for configuring the Workforce Management Data Services. You can access this tool on the Windows Start menu at the following path:

For Windows Server 2022 and 2025:
Start > Aspect > WFM Data Services Configuration for Workforce Management

This utility enables you to configure Workforce Management Data Services for Aspect Workforce Engagement Management to connect to the appropriate services provided by Workforce Management, as well as to specify other relevant Workforce Management settings.

5.4.1 Basic Features

The Workforce Management Data Services configuration utility is organized into multiple tabs. Some tabs display only when you have selected Advanced Mode. Each tab contains a collection of related configuration settings. Some settings are further organized into groups within the tab. When a field is invalid, a red triangle warning icon appears next to the field. This icon provides a tool tip that explains the reason why the field is invalid.

If a group contains an invalid field, or is invalid for any other reason, then the same warning icon appears at the bottom of the group. If any field or group is invalid on a tab, then a warning icon also appears on the tab title. You can save the configuration while invalid, but a warning message displays.

The configuration tool automatically opens the correct configuration file if both the tool and configuration file have been delivered with the Aspect Workforce Engagement Management installer.

If the tool does not open the configuration file automatically, or if another configuration file is to be edited, select **File > Open**. By default, the correct configuration file is delivered to the following path:

\<ProgramFiles>\Alvaria\Workforce Engagement Management\Default\Web\WfmData

To commit changes, select **File > Save** or **File > Safe As**. The **File > Advanced Mode** menu item toggles the visibility of advanced configuration settings that usually you do not need to change.

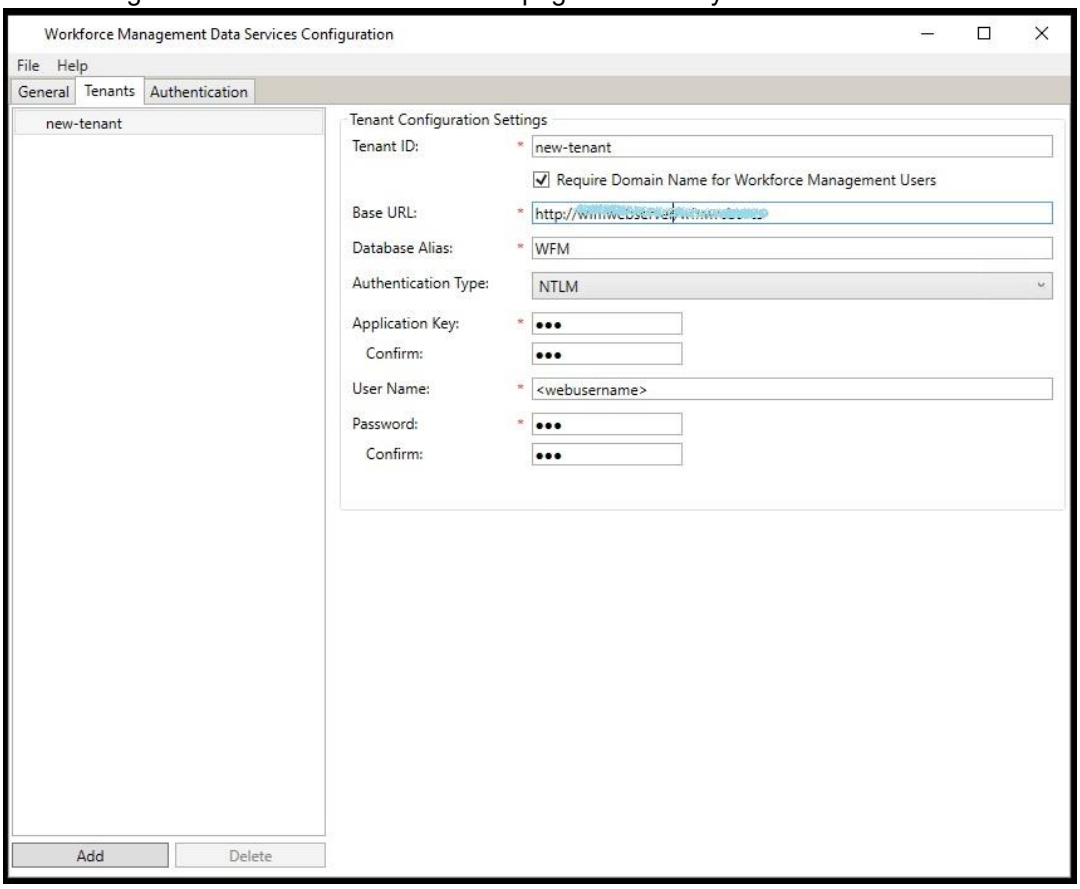
5.4.2 General Tab Configuration

The General tab of the configuration utility is used to input the encryption key.

The Encryption Key is the key used to encrypt the various passwords that are needed to connect to the Workforce Management Web services. This is a required value. This string can be of any length and can contain any characters. The Encryption Key is a different entity from the Application Key, described earlier in Updating the Application Key in Aspect Workforce on page 5-38.

5.4.3 Tenants Tab Configuration

The following screen shot shows the Tenants page of the utility.



The following sections describe the fields on the Tenants page.

5.4.3.1 Tenant ID

To change the name of a Tenant ID, enter the value here. This is the tenant identifier for the Workforce Management Data layer, and must match the Workforce Management Tenant ID (see Tenants Tab on page 4-26) found in the Workforce Engagement Management Configuration.

Since the Tenant ID is used as part of the URL to access Workforce Engagement Management, no special characters that would be rejected by a browser can be used.

If the new tenant name is not acceptable, a warning icon will be displayed.

To add a new tenant, click the Add button on the lower-left side of the Tenants tab and complete the required fields.

5.4.3.2 Require Domain Name for Workforce Management Users

Indicates whether or not the user within the Aspect Workforce database must be prepended with the Domain Name to which the user is authenticating. If this feature is enabled, Workforce Management user accounts must exist which are prefixed with the domain of the Aspect Workforce Engagement Management user.

Enabling this feature is useful if you have Aspect Workforce Engagement Management users spread across multiple domains. In that case, using the domain name is recommended for authentication to prevent collision issues with user names. Note that local machine accounts will need to be prefixed with the Aspect Workforce Engagement Management server name if this feature is enabled.

For example, if the Aspect Workforce Engagement Management server is named **lom-wfo-01**, and you are using local machine users, the users in Workforce Management must be prefixed with **lom-wfo-01** when this feature is enabled. For example: **lom-wfo-01\wfouser1**. If the same server is joined to the **corporate_global** domain, the same user in Workforce Management would be named **corporate_global\wfouser1**. If the Require Domain Name feature is disabled, you can name your Workforce Management user simply **wfouser1**.

Enabling this feature also allows a user to connect two tenants to the same database alias while having Workforce Engagement Management users mapped to different users, one with domain name and one without. This allows a single windows identity that could be a supervisor in one tenant and an employee in another just by changing the domain name.

5.4.3.3 Database Alias

The alias used to identify the Aspect Workforce database that the Workforce Management Web Services will use.

5.4.3.4 Authentication Type

The type of authentication to use when connecting to the Workforce Management Web Services. This can be either NTLM or Basic. This setting must match the setting configured for the web services during installation of the Workforce Management Web Services.

1. NTLM (Windows)

The NTLM method uses the default authentication protocol used by Windows operating systems. This option uses the User Name and Password specified when accessing the Aspect Web Services, and transmits the password across the network using encryption.

2. Basic

The Basic method of authentication will use the standard HTTP Basic authentication implementation. This option uses the User Name and Password specified when accessing the Aspect Web Services, and transmits the password across the network in plain text (a less secure method than encryption).

5.4.3.5 Application Key

Enter the same key that you created in the section Updating the Application Key in Aspect Workforce.

5.4.3.6 User Name

The user name that is used to access the Workforce Management web services. This user must be a domain account or a local account on the WFM Web Services web server and must also be a user in Aspect Workforce, such as WFMDISPATCHER.

5.4.3.7 Password

The password associated with the user name in the previous section, used to access the Workforce Management web services.

5.4.4 Authentication Tab

To configure the Authentication tab for Workforce Management, refer to the settings in Workforce Engagement Management's Authentication tab (see Authentication Tab on page 428). Copy the values from Workforce Engagement Management's configuration to Workforce Management. Then, apply the following additional changes.

- If using Federation/Claims-based Authentication
- Copy the value from the **Token Server Realm/Audience** field into the **Additional Audience** field.
- Edit the **Token Server Realm/Audience** field value, changing the trailing **/WFO** to **/WfmData**.

5.4.5 Saving Your Settings

After configuring the General and Workforce Management Web Services pages, save your settings by selecting **File > Save** in the main menu of the tool. After saving, close the tool by selecting **File > Exit**.

5.4.6 Advanced Mode

To display the advanced settings tabs and fields, select **File** > **Advanced Mode** in the Aspect Workforce Data Services configuration utility. When **Advanced Mode** is enabled, several advanced fields become visible. These settings typically do not need to be changed and should be changed with caution, since changing them may result in undesired behavior.

5.4.6.1 General Tab

The following additional fields become visible on the **General** tab when **Advanced Mode** is enabled:

1. CORS Allowed Origins

If the WFM data services should accept AJAX requests for data from a web page hosted on a different domain, the WEM application and the domains that are allowed to make these requests can be specified in this field in a comma-separated list. For example, if a web page hosted on a web page with the URL http://test1.customer.com/wfoUtility.html should be able to invoke the WFM data services hosted on another domain, then http://test1.customer.com can be specified in this field to allow the WFM data services to accept these requests. Otherwise, the browser will not allow such requests.

2. Anti-Forgery Settings

These settings allow the WFM data services anti request forgery settings to be configured. By default, the WFM data services do not allow requests to be made without a caller possessing anti-forgery tokens issued by the WEM application.

- **Enabled (Checkbox)**

  This setting disables the anti-forgery feature. This setting should remain enabled.

- **Anti-Forgery Claim Type**

  If a non-default SAML attribute was specified Alternative SAML Name Claim Type Schema Mapping on page 4-32, then that value should be specified here as well.

- **Exempt endpoints**

  Specify a pipe (|) separated list of the WFM data services URLs to exempt from the antiforgery feature (when enabled). This list should never be changed.

5.4.6.2 Authentication Tab

The Additional settings become visible on the Authentication tab. For more information, see Authentication Tab on page 4-28.

5.5 Configuring Aspect Workforce Engagement Management for Real-Time Adherence

If you plan to use the Real-Time Adherence (RTA) feature in Workforce Engagement Management you will need to:

1. Install RabbitMQ. See Chapter 20 RabbitMQ in the *Aspect Workforce Installation Guide* for instructions. The following sections must be followed:
   a. 20.1 Installing RabbitMQ
   b. 20.2 Creating a RabbitMQ Administrator Account
      Aspect recommends setting up a dedicated RTAWebUser administrative account for this purpose.
   c. (Optional but recommended) 20.3 Disabling the RabbitMQ Guest account
   d. 20.4 Configuring RabbitMQ for RTAWeb
   e. (Optional but recommended) 20.5 Post-Installation Recommendations for RabbitMQ
2. Configure the RTAListen service to receive alarms from your designated ACD. See section 2.3 Creating or Editing a Server Instance in the *Aspect Workforce Perform Installation Guide*.
3. Configure the RTA Alarm Calculator service. See section 6.5 Configuring an RTA Alarm Calculator in the *Aspect Workforce Perform Installation Guide*.
   a. It is recommended an RTA security profile be assigned to the RTA Alarm Calculator account to limit unnecessary messages causing alarm latency. See Using Security Profiles in Chapter 1 of the *Aspect Workforce Perform System Administrators Guide*.
4. Start\restart the following services:
   a. RTAListen
   b. RTA Alarm Calculator

Users should now be able to login to Workforce Engagement Management to begin setting up their RTA workspaces. See *Workforce Engagement Management documentation* for *Administrators, Supervisors* and *Agents*.

6. Configure Aspect Quality

- Either Windows Server 2022 or Windows Server 2025 is required for both the Aspect Workforce Engagement Management Web server and the Aspect Quality Web Services Server.
- Verify that the Aspect Quality Server is installed and configured (for more information, see the *Aspect Quality Server Installation Guide*).
- Complete an installation checklist, which should contain the following information.
- The machine name for the Aspect Quality Database server.
- The Aspect Quality Current Database name.
- If SQL Server is configured for SQL Authentication, determine the SQL User ID and Password to access the Aspect Quality database.
- The installation account; Aspect recommends that you use a Domain User who is also a Local Administrator.
- The Aspect Quality Web Services configuration file is Web.config, and it resides in the Aspect Quality installation directory in the Web.config directory. You can find the directory on the server where you installed the Aspect Quality Web Service.

  C:\Program Files (x86)\Alvaria Software\AQM\Quality.WebServices

  Note: Aspect strongly recommends that you backup the configuration file to manually reapply the custom settings after installing Aspect Quality.
- Verify operating system requirements (for more information, see the *Aspect Quality Hardware and Software Guide*).

Note: If you want to access the Aspect Quality area of Workforce Engagement Management, using Internet Explorer on a Windows Server operating system, you must have the Windows Desktop Experience feature installed on the server. To install and configure Windows Desktop Experience, see the *Aspect Quality Server Installation Guide.*

6.1 Install Aspect Quality

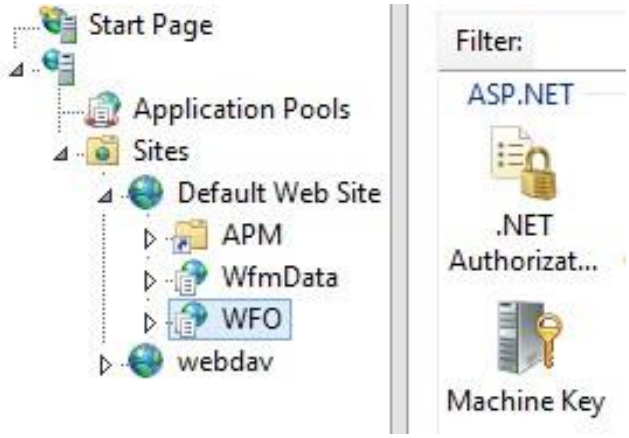
See the *Aspect Quality Server Installation Guide* to install Aspect Quality before configuring it with Aspect Workforce Engagement Management.

Warning: Be aware that a Repair installation reapplies the default web.config file and overwrites any previous edits that you made.

6.2 Set Machine Key for CSRF Anti-Forgery Token

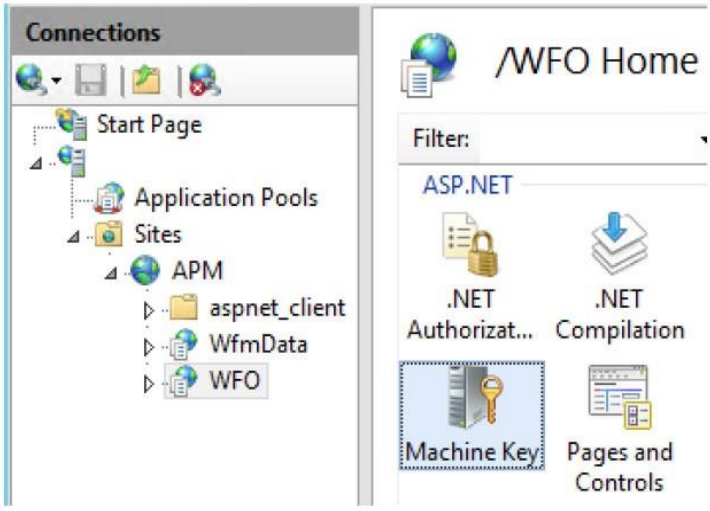
Verify that you have set the machine key for CSRF anti-forgery token.

1. Based on the procedure that you completed in Set Machine Key for CSRF Anti-Forgery Token, log onto the Workforce Engagement Management server as an Administrator.
2. Open **IIS, Start > Administrative Tools > Internet Information Services (IIS) Manager**.
3. On the left-hand pane, navigate to the Workforce Engagement Management Application. Typically, under **Server > Sites > Default Web Site > WFO.**
4. In the middle pane, double click **Machine Key**.



The Machine Key pane opens.

5. Copy the **Validation Key** and **Decryption Key**.
6. Complete the following steps for all Quality application servers.
   a. Log onto the appropriate Workforce Engagement Management or application server as an Administrator.
   b. Open IIS, **Start > Administrative Tools > Internet Information Services (IIS) Manager**
   c. On the left-hand pane, navigate to Quality (Quality Web Service): **Server > Sites > Default Web Site > QualityWebService**.
   d. In the middle pane, double click **Machine Key**.



e. Set the following properties:

i. - Validation method: HMACSHA256 ii. - Encryption method: AES iii. - Validation Key - Automatically generate at runtime: Deselect the checkbox iv. - Validation Key - Generate a unique key for each application: Deselect the checkbox

v. - Decryption Key - Automatically generate at runtime: Deselect the checkbox

vi.- Decryption Key - Generate a unique key for each application: Deselect the checkbox

f. Paste the **Validation Key** and **Decryption Key** from the Workforce Engagement Management application that you copied in step 5. ***These values must match across all Workforce Engagement Management and product application servers for CSRF protection to work.***

g. In the right-hand pane, click **Apply**, and exit IIS Manager.

6.3 Configure Quality Web Services

Once you have run the Server InstallShield Wizard (to install Quality Web Services, see *Aspect Quality Server Installation Guide*, Chapter 4: Server Setup), you must configure the Quality Web Services.

For more information about the Quality Web Service settings, see Customize Settings with Configuration Files on page 6-68.

6.3.1 Configure QWS in the Aspect Quality Configuration Utility

The first step in configuring Quality Web Services is to define the Aspect database and the Web Server role using the Aspect Quality Configuration Utility.

1. Launch the **Aspect Quality Configuration Utility**. The Configuration Utility opens with the General tab active.
2. In the General tab, select the **Web Server** check box.
3. Click **Apply**.
4. Select the **Database** tab.
5. On the Database tab, enter the database details that you provided for the Primary server.

   Note: For more specific information, see section 6.2 Configure Database Access in Chapter 6: Using the Configuration Utility, of the *Aspect Quality Server Installation Guide.*

6. Test the database connectivity by clicking **Test Database Connection**. If the connection was successful, the Success message opens.

   Note: Ensure that you test the database connection on each server you configure.

Note: If unsuccessful, check with the Database Administrator to verify the Authentication type, user name and password. Also, troubleshoot the data connection.

7. Click **OK**.
8. On the Database tab, click **Apply**.
9. Select the **Web Server** tab.
10. On the Web Server tab, enter the Impersonation credentials that you provided for the Primary server.

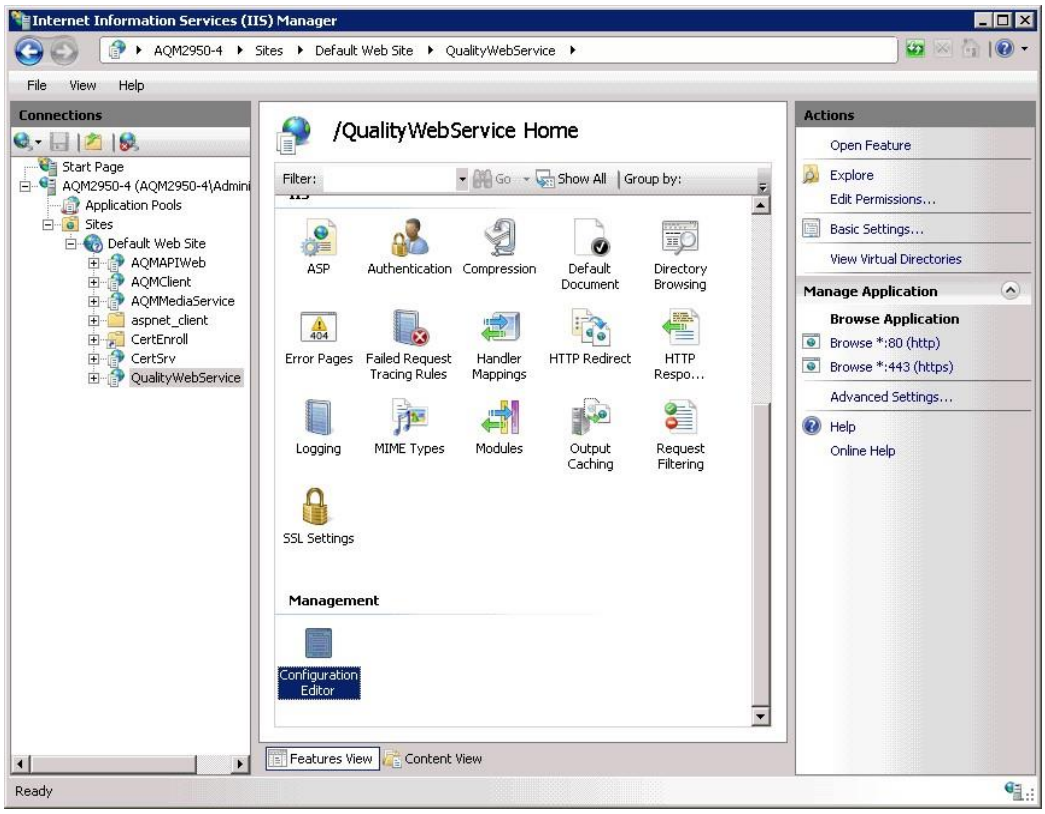
    Note: For more specific information, see section 6.3 Specify Web Server Credentials in Chapter 6: Using the Configuration Utility of the *Aspect Quality Server Installation Guide*.

11. On the Web Server tab, click **Apply**.

6.3.2 Configure QWS in IIS Manager

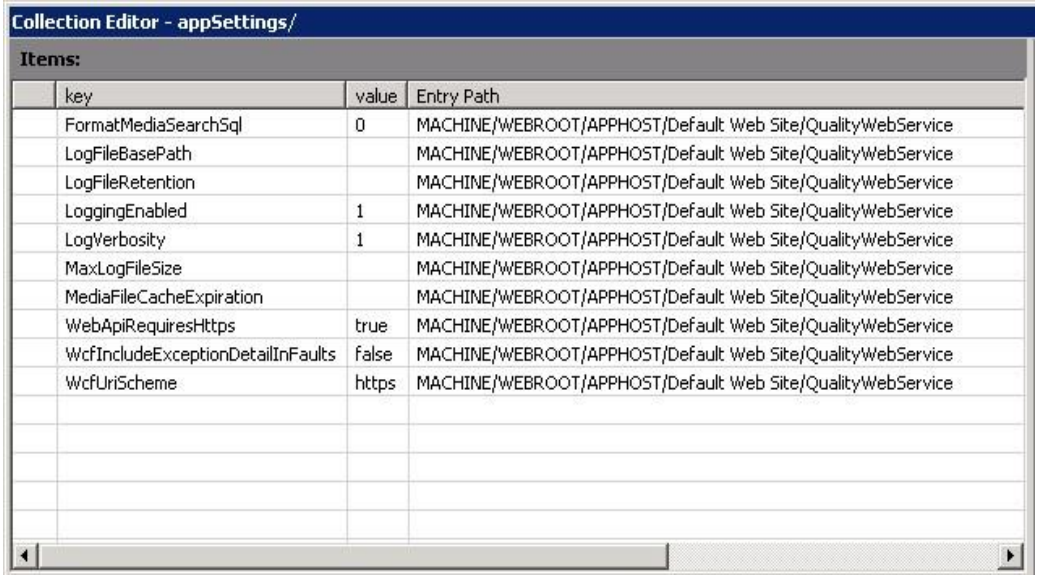
Perform the following steps to configure Quality Web Services for Aspect Workforce Engagement Management-Aspect Quality.

1. Log in to the Quality Web Services server.
2. Launch the **IIS Manager**.
3. In the left pane, expand the **Sites** directory.
4. Select **QualityWebService**.
5. In the right pane, double-click **Configuration Editor**.



The Configuration Editor pane opens.

6. In the Actions pane, click **Edit Items**. The Collection Editor - app settings window opens.



7. Modify the following settings as needed.

Key	Modify to...

LogFileBasePath	the directory location where the log files are created. Leaving this empty causes the log files to be created in a default location: C:\ProgramData\Alvaria Software\Quality Management\Log\QualityWebService
LogFileRetention	the number of days that the log file is retained before being recycled. A value of zero indicates permanent retention.
LoggingEnabled	set the value to 1 to turn on logging; otherwise, set to false (0).
LogVerbosity	the verbosity level: 0 = low, 1 = normal, 2 = high, 3 = extreme.
MaxLogFileSize	the maximum size in byes of each log file before it rolls over to a new log file.

8. When finished modifying the settings, close the Collection Editor - appSettings window.
9. Verify that the temporary storage for media files exists and is accessible in the following location:

   C:\ProgramData\Alvaria Software\Quality Management\VoiceRec\Temp

10. Configure Transport Type.

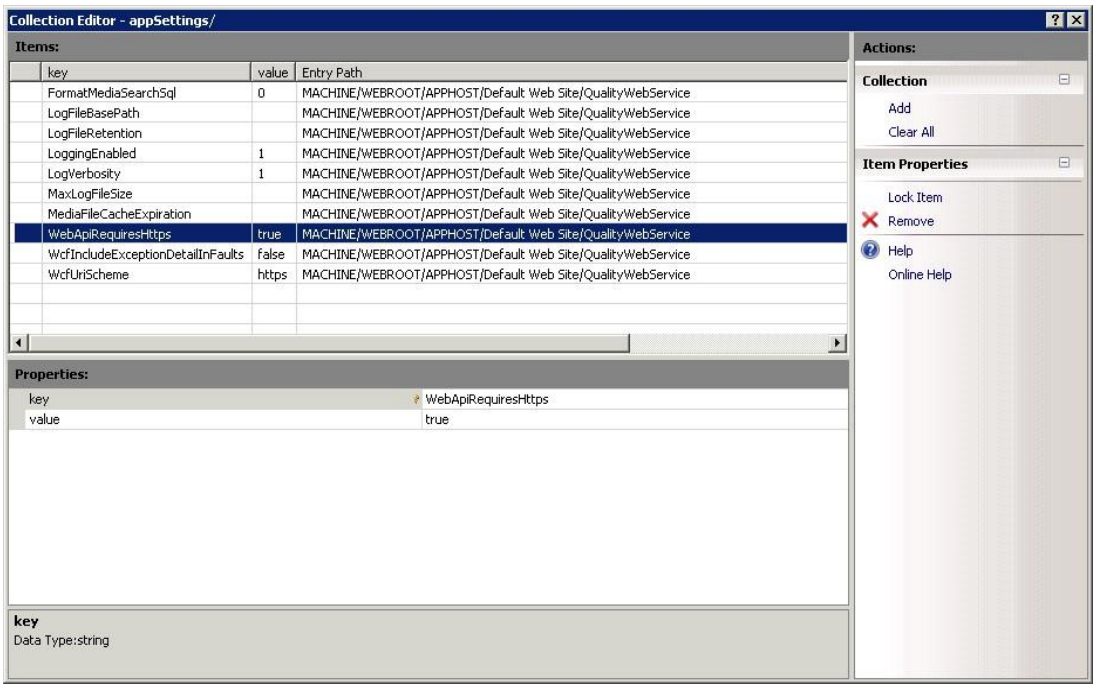
6.3.3 Configure Transport Type

Configure the transport type - either http or https - for the communication between the Web client and the Quality Web Services.

Note: Aspect strongly recommends that you use https for all productions systems for Quality Web Services. If you do not enable https, all communication between the Aspect Workforce Engagement Management browser and the Quality Web Services is unencrypted. This includes any information stored in Aspect Quality, including media (audio, video, and audio/video).

Perform the following steps for either transport type that you need.

1. If you are not already logged in, log in to the Quality Web Services server (usually the Web server).
2. Launch the **IIS Manager**.
3. In the left pane, expand the **Sites** directory.
4. Click **QualityWebService**. The QualityWebService Home pane opens.
5. Double-click **Configuration Editor**. The Configuration Editor pane opens.
6. From the Items list, select **WebApiRequiresHttps**.



7. If you want to use https, in the value field, type **true**.

   OR

   If you want to use http, in the value field, type **false**.

   Note: Aspect strongly recommends that you use https for all productions systems for Quality Web Services. If you do not enable https, all communication between the Aspect Workforce Engagement Management browser and the Quality Web Services is unencrypted. This includes any information stored in Aspect Quality, including media (audio, video, and audio/video).

8. When finished modifying the settings, close the Collection Editor - appSettings window.**Note:** If you use https as the transport type, see Deploy the SSL Certificate for https.

   If you use http as the transport type, you do not need to create and deploy an SSL certificate; skip to Configure Aspect Workforce Engagement Management to Access Aspect Quality.

6.3.4 Deploy the SSL Certificate for https

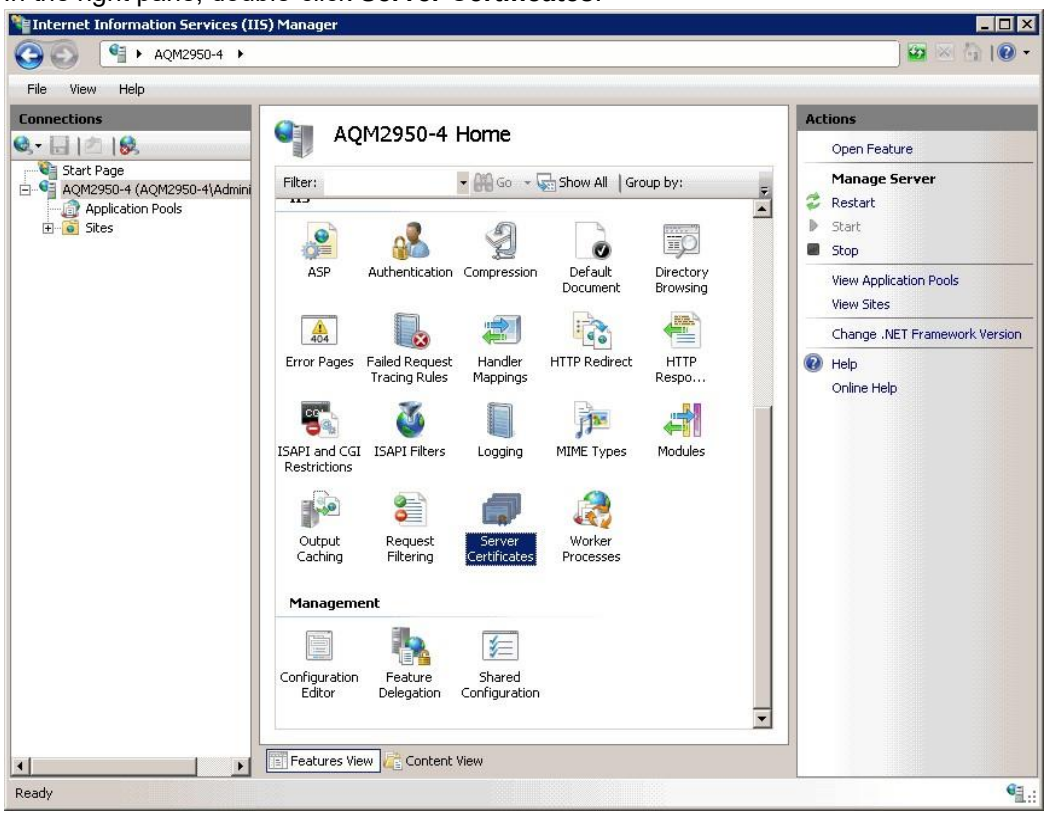
If you use https as the transport type, you must deploy the SSL certificate on the Quality Web Services server and on the Aspect Workforce Engagement Management server.

Note: Aspect recommends using a certificate generated by an internal trusted certificate authority or a commercial trusted certificate authority.

If you already have an SSL certificate created, go to Deploy the SSL Certificate for https.

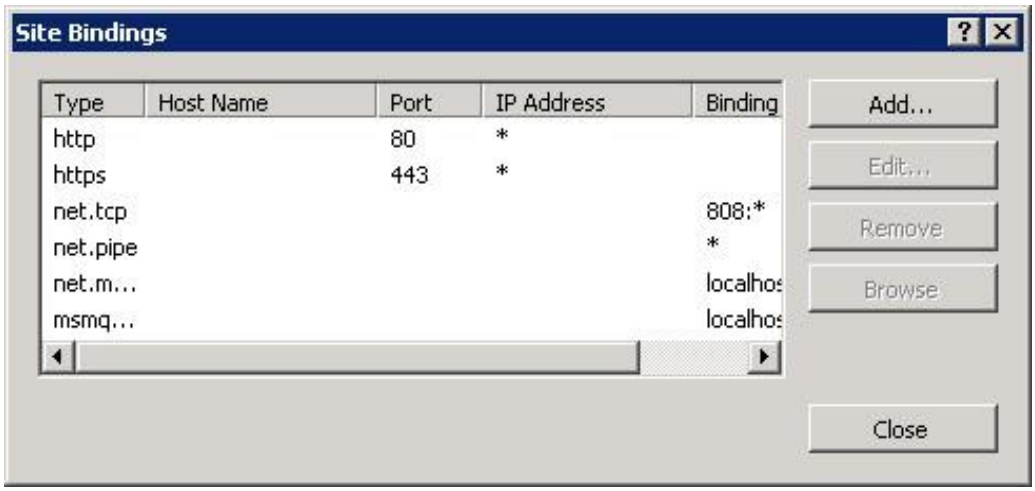
6.3.4.1 Deploy the SSL Certificate for https

1. If you are not already logged in, log in to the Quality Web Services server (usually the Web server).
2. Launch the **IIS Manager**.
3. In the left pane, select the Web server name. The Web server Home pane opens in the right pane.
4. In the right pane, double-click **Server Certificates**.

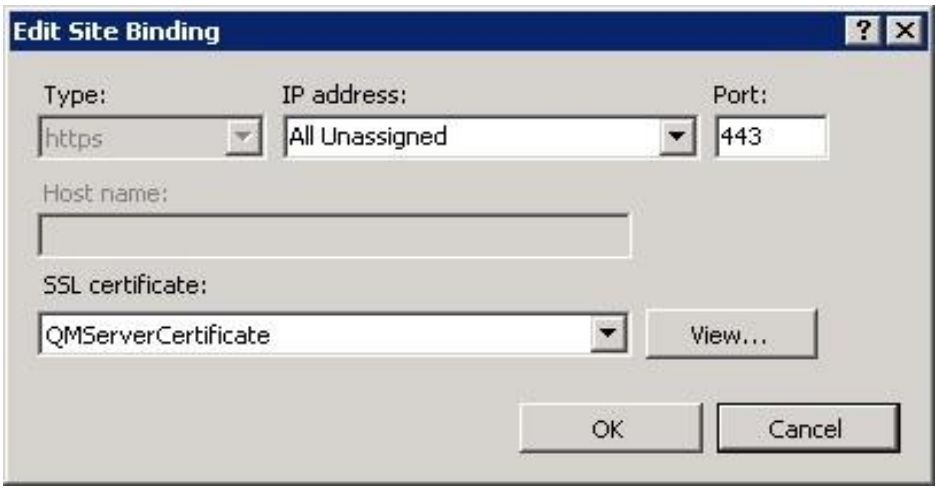


The Server Certificates pane opens in the right pane.

5. In the left pane, expand the **Sites** directory.
6. Select the **Default Web Site** directory. The Default Web Site Home pane opens.
7. In the Actions pane, under Edit Site, select **Bindings**. The Site Binding window opens.



8. From the Site Bindings list, in the Type column, select **https**.
9. Click **Edit**. The Edit Site Bindings window opens.
10. From the SSL certificate drop-down list box, select the SSL certificate name that you created.



11. Click **OK**. The Edit Site Binding window closes and the Site Bindings window is active.
12. Click **Close**. The Site Bindings window closes, and the Default Web Site Home pane is active.
13. See the following section to enable your browser to communicate using SSL.
    - Install the Certificate for Microsoft Edge or Google Chrome Browsers

6.3.4.2 Install the Certificate for Microsoft Edge or Google Chrome Browsers

If you are using self-signed certificates, each browser that you use with Aspect Workforce Engagement Management must have a certificate installed before you can use Aspect Workforce Engagement Management. If you are using trusted internal or external certificates,

you do not need to have a certificate installed before you can use Aspect Workforce Engagement Management.

Note: The same requirement exists for Mozilla Firefox browser users. To install the certificate for the browser machine for Mozilla Firefox, skip to Install the Certificate for Mozilla Firefox Browsers on page 6-58.

1. On the Web Client server, launch **Microsoft Edge**.
2. Browse to the **Workforce Engagement Management** homepage. Because the server certificate that you deployed in the previous section (Deploy the SSL Certificate for https) is not a trusted site, the following window opens.

3. **View Certificate**. The Certificate Import Wizard window opens.
4. Click **Install Certificate**. The Welcome to the Certificate Import Wizard window opens.

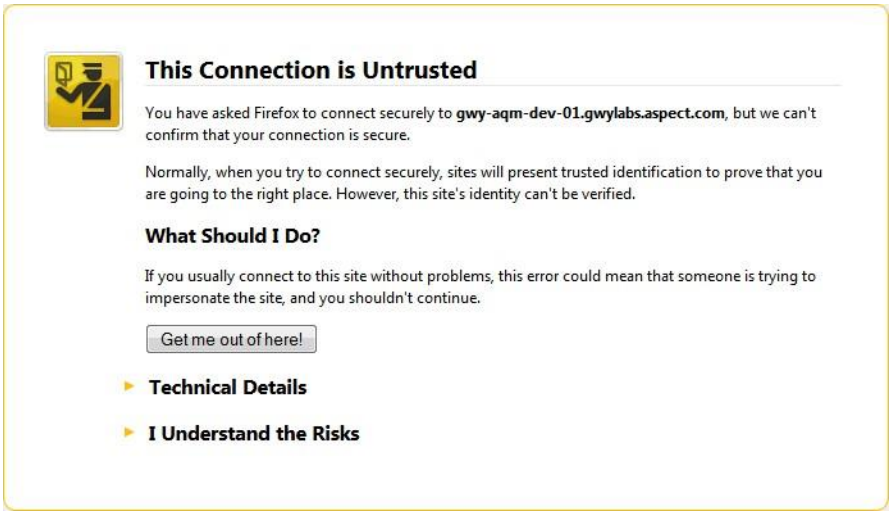
5. Click **Next**.
6. Click **Place all certificates in the following store**.
7. Click **Browse** (the Ellipsis button).
8. Verify that the **Show physical stores** check box is selected.
9. In the Trusted Root Certification Authority section, click **Local Computer**.

10. Click **OK**.
11. Click **Next**.
12. Click **Finish**.

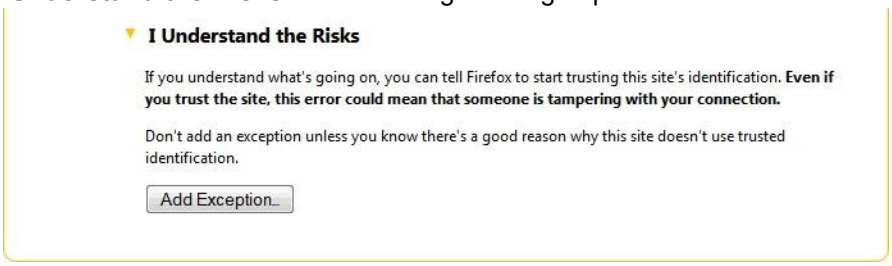
6.3.4.3 Install the Certificate for Mozilla Firefox Browsers

The server certificate that you created (for example, in Deploy the SSL Certificate for https on page 6-53) is now imported in the Trusted Root Certification Store on the Web client and requests to access Quality Web Services using Microsoft Edge and Google Chrome are valid. However, if you use Mozilla Firefox, you must perform the following steps to allow access to Quality Web Services.

1. Launch **Mozilla Firefox**. The Firefox Start Page window opens.
2. Browse to the Quality Web Services endpoint as you configured within IIS Manager for the Quality Web Services web application. In this example, the endpoint is https://gwy-aqm-dev-01.gwylabs.Alvaria.com/qualitywebService/api The This Connection is Untrusted window opens.



3. Click **I Understand the Risks**. The following message opens at the bottom of the window.



4. Click **Add Exception**.

Warning: Ensure that the host portion of the URI matches the host name of the certificate that you issued (for example, in Deploy the SSL Certificate for https on page 6-53). Notice that the host name is fully qualified.

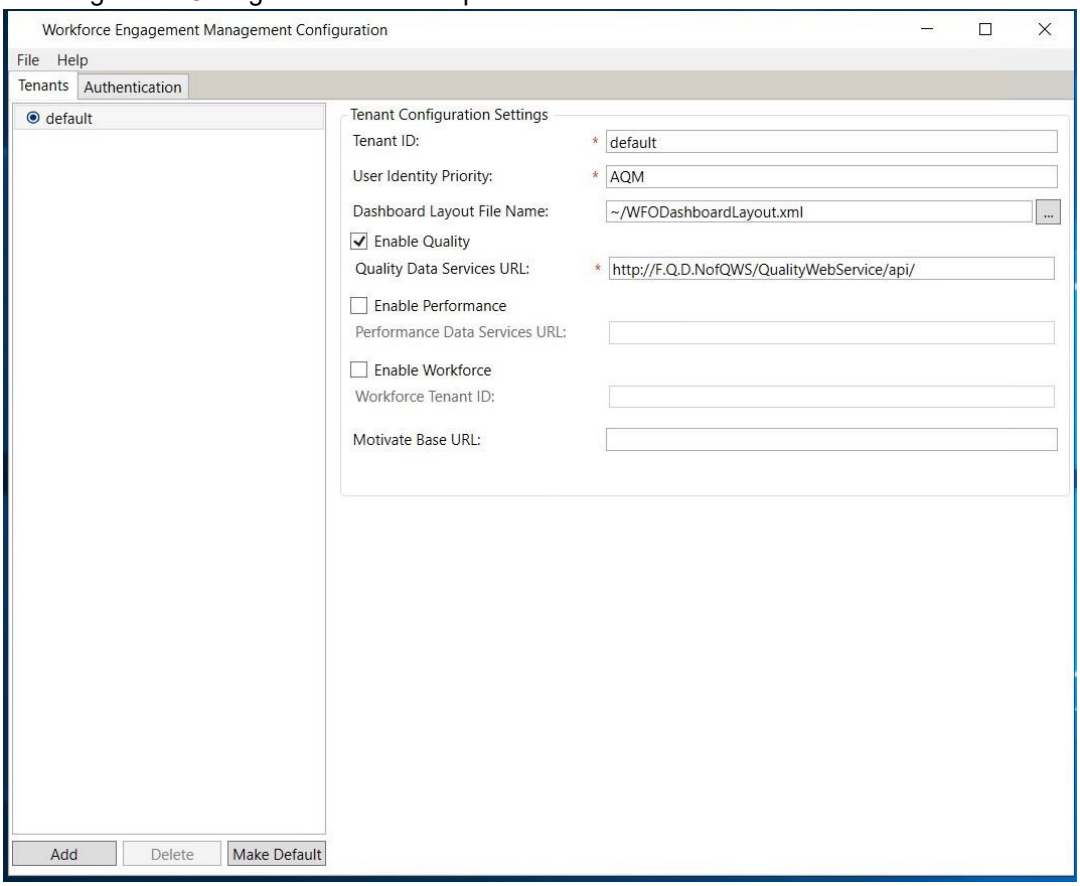
The Add Security Exception window opens.

5. Verify that the **Permanently store this exception** check box is selected.
6. Click **Confirm Security Exception**. The browser launches the now-trusted site.

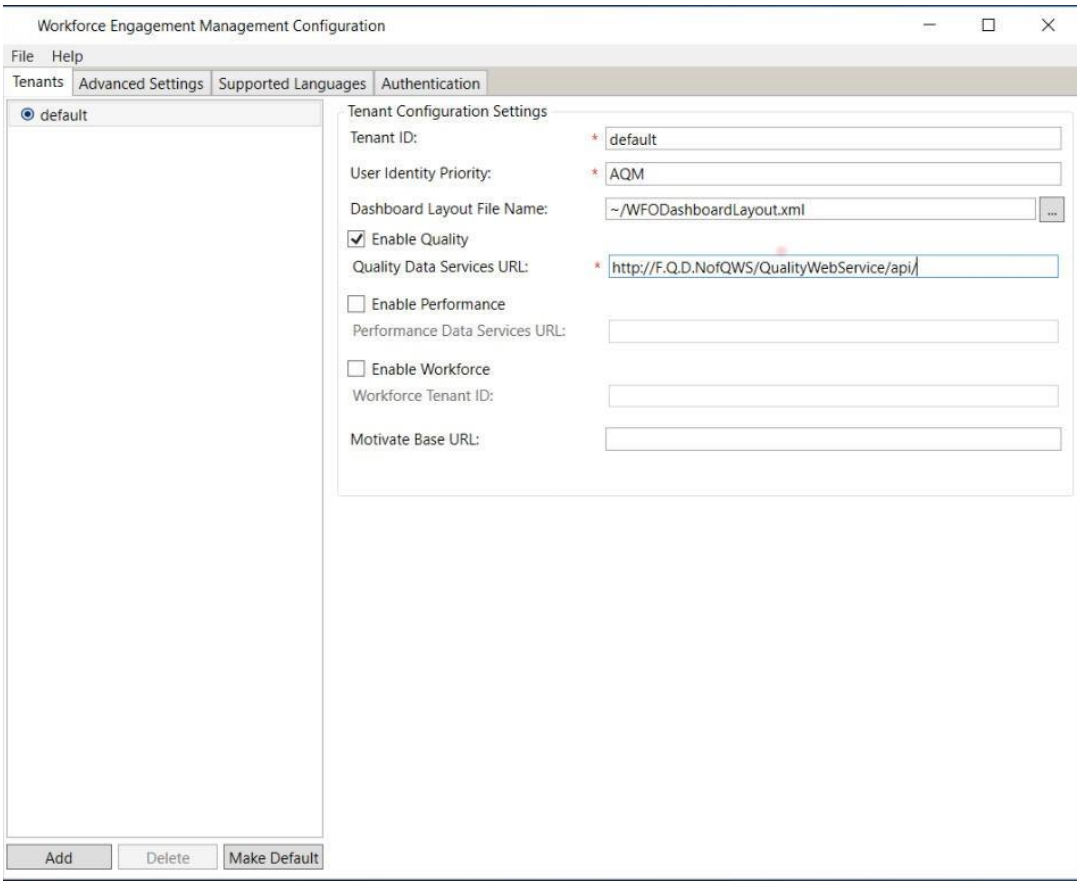
6.4 Configure Aspect Workforce Engagement Management to Access Aspect Quality

The following configuration steps are required so that Aspect Workforce Engagement Management can access Aspect Quality.

1. Log in to the Workforce Management Web application server.
2. From the Aspect program group, click the Workforce Engagement Management menu.
3. Click **Workforce Engagement Management Configuration**. The Workforce Engagement Management Configuration window opens with the Tenants tab active.



4. Select the **Enable Quality Management check box**.
5. In the Quality Web Services URL text box, type the URL to the Aspect Quality Web Services endpoint. In this example, the endpoint is: https://F.Q.D.NofQWS/QualityWebService/api/



6. Select **File>Save**.

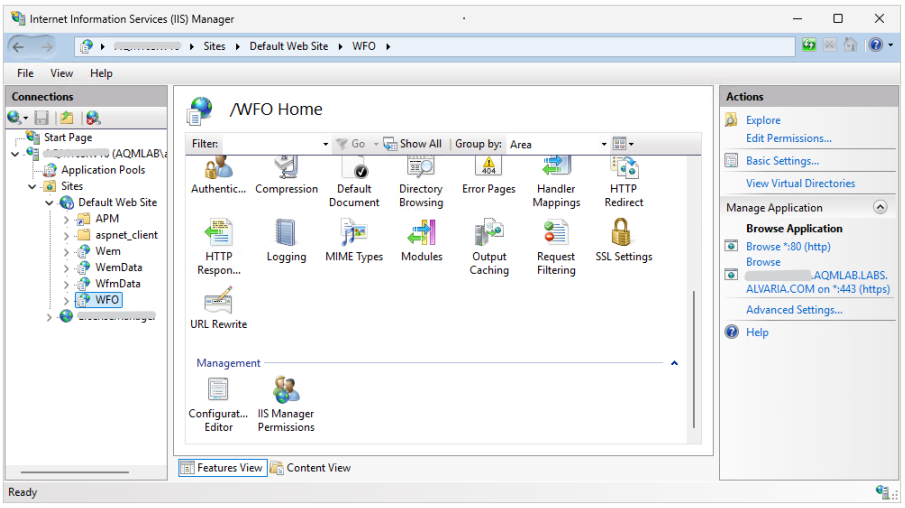
Warning: Ensure that the host portion of the URL matches the host name of the certificate that you issued in Deploy the SSL Certificate for https. Notice that the host name is fully qualified.

6.4.1 Configuring WFO in IIS Manager

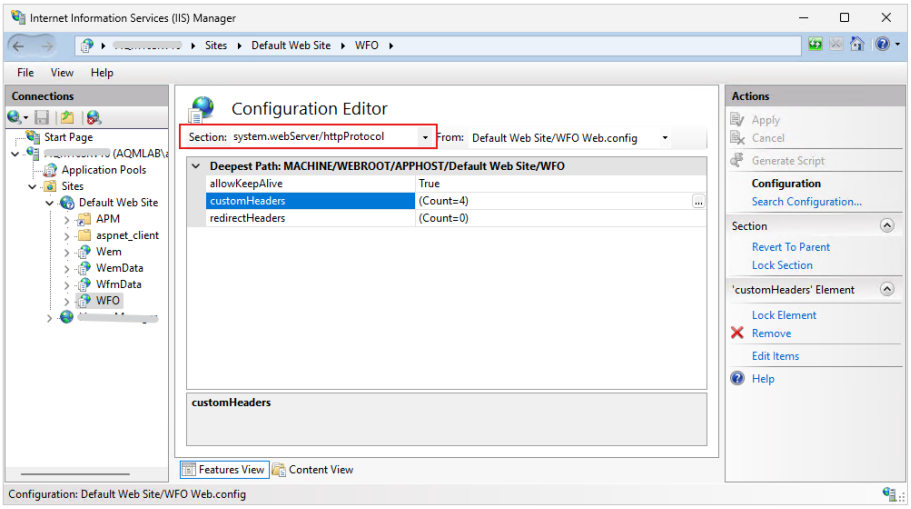
The Content-Security-Policy (CSP) header tells the browser which origins are allowed for things like scripts, XHR/fetch/websockets (connect-src), styles, etc. Typical directive involved for API calls is connect-src. If the CSP lists only 'self' and the QualityWebService (backend) is on a different host, the browser will block fetch/XHR/WS calls to that host until it is allowed by the CSP.

Perform the following steps to configure Content-Security-Policy in Aspect Workforce Engagement Management

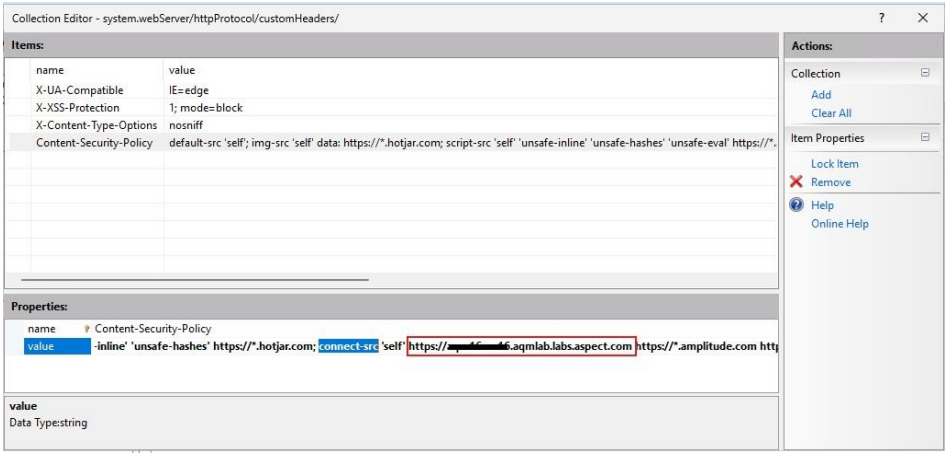
1. Log in to the Aspect Workforce Engagement server.
2. Launch the IIS Manager.
3. In the left pane, expand the Sites directory.
4. Select WFO.
5. In the right pane, double-click Configuration Editor.



6. The Configuration Editor pane opens.



7. In the Section dropdown, select system.webServer/httpProtocol.
8. Select the CustomHeaders in the grid.
9. In the Actions pane, click Edit Items. The Collection Editor window opens.



10. In the Items section, select Content-Security-Policy.

11. In the Properties section, corresponding to the value, add the Fully Qualified Domain Name url of the Quality Web Service server next to the connect-src.

12. When finished modifying the settings, close the Collection Editor window.

6.5 Licensing

Aspect Quality has a licensing structure.

Note: To download the license file, see Upload the License File on page 6-65.

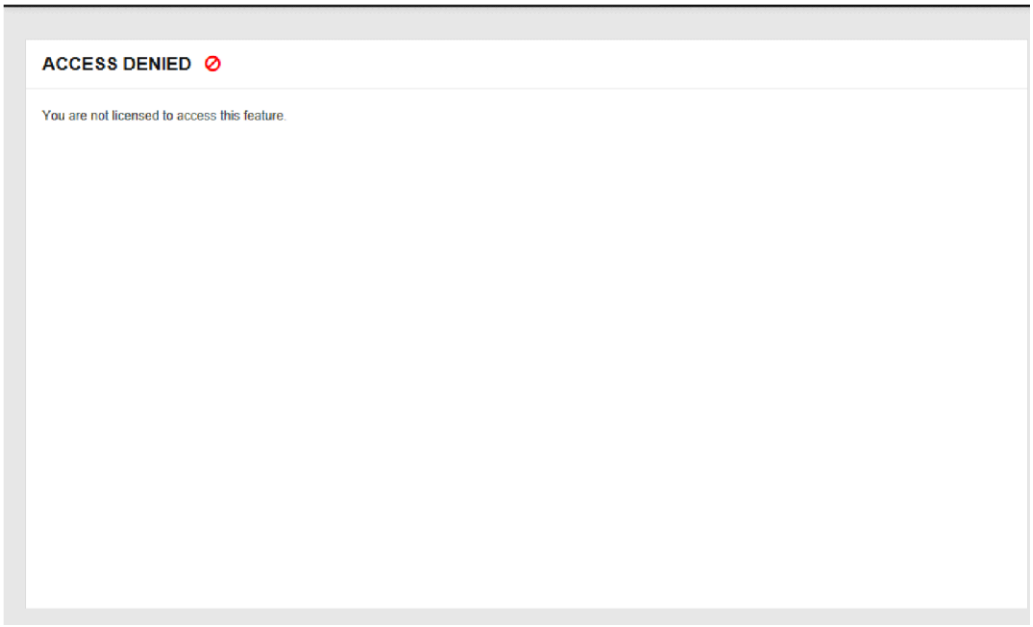
The following table outlines the features available within Aspect Quality that can be licensed on a per-user basis, and the type of access that the license provides to a user.

License Feature	Description	Access
General Access	The license required to access any part of the Aspect Quality.system	• Access Aspect Quality using the Workforce Engagement Management UI • Access Aspect Quality using the Aspect Quality UI • Search for interactions • View interaction details • Listen to/watch recorded interactions
Voice Recording	The license required for Aspect Quality to record users' voice conversations	• Voice Recording licenses do not provide users any additional access to the Workforce Engagement Management system
Screen Recording	The license required for Aspect Quality to record users' voice PC screen content when logged into the Agent Desktop Client	• Screen Recording licenses do not provide users any additional access to the Workforce Engagement Management system
Encrypt Recording	The license required for Aspect Quality to encrypt voice and screen recording files	• Encryption licenses do not provide users any additional access to the Workforce Engagement Management system
Export Recording	The license required for the Aspect Quality system to export user audio/ screen recordings and associated metadata as part of a mass export operation using the Aspect Quality Exporter service, or using the Aspect Quality UI mass export feature	• Enables Aspect Quality UI export feature for administrators when at least one user in the system is licensed for export
License Feature	**Description**	**Access**

Evaluation	The license required for users to utilize and access Aspect Quality evaluation functionality and data	• Create/edit evaluation templates • Perform interaction evaluations • Search by and display evaluation attributes when searching for interactions • Perform evaluation calibration • Create, edit, run, and view reports • Create tasks for interactions or activities that are not monitored by the Workforce Engagement Management system • Share evaluation scores with Aspect Workforce • Configure mentor permissions for interaction evaluation creation, edit, and review • With an Aspect Performance system configured, and a Coaching license on that system, you can assign coaching
Speech Analytics	The license required for users to utilize and access the Speech Analytics feature.	• Search by and display interactions based on matching speech Category.
Email	The license required for users to utilize and access Email interactions.	• Search by and display Email interactions and related criteria features.
Chat	The license required for users to utilize and access Chat interactions	• Search by and display Chat interactions and related criteria features.
SMS	The license required for users to utilize and access SMS (text) interactions.	• Search by and display SMS interactions and related criteria features.

If you are in the Aspect Quality UI, and you attempt to navigate to a component to which you do not have a license, the following message opens.

If you are in the Workforce Engagement Management UI, and you attempt to navigate to a component to which you do not have a license, the following message opens.


ACCESS DENIED
You are not licensed to access this feature.

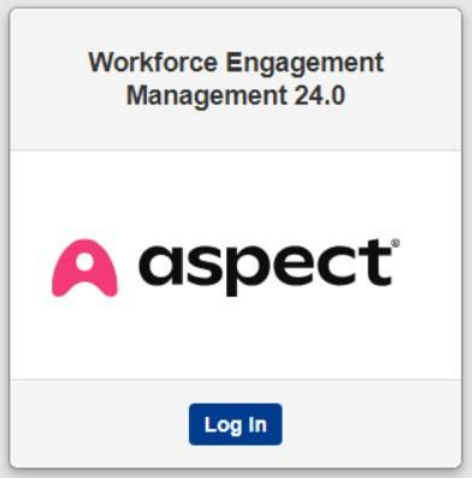
6.5.1 Upload the License File

When you log in to Workforce Engagement Management to use Aspect Quality for the first time, you must upload the license file. The license file manages the total number of users allowed in Aspect Quality by site.

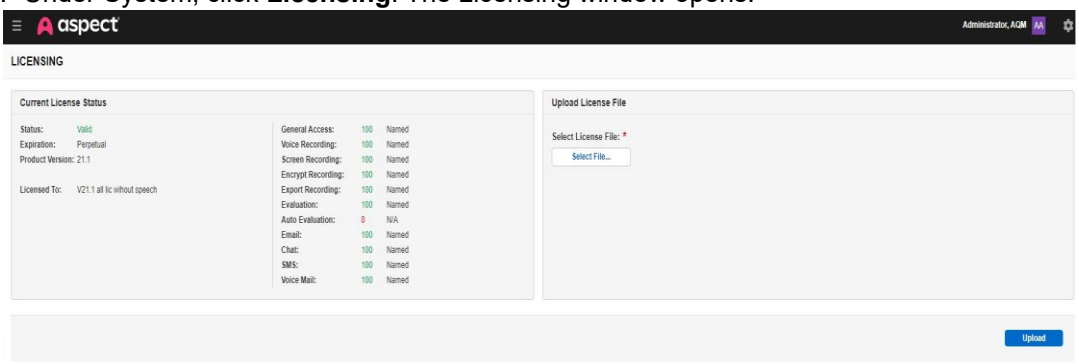
Note: You should receive the license file as part of your Aspect Quality installation package. You can store the .lic file anywhere, as long as you can access it when you perform the following steps.

To upload the license file, perform the following steps.

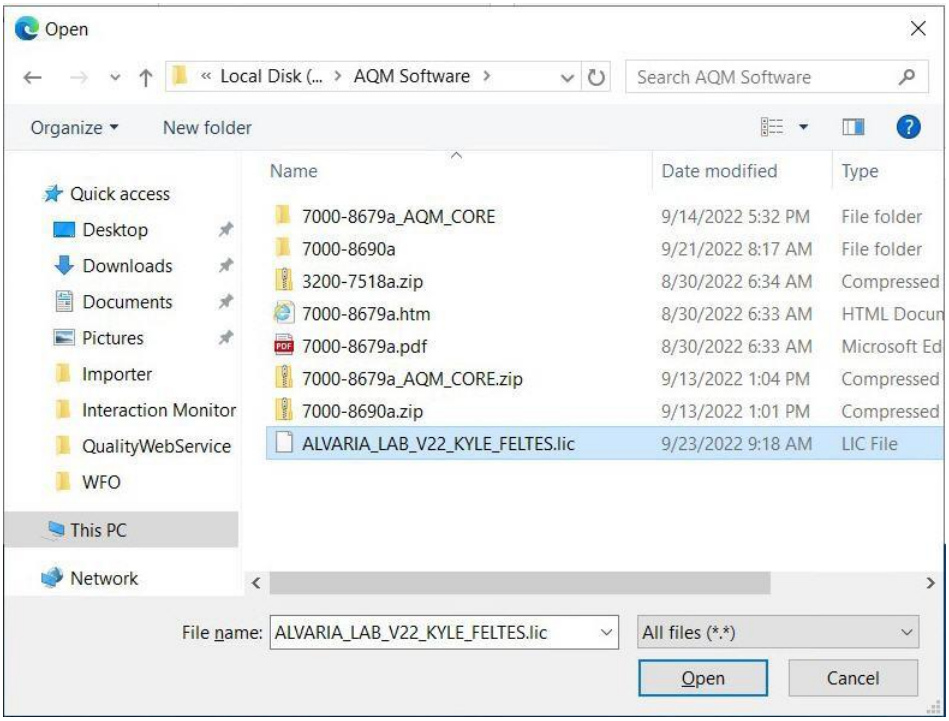
1. Launch Workforce Engagement Management.



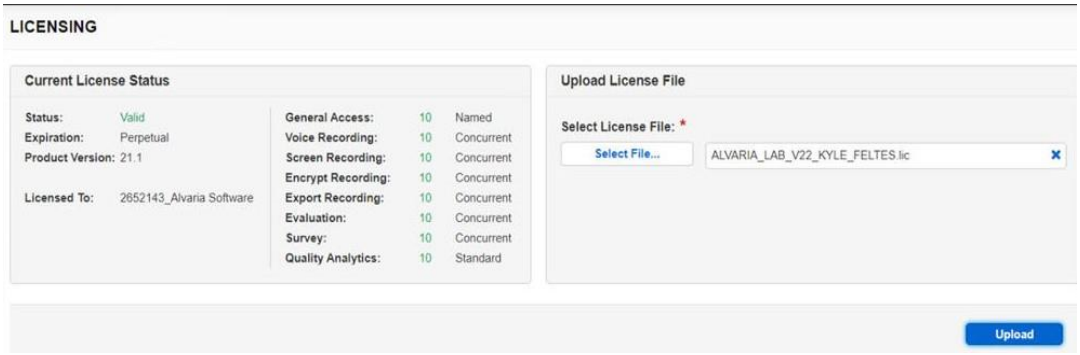
2. Click **Log In**. The Workforce Engagement Management dashboard opens.
3. Log in as the Administrator.
4. Select **Menu > Administration**.
5. Under System, click **Licensing**. The Licensing window opens.



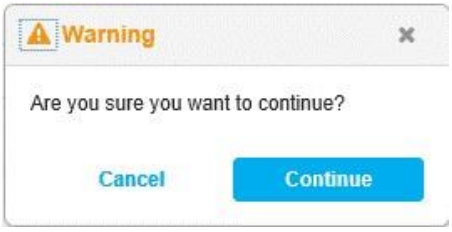
6. In the right pane, click **Browse**.
7. Browse to the location of the license file.



8. Select the license file and click **Open**. The license file name displays in the Select License File text box.



9. Click **Upload**. A Warning message opens to verify that you want to continue.



10. Click **Continue**. The Licensing window populates with the number of licenses that are valid for each feature. In the following example, there are 2000 licenses each for each feature.

Note: After you upload a Voice Recording license, you must restart the Aspect Quality service.

11. Now that you have uploaded the license file, you can use the features for which you are licensed. To use Aspect Quality, close the browsers and re-launch the Workforce Engagement Management web client.

6.6 Configure Speech Analytics

To configure Workforce Engagement Management - Aspect Quality with speech analytics, see the *Aspect Quality Server Installation Guide*, specifically the appendix entitled Configure Speech Analytics.

6.7 Customize Settings with Configuration Files

The Aspect Quality Web Services configuration file is **Web.config**, and it resides in the Aspect Quality installation directory in the Web.config directory. You can find the directory on the server where you installed the Aspect Quality Web Service.

C:\Program Files (x86)\Alvaria Software\AQM\Quality.WebServices

This section describes optional configuration changes you may need to make to the Aspect Quality system. The changes are global (the changes affect the entire Aspect Quality system) and you should only make the changes if you need them for functionality. You make the changes in this section by using process-specific configuration files.

Note: If you previously backed up the Aspect Quality Web Services configuration file, then you must manually reapply any custom settings. *Do **not** replace or overwrite the entire file, because newer Aspect Quality functionality may become inoperable.*

6.7.1 AuthorizeClaimType

Description: Specifies claim/assertion type used to perform authorization when using

claimsbased authentication. Default Value: Name Valid Values: Email, Name

Example:

```
<add key="AuthorizeClaimType" value="Email" />
```

6.7.2 DashboardFileName

Description Specifies the location of the Dashboard Layout file.

Default Value: ~/AQMDashboard.xml

Valid Values: Empty or any valid file path

Example:

```
<add key="DashboardFileName" value="~/AQMDashboard.xml" />
```

6.7.3 FormatMediaSearchSql

Description: Specifies whether media search SQL queries should be formatted for better readability.

Default Value: 0

Valid values: 0 - Do not format queries, 1 - Format queries

6.7.4 LogFileBasePath

Description: Specifies the log file base folder location. When empty, the log file is located in ProgramData (Alvaria Software\Quality Management\Log).

Default Value: Empty

Valid values: Empty or any valid file path

Example:

```
<add key="DLogFileBasePath" value="" />
```

6.7.5 LogFileRetention

Description: Number of days the log file is retained before being recycled. A value of zero indicates permanent retention.

Default Value: Empty

Valid values: Empty, positive integer values

Example:

```
<add key="LogFileRetention" value="" />
```

6.7.6 LoggingEnabled

Description: Specifies whether logging is enabled.

Default Value: 1

Valid Values: 0 - Disabled, 1 - Enabled

6.7.7 LogVerbosity

Description: Specifies the level of detail for logging.

Default Value: 1

Valid Values: 0 - Low, 1 - Normal, 2 - High, 3 - Extreme

6.7.8 MaxLogFileSize

Description: Specifies the maximum size, in bytes, for each log file before it rolls over to a new one.

Default Value: 200000000

Valid Values: Empty, positive integer values

6.7.9 MaxResolution

Description: Specifies the maximum output resolution for H.264 video streams.

Default Value: Empty

Valid Values: Empty, positive integer values

Example:

```
<add key=”H264MaxResolution” value=”2048,2048” />
```

6.7.10 MediaFileCacheExpiration

Description: Specifies the duration of inactivity in minutes after which a media file is removed from the cache.

Default Value: 15

Valid Values: Empty, positive integer values

6.7.11 MediaFileLoadTimeOut

Description: Defines a time out value in minutes when loading media files to be streamed to the client.

Default Value: 5 (minutes)

Valid Values: Values less than 5 minutes are ignored

Example

```
<add key="MediaFileLoadTimeOut" value="5" />
```

6.7.12 RestrictedFileUploadExtensions

Description: Allows the administrator to restrict some of the file types. The extensions mentioned in this option are not allowed to add as an attachment by any user.

Example:

```
<add key="RestrictedFileUploadExtensions"
value="exe,bat,js,vbs,ps1" />
```

Values: By default the exe, bat, js, vbs, and ps1 are file types that are restricted from being added as an attachment.

6.7.13 TimeZone

Description: Specifies the time zone buckets to use when returning summarized analytics data.

Default Value: UTC

Valid Values:

Value	Description
Dateline Standard Time	(UTC-12:00) International Date Line West
UTC-11	(UTC-11:00) Coordinated Universal Time-11
Hawaiian Standard Time	(UTC-10:00) Hawaii
Alaskan Standard Time	(UTC-09:00) Alaska
Pacific Standard Time (Mexico)	(UTC-08:00) Baja California
Pacific Standard Time	(UTC-08:00) Pacific Time (US & Canada)
US Mountain Standard Time	(UTC-07:00) Arizona
Mountain Standard Time (Mexico)	(UTC-07:00) Chihuahua, La Paz, Mazatlan
Mountain Standard Time	(UTC-07:00) Mountain Time (US & Canada)
Central America Standard Time	(UTC-06:00) Central America
Central Standard Time	(UTC-06:00) Central Time (US & Canada)
Central Standard Time (Mexico)	(UTC-06:00) Guadalajara, Mexico City, Monterrey
Canada Central Standard Time	(UTC-06:00) Saskatchewan
SA Pacific Standard Time	(UTC-05:00) Bogota, Lima, Quito
Eastern Standard Time	(UTC-05:00) Eastern Time (US & Canada)
US Eastern Standard Time	(UTC-05:00) Indiana (East)
Venezuela Standard Time	(UTC-04:30) Caracas
Paraguay Standard Time	(UTC-04:00) Asuncion
Atlantic Standard Time	(UTC-04:00) Atlantic Time (Canada)
Central Brazilian Standard Time	(UTC-04:00) Cuiaba

SA Western Standard Time	(UTC-04:00) Georgetown, La Paz, Manaus, San Juan
Pacific SA Standard Time	(UTC-04:00) Santiago
Newfoundland Standard Time	(UTC-03:30) Newfoundland
E. South America Standard Time	(UTC-03:00) Brasilia
Argentina Standard Time	(UTC-03:00) Buenos Aires
SA Eastern Standard Time	(UTC-03:00) Cayenne, Fortaleza
Greenland Standard Time	(UTC-03:00) Greenland

Value	Description
Montevideo Standard Time	(UTC-03:00) Montevideo
Bahia Standard Time	(UTC-03:00) Salvador
UTC-02	(UTC-02:00) Coordinated Universal Time-02
Mid-Atlantic Standard Time	(UTC-02:00) Mid-Atlantic
Azores Standard Time	(UTC-01:00) Azores
Cape Verde Standard Time	(UTC-01:00) Cape Verde Is.
Morocco Standard Time	(UTC) Casablanca
UTC	(UTC) Coordinated Universal Time
GMT Standard Time	(UTC) Dublin, Edinburgh, Lisbon, London
Greenwich Standard Time	(UTC) Monrovia, Reykjavik
W. Europe Standard Time	(UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
Central Europe Standard Time	(UTC+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
Romance Standard Time	(UTC+01:00) Brussels, Copenhagen, Madrid, Paris
Central European Standard Time	(UTC+01:00) Sarajevo, Skopje, Warsaw, Zagreb
W. Central Africa Standard Time	(UTC+01:00) West Central Africa
Namibia Standard Time	(UTC+01:00) Windhoek
GTB Standard Time	(UTC+02:00) Athens, Bucharest
Middle East Standard Time	(UTC+02:00) Beirut

Egypt Standard Time	(UTC+02:00) Cairo
Syria Standard Time	(UTC+02:00) Damascus
South Africa Standard Time	(UTC+02:00) Harare, Pretoria
FLE Standard Time	(UTC+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius
Turkey Standard Time	(UTC+02:00) Istanbul
Israel Standard Time	(UTC+02:00) Jerusalem
E. Europe Standard Time	(UTC+02:00) Nicosia
Jordan Standard Time	(UTC+03:00) Amman
Arabic Standard Time	(UTC+03:00) Baghdad
Kaliningrad Standard Time	(UTC+03:00) Kaliningrad, Minsk
Arab Standard Time	(UTC+03:00) Kuwait, Riyadh
E. Africa Standard Time	(UTC+03:00) Nairobi
Iran Standard Time	(UTC+03:30) Tehran

Value	Description
Arabian Standard Time	(UTC+04:00) Abu Dhabi, Muscat
Azerbaijan Standard Time	(UTC+04:00) Baku
Russian Standard Time	(UTC+04:00) Moscow, St. Petersburg, Volgograd
Mauritius Standard Time	(UTC+04:00) Port Louis
Georgian Standard Time	(UTC+04:00) Tbilisi
Caucasus Standard Time	(UTC+04:00) Yerevan
Afghanistan Standard Time	(UTC+04:30) Kabul
Pakistan Standard Time	(UTC+05:00) Islamabad, Karachi
West Asia Standard Time	(UTC+05:00) Tashkent
India Standard Time	(UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Sri Lanka Standard Time	(UTC+05:30) Sri Jayawardenepura
Nepal Standard Time	(UTC+05:45) Kathmandu
Central Asia Standard Time	(UTC+06:00) Astana
Bangladesh Standard Time	(UTC+06:00) Dhaka

Ekaterinburg Standard Time	(UTC+06:00) Ekaterinburg
Myanmar Standard Time	(UTC+06:30) Yangon (Rangoon)
SE Asia Standard Time	(UTC+07:00) Bangkok, Hanoi, Jakarta
N. Central Asia Standard Time	(UTC+07:00) Novosibirsk
China Standard Time	(UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi
North Asia Standard Time	(UTC+08:00) Krasnoyarsk
Singapore Standard Time	(UTC+08:00) Kuala Lumpur, Singapore
W. Australia Standard Time	(UTC+08:00) Perth
Taipei Standard Time	(UTC+08:00) Taipei
Ulaanbaatar Standard Time	(UTC+08:00) Ulaanbaatar
North Asia East Standard Time	(UTC+09:00) Irkutsk
Tokyo Standard Time	(UTC+09:00) Osaka, Sapporo, Tokyo
Korea Standard Time	(UTC+09:00) Seoul
Cen. Australia Standard Time	(UTC+09:30) Adelaide
AUS Central Standard Time	(UTC+09:30) Darwin
E. Australia Standard Time	(UTC+10:00) Brisbane
AUS Eastern Standard Time	(UTC+10:00) Canberra, Melbourne, Sydney
West Pacific Standard Time	(UTC+10:00) Guam, Port Moresby
Tasmania Standard Time	(UTC+10:00) Hobart
Value	**Description**
Yakutsk Standard Time	(UTC+10:00) Yakutsk
Central Pacific Standard Time	(UTC+11:00) Solomon Is., New Caledonia
Vladivostok Standard Time	(UTC+11:00) Vladivostok
New Zealand Standard Time	(UTC+12:00) Auckland, Wellington
UTC+12	(UTC+12:00) Coordinated Universal Time+12
Fiji Standard Time	(UTC+12:00) Fiji
Magadan Standard Time	(UTC+12:00) Magadan
Kamchatka Standard Time	(UTC+12:00) Petropavlovsk-Kamchatsky - Old
Tonga Standard Time	(UTC+13:00) Nuku 'alofa
Samoa Standard Time	(UTC+13:00) Samoa

6.7.14 WebApiRequiresHttps

Description: Specifies whether HTTPS should be enforced for all Web Application Program Interface (API) requests. Valid Values: true (default), false

Example:

```
<add key="WebApiRequiresHttps" value="false" />
```

6.7.15 WcfUriScheme

To configure the Aspect Quality Web Service to accept Windows Communication Foundation (WCF) calls over http, perform the following steps.

Description: URI scheme to be used when the WCF service is being accessed.

Valid Values: http, https (default)

Example:

```
<add key="WcfUriScheme" value="http" />
```

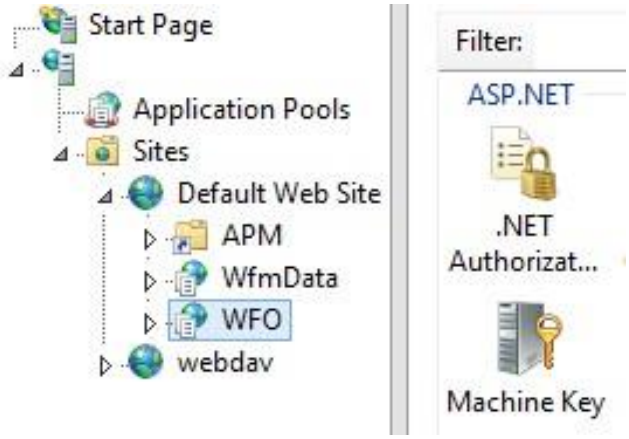
7. Configure Aspect Performance

Before you begin, see the *Aspect Performance Installation Guide* to install Performance and to verify that it is running.

7.1 Set Machine Key for CSRF Anti-Forgery Token

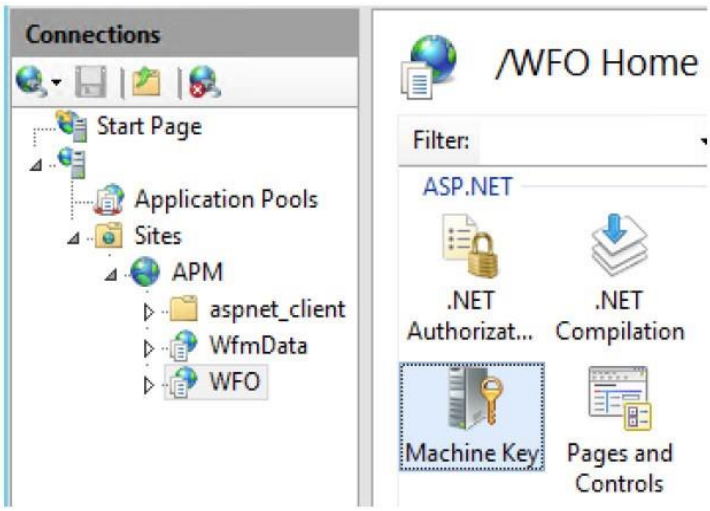
Verify that you have set the machine key for CSRF anti-forgery token.

1. Based on the procedure that you completed in Set Machine Key for CSRF Anti-Forgery Token, log onto the Workforce Engagement Management server as an Administrator.
2. Open **IIS, Start > Administrative Tools > Internet Information Services (IIS) Manager**.
3. On the left-hand pane, navigate to the Workforce Engagement Management Application. Typically, under **Server > Sites > Default Web Site > WFO.**
4. In the middle pane, double click **Machine Key**.



The Machine Key pane opens.

5. Copy the **Validation Key** and **Decryption Key**.
6. Complete the following steps for all Performance application servers, for each Instance installed.
   a. Log onto the appropriate Workforce Engagement Management or application server as an Administrator.
   b. Open IIS, **Start > Administrative Tools > Internet Information Services (IIS) Manager**
   c. On the left-hand pane, navigate to Performance: **Server > Sites > Default Web Site > APM > ServiceLayer > <Instance Name>** where ***<Instance Name>*** is the name of the instance name, typically **APM01**. This needs to be done per instance.
   d. In the middle pane, double click **Machine Key**.



   e. Set the following properties:
      i. - Validation method: HMACSHA256 ii. - Encryption method: AES iii. - Validation Key - Automatically generate at runtime: Deselect the checkbox iv. - Validation Key - Generate a unique key for each application: Deselect the checkbox
      v. - Decryption Key - Automatically generate at runtime: Deselect the checkbox
      vi.- Decryption Key - Generate a unique key for each application: Deselect the checkbox
   f. Paste the **Validation Key** and **Decryption Key** from the Workforce Engagement Management application that you copied in step 5. ***These values must match across all Workforce Engagement Management and product application servers for CSRF protection to work.***
   g. In the right-hand pane, click **Apply**, and exit IIS Manager.

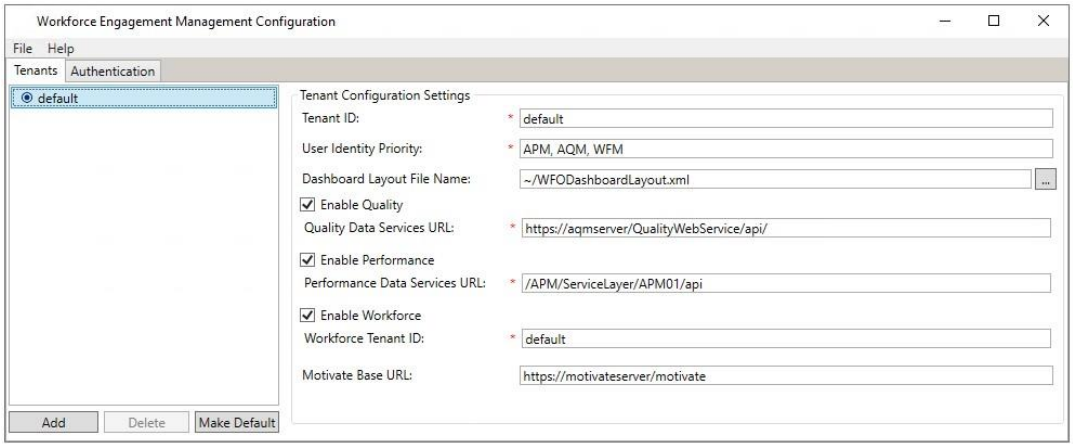
7.2 Configuring Performance

Aspect Performance runs on the Aspect Workforce Engagement Management platform. You must configure Aspect Workforce Engagement Management to point to the Performance data services, as follows:

Note: If you have multiple Instances, you must create a Workforce Engagement Management Tenant for each Instance. To create a tenant, see Tenants Tab on page 4-26.

1. Launch the Aspect Workforce Engagement Management configuration tool. The shortcut to the tool should be available on the server on which Aspect Workforce Engagement Management was installed. The Workforce Engagement Management Configuration window opens with the Tenants tab active.

2. In the Tenant Configuration Settings section of the window, select the **Enable Performance** check box.



Note: If the value is blank, the tool defaults the value to: /APM/ServiceLayer/<InstanceName>/api where Instance Name is the name of your instance.

3. In the **Performance Data Services URL** text box:

   If you are using the same server for the Aspect Workforce Engagement Management and the Aspect Performance Services, type

   /APM/ServiceLayer/<InstanceName>/api

   OR

   If you are using a different server for the Aspect Workforce Engagement Management and Aspect Performance Services, type **http<s>:///[Server Name, Fully Qualified Domain name or IP Address]<:[port]>// APM/ServiceLayer/<InstanceName>/api**

   Where the values in [ ] must be changed based on the following, and the values in < > are optional:

   - **<s>** - Choose whether to select https if in an SSL environment.
   - **[Server Name, Fully Qualified Domain name or IP Address]** – The Server, Fully Qualified Domain Name or IP address value on which the Aspect Performance Services is configured. This is installed using the Aspect Performance Services installation.

Note: If using https, ensure the fully-qualified name matches the name specified in the appropriate certificate.

- **<:[port]>** - If using non-default ports, enter the port value here.
- **[InstanceName]** - The name of the Performance instance. By default, this is **APM01**.

Note: In a load-balanced environment, enter the Load Balancer name or IP, not the Server name or IP of the server on which the Aspect Performance Services is configured.

Warning: If using Workforce Engagement Management in a load-balanced environment, and you use Aspect Performance with Reporting Services, then you must enable Sticky Sessions on the connections to the Workforce Engagement Management servers. If you do not enable Sticky Sessions, then the RS Reports do not execute.

4. Select **File** > **Save**.

8. Verifying the Installation

Before you can verify the installation of Aspect Workforce Engagement Management, you must have Performance, Quality, and Workforce installed and configured with Workforce Engagement Management. See the following chapters for information on how to install and configure the Performance, Quality, and Workforce Management features with Workforce Engagement Management.

- Chapter 5, Configure Aspect Workforce
- Chapter 6, Configure Aspect Quality
- Chapter 7, Configure Aspect Performance

Once you have Workforce Management, Quality, and Performance configured with Workforce Engagement Management, return to this section to verify the Workforce Engagement Management installation.

To verify the installation, log in to Aspect Workforce Engagement Management and check for the presence of data.

8.1 About the Windows Credentials Dialog

When logging in to Aspect Workforce Engagement Management, your browser settings determine whether you are presented with a Windows Credentials dialog. If this dialog is displayed, you must provide correct Windows credentials before the Aspect Workforce Engagement Management Dashboard opens.

Note: Firefox and Safari are also supported browsers. Both present the Windows Credentials window, regardless of which URL method you use. You can change Firefox's behavior so that it does not prompt when using intranet URLs. See your IT administrator for details on how to set the correct behavior in Firefox or Safari.

8.1.1 For Microsoft Edge

Depending on the format of the URL you use to access the Aspect Workforce Engagement Management web site, Windows behaves as follows:

- **http://*webserver*/wfo/*tenantid***, where ***webserver*** is the machine name of your Aspect Workforce Engagement Management web server and ***tenantid*** is the name of the tenant you are attempting to connect to:

If you access a machine using this URL format, the machine is considered to be in the *Intranet* Zone by default. For this reason, Microsoft Edge does not prompt for credentials (assuming the default User Authentication Security Settings for the Local Intranet Zone have not been changed). Instead, Windows evaluates the credentials that the current Windows user supplied when logging in to the machine.

This URL format does not allow a user to log into Aspect Workforce Engagement Management as a different Windows user than the currently logged-in user. This could be an issue in the following cases:

- When validating the installation, since the user who installs Aspect Workforce Engagement Management is unlikely to be an Aspect Workforce Engagement Management user.
- When the current Windows user is logged onto a domain that is not trusted by the Aspect Workforce Engagement Management web server's domain.

- **http://*webserver.domain*.com/wfo/tenantid**, where:
- ***webserver*** is the machine name of your Aspect Workforce Engagement Management web server
- ***domain*** is the domain name of the Aspect Workforce Engagement Management web server
- ***tenantid*** is the name of the tenant listed in the Workforce Engagement Management configuration tool

If you access a machine using this URL format, the machine is considered to be in the *Internet* Zone by default. For this reason, Microsoft Edge prompts for credentials (assuming the default User Authentication Security Settings for the Internet Zone have not been changed). This URL format allows for the current Windows user to log into Aspect Workforce Engagement Management as a different Windows user.

- **http://*webserver_IP*/wfo/tenantid**, where ***webserver_IP*** is the IP address of your Aspect Workforce Engagement Management web server and ***tenantid*** is the name of the tenant you are attempting to connect to.

If you access a machine using this URL format, the behavior of Microsoft Edge is the same as that described immediately above for the **http://*webserver.domain*.com/wfo/tenantid** URL format.

8.1.2 For Google Chrome

Depending on the format of the URL you use to access the Aspect Workforce Engagement Management web site, Windows behaves as follows:

- **http://*webserver*/wfo/*tenantid***, where ***webserver*** is the machine name of your Aspect Workforce Engagement Management web server and ***tenantid*** is the name of the tenant you are attempting to connect to:

If you access a machine using this URL format, Google Chrome authenticates with the credentials of the currently logged-in Windows user.

This could be an issue in the following cases:

- When validating the installation, since the user who installs Aspect Workforce Engagement Management is unlikely to be an Aspect Workforce Engagement Management user.

When the current Windows user is logged onto a domain that is not trusted by the Aspect Workforce Engagement Management web server's domain.

- **http://*webserver.domain*.com/wfo/*tenantid***, where:
- ***webserver*** is the machine name of your Aspect Workforce Engagement Management web server
- ***domain*** is the domain name of the Aspect Workforce Engagement Management web server
- ***tenantid*** is the name of the tenant listed in the Workforce Engagement Management configuration tool

If you access a machine using this URL format, Google Chrome prompts for Windows credentials.

- **http://*webserver_IP*/wfo/*tenantid***, where ***webserver_IP*** is the IP address of your Aspect Workforce Engagement Management web server and ***tenantid*** is the name of the tenant you are attempting to connect to

If you access a machine using this URL format, Google Chrome prompts for Windows credentials.

8.2 Logging In

To log in to Aspect Workforce Engagement Management:

1. Do one of the following:
   - Double-click the Workforce Engagement Management shortcut on the Workforce Engagement Management server desktop.
   - In the address bar of your browser, enter the following URL, where *wfo server name* is the machine name of your Aspect Workforce Engagement Management web server:

     http://*wfo server*/wfo
     or
     http://*wfo server*/wfo/tenantID

   The Aspect Workforce Engagement Management splash screen opens.
2. Click Log In. The Aspect Workforce Engagement Management Dashboard opens.

   If a message is displayed stating that Java Scripts are blocked, you must enable Java Scripts before you can log in to Aspect Workforce Engagement Management.

   Depending on your browser settings, you may be prompted to enter Windows credentials after clicking Log In. If you are prompted for Windows credentials, type a valid Aspect Workforce Engagement Management user name and password, and click OK.
3. On the Aspect Workforce Engagement Management Dashboard, under **Workforce Management**, click one of the module names, such as Personal Account Balances.

   If the module loads and data displays, you have successfully installed Aspect Workforce Engagement Management.

   Note: The Aspect Workforce Engagement Management user account that you are using to verify the installation must have the appropriate permissions configured in Aspect Workforce to access the module. (For example, Empower system locks and any applicable Empower instance locks.)

4. On the Aspect Workforce Engagement Management dashboard, under **Quality**, click one of the module names, such as Search Interaction.

   If the module loads and displays data, you have successfully installed Aspect Workforce Engagement Management.

5. On the Aspect Workforce Engagement Management dashboard, under **Performance**, click one of the module names, such as Awards.

   If the module loads and data displays, you have successfully installed Aspect Workforce Engagement Management.

8.2.1 Enabling Java Scripts

The Aspect Workforce Engagement Management UI Application uses Java Scripts. When you access the Aspect Workforce Engagement Management web site and a message is displayed stating that Java Scripts are being blocked, you must complete the following procedure to enable the scripts.

Note: Before you begin, if you are connecting from a server, use Server Manager to verify that Internet Explorer Enhanced Security (which blocks Java Scripts) is disabled. To do this, select **Local Server** on the Server Manager Dashboard. Under **Properties**, verify that the status of the **IE Enhanced Security Configuration** is **Off**. If it is not, click **On**, and select the **Off** radio button for both Administrators and Users.

To enable Java Scripts:

1. On the Aspect Workforce Engagement Management client machine (not the Aspect Workforce Engagement Management web server), launch **Microsoft Edge**.
2. Select **Tools > Internet Options**.
3. On the **Security** tab, make sure the icon for the **Internet** zone is selected.
4. Click **Custom Level**.
5. In the list of Security Settings, scroll near the bottom of the list to the **Scripting** node.
6. For the **Active Scripting** setting, select **Enable**, 7. Click **OK**, and click **Yes** to confirm the

   Warning message.

8. Click **OK** to close the Internet Options window.
9. Close **Microsoft Edge**, and repeat the procedure.

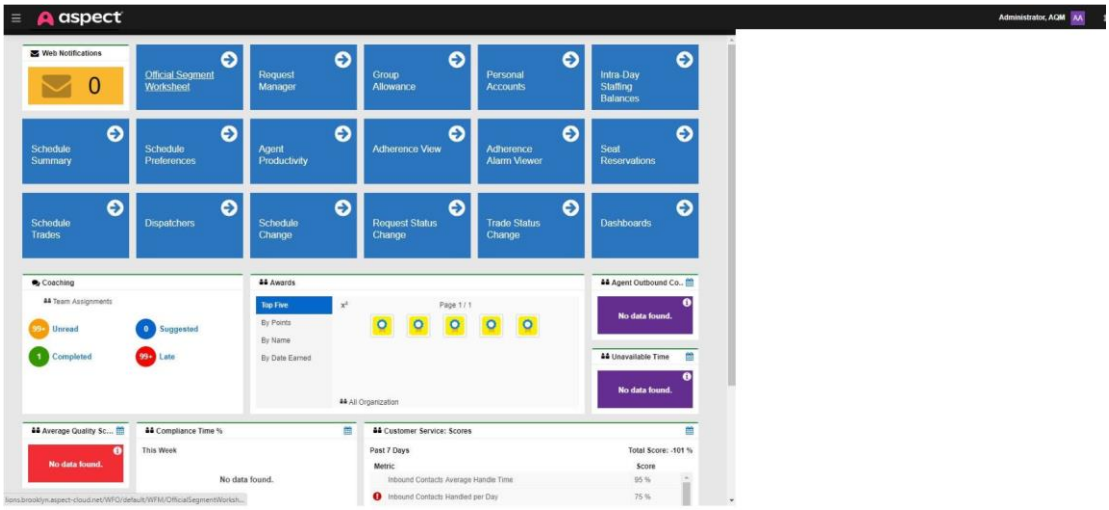
9. Dashboard Configuration

This section describes how to configure the Aspect Workforce Engagement Management dashboard if you choose not to use the default Aspect Workforce Engagement Management dashboard layout.

The Aspect Workforce Engagement Management dashboard is the first screen a user encounters upon logging into the system. The dashboard is a collection of widgets, each of which provides an at-a-glance summary of information that may be important to a user's daily

activities. The content of the dashboard is configurable; as an administrator you can control what widgets appear, their positions, and what subsystems (Workforce, Performance or Quality) contribute widgets to the dashboard.

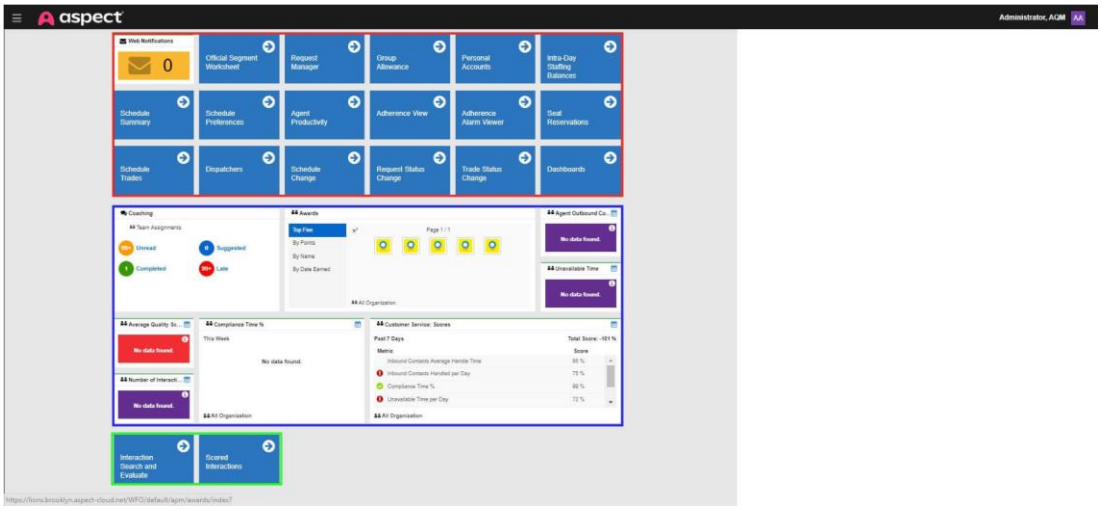
The following screen shot shows the Aspect Workforce Engagement Management dashboard.



The Aspect Workforce Engagement Management dashboard is actually a collection of multiple dashboards, each of which is contributed by the Aspect Workforce, Aspect Quality, or Aspect Performance subsystems. This chapter explains how to configure the Dashboard Layout, but not how to configure the widgets within a dashboard in the layout.

9.1 Dashboard Organization

The Aspect Workforce Engagement Management dashboard is actually composed of multiple dashboards stacked vertically on the screen. In the image below, artificial borders have been added to emphasize the two separate dashboards. The dashboard bordered in red is provided by the Workforce subsystem, while the dashboard bordered in blue is provided by the Performance subsystem. The dashboard bordered in green is provided by the Quality subsystem.



It is important to recognize that each sub-dashboard occupies one or more entire horizontal lines and that widgets from different subsystems cannot intermingle. Widgets from different subsystems can never appear in the same horizontal line on the Aspect Workforce Engagement Management dashboard.

If an Aspect Workforce Engagement Management user is not a valid user, or does not have permissions to see the configured dashboard, then the dashboard for that system is not displayed.

The definition of this collection of dashboards is called a Dashboard Layout. The Dashboard Layout controls only how dashboards are arranged on the Aspect Workforce Engagement Management dashboard, not how the widgets are arranged within a dashboard.

9.2 Locating and Using a Dashboard Layout Definition File

The Aspect Workforce Engagement Management installer delivers one default dashboard layout definition file. This file can be found by opening the folder were Aspect Workforce Engagement Management was installed and browsing to the following folder:

\Alvaria\Workforce Engagement Management\Default\Web\WFO

The default dashboard layout file is named **WFODashboardLayout.xml**. This file can be opened in any text editor. You may wish to make a copy of this file to preserve the original as a backup. Also, by editing and using a copy of the default dashboard layout file, the installer will not overwrite your changes if your Aspect Workforce Engagement Management installation is changed, upgraded, or repaired. The installer will overwrite the default dashboard layout definition file every time it is run.

By default, Aspect Workforce Engagement Management is not configured to use any dashboard layout. You can change the system configuration to use the default dashboard (or a copy) using the Aspect Workforce Engagement Management Configuration tool. This tool is

described in Enabling Workforce Management in Aspect Workforce Engagement Management on page 4-28.

9.3 Editing the Dashboard Layout

If UAC is enabled, copy the dashboard layout file to your desktop before you edit it. After editing the file, copy the edited file to the original folder:

\Alvaria\Workforce Engagement Management\Default\Web\WFO\.

The default contents of the dashboard layout file, WFODashboardLayout.xml, is shown below:

```
<?xml version="1.0" encoding="utf-8"?>
<WFODashboardLayout>
  <Dashboards>
    <Dashboard>
      <Name>WFM</Name>
      <URI>DashboardData/GetDashboard</URI>
      <MaxHeight>100</MaxHeight>
      <AreaName>WFM</AreaName>
    </Dashboard>
    <Dashboard>
      <Name>APM</Name>
      <URI>/Dashboard/GetDashboard</URI>
      <MaxHeight>100</MaxHeight>
      <AreaName>APM</AreaName>
    </Dashboard>
    <Dashboard>
      <Name>AQM</Name>
      <URI>/Dashboard/GetDashboard</URI>
      <MaxHeight>100</MaxHeight>
      <AreaName>AQM</AreaName>
    </Dashboard>
  </Dashboards>
</WFODashboardLayout>
```

This file is an XML file with a <WFODashboardLayout> element as its root. This element may contain multiple <Dashboard> elements within a <Dashboards> container element. The order in which the <Dashboard> elements appear in the XML dictates the order they will appear on screen for a user.

Each <Dashboard> node contains three child elements:

<Name>

This node contains text that uniquely identifies the dashboard in the layout. This value is not shown to the user, nor does it necessarily correlate to a subsystem product name. The only requirement is that the name is unique within the dashboard layout.

<MaxHeight>

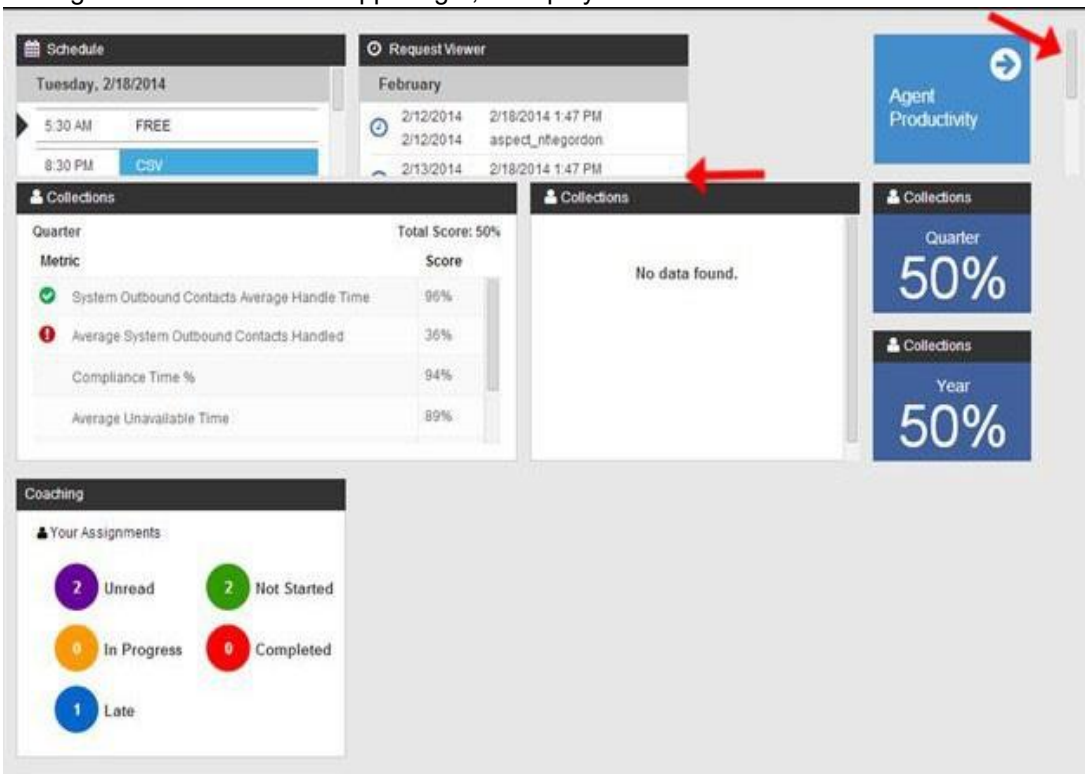
This value controls the maximum number of rows a dashboard may occupy. If the dashboard contains widgets that extend beyond this value, then the dashboard will scroll. If fewer rows are required to display the entire dashboard than the MaxHeight setting dictates, then the

remaining rows are collapsed so there are no blank rows between dashboards within the Dashboard Layout.

The maximum value for this field is 100, which is the default used for all dashboards in the default dashboard layout definition file. It is considered a configuration error to place a widget such that it would extend beyond the 100th row.

This setting can be useful if the number of rows on a dashboard is not constant, as is the case in Performance Management dashboards. By limiting the maximum number of rows a dashboard can occupy, you can guarantee that subsequent dashboards are not pushed off of the screen.

In the example below, the first dashboard is restricted to a MaxHeight of 1 row, as shown by the horizontal arrow on the left. Widgets taller than one row are clipped. A scroll bar, shown by the diagonal red arrow on the upper right, is displayed to scroll within this dashboard.



<AreaName>

This setting indicates the subsystem to which this dashboard belongs. Its value should be **WFM** for a Workforce dashboard, **APM** for a Performance dashboard, or **AQM** for a Quality dashboard.

9.4 Designing a Dashboard

Although this chapter does not discuss laying out the widgets within a dashboard, there are some general rules about widget placement that must be satisfied for a dashboard to be displayed. If any of these rules are violated, an error will occur.

- A widget cannot extend beyond the 6th column. If a widget's position is beyond the 6th column, or if its width and position combined extend beyond the 6th column, then an error will occur.
- A widget cannot extend beyond row 100. If a widget's position is beyond the 100th row, or if its position combined with its height extends beyond the 100th row, then an error will occur.
- Widgets cannot overlap. If any two widgets' position and size would cause an overlap, then an error will occur.
- Blank space is allowed. Widgets are placed absolutely and do not reflow to fill empty space.

9.5 Aspect Workforce Dashboard Configuration

In previous releases of Workforce Engagement Management, Workforce Management dashboard configuration was maintained in an XML file on the server. However, from version 8.3 onwards, this function has moved to a dedicated module within the Workforce Management web interface itself - the Dashboard Editor (this is similar to how dashboards are administered in Aspect Performance). For further information on how to configure Workforce Management dashboards in Workforce Engagement Management, refer to the *Dashboard Configuration Guide* on the Product Documentation library, or the *Aspect Workforce Workforce Engagement Management Administrator Fundamentals* course on Aspect Active Learning, which are accessible at the following link:

For Customers:

Go to https://Alvaria.force.com/community/Home.

- **Training**: Under **Documentation and Training**, click the Aspect Active Learning link. Under the My Info tile, click **Learning**. Browse the courses on the Find Learning tile.
- **Documentation**: Under **Documentation and Training**, click the Product Documentation link. Navigate to **Knowledge Library** > **Product Documentation** > **Aspect Workforce**.

For Partners:

Go to https://Alvaria.force.com/CustomerCenter/. Under Quick Links, click the Technical Training (Aspect Active Learning) link.

- **Training**: Under **Documentation and Training**, click the Aspect Active Learning link. Under the My Info tile, click **Learning**. Browse the courses on the Find Learning tile.
- **Documentation**: Under Quick Links, click the Product Documentation link. Navigate to **Knowledge Library** > **Product Documentation** > **Aspect Workforce**.

9.6 Aspect Quality Dashboard Configuration

Use this section to design a dashboard for Workforce Engagement Management that is composed of Aspect Quality widgets. The dashboard that you design appears on the

Workforce Engagement Management dashboard, which can also include dashboards from other Aspect subsystems, such as Workforce Management or Aspect Performance.

The Aspect Quality dashboard is shared among all Aspect Quality users and cannot vary by user. The dashboard is only displayed for Aspect Quality users, so if a Workforce Engagement Management user is not an Aspect Quality user, that user does not see the Aspect Quality dashboard.

9.6.1 Aspect Quality Widgets

Currently, there are two types of Aspect Quality widget in Workforce Engagement Management.

When clicked, link widgets, such as Interaction Search and Evaluate, Scored Interactions, and Analytics Dashboard, navigate to an Aspect Quality module in Workforce Engagement Management.

Note: Analytics Dashboard will be enabled only when the speech integration is activated.

The Quality Score by Category widget displays the number of calls and the quality score for each speech category for a given time period.

9.6.2 Navigation

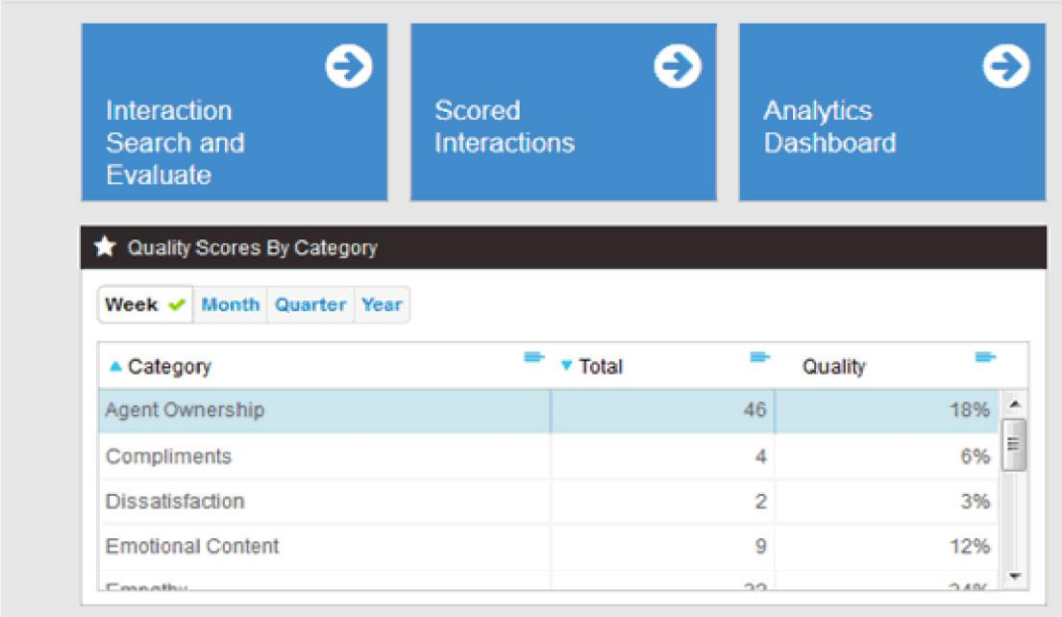
Use the Interaction Search widget to navigate to the Aspect Quality Search module in Workforce Engagement Management.

9.6.3 Default Dashboard Definition Files

Aspect Quality dashboards are defined in an XML file. When you install Workforce Engagement Management, one default Aspect Quality dashboard definition file installs with it. You can find the files in **<InstallDir>\AQM\Quality.WebServices**, where **<InstallDir>** is the directory in which the Aspect Quality back end is installed.

9.6.4 AQMDashboard.xml Definition File

The AQMDashboard.xml file defines an Aspect Quality dashboard that occupies two rows. It includes navigation widgets for three modules: Interaction Search and Evaluate, Scored Interactions and Analytics Dashboard, and Quality Score By Category widget.



The dashboard is ideal to use when Workforce Engagement Management is also connected to other subsystems that contribute a dashboard, such as Aspect Performance or Aspect Workforce.

9.6.5 Editing a Dashboard Definition File

To edit a dashboard definition file, begin with a copy of the default AQMDashboard.xml file and open it in a text editor. The installer overwrites the AQMDashboard.xml file every time the installer runs, so making copies prevents your changes from being overwritten by mistake.

The root node of this XML document is the <Dashboard> node. Within this node, there are three child nodes which contain important configuration information for Aspect Quality and you should not change these nodes: ScriptPath, TemplatePath, and Prefix.

The Dashboard node must also contain a <Widgets> node, which holds the layout information for individual widgets. The minimum definition for an Aspect Quality dashboard with no widgets is:

```
<Dashboard>
  <ScriptPath>Areas/AQM/Scripts/Widgets</ScriptPath>
  <TemplatePath>AQM/Templates</TemplatePath>
  <Prefix>AQM</Prefix>
  <Widgets/>
</Dashboard>
```

9.6.6 Adding a Widget to the Dashboard

To add a widget to the dashboard, add a Widget node to the Widgets node. This node must have four child elements.

Child Element	Description/Value
XPosition	The column in which this widget appears. The value must be between 1 and 6.
YPosition	The row in which this widget appears. The value must be between 1 and 100.
Parameters	Holds instance specific details for a widget. This node is not currently used and is always empty.
WidgetTypeID	The type of widget to add to the dashboard. The widget type dictates the size of the widget when displayed on a dashboard. **Note:** See the following table for information on available widget type and size.

The valid widget types for Aspect Quality are:

WidgetTypeID	Type	Height	Width	Notes
AnalyticsDashboardLinkWidget	Navigation	1	1	Analytics Dashboard
InteractionSearchLinkWidget	Navigation	1	1	Interaction Search
ScoredInteractionLinkWidget	Navigation	1	1	Scored Interaction Search

9.6.6.1 AnalyticsDashboardLinkWidget

The dashboard definition below is the complete definition for an Aspect Quality dashboard with an Analytics Dashboard link widget:

```
<Dashboard>
  <ScriptPath>Areas/AQM/Scripts/Widgets</ScriptPath>
  <TemplatePath>AQM/Templates</TemplatePath>
  <Prefix>AQM</Prefix>
  <Widgets>
    <Widget>
      <XPosition>1</XPosition>
      <YPosition>1</YPosition>
      <Parameters />
```

```
            <WidgetTypeID>AnalyticsDashboardLinkWidget</WidgetTypeID>
          </Widget>
        </Widgets>
</Dashboard>
```

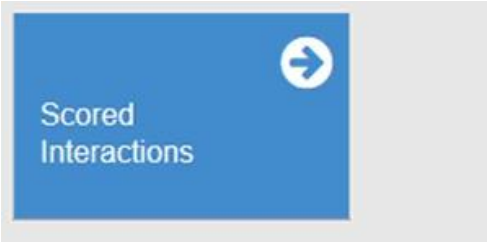
The dashboard appears to the user as:

9.6.6.2 ScoredInteractionLinkWidget

The dashboard definition below is the complete definition for an Aspect Quality dashboard with an Analytics Dashboard link widget:

```
<Dashboard>
  <ScriptPath>Areas/AQM/Scripts/Widgets</ScriptPath>
  <TemplatePath>AQM/Templates</TemplatePath>
  <Prefix>AQM</Prefix>
  <Widgets>
    <Widget>
      <XPosition>1</XPosition>
      <YPosition>1</YPosition>
      <Parameters />
      <WidgetTypeID>ScoredInteractionLinkWidget</WidgetTypeID>
    </Widget>
  </Widgets>
</Dashboard>
```

The dashboard appears to the user as:



9.6.6.3 InteractionSearchLinkWidget

The dashboard definition below is the complete definition for an Aspect Quality dashboard with an Interaction Search and Evaluate link widget:

```
<Dashboard>
```

```
    <ScriptPath>Areas/AQM/Scripts/Widgets</ScriptPath>
    <TemplatePath>AQM/Templates</TemplatePath>
    <Prefix>AQM</Prefix>
    <Widgets>
      <Widget>
        <XPosition>1</XPosition>
        <YPosition>1</YPosition>
        <Parameters />
        <WidgetTypeID>InteractionSearchLinkWidget</WidgetTypeID>
      </Widget>
  </Widgets>
  </Dashboard>
```

The dashboard appears to the user as:

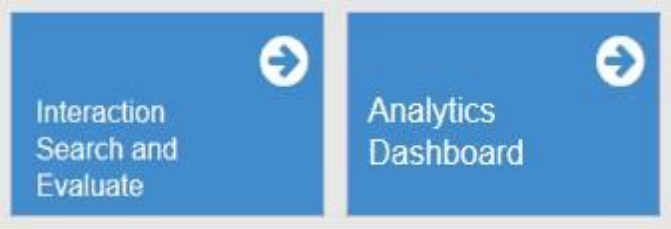
9.6.7 Widget Layout and Best Practices

To ensure the dashboard widgets load correctly, you must perform a valid dashboard configuration.

The dashboard definition below contains both the Interaction Search and Evaluate link widget and the Analytics Dashboard link widget.

```
<?xml version="1.0" encoding="utf-8"?>
<Dashboard>
  <ScriptPath>Areas/AQM/Scripts/Widgets</ScriptPath>
  <TemplatePath>AQM/Templates</TemplatePath>
  <Prefix>AQM</Prefix>
  <Widgets>
    <Widget>
      <XPosition>1</XPosition>
      <YPosition>1</YPosition>
      <Parameters />
      <WidgetTypeID>InteractionSearchLinkWidget</WidgetTypeID>
    </Widget>
    <Widget>
      <XPosition>2</XPosition>
```

```
      <YPosition>1</YPosition>
      <Parameters />
      <WidgetTypeID>AnalyticsDashboardLinkWidget</WidgetTypeID>
    </Widget>
  </Widgets>
</Dashboard>
```



Note: If you change the AnalyticsDashboardLinkWidget XPosition to **1**, the following error message opens.

This error occurs because widgets cannot overlap within a dashboard. Similar errors occur if you do not position a widget within columns 1-6 or rows 1-100. Errors also occur if a widget's height or width would position part of the widget outside of this range.

9.7 Aspect Performance Dashboard Configuration

For information about the Aspect Performance dashboard configuration, see the *Aspect Performance System Administrator Guide.*

A. Troubleshooting

This appendix describes how Aspect Workforce Engagement Management connects to Workforce Management through the Workforce Management Web Services and how to troubleshoot common problems when connecting Aspect Workforce Engagement Management to Workforce Management.

This appendix focuses on troubleshooting problems with the Workforce Management Data Services for Aspect Workforce Engagement Management and, to a limited extent, Workforce Management Web Services. Problems will be discussed from the perspective of errors that occur in the Aspect Workforce Engagement Management client.

A.1 About the Architecture

Aspect Workforce Engagement Management consists of the following web applications:

- The **Workforce Engagement Management** web application provides the HTML resources needed for a web browser to run the Aspect Workforce Engagement Management client. This web application does not provide any application data.
- The **Workforce Data Services for Workforce Engagement Management** web application provides data for the Workforce Management features in Aspect Workforce Engagement Management. This web application reads and writes data to the Workforce Management Web API layer. The Workforce Management Web API (also known as Workforce Management Web Services) is a Workforce Management component, not an Aspect Workforce Engagement Management component. Only limited troubleshooting for this layer will be discussed in this appendix.
- The **Quality Data Services for Workforce Engagement Management** web application provides data for the Quality features in Aspect Workforce Engagement Management. This web application reads and writes data to the Quality Web API layer. The Quality Web API (also known as Quality Web Services, or QWS) is a Quality component, not an Aspect Workforce Engagement Management component. Only limited troubleshooting for this later is discussed in this appendix.
- The **Performance Web API** web application provides data for the Performance Management features in Aspect Workforce Engagement Management. This web application reads and writes data to the Performance Management database.

A.2 Authentication Problems

The following screen shot indicates that the user's browser could connect to one or more back-end services, but all reported that the current user's credentials are not valid.

Note: If claims-based authentication is configured, then this screen remains visible for only a few seconds before the user's browser is redirected to your authentication server to log out. Afterwards, a Workforce Engagement Management window appears, indicating that the user is logged out.

This problem can occur for the following reasons:

The Workforce Management application key is incorrect

Verify that the application key configured in Aspect Workforce matches the application key configured in Aspect Workforce Engagement Management.

To set the Workforce Management application key in Aspect Workforce, use the **Special > Update Application Key** menu option in the Users module of Aspect Workforce.

For instructions on setting this key in Aspect Workforce Engagement Management, see Updating the Application Key in Aspect Workforce on page 5-38.

The Workforce Management user name does not match the user name expected by Aspect Workforce Engagement Management

This can occur when the Workforce Management Data Services for Aspect Workforce Engagement Management are configured to require a domain name to be part of the Aspect Workforce user name, but no such user exists in Aspect Workforce (or vice versa).

You can verify which Aspect Workforce user is expected by consulting the WfmData log file and locating entries similar to the following:

```
2014-02-19 07:22:59.4712      Error 15    Unhandled controller
exception: action "GetDBInformation" on controller "Common" for user
"DOMAIN\USER1" raised an exception.


USER1 is not a valid WFM user type for this operation. (Employee)
```

In this case, the Aspect Workforce Engagement Management user is **DOMAIN\USER1**, as indicated by the first line, but the second line refers only to **USER1** as the Aspect Workforce user. This indicates that the user **DOMAIN\USER1** has been mapped to **USER1** instead of **DOMAIN\USER1** in Aspect Workforce Engagement Management.

To resolve this issue, verify that an Aspect Workforce user exists that includes the domain name. For more information, see Require Domain Name for Workforce Management Users on page 5-42.

Claims-based authentication is configured, but the value in the name claim does not match a user name in any back-end system.

By default, Workforce Engagement Management expects a SAML token to contain an assertion named http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name. If that assertion does not exist, or if it contains a value that is not a valid user in any back-end system, then the user is not authenticated. Verify that your SAML tokens contain a claim named http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name and that the value is a valid user in at least one back-end system. For details, see Configure the ADFS Claims on page C-114.

Claims-based authentication is configured, but the machine key is not synchronized between the UI and the data applications.

All Workforce Engagement Management web applications must have their machine keys synchronized to share SAML-based identity tokens. Verify that you have completed Configure the ADFS Claims on page C-114 properly.

The machine encryption keys are not the same in the WEM and back-end services applications

This problem occurs when the machine encryption key is not synchronized between the backend services for the Aspect Workforce Engagement Management application and the Workforce Engagement Management application.

If you observe the following error logged to the WfmData log file, then the machine keys may not be synchronized:

```
Exception: ID1026: Failed to read and validate security token:
CryptographicException Error occurred during a cryptographic
operation.
```

Verify that the machine keys have been synchronized as described in Set Machine Key for CSRF Anti-Forgery Token.

The SAML signing certificate thumbprint does not match the certificate used to sign a SAML token

This problem can occur when the certificate thumbprint that is configured in the Workforce Engagement Management application does not match the thumbprint the SAML server used to sign the SAML certificate.

If you observe the following error logged to the WEM log file, then the wrong thumbprint may be configured in Workforce Engagement Management

```
System.IdentityModel.Tokens.SecurityTokenException: ID4175: The
issuer of the security token was not recognized by the
IssuerNameRegistry. To accept security tokens from this issuer,
configure the IssuerNameRegistry to return a valid name for this
issuer.
```

Verify that the correct thumbprint is configured as described in section 7.2.2.2.3.

The Token Server Realm/Audience does not match the relying party identifier configured on the SAML server

This problem can occur when the Token Server Realm/Audience value that is configured in the Workforce Engagement Management application is not the value configured on the SAML server that the user used to sign in.

If you observe the following error logged to the WEM log file, then the relying party Id configured for Workforce Engagement Management does not match the relying party ID configured on the SAML server:

```
System.IdentityModel.Tokens.AudienceUriValidationFailedException:
ID1038: The AudienceRestrictionCondition was not valid because the
specified Audience is not present in AudienceUris.
```

Verify that the SAML server and Workforce Engagement Management is configured as described in Token Server Issuer on page 4-29.

A.3 Logging

This section describes the basic settings that are often changed for Support troubleshooting. For assistance in changing the default logging configuration, contact Aspect Customer Care.

Workforce Engagement Management uses NLog for logging. NLog is a very versatile tool that is highly configurable. As such, only basic/general settings will be mentioned in this section, but more complete documentation can be found here: https://nlog-project.org/config/

There are separate NLog configuration files for each portion/level of the product. They will be mentioned separately below.

A.3.1 Workforce Engagement Management

The configuration file can be found here by default: C:\Program Files\Alvaria\Workforce Optimization\Default\Web\WFO\NLog.config

In the <targets> section, it's recommended to set the following attributes to the desired directory structure for each target:

- **fileName**
- **archiveFileName**

In the <rules> section, it's recommend to set the minlevel value to:

- **Trace** for verbose logging output
- **Info** for default/standard logging output

All other settings can be left at default.

A.3.2 Workforce Management Engagement - Workforce

The configuration file can be found here by default: C:\Program Files\Alvaria\Workforce Optimization\Default\Web\WFMData\NLog.config

In the <targets> section, it's recommended to set the following attributes to the desired directory structure for each target:

- **fileName**
- **archiveFileName**

In the <rules> section, it's recommend to set the minlevel value to:

- **Trace** for verbose logging output
- **Info** for default/standard logging output

B. Notes on the IIS Role Services for Windows

When you are using Server Manager to configure role services for IIS for Windows, several default selections are not required by Aspect Workforce Engagement Management and can be disabled if you prefer or if disabling them is required by your company policy.

In the following table, the roles services indicated by a green-shaded cell are not required.

***Table B-1** Optional IIS Role Services (Green-Shaded Cells)*

Category / Role Service	When Selecting Application Server > Web Server
Common HTTP Features	
Default Document	Default
Directory Browsing	Default
HTTP Errors	Default
Static Content	Default
HTTP Redirection	Default
WebDAV Publishing	
Health and Diagnostics	
HTTP Logging	Default
Custom Logging	
Logging Tools	Default
ODBC Logging	
Request Monitor	Default
Tracing	
Performance	
Static Content Compression	Default

Dynamic Content Compression	Default

Table B-1 *Optional IIS Role Services (Green-Shaded Cells) (Continued)*

Category / Role Service	When Selecting Application Server > Web Server
Security	
Request Filtering	Default
Basic Authentication	Default [1]
Centralized SSL Certificate Support	
Client Certificate Mapping Authentication	Default
Digest Authentication	Default
IIS Client Certificate Mapping Authentication	Default
IP and Domain Restrictions	Default
URL Authorization	Default
Windows Authentication	Default
Application Development	
.Net Extensibility 3.5	
.Net Extensibility 4.7/4.8	Default
Application Initialization	
ASP	
ASP.NET 3.5	
ASP.NET 4.7/4.8	Default
CGI	
ISAPI Extensions	Default
ISAPI Filters	Default
Server Side Includes	

WebSocket Protocol	
FTP Server	
FTP Service	
FTP Extensibility	

Table B-1 *Optional IIS Role Services (Green-Shaded Cells) (Continued)*

Category / Role Service	When Selecting Application Server > Web Server
Management Tools	
IIS Management Console	Default
IIS 6 Management Compatibility	
IIS Management Scripts and Tools	Default
Management Service	

[1] Required if Aspect Workforce Web Services will be configured to use Basic or both Basic and Windows Authentication

C. Security and Authentication

C.1 Windows-Integrated Authentication

Aspect Workforce Engagement Management relies on Windows integrated security, which is handled by IIS to authenticate the user.

Using Windows authentication, Aspect Workforce Engagement Management never handles user credentials directly. This means that the Aspect Workforce Engagement Management server must be joined to a domain in which IIS can validate user credentials. It is also possible for IIS to authorize local user accounts defined on the Aspect Workforce Engagement Management Windows server itself.

Note: It is also possible for IIS to authenticate local user accounts defined on the Aspect Workforce Engagement Management Windows server itself, but this is only true for Aspect Workforce; it does not apply to Aspect Quality or Aspect Performance, which do not support the use of local user accounts.

C.2 Claims-Based Authentication

Using claims-based authentication, Aspect Workforce Engagement Management users are able to utilize single sign-on when logging in. This gives users the benefit of being able to launch Aspect Workforce Engagement Management from multiple systems that utilize Active Directory Federation Services (ADFS) authentication servers.

Workforce Engagement Management needs to communicate with a token server, thus requiring additional configuration as described in Claims-Based Authentication on page C-103, and also in the following sections.

- For Aspect Workforce, in Claims-based Authentication for Workforce Management on page C-135.
- For Aspect Quality, in Claims-based Authentication for Quality Web Services in Quality on page C-135.
- For Aspect Performance, in Claims-based Authentication for Performance Management on page C-138.

C.2.1 Product Authorization

The following information is a high-level overview of how each of the three Workforce Engagement Management products authorizes users.

Aspect Workforce enforces application security for the authenticated user using certain Aspect Workforce system and instance locks that are defined in the Workforce Management desktop client application. For more information, see the *Aspect Workforce Installation Guide.*

Aspect Performance users are granted access based on their Agent and/or Team mapping, and the Roles that they are assigned to them. For more information, see the *Aspect Performance System Administrator Guide*.

For Aspect Quality users, users are authorized using Windows Integrated Authentication. For more information, see the *Aspect Quality Security Guide*.

C.3 Claims Authentication for Workforce Engagement Management

Configuring claims authentication for Workforce Engagement Management depends on completion of the following:

- Configure the ADFS Relying Parties
- Configure the ADFS Claims
- Export the ADFS Certificates
- Install the ADFS Certificates
- Save and close the file.

C.4 Configure the ADFS Relying Parties

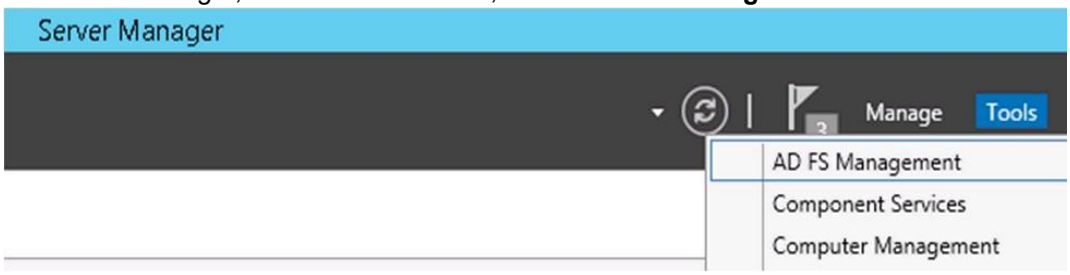
Configure the ADFS relying parties based on which version of Windows Server you use.

- For Windows Server 2022 and 2025/ADFS 4.0 on page C-104

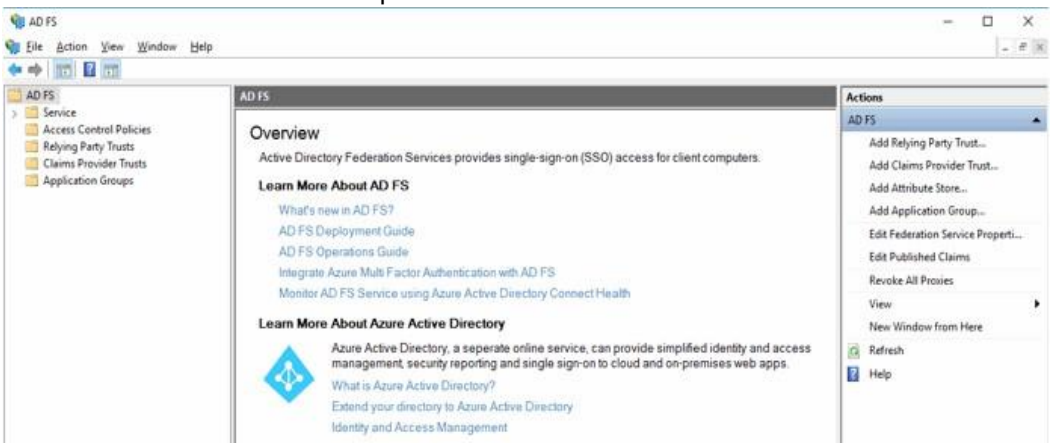
C.4.1 For Windows Server 2022 and 2025/ADFS 4.0

The Workforce Engagement Management Service Layer must be added as a relying party trust in ADFS so that it can authenticate correctly. These procedures need to be performed on the ADFS 3.0 Server.

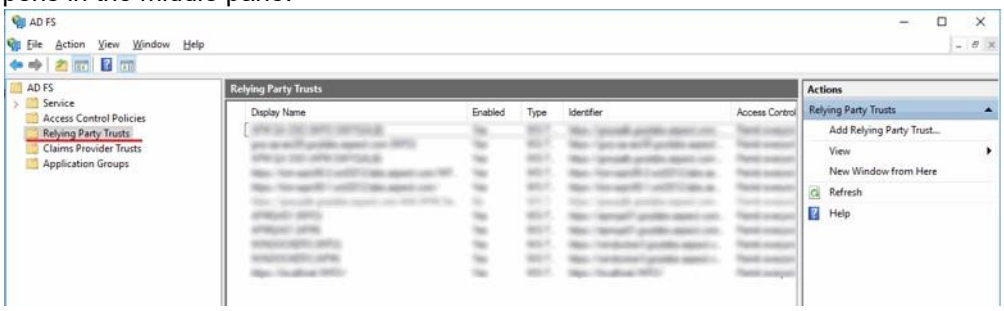
1. Launch ADFS.
2. In Server Manager, from the Tools menu, Select **AD FS Management**.



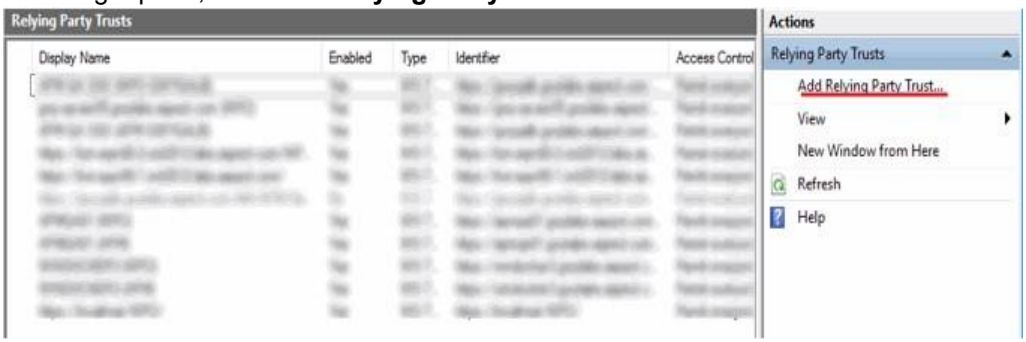
The AD FS Overview window opens.



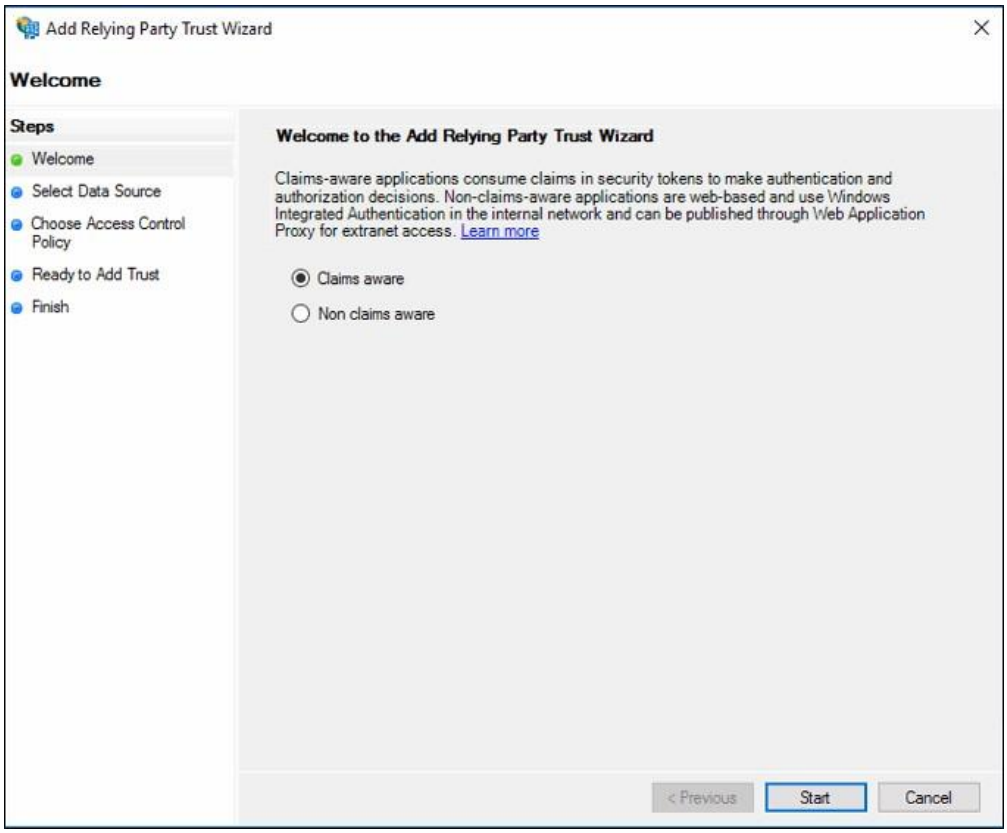
3. In the left pane, select the **Relying Party Trusts** directory. The Relying Party Trusts pane opens in the middle pane.



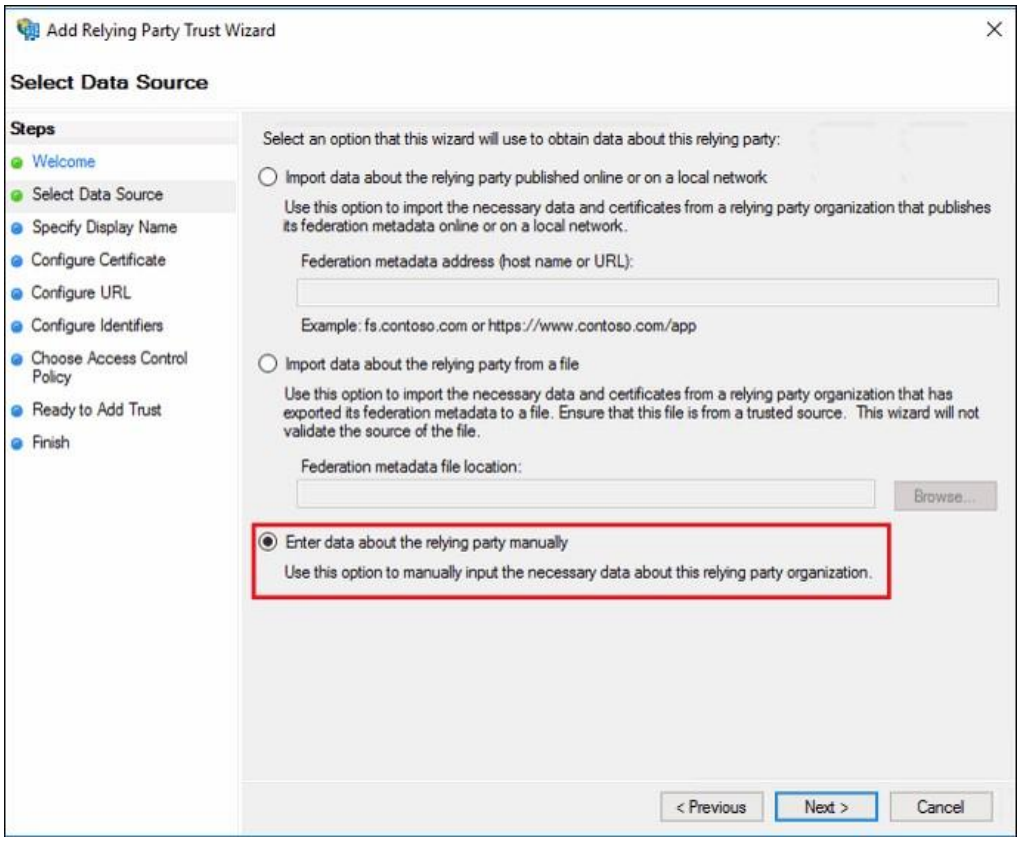
4. In the right pane, click **Add Relying Party Trust**.



The Add Relying Party Trust Wizard opens with the Welcome tab active.

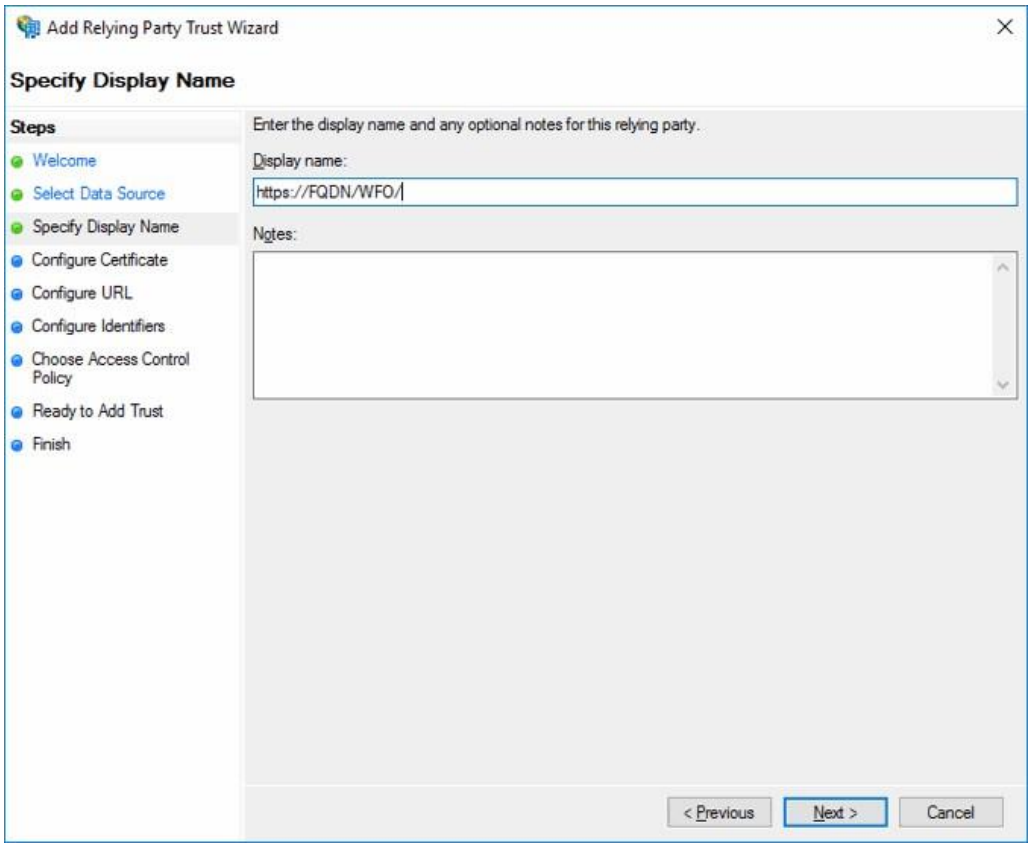


5. Select the **Claims aware** option.
6. Click **Start**. The Select Data Source tab opens.
7. Select the **Enter data about the relying party manually** option.

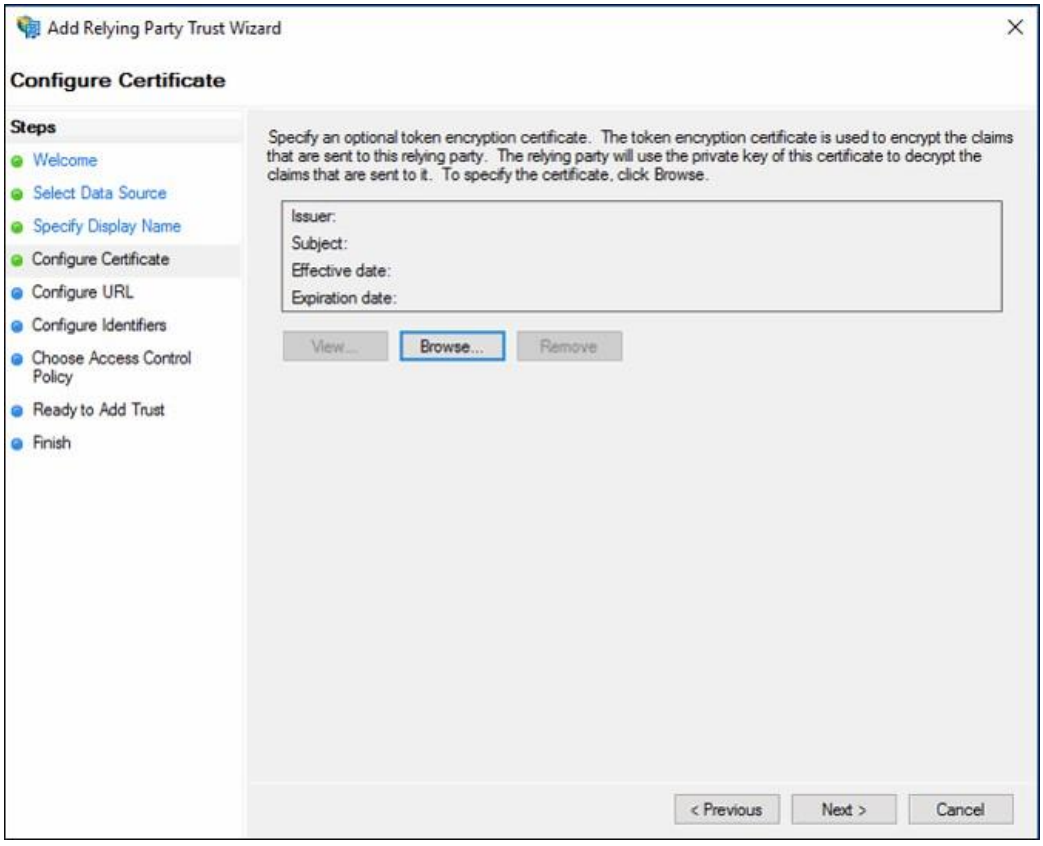


8. Click **Next**. The Specify Display Name tab opens.
9. In the Display name text box, type any display name that you want. Aspect recommends that you type the URL of the web site that you want to set up as a relying party.
10. Enter the FQDN of the Workforce Engagement Management URL.

    Note: A trailing forward slash is required to facilitate single sign-out. The case of the URL is important for single sign-out broadcasts to relying parties from ADFS.


Add Relying Party Trust Wizard
Specify Display Name
Steps
Welcome
Select Data Source
Specify Display Name
Configure Certificate
Configure URL
Configure Identifiers
Choose Access Control Policy
Ready to Add Trust
Finish
Enter the display name and any optional notes for this relying party.
Display name:
https://FQDN/WFO/
Notes:
< Previous
Next >
Cancel

11. Click . The Configure Certificate tab opens.

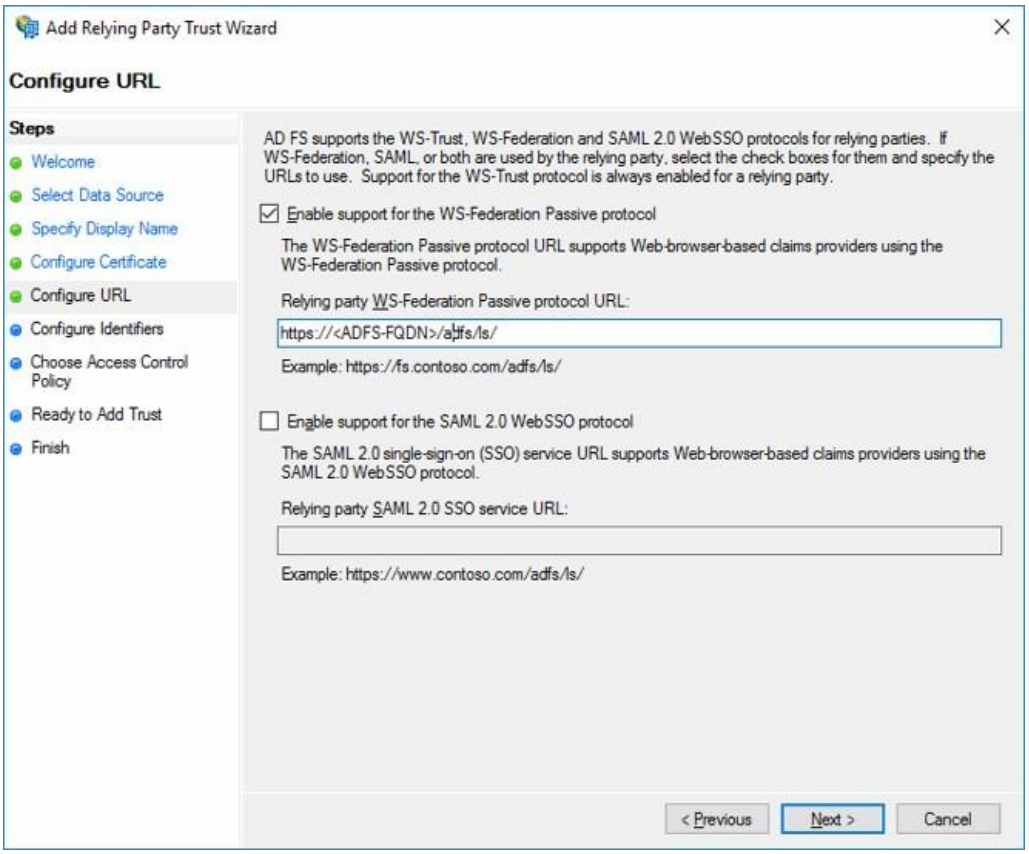


12. Click **Next**. The Configure URL tab opens.

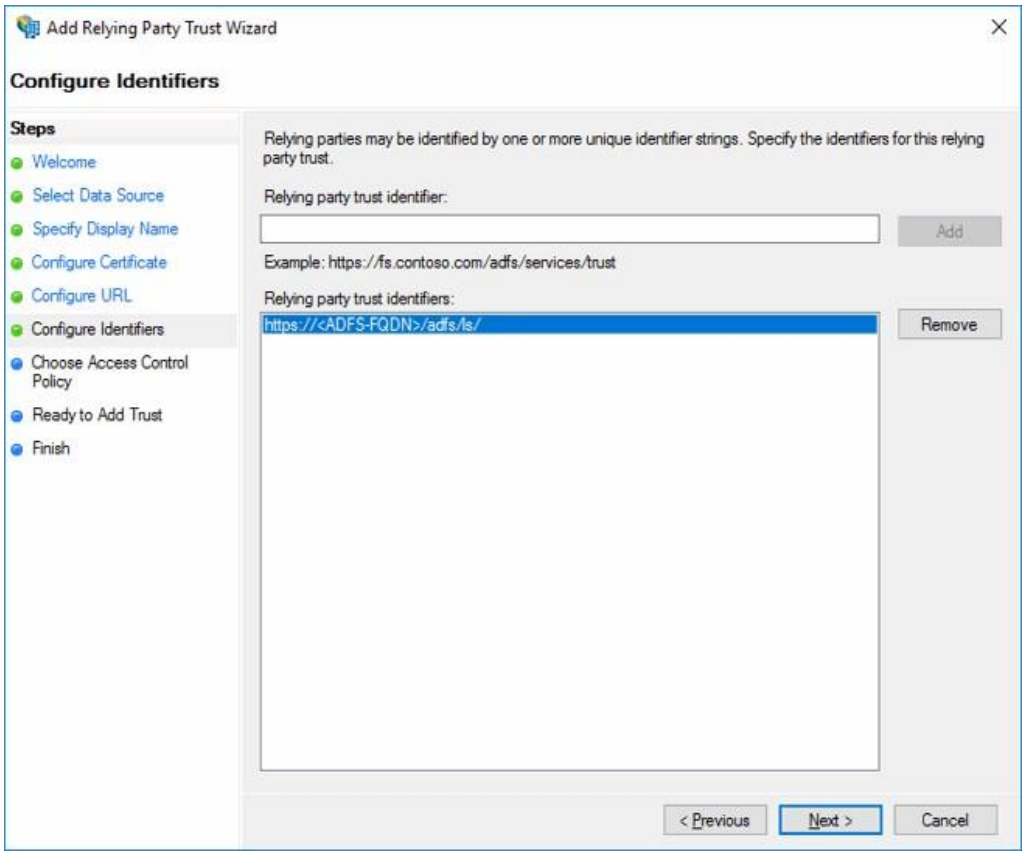
13. Verify that the **Enable support for the WS-Federation Passive protocol** check box is selected.

14. In the Relying Party WS-Federation Passive protocol URL text box, type the fully-qualified URL of the Workforce Engagement Management URL.

Next

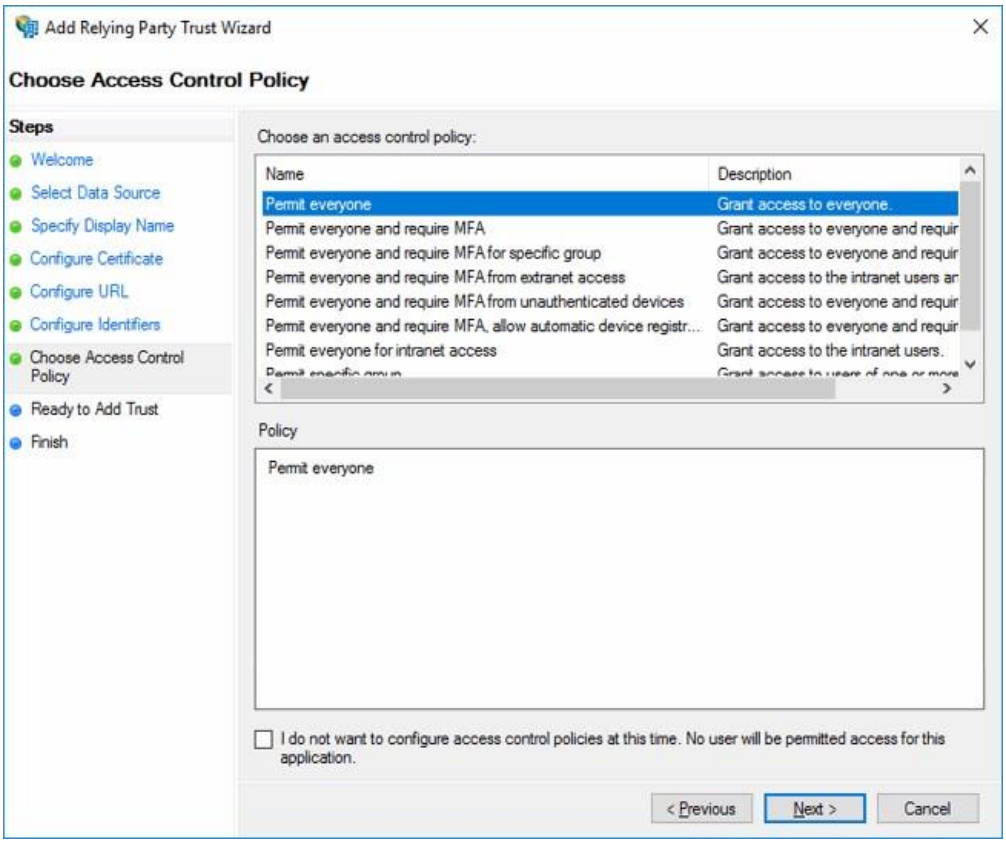


15.Click . The Configure Identifiers tab opens.

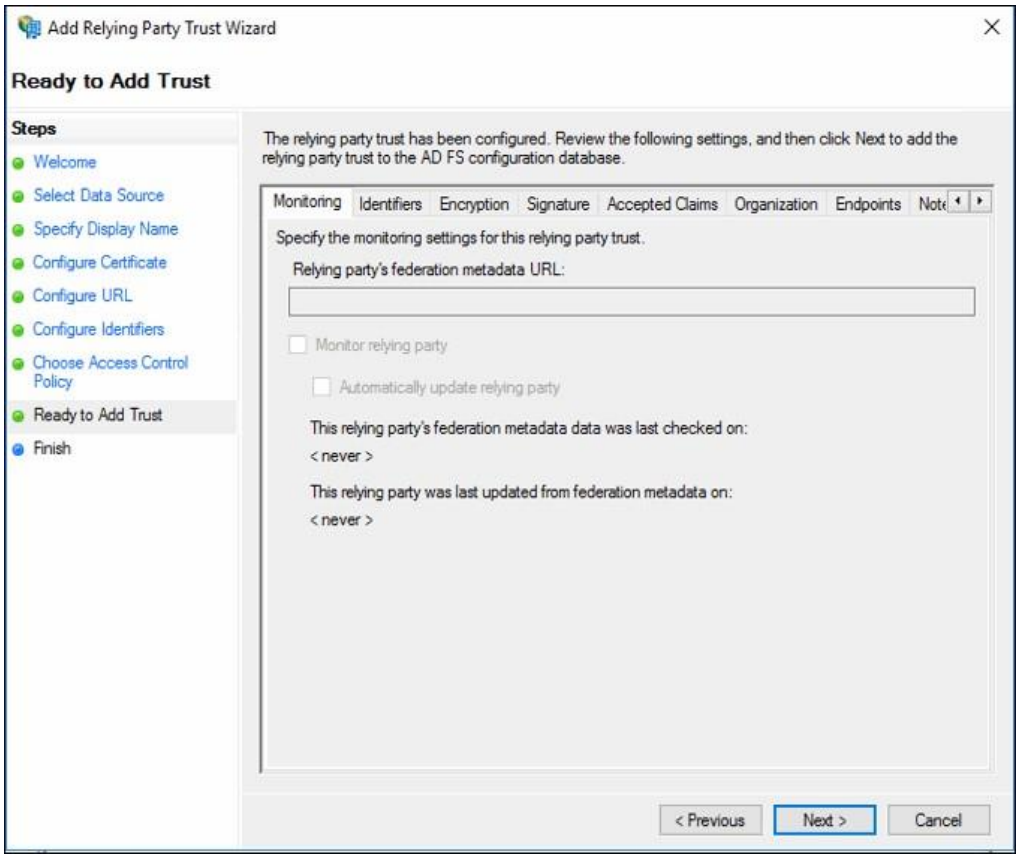


16. Accept the default by clicking **Next**. The Choose Access Control Policy tab opens.
17. From the Choose an access control policy list, select **Permit everyone**.

Next

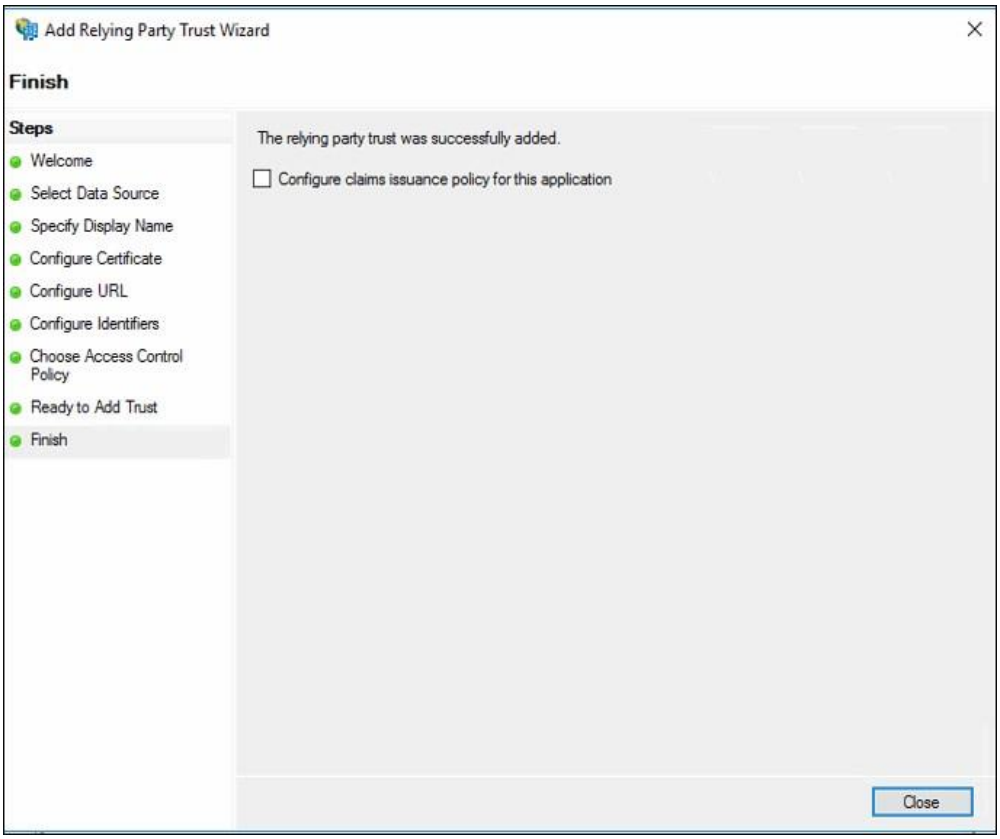


18.Click . The Ready to Add Trust tab opens.



19. Accept the default by clicking **Next**. The Finish tab opens.

Next



20.Accept the default by clicking **Close**.

C.4.2 Configure the ADFS Claims

To create the claims, you must define three claims transformation rules.

Rule Name	Inbound Claim	Outbound Claim
Name	Windows account name	Name
Windows account name	Windows account name	Windows account name
Email address	Email addresses	Email address

Perform these procedures on the Active Directory Federation Services (ADFS) server.

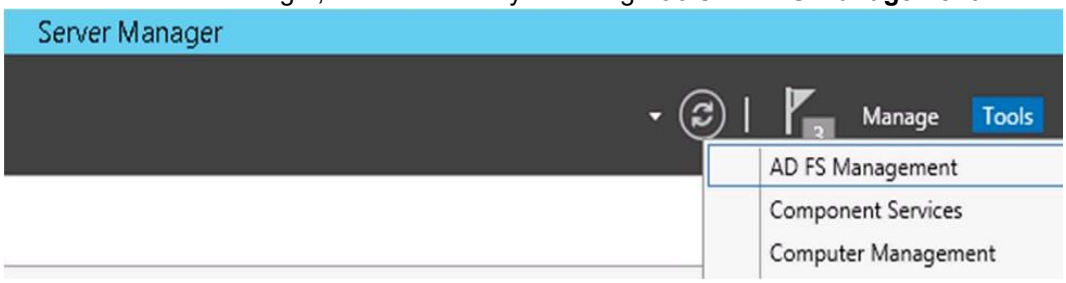
- Configure the Name Claim
- Configure the Windows Account Name Claim
- Configure the Email Address Claim

C.4.2.1 Configure the Name Claim

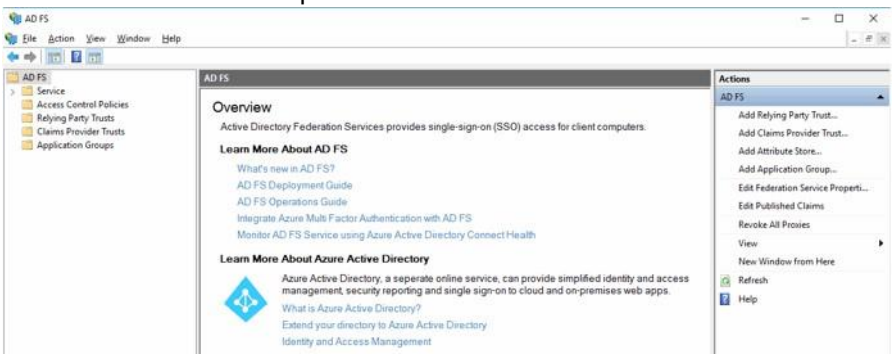
- For Windows Server 2022 and 2025/ADFS 4.0 on page C-115

C.4.2.2 For Windows Server 2022 and 2025/ADFS 4.0

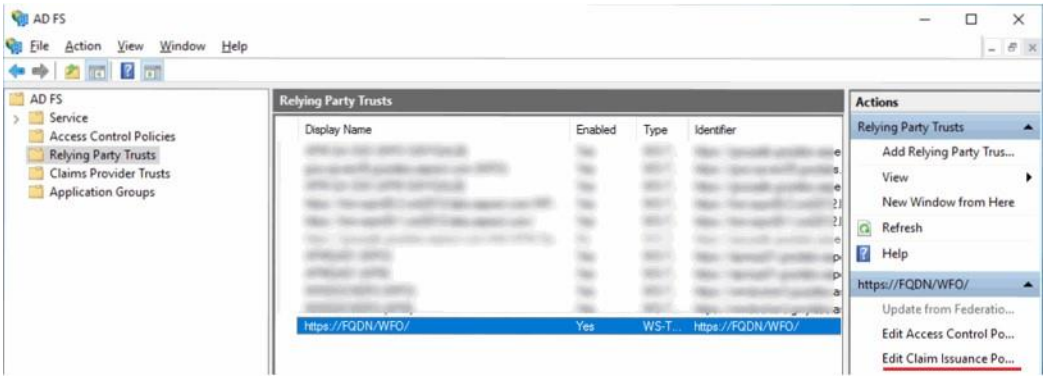
1. From the Server Manager, launch ADFS by selecting **Tools>AD FS Management**.



The AD FS Overview window opens.

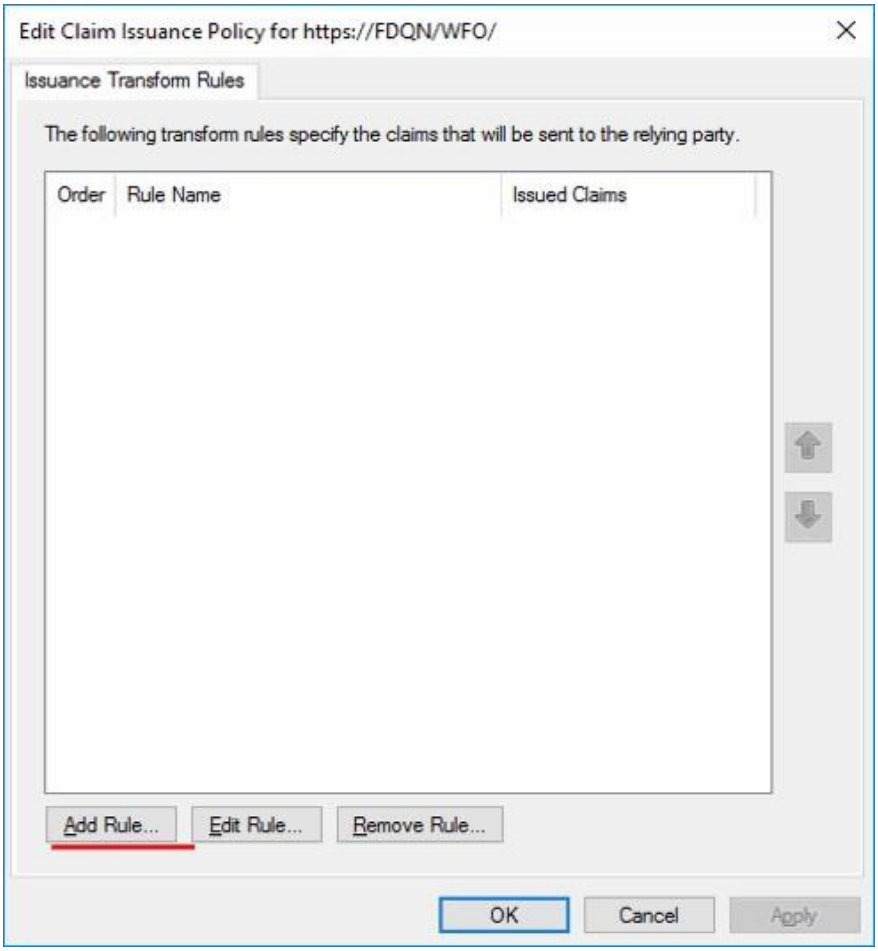


2. In the left pane, select the **Relying Party Trusts** directory. The Relying Party Trusts display in the middle pane.
3. From the middle pane, select the relying party trust that you created in the previous section. The relying party trust displays in the Actions pane.
4. In the Action pane, click **Edit Claim Issuance Policy**.



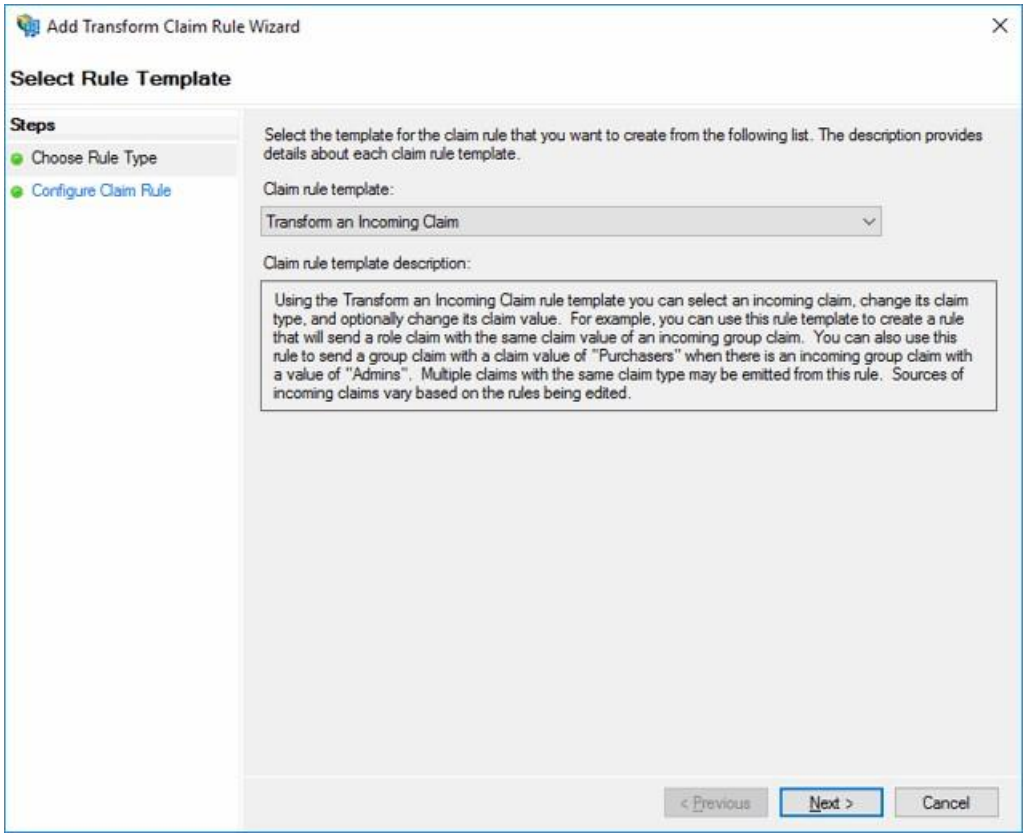
The Edit Claim Issuance Policy window opens with the Issuance Transform Rules tab active.

5. Click **Add Rule**.

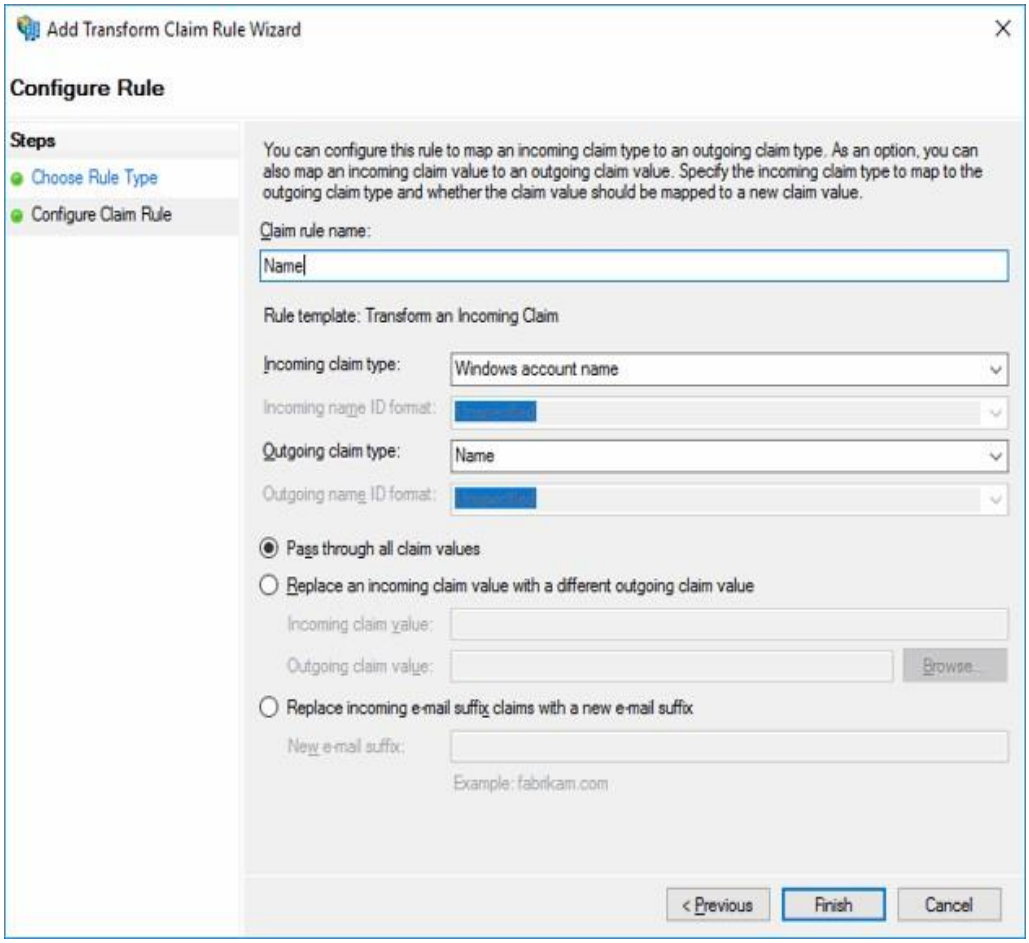


The Add Transform Claim Rule Wizard window opens with the Choose Rule Type option selected.

6. From the Claim rule template drop-down list box, select the **Transform an Incoming Claim** template.



7. Click **Next**. The Configure Claim Rule window opens.
8. In the Claim rule name text box, type **Name**.
9. From the Incoming claim type drop-down list box, select **Windows account name**.
10. From the Outgoing claim type drop-down list box, select **Name**.
11. Select the **Pass through all claim values** option.



12. Click **Finish**. The Add Transform Claim Rule Wizard window closes and the Edit Claim Issuance Policy window displays with the Issuance Transform Rules tab active.
13. Go directly to Configure the Windows Account Name Claim on page C-118.

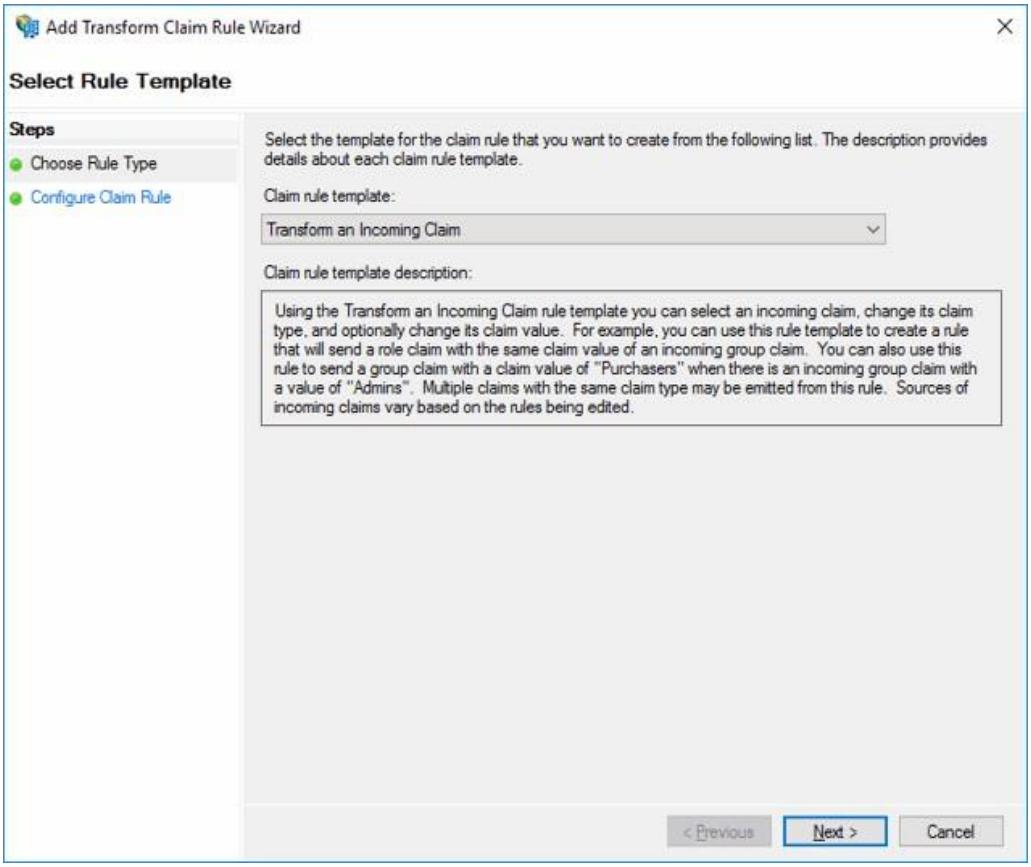
C.4.2.3 Configure the Windows Account Name Claim

C.4.2.4 For Windows Server 2022 and 2025/ADFS 4.0

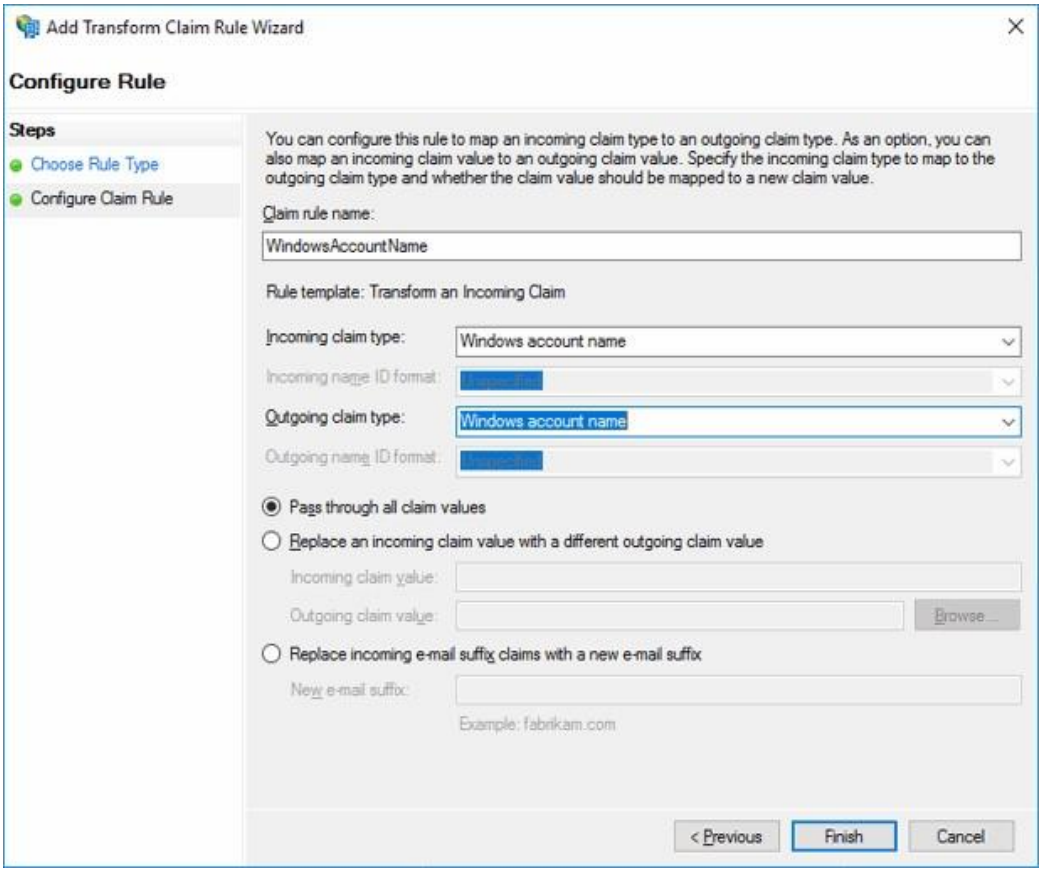
1. From the Edit Claim Issuance Policy window, on the Issuance Transform Rules tab, click **Add Rule**.

   The Add Transform Claim Rule Wizard opens to the Select Rule Template window, with the Choose Rule Type tab active.

2. From the Claim rule template drop-down list box, select **Transform an Incoming Claim**.



3. Click **Next**. The Configure Claim Rule tab opens.
4. In the Claim rule name text box, type **WindowsAccountName** (no spaces between the words).
5. From the Incoming claim type drop-down list box, select **Windows account name**.
6. From the Outgoing claim type drop-down list box, select **Windows account name**.
7. Select the **Pass through all claim values** option.



8. Click **Finish**. The Add Transform Claim Rule Wizard window closes and the Edit Claim Issuance Policy window opens with the Issuance Transform Rules tab active.
9. Go directly to Configure the Email Address Claim on page C-120.

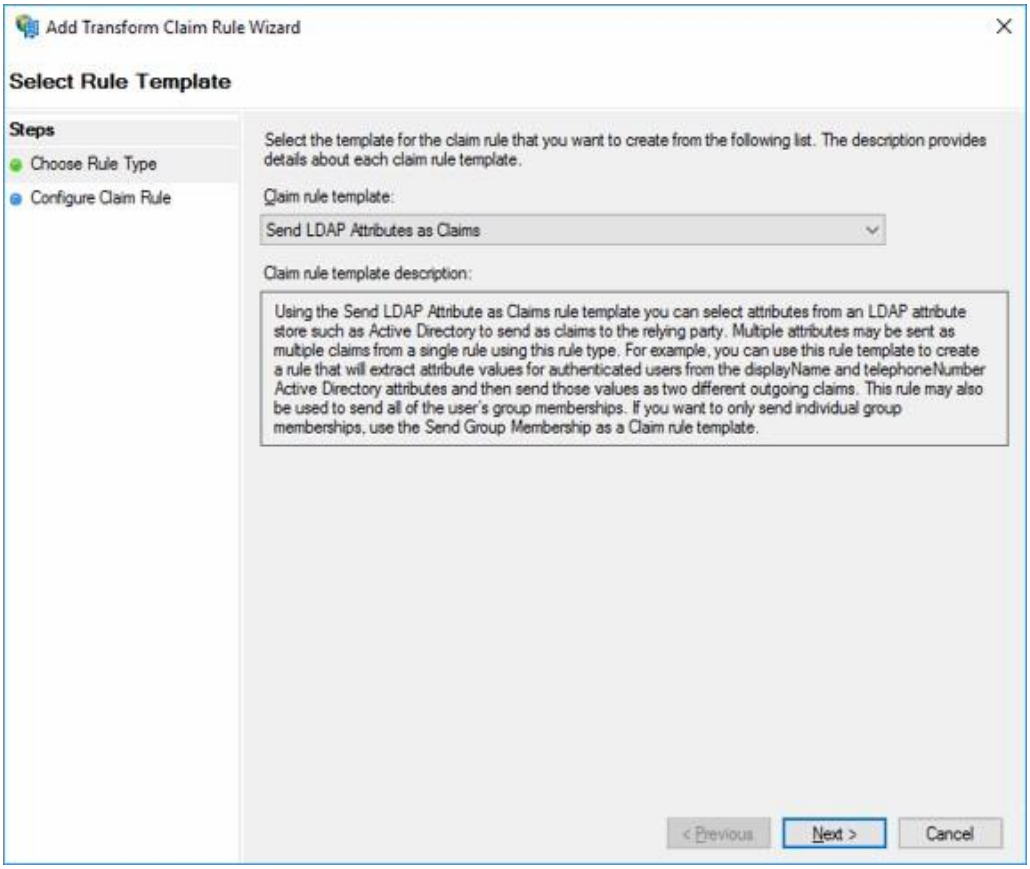
C.4.2.5 Configure the Email Address Claim

- For Windows 2019 and 2022/ADFS 4.0 on page C-120

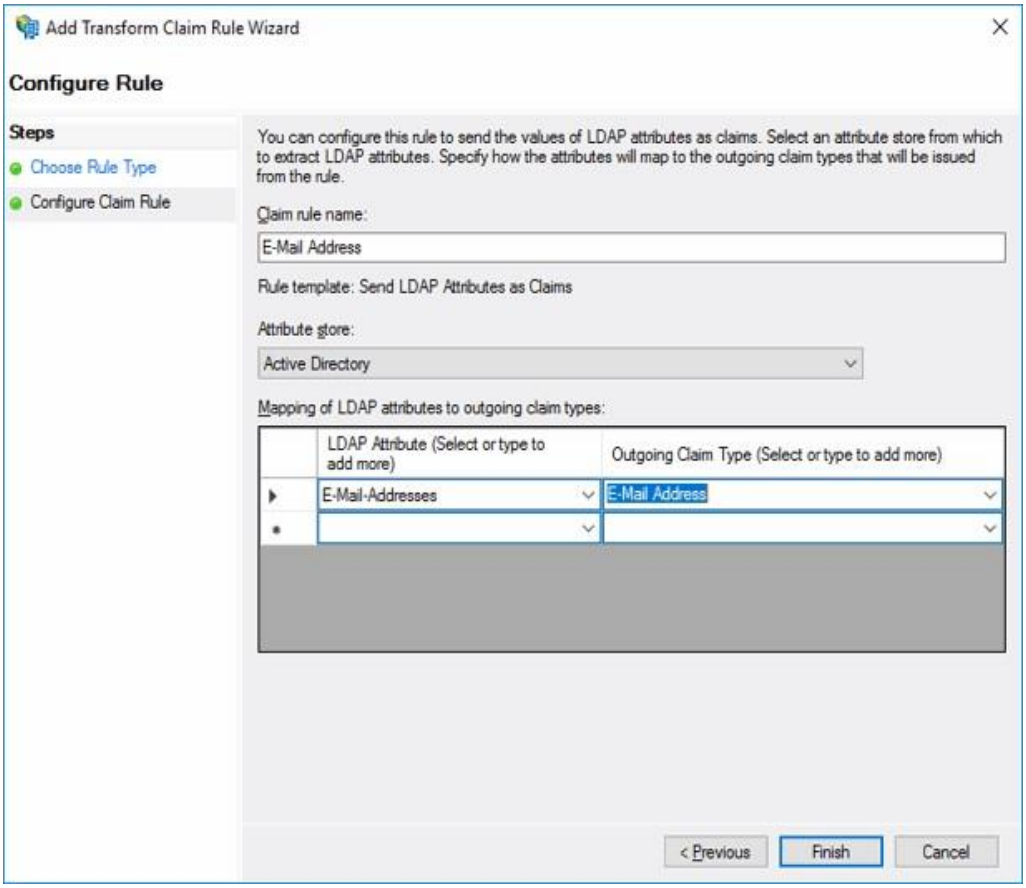
C.4.2.6 For Windows 2019 and 2022/ADFS 4.0

1. From the Edit Claim Issuance Policy window, on the Issuance Transform Rules tab, click **Add Rule**.

   The Add Transform Rule Wizard opens to the Select Rule Template tab, with the Choose Rule Type tab active.
2. From the Claim rule template drop-down list box, select the **Send LDAP Attributes as Claims** template.

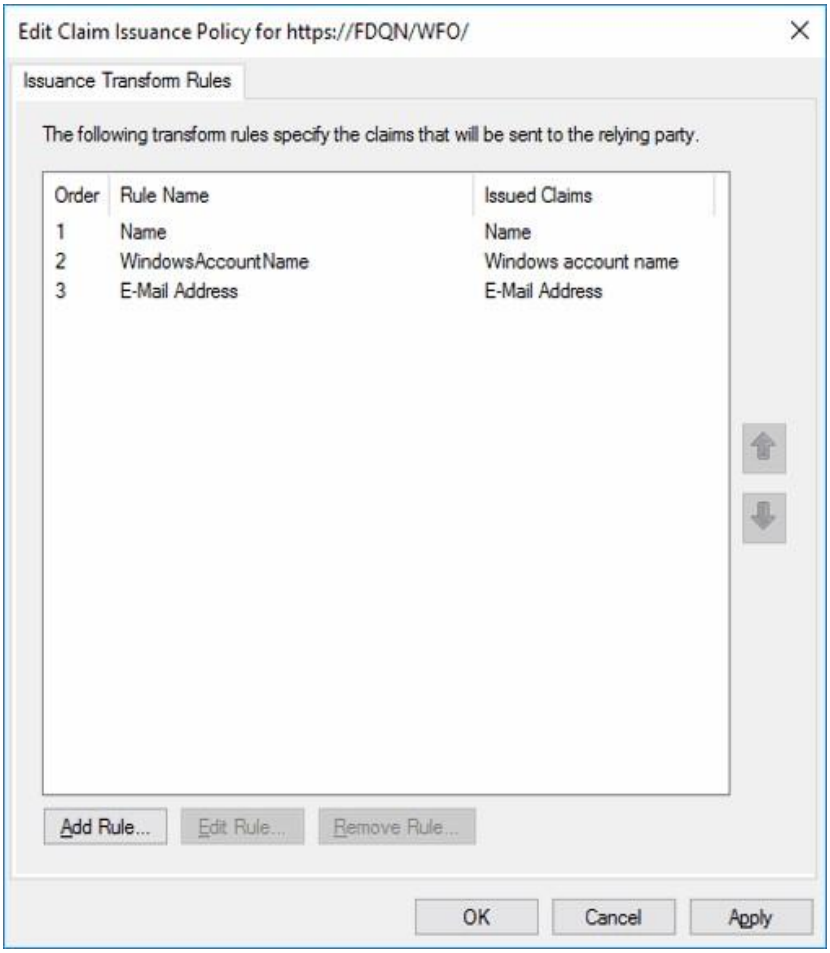


3. Click **Next**. The Configure Claim Rule tab opens.
4. In the Claim rule name text box, type **E-Mail Address**.
5. From the Attribute store drop-down list box, select **Active Directory**.
6. In the Mapping of LDAP attributes to outgoing claim types table, from the LDAP Attribute drop-down list box, select **E-mail-Addresses**.
7. From the Outgoing Claim Type drop-down list box, select **E-Mail Address**.



8. Click **Finish**. The Add Transform Claim Rule Wizard closes and the Edit Claim Issuance Policy window displays with the Issuance Transform Rules tab active.

   The three claim rules that you created display in the list box.



9. Click **OK**. The Edit Claim Issuance Policy window closes.

C.4.3 Export the ADFS Certificates

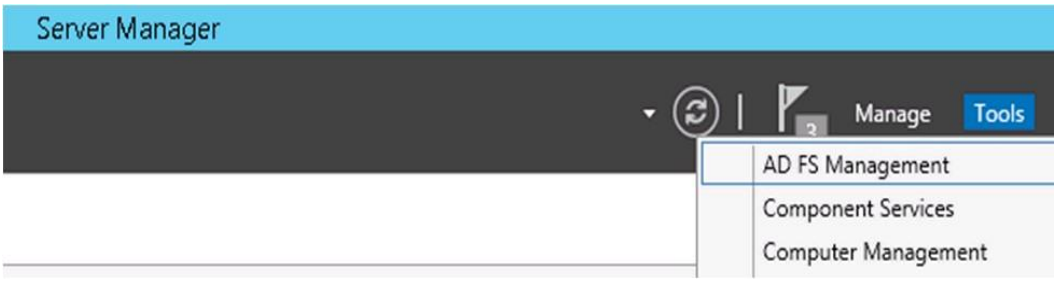
You already may have performed these procedures; they are included again here for reference.

- For Windows 2019 and 2022/ADFS 4.0 on page C-123

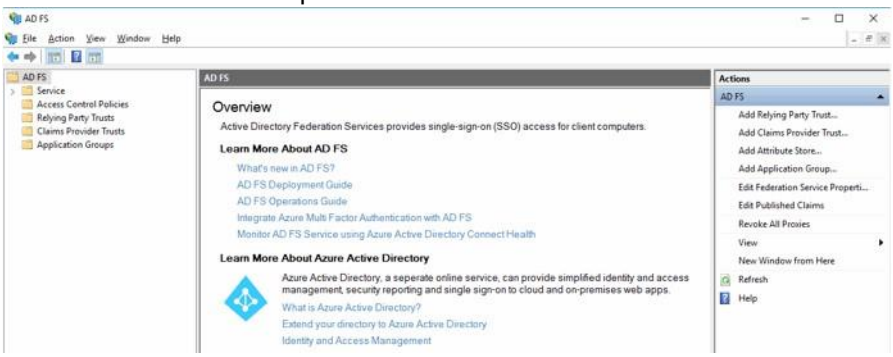
C.4.3.1 For Windows 2019 and 2022/ADFS 4.0

To export the Active Directory Federation Services (ADFS), perform these procedures on the ADFS 3.0 server.

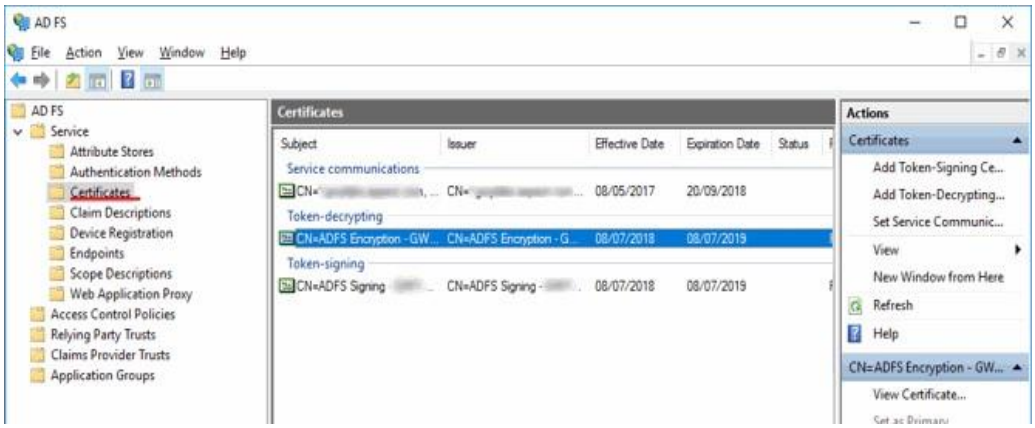
1. In Server Manager, launch ADFS by selecting **Tools>AD FS Management**.



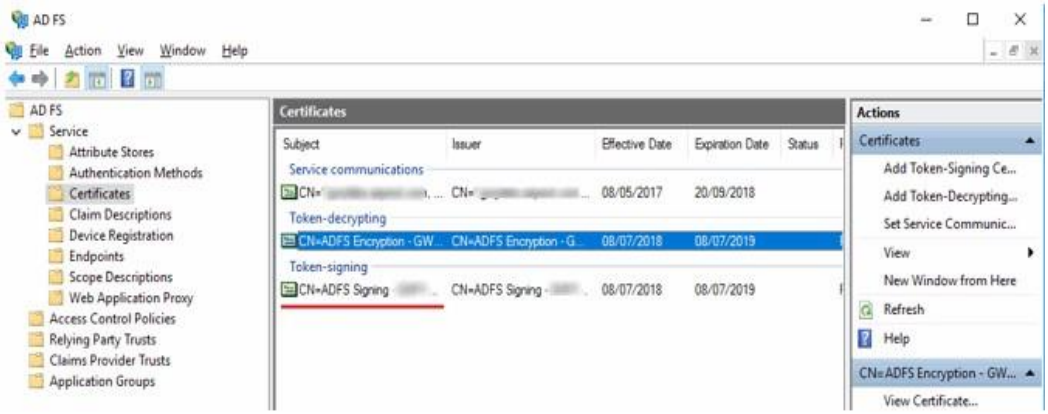
The AD FS Overview window opens.



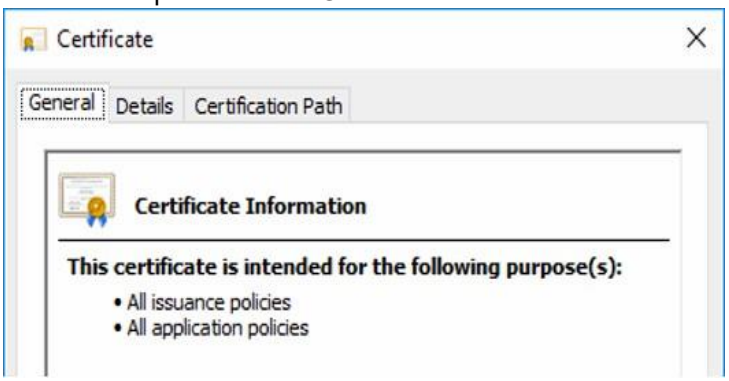
2. In the left pane, expand the **Services** directory.
3. Select the **Certificates** directory. The Certificates display in the middle pane.



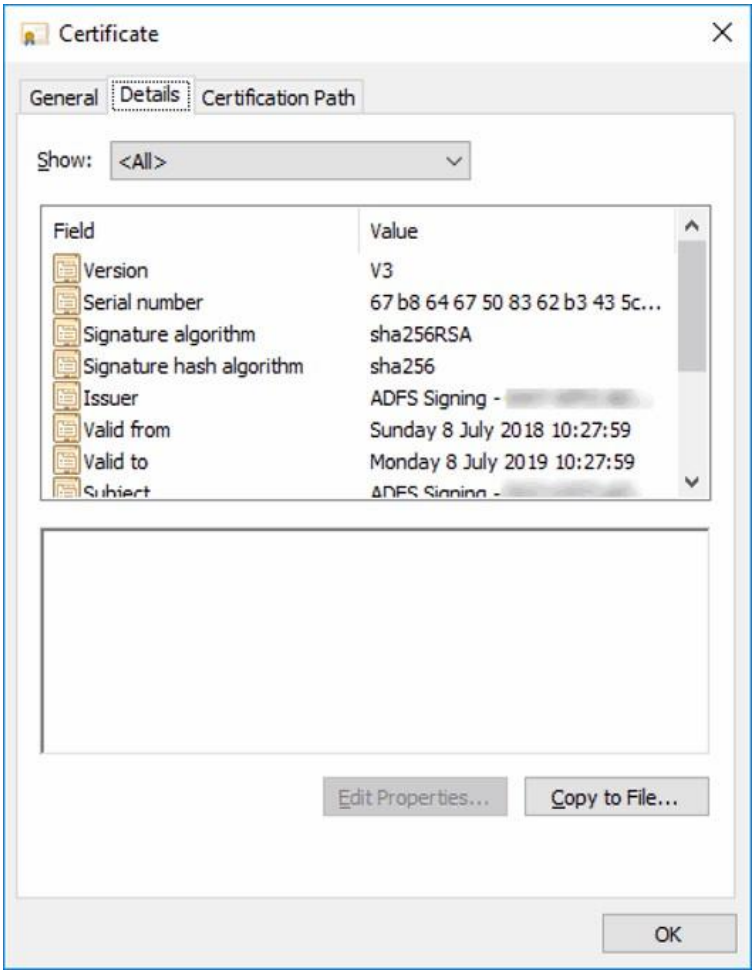
4. To open the certificate, in the Certificates list, identify the Token-signing certificate, and double-click it.



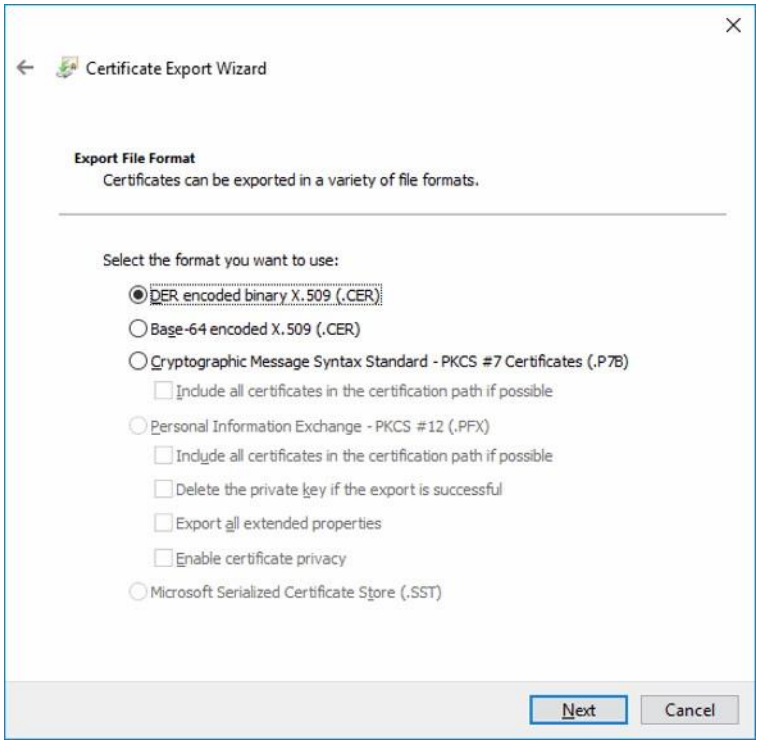
The Certificate window opens with the General tab active.



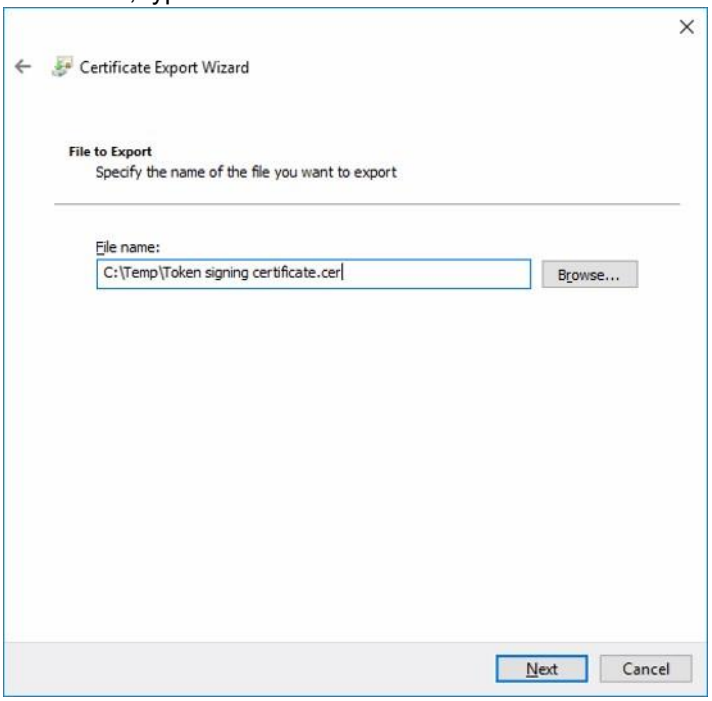
5. To view the certificate details, select the **Details** tab.



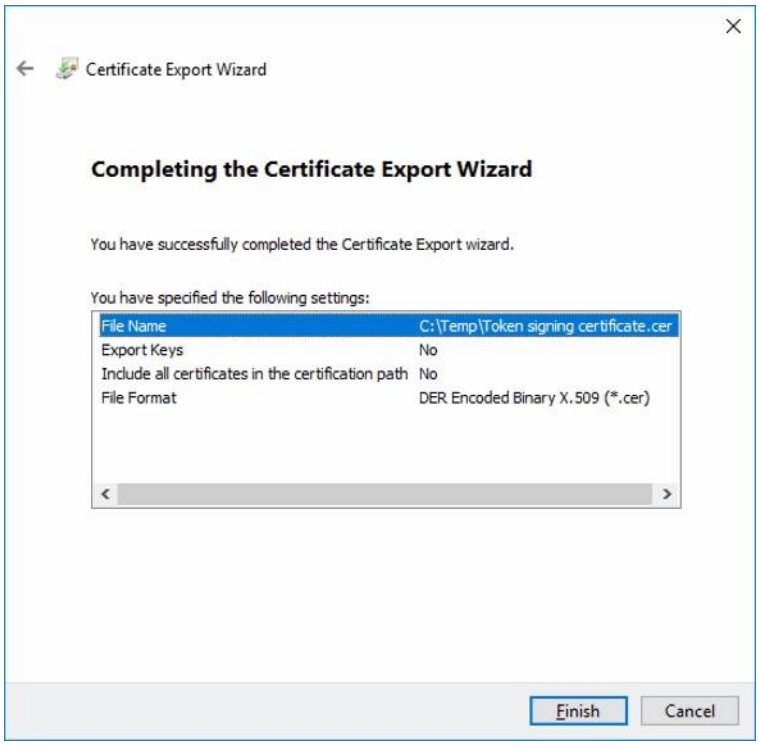
6. To export the Token-signing certificate, click **Copy to File**. The Welcome to the Certificate Export Wizard window opens.



7. Click **Next**. The Export File Format window opens.
8. Select the **DER encoded binary X.509 (.CER)** option.
9. Click **Next**. The File to Export window opens.
10. In the File name text box, type a file name.

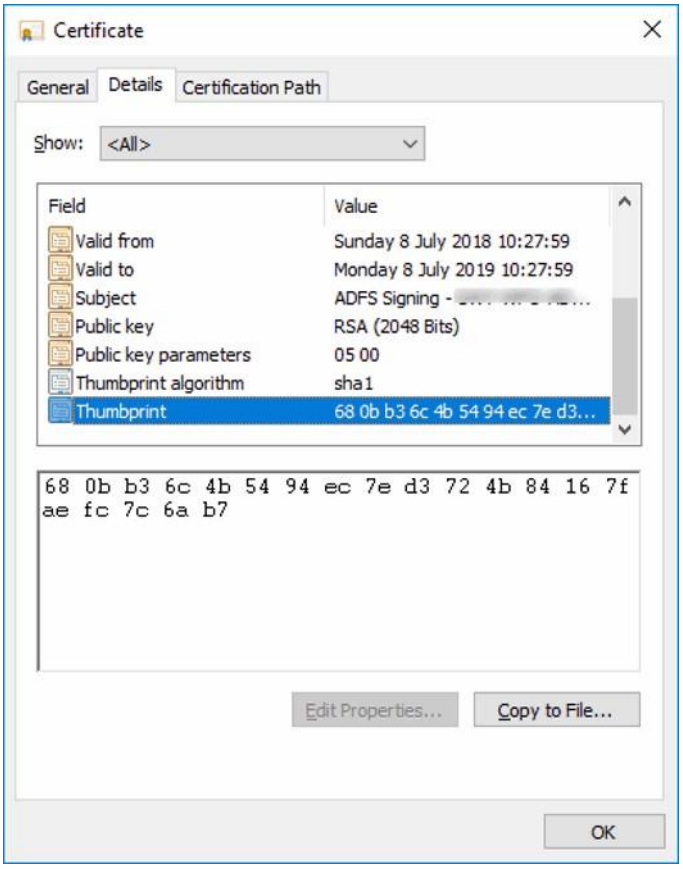


11. Click **Next**. When the export is finished, the Completing the Certificate Export Wizard window opens.

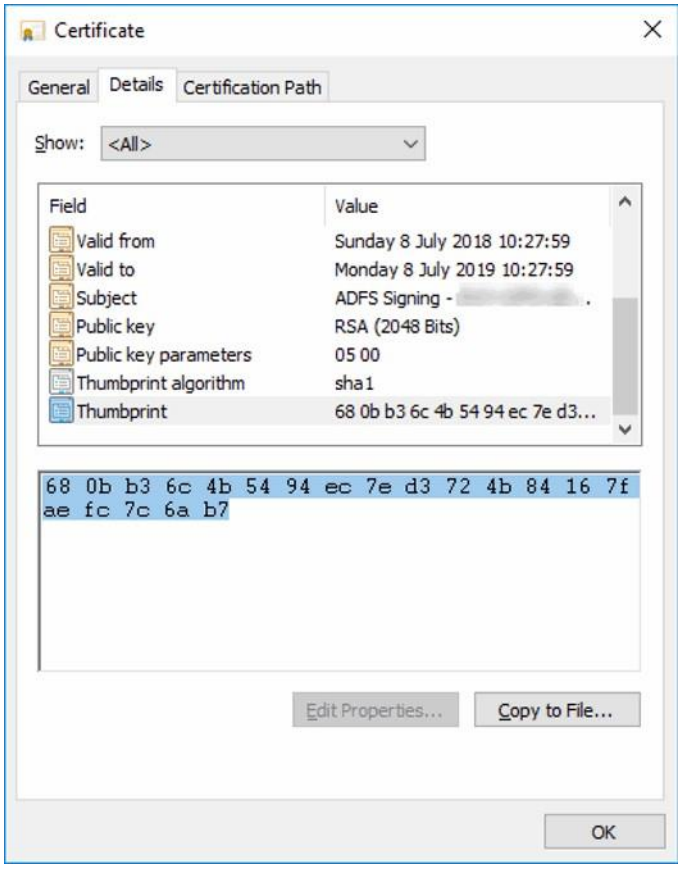


12. Click **Finish**. The Certificate Export Wizard closes and the Certificate window displays with the Details tab active.

13. Scroll down the list box and select **Thumbprint**.



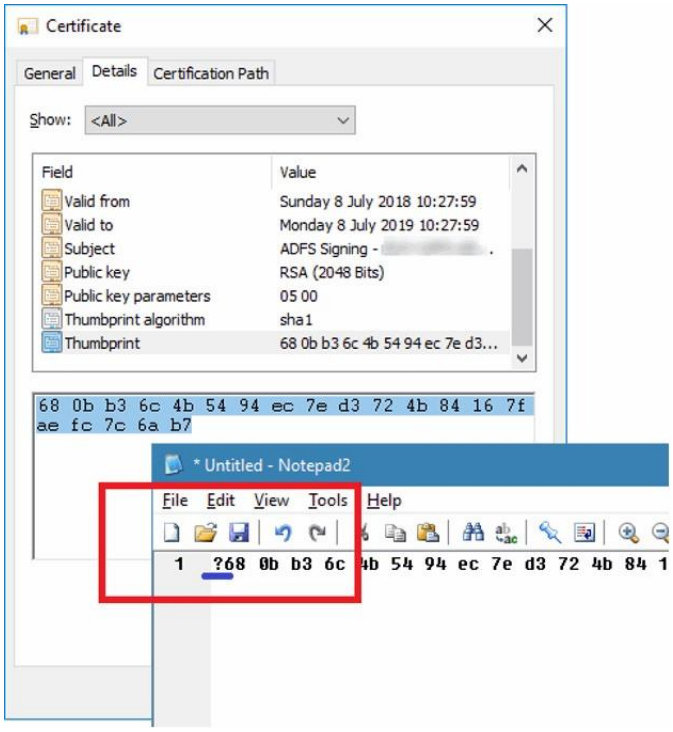
14. In the text box at the bottom of the window, select the Thumbprint text.



15. Copy the text by pressing **Ctrl+C**.
16. Launch Notepad2 or Notepad++.

    Note: Do **not** use the version of Notepad that comes with Windows because a necessary leading character is hidden from you in that version.

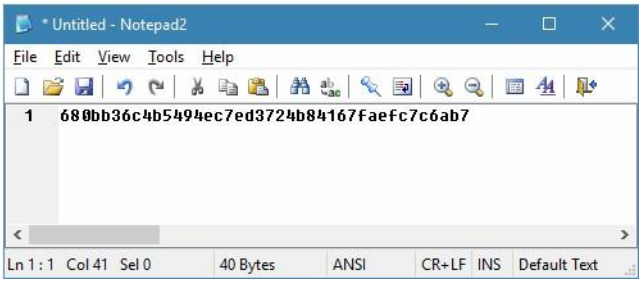
17. Paste the text by pressing **Ctrl+V**.



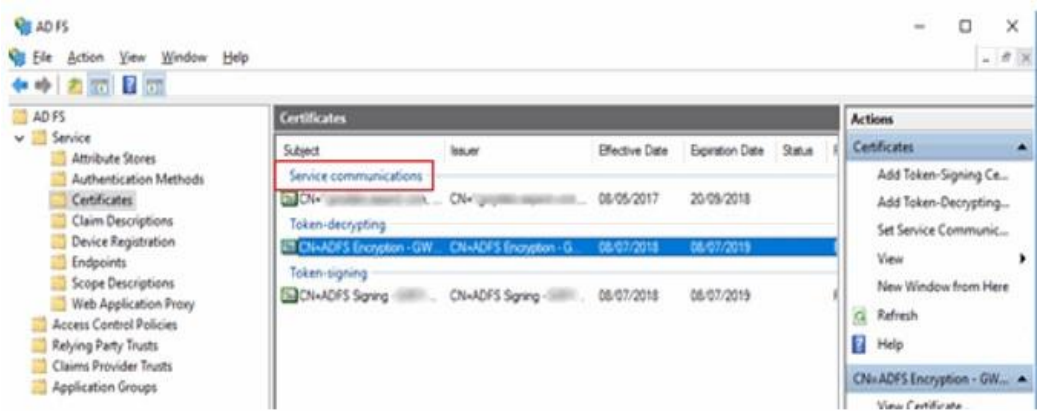
There is an extra, unexpected character in the text. This character causes problems if you do not remove it. The white space and lower case letters also cause problems.

18. Therefore,
    a. Remove the extra character.
    b. Remove all the white space.
    c. Capitalize all the letters.

    The result looks similar to the following:



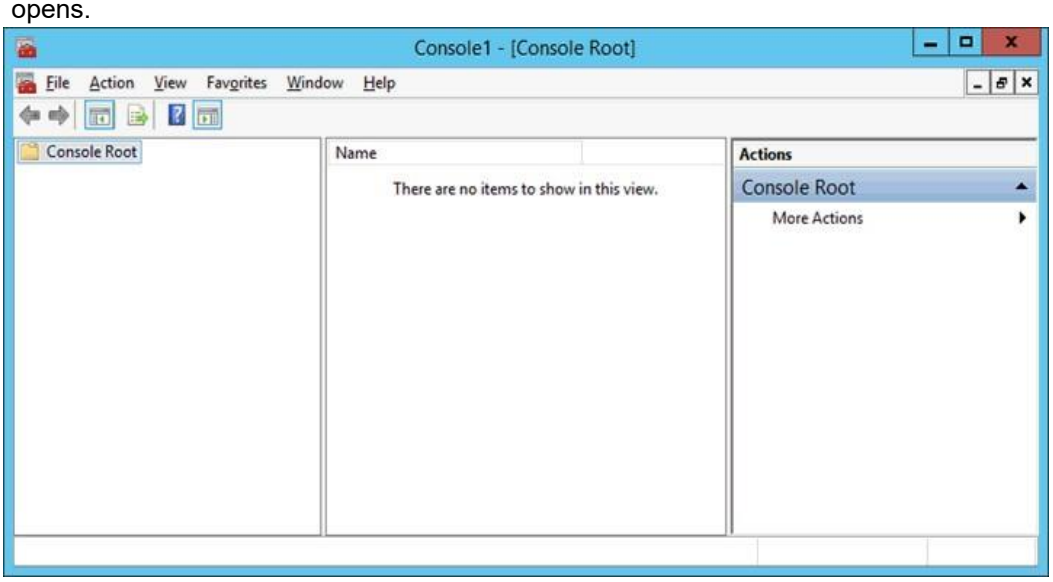
19. Because you need this file later in the procedure, save the file by selecting **File>Save**.
20. Repeat steps 4 through 12 to export the Service Communication certificate.



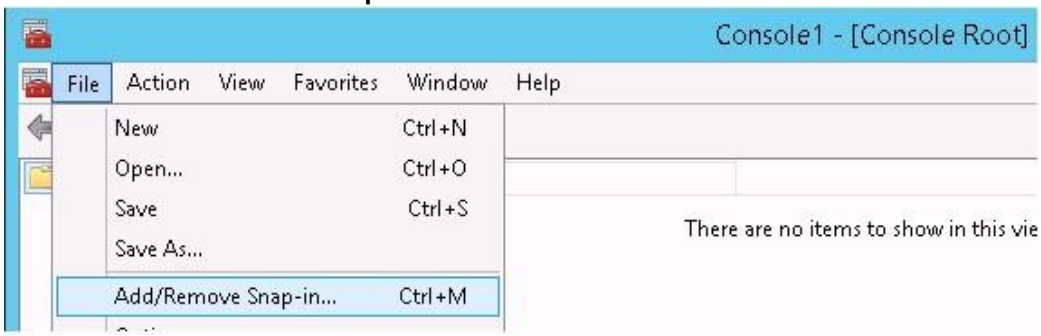
C.4.4 Install the ADFS Certificates

Perform these procedures on each Aspect Workforce Engagement Management server with back-end services (Workforce, Quality, and Performance).

1. Launch Microsoft Management Console by running **mmc.exe**. The Console window opens.



2. Select **File>Add/Remove Snap-in**.

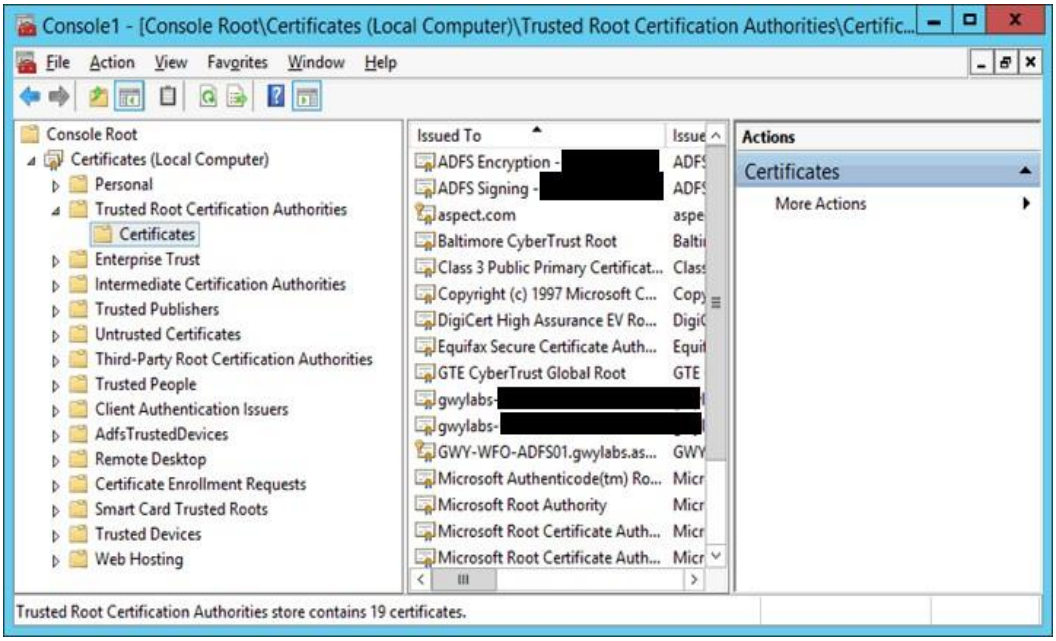


The Add or Remove Snap-ins window opens.

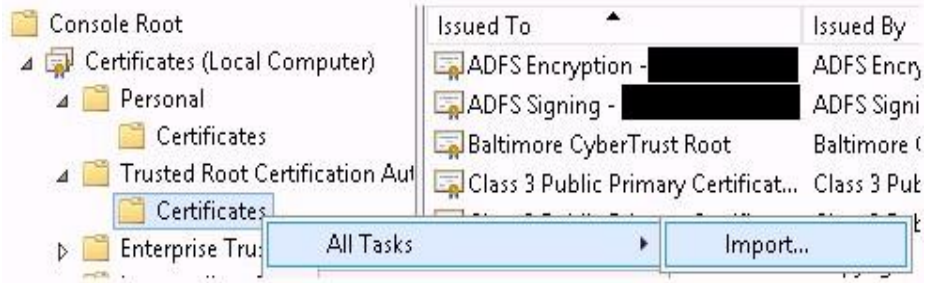
3. In the Available snap-ins list box, select **Certificates**.
4. Click **Add**. The Certificates snap-in window opens.
5. Select the **Computer account** option.

6. Click **Next**.The Select Computer window opens.
7. Select the **Local computer** option.

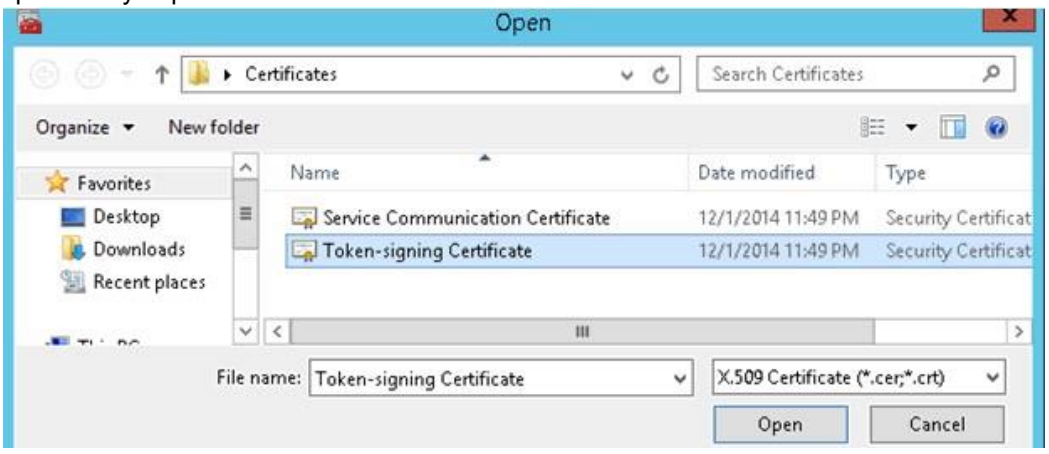
8. Click **Finish**. The Select Computer window closes and the Add or Remove Snap-ins window is active.
9. Click **OK**. The Add or Remove Snap-ins window closes and the Microsoft Management Console window is active.
10. In the left pane, expand the **Trusted Root Certification Authorities** directory.
11. Select the **Certificates** directory.



12. Right-click the Certificates directory and select **All Tasks>Import**.



13. A window opens, from which you can browse to the **Token-signing Certificate** that you previously exported.



14. Click **Open**. The Certificate Import Wizard window opens.

15. Select the **Place all certificates in the following store** option.

16. In the Certificate store text box, select **Trusted Root Certification Authorities**.

17. Click **Next**.
18. Click **Finish**. The Certificate Import Wizard window closes and the Microsoft Management Console window is active.
19. Repeat steps 11 through 18 to install the **Service Communication** certificate.

C.4.5 Claims-based Authentication for Workforce Management

To configure the Authentication tab for Workforce Management, follow the instructions in Authentication Tab on page 5-43.

C.5 Claims-based Authentication for Quality Web Services in Quality

Configuring claims-based authentication for Quality Web Services depends on completion of the following.

C.5.1 Modify the Quality Web Services web.config

Perform these procedures on the Quality Web Services server.

1. Open the web.config file by navigating to the installation folder for the Quality Web Services, which is typically

   C:\Program Files (x86)\Alvaria Software\AQM\Quality.WebServices

2. Change the authentication mode from Windows to None, for example:

```
<httpRuntime targetFramework="4.5" />
<authentication mode="None" />
 <authorization
```

3. Search for **identityConfiguration** section which is located in the system.identityModel section.
4. On the identityConfiguration element, ensure that the attribute **saveBootstrapContext** with a value of **false** is present. For example:

   <identityConfiguration saveBootstrapContext=”false”>

5. Add the following content directly beneath the **claimsAuthenticationManager** section:

```
<audienceUris>
  <add value="https://wfowebserver.domain.com/" />
  <add value="https://qualitywebserver.domain.com/" />
</audienceUris>
<certificateValidation certificateValidationMode="None" />
```

```
<issuerNameRegistry
type="System.IdentityModel.Tokens.ConfigurationBasedIssuerNameRe
gistry, System.IdentityModel, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=b77a5c561934e089">
  <trustedIssuers>
    <add thumbprint="12963382EFD52A9737BAA026DAE2AF9DC7E9033E"
name="http://adfsserver.domain.com/adfs/services/trust" />
  </trustedIssuers>
</issuerNameRegistry>
<securityTokenHandlers>
  <remove
type="System.IdentityModel.Tokens.SessionSecurityTokenHandler,
System.IdentityModel, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=b77a5c561934e089" />
  <add
type="System.IdentityModel.Services.Tokens.MachineKeySessionSecu
rityTokenHandler, System.IdentityModel.Services,
Version=4.0.0.0, Culture=neutral,
PublicKeyToken=b77a5c561934e089" />
</securityTokenHandlers>
```

6. The relevant places that you must update are:
   a. In the **audienceUris** section, the first value must be the FQDN of the Workforce Engagement Management UI web server.

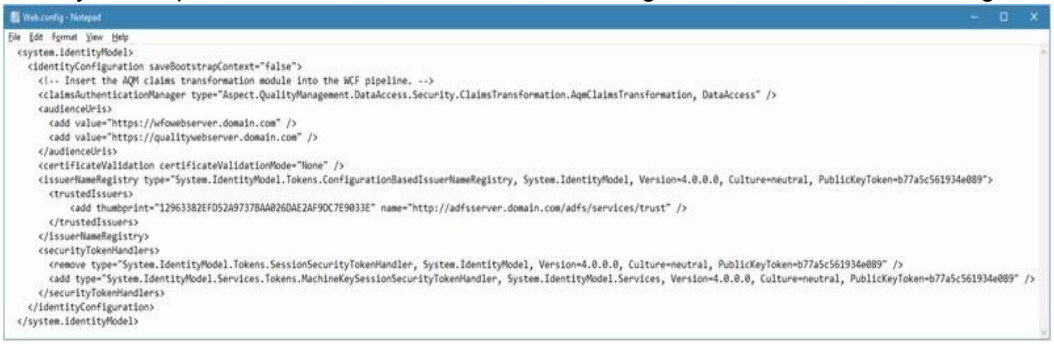
      The second value must be the FQDN of the Quality Web Services server.

      Note: The URLs are case sensitive and must contain a trailing forward slash.

   b. In the **trustedIssuers** section, the thumbprint must be thumbprint of the token signing certificate that you previously exported.

      The **name** must be the FQDN of the ADFS server with the trailing path /adfs/services/trust.

   After you complete these modifications, the web.config looks similar to the following:



7. Directly beneath the system.identityModel section, add the **system.identityModel.services** section:

```
<system.identityModel.services>
  <federationConfiguration>
```

```
    <cookieHandler requireSsl="true" />
    <wsFederation passiveRedirectEnabled="true" issuer="https://
adfsserver.domain.com/adfs/ls/" realm=" https://
wfowebserver.domain.com/" requireHttps="true" />
  </federationConfiguration>
</system.identityModel.services>
```

8. The relevant places that you must update are:
   a. In the **wsFederation** section, the **issuer** must be the FQDN of the ADFS server with the trailing path
      `/adfs/ls/`
   b. The **realm** must be the FQDN of the Workforce Engagement Management UI web server.

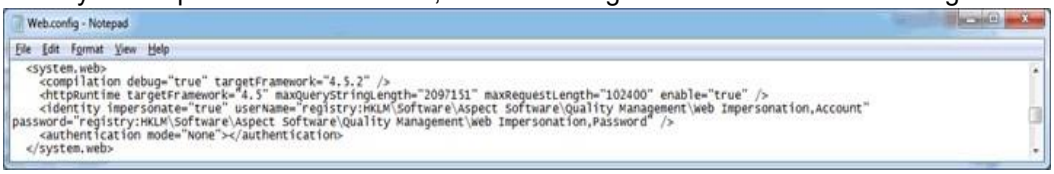
      Note: The URL is case sensitive and must contain a trailing forward slash.

   After you complete these modifications, the web.config looks similar to the following:

9. Directly beneath the **identity** section which is inside the **system.web** section, add the authentication section:

```
<authentication mode="None"></authentication>
```

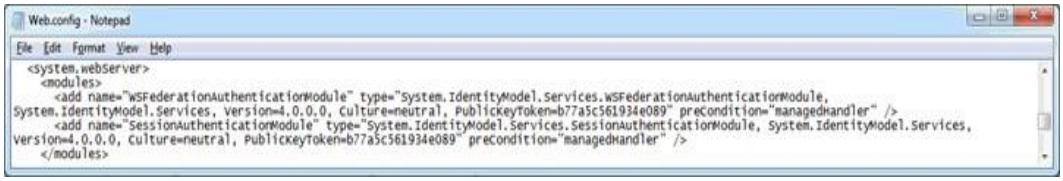
   After you complete this modification, the web.config looks similar to the following:



10. Inside the **system.webServer** section, add the **modules** section at the beginning:

```
<modules>
  <add name="WSFederationAuthenticationModule"
type="System.IdentityModel.Services.WSFederationAuthenticationMo
dule, System.IdentityModel.Services, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b77a5c561934e089"
preCondition="managedHandler" />
  <add                          name="SessionAuthenticationModule"
type="System.IdentityModel.Services.SessionAuthenticationModule
,         System.IdentityModel.Services,         Version=4.0.0.0,
Culture=neutral,                PublicKeyToken=b77a5c561934e089"
preCondition="managedHandler" / >
</modules>
```

    After you complete this modification, the web.config looks similar to the following:



11. To save the changes that you made to the web.config file, select **File>Save**.

C.6 Claims-based Authentication for Performance Management

To configure the Performance Management Web API Web Config file, perform the following:

Note: This needs to be done on each Performance Management Application Server.

Warning: Modifying the web.config file and leaving it in an invalid state can stop Performance Management from working. Perform a backup before modifying the file, and also ensure that the XML syntax is correct, before saving the file.

1. Edit the Performance Management Web API web.config file, typically found under:

   C:\Program Files\Alvaria\Performance Management\Services\Web\Service Layer\<*InstanceName*>

   Where ***<InstanceName>*** is the name of the instance you are configuring. Typically, this is APM01.

2. Change the authentication mode from **Windows** to **None**, for example:

   <httpRuntime targetFramework="4.5" />

   <authentication mode="*None*" />

   <authorization>

3. Under the **modules** tags, add the following:

<modules>

<remove name="WebDAVModule" />

<remove name="OPTIONSVerbHandler" />

<add name="WSFederationAuthenticationModule" type="System.IdentityModel.Services.WSFederationAuthenticationModule, System.IdentityModel.Services, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" preCondition="managedHandler"/>

<add name="SessionAuthenticationModule" type="System.IdentityModel.Services.SessionAuthenticationModule, System.IdentityModel.Services, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" preCondition="managedHandler"/>

</modules

4. Under the **<identityConfiguration>** tag add the ***saveBootstrapContext="true"*** attribute and the following new tags.

   Adjust these values for your environment:

   - **<UIServer>** - The fully qualified name of the server that the Workforce Engagement Management UI is installed on.
   - **<APMServer>** - The fully qualified name of the server that the Performance Management application is installed on.
   - **<InstanceName>** - The name of the Performance Management instance. This is typically APM01.
   - **<ADFSServer>** - The fully qualified name of the ADFS server that is being used.
   - **<CertificateThumbprint>** - The thumbprint of the token server signing certificate being used.

   Note: The URI entered under the ***audienceUris*** must point to the Performance Management Application Server fully qualified domain name in a single server install, or the Network Load Balancer fully qualified domain name in a load balanced install. These must be an HTTPS connection. These must match the value used in the ADFS server and in IIS, and are Case Sensitive.

```
<system.identityModel>
  <identityConfiguration saveBootstrapContext="true">
<claimsAuthenticationManager
type="Alvaria.PM.Security.WebAPI.ApmClaimsAuthenticationManager,
Alvaria.PM.Security.WebAPI" />
  <claimsAuthorizationManager
type="Alvaria.PM.Security.WebAPI.ApmClaimsAuthorizationManager,
Alvaria.PM.Security.WebAPI" />
  <audienceUris mode="Always">
<add value="https://<UIServer>/WFO/" />
<add value="https://<APMServer>/APM/ServiceLayer/<InstanceName>/api/" />
  </audienceUris>
  <certificateValidation certificateValidationMode="None"/>

  <issuerNameRegistry
type="System.IdentityModel.Tokens.ConfigurationBasedIssuerNameRegistry,
System.IdentityModel, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=b77a5c561934e089">
    <trustedIssuers>
      <add thumbprint="<CertificateThumbprint>" name="https://<ADFSServer>/
adfs/services/trust" />
    </trustedIssuers>
  </issuerNameRegistry>
```

```
<securityTokenHandlers>
<add type="System.IdentityModel.Services.Tokens.MachineKeySessionSecurityTokenHandler, System.IdentityModel.Services, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
<remove type="System.IdentityModel.Tokens.SessionSecurityTokenHandler, System.IdentityModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
</securityTokenHandlers>
</identityConfiguration>
</system.identityModel>
```

5. Before the final closing **</configuration>** tag add the following values, adjusting them for your own environment:
   - **<ADFSServer>** - The fully qualified name of the ADFS server that is being used.
   - **<APMServer>** - The fully qualified name of the server that the Performance Management application is installed on.
   - **<InstanceName>** - The name of the Performance Management instance. This is typically APM01.

   Note: The URI entered under the **wsFederation** must point to the Performance Management Application Server fully qualified domain name in a single server install, or the Network Load Balancer fully qualified domain name in a load balanced install. This must be an HTTPS connection. This must match the value used in the ADFS server and in IIS, and is Case Sensitive.

```
<system.identityModel.services>
<federationConfiguration>
<cookieHandler requireSsl="true" />
<wsFederation passiveRedirectEnabled="true" issuer="https:// <ADFSServer>/adfs/ls/" realm="https://<APMServer>/APM/ ServiceLayer/<InstanceName>/api/" requireHttps="true" />
</federationConfiguration>
</system.identityModel.services>
</configuration>
```

6. Save and close the file.

About Aspect®

Aspect is dedicated to transforming the service economy by humanizing the workforce experience. Their WorkforceOS platform offers a robust workforce management solution that aligns employee preferences with business needs enhancing scheduling, predictive insights, and collaboration tools. Supported by its parent company, Alvaria Inc., which boasts over 50 years of leadership in workforce management technology, Aspect is a trusted partner for large global enterprises across key sectors, including financial services, airlines, automotive, insurance, retail, telecommunications, and utilities. The Aspect WorkforceOS stands out as the only culture-drive n WEM software designed to foster work-life balance while maximizing ROI for businesses. For more details, visit www.aspect.com