Aspect Workforce™ Installation Guide

25

RELEASE DATE: 11/7/2025 REVISED DATE: 5/26/2026

Rev B
January 22, 2026

Contents

Revision History

Date	Description	Section
11/7/2025	Rev A	• WEM/Workforce Cloud place limits on number of recipients on emails. This value is set in the MaxRecipientsPerEmail parameter. See section Setting Registry Parameters for SMTP for more information. • Microsoft Access Database Engine is no longer supported and is no longer a recommended install. See About Automatically Installed Components, Installing the Main Application Server for SQL Server, Installing Third-Party Components, Installing SQLite Driver, Before You Upgrade, and Upgrading User Workstations.
1/22/2026	Rev B	• Update RabbitMQ version. See Installing RabbitMQ using Chocolatey. • Minor formatting changes. • Addition of new columns to InContact Historical Connector reports.
5/26/2026	Rev C	• Updated Upgrade Considerations section to include latest version information.

About this Guide

This guide contains procedures for installing the Aspect Workforce™ software and optional features. Important related information can be found in the following documents:

- For background information about the installation process, see the *Aspect Workforce™ Planning Guide*.
- For product compatibility information, including supported versions of database platforms, operating systems, and third-party products, see the *Aspect Workforce™ Release Note.*
- For information about Training, Technical Support, commenting on the documentation, and a list of additional documentation see the appropriate product Release Notes documents available on the Aspect documentation portal.

Note: The instructions in this guide refer to the standard installation program provided by Aspect. If you are using a setup program provided by a third party, the name of the product or software distributor might not be the same as the names given in this guide.

Audience

This guide is intended for the installing engineer who understands the requirements, responsibilities, and critical dates related to the Aspect Workforce™ installation. It is assumed that the necessary planning and preparation for implementation has been completed prior to installing and configuring the Aspect Workforce™ software.

This guide is also intended for supervisors, call center agents, system administrators, or network administrators who are involved in installing and configuring the Aspect Workforce™ software on a workstation or a network.

Organization of this Guide

This guide is organized as follows:

- Aspect Workforce™ System Overview, provides information about Aspect Workforce™ systems, types of installations, order of installation tasks, and installation of optional features.
- Installation Overview, provides an overview of the Aspect Workforce™ system installation and configuration process.
- Pre-installation Overview and Initial Verification, provides information about completing preinstallation tasks as well as meeting database and third-party software requirements.
- Configuring SQL Server, provides information about database roles and user accounts, and procedures for manually and automatically configuring SQL Server for Aspect Workforce™. It also provides a procedure for importing a sample database.

- Configuring Oracle, contains information about database roles and user accounts, and procedures for manually and automatically configuring Oracle for Aspect Workforce™. It also provides a procedure for importing a sample database and describes passwords and Oracle roles.
- Installing the Main Application Server for SQL Server, contains information about installing and uninstalling the Aspect Workforce™ main application server in a SQL Server environment.
- Installing the Main Application Server for Oracle, contains information about installing the Aspect Workforce™ main application server in an Oracle environment.
- Installing and Configuring WFM Services, contains information about installing WFM services including the WFM Listen service, as well as explains the TCSSERVICES user account and how to configure WFM services.
- Installing a Secondary Application Server, describes the tasks you need to complete before installation, and provides information about using the installation wizard to install and uninstall the secondary application server.
- Configuring the Aspect Message Routing Service, describes how to install and configure the Aspect Message Routing Service for use in load balancing.
- Configuring AMR for Common Scenarios, provides detailed configuration information that you can use to implement common load balancing scenarios, such as distributed TallyServer and distributed Checker. You configure these scenarios with the Aspect Message Routing Service (AMR) Configuration Editor.
- Installing User Workstations, describes the tasks you need to complete before setting up the workstation, how to install and uninstall the user workstation, and also contains procedures for installing the user workstation from the command prompt.
- Installing with a Command Line, provides instructions for installing the Aspect Workforce™ client program on a user workstation using a command line.
- Installing the Client on Windows Terminal Server, describes the tasks you need to complete to set up the Windows Server 2022 and 2025 terminal server.
- Installing the Client in a Citrix Environment, describes the steps required to install the Aspect Workforce™ client program in a Citrix environment.
- Post-Installation Administrative Tasks, provides information about administrative tasks to complete after you install Aspect Workforce™ or upgrade to it from an earlier version.
- Upgrading for SQL Server provides information for SQL Server users who are upgrading Aspect Workforce™ from version 20.0 or later to this version of Aspect Workforce™.
- Upgrading for Oracle, provides instructions for Oracle users who are upgrading Aspect Workforce™ from version 20.0 or later to this version of Aspect Workforce™.
- Applying Workforce Updates, describes how to set up the optional feature that lets you export Aspect Workforce™ agent schedule information into a time and attendance system.
- Appendix A Installation Checklists, contains checklists for SQL Server and Oracle RDBMS's that you can use when installing and configuring Aspect Workforce™.
- Appendix B, File Installation Paths, contains location of the 32-bit and 64-bit files which depends on the installation path you select when installing Aspect Workforce™.

- Appendix C, Security Segregation for User Management, section highlights the security perspective by segregating the rights for business users from IT staff.
- Appendix D, IIS Logging, section provides a cursory overview of IIS and describes the basic settings that are often changed for Aspect Customer Care troubleshooting.

Aspect Workforce™ System Overview

This chapter provides an overview of the Aspect Workforce™ system.

About the System

This section contains information about the Aspect Workforce™ database server, main and secondary application servers, and client.

Database Server

The database server is an Aspect Workforce™ dedicated server that hosts the Oracle or SQL Server database for Aspect Workforce™. The database stores and validates all Aspect Workforce™ information.

Main and Secondary Application Servers

The main application server contains configuration components of the Aspect Workforce™ installation. It hosts one or more Aspect Workforce™ (WFM) system services. In large installations, secondary application servers connected through a LAN typically host various WFM system services.

The main application server exclusively:

- Hosts the installation database, which contains configuration data about installed applications and services.
- Runs the Information Server system service, which provides configuration information to all Aspect Workforce™ processes, secondary application servers, and clients.
- Hosts shared folders for installation points.
- The main application server and secondary application servers can both run the following:
- System services that interact with the Aspect Workforce™ client (specifically, Updater and Tally Server).
- System services that perform background processing, such as WFM AutoRun, WFM Checker, WFM Express Checker and WFM ACD Processing.

Client

The Aspect Workforce™ client is a Microsoft Windows application. It is the main program used to access the functionality of Aspect Workforce™. Using the client software, users can forecast call volume and staffing requirements, create schedules for their staff, and manage schedules.

The Aspect Workforce™ client accesses the database and performs processing locally for most tasks. Additionally, it communicates with the Updater and Tally Server processes running on the application server to enforce business rules for schedule changes.

Types of Installation

Depending on the size and specific requirements of your organization, you create one of the following Aspect Workforce™ installation configurations:

- **Standard Installation—**A standard installation includes a database server, main application server, and user workstations, all connected through a LAN. The main application server software includes all the necessary functionality of the secondary server software on a single machine.
- **Distributed Installation—**In a distributed installation, two or more machines serve as application servers. The main application server holds all the Aspect Workforce™ shared folders, including client setup files, and some Aspect Workforce™ system services.

  Other Aspect Workforce™ system services are installed on additional machines. For example, the Updater service might reside on one machine, with the Tally server service residing on another machine, and all other services on the main application server. For information about Aspect Workforce™ services, see the Aspect Workforce™ System Administrator Guide.
- **Multisite Installation—**In a multisite installation, one location houses the database server, application server, some user workstations, and possibly one or more ACDs. Additional user workstations and ACDs are set up at other locations. In this configuration, user workstations operate over the wide-area network (WAN) using Microsoft Terminal Services software.
- **Standalone Installation—**In a standalone installation, the database server software, application server software, and client software is installed on a single machine, which may or may not be connected to a network. The standalone installation can be used when the number of supported agents is small.

Installation Overview

This chapter provides an overview of the Aspect Workforce™ system installation and configuration process.

For a summary of the installation process, see the section appropriate to your installation:

New Installations

When installing Aspect Workforce™, you complete pre-installation, installation, and post-installation tasks. For details, see the section appropriate to your database.

For SQL Server

The following provides an overview of the Aspect Workforce™ installation process:

Complete pre-installation tasks listed in Pre-installation Overview.

Complete installation tasks:

a. Install the main application server software. See Installing the Main Application Server for SQL Server.

b. Configure your database for Aspect Workforce™ using the WFM Database Manager. See Creating and Configuring the Database.

c. Install and configure WFM system services. See Installing and Configuring WFM Services.

d. For distributed installations only: Install one or more secondary application servers. See Installing a Secondary Application Server.

e. For all installations except standalone: Install the Aspect Workforce™ client software on user workstations. See Installing User Workstations.

f. If accessing Aspect Workforce™ over a LAN or WAN: Ensure access to Windows Remote Desktop Services (RDS) from workstations to the remote desktop server and install the Aspect Workforce™ client software on the remote desktop server. See Installing the Client on Windows Terminal Server.

Complete post-installation tasks. See Post-Installation Administrative Tasks.

For Oracle

The following provides an overview of the Aspect Workforce™ installation process:

1. Complete pre-installation tasks listed in Pre-installation Overview.
   a. Install the main application server software. See Installing the Main Application Server for Oracle.

b. Configure your database for Aspect Workforce™ using the WFM Database Manager. See Creating and Configuring the Database.

c. Install and configure WFM system services. See Installing and Configuring WFM Services.

d. For distributed installations: Install one or more secondary application servers. See Installing a Secondary Application Server.

e. For all installations except standalone: Install the Aspect Workforce™ client software on user workstations and terminal servers. See Installing User Workstations.

f. If accessing Aspect Workforce™ over a LAN or WAN: Ensure access to Windows Remote Desktop (RDS) from workstations to the remote desktop server and install the Aspect Workforce™ client software on the remote desktop server. See Installing the Client on Windows Terminal Server.

2. Complete post-installation tasks. See Post-Installation Administrative Tasks.

Upgrade Considerations

If you are upgrading Aspect Workforce™, Upgrading for SQL and Upgrading for Oracle discuss upgrade procedures for SQL Server and Oracle deployments. One of these procedures involves upgrading the RDBMS itself to the following versions:

- SQL 2022
- Oracle 19c

Note: For compatibility information regarding RDMBS release levels, see the *Aspect Workforce™ Release Note* (Compatible Database Platforms section).

Some WFM services will require installation of the RabbitMQ message broker service. See RabbitMQ for use cases and instructions.

Before you upgrade Aspect Workforce™, be aware of the following considerations. All these topics are discussed in detail in the respective upgrade chapters. Briefly, these new considerations are the following, grouped by the Aspect Workforce™ version that you are upgrading from.

Note about the SQL Native Client

With Aspect Workforce™ 22, the SQL Native Client has been deprecated. You must download and install the Microsoft OLE DB **Driver** for SQL Server.

Note: This is NOT the same as the Microsoft OLE DB **Provider** for SQL Server.

You will need to download the latest **Driver** from the Microsoft website. See Installing the Client Software.

Once installed, wither you are upgrading on existing or new hardware, the database alias will need to be configured to utilize the new **Driver**. See Configuring an Existing or Sample Database.

From Aspect Workforce™ 22 and Later

You can directly upgrade both the Aspect Workforce™ software and the Aspect Workforce™ database schema from 22 or later to 25.

If you are upgrading from Aspect Workforce™ 22 or later, you must understand the following:

- (SQL Server Users Only) Upgrade to SQL Server 2022—Aspect Workforce™ 25 supports SQL Server 2022 only. If required, upgrade SQL Server by running the SQL Server 2022 installation program.
- (Oracle Users Only) Upgrade to Oracle 19c—Aspect Workforce™ 25 supports Oracle 19c only. If required, upgrade your Oracle database server to 19c.

 **Note**: You must install both the 32-bit and the 64-bit Oracle clients on all application servers. Client workstations only require the 64-bit client.

From Aspect Workforce™ 21.1 and Earlier

Aspect supports direct *database schema* upgrades from Aspect Workforce™ 21.1 to Aspect Workforce™ 24. Aspect supports direct *software* upgrades from Aspect Workforce™ 22 and later to Aspect Workforce™ 25. To upgrade version 21.1 software to version 25, you must first either upgrade the software to 22 and then upgrade the software to version 25 or uninstall 21.1 and install version 25. If you are upgrading from an earlier version, you must uninstall your current version and install version 25.

If you are upgrading from Aspect Workforce™ 21.1 or earlier, you must understand the following:

- **(SQL Server Users Only) Upgrade to SQL Server 2022** - Aspect Workforce™ 25 supports SQL Server 2022 only. Upgrade SQL Server by running the SQL Server 2022 installation program.
- **(Oracle Users Only) Upgrade to Oracle 19c -** Aspect Workforce™ 25 supports Oracle 19c only. Upgrade your Oracle database server to 19c.

 **Note**: You must install both the 32-bit and the 64-bit Oracle clients on all application servers. Client workstations only require the 64-bit client.

Upgrade Compatibility Verification Tool

Before upgrading the software, you must run the Aspect Workforce™ Upgrade Compatibility Verification Tool.

Using the tool helps to resolve perceived conflicts and redundancies which may be present in the legacy database. For more information, see Running the Verification Tool for Oracle and Running the Verification Tool for SQL Server.

Installing Optional Features

You can also install the following optional features of Aspect Workforce™:

- **Tally Server and Checker Load Balancing**—Your Aspect Customer Care representative can help you determine whether these features would be of use to you. For setup instructions, see Configuring

the Aspect Message Routing Service and Configuring AMR for Common Scenario Scenarios. For background information, see the *Aspect Workforce™ Planning Guide.*

- **RabbitMQ**–Some optional features of the Aspect Workforce™ suite, such as emailing reports, RTA Web or Mobile and Universal Notifications, require RabbitMQ. For more information, see RabbitMQ, the Empower Installation Guide, and the Workforce Engagement Management Installation Guide.

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™ and for related procedures.

The table below describes the actions required to perform common installation-related procedures in Aspect Workforce™.

Installation-related procedure	Action Required
Installing	Launch **Setup.exe** from the Aspect Workforce™ software CD. When installing with the command line, launch the command window using the **Run As Administrator** option.
Upgrading	Launch **Setup.exe** from the Aspect Workforce™ software CD. When installing with the command line, launch the command prompt with administrative privileges.
Adding features after initial installation	Launch **Setup.exe** from the Aspect Workforce™ software CD and select **Modify** in the Program Maintenance dialog box. When installing with the command line, launch the command prompt with administrative privileges. **Note:** You cannot make changes using **Control Panel > Programs > Programs And Features**.

Repairing	Launch **Setup.exe** from the Aspect Workforce™ software CD and select **Repair** in the Program Maintenance dialog box. When installing with the command line, launch the command prompt with administrative privileges.  **Note:** You cannot repair using **Control Panel > Programs > Programs And Features**.
Uninstalling	Do either of the following: • Launch **Setup.exe** from the Aspect Workforce™ software CD and select the **Remove** option. • In the Windows Control Panel, go to **Programs > Programs And Features**. Select **Workforce** in the list of programs 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.

Pre-installation Overview and Initial Verification

This chapter provides pre-installation information for Aspect Workforce™.

Pre-installation Overview

Before you install Aspect Workforce™, complete the following tasks:

1. See the *Aspect Workforce™ Release Note* for any new requirements or procedures. Especially review the sections about compatibility and implementation.
2. **Complete an installation checklist**. See Appendix A: Installation Checklists.
3. **Set up the recommended installation accounts**. See Setting Up Installation Accounts.
4. **Verify OS requirements**. See Meeting OS Requirements.

5. **Set up the database environment** for Aspect Workforce™. See Configuring SQL Server, or Configuring Oracle, depending on your database type., depending on your database type.
6. **Configure a physical SMTP server** for report-handling. See Configuring the SMTP Server.

Setting Up Installation Accounts

All Aspect Workforce™ applications should be installed with user accounts that are:

- Domain accounts, *and*
- Local administrators on all Aspect Workforce™ servers in your deployment Work with your network administrator to set up these accounts.

Meeting OS Requirements

This section describes Aspect Workforce™ requirements that relate to the Microsoft operating system.

See “System Requirements,” in the *Aspect Workforce™ Planning Guide* for detailed information about hardware and operating system requirements.

Verifying Installation of OS Service Packs

Depending on your operating system, Aspect Workforce™ may require a specific Windows service pack for the OS. Service packs may be required for the application server, database server, and user workstations. For a list of required service packs for each supported operating system, see the *Aspect Workforce™ Release Note.*

To check the OS version and service pack, open a command prompt and enter **winver**.

About Automatically Installed Components

If you use the installation wizard to install the main application server, secondary application server, or user workstation, the installation wizard automatically checks for the following components and installs them if they are not present. You do not need to install these components yourself:

- Microsoft .NET Framework 4.8
- Microsoft Visual C++ 2017 Redistributable packages (x86 and x64)
- SQLite ODBC Driver for Win64 (used for Workforce report functionality)
- SQLite ODBC Driver, 32-bit, version 3.50.4 (new in Workforce 25)

If you are using the command line installation instead of the wizard, some of these components must be installed manually. For more information, see Installing with a Command Line.

For the installed version or versions of the components listed above, see the *Aspect Workforce™ Release Note.*

Configuring the SMTP Server

An SMTP server is required for exporting reports to email from Aspect Workforce™. The SMTP server requirements changed with the Aspect Workforce™ 21.1 release in that only *explicit* encryption is supported.

Work with your IT department to:

- Obtain the IP address of your SMTP server, and the username and password of a currently valid email account that is dedicated for use by Aspect Workforce™.
- Configure the SMTP server to accept connections from the server where the Notification Queue Manager service is installed. This server is typically the Aspect Workforce™ main application server.
- Decide whether to use encryption when exporting reports to email.

Configuring for Explicit Encryption

Notification Queue Manager supports *explicit* encryption in which servers connect to each other on an unencrypted channel and then negotiate an encrypted connection. To use certificate-based encryption between Notification Queue Manager and an SMTP server using explicit encryption, configure your server to offer the STARTTLS option on port **25** if encryption is not needed or port **587** if encryption is required.

Configuring SQL Server

This chapter contains information about setting up the SQL Server database server for Aspect Workforce™.

Note: To proceed with the setup process, you must have system administrator access to the SQL Server database server.

About the Requirements

When using the SQL Server option, the database server runs the SQL Server database software and stores the Aspect Workforce™ data.

To avoid conflicts, Aspect recommends the SQL Server software reside on a dedicated server that runs only databases that are used with Aspect Workforce™.

Aspect recommends a minimum of five separate disk drives, either single non-RAID drives or separate RAID arrays. For questions about RAID, contact your Aspect Customer Care representative.

Each disk drive requires NTFS formatting. Also, unless you have battery-powered write cache, Microsoft recommends that you disable disk write caching. For details about how to do this, consult the documentation for your operating system or disk drive.

To see the recommended use for each disk drive on your database server, see the document, *Aspect Workforce™ Hardware Recommendations*.

Installing and Configuring SQL Server

Aspect Workforce™ requires SQL Server 2022, which must be installed on the database server that you plan to use for Aspect Workforce™.

After installing SQL Server, configure it for use with Aspect Workforce™ as described in this procedure. Settings not specifically described here depend on the requirements of your organization.

Note: Install all Windows Updates on the database server before installing SQL Server 2022. To check for updates in Windows Server 2022 and 2025, select **Start > Settings (Cog Wheel) > Update and Security > Check For Updates.**

To install and configure SQL Server 2022:

1. Launch the setup program for **SQL Server 2022** on the database server. After preliminary processing, the **SQL Server Installation Center** window opens.
2. On the left of the window, click **Installation**.
3. On the right, click New SQL Server Stand-Alone Installation Or Add Features To An Existing Installation. (If upgrading SQL Server from an earlier version, click Upgrade from a previous version

   of SQL Server, and proceed as directed by the wizard. None of the steps in the upgrade process require special configuration for Aspect Workforce™.) Preliminary processing begins to run.
4. In the **Product Key** window, enter the **product key** if it does not prepopulate, and click **Next**.
5. In the **License Terms** window, select the check box to accept the license terms, and click **Next**.
6. In the **Microsoft Update** window, select the **check box** to check for updates or leave the box unchecked, according to your preference, and click **Next**. Several processes run automatically. The Feature Selection window opens.
7. Configure the **Feature Selection** window as follows:

- Under Instance Features, select Database Engine Services.
- Under **Shared** Features, select Client Tools Connectivity

8. Click **Next**. The Feature Rules window opens, checks the required rules, and displays the results in the window.

   If any rule failed, click the **Failed** link for instructions, and install the required software. Then, in the Feature Rules window, click **Re-run** to verify that the required software was installed successfully.
9. In the **Instance Configuration** window, accept the default settings, or make the desired changes to them, and click **Next**.
10. In the **Server Configuration** window, on the **Service Accounts** page, do one of the following:

- Accept the default account settings that are displayed, or
- Configure the accounts as desired.

11. Click the **Collation** tab.
12. Next to the **Database Engine** field, click **Customize**.

13. Select the radio button for Windows Collation Designator And Sort Order.
14. In the **Collation Designator** drop-down list and in the check boxes that follow, make the following selections based on your locale. (For more information about this step, see Notes on the Collation Designator).
    - For English (US), Brazilian Portuguese, French (France), French (Canadian), German, and Spanish installations:
    - In the Collation Designator field, select **Latin1_General_100** from the drop-down list.
    - Select the check boxes for **Case-sensitive** and **Accent-sensitive**.
    - For **Japanese** installations:
    - Select Japanese_Unicode.
    - Select Case-sensitive, Accent-sensitive, Kana-sensitive.
    - For **Korean** installations:
    - Select **Korean_100** in the list.
    - Select the check boxes for Case-sensitive, Accent-sensitive, and Kana-sensitive.
    - For **Russian** installations:
    - Select **Cyrillic_General_100** in the list.
    - Select the check boxes for Case-sensitive, Accent-sensitive, and Kana-sensitive.
    - For **Simplified Chinese** installations:
    - Select Chinese_Simplified_Pinyin_100 in the list.
    - Select the check boxes for Case-sensitive, Accent-sensitive, and Kana-sensitive.
    - For **Traditional Chinese** installation:
    - Select Chinese_Taiwan_Bopomofo_90 in the list.
    - Select the check boxes for Case-sensitive, Accent-sensitive, and Kana-sensitive.
15. Click **OK** and click **Next**.
16. In the **Database Engine Configuration** window, first set up SQL Server administrators by configuring the **Server Configuration** page:
    a. In the **Authentication Mode** section, select the radio button for **Mixed Mode**.
    b. In the **Specify The Password** field, type the desired **password** in both password fields.
    c. In the **Specify SQL Server Administrators** section, add administrators by doing one of the following:

- Click **Add Current User** to add the user who is currently logged into the server.
- Click Add to select a user.

  SQL Server administrators can be set up only by using this page.

17. On the **Data Directories** page, accept the default paths, or click the browse button to select another directory.

For more information, see About the Requirements.

18. On the **TempDB** page, accept the defaults, or change the TempDB configuration as needed.
19. On the **FILESTREAM** page, clear any check boxes that are selected, and click **Next**. A few processes run automatically, after which the **Ready To Install** window is displayed.
20. In the **Ready To Install** window, verify the features to be installed, and click **Install**. The **Installation Progress** window opens.
21. When the setup process is complete, the **Complete** window opens, showing information about the installation.
22. Click **Close**. SQL Server as been installed successfully.

Installing SQL Server Management Studio

After installing SQL Server 2022, you can download and install SQL Server Management Studio from the Microsoft website. No specific configuration is required for Aspect Workforce™ when installing SQL Server Management Studio

To install:

1. Launch the setup program for **SQL Server 2022** on the database server. After preliminary processing, the **SQL Server Installation Center** window opens.
2. On the left of the window, click **Installation**.
3. On the right, click **Install SQL Server Management Tools.** A browser window launches.
4. Following the instructions in the webpage, download and install **SQL Server Management Studio**.

Note: You can download SQL Server Management Studio here.

Notes on the Collation Designator

Note the following when completing the step about the Collation Designator (see step 20, in the Installing and Configuring SQL Server section, above) Aspect Workforce™ requires a case-sensitive sort order. This can be set at the server level, using a SQL Server instance-wide setting, or it can be set at the database level, using a setting specific to the Aspect Workforce™ database. To implement the SQL Server Instance wide-setting, ensure that you select the appropriate collation settings (for example, “<server default>”) from the lists shown in the relevant step of the procedure.

- If you plan to enter data in multiple languages (such as English, Simplified Chinese, and German) in one database, set the Collation Designator to the primary language.

Installing the SQL Server Client Software

To communicate with your database application server and user workstation in your Aspect Workforce™ network requires Microsoft OLE DB **Driver** for SQL Server.

Note: This is NOT the same as the Microsoft OLE DB **Provider** for SQL Server that is provided automatically by Microsoft.

To install the Microsoft OLE DB **Driver** for SQL Server on your application servers and user workstations, download the latest supported version from the Microsoft OLE DB Driver for SQL Server web page available at the Microsoft Download Center, here.

On the web page, under the latest supported version click **Download x64 Installer.**

Note: Installation of the Microsoft Visual C++ Redistributable is a requirement of the Microsoft OLE DB **Driver** for SQL Server.

Note: The Microsoft OLE DB **Driver** for SQL Server needs to be installed and not the Microsoft OLE DB **Provider** for SQL Server.

Setting Up the SQL Database Server

This section explains how to set up the database server for Aspect Workforce™.

Setting Up the Aspect Workforce™ Database

After installing SQL Server on the database server, set up the Aspect Workforce™ database.

1. On the database server, log in to **SQL Server Management Studio** as the system administrator (**sa**) by completing the fields as follows, and click **Connect**:

- **Server Type:** Select Database Engine.
- **Server Name:** Browse to the database server, on the Local Servers page, under Database Engine.
- **Authentication:** Select SQL Server Authentication.
- **Login:** Type sa.
- **Password:** Type the password you set up when configuring SQL Server.

  For more information, see step 16 in the steps under Installing and Configuring SQL Server.

2. In the tree on the left, browse to **Security > Logins**.
3. Right-click the **Logins** folder, and select **New Login** from the shortcut menu.
4. Create a new login by completing the fields as follows:

- **Login Name**: Type a login name, such as **TCSDBOWNER**. (Preferably, use all uppercase letters.)

  Note: For convenience throughout this guide, we refer to the user who manages the Aspect Workforce™ database as TCSDBOWNER. But you can use any Login Name you choose. If you wish, you can use the sa (system administrator) account to manage the Aspect Workforce™ database. But if you do not want the Aspect Workforce™ database owner to have full access to the database server, create a different Login Name than sa.

- **SQL Server Authentication:** Select the **radio** button for this option.
- **Password:** Type a **password** for the Aspect Workforce™ database owner, such as tcsdbowner. (Preferably, use all lowercase letters.)
- Enforce Password Policy: Clear the check box.

Note: You do have the option to use a Windows account as the WFM owner. The steps that follow still apply.

5. In the **TCSDBOWNER** account that you are creating, click the **Server Roles** page on the left, and select the check boxes for the following roles:

- dbcreator
- public

6. Click **OK** to create the TCSDBOWNER account.
7. In the SQL Server Management Studio main window, right-click the **Databases** folder in the tree on the left.
8. Select New Database…
9. Select the **General Page,** and proceed as follows:
   a. Name the database **WFM** (or local equivalent).
   b. Set the database owner as **TCSDBOWNER** (or the login name for the database owner you created in Create a new).
   c. Configure the **WFM** data file (in the Database Files list) as follows:
   d. Set the Logical Name of the WFM file to WFM_DATA.
   e. Set the Initial Size of the database to **50 MB**.
   f. Set the Autogrowth setting to **By 10 Percent, Unlimited Growth**.
   g. Place the file on disk drive 5.

      For databases that need to be stored on more than one disk drive, you can also use files and filegroups. For more information about files and filegroups, download “SQL Server 2022 Documentation” from here. (Subject to change by Microsoft)
      For more information about setting up disk drives, see About the Requirements.

   Configure the **WFM log** file for transactions as follows:
   a. Set the Logical Name of the WFM_log file to WFM_LOG.
   b. Set the Initial Size of the transaction log files to 25 MB.
   c. Set the Autogrowth setting to By 10 Percent, Unlimited Growth.
   d. Place the file on disk drive **3**.

e. Configure an **WFM index file** as follows:

f. Click **Add,** and set the Logical Name to **WFM_INDEX**.

g. In the Filegroup column, use the drop-down list to select **<new filegroup>**.

h. In the New Filegroup dialog box, type a **filegroup name** (for example, INDEXES), and click **OK**. i.

Set the File Type to **Rows Data**.

j. Set the Initial Size of the index file to **50 MB**.

k. Set the Autogrowth setting to **By 10 Percent, Unlimited Growth**.

l. Place the file on disk drive **4**.

10. Select the **Options** page and proceed as follows.

a. If you did not configure an instance-wide collation setting for your locale (as described in Notes on the Collation Designator select the appropriate **Collation** setting:

- Western European (English (US), Brazilian Portuguese, French (France), French (Canadian), German, and Spanish): Latin1_General_100_CS_AS
- Japanese: Japanese_Unicode_CS_AS_KS
- Korean: Korean_100_CS_AS_KS
- Russian: Cyrillic_General_100_CS_AS_KS
- Simplified Chinese: Chinese_Simplified_Pinyin_100_CS_AS_KS
- Traditional Chinese: Chinese_Taiwan_Stroke_90_CS_AS_KS

b. In the **Recovery Model** field, select **Simple**.

Note: Unless your database administrator specifies otherwise, Aspect recommends the **Simple** Recovery Model method. For information about backup models you can use, see the SQL Server Books Online, typically available on the **Start** menu. If you do not have an on-site administrator, Aspect has specific recommendations for configuring automatic database backups.

Contact Aspect Customer Care for assistance. If your site has a SQL Server database administrator (DBA), ensure that the DBA selects, implements, tests, and troubleshoots a backup and recovery model to suit your business needs.

c. In the Compatibility Level field, select SQL Server 2022 (160).

d. Click **OK** to create the database.

Configuring the Aspect Workforce™ Database for SQL Server

After setting up the database server, you must configure the SQL server database to support Aspect Workforce™. The configuration process consists of the following:

- Configuring the database software.
- Setting database parameters.
- Creating standard database roles and users with default user names and passwords.

The configuration process can be completed using an automated script or completed manually, as described in the following sections.

Configuring with an Automated Script

You can configure the SQL Server database using an automated SQL script.

The script sets database properties, creates standard roles for your database, and creates users with default user names and passwords. If you want to use user names or passwords other than the default, edit the script before you run it.

Note: The application role passwords in this script must obey Windows security policy requirements. It is a best practice to modify these passwords. Please modify these default passwords in accordance with your policy. Later, you will use WFM Database Manager to make a corresponding change to the encrypted role password stored in the WFM database, using the Modify Application Role Password feature. For more information, see Changing Default Passwords.

To configure the SQL Server database using an automated script:

1. Insert the Aspect Workforce™ Software CD into the database server.
2. Log in to **SQL Server Management Studio** as a system administrator.
3. On the toolbar, click **New Query**.
4. From the drop-down list under the toolbar, select the **WFM** database.
5. Using the **Open File** toolbar button, load the script from the following location, where ***x*** is the letter of your CD drive: ***x*:\Utility\SQL Scripts\MSSConfigure2022.SQL**
6. Close any other **query windows** that are open.
    - Loading the SQL script sometimes opens another query window.
7. On the toolbar, click **Execute** to run the script. If the script runs successfully, you can view the new users in SQL Server Management Studio after pressing F5 to refresh the interface. View the new users (such as NOTF_USER and TCSADMIN) at the following path: ***db server*** **> Databases >** ***WFM db*** **> Security > Users**

    where:

- ***db server*** is the name of the server where SQL Server is installed
- ***WFM db*** is the name of your Aspect Workforce™ database

Configuring Manually

You can configure the SQL Server database manually using the SQL Server Management Studio.

To configure the SQL Server database manually:

1. From the Start menu, open SQL Server Management Studio by selecting **Start > Microsoft SQL Tools > SQL Server Management Studio**.
2. Log in as a system administrator. SQL Server Management Studio connects to your server.
3. In the toolbar, select the **New Query** button, and select the **WFM** database.
4. Set the **database properties** using the following query:

```
DECLARE @database NVARCHAR(128) SELECT
@database = DB_NAME()
exec ('ALTER DATABASE ' + @database + ' SET SINGLE_USER WITH ROLLBACK
IMMEDIATE')
exec ('ALTER DATABASE ' + @database + ' SET READ_COMMITTED_SNAPSHOT
ON')
exec ('ALTER DATABASE ' + @database + ' SET AUTO_CREATE_STATISTICS ON')
exec ('ALTER DATABASE ' + @database + ' SET AUTO_UPDATE_STATISTICS
ON') exec ('ALTER DATABASE ' + @database + ' SET ANSI_NULLS ON')
exec ('ALTER DATABASE ' + @database + ' SET ANSI_WARNINGS ON')
exec ('ALTER DATABASE ' + @database + ' SET CURSOR_CLOSE_ON_COMMIT
OFF') exec ('ALTER DATABASE ' + @database + ' SET QUOTED_IDENTIFIER
ON') exec ('ALTER DATABASE ' + @database + ' SET RECURSIVE_TRIGGERS
OFF')
exec ('ALTER DATABASE ' + @database + ' SET RECOVERY SIMPLE WITH
NO_WAIT') exec ('ALTER DATABASE ' + @database + ' SET
MULTI_USER') exec sp_dbcmptlevel @database, 160 exec ('ALTER
DATABASE ' + @database + '
SET QUERY_STORE = ON
 (OPERATION_MODE = READ_WRITE,
   CLEANUP_POLICY = (STALE_QUERY_THRESHOLD_DAYS = 30),
   DATA_FLUSH_INTERVAL_SECONDS = 900,
   MAX_STORAGE_SIZE_MB = 1024,
   INTERVAL_LENGTH_MINUTES = 15,
   SIZE_BASED_CLEANUP_MODE = AUTO,
   MAX_PLANS_PER_QUERY = 200,
   WAIT_STATS_CAPTURE_MODE = ON,
   QUERY_CAPTURE_MODE = CUSTOM,
   QUERY_CAPTURE_POLICY = (
     EXECUTION_COUNT = 30,
```

```
TOTAL_COMPILE_CPU_TIME_MS = 1000,
TOTAL_EXECUTION_CPU_TIME_MS = 100))')
```

5. Close the **New Query** window. (You do not need to save the query.)
6. Create Aspect Workforce™ **roles** and **logins** as follows:
   a. Create the TCS_UPDATER Application Role.:
      - Select **WFM database > Security > Roles**, right-click the **Roles** folder, and select **New Application Role** from the shortcut menu.
      - In the Role Name field, type **TCS_UPDATER**.
      - In the Default Schema field, type **dbo**.
      - In the Password and Confirm Password fields, type **tcs_updat3r**.

        The **tcs_updat3r** password, like the **tcs_cli3nt** password in step b, are default passwords. It is a best practice to modify these passwords. Note that the application role passwords must obey Windows security policy requirements. Please modify these default passwords in accordance with your policy. Later, you will use WFM Database Manager to make a corresponding change to the encrypted role password stored in the WFM database, using the Modify Application Role Password feature. For more information, see Changing Default Passwords.
      - Click **OK** to save the role.
   b. Create the **TCS_CLIENT** Application Role:
      - Select WFM database > Security > Roles, right-click the Roles folder, and select New Application Role from the shortcut menu.
      - In the Role Name field, type TCS_CLIENT.
      - In the Default Schema field, type dbo.
      - In the Password and Confirm Password fields, type **tcs_cli3nt**.
      - Click O**K** to save the role.
   c. Create the **TCS_UPDATER_DB** role in the WFM database:
      - Select WFM database > Security > Roles, right-click the Roles folder, and select New Database Role from the shortcut menu.
      - In the Role Name field, type TCS_UPDATER_DB.
      - Click **OK** to save the role.
   d. Create the **TCS_CLIENT_DB** role:
      - Select WFM database > Security > Roles, right-click the Roles folder, and select New Database Role from the shortcut menu.
      - In the Role Name field, type TCS_CLIENT_DB.
      - Click Add to add the TCS_UPDATER_DB database role.

7. Add the application **roles** as role members for their corresponding database roles by opening a New Query and running the following statement:

```
exec sp_addrolemember 'TCS_CLIENT_DB', 'TCS_CLIENT' exec
sp_addrolemember 'TCS_UPDATER_DB', 'TCS_UPDATER'
```

8. Create a SQL Server login, such as **TCSADMIN**, for the Aspect Workforce™ administrator account as follows:

Note: For convenience throughout this guide, we refer to the administrator account for Aspect Workforce™ as **TCSADMIN**. But you can use any Login Name you choose.

   a. Expand the **Security folder**, right-click **Logins**, and choose **New Login**.

      This is the Security folder for SQL Server, not for the WFM database.

   b. For the user name, type the name of the administrator account, such as **TCSADMIN**.

   c. Select SQL Server Authentication, and enter a password, such as qqq. Clear Enforce Password Policy.

   d. From the **User Mapping** page, select the **WFM database**, and leave the **public** role selected. (Do not select any other database roles, such as TCS_CLIENT_DB or TCS_UPDATER_DB.)

   e. Accept all defaults unless directed otherwise.

   f. Click **OK** to create the login ID and associated database user.

9. Create **logins** and **passwords** for the users shown in the following table by using the following guidelines:

- You can use the default user names and passwords (such as **TCSACDPROC** / **tcsacdproc**), or you can create your own user names and passwords.
- Ensure that all user names are created using uppercase letters.
- When entering the passwords, use the same name as the login names, but use lower-case letters; for example, if the login name is TCSACDPROC, use the password tcsacdproc. Exception: for NOTF_USER, use qqq as the password. You can change the password later if you wish.
- For each account, use the same settings that you used when creating the TCSADMIN account in Step 7. (Bulleted items are expansions beyond the Aspect Workforce™ core software.)

User Name	Password	Use
TCSTALLYSERVER	tcstallyserver	WFM Tallyserver
TCSACDPROC	tcsacdproc	WFM ACD File Processing

TCSAPPROC	tcsapproc	WFM AP File Processing
TCSAUTORUN	tcsautorun	WFM Autorun

User Name	Password	Use
TCSUPDATER	tcsupdater	WFM Updater
TCSCHECKER	tcschecker	WFM Checker
WFMFSMONITOR	wfmfsmonitor	• Encompass
WFMEXPORTER	wfmexporter	• Encompass • Aspect Campaign Optimizer Adapter
WFMIMPORTER	wfmimporter	• Encompass
NOTF_USER	qqq	• Empower • Encompass • Aspect Campaign Optimizer Adapter WFM core (for Email Reports)

WFMDISPATCHER	wfmdispatcher	• Empower • WFM Web Services • Workforce Engagement Management • Encompass • Aspect Campaign Optimizer Adapter
RTALISTEN	rtalisten	• Perform
WFMSEGEXPORT	wfmsegexport	• Empower
WFMSEGEXPORTDBMON	wfmsegexportdbmon	• Empower
WFMALARMPROVIDER	wfmalarmprovider	• Perform
WFMCSMONITOR	wfmcsmonitor	• Encompass
WFMEXPRESSCHECKER	wfmexpresschecker	WFM Express Checker

10. Create **logins** and **passwords** for each person who will use Aspect Workforce™. On the User Mapping page, the PUBLIC role (granted by default) is required. See Adding New Users for more information.

Importing the Sample WFM Database

You can import a sample database, included on your distribution CD, for training and experimentation. When installing the main application server, configure the sample database for Aspect Workforce™. For more information, see Installing the Main Application Server for SQL Server. Importing the sample database is not required to run Aspect Workforce™.

You can also use this procedure to import an existing database by substituting the required information for that database. After importing the database, configure it for Aspect Workforce™ by using the WFM Database Manager. (WFM Database Manager is not available until you have installed Aspect Workforce™.) For more information, see Configuring an Existing or Sample Database.

To import the sample database:

1. Stop the WFM TallyServer and WFM Updater system services if they are running.
2. Since these are Aspect Workforce™ services, it is possible that they have not been installed yet. For more information, see Installing and Configuring WFM Services.
3. Insert your distribution CD.
4. Browse to the following file, where ***x*** is the letter of your CD drive: ***x*:\Sample Data for MS SQL Server\TCS_SAMPLE.BAK**
5. Copy the **TCS_SAMPLE.BAK** file to a location on your database server disk drive. For example: C:\Program Files\Microsoft SQL Server\BACKUP
6. Launch SQL Server Management Studio.
7. Log in using **SQL Server Authentication** and the **sa** login ID.
8. Expand the tree, right-click the **Databases** folder, and select **Restore Database** from the shortcut menu.
9. In the **Restore Database** dialog box, select the **General** page.
10. In the **Source** section, select the **Device** button, and click the lookup button next to the **Device** field. The **Specify Backup Devices** dialog box opens.
11. Click **Add** to open the **Locate Backup File** dialog box.
12. Browse to the location of the **TCS_SAMPLE.BAK** file on your database server and select the file. For more information, see step 4, above.
13. Click **OK** to close the Locate Backup File dialog box and click **OK** to close the **Specify Backup Devices** dialog box.
14. In the **Restore** column, select the **Restore** check box next to the name of the sample database.
15. In the upper left, select the **Files** page.
16. In the Restore Database Files As section, select the **Relocate All Files To Folder** check box.
17. In the **Data File Folder** field, verify the path to your Aspect Workforce™ DATA folder. If the path is incorrect, click the lookup button next to the field, browse to the correct destination folder, and click **OK**.
18. Do the same for the **Log File Folder** field: Verify the path to your Aspect Workforce™ LOG folder. If the path is incorrect, click the lookup button next to the field, browse to the correct destination folder.
19. Click **OK** to restore the database. A progress indicator tracks the progress, and a notification is displayed when the process has completed successfully.
20. If you restored the sample database, skip to step 22.
21. If you restored an existing database, do the following:
    a. In SQL Server, browse to the folder:

computer/Databases/*restored db*/Security/Users

where:

computer is the machine name of your database server ***restored db*** is the name of the existing ***database*** you restored

b. Delete all **WFM users**, if any (such as TCSADMIN, WFMDISPATCHER, and so on) by rightclicking each user and selecting **Delete**. You cannot delete the native users such as *dbo* and *guest*. If no WFM users are present in the Users folder, go to step 22; if WFM users were present and you deleted them, go to the next step.

c. In SQL Server, browse to the following folder, where ***computer*** is your database server name:

computer/Security/Logins

d. Right-click a **WFM user** (that is, one of those you deleted in step b), and select **Properties**.

e. On the User Mapping page, select the **check box** next to the restored database, and click **OK**.

f. Repeat step d and step e for every user you deleted in step b.

22. Click the **New Query** button in the toolbar and select the **TCS_SAMPLE** database.

23. In the toolbar, click the **Open File** icon, and load the following script file (included on your distribution CD), where ***x*** is the drive letter of your CD drive: ***x*:\Sample Data for MS SQL Server\TCS_SAMPLE_CONFIG.SQL**

24. In the toolbar, click **Execute** to run the script. If the script runs successfully, you can view the new users in SQL Server Management Studio after pressing F5 to refresh the interface. View the new users (such as NOTF_USER and TCSADMIN) at the following path:

25. *db server* > Databases > TCS_SAMPLE > Security > Users where:

db server is the name of the server where SQL Server is installed ***WFM db*** is the name of your ***Aspect Workforce™*** database

This script automates the sample database configuration process. The script creates standard roles for your sample database and also creates users with default user names and passwords. To use names or passwords other than the default, edit the script.

Note: In addition to the roles and users created for the sample database in the SQL Query Window, you need a database login ID for each person who will use the database. For details, see Adding New Users.

Adding New Users

Create SQL Server logins and passwords for each person who will use the Aspect Workforce™ desktop client. Creating SQL Server logins differs depending if your Aspect Workforce™ database is configured to use Application Roles or Database Roles.

The Application Roles feature, introduced in release 8.0, implements password protection and thereby enforce a higher level of security for database access. With this feature enabled, Aspect Workforce™ users can access the Aspect Workforce™ database to add, delete, or modify data only when they are logged in to Aspect Workforce™. If you chose not to implement this feature since it was introduced in version 8.0, then security will continue to be enforced using Database Roles.

Application Roles is the installation default for the current version of Aspect Workforce™; Database Roles was the only option available in legacy versions of Aspect Workforce™ and is included here if you previously chose to continue to use Database Roles.

Note: Database logins are only required for Aspect Workforce™ desktop client users. Workforce Engagement Management users do not need a database login ID.

Adding New Login IDs for Application Roles

If you are using Application Roles, create database login IDs for Aspect Workforce™ users as follows:

1. Add the logins directly in SQL Server Management Studio using either the Windows or SQL Server Authentication option for each login.
2. Assign the **public** database role for the Aspect Workforce™ database.
3. When creating the new login in SQL Server, associate the login with the appropriate databases for that user, making sure to select the **public** database role.

Adding New Users for Database Roles

If you are using Database Roles, to add new users:

1. Add the logins directly in SQL Server Management Studio using either the Windows or SQL Server Authentication option for each login.
2. Assign the **TCS_CLIENT_DB** role and **public** database role for the Aspect Workforce™ database to each login.

Implementing Windows Authentication for SQL Server

If desired, both user accounts and system service accounts in Aspect Workforce™ can use Windows Authentication. If you are using Database Roles instead of Application Roles (the default), you must assign the TCS_CLIENT role to each of these user accounts and system service accounts. For help with configuring Windows Authentication, contact your SQL Server database administrator.

Changing Default Passwords

If you do not want to use the default passwords for the SQL Server Application Roles, you can substitute others. Note, however, that passwords used by the Application Roles are saved as follows:

- SQL Server stores them within its system database, allowing access to SQL Server.
- Aspect Workforce™ encrypts and stores them within the Aspect Workforce™ database.

If you do not use the default passwords when you create the Application roles, you must change the passwords stored by Aspect Workforce™ such that they match the ones that you set up in SQL Server. Do this after you install the main application server software.

To change default passwords:

1. Log in to your main application server. For Windows Server 2022 and 2025, select **Start > Aspect > WFM Database Manager**. The **Database Manager** window opens.
2. In the list of database aliases, select the desired Aspect Workforce™ **database**.
3. In the main menu, select Tools > Modify Application Role Password.
4. Verify that the option for Log In Using a Specific User Name And Password is selected.
5. In the User Name field, type the name of the desired application role: either **TCS_CLIENT** or **TCS_UPDATER**.
6. In the Password field, type the new **password** you have chosen, and click **OK**.
7. Repeat In the User Name field, type the name of the desired application role: either and In the Password field, type the new for the other application role.

In the main menu, select **File > Exit**.

Configuring Oracle

This chapter provides information about setting up an Oracle database environment for Aspect Workforce™.

Note: To complete Oracle database server configuration steps, you must have system administrator access to the Oracle database server.

Verifying Database Server Requirements

This section contains information about Oracle software requirements.

Verifying the Oracle Server Configuration

With the Oracle database option, the database server runs the database software—Oracle Database 19c—and stores the Aspect Workforce™ data. For best results, follow the Oracle Optimal Flexible Architecture (OFA) standard. This set of configuration guidelines gives you faster, more reliable Oracle databases that require less work to maintain.

Note: Aspect Workforce™ requires that the NLS_NCHAR_CHARACTERSET be set to AL16UTF16. Base your selection of the NLS_CHARACTERSET on the customer's in-house requirements for Oracle user accounts, tablespace names, and other system objects.

If you chose to configure your Oracle database server with a container database, be aware that Aspect Workforce™ cannot use a common application role defined in a container database. Instead, you must create local roles at the pluggable database level. Local roles may be granted to common or local users, but you must grant them locally (for example, you cannot grant local roles at the container level).

Upgrading Oracle

Aspect Workforce™ requires a specific version of Oracle Database Server 19c. For the specific Oracle version required, see the *Aspect Workforce™ Release Note.* If you have an earlier version, upgrade the Oracle Database Server *before* installing Aspect Workforce™.

To upgrade Oracle:

1. Create an **export file** of your Aspect Workforce™ database.
2. Upgrade your database server software.
3. Upgrade your **database client software** on your main application server, secondary application servers, and user workstations. For more information, see Installing the Client Software.

Installing the Client Software

To communicate with your database, each application server and user workstation in your Aspect Workforce™ network requires the Oracle client software.

Note: Ensure that you remove any Oracle software earlier than Oracle Database 19c before you install the new database client software. This includes the 12c, 11g R2, 10g, and 9i clients, the Oracle Home Directory, the Oracle folder typically under **C:\Program Files**, and the Oracle registry key under **HKLM\Software**. You must restart the server after the client installation.

When installing the Oracle client software using the traditional installation format, select the **Administrator** or **Custom** installation type. If you select **Custom**, you must select the following components:

- Oracle Net
- SQL*Plus
- Oracle Provider for OLE DB interfaces

Starting with Oracle Database 19c, in addition to the traditional installation format, installation and configuration of Oracle Database Client software is simplified with image-based installation. Using imagebased installation, you can install Oracle Database Client 32-bit and 64-bit configurations of the **Administrator** installation type. See the Oracle 19c installation instructions for more information on installing the Oracle client. Note the following:

- Aspect Workforce™ application servers require both the 32-bit and 64-bit versions of the client software. Aspect recommends installing the 32-bit version first and then the 64-bit version. When installing the 64-bit version, the traditional Oracle installation wizard will default to the same Oracle Base Directory as the 32-bit version, but will default to a different Software Location, as the versions must be installed to separate Oracle Home directories. Aspect recommends using the default installation paths.
- Aspect Workforce™ client workstations only require the 64-bit client. You do not need to install the 32-bit client on the workstations.
- You must restart the server after each client installation.

See the *Aspect Workforce™ Release Note* to determine which patch, if any, is required to be applied after installing the Oracle client. Download the patch from Oracle, and follow the provided installation procedures. Also review the Known Issues section for any Oracle client installation issues, and applicable, known work-arounds.

Setting up the Database Server

This section explains how to set up the database server for Aspect Workforce™.

About Database Roles and User Accounts

In addition to the roles and user accounts described in this chapter, you need a database login ID for each person who will use Aspect Workforce™. The Users module in Aspect Workforce™ gives you the ability to add these database login IDs when you define users. Alternately, you can add logins directly to Oracle, and then create users in Aspect Workforce™.

Note: Database logins are only required for Aspect Workforce™ desktop client users. Workforce Engagement Management users do not need a database login ID.

When creating database login IDs directly in Oracle (and then adding corresponding users in Aspect Workforce™), you must assign the **TCS_CLIENT** role to each Aspect Workforce™ user.

Note: Do not make the **TCS_CLIENT** or **TCS_UPDATER** role a default role for Aspect Workforce™ users. Making either role a default role for a given user enables the user to bypass Aspect Workforce™ security. If you use the Oracle Enterprise Manager software when working with users and roles, be aware that it automatically sets a role as a default role. You must clear the default role option when you assign the role to a user.

When using the Aspect Workforce™ Users module to add users with access to Oracle, you must grant specific permissions to the database schema user. In Oracle, a stored procedure runs with the permissions granted to the user that created the stored procedure. Aspect Workforce™ stored procedures are normally created by the user associated with the database schema (typically, **TCSDBOWNER**). To enable the database account features in the user interface, the following permissions must be granted to the database schema user:

- GRANT CREATE USER to schema_user;
- GRANT TCS_CONNECT to schema_user WITH ADMIN OPTION;
- GRANT TCS_CLIENT to schema_user WITH ADMIN OPTION;

Implementing Windows Authentication for Oracle

If desired, Aspect Workforce™ user accounts and Aspect Workforce™ system service accounts can use Operating System Authentication. To implement this authentication method, you must assign the TCS_CLIENT role to each account. Also, specific Oracle settings must be enabled to authenticate external (that is, Windows) accounts. For help with configuring Oracle, contact your Oracle database administrator.

Configuring the Aspect Workforce™ Database for Oracle

You can set up Oracle for Aspect Workforce™ manually or automatically, as explained in the following sections:

Configuring Manually

Note: Due to a change in Oracle 12 and higher, a role can no longer inherit another passwordprotected role. So, when configuring your Aspect Workforce™ schema, do not grant the TCS_CLIENT role to the TCS_UPDATER role.

To configure Oracle for Aspect Workforce™ manually:

1. Create two **roles** on your Oracle server: **TCS_CLIENT** and **TCS_UPDATER**. These roles require password authentication.

   Note: The Aspect Workforce™ database is configured to use tcs_cli3nt and tcs_updat3r, respectively, for default passwords. If you do not want to use these default passwords, create different

roles with new passwords. After you create the database schema, you must change the passwords stored by Aspect Workforce™. For details, see Changing Default Passwords.

2. Create two **tablespaces** on your Oracle server: **TCS_DATA** and **TCS_INDEXES**. If you have four disk drives as recommended by Aspect, place each tablespace on disk drives separate from your SYSTEM tablespace for best performance. Use the following parameters for your WFM tablespaces:
   a. TCS_DATA minimum size: 500 MB
   b. TCS_INDEXES minimum size: 800 MB
   c. Create both tablespaces as Locally Managed With Automatic Extent Allocation and Automatic Segment Space Management.

3. Create two **users** on your Oracle server: **TCSDBOWNER** and **TCS_SAMPLE**. (You will eventually need to create an Oracle login ID for each user who will connect to the Aspect Workforce™ database. You must create these first two before continuing.) Both users require a password, and both must have the following Oracle system privileges:

ALTER SESSION	ALTER USER	CREATE PROCEDURE
CREATE SEQUENCE	CREATE SESSION	CREATE TRIGGER
CREATE VIEW	RESTRICTED SESSION	CREATE TABLE

Both users also require the following privileges:

- **SELECT** on "SYS"."V_$VERSION"
- **SELECT** on ANY DICTIONARY
- **EXECUTE** on DBMS_LOCK
- **EXECUTE** on DBMS_LOB
- **EXECUTE** on DBMS_SQL

Note: Only the TCSDBOWNER and TCS_SAMPLE users require these privileges, as they are the “owners” of the Aspect Workforce™ database and sample database. Regular users require only a small part of this list.

Note: It is possible to utilize a Windows account as the WFM owner. Assign permissions and quotas as defined in these steps for that account.

4. Grant the appropriate **quota** for the TCSDBOWNER and TCS_SAMPLE users on the Oracle tablespaces. For best results, use an **UNLIMITED** quota.

5. Create the following **users** on your Oracle server and assign the indicated roles. These users are for automated processes that must access the database. They require a password and the **CREATE SESSION** and **ALTER SESSION** Oracle system privileges.

- The passwords listed here are not mandatory. If you choose to use different passwords, you must configure each Aspect Workforce™ system service with the appropriate password.
- If a user is needed only for a specific enhancement package, that package is indicated as a bulleted item in the Use column. If you are not using that package, the user does not need to be created.

User Name	Password	Role	Use
TCSADMIN	qqq	TCS_CLIENT	Main Administrator

User Name	Password	Role	Use
TCSTALLYSERVER	tcstallyserver	TCS_CLIENT	WFM Tallyserver
TCSACDPROC	tcsacdproc	TCS_CLIENT	WFM ACD File Processing
TCSAPPROC	tcsapproc	TCS_CLIENT	WFM AP File Processing
TCSAUTORUN	tcsautorun	TCS_CLIENT	WFM Autorun
TCSUPDATER	tcsupdater	TCS_UPDATER	WFM Updater
TCSCHECKER	tcschecker	TCS_CLIENT	WFM Checker
WFMFSMONITOR	wfmfsmonitor	TCS_CLIENT	• Encompass

WFMEXPORTER	wfmexporter	TCS_CLIENT	• Encompass • Aspect Campaign Optimizer Adapter
WFMIMPORTER	wfmimporter	TCS_CLIENT	• Encompass
NOTF_USER	qqq	TCS_CLIENT	• Empower • Encompass • Aspect Campaign Optimizer Adapter WFM core (for Email Reports)
WFMDISPATCHER	wfmdispatcher	TCS_CLIENT	• Empower • WFM Web Services • Workforce Engagement Management • Encompass • Aspect Campaign Optimizer Adapter
RTALISTEN	rtalisten	TCS_CLIENT	• Perform
WFMSEGEXPORT	wfmsegexport	TCS_CLIENT	• Empower

User Name	Password	Role	Use
WFMSEGEXPORT DBMON	wfmsegexportdbmon	TCS_CLIENT	• Empower

WFMALARMPROVIDER	wfmalarmprovider	TCS_CLIENT	• Perform
WFMCSMONITOR	wfmcsmonitor	TCS_CLIENT	• Encompass
WFMEXPRESSCHECKER	wfmexpresschecker	TCS_CLIENT	WFM Express Checker

Configuring with an Automated Script

To automate the Oracle setup, use the following SQL script, where ***x*** is the letter of the CD drive: **x:\Utility\SQL Scripts\InitTCS.sql**

Note the following information regarding this script:

- The script cannot be executed in the exact form shown. You must customize it for your organization.
- The first few lines of the script—those for tablespaces—have been commented out. You must supply a path and file name for the two files that are created with your tablespaces, and you must uncomment the appropriate script commands.

  For example, the following SQL statements:

```
CREATE TABLESPACE TCS_DATA
DATAFILE 'fill this in' SIZE 5000M
EXTENT MANAGEMENT LOCAL AUTOALLOCATE SEGMENT
SPACE MANAGEMENT AUTO;
```

  must be modified for your database as in the following example:

```
CREATE TABLESPACE TCS_DATA
DATAFILE 'D:\TCS_ORA\TCSDATA.ORA' SIZE 8000M
EXTENT MANAGEMENT LOCAL AUTOALLOCATE SEGMENT
SPACE MANAGEMENT AUTO;
```

- The path that you specify for each data file must already exist or Oracle won't be able to create the data file. In the previous example, D:\TCS_ORA must already exist or the script will fail.
- You must be logged in to your database server locally when you run the script.
- Log in to your Oracle server as **SYS** (connecting as **SYSDBA**), and insert your **distribution CD.**

Note: If you do not log in as **SYS** (with **SYSDBA** role), you cannot grant permissions and the database setup fails.

- The script creates users and roles with the default user names and passwords. If you want usernames or passwords other than the default, edit the **script.**

Note: The Oracle database can be configured in various ways. The script, for example, creates and uses the TCS_CONNECT role. This role automates the assignment of connection permissions. The manual setup instructions do not call for this role. Either method is valid.

Importing the Sample WFM Database

An optional sample database is included on your distribution CD for training and testing, which you can import for use with Aspect Workforce™.

Note: The TCS_SAMPLE_DP.DMP file included in your distribution CD was exported using Oracle's Data Pump utility (EXPDP) rather than the older EXP utility.

To import the sample database:

1. Stop the **Tally Server** and **Updater** system services if they are running.
2. Log in as an administrator to your database server.
3. Before importing the TCS_SAMPLE_DP.DMP file using the IMPDP utility, a directory object that can be accessed by the TCS_SAMPLE user must exist. The directory object is only a pointer to a physical directory and creating it does not actually create the physical directory on the file system. If you already have defined a directory object for IMPDP/EXPDP jobs, make sure the TCS_SAMPLE user has the proper permissions to the object, and continue with step 6.
4. Using SQL Plus, log in as **sysdba** and execute the following two operations:

- SQL> CREATE OR REPLACE DIRECTORY *<Directory_Name>* AS '*<Path>*';
- SQL> GRANT READ, WRITE ON DIRECTORY *<Directory_Name>* TO tcs_sample; where:

<Directory_Name> is the desired name of the directory object
<Path> is the path on the file system that will be used by this directory object

Note: You can manually create the path before or after creating the directory object.

5. Exit SQL Plus.
6. Insert your **distribution CD**, and copy the following file to the physical path for the IMPDP/EXPDP directory object: **x:\Sample Data for Oracle\TCS_SAMPLE_DP.DMP**
7. Launch the **IMPDP utility**, and enter the following command (if using Oracle on a Windows operating system, open a command prompt instead):

```
impdp tcs_sample/<Password>@<DatabaseInstanceName>
DIRECTORY=<DirectoryObjectName> DUMPFILE=TCS_SAMPLE_DP.DMP
LOGFILE=TCS_SAMPLE_DP_IMPORT.LOG
```

where:

<Password> is the appropriate password for the tcs_sample user
<DatabaseInstanceName> is the name of your Oracle instance
<DirectoryObjectName> is the EXPDP/IMPDP Directory.

8. After the file has been imported, compile **database objects** as follows:

- Using the Oracle SQL*Plus utility, for example, log in to the **database** using the **TCS_SAMPLE** login ID.
- Compile the **TCS_SAMPLE** schema using the following entry:
- SQL> EXECUTE DBMS_UTILITY.COMPILE_SCHEMA('TCS_SAMPLE');
- Then execute the following to compile the database triggers: `SQL>EXECUTE COMPILE_TRIGS;`

Note: In addition to the roles and user accounts created for Oracle, you will need a database login ID for each employee who will use the sample database. Assign the **TCS_CLIENT** role to each user.

Changing Default Passwords

If you do not want to use the default passwords for the required Oracle roles, you can substitute others. Note, however, that passwords used by the required Oracle roles are saved as follows:

- Oracle stores them, allowing access to the database.
- Aspect Workforce™ encrypts and stores them within the database.

If you do not use the default passwords when you create the required Oracle roles, you must change the passwords stored by Aspect Workforce™ such that they match the ones that you set up in Oracle. Do this after you install the main application server software.

Changing some default passwords is also necessary after upgrades, to change the password from uppercase to lowercase.

To change default passwords:

1. Log in to your main application server and for Windows Server 2022 and 2025, select **Start** > **Aspect > WFM Database Manager**. The **Database Manager** window opens.
2. In the list of database aliases, select the desired Aspect Workforce™ **database**.
3. In the main menu, select **Tools > Modify Application Role Password**.
4. Verify that the option for **Log In Using a Specific User Name And Password** is selected.
5. In the User Name field, type the name of the desired application role: either **TCS_CLIENT** or **TCS_UPDATER**.
6. In the Password field, type the new **password** you have chosen, and click **OK**.
7. Repeat the steps above for the other application role.
8. In the main menu, select **File > Exit**.

Installing the Main Application Server for SQL Server

This chapter contains information about installing the Aspect Workforce™ main application server in a SQL Server environment.

The installation program automates several tasks that were formerly manual steps in prior releases of Aspect Workforce™. As you progress through the installation wizard, some of the processes might require several minutes to complete. This is normal and does not indicate any issues with your hardware, software, or the installer. When the installation is complete, a wizard screen confirms that the installation was successful.

Prerequisites

Before you install your main application server, complete the following procedures or verify that they have been completed:

- You have administrator access to the main application server.
- You check the release note for any new requirements or procedures.
- The SQL Server database server and Aspect Workforce™ database have been configured. For more information, see Configuring SQL Server.
- The Microsoft OLE DB Driver for SQL Server is installed on the main application server. For more information, see Installing the Client Software.
- The server is in Administrator mode (that is, Remote Desktop For Administration mode) and not in Terminal Server mode.
- For Windows Server 2022 or 2025, open Server Manager and verify that the Remote Desktop Services role has not been installed.
- If you plan to install Aspect Workforce™ on any drive other than the C drive, you have granted the necessary permissions to users. For more information, see Installing on a Non-C Drive.

Security and Permissions Considerations

This sections describes issues related to permissions and security that may pertain to your deployment of Aspect Workforce™.

About Shared Folders

Installing the main application server software creates several shared folders for installing the secondary and client software from the main application server, for storing installation data, and for running reports. These folders are created with Change and Read permissions for Users of the computer. This setting places the machine at only marginal risk of infection by certain viruses.

Before installing the main application server software, you should determine a comfortable level of security to use for these folders. After installation and configuration of Aspect Workforce™, you can configure the folders to use the required permissions. For details, see Restricting User Access to Shared Folders.

Installing on a Non-C Drive

When you install the Aspect Workforce™ on any drive other than the C drive, you must ensure that users have permissions to the installation folder. Granting these permissions enables users to access commonly-used Aspect Workforce™ services.

The default installation folder for Aspect Workforce™ is the following, where ***x*** is the letter of the non-C drive: ***x*:\Program Files\Alvaria\Workforce**

Ensure that one of the following has permissions to that folder:

- Users group on the local machine
- Individual user who is launching the client

Unless you have a *standalone* installation, you must grant the same permissions on all servers where Aspect Workforce™ is not installed on the C drive. A standalone installation is one in which all Aspect Workforce™ services, such as Tally Server and Updater, are running on the same computer.

About File Installation Paths

Aspect Workforce™ delivers both 32-bit and 64-bit files. The location of the files depends on the installation path you select when installing Aspect Workforce™. See the table in Appendix B for details on where files are delivered.

Installing the Main Application Server

When performing this and other installation-related procedures, always log in to the server with an account that is both a domain account and a local administrator on all Aspect Workforce™ servers in your deployment.

Install the main application server from the product CD.

To install the main application server software:

Log in as an administrator to the server designated as the main application server.

1. Insert the Aspect Workforce™ Software CD, and open the file Setup.exe. The product selection window of the installation wizard opens.
2. Click **Aspect Workforce™**. If any prerequisite software is not already installed on the server, then the Aspect Prerequisite Installer window opens, displaying a list of prerequisite but uninstalled software. Click Install to install the prerequisite software. When installation is complete, the Welcome window of the Install Wizard For Workforce opens.
3. Click **Next**. The Destination Folder window opens.

4. To accept the default (recommended) location for the program files, click **Next**. Otherwise, click **Change**, and browse to or type a different path, and click OK. The Data Folder window opens.
5. To accept the default (recommended) location for the data files, click **Next**. Otherwise, click **Change**, and browse to or type a different path, and click OK.
6. If you choose another path, add \WFMData to the end of the path to create the shared folder for the data files. Example: **E:\Applications\Alvaria\WFMData**

   Since all files and folders for ACD data are stored in this path, ensure that the drive you select is sized appropriately. ACD data files can require several gigabytes of drive space.
7. The **Custom Setup** window opens.
8. Click the Main Application Server icon, and select This Feature, And All Subfeatures, Will Be Installed On Local Hard Drive.

   Note: Do not select Secondary Application Server or User Workstation. The wizard automatically installs components for the secondary application server and the Aspect Workforce™ client on the main application server.
9. If you want to install the WFM Listen service on the main application server, click the **Listen System Service** icon, and select **This Feature, And All Subfeatures, Will Be Installed On Local Hard Drive**.

   After installing the main application server, you configure WFM Listen using the Listen Configuration Editor. For more information, see Using the Listen Configuration Editor. You can also install Listen on a secondary application server.
10. If you want to enable load balancing (that is, distributed mode for Tally Server, Checker, or both), click the Aspect Message Routing Service icon, and select **This Feature, And All Subfeatures, Will Be Installed On Local Hard Drive**.

    After installing the main application server, you configure the Aspect Message Routing Service using the Aspect Message Routing Platform Configuration Editor. For more information, see Configuring Aspect Message Routing.
11. If you want to install the WFM Historical Connectors (install files required to configure Five9, InContact, and Zendesk historical connectors), click the **WFM Historical Connectors** icon, and select **This Feature, And All Subfeatures, Will Be Installed On Local Hard Drive**.

    After installing the main application server, you configure the WFM Historical Connectors using the WFM Historical Connector Configuration. For more information, see Using the WFM Historical Connector Configuration. You can also install the WFM Historical Connectors on a secondary application server.
12. Click **Next**. The DCOM Servers window opens.
13. The main application server communicates with the machines hosting the Updater, ACD Processing, Checker, and Tally Server services. If these services will be hosted by machines other than the main application server, type the correct machine names before clicking **Next**. The Ready to Install window opens.
14. Click **Install.** After the files are installed, the Install Wizard Completed window is displayed.
15. Click **Finish** and click **Exit** to close the wizard.

Creating and Configuring the Database

Use the WFM Database Manager program on your main application server to create and configure a new Aspect Workforce™ database. You can also use the WFM Database Manager to configure an existing Aspect Workforce™ database. Both procedures are described in this section.

Creating and Configuring a New Database

Do not use this procedure to configure an existing or sample database. Instead, see Configuring an Existing or Sample Database.

Note: If you configured a Windows Account as the WFM owner, either use **Run As different user** when launching DBManager, or login to the server as the database owner's windows account. After which you must select **Log in using Windows Integrated security** when prompted for a WFM login in DBManager.

To create and configure a new Aspect Workforce™ database:

1. Do the following for Windows Server 2022 and 2025: Select **Start** > **Aspect >** WFM **Database Manager**.
2. The first time you use the WFM Database Manager after installing the main application server, the **Select RDBMS** dialog box opens.
3. Select the **SQL Server 2022** option and click **OK**. The Database Manager window opens.
4. Select **File > New Database**. The Configure Database Connection Alias dialog box opens.
5. In the Database Connection Alias field, type the name you want to use for your database.
6. Click the **Connection String** lookup button. The Data Link Properties dialog box opens.
7. On the Provider page, select Microsoft OLE DB Driver 19 for SQL Server and click Next.
8. Unless your SQL Server administrator has installed a signed certificate on the database server for the purposes of encrypting connections to the database, click on the **Advanced** tab, and change the **Connection encryption** from **Mandatory** to **Optional** and set the Connect timeout to 5.
9. Click on the **Connection** tab, and in the server name field, select or type the database server fully qualified domain name.
10. Select the button for Use A Specific User Name And Password and clear the Blank Password check box.
11. For security reasons, you cannot use the Allow Saving Password option to save user names or passwords to the connection alias.
12. Enter the TCSDBOWNER user name and password that you assigned to the TCSDBOWNER user to enable testing of your database connection.

    (For more information, see Setting Up the Aspect Workforce™ Database, step 4.)
13. Select the Select The Database radio button and select the name of the Aspect Workforce™ database from the adjacent drop-down list.

14. Click **Test Connection** and click OK after the confirmation message is displayed.
15. Click OK to close the Data Link Properties dialog box.
16. Click OK to close the Configure Database Connection Alias dialog box. The Database Manager dialog box, used for login configuration, opens.
17. Select the Log In Using A Specific Name And Password button.
18. In the User Name field, type the **TCSDBOWNER** user name.
19. In the **Password** field, type the password you assigned to the TCSDBOWNER user name.
20. Click **OK**. The Schema Version Information dialog box opens.
    - The **Please Select An Available Schema Version** drop-down list is disabled, because the most current schema version is selected automatically and displayed for informational purposes only. You cannot change the schema version that will be used.
21. Click OK. The Select Prepopulation Data Language dialog box opens.
22. From the drop-down list, select the appropriate prepopulated language.

    During database creation, Aspect Workforce™ prepopulates language-specific configuration data. The list shows all locales in which the Aspect Workforce™ user interface is localized.
23. Click **OK**. The DB Time Zone dialog box opens.
24. Use the drop-down list to select the time zone of the physical location of your database server and click **OK**. The ADMIN Time Zone dialog box opens.

    Note: The selected time zone must match the time zone that is currently used on the database server.
25. Use the drop-down list to select the time zone of the physical location of the person designated as the Aspect Workforce™ administrator and click OK.
26. The SQL Server File Groups dialog box opens, with default selections displayed for your database. (If required, use the drop-down lists to select the appropriate SQL Server file groups instead.)
27. Click **OK**. The Confirm dialog box opens, informing you that a new schema installation will be performed.
28. To continue, click Yes. The Database Manager configures your database for Aspect Workforce™. Multiple windows will open indicating the work being performed.
29. Do not Cancel this operation unless necessary. If errors occur, review the schema log (located at C:\ProgramData\Aspect\Workforce Management\log) and correct any issues. In most cases this will require you to drop the new schema and create the database again. Contact Aspect Professional Services for assistance.
30. When the process is complete, an information dialog box opens with the message that the schema has been successfully created.

31. Click **OK**. The Database Manager window is displayed, showing your new database alias in the Active state.
32. Repeat this entire procedure for each additional database that you want to create. If you are finished, close the Database Manager.

    After you complete this procedure, it is not necessary to do the next procedure, Configuring an Existing or Sample Database.

Configuring an Existing or Sample Database

If you have an existing Aspect Workforce™ database, or if you want to create a connection alias for the sample database provided with the product, use the WFM Database Manager on your main application server to configure the database.

Using the sample WFM database is optional. Before you create a connection alias to enable the sample WFM database, import the database as explained in Importing the Sample Database.

Note: If you configured a Windows Account as the WFM owner, either use **Run As different user** when launching DBManager, or login to the server as the database owner's windows account. After which you must select **Log in using Windows Integrated Security** when prompted for a WFM login in DBManager.

To configure an existing or sample Aspect Workforce™ database:

1. Do the following for Windows Server 2022 and 2025: Select **Start** > **Aspect** > WFM **Database Manager**. The Database Manager window opens.
2. Select **Tools > Select RDBMS**, and choose SQL Server 2022, and click OK.
3. Select **Tools > Create Database Connection Alias**. The Configure Database Connection Alias dialog box opens.
4. In the Database Connection Alias field, type the name you want to use for your database.
5. Click the **Connection String** lookup button. The Data Link Properties dialog box opens.
6. On the Provider page, select Microsoft OLE DB Driver 19 for SQL Server, and click Next.
7. Unless your SQL Server administrator has installed a signed certificate on the database server for the purposes of encrypting connections to the database, click on the **Advanced** tab, and change the **Connection encryption** from **Mandatory** to **Optional.**
8. Click on the **Connection** tab, and in the server name field, select or type the database server fully qualified domain name.
9. Select the button for Use A Specific User Name And Password and clear the Blank Password check box.

   For security reasons, you cannot save user names or passwords to the connection alias (by using the Allow Saving Password option).
10. Type the user name and password of the owner of this database.

11. If you are using the sample database, or an imported database, then the database owner is the **sa** account.
12. Select the Select The Database radio button and select the name of the existing or sample Aspect Workforce™ database from the adjacent drop-down list.
13. Click **Test Connection** and click OK after the confirmation message is displayed.
14. Click OK to close the Data Link Properties dialog box.
15. Click OK to close the Configure Database Connection Alias dialog box. The new database connection alias is saved, and the Database Manager window is displayed with a list of the current database aliases.

    After creating a database connection alias, the schema version is listed as Unknown. If the existing database is at the current release schema, the database can be used. To upgrade from a previous release schema, see Upgrading the Database .
16. To activate the database if it is not already activated, select it in the list, and select **File** > **Activate Database**. The State of the database changes to Active.
17. Select **File > Exit** to exit Database Manager.

Installing the Services

After installing the main application server, complete the following post-installation procedures for the WFM services, WFM Listen, and the Aspect Message Routing Service.

Complete all procedures on the main application server, in the order shown below.

1. Install WFM services using the WFM Service Installer. See Using the WFM Service Installer.
2. If you installed the WFM Listen service, configure the service using the Listen Configuration Editor. See Using the Listen Configuration Editor.
3. If you installed the Aspect Message Routing Service for load balancing, configure the service using the Aspect Message Routing Platform Configuration Editor. See Configuring Aspect Message Routing.
4. If you installed the WFM Historical Connector, configure the service using the Historical Connector Configuration. See Using the WFM Historical Connector Configuration.

Using Email Reports

Email Reports replaces the Export to MAPI feature that was available in earlier versions of Aspect Workforce™. If you want to use Email Reports, see Enabling Email Reports.

Upgrading

To upgrade the main application server for Aspect Workforce™, see Upgrading for SQL Server.

Uninstalling

Uninstall the main application server for Aspect Workforce™ in either of the following ways:

- Use the Programs And Features feature in the Windows Control Panel
- Use the Aspect Workforce™ installation program

Uninstalling with Windows Control Panel

To uninstall with Windows Control Panel, use this path:**Start > Control Panel > Programs > Programs And Features > Workforce > Uninstall**

Uninstalling with the Installation Program

To uninstall the main application server with the installation program:

1. Log in as an administrator to the server designated as the main application server.
2. Insert the Aspect Workforce™ Software CD and open the file Setup.exe. The product selection window of the installation wizard opens.
3. Click Aspect Workforce™. The Welcome window of the Install Wizard for Workforce opens.
4. Click **Next**. The Program Maintenance dialog box opens.
5. Select **Remove and** click **Next**. The Remove The Program window opens.
6. Click **Remove**. The Uninstalling Aspect Workforce™ window opens. When Aspect Workforce™ has been removed successfully, the Install Wizard Completed window is displayed.
7. Click **Finish**. If a reboot message is displayed, click No in the message, and reboot the server manually after exiting the wizard.

Installing the Main Application Server for Oracle

This chapter contains information about installing the Aspect Workforce™ main application server in an Oracle environment.

Before You Begin

Installing and configuring the main application server software requires administrator access to the machine that will run it. Before you set up your main application server, verify that:

- You have administrator access to the main application server.
- You check the release note for any new requirements or procedures.
- The Oracle database server and Aspect Workforce™ database have been configured. For more information, see Configuring Oracle.
- The Oracle client is installed on the main application server. For more information, see Installing the Client Software.
- Ensure that the server is in Administrator mode (that is, Remote Desktop For Administration mode) and not in Terminal Server mode.
- For Windows Server 2022 or 2025, open Server Manager and verify that Remote Desktop Services has not been installed.

About Shared Folders

Installing the main application server software creates several shared folders. These shared folders contain files for installing the secondary and client software from the main application server, for storing installation data, and for running reports. These folders are created with Change and Read permissions for Users of the computer. This setting places the machine at only marginal risk of infection by some viruses.

Before installing the main application server software, you should determine a comfortable level of security to use for these folders. After installation and configuration of Aspect Workforce™, you can configure the folders to use the required permissions. For details, see Restricting User Access to Shared Folders.

Installing on a Non-C Drive

When you install the Aspect Workforce™ on any drive other than the C drive, you must ensure that users have permissions to the installation folder. Granting these permissions enables users to access commonly-used Aspect Workforce™ services.

The default installation folder for Aspect Workforce™ is the following, where ***x*** is the letter of the non-C drive: ***x*:\Program Files\Alvaria\Workforce**

Ensure that one of the following has permissions to that folder:

- Users group on the local machine
- Individual user who is launching the client

Unless you have a *standalone* installation, you must grant the same permissions on all servers where Aspect Workforce™ is not installed on the C drive. A standalone installation is one in which all Aspect Workforce™ services, such as Tally Server and Updater, are running on the same computer.

About File Installation Paths

Aspect Workforce™ delivers both 32-bit and 64-bit files. The location of the files depends on the installation path you select when installing Aspect Workforce™. See the table in Appendix B for details on where files are delivered.

Installing the Main Application Server

When performing this and other installation-related procedures, always log in to the server with an account that is both a domain account and a local administrator on all Aspect Workforce™ servers in your deployment.

Install the main application server from the product CD.

To install the main application server software:

1. Log in as an administrator to the server designated as the **main application server.**
2. Insert the **Aspect Workforce™ Software CD** and open the file **Setup.exe**. The product selection window of the installation wizard opens.
3. Click **Aspect Workforce™**. If any prerequisite software is not already installed on the server, then the Aspect Prerequisite Installer window opens, displaying a list of prerequisite but uninstalled software. Click **Install** to install the prerequisite software. When installation is complete, the Welcome window of the **Install Wizard for Workforce** opens.

    **Note:** Microsoft Data Access Engine is no longer required. Aspect recommends that you uninstall the Microsoft Access Database Engine.
4. Click **Next**. The **Destination Folder** window opens.
5. To accept the default (recommended) location for the program files, click **Next**. Otherwise, click **Change**, and browse to or type a different **path**, and click **OK**. The Data Folder window opens.
6. To accept the default (recommended) location for the data files, click **Next**. Otherwise, click **Change**, and browse to or type a different **path**, and click **OK**.

   If you choose another path, add **\WFMData** to the end of the path to create the shared folder for the data files. Example: **E:\Applications\Alvaria\WFMData**
   Since all files and folders for ACD data are stored in this path, ensure that the drive you select is sized appropriately. ACD data files can require several gigabytes of drive space. The **Custom Setup** window opens.

7. Click the Main Application Server icon**,** and select This Feature, And All Subfeatures, Will Be Installed On Local Hard Drive.

   Note: Do not select Secondary Application Server or User Workstation. The wizard automatically installs components for the secondary application server and the Aspect Workforce™ client on the main application server.

8. If you want to install the WFM Listen service on the main application server, click the **Listen System Service** icon**,** and select **This Feature, And All Subfeatures, Will Be Installed On Local Hard Drive**.

   After installing the main application server, you configure WFM Listen using the Listen Configuration Editor. For more information, see Using the Listen Configuration Editor. You can also install Listen on a secondary application server.

9. If you want to enable load balancing (that is, distributed mode for Tally Server, Checker, or both), click the **Aspect Message Routing Service** icon, and select **This Feature, And All Subfeatures, Will Be Installed On Local Hard Drive**.

   After installing the main application server, you configure the Aspect Message Routing Service using the Aspect Message Routing Platform Configuration Editor. For more information, see Configuring Aspect Message Routing.

10. If you want to install WFM Historical Connectors (install files required to configure Five9, InContact, and Zendesk historical connectors), click the **WFM Historical Connectors** icon, and select **This Feature, And All Subfeatures, Will Be Installed On Local Hard Drive.**

    After installing the main application server, you configure WFM Historical Connectors using the Historical Connectors Configuration. For more information, see Using the WFM Historical Connector Configuration. You can also install Historical Connectors on a secondary application server.

11. Click **Next**. The **DCOM Servers** window opens.

12. The main application server communicates with the machines hosting the Updater, ACD Processing, Checker, and Tally Server services. If these services will be hosted by machines other than the main application server, type the correct **machine names** before clicking **Next**. The **Ready to Install** window opens.

13. Click **Install**. After the files are installed, the Install Wizard Completed window is displayed.

14. Click **Finish**. If a reboot message is displayed, click **No** in the message, and reboot the server manually after exiting the wizard.

Creating and Configuring the Database

Use the WFM Database Manager program on your main application server to create and configure a new Aspect Workforce™ database or to configure an existing Aspect Workforce™ database.

Note: If you configured a Windows Account as the WFM owner, either use **Run As different user** when launching DBManager, or login to the server as the database owner's windows account. After which you must select **Log in using Windows Integrated Security** when prompted for a WFM login in DBManager.

Additional Note for Oracle: When defining the Schema name in DBManager, you will need to place the owner account in quotes in this format - "OPS$*domain\username*" where *domain\username* is the WFM schema owner.

Creating a New Database

To create and configure a new Aspect Workforce™ database:

1. For Windows Server 2022 and 2025: Select **Start** > **Aspect > WFM Database Manager**. The **Database Manager** window opens.
2. The first time you use the WFM Database Manager after installing the main application server, the **Select RDBMS** dialog box opens.
3. Select the **Oracle 19c** option and click **OK**. The **Database Manager** window opens.
4. Select File > New Database. The **Configure Database Connection Alias** dialog box opens.
5. In the **Database connection alias** field, type the **name** you want to use for your database.
6. Click Lookup For The Connection String. The **Data Link Properties** dialog box opens.
7. Select **Oracle Provider for OLE DB and** click **Next**. The **Connection** page opens.
8. Click the **Data Source** field and type the **TNSNAME** for Oracle.
9. To test connectivity to your database, type the **user name** (such as TCSDBOWNER) and **password** you assigned to the owner of the Aspect Workforce™ database. Then click **Test Connection and** click **OK**.

   Note: For security reasons, you cannot save user names or passwords to the connection alias (using the Allow Saving Password option).
10. To close the Data Link Properties dialog box, click **OK**.
11. Click the **Schema Name** field in the Configure Database Connection Alias dialog box and type the **name** of the database owner; for example, TCSDBOWNER.
12. To close the Configure Database Connection Alias dialog box, click OK. The **Database Manager** login dialog box opens.
13. In the **User name** field, type the **TCSDBOWNER** user name.
14. Click the **Password** field, type the **password** you assigned to the TCSDBOWNER user name, and click **OK**. The **Schema Version Information** dialog box opens.

    The **Please Select An Available Schema Version** drop-down list is disabled, and the most current schema version is selected automatically and displayed for informational purposes only. You cannot change the schema version that will be used.
15. Click OK. The **Select Prepopulation Data Language** dialog box opens
16. From the drop-down list, select the appropriate **prepopulated language**.

During database creation, Aspect Workforce™ prepopulates language-specific configuration data. The list shows all locales in which the Aspect Workforce™ user interface is localized.

17. Click **OK**. The **DB Time Zone** dialog box opens.
18. Use the drop-down list to select the **time zone** of the physical location of your database server and click **OK**. The **Administrator Time Zone** dialog box opens.

    Note: The selected time zone must match the time zone that is currently used on the database server.
19. Use the drop-down list to select the **time zone** of the physical location of the person designated as the Aspect Workforce™ administrator (which by default is **TCSADMIN**) and click **OK**. The **Oracle Tablespaces** dialog box opens.

    Default selections open for your database.
20. If required, use the drop-down lists to identify the Oracle **tablespaces** that the Database Manager will use for your new database, and click **OK**. The **Confirm** dialog box opens.
21. Click **Yes** to continue. The Database Manager configures your database for Aspect Workforce™.

    When the process completes, an information dialog box opens with the message that the schema has been successfully created.
22. Click **OK**.
23. Repeat this entire **procedure** for each database to add.

Configuring an Existing or Sample Database

If you have an existing Aspect Workforce™ database, or if you want to create a connection alias for the sample database provided with the product, use the WFM Database Manager on your main application server to configure the database.

Using the sample WFM database is optional. Before you create a connection alias to enable the sample WFM database, import the database as explained in Importing the Sample Database.

Note: To use a Windows Account as the WFM owner, either use **Run As different user** when launching DBManager, or login to the server as the database owner's windows account. After which you must select **Log in using Windows Integrated Security** when prompted for a WFM login in DBManager.

Additional Note for Oracle: When defining the Schema name in DBManager, you will need to place the owner account in quotes in this format - "OPS$*domain\username*" where *domain\username* is the WFM schema owner

To configure an existing or sample Aspect Workforce™ database:

1. For Windows Server 2022 and 2025, select **Start** > **Aspect > WFM Database Manager**. The **Database Manager** window opens.
2. Select **Tools > Select RDBMS** and choose **Oracle 19c**.

3. Select Tools > Create Database Connection Alias. The **Configure Database Connection Alias** dialog box opens.
4. In the **Database Connection Alias** field, type the **name** you want to use for your database.
5. Click Lookup For The Connection String. The **Data Link Properties** dialog box opens.
6. Select Oracle Provider for OLE DB and click Next. The **Connection** page opens.
7. Click the **Data Source** field and type the **TNSNAME** for Oracle.
8. To test connectivity to your database, enter the **TCSDBOWNER user name** and the **password** you assigned to the TCSDBOWNER user name, and click **Test Connection,** and click **OK**.

   Note: For security reasons, you cannot save user names or passwords to the connection alias (using the Allow Saving Password option).
9. To close the Data Link Properties dialog box, click OK. The **Configure Database Connection Alias** dialog box opens.
10. Click the **Schema Name** field and type the **name** of the database owner; for example, TCSDBOWNER.
11. To close the **Configure Database Connection Alias** dialog box, click **OK**. The new database connection alias is saved.
12. To activate the database, select **File** > **Activate Database**.
13. If the database is at the current release schema, the database can be used. If the database is at a previous release schema, see Upgrading the Database .

Installing and Configuring WFM Services

After installing the main application server, complete the following post-installation procedures for the WFM services, WFM Listen, and the Aspect Message Routing Service.

Complete all procedures on the main application server, in the order shown below.

1. Install WFM services using the WFM Service Installer. See Using the WFM Service Installer.
2. If you installed the WFM Listen service, configure the service using the Listen Configuration Editor. See Using the Listen Configuration Editor.
3. If you installed the Aspect Message Routing Service for load balancing, configure the service using the Aspect Message Routing Platform Configuration Editor. See Configuring Aspect Message Routing.
4. If you installed the WFM Historical Connector, configure the service using the Historical Connector Configuration. See Using the WFM Historical Connector Configuration.

Using Email Reports

Email Reports replaces the Export to MAPI feature that was available in earlier versions of Aspect Workforce™. If you want to use Email Reports, see Enable Email Reports.

Upgrading

To upgrade the main application server for Aspect Workforce™, see Upgrading for Oracle.

Uninstalling

Uninstall the main application server for Aspect Workforce™ in either of the following ways:

- Use the Programs And Features feature in the Windows Control Panel.
- Use the Aspect Workforce™ installation program.

Uninstalling with Programs And Features

To uninstall with Programs And Features in Windows, use this path: **Start > Control Panel > Programs > Programs And Features > Workforce > Uninstall**

Uninstalling with the Installation Program

To uninstall the main application server with the installation program:

1. Log in as an administrator to the server designated as the **main application server.**
2. Insert the **Aspect Workforce™ Software CD** and open the file **Setup.exe.** The product selection window of the installation wizard opens.
3. Click **Aspect Workforce™**. The Welcome window of the **Install Wizard for Workforce** opens.
4. Click **Next**. The **Program Maintenance** dialog box opens.
5. Select **Remove and** click **Next**. The **Remove The Program** window opens.
6. Click **Remove**. The **Uninstalling Aspect Workforce™** window opens. When Aspect Workforce™ has been removed successfully, the **Install Wizard Completed** window opens.
7. Click **Finish**. If a reboot message is displayed, click **No** in the message, and reboot the server manually after exiting the wizard.

Installing and Configuring WFM Services

This chapter describes how to install and configure the Aspect Workforce™ services, including the WFM Listen service. It also describes the TCSSERVICES user account.

Using the WFM Service Installer

Use the Aspect Workforce™ Service Installer (WFM Service Installer) to install Aspect Workforce™ services on your main and, later, your secondary application server. After installation, these services will open in Windows Services. Typically, Aspect Workforce™ service names begin with *WFM*, such as *WFM Updater*.

WFM Information Server is automatically installed on your main application server by the installation program. You can install all services required for Aspect Workforce™ on your main application server. In a distributed installation, one or more secondary application servers can host any of the required or supplementary WFM services.

Identifying the Required Services

Install only the services required for your deployment of Aspect Workforce™. Some services are required in all deployments, while others are required only when you are using a specific enhancement package (such as Empower) or a specific feature (such as Segment Export).

The following table shows the available WFM services that are required for various deployments of Aspect Workforce™. (The WFM Listen service and the Aspect Message Routing Service, although listed in the table, are not installed or configured with the WFM Service Installer.) Some of the services are not visible in the WFM Service Installer unless you have installed the corresponding package, such as Encompass.

Required Services for Various Deployments

Service Name	Description	When Required
WFM Information Server	Provides configuration information to Aspect Workforce™ clients and application servers.	In all deployments. WFM Information Server is installed automatically, on the main application server only, by the Aspect Workforce™ installation program. No user action is required to install or configure this service.

Service Name	Description	When Required
WFM AutoRun	Automates routine tasks.	In all deployments. Install on multiple servers if the quantity and/or size of the AutoRun jobs exceeds the processing capacity of the AutoRun server.
WFM TallyServer	Provides continuous schedule resolution and state tallies.	In all deployments. Install on multiple servers when using Tally Server load balancing or when dedicating a specific Tally Server for a unique use, such as Real-Time Adherence servers.
WFM Updater	Provides transaction control for schedule updates.	In all deployments but can only be installed on either the main *or* secondary application server.
WFM ACD Processing services: • WFM ACD Proc • WFM Parser • WFM AP Proc • WFM AP Parser	Processes ACD data.	In all deployments but can only be installed on either the main *or* secondary application server. Installing this service requires you to review settings for two services: WFMACDPROC and WFMAPPROC.

WFM Checker	Provides request management validation.	In all deployments but can only be installed on either the main *or* secondary application server. WFM Checker is used only with Aspect Workforce™ Engagement Management for the Request Management modules.

Service Name	Description	When Required
WFM Express Checker	Provides express validation of overtime and time-off requests.	In all deployments but can only be installed on either the main *or* secondary application server. WFM Express Checker is used only with Aspect Workforce™ Engagement Management with the Request Management modules.

WFM Dispatcher Service	Dispatches internal messages among multiple controllers. Configured in WFM Service Installer and required to be specified in the AMR Configuration Editor. In WFM Service Installer, this service is not associated with specific databases.	Only if using: • Aspect Workforce™ Engagement Management • Empower • Encompass • Campaign Optimizer Adapter • WFM Checker load balancing • Aspect WFM Web Services Install on multiple servers when using Checker load balancing (that is, *distributed* Checker), or when load dictates additional WFM Dispatchers are required.
WFM Notification Queue Manager	Manages notification queue and forwards notifications to appropriate endpoint. Install one instance of this service for each database.	Only if using: • Notification Server • Encompass • Campaign Optimizer Adapter • email reports feature
WFM Request Status Change Event Generator  **Note:** This service is delivered by the Empower Installation Package.	Generates and analyzes WFM Checker request status change events.	Only if using Notification Server

Service Name	Description	When Required

WFM Schedule Change Event Generator  **Note:** This service is delivered by the Empower Installation Package.	Generates and analyzes schedule change events.	Only if using Notification Server
WFM Schedule Trade Event Generator  **Note:** This service is delivered by the Empower Installation Package.	Generates and analyzes schedule trade events.	Only if using Notification Server
WFM SMTP Notification Worker  **Note:** See Install the WFM SMTP Notification Worker Service for how to configure this service for emailing reports interactively and using WFM Autorun without the Empower add-on. Additional instructions for email notifications with Empower are in the *Empower Installation Guide*.	Manages interactive and Autorun pushed emails as well as Empower email notifications, formats them as needed, and sends them to RabbitMQ for delivery to the SMTP server.	When: • Emailing reports from WFM • Email Notifications from Notification Server or Workforce Engagement Management

WFM HTTP Notification Worker  **Note:** See the *Empower Installation Guide* for how to configure this service for Web Notifications.	Manages pushed web notifications to Workforce Engagement Management.	Only if using: • Notification Server • Web Notifications

Service Name	Description	When Required
WFM Mobile Notification Worker  **Note:** See the *Empower Installation Guide* for how to configure this service for Mobile Notifications.	Manages pushed mobile notifications, formats them as needed, and sends them to RabbitMQ for delivery to the mobile endpoint.	Only if using: • Notification Server • Mobile Notifications
WFM Universal Notification Worker  **Note:** See the *Empower Installation Guide* for how to configure this service for Universal Notifications.	Manages pushed universal notifications, formats them as needed, and sends them to RabbitMQ for delivery to the mobile endpoint.	Only if using: • Notification Server • Universal Notifications
WFM Segment Export DB Monitor	Monitors which segments are exported to Microsoft Exchange.	Only if using Segment Export

WFM Segment Export	Exports official segments to Microsoft Exchange as calendar appointments.	Only if using Segment Export
WFM Web Service Exporter	Exports WFM web service data to remote sites.	Only if using: • Encompass • Campaign Optimizer Adapter
WFM Web Service Importer	Imports queued WFM web service data from remote sites.	Only if using Encompass
WFM Outsourcer FS Monitor	Monitors a specified folder for new files containing XML import jobs.	Only if using Encompass
WFM Encompass Cloud Storage Monitor	Monitors a cloud storage repository for new files containing XML import jobs.	Only if using Encompass
Service Name	**Description**	**When Required**
eWFMData Scheduler  **Note:** This component is installed outside of WFM Service Installer. For additional information, see the *Aspect Connector for Avaya Aura Contact Center Integration Guide*.	Enables connections to multiple SCCS machines and to SCCS machines in different time zones.	Only if obtaining data from a Nortel Symposium Call Center Server (SCCS) or Avaya Aura Contact Center

WFM Alarm Provider	Connects to one or more RTA Alarm Calculators and receives the feed of activity and schedule conditions. The Alarm Provider applies WFM alarm rules to convert these conditions into activity and schedule alarms and updates them in the WFM database.	Only if using Perform
Aspect Message Routing Service[1]	Mediates messaging between the Dispatcher or TallyServer services and Aspect Workforce™.	Only if using: • Aspect Workforce™ Engagement Management • Load balancing for the Checker or TallyServer services. • Empower • Encompass • Campaign Optimizer Adapter • Aspect WFM Web Services
WFM Listen[2]	Retrieves ACD data and writes it to a location where it can be processed by the WFM Parser service.	In all deployments. Can be installed on either the main *or* secondary application server.

Service Name	Description	When Required

[1] The Aspect Message Routing Service is installed with the Aspect Workforce installer and configured with the AMR Configuration Editor. For more information, see Configuring the Aspect Message Routing Service.

[2] The WFM Listen service is installed with the Aspect Workforce installer and configured with the Listen Configuration Editor. For more information, see Installing and Configuring Listen.

WFM Historical Connectors  **Note:** The configuration utility to install these services is installed by the Aspect Workforce™ install package.	Used to retrieve ACD data from multiple ACD vendors, such as Five9, InContact, and Zendesk.	Only if obtaining data from the ACD vendors.

Requirements for Sample Database

In most cases, the Aspect Workforce™ sample database requires only AutoRun, Tally Server, and Updater to be set up in WFM Service Installer.

For detailed information about these services, see the *Aspect Workforce™ Planning Guide*.

Installing the WFM Services

Install the Aspect Workforce™ services on your main or secondary application server for each Aspect Workforce™ database by using the WFM Service Installer.

To install WFM services:

1. For Windows Server 2022 and 2025: Select **Start > Aspect > WFM Service Installer**. The WFM **Service Installer** window opens.
2. Select **Edit > Add**. The **Add Services** dialog box opens.
3. Select a **service** (for example, WFM AutoRun), and click **OK**.

   If you have more than one database, the **Select Databases** dialog box opens. Select the database (or multiselect databases) to use with the service.
   The service details dialog box for the selected service is displayed.
4. View the **settings** for the service, and click **OK** to accept the settings after noting the following:

- For the **WFM ACD Processing** service only, clicking OK to accept the settings opens the service details dialog box for a second service associated with this service, where you view the settings, and again click OK. The LocalService name for these two services is ACDProc.
- For the **WFM Updater** service, you can click the **Add** button and install Updater Plug-in Rules, such as the Minimum Shift Break Rule. For more information, see Using Updater Plug-In Rules.
- For the **WFM Dispatcher** service, no database associations are required. Instead, when you configure the Aspect Message Routing Service in Configuring the Aspect Message Routing Service, you associate this instance of the WFM Dispatcher Service with a service pool to handle work from Aspect Workforce™ components.
- For the **WFM Notification Queue Manager** service or any of the Notification Worker services, one instance of the service is required for each database.

- Do not modify any other default settings for any WFM services without consulting your Aspect Customer Care representative.

5. To add the same service for another database, select the service, select **Edit > Connect Database**, and select the **database**.
6. To add another service, go back to step 2.
7. When you are finished, select **Edit > Set COM Security Limits**. The Set COM Security Limits dialog box opens.
8. Click **OK** to set machine-wide security limits, as described in the box; otherwise, click **Cancel**.

   For more information about the effect of this setting, see Modifying COM Security Limits MachineWide.
9. Select **File > Save** and select **File > Exit**.

 **Caution:** In Windows Services, do not change the Startup Type for any WFM service to *Automatic (Delayed Start)*. Aspect Workforce™ does not support that startup type.

Configuring WFM Notification Queue Manager

If you have not already installed the WFM Notification Queue Manager service to support an Aspect Workforce™ enhancement package, such as Empower, do so now to help enable the Email Reports feature.

For the Email Reports feature to operate, you must use the WFM Service Installer to register and configure the WFM Notification Queue Manager service on an application server. This service manages the queue of messages in the Aspect Workforce™ database. The WFM Service Installer installs the service when you configure it, as described in this section. If you use Empower, the settings you configure here are used by Notification Server.

To configure the WFM Notification Queue Manager service:

1. On the main or secondary application server, open the WFM Service Installer, located at the following path: Windows Server 2022 and 2025: **Start** > **Aspect > WFM Service Installer**. The **Aspect Service Installer** window opens.
2. Select **Edit > Add.** The **Add Services** dialog box opens.
3. Select WFM Notification Queue Manager and click OK.

   If you have more than one Aspect Workforce™ database alias, the **Select Databases** dialog box opens. Select the desired **alias** from the list, and click **OK**. The **WFM Notification Queue Manager** dialog box opens.
4. Review and update (as necessary) the **default values** for the parameters listed in the table below.
5. Click **OK**.
6. Select **File > Save** to register the service with the Service Control Manager.

Parameter	Description	Default
UserName	The user account for Notification Server.  **Note:** The database configuration script that you manually executed when first installing Aspect Workforce™ creates the default username. Change the default username only if you modified the user name in the database configuration script.	NOTF_USER
Password	The password that Notification Server uses to connect to the Aspect Workforce™ database.  **Note:** The database configuration script that you manually executed when first installing Aspect Workforce™ creates the default password. Change the default password only if you modified the password in the database configuration script. To enter or change a password, click the button (**...**) at the far right of the Password row. Then, on the Password dialog box, type the **password**, confirm the password, and click **OK**. The encrypted password is displayed in the password field.	<encrypted>

QueueProcInterval	Specifies the interval (in seconds) between queuing the NOTF table for new notifications.	10
CIPUserName and CIPPassword	Specifies the **username** and **password** that the Contact Info Provider component uses to retrieve notification recipient information from the Aspect Workforce™ database.	NOTF_USER By default, both fields contain the same values as the UserName and Password fields. Do not change the CIPUserName or CIPPassword values unless you changed the

Parameter	Description	Default
		UserName and Password values.
CIPAlias	Specifies a valid Aspect Workforce™ database alias for the Contact Info Provider. This value is set automatically according to the selected database alias.	Do not change this value.
FAX	(Ignore. Reserved for future use.)	Do not change this value.

PAGER	(Ignore. Reserved for future use.)	Do not change this value.
PHONE	(Ignore. Reserved for future use.)	Do not change this value.
Integrated Security	Determines whether this service uses Windows Integrated Security for authentication. If your Aspect Workforce™ database is appropriately configured, you can configure this service to log on using a Windows domain account instead of the Local System account. In such a configuration, the domain account running the service is used to authenticate to your database, not the username listed for the service in the WFM Service Installer.	0 (disabled). To enable Integrated Security, change the default value from 0 to 1.
MaxMemKBytes	Specifies the maximum amount of memory, in kilobytes, that the service can use until the service is restarted.	200000

Parameter	Description	Default

RabbitHostUrl  **Note:** See RabbitMQ for details.	The URL for the RabbitMQ service. The port that is used for RabbitMQ is specified in the RabbitMQ.conf file and can be specified for the Notification Server Queue Manager in the RabbitHostUrl setting. The port is specified after the server name. This should be updated with the servername of the rabbitmq server (aka. rabbitmq://wfmappserverAspect.com<:*port/virtualHostname*>.) This could either be the IP address, server shortname, or fully qualified domain name (FQDN), depending on what works best in the customer's environment. FQDN is recommended. Port is required if TLS encryption is enabled and optional otherwise.	rabbitmq://localhost
RabbitUsername	The RabbitMQ username.	guest
RabbitPassword	The RabbitMQ password.	
HeartbeatTimespan	Specifies the heartbeat interval, in seconds, used to maintain the connection, to RabbitMQ. Setting this value to zero will disable heartbeats, allowing the connection to timeout after an inactivity period.	15 seconds

TransactionTimeout Timespan	Transactions are a way to encapsulate the pipe behavior in a transaction. This value sets the timeout (wait time) for the RabbitMQ transactions to be committed.	30 seconds
UseSsl	Specifies RabbitMQ connection type. Set to 0 for non-encrypted and 1 for encrypted. Contact Aspect Customer Care for assistance.	0
Parameter	**Description**	**Default**
SslProtocols	This value is used only if UseSsl is set to 1. If UseSsl is set to 0 (the default), this value is ignored. Contact Aspect Customer Care for assistance.	3072

Depending on your anti-virus software, you might need to exclude the **NotificationQueueManager.exe** process from being blocked. You can browse to this process at the following path: **C:\Program Files\Alvaria\Workforce\NotificationQueueManager.exe**

Install the WFM SMTP Notification Worker Service

Email Notifications require a worker service that must be installed on the same server as the Notification Queue Manager service. It is installed using the WFM Service Installer.

1. On the server with the Notification Queue Manager service, do the following:
   a. Windows Server 2022 and 2025: Select **Start > Aspect > WFM Service Installer**.
   b. The Aspect Service Installer window opens.

2. Select **Edit > Add**. The **Add Services** dialog box opens.
3. Select the **WFM SMTP Notification Worker** service and click **OK**.
   a. If you have more than one database, the **Select Databases** dialog box opens. Select the **database** to use with the service.
   b. This service has no parameters to configure.

Setting Registry Parameters for SMTP

If you have not already set the registry parameters to support an Aspect Workforce™ enhancement package, such as Empower, do so now to help enable the Email Reports feature. You will set the registry parameters on the server hosting the WFM Notification Queue Manager service.

To set the registry parameters for SMTP:

1. Log in to the application server with a domain account that is also a local administrator.
2. For Windows Server 2022 and 2025: Select **Start > Aspect > WFM SMTP Parameters Registry Editor**. The editor window opens.
3. Double-click the **first parameter** name in the list. The **Edit Registry Value** dialog box opens.
4. Configure each **parameter** in turn, using the guidelines in the following table. Typically, only the parameters in ***boldface italics*** require configuration.

Parameter Name	Description	Default Value
(Default)	Name of the Registry key.	eWFM Advanced Modules

Parameter Name	Description	Default Value
BaseURI	Ignore. This setting is used only for Notification Server in Empower. It does not apply to the Email Reports feature.	http://*web server name*/NotificationServer/eWfmSmtpDispatcher where *web server name* is the name of the Aspect Workforce™ web server

CircuitBreakerActiveThreshold	Circuit breaker is a mechanism to protect resources from being overloaded when there is a failure. A circuit breaker detects repeated failures and trips, preventing further calls to the service and giving it time to recover. This is the number of messages that must reach the circuit breaker in a tracking period before the circuit breaker can trip.	10
CircuitBreakerResetIntervalTimespan	The time between the circuit breaker trip and the first attempt to close the circuit breaker.	5 minutes
CircuitBreakerTrackingPeriodTimespan	The window of time before the success / failure counts are reset to zero.	1 minute
CircuitBreakerTripThreshold	This percentage is based on the ratio of successful to failed attempts. When set to 15, if the ratio exceeds 15%, the circuit breaker opens and remains open until the CircuitBreakerResetIntervalTimespan expires.	15
ConcurrencyLimit	The maximum number of messages consumed, concurrently (in parallel).	1
Encrypt	Indicates whether login credentials passed to the SMTP server are sent encrypted using SMTP over TLS.	0 (That is, *not* encrypted.)

Parameter Name	Description	Default Value
MaxRecipientsPerEmail	The limit on the number of recipients to which an email can be sent. **Note:** Some SMTP servers place a limit on the number of recipients in an email. The default is 50; multiple emails	50
	breaking up the recipients list will be sent based on this value. The value can be adjusted as needed. Contact your IT department for assistance.	
Password	The password for the Username account.	(No default value)
PrefetchCount	The number of unacknowledged messages that can be processed concurrently from our code.	1
RateLimit	The maximum number of messages consumed within a time period.	20
RetryCount	The retry count if there is a problem communicating with the dispatcher.	5
RetryInitialIntervalTimespan	The time period after which the first retry attempt will be made.	10 seconds
RetryInterval	The retry interval if there is a problem communicating with the dispatcher.	0

RetryIntervalIncrementTimespan	The time period after which, subsequent retry times will be made, until the limit is reached.	30
RetryLimit	The maximum number of retry attempts, before a message is sent to the _error queue.	3
SenderID	Can be any value but cannot be blank. For example, you can use the same value as the Username. This value is used to populate the From field in emails.[3]	(No default value)
SMTPPort	Port number on which to communicate with the SMTP server.	25
SMTPServer	IP address of your corporate SMTP server.	(No default value)

Parameter Name	Description	Default Value
Timeout	Maximum time to wait for the SMTP server to accept an email message.	1 second
Username	Valid account name (such as name@domain.com)	(No default value)

5. Close the **SMTP Parameters Registry Editor** window.

[3] Depending on your SMTP server policies, the SenderID might need to be either a properly formed but non-working account, or a fully valid account.

Installing ACD Streams

Use the WFM Service Installer to install one or more ACD streams. For assistance, contact Aspect Customer Care.

For more information about installing streams, see Using the Listen Configuration Editor and Setting Up Data Capture.

Installing and Configuring Listen

WFM Listen is a Windows system service that continually checks the ACD directories on the application server for new ACD data files. When a new file is found, Listen copies it to the appropriate directory where it is then processed by the WFM Parser system service. You typically install Listen on the server where your ACD writes its data files.

If you are using multiple databases, you must ensure that the ACD Stream IDs for each configured ACD are unique across all installed databases. See the *Aspect Workforce™ Online Help* for additional information on creating ACD instances.

Security Considerations

Note the following security considerations:

- If you use Listen to transfer files to the application server from a server where the ACD writes its data files, then Listen must use a named account to log in to that server. This configuration is known as Remote Listen.
- If you use Aspect Workforce™ Management Adapter (WFM Adapter) to retrieve data, and if the WFM Adapter is not installed on the main application server, you must set up Listen to run as a named account.

Installing the WFM Listen Service

If you have not already installed the WFM Listen service as part of your installation of the main application server for Aspect Workforce™, you can install it now, as explained below.

You can install the WFM Listen service on a main or secondary application server.

To install the WFM Listen service:

1. Insert the Aspect Workforce™ CD in the CD drive of either the main application server or the secondary application server.
2. Navigate to the CD root folder and double-click **Setup.exe**. The product selection window of the installation wizard opens.
3. Click **Aspect Workforce™**. If any prerequisite software is not already installed on the server, then the Aspect Prerequisite Installer window opens, displaying a list of prerequisite but uninstalled software. Click **Install** to install the prerequisite software. When installation is complete, the Welcome window of the **Install Wizard for Workforce** opens.
4. Click **Next**. The **Program Maintenance** window opens.

5. Select **Modify** and click **Next**. The C**ustom Setup** window opens.
6. Click the **Listen** icon, and select This Feature, And All Subfeatures, Will Be Installed On Local Hard Drive.
7. Click **Next**. The **Ready to Install** window opens, displaying a list of the DCOM servers.
8. Click **Install**. The installation proceeds, and afterwards the **Installation Complete** window opens.
9. Click **Finish**.

Using the Listen Configuration Editor

You can install the WFM Listen system service automatically when you install Aspect Workforce™. But whether you install this service during or after installing Aspect Workforce™, you must use the Listen Configuration Editor to *configure* the WFM Listen service afterwards.

Note: It is not necessary to configure Listen after an upgrade. If you upgrade Listen while upgrading Aspect Workforce™, your Listen configuration settings are persisted.

Configuring WFM Listen

To configure WFM Listen:

1. Log in as an administrator to the **server** where you installed Aspect Workforce™.
2. For Windows Server 2022 and 2025: Select **Start** > **Aspect > WFM Listen Configuration Editor**. The Listen Configuration windows opens.
3. Select **Edit > Add.** The **Select Streams** dialog box opens.
4. Select the **check box** next to each stream that you want to configure and click **OK**. The **ACD Streams Configuration** dialog box opens.
5. On the **General** page, view the following default settings, which you can modify only *after* you have added the stream:

- **Archive Limit (Days)** — Shows the **number of days** that ACD reports are to be kept in the data folder.

  These settings apply to all ACD streams you have selected. WFM Listen deletes files older than the number of days you specify here. But the longer you keep the Listen ACD data files, the more hard disk space is used. The default value of **7** days works well for most users.

- **Minimum Free Megabytes** — Shows the **number of MB of hard disk space** on the application server you want to remain unused.

  Since Listen copies an ACD report to the application server disk drive about every 30 minutes, the amount of space used by Listen files can quickly become large. Because the application server can become unstable when there is insufficient disk space, Listen checks this setting before each operation. If the available disk space is less than the minimum you specify here, Listen copies no additional information to the disk drive. The default value of **20** MB works well for most users.

6. Click a **stream number tab** (Stream1, Stream2, and so on) to the right of the General tab and select the **stream** in the Sources list.
7. Click **Edit**. The stream configuration window for the selected stream opens, with the stream number displayed in the window's title bar.
8. Select an option for the **Source Parameters** by using the following guidelines:

- **ACD File —** Select this option if Listen will retrieve ACD data from a directory on the application server or on another machine attached to your LAN (for example, the ACD).
- **Serial Port** — Select this option if Listen will retrieve ACD data for this stream using a direct connection to an application server serial port. Use this option if a serial cable connects the application server to the ACD.
- **Cloud Storage Container —** Select this option if Listen will retrieve ACD data from an Amazon S3, Azure, or Google cloud location.

9. Configure the source parameters as follows:

- For the ACD File option, see Configuring Source Parameters: ACD File
- For the Serial Port option, see Configuring Source Parameters: Serial Port.
- For Cloud Storage Container option, see Configuring Source Parameters: Cloud Storage Container.

  The source parameters displayed in the window are different, depending on which option you choose.

10. In the **Stream<#>** configuration window, select the **Copy Output To** check box if you want Listen to provide ACD data to an additional location. (For example, a lab server or a server in a multitenant installation.) If you select this box, you must also provide an output filename and location in the **Output ACD File** field.
11. Select **Additional Log Options** check boxes as desired.

    Note that each additional logging level uses additional system resources. Most users should select only the **All Warnings** and **File Open And Close** check boxes.
12. When you have finished configuring this stream, click **OK**. The **ACD Streams Configuration** window is displayed with the stream you configured.
13. Use other available **options** in this window as desired:

- To change the name of a stream, type the new **name** in the **Display Name** field

  For example, you might want to change the name for Stream1 to Aspect_Primary, and change Stream2 to Aspect_Backup.
- Use the **buttons** on the right of the page to Add, Edit, and Delete streams.

  For example, click **Add** to add a new stream to the selected stream page.

14. If you are finished with this stream page, click **OK**.
15. To configure another stream, go back to Select .
16. Select **File > Exit.**
17. Go to Setting Up Data Capture.

Configuring Source Parameters: ACD File

If you chose **ACD File** as your preferred option for source parameters (see step 8), use the following instructions to complete Configure the source parameters as follows:.

To configure source parameters in the ACD file:

1. In the **Input ACD File** field, verify the **path** and **file name** of the ACD data file that Listen is to retrieve.

   
   Note: The ProgramData path is editable in the installation process.
   Example:
   C:\ProgramData\Alvaria\Workforce\WFMData\Listen\Stream1\ACD01.ITF
   If the ACD is not configured to save reports directly to the application server (meaning that you are using Remote Listen instead), then this setting typically takes the following form: ***Server**Share**File*** where:

- ***Server*** is the name of the machine where ACD files are stored; that is, the name that the machine uses to identify itself on your LAN
- ***Share*** is the name of the shared folder where the ACD files are stored
- ***File*** is the path and file name assigned to ACD data files

2. Verify the **Output Filename**, which is rarely changed, or enter the **path** and **file name** of the ACD data file to be used for Listen output. The path and file name is:

   C:\ProgramData\Alvaria\Workforce\WFMData\TcsParser\Stream1
   Stream1.ITF

   
   Note: The ProgramData path is editable in the installation process.
   If the ACD is not configured to send reports directly to the application server, then this setting typically takes the following form:

   Server**Share**File

   where:

- ***Server*** is the name of the machine where ACD files are sent; that is, the name that the machine uses to identify itself on your LAN
- ***Share*** is the name of the shared folder in Aspect Workforce™ where the ACD files are sent: for example, WFMParser for storing forecasting, scheduling, and tracking data, and APParser for storing agent productivity data
- ***File*** is the path and file name assigned to ACD data files

3. Resume the procedure Configuring WFM Listen by going to step 10.

Configuring Source Parameters: Serial Port

If you chose Serial Port as your preferred option for source parameters (see step 8), use the following instructions to complete Configure the source parameters as follows:.

To configure source parameters for a serial port:

1. Use the **Baud Rate** drop-down list to select the speed at which the ACD will send data.

   For assistance with this setting, contact your ACD administrator.

2. Use the **COM Port** drop-down list to select the COM port *on this computer* that the ACD is connected to.

3. Click **Advanced** to specify advanced communication settings for this serial connection. The **Advanced Options** dialog box opens.

   For assistance with these settings, contact your ACD administrator.

4. Click **OK** to close the **Advanced Options** dialog box.

5. Go to step 10.

Configuring Source Parameters: Cloud Storage Container

If you choose Cloud Storage Container as your preferred option for source parameters (see step 8), use the following instructions to complete Configure the source parameters as follows:.

Note: Contact your cloud storage vendor for information on setting up the cloud storage container. WFM Listen will require read, write, and delete permissions.

Listen supports connecting to the following cloud storage options:

- Amazon Simple Storage Service (S3)
- Azure Blob Storage (ABS) • Google Cloud Storage (GCS) The process involves:

1. Configuring the cloud storage container connection information in Aspect Workforce™:

- Configuring Amazon Simple Storage Service (S3) in WFM in the Workforce User Guide
- Configuring Azure Blob Storage in WFM in the Workforce User Guide
- Configuring Google Cloud Storage (GCS) in WFM in the Workforce User Guide

2. Configuring the WFM Listen Cloud Source Definition

3. Configuring the Source Parameters for the Cloud Storage Container.

   Note: For more on required permissions, see Configuring the Source Parameters for the Cloud Storage Container in WFMListen Configuration.

Configuring the WFM Listen Cloud Source Definition

1. In WFM, navigate to Configuration > Data Capture > WFM Listen Cloud Sources.
2. Right Click on the right grid and select **Add**.
3. The WFM Listen Cloud Source Definition will open.
4. On the **General** tab enter the:

a. **Code** – The name of the WFM Listen Cloud Source Definition.

b. **Description** – A description of the WFM Listen Cloud Source Definition.

5. On the **Details** tab:

a. Monitor –

- Container – Select the Cloud Storage Container.
- Path prefix – Enter the path prefix utilized when configuring the reports. (eg. Reports)

b. Success Archive – (recommended) check the **Archive successful imports** check box

- Container – Select the Cloud Storage Container.
- Path prefix – Enter the path prefix for WFMListen to utilize when archiving successful reports. (eg. Success)

c. Failure Archive – (recommended) check the **Archive failed imports** check box

- Container – Select the Cloud Storage Container.
- Path prefix – Enter the path prefix for WFMListen to utilize when archiving failed reports. (eg. Fail)

Note: Do not utilize the same Path prefix as the Monitor for the Success and Failure Archive. This can cause Listen to pick these files up as new and infinitely process those files again. Utilize different Path prefixes.

6. On the **Memo** tab – Enter any descriptive text (as needed) referring to the WFM Listen Cloud Source Definition.

Configuring the Source Parameters for the Cloud Storage Container in WFMListen Configuration

Once the WFM Listen Cloud Source Definition is configured, in WFM Listen Configuration configure the Source Parameters for the desired stream:

1. Source Type – select Cloud storage container.
2. Configuration –

a. Select the ellipsis (…)

b. Login with a WFM Administrative account.

c. Enter or select the ellipsis (…) to choose the WFM Listen Cloud Source.

d. **Poll Interval** – (default 1:00) – Can be adjusted as needed based on the frequency that the ACD will be producing reports. This must match the ACD unit for the ACD instance. **e.** Click **OK.**

3. Verify the **Output Filename**, which is rarely changed, or enter the **path** and **file name** of the ACD data file to be used for Listen output. The path and file name are:
C:\ProgramData\Alvaria\Workforce\WFMData\TcsParser\Stream1\ Stream1.ITF

Note: The ProgramData path is editable in the installation process.
If the ACD is not configured to send reports directly to the application server, then this setting typically takes the following form: \\Server\Share\File where:

- ***Server*** is the name of the machine where ACD files are sent; that is, the name that the machine uses to identify itself on your LAN
- ***Share*** is the name of the shared folder in Aspect Workforce™ where the ACD files are sent: for example, WFMParser for storing forecasting, scheduling, and tracking data, and APParser for storing agent productivity data
- ***File*** is the path and file name assigned to ACD data files

4. Resume the procedure Configuring WFM Listen by going to step 10.

Setting Up Data Capture

To capture data from the ACD streams you added and configured in the Listen Configuration Editor, additional setup actions must be completed in the Aspect Workforce™ client software. For detailed instructions, see the *Aspect Workforce™ Online Help*.

To set up data capture:

1. Create an ACD instance for each stream.

   How: Use the ACD/Contact Server Instances module. See ACD/AP Instance References in WFM.

2. Install the ACD instances. (If you have enabled UAC, see Installing ACD Instances with UAC Enabled for more information.)

   How: Use the ACD/Contact Server Instances module. Installing the ACD instances installs parser scripts (used to parse the data from your ACD vendor) in the following folder for all installed ACD streams, where ***x*** is the stream number:
   C:\Program Data\Alvaria\Workforce\WFMData\TcsParser\Stream*x*\Scripts

   Note: The ProgramData path is editable in the installation process.

3. Create a contact data group for each appropriate split/gate sent by your ACD vendor.

   How: Use the Contact Data Group Definitions module.

   Note: If your ACD instance model is Aspect Unified IP, you can complete this step and step 4 from within the ACD/Contact Server Instances module.

4. Associate each contact data group with the appropriate forecast group.

   How: Use the Forecast Group Definitions module.

Installing ACD Instances with UAC Enabled

If you installed the WFM ACD Processing services with User Account Control enabled, then Aspect Workforce™ users must meet one of the following requirements to install an ACD instance:

- Launch Aspect Workforce™ using the Run As Administrator option. (To use this option, right-click the desktop icon for Aspect Workforce™, and select Run As Administrator from the shortcut menu.)
- Have permission to write to and modify all files and folders in the WFMData folder. A typical path to this folder is: C:\ProgramData\Alvaria\Workforce\WFMData

ACD/AP Instance References in WFM

When installing ACD/AP instances in WFM refer to the following table:

Device	Workforce ACD\AP Instance
Alvaria CX Suite	TCSLAN (See Capturing Historical Data from the Alvaria CX Suite)
Amazon Connect	AMZCONNECT
Aspect Unified IP	UNIFIEDIP
AVAYA AURA	NTSYMP
AVAYA CMS	LUCENT
AVAYA IQ	AVAYAIQ
Avaya Oceania	TCSLAN
Cisco	TCSLAN
*Custom	TCSLAN

Five9	TCSLAN
Genesys	TCSLAN
InContact	TCSLAN
KANA	KANA
Moxie	TCSLAN
Salesforce	TCSLAN
Twilio	TCSLAN
Ujet	TCSLAN
ZenDesk	TCSLAN

Note: This is a sample list of the most currently utilized ACD vendors. If an ACD is not listed, contact the ACD vendor and/or Aspect Professional Services for assistance. For more on the TCSLAN instance refer to the *Aspect Workforce™ Data Interface Specifications Guide*.

Capturing Historical Data from the Alvaria CX Suite

For Alvaria CX Suite, the historical reports to follow the TCSLAN format. See the *Aspect Workforce™ Data Interface Specifications Guide*.

For information on how these statistics are tabulated, contact Alvaria Customer Care and ask to speak to a representative for your Alvaria CX Suite.

Concerning per-interval ACD Reports

From the TCSLAN specification, Alvaria CX Suite provides a TCSDATA report covering all campaigns for the configured contact types (Inbound, Outbound, Email, Chat) at the desired interval - 15, or 30 minutes. Configure the ACD Instance to match the timezone of the Alvaria CX Suite data and the reporting interval of the TCSDATA report provided.

- When configuring Alvaria CX Suite to send data to WFM, request the Aspect Professional Services representative sends most currently available “NEW” format.

- When configuring Contact Data Groups, use the **DEF01** formula set for all contact types.
- As of CX Suite 23.1.1, Alvaria CX does provide outbound, email, and chat campaign information (Number of Right-Party Contacts, Average Handle Time of Right-Party Connects, Number of Contacts Attempted, etc.). Contact Alvaria Customer Care for assisance.

Alvaria CX does not provide an SGDATA report, but the TCSDATA report does contain an Average Positions Staffed (APS) statistic from the perspective of the campaign and not a workgroup.

If the APS statistic is desired, when configuring Agent Data Groups, use the **DEF01** formula set.

Note: This statistic is most accurate if the agents are only assigned to a single campaign. If agents can be assigned to multiple campaigns at the same time, then the APS statistic becomes less meaningful. Adding multiple campaigns as agent data groups under a single staff group will produce an inaccurate APS statistic.

Concerning Daily Agent Productivity Reports

Alvaria CX will provide a daily Agent Productivity report with agent login\logout and activity information following the TCSLAN format.

When configuring the Agent Productivity instance in WFM, use the **DEF01** formula set.

- As of CX Suite 23.2.1, Alvaria CX Suite can provide “soft” sign outs for Lunches, Breaks, Meeting, etc. If you wish to accurately monitor agent adherence to on-phone activities in Aspect Workforce™, it is recommended to configure Alvaria CX for these “soft” signouts. Otherwise, agents will be required to sign off the Alvaria CX Suite during these off-phone activities. Contact Alvaria Customer Care for assistance.

Using the WFM Historical Connector Configuration

After installing the Aspect Workforce™ Historical Connectors feature on your Aspect Workforce™ main or secondary application server, you use the WFM Historical Connector Configuration utility to configure and install services for the cloud-based ACDs.

Note: The configuration utility to install these services is installed by the Aspect Workforce™ install package.

Configuring WFM Historical Connectors

To configure WFM Historical Connectors:

1. Log in as an administrator to the **server** where you installed Aspect Workforce™.
2. For Windows Server 2022 and 2025: Select **Start** > **Aspect > WFM Historical Connector Configuration**. The Historical Connector Configuration windows opens.
3. Select **File** > **New Historical Connector...** The **Choose Historical Connector** dialog box opens.

4. Select the **Connector type** from the available drop-down options that you want to configure, and click **OK**. The **Edit ACD Configuration** dialog box opens.

   There are three available options in the drop-down list. These are Five9, InContact and Zendesk.

- To add a Five9 Historical Connector, see Adding a Five9 Historical Connector.
- To add an InContact Historical Connector, see Adding an InContact Historical Connector.
- To add a Five9 Historical Connector, see Adding a Zendesk Historical Connector.

5. After entering the details for the selected connector on the **Edit** page, click **OK**.

Adding a Five9 Historical Connector

You can configure the following settings for a Five9 Historical Connector:

Parameter	Description	Default
Service settings:		
Instance name	Enter a descriptive label.	
Log On As....	Click this button to configure Log On As credentials for the service.	Local System
Automatically start	Select this checkbox to configure the service to start automatically at system start and when you save changes.	(checked)
Automatically restart	Select this checkbox to configure service recovery options that will restart the service-on-service failure.	(checked)
Five9 parameters:		

Username	Five9 User Name (identifies the Five9 tenant).	
Password	Five9 API password.	

Parameter	Description	Default
Five9 time zone	Enter the IANA time zone of data displayed in the Five9 custom reports. For the list of IANA time zones, see https://nodatime.org/TimeZones. **Note:** See Configuring Five9 Custom Reports: for the list of applicable custom reports.	US/Pacific
Report time zone	Time zone of the WFM ACD reports produced by the connector. The report time zone is also an IANA time zone that can be selected from the Noda Time list. For the list of IANA time zones, see https://nodatime.org/TimeZones. **Note:** The time zone must match the equivalent Aspect Workforce™ time zone specified for the ACD Instance. Aspect Workforce™ does not use the IANA time zone list, but instead, maintains an independent list of time zones relevant to Aspect Workforce™. Use the time zone label and bias (i.e. offset from UTC/GMT) in Aspect Workforce™ to identify the appropriate IANA time zone. For example, the Aspect Workforce™ time zone of "(UTC-05:00) Eastern Time (US & Canada)" is the equivalent IANA time zone of "US/Eastern."	US/Eastern

Call log report delay (sec)	Specify the time in seconds to wait for the call log report to complete within Five9.	200
General report delay (sec)	Specify the time in seconds to wait for other reports to complete within Five9.	150
Max retries	Specify the maximum attempts made to generate custom Five9 reports.	2
Max report span	Specify the maximum time span of report. You may need to configure a limit for larger Five9 tenants.  **Note:** Five9 API limit is 50,000 report rows.	24:00
Call Log pre buffer		2:00
Report timeout	Maximum time (h:mm) to wait for the Five9 system to generate a custom report.	0:15

Parameter	Description	Default
Max login ID length	Maximum length of the Login ID field. (0 to 255)	7

Login ID	Select how WFM will recognize agent's in Five9 – Agent ID or Agent User Name. (see Note1)	Agent ID
Limit User - Skill Lookups	When the Five9 historical connector calculates an agent's contribution to Average Positions Staffed (APS), it divides the agent's signed-in time among the skills in which the agent worked. If none of an agent's signed-in time during a reporting interval is associated with a skill, Example., If the agent was available for the entire reporting interval, the Five9 historical connector divides the agent's signed-in time evenly across the skills assigned to the agent. To determine the agent's skill assignments, the Five9 historical connector calls the getUsersInfo web service. If the Limit user-skill lookups checkbox is unchecked, the Five9 historical connector will load user-skill assignments for all agents with a single call to getUsersInfo. If your Five9 system has too many agents, this call may fail with an API timeout. In that case, you can check the Limit user-skill lookups checkbox and the getUsersInfo will be limited to agents whose username matches the first Search prefix length characters of the agent's username. Checking Limit user-skill lookups and increasing Search prefix length will reduce the number of users loaded per getUsersInfo call, reducing the likelihood of a timeout. This will also increase the number of getUsersInfo calls required, which may eventually exceed the Five9 API limit for the getUsersInfo web service.	(unchecked)
Search prefix length	Used in conjunction with the Limit User – Skill Lookups checkbox. (See above description.)	1

Admin Web Service Endpoint	The URL used to call the Five9 Admin web services. The default URL, https://api.five9.com:443/wsadmin/v9_5/AdminWebService, is appropriate for Five9 instances in the US region. For Five9 instances in other regions, you should supply the appropriate regional endpoint URL. Consult with your Five9 representative for more information.  **Note:** The Five9 connector service was built to target version 9.5 of the Five9 web services, so your URL should include v9_5.	https://api.five9.com:443/wsadmin/v9_5/AdminWebService

Parameter	Description	Default
User-skills cache lifetime	The maximum amount of time user-skills are retained in the cache to reduce the number of calls to the getUsersInfo webservice and prevent the connector from making multiple overlapping calls.	1:00:00
Skills cache lifetime	The maximum amount of time skills are retained in the cache to reduce the number of calls to the getUsersInfo webservice and prevent the connector from making multiple overlapping calls.	1:00:00
Infer sign outs	Select the **Infer sign outs** checkbox and click the **Reasons...** button. • Can configure not-ready reasons that should be treated as signing out. • Reason codes are not case-sensitive. • Only used by Agent Productivity. Average Position Staffed (APS) calculation removes all not-ready spans.	(unchecked)
Report parameters:		

Reporting interval	Reporting Interval (15, 30, or 60 minutes) of the data in the interval report.  **Note:** Must match the ACD unit of the Aspect Workforce™ ACD Instance.	30
Days to keep local output	For diagnostic purposes.	7
Interval report delay (sec)	Number of seconds to wait after the end of a reporting period before attempting to produce the report.	0
Interval reship time	Every day at the Interval reship time, the Historical Connector reships all of yesterday's interval data (to capture long-running calls).	3:00 AM
Agent productivity start time	Not used.  **Note:** The Agent productivity report always covers 24 hours.	12:00:00 AM
Agent productivity end time		11:59:59 AM
Parameter	**Description**	**Default**
Agent productivity output time	Every day at Agent productivity output time, ship Agent Productivity report.	12:01 AM
Days to reship on start	Number of days of interval and Agent Productivity reports to reship when the Historical Connector service starts. Used in conjunction with *Run historical immediately* option.	0

Run historical immediately	If checked, the Historical Connector will reship data immediately after restart. Use this option to reship missing data. **Note:** • Always reships interval data for the current day plus the number of days specified in *Days to reship on start* option. • *Days to reship on start* option is ignored if you don't check Run historical immediately option. • You cannot reship a selected range of times or days.	(checked)
Hours to reship each interval	The number of hours reshipped on each interval.	2
Delivery Options:		
Pickup folder	Copy to the WFM Listen stream folder or to a local folder that WFM Listen picks up from a share. Default based on where WFM Parser is installed. • Local folder if installed locally • UNC path if installed remotely	C:\ProgramData\Aspect\Workforce Management\WFMData\Listen\Stream1
WebDAV	Copy files to a WebDAV "stream" location that the WFM Listen service picks up from. Provide the Username, Password, and WebDAV URL	

Note1: The Five9 Historical and RTA connectors were originally designed by APS to send a numeric agent ID as the ACD login ID in the AP report and in RTA state changes. This was because the numeric ID can be at most 20 characters long, so it was suitable for older WFM versions where the max ACD login ID length was 20 characters. The more natural way to identify Five9 agents is by agent username (normally an email address). Agent username is more visible to Five9 users. WFM Historical Connector Configuration and RTA Server Configuration have been updated to support configuring the login ID for Five9. The Login ID combo box can be configured as Agent ID (default) or Agent User Name. Users that select Agent User Name should also configure Max login ID length as 255 (the maximum length of an email address).

Five9 Historical Connector Reports

Interval Report

WFM data Element	Five9 Reports	Five9 Columns	Calculation if Element is Calculated	Data Source	Web Service Used
Time Stamp			Start Date of the reporting interval		
Period			End time of the reporting interval		
"TCSDATA" Constant/Literal	NA	NA	NA	NA	NA
Contact Group ID	CustomCall-Log CustomInbound-Calls-by30-Intervalby-Date	SKILL		Call Log	AdminWebService runReport
Contacts Offered (NCO)	CustomCall-Log CustomInbound-Calls-by30-Intervalby-Date	CALL ID	NCO1 = (Count CALL ID where CALL ID Is unique) from CustomCall-Log NCO2 = CALLS from Custom-Inbound-Calls-by-30-Intervalby-Date NCO = max(NCO1, NCO2)	Call log	AdminWebService runReport

Contacts Handled (NCH)	CustomCall-Log CustomInbound-Calls-by30-Intervalby-Date	CALL ID, AGENT, DISPOSITION	NCH1 = (Count CALL ID where CALL ID is Unique and where AGENT Not [None] and DISPOSITION does not contain 'Transfer') from Custom-Call-Log NCH2 = NCO2 - ABD2 NCH = max(NCH1, NCH2)	Call Log	AdminWebService runReport
Average Talk Time (ATT)	Custom-Call-Log	TALK TIME LESS HOLD AND PARK	If (NCH1 <= 0) ATT = 0 else	Call Log	AdminWebService runReport

WFM data Element	Five9 Reports	Five9 Columns	Calculation if Element is Calculated	Data Source	Web Service Used
			ATT = (Sum TALK TIME LESS HOLD AND PARK) / (NCH1)		

Average After Contact Work Time (ACWT)	Custom-Call-Log	AFTER CALL WORK TIME	If (NCH1 <= 0)
			ACWT = 0
			else
			ACWT = (Sum AFTER CALL WORK TIME)/ (NCH1)
				Call Log	AdminWebService runReport

Average Delay (ASA)	Custom-Call-Log	SPEED OF ANSWER	If (NCH1 <= 0)
			ASA = 0
			else
			ASA = (Sum SPEED OF ANSWER) / (NCH1)
				Call Log	AdminWebService runReport

Percent Service Level (%SL)	CustomCall-Log CustomInbound-Calls-by30-Intervalby-Date	CALL ID, SERVICE LEVEL	SLCount = SERVICELEVELcount from Custom-Inbound-Calls-by-30Interval-by-Date If SLCount <= 0 %SL = (((Count CALL ID where SERVICE LEVEL = 1)/(NCO1)) * 100) else %SL = (SLCount / NCO1) * 100	Call Log	AdminWebService runReport
Average Positions Staffed (APS)	Custom-Agent-StateReport	TIMESTAMP, STATE, REASONCODE	APS = sum of signedin time by SKILL / length of reporting interval See below for details	Agent	AdminWebService runReport getUsersInfo

Actual Abandons (ABD)	CustomCall-Log
	CustomInbound-Calls-by30-Intervalby-Date
		CALL ID, DISPOSITION	ABD1 = (Count CALL ID where CALL ID is unique and DISPOSITION = 'Abandon')
			ABD2 = ABANDONEDcount from Custom-Inbound-Calls-by-30Interval-by-Date
			If (ABD2 <= 0)
			ABD = ABD1
			Else
			ABD = ABD2
				Call Log	AdminWebService runReport

Average Positions Staffed (APS) Calculation

To calculate APS, the connector looks at the rows of the Custom-Agent-State-Report. It builds up a list of time endpoints for each agent. It records the following information for the time endpoints:

- Start time – the TIMESTAMP column on the report.
- Endpoint type – if (STATE = 'Logout') or ((STATE = 'Not Ready') and (REASONCODE is in the configured list of signed-out reasons), then the endpoint type is a logout, else the endpoint type is a login.
- Skill – the SKILL column on the report. A SKILL of '[None]' means the state span is not associated with a particular skill.

Next, the connector constrains the lists of endpoints to the reporting interval. If the agent was signed in before the start of the reporting interval, the start time of that endpoint is changed to the start of the

reporting interval. If the agent is signed in at the end of the reporting interval, the connector adds a logout endpoint with a Start time that matches the end of the reporting interval.

For example, assume Custom-Agent-State-Report contains the following rows for an agent. Assume 'Break' is marked as a signed-out reason. The connector is generating a WFM report for the 8:00 AM – 8:30 AM interval, but it ran the Custom-Agent-State-Report for 7:00 AM – 9:00 AM (as part of a reship of the previous 2 hours).

TIMESTAMP	SKILL	STATE	REASONCODE
7:00:00 AM	[None]	Logout	End Shift
7:35:00 AM	[None]	Login	
7:35:00 AM	[None]	Not Ready	Not Ready
7:35:30 AM	[None]	Ready	
8:05:00 AM	Skill1	Ringing	
8:05:30 AM	Skill1	On Call	
8:07:00 AM	Skill1	After Call Work	
8:07:30 AM	[None]	Ready	
8:09:00 AM	[None]	Not Ready	Break
8:24:00 AM	[None]	Not Ready	Project
8:45:00 AM	[None]	Logout	End Shift

The connector calculates the following time endpoints for this agent:

Start Time	Endpoint Type	Skill
8:00:00 AM	Login	[None]
8:05:00 AM	Login	Skill1
8:05:30 AM	Login	Skill1

8:07:00 AM	Login	Skill1
8:07:30 AM	Login	[None]

Start Time	Endpoint Type	Skill
8:09:00 AM	Logout	[None]
8:24:00 AM	Login	[None]
8:30:00 AM	Logout	[None]

The connector combines adjacent login spans for the same skill:

Skill	Login Time	Logout Time
[None]	8:00:00 AM	8:05:00 AM
Skill1	8:05:00 AM	8:07:30 AM
[None]	8:07:30 AM	8:09:00 AM
[None]	8:24:00 AM	8:30:00 AM

The connector now sums the signed-in time for the agent by skill. For this agent we get:

- Skill1 – 2:30
- [None] – 12:30

If the agent did any skill work, the time attributed to the [None] skill is distributed to the skills they worked. In this case, all of the agent's signed-in time would be counted against Skill1. If the agent worked on multiple skills, the non-skill time is distributed in the same proportions as the skill work. For example, assume the agent's skill times look like:

- Skill1 – 5:00
- Skill2 – 10:00
- [None] – 9:00

The agent spent 15 minutes total working on skills, so the non-skill time would be divided as follows:

- 5/15 = 1/3 of the time for Skill1, i.e., 3:00
- 10/15 = 2/3 of the time for Skill2, i.e., 6:00

So, the agent would contribute 8 minutes of time to Skill1 and 16 minutes of time to Skill2.

If the agent spent no time during the reporting interval working on any skills, e.g., they were in the Ready state for the entire reporting interval, then the agent's time will be divided evenly among the skills assigned. The agent skill assignments come from the getUsersInfo web service.

When the connector evaluates all agents, it will have a total signed-in time value for each skill. The APS value for the skill is: Total signed-in time / the length of the reporting interval

For example, say 3:45:27 is the total signed-in time for Skill1. 3:45:27 = 3*60*60 + 45*60 + 27 = 13527 seconds. In this example, the reporting interval is 30 minutes, 1800 seconds, so the APS values for Skill1 is: 13527 / 1800 = 7.515

Ignoring Custom-Inbound-Calls-by-30-Interval-by-Date

Several of the statistics on the interval report can come from Custom-Call-Log or Custom-Inbound-Callsby-30-Interval-by-Date. If you choose to ignore the values on the Custom-Inbound-Calls-by-30-Intervalby-Date report, you can edit that report definition and add a filter that will match no rows. In that case, the report will still have the required format, but the connector will calculate all statistics as 0's for all skills on that report, so the connector will use the statistics calculated from the Custom-Call-Log report.

Agent Productivity Report

WFM data Element	Five9 Reports	Five9 Columns	Calculation if Element is Calculated	Data Source	Web Service Used
Agent ID	Custom-AgentTime-Card Custom-Agent-State-Report	AGENT ID Last max login ID length characters		Agent	AdminWebService runReport
ACD Group ID	Custom-Agent-State-Report	SKILL 30 characters maximum	If the agent worked on 1 or more skills during the SIT/SOT span, statistics for those skills will be calculated. Otherwise, a row of 0 statistics will be displayed for a skill of "0".	Agent	AdminWebService runReport
Sign-In Time (SIT)	Custom-AgentTime-Card Custom-Agent-State-Report	LOGIN TIMESTAMP	See below	Agent	AdminWebService runReport
Sign-Out Time (SOT)	Custom-AgentTime-Card Custom-Agent-State-Report	LOGOUT TIMESTAMP	See below	Agent	AdminWebService runReport

Number of Contacts Handled (NCH)	Custom-Agent-State-Report	CALL ID, SKILL	For each SKILL, for rows where TIMESTAMP falls within the SIT/SOT pair. NCH = (Count CALLID where CALL ID Is unique)	Agent	AdminWebService runReport
Average Talk Time (ATT)	Custom-Agent-State-Report	TALK TIME LESS HOLD AND PARK	For each SKILL, for rows where TIMESTAMP falls within the SIT/SOT pair. ATT = (Sum TALK TIME LESS HOLD AND PARK) / (NCH)	Agent	AdminWebService runReport
Average After-Contact Work Time (AWT)	Custom-Agent-State-Report	AFTER CALL WORK TIME	For each SKILL, for rows where TIMESTAMP falls within the SIT/SOT pair.	Agent	AdminWebService runReport

WFM data Element	Five9 Reports	Five9 Columns	Calculation if Element is Calculated	Data Source	Web Service Used
			AWT = (Sum AFTER CALL WORK TIME)/ (NCH)		
Number of Outbound Contacts (NOC)	Custom-Agent-State-Report	CALL ID, CALL TYPE	Where TIMESTAMP falls within the SIT/SOT pair. NOC = (Count CALL ID where CALL ID is unique and CALL TYPE= 'Manual')	Agent	AdminWebService runReport

Average Outbound Talk Time (AOTT)	Custom-Agent-State-Report	CALL TYPE, TALK TIME LESS HOLD & PARK	Where TIMESTAMP falls within the SIT/SOT pair. AOTT = Sum TALK TIME LESS HOLD AND PARK where STATE = 'On Call' and CALL TYPE= 'Manual')/ (NCH)	Agent	AdminWebService runReport
Average Outbound After-Contact Work Time (AOWT)	Custom-Agent-State-Report	AFTER CALL WORK TIME, CALL TYPE	Where TIMESTAMP falls within the SIT/SOT pair. AOWT = (Sum AFTER CALL WORK TIME where STATE = 'After Call Work' and CALL TYPE= 'Manual')/ (NCH)	Agent	AdminWebService runReport
Available Time (AVL)	Custom-Agent-State-Report	NOT READY TIME	Where TIMESTAMP falls within the SIT/SOT pair. AVL = (SOT - SIT) - (Sum NOT READY TIME)	Agent	AdminWebService runReport
Unavailable Time (UNAVL)	Custom-Agent-State-Report	NOT READY TIME	Where TIMESTAMP falls within the SIT/SOT pair. UNAVL = (Sum NOT READY TIME)	Agent	AdminWebService runReport
WFM data Element	**Five9 Reports**	**Five9 Columns**	**Calculation if Element is Calculated**	**Data Source**	**Web Service Used**
Plugged-In Percentage (PIP)	Custom-Agent-State-Report	WAIT TIME	Where TIMESTAMP falls within the SIT/SOT pair. PIP = ((((SOT - SIT) - (Sum WAIT TIME)) / (SOT - SIT)) *100)	Agent	AdminWebService runReport

Calculating Sign-In Time (SIT) and Sign-Out Time (SOT)

The connector calculates SIT/SOT values by agent by looking at two reports: Custom-Agent-Time-Card and Custom-Agent-State-Report. The first pass of SIT/SOT values comes from Custom-Agent-TimeCard. If you configure a list of signed-out reasons, then the connector looks at Custom-Agent-StateReport for any Not Ready STATE spans with a REASONCODE that matches one of the signed-out reasons. If it finds any, it adds a sign-out at the start of the Not Ready span and a sign-in at the end of the Not Ready span.

Interval Report Columns

- C1: NCO
- C2: NCH
- C3: ATT (based on TALK TIME LESS HOLD AND PARK)
- C4: AWT
- C5: Average Delay
- C6: Service Level %
- C7: APS
- C8: Abandons
- C9: Average Conference Time (calculated if CONFERENCE TIME is on the Custom-Call-Log report, 0 otherwise)
- C10: Average Hold Time (calculated if HOLD TIME is on the Custom-Call-Log report, 0 otherwise)
- C11: Average Park Time (calculated if PARK TIME is on the Custom-Call-Log report, 0 otherwise)
- C12: Average Consult Time (calculated if CONSULT TIME is on the Custom-Call-Log report, 0 otherwise)

Agent Productivity Report Columns

- C1: SIT
- C2: SOT
- C3: NCH
- C4: ATT (based on TALK TIME LESS HOLD AND PARK)
- C5: AWT
- C6: PIP
- C7: NOC
- C8: OTT (based on TALK TIME LESS HOLD AND PARK)
- C9: OWT
- C10: Available Time
- C11: Unavailable Time
- C12: Average Conference Time (calculated if CONFERENCE TIME is on the Custom-Agent-StateReport report, 0 otherwise; calculated for calls counted in NCH)

- C13: Average Hold Time (calculated if HOLD TIME is on the Custom-Agent-State-Report report, 0 otherwise; calculated for calls counted in NCH)
- C14: Average Park Time (calculated if PARK TIME is on the Custom-Agent-State-Report report, 0 otherwise; calculated for calls counted in NCH)
- C15: Average Outbound Conference Time (calculated if CONFERENCE TIME is on the CustomAgent-State-Report report, 0 otherwise; calculated for calls counted in NOC)
- C16: Average Outbound Hold Time (calculated if HOLD TIME is on the Custom-Agent-State-Report report, 0 otherwise; calculated for calls counted in NOC)
- C17: Average Outbound Park Time (calculated if PARK TIME is on the Custom-Agent-State-Report report, 0 otherwise; calculated for calls counted in NOC)
- C18: Average Consult Time (calculated if CONSULT TIME is on the Custom-Agent-State-Report report, 0 otherwise; calculated for calls counted in NCH)
- C19: Average Outbound Consult Time (calculated if CONSULT TIME is on the Custom-Agent-StateReport report, 0 otherwise; calculated for calls counted in NOC)

By default, the CONSULT TIME column will not appear in the Custom-Agent-State-Report report. Customers must add this column if they want to use Average Consult Time/Average Outbound Consult Time in their ATT/OTT calculations.

Report Scheduling Notes

- Every 30 minutes, the Historical Connector automatically generates the latest interval report(s). If you have selected a Reporting Interval of 15 minutes, then two 15-minute reports will be generated every 30 minutes.
- Every two hours, the Historical Connector automatically reships the previous two hours of interval data (to capture long-running calls).

Configuring Five9 Custom Reports

The Five9 historical connector depends on the following Five9 custom reports:

- Custom-Call-Log – used by interval report.
- Custom-Agent-Skill-Login-Time – used by interval report.
- Custom-Agent-State-Report – used by interval and Agent Productivity reports.
- Custom-Inbound-Calls-by-30-Interval-by-Date – used by interval report.
- Custom-Agent-Time-Card – used by Agent Productivity report.

Aspect has a set of reference Five9 reports that show how these custom reports should be configured.

Aspect Professional Services can configure these custom reports in your Five9 system.

Five9 Web Services

Aspect Workforce™ reports based on custom Five9 report data.

The Historical Connector makes the following web service calls to:

- Run a custom Five9 report, runReport.

- Test whether a custom Five9 report has completed, isReportRunning.
- Download custom Five9 report data, getReportResultCsv.
- Get the list of skills (Five9 work type), getSkills. So, the Historical Connector can supply 0's for skills with no work.
- Load the skill assignments of Five9 users (agents), getUsersInfo

Adding an InContact Historical Connector

You can configure the following settings for an InContact Historical Connector:

Parameter	Description	Default
Service Settings:		
Instance name	Enter a descriptive label.	
Log On As....	Click this button to configure Log On As credentials for the service.	LocalSystem
Automatically start	Select this checkbox to configure the service to start automatically at system start and also when you save changes.	(checked)
Automatically restart	Select this checkbox to configure service recovery options that will restart the service-on-service failure.	(checked)

Authentication	Parameter	Description	Default

InContact Parameters:					
Legacy	**CXOne**	**CXOne with OpenID**	**Note:** The will determine w Authentication mode available. ıich Parameters are		Legacy
X	X	X	API Version	Web service version, part of the web service URL. May vary across tenants.	v13.0

Authentication			Parameter	Description	Default
	X	X	Discovery URL	Discovery URL for CXOne. Contact your IT Department for assistance.	https://na1.niceincontact.com/.wellknown/cxoneconfiguration
X			Username	InContact Username identifies the InContact API user.	
X			Password	InContact API password.	

		X	Client ID	Web service Client ID for the CXone with OpenID API. Contact your IT Department for Assistance.	
		X	Client Secret	Web service Client secret for the CXOne with OpenID API. Contact your IT Department for Assistance.	
	X	X	Access key ID	Access key ID for the CXone API. Contact your IT Department for Assistance.	
	X	X	Access key secret	Access key secret for the CXone API. Contact your IT Department for Assistance.	

X			Base URL	Base URL is for authorization requests.  **Note:** The default value may	https://api.incontact .com/InContactAuth orizationServer/

Authentication			Parameter	Description	Default
				work, but you may need to change the URL based on your InContact configuration.	
X			Service base URL	For web services, the default URL may work, but you may need to change the URL based on your InContact configuration.	https://api.incontact.com/inContactAPI/services/
X			Vendor name	Part of the authorization key supplied to InContact.	Aspect
X			Application name	Part of the authorization key.	AspectWFM

X			Application secret	Part of the authorization key.  **Note:** You will need to register an API application for the InContact historical connector to use in the InContact system. Supply the values you used when registering the API application.	

Authentication	Parameter	Description	Default

X			Report time zone	Time zone of the WFM ACD reports produced by the connector. The report time zone is also an IANA time zone that can be selected from the Noda Time list. For the list of IANA time zones, see https://nodatime.org/TimeZones  **Note:** The time zone must match the equivalent Aspect Workforce™ time zone specified for the ACD Instance. Aspect Workforce™ does not use the IANA time zone list, but instead, maintains an independent list of time zones relevant to Aspect Workforce™. Use the time zone label and bias (i.e. offset from UTC/GMT) in Aspect Workforce™ to identify the appropriate IANA time zone. For example, the Aspect Workforce™ time zone of "(UTC05:00) Eastern Time (US & Canada)" is the equivalent IANA time zone of "US/Eastern."	US/Eastern

X	X	X	Infer sign outs	Check this checkbox to allow certain Reasons to be inferred as sign	(unchecked)

Authentication			Parameter	Description	Default
				outs. The **Reasons** button is disabled unless this is checked.	
X	X	X	Reasons	The list of Reasons you would like to infer as sign-outs. One reason code per line.	(disabled)
X	X	X	Short call threshold (sec)	Threshold for counting an abandoned call as a short abandon.	15
X	X	X	Agent timecard report ID	ID of custom InContact report.	10
X	X	X	Agent state log report ID	ID of custom InContact report.	350083
X	X	X	Call details report ID	ID of custom InContact report.	48

X	X	X	Skills to Exclude from APS	Time spent working on skills listed here will be divided among the agent's nonexcluded skills when calculating APS.	
X	X	X	Agent-skills cache lifetime	The length of time to cache agent skill assignments defined in the inContact system.	00:30:00
X	X	X	Skills cache lifetime	The length of time to cache the list of skills defined in the inContact system.	0:30:00

Authentication			Parameter	Description	Default
X	X	X	Web service timeout	Timeout value when attempting connectivity to the InContact webservices.	0:15:00

X	X	X	Calculate APS	The Agent State Log inContact CSV report includes a column called OutState, which holds the reason name (OutState_Code holds the reason number). If you uncheck this box, the historical connector will create SIT/SOT pairs solely based on the contents of Agent Time Card CSV report (which list the hard signin/sign-out pairs for the agents). By checking this box, the historical connector will calculate SIT/SOT pairs based on the Agent State Log report. Any signedout reasons are treated as a sign out at the beginning of the reason and sign in at the end of the reason. The time spent during any signed-in reasons are counted in Unavailable time. For APS purposes, all Unavailable reasons are treated as signedout. Checking this checkbox updates the APS calculation to include time in	(checked)
Authentic ıtion			**Parameter**	**Description**	**Default**

				signed-in reasons, e.g., project time.	

Parameter	Description	Default
Report Parameters:		
Reporting interval	Reporting Interval (15, 30, or 60 minutes) of the data in the interval report. **Note:** Must match the ACD unit of the Aspect Workforce™ ACD Instance.	30
Days to keep local output	For diagnostic purposes.	7
Interval report delay (sec)	Number of seconds to wait after the end of a reporting period before attempting to produce the report.	0
Interval reship time	Every day at the Interval reship time, the Historical Connector reships all of yesterday's interval data (to capture long-running calls).	3:00 AM
Agent productivity start time	Not used. **Note:** The Agent productivity report always covers 24 hours.	12:00:00 AM
Agent productivity end time		11:59:59 PM
Agent productivity output time	Every day at Agent productivity output time, ship Agent Productivity report.	12:01 AM

Days to reship on start	Number of days of interval and Agent Productivity reports to reship when the Historical Connector service starts. Used in conjunction with *Run historical immediately* option.	0

Parameter	Description	Default
Run historical immediately	If checked, the Historical Connector will reship data immediately after restart. Use this option to reship missing data. **Note:** • Always reships interval data for the current day plus the number of days specified in *Days to reship on start* option. • *Days to reship on start* option is ignored if you do not check Run historical immediately option. • You cannot reship a selected range of times or days.	(checked)

Authentication	Parameter	
Delivery Options:		
Pickup folder	Copy to WFM Listen stream folder or to a local folder that WFM Listen picks up from a share. Default based on where WFM Parser is installed. • Local folder if installed locally • UNC path if installed remotely	C:\ProgramData\Aspect\Workforce Management\WFM Data\Listen\Stream 1
WebDAV	Copy files to a WebDAV "stream" location that the WFM Listen service picks up from. Provide the Username, Password, and WebDAV URL	

Interval Report Columns

- C1 – NCO (contactsOffered from the /skills/summary web service)
- C2 – NCH (contactsHandled from the /skills/summary web service
- C3 – ATT (averageTalkTime from the /skills/summary web service)
- C4 – AWT (averageWrapTime from the /skills/summary web service)
- C5 – Delay (averageSpeedToAnswer from the /skills/summary web service)
- C6 - SL % ((contactsWithinSLA / contactsOffered) * 100) from the /skills/summary web service)
- C7 – APS*
- C8 – Abandons (abandonCount from the /skills/summary web service)
- C9 - Short Abandons
- C10 - Contacts with service (contactsWithinSLA from the /skills/summary web service)**
- C11 - Contacts out of service (contactsOutOfSLA from the /skills/summary web service)**
- C12 - Service Level from inContact (serviceLevel from the /skills/summary web service)**

* Total agent time for skill (in milliseconds) / reporting interval length (in milliseconds). To calculate Total agent time for skill, the InContact historical connector looks at the agent state spans from the Agent State Log report. It only counts time that overlaps the reporting interval.

** These columns are calculated based on the way each skill is configured in inContact. If a skill is configured to exclude abandons from the service level calculation, abandoned contacts will not be counted in these columns. The serviceLevel value from /skills/summary is calculated as follows:

```
100 * contactsWithinSLA / (contactsWithinSLA + contactsOutOfSLA)
```

The serviceLevel value is an integer. If that precision is sufficient, the following formula for SL% can be used::

```
SPLIT ["*", C12]
```

For maximum precision avaailable, the following formula for SL% should be used:

```
SPLIT ["*", 100 * C10 + (C10 + C11)]
```

Report Scheduling Notes:

Reports are scheduled on the reporting interval. Every reporting interval, the connector ships the current report and the previous 2 hours worth of interval data (to capture long running calls).

Configuring Custom InContact Reports:

The InContact historical connector depends on the following InContact reports:

- Call Details – used by interval report.
- Agent State Log – used by interval and Agent Productivity reports.
- Agent Time Card – used by Agent Productivity report.

InContact Web Services:

Aspect Workforce™ reports based on a mix of custom InContact report data and other web services.

- /skills – used by the interval report, to report 0's for skills with no work. The results of the /skills web service is what is cached in the Skills cache.
- /skills/summary – used by the interval report, returns contact stats by skill.
- /agents/skills?isSkillActive=true – used by the interval report, returns agent skill assignments, used in Agent Position Staffed (APS) calculation, to apportion time of an agent with no skill work during the interval. The results of the /agent/skills web service is what is cached in the Agent-skills cache.
- /report-jobs/datadownload/{reportID} – used to run a custom report.
- /files?filename={reportFileName} – used to download report data.

Adding a Zendesk Historical Connector

There are two possible ZenDesk Historical Connectors:

- Zendesk (Tickets)
- Zendesk (Chat)

Though similar, there are some differences in the configuration parameters.

Zendesk (Tickets)

You can configure the following settings for a Zendesk (Tickets) Historical Connector:

Parameter	Description	Default
Service settings:		
Instance name	Enter a descriptive label.	
Log On As....	Click this button to configure Log On As credentials for the service.	LocalSystem
Automatically start	Select this checkbox to configure the service to start automatically at system start and also when you save changes.	(checked)
Automatically restart	Select this checkbox to configure service recovery options that will restart the service-on-service failure.	(checked)

Zendesk paramete s:		
Ticket service URL	Base URL for email web services.  **Note:** Need to replace <customer> with the Zendesk tenant name.	https://<customer>.zendesk.com/api/v2/incremental/tickets.json?include=metric_sets
Email API token	Bearer token for authenticating email web service calls. Of the form: Bearer <hexadecimal string>  **Note:** You will need to generate an Oauth token for the Zendesk historical connector to use with email web service calls. Consult the Zendesk documentation for details.	
Report parameters:		
Reporting interval	Reporting Interval (15, 30, or 60 minutes) of the data in the interval report.	30

Parameter	Description	Default
	 **Note:** Must match the ACD unit of the Aspect Workforce™ ACD Instance.	
Days to keep local output	For diagnostic purposes.	7
Interval report delay (sec)	Number of seconds to wait after the end of a reporting period before attempting to produce the report.	0

Interval reship time	Not used.	12:00 AM
Agent productivity start time	The Agent productivity report is limited to this range of time. The daily reship of interval reports is limited to this range of time.	12:00:00 AM
Agent productivity end time		11:59:59 PM
Agent productivity output time	Every day at Agent Productivity output time ship Agent Productivity report data for yesterday.	12:01 AM
Days to reship on start	Number of days of interval and Agent Productivity reports to reship when the Historical Connector service starts. **Note:** You cannot reship a selected range of times or days.	0
Interval report offset (hours)	The number of hours of interval report data to reship for each reporting interval.	2
Parameter	**Description**	**Default**
Report Time Zone	Time zone of the WFM ACD reports produced by the connector. The report time zone is also an IANA time zone that can be selected from the Noda Time list. For the list of IANA time zones, see https://nodatime.org/TimeZones. **Note:** The time zone must match the equivalent Aspect Workforce™ time zone specified for the ACD Instance. Aspect Workforce™ does not use the IANA time zone list, but instead, maintains an independent list of time zones relevant to Aspect Workforce™. Use the time zone label and bias (i.e. offset from UTC/GMT) in Aspect Workforce™ to identify the appropriate IANA time zone. For example, the Aspect Workforce™ time zone of "(UTC-05:00) Eastern Time (US & Canada)"is the equivalent IANA time zone of "US/Eastern."	Etc/UTC
Delivery Options:		

Pickup folder	Copy to WFM Listen stream folder or to a local folder that WFM Listen picks up from a share. Default based on where WFM Parser is installed. • Local folder if installed locally • UNC path if installed remotely	C:\ProgramData\Aspect\Workforce Management\WFM Data\Listen\Stream 1
WebDAV	Copy files to a WebDAV "stream" location that the WFM Listen service picks up from. Provide the Username, Password, and WebDAV URL.	

Zendesk (Chat)

You can configure the following settings for a Zendesk (Chat) Historical Connector:

Parameter	Description	Default
Service settings:		
Instance name	Enter a descriptive label.	
Log On As....	Click this button to configure Log On As credentials for the service.	LocalSystem

Parameter	Description	Default
Automatically start	Select this checkbox to configure the service to start automatically at system start and also when you save changes.	(checked)
Automatically restart	Select this checkbox to configure service recovery options that will restart the service-on-service failure.	(checked)
Zendesk paramete s:		

Chat service base URL	Base URL for chat web services.	https://www.zopim.com/api/v2/chats
Chat API token	Bearer token for authenticating chat web service calls. Of the form: Bearer <hexadecimal string> **Note:** You will need to generate an Oauth token for the Zendesk historical connector to use with chat web service calls. Consult the Zendesk documentation for details.	
Report parameters:		
Reporting interval	Reporting Interval (15, 30, or 60 minutes) of the data in the interval report. **Note:** Must match the ACD unit of the Aspect Workforce™ ACD Instance.	30
Days to keep local output	For diagnostic purposes.	7
Interval report delay (sec)	Number of seconds to wait after the end of a reporting period before attempting to produce the report.	0
Interval reship time	Not used.	12:00 AM
Agent productivity start time	The Agent productivity report is limited to this range of time.	12:00:00 AM

Parameter	Description	Default
Agent productivity end time	The daily reship of interval reports is limited to this range of time.	11:59:59 PM
Agent productivity output time	Every day at Agent Productivity output time ship Agent Productivity report data for yesterday.	12:01 AM
Days to reship on start	Number of days of interval and Agent Productivity reports to reship when the Historical Connector service starts.  **Note:** You cannot reship a selected range of times or days.	0
Interval report offset (hours)	The number of hours of interval report data to reship for each reporting interval.	2
Report Time Zone	Time zone of the WFM ACD reports produced by the connector. The report time zone is also an IANA time zone that can be selected from the Noda Time list. For the list of IANA time zones, see https://nodatime.org/TimeZones.  **Note:** The time zone must match the equivalent Aspect Workforce™ time zone specified for the ACD Instance. Aspect Workforce™ does not use the IANA time zone list, but instead, maintains an independent list of time zones relevant to Aspect Workforce™. Use the time zone label and bias (i.e. offset from UTC/GMT) in Aspect Workforce™ to identify the appropriate IANA time zone. For example, the Aspect Workforce™ time zone of "(UTC-05:00) Eastern Time (US & Canada)"is the equivalent IANA time zone of "US/Eastern."	Etc/UTC

Delivery Options:		
Pickup folder	Copy to WFM Listen stream folder or to a local folder that WFM Listen picks up from a share. Default based on where WFM Parser is installed. • Local folder if installed locally • UNC path if installed remotely	C:\ProgramData\Aspect\Workforce Management\WFM Data\Listen\Stream 1
Parameter	**Description**	**Default**
WebDAV	Copy files to a WebDAV "stream" location that the WFM Listen service picks up from. Provide the Username, Password, and WebDAV URL.	

Report Scheduling Notes:

- Based on the specified Reporting Interval and the specified Interval report offset, the Historical Connector automatically generates the interval report(s) every 15, 30, or 60 minutes. For example, if the Reporting Interval is 15 minutes and the Interval report offset is 2 hours, then the Historical Connector will generate interval reports covering the previous 2 hours every 15 minutes.

Zendesk Historical Connector Times:

- When configuring the email and chat ACD instance in Aspect Workforce™, set the time zone for both ACD Instances to UTC.
- Data in Zendesk is stored in UTC.
- Report data will also be in UTC.

Zendesk Web Services:

- All statistics come from web service calls.

Setting Security Permissions for Services

There are COM security permissions that affect access to services, as well as machine-wide COM security limits that enforce launch and activation restrictions. In addition, there are other COM security settings that affect access to the following Aspect Workforce™ services: Updater, Checker, Tally Server, ACD Proc, and AP Proc.

So, to enable service access for all users, WFM Service Installer automatically implements servicespecific permissions that provide access, launch, and activation permissions for the group Everyone and for Anonymous Logon. These permissions apply to the services listed in the Required Services For Various Deployments table as well as to the Information Server, which runs on the main application server only. These custom permissions override the default COM security permissions and can be modified using Windows Component Services to increase security if required.

To modify the default machine-wide COM security limits, you can modify the COM security limits manually or use WFM Service Installer to overwrite the default COM security limits so that access to the Aspect Workforce™ services is not restricted.

Modifying COM Security Limits Machine-Wide

You can modify the default machine-wide COM security limits using WFM Service Installer or Windows Component Services.

With the WFM Service Installer

Using the WFM Service Installer, you can modify the default machine-wide COM security limits to ensure that access to the Aspect Workforce™ services is not restricted. When you choose this option, the WFM Service Installer sets security limits on a per user or per group basis as shown in the table below.

Permission Limits	User or Group	Permissions
Access	Everyone, Anonymous Logon	• Local Access = Allow • Remote Access = Allow
Launch And Activation	Everyone, Anonymous Logon	• Local Launch = Allow • Remote Launch = Allow • Local Activation = Allow • Remote Activation = Allow

To modify the default COM security settings using the WFM Service Installer, do the following:

1. For Windows Server 2022 and 2025: Select **Start > Aspect > WFM Service Installer**. The Aspect Service Installer window opens.
2. Select Edit > Set COM Security Limits. The **Set COM Security Limits** confirmation window opens.
3. Click **OK**.

Note: If required, you can modify the Aspect Workforce™ custom COM security limits manually as described in Modifying WFM Service Permissions Individually.

With Windows Component Services

To modify or increase security, you can modify the machine-wide COM security limits manually.

To edit the COM security settings manually:

1. For Windows Server 2022 and 2025: Select **Start > Windows Administrative Tools > Component Services**. The **Component Services** window opens.

2. In the tree on the left, locate **My Computer** in the **Component Services** folder, right-click it, and select **Properties**. The **My Computer Properties** dialog box opens.
3. Select the **COM Security** tab, and edit the limits as needed.

Modifying WFM Service Permissions Individually

By default, WFM Service Installer implements Aspect Workforce™ service-specific permissions that provide launch and activation permissions for the group Everyone and for Anonymous Logon. These custom permissions override the default COM security permissions and can be modified using Windows Component Services to increase security, if required. By default, WFM Service Installer implements the following permissions:

Service(s)	Permission Limits	User or Group	Permissions
WFM Updater WFM ACD Proc	Access	Everyone, Anonymous Logon	Use default
Service(s)	**Permission Limits**	**User or Group**	**Permissions**
WFM AP Proc WFM Checker	Launch And Activation	Everyone, Anonymous Logon	• Local Launch = Deny • Remote Launch = Deny • Local Activation = Allow • Remote Activation = Allow
WFM Tally Server	Access	Everyone, Anonymous Logon	Use default
	Launch And Activation	Everyone, Anonymous Logon	• Local Launch = Allow • Remote Launch = Allow • Local Activation = Allow • Remote Activation = Allow

WFM Information Server **Note:**The Information Server is not added by WFM Service Installer, but instead, is installed only on the Aspect Workforce™ main application server by the Aspect Workforce™ installation program.	Access	Everyone, Anonymous Logon	Use default
	Launch And Activation	Everyone, Anonymous Logon	• Local Launch = Allow • Remote Launch = Allow • Local Activation = Allow • Remote Activation = Allow

To modify the default Aspect Workforce™ COM service permission settings:

1. For Windows Server 2022 and 2025: Select **Start > Windows Administrative Tools > Component Services**. The **Component Services** window opens.
2. In the tree on the left, expand the following folders in sequence: **Component Services** > C**omputers > My Computer > DCOM Config**.
3. In the tree, right-click the **WFM service** (such as WFM Updater) for which to modify the security permissions and select **Properties**.
4. Select the **Security** tab.
5. Modify the **permissions** as needed.

About Password Encryption

Aspect Workforce™ provides additional security by automatically encrypting all passwords before storing them in the registry, installation database, or configuration files. Encryption disguises the password in alternate characters so that others, even administrators, cannot read it.

You can see examples of encrypted passwords in the WFM Service Installer for all installed services.

Managing Network Access by WFM Services

Some WFM services, such as WFM AutoRun and WFM Listen, can require network access. For example, WFM AutoRun requires network access if you install it on a server other than the main application server, or if AutoRun needs to print or export to network resources. WFM Listen requires a named network account if it will be moving files across the network.

In most cases, you must create a Windows login ID (typically, **TCSSERVICES**) for use by these Aspect Workforce™ system services. For instructions on using the TCSSERVICES account for network access, see Using TCSServices for Network Access by WFM Services.

Requirements for the TCSServices Account

Instead of using the system account for some services, you can configure all WFM system services to run under a named user account, typically named TCSSERVICES. The TCSSERVICES login ID is mandatory unless you configure your ACD to write ACD data directly to your main application server and you install AutoRun on the main application server.

The TCSSERVICES account:

- Must be a local or domain account.

- On the application servers only, must have the special user rights to Log On As A Batch Job and Log On As A Service.
- On the application servers only, must have permission for multiple concurrent logins.

If you create the TCSSERVICES account as a *local account,* you must create it on the following computers:

- Your main application server
- Any applicable secondary application servers
- Each machine that contains a shared folder that Aspect Workforce™ needs to access

If you create the TCSSERVICES account as a *domain account,* and if you will be configuring some or all Aspect Workforce™ system services to use Windows Integrated Security, see Enabling Integrated Security for WFM Services for more information.

Note: It is recommended that customers using Integrated Security for WFM service accounts should use different accounts for each service, as opposed to one domain account for all services.

About WFM AutoRun and Network Access

You use the WFM AutoRun system service to run various Aspect Workforce™ processes automatically at scheduled times. Many resources required by AutoRun are located on the main application server and cannot be moved. In cases where AutoRun is not installed on the main application server, AutoRun must use the TCSSERVICES user account (rather than being configured to log in with the system account).

If you install the AutoRun service on your main application server, you can configure it to use the system account. However, note that AutoRun functionality is limited when you configure it to use the system account. Specifically, with the system account, AutoRun cannot:

- Print to a network printer. Automatic report printing, for example, cannot be configured unless the target printer is connected to the main application server using a non-authenticated interface (serial port, parallel port, SCSI port, USB port, and so on.).
- Export reports (including IDP data in HTML format) to a shared network folder.
- Execute non-Aspect Workforce™ commands that require network access. You can use AutoRun to launch non-Aspect Workforce™ processes: for example, to start the nightly Aspect Workforce™ backup process. However, if the process needs to read or write data in a shared network folder, AutoRun must have network access.
- Process data for some optional Aspect Workforce™ modules. Kronos export and Aspect Spectrum Download typically require that AutoRun can write Aspect Workforce™ data to a shared folder on your network. If AutoRun does not have network access, these modules might be unable to read or write needed files.

About WFM Listen and Network Access

The WFM Listen system service moves ACD data files to a folder on the main application server. The location where Listen gets those ACD data files determines whether Listen requires network access. For example, your ACD might be configured to write ACD files to a folder on its own disk drive. This is a network location from the Listen perspective. Listen must be able to log in to your network and access a shared folder on the ACD. Or, your ACD might be configured to write ACD data files to a LAN file server. This is a network resource and Listen must be able to log in to your network and access the shared folder on the file server.

The only circumstance where Listen can be configured to use the SYSTEM account is when your ACD is configured to write data files directly to a folder on your main application server. And in this case, the ACD service that writes the data files must be able to log in to your network and to access the shared destination folder on your main application server.

Using TCSServices for Network Access by WFM Services

You must ensure that all WFM services on all application servers can access the machines in your Aspect Workforce™ network. Most services use system accounts. The exceptions are the WFM Listen and WFM AutoRun services, which typically use the TCSSERVICES domain account.

The TCSSERVICES account must have the appropriate level of permission for the server where these two services are installed. Set the permission levels according to whether you intend to run these services with administrator or non-administrator accounts.

To configure network access for WFM services:

1. Log in to the **application server.**
2. Go to Administrative Tools > Services.
3. Double-click the **service**, and do one of the following depending on the account:

- If the selected service will use the **TCSSERVICES** login ID (for example, WFM Listen or WFM AutoRun):
  a. On the **General** page, in the **Startup Type** field, select **Automatic**. (Do not select Automatic [Delayed Start]).
  b. On the **Log On** page, in the **Log On As** section, select the **This Account** button.
  c. Browse to and select the **TCSSERVICES** login ID.
  d. Enter and confirm the **TCSSERVICES** password.
  e. Click **OK.** If this is the first service using the account, a message box is displayed, showing that the service has been granted the Log On As A Service right.
  f. In the **Services** window, right-click the **service** you just configured, and click **Start**. The selected service will use the **system account**.
  g. On the **General** page, in the **Startup Type** field, select **Automatic**.
  h. Click **OK,** and you are returned to the **Services** dialog box.
  i. Select the service you just configured, and click **Start**.

4. After configuring all the system services, select **File > Exit** to close the Services dialog box.

Enabling Integrated Security for WFM Services

By default, integrated security for Aspect Workforce™ services is *not* enabled. But if you so choose, and if your Aspect Workforce™ database is configured accordingly, all Aspect Workforce™ system services can log on using a Windows domain account (either a standard domain account or a Group Managed Service Account (gMSA)) instead of the Local System account. In this configuration, the domain account running the Aspect Workforce™ system service is used to authenticate to your Aspect Workforce™ database instead of the username listed for the service in the WFM Service Installer.

Note: It is recommended that customers using Integrated Security for WFM service accounts should use different accounts for each service, as opposed to one domain account for all services.

To enable Windows Integrated Security for a service:

1. For Windows Server 2022 and 2025: Select **Start > Aspect > WFM Service Installer**. The Aspect **Service Installer** window opens.
2. Select a **service** and select **Edit > Edit**. The service window opens.
3. Select the **tab** for the database alias to which this change applies.
4. Set the **Integrated Security** value to 1.
5. Select **OK** to close the dialog box.
6. Select **File > Save**.
7. Select **File > Exit**.

Requirements for Domain Login Accounts for Services

When you use domain accounts to run Aspect Workforce™ services, ensure that each account meets the following requirements:

- One account can be used to run all Aspect Workforce™ system services, or each service can use a separate domain account.

  Note: It is recommended that customers using Integrated Security for WFM service accounts should use different accounts for each service, as opposed to one domain account for all services.
- If your Aspect Workforce™ implementation spans multiple domains, all domains must have two-way trusts established.
- Verify that appropriate domain accounts have been configured in your Aspect Workforce™ database. For more information, see Implementing Windows Authentication for SQL Server or Implementing Windows Authentication for Oracle.
- Verify that, for all domain accounts, corresponding administrative user accounts have been configured in the Aspect Workforce™ Users module.
- Verify that each domain account is part of the local administrators group on the appropriate Aspect Workforce™ application server. (This is not necessary if a service is running under a nonadministrative account. See Running WFM Services with Non-Administrative Accounts).
- Verify that each domain account is configured such that its password does not expire.
- Verify that each domain account has, as the **Local Security Policy**, **Log On As A Service**.

Special Notes for Group Managed Service Accounts (gMSA)

- For Group Managed Service Accounts (gMSA), when entering a gMSA username, no password is necessary. If prompted for a password, the password is not required.
- The WFM Service Installer initially sets up a localuser account. To change the account, use services.msc from the Command Prompt. This will start the Services console, the UI in Windows that is used to manage background services.

Cloud Storage Container Permissions

For the Workforce client and several of the Workforce services , the capability has been added to import or export data from several cloud storage vendors (Amazon S3, Azure, Google). Workforce will require an account for access. Be sure that the cloud storage account used for this purpose has the appropriate permissions.

In general:

- WFM Listen requires Read, and Delete access. Write access is also required if Archiving is turned on.
- WFM Autorun requires Read and Write access.
- Encompass requires Read and Write access.
- A Workforce client user at minimum requires Read and Write access to import\export files in the Workforce client.

Additional access may be required for users to manage files outside of Workforce. Contact your vendor for assistance.

For Amazon S3 cloud storage, it has been determined that:

- WFM Listen needs ListBucket, GetObject, and DeleteObject, plus PutObject access if you are archiving.
- WFM Autorun needs ListBucket, PutObject and/or GetObject and DeleteObject access depending on the job.

For Azure and Google, contact the vendor for assistance.

Server-managed cloud storage encryption has been tested and is supported by Aspect. The various cloud storage applications also support additional levels of encryption and security. Utilization of these methods may require additional assistance. Contact Aspect Customer Care for assistance before implementing these features.

Hiding Database Aliases at Login

When you have set up multiple databases in your Aspect Workforce™ deployment, users can choose which database alias to connect to during the client login by selecting it from a drop-down list. If you want to hide multiple database aliases from users and require them to enter a specific database alias when logging in, you can disable the drop-down menu by setting a parameter within the WFM Service Installer general parameters. This feature enables you to compartmentalize information so that you can provide unique views to business-level users.

If you choose to restrict database access, users must supply the correct database name at login.

To remove the database alias selection list during client login:

1. For Windows Server 2022 and 2025: Select **Start > Aspect > WFM Service Installer**. The Aspect Service Installer window opens.
2. Select **Edit > General Parameters**. The **General Parameters** window opens.
3. Double-click the **LoginHideAliases** parameter. The edit window for this parameter opens.
4. In the parameter field, type **Y**.
5. Close the **LoginHideAliases** window and close the **General Parameters** window.
6. When prompted, click **Yes** to save your changes to the General Parameters.

7. In the WFM Service Installer window, select **File** > **Save** to save your changes to the Installation database.
8. In the WFM Service Installer window, select **File** > **Exit**.

If you edit the LoginHideAliases parameter from a secondary application server, you must restart the WFM Information Server service on the Aspect Workforce™ main application server before the change takes affect. If you make the change on the main application server, the service is automatically restarted.

Using Updater Plug-In Rules

When you install the Updater service (see Installing the WFM Services), the service operates with a set of *internal* (or native) rules to provide validation and transaction control for Aspect Workforce™ schedule update requests. But you can extend the functionality of Updater by using *Updater plug-in rules.* These plug-in rules are Component Object Model (COM) components containing business logic that is not part of the standard functioning and validating processes of Updater, but that might be needed to meet the special needs of a user. The table below compares the two types of Updater rules.

Internal Rules	Plug-In Rules
Are native to the Aspect Workforce™ Updater service.	Are developed by systems integrators and developers as COM objects.
Are part of the standard Aspect Workforce™ product.	May or may not be part of the standard Aspect Workforce™ product.
Provide the core validation functionality of Updater.	Extend the functionality of Updater by adding specific validation capabilities that a user requires.
Are loaded (prepopulated) in Aspect Workforce™ when Aspect Workforce™ is installed.	After installation of Aspect Workforce™, can be loaded by users into Aspect Workforce™ through the native Windows tool, Regsvr32.
Internal Rules	**Plug-In Rules**
Are configured within the Aspect Workforce™ user interface, such as through segment entry rules.	Must be added to Updater and configured using the WFM Service Installer.
Generate Updater violation messages when rule validation fails.	Also generate Updater violation messages when rule validation fails.

For more information about the Updater service, see the *Aspect Workforce™ Online Help and the Aspect Workforce™ Planning Guide.*

About the Minimum Shift Break Rule

Aspect Workforce™ includes an Updater plug-in rule, the *Minimum Shift Break Rule.* You can use this rule to ensure that a specified minimum period elapses between the end of an employee's shift and the beginning of his next shift. This rule is especially useful in geographical regions, such as the European Union, when government regulations require that such a minimum off-work period be observed.

Process Overview for Deployment

Integrating an Updater plug-in rule into your Aspect Workforce™ deployment consists of the following processes:

1. A systems integrator or developer creates a COM component containing the business rule or logic that you want to make available within Updater.
2. The Aspect Workforce™ system administrator registers the COM object program on the Updater server using Regsvr32.
3. The Aspect Workforce™ administrator adds the new rule to the list of available Updater rules using the WFM Service Installer program.
4. The Aspect Workforce™ administrator, still using WFM Service Installer, configures the new rule according to your preference.

The following procedures provide specific instructions for using the WFM Service Installer to add and configure Updater plug-in rules.

Adding a Rule

To add an Updater plug-in rule:

1. In the WFM Service Installer window, select **Edit > Configure Updater Rules**. The **Configure Updater Rules** dialog box opens.
2. Click **Add.** The **Updater Rule** dialog box opens.
3. Type a **name** (program ID) and **description** for the rule and click **OK**.
4. Click **OK** again to close the Configure Updater Rules dialog box.
5. In the WFM Service Installer window, select the **WFM Updater** service.
6. Select Edit > Edit.
7. Click **Add,** select the **rule** to add from the Select Updater Rule dialog box, and click **OK**.
8. To change the order in which Updater processes the plug-in rules, drag and drop the **rules** in the list.

Configuring a Rule

To configure an Updater plug-in rule:

1. In the WFM Service Installer window, select the **WFM Updater** service.

2. Select **Edit > Edit**. The **WFM Updater** dialog box opens.
3. In the Rules list, select the **rule** to configure, and click **Configure**.

   Note: Only Updater plug-in rules can be configured. For internal Updater rules, the Configure button is disabled.
   The dialog box for the selected rule opens.
4. In the Timeout (sec) field, type the **number of seconds** you want to elapse before automatically ending the processing of a rule.
5. Next to the Configuration field, select the **Lookup** button. The configuration dialog box for the selected rule opens. (See example below.) All Updater plug-in rules have a unique configuration dialog box that reflects the specific properties that the rule enforces.

6. Define **rule-specific options.**

   For example, in the Minimum Shift Break Configuration dialog box, shown in the preceding picture, you can define properties such as Superstates (Aspect Workforce™ superstates) and Minutes Between Shifts (the minimum number of minutes that must elapse between the end of one shift and the beginning of the next for a given employee).
7. Click **OK** to close the rule configuration dialog box.
8. Click **OK** to close the rule dialog box.
9. In the WFM Updater dialog box, click **OK** to save your rule configuration.

After finishing this chapter, if you installed the Aspect Message Routing Service for load balancing, configure the service using the Aspect Message Routing Platform Configuration Editor. See Configuring Aspect Message Routing.

Installing a Secondary Application Server

The instructions in this chapter apply only if you want to create a distributed installation using a main application server and one or more secondary application servers. For details about distributed installations, see the *Aspect Workforce™ Planning Guide.* If you do not want to create a distributed installation, go to Installing User Workstations.

If you have more than one secondary application server, complete the installation procedures for each.

Note: The installation program automates several tasks that were formerly manual steps in prior releases of Aspect Workforce™. As you progress through the installation wizard, some of the processes might require several minutes to complete. This is normal and does not indicate any issues with your hardware, software, or the installer. When the installation is complete, a wizard screen confirms that the installation was successful.

Prerequisites

Before you install your secondary application server, complete the following procedures or verify that they have been completed:

- You have administrator access to the computers on which you want to install and configure the secondary application server software. These servers include the main application server and any Checker or Tally Server servers that you specify during the configuration.
- You check the release note for any new requirements or procedures.
- The database server and the Aspect Workforce™ database have been configured.
- The database client is installed on the secondary application server:
- For Oracle, see Installing the Client Software.
- For SQL Server, see Installing the SQL Server Client Software.
- The server is in Administrator mode (that is, Remote Desktop For Administration mode) and not in Terminal Server mode, as follows:
- For Windows Server 2022 or 2025, open Server Manager and very that Remote Desktop Services has not been installed.

About File Installation Paths

Aspect Workforce™ delivers both 32-bit and 64-bit files. The location of the files depends on the installation path you select when installing Aspect Workforce™. See the table in Appendix B for details on where files are delivered.

Installing a Secondary Application Server

You can install a Aspect Workforce™ secondary application server in either of two ways:

- Launch the installation wizard from the product CD.
- Run the installation wizard from the main application server.

Installing from the Product CD

You can install the secondary application server using the product CD.

To install the secondary application server software:

1. Log in to the server designated as the **secondary application server.**
2. Insert the **Aspect Workforce™ Software CD** and open the file **Setup.exe**. The product selection window of the installation wizard opens.

3. Click **Aspect Workforce™**. If any prerequisite software is not already installed on the server, then the Aspect Prerequisite Installer window opens, displaying a list of prerequisite but uninstalled software. Click **Install** to install the prerequisite software. When installation is complete, the Welcome window of the **Install Wizard for Workforce** opens.
4. Click **Next**. The **Destination Folder** window opens.
5. To accept the default (recommended) location for the program files, click **Next**. Otherwise, click **Change**, and browse to or type a different **path**, and click **OK**. The Data Folder window opens.
6. To accept the default (recommended) location for the data files, click **Next**. Otherwise, click **Change**, and browse to or type a different **path**, and click **OK**.

   Since all files and folders for ACD data are stored in this path, ensure that the drive you select is sized appropriately. ACD data files can require several gigabytes of drive space. The **Custom Setup** window opens.
7. Click the Secondary Application Server icon**,** and select This Feature, And All Subfeatures, Will Be Installed On Local Hard Drive.

   Do *not* select the **User Workstation** icon. The wizard automatically includes Aspect Workforce™ client components with the secondary application server.
8. If you want to install the WFM Listen service, click the **Listen** icon**,** and select **This Feature**, And All Subfeatures, Will Be Installed On Local Hard Drive.

   After installing the secondary application server, you configure WFM Listen using the Listen Configuration Editor. For more information, see Using the Listen Configuration Editor.
9. If you want to enable load balancing (that is, distributed mode for Tally Server, Checker, or both), click the **Aspect Message Routing Service** icon, and select **This Feature, And All Subfeatures, Will Be Installed On Local Hard Drive**.

   After installing the secondary application server, you configure the Aspect Message Routing Service using the Aspect Message Routing Platform Configuration Editor. For more information, see Configuring Aspect Message Routing.
10. If you want to install the WFM Historical Connectors (install files required to configure Five9, InContact, and Zendesk historical connectors), click the **WFM Historical Connectors** icon, and select **This Feature, And All Subfeatures, Will Be Installed On Local Hard Drive**.

    After installing the secondary application server, you configure the WFM Historical Connectors using the WFM Historical Connector Configuration. For more information, see Using the WFM Historical Connector Configuration.
11. Click **Next**. The **Main Application Server** window opens.
12. Type the **machine name** of the main (not the secondary) application server and click **Next**. The **DCOM Servers** window opens.

    If the DCOM Servers window does not open and you get a message instead, use the IP address of the main application server instead of the server name.
13. In the **DCOM Servers** window, verify or type the **machine name** that is running each of the TallyServer, Updater, Checker, and ACD Processing Server services.

    The fields in this window are populated as follows:

- If the service has been added in the WFM Service Installer on the main application server or on another secondary application server, then the field displays the name of that server.

- If the service has not been added yet, then the field is blank. In this case, type the name of the server that will host this service.
- If the Tallyserver service has been added to multiple servers, then the drop-down list for the Tallyserver field displays the names of these servers. In this case, select the name of the Tallyserver host server that your secondary application server will access. If you want to install Tallyserver on the secondary application server that you are now installing, type the name of that server.
- The user needs to select which Tallyserver service this application server will use. If Tallyserver will be installed on this secondary app, then the user can type the current server name into

  There are additional COM security settings that affect access to the Aspect Workforce™ services. So, to enable service access for all users, you must configure your security settings as described in Using the WFM Historical Connector Configuration.

14. Click **Next**. The **Ready To Install** window opens.
15. Click **Install**. The **Installing Aspect Workforce™** window opens, showing the status of the installation. When the installation has completed successfully, the **Install Wizard Completed** window opens.
16. Click **Finish** and click **Exit** to close the wizard.
17. On the *main* application server, restart the **WFM Information Server** service.

Installing from the Main Application Server

Use the installation wizard to install the secondary application server software from the main application server.

To install the secondary application server from the main application server:

1. Log in to the **secondary application server.**
2. Using Windows Explorer, locate and double-click the following file, where ***MainAppServer*** is the machine name assigned to the main application server:
   ***MainAppServer*\WFMSetup\Workforce\Setup.exe**

   If any prerequisite software is not already installed on the server, then the Aspect Prerequisite Installer window opens, displaying a list of prerequisite but uninstalled software. Click **Install** to install the prerequisite software. When installation is complete, the **Welcome** window of the **Install Wizard for Workforce** opens.
3. Click **Next**. The **Destination Folders** window opens.
4. To accept the default (recommended) location for the program files, click **Next**. Otherwise, click **Change**, and browse to or type a different **path**, and click **OK**. The Data Folder window opens.
5. To accept the default (recommended) location for the data files, click **Next**. Otherwise, click **Change**, and browse to or type a different **path**, and click **OK**.

   Since all files and folders for ACD data are stored in this path, ensure that the drive you select is sized appropriately. ACD data files can require several gigabytes of drive space. The **Custom Setup** window opens.
6. Click the Secondary Application Server icon**,** and select This Feature, And All Subfeatures, Will Be Installed On Local Hard Drive.

   Do *not* select the **User Workstation** icon. The wizard automatically includes Aspect Workforce™ client components with the secondary application server.

7. If you want to install the WFM Listen service, click the Listen icon**,** and select This Feature, And All Subfeatures, Will Be Installed On Local Hard Drive.

   After installing the application server, you configure WFM Listen using the Listen Configuration Editor. For more information, see Using the Listen Configuration Editor.

8. If you want to enable load balancing (that is, distributed mode for Tally Server, Checker, or both), click the **Aspect Message Routing Service** icon, and select **This Feature, And All Subfeatures, Will Be Installed On Local Hard Drive**.

   After installing the secondary application server, you configure the Aspect Message Routing Service using the Aspect Message Routing Platform Configuration Editor. For more information, see Configuring Aspect Message Routing.

9. If you want to install the WFM Historical Connectors (install files required to configure Five9, InContact, and Zendesk historical connectors), click the **WFM Historical Connectors** icon, and select **This Feature, And All Subfeatures, Will Be Installed On Local Hard Drive**.

   After installing the secondary application server, you configure the WFM Historical Connectors using the WFM Historical Connector Configuration. For more information, see Using the WFM Historical Connector Configuration.

10. Click **Next**. The Main Application Server window opens, displaying the name of the main application server.

11. Click **Next**. The **DCOM Servers** window opens.

    If the DCOM Servers window does not open and you get a message instead, use the IP address of the main application server instead of the server name in Click .

12. In the **DCOM Servers** window, verify or type the **machine name** that is running each of the TallyServer, Updater, Checker, and ACD Processing Server services.

    The fields in this window are populated as follows:

- If the service has been added in the WFM Service Installer on the main application server or on another secondary application server, then the field displays the name of that server.
- If the service has not been added yet, then the field is blank. In this case, type the name of the server that will host this service.
- If the Tallyserver service has been added to multiple servers, then the drop-down list for the Tallyserver field displays the names of these servers. In this case, select or type the name of the Tallyserver host server that your secondary application server will access. If you want to install

  Tallyserver on the secondary application server that you are now installing, select or type the name of that server.

  There are additional COM security settings that affect access to the Aspect Workforce™ services. So, to enable service access for all users, you must configure your security settings as described in Using the WFM Historical Connector Configuration.

13. Click **Next**. The **Ready To Install** window opens.

14. Click **Install**. The **Installing Aspect Workforce™** window opens, showing the status of the installation. When the installation has completed successfully, the **Install Wizard Completed** window opens.

15. Click **Finish** to close the wizard.

16. On the *main* application server, restart the **WFM Information Server** service.

Installing the Services

After installing the secondary application server, complete the following post-installation procedures for the WFM services, WFM Listen, and the Aspect Message Routing Service.

Complete all procedures on the secondary application server in the order shown below.

1. Install WFM services using the WFM Service Installer. See Using the WFM Service Installer.
2. If you installed the WFM Listen service, configure the service using the Listen Configuration Editor. See Using the Listen Configuration Editor.
3. If you installed the Aspect Message Routing Service for load balancing, configure the service using the Aspect Message Routing Platform Configuration Editor, see Configuring Aspect Message Routing.
4. If you installed the WFM Historical Connectors, configure the appropriate connector(s) using the WFM Historical Connector Configuration. See Using the WFM Historical Connector Configuration.

Upgrading

To upgrade the secondary application server for Aspect Workforce™, see Upgrading for SQL Server or Upgrading for Oracle.

Uninstalling

Uninstall the secondary application server for Aspect Workforce™ in either of the following ways:

- Use the Programs And Features feature in the Windows Control Panel
- Use the Aspect Workforce™ installation program

Uninstalling with Windows Control Panel

To uninstall with Windows Control Panel, use this path:

Start > Control Panel > Programs > Programs And Features > Workforce > Uninstall

Uninstalling with the Installation Program

You can uninstall the secondary application server for Aspect Workforce™ by using the installation program on the Aspect Workforce™ product CD or on the main application server.

To uninstall the secondary application server with the installation program:

1. Log in as an administrator to the **secondary application server.**
2. Using Windows Explorer, browse to and double-click the following file, where ***MainAppServer*** is the machine name assigned to the main application server:
   ***MainAppServer*\WFMSetup\Workforce\Setup.exe**
3. The product selection window of the installation wizard opens.
4. Click **Aspect Workforce™**. The Welcome window of the **Install Wizard for Workforce** opens.
5. Click **Next**. The **Program Maintenance** dialog box opens.
6. Select **Remove and** click **Next**. The **Remove The Program** window opens.

7. Click **Remove**. The **Uninstalling Aspect Workforce™** window opens. When Aspect Workforce™ has been removed successfully, the **Install Wizard Completed** window opens.
8. Click **Finish** and click **Exit** to close the wizard.

Modifying

After you have installed Aspect Workforce™ on the secondary application server, you can modify some of the settings you specified during the initial installation. For example, you might want to change one of the DCOM servers.

You can modify the secondary application server for Aspect Workforce™ by using the installation program. The installation program can be found on the Aspect Workforce™ product CD, or on the main application server, as described below.

To modify the secondary application server using the installation program on the main application server:

1. Log in as an administrator to the **secondary application server.**
2. Using Windows Explorer, browse to and double-click the following file, where ***MainAppServer*** is the machine name assigned to the main application server:
   ***MainAppServer*\WFMSetup\Workforce\Setup.exe**
3. The product selection window of the installation wizard opens.
4. Click **Aspect Workforce™**. The Welcome window of the **Install Wizard For Workforce** opens.
5. Click **Next**. The **Program Maintenance** dialog box opens.
6. Select **Modify** and click **Next**. Each page in the wizard shows the current settings, beginning with the Custom Setup page.
7. Proceed through the wizard, changing only the **settings** you want to substitute now.
8. Click **Exit** to close the wizard.
9. On the *main* application server, restart the **WFM Information Server service**.

Configuring the Aspect Message Routing Service

This chapter provides a general description of how to install and configure the Aspect Message Routing Service (AMR). It provides details, screenshots, and field descriptions for every page in the Aspect Message Routing Platform Configuration Editor.

To configure AMR for your specific routing scenario, use this chapter together with Configuring AMR for Common Scenarios. In that chapter, you will find the specific settings that are required or recommended in the AMR editor to achieve your desired routing results.

About the Aspect Message Routing Service

The Aspect Message Routing Service is a component of Aspect Workforce™ that is used in load balancing. AMR is also required for all Aspect components that require the WFM Web Services, such as Aspect Workforce™ Engagement Management or Empower.

AMR acts much like a traffic cop to mediate messaging between the Dispatcher and TallyServer services and Aspect Workforce™. If you plan to use load balancing (also known as *distributed mode*), you must install and configure the Aspect Message Routing Service, as described in this chapter.

AMR is a reusable component that can be implemented with other Aspect products in addition to Aspect Workforce™.

For information about how to set up load balancing for common scenarios, including Checker and Tally Server load balancing, see Configuring AMR for Common Scenarios.

Installing Aspect Message Routing

If you have not already installed Aspect Message Routing as part of your installation of the main or secondary application server for Aspect Workforce™, you can install it now as explained below.

Note the following:

- You cannot install the Aspect Message Routing Service on a user workstation.
- You can install the Aspect Message Routing Service on another server as a backup, but you cannot install the service on more than two servers. The first installed AMR service is designated as the primary AMR server, and the second installed AMR service is designated as the backup AMR server.
- The primary Aspect Message Routing Service can be installed on either a main or secondary application server. Likewise, the backup Aspect Message Routing Service can be installed on either a main or secondary application server. But if you install the Aspect Message Routing Service on a secondary application server instead of the main application server, then the AMR service requires network credentials to access the AMR configuration file, which is installed only on the main application server. For instructions about configuring network access to the main application server, see Obtaining a Domain Account, Configuring Network Access for the AMR Service, and Verifying Folder Permissions.

To install the Aspect Message Routing Service:

1. Insert the **Aspect Workforce™ Software CD** in the CD drive of either the main application server or the secondary application server.
2. Browse to the CD root folder and double-click **Setup.exe**. The **Welcome** window opens.
3. Click **Next**. The **Program Maintenance** window opens.
4. Select **Modify** and click **Next**. The C**ustom Setup** window opens.
5. Click the **Aspect Message Routing Service** icon, and select This Feature, And All Subfeatures, Will Be Installed On Local Hard Drive.
6. Click **Next**. Click **Next**. The **Main Application Server** window opens, showing the machine name of the main application server.
7. Click **Next**. The Ready To Modify The Program window opens.
8. Click **Install**. The installation proceeds, and afterwards the **Installation Complete** window opens.
9. Click **Finish**. The product selection window of the installation wizard opens again.
10. Click **Exit** to close the wizard.

Configuring the Aspect Message Routing Service

The values you use to configure the AMR service depend on the type of scenario that you want to implement, such as distributed Tally Server or distributed Checker. For configuration values that are recommended for common load balancing scenarios, see Configuring AMR for Common Scenarios.

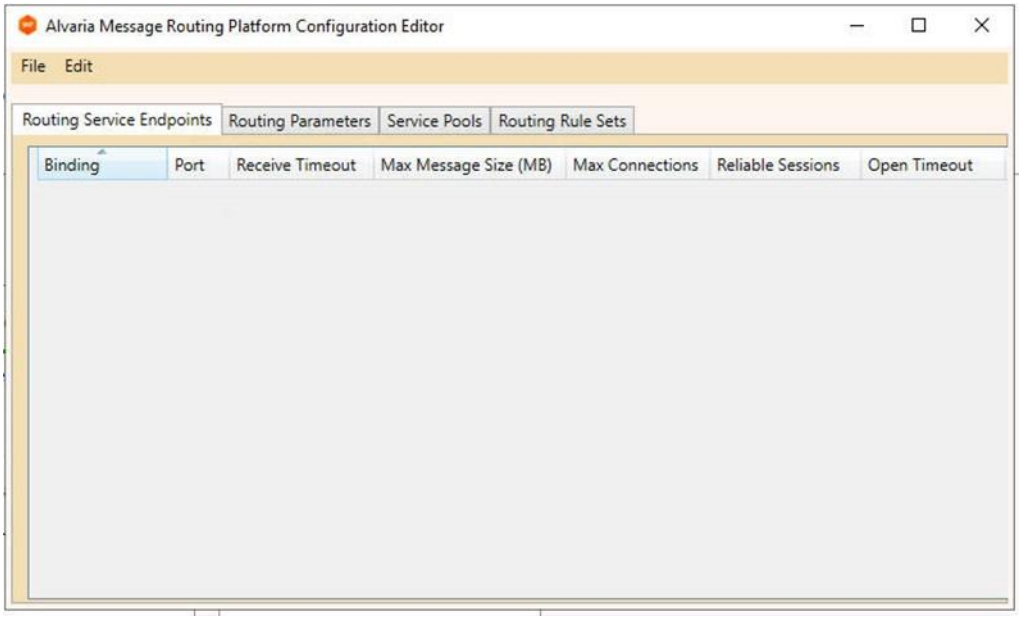
Note: If machines in your Aspect Workforce™ deployment have multiple network cards, the IP address might be required instead of the machine name when configuring AMR settings.

To configure the Aspect Message Routing Service.

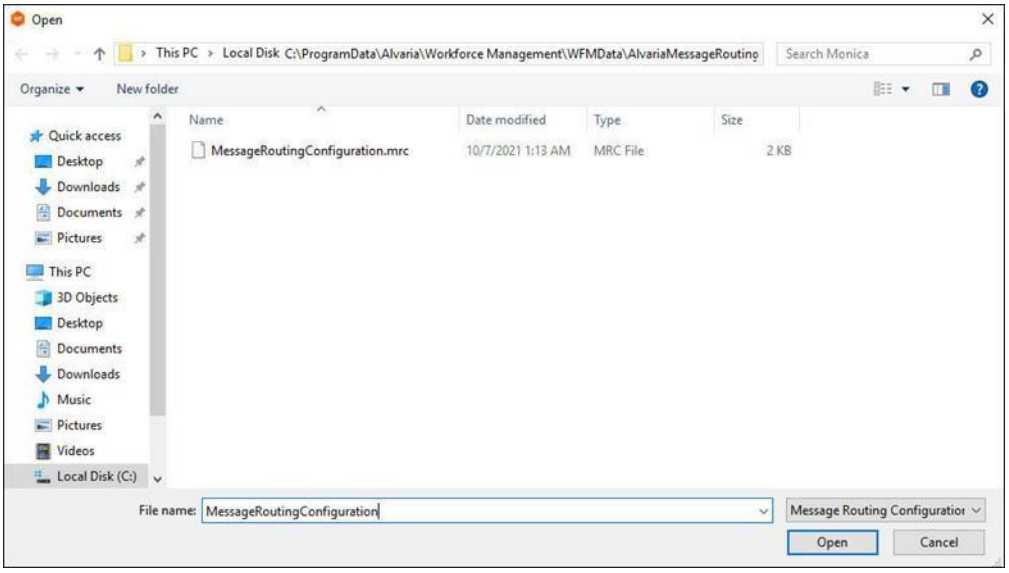
1. On the machine where AMR is installed, do the following:

- Windows Server 2022 or 2025: Select **Start > Aspect > AMR Configuration Editor**.

  The Aspect Message Routing Platform Configuration Editor opens.



2. Select **File > Open**. The following window opens.



3. In the address bar, browse to the **MessageRoutingConfiguration.mrc** file as follows:

- If you installed Aspect Message Routing on the main application server, and you used the default path for data files during the installation of the Aspect Workforce™ main application server, the path is:

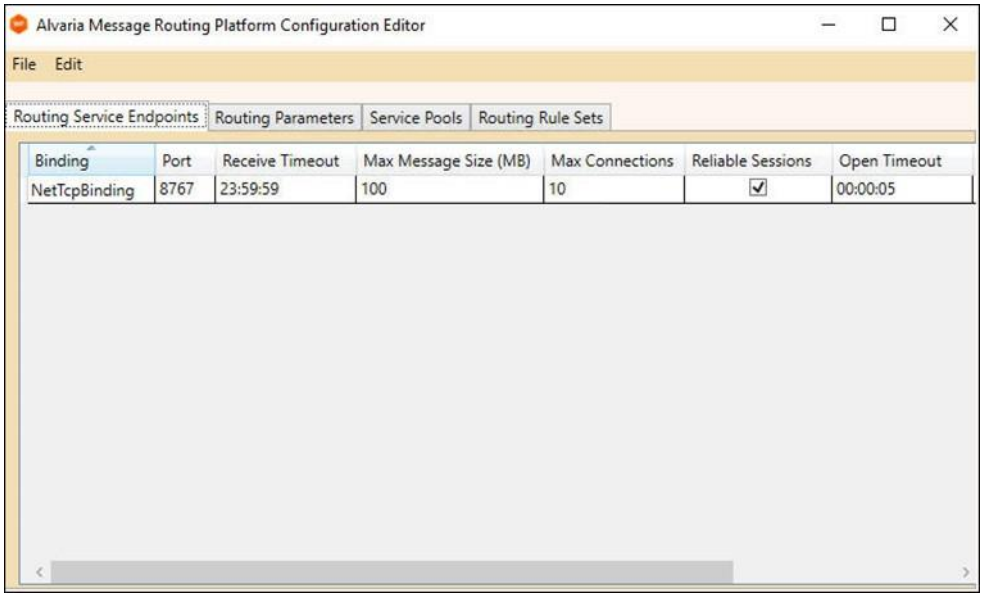
  C:\ProgramData\Aspect\Workforce\WFMData\ AspectMessageRouting

- If you installed Aspect Message Routing on a secondary application server, you must path to the main application WFMData share using a UNC path: ***<main application server>*\WFMData\AspectMessageRouting**

  where ***<main application server>*** is the machine name or IP address of the main application server for Aspect Workforce™.

  Note: If you have installed Aspect Message Routing at a different location than the default, make sure you browse to the correct folder.

4. Double-click the **MessageRoutingConfiguration.mrc** file. The Aspect Message Routing Platform Configuration Editor reopens with the Routing Service Endpoints tab open and populated with default values.

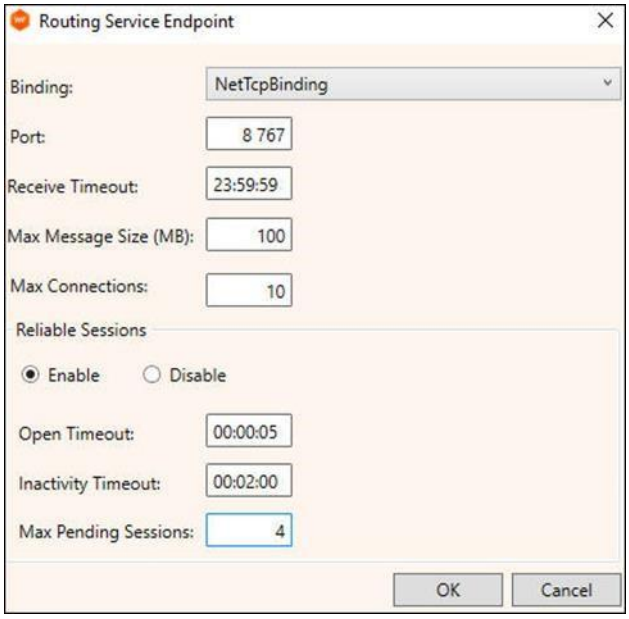


Note: The AMR Editor automatically loads the selected configuration file the next time the same user opens the editor. However, if a different user opens the editor, the user must enter the path for the configuration file.

The parameters on the Routing Service Endpoints tab define how Aspect Workforce™ *components* (such as the Aspect Workforce™ client and Empower) and service *endpoints* (such as WFM Dispatcher and WFM Tallyserver) communicate with the Aspect Message Routing Service. The dialog displays a list of Windows Communications Foundation (WCF) service endpoints that the Aspect Message Routing Service exposes to clients.

Note: Although you can edit the values of these parameters, as explained in the next step, typically you can use the default values.

5. To edit the parameters of an existing endpoint, right-click the row of parameters, and select **Edit**. The Routing Service Endpoint window opens.



The **Routing Service Endpoint** parameters are defined as follows:

Parameter Name	Description	Default Value
Binding Type	The transport protocol used to make calls to the Aspect Message Routing Service. Supported values include: NetTcpBinding, BasicHttpBinding, and WsHttpBinding. For Aspect Workforce™ applications, the binding type should be **NetTcpBinding**.	NetTcpBinding
Port Number	Specifies the port number to be used when communicating with the Aspect Message Routing Service.	8767
Receive Timeout	Specifies the maximum time allowed to receive a request and return a response	23:59:59
Max Message Size (MB)	The maximum size allowed for a message.	100 mb

Max Connections	Maximum number of outbound connections from a NetTcp connection. (Applies only if the Binding Type parameter is **NetTcpBinding**.	10
Parameter Name	**Description**	**Default Value**
Reliable Sessions	Boolean value used to enable/disable Reliable Sessions. Reliable Sessions is a feature that provides end-to-end message transfer reliability between SOAP endpoints on a potentially unreliable network. See the Note about Reliable Sessions, below.	Enable
Open Timeout	With Reliable Sessions enabled, this setting specifies the maximum time to spend opening a connection to the Aspect Message Routing Service.	5 seconds
Inactivity Timeout	With Reliable Sessions enabled, this setting specifies the maximum time to keep an inactive session alive. Note that a keep-alive mechanism keeps the session active indefinitely.	2 minutes
Max Pending Sessions	Maximum size of the queue of pending reliable sessions.	4

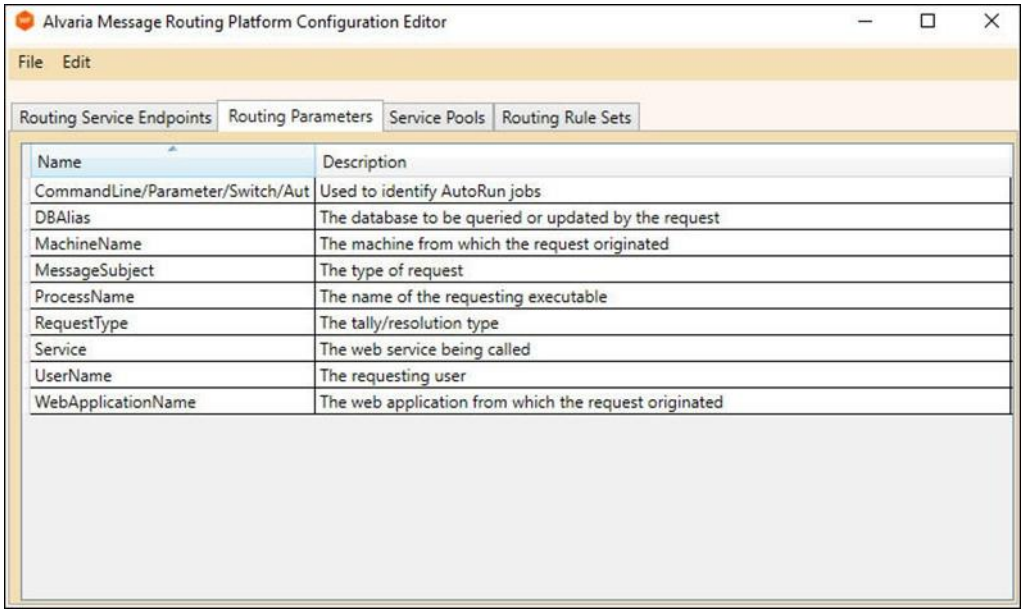
Note: In cases where heavy network traffic is anticipated, Aspect recommends disabling Reliable Sessions. Once disabled, specific timeout values will be required. Contact Aspect Customer Care for assistance.

6. Accept the default values or make any required changes. Click **OK** when done.

   If you change any default values, you must complete the following tasks *after* configuring AMR:

   - Edit general parameters in the WFM Service Installer (see Editing General Parameters).
   - Restart services and other entities (see Restart Requirements).

7. Select the **Routing Parameters** tab. The following window opens.

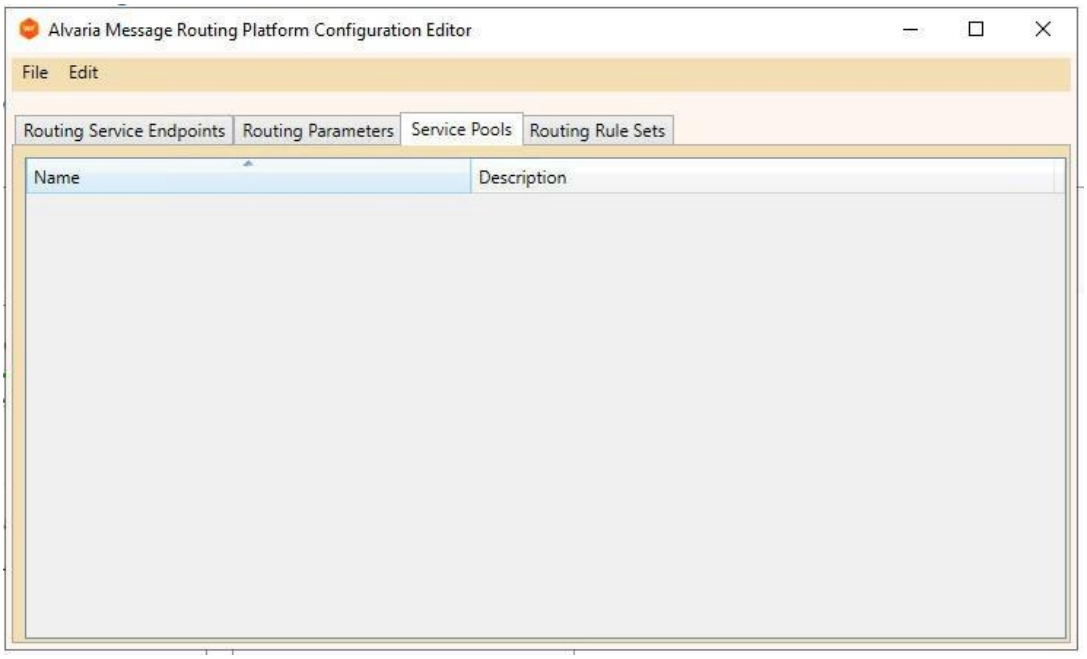


Routing Parameters define the message content that the Aspect Message Routing Service uses when routing messages to Aspect Workforce™ service endpoints, such as WFM Dispatcher and WFM Tallyserver services. When configured in Routing Rule Sets (see Step15), these parameters can be used to route specific messages to specific Service Pools.

8. To edit an existing parameter, right-click it, and select **Edit**. The Routing Parameter dialog box opens.

   You can edit the Description field (although this should rarely be necessary), but you should not edit any of the default Names. If you do so, AMR will not be able to route messages, since these parameters are hard-coded in the Aspect Workforce™ services. Do not create additional parameters since these will be ignored for Aspect Workforce™ applications. Click **OK** after making any changes.

9. Select the **Service Pools** tab. The following window opens.

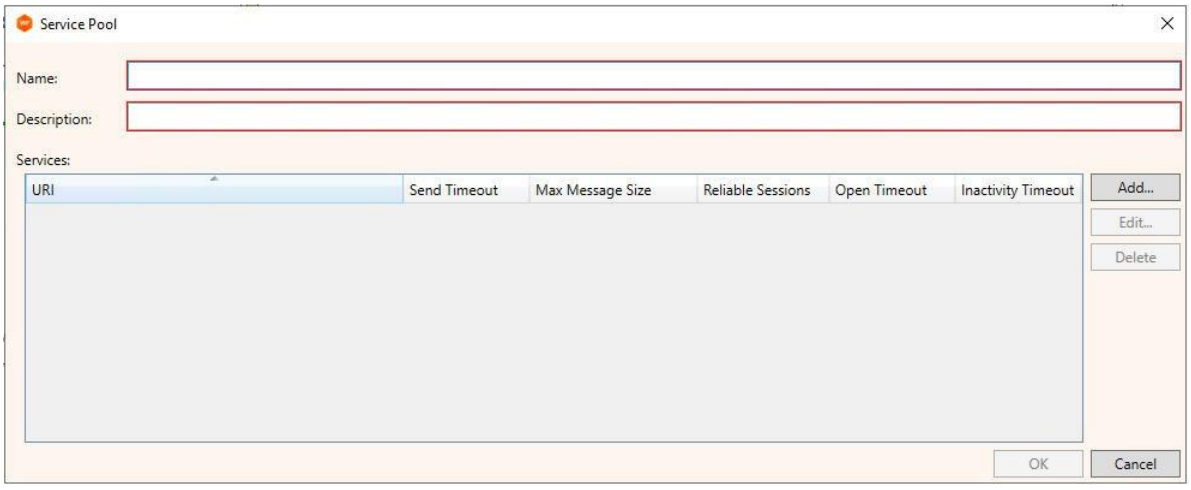


Service Pools define a pool of WFM Dispatcher or WFM TallyServer services available to handle work from various Aspect Workforce™ components, such as Empower, WFM Web Services, or the Aspect Workforce™ client. A Service Pool must consist of one or more WFM Dispatcher or WFM

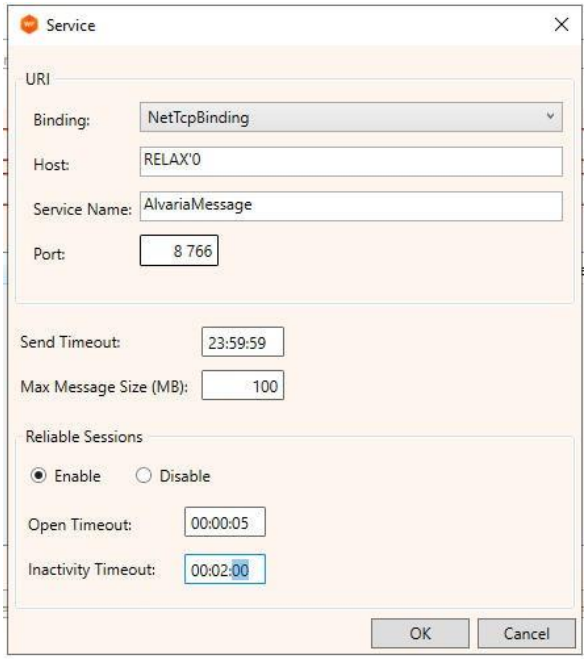
TallyServer services. If a Service Pool consists of multiple WFM Dispatcher or multiple WFM TallyServer services, the Aspect Message Routing Service will route messages using round-robin load balancing.
Additionally, you can create multiple WFM Dispatcher and WFM TallyServer Service Pools in order to divide and isolate message-handling so that requests from one component of Aspect Workforce™ do not affect the performance of other components. For example, you can route WFM TallyServer requests from Autorun jobs or Real-Time Adherence servers to a particular service pool, and WFM TallyServer requests from Aspect Workforce™ rich client users to a different service pool ensure each type of request does not affect the performance of the other. In the example screen shot above, no Service Pools have yet been added.

Note: The following screen shots describe, as an example only, how to add a single WFM TallyServer pool. In this example, the name of the pool is **WFM TallyServer** and the pool description is the same. For the settings appropriate to your own routing scenario, remember to consult Configuring AMR for Common Scenarios.

10. To add a Service Pool, right-click in the window, and select **Add** from the shortcut menu. The **Service Pool** window opens.



11. Type a **Name** and **Description** and click **Add**. The **Service** dialog box opens, where you add Dispatcher and TallyServer machines to a pool. (In the following screenshot, some parameters have been supplied as examples.)

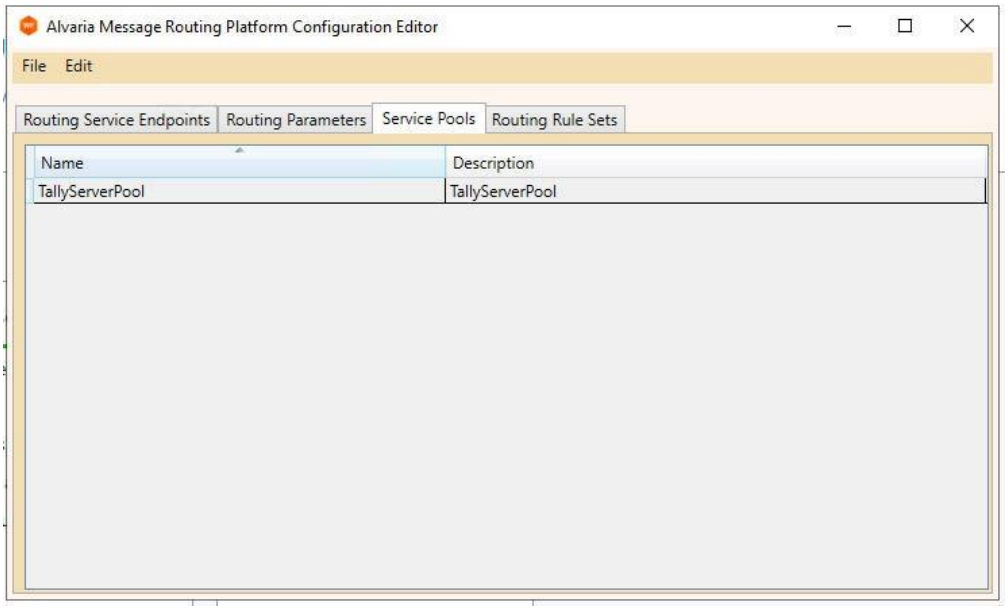


The parameters on the **Services** window are similar to those described in Editing General Parameters.

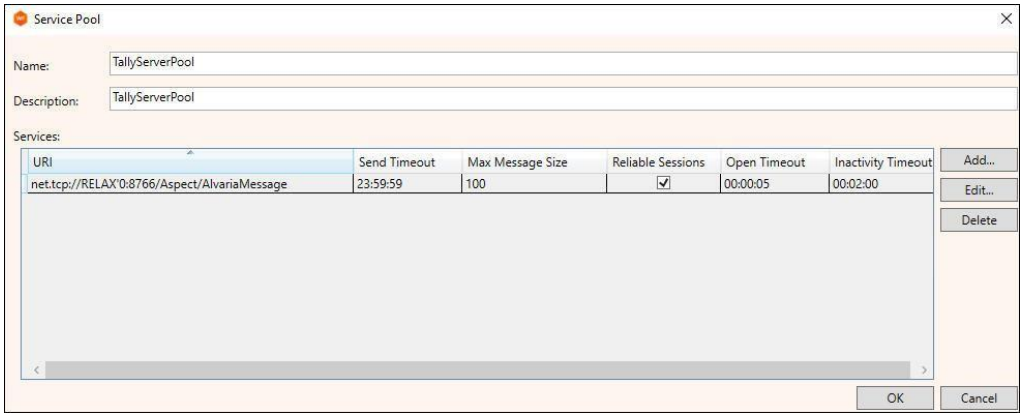
Parameter Name	Description	Default Value
Binding	The transport protocol used to make calls to the Aspect Message Routing Service. For Aspect Workforce™ applications, the binding type should be **NetTcpBinding**. Other supported values include: NetTcpBinding, BasicHttpBinding, and WsHttpBinding.	NetTcpBinding
Host	The name or IP address of the machine where this Dispatcher service is (or will be) installed.	(Type the machine name or IP address in the field.)
Service Name	The identifier Aspect Workforce™ services use when communicating with the Aspect Message Routing Service.	AspectMessage

Port	Specifies the port number that the Dispatcher or TallyServer service uses. The value must match the value of the **AMRPort** parameter in the WFM Service Installer for that service.	Type the appropriate value in the field: Dispatcher: 8765 TallyServer: 8766
Parameter Name	**Description**	**Default Value**
Send Timeout	Specifies the maximum time allowed to send a request and receive a response	23:59:59
Max Message Size (MB)	The maximum size allowed for a message.	100mb
Reliable Session s	Boolean value used to enable/disable Reliable Sessions. Reliable Sessions is a feature that provides end-to-end message transfer reliability between SOAP endpoints on a potentially unreliable network.	Enable
Open Timeout	With Reliable Sessions enabled, this setting specifies the maximum time to spend opening a connection to the Aspect Message Routing Service.	5 seconds
Inactivity Timeout	With Reliable Sessions enabled, this setting specifies the maximum time to keep an inactive session alive. Note that a keep-alive mechanism keeps the session active indefinitely.	2 minutes

12. Complete or edit the fields in the **Services** window using the descriptions in the preceding table and click **OK**. (Fields with a red border still require a valid value.) The **Service Pools** window reopens with the newly added Service Pool displayed.



13. To view the services you just added to the pool, double-click the service pool. The Service Pool window opens, showing a list of URIs that correspond to each machine where an instance of the Dispatcher or TallyServer service is installed or will be installed for that service pool.



14. To add, edit, or delete a URI, use the corresponding buttons on the right of the dialog box.

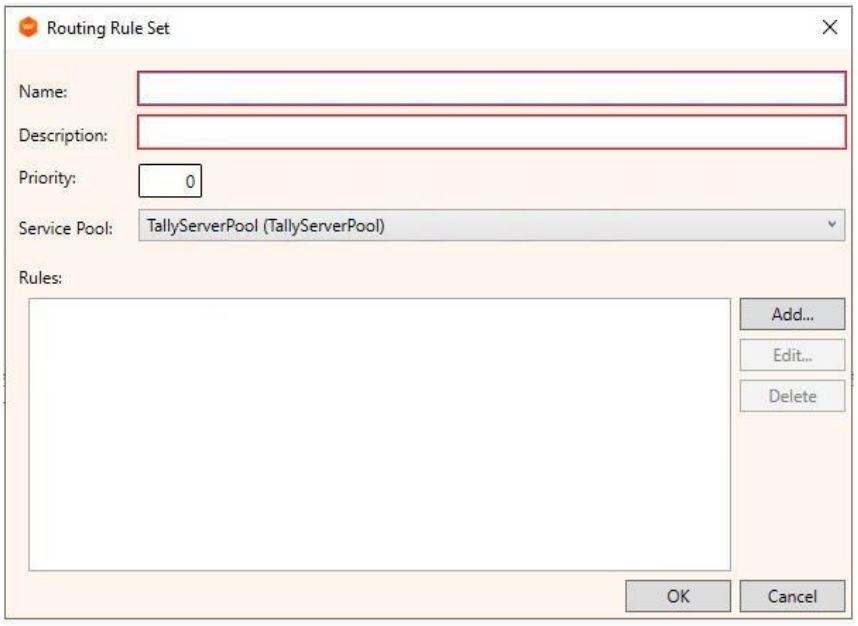
15. Select the **Routing Rule Sets** tab. The Routing Rule Sets page is displayed.

    Routing Rule Sets are used to define the message content that is used to determine whether a given message should be assigned to a particular Service Pool, and therefore routed to one of the pool's WFM Dispatcher or WFM TallyServer services. Each routing rule in a set specifies how a given Routing Parameter should be evaluated to determine if a given message matches a pool. Each routing rule specifies that a given routing parameter is either "equal to" or "not equal to" a given string. Some examples of potential routing rules are listed below.

- MachineName equals 'WFMApp01'
- MachineName does not equal 'WFMApp01'
- WebApplicationName equals 'EAMWeb'

  For a message to match a routing rule set, the routing information in the message must mach *all* of the rules in the routing rule set. However, if more than one rule exists in a rule set for a given parameter, then the routing information for the message must match only one of those rules. A rule set must not have both an "equal to" rule and a "not equal to" rule for the same routing parameter. For more information about routing rules and routing rule sets, see Understanding Routing Rule Sets.

16. To add a new rule set, right-click on the **Routing Rule Sets** window, and select **Add**. The **Routing Rule Set** window opens.



In the **Routing Rule Set** window, complete the fields by referring to the following table:

Field	Description
Name	Enter a Name. For example, “TallyServer Rule 1”
Description	Enter a description. For example, “Rule for TallyServer”.

Priority	You can leave the priority at zero (0) unless you have more than one Dispatcher or TallyServer pool. The priority of a routing rule set is specified as an integer equal to or greater than zero, with zero being the lowest priority. Messages are evaluated against routing rule sets with the highest numerical priority first. That is, first the Routing Rule Set with the highest priority–for example, 5–is evaluated against the message. If the message matches that routing rule set, it is not evaluated against lower priority routing rule sets, such as those with priority 4, 3, 2, and so on. Note that one or more routing rule sets can have the same priority. When routing rule sets have the same priority, the routing rules must be defined such that a message cannot match more than one of the routing rule sets.
Service Pool	The pool of machines that the rule set will be associated with.
Field	**Description**
Rules	The list of rules that make up the Rule Set. In the preceding screenshot, no rules have yet been added. If you have only one pool (either Dispatcher or TallyServer) and you do not define any rules, all work goes to that pool. If you have both Dispatcher and TallyServer pools, you must define rules to specify which pool receives the message.

17. To add a new rule to the rule set, click **Add**. The **Routing Rule** window opens

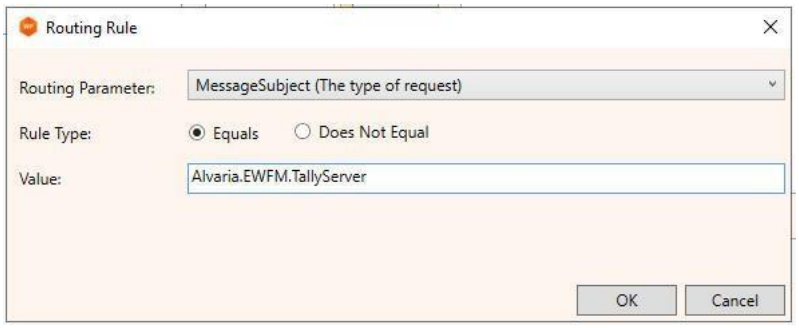
Note: In a scenario where there is only one pool, such as a single Dispatcher pool or a single TallyServer pool, you do not need to specify any rules. Instead, simply complete To add a new rule set, right-click on the to create the **Rule Set**, provide a **Name** and a **Description**, leave the **Priority** at zero, select the **Service Pool**, and then click **OK**. (You must always create a *rule set* for a service pool, even if it contains no rules.) For more complex scenarios, see Configuring AMR for Common Scenarios. That chapter explains in detail how to set up rules correctly for a variety of common scenarios.

18. To configure a rule, complete the **fields** by referring to the following table:

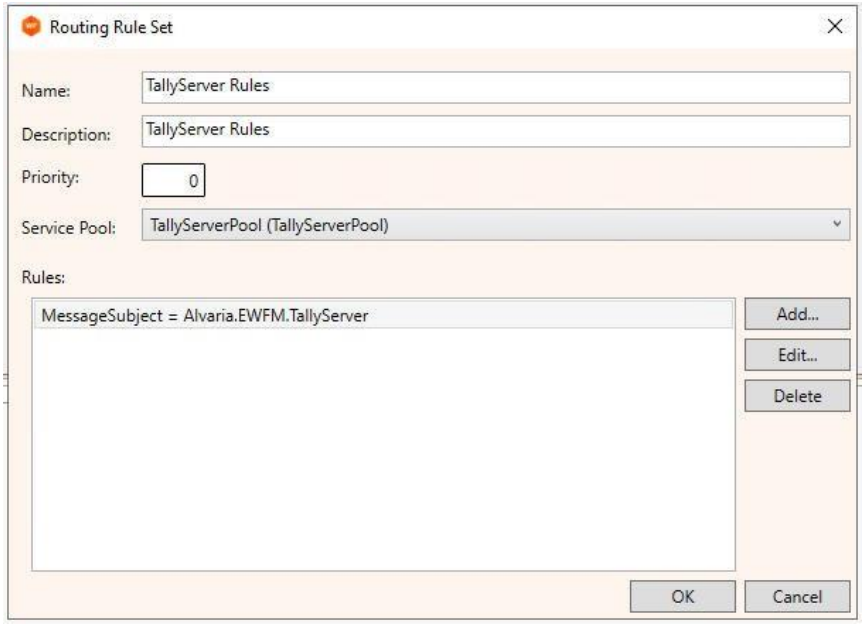
Field	**Description**

Routing Parameters	Select the desired parameter from the drop-down list. For more information about these parameters, see Routing Parameters – Extended Descriptions.
Rule Type	Select the appropriate radio button (**Equals** or **Does Not Equal**) depending on whether you want the specified Routing Parameter to equal the specified Value (see next row).
Value	Type the value that you want to associate with the Routing Parameter. For more information about these parameters, including valid values, see, the Routing Parameters – Extended Descriptions.

19. Following is an example of a completed Routing Rule window:



20. After configuring the rule, click **OK**. The **Routing Rule** window closes, and the **Routing Rule Sets** window displays the new rule.



21. To add another rule, go back to To add a new rule to the rule set, click .

    You can edit or delete an existing rule by right-clicking it and selecting either **Edit** or **Delete**.

22. When you are finished adding rules, click **OK**. The main **Aspect Message Routing Platform Configuration Editor** window reopens.

23. Click **File > Save** and close the window.

24. In Windows Services, restart the **Aspect Message Routing Service**.

Routing Parameters Table

The following table describes the available routing parameters for the Aspect Message Routing Service. In addition to the description, the table provides the typical use of each parameter, along with valid values. Use the information in this table when configuring routing rules in To add a new rule to the rule set, click . Valid values in italics and brackets, such as ***<requesting machine name>***, are descriptions of valid values rather than actual valid values.

Not all of the available parameters are practical to use with the core Aspect Workforce™ product. Some are used primarily with Aspect Workforce™ enhancement packages, such as Empower. For guidance, see the **For Use With** column in the table below.

Routing Parameters – Extended Descriptions

Parameter	Description	Use Cases	For Use With	Valid Values

CommandLine/Parameter/Switch/Autorun	Identifies specific AutoRun jobs.	Used where distinct pooling for AutoRun jobs is wanted for performance reasons, such as isolating requests for resourceintensive AutoRun jobs.	WFM TallyServer load balancing	AutoRun
DBAlias	The database to be queried or updated by the request.	Used in multi-tenant environment s where distinct pooling for each tenant is wanted for performance reasons.	• WFM TallyServer load balancing • WFM Checker load balancing • Empower • Aspect Workforce™ Web Services	*<Aspect Workforce™ database alias>*
MachineName	The machine from which the request originated.	Used where distinct pooling for a particular server is wanted, such as isolating requests from a particular web server or terminal server.	• WFM TallyServer load balancing • WFM Checker load balancing • Empower • Aspect Workforce™ Web Services	*<requesting machine name>*

Parameter	Description	Use Cases	For Use With	Valid Values

MessageSubject	The type of request.	Used where distinct pooling for a particular type of request is wanted for performance reasons, such as isolating WFM Tallyserver requests.	• WFM TallyServer load balancing • WFM Checker load balancing • Empower • Aspect Workforce™ Web Services • Distributed Multi-Channel Performance Simulations	Aspect.EWFM.Controller.Account Aspect.EWFM.Controller.Admin Aspect.EWFM.Controller.AgentProductivity Aspect.EWFM.Controller.Checker Aspect.EWFM.Controller.CheckerQM Aspect.EWFM.Controller.Employee Aspect.EWFM.Controller.Forecast Aspect.EWFM.Controller.IDP Aspect.EWFM.Controller.ImportMap Aspect.EWFM.Controller.Preference Aspect.EWFM.Controller.Schedule Aspect.EWFM.Controller.ShiftBid Aspect.EWFM.Controller.Trade Aspect.EWFM.Controller.TrialSchedule Aspect.EWFM.Controller.PopMessage Aspect.EWFM.Controller.NS Aspect.EWFM.Controller.Seat Aspect.EWFM.TallyServer Aspect.EWFM.MCP.Simulate

Parameter	Description	Use Cases	For Use With	Valid Values
ProcessName	The name of the requesting executable.	Used where distinct pooling for a particular type of request is wanted for performance reasons, such as isolating WFM Tallyserver requests from RealTime Adherence servers.	• WFM TallyServer load balancing • WFM Checker load balancing • Empower • Aspect Workforce™ Web Services	*<program executable name>*

RequestType	The tally/resolution type.	Used where distinct pooling for a particular type of WFM Tallyserver request is wanted for performance reasons, such as isolating Schedule Resolution requests.	WFM TallyServer load balancing	• MBSR (Moment Based Schedule Resolution)–for handling Intra-Day Time Line-only requests. • MBTPT (Moment Based Time Period Tally)–for handling Intra-Day Performance-only requests. • NDBSLT (Nominal Date Based Schedule List Tally)–for handling Agent Productivityonly requests. • NDBST (Nominal Date Based Schedule Tally)–for handling Superstate Houronly requests.

Parameter	Description	Use Cases	For Use With	Valid Values

Service	The web service being called.	Used where distinct pooling for a particular WFM Web Service request is wanted for performance reasons, such as isolating APAgentProductivity.ewf m web service requests.	• Empower • Aspect Workforce™ Web Services	*<WFM Web Service request name>* For a complete list of the request names for the Aspect Workforce™ Web Services, see the Aspect® Workforce – Software Development Kit.
UserName	User name of the requesting Aspect Workforce™ user.	Used where distinct pooling for requests made by a particular Aspect Workforce™ user is wanted for performance reasons, such as isolating requests for resourceintensive users.	WFM TallyServer load balancing	*<Aspect Workforce™ user name>*
WebApplicationName	The web application from which the request originated.	Used where distinct pooling for web applications is wanted for performance reasons, such as isolating all WFM Web Service requests.	• Empower • Aspect Workforce™ Web Services	• EAMWeb – for Empower. • AWS – for Aspect Web Services.

Installing AMR on a Backup Server

AMR can be installed on a second server as a backup to the primary AMR server. If the backup AMR service is installed on a secondary application server, you must configure network access for the AMR service to the AMR configuration file.

This section describes how AMR operates when you are using a backup AMR server. It also describes the post-installation tasks you must complete to implement the backup AMR server. Complete these tasks *after* you have installed and configured AMR on the backup AMR server, as described in Installing Aspect Message Routing and Configuring Aspect Message Routing.

About the Backup AMR Server and Failover

When a backup AMR server is installed, the interaction of the primary and backup AMR servers is as follows.

If the primary Aspect Message Routing Service becomes unavailable (because of, for example, a server reboot or a network issue), a message will attempt to be routed to the primary service until the timeout period has elapsed. (The timeout value is controlled by the **AMR Open Timeout** parameter).

If a backup AMR service has been installed, then once the timeout period has elapsed, the message will be routed to the backup service. This process will continue until the primary service is available. In other words, a message will *always* be routed to the primary service before being routed to the backup service.

So, once the primary service is available, no user intervention is required. Messages are again routed to the primary service. But while messages are routed to the backup service, there is a small delay in message processing because of the timeout period that must elapse before messages are routed to the backup service.

Obtaining a Domain Account

The AMR service on the backup AMR server (or the primary AMR service on a secondary application server) must access the AMR configuration folder, which is installed only on the Aspect Workforce™ main application server. As such, the AMR service requires a domain account to access that folder.

Contact your network administrator to obtain the name and password for this domain account. Sample account name: **AMR**.

Note: In many deployments, the AMR service can operate using the Local System account rather than a network account. For this to occur, the default permissions for the WFMData shared folder (and its subfolders) on the main application server cannot be changed, and domain group policies must not prevent the use of a Local System account. If either of these conditions cannot be met, you must use a network account.

Configuring Network Access for the AMR Service

Use Windows Services to associate your new domain account for AMR with the AMR service.

To configure network access for the AMR service:

1. Log in to the **backup AMR server**.
2. In Windows, go to Administrative Tools > Services.
3. In Windows Services, stop the **Aspect Message Routing Service**.
4. Double-click **Aspect Message Routing Service**.

5. On the **General** page, in the **Startup Type** field, select **Automatic**.
6. On the **Log On** page, in the **Log On As** section, select the **This Account** button.
7. Browse to and select the **AMR** login ID.
8. Enter and confirm the **AMR** password.
9. Click **OK.** A message box is displayed, showing that the service has been granted the Log On As A Service right.
10. In the **Services** window, right-click the Aspect Message Routing Service, and click **Start**.
11. Select **File > Exit** to close the Services dialog box.

Verifying Folder Permissions

The AMR network account for the backup AMR server requires Read access to the AMR configuration folder on the Aspect Workforce™ main application server. Access to this folder is configured automatically by the Aspect Workforce™ installation program. So typically you do not need to configure folder permissions yourself. You can use the following procedure to verify that the correct permissions for the AMR service are in place.

To verify AMR folder permissions:

1. Log in as an administrator to the Aspect Workforce™ **main application server**.
2. Use **Start > Run** to browse to the following folder, where ***MainApp*** is the machine name or IP address of the server: ***MainApp*\WFMData**
3. Right-click the **WFMData** folder and select **Properties**.
4. On the **Sharing** page, click **Share**.
5. In the list of accounts, verify that the **Everyone** account exists, and that it has been assigned the **Read** permission level.
6. If this account does not exist, add the **AMR domain account**, and set the permission level at **Read**.
7. On the **Security** page, verify that the setting for the **Read** permission for the AMR domain account is **Allow**.

Configuring AMR for Common Scenarios

This chapter provides detailed configuration information that you can use to implement common load balancing scenarios. You configure these scenarios with the Aspect Message Routing Service (AMR) Configuration Editor. Where necessary, you can modify the configuration details provided here to meet your specific needs; for example, by adding additional routing rules.

Use this chapter in conjunction with Configuring the Aspect Message Routing Service, which provides step-by-step instructions and screenshots of key dialog boxes. The present chapter provides the specific settings you enter in each dialog box to implement a given scenario.

About the Scenarios

Many of the load-balancing scenarios described in this chapter can be used together in the same deployment. They can also be used with other scenarios involving Empower and Real-Time Adherence.

When used in combination, these scenarios enable requests from both Windows and web clients to be handled in round-robin fashion with minimal customization by the user.

The main scenarios provided here and fully described are:

- Distributed TallyServer
- TallyServer with AutoRun calls in a separate pool
- Distributed Checker

In addition, other commonly used scenarios are described in brief.

All scenarios adhere to the standards of the Aspect Message Routing Service, meaning that all requests are routed to one and only one endpoint. When modifying the recommended configuration settings provided here, be careful that you maintain this condition. If you set up the routing rules such that a request can not match any service pool, or can match more than one pool, an error will result.

For configuration details of common scenarios related to the enhancement packages, such as Empower, see the installation guide for that package.

Configuring Distributed TallyServer

This section describes load balancing with the TallyServer service and provides a procedure for implementing it.

About Distributed TallyServer

With the Aspect Message Routing Service, you can automatically route requests for Intra-Day Performance (IDP), Intra-Day Time Line, Agent Productivity (AP), and other schedule resolution-related information to several Tally Server machines. This lets you scale Aspect Workforce™ when you have a high number of these requests being made at the same time from a number of workstations.

Request Handling Method

AMR spreads incoming requests across parallel Tally Server machines using a round-robin approach. For example, in a configuration with three Tally Server machines, the service sends each request as it arrives to Tally Server 1, then Tally Server 2, then Tally Server 3, then back to 1, and so on. This logic decreases processing time: AMR balances workload to avoid having long queues of tasks on any single Tally Server machine.

To help ensure that Tally Server remains very responsive to interactive TallyServer requests, you can set up a dedicated TallyServer pool for AutoRun requests only. For more information about isolating AutoRun requests in a distributed TallyServer scenario, see Configuring an AutoRun Pool.

Configuring Distributed TallyServer

To configure distributed TallyServer:

1. On the server where AMR is installed, do the following:

- Windows Server 2022 or 2025: Select Start > Aspect > AMR Configuration Editor.

  The Aspect Message Routing Platform Configuration Editor opens.

2. If the configuration file is not already open, select **File > Open** to browse to the **MessageRoutingConfiguration.mrc** file.

For the default path to the configuration file, see Configuring the Aspect Message Routing Service, step 2. When you open the editor, the previously configured values for the configuration file are displayed. (Or, if you have never edited the file, the original default values of the file are displayed instead.)

3. On the Routing Service Endpoints page, a preconfigured endpoint is displayed, showing the default values. Typically, you do not need to change these default values, which are described in the following table:

Parameter	Value
Binding	NetTcpBinding (Recommended binding for Aspect Workforce™.)
Port	8767 (default port for AMR service) (Changes to this default value require a corresponding change to the **AMRPrimaryPort** or **AMRBackupPort** general parameter in the WFM Service Installer and a restart of the AMR service.)
Receive Timeout	23:59:59 (The maximum value.)
Parameter	**Value**
Max Message Size (MB)	100 (Changes to this default value require a corresponding change to the **AMRMaxMessageSizeMB** general parameter in the WFM Service Installer and a restart of the AMR service.)

Max Connections	Maximum number of outbound connections from a NetTcp connection. (Applies only if the Binding Type parameter is **NetTcpBinding**.
Reliable Sessions option	Enable
Open Timeout	00:00:05
Inactivity Timeout	00:02:00
Max Pending Sessions	Maximum size of the queue of pending reliable sessions.

4. If you do need to change a default value, right-click the endpoint, and select **Edit** from the shortcut menu. The Routing Service Endpoint dialog box opens. Edit the desired **value** and click **OK**.
5. Click the **Routing Parameters** tab. The Routing Parameters page is displayed, showing the entities that you can use to configure your routing rules.

   You configure these parameters when setting up routing rules on the Routing Rule Sets page.
6. Review the parameter names and their descriptions, and click the **Service Pools** tab. The Service Pools page is displayed.

   A *service pool* is one or more routing endpoints (that is, computers) for a request. AMR routes a request to a pool if the request matches the routing rules for that pool. All endpoints in a pool must be of the same type: either TallyServer machines or Dispatcher machines, but not a combination of both. So, for this scenario, ensure that all machines you select for the pool are TallyServer machines.
7. Right-click in the grid and select **Add** from the shortcut menu. The Service Pool dialog box opens.
8. Type a Name and Description for the pool, such as **TallyServer Pool** (for both values).
9. Click **Add** next to the Services box. The Service dialog box is displayed.
10. Configure the parameters using the following recommended settings as guidelines:

Parameter	Value

Binding	NetTcpBinding
Host	*<machine name or IP address for a Tally Server>* An IP address may be required if the machine has multiple network cards.
Service Name	AspectMessage (Do not change.)
Port	8766 (default port for TallyServer) (Changes to this default value require a corresponding change to the **AMRPort** parameter. That is, in the WFM Service Installer on the given host, edit the WFM TallyServer service by changing the value of the **AMRPort** parameter to the new value.)
Send Timeout	23:59:59 (The maximum value.)
Max Message Size (MB)	100
Reliable Sessions option	Enable
Open Timeout	00:00:05
Inactivity Timeout	00:02:00

12. Click **OK**.
13. To add another Tally Server to the pool, go back to Click .

    To take advantage of load balancing, you must have at least two Tally Servers in a pool. But AMR still functions correctly with only one TallyServer in the pool.
14. After adding all the desired Tally Servers to the pool, click **OK** to close the Service Pool dialog box.
15. In the editor, click the **Routing Rule Sets** tab. The Routing Rule Sets page is displayed.

    Routing rules sets are instructions to AMR for handling a request. Set up a separate rule for each method of handling a TallyServer request that you want AMR to execute. The configuration of rules sets varies greatly depending on your individual routing needs. For more information, see Understanding Routing Rule Sets.
16. Right-click in the grid and select **Add** from the shortcut menu. The Routing Rule Set dialog box is displayed.

    The rules you set up in this dialog box govern how the Aspect Message Routing Service handles TallyServer calls.
17. Type a Name and Description for the routing rule set, such as **TallyServer Rules** (for both values).
18. Type a value for the priority, such as **0**.

    The routing service evaluates rules in priority order, beginning with the highest numerical value. Different rule sets can have the same priority value, in which case they are evaluated in parallel.
19. For the Service Pool field, select the pool you named in Type a Name and Description for the pool, such as from the drop-down list.
20. Click the **Add** button to the right of the Rules box. The Routing Rule dialog box opens.
21. Configure the parameters as follows:

Parameter	Value
Routing Parameter	MessageSubject (The parameters in the drop-down list correspond to the parameters described on the Routing Parameters page of the editor.)
Rule Type	Equals
Value	Aspect.EWFM.TallyServer (not case-sensitive)

22. Click **OK**. The new rule is displayed in the list of rules in the Routing Rule Set dialog box.

23. To add another rule, go back to step 20.

    Adding rules is a way of routing requests into smaller, more precisely-defined categories. Other relevant parameters for which you might want to configure rules are shown in the following table. For fuller descriptions of the parameters, see Routing Parameters – Extended Descriptions.

Parameter	Comment
MachineName	Computer that is the source of the request.
ProcessName	Specify: • tcs.exe for Aspect Workforce™ • RTAListen.exe for Real-Time Adherence
Parameter	**Comment**
DBAlias	Name of the desired Aspect Workforce™ database.
UserName	Database user that issued the request.
CommandLine	Used to identify AutoRun jobs.
RequestType	One of four Tally/Resolution types: • MBSR for Intra-Day Time Line • MBTPT for IDP • NDBSLT for AP • NDBST for superstate hours

24. Click **OK**. The main page of the editor is displayed.

25. Select **File > Save** to save your changes.

26. Go to Editing AMR Values in WFM Service In and make the required changes in the WFM Service Installer.

Configuring an AutoRun Pool

This section describes load balancing when using an AutoRun pool and provides a procedure for implementing it.

About Using a Dedicated Pool for AutoRun

You can configure the Aspect Message Routing Service to have all AutoRun requests handled by a separate TallyServer pool that is different from the pool you set up previously for Distributed TallyServer.

General Approach and Request Handling Method

To implement this AutoRun scenario, you set up a second Tally Server service pool for requests from AutoRun. Then you associate the AutoRun Tally Server pool with a routing rule set that has a higher priority value than the routing rule set associated with the Distributed Tally Server pool.

AMR evaluates requests against the AutoRun Tally Server pool first because of the higher priority. Any Tally Server requests that originate from AutoRun jobs will match the routing rule set associated with the AutoRun Tally Server pool, so AMR will route those requests to that pool. All other Tally Server requests will match the routing rule set associated with the Distributed Tally Server pool and will be routed to that pool instead.

Configuring an AutoRun Pool

To configure a pool for AutoRun:

1. On the server where AMR is installed, do the following:

- Windows Server 2022 or 2025: Select **Start > Aspect > AMR Configuration Editor**.

  The Aspect Message Routing Platform Configuration Editor opens.

2. If the configuration file is not already open, select **File > Open** to browse to the **MessageRoutingConfiguration.mrc** file.

   For the default path to the configuration file, see Configuring the Aspect Message Routing Service, step 2. When you open the editor, the previously configured values for the configuration file are displayed. (Or, if you have never edited the file, the original default values of the file are displayed instead.)

3. On the Routing Service Endpoints page, a preconfigured endpoint is displayed, showing the default values. Typically, you do not need to change these default values, which are described in the following table:

Parameter	Value

Binding	NetTcpBinding
Port	8767 (default port for AMR service) (Changes to this default value require a corresponding change to the **AMRPrimaryPort** or **AMRBackupPort** general parameter in the WFM Service Installer and a restart of the AMR service.)
Receive Timeout	23:59:59
Max Message Size (MB)	100
Max Connections	Maximum number of outbound connections from a NetTcp connection. (Applies only if the Binding Type parameter is **NetTcpBinding**.
Reliable Sessions option	Enable
Open Timeout	00:00:05
Inactivity Timeout	00:02:00
Max Pending Sessions	Maximum size of the queue of pending reliable sessions.

4. If you do need to change the default value, right-click the endpoint, and select **Edit** from the shortcut menu. The Routing Service Endpoint dialog box opens. Edit the desired value and click **OK**.

5. Click the **Routing Parameters** tab. The Routing Parameters page is displayed.
6. Review the parameter names and their descriptions. You configure these parameters when setting up routing rules on the Routing Rule Sets page.
7. Click the **Service Pools** tab. The Service Pools page is displayed.
8. Right-click in the grid and select **Add** from the shortcut menu. The Service Pool dialog box opens.
9. Type a **Name** and **Description** for the pool, such as **TallyServer Pool - AutoRun** (for both values).
10. Click **Add** next to the Services box. The Service dialog box is displayed.
11. Configure the **parameters** as follows:

Parameter	Value
Binding	NetTcpBinding
Host	*<machine name or IP address for the Tally Server handling AutoRun calls>* An IP address may be required if the machine has multiple network cards.
Service Name	AspectMessage
Port	8766 (default port for TallyServer)
Send Timeout	23:59:59
Max Message Size (MB)	100
Reliable Sessions option	Enable

Open Timeout	00:00:05
Inactivity Timeout	00:02:00

12. Click **OK** and click **OK** to close the Service Pool dialog box.
13. In the editor, click the **Routing Rule Sets** tab. The Routing Rule Sets page is displayed.
14. Right-click in the grid and select **Add** from the shortcut menu. The Routing Rule Set dialog box is displayed.

    The rules you set up in this dialog box governs how the Aspect Message Routing Service handles TallyServer calls for AutoRun. For more information, seeUnderstanding Routing Rule Sets.
15. Type a **Name** and **Description** for the routing rule set, such as **TallyServer Rules - AutoRun** (for both values).
16. Type a value for the priority, such as **5**, that is higher than the value you assigned to the distributed TallyServer pool.

    The Aspect Message Routing Service evaluates requests against routing rule sets in priority order, beginning with the highest numerical value. Because you assigned a higher value in this step, AMR will evaluate requests against the routing rule set associated with the AutoRun Tally Server Pool before it evaluates requests against the routing rule set associated with the Distributed Tally Server pool. (For more information, see Configuring Distributed TallyServer).
17. For the Service Pool field, select the **pool** you named in Type a from the drop-down list.
18. Click the **Add** button to the right of the Rules box. The Routing Rule dialog box opens.
19. Configure the parameters as follows:

Parameter	Value
Routing Parameter	CommandLine/Parameter/Switch/AutoRun
Rule Type	Equals
Value	AutoRun

20. Click **OK**. The new rule is displayed in the list of rules in the Routing Rule Set dialog box.
21. Click **OK**. The main page of the editor is displayed.

22. Select **File > Save** to save your changes.

23. Go to Editing AMR Values in WFM Service In and make the required changes in the WFM Service Installer.

Configuring Distributed Checker

This section describes load balancing with Checker and provides a procedure for implementing it.

About Checker Load Balancing

With Checker load balancing, the Aspect Message Routing Service routes requests for schedule changes to several secondary application servers running the Dispatcher service. Examples of these schedule change requests are requests for vacation or overtime.

The Dispatcher service dispatches internal Aspect Workforce™ messages among multiple controllers. This service enables Aspect Message Routing (AMR) to communicate with the following applications, which are used in request processing:

- Schedule controller, which writes requests to the Aspect Workforce™ database
- Checker controller, which provides for the approval or denial of requests based on Checker rules you set up, then writes the results to the Aspect Workforce™ database

Request Handling Method

For both distributed (that is, load-balanced) and non-distributed WFM Checker, schedule requests that affect other queued schedule requests are processed serially, in the order in which they were submitted. Examples are schedule requests from different agents who are associated with the same group allowance account. By contrast, schedule requests that are completely independent—that is, they do not affect other schedule requests—are processed in parallel. If a large number of these independent requests enters the system, WFM Checker processing is determined and possibly limited by available server resources.

The Checker load-balancing option lets you scale your Aspect Workforce™ installation to handle a high number of requests entering the system simultaneously. It does so by leveraging WFM Dispatcher to take advantage of additional hardware. Aspect Message Routing spreads incoming requests across Dispatcher machines using a round-robin approach. For example, in a configuration with three Dispatcher machines, the software routes to Dispatcher 1, then to Dispatcher 2, then to Dispatcher 3, then to Dispatcher 1 again, and so on.

Using in More Complex Deployments

Special handling might be required if, in addition to Distributed Checker, your deployment includes any of the following:

- An Aspect Advanced Module (that is, Empower, Encompass, or Aspect Campaign Optimizer Adapter)
- An interface with another Aspect product
- A third-party interface with the Aspect Workforce™ Web Services
- For more information, see Dispatcher Pools for Empower and Web Services and Dispatcher Pools for Checker and Non-Checker Requests.

Configuring Distributed Checker

To configure distributed Checker:

1. On the server where AMR is installed, do the following:

- Windows Server 2022 or 2025: Select **Start > Aspect > AMR Configuration Editor**.

  The Aspect Message Routing Platform Configuration Editor opens.

2. If the configuration file is not already open, select **File > Open** to browse to the **MessageRoutingConfiguration.mrc** file.

   For the default path to the configuration file, see Configuring Aspect Message Routing, step 2. When you open the editor, the previously configured values for the configuration file are displayed. (Or, if you have never edited the file, the original default values of the file are displayed instead.)

3. On the Routing Service Endpoints page, a preconfigured endpoint is displayed, showing the default values. Typically, you do not need to change these default values, which are described in the following table:

Parameter	Value
Binding	NetTcpBinding
Port	8767 (default port for AMR service) (Changes to this default value require a corresponding change to the **AMRPrimaryPort** or **AMRBackupPort** general parameter in the WFM Service
Parameter	**Value**
	Installer and a restart of the AMR service.)
Receive Timeout	23:59:59

Max Message Size (MB)	100
Max Connections	Maximum number of outbound connections from a NetTcp connection. (Applies only if the Binding Type parameter is **NetTcpBinding**.
Reliable Sessions option	Enable
Open Timeout	00:00:05
Inactivity Timeout	00:02:00
Max Pending Sessions	Maximum size of the queue of pending reliable sessions.

4. If you do need to change a default value, right-click the endpoint, and select **Edit** from the shortcut menu. The Routing Service Endpoint dialog box opens. Edit the desired **value** and click **OK**.
5. Click the **Routing Parameters** tab. The Routing Parameters page is displayed.
6. Review the **parameter names** and their **descriptions**. You configure these parameters when setting up routing rules on the Routing Rule Sets page.
7. Click the **Service Pools** tab. The Service Pools page is displayed.
8. Right-click in the grid and select **Add** from the shortcut menu. The Service Pool dialog box opens.
9. Type a Name and Description for the pool, such as **Dispatcher Pool - Checker** (for both values).
10. Click **Add** next to the Services box. The Service dialog box is displayed.
11. Configure the **parameters** as follows:

Parameter	Value
Binding	NetTcpBinding

Parameter	Value
Host	*<machine name or IP address for a Dispatcher>* An IP address may be required if the machine has multiple network cards.
Service Name	AspectMessage
Port	8765 (default port for Dispatcher) (Changes to this default value require a corresponding change to the **AMRPort** parameter. That is, in the WFM Service Installer on the given host, edit the WFM Dispatcher Service by changing the value of the **AMRPort** parameter to the new value.)
Send Timeout	23:59:59
Max Message Size (MB)	100
Reliable Sessions option	Enable
Open Timeout	00:00:05
Inactivity Timeout	00:02:00

12. Click **OK**.
13. To add another Dispatcher to the pool, go back to Click .

    To take advantage of load balancing, you must have at least two Dispatchers in a pool. But AMR will still function correctly with only one Dispatcher in the pool.
14. After adding all the desired Dispatchers to the pool, click **OK** to close the Service Pool dialog box.
15. In the editor, click the **Routing Rule Sets** tab. The Routing Rule Sets page is displayed.
16. Right-click in the grid and select **Add** from the shortcut menu. The Routing Rule Set dialog box is displayed.

The rules you set up in this dialog box govern how the Aspect Message Routing Service handles Checker and Dispatcher calls. needs. For more information, seeUnderstanding Routing Rule Sets.

17. Type a **Name** and **Description** for the routing rule set, such as **Dispatcher Rules - Checker** (for both values).

18. Type a **value** for the priority, such as **0**.

    The routing service evaluates rules in priority order, beginning with the highest numerical value. Different rule sets can have the same priority value.

19. For the Service Pool field, select the **pool** you named in Type a Name and Description for the pool, such as from the drop-down list.

20. Click the **Add** button to the right of the Rules box. The Routing Rule dialog box opens.

21. Configure the parameters as follows:

Parameter	Value
Routing Parameter	MessageSubject (The parameters in the drop-down list correspond to the parameters described on the Routing Parameters page of the editor.)
Rule Type	Equals
Value	Aspect.EWFM.Controller.CheckerQM

22. Click **OK**. The new rule is displayed in the list of rules in the Routing Rule Set dialog box.

23. Click **OK**. The main page of the editor is displayed.

24. Select **File > Save** to save your changes.

25. Go to Editing AMR Values in WFM Service In and make the required changes in the WFM Service Installer.

Optimizing WFM Checker for Load Balancing

To help ensure that the WFM Checker service operates at maximum efficiency, follow these tuning tips:

- In WFM Service Installer, verify that the following Checker parameters are suitable for the configured number of total Dispatcher threads:

MaxCheckerThreads + MaxPreProcessorThreads = Total number of required threads for all Dispatchers that are handling Checker work
For example, if MaxCheckerThreads = 4 and MaxPreProcessorThreads = 2 (these are the default values), then the total number of threads for all installed Dispatchers handling Checker work must be 6 or greater.

- If Checker work is not partitioned from other work, such as when Distributed Checker and Empower share the same Dispatcher pool, then ensure that the total number of threads for all installed Dispatchers is greater than MaxCheckerThreads + MaxPreProcessorThreads. Setting these Checker parameters correctly in the WFM Service Installer helps ensure that Checker and non-Checker work can be processed in a timely fashion. (This type of non-partitioned deployment is not recommended.)
- In the WFM Service Installer, configure the ThreadCount parameter for the WFM Dispatcher service. If WFM Dispatcher is connected to multiple databases, this thread count is applied independently for each database.
- When WFM Checker is operating under a high load (such as when Rechecking Open Requests), consider utilizing the CPU of all Dispatchers that are handling Checker work as fully as possible. Through trial and error, you can increase the MaxCheckerThreads in tandem with the ThreadCount of the Dispatchers that are handling Checker work until you are using all CPUs on the Dispatcher servers.

Configuring Other Scenarios in Brief

This section provides brief overviews of how to configure additional scenarios. Some scenarios are similar to those already described. But although the scenarios are similar, the configuration approach is different: usually, the goal is to separate a single type of request from all other request types.

Because of the flexibility of the Aspect Message Routing Service, you can effectively obtain the same routing results from a variety of configuration setups.

These overviews assume that you are familiar with the AMR Configuration tool and the related terms and concepts described previously in this chapter and in Configuring the Aspect Message Routing Service.

Dispatcher Pools for Empower and Web Services

This scenario involves creating two separate Dispatcher pools as follows:

- A Dispatcher pool for Empower —Used for Empower requests only.
- A Dispatcher pool for Aspect Workforce™ Web Services requests—Used by Encompass, Aspect Campaign Optimizer Adapter, Aspect Workforce™ Engagement Management, and other Aspect products that call the web services. Examples of these other Aspect products are Aspect Performance™ and Aspect Quality™.

Using the following guidelines ensures that requests that match routing rules for Empower are handled by a separate Dispatcher pool from requests that match routing rules for the Aspect Workforce™ Web Services. Further, it prevents any requests that match routing rules in a distributed Checker scenario from matching routing rules in either the Empower Dispatcher pool or the Aspect Web Services Dispatcher pool.

The Aspect Message Routing Service is *required* for communication from the Aspect advanced modules and the Aspect Workforce™ Web Services to the Aspect Workforce™ database, and for communication from the database to the advanced modules and the web services.

For Empower Dispatchers:

1. Create a service pool for the Empower advanced module, such as **EAM**.

2. Define a routing rule for this pool using the parameter **WebApplicationName**, with the value **equal** to **EAMWeb**.

For Aspect Workforce™ Web Services Dispatchers:

1. Create a service pool for the Aspect Web Services, such as **AWS**.
2. Define a routing rule for this pool using the parameter **WebApplicationName**, with the value **equal** to **AWS**.

Dispatcher Pools for Checker and Non-Checker Requests

You can configure a scenario for Checker Dispatchers by creating two service pools that separate requests into the Checker and non-Checker categories. This scenario is based on the scenario described in Configuring Distributed Checker. But it extends that scenario by ensuring that requests unrelated to Checker are handled in a separate pool.

To configure Checker Dispatcher:

1. Create a service pool for Checker requests.
2. Define a routing rule for this pool using the parameter **MessageSubject**, with the value **equal** to **Aspect.EWFM.Controller.CheckerQM**.
3. Create a service pool for non-Checker requests.
4. Define a routing rule for this pool using the parameter **MessageSubject**, with the value ***not*** **equal** to **Aspect.EWFM.Controller.CheckerQM**.

Tally Servers for Real-Time Adherence

You can configure a scenario for Real-Time Adherence Tally Servers using a similar process to that for configuring Dispatcher pools for Checker. Create two service pools that separate requests into those related to Real-Time Adherence and those not related to Real-Time Adherence. In this case, the service (TallyServer) is the same in both pools, and the process that generated the request is the basis of the routing.

To configure Real-Time Adherence Tally Servers:

1. Create a service pool for Real-Time Adherence requests.
2. Define a routing rule for this pool using the parameter **MessageSubject**, with the value **equal** to **Aspect.EWFM.TallyServer**.
3. Define a second routing rule for this pool using the parameter **ProcessName**, with the value **equal** to **RTAListen.exe**.
4. Create a service pool for requests not pertaining to Real-Time Adherence.
5. Define a routing rule for this pool using the parameter **MessageSubject**, with the value **equal** to **Aspect.EWFM.TallyServer**.
6. Define a second routing rule for this pool using the parameter **ProcessName**, with the value ***not*** **equal** to **RTAListen.exe**.

Tally Servers for Non-Distributed Checker

This section describes how to route Tally Server requests from Checker to a dedicated pool of TallyServers that handle Checker requests only. This approach does not require multiple Dispatchers to be configured first. (That is, use this scenario with a non-distributed Checker deployment.) To configure Tally Servers for non-distributed Checker:

1. Create a service pool of TallyServers for Checker requests.
2. Define a routing rule for this pool using the parameter **MessageSubject**, with the value **equal** to **Aspect.EWFM.TallyServer**.
3. Define a second routing rule for this pool using the parameter **ProcessName**, with the value **equal** to **WFMChecker.exe**.

Tally Servers for Distributed Checker

Like the previous section, this section describes how to route Tally Server requests from Checker to a dedicated pool of TallyServers that handle Checker requests only. But, in contrast, this approach assumes that you have configured multiple Dispatchers in a distributed Checker deployment.

To configure Tally Servers for distributed Checker:

1. Create a service pool of TallyServers for Checker requests.
2. Define a routing rule for this pool using the parameter **MessageSubject**, with the value **equal** to **Aspect.EWFM.TallyServer**.
3. Define a second routing rule for this pool using the parameter **MachineName**, with the value **equal** to ***<machine name of Checker Dispatcher host>***.

Dispatcher Pool for Multi-Channel Performance Simulations

You can configure a scenario for Multi-Channel Performance (MCP) Simulation Dispatchers by creating two service pools that separate requests into the MCP Simulation and non-MCP Simulation categories. This scenario ensures that requests unrelated to MCP simulations are handled in a separate pool.

Note: Due to the potential for long-running, CPU-intensive calculations, Aspect recommends always creating a separate Dispatcher pool for Distributed MCP Simulations to ensure other areas of Aspect Workforce™, such as the Workforce Engagement Management Web User Interface, are not affected by long-running MCP simulations.

To configure MCP Dispatcher:

1. Create a service pool for MCP Simulation requests.
2. Define a routing rule for this pool using the parameter **MessageSubject**, with the value **equal** to **Aspect.EWFM.MCP.Simulate**.
3. Create a service pool for non-MCP Dispatcher requests.
4. Define a routing rule for this pool using the parameter **MessageSubject**, with the value ***not*** **equal** to **Aspect.EWFM.MCP.Simulate**.

Editing AMR Values in WFM Service Installer

In the AMR Configuration Editor, the values you set for some fields must match values in the WFM Service Installer. This section provides an overview of how the values in the two utilities relate to each other and describes how to make the necessary changes.

After completing this section, restart WFM services and other entities as required. The necessary restarts are described in Restart Requirements.

About AMR Values and WFM Service Installer

In the AMR editor, fields on the Routing Service Endpoint dialog box are prepopulated with default values. These default values represent AMR-related general parameters in the WFM Service Installer. When using the AMR editor, if you change any of these default values to suit your company's needs, you must make a corresponding change to the AMR general parameter in the WFM Service Installer.

Also, on the Service Pools page in the AMR editor, the **Port** field corresponds to a service-specific parameter named **AMRPort** for the TallyServer and Dispatcher services. When using the AMR editor, if you specify a port number different from the default value for that service (8766 for TallyServer and 8765 for Dispatcher), you must change the corresponding value in WFM Service Installer to match.

In addition, load balancing scenarios for Distributed Checker and Distributed TallyServer require additional configuration updates to these services in WFM Service Installer.

Other general parameters for the AMR service, such as the AMRPrimaryHost, are set automatically during the first installation of AMR and also during the backup installation of AMR, if you have a backup. Typically, these parameters do not require editing in the WFM Service Installer.

Editing General Parameters

When you configure routing service endpoints in the AMR Configuration Editor, any changes you make to the default values must also be made in the WFM Service Installer. All fields on this dialog box correspond to AMR general parameters, which are configured in the WFM Service Installer.

The following table shows the fields in the Routing Service Endpoint dialog box and their corresponding general parameters. For descriptions of these fields, see Configuring Aspect Message Routing, step 5.

Field in AMR Editor	General Parameter
Binding	AMRPrimaryBinding
Port	AMRPrimaryPort
Receive Timeout	AMROperationTimeout
Max Message Size (MB)	AMRMaxMessageSizeMB
Reliable Sessions	AMRReliableSession

Open Timeout	AMROpenTimeout
Inactivity Timeout	AMRInactivityTimeout

To edit a general parameter:

1. On a server where AMR is installed, do the following:

   Windows Server 2022 or 2025: Select **Start > Aspect > WFM Service Installer**. The Aspect **Service Installer** window opens.

2. Select **Edit > General Parameters.** The **General Parameters** window opens.
3. In the list of parameters, double-click a **parameter** that you want to change. The **Edit General Parameter** dialog box opens.

   All AMR-related parameters begin with **AMR**.

4. Type the new **value** for the parameter.

   For guidance, see the table above.

5. To edit another parameter, go back to In the list of parameters, double-click a .
6. When you have finished editing the parameters, close the **Edit General Parameter** dialog box, and close the **General Parameters** dialog box.
7. In the Aspect Service Installer main window, select **File > Save** to save your changes.

   Note: If you are editing the General Parameters on the secondary application server instead of the main application server, then log in to the main application server, and restart the WFM Information Server service in Windows services.

Editing Service-Specific Parameters

All Dispatcher machines must be configured in the AMR editor to use the same port (default **8765**), and this port must also match the *service-specific* parameter, **AMRPort**, for the Dispatcher service in the WFM Service installer. Likewise, all TallyServer machines must be set up in the AMR editor to use the same port (default **8766**), and this port must also match the *service-specific* parameter, **AMRPort**, for the TallyServer service in the WFM Service installer.

In addition, for both Dispatcher and TallyServer, you must configure the **AMRHost** parameter as described in the following procedures.

Editing the TallyServer Service

Complete this procedure for each TallyServer instance in your deployment.

To edit the TallyServer service for AMR:

1. On a server where a TallyServer is installed, do the following:

   - Windows Server 2022 or 2025: Select **Start > Aspect > WFM Service Installer**.

   The Aspect **Service Installer** window opens.

2. In the list of services, select **WFM TallyServer**. The parameters with their current values are displayed on the right.
3. Select **Edit > Edit**. The WFM TallyServer dialog box is displayed.
4. On the General page, for the **AMRHost** parameter, do one of the following:
   - Leave the value of the parameter blank (recommended)
   - For servers with more than one network interface card (NIC), type the IP address of the NIC card on the server where the WFM Dispatcher service is installed.
5. For the **AMRPort** parameter, verify that the value is **8766** (default) or the value you replaced it with in the AMR editor.
6. If you changed the default values for **Max Connections** and **Max Pending Sessions** in the AMR Configuration Editor, change the corresponding values here to match the same values.

   That is, change the values for **AMRMaxConnections** and **AMRMaxPendingSessions**, respectively. For more information, see step 5, above.
   This port number must match the port number you have configured for the TallyServer machines in the AMR editor.
7. Click **OK**. The new values for the AMRHost and AMRPort parameters are displayed in the Aspect Service Installer main window.
8. Select **File > Save** and select **File > Exit**.

Editing the Dispatcher Service

Complete this procedure for each Dispatcher instance in your deployment.

To edit the Dispatcher service for AMR:

1. On a server where a TallyServer is installed, do the following:

- Windows Server 2022 or 2025: Select **Start > Aspect >** WFM Service Installer.

  The Aspect **Service Installer** window opens.

2. In the list of services, select **WFM Dispatcher Service**. The parameters with their current values are displayed on the right.
3. Select **Edit > Edit**. The WFM Dispatcher Service dialog box is displayed.
4. On the General page, for the **AMRHost** parameter, do one of the following:

- Leave the value of the parameter blank (recommended)
- For servers with more than one network interface card (NIC), type the IP address of the NIC card on the server where the WFM Dispatcher service is installed.

5. For the **AMRPort** parameter, verify that the value is **8765** (default) or the value you replaced it with in the AMR editor.
6. If you changed the default values for **Max Connections** and **Max Pending Sessions** in the AMR Configuration Editor, change the corresponding values here to match the same values.

   That is, change the values for **AMRMaxConnections** and **AMRMaxPendingSessions**, respectively. For more information, see step 5, above.
   This port number must match the port number you have configured for the Dispatcher machines in the AMR editor.

7. Click **OK**. The new values for the AMRHost and AMRPort parameters are displayed in the Aspect Service Installer main window.
8. Select **File > Save** and select **File > Exit**.

Additional Editing for Distributed Checker

If you are implementing a distributed Checker scenario, edit the WFM Checker service in the WFM Service Installer.

To edit the Checker service for AMR:

1. On a server where the Checker service is installed, do the following:

- Windows Server 2022 or 2025: Select **Start > Aspect >** WFM Service Installer.

  The Aspect **Service Installer** window opens.

2. Select **WFM Checker** in the list of services and select **Edit > Edit**. The WFM Checker editor window opens.
3. Click the tab for the **database alias** you are using.
4. For the **CheckerMessageTransportProgId** parameter and the **PreprocessorMessageTransportProgId** parameter, change the displayed value (that is, **Aspect.EWFM.DirectMessageTransport**) to the following: **Aspect.EWFM.AMRMessageTransport**
5. Click **OK**.
6. In the Aspect Service Installer main window, select **File > Save**, and select **File > Exit**.

Additional Editing for Distributed TallyServer

If you are implementing a distributed TallyServer scenario, edit a general parameter related to TallyServer in the WFM Service Installer.

To edit the TallyServer general parameter:

1. On the main application server, do the following for Windows Server 2022 or 2025: Select **Start > Aspect > WFM Service Installer**. The Aspect **Service Installer** window opens.
2. Select **Edit > General Parameters**. The General Parameters window opens.
3. Double-click the **TallyTransport** parameter in the list. The Edit General Parameter dialog box opens.
4. Change the displayed value (that is, **COM**) to **AMR**, and close the dialog box. The new value is displayed in the General Parameters window.
5. Close the **General Parameters** window, and click **Yes** to save your change.
6. In the Aspect Service Installer main window, select **File > Save**, and select **File > Exit**.

Note: If you are editing the TallyTransport general parameter on the secondary application server instead of the main application server, then log in to the main application server, and restart the WFM Information Server service in Windows services.

Restart Requirements

When you make certain types of changes in the AMR Configuration Editor, you must restart Aspect Workforce™ services and sometimes other entities. Complete these restarts *after* you have made any required edits to the general parameters in the WFM Service Installer (see Editing AMR Values in WFM Service Installer)

The following table describes the restart requirements. The cross-references in the Change column refer to the relevant step in the Configuring Aspect Message Routing procedure where this change is performed.

Change	Restart Information
Modifying AMR endpoints (see step 6, above)	Always restart: • AMR service • WFM Dispatcher (all instances) • WFM Information Server (on the main application server—only if you needed to edit a general parameter on the secondary application server. See Editing General Parameters). • Internet Information Services (if installed for an enhancement package such as Empower) If using Distributed TallyServer, also restart: • WFM TallyServer (all instances) • Aspect Workforce™ client (on all client machines) • RTAListen (all instances)

Change	Restart Information
Adding or modifying service pools (That is, creating new pools, or removing WFM Dispatcher or WFM TallyServer records) (see step 9, above)	Always restart: • WFM services (that is, TallyServer or WFM Dispatcher instances) if you made a change that requires a corresponding change in the WFM Service Installer (such as changing the port). See Editing Service-Specific Parameters. Do not restart: • AMR service(s)—main and backup. (The AMR service monitors the configuration file and automatically loads any changes once they are saved.) • WFM services that you added, removed, or modified, unless you made the qualified change described previously.

Adding or modifying routing rule sets (see step 15, above)	Do not restart any services. (If you create new routing rule sets or modify existing rule sets—such as by adding, removing, or modifying rules in a specific rule set—you do not need to restart any services. The AMR service monitors the AMR configuration file and automatically loads any changes once they are saved.)

Understanding Routing Rule Sets

This section describes how to interpret rule sets and how to differentiate rules sets so that they match your routing objectives.

For a full list of the available parameters that you can use to build your routing rules and routing rule sets, see Routing Parameters Table. The table provides the following information for each routing parameter:

- Parameter name
- Parameter description
- Use cases for implementing the parameter
- Aspect applications for which the parameter is suitable
- Valid values for the parameter

Interpreting Routing Rule Sets

Consider this moderately complex routing rule set:

MessageSubject = Aspect.EWFM.Controllers.IDP
MessageSubject = Aspect.EWFM.Controllers.NS
DBAlias = WFMPROD
MachineName ≠ WebServer3
MachineName ≠ WebServer4

Two of the rules state that the MessageSubject parameter must be equal to a given value. Two other rules state that the MachineName parameter must *not* be equal to a given value. What attributes, then, must a message contain to match this sample routing rule set?

To match this routing rule set, a message must have the following attributes:

- Must be either an IDP or a Notification server request.

  Specifically, the MessageSubject parameter in the request must be either **Aspect.EWFM.Controllers.IDP** (indicating an IDP request) or **Aspect.EWFM.Controllers.NS** (indicating a Notification Server request).

- Must be a request for the WFMPROD database.
- Must not be a request that comes from WebServer3 or WebServer4.

  In other words, a request from any server in the deployment except these two is acceptable.

From this example, we can generalize some rules about requests and routing rule sets:

1. If a parameter has more than one value that it can be equal to, then the request need only match one of the values.
2. If a parameter has more than one value that it *cannot* be equal to, then the request can match any other value except those.
3. If no rules are set up for a service pool, then the pool will receive all messages.
4. If a request matches more than one routing rule set having the same priority, an error results.

Differentiating Routing Rule Sets

It is important to differentiate routing rule sets from each other to avoid, for example, routing requests to a machine that cannot handle the request. When a message is routed to the wrong service, an error results.

Consider the following common scenario, which routes messages to the wrong service because the routing rule sets are not sufficiently differentiated.

Pools:

- TallyServer pool—for Distributed TallyServer requests
- Dispatcher pool—for requests from Empower, Aspect Workforce™ Web Services, Multi-channel Performance Simulations, Encompass, and Aspect Campaign Optimizer Adapter

Routing rule sets:

- TallyServer routing rule set:

  MessageSubject = Aspect.EWFM.Tallyserver
- Dispatcher routing rule set:

  (No rules created.)

Routing rule set priority:

Both rules sets configured at priority **0** (zero).

Expected behavior:

Since the TallyServer rule set has the MessageSubject specified as Tallyserver, AMR is correctly configured.

However, it is a little more complicated than that.

Actual behavior:

Since both rule sets have the same priority (that is, 0), the rule sets are evaluated in parallel. And because the Dispatcher rule set has no rules, it is configured to handle all requests. So a TallyServer request would match the routing rule set for *both* pools. Any request that matches multiple routing rule sets of the same priority (in this case, priority 0), is not routed and results in an error.

Solution:

Change the priority of the TallyServer rule set to a greater value than the Dispatcher rule set.

This change ensures that all TallyServer messages are handled by the TallyServer rule set, and *only* the TallyServer rule set. This is because, when a message matches a rule set, the Aspect Message Routing Service stops further rule evaluation for that message.

Another solution is to leave the priority of both rule sets with the same value (0), but to add the following rule to the empty Dispatcher rule set:

MessageSubject != Aspect.EWFM.Tallyserver

Note: The rule type **Does Not Equal** is rendered as **!=** when viewing the rule in the Routing Rule Set dialog box.

Installing User Workstations

This chapter provides an overview and instruction for setting up each workstation that will run the Aspect Workforce™ client. Instructions for uninstalling the client are also provided.

Note: The installation program automates several tasks that were formerly manual steps in prior releases of Aspect Workforce™. As you progress through the installation wizard, some of the processes might require several minutes to complete. This is normal and does not indicate any issues with your hardware, software, or the installer. When the installation is complete, a wizard screen confirms that the installation was successful.

Before You Begin

Verify the prerequisites to the installation. You then have several options for installing the client software.

Verifying Prerequisites

Before you set up a workstation, verify that:

- You have administrator access to the designated client machine.
- Your workstation uses a supported operating system. Check the Aspect Workforce™ Release Note for this information.
- The database client is installed on the workstation:
- For Oracle, see Installing the Client Software.
- For SQL Server, see Installing the SQL Server Client Software.

Installation Options

You can install the Aspect Workforce™ client in any of three ways:

- Launch the installation wizard from the distribution CD.
- Run the installation wizard from the main application server.
- Install with a command line using an XML configuration file provided with the product. For instructions on using this options, see Installing with a Command Line.

Installing from the Product CD

To install the Aspect Workforce™ client from the product CD:

1. Log in as an administrator to the user workstation.
2. Insert the **Aspect Workforce™ Software CD** and open the file **Setup.exe**. The product selection window of the installation wizard opens.
3. Click **Aspect Workforce™**. If any prerequisite software is not already installed on the server, then the Aspect Prerequisite Installer window opens, displaying a list of prerequisites but uninstalled software. Click **Install** to install the prerequisite software. When installation is complete, the Welcome window of the **Install Wizard For Workforce** opens.

4. Click **Next**. The **Destination Folders** window opens.
5. To accept the default (recommended) location for the program files, click **Next**. Otherwise, click **Change**, and browse to or type a different **path**, and click **OK**. The Data Folder window opens.
6. To accept the default (recommended) location for the data files, click **Next**. Otherwise, click **Change**, and browse to or type a different **path**, and click **OK**. The **Custom Setup** window opens.
7. Click the User Workstation **icon**, and select This Feature, And All Subfeatures, Will Be Installed On Local Hard Drive.
8. Click **Next**. The Main Application Server window opens.
9. Type the name of the **Aspect Workforce™ main application server** and click **Next**. The DCOM Servers window opens.
10. In the **DCOM Servers** window, verify or type the **machine name** that is running each of the TallyServer, Updater, Checker, and ACD Processing Server services.

    The fields in this window are populated as follows:

- If the service has been added in the WFM Service Installer on the main application server or on another secondary application server, then the field displays the name of that server.
- If the service has not been added yet, then the field is blank. In this case, type the name of the server that will host this service.
- If the Tallyserver service has been added to multiple servers, then the drop-down list for the Tallyserver field displays the names of these servers. In this case, select the name of the Tallyserver host server that your workstation will access. If Tallyserver will be installed later on a server that is not displayed, then type the name of that server.

11. Click **Next**. The **Ready To Install** window opens.
12. Click **Install**. The **Installing Aspect Workforce™** window opens, showing the status of the installation. When the installation has completed successfully, the **Install Wizard Completed** window opens.
13. Click **Finish** and click **Exit** to close the wizard.

Installing from the Main Application Server

To install the Aspect Workforce™ client from the main application server, complete the following procedure:

To install the client:

1. Log in as an **administrator** on the workstation that will run the Aspect Workforce™ client software.
2. Using **Start > Run**, locate and double-click the following file, where ***MainAppServer*** is the machine name assigned to your main application server: ***MainAppServer*\WFMSetup\Workforce\Setup.exe**

   If any prerequisite software is not already installed on the server, then the Aspect Prerequisite Installer window opens, displaying a list of prerequisite but uninstalled software. Click **Install** to install the prerequisite software. When installation is complete, the **Welcome** window of the **Install Wizard For Workforce** opens, and the installer completes some preliminary tasks automatically.

3. Click **Next**. The **Destination Folders** window opens.

4. To accept the default (recommended) location for the program files, click **Next**. Otherwise, click **Change**, and browse to or type a different **path**, and click **OK**. The Data Folder window opens.
5. To accept the default (recommended) location for the data files, click **Next**. Otherwise, click **Change**, and browse to or type a different **path**, and click **OK**. The **Custom Setup** window opens.
6. Click the User Workstation **icon**, and select This Feature, And All Subfeatures, Will Be Installed On Local Hard Drive.
7. Click **Next**. The Main Application Server window opens.
8. Type the name of the **Aspect Workforce™ main application server**, and click **Next**. The DCOM Servers window opens.
9. In the **DCOM Servers** window, verify or type the **machine name** that is running each of the TallyServer, Updater, Checker, and ACD Processing Server services.

   The fields in this window are populated as follows:

- If the service has been added in the WFM Service Installer on the main application server or on a secondary application server, then the field displays the name of that server.
- If the service has not been added yet, then the field is blank. In this case, type the name of the server that will host this service.
- If the Tallyserver service has been added to multiple servers, then the drop-down list for the Tallyserver field displays the names of these servers. In this case, select the name of the Tallyserver host server that your workstation will access. If Tallyserver will be installed later on a server that is not displayed, then type the name of that server.

10. Click **Next**. The **Ready To Install** window opens.
11. Click **Install**. The **Installing Aspect Workforce™** window opens, showing the status of the installation. When the installation has completed successfully, the **Install Wizard Completed** window opens.
12. Click **Finish** to close the wizard.

Upgrading

To upgrade the client software for Aspect Workforce™, see Upgrading for SQL Server or Upgrading for Oracle.

Uninstalling

Uninstall the Aspect Workforce™ client by either:

- Using the Programs And Features feature in the Windows Control Panel
- Using the Aspect Workforce™ installation program

Uninstalling with Windows Control Panel

To uninstall with Windows Control Panel, use this path: **Start > Control Panel > Programs And Features > Workforce > Uninstall**

Uninstalling with the Installation Program

You can uninstall the Aspect Workforce™ client using the Aspect Workforce™ installation program on the main application server.

To uninstall the client with the installation program:

1. Log in as an administrator on the workstation where the Aspect Workforce™ client software is installed.
2. Using **Start > Run**, browse to and double-click the following file, where ***MainAppServer*** is the machine name assigned to your main application server:
   ***MainAppServer*\WFMSetup\Workforce\Setup.exe**

   The **Welcome** window of the **Install Wizard for Workforce** opens.
3. Click **Next**. The **Program Maintenance** window opens.
4. Select **Remove** and click **Next**. The **Remove The Program** window opens.
5. Click **Remove**. After Aspect Workforce™ has been uninstalled successfully, the **Install Wizard Completed** window is displayed.
6. Click **Finish** to exit the wizard.

Installing the Client on Windows Terminal Server

If you plan to access Aspect Workforce™ over a WAN, you must install the Aspect Workforce™ client on a computer configured with Windows Terminal Services (WTS). WTS for Aspect Workforce™ is a serverclass PC running Windows Server 2022 or 2025 with Terminal Services enabled. If you want to allow web access to WTS in addition to Remote Desktop Connection, Internet Information Services (IIS) must also be enabled, but web access to WTS is not required.

Microsoft also refers to Windows Terminal Services as Remote Desktop Services.

Note: The installation program automates several tasks that were formerly manual steps in prior releases of Aspect Workforce™. As you progress through the installation wizard, some of the processes might require several minutes to complete. This is normal and does not indicate any issues with your hardware, software, or the installer. When the installation is complete, a wizard screen confirms that the installation was successful.

Prerequisites

Before installing the Aspect Workforce™ client on a Windows Terminal Server, complete the following procedures or verify that they have been completed:

- You have administrator access to the terminal server.
- Your terminal server uses a supported operating system. Check the *Aspect Workforce™ Release Note* for this information.
- You check the release note for any new requirements or procedures.
- The database server and Aspect Workforce™ database have been configured. (It is not required that they be installed on the terminal server.)
- The database client is installed on the terminal server.
- For Oracle, see Installing the Client Software.
- For SQL Server, see Installing the SQL Server Client Software.
- Terminal server users and groups have been configured.

Note: For Oracle users, all terminal server users require Read access to the Oracle Home Directory to enable them to log in to Aspect Workforce™.

Installing the Client on the WTS Server

You install the Aspect Workforce™ client software on your WTS server in much the same way that you install it on a user workstation.

To install the Aspect Workforce™ client software on your Windows terminal server:

1. Log in as an administrator to the terminal server.
2. Browse to and launch the Aspect Workforce™ client setup program, Setup.exe, at one of the following locations:

- The main application server. The typical path is the following, where ***MainAppServer*** is the machine name of your main application server: ***MainAppServer*\WFMSetup\Workforce**
- The Aspect Workforce™ product CD.

  If any prerequisite software is not already installed on the server, then the Aspect Prerequisite Installer window opens, displaying a list of prerequisite but uninstalled software. Click **Install** to install the prerequisite software. When installation is complete, the Welcome window of the **Install Wizard for Workforce** opens, and the installer completes some preliminary tasks automatically.

3. Continue by referring to the steps provided in Installing from the Main Application Server, beginning with step 3.

Accessing the WTS Server

You can deploy a WTS server using a local client or a web browser.

Using a Local Client

Remote users can connect to the WTS server using a Terminal Server client installed on user workstations. You can retrieve this client software from the Microsoft Download Center using this link: ***http://www.microsoft.com/downloads/en/default.aspx***

Using a Web Browser

You can also enable Terminal Server access through a web browser. Please contact your Windows Terminal Server administrator for more information.

Installing the Client in a Citrix Environment

This chapter describes the tasks required to install the Aspect Workforce™ client program in a Citrix environment.

Overview

Citrix XenApp is an application delivery system that enables Windows applications to be virtualized, centralized, and managed in the datacenter. The applications can then be delivered as a service to users on a variety of devices. Check the *Aspect Workforce™ Release Note* to determine which version of Citrix XenApp is supported by Aspect Workforce™.

Integrating Aspect Workforce™ clients with Citrix consists of the following basic tasks:

1. Ensure that your deployment environment meets both the Citrix and Aspect requirements. See Requirements.
2. Run the Aspect Workforce™ installer on the XenApp Server and install the client workstation. The Aspect Workforce™ client is a standard Windows *rich client*. See Installing the Client Application.
3. Publish the Aspect Workforce™ client as an Application in the Citrix environment. See Publishing the Client as an Application in Citrix.

4. Install a Windows plug-in to enable users to access the published Aspect Workforce™ client Application. See Installing the Plug-In.

Requirements

This section lists required Citrix and Aspect requirements.

Citrix Requirements

The following software versions and updates are required to be installed in the server farm to use applications that use WPF technology.

Do not install XenApp on a domain controller. Citrix does not support installing XenApp on a domain controller.

Do not join servers running this XenApp version to a deployment with servers running previous XenApp versions (including early release and Technical Preview versions).

You must use the AppCenter from the 6.5 media to manage the XenApp 6.5 farm. Citrix does not support using a console from a previous XenApp release to manage XenApp 6.5 farms. (But you can use the AppCenter from the XenApp 6.5 media to manage a XenApp 6.0 farm.)

The Citrix solution is supported on all operating systems supported by Aspect Workforce™.

Aspect Requirements

The Aspect deployment environment has the following requirements:

You must create users in Active Directory or LDAP for the agents, supervisors, and administrators you want to be able to log in to client applications. These users must have roaming profiles. The actual rights that determine which applications these users can log into are determined in Citrix during the application publishing process.

There are no special requirements that apply to the Aspect Workforce™ servers, or to the Aspect Workforce™ installation process.

Installing the Client Application

Install the Aspect Workforce™ client on the Citrix Server by running the Aspect Workforce™ installation program on the XenApp server that will host the application.

To install the Aspect Workforce™ client on the Citrix Server:

1. Insert the **Aspect Workforce™ Software CD** in the CD drive of the Citrix XenApp server.
2. Follow the client installation procedure as described in Installing User Workstations. Ensure that the Aspect Workforce™ client application is installed in the Program Files folder on the Citrix machine.

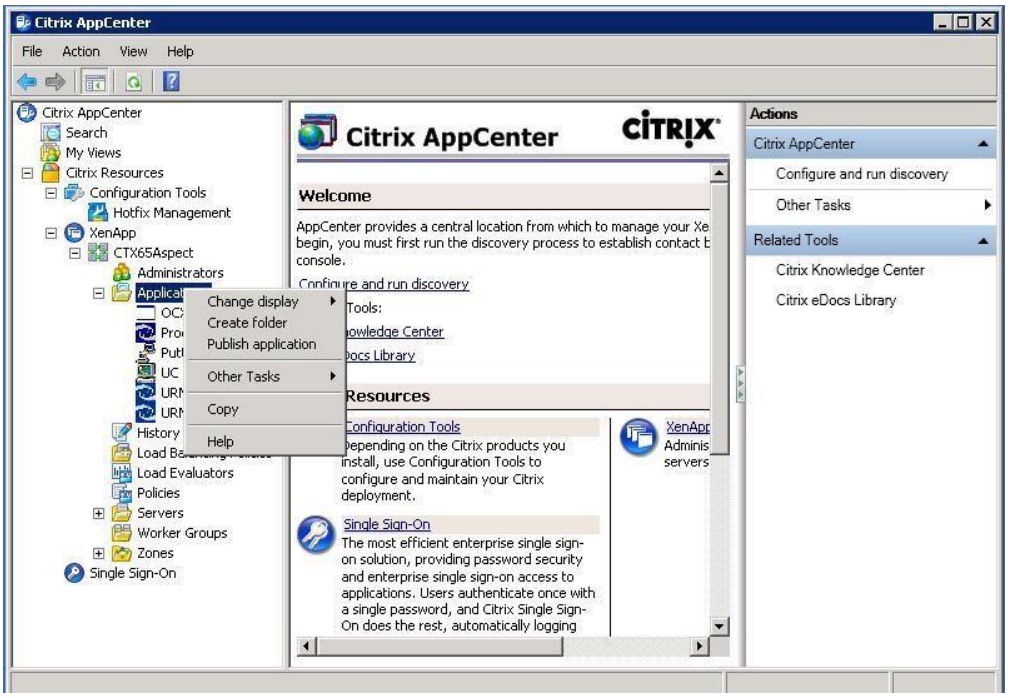
Publishing the Client as an Application in Citrix

Citrix provides two methods of publishing applications: publishing as Applications or as Web Content. The procedure in this section can be used to publish Windows clients, such as the Aspect Workforce™ client, as Applications.

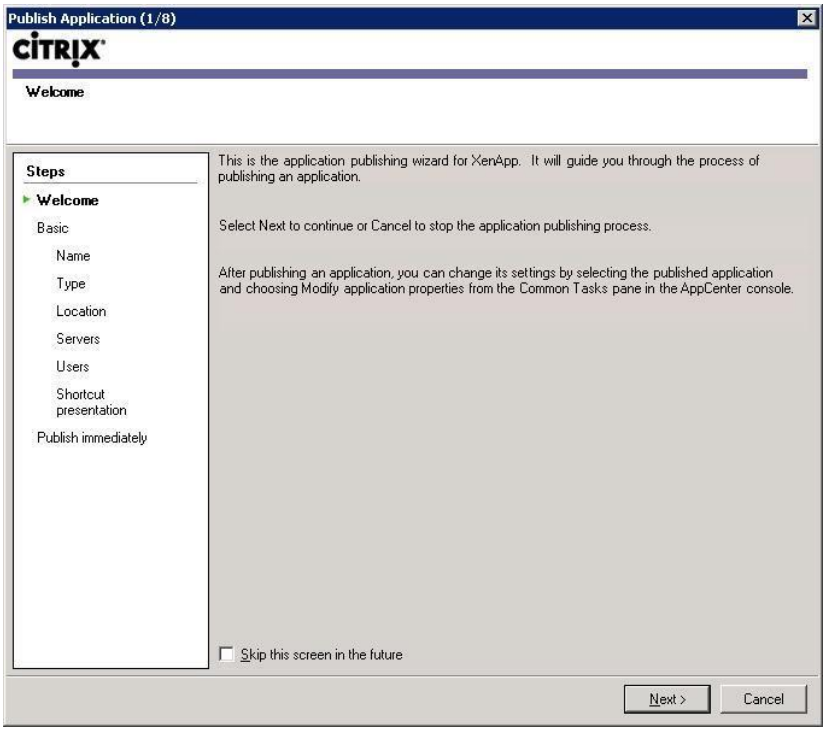
The following procedure is an example of one way you could publish an application. Your IT department may prefer a different method.

To publish the Aspect Workforce™ client as an application in Citrix:

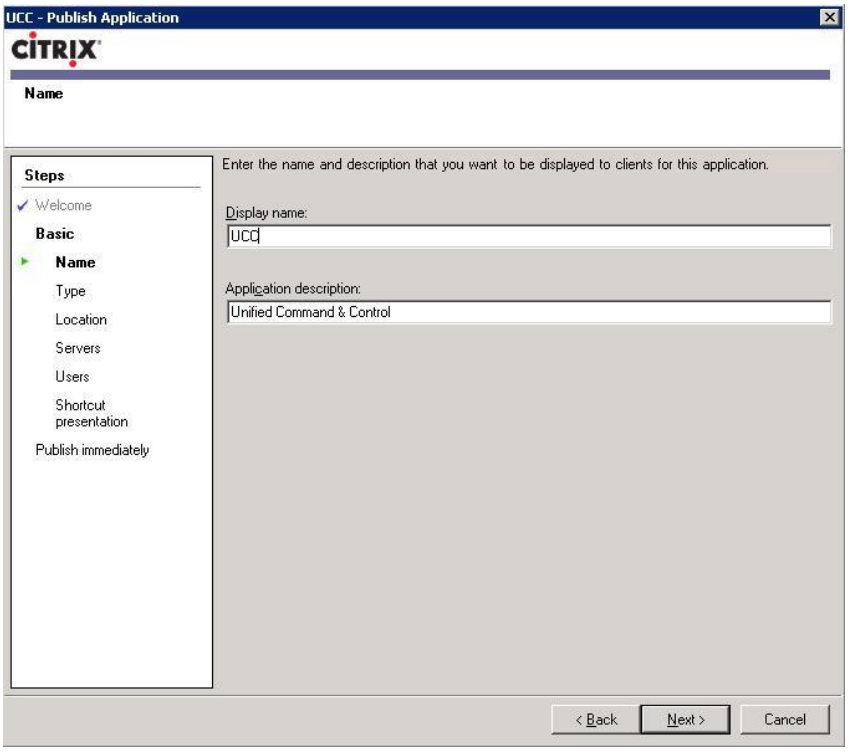
1. Log into the Citrix server, and launch the **Citrix AppCenter**.



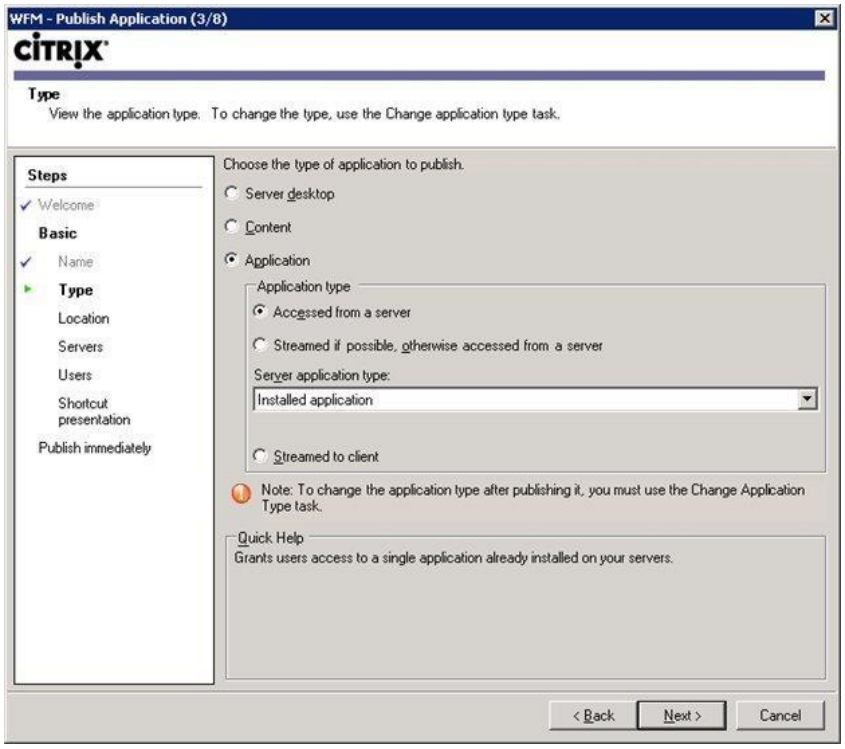
2. Expand **Citrix Resources** and expand **XenApp**.
3. Under **XenApp**, expand the name of your deployment farm, and right-click the **Application** folder.
4. In the shortcut menu, select **Publish Application**. The **Welcome** window opens.



5. Click **Next**. The **Name** window opens.



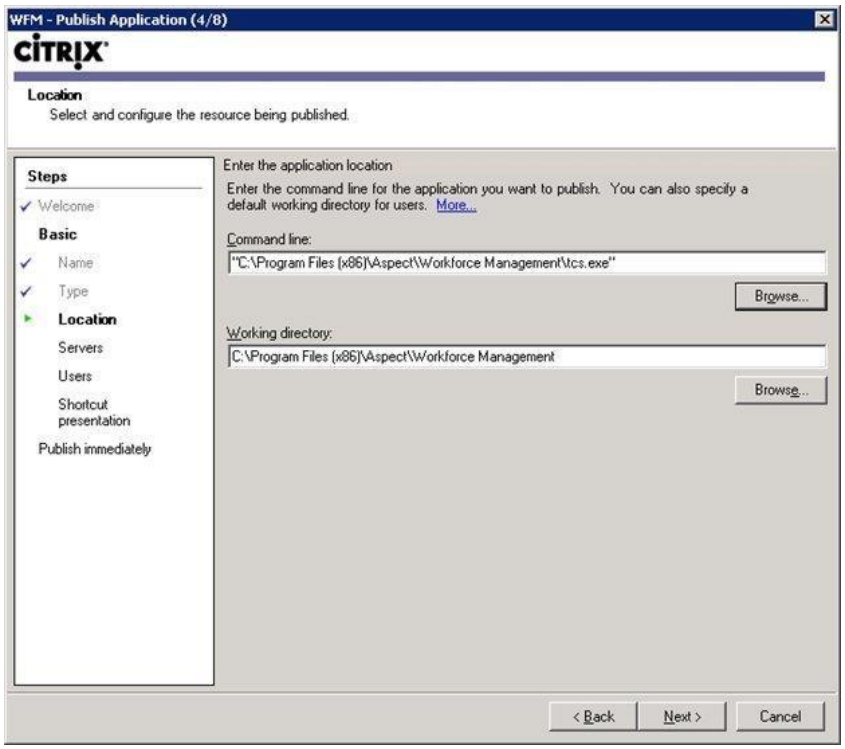
6. Type a **Display Name** and **Application Description** for the Aspect Workforce™ client application that you want to publish and click **Next**. The **Type** window opens.



7. On the **Type** window, make the following selections:
8. Select Application.
    a. Under Application Type, select Accessed From A Server.

b. From the Server Application Type drop-down list, select Installed Application.

9. Click **Next**. The **Location** window opens.



10. In the **Location** window, make the following entries:

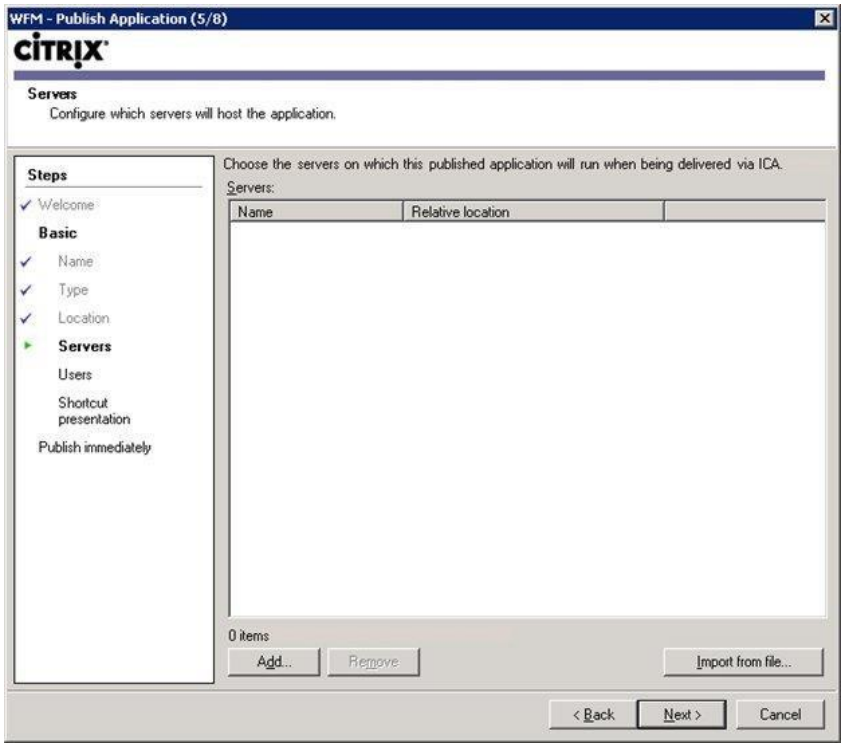
In the **Command Line** field, browse to the installed path of the Aspect Workforce™ client application that you want to publish. The default path is:

“C:\Program Files\Alvaria\Workforce\tcs.exe”

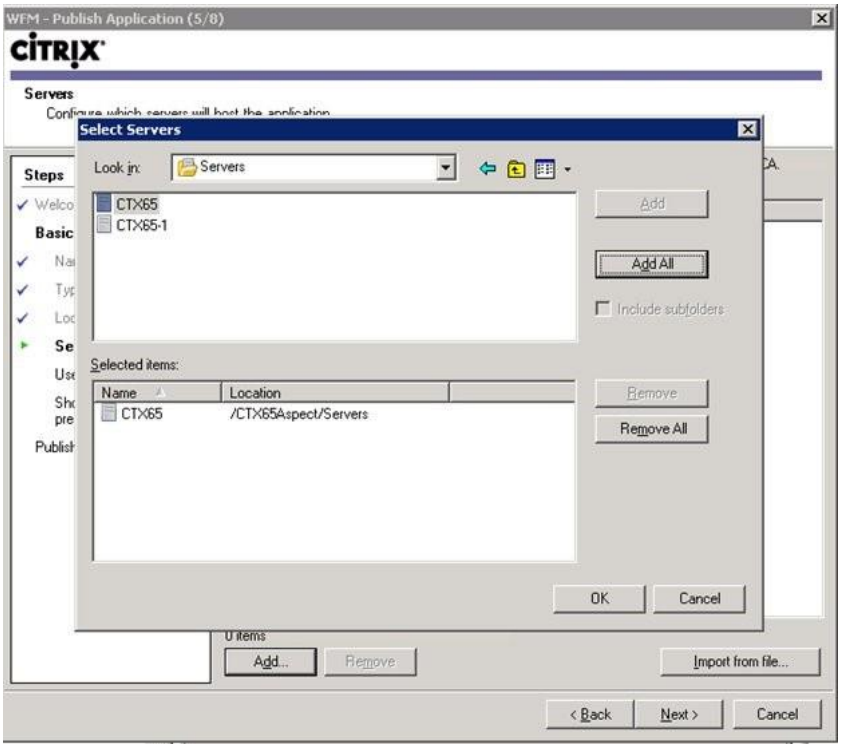
In the **Working Directory** field, browse to the folder you want to use as a working directory. By default, the default Working Directory is selected as follows:

C:\Program Files\Alvaria\Workforce

11. Click **Next**. The **Servers** window opens.



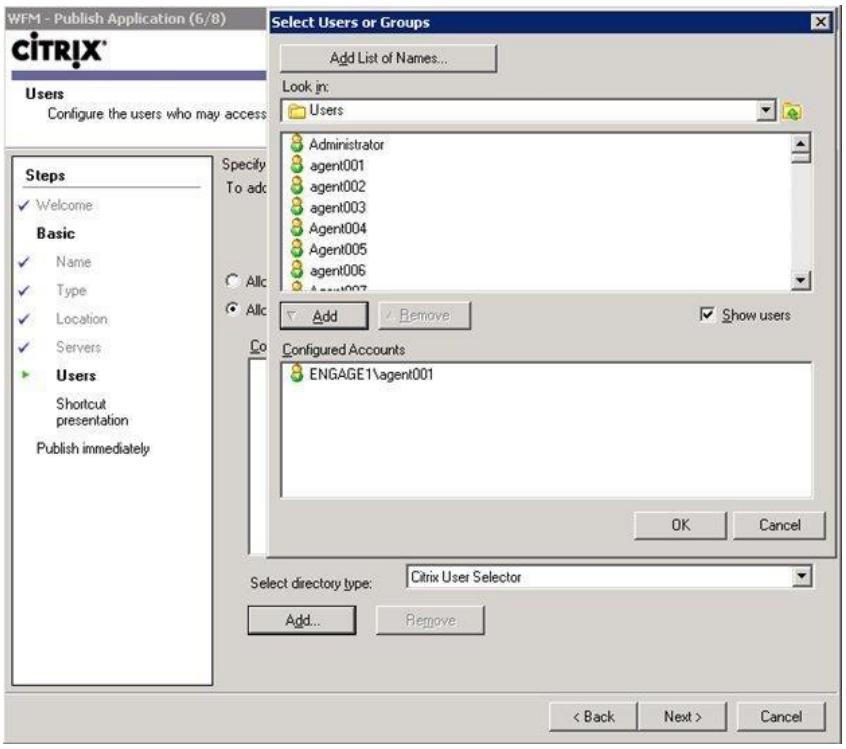
12. In the **Servers** window, click **Add**. The **Select Servers** window opens.



13. The **Look In** field displays the machine names of all Citrix servers that are available to run the installed client application. Select the **server** or servers you want to use and click **Add**. The selected server name is displayed in the **Selected Items** field.

14. Click **OK** to close the **Select Servers** window. The **Servers** window now displays the name of the selected Citrix server. Click **Next**. The **Users** window opens.

15. Select either **Allow Anonymous Users** or **Allow Only Configured Users**. If you select **Allow Only Configured Users**, select a directory type from the drop-down list, and click **Add.** The **Select Users or Groups** window opens.



16. Use this window to add users who will have access rights on the published application. To add the users, click the **Add List Of Names** button. The **Add List Of Names** window opens.

17. Do one of the following:

    a. To enter users individually:

        i. Enter the **users** one by one. You can add any number of users.

        ii. Click the **Check Names** button to determine the validity of the entered users.

        iii. When the validity is verified, click **OK**. The Select Users Or Groups window closes. b. To

    enter a group of users:

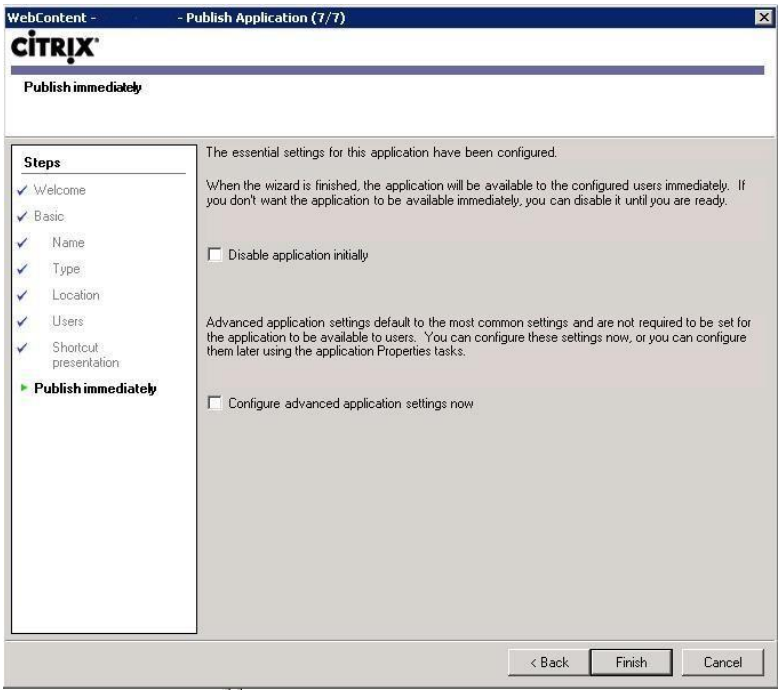
    i. In Active Directory, create a group that contains all the required users.

    ii. In the Add List Of Names window, click the **Select Users Or Groups** button. The Select Users Or Groups window opens.

    iii. Select the **Active Directory group** you just created, and click **Next**. The Select Users Or Groups window closes.

    iv. In the Users windows, click **Next**. The **Shortcut Presentation** window opens.

18. Configure the location and appearance of the client application shortcut and click **Next**. The **Publish Immediately** window opens.



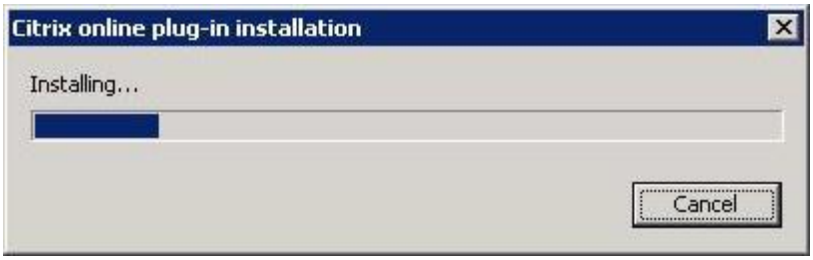
19. If you want to publish the client application immediately and use the preconfigured default settings, click **Finish**. You can now view the published Aspect Workforce™ client application under the Application node in the Citrix AppCenter.

Installing the Plug-In

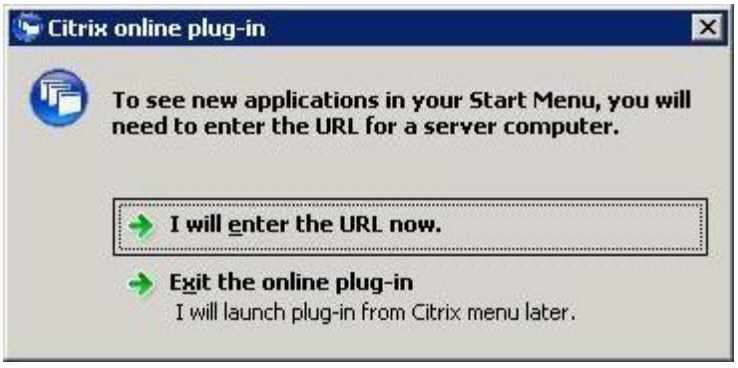
Before users can access published Applications such as the Aspect Workforce™ client, you must download a Windows plug-in and install it on your client machines.

To download the Windows plug-in:

1. Go to http://citrix.com/downloads, and download the **Windows Online Plug-in**.



2. Launch the **plug-in**.



3. Click **I Will Enter The URL Now**, and enter the name of the server that is hosting your published resources.

4. Click **Update**. The login window opens.

5. Enter your **credentials** and click **OK**.

6. After login is complete, right-click the **Online Plug-in** displayed on the taskbar to access the Aspect Workforce™ client application.

Installing with a Command Line

This chapter provides instructions for installing the Aspect Workforce™ program using a command line.

About Command Line Installation

Installing Aspect Workforce™ with the command line involves using an XML configuration file provided with the product. Before installing, you edit the XML configuration file to reflect your deployment environment. When you install with the command line, you bypass the Aspect Workforce™ installer and install the software directly.

By editing the variables in the XML configuration file, you can replicate any number of deployment configurations. For example, you can set up multiple configuration files, each representing the setup of a different server in the deployment. You can then use each configuration file to install Aspect Workforce™ on the computers in that specific environment.

Verifying Prerequisites

Before you install with the command line, verify that:

- You have administrator access to the designated machine.
- The server uses a supported operating system. Check the *Aspect Workforce™ Release Note* for this information.
- The database client is installed on the workstation:
- For Oracle, see Installing the Client Software.
- For SQL Server, see Installing the SQL Server Client Software.
- The appropriate third-party components are installed on the server. Check the *Aspect Workforce™ Release Note* for this information.

Installing Third-Party Components

If you plan to install Aspect Workforce™ using a command line, you must first install the Microsoft Visual Studio Redistributable Package, .NET 4.8, 32-bit SQLite ODBC driver, Crystal Reports, PerfmonIntegration, and SQLite.

Installing the Visual Studio Redistributable Package

Install the Microsoft Visual Studio Redistributable Package on all Aspect Workforce™ client machines.

You can access the package from the product CD at the following path, where ***x*** is the drive letter of the *Aspect Workforce™ Software* CD:

- ***x*:\WFM\Prereq**VSRuntime**\VS2017\vc_redist.x64.exe**
- ***x*:\WFM\Prereq**VSRuntime**\VS2017\vc_redist.x86.exe**

Installing .NET Framework 4.8

Install .NET by running the .NET Framework installer. There are two ways to access the installer:

- Run the .NET installer at the following path on the Aspect Workforce™ software CD, where ***x*** is the drive letter of the CD drive: ***x*:\WFM\Prereq\DotNet\ndp48-x86-x64-allos-enu.exe**
- If permitted by your Group Policy, download .NET Framework, including any service packs specified in the Release Note, from the Microsoft Download Center.

If the installation program displays a message stating that .NET Framework is already installed on your computer, no further action is required.

Installing SQLite Driver

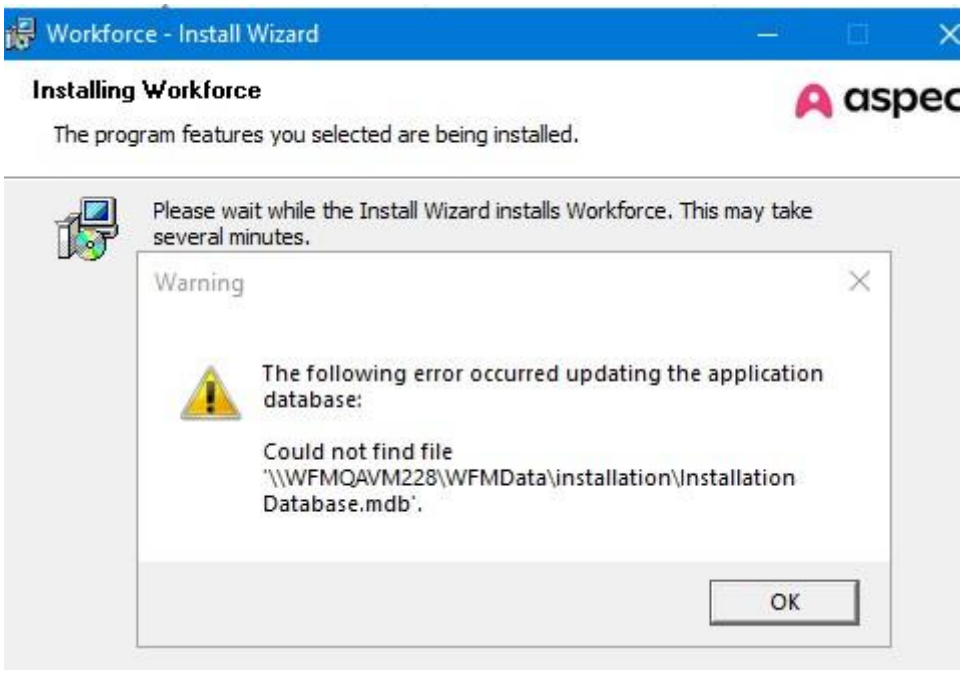
32-bit

Install SQLiteon all Aspect Workforce™ client machines.

You can access the package from the product CD at the following path, where ***x*** is the drive letter of the *Aspect Workforce™ Software* CD:

- *x*:\WFM\Prereq\AccessDatabaseEngine\AccessDatabaseEngine_x64.exe (need a new path for SQLite) (do I need a new section (like the Installing SQLite ODBCDriver for Win64, for SQLite ODBC Driver, 32-bit or is that what THIS is????)

Important Note: for Workforce 25 upgrades and new installations, the workstation will report a warning due to database changes related to the change from Microsoft Acess to SQLite.



This is an expected issue when running the installer interactively. The installation database is being converted from Access to SQLite and no real error is occuring. Customers can safely click the OK button to dismiss the dialogue.

Note: Microsoft Data Access Engine is no longer required. Aspect recommends that you uninstall the Microsoft Access Database Engine.

64-bit

Install the SQLite ODBC Driver for Win64 on all Aspect Workforce™ client machines. You can access the package from the product CD at the following path, where ***x*** is the drive letter of the *Aspect Workforce™ Software* CD:

- *x*:\WFM\Prereq\SQLite\sqliteodbc_w64.exe

Installing SAP Crystal Reports Runtime Engine for .NET Framework (x64)

Install the SAP Crystal Reports runtime engine for .NET Framework (x64) on all Aspect Workforce™ client machines.

You can access the package from the product CD at the following path, where ***x*** is the drive letter of the *Aspect Workforce™ Software* CD:

- *x*:\WFM\Prereq\CrystalReports\CRRuntime_64bit_13_0_38.msi

Installing Alvaria Performance Monitor Integration

Install the Alvaria Performance Monitor Integration on all Aspect Workforce™ client machines. You can access the package from the product CD at the following path, where ***x*** is the drive letter of the *Aspect Workforce™ Software* CD:

- *x*:\WFM\Prereq\PerfmonIntegration\PerfmonIntegration.msi

Installing an Application Server with a Command Line

The main and secondary Aspect Workforce™ application servers can be installed with a command line, using an XML configuration file provided with the product. In so doing, you bypass the Aspect Workforce™ installer and install the software directly. The Main Application Server must be installed before any Secondary Application Servers.

Editing the Configuration File

Before installing, edit the configuration file by inserting your own values for the parameters, such as the components to be installed and names of the DCOM servers. Comments in the configuration file provide additional information.

To edit the configuration file:

1. Browse to the following location on the Aspect Workforce™ product CD, where ***x*** is the drive letter of the CD: ***x*:\Utility\WFM_Config.xml**
2. Copy the **.xml file** to the local drive for editing.
3. Right-click the **.xml file**, select **Properties**, and remove the **Read-Only attribute**.
4. Open **Notepad** and drag the **.xml file** into Notepad.
5. Add your own **values** to the file based on your Aspect Workforce™ deployment and save the file.

Sample Application Server Configuration File

Following is a sample configuration file, showing values from an actual Aspect Workforce™ deployment substituted for the placeholder values.

```
<?xml version="1.0" encoding="utf-8"?>
<Install>
  <Options>
      <Features>
<!-- Values are Local or Absent.  All other values will be ignored and
install defaults used. -->            <MAS>Local</MAS>
            <SAS>Absent</SAS>
            <UW>Absent </UW>
            <LIS>Local</LIS>
            <AMR>Local</AMR>
            <WHC>Absent</WHC>
      </Features>
<!-- Enter the desired paths. If null install defaults used. -->
      <INSTALLDIR>D:\Applications\Aspect\Workforce</INSTALLDIR>
    <WFMDATA>D:\Applications\Aspect\Workforce\WFMData</WFMDATA>
<!-- Enter the servers names to be used for these values.  These values are
REQUIRED and if left empty installation errors will be occur unless using the
DISABLE_VALIDATION command line switch. -->
<DCOM_SRVR_INFO>COBRA01</DCOM_SRVR_INFO>
      <DCOM_SRVR_UPDATER>COBRA01</DCOM_SRVR_UPDATER>
      <DCOM_SRVR_ACDPROC>COBRA01</DCOM_SRVR_ACDPROC>
      <DCOM_SRVR_CHKR>COBRA02</DCOM_SRVR_CHKR>
      <DCOM_SRVR_TALLY>COBRA01</DCOM_SRVR_TALLY>
</Options>

</Install>
```

Results

The following results are produced when you use the command line installation with the sample configuration file shown in the previous section:

- Aspect Workforce™ Main Application Server (MAS) is installed on the Local machine
- Aspect Workforce™ Secondary Application Server (SAS) and User Workstation (UW) are not installed on the **Local** machine. (Note: MAS, SAS, AND UW can never be installed on the same machine)
- WFM Listen (LIS) is installed on the **Local** machine.
- Aspect Message Routing Service (AMR) is installed on the **Local** machine.
- WFM Historical Connectors feature (WHC) is not installed on the **Local** machine.
- Aspect Workforce™ installation files have been written to the **D:\Applications\Alvaria\Workforce** directory.
- Aspect Workforce™ data files will be written to the **D:\Applications\Alvaria\Workforce\WFMData** directory.
- Client is configured to access **COBRA01** (that is, the main application server) as the server hosting the WFM Information Server service.

- Client is configured to access **COBRA01** as the server hosting the WFM Updater service.
- Client is configured to access **COBRA01** as the server hosting the WFM ACD Processing services.
- Client is configured to access **COBRA02** as the server hosting the WFM Checker service.
- Client is configured to access **COBRA01** as the server hosting the WFM TallyServer service.

Using the Command Line

After editing the configuration file, install the Aspect Workforce™ client application server the command line.

Before running the command, open a command prompt with elevated privileges, using the **Run As Administrator** option.

Note: Type, rather than copy, the commands into a Notepad file before pasting them into the command window. The Windows installer sometimes misinterprets quotation marks that originate in a file type other than a plain text file, such as Notepad.

The format of the command line is as follows: msiexec /i "*CD Drive*:\WFM\wfm.msi" CONFIG_FILE="*Drive*:*Directory*\ WFM_Config.xml" /qb
where:

- ***CD Drive*** is the machine name of the Aspect Workforce™ main application server.
- ***Drive*** is the drive letter of the drive where your edited XML configuration file is stored.
- ***Directory*** is the folder or nested path containing your edited XML configuration file.

Installing a User Workstation with a Command Line

The Aspect Workforce™ client can be installed with a command line, using an XML configuration file provided with the product. In so doing, you bypass the Aspect Workforce™ installer and install the software directly.

Editing the Configuration File

Before installing, edit the configuration file by inserting your own values for the parameters, such as the names of the components to be installed and the DCOM servers. Comments in the configuration file provide additional information.

To edit the configuration file:

1. Browse to the following location on the Aspect Workforce™ product CD, where ***x*** is the drive letter of the CD: ***x***:\Utility\WFM_Config.xml
2. Copy the **.xml** file to the local drive for editing.
3. Right-click the **.xml file,** select **Properties**, and remove the **Read-Only attribute**.
4. Open **Notepad** and drag the **.xml file** into Notepad.
5. Add your own **values** to the file based on your Aspect Workforce™ deployment and save the file.

Sample User Workstation Configuration File

Following is a sample configuration file, showing values from an Aspect Workforce™ deployment substituted for the placeholder values.

```
<?xml version="1.0" encoding="utf-8"?>
<Install>
  <Options>
      <Features>
<!-- Values are Local or Absent.  All other values will be ignored and
install defaults used. -->             <MAS>Absent</MAS>
            <SAS>Absent</SAS>
            <UW>Local</UW>
            <LIS>Absent</LIS>
            <AMR>Absent</AMR>
            <WHC>Absent</WHC>
      </Features>
<!-- Enter the desired paths. If null install defaults used. -->
      <INSTALLDIR>D:\Applications\Alvaria\Workforce</INSTALLDIR>
    <WFMDATA>D:\Applications\Alvaria\Workforce\WFMData</WFMDATA>
<!-- Enter the servers names to be used for these values.  These values are
REQUIRED and if left empty installation errors will be occur unless using the
DISABLE_VALIDATION command line switch. -->
<DCOM_SRVR_INFO>COBRA01</DCOM_SRVR_INFO>
      <DCOM_SRVR_UPDATER>COBRA01</DCOM_SRVR_UPDATER>
      <DCOM_SRVR_ACDPROC>COBRA01</DCOM_SRVR_ACDPROC>
      <DCOM_SRVR_CHKR>COBRA02</DCOM_SRVR_CHKR>
      <DCOM_SRVR_TALLY>COBRA01</DCOM_SRVR_TALLY>
</Options>

</Install>
```

Results

The following results are produced when you use the command line installation with the sample configuration file shown in the previous section:

- Aspect Workforce™ User Workstation (UW) is installed on the Local machine.
- Aspect Workforce™ installation files have been written to the D:\Applications\Alvaria\Workforce directory
- Aspect Workforce™ data files will be written to the D:\Applications\Alvaria\Workforce\WFMData directory
- Client is configured to access COBRA01 (that is, the main application server) as the server hosting the WFM Information Server service
- Client is configured to access COBRA01 as the server hosting the WFM Updater service
- Client is configured to access COBRA01 as the server hosting the WFM ACD Processing services
- Client is configured to access COBRA02 as the server hosting the WFM Checker service
- Client is configured to access COBRA01 as the server hosting the WFM TallyServer service

Using the Command Line

After editing the configuration file, install the Aspect Workforce™ client using the command line. The format of the command line depends on whether the main application server has already been installed.

Before running either command, open a command prompt with elevated privileges, using the **Run As Administrator** option.

Note: Type rather than copy, the commands into a Notepad file before pasting them into the command window. The Windows installer sometimes misinterprets quotation marks that originate in a file type other than a plain text file, such as Notepad.

If Main Application Server is Installed

If the main application server has already been installed, the format of the command line is as follows:

msiexec /i "*MainAppServer*\WFMSetup\Workforce Management\Install\wfm.msi" CONFIG_FILE="*Drive*:*Directory*\WFM_Config.xml" /qb where:

- **MainAppServer** is the machine name of the Aspect Workforce™ main application server.
- **Drive** is the drive letter of the drive where your edited XML configuration file is stored.
- **Directory** is the folder or nested path containing your edited XML configuration file.

If Main Application Server is Not Installed

If the main application server has not yet been installed, the format of the command line is as follows:

msiexec /i "*CD Drive*:\WFM\wfm.msi" CONFIG_FILE="*Drive*:*Directory*\WFM_Config.xml" DISABLE_VALIDATION=1 /qb where:

- **CD Drive** is the drive letter of the CD drive with the Aspect Workforce™ software CD inserted.
- **Drive** is the drive letter of the drive where your edited XML configuration file is stored.
- Directory is the folder containing your edited XML configuration file You must always use the **DISABLE_VALIDATION** command line switch.

Post-Installation Administrative Tasks

This chapter provides information about administrative tasks to complete after you install Aspect Workforce™ or upgrade to it from an earlier version.

For more information about administrating Aspect Workforce™, see the *Aspect Workforce™ System Administrator Guide.*

Note: When performing these post-installation tasks, always log in to the server as a member of the local Administrators group.

Importing the License File

Note: This section applies to new installations only and not to upgrades.

License files specify the maximum number of agents you are licensed for in your Aspect Workforce™ system. Licenses can be of either of two types:

- **Maximum number of *Active Employees*.** These are employees designated as Active in the Employee Records module of Aspect Workforce™. An Active employee is one who is currently part of your working staff. This type of license is the more common license.
- **Maximum number of *Concurrent Employees*.** Concurrent employees are those who have a schedule at a given moment.

Import your license file from the *Aspect Workforce™ – License File CD,* provided in the product package, or from a location on the network where the license file has been saved.

You import, export, and manage your license file from within the Aspect Workforce™ user interface. For import instructions, see below. For information about importing, exporting, and managing your license and license file, see the *Aspect Workforce™ online Help*.

About the License File CD

The *Aspect Workforce™ – License File CD* may contain more than one license file if you have a multitenant installation. Use these guidelines when importing license files:

- If the CD contains only one license file, then import it into each Aspect Workforce™ database you are using.
- If the CD contains more than one license file, determine the correct one to import by referring to the license file format, ***xxxx.yyyy***, where:
- ***ex*** is a number that identifies your company's unique Aspect Workforce™ system ID
- ***yyyy*** is the number of licenses for a specific database.

Before Importing a License File

Before importing a license file, ensure that:

- Aspect Workforce™ server software for the main application server is installed and configured.

  For instructions, see Installing the Main Application Server for Oracle or Installing the Main Application Server for SQL Server, depending on your RDBMS.
- Aspect Workforce™ client software is installed on the machine you are using to import the license file.

  For instructions, see Installing User Workstations.

To Import a License File

To import a license file:

1. Launch **Aspect Workforce™**. The Login dialog box opens.
2. In the drop-down list for the Database field, select the **database** for which you want to import a license file.
3. Type a **User Name** and **Password** for an administrator account and click **OK.**
4. If you are logging in with Windows Integrated Security, the Windows account must also be an Aspect Workforce™ administrator account.
5. On the main menu, select Help > About. The About Aspect Workforce™ window opens.
6. On the General page, click **License.** The **License Info** window opens.
7. Click Import.

8. Browse to the **Aspect Workforce™ – License File CD and** double-click the **file** with the .LIC extension.

   A message box opens, stating that your license information was updated, and details of your imported license file appear in the License Info dialog box. For more information about the names and values shown, see the *Aspect Workforce™ Online Help.*

9. Click **OK** to close the update message window, click **OK** to close the License Info window, and click **OK** to close the About window.

10. To import a license file for another database, select **File > Log In As Other User** on the main menu, and go back to step 2.

Restricting User Access to Shared Folders

Installing the main application server software creates several shared folders. These shared folders are used when installing the secondary application server and client software from the main application server, for storing installation data, and for running reports. The table below describes these shared folders.

Shared Folder	Default Path on Application Server	Description
WFMData	C:\ProgramData\Aspect\ Workforce\ WFMData	Stores the Installation subfolder with the installation database, the Reports subfolder with report formats, and input and output subfolders for ACD data.
WFMSetup	C:\Program Files\Alvaria\ Workforce\WFMSetup	Stores Installation files for secondary application servers and user workstations. Also contains subfolders used by Aspect Workforce™ modules.

The installation program sets share permissions for WFMData as follows:

- **Local Admin Group** —Change and Read
- **Local Users group** —Change and Read

The installation program sets share permissions for WFMSetup as follows:

- **Local Admin Group** — Change and Read
- **Local Users group** —Read

Note: During upgrades, the installation program configures these same permissions. These settings place the machine at only marginal risk of infection by certain viruses.

Note: Aspect Workforce™ administrators who perform any of the following actions require Change access to *both* folders:

- Adding or deleting application servers
- Modifying or installing Aspect Workforce™ system services
- Installing Aspect Workforce™ enhancement packages (for example, Empower or Perform.)

Excluding Shared Folders from Anti-Virus Scanning

Shared folders allow Aspect Workforce™ clients, as well as services running on other machines, access to installation points and configuration information.

In certain cases, anti-virus scanning of WFMData subfolders interferes with the services that access this folder to read and write ACD information. To prevent this, you should exclude the following files in the WFMData subfolders from anti-virus scanning:

- *.ITF
- TC*.*
- , ACD0x.nnn
- *.DAT

Stopping and Starting System Services

Depending on the needs of your organization, it might be necessary to stop Aspect Workforce™ system services on the main or secondary server from time to time. While there is little risk of damage to your database, shutting down the system services improperly can cause the loss of data associated with inprogress activities. In addition to performing regular backups to safeguard your database, use the instructions in this section to protect your in-progress activity data when stopping and starting Aspect Workforce™ system services.

Stopping System Services

The most important step in shutting down your application server system services is terminating all user connections to the database. You can physically ask each user to finish up and log out and you can force users to log out from within Aspect Workforce™. Either method ensures that all in-progress operations are completed and the associated data is safely stored in your database.

After all users log out of the database, follow standard Windows procedures for stopping a system service. Except for Tally Server and Information Server, the order in which the services are stopped is not important. Because Tally Server and Information Server can restart without intervention if queried by one of the other services, stop these two services last. To do this, stop the Tally Server, then stop the Information Server.

Note: The WFM Listen service is a critical component of your ACD interface and should not be stopped for routine reasons. Stopping this service can cause a loss of ACD data. If you are stopping your Aspect Workforce™ system services to perform routine database maintenance (including backups), do not stop the Listen service.

After making sure all users are logged out and stopping system services, you should lock the database to prevent anyone from logging in. For Oracle users, this means enabling a restricted session. For SQL Server users, this means restricting database access to the database owner.

Starting System Services

To start your Aspect Workforce™ system services after a routine shutdown, make sure your database server software is running and that the database is not locked. For Oracle users, this means ensuring that a restricted session is not enabled. For SQL Server users, this means removing previous restrictions.

After you have made sure that your database is available, follow standard Windows procedures to start the system services. Note that all services are also configured to start automatically upon restart.

Running WFM Services with Non-Administrative Accounts

None of the WFM services require administrator permissions for user accounts. So if you want to increase security on application servers where your services are running, you can create non-administrative accounts for one or more services and configure each service to log on as that non-administrative account.

By default, all WFM services are configured to run with the Local System account, which is an administrator account. The account configuration occurs when services are installed automatically during the installation of Aspect Workforce™, or when they are installed manually using the WFM Service Installer.

Contact Aspect Customer Care for assistance before configuring a service to log on as a regular user. In most cases, additional configuration is required that is specific to each service.

Configuring a Service to Log On As A Regular User

To run a service as a non-administrative account, use Windows Services Microsoft Management Console (MMC) to change the Local System account to a regular user account. The user account can be a local account on the server or a domain account.

To configure a service to log on as user:

1. Do the following:
   - Windows Server 2022 or 2025: Select **Start > Windows Administrative Tools > Services**.

   The Services (MMC) window opens.
2. In the list of services, select and stop the **service** using the shortcut menu.
3. Double-click the **service**. The **Properties** dialog box for the service opens.
4. Click the **Log On** tab.
5. Under **Log On As**, select the radio button for **This Account**.
6. Use the **Browse** button to select the account to use for this service, and type and confirm the **password**.

   If necessary, use the Windows Server Manager to create a new local user account, or create a new domain user account.

7. Click **OK**.
8. In the list of services, select and start the **service**.

Note: Repeat this procedure whenever you make changes to a service (such as changing a parameter value) using the WFM Service Installer.

About Additional Configuration Tasks

In most cases, if you configure a service to run with a non-administrative account, you must complete additional configuration steps to enable the service to run properly. For example, if you configure the WFM Tally Server service to log in a a regular user, some configuration changes might be required to grant that user permission to launch the service's database accessor.

Contact Aspect Customer Care for assistance in completing the additional configuration tasks.

Verifying Your Installation

To verify your installation of Aspect Workforce™, run the tests in this section.

Prerequisites

Before verifying your installation, make sure the following conditions are met:

- The WFM Sample database is installed.
- The WFM Updater and WFM TallyServer services are installed for the WFM Sample database (named TCS_SAMPLE), and these services are started.

Logging In

Before verifying that the key features of Aspect Workforce™ are working, log in to the software.

To log in:

1. Launch **Aspect Workforce™** by selecting **Start > Aspect > Workforce**. (This path may vary slightly, depending on your operating system.)
2. In the Database field, use the drop-down list to select the sample database, **TCS_SAMPLE**, which is the database you will use for the verification tests.
3. Type your **User Name** and **Password**, and click **OK**. The main window opens.
4. From the main menu, select **Tools > Options.**
5. In the Options window, click the **Advanced** tab, and ensure that the **Refresh On Save** check box is selected.
6. Click **OK**.

Verifying the Forecasting Feature

Verify that the forecasting feature is working. To do this, use the Forecasting Wizard to run a staffing forecast. Simply accept the default settings, and view the resulting report.

To verify the forecasting feature:

1. In Aspect Workforce™, click the **Forecasting** navigation button. The Forecasting modules tree opens.
2. Click **Forecasting Wizard.**
3. In the Forecasting Wizard view, click **Open.** The Forecasting Wizard opens.
4. Proceed through the wizard to configure a forecast. To do this, make the following selections, and click **Next** after completing each page:

- Select the **Staffing** radio button.
- Use the Routing Set lookup button to select the **CSV** routing set.
- Leave the preselected default information for the **CSV** forecast group.
- Leave the preselected default information for the **CSV** staff group.
- Leave the default **From** and **To** dates of the forecast, making sure that the From date is a Sunday.
- Leave the default value for the **run name.**
- Leave the default values for the **Time Zone** and **FTE Definition.**

5. Click **Finish** to create a forecast. When the forecast is complete, the Print Options dialog box opens.
6. On the General page, make sure the **Preview** radio button is selected, and click **OK** to preview the forecast. An Intra-Day Staffing Forecast report opens.
7. Verify that the first page of the forecast report contains at least a few non-zero values. If so, the Forecasting feature is working.

Verifying the Scheduling Feature

Verify that the scheduling feature is working.

To verify the scheduling feature:

1. In Aspect Workforce™, click the **Scheduling** navigation button. The Scheduling modules tree opens.
2. Click **Scheduling Wizard.**
3. In the Scheduling Wizard view, click **Open.** The Scheduling Wizard opens.
4. Proceed through the wizard to configure a scheduling run. To do this, make the following selections, and click **Next** after completing each page:

- Select the **Template-based** radio button.
- In the Name field, type **TEST**, and in the Description field, type **Test Schedules.**
- Click the Forecast Run lookup button, and select the staffing forecast you created when verifying the forecasting feature. (For instructions, see Verifying the Forecasting Feature.)

  Find this forecast by scrolling through the forecast runs in the form until you find it.
- Leave the default **From** and **To** dates of the scheduling run.
- Leave the default values for **Rule Set** and **Minimum Interbreak Interval.**
- Leave the default values for **Name** and **Description** of the schedule set.
- Leave the default values on the staff groups page.

5. Click **Finish** to generate schedules. When the schedule run is complete, the Print Options dialog box opens.

6. On the General page, make sure the **Preview** radio button is selected, and click **OK** to preview the schedule run. A Template-Based Schedule Run report opens.
7. Verify that the schedule run report contains schedules. If so, the Scheduling feature is working.

Verifying the Tracking Feature

Two tests are needed to verify that the tracking feature is working. Specifically, these tests validate that the WFM Updater and WFM TallyServer services are working.

Saving an Official Segment

Save an official segment to help verify that the tracking feature is working. Specifically, this test validates that the Updater service is working.

To save an official segment:

1. In Aspect Workforce™, click the **Tracking** navigation button. The Tracking modules tree opens.
2. Click **Official Schedule Editor.** The Official Schedule Editor view opens.
3. Use the **Single Employee** lookup button to select any sample employee and click **Open**. (Do not change the default value in the Nominal Date field.) The Official Schedule Editor window opens.
4. Right-click anywhere in the window and select **Add** from the shortcut menu.
5. On the **Segment** page, in the **Type** section, select the **Detail** radio button.
6. Use the Code lookup button to select the **SHIFT** segment code and click **OK**. The segment information appears on the calendar in bold text.
7. Click the **Save** toolbar icon to save the new segment.

   If the segment information now appears in plain text instead of bold text, then the segment was saved successfully. You have now validated that the Updater service is working.

Creating an Intra-Day Performance Report

Create and intra-day performance report to help verify that the tracking feature is working. Specifically, this test validates that the TallyServer service is working.

To save an official segment:

1. In Aspect Workforce™, click the **Tracking** navigation button. The Tracking modules tree opens.
2. In the tree, click **Intra-Day Performance.** The Intra-Day Performance view opens.
3. Right-click in the view and select **Add** from the shortcut menu. The Create Intra-Day Performance dialog box appears.
4. Complete the fields on the General page as follows:

- Use the **Routing Set** lookup button to select the **CSV** routing set.
- In the **From** and **To** fields (for Date Range), use the down arrow button to select the **current date** from the calendar for both fields.
- In the **Start** and **Stop** fields (for Time Range), leave the default values.

  Leave the default values on the other pages on this dialog box.

5. Click **OK** to create the intra-day performance forecast.
6. In the Intra-Day Performance view, find the intra-day performance forecast that you just created. If you find the forecast, you have validated that the TallyServer service is working.

   If you don't see the forecast, expand the routing set types (Multiskill:No and Multiskill:Yes), identify your routing set, and find your forecast.

Verifying Database Connectivity

To verify connectivity between Aspect Workforce™ and your Oracle or SQL Server database:

1. Launch Aspect Workforce™ by selecting **Start > Aspect > Workforce.** (This path may vary slightly, depending on your operating system.) The **Login** dialog box opens.
2. In the **Database** field, use the drop-down list to select your **database**.
3. Type the user name and password for the Aspect Workforce™ administrator account (which by default is **TCSADMIN**/**qqq**).
4. Click **OK**. If Aspect Workforce™ cannot connect to Oracle or SQL Server, an error message appears. Otherwise, the Aspect Workforce™ client interface opens.

Verifying ACD Connectivity

To verify that your installation of Aspect Workforce™ is connected to your ACD interface, run the tests in this section.

Prerequisites

Before verifying your ACD connectivity, make sure the following conditions are met:

- The ACD vendor is shipping the report to the agreed location.
- Contact and Agent data groups are correctly defined in Aspect Workforce™.

The following ACD processing services are started. These are Windows services and can be set to automatic.

- WFM Listen
- WFM Parser
- WFM ACD Proc

Verifying ACD Connectivity

Verify that the ACD data processing is functional.

To verify ACD data processing:

1. Launch **Aspect Workforce™** by selecting **Start > Aspect > Workforce**. (This path may vary slightly, depending on your operating system.)
2. In the **Database** field, use the drop-down list to select the **production database**. The production database is usually named **WFM**
3. Type your **User Name** and **Password** and click **OK**. The main window opens.

4. Click the **Forecasting** navigation button. The Forecasting modules tree opens.
5. In the tree, click **Actual Data.** The Actual Data view opens.
6. In the view, do the following:

- Click the **Contact Group Data** radio button.
- Use the **Data Group** lookup button to select a data group.
- In the **Date** field, use the down arrow button to select the **current date** from the calendar.

7. Click **Open.** The Contact Statistics dialog box opens.
8. Scroll through the time periods to verify that call statistics appear.

Relevant columns to check are NCO (Number of Calls Offered) and AHT (Average Handle Time). If you see call statistics in these columns, then ACD call statistics are populating your database. You have now verified that your installation of Aspect Workforce™ is connected to your ACD interface.

Verifying Security Profiles

To verify that security profiles were preserved during an upgrade:

1. Open the **Security Profiles** module. The list of defined security profiles appears on the right.
2. Select a **profile** from the list.
3. Verify that the **settings** are correct.

Upgrading for SQL Server

This chapter provides information for SQL Server users who are upgrading from version 21.0 or later to this version of Aspect Workforce™.

Note: Although you cannot directly upgrade the Aspect Workforce™ *software* from version 21.1 to 24, you can use a procedure in this chapter to directly upgrade the *database schema* from version 21.1 to 24.

For compatibility information regarding SQL Server release levels, see the *Release Note* (Compatible Database Platforms section). For more information about installing and configuring SQL Server for this release, see Configuring SQL Server.

The installation program automates several tasks that were formerly manual steps in prior releases of Aspect Workforce™. As you progress through the installation wizard, some of the processes might require several minutes to complete. This is normal and does not indicate any issues with your hardware, software, or the installer. When the installation is complete, a wizard screen confirms that the installation was successful.

Pre-Upgrade Tasks

Before upgrading Aspect Workforce™, ensure that you have met all pre-installation requirements listed in Pre-installation Overview and Initial Verification.

Then complete the following tasks. All tasks are described later in the chapter.

1. Run the Aspect Workforce™ Upgrade Compatibility Verification Tool.
2. Upgrade your Aspect Workforce™ database to SQL Server 2022.

Note: For compatibility information regarding RDMBS release levels, see the *Aspect Workforce™ Release Note* (Compatible Database Platforms section).

Running the Verification Tool

Run the verification tool to resolve conflicts in your database.

About the Verification Tool

The Aspect Workforce™ Upgrade Compatibility Verification Tool pinpoints database conflicts, called *violations* or *duplicates*. Once the tool has pinpointed these conflicts, you resolve them by logging in to Aspect Workforce™ and making the necessary changes to the data, or by contacting Aspect Customer Care for assistance.

Running the Verification Tool

One or two weeks before upgrading, run the Aspect Workforce™ Upgrade Compatibility Verification Tool (provided on the product CD) to identify and resolve any conflicts that may exist in your database.

You will also run the tool as part of the normal upgrade procedures described in this chapter. But we recommend that you do a preliminary run before upgrading, since the conflict resolution process can potentially be time-consuming, especially with a large database. In this way, your upgrade progress will not be impeded and will likely proceed more quickly and smoothly.

Run the Aspect Workforce™ Upgrade Compatibility Verification Tool on all databases that you plan to upgrade.

To run the Verification Tool:

1. Insert the **Aspect Workforce™ Software CD** in the CD drive of the main application server, and browse to the file ***x:*\Utility\DbVer.exe**, where ***x*** is the drive letter of the CD drive.
2. Copy the **DbVer.exe** file to a folder on the main application server and open the **file** from this folder. The main window of the **Aspect Workforce™ Upgrade Compatibility Verification** dialog box opens.
3. Under Select RDBMS Type, select your *current* SQL version as the database platform type.
4. Complete the fields as follows:

- **Server Name**: Host name of the SQL Server machine.
- **Database Name**: Name of the Aspect Workforce™ database. The Database Name is case-sensitive and must match exactly the database name as it appears in SQL Server.

  For instructions on finding the name of your SQL Server machine and Aspect Workforce™ database, see Configuring an Existing or Sample Database.

5. Click **Connect**. The **Database Login** dialog box opens.
6. Type the **User Name** and **Password** for the owner of the database and click **OK**.

   Typically, this User Name is **TCSDBOWNER**.
   After the tool connects to the database, the main window opens.
7. Click **OK** to begin verification. After the tool searches the database, it displays one of the following results:

- If violations were found, the tool displays details of the violations in the main window. Go to Navigate to the log file, .

- If no violations were found, the tool displays this message in the main window: No Violations Found. In this case, you do not need to take any further action. Click **Close** to exit the tool.

8. Navigate to the log file, **23UpgCompat.log**, to view and print the details.

   The log file is stored in the following location on the machine that you are running the tool from (not on the machine where the database is stored):
   C:\ProgramData\Aspect\Workforce Management\log
   To view the file, open Notepad, and drag the **23UpgCompat.log** file into the Notepad window.

9. Log in to your current version of **Aspect Workforce™ and** resolve the **violations** by modifying the data identified in the 23UpgCompat.log file.

   You might need an experienced Aspect Workforce™ user, or Aspect Customer Care representative to complete this step. For guidelines on modifying the data, see Resolving Database Conflicts.

10. Re-run the tool, resolving violations each time from step 8 and step 9 until no violations are found.

Resolving Database Conflicts

The following table shows typical database conflicts and suggestions for resolving them in Aspect Workforce™.

- It is assumed that the names shown for each example refer to different people, rather than being duplicate entries for the same person.
- There are other possible resolutions in addition to the ones shown. The important thing is that each item in the database be unique.

Typical Conflicts and Resolutions

Conflict	Cause	Resolution	Solution
John Williams conflicts with: JOHN WILLIAMS	Using case as a differentiator.	John A. Williams does not conflict with: John E. Williams	Include middle initial.
Allen Jackson conflicts with: Allen Jackson	Using leading spaces as a differentiator.	Allen Jackson does not conflict with: Allen_Jackson	Substitute underscore for leading spaces.

Upgrading to SQL Server 2022

If you were using a previous version of SQL Server, upgrade SQL Server by running the SQL Server 2022 installation program. None of the steps in the upgrade process require special configuration for Aspect Workforce™.

For installation instructions, see Installing SQL Server Management Studio.

To determine the version of SQL Server that you are currently running, log in to SQL Server Management Studio and execute the following query:

```
SELECT @@VERSION
```

The Planning page of the installation wizard provides tools and information, such as the Upgrade Advisor, for performing a successful upgrade.

When upgrading SQL Server, refer to the documentation provided with the SQL Server product for upgrading SQL Server instances.

Upgrade Overview

The following list shows the tasks required to upgrade Aspect Workforce™ and the correct sequence of those tasks. When performing these upgrade tasks, always log in to the server with a domain account that is also a member of the local Administrators group.

1. Re-running the Verification Tool
2. Restricting Your Database
3. Backing Up Your Database
4. Stopping the WFM Services
5. Uninstalling the Microsoft Access Database Engine (optional)
6. Upgrading the Main Application Server
7. Upgrading the Database
8. Persisting Database Roles
9. If you are installing AMR on the main application server for the first time during the upgrade, you must complete additional upgrade tasks in the Aspect Message Routing Platform Configuration Editor. For more information, see Configuring the Aspect Message Routing Service.
10. Upgrading a Secondary Application Server
11. Upgrading User Workstations
12. Upgrading the Sample Database
13. Removing Database Restrictions

Upgrade Procedures

This section provides procedures for the tasks outlined in the upgrade overview. Complete these tasks in the order shown.

Re-running the Verification Tool

Even if you have run the Aspect Workforce™ Upgrade Compatibility Verification Tool previously to identify and resolve any conflicts in your database, run the tool again in case a few conflicts have emerged while you used Aspect Workforce™ in the intervening time. Running the tool should be much quicker now.

For instructions, see Running the Verification Tool.

Restricting Your Database

Verify that no users other than the database owner can connect to the database while the upgrade process is in progress.

To restrict your database:

1. In **SQL Server Management Studio**, log in to your database as a **system administrator**.
2. Right-click your **database and** select **Properties**. The **Properties** dialog box opens.
3. On the left, select the **Options** page. The **Options** page opens.
4. In the **State** section**,** for the **Restrict Access** option, select **RESTRICTED_USER** from the drop-down list, and click **OK**. The **Open Connections** dialog box opens.
5. Click **Yes** to close all other connections to the database.
6. Exit **SQL Server Management Studio.**

Backing Up Your Database

Always back up of your database before installing an upgrade.

Caution: An upgrade can change the internal structure of your database. If a hardware or software failure were to occur during this process, you could lose your data. Your SQL Server database administrator can help you with the backup process of exporting *.MDF and *.LDF files for your Aspect Workforce™ database.

Stopping the WFM Services

Note: If you are using Distributed Checker, contact Aspect Customer Care for guidance on stopping the Checker service.

To shut down Aspect Workforce™ services:

1. Verify that all **users** are logged out.

   You cannot perform this upgrade while Aspect Workforce™ users are logged in to the database. In SQL Server Management Studio, you can run the following query against the Aspect Workforce™ database to identify users who are logged in: **sp_who**

2. Stop all **application server services:**

   - Log in to each main and secondary application server in turn
   - Access **Windows Services**: and for Windows Server 2022 or 2025: Select **Start > Windows Administrative Tools > Services**. The **Services** dialog box opens.

3. One at a time, right-click each **WFM service,** and select **Stop** from the shortcut menu. Note the following:

- Also stop the Aspect Message Routing Service, including the backup instance of the service if you have installed a backup on another server.
- If you are using Perform, also stop the RTAListen service if it is logged in to the database.

Uninstalling the Microsoft Access Database Engine (optional)

To remove the currently installed MS Access DB Engine:

1. Open the Control Panel
2. Under Programs click Uninstall a program
3. Select the Microsoft Access Database Engine
4. Click Uninstall
5. Follow the on-screen prompts.
6. Reboot the system.

Note: Upgrading the MS Access DB Engine may cause issues with other Microsoft products installed on the same system. Contact Microsoft for assistance.

Upgrading the Main Application Server

Complete the verification tasks to ensure that your server is ready for the upgrade, and then upgrade the server.

Note: If your install path was a location other than the **C:\Program Files\Alvaria** folder, then the upgrade will persist to that location.

Verification Tasks

Before you upgrade your main application server software, verify that:

- You check the release note for any new requirements or procedures.
- The SQL Server database server has been upgraded.

  For more information, see Upgrading to SQL Server 2022.
- The SQL Server database client has been upgraded on the main application server.

  For more information, see Installing the Client Software.
- Uninstalling the Microsoft Access Database Engine (optional)
- For each WFM system service, you have noted the value for the following service settings: **Log On As** and **Startup Type.**

  You will need this information to reconfigure these settings after the upgrade is complete. An easy way to note this information is to perform a screen capture in the Services window. (To find this window, select **Start > Windows Administrative Tools > Services**). Make sure that the Log On As and Startup Type columns are expanded so that the full setting value is visible.

Note: The passwords to all accounts will be removed upon upgrade, so please ensure that you have a record of these passwords.

Upgrading the Main Application Server

Upgrade the main application server after completing the verification tasks.

To upgrade the main application server software:

1. Log in to your **main application server** and insert the **Aspect Workforce™ Software CD.**
2. Open the file **Setup.exe**. The product selection window of the installation wizard opens.
3. Click **Aspect Workforce™**. If any prerequisite software is not already installed on the server, then the Aspect Prerequisite Installer window opens, displaying a list of prerequisite but uninstalled software. Click **Install** to install the prerequisite software. When installation is complete, the Welcome window of the **Install Wizard For Workforce** opens, and the installer completes some preliminary tasks automatically.
4. Click **Next**. The **Destination Folder** window opens, displaying the path to the program files. If your previous version was installed in a location other than the **C:\Program Files\Alvaria** path, the location will persist.
5. Click **Next**. The **Data Folder** window opens, displaying the path to the data files. If your install path was a location other than the **C:\Program Files\Alvaria** folder, then the upgrade will persist to that location.
6. Click **Next**. The **Custom Setup** window opens, showing the **Main Application Server** icon already selected.

   Note: Do not select Secondary Application Server or User Workstation. The wizard automatically installs components for the secondary application server and the Aspect Workforce™ client on the main application server.
7. If WFM Listen is already installed on the main application server, then the WFM Listen Service icon is preselected in the Custom Setup window. Leave the icon selected to upgrade the service. But if WFM Listen is not already installed and you want to install it on the main application server now, click the **Listen System Service** icon**,** and select **This Feature, And All Subfeatures, Will Be Installed On Local Hard Drive**.

   If you are installing WFM Listen on the main application server now, then after upgrading the main application server, you must configure WFM Listen using the Listen Configuration Editor. For more information, see Using the Listen Configuration Editor.
8. If the Aspect Message Routing Service (AMR service) is already installed on the main application server, then the AMR service icon is preselected in the Custom Setup window. Leave the icon selected to upgrade the service. But if the AMR service is not already installed and you want to install it on the main application server now, click the **Aspect Message Routing Service icon**, and select **This Feature, And All Subfeatures, Will Be Installed On Local Hard Drive**.

   The Aspect Message Routing Service is an optional component of Aspect Workforce™ that is used to enable load balancing (that is, distributed mode for Tally Server, Checker, or both), and is a main component of Empower and Workforce Engagement Management. If you are installing the AMR service on the main application server now, then after upgrading the main application server, you must configure the Aspect Message Routing Service using the Aspect Message Routing Platform Configuration Editor.

   For more information about configuring AMR, see Configuring the Aspect Message Routing Service. For more information about how to set up load balancing for various scenarios, see Configuring AMR for Common Scenarios.

9. If you want to install the WFM Historical Connectors (install files required to configure Five9, InContact, and Zendesk historical connectors), click the **WFM Historical Connectors** icon, and select **This Feature, And All Subfeatures, Will Be Installed On Local Hard Drive**.
   After installing the main application server, you configure the WFM Historical Connectors using the WFM Historical Connector Configuration. For more information, see Using the WFM Historical Connector Configuration. You can also install the WFM Historical Connectors on a secondary application server.
10. Click **Next**. The **DCOM Servers** window opens, displaying the machines names of the servers currently hosting the DCOM services.
11. Click **Next**. Or, if you plan to change the host server for any of these services after the upgrade, type the name of the new server in the corresponding field, and click **Next**. The **Ready to Install** window opens.
12. Click **Install**. After the files are installed, the **Install Wizard Completed** window is displayed.
13. Click **Finish**. If a reboot message is displayed, click **No** in the message, and reboot the server manually after exiting the wizard.

Validating and Configuring the Services

If you have upgraded the WFM Listen service and the Aspect Message Routing Service as part of your main application server upgrade, then it is not necessary to change their configuration with their configuration editors. Simply validate the WFM services, as explained in the next section.

Validating the WFM Services

After you upgrade your application server software, use Windows Services to verify that all required WFM services are properly configured. Refer to your notes for the proper service settings. For more information, see Verification Tasks.

If the Email Reports feature is enabled, verify that WFM service configurations have not changed. See Enabling Email Reports.

For more information about modifying security permissions for Aspect Workforce™ services, see Setting Security Permissions for Services.

Using the Listen Configuration Editor

If the WFM Listen service was already installed on the main application server before upgrading, and you included this service as part of the upgrade, it is not necessary to use the Listen Configuration Editor to update your stream configuration. Your existing stream configurations are preserved from your earlier version of Aspect Workforce™

But if you are installing the WFM Listen service on the main application server for the first time during the upgrade, or if you want to change your stream configurations, access the Listen Configuration Editor at the following path:

- Windows Server 2022 or 2025: **Start > Aspect > Listen Configuration Editor**

For more information, see Using the Listen Configuration Editor.

Using the AMR Configuration Editor

If the Aspect Message Routing Service was already installed on the main application server before upgrading, and you included this service as part of your upgrade, it is not necessary to use the AMR Configuration Editor to update your AMR configuration. The installation program upgrades the AMR service automatically.

But if you are installing AMR on the main application server for the first time during the upgrade, you must complete additional upgrade tasks in the Aspect Message Routing Platform Configuration Editor. For more information, see Configuring the Aspect Message Routing Service.

Using the WFM Historical Connector Editor

If you are instaling the WFM Historical Editor on the main application server for the first time during the upgrade, you must complete additional upgrade tasks in the WFM Historical Connector Editor. For more information, see Using the WFM Historical Connector Configuration.

Upgrading the Database for SQL Server

To upgrade an existing database connection alias, you use the WFM Database Manager program on your main application server to upgrade the Aspect Workforce™ database. The following procedure also updates the database alias connections strings. Before you upgrade your Aspect Workforce™ database, you must back up the database, as described in Backing Up Your Database.

Note: If you added custom objects to your Aspect Workforce™ schema (for example, indexes or constraints), the WFM Database Manager prompts you during the database upgrade and then drops, removes, or deletes the custom objects if you choose to proceed. After the upgrade, your SQL Server database administrator must add the objects.

Note: If you configured a Windows Account as the WFM owner, either use **Run As different user** when launching DBManager, or login to the server as the database owner's windows account. After which you must select **Log in using Windows Integrated security** when prompted for a WFM login in DBManager.

To upgrade your database:

1. For Windows Server 2022 or 2025: Select **Start** > **Aspect > WFM Database Manager**.

   The **Database Manager** window opens.

2. Select the desired **database alias** and select **File > Upgrade Database**. The **Database Manager** login dialog box opens.

3. In the User Name field, type the **TCSDBOWNER** user name.

4. Click the **Password** field, type the password that you assigned to the TCSDBOWNER user name, and click **OK**. The **Schema Version Information** dialog box opens with the schema field disabled.

   If you are upgrading the sample database, type the password for the database owner instead.

5. Click **OK**. The **Select Prepopulation Data Language** dialog box opens.

6. Select the appropriate prepopulated **language** from the drop-down list.

   During the database upgrade, Aspect Workforce™ prepopulates language-specific configuration data. The selected language must match the current language of the Aspect Workforce™ database.

7. Click **OK**. The **SQL Server File Groups** dialog box opens. Default selections appear for your database.

   If desired, use the drop-down list to select alternate file groups.

8. Click **OK**. The **Confirm** dialog box opens.

9. Click **Yes**.

10. In the **Users** window, review the user information displayed, and click **OK**. The **Update User Name And Timestamp** dialog box opens.

Note: The selected time zone must match the time zone that is currently used on the database server.

11. Complete the fields as follows, and click **OK**:

    - In the **Updated By** field, leave the default selection, or use the browse button to select the Aspect Workforce™ user you want to associate with *existing* data in your database.
    - In the **Updated Timestamp** field, leave the default selection, or use the arrows to select another date and time that you want to associate with existing data in your database. The default value is the current system time.

    The WFM Database Manager upgrades the database. Depending on the size of your database, this process could take several hours to complete. When the database upgrade process is complete, a message appears, stating that the schema was successfully upgraded.
    If the upgrade program encounters an error, the Database Error window opens with details of the error:

    - **General** page: States that an unexpected error has occurred.
    - **Advanced** page: Provides details about the error, such as an invalid column name.
    - **Terminate Options** page: Provides a **Terminate Application** button that you can click to halt the upgrade in case the system is not responding.
    - If you encounter an error, **DO NOT CLOSE OUT THIS WINDOW**. Contact Aspect Customer Care IMMEDIATELY for assistance.

12. After you see the message verifying the successful upgrade, click **OK**. The Database Manager window is displayed, showing the upgraded schema version for your database alias.

13. Repeat this entire procedure for each database that you want to upgrade.

14. When you are finished upgrading your databases, select **File > Exit** in the Database Manager window.

Persisting Database Roles

Note: Skip this section if you are using Application Roles (default) instead of Database Roles (not typical).

The Application Roles feature, introduced in release 8.0, implements password protection and thereby enforce a higher level of security for database access. When you implement this feature, Aspect Workforce™ users can access the Aspect Workforce™ database to add, delete, or modify data *only* when they are logged in to Aspect Workforce™.

If you chose not to implement this feature since it was introduced in version 8.0, then security will continue to be enforced using database roles. To continue using Database Roles (not recommended) from a legacy version of Aspect Workforce™, complete the following actions in the order shown:

1. Log in to your main application server.
2. Do the following:

    - Windows Server 2022 or 2025: Select **Start** > **Aspect** > **WFM Database Manager**. The **Database Manager** window opens.

3. In the list of database aliases, select the desired Aspect Workforce™ **database**.
4. In the main menu, select Tools > Modify Application Role Password.
5. Verify that the option for **Log In Using a Specific User Name And Password** is selected, and log in as the database schema owner, typically **TCSDBOWNER**.
6. Select **TCS_CLIENT** role and click the **Active Toggle** button to set the application role to **Inactive**.
7. Select **TCS_UPDATER** role and click the **Active Toggle** button to set the application role to **Inactive**.
8. Click **OK**.
9. In the main menu, select **File** > **Exit**.

Upgrading a Secondary Application Server

If you are upgrading Aspect Workforce™ and you have only one application server (that is, if you have a main application server with secondary application server software), the installation wizard upgrades the installed services automatically. If you have a distributed installation, you must manually upgrade the services installed on each secondary application server.

Before You Upgrade

Before you upgrade your secondary application server software, note the value of the service settings for each WFM system service. Specifically, note the value for the **Log On As** and **Startup Type** service settings. You will need this information to reconfigure these settings after the upgrade is complete. An easy way to note this information is to perform a screen capture in the Services window. (To access this window, select **Start > Windows Administrative Tools > Services**). Make sure that the Log On As and Startup Type columns are expanded so that the full setting value is visible.

In addition, ensure that the SQL Server database client has been upgraded on the secondary application server. For instructions see, Installing the SQL Server Client Software. To verify the required version of the database client, see the *Aspect Workforce™ Release Note*.

If the Microsoft Access Database Engine was installed only for use with Aspect Workforce and is not used outside of Aspect Workforce, we recommend you uninstall it. For instructions, see Uninstalling the Microsoft Access Database Engine (optional).

Upgrading the Secondary Application Server

To upgrade a secondary application server:

1. Log in to a **secondary application server and** launch **Windows Explorer.**
2. Locate and double-click the following **file**, where ***MainAppServer*** is the machine name of the main application server: ***MainAppServer*\WFMSetup\Workforce Management\Setup.exe**

   If any prerequisite software is not already installed on the server, then the Aspect Prerequisite Installer window opens, displaying a list of prerequisites but uninstalled software. Click **Install** to install the prerequisite software. When installation is complete, the Welcome window of the **Install Wizard For Workforce** opens, and the installer completes some preliminary tasks automatically.
3. Click **Next**. The **Destination Folder** window opens, displaying the path to the program files. If your previous version was installed in a location other than the **C:\Program Files\Alvaria** path, the location will persist.

4. Click **Next**. The **Data Folder** window opens, displaying the path to the data files. If your previous version was installed in a location other than the **C:\ProgramData\Aspect** path, the location will persist.
5. Click **Next**. The **Custom Setup** window opens, showing the **Secondary Application Server** icon already selected.

   Note: Do not select User Workstation. The wizard automatically installs components for the secondary application server and the Aspect Workforce™ client on the main application server.
6. If WFM Listen is already installed on the secondary application server, then the WFM Listen Service icon is preselected in the Custom Setup window. Leave the icon selected to upgrade the service. But if WFM Listen is not already installed and you want to install it on the secondary application server now, click the **Listen System Service** icon**,** and select **This Feature, And All Subfeatures, Will Be Installed On Local Hard Drive**.

   If you are installing WFM Listen on the secondary application server now, then after upgrading the secondary application server, you must configure WFM Listen using the Listen Configuration Editor. For more information, see Using the Listen Configuration Editor.
7. If the Aspect Message Routing Service (AMR service) is already installed on the secondary application server, then the AMR service icon is preselected in the Custom Setup window. Leave the icon selected to upgrade the service. But if the AMR service is not already installed and you want to install

   it on the secondary application server now, click the **Aspect Message Routing Service icon**, and select **This Feature, And All Subfeatures, Will Be Installed On Local Hard Drive**.

   The Aspect Message Routing Service is an optional component of Aspect Workforce™ that is used to enable load balancing (that is, *distributed mode* for Tally Server, Checker, or both), and is a main component of Empower and Workforce Engagement Management. If you are installing the AMR service on the secondary application server now, then after upgrading the secondary application server, you must configure the Aspect Message Routing Service using the Aspect Message Routing Platform Configuration Editor.

   For more information about configuring AMR, see Configuring the Aspect Message Routing Service. For more information about how to set up load balancing for various scenarios, see Configuring AMR for Common Scenarios.
8. If you want to install the WFM Historical Connectors (install files required to configure Five9, InContact, and Zendesk historical connectors), click the **WFM Historical Connectors** icon, and select **This Feature, And All Subfeatures, Will Be Installed On Local Hard Drive**.

   After installing the secondary application server, you configure the WFM Historical Connectors using the WFM Historical Connector Configuration. For more information, see Using the WFM Historical Connector Configuration.
9. Click **Next**. The **Main Application Server** window opens, showing the name of the current main application server.
10. Click **Next**. The **DCOM Servers** window opens, displaying the machines names of the servers currently hosting the DCOM services.

    If the DCOM Servers window does not open and you get a message instead, use the IP address of the main application server instead of the server name in step 8.
11. Click **Next**. Or, if you plan to change the host server for any of these services after the upgrade, type the name of the new server in the corresponding field, and click **Next**. The **Ready to Install** window opens.

12. Click **Install**. After the files are installed, the **Install Wizard Completed** window is displayed.
13. Click **Finish**. If a reboot message is displayed, click **No** in the message, and reboot the server manually after exiting the wizard.

Validating and Configuring the Services

If you have upgraded the WFM Listen service and the Aspect Message Routing Service as part of your secondary application server upgrade, then it is not necessary to change their configuration with their configuration editors. Simply validate the WFM services, as explained in the next section.

Note: The passwords to all accounts will be removed upon upgrade, so please ensure that you have a record of these passwords.

Validating the WFM Services

After you upgrade your secondary application server software, use Windows Services to verify that all required WFM services are properly configured. Refer to your notes for the proper service settings. For more information, see Verification Tasks.

For more information about modifying security permissions for Aspect Workforce™ services, see Setting Security Permissions for Services.

Using the Listen Configuration Editor

If the WFM Listen service was already installed on the secondary application server before upgrading, and you included this service as part of the upgrade, it is not necessary to use the Listen Configuration Editor to update your stream configuration. Your existing stream configurations are preserved from your earlier version of Aspect Workforce™

But if you are installing the WFM Listen service on the secondary application server for the first time during the upgrade, or if you want to change your stream configurations, access the Listen Configuration Editor at the following path:

- Windows Server 2022 or 2025: **Start > Aspect > Listen Configuration Editor**.

Using the AMR Configuration Editor

If the Aspect Message Routing Service was already installed on the secondary application server before upgrading, and you included this service as part of your upgrade, it is not necessary to use the AMR Configuration Editor to update your AMR configuration. The installation program upgrades the AMR service automatically.

But if you are installing AMR on the secondary application server for the first time during the upgrade, you must complete additional upgrade tasks in the Aspect Message Routing Platform Configuration Editor. For more information, see Configuring the Aspect Message Routing Service.

Using the WFM Historical Connector Configuration

If you installed the WFM Historical Connectors, configure the appropriate connector(s) using the WFM Historical Connector Configuration.

Upgrading User Workstations

Before upgrading the client software, install the Microsoft OLE DB Driver for SQL Server on all workstations. For instructions, see Installing the SQL Server Client Software. If prompted to install specified versions of prerequisite software, such as the Windows Installer or .NET Framework, follow the

prompts to install the prerequisite software. Aspect recommends that you uninstall the Microsoft Access Database Engine. For instructions, see Uninstalling the Microsoft Access Database Engine (optional)
You can upgrade the client software by:

- Following the procedure provided in this section.
- Using a command line. Upgrading the client with the command line follows the same procedure as installing with the command line. For instructions, see Installing with a Command Line.

To upgrade the client software:

1. Log in as an administrator to the **user workstation and** launch **Windows Explorer.**
2. Locate and double-click the following **file**, where ***MainAppServer*** is the machine name assigned to your main application server: ***MainAppServer*\WFMSetup\Workforce Management\Setup.exe**

   If any prerequisite software is not already installed on the workstation, then the Aspect Prerequisite Installer window opens, displaying a list of prerequisites but uninstalled software. Click **Install** to install the prerequisite software. When installation is complete, the Welcome window of the **Install Wizard For Workforce** opens, and the installer completes some preliminary tasks automatically.
3. Click **Next**. The **Destination Folder** window opens, displaying the path to the program files. If your previous version was installed in a location other than the **C:\Program Files\Alvaria** path, the location will persist.
4. Click **Next**. The **Data Folder** window opens, displaying the path to the data files. If your previous version was installed in a location other than the C:\ProgramData\Aspect path, the location will persist.
5. Click **Next**. The **Custom Setup** window opens, showing the **User Workstation** icon already selected.
6. Click **Next**. The **Main Application Server** window opens.
7. Verify or type the **machine name** of the main application server and click **Next**. The **DCOM Servers** window opens, displaying the machines names of the servers currently hosting the DCOM services.
8. Click **Next**. Or, if you plan to change the host server for any of these services after the upgrade, type the name of the new server in the corresponding field, and click **Next**. The **Ready to Install** window opens.
9. Click **Install**. After the files are installed, the **Install Wizard Completed** window is displayed.
10. Click **Finish**. If a reboot message is displayed, click **No** in the message, and reboot the server manually after exiting the wizard.

Upgrading the Sample Database

The sample database is optional. If you do not want to upgrade it, skip this step and continue with Removing Database Restrictions.

Note: If you have added custom objects to your Aspect Workforce™ schema (for example, indexes or constraints), the WFM Database Manager prompts you and then drops them if you choose to proceed. After the upgrade, your SQL Server database administrator must add the objects back to the schema.

To upgrade your sample database:

1. Log in to your main application server.
2. Do the following:

- Windows Server 2022 or 2025: Select **Start** > **Aspect > WFM Database Manager**.

The **Database Manager** window opens.

3. Follow the instructions for Upgrading the Database for SQL Server (starting with step 2), making the following changes during the procedure:
4. In step 2, substitute the sample database alias—typically, WFM_SAMPLE—for the main database alias (typically, WFM).

   In step 3 and step 4, log in to the database with the **user name** and **password** for the **TCS_Sample** database.

   This is the password you set up when configuring SQL Server. See step 16 in Installing and Configuring SQL Server.

Removing Database Restrictions

Remove database restrictions to revert your database to its previous state, before the upgrade. These are the restrictions you set in Restricting Your Database.

To remove database restrictions:

1. Log in to your database server as an administrator.
2. Open **SQL Server Management Studio** and log in to the database engine as a **system administrator**.
3. Right-click your **database and** select **Properties**. The **Properties** dialog box opens.
4. Select the **Options** tab. The **Options** page opens.
5. In the **State** section (which is displayed near the bottom of the scrolling list)**,** for the **Restrict Access** option, select **MULTI_USER** from the drop-down list.
6. Click **OK**. If the **Open Connections** message opens, click **Yes**. The **(Restricted User)** tag is removed from the database in the Databases list.
7. To remove restrictions from another database, go back to step 3.
8. Select **File > Exit** to exit SQL Server Management Studio.

Enabling Optional Features

After upgrading, you can enable the following optional features:

- Enabling Email Reports
- Running WFM services with non-administrative accounts

Enabling Email Reports

This section applies only if you plan to use the Email Reports feature.

To enable Emailing Reports in WFM for the first time, or to continue to receive emailed reports, you will need to see:

1. Configuring the SMTP Server

Note: If your SMTP server was previously connected via port 465, review for updated requirements.

2. Configuring WFM Notification Queue Manager
3. Setting Registry Parameters for SMTP

Running WFM Services with Non-Administrative Accounts

After upgrading, all WFM services are automatically configured to run with local system accounts. But you can increase security on your application servers by configuring any number of WFM services to run with a regular user account.

For instructions, see Running WFM Services with Non-Administrative Accounts.

Post-Upgrade Administrative Tasks

Refer to Post-Installation Administrative Tasks for any additional post-upgrade tasks you might need to complete. The chapter also includes procedures you can use to verify that your upgrade was successful.

Upgrading for Oracle

This chapter provides instructions for Oracle users who are upgrading from version 21.1 or later of Aspect Workforce™ to this version of Aspect Workforce™.

Although you cannot directly upgrade the Aspect Workforce™ *software* from version 21.1 to 24, you can use a procedure in this chapter to directly upgrade the *database schema* from version 21.1 to 24. For more information, see Upgrade Considerations.

For compatibility information regarding Oracle release levels, see the *Release Note* (Compatible Database Platforms section). For more information about installing and configuring Oracle 19c, see Configuring Oracle.

The installation program automates several tasks that were formerly manual steps in prior releases of Aspect Workforce™. As you progress through the installation wizard, some of the processes might require several minutes to complete. This is normal and does not indicate any issues with your hardware, software, or the installer. When the installation is complete, a wizard screen confirms that the installation was successful.

Pre-Upgrade Tasks

Before upgrading to Aspect Workforce™, complete the following tasks:

1. Run the Aspect Workforce™ Upgrade Compatibility Verification Tool.
2. Verify the permissions for the schema owner.
3. Upgrade your Aspect Workforce™ database server to Oracle 19c.

For compatibility information regarding RDMBS release levels, see the *Aspect Workforce™ Release Note* (Compatible Database Platforms section). These tasks are described in the following sections.

Running the Verification Tool

Run the verification tool to resolve conflicts in your database.

About the Verification Tool

The Aspect Workforce™ Upgrade Compatibility Verification Tool pinpoints database conflicts, called *violations* or *duplicates*. Once the tool has pinpointed these conflicts, you resolve them by logging in to Aspect Workforce™ and making the necessary changes to the data, or by contacting Aspect Customer Care for assistance.

Running the Verification Tool

One or two weeks before upgrading, run the Aspect Workforce™ Upgrade Compatibility Verification Tool (provided in the product package) to identify and resolve any conflicts that may exist in your database.

You will also run the tool as part of the normal upgrade procedures described in this chapter. But we recommend that you do a preliminary run before upgrading, since the conflict resolution process can potentially be time-consuming, especially with a large database.

Run the Aspect Workforce™ Upgrade Compatibility Verification Tool on all databases that you plan to upgrade.

To run the tool:

1. Insert the **Aspect Workforce™ Software CD** in the CD drive of the main application server, and navigate to the file ***x:*\Utility\DbVer.exe**, where ***x*** is the name of the CD drive.
2. Copy the **DbVer.exe** file to a folder on the main application server and open the **file** from this folder. The main window of the **Aspect Workforce™ Upgrade Compatibility Verification** dialog box opens.
3. Under Select RDBMS Type, select **Oracle 10g/11g/12c/19c** as the database platform type.
4. Complete the **Host Name** field by typing the Oracle Service Name from the TNSNames.ora file.
5. Click **Connect**. The **Database Login** dialog box opens.
6. Type the **User Name** and **Password** for the owner of the schema and click **OK**.

   Typically, this User Name is **TCSDBOWNER**.
   After the tool connects to the database, the main window opens.
7. Click **OK** to begin verification. After the tool searches the database, it displays any violations in the main window.
8. If violations were found, browse to the log file, **23UpgCompat.Log**, and view and print the **details**.

   The log file is stored in the following location: **C:\ProgramData\Aspect\Workforce Management\log**
9. Log in to your current version of **Aspect Workforce™** and resolve the **violations** by modifying the data identified in the 23UpgCompat.log file.

   You might need an experienced Aspect Workforce™ user, or Aspect Customer Care to complete this step. For guidelines on modifying the data, see Resolving Database Conflicts.
10. Re-run the **tool**, resolving violations each time in step 14 and step 15, until no violations are found.

Resolving Database Conflicts

The following table shows typical database conflicts and suggestions for resolving them in Aspect Workforce™.

It is assumed that the names shown for each example refer to different people, rather than being duplicate entries for the same person.

There are other possible resolutions in addition to the ones shown. The important thing is that each item in the database be unique.

Conflict	Cause	Resolution	Solution
John Williams conflicts with: JOHN WILLIAMS	Using case as a differentiator.	John A. Williams does not conflict with: John E. Williams	Include middle initial.
Allen Jackson conflicts with: Allen Jackson	Using leading spaces as a differentiator.	Allen Jackson does not conflict with: Allen_Jackson	Substitute underscore for leading spaces.

Database modification action for Oracle upgrades from 21.1

For Oracle upgrades from 21.1, an Out of Memory error can be encountered if there are a large number of PEND records in the NOTF table. Prior to upgrading, run the following query on the WFM database to prevent this issue. This will remove notifications that have been in PEND for 7 days or more.

```
DECLARE   v_done
NCHAR(1) := 'F'; BEGIN
  LOOP     EXIT WHEN v_done =
'T';          delete       from
NOTF      where PROC_TS <
(SYSDATE - 7)        and
PROC_STATUS = 'PEND'        and
rownum <= 50000;          IF
SQL%ROWCOUNT < 50000 THEN
v_done := 'T';       commit;
ELSE       commit;     END IF;
```

```
    END LOOP;
END;
```

Verifying the Schema Owner Permissions

Ensure that the permissions for the schema owner are set as described in the section Configuring Manually. In particular, verify that the schema owner (for example, TCSDBOWNER) has been granted the EXECUTE privilege on DBMS_LOB.

Upgrading to Oracle 19c

Verify you are running Oracle 19, and if not, upgrade Oracle by running the Oracle 19c installation program. None of the steps in the upgrade process require special configuration for Aspect Workforce™.

For installation instructions, see Upgrading Oracle.

You must install both the 32-bit and 64-bit clients on all application servers. Client workstations only require the 64-bit client.

Upgrade Overview

The following list shows the tasks required to upgrade Aspect Workforce™ and the correct sequence of those tasks. When performing these upgrade tasks, always log in to the server with a domain account that is also a member of the local Administrators group.

- Re-running the Verification Tool
- Stopping the WFM Services
- Restricting Your Database
- Backing Up Your Database
- Uninstalling the Microsoft Access Database Engine (optional)
- Upgrading the Main Application Server
- Upgrading the Database
- Upgrading a Secondary Application Server
- Upgrading User Workstations
- Configuring User System Privileges
- Upgrading Your Sample Database
- Enabling Your Database

Upgrade Procedures

This section provides procedures for the tasks outlined in the upgrade overview. Complete these tasks in the order shown.

Re-running the Verification Tool

Even if you have run the Aspect Workforce™ Upgrade Compatibility Verification Tool previously to identify and resolve any conflicts in your database, run the tool again in case a few conflicts have emerged while you used Aspect Workforce™ in the intervening time. Running the tool should be much quicker now.

For instructions, see Running the Verification Tool.

Stopping the WFM Services

If you are using Distributed Checker, contact Aspect Customer Care for guidance on stopping the Checker service.

To stop Aspect Workforce™ services:

1. Verify that all **users** are logged out. You cannot perform this upgrade while Aspect Workforce™ users are logged in to the database.
2. Stop all **application server services.** To do this, log in to each main and secondary application server in turn, and complete the following steps:
   a. Do the following to access **Windows Services**: Windows Server 2022 or 2025: Select **Start > Windows Administrative Tools > Services**. The **Services** dialog box opens.
   b. One at a time, right-click each **WFM service,** and select **Stop** from the shortcut menu. Note the following:

- Also stop the Aspect Message Routing Service, including the backup instance of the service if you have installed a backup on another server.
- If you are using Perform, also stop the RTAListen service if it is logged in to the database.

Restricting Your Database

Verify that no users can connect to the database while the upgrade process is in progress. To do this, enable an Oracle restricted session (using SQL*Plus, for example).

To restrict database access:

1. Log in to the **database** using a login ID with **SYSDBA** privileges.
2. Enable **restricted sessions** for your Oracle database.
3. Log out of the **database**.

Backing Up Your Database

Always back up your database before installing an upgrade.

Caution: An grade can change the internal structure of your database. If a hardware or software failure occurs during this process, you could lose your data. Your Oracle database administrator can help you with the backup process of exporting a *.DMP file of your Aspect Workforce™ database.

Uninstalling the Microsoft Access Database Engine (optional)

To remove the currently installed MS Access DB Engine:

1. Open the Control Panel.
2. Under Programs click Uninstall a program.
3. Select the Microsoft Access Database Engine.
4. Click Uninstall.

5. Follow the on-screen prompts.
6. Reboot the system.

Upgrading the Main Application Server

Complete the verification tasks to ensure that your server is ready for the upgrade, and then upgrade the server.

Verification Tasks

Before you upgrade your main application server software, verify that:

- You check the release note for any new requirements or procedures.
- The Oracle database server has been configured.
- The Oracle database client has been upgraded on the main application server.
- Uninstalling the Microsoft Access Database Engine (optional).
- For each WFM system service, you have noted the value for the following service settings: Log On As and **Startup Type.**

You will need this information to reconfigure these settings after the upgrade is complete. An easy way to note this information is to perform a screen capture in the Services window. (To find this window, select **Start > Administrative Tools > Services**). Make sure that the Log On As and Startup Type columns are expanded so that the full setting value is visible.

The passwords to all accounts will be removed upon upgrade, so please ensure that you have a record of these passwords.

Upgrading the Main Application Server

Upgrade the main application server after completing the verification tasks.

To upgrade the main application server software:

1. Log in to your **main application server** and insert the **Aspect Workforce™ Software CD.**
2. Open the file **Setup.exe**. The product selection window of the installation wizard opens.
3. Click **Aspect Workforce™**. If any prerequisite software is not already installed on the server, then the Aspect Prerequisite Installer window opens, displaying a list of prerequisite but uninstalled software. Click **Install** to install the prerequisite software. When installation is complete, the Welcome window of the **Install Wizard for Workforce** opens.
4. Click **Next**. The **Destination Folder** window opens, displaying the path to the program files. If your previous version was installed in a location other than the **C:\Program Files\Alvaria** path, the location will persist.
5. Click **Next**. The **Data Folder** window opens, displaying the path to the data files. If your previous version was installed in a location other than the **C:\ProgramData\Aspect** path, the location will persist.
6. Click **Next**. The **Custom Setup** window opens, showing the **Main Application Server** icon already selected.

7. Do not select Secondary Application Server or User Workstation. The wizard automatically installs components for the secondary application server and the Aspect Workforce™ client on the main application server.

8. If WFM Listen is already installed on the main application server, then the WFM Listen Service icon is preselected in the Custom Setup window. Leave the icon selected to upgrade the service. But if WFM Listen is not already installed and you want to install it on the main application server now, click the **Listen System Service** icon**,** and select **This Feature, And All Subfeatures, Will Be Installed On Local Hard Drive**.

   If you are installing WFM Listen on the main application server now, then after upgrading the main application server, you must configure WFM Listen using the Listen Configuration Editor. For more information, see Using the Listen Configuration Editor.

9. If the Aspect Message Routing Service (AMR service) is already installed on the main application server, then the AMR service icon is preselected in the Custom Setup window. Leave the icon selected to upgrade the service. But if the AMR service is not already installed and you want to install it on the main application server now, click the **Aspect Message Routing Service icon**, and select **This Feature, And All Subfeatures, Will Be Installed On Local Hard Drive**.

   The Aspect Message Routing Service is an optional component of Aspect Workforce™ that is used to enable load balancing (that is, distributed mode for Tally Server, Checker, or both). If you are installing the AMR service on the main application server now, then after upgrading the main application server, you must configure the Aspect Message Routing Service using the Aspect Message Routing Platform Configuration Editor.

   For more information about configuring AMR, see Configuring the Aspect Message Routing Service. For more information about how to set up load balancing for various scenarios, see Configuring AMR for Common Scenarios.

10. If you want to install the WFM Historical Connectors (install files required to configure Five9, InContact, and Zendesk historical connectors), click the **WFM Historical Connectors** icon, and select **This Feature, And All Subfeatures, Will Be Installed On Local Hard Drive**.

    After installing the main application server, you configure the WFM Historical Connectors using the WFM Historical Connector Configuration. For more information, see Using the WFM Historical Connector Configuration. You can also install the WFM Historical Connectors on a secondary application server.

11. Click **Next**. The **DCOM Servers** window opens, displaying the machines names of the servers currently hosting the DCOM services.

12. Click **Next**. Or, if you plan to change the host server for any of these services after the upgrade, type the name of the new server in the corresponding field, and click **Next**. The **Ready to Install** window opens.

13. Click **Install**. After the files are installed, the **Install Wizard Completed** window is displayed.

14. Click **Finish**. If a reboot message is displayed, click **No** in the message, and reboot the server manually after exiting the wizard.

Installing the AMR Service (Optional)

The *Aspect Message Routing Service* is required only if you are planning to use load balancing, or planning to install Empower and/or Workforce Engagement Management. After installing the service, use the AMR Configuration Editor to configure the service. For more information, see Configuring the Aspect Message Routing Service.

You can install the Aspect Message Routing Service only after upgrading the main or secondary application server. Unlike in a fresh install, you cannot install the Aspect Message Routing Service while *upgrading* the server.

To install the Aspect Message Routing Service:

1. Log in to your **main application server** and insert the **distribution CD.**
2. Open the file **Setup.exe.** The **Welcome** window opens. 3. Click **Next**. The

   Program Maintenance window opens.
4. Select **Modify** and click **Next**. The **Custom Setup** window opens.
5. Click the **Aspect Message Routing Service** icon, and select **This Feature, And All Subfeatures, Will Be Installed On Local Hard Drive**.
6. Click Next. The **Ready To Install** window opens, listing the Aspect Workforce™ DCOM servers in your deployment.
7. Click **Install**. The **Installing Aspect Workforce™** window opens and begins installing the needed files. When the installation is complete and successful, the **Installation Complete** window opens.
8. Click **Finish**.

Validating and Configuring the Services

If you have upgraded the WFM Listen service and the Aspect Message Routing Service as part of your main application server upgrade, then it is not necessary to change their configuration with their configuration editors. Simply validate the WFM services, as explained in the next section.

Validating the WFM Services

After you upgrade your application server software, use Windows Services to verify that all required WFM services are properly configured. Refer to your notes for the proper service settings. For more information, see Verification Tasks.

If the Email Reports feature is enabled, verify that WFM service configurations have not changed. See Enabling Email Reports for more information.

In Windows, there are additional COM security settings that affect access to the Aspect Workforce™ services. There are COM security permissions that affect access to services, as well as machine-wide COM security limits that enforce launch and activation restrictions. So, to enable service access for all users, you must configure your security settings as described in Setting Security Permissions for Services.

Using the Listen Configuration Editor

If the WFM Listen service was already installed on the main application server before upgrading, and you included this service as part of the upgrade, it is not necessary to use the Listen Configuration Editor to update your stream configuration. Your existing stream configurations are preserved from your earlier version of Aspect Workforce™

But if you are installing the WFM Listen service on the main application server for the first time during the upgrade, or if you want to change your stream configurations, access the Listen Configuration Editor at the following path: Windows Server 2022 or 2025: **Start** > **Aspect > WFM Listen Configuration Editor**

Using the AMR Configuration Editor

If the Aspect Message Routing Service was already installed on the main application server before upgrading, and you included this service as part of your upgrade, it is not necessary to use the AMR Configuration Editor to update your AMR configuration. The installation program upgrades the AMR service automatically.

But if you are installing AMR on the main application server for the first time during the upgrade, you must complete additional upgrade tasks in the Aspect Message Routing Platform Configuration Editor. For more information, see Configuring the Aspect Message Routing Service d Configuring AMR for Common Scenario Scenarios chapters.

Using the WFM Historical Connector Configuration

If you installed the WFM Historical Connectors, configure the appropriate connector(s) using the WFM Historical Connector Configuration.

Upgrading the Database

To upgrade an existing database connection alias, you use the WFM Database Manager program on your main application server to upgrade the Aspect Workforce™ database. Before you upgrade your Aspect Workforce™ database, you must back up the database, as described in Backing Up Your Database.

If you added custom objects to your Aspect Workforce™ schema (for example, indexes or constraints), the WFM Database Manager prompts you during the upgrade and then drops, removes, or deletes the custom objects if you choose to proceed. After the upgrade, your Oracle database administrator must add the objects.

 **Note:** If you configured a Windows Account as the WFM owner, either use **Run As different user** when launching DBManager, or login to the server as the database owner's windows account. After which you must select **Log in using Windows Integrated Security** when prompted for a WFM login in DBManager.

 **Additional Note for Oracle:** This should have already been previously configured but as a reminder, when defining the Schema name in DBManager, you will need to place the owner account in quotes in this format - "OPS$*domain\username*" where *domain\username* is the WFM schema owner.

To upgrade your database:

1. Do the following: Windows Server 2022 or 2025: **Start** > **Aspect > WFM Database Manager** The **Database Manager** window opens.
2. Select the **database alias** and select **File > Upgrade Database**. The **Database Manager** login dialog box opens.
3. In the User Name field, type the **TCSDBOWNER** user name.
4. Click the **Password** field, type the password that you assigned to the TCSDBOWNER user name, and click **OK**. The **Schema Version Information** dialog box opens with the schema field disabled.
5. Click **OK**. The **Select Prepopulation Data Language** dialog box opens.
6. Select the appropriate prepopulated **language** from the drop-down list.

   During the database upgrade, Aspect Workforce™ prepopulates language-specific configuration data. The selected language must match the current language of the Aspect Workforce™ database.
7. Click **OK**. The **Oracle Tablespaces** dialog box opens. Default selections appear for your database.

If desired, use the drop-down list to select alternate file groups.

8. Click **OK**. The **Confirm** dialog box opens.
9. Click **Yes**.
10. In the **Users** window, review the user information displayed, and click **OK**. The **Update User Name And Timestamp** dialog box opens.
11. Complete the fields as follows, and click **OK**:

    In the **Updated By** field, leave the default selection, or use the browse button to select the Aspect Workforce™ user you want to associate with *existing* data in your database.

    In the **Updated Timestamp** field, leave the default selection, or use the arrows to select another date and time that you want to associate with existing data in your database. The default value is the current system time.

    The WFM Database Manager upgrades the database. Depending on the size of your database, this process could take several hours to complete. When the database upgrade process is complete, a message appears, stating that the schema was successfully upgraded.
    If the upgrade program encounters an error, the Database Error window opens with details of the error:

    General page: States that an unexpected error has occurred.

    Advanced page: Provides details about the error, such as an invalid column name.

- **Terminate Options** page: Provides a **Terminate Application** button that you can click to halt the upgrade in case the system is not responding.

    If you encounter an error, **DO NOT CLOSE OUT THIS WINDOW**. Contact Aspect Customer Care IMMEDIATELY for assistance.

12. After you see the message verifying the successful upgrade, click **OK**. The Database Manager window is displayed, showing the upgraded schema version for your database alias.
13. Repeat this entire procedure for each database that you want to upgrade.
14. When you are finished upgrading your databases, select **File > Exit** in the Database Manager window.

Upgrading a Secondary Application Server

If you are upgrading Aspect Workforce™ and you have only one application server (that is, if you have a main application server with secondary application server software), the installation wizard upgrades the installed services automatically. If you have a distributed installation, you must manually upgrade the services installed on each secondary application server.

Before You Upgrade

Before you upgrade your secondary application server software, note the value of the service settings for each WFM system service. Specifically, note the value for the **Log On As** and **Startup Type** service settings. You will need this information to reconfigure these settings after the upgrade is complete. An easy way to note this information is to perform a screen capture in the Services window. (To access this window, select **Start > Administrative Tools > Services**). Make sure that the Log On As and Startup Type columns are expanded so that the full setting value is visible.

In addition, ensure that the Oracle database client has been upgraded on the secondary application server. For instructions see, Installing the Client Software. To verify the required version of the database client, see the *Aspect Workforce™ Release Note*.

If the Microsoft Access Database Engine was installed only for use with Aspect Workforce and is not used outside of Aspect Workforce, we recommend you uninstall it. For instructions, see Uninstalling the Microsoft Access Database Engine (optional).

Upgrading the Secondary Application Server

To upgrade a secondary application server:

1. Log in to a **secondary application server and** launch **Windows Explorer.**
2. Locate and double-click the following **file**, where MainAppServer is the machine name of the main application server: ***MainAppServer*\WFMSetup\Workforce Management\Setup.exe**

   If any prerequisite software is not already installed on the server, then the Aspect Prerequisite Installer window opens, displaying a list of prerequisites but uninstalled software. Click **Install** to install the prerequisite software. When installation is complete, the Welcome window of the **Install Wizard for Workforce** opens.
3. Click **Next**. The **Destination Folder** window opens, displaying the path to the program files. If your previous version was installed at the **C:\Program Files(x86)** path, the location will persist, even though the software is 64-bit.
4. Click **Next**. The **Data Folder** window opens, displaying the path to the data files. If your previous version was installed at the **C:\Program Files(x86)** path, the location will persist, even though the software is 64-bit.
5. Click **Next**. The **Custom Setup** window opens, showing the **Secondary Application Server** icon already selected.

   Caution: Do not select User Workstation. The wizard automatically installs components for the secondary application server and the Aspect Workforce™ client on the main application server.
6. If WFM Listen is already installed on the secondary application server, then the WFM Listen Service icon is preselected in the Custom Setup window. Leave the icon selected to upgrade the service. But if WFM Listen is not already installed and you want to install it on the secondary application server now, click the **Listen System Service** icon**,** and select **This Feature, And All Subfeatures, Will Be Installed On Local Hard Drive**.

   If you are installing WFM Listen on the secondary application server now, then after upgrading the secondary application server, you must configure WFM Listen using the Listen Configuration Editor. For more information, see Using the Listen Configuration Editor.
7. If the Aspect Message Routing Service (AMR service) is already installed on the secondary application server, then the AMR service icon is preselected in the Custom Setup window. Leave the icon selected to upgrade the service. But if the AMR service is not already installed and you want to install it on the secondary application server now, click the **Aspect Message Routing Service icon**, and select **This Feature, And All Subfeatures, Will Be Installed On Local Hard Drive**.

   The Aspect Message Routing Service is an optional component of Aspect Workforce™ that is used to enable load balancing (that is, *distributed mode* for Tally Server, Checker, or both), and is a main component of Empower and Workforce Engagement Management. If you are installing the AMR service on the secondary application server now, then after upgrading the secondary application server, you must configure the Aspect Message Routing Service using the Aspect Message Routing Platform Configuration Editor.
   For more information about configuring AMR, see Configuring the Aspect Message Routing Service.
   For more information about how to set up load balancing for various scenarios, see Configuring AMR for Common Scenarios.

8. If you want to install the WFM Historical Connectors (install files required to configure Five9, InContact, and Zendesk historical connectors), click the **WFM Historical Connectors** icon, and select **This Feature, And All Subfeatures, Will Be Installed On Local Hard Drive**.

   After installing the secondary application server, you configure the WFM Historical Connectors using the WFM Historical Connector Configuration. For more information, see Using the WFM Historical Connector Configuration. You can also install the WFM Historical Connectors on a secondary application server.

9. Click **Next**. The **Main Application Server** window opens, showing the name of the current main application server.
10. Click Next. The **DCOM Servers** window opens, displaying the machines names of the servers currently hosting the DCOM services.
11. Click **Next**. Or, if you plan to change the host server for any of these services after the upgrade, type the name of the new server in the corresponding field, and click **Next**. The **Ready to Install** window opens.
12. Click **Install**. After the files are installed successfully, the **Install Wizard Completed** window is displayed.
13. Click **Finish**. If a reboot message is displayed, click **No** in the message, and reboot the server manually after exiting the wizard.

Validating and Configuring the Services

If you have upgraded the WFM Listen service and the Aspect Message Routing Service as part of your secondary application server upgrade, then it is not necessary to change their configuration with their configuration editors. Simply validate the WFM services, as explained in the next section.

The passwords to all accounts will be removed upon upgrade, so please ensure that you have a record of these passwords.

Validating the WFM Services

After you upgrade your secondary application server software, use Windows Services to verify that all required WFM services are properly configured. Refer to your notes for the proper service settings. For more information, see Before You Upgrade.

In Windows, there are additional COM security settings that affect access to the Aspect Workforce™ services. There are COM security permissions that affect access to services, as well as machine-wide COM security limits that enforce launch and activation restrictions. So, to enable service access for all users, you must configure your security settings as described in Setting Security Permissions for Services.

Using the Listen Configuration Editor

If the WFM Listen service was already installed on the secondary application server before upgrading, and you included this service as part of the upgrade, it is not necessary to use the Listen Configuration Editor to update your stream configuration. Your existing stream configurations are preserved from your earlier version of Aspect Workforce™

But if you are installing the WFM Listen service on the secondary application server for the first time during the upgrade, or if you want to change your stream configurations, access the Listen Configuration Editor. You can access the editor at the following path: Windows Server 2022 or 2025: **Start** > **Aspect > Listen Configuration Editor**

Using the AMR Configuration Editor

If the Aspect Message Routing Service was already installed on the secondary application server before upgrading, and you included this service as part of your upgrade, it is not necessary to use the AMR Configuration Editor to update your AMR configuration. The installation program upgrades the AMR service automatically.

But if you are installing AMR on the secondary application server for the first time during the upgrade, you must complete additional upgrade tasks in the Aspect Message Routing Platform Configuration Editor. For more information, see Configuring the Aspect Message Routing Service.

Using the WFM Historical Connector Configuration

If you installed the WFM Historical Connectors, configure the appropriate connector(s) using the WFM Historical Connector Configuration. See Using the WFM Historical Connector Configuration.

Upgrading User Workstations

Upgrade the client software on all user workstations. You can upgrade the client software by:

- Following the procedure provided in this section.
- Using a command line. Upgrading the client with the command line follows the same procedure as installing with the command line. For instructions, see Installing with a Command Line.

Before upgrading the client workstation, ensure that the Oracle database client has been upgraded on the workstation. For instructions see, Installing the Client Software. To verify the required version of the database client, see the *Aspect Workforce™ Release Note*.

If the Microsoft Access Database Engine was installed only for use with Aspect Workforce and is not used outside of Aspect Workforce, we recommend you uninstall it. For instructions, see Uninstalling the Microsoft Access Database Engine (optional).

1. Log in as an administrator to the **user workstation and** launch **Windows Explorer.**
2. Locate and double-click the following **file**, where ***MainAppServer*** is the machine name assigned to your main application server: ***MainAppServer*\WFMSetup\Workforce Management\Setup.exe**

   If any prerequisite software is not already installed on the workstation, then the Aspect Prerequisite Installer window opens, displaying a list of prerequisite but uninstalled software. Click **Install** to install the prerequisite software. When installation is complete, the Welcome window of the **Install Wizard for Workforce** opens.
3. Click **Next**. The **Destination Folder** window opens, displaying the path to the program files. If your previous version was installed at the **C:\Program Files(x86)** path, the location will persist, even though the software is 64-bit.
4. Click **Next**. The **Data Folder** window opens, displaying the path to the data files. If your previous version was installed at the **C:\Program Files(x86)** path, the location will persist, even though the software is 64-bit.
5. Click **Next**. The **Custom Setup** window opens, showing the **User Workstation** icon already selected.
6. Click **Next**. The **Main Application Server** window opens.
7. Verify or type the **machine name** of the main application server and click **Next**. The **DCOM Servers** window opens, displaying the machines names of the servers currently hosting the DCOM services.
8. Click **Next**. Or, if you plan to change the host server for any of these services after the upgrade, type the name of the new server in the corresponding field, and click **Next**. The **Ready to Install** window opens.

9. Click **Install**. After the files are installed, the **Install Wizard Completed** window is displayed.
10. Click **Finish**. If a reboot message is displayed, click **No** in the message, and reboot the server manually after exiting the wizard.

Configuring User System Privileges

If you granted Oracle object privileges for any Aspect Workforce™ database object to any user, those privileges are removed during the upgrade process and are not restored automatically. You must grant any object privileges for any database objects once again.

You can create a script that automatically grants the appropriate privileges. Refer to your Oracle documentation for instructions.

Upgrading Your Sample Database

The sample database is optional. If you don't want to upgrade it, skip this step and continue with Enabling Your Database.

If you added custom objects to your Aspect Workforce™ schema (for example, indexes or constraints), the WFM Database Manager prompts you and then drops them if you choose to proceed. After the upgrade, your Oracle database administrator must add the objects.

To upgrade your sample database:

1. Log in to your main application server.
2. Do the following: Windows Server 2022 or 2025: **Start > Aspect > WFM Database Manager** The **Database Manager** window opens.
3. Follow the instructions for Upgrading the Database, with the following changes:
   a. Substitute the sample database alias—typically WFMSAMPLE—for the main (WFMDATA) database alias.
   b. Log in to the database as **TCS_SAMPLE** with a password of **tcs_sample**.

Enabling Your Database

To enable your database, log in to the database using an administration tool (SQL*Plus, for example) and disable the Oracle restricted session you set up earlier (Restricting Your Database).

To enable the database:

1. Log in to the **database** using a login ID with **SYSDBA** privileges.
2. Disable **restricted sessions** for your Oracle database.
3. Log out of the **database server.**

Enabling Optional Features

After upgrading, you can enable the following optional features:

- Enabling Email Reports
- Running WFM services with non-administrative accounts

Enabling Email Reports

This section applies only if you plan to use the Email Reports feature .

To enable Emailing Reports in WFM for the first time, or to continue to receive emailed reports, you will need to see:

1. Configuring the SMTP Server.
2. If your SMTP server was previously connected via port 465, review for updated requirements.
3. Configuring WFM Notification Queue Manager.
4. Setting Registry Parameters for SMTP.

Running WFM Services with Non-Administrative Accounts

After upgrading, all WFM services are automatically configured to run with local system accounts. But you can increase security on your application servers by configuring any number of WFM services to run with a regular user account.

Post-Upgrade Administrative Tasks

Refer to Post-Installation Administrative Tasks for any additional post-upgrade tasks you might need to complete. The chapter also includes procedures you can use to verify that your upgrade was successful.

Applying Workforce Updates

As technical improvements to the Aspect Workforce™ software occur, it will be necessary to periodically apply updates. For Aspect Workforce™, incremental updates are cumulative. In general, it is best to apply all available updates at the same time, though it is possible to apply updates to individual modules. Updates are obtained and applied under guidance from Aspect Customer Care.

These instructions are provided as a general guideline. Some updates may require specific instructions. Contact Aspect Customer Care for assistance.

In summary, the process is to:

- Perform the Pre-Installation Steps
- Apply Workforce Updates to the Servers and Workstations
- Apply Workforce Database Updates
- Perform the Post-Installtion Steps

Pre-Installation Steps

Before applying the update follow these steps:

1. In general, updates will be provided as a compressed zip file. Copy this file to each server or workstation.
2. Unzip the file.
3. Stop all WFM related services (including RTA) on all application servers.

Apply Workforce Updates to the Servers and Workstations

Follow these steps:

1. In the uncompressed update files, right-click on **Patch.exe** and select Run as Administrator (click **Yes** if prompted). This will open the **Aspect Patch Installer** window.
2. If the update is not appropriate for your version of Workforce, an error message will display. Click **OK** and contact Aspect Customer Care.
3. In the window, the list of locally installed Aspect Workforce™ modules (Workforce, Real-Time Adherence, WFM Advanced Modules, WFM Web Services) that can be updated will be listed and the Action state (*Remove Pending* or *Install Pending*).
   a. If this update has been applied previously, the update installer assumes you want to remove the previously applied update and will mark it as *Remove Pending*.

      If you want to keep the pre-existing updates, right-click the module and select **Disable**. This will change the state to *Disabled*.

   b. If this update has not been applied previously, the module status will be *Install Pending*.
4. Click **Start** to begin the update installation process. There is a step and progress bar at the bottom. Each module's Action state will show *Processing* as the update is being applied, and *Complete* when finished. Click **Cancel** at any time to roll back the update installation to the pre-update state.

If any update does not install properly, it will show an action state of *Failed*. Contact Aspect Customer Care for assistance.

5. Once all modules show *Complete*, Click **Exit** to close the window.
6. Alternately, for WFM and RTA client workstations, you can browse to the following locations and individually execute the Patch.exe remotely (as Administrator) from the Main application server. Substitute servername for the name of the server:
    - WFM Client: *servername*\WFMSetup\Workforce Management\Patch
    - RTA Client: *servername*\RTASetup\Patch

Command Line Installs

Note: If you want to use the command line install to apply updates for the WFM and RTA clients on user workstations, use the following commands.

For WFM

- Command Line with UI (open Command Prompt with elevated privileges): Msiexec /update "<path to wfm.msp>"
- Command Line without UI, e.g. Silent Install (open Command Prompt with elevated privileges)
  Msiexec /update "<path to wfm.msp>" /qb

For RTA

- Command Line with UI (open Command Prompt with elevated privileges) Msiexec /update "<path to rta.msp>"
- Command Line without UI, e.g. Silent Install (open Command Prompt with elevated privileges) Msiexec /update "<path to rta.msp>" /qb

The /qb option will show a progress bar. For no progress bar use /qn instead of /qb.

Apply Workforce Database Updates

Follow these steps to apply any WFM Database updates (if applicable).

Before beginning, be sure to have a current database backup. Any errors encountered while applying scripts may require restoring the database to the most recent backup to diagnose and correct the issue.

Note: If you configured a Windows Account as the WFM owner, either use **Run As different user** when launching DBManager, or login to the server as the database owner's windows account. After which you must select **Log in using Windows Integrated Security** when prompted for a WFM login in DBManager.

Additional Note for Oracle: This should have already been configured, but as a reminder, when defining the Schema name in DBManager, you will need to place the owner account in quotes in this format - "OPS$*domain\username*" where *domain\username* is the WFM schema owner.

On the Main application server:

1. Go to **Start > Aspect > WFM Database Manager** (click Yes if prompted)
2. Highlight the desired database alias in the window.
3. Click **Tools > Apply Code Mod\Hotfix Scripts**.
4. Login as the database owner account (default: TCSDBOWNER)
5. The **Apply Code Mod/Hotfixes** window will appear with a numbered list of scripts to apply.
   a. If there are no Applicable Scripts, it will say <<*No applicable updates found*>>, click **Close**
6. Click **Apply Scripts**.
   a. If any errors are encountered contact Aspect Customer Care for assistance.
7. Once the scripts have been applied, click **OK** and **Close**.
8. Exit the WFM Database Manager.

It is not always possible to easily remove Database related updates. If you require rolling back database updates, contact Aspect Customer Care for assistance.

Post-Installation Steps

Follow these steps after applying updates to the servers and workstations:

1. Restart the WFM Information Server service.
2. Follow any module specific (Perform) Post-Installation steps.
3. Restart all remaining WFM services (including RTA).

Uninstalling Updates

If after applying an update to a module, you decide to remove it, follow the steps below.

1. Aspect does not recommend removing Workforce updates using Window's Control Panel. Utilize Aspect's Patch.exe.
2. It is not always easily possible to remove Database related updates. If you require rolling back database updates, contact Aspect Customer Care for assistance.

Steps:

1. Stop all WFM services.

3. Locate the Patch.exe.
4. Right-click and select **Run as Administrator.**
5. In the window, the list of locally installed Workforce modules will be listed.
6. The update installer assumes you want to remove the previously applied updates and will mark them as *Removal Pending.*
   a. If you want to keep any of the updates, right-click the module and select **Disable**. This will change the state to *Disabled*. That module's update will not be removed.

7. Click **Start** to begin the update removal process. There is a step and progress bar at the bottom. Each module's Action state will show *Processing* as the update is being removed, and *Complete* when finished.

RabbitMQ

RabbitMQ is a message broker allowing asynchronous messaging between publishers and receivers with message acknowledgement. RabbitMQ uses the Advanced Message Queuing Protocol (amqp). RabbitMQ is needed for the Email Reports feature, or if you are utilizing Notification Server or the RealTime Adherence feature in Aspect Workforce™ Engagement Management.

Aspect recommends using Chocolately to install Rabbit MQ.

Installing Chocolatey

Chocolatey is a tool that automates the installation of RabbitMQ and any dependencies. RabbitMQ has dependencies related to Erlang/OTP. Aspect recommends installing RabbitMQ using Chocolatey as the installer will manage any dependency issues.

Note: If you choose to install RabbitMQ and Erlang/OTP manually using the Windows installer, you should be aware that there are dependency issues related to RabbitMQ (RabbitMQ does not currently support all versions of Erlang/OTP.) For a manual installation, you should review the RabbitMQ documentation and the version of RabbitMQ supported by Aspect Workforce. See the *Aspect Workforce Product Release Note, Compatible Server-side Operating Systems and Components.*

To install Chocolatey:

1. Go to https://community.chocolatey.org/
2. Click on the “Install Chocolatey” button.
3. (optional) Subscribe to the Chocolatey Newsletter if you so desire – otherwise skip this step.
4. Review the Requirements and click “Individual”.
5. On the server desktop, open PowerShell as an Administrator.
6. Back at the website click the blue icon at the far right under “Now run the following command” to copy the command. (The pop-up will say “Copied!”)
7. In the PowerShell window, right-click to paste (or press Ctrl-V on your keyboard).
8. Press Enter.
9. If prompted, Type A and press enter.

Chocolatey will be installed once you are returned to the command prompt. Leave the window open to install RabbitMQ.

Installing RabbitMQ using Chocolatey

1. Once Chocolatey has been installed, type the following command in the PowerShell window: `choco install rabbitmq --version=4.1.4`
2. If prompted, type A to run the script.
3. The install is finished when you are returned to a command prompt.
4. Close the PowerShell window.

5. Go to the Windows **Start > RabbitMQ Server > RabbitMQ Command Prompt**.
   - Click Yes if prompted.
6. Run the following commands:
   - rabbitmq-plugins enable rabbitmq_management
   - rabbitmq-plugins enable rabbitmq_shovel
   - rabbitmq-plugins enable rabbitmq_shovel_management
7. Response will indicate that the feature has been enabled.
8. Click on **Start > RabbitMQ Server > RabbitMQ service - stop**.
   - Click Yes if prompted.
9. Click on **Start > RabbitMQ Server > RabbitMQ service – start**.
   - Click Yes if prompted.
10. Go to http://localhost:15672 in a browser.
    - There can sometimes be a delay activating RabbitMQ's administration website after service restart. If it does not immediately appear, wait a few moments, and try again.
11. Login to RabbitMQ
    - Login: guest
    - Password: guest.

Note: Best practice is to create a new administrative account and disable the guest account.

Creating a RabbitMQ Administrator account

It is the best practice to create a new RabbitMQ administrator account and disable the default guest account. This will secure RabbitMQ from outside access.

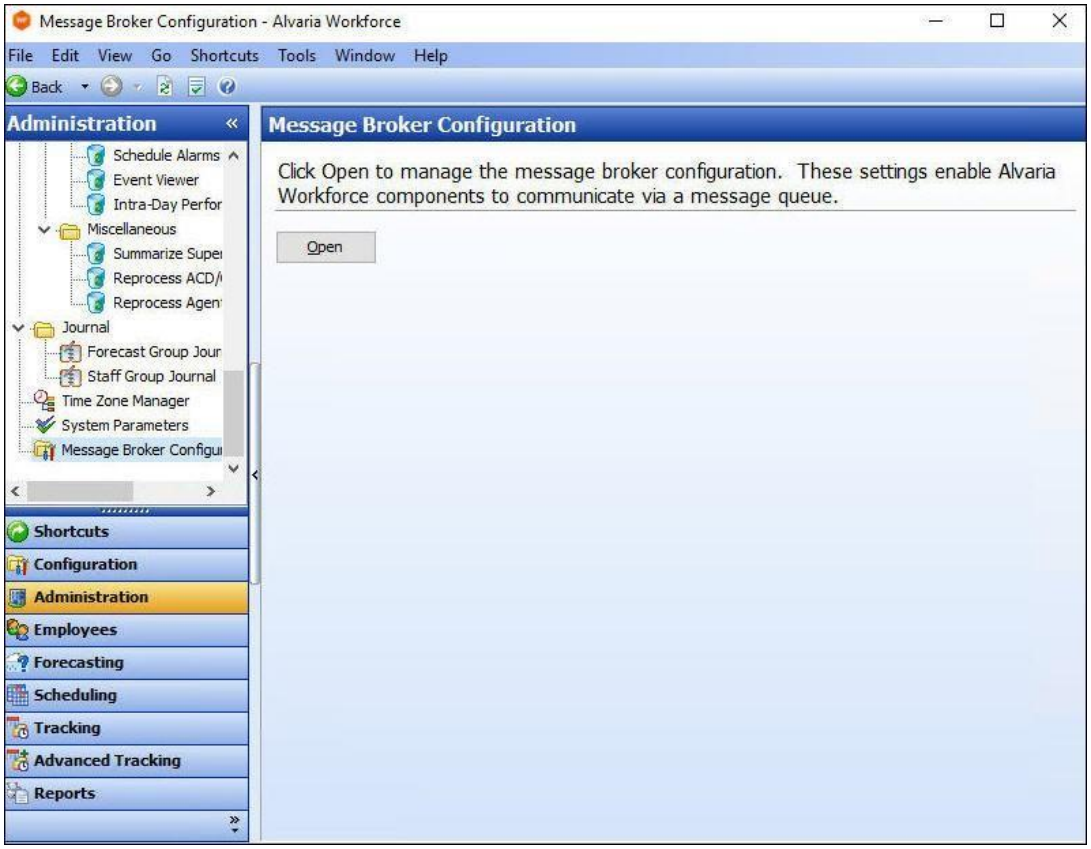
1. In a browser go to http://localhost:15672 .
2. Log in to RabbitMQ (using the guest\guest account).
3. Click on the **Admin** tab.
4. Click on **Add a user** drop-down area.
5. Enter a new username (eg. WFMAdmin).
6. Enter a new password.
7. Confirm the password.
8. Under **Tags** type **admin**.
9. Click Add user.
10. Click on the new user's username in the table.
11. Under Permissions, click Set permission.
12. Logout of RabbitMQ.

Disabling RabbitMQ Guest account

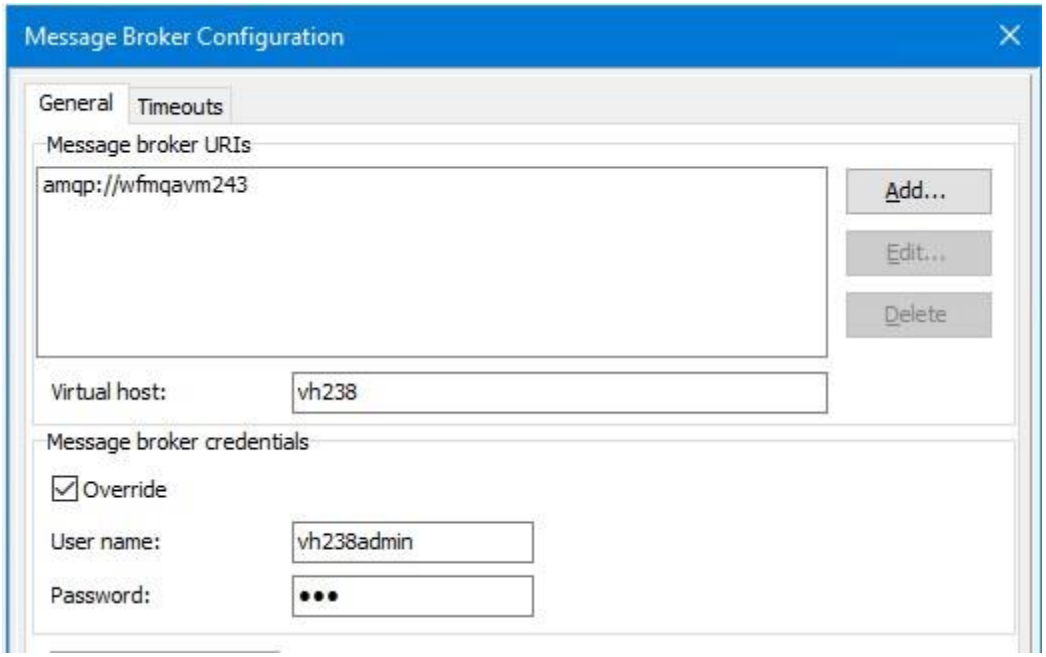
1. In a browser go to HTTP://localhost:15672.
2. Log in as a RabbitMQ administrator (not guest).
3. Click on Admin.
4. Click on the guest username in the table.
5. Scroll down and select Update this user.
6. Remove the administrator from tags.
7. Either enter a new password or the same password and confirm it.
   a. Changing the password will add an additional level of security.
8. Click Update user.
9. Logout of RabbitMQ.

Configuring RabbitMQ for RTA Web

1. On the Workforce Rich Client, go to Administration> **Message Broker Configuration**. In the Message Broker window click **Open.**

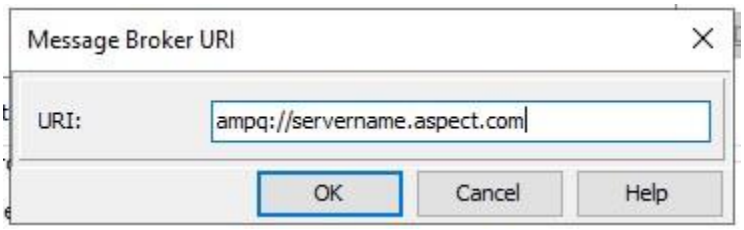


2. The Message Broker Configuration window opens.



3. In the **General** Tab click **Add** to add the URL for RabbitMQ to configure it with the Rich Client. In the Message Broker URI window enter the URL and click **OK.** (for example, amqp://rabbitMQserver.aspect.com). If the **Virtual host** field is left blank, the default (/) will be used.

Note: If TLS encryption is being used, the URI will begin with **`ampqs`**.



4. In the Message Broker credentials section select the check box for **Override** and enter the user name and password of the RabbitMQ administrator added for WFM access (See Creating a RabbitMQ Administrator account).
5. Click the **Test Connection button** to check whether the connection was successful.

Using Virtual Hosts with RabbitMQ

Using virtual hosts with RabbitMQ allows multiple tenans to share one RabbitMQ server.

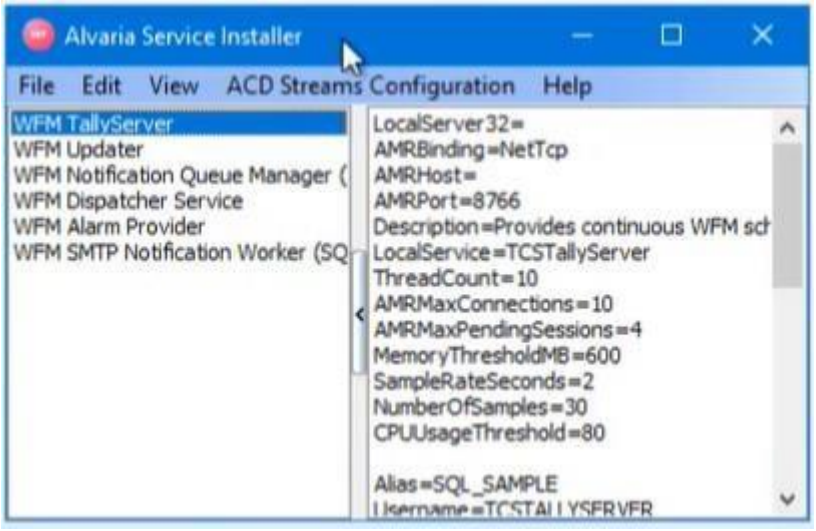
Use RabbitMQ Management to add a virtual host.

1. Go to the **Admin** tab and select the **Virtual Hosts** menu option.
2. To add a new virtual host, expand the Add a new virtual host area. Enter a **Name** (required) and other desired (optional) fields. Click the **Add virtual host** button.
3. The new virtual host will be shown in the table. The assigned user access defaults to the login account used to create the virtual host.

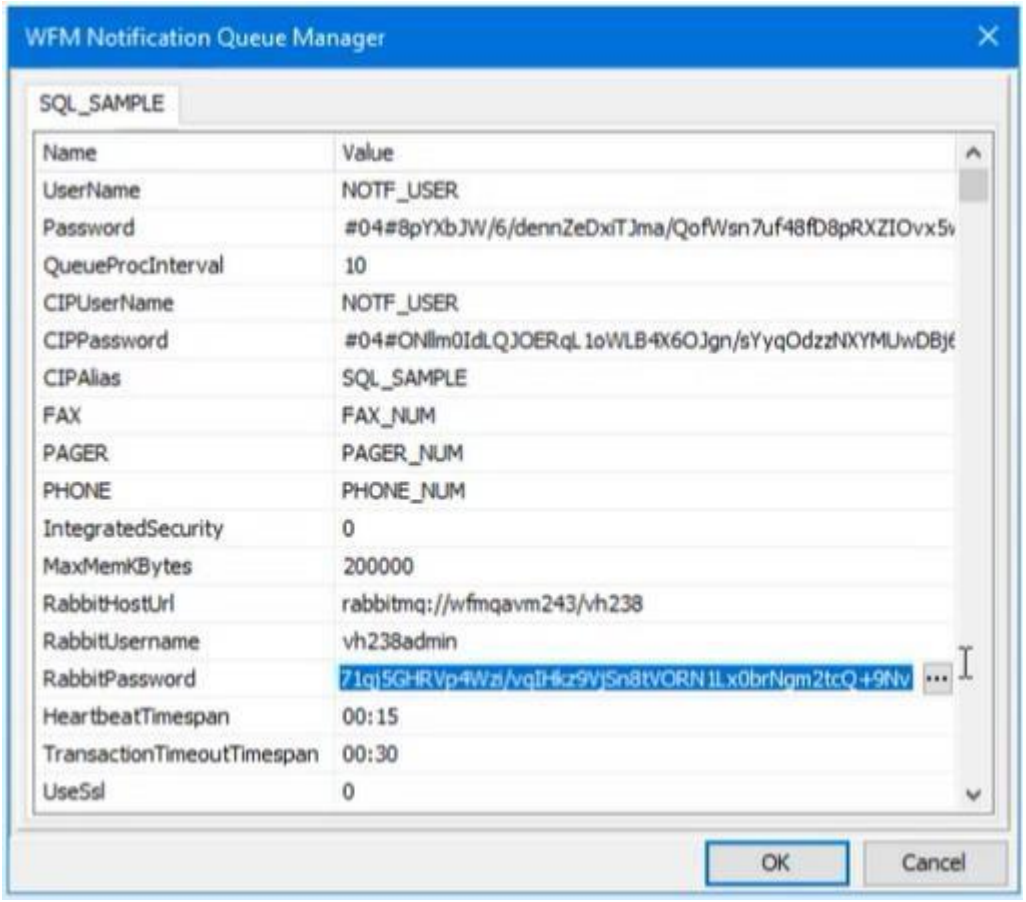
4. If a unique user is desired for each virtual host, follow the instructions in the Creating a RabbitMQ Administrator account, above, then select the virtual host to edit the user permissions.

   Note: / is the default virtual host.

5. On the Workforce server hosting the Notification Queue Manager, open Service Installer.



6. Edit the Notification Queue Manager service, changing the following:



- **RabbitHostUrl=**

rabbitmq://<*rabbitmq_host*>/<*virtual_hostname*> •

RabbitUsername & **RabbitPassword** defined for virtual host

access

7. Save the changes you've made.
8. Restart all the Notification Worker services listed below as they read RabbitMQ connection details from the Notification Queue Manager configuration.

- WFM HTTP Notification Worker
- WFM Mobile Notification Worker
- WFM MultiSite Notification Worker
- WFM SMTP Notification Worker
- WFM Universal Notification Worker

9. The **RabbitMQ Management > Connections** tab will show a separate connection on the virtual host for each running worker service.

Note: Find additional information about RabbitMQ Virtual Hosts here.

Enabling TLS in RabbitMQ

Enabling TLS support in RabbitMQ allows encrypted communication between a client and a server.

There are prerequisites required for enabling TLS:

- A Certificate Authority certificate bundle (a set of certificates it considers to be trusted in a file known as a bundle)
- A certificate (public key) file
- A private key file

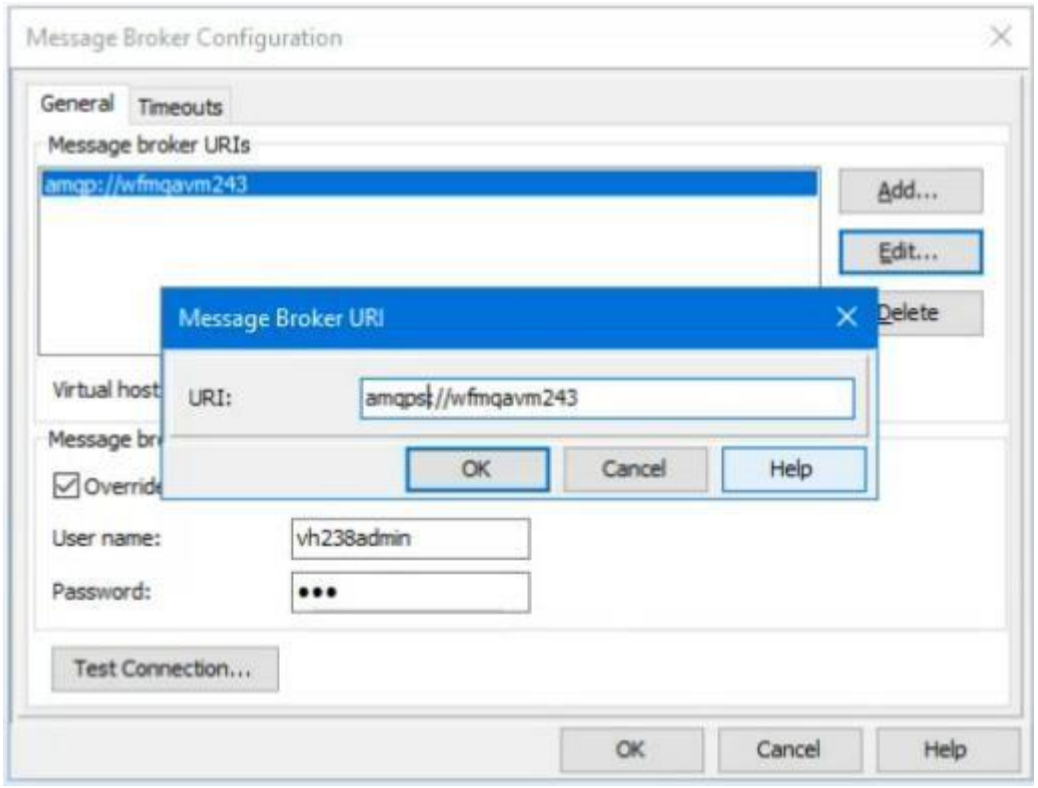
Note: For more information, see Enabling TLS Support in RabbitMQ.

Changes on the RabbitMQ Server

The following changes must be made on the RabbitMQ Server:

1. Copy the CA bundle files to the local file system and make sure it is readable by the effective user of the RabbitMQ node process.
2. Add the CA certificate to the Trusted Root Certification Authorities of the machine where RabbitMQ is running.
3. Update the RabbitMQ configuration (Rabbitmq.conf) with the following changes:

```
listeners.ssl.default = 5671
ssl_options.cacertfile = /path/to/ca_certificate.pem
ssl_options.certfile = /path/to/server_certificate.pem
```




```
ssl_options.keyfile = /path/to/server_key.pem
ssl_options.versions.1 = tlsv1.2
```

The location of the file varies by installation. Refer to RabbitMQ Configuration for configuration file location.

Changes on the Workforce Application Servers

On each of the Workforce servers that connect to RabbitMQ, insure the following:

- The required security protocol must be TLS 1.2.
- The CA certificate for the RabbitMQ server must be added to the Trusted Root Certification Authorities of each machine that connects to RabbitMQ.
- For RTA Web, use the Workforce Rich Client to edit the Message Broker Configuration:

1. The Message Broker Configuration must include an **s** for secure transport: `amqps://wfmqavm243`

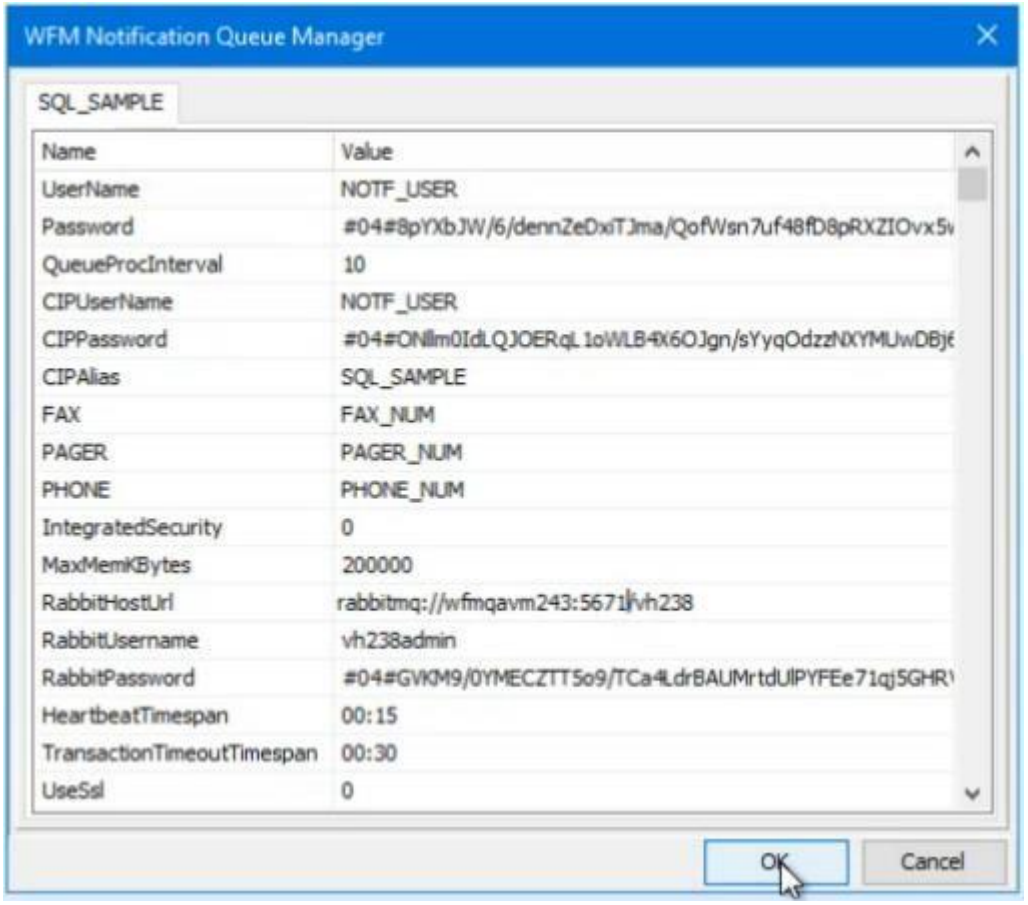
Note: The Message Broker Configuration “Test Connection” should be used to verify the encrypted connection between the WFM application server hosting services that connect to RabbitMQ. This can be used for both RTA-Web services using Message Broker Configuration and Notification services which do not use Message Broker Configuration.

2. The following dependent services must be restarted for the configuration to be recognized:

- RTA Listen

- IIS (for RTA in Workforce Engagement Management)

For Notification-related services, open the WFM Service installer, then open the WFM Notification Queue Manager to configure it to use TLS:



1. Update the RabbitHostURL parameter:

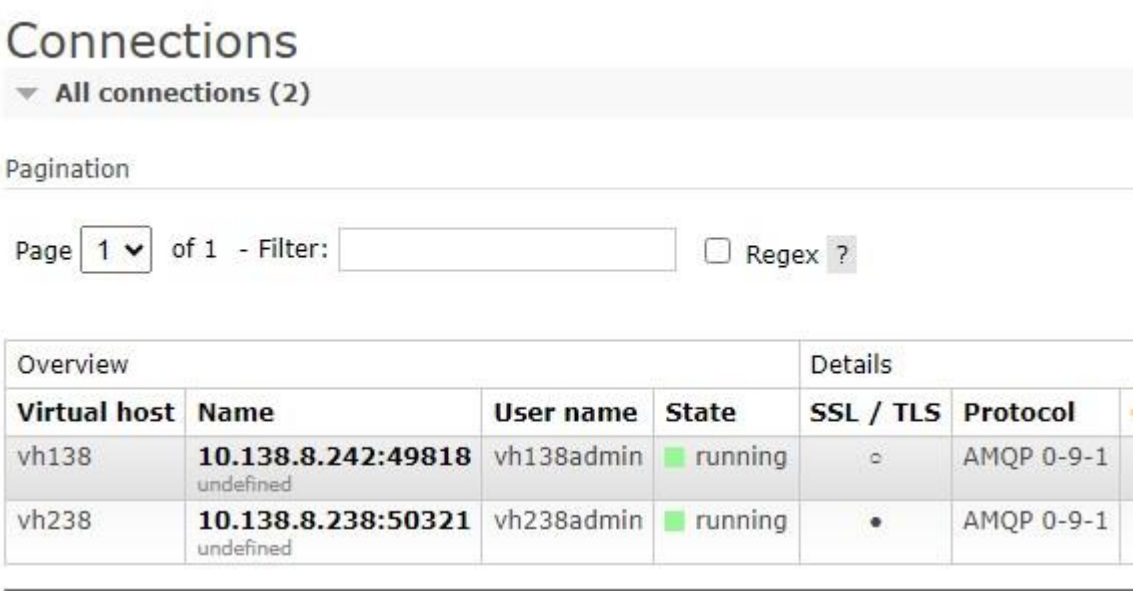
- **If not using TLS:** rabbitmq://RabbitServer
- **If using TLS:** rabbitmq://RabbitServer:5671

2. The port configured must match the SSL listener port in the RabbitMQ configuration file.
3. Restart all the Notification Worker services listed below as they read RabbitMQ connection details from the Notification Queue Manager configuration.

- WFM HTTP Notification Worker
- WFM Mobile Notification Worker
- WFM MultiSite Notification Worker
- WFM SMTP Notification Worker
- WFM Universal Notification Worker

Validating the TLS Connection

To validate that the connection to TLS is enabled, on the RabbitMQ server, view the connections in RabbitMQ Management. Any connections that are using encrypted communication will have a solid dot in the SSL/TLS column:



Upgrading RabbitMQ

To upgrade RabbitMQ, choose the option below that matches your upgrade scenario:

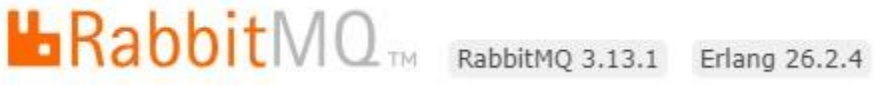
- If you have a single node installation and are planning an incremental upgrade, follow the instructions in Single Node Installation With Incremental Upgrade.
- If you have a cluster installation, follow the instructions for upgrading multiple nodes at the RabbitMQ website.
- If your planned upgrade jumps multiple release series (for example from 3.9.x to 3.13.x), follow the instructions in the RabbitMQ Version Upgradability section at the RabbitMQ website.

Caution: This process will delete all data in RabbitMQ (definitions and messages). The definitions can be preserved using export/import.

Single Node Installation with Incremental Upgrade

1. Determine which version of RabbitMQ and Erlang OTP are currently in place.

   Tip: Find those versions at the header after logging in as an administrator:

2. Decide on the version to which you plan to upgrade.
3. Verify version compatibilities between RabbitMQ and Erlang at https://www.rabbitmq.com/docs/whicherlang.
4. Download all required versions as per your upgrade path.
5. In a browser go to HTTP://localhost:15672.

6. Log in as a RabbitMQ administrator.
7. On the **Overview** tab, go to the **Export definitions** section.
8. Click on **Download broker definitions** and store them in a convenient location.
9. On the **Admin** tab, click on **Feature Flags**.
10. Verify all feature flags have been enabled prior to upgrading RabbitMQ by clicking **Enable** in the **State** column.

Installation Steps

1. Launch the RabbitMQ setup file.
2. A dialog box displays stating that RabbitMQ is already installed will be displayed. Click OK.
3. Follow the installation wizard steps as usual, selecting the components to install that you would normally install.
4. Post-installation, verify that you can access RabbitMQ via the browser.
5. Check and enable all feature flags as in the section above.
6. Continue with the Erlang upgrade.
7. Repeat all steps for each incremental upgrade.

Erlang Upgrade

1. Launch the installer and install the new version.
2. After the upgrade is complete, check RabbitMQ access again.

Fallback

If there are post-upgrade errors that cannot be fixed, follow the steps below:

1. Uninstall both RabbitMQ and Erlang OTP.
2. Install both the latest version of Erlang OTP and RabbitMQ.
3. Verify that the necessary plugins are enabled: rabbitmq_management, rabbitmq_shovel, and rabbitmq_shovel_management.
4. In a browser go to HTTP://localhost:15672
5. Verify if settings persisted.
6. If necessary, import the backed-up broker definitions.
    a. On the **Overview** tab, go to the **Import definitions** section.
    b. Click **Choose File** and select your previously exported configuration.
    c. Click Upload broker definitions.
    d. RabbitMQ asks before upgrade; click **OK**.

e. The message Your definitions were imported successfully should appear.

Troubleshooting

RabbitMQ Won't Start

1. Open RabbitMQ Command Prompt (via the **Start** menu).
2. Run the following commands to re-install the Windows service:
   a. rabbitmq-service remove
   b. rabbitmq-service install
   c. rabbitmq-service start

RabbitMQ Shows Wrong Version of Erlang after Upgrade of Erlang:

1. Check if RabbitMQ can be restarted (if not, follow the steps in RabbitMQ Won't Start.)
2. After a service restart, the version number should be correct.

Post-installation Recommendations for RabbitMQ

Aspect strongly recommends the following:

1. If using RTA Web, create a separate RabbitMQ administrator account such as **RTAWebUser.** For more information, see Creating a RabbitMQ Administrator account.
2. If configuring any type of notification, create a separate RabbitMQ administrator account such as **WFMNSUser.** For more information, see Creating a RabbitMQ Administrator account.
3. Use complex passwords to keep them secure. For more information, see Creating a RabbitMQ Administrator account.
4. Disable the RabbitMQ guest account. For more information, see Disabling RabbitMQ Guest account.
5. Depending on your firewall settings, the following ports need to be available for the RabbitMQ server: 5671, 5672, and 15672.

Appendix A. Installation Checklists

This appendix contains checklists to complete before you install Aspect Workforce™.

SQL Server Environment Checklist

When you install Aspect Workforce™ for SQL Server, you enter the configuration information listed in the table below. For quick reference, have this completed checklist on hand during installation.

☐	Determine the machine names for the Aspect Workforce™ application server and database server. These are the names the machines use to identify themselves on your network. You might also need to know, depending on your ACD interface configuration, the machine name assigned to ACDs: main application server _____ database server_____ secondary application servers _____ ACDs _____
☐	Using the Email Reports feature requires configuration of a physical SMTP server. Write the IP address of the SMTP server, a valid account name (such as name@domain.com) and the password for that account. IP address of the SMTP server _____ Account Name (Username) _____ Password _____
☐	In most cases, at least one Aspect Workforce™ system service will require a network login ID. This can be a domain login ID or a local login ID. If you do not want to use the default password for the system services, specify a different one: Services logon name — Default password — Password to use TCSSERVICES — tcsservices — _____ **Note:** It is recommended that customers using Integrated Security for WFM service accounts should use different accounts for each service, as opposed to one domain account for all services.

☐	All Aspect Workforce™ users require a database login name and password. You will create the following users during the installation process. If you do not want to use the default passwords for database access, specify the ones you prefer to use. You can also change the logon names if you wish. Logon name — Default password — Password to use TCS_SAMPLE — tcssample — _____ TCSADMIN — qqq — _____

	TCSTALLYSERVER	tcstallyserver	_____
	TCSUPDATER	tcsupdater	_____
	TCSACDPROC	tcsacdproc	_____
	TCSAPPROC	tcsapproc	_____
	TCSAUTORUN	tcsautorun	_____
	TCSCHECKER	tcschecker	_____
	WFMFSMONITOR	wfmfsmonitor	_____
	WFMEXPORTER	wfmexporter	_____
	WFMIMPORTER	wfmimporter	_____
	NOTF_USER	qqq	_____
	WFMDISPATCHER	wfmdispatcher	_____
	RTALISTEN	rtalisten	_____
	WFMALARMPROVIDER	wfmalarmprovider	_____
	WFMSEGEXPORTDBMON	wfmsegexportdbmon	_____
	WFMSEGEXPORT	wfmsegexport	_____
	WFMCSMONITOR	wfmcsmonitor	_____
	WFMEXPRESSCHECKER	wfmexpresschecker	_____
☐	Note that, in addition to user names and passwords, all Aspect Workforce™ users and processes must have standard security roles in your database. Depending on the level of security you desire, these may be *application* roles (more secure) or *database roles* (less secure). In this release, the installation script—executed in SQL Server Management Studio—does not grant database roles directly to users. Instead, the script grants application roles to users.		

☐	In most cases, use the default installation path for the Aspect Workforce™ software: **C:\Program Files\Alvaria\Workforce**. If you cannot use this path (for example, if you need to place the files on a different hard disk), specify the one you will use: Path to use: _____

☐	Determine the number of ACD streams you will need. See the *Aspect Workforce™ Planning Guide* for details. Number of streams: _____
☐	Determine the amount of free disk space you want to maintain on the application server. Since the WFM Listen system service copies an ACD report to the application server disk drive approximately every 30 minutes, the amount of space used by ACD files can grow quickly. WFM Listen will stop copying files to the disk drive if your specified minimum is reached: Default minimum Desired minimum 20 MB _____
☐	Determine the number of days you want Aspect Workforce™ to store raw ACD data files after they have been processed and added to your database: Default archive limit Desired archive limit 7 days _____
☐	For each stream you plan to have, you must specify a stream ID and path. Typically, the stream ID is a two-digit number. For example: Stream ID 01 or 02. Specify a path to the ACD data files. Use a UNC path unless the files are stored on your application server. For example: **\\Aspect_MIS\WFMRpts\Stream01\ACD01.ITF**. Use **C:\<*path*>\<*filename*>** if the files are on the application server. Use a Comment to help you associate the stream with its Stream ID. For example: Tucson CallCenter ACD. Stream ID Comment Path _____ _____ _____ _____ _____ _____ _____ _____ _____

	_____ _____ _____
☐	For each stream you plan to have, determine whether the stream will provide data for another instance of Aspect Workforce™ that is running concurrently (such as an instance on a lab server or on a server in a multitenant installation). For each such stream, you must tell the Aspect Workforce™ wizard where the data for the other version will be stored. If the storage point is the application server, use **C:\<*path*>\<*filename*>**. Otherwise, use a UNC path. Stream ID Output file path _____ _____ _____ _____ _____ _____ _____ _____

Oracle Environment Checklist

When you install Aspect Workforce™ for Oracle, you enter the configuration information listed in the table below. For quick reference, have a completed checklist on hand during installation.

☐	Determine the machine names for the Aspect Workforce™ application servers and the TNSNAME for Oracle. You might also need to know, depending on your ACD interface configuration, the machine name assigned to ACDs: main application server _____ database server _____ secondary application servers _____ TNSNAME for Oracle _____ ACDs _____
☐	Using the Email Reports feature requires configuration of a physical SMTP server. Write the IP address of the SMTP server, a valid account name (such as name@domain.com) and the password for that account. IP address of the SMTP server _____ Account Name (Username) _____ Password _____

☐	In most cases, at least one Aspect Workforce™ system service will require a network login ID. This can be a domain login ID or a local login ID. If you don't want to use the default password for the system services, specify a different one: Services logon name — Default password — Password to use TCSSERVICES — tcsservices — _____ It is recommended that customers using Integrated Security for WFM service accounts should use different accounts for each service, as opposed to one domain account for all services.
☐	All Aspect Workforce™ users require a database login name and password. You will create the following users during the installation process. If you do not want to use the default passwords for database access, specify the ones you prefer to use. You can also change the logon names if you wish. Logon name — Default password — Password to use TCSDBOWNER — tcsdbowner — _____ TCS_SAMPLE — tcssample — _____ TCSADMIN — qqq — _____ TCSTALLYSERVER — tcstallyserver — _____ TCSUPDATER — tcsupdater — _____ TCSACDPROC — tcsacdproc — _____ TCSAPPROC — tcsapproc — _____ TCSAUTORUN — tcsautorun — _____ TCSCHECKER — tcschecker — _____ WFMFSMONITOR — wfmfsmonitor — _____ WFMEXPORTER — wfmexporter — _____ WFMIMPORTER — wfmimporter — _____ NOTF_USER — qqq — _____ WFMDISPATCHER — wfmdispatcher — _____

	RTALISTEN	rtalisten	_____
	WFMALARMPROVIDER	wfmalarmprovider	_____
	WFMSEGEXPORTDBMON	wfmsegexportdbmon	_____
	WFMSEGEXPORT	wfmsegexport	_____
	WFMCSMONITOR	wfmcsmonitor	_____
	WFMEXPRESSCHECKER	wfmexpresschecker	_____

☐ In addition to user names and passwords, all Aspect Workforce™ users and processes must be assigned an Oracle role. You will create the following roles, with passwords, during the installation process. If you don't want to use the default password for these roles, specify the passwords you will use instead:

Role	Default password	Password to user
TCS_CLIENT	tcs_client	_____
TCS_UPDATER	tcs_updater	_____

☐ In most cases, use the default installation path for the Aspect Workforce™ software: **C:\Program Files\Alvaria\Workforce**. If you cannot use this path (for example, if you need to place the files on a different hard disk), specify the path you will use instead: Path to use: _____

☐ Determine the number of ACD streams you will need. See the *Aspect Workforce™ Planning Guide* for details.

Number of streams: _____

☐ Determine the amount of free disk space you want to maintain on the application server. Since the WFM Listen system service copies an ACD report to the application server disk drive approximately every 30 minutes, the amount of space used by ACD files can grow quickly. WFM Listen will stop copying files to the disk drive if your specified minimum is reached:

Default minimum	Desired minimum
20 MB	_____

☐	Determine the number of days you want Aspect Workforce™ to store raw ACD data files after they have been processed and added to your database: Default archive limit Desired archive limit 7 days _____
☐	For each stream you plan to have, you must specify a stream ID and path. Typically, the stream ID is a two-digit number. For example: Stream ID 01 or 02. Specify a path to the ACD data files. Use a UNC path unless the files are stored on your application server. For example: **\\Aspect_MIS\WFMRpts\Stream01\ACD01.ITF**. Use **C:\<*path*>\<*filename*>** if the files are on the application server. Use a Comment to help you associate the stream with its Stream ID. For example: Tucson CallCenter ACD. Stream ID Comment Path _____ _____ _____ _____ _____ _____ _____ _____ _____ _____ _____ _____
☐	For each stream you plan to have, determine whether the stream will provide data for another instance of Aspect Workforce™ that is running concurrently (such as an instance on a lab server or on a server in a multitenant installation). For each such stream, you must tell the Aspect Workforce™ wizard where the data for the other version will be stored. If the storage point is the application server, use **C:\<*path*>\<*filename*>**. Otherwise, use a UNC path. Stream ID Output file path _____ _____ _____ _____ _____ _____ _____ _____

Appendix B. **File Installation Paths**

Aspect Workforce™ delivers both 32-bit and 64-bit files. The location of the files depends on the installation path you select when installing Aspect Workforce™.

The following tables give further details regarding where files are delivered.

Location of 64-Bit Files

The following table displays where the 64-bit files are delivered:

Type	Specified Installation Directory	Location of 64-bit files	
		Program Files	Common Files
Default Path	C:\Program Files\Alvaria\Workforce	C:\Program Files\Alvaria\Workforce	C:\Program Files\ Common Files\ Alvaria Shared
Non-default path within C:\Program Files	C:\Program Files\WFM	C:\Program Files\WFM	
Non-default Path on C:	C:\Apps\WFM\	C:\Apps\WFM\	
Non-default path on E:	E:\Apps\WFM\	E:\Apps\WFM\	
Upgrade with default path	C:\Program Files \Aspect\Workforce	C:\Program Files \Aspect\Workforce	
Upgrade with nondefault path	E:\Apps\WFM\	E:\Apps\WFM\	

Location of 32-Bit Files

The following table displays where the 32-bit files are delivered:

Type	Specified Installation	Location of 32-bit files

	Directory	Program Files	Common Files
Default Path	C:\Program Files\Alvaria\Workforce	C:\Program Files (x86) \Alvaria\Workforce	C:\Program Files (x86)\ Common Files\ Alvaria Shared
Non-default path within C:\Program Files	C:\Program Files\WFM	C:\Program Files (x86) \WFM	
Non-default Path on C:	C:\Apps\WFM\	C:\Apps\WFM\Bin32	
Non-default path on E:	E:\Apps\WFM\	E:\Apps\WFM\Bin32	
Upgrade with default path	C:\Program Files (x86) \Aspect\Workforce	C:\Program Files (x86) \Aspect\Workforce	
Upgrade with nondefault path	E:\Apps\WFM\	E:\Apps\WFM\Bin32	

Appendix C. **Security Segregation for User Management**

This section highlights the security perspective by segregating the rights for business users from IT staff.

The Workforce rich client can be run in some special modes when launched with the command-line switch options described below. These options are intended to be used together, and enable:

- One group of users, who should be WFM Admin users, to create, edit and delete WFM users while preventing access to other WFM functions.
- Second group of users, who can be WFM Admin, Regular, or Employee users, to be unable to create users, delete users, or edit a small set of user fields (name; alternative name; security profile, filter profiles, and seat filter profiles; active flag; user type; employee; secondary login ID; secondary

password) but will be able to fully use other WFM functions as governed by their WFM User Type, and Security and Filter profiles.

To take advantage of this capability:

- The first group of users should be given a shortcut that launches tcs.exe with the /OnlyUserAdmin command-line switch. If the /OnlyUserAdmin command-line switch is present, the WFM client will hide all modules other than the Users module.
- The second group of users should be given a shortcut that launches tcs.exe with the /NoUserAdmin command-line switch. If the /NoUserAdmin command-line switch is present, the Users module will disable access to most of the features of that module.

Appendix D. IIS Logging

This section provides a cursory overview of IIS and describes the basic settings that are often changed for Aspect Customer Care troubleshooting.

Brief Overview of IIS

IIS contains modules that perform functions for both the application and Web server roles in Window Server. The modules handle the duties of listening for server requests, managing processes, and reading configuration files.The modules contain protocol listeners, services (World Wide Web Publishing Service, for example), and Windows Process Activation Service (WAS). Modules also autheticate client credentials and manage cache activity.

The latest IIS architecture provides the ability to control the modules of IIS that you want on your servers and allow you to customer a server to a specific role in your environment. The native modules of the current IIS architecture include the following:

- HTTP Modules
- Security Modules
- Content Modules
- Compression Modules
- Caching Modules
- Logging and Diagnostics Modules
- Managed Support Modules

The focus of this appendix is on logging. For more general information about IIS, see Microsoft's IIS documentation.

Logging Overview

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 are mentioned in this section. 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.

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 recommended to set the minlevel value to:

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

All other settings can be left at the default settings.

Workforce Engagement Management - 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 recommended to set the minlevel value to:

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

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, which describes optional IIS Role Services, the roles services indicated by a greenshaded cell are not required.

Category / Role Service	When Selecting Application Server > Web Server

Common HTTP Features

Category / Role Service		When Selecting Application Server > Web Server
	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
Security		
	Request Filtering	Default
Category / Role Service		**When Selecting Application Server > Web Server**
	Basic Authentication	Default[4]

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

	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

Category / Role Service		When Selecting Application Server > Web Server
	ISAPI Filters	Default
	Server Side Includes	
	WebSocket Protocol[5]	Required
FTP Server		

[5] Note that while **NOT** required for logging, the WebSocket Protocol is a **requirement** and is necessary for Workforce Engagement Management RTA functionality.

	FTP Service	
	FTP Extensibility	
Management Tools		
	IIS Management Console	Default
	IIS 6 Management Compatibility	
	IIS Management Scripts and Tools	Default
	Management Service	

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-driven WEM software designed to foster worklife balance while maximizing ROI for businesses. For more details, visit www.aspect.com