sopheon

Sopheon Accolade®

Installation Guide

Version: 17.1

About Sopheon Accolade®

Document Name:	Installation Guide
Document Version:	1
Software Version:	Sopheon Accolade 17.1
Document Date:	November 2024

Ownership of Software and Documentation

The Sopheon® software described in this documentation is furnished under a license agreement and may be used only in accordance with the terms of that license agreement.

Sopheon Corporation and its associated Sopheon Group companies, including its subsidiaries, its immediate holding company and its ultimate holding company (together, "Sopheon") have created and own all rights to the software and documentation. Licensees of the software have purchased a limited right to use the software in accordance with their license agreement.

Copyright Notice

Trademarks

No Warranty

The technical documentation is being delivered to you AS-IS, and Sopheon makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Sopheon reserves the right to make changes without prior notice. In no circumstances will Sopheon, its agents or employees be liable for any special, consequential or indirect loss or damage arising from any use of or reliance on any materials in this documentation or in the software.

Patents

Aspects of Sopheon software are protected by U.S. Patents 5634051, 6632251, and 6526404; European Patent EP0914637; and by U.K. Patent GB2341252A.

Contents

About this Guide

Welcome to the *Sopheon Accolade Installation Guide*. This guide contains instructions for installing, configuring, and upgrading Accolade, which includes Accolade Process Manager™, Accolade Portfolio Center, and Accolade Innovation Planning.

Who Should Read This Guide

You should read this guide if you are installing Accolade. This guide assumes you are familiar with Accolade and setting up and administrating databases, including the following:

- Accolade, its procedures, and concepts
- Internet Information Services (IIS) administration
- Database administration
- Security administration
- Domain administration
- Windows Firewall administration

Contents of This Guide

This guide describes how to install, upgrade, and configure Accolade and is divided into the following chapters:

- Chapter 1 - Provides an overview of Accolade configurations and resources needed for installation.
- Chapter 2 - Describes how to create the Accolade databases.
- Chapter 3 - Describes how to install and configure Accolade.
- Chapter 4 - Describes how to configure users' client computers for Accolade.
- Chapter 5 - Describes how to upgrade Accolade to the current version.
- Chapter 6 - Describes how to log on to Accolade and recommends other sources of information about Accolade.
- Appendix A - Describes how to enable and configure the MSDTC service.
- Appendix B - Provides information about installing Accolade in a server farm for load balancing.
- Appendix C - Contains the list of roles, role services, and features that should be installed on the application server.
- Appendix D - Contains instructions for database management tasks.
- Appendix E - Contains additional information about secure network practices for Accolade.
- Appendix F - Contains the list of Accolade parameters with their descriptions.

Font Conventions

- This **bold font** is used for important words and the names of the items you need to identify.

Create a SQL account named “Geneva”, and give this account the **VS_Write** database role.

- `This fixed-width font` is used for examples of code, paths, and URLS.

  `https//:your-server-name:port-number/`

- *This italic font* is used for document names.
- *An italic font* enclosed in brackets shows what information is displayed in this location when the information is changeable, rather than fixed.

  Process Document - Smart Excel <*version*>.xlt

- Blue text indicates a cross-reference link that you can click to take you to that location.

Icon Conventions

 - Indicates a section with Sopheon best practices for system setup.

 - Indicates a tip to assist with Accolade configuration or management.

- Indicates an example use case to assist with component configuration.

Important! This is an important statement. Read it carefully before proceeding with an action.

Contacting Technical Publications

To send comments and suggestions regarding this document, send email to techpubs@sopheon.com.

Chapter 1

Installation Overview

This guide describes the process of installing or upgrading Accolade and refers to files as located in the “installation software.” The installation software is the set of files in **Accolade_ v17.1.x_Installation.zip** that is available from Sopheon. In addition, the file **Accolade_ v17.1.x_Documentation.zip** contains Accolade user documentation. File names within these folders include the version number, such as 17.1 for minor releases or 17.1.1 for point release.

Important! *Do not* copy server names, user names, or any other content from screen shots in this installation guide. Correct content is described in the document text.

Roles Required for Accolade Installation

A single individual can perform the Accolade installation, or it can require three different people with different expertise and different rights to components on your system.

- **Domain Administrator** - The domain administrator creates Accolade users, user groups, and perhaps service accounts on the domain.
- **Database Administrator** - The database administrator creates the Accolade databases. This person needs administrator rights on the database server and a login with the fixed server roles of **sysadmin** and **public** and English as the default language on the SQL Server instance. See "Installing the Accolade Databases" on page 15.
- **Application Administrator** - The application administrator installs and configures the Accolade application. This person needs administrator rights on the application server. See "Installing the Accolade Application Software" on page 93.

Required User Accounts for Accolade Users

Accolade may require end user accounts on the domain for the employees who use Accolade and optional service accounts.

The domain administrator can create service accounts for the following:

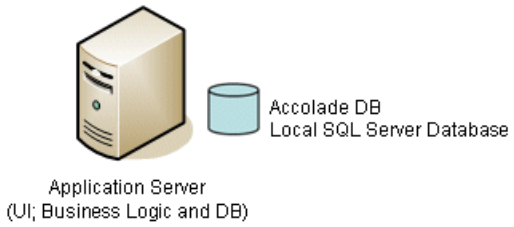
- A domain account for an SQL Server login if Accolade is installed with Windows authentication for its database connection.

  An existing domain account can be used because this account does not need to be reserved for this use or to have a special name. Sopheon recommends that you create this login domain account with a strong password that never expires. To allow passwords to expire, the account's password must be updated using the Database Configuration page within the Accolade Administration Console. See "Configuring Accolade" on page 30.
- A second account is needed for the service account that manages the automatic upload of reference tables within Accolade. This account is associated with the Accolade user assigned the Service Account role in Accolade. See "Enabling Automatic Upload of Reference Tables" on page 59.

Typical Accolade Server Configurations

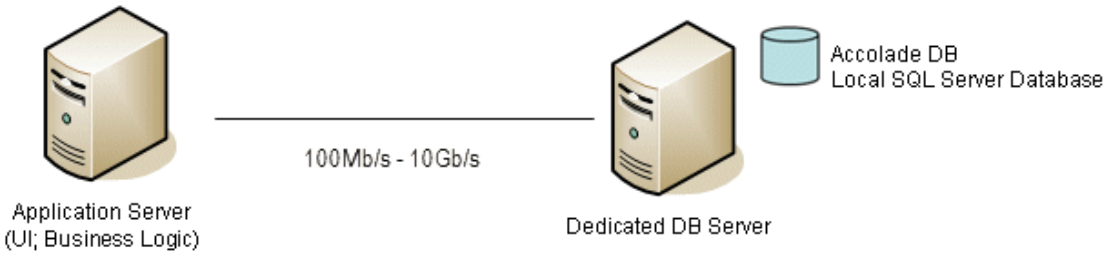
This section describes two typical Accolade server configurations. These illustrations show server configurations for Accolade only. If Dashboards for Accolade is also installed in your implementation, an additional server is required for that application.

Configuration 1 - Single Server



In the simplest configuration, the Accolade database is stored on the application/Web server.

Configuration 2 - Separate Database Server



A larger database might require a configuration in which the database is stored on a separate server, either a dedicated server or a multi-database server.

Chapter 2

Installing the Accolade Databases

This chapter describes how to install the Accolade databases. Accolade requires a primary database, usually named Accolade, a database for snapshots, and at least one database for Accolade Portfolio Optimizer scenarios if running Portfolio Optimizer.

Installing the Accolade databases requires that you complete the following:

1. Review and ensure that your system meets the database requirements.
2. Create the Accolade database, the snapshots database, and one or more scenarios databases.
3. Create the Accolade database login.

Important! If your installation requires a load balancing configuration, review the information in "Load Balancing - High Availability" on page 109 before continuing.

Database Prerequisites

Important! Before beginning the Accolade database installation, review the requirements in the *Sopheon Accolade v17.1 Software and Hardware Requirements* document to ensure your system meets the requirements.

To configure the prerequisites and to install and configure the Accolade application, you must be an administrator on the application server. Also ensure the following options are set:

- SQL Server's **Full Text Search** is installed and enabled on the database server. Ensure that the service **SQL Full-text Filter Daemon Launcher (MSSQLSERVER)** is started and that its **Startup Type** is set to **Automatic**.
- The Accolade, snapshots, and scenarios database have the same owner. The owner must be a **SQL login** with the **sysadmin** and **public** server roles and **English** set as the default language.

  Sopheon recommends that this login's domain account have a strong password that never expires. However, if you want to allow passwords to expire, you must periodically change the account's password using the Database Configuration settings in the Accolade Administration Console.

Enabling Support for Documents

Accolade searches text contained in Microsoft Office and HTML documents as well as text files and online forms. If you need to index other file formats such as PDFs or MSG (email) files, contact Sopheon Customer Support.

If Accolade users upload any documents with Microsoft file formats, you must install MS Office IFilters to enable text search in Accolade. Install the versions of IFilter that are appropriate for the database server's operating system.

Note: Accolade can search for the name of any document without the need for an IFilter.

To install the filter pack to enable Microsoft Office document support:

1. Browse to the installation software in **Accolade_v17.1.x_Installation.zip**, and open the following folder:

   `Server Installation (Database)\MS Office Support.`

2. Open the 64-bit or 32-bit folder and run the two files that are appropriate for your database server version.

Server Version	Files
64-bit server	Run both of the following in the order listed:

Server Version	Files
	• FilterPackx64.exe • FilterPack64bit.exe
32-bit server	Run both of the following in the order listed: • FilterPackx86.exe • FilterPack32bit.exe

If a secondary window flashes, displaying and immediately disappearing, when you run a FilterPack file, IFilter is already installed.

3. After installing both filter packs for your database version, install the service packs and updated filter packs available in the following locations. Run both packs even if you are running a different Microsoft Office version.
   - **Office 2010 Filter Pack SP2** - https://support.microsoft.com/en-us/kb/2687447.
   - **Update for Microsoft Filter Pack 2.0** - https://support.microsoft.com/en-us/kb/2881026.
4. From SQL Management Studio, run both of the following scripts:
   - EXEC SP_FULLTEXT_SERVICE 'load_os_resources', 1
   - EXEC SP_FULLTEXT_SERVICE 'verify_signature', 0
5. Restart the database.

Creating the Accolade Databases

Accolade uses the following databases:

- **Accolade** - The main database that contains most of the data created and stored in Accolade.
- **Snapshots** - A secondary database that stores snapshots of metrics, matrices, project metadata, and resource data.
- **Scenarios** - One or more work databases that improve performance for concurrent users of Portfolio Optimizer. No backups are needed for this database.

The databases can be installed on the same computer as the Accolade application, or they can be on a separate computer.

The instructions in this section are valid for all supported versions of SQL Server.

To create the databases, log on to the SQL Server instance with a login that is the fixed server role of **sysadmin** (as well as the **public** role, which is assigned by default) and ensure the login has **English** selected in the **Default language** list. This login is mapped to the database owner with the **db_owner** and **public** role memberships for each database. Creating the databases requires the following:

- Creating the Accolade and snapshots databases.
- Creating Accolade and snapshots database schemas.
- Creating and configuring the scenarios databases.
- Creating the scenarios database schemas.

Each of these steps is described in detail in the sections below.

Creating the Accolade and Snapshots Databases

1. Using **SQL Server Management Studio**, create a new SQL Server database for Accolade. Name the database to identify its purpose, for example, Accolade.
2. On the **General** page of the New Database window, ensure that the **Use full text indexing** check box is selected.

   Initial size and autogrowth values depend on Sopheon's technical requirements analysis of your implementation.
3. Click **Options**.
4. In the **Compatibility level** field, select one of the below options. Sopheon recommends matching this with the SQL version being used.
   - **SQL Server 2019 (150)**
   - **SQL Server 2022 (160)**
5. Set the following options:
   - **Auto Update Statistics Asynchronously** to **True**.
   - **Default Cursor** to **LOCAL**.
6. Create the database.
7. Repeat step 1 to create the snapshots database.

   The snapshots database name must begin with the name of the main database and must use the following format: *<main database name>*_Snapshots

   For example, Accolade_Snapshots.
8. Select the same owner and the same options for the snapshots database as for the Accolade database.

Creating Accolade and Snapshot Database Schemas

1. In **SQL Server Management Studio**, browse to the installation software and open the following folder:

   ```
   Server Installation (Database)\Database Scripts\Create.
   ```
2. Select the Accolade database and run the **Accolade v17.1- Main - Create.sql** script.
3. Select the snapshots database and run the **Accolade v17.1-Snapshots - Create.sql** script.

Creating the Scenarios Databases

Important! You must create at least one scenarios database even if your company does not use Portfolio Optimizer. If you need to increase the number of scenarios databases after Accolade is installed but without upgrading Accolade, stop Accolade (including IIS, the Autoloader Service, and the Time Tasked Service) prior to completing the procedure below.

To create the scenarios databases:

1. Browse to the installation software and open the following folder:

   `Server Installation (Database)\Database Scripts\Create.`

2. To specify the number and size of the scenarios databases, edit the script **Accolade v17.1 - Scenario - Create Database.sql** script.

3. Scroll down to a block of SET statements containing the following variables and enter the value you want. Each variable applies to all scenarios databases.

   Sopheon recommends that you create one scenarios database for each expected concurrent user of Portfolio Optimizer.

Variable	Description	Default Value
@NumDBs	Number of databases to create The number of concurrent databases you select does not limit the actual number of concurrent users of Portfolio Optimizer.	1
@MDFFileGrowth	Autogrowth for MDF (master data) files	50 MB
@MDFFileSize	Initial size of MDF files	1 GB
@LDFFileGrowth	Autogrowth for LDF (log) files	50 MB
@LDFFileSize	Initial size of LDF files	500 MB

   Values for the File variables default to MB if units are not specified. Add GB to specify a size in gigabytes.

4. Run the script on the Accolade database to create the scenarios databases.

   The new databases are named <*main database name*>_Scenarios_<*number*>.

   For example: Accolade_Scenarios_3

5. Browse to the installation software and open the following folder:

   `Server Installation (Database)\Database Scripts\Other Scripts`

6. Run **Prepare Restored Database Script.sql** on each of the new scenarios databases and refresh the SSMS.

   Replace <NewDBOwner> with the name of the owner of the Accolade and snapshots databases.

7. Browse to the installation software and open the following folder:

   `Server Installation (Database)\Database Scripts\Create`

8. Run the **Accolade v17.1 - Scenario - Create.sql** script on each of the scenarios databases.
9. If you stopped the Accolade prior to starting this procedure, restart the application server, including IIS, the Autoloader Service, and the Time Tasked Service.

Creating the Accolade Database Login

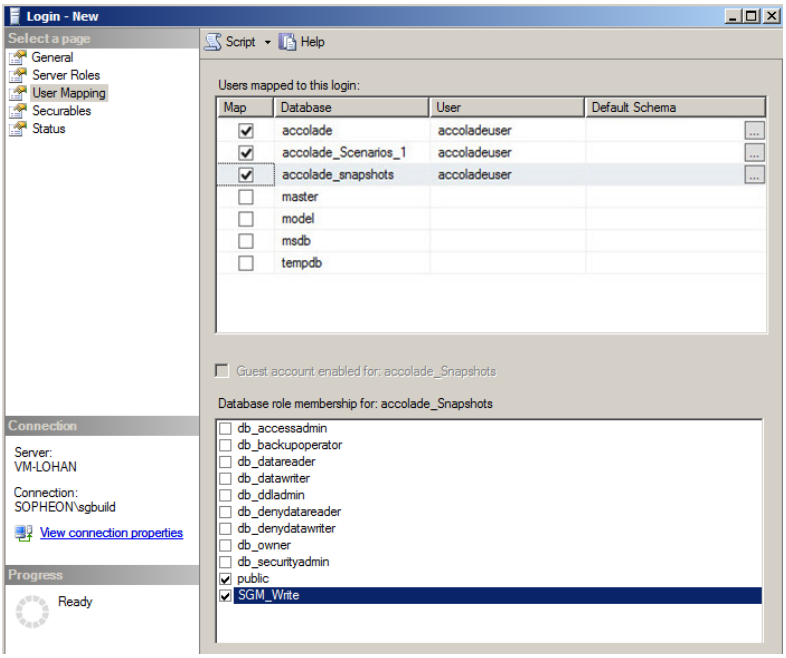
Create the Accolade login for the Accolade, snapshots, and scenarios databases.

1. In **SQL Server Management Studio**, expand the **Security** folder.
2. Right-click the **Logins** folder and select **New Login** to display the New Login dialog box.
3. Do one of the following to create a login using either Windows authentication SQL Server authentication:

Authentication Type	Steps
Windows Authentication	1. In the **Login name** field, enter the domain login account's name. 2. Select the **Windows authentication** option. 3. In **Default database** field, select the Accolade database. 4. In **Default language** field, select **English**. 5. In the **Select a page** list on the left, select **User Mapping**. 6. Select the Accolade database, ensure that the **public** role is selected and select the **SGM_Write** role. 7. Map the login to the snapshots and scenarios databases with the same roles.
SQL Server Authentication	1. In the **Login name** field, enter the domain login account's name. 2. Select the **SQL Server authentication** option. 3. Enter and confirm the login's password. Note the name and password to use later in configuring the application server. See "Configuring Accolade" on page 30. 4. In the **Default database** field, select the Accolade database. 5. In **Default language** field, select **English**.

Authentication Type	Steps
	6. In the **Select a page** list on the left, select **User Mapping**. 7. Select the Accolade database, ensure that the **public** role is selected, and select the **SGM_Write** role. 8. Map the login to the snapshots and scenarios databases with the same roles.

Note: If you set up the Accolade database login using Windows Authentication, you must add a user login to the database for each user added to the following Windows services: Time Task Service, Autoloader Service, and Active Directory Service. Add individual user logins to the database after adding them to the appropriate Windows service.



You have completed the installation of this database. To continue the installation, proceed to the next chapter.

Chapter 3

Installing the Accolade Application

This chapter describes the installation and configuration of the Accolade application. The Accolade installation is divided into the following general steps:

1. Install the prerequisites on the application server.
2. Install the Accolade application on the application server.
3. Configure Accolade with the Accolade Administration Console.

If your network configuration sets the Network Service to not have access across the network, also refer to "Secure Network Best Practices" on page 126.

Important! If your installation requires a load balancing configuration, review the information in "Load Balancing - High Availability" on page 109 before continuing.

Reinforcing Security

Complete the following steps to strengthen security when installing or upgrading Accolade.

- Enable Secure Socket (TLS) on the Accolade main website. See "Enabling Secure Sockets" on page 62.
- Configure Distributed Cache server passwords. See "Setting Up Distributed Cache Servers " on page 40
- Set the Accolade application pools to use a domain user. See "Secure Network Best Practices" on page 126.
- Implement Windows Groups for added security. See "Running the Initial Configuration Wizard" on page 30.
- Configure Accolade application website timeout via the timeout system parameters. See "Timeouts" on page 149.
- Encrypt SQL Server connection between the application server and database. Force the encryption flag in the SQL Server Configuration Manager.
- Accolade requires that TLS 1.2 is enabled on both the client and the server.

Application Server Prerequisites and Installation

Before beginning the Accolade installation, complete the following prerequisites in the order listed below. Additional details about installing these prerequisites are provided in the sections below. See the *Sopheon Accolade v17.1 Software and Hardware Requirements* document for a full list of the hardware and software required for the application server. To configure the prerequisites and to install and configure the Accolade application, you must be an administrator on the application server.

Note: Sopheon recommends that you disable the virus protection software on the application server while you are installing and configuring Accolade, its prerequisites, or components.

Installing Windows Roles, Services, and Features

On the application server, install the following roles and features for Web Server (IIS).

The complete list of roles and roles services on the application server is shown in "Application Server Roles, Role Services, and Features" on page 117.

To Install Windows server roles, services, and features on Windows Server 2022:

1. In **Administrative Tools**, open **Server Manager**.
2. In the **Dashboard's Quick Start** menu, click **Add roles and features**.
3. If shown the **Before You Begin** page, click **Next.**

4. On the **Installation Type** page, select **Role-based or feature-based installation**, and click **Next**.
5. On the **Server Selection** page, select **Server Selection**, ensure the correct server is selected and click **Next** to proceed to **Server Roles**.
6. On the **Select Server Roles** page, select the **Web Server (IIS)** role and accept all its default settings.
7. Under **Web Server (IIS)**, expand the **Web Server (IIS) > Management Tools** and select **IIS Management Compatibility** and ensure the following options are also selected:
   - IIS Metabase Compatibility
   - IIS Management Console
   - IIS Scripting Tools
   - IIS WMI Compatibility
6. Also under **Web Server (IIS)** page, enable the following additional **Web Server (IIS)** services:
   - Web Server > Common HTTP Features > HTTP Redirection
   - Web Server > Health Diagnostics > Logging Tools

     If SMTP Server is set, also check OBDC Logging.
   - Web Server > Performance > Dynamic Content Compression
   - Web Server > Security

     Select the appropriate options based on your security configuration.

   Note: Ensure that all Web Server (IIS) roles listed under "Roles and Services in Windows Server 2022" on page 117 are enabled.

7. On the **Select Features** page, select the **.NET Framework 4.8 Features**, expand it and **WCF Services**, and select the following:
   - **.NET Framework 4.8** - .NET Framework 4.8 is installed by default with Windows Server 2022.

     Accolade may require a different version of .NET Framework be installed. See the *SopheonAccolade v17.1 Software and Hardware Requirements* document for a full list of the hardware and software required for the server.

   - **HTTP Activation**
   - **Message Queuing Activation**
   - **Named Pipe Activation**
   - **TCP Activation**

- **TCP Activation**
- **TCP Port Sharing**

8. Also on the **Select Features** page, select **Management OData IIS Extension**.

   Note: Ensure that all Features listed under "Roles and Services in Windows Server 2022" on page 117 are enabled.

9. Click **Next**, confirm that all needed roles, role services, and features are selected, and click **Install**.
10. After the installation finishes, confirm that all the installations succeeded and click **Close**.

To Install Windows server roles, services, and features on Windows Server 2019:

1. In **Administrative Tools**, open **Server Manager**.
2. In the **Dashboard's Quick Start** menu, click **Add roles and features**.
3. In the console tree, select **Server Selection**, ensure the correct server is selected, and select **Server Roles**.
4. On the **Select Server Roles** page, select the **Web Server (IIS)** role and accept all its default settings.
5. On the **Web Server (IIS)** page, expand the **Web Server (IIS) > Management Tools** and select **IIS Management Compatibility** and ensure the following options are also selected:
   - IIS Metabase Compatibility
   - IIS Management Console
   - IIS Scripting Tools
   - IIS WMI Compatibility
6. Also on the **Web Server (IIS)** page, enable the following additional **Web Server (IIS)** services:
   - Web Server > Common HTTP Features > HTTP Redirection
   - Web Server > Health Diagnostics > Logging Tools

     If SMTP Server is set, also check OBDC Logging.
   - Web Server > Performance > Dynamic Content Compression
   - Web Server > Security

     Select the appropriate options based on your security configuration.
7. On the **Select Features** page, select the **.NET Framework 4.7 Features**, expand it and **WCF Services**, and select the following:
   - **.NET Framework 4.7** - .NET Framework 4.7 is installed by default with Windows Server 2019.

Accolade may require a different version of .NET Framework be installed. See the *Sopheon Accolade v17.1 Software and Hardware Requirements* document for a full list of the hardware and software required for the server.

- **HTTP Activation**
- **Message Queuing Activation**
- **Named Pipe Activation**
- **TCP Activation**
- **TCP Activation**
- **TCP Port Sharing**

8. Also on the **Select Features** page, select **Management OData IIS Extension**.
9. Click **Next**, confirm that all needed roles, role services, and features are selected, and click **Install**.
10. After the installation finishes, confirm that all the installations succeeded and click **Close**.

Important! If the SecurityProtocol value is greater than your TLS, verify your operating system registry has the latest enabled. If this option is not available for your operating system, run Windows updates and update the registry keys to enable the latest TLS.

Browser Tab Limitations on Non-HTTP/2 Servers

When using Accolade on servers without HTTP/2 enabled, users may experience limits on the number of browser tabs that can be opened simultaneously. This is due to browser restrictions on concurrent server calls. Depending on the content of the tabs, Accolade may become unresponsive with as few as 2 to 5 open tabs. Pages with high server interaction contribute to this issue.

To avoid these limitations, ensure the server hosting Accolade supports HTTP/2.

Installing the ASP.NET Core Runtime and ASP.NET Core Module (ANCM) for IIS

Downloading and installing the ASP.NET Core Module (ANCM) and the ASP.NET Core Runtime for .NET 8.0 is a prerequisite for the application server. The Hosting Bundle for .NET 8.0 contains both the ASP.NET Core Runtime as the ASP.NET Core Module. Refer to Microsoft's technical documentation for install Hosting Bundler for .NET 8.0.

Installing .NET Framework

See the *Sopheon Accolade v17.1 Software and Hardware Requirements* document for the .NET Framework version required for the Accolade installation.

Important! .NET Framework must be installed *after* roles, services, and features to ensure proper configuration of IIS. If the server already has .NET installed when you install the roles, install .NET Framework again after the roles are installed.

Installing Windows Important Updates

Ensure that all Windows important updates have been installed on the application server and reboot the server.

Enabling IIS Compression

Dynamic compression speeds data transfer between the server and client machines.

1. In **Administrative Tools**, open **Internet Information Services (IIS) Manager**.
2. In the **Connections** pane, click <*server name*>.

   Compression must be set at the server level.
3. In the server's **Home** page, double-click **Compression**.

   Ensure that both the **Enable dynamic content compression** and **Enable static content compression** check boxes are selected.
4. If you have changed any settings, click **Apply** in the **Actions** pane.

Selecting English US as the Application Server Language

1. In the Windows **Control Panel**, open the **Region and Language** dialog box.

   In Windows 7 and later, select to view the Control Panel by icons and select Region.
2. In the **Format** drop-down list, select **English (United States)**.
3. Click the **Administrative** tab.
4. In the **Language for non-Unicode programs** section, click **Change system locale**, select **English (United States)**, and click **OK**.
5. On the **Administrative** tab, click **Copy settings**.

   This step and the next step configure the Network Service account with the correct language setting.
6. Select both the **Default user account** and the **System accounts** check boxes.
7. Click **OK**.

Ensuring there is an NTFS Partition on the Server

Accolade must be installed on an NTFS partition. Format the drive to store NTFS files.

Configuring MSDTC Service Security Settings

If the database server is on a different computer from the application server, you should have already enabled the **Distributed Transaction Coordinator (MSDTC service)** on this server. See "Installing Windows Roles, Services, and Features" on page 24.

Configure the service's security settings to match those on the database server. For details, see "Enabling and Configuring the MSDTC Service" on page 105.

Configuring Accolade User Groups

Whether to create a user group specifically for Accolade users involves a trade-off between security and maintenance cost. While it is not necessary to create either a domain or a local user group specifically for Accolade, doing so provides greater security. The alternatives are to use an existing group, create a group for Accolade users, or even create multiple groups, for example, for separate installations in different divisions.

The following options are most common:

- To minimize system maintenance, you can use an existing user group instead of creating a specific Accolade users group. You could use, for example, a group for the divisions that use Accolade. However, this option provides a reduced level of security.
- Create one user group for all Accolade users. This alternative keeps Accolade security high but requires you to add users to the group when adding users to Accolade

Installing the Accolade Application Software

Note: If your network configuration sets the Network Service to not have access across the network, also see "Secure Network Best Practices" on page 126.

Prior to installing the Accolade application, disable User Account Control (UAC). If your company policy does not allow the disabling of UAC, you must run the installation from the command line.

To install the Accolade application:

1. Browse to the installation software, open the **Server Installation (Application)** folder, and run **Accolade v17.1 Server.msi**.

   If UAC is enabled, open a command prompt and enter the following: `msiexec /i <full path and file name>`.

   The command prompt needs to be launched as a local admin.

   For example: `msiexec /i "c:\install files\server installation\Accolade v17.1 Server.msi"`

2. On the Customer Information page, ensure that the **User Name** and **Organization** information is correct.
3. In the **Serial Number** field, enter the serial number assigned to you.

Serial numbers are case sensitive.

4. On the Destination Folder page, accept the default installation location or browse to a custom location.

   Note the location that you select. You need the location when you configure Accolade.

   The default location is: `C:\Program Files\Sopheon\Accolade\`

5. On the Ready to Install the Program page, click **Install** and wait while the installation completes.
6. On the InstallShield Wizard Complete page, click **Finish**.

   If the Accolade Application installation does not complete, even when run from the command line, navigate to the Local Policy Editor (Local Security Policy > Local policy > Security Options > User Account Control: Run All Administrators in Admin Approval Mode) and set the **User Account Control: Run All Administrators in Admin Approval Mode** setting to **Disabled** and run the installation again.
7. Install the Accolade Cache service:

   1. Browse to the installation software.
   2. Open the Server Installation (Application) folder.
   3. Run "Install_Memurai_as_AccoladeCacheService.ps1".
   4. Verify a service named "Accolade Cache Service" is running.

Continue with the next section to configure Accolade.

Configuring Accolade

Complete the tasks outlined in this section to configure the Accolade application's connection, authentication, timeout settings, initial language settings, and other settings required to run Accolade and its components.

Important! If you change a database, website, or currency setting to reconfigure Accolade after the initial configuration, you must recycle the Accolade website's application pool for the change to take effect.

Running the Initial Configuration Wizard

After Accolade is installed, use the **Configuration Wizard** available in the Accolade Administration Console to run the initial configuration. The initial configuration sets connections to the servers, authentication, website settings, SMTP settings, and administration login information.

Important! For the Administration Console to operate correctly, you must be a domain user with administrative rights on the application server.

If you are a local user with administrative rights on the server instead, you must turn off User Account Control (UAC) on the server while you are using the console.

To run the initial configuration:

1. Open the Accolade Administration Console on the application server.

   The console is available in the **Sopheon** folder in the application server's **Start** menu and displays the **Configuration Wizard** on first use after installing the Accolade application software.

2. On the Database Configuration page, ensure that default values in the **Connection** section are correct for a database named “Accolade” that uses Windows authentication and that is installed on the application server.

   Update the information, if necessary.

   If you set up a load balanced configuration and change the database configuration after setup, the IIS and all Accolade Windows services will need to be restarted on the distributed cache machine for the changes to update. Additionally, the defined cache servers may also need to be disconnected from their previous cache network.

3. In the Authentication section, select the authentication type and enter credentials of the login account selected in "Creating the Accolade Database Login" on page 20.

   - **Windows Authentication** - Enter the name and password of the domain user account selected as the database login.

     For a domain account, enter the name using the format *<domain name>\<account name>.*

   - **SQL Server Authentication** - Enter the Accolade database login’s name and password.

4. If you have set up a load balanced configuration, use the Distributed Cache Configuration page to configure the cache servers and designate their usages. Review the default settings and make changes as necessary for your configuration.

Tab	Description
Cache Servers	Available cache servers are listed by their domain name or IP address along with their port number and local host. To remove a cache server click **Remove** in the server row.
Usages	Application server machine names are listed along with the cache server host:port. To add application servers, click **Click here to add a new row** under the last line. Select the cache server from the dropdown menu which the application server should use for 'get' requests. Click **Apply**.

Tab	Description
	To remove a cache server click **Remove** in the server row under the Remove column.

If an application server is part of a load balanced group and does not have a listing under designated usages, it sends 'get' requests to the master server in the load balance configuration. If the distributed caching configuration is changed, restart all Accolade Windows Services and IIS on all load balanced servers.

5. On the Proxy Configuration page, enter the information needed if you make use of a Proxy Server.

Field	Description
Enabled	Tick the check box if you want to make use of a Proxy Server. When enabled, all outgoing HTTP and WebSocket requests go through the proxy.
Proxy Address	The proxy URI to be used, for example https://proxy.company.com
Use Default Credentials	Specifies whether the default credentials for this host are used to access the web proxy.
Bypass On Local	Specifies whether the proxy is bypassed for local resources. Local resources include the local server (http://localhost, http://loopback, or http://127.0.0.1) and a URI without a period (http://webserver)
Bypass List	Provides a set of regular expressions that describe addresses that do not use a proxy. Each expression should be on a seperate line. For example: server1\.subdomain\.domain\.com$ server1\.subdomain\.domain\.com$

6. On the Website Configuration page, review the default settings and make changes as necessary for your configuration.

Tab	Description
DNS Name	Enter the Web server's fully qualified domain name.
IP Address	Enter the Web server's IP Address or use the *-wildcard to leave it unassigned.
SSL Certificate	Select the SSL certificate to configure the https protocol binding. If a certificate is not selected, the http protocol binding should be used.
Port Number	Enter the Accolade IIS port number. The port number default (80 or 443) is based on the protocol.

Tab	Description
Windows Groups	Windows Groups is used for pages in Accolade that use the transfer directory to display data, such as Charts & Reports, or web services to transfer data, such as Accolade Office Extensions. These rights are restricted to a small number of directories inside the Accolade installation directory. This setting does not control user access or rights to the system, but if not set up properly, pages using the transfer directory will not work correctly. Add the names of Windows users or groups of users who have access to Accolade, plus the following: • Surrogate user that connects to the database. • User accounts required for integrations, such as between Idea Lab and Accolade. • If necessary, domain user for network access. See "Secure Network Best Practices" on page 120.
Main Transfer Folder	If you want to move the document transfer folder to a custom location, browse to the location. The transfer folder must be on the application server. Must be in a different directory than the **Idea Transfer** folder.
Idea Transfer Folder	If you want to move the idea transfer folder to a custom location, browse to the location. The transfer folder must be on the application server and must be in a different directory than the **Main Transfer** folder.
Application Pool User	The Application Pool Identity user that the Accolade Portfolio Optimizer and the main Accolade website will run under. When entering the Identity user for Built-in users, separate with spaces such as **Application Pool Identity, Network Service, Local Service** or **Local System**. If this is blank then the user is set to the Built-in Network Service Application Pool Identity. When using Windows Integrated Authentication for Accolade Database Login, IIS Application Pool Identity must either be a Network Service or the same Windows User as used for the Database Login. When the App Pool User is set with a Windows User, the App Pool's setting **Load User Profile** is set to **True**. Otherwise, it will be set to **False**. For best practices on what Identity user to use, see "Secure Network Best Practices" on page 120.

Tab	Description
App Pool Password	The password for the Application Pool Identity user. This should remain blank if the Application Pool Identity is set to a **Built-in Identity, Application Pool Identity, Network Service, Local Service** or **Local System**.

If you have moved the transfer directories without using the console, make sure that you browse to the new locations on the Website Configuration page and re-apply the website settings.

When making changes to this page in a load balanced configuration, stop the Accolade website in IIS on each application server and every Accolade service not including the Cache Service to ensure the following settings are correctly reloaded when each app server is brought back up.

- Authentication Type.
- Transfer Directory Folders. If you change either of the directory folders, reapply the settings on the Website Configuration page to all application servers in a load balanced configuration to properly apply the security settings to the application server's particular transfer folder.

7. On the Authentication Configuration page, review the default settings for the Service Credentials and make changes as necessary for your configuration.

Field	Description
Task Service User Name	Enter the name of the user to be authenticated. These are the credentials task services use to validate connections Accolade.
Task Service Password	Enter the password of the user to be authenticated. These are the credentials task services use to validate connections to Accolade.

8. Select the Authentication Type.
9. Review the default settings and make changes as necessary for your configuration.

SopheonID

Field	Description
Client ID*	Unique identifier for your registered application. Enter the saved value of the Client ID for the app you registered with the OpenID Provider.
Client Secret*	Required if Accolade is configured as a confidential client. This will use the Hybrid Flow (aka Implicit Flow with Form Post and Authorization Code Flow) to sign in the user.

Field	Description
Region*	The AWS region of the target User Pool, for example: us-east-2
User Pool ID*	The ID of the target User Pool, for example: us-east-2_9mcupUb61
Name Claim Type	The claim type to identify the user's login name. Defaults to: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name if omitted. For example: preferred_username.
Prompt	A space-delimited list of string values that specifies whether the authorization server prompts the user for reauthentication and consent. For example, select_account.
Max Age	Maximum Authentication Age. Specifies the allowable elapsed time since the last time the end-user was actively authenticated by the OpenID Provider. If the elapsed time is greater than this value, the OpenID Provider must attempt to actively re-authenticate the enduser. For example: 3600 (60 minutes).

OpenID Connect

Field	Description
Client ID*	Unique identifier for your registered application. Enter the saved value of the Client ID for the app you registered with the OpenID Provider.
Client Secret*	Required if Accolade is configured as a confidential client. This will use the Hybrid Flow (aka Implicit Flow with Form Post and Authorization Code Flow) to sign in the user.
Authority*	The Authority is the base address for the well-known OpenID configuration document: <Authority>/.well-known/openid-configuration. For example, for Microsoft Entra ID, this might be: https://login.microsoftonline.com/organizations/v2.0/
Name Claim Type	The claim type to identify the user's login name. Defaults to: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name if omitted. For example: preferred_username.
Prompt	A space-delimited list of string values that specifies whether the authorization server prompts the user for reauthentication and consent. For example, select_account.
MaxAge	Maximum Authentication Age. Specifies the allowable elapsed time since the last time the end-user was actively authenticated by the OpenID Provider. If the elapsed time is greater than this value, the OpenID Provider must attempt to actively re-authenticate the end-user. For example: 3600 (60 minutes).
Scopes	Specifies the scopes for which you want to request authorization, which dictates which claims (or user attributes) you want returned. These must be separated by a space. Defaults to ‘openid profile’ if omitted.

Note: The Redirect URI to be configured in the OpenID Provider should have the path '/signin-oidc'. For example: https://<accolade-server>.company.com/signin-oidc.

For customers with legacy requirements for API token requests and as a backwards compatibility measure, the OAuth 2.0 Resource Owner Password Credentials (ROPC) Grant flow can be enabled by selecting 'Yes' for the "Enable ROPC" setting.

If enabled, the following details should be supplied:

Field	Description
Token Endpoint*	The URL of the token endpoint where clients obtain identity and access tokens in exchange for an OAuth 2.0 grant. For example: https://login.microsoftonline.com/organizations/oauth2/v2.0/token
Client ID*	Unique identifier for your registered application. Enter the saved value of the Client ID for the app you registered with the OpenID Provider.
Client Secret	Your application's Client Secret.
Client Assertion	A different form of client_secret, generated using a certificate.
Name Claim Type	The claim type to identify the user's login name. Defaults to: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name if omitted. For example, preferred_username.
Scopes	Specifies the scopes for which you want to request authorization, which dictate which claims (or user attributes) you want returned. These must be separated by a space. Defaults to 'openid profile' if omitted.
Timeout	HTTP Request timeout. Defaults to 00:01:40 (1 minute and 40 seconds) if omitted.

Note: It is mandatory to include a value for either Client Secret or Client Assertion.

WS-Federation

Field	Description
Realm	A securely configured domain to share resources securely. The realm is the uniform resource identifier (URI) of the application. For example: https://<accolade-server>.company.com
Metadata Address*	The WS-Federation identity provider metadata file location. The address to retrieve the WS-Federation metadata, for example: https://<ADFS

Field	Description
	FQDN>/FederationMetadata/200706/FederationMetadata.xml This could also be a local file, for example: file://c:/folder/federationmetadata.xml.
Name Claim Type	The claim type to identify the user's login name. Defaults to: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name if omitted.
Freshness	Indicates the desired maximum age of authentication specified in minutes; if specified as "0" it indicates to re-prompt the user for authentication.
Active Requestor Address	WS-Trust 1.3 endpoint to enable the ROPC grant flow in Accolade. For example: https://<ADFS FQDN>/adfs/services/trust/13/UsernameMixed

Windows

No additional settings are needed for this Authentication Type.

Basic

Field	Description
Realm	A securely configured domain to share resources securely. The realm is the uniform resource identifier (URI) of the application. For example, https://<accolade-server>.company.com
Default Domain	Enter the domain the web server is on.

Note: Different Authentication Providers use cookie names of different lengths and web infrastructure policies may need to be revised to cater for longer cookie names.

10. See the section “Configuring Organization Information” for information on the Organization Information page.

11. On the SMTP Settings page, enter the connection settings for an external (corporate) SMTP server or for the Accolade server if you are not relaying notifications.

    If you plan to send Accolade notifications using the Accolade server instead of through an external relay server, ensure that the SMTP service is installed and configured on the Accolade server according to Microsoft’s instructions.

    If in a load balanced configuration, changes to the SMTP configuration only need to be made on one application server.

Field	Description
Connection Settings	
SMTP Server	Enter the SMTP server's name.
Reply Address	Enter an address to which mis-addressed Accolade emails are forwarded.
Port Number	Enter the SMTP port number. The default is port 25.
Authentication Settings	
Type	Select an authentication type.
User Name	Enter the name of the user that connects to the SMTP server from Accolade. A user is needed only when Windows authentication is selected and the SMTP server is configured to require authentication.
Password	Enter the user's password.
SSL Connection Mode	None: Provided for legacy compatibility. Opportunistic: Elevates the connection to use TLS encryption immediately after reading the greeting and capabilities of the server, but only if the server supports the STARTTLS extension. This is provided as a compatibility option. Forced: Elevates the connection to use TLS encryption immediately after reading the greeting and capabilities of the server. If the server does not support the STARTTLS extension, then the connection will fail. Most secure option.
SMTP SSL Trusted Cert Thumbprint	(Optional) The thumbprint of a the SSL certification used by the SMPT server. Used for troubleshooting connection errors by removing validation against a trusted certificate with a matching thumbprint.

To test the connection, enter an email address you to use to receive a test message and click **Test Settings**.

12. On the Administrator Login page, click **Browse** and enter the domain and name of the initial user to log on to Accolade as the default Administrator user. Use the *<domain name>\<user name>* format.
13. Click **Next**, verify your settings, and click **Finish** to configure Accolade for initial use and close the Configuration Wizard.

    Subsequent settings can be accessed through the console's Navigation pane.

Configuring Organization Information

After completing the Configuration Wizard or when upgrading Accolade to a new version, use the Accolade Administration Console to specify information about your organization, and if applicable, Acclaim Projects integration details.

To set the organization name:

Important! Once a name is entered and saved, the information becomes read only and cannot be changed.

1. If necessary, from the Windows **Start** menu, select the **Sopheon Accolade Administration Console**.
2. In the Navigation pane, select **Organization Information**.
3. In the **Organization Name** field, add the name of your organization.
4. Click **Apply** to save your changes.

To set the Acclaim Projects URL and Integration ID:

Important! This must only be populated if your organization has purchased integration with Acclaim Projects.

1. If necessary, from the Windows **Start** menu, select the **Sopheon Accolade Administration Console**.
2. In the Navigation pane, select **Organization Information**.
3. In the **Integration ID** field, enter your organization's integration ID for Accolade to connect to Acclaim Projects.
4. In the **Acclaim Projects URL** field, enter your organization's fully qualified URL to the Acclaim Projects website.
5. Click **Apply** to save your changes.

Configuring Accolade Parameters

Use the Accolade Administration Console to set system parameters.

To configure an Accolade parameter:

1. If necessary, from the Windows **Start** menu, select the **Sopheon Accolade Administration Console**.
2. In the Navigation pane, select **Standard Parameters**.
3. Select the **Show Advanced** check box if you need to display advanced parameters or to view read-only parameters.

Caution! Advanced parameters are more likely to damage your system if you make an error. Sopheon recommends that you not modify advanced parameters unless you have expert knowledge of Accolade or are directed to do so by a Sopheon Customer Support representative.

4. Click a row in the **Value** column and enter a value to set each parameter that you want to change from its default setting

   The remaining sections in this chapter describe how to use some of the parameters to set items like search language and currency. For descriptions of each parameter and their allowed values, see "Accolade System Parameters" on page 129.

Setting Up Distributed Cache Servers

Configure distributed cache for your organization's application setup and implementation. The distributed cache provides Accolade with a consistent and shared cache, which is accessible to Accolade programs and services running in their own memory spaces, or in load balanced environments. Using this cache improves system performance by reducing the need to query the database server. The cache primarily stores configuration related data such as process model settings and resource strings among other data objects in a serialized format. Follow the appropriate setup instructions for whether your organization is running in a load balanced configuration or a single application server. For information on load balance configurations see "Load Balancing - High Availability" on page 109. Additionally, select to add password protection for the cache server for an additional layer of security.

Important! The cache service installs with a default port of 6379. If you change this port, it is up to your team to maintain that configuration on upgrades.

The distributed cache is shipped with a default max memory usage of 1GB with the following value:

```
maxmemory 1073741824
```

When memory limit is reached, the least recently used cache entries are evicted to make space. If cache performance shows many memory-caused cache evictions, update the max memory value in the memurai.conf file in the Server Installation (Application) directory of the Accolade install media path. Additionally, update the memory for each Cache Service instance and restart the service.

Configuring Distributed Cache for a Single Application Server

If you are configuring distributed cache for a single application server, only one application server hosts the Accolade website, the Accolade Cache Windows Service, and other Accolade Windows Services. Additionally, the cache service only needs to be accessible to programs on the application server.

To configure distributed cache for a single application server:

1. Install the Accolade Cache service:
   1. Browse to the installation software.
   2. Open the Server Installation (Application) folder.

3. Run "Install_Memurai_as_AccoladeCacheService.ps1".
4. Verify a service named "Accolade Cache Service" is running.

2. Open the Administration Console on the application server.
3. On the Distributed Cache Configuration page, ensure there is a single cache server entry in the **Cache Servers** tab.

   If your IT policy *does not* allow applications to make connections via loop back addresses, do the following:

   - Ensure the cache servers are listed with the machine's domain name and the cache service port.
   - Adjust the firewall rules to allow connections from the machine itself.

   If your IT policy *does* allow applications to make connections via loop back addresses, do the following:

   - List the cache server as localhost with the cache service port.
   - Configure the firewall to prevent external access to the port the cache service uses.
4. Set the cache service password to the default value of "password". This can be updated in the next section.
5. Click **Apply** to save your changes.

   Do not specify designated usages on the **Usages** tab.

Setting Up Distributed Cache Server Passwords

In configuring distributed cache, you may choose to add additional protection against access in the event of a firewall failure. You can set cache server passwords to ensure additional security.

Important! As it is designed to be accessed by trusted clients inside trusted environments, the Memurai instance must not be exposed directly to the internet or, in general, to an environment where untrusted clients can directly access the Memurai TCP port or UNIX socket. In these cases, the web application mediates access between Memurai and untrusted clients (the user browsers accessing the web application). When the authorization layer is enabled, Memurai will refuse any query by unauthenticated clients. A client can authenticate itself by sending the AUTH command followed by the password.
The password is set by the system administrator in clear text inside the memurai.conf file. It should be long enough to prevent brute force attacks for two reasons:

- Memurai is very fast at serving queries. Many passwords per second can be tested by an external client.

- The Memurai password is stored in the memurai.conf file and inside the client configuration. Since you do not need to remember it, the password can have a maximum length of 512 characters.

To set cache server passwords:

1. Turn off any running Accolade websites and Windows Services including the cache service.
2. Open the memurai.conf file in the Server Installation (Application) directory of the Accolade install media path.
3. Add the following line to have the service run with a password.

   ```
   requirepass "password"
   ```
4. Restart the Accolade Cache Service.
5. Open the Administration Console and navigate to the Distributed Cache Configuration page.
6. Add the password to the corresponding row of the cache server listing and click **Apply**.
7. Restart the services that you previously turned off and restart the Accolade website.

Configuring Distributed Cache for a Load Balanced Environment

In a standard load balanced configuration, the Cache Service runs on each application server in the configuration, with one server designated as the master server.

When upgrading to new versions of Accolade, save off the memurai.conf files if your organization's IT department made any specific configuration changes. Doing this ensures that configuration settings can be reapplied after upgrade, uninstall, and reinstall. Additionally, you will need to reestablish links between the servers in the load balanced configuration. Do this by navigating to the Distributed Cache page of the Administration Console on one of the servers and clicking **Apply**.

To setup distributed cache for a load balanced configuration:

1. Install the Accolade Cache service on both servers
    1. Browse to the installation software
    2. Open the Server Installation (Application) folder
    3. Run "Install_Memurai_as_AccoladeCacheService.ps1"
    4. Verify a service named "Accolade Cache Service" is running
2. Update memurai.conf to include both machine IP addresses

1. Turn off any running Accolade websites and Windows Services including the cache service.
2. Open the memurai.conf file in the Server Installation (Application) directory of the Accolade install media path.
3. Add the IP address of the other machine at the end of the line with the bind attribute
    1. Ex: bind 127.0.0.1 <current server IP> <other server IP>
4. Restart the Accolade Cache Service.
5. Restart the services that you previously turned off and restart the Accolade website.

3. Open the Administration Console on the application server and navigate to the Distributed Cache Configuration page.
4. Click the **Cache Servers** tab and ensure each application server domain name is listed as the host along with the port the server is running against.
5. Designate one cache server as the master server.
6. Click the **Usages** tab and ensure each application server name is paired correctly with the cache server that exists on that machine.

Example

The machine name is Win2016-01.

The domain name for the machine is testserver01.

The cache service is running with the default configuration against port 6379.

The designated usage row should read Win2016-01 paired with cache server testserver01:6379.

7. Adjust the firewall settings on each application server to allow communication between the master machine's cache service port and every other machine's cache service port.

Enabling Modules and Components

To enable Accolade modules and components that require license keys, enter the license keys that Sopheon provided to you in the appropriate license key parameter at the beginning of the list of parameters.

To enable Dashboards for Accolade, install and configure the Qlik server as described in the corresponding *Dashboards for Accolade Installation Guide*, and enter the licenses that Sopheon provided to you into the Qlik Management Console.

Note: Accolade Process Manager is enabled automatically with the Accolade installation.

Setting Up Microsoft Teams Connection Functionality

To install the Microsoft Teams functionality, you must:

1. Register the application in Microsoft Entra ID
2. Set up Accolade Administration Console settings
3. Apply collaboration integration settings in Accolade as required

---

Important! Setting up Microsoft Teams connection functionality requires a Microsoft Entra ID Administrator who holds the role of either a Global Administrator or, more specifically, an Application Administrator or Cloud Application Administrator.

Note: If the Microsoft Teams Integration is being used on multiple environments (e.g. test and production), you can choose either to add additional Redirect URIs or create separate app registrations.

Registering the Application in Microsoft Entra ID

To allow Accolade's Microsoft Teams Connection Functionality to connect with Microsoft Teams, you must first register and configure the application in Microsoft Entra ID.

Registering the Microsoft Teams Connection Functionality requires the following steps:

1. Register the application.
2. Add permissions for the application.

To register the application in Microsoft Entra ID:

1. Sign into the Microsoft Entra ID Management Portal, and select theMicrosoft Entra ID tenant that you want.
2. Select the **Microsoft Entra ID** service.
3. In the left navigation pane, under **Manage**, select **App registrations**.
4. Select **New registration**.
5. In **Register an application**, enter the following:
    1. Enter an application name of your choice (this name will not display to users).
    2. Under **Supported account types**, select **Accounts in this organizational directory only** to map to Microsoft Entra ID only single-tenant.
    3. In the **Redirect URI (optional)** > **Select a platform** section, select **Single-page application (SPA)**.

4. Enter your Accolade instance URL (https://your.accolade.net/) in the Redirect URI field to the right. The URI must exactly match the Redirect URI configured with the Provider. The URI is usually the public origin of the Accolade server. For example: <https://<accolade-server>.company.com>

6. Click on **Register** to create the application. You will be redirected to the **Overview** page.

   Microsoft Entra assigns a unique Application (client)ID for the application. You will need this value, and possibly the tenant id, when configuring the Microsoft Teams Connection Functionality.

   1. In the Overview page, on the right-hand side, next to **Redirect URIs**, click on the **1 spa** hyperlink. You will be redirected to the **Authentication** page.
   2. In the **Single-page** application area, under the Accolade server URI, click **Add URI**.
   3. In the box which is shown, enter the Accolade server URI together with /blank.htm, for example https://accolade.example.com/blank.htm

   ---

   Important! If the Microsoft Teams Integration is being used on multiple environments (e.g. test and production), you can choose either to add additional Redirect URIs or create separate app registrations.

To configure permission settings for the application:

1. Navigate to the application's **Overview** page.
2. From the left navigation pane, select **API permissions**.
3. Under the **Configured permissions** section, click on **Add a permission**.
4. From the right pane, select **Microsoft Graph**.
5. Click on **Delegated Permissions** and select the following permissions:
   - Channel.Create
   - ChannelMember.Read.All
   - Channel.ReadBasic.All
   - ChannelMessage.Send
   - Group.Read.All
   - TeamMember.ReadWrite.All
   - Team.Create
   - Team.ReadBasic.All
   - TeamsTab.Create

- TeamsTab.ReadWrite.All
- User.Read.All

Note: By default, the API permission for User.Read is configured. This gets overruled by User.Read.All.

6. Click on **Add permissions** to save these settings.
7. Click **Grant admin consent for <your tenant>** to give admin consent for the selected application permissions.

Important! These permissions are delegated permissions, meaning individuals will need the appropriate permissions in MS Teams to carry out the tasks (e.g., creating a team).

Accolade Administration Console Settings

To configure Accolade's Microsoft Teams Connection Functionality, the following changes must be done in the Accolade Administration Console:

1. Open the Accolade Administration Console. From the navigation pane, select **Standard Parameters**.
2. Select **Category Integrations**, and click on the **Show Advanced** check-box.
3. As necessary for your configuration, make the following changes:

Field	Description
MS 365 Application (client) ID	The Application (client) ID of the application registered in Microsoft Entra ID (see above).
MS 365 Directory (tenant) ID	The Directory (tenant) ID of the application registered in Microsoft Entra ID (see above). The tenant ID can be a GUID (the ID of your Microsoft Entra ID instance), for single-tenant applications, or a domain name associated with your Microsoft Entra ID instance (also for single-tenant applications) Placeholders can also be used as a tenant ID in place of the Microsoft Entra ID authority audience enumeration: • *Organizations* for a multitenant application • *Consumers* to sign in users only with their personal accounts • *Common* to sign in users with their work and school accounts or their personal Microsoft accounts Default: organizations

Field	Description
MS 365 Prompt Type	Specifies how the user should be prompted to authenticate. The prompt parameter can be used to make sure that the End-User is still present for the current session or to bring attention to the request. Space delimited, case sensitive list of ASCII string values that specifies whether the End-User is prompted for reauthentication and consent. Defined values are: • **none** - Do not display any authentication or consent user interface pages. An error is returned if an End-User is not already authenticated or the Client does not have pre-configured consent for the requested Claims or does not fulfill other conditions for processing the request. Cannot be used in combination with other values. • **login** - Prompt the End-User for reauthentication. If it cannot reauthenticate the End-User, an error is returned. • **consent** - Prompt the End-User for consent before returning information to the Client. If it cannot obtain consent, an error is returned. • **select_account** - Prompt the End-User to select a user account. This enables an End-User who has multiple accounts to select amongst the multiple accounts that they might have current sessions for. If an account selection choice made by the End-User cannot be obtained, an error is returned. Default: select_account
MS 365 Domain Hint	Domain hints are directives that are included in the authentication request from an application. They can be used to accelerate the user to their federated IdP sign-in page. Or they can be used by a multi-tenant application to accelerate the user straight to the branded Microsoft Entra ID sign-in page for their tenant. If included, leads to a more streamlined user experience. An example of a domain hint would be a domain name such as sopheon.com. Default: empty.
MS 365	The default URI Scheme to use for the MS Teams integration.

Field	Description
URI Scheme	This indicates the user experience when transitioning between Accolade and MS Teams. 0 = use the launcher (the Microsoft intermediate step which allows the user to select whether to use the MS Teams App or the web app), 1 = msteams scheme (use the MS Teams app), 2 = https scheme (use the web app). Default: 1

Note: The other settings under the Integration Category are for other integrations.

4. Click **Apply** to save your changes.

Important! After setting up the Accolade Administration Console, ensure that you apply the required Microsoft Teams collaboration integration settings in Accolade to enable the functionality:

- Connect Accolade Project to Teams Channel
- Create New Channel for Project
- Create New Team for Project

Setting Up Integration to Microsoft 365 Word, PowerPoint, and Excel Applications with OneDrive and MS Teams

Accolade's integration to the web versions of Microsoft 365 Word, PowerPoint and Excel share settings with the Microsoft Teams Connection Functionality described in the previous section.

If you are using both integrations, follow the steps under Setting Up Microsoft Teams Connection Functionality, then see Setting Up Microsoft 365 Integration After Microsoft Teams.

If you are only setting up the integration to the web versions of the Word, PowerPoint and Excel, see Setting Up Microsoft 365 Integration Only.

Setting Up Microsoft 365 Integration After Microsoft Teams

To configure permission settings for the application:

1. Navigate to the application's **Overview** page.
2. From the left navigation pane, select **API permissions**.

3. Under the **Configured permissions** section, click on **Add a permission**.
4. From the right pane, select **Microsoft Graph API**.
5. Click on **Application Permissions**, and select the following delegated permissions:
    - Files.ReadWrite
6. Click on **Add permissions** to save these settings.
7. Click **Grant admin consent** to give admin consent for the selected application permissions.

To configure the integration to web versions of Microsoft 365 Word, PowerPoint and Excel with OneDrive and/or MS Teams:

1. Open the **Accolade Administration Console**.
2. From the navigation pane, select **Standard Parameters**.
3. Select **Category Integrations**, and click on the **Show Advanced** check-box.

4. As necessary for your configuration, make the following changes:

Field	Description
MS 365 Default Download Mode	The default download mode when users download a document from Accolade (can be overridden in each user's preferences). 0 = Prompt, 1 = Download locally, 2 = Download to OneDrive, 3 = Download to MS Teams if a channel is connected, otherwise locally, 4 = Download to MS Teams if a channel is connected, otherwise to OneDrive Default: 1
Integration with OneDrive	Enable (1) or disable (0) the ability to download documents to OneDrive. Default = 0
Integration with MS Teams Files	Enable (1) or disable (0) the ability to download documents to MS Teams. Default = 0
MS Teams Channel Files Folder	The folder name used in connected MS Teams Channels and under which Accolade project files will be downloaded in subfolders. Primarily applicable in situations where multiple Accolade servers share the same MS Teams environment. Avoid invalid characters in the MS Teams file path. Max. 64 characters. Can be left empty. Default: empty

5. Click on **Apply** to save your changes.

After setting up the Accolade Administration Console, ensure that you apply the Microsoft 365 integration option in Accolade to enable the functionality:

- Integrate with OneDrive
- Integrate with MS Teams Files

Setting Up Microsoft 365 Integration Only

To integrate the web versions of Microsoft 365 Word, PowerPoint and Excel, you must register the application in Microsoft Entra ID. In addition, you will need to deploy 3 add-ins.

Registering the integration to web versions of Microsoft 365 apps requires the following steps:

1. Register the application.
2. Add permissions for the application.

To register the application in Microsoft Entra ID:

1. Sign into the Microsoft Entra ID Management Portal, and select theMicrosoft Entra ID tenant that you want.
2. Select the **Microsoft Entra ID** service.
3. In the left navigation pane, under **Manage**, select **App registrations**.
4. Select **New registration**.
5. In **Register an application**, enter the following:
    1. Enter an application name of your choice (this name will not display to users).
    2. Under **Supported account types**, select **Accounts in this organizational directory only** to map to Microsoft Entra ID only single-tenant.
    3. In the **Redirect URI (optional)** > **Select a platform** section, select **Single-page application (SPA)**.
    4. Enter your Accolade instance URL (https://your.accolade.net/) in the Redirect URI field to the right. The URI must exactly match the Redirect URI configured with the Provider. The URI is usually the public origin of the Accolade server. For example: <https://<accolade-server>.company.com>
6. Click on **Register** to create the application. You will be redirected to the **Overview** page.

    Microsoft Entra ID assigns a unique Application (client)ID for the application. You will need this value, and possibly the tenant id, when configuring the Microsoft Teams Connection Functionality.

    1. In the Overview page, on the right-hand side, next to **Redirect URIs**, click on the **1 spa** hyperlink. You will be redirected to the **Authentication** page.
    2. In the **Single-page** application area, under the Accolade server URI, click **Add URI**.
    3. In the box which is shown, enter the Accolade server URI together with /blank.htm, for example https://accolade.example.com/blank.htm

    ---

    Important! If the MS Teams Integration is being used on multiple environments (e.g. test and production), you can choose either to add additional Redirect URIs or create separate app registrations.

To configure permission settings for the application:

1. Navigate to the application's **Overview** page.
2. From the left navigation pane, select **API permissions**.

3. Under the **Configured permissions** section, click on **Add a permission**.
4. From the right pane, select **Microsoft Graph API**.
5. Click on **Delegated Permissions** and select the following permission:
   - Files.ReadWrite
6. Click on **Add permissions** to save.
7. Click **Grant admin consent** to give admin consent for the selected application permissions.

Important! These permissions are delegated permissions, meaning individuals will need the appropriate permissions in MS Teams to carry out the tasks (e.g., creating a team).

To configure the integration to web versions of Microsoft 365 Word, PowerPoint and Excel with OneDrive:

1. Open the **Accolade Administration Console**.
2. From the navigation pane, select **Standard Parameters**.
3. Select **Category Integrations**, and click on the **Show Advanced** check-box.
4. As necessary for your configuration, make the following changes:

Field	Description
MS 365 Application (client) ID	The Application (client) ID of the application registered in Microsoft Entra ID (see above).
MS 365 Directory (tenant) ID	The Directory (tenant) ID of the application registered in Microsoft Entra ID (see above). The tenant ID can be a GUID (the ID of your Microsoft Entra ID instance), for single-tenant applications, or a domain name associated with your Microsoft Entra ID instance (also for single-tenant applications) Placeholders can also be used as a tenant ID in place of the Microsoft Entra ID authority audience enumeration: • *Organizations* for a multitenant application • *Consumers* to sign in users only with their personal accounts • *Common* to sign in users with their work and school accounts or their personal Microsoft accounts Default: organizations
MS 365 Prompt	Specifies how the user should be prompted to authenticate.

Field	Description
Type	The prompt parameter can be used to make sure that the End-User is still present for the current session or to bring attention to the request. Space delimited, case sensitive list of ASCII string values that specifies whether the End-User is prompted for reauthentication and consent. Defined values are: • **none** - Do not display any authentication or consent user interface pages. An error is returned if an End-User is not already authenticated or the Client does not have pre-configured consent for the requested Claims or does not fulfill other conditions for processing the request. Cannot be used in combination with other values. • **login** - Prompt the End-User for reauthentication. If it cannot reauthenticate the End-User, an error is returned. • **consent** - Prompt the End-User for consent before returning information to the Client. If it cannot obtain consent, an error is returned. • **select_account** - Prompt the End-User to select a user account. This enables an End-User who has multiple accounts to select amongst the multiple accounts that they might have current sessions for. If an account selection choice made by the End-User cannot be obtained, an error is returned. Default: select_account
MS 365 Domain Hint	Domain hints are directives that are included in the authentication request from an application. They can be used to accelerate the user to their federated IdP sign-in page. Or they can be used by a multi-tenant application to accelerate the user straight to the branded Microsoft Entra ID sign-in page for their tenant. If included, leads to a more streamlined user experience. An example of a domain hint would be a domain name such as sopheon.com. Default: empty.
MS 365 URI Scheme	The default URI Scheme to use for the MS Teams integration. This indicates the user experience when transitioning

Field	Description
	between Accolade and MS Teams. 0 = use the launcher (the Microsoft intermediate step which allows the user to select whether to use the MS Teams App or the web app), 1 = msteams scheme (use the MS Teams app), 2 = https scheme (use the web app). Default: 1
MS 365 Default Download Mode	The default download mode integration. 0 = prompt, 1 = download locally, 2 = download to OneDrive, 3 = download to MS Teams or locally, 4 = download to MS Teams or OneDrive. Default = 1.
Integration with OneDrive	Enable (1) or disable (0) the ability to download documents to OneDrive. Default = 0.

5. Click on **Apply** to save your changes.

To deploy the Microsoft 365 Add-Ins:

The three Accolade add-ins enable the web versions of Microsoft 365 applications to connect to a non-Microsoft 365 service (Accolade) and to upload data from OneDrive into Accolade.

1. Download and save the add-ins manifest (.xml file) from the following URL:

   `https://(servername)/CloudOffice/Office/Addins/manifest`

   If the add-in is used with more than one server, add an AppDomain element for each server to the AppDomains element.

2. Open the **Microsoft 365 Admin Portal**.
3. Navigate to **Settings > Integrated Apps**.
4. Upload **Custom App**.
5. Select **Office Add-in** as the **App Type**.
6. Upload the .xml manifest file saved earlier, and validate it.

   Notes: You may need to update the number in the Version element to be higher than any previously uploaded versions.

7. Go to the Users tab.
8. Assign users by selecting users or user groups as needed.

Important! After setting up the Accolade Administration Console, ensure that you apply the Microsoft 365 integration option in Accolade to enable the functionality:

- Integrate with OneDrive

Setting Up Integration to Acclaim Projects

Important! This must only be done if your organization has purchased integration with Acclaim Projects.

You must complete the following steps to set up Accolade's integration to Acclaim Projects with Data Bus:

1. Ensure Organization Information is set up, with an Integration ID and Acclaim Projects URL. For more on this, see Configuring Organization Information.
2. Set up Accolade Data Bus settings via the Administration Console.
3. Configure the Task Service User via Accolade.
4. Restart Accolade Time Task Service.

Important!

- Ensure that the Accolade Application Server can access the URL issued with your integration license, either directly or via an outbound proxy server.
- The Accolade Web Server must be configured with HTTPS.

To configure Accolade Data Bus settings for integration with Acclaim Projects:

1. Open the Accolade Administration Console. From the navigation pane, select **Standard Parameters**.
2. Select the category **Data Bus**, and click on the **Show Advanced** check-box.
3. In the **Data Bus WebSocket URL** field, enter the URL issued with your integration license.
4. *(Optional)* As necessary for your configuration, make changes to the following:

Field	Description
WebSocket Keep Alive Interval	The frequency at which to send Ping/Pong keep-alive control frames.

Field	Description
WebSocket Reconnect Timeout	The duration to wait before reconnection if no messages have been received from the server.
WebSocket Error Reconnect Timeout	The duration to wait before reconnection if last connection failed.

5. Click **Apply** to save your changes.

To configure the Task Service User on Accolade:

1. Log on to Accolade, and navigate to **System > User Admin**.
2. Locate and click on the user utilized for Accolade Task Service.
3. Open the **Roles and Rights** tab. Under Process Execution, select **Process Manager**, and under Administrative, select **Service Account**.
4. Open the **Access Groups** tab, and give all project rights for all groups. To do this, under **User Admin > Member Of**, select all check-boxes, and under **Projects**, select all check-boxes for all groups.
5. Open the **Security Lists** tab, if available, and select all check-boxes.
6. Open the **Security Profiles** tab, if available, and ensure no check-boxes are selected or deselect all.
7. Click **Save**.

To restart Accolade Time Task Service:

1. Open Windows Services.
2. Locate **Accolade Time Task Service**, right-click and select **Restart**.
3. Ensure no errors were triggered in the Accolade application after the restart, via the Logs page at **System > Diagnostics > Logs**.

Setting Up PDF Export Functionality for Accolade Time View

Important!

- Ensure that the Accolade Application Server can access this URL:

  `https://pdfexport.sopheon.net`

- The Accolade Web Server must be configured with HTTPS.

To configure Accolade to be able to utilize the PDF Export function in Accolade's Time View page:

1. Open the Accolade Administration Console. From the navigation pane, select **Standard Parameters**.
2. Search for name **PDF Export**, and click on the **Show Advanced** check-box.
3. In the **PDF Export Server URL** field, ensure the following value is entered:
   `https://pdfexport.sopheon.net`
4. In the **PDF Export Server Resources URL** field, ensure the following value is entered:
   `https://pdfexportresources.sopheon.net/accolade/{major}.{minor}`

Selecting the Search Language

The Accolade Search feature works best if it is configured for a specific language. If you have a standard corporate language that most or all your documents are written in, use the Local ID (LCID) of that language as the value of the advanced parameter **Default Search Language ID**. The default value **1033**, for US English.

If your installation requires searching for documents written in two or more languages, do one of the following:

- Select the language that has the most complex patterns or symbols for denoting the boundaries between words (word breakers) such as dash (-), comma (,), space, and others. For example, if you need to search on English, Spanish, and German, you could select German, because the German language includes the English patterns for breaking words while the English language does not include the German pattern of compound words.
- Select the Neutral language (with LCID of 0), which is generally successful at interpreting word breakers in a variety of Western languages. However, using this LCID has been linked to incorrect or incomplete search results.

For non-Western languages, such as Chinese, it is only possible to search in a single language.

To change the default search language:

1. To find the correct LCID value, start SQL Management studio and run the following query on the Accolade database. The query returns a list of LCIDs for all the languages that the database instance supports.

```
SELECT FL.LCID,
  FL.[Name]
FROM SYS.FULLTEXT_LANGUAGES FL WITH (NOLOCK)
ORDER BY FL.[Name]
```

2. Select the correct LCID from the required list and enter it in the Default Search Language ID parameter in the Administration Console.

Select the Show Advanced option to locate the parameter.

To rebuild the full-text indexes using the new language:

1. In SQL Server Management Studio, expand the Accolade database and right-click the **SGM_FileStoreSearch** table.
2. Select **Full-Text** index and click **Properties**.
3. In the Full-Text Index Properties window, open the **Columns** page.
4. In the **Language for Word Breaker** column, open the list in each row selected with a check mark and select the language whose LCID you are using.
5. Open the **General** page.
6. In the **Actions** section, select the **Repopulate index** check box, ensure the **Full** option is selected, and click **OK**.
7. Repeat this process for the **SGM_ProjectSearch** table.

Setting System Transaction Timeout

Set the length of time that the server waits for a transaction to complete before timing out.

To set the system transaction timeout:

1. In the server's **Administrative** Tools, open **Component Services**.
2. Expand **Component Services** then **Computers**.
3. Right-click **My Computer** and select **Properties**.
4. Click the **Options** tab.
5. In the **Transaction timeout (seconds)** field, enter **1200**.

   If the timeout entered in the **Accolade Table Wizard Timeout** parameter is greater than 1200, enter that time in the **Transaction timeout (seconds)** field or the greater of the times entered for Table Wizard Timeout.

Selecting the Corporate Currency

To measure and report on amounts as currencies, select the corporate currency in the Administration Console. See the Accolade online Help for information about setting currency conversions for projects and reports. If in a load balanced configuration, changes to the currency configuration only need to be made on one application server.

Important! If you must change the corporate currency after Accolade has been in use, you must also change the conversion factors in the Currency reference table and repair all reports that include currencies.

To select a corporate currency:

1. In the Accolade Administration Console, select **Currency Configuration** in the Navigation pane.
2. Select the currency that is your company's primary currency,
3. Click **Apply** to save your changes.

Enabling Automatic Upload of Reference Tables

You can configure reference table versions to upload to Accolade automatically when new versions are placed in a directory on the application server, or an FTP. Files placed in the directory or on the FTP site are automatically uploaded to Accolade.

Note: Accolade supports both FTP and FTPs for file uploads.

To enable automatic upload for reference tables Administrators must first complete the following:

- Configure the upload directory or FTP location
- Setup the Autoloader Service User in Accolade

After the location and service user are created, Process Designers and table owners can enable individual reference tables for automatic uploading.

Configure the Upload Directory or FTP Location

Administrators must create a folder that acts as the drop box location. On the application server, create or identify the following directories:

- The directory to use as the drop box location.
- A directory used to store service error messages.

These can be the same folder.

Set Up the Autoloader Service User

The Accolade Autoloader Service requires a user account to upload new document versions to Accolade. The user account you create or define for the autoloader service on the application server is automatically added to Accolade as a user with the Service Account user role. Grant the **Logon as a service** right to this user account.

Important! If you created the Accolade database login using Windows Authentication, you must add the user login to the database after adding the user to the Autoloader Service. Do this by following the instructions outlined in "Creating the Accolade Database Login" on page 20. Additionally, set up Autoloader Service users as Accolade users. Do not use Local System.

To setup the Autoloader Service User:

1. On the application server, from the **Start** menu, select **Administrative Tools > Local Security Policy**.
2. Open the **Local Policies** folder and open the **User Rights Assignment** folder.
3. Right-click the **Log on as a service policy** and select **Properties**.
4. In the **Local Security Setting** tab, add a service user for the upload service.
5. Click **OK** to save your changes.

After you have defined the service user on the application server, configure the Accolade Autoloader Service in the Accolade Administration Console. Additionally, after setting up the autoloader service user, add the user login to the database if you created the Accolade login using Windows Authentication.

To configure the Autoloader Service:

1. In the Accolade Administration Console, select **Autoloader Configuration** in the Navigation pane.
2. In the **Service Account User** field, add the service account user you created above and enter its password.

   This user is added to Accolade as a user with the Service Account user role.
4. Select the **Enabled Service** check box and enter a **Retry Delay on Error** time period in milliseconds to set the retry rate if the service encounters errors.
5. In the **File Locations** section, enter the input and output locations for the directory or FTP site in the fields appropriate for your setup.
6. Click **Apply** to save your changes.

To modify the Autoloader Service in a load balance environment:

For information regarding load balance environments, see "Load Balancing - High Availability" on page 109.

1. Stop any running Autoloader Windows Service instances on all load balanced servers.
2. Make the same change on each load balance server on the Autoloader Configuration page on the Administration Console.
3. Re-enable any previously active Autoloader Windows Service instances on all load balanced servers.

Enable the Reference Table for Automatic Uploading

Administrators, Process Designers, and a reference table's owner can configure new or existing reference tables to upload all its versions automatically when new versions are saved to the directory or FTP location.

To enable a reference table for automatic upload, select the **Enable Automatic Loading** check box in the reference table details, and select a scheduling option.

Configuring Resource Planning Time Periods

If your company has purchased Resource Planning, specify the time periods (weeks, months, or quarters) to be used in planning resource needs. If in a load balanced configuration, changes to the resource planning time period configuration only need to be made on one application server.

Important! If resource planning data has been entered into Accolade, you cannot update the planning periods using the Administration Console.

To configure resource planning time periods:

1. In the Accolade Administration Console, select **Resource Planning** in the Navigation pane.
2. In the **Planning Period** field, select the period of time that a single cell in a resource plan represents.
3. In the **Periods Back** field, enter the number of periods before the present period in which resources can be planned and data is retained.

   Enter a whole number not exceeding 120.
4. In the **Periods Forward** field, enter the number of periods in the future in which resources can be planned.

   Enter a whole number not exceeding 2400.
5. Click **Apply** to save your changes.

Note: Years do not extend beyond 12/31/9999 if years is the selected time period.

Configuring the Accolade Timed Task Service

The Accolade Timed Task Service must have access to the Accolade website, which requires it to run using an account with access to the system. Set the Accolade Timed Task Service to run using an Accolade Service Account user.

Important! If you created the Accolade database login using Windows Authentication, you must add the user login to the database after adding the user to the Time Task Service. Do this by following the instructions outlined in "Creating the Accolade Database Login" on page 20.

To create or configure the Service User Account:

1. Create or identify the user account that the Accolade Timed Task Service uses.
2. On the web server, in Administrative Tools, click **Local Security Policy**.

3. Expand the **Local Policies** folder.
4. Select the **User Rights Assignment** folder.
5. Right-click the **Log on as a service** policy and click **Properties**.
6. Add this user to the **Local Security Setting** tab.

To add the user to the Accolade Timed Task Service:

1. Open the Accolade Administration Console on the application server.
2. Select the **Authentication Configuration** tab.
3. Enter your task service user name and task service password.

   This creates a new user with appropriate rights in Accolade or updates an existing user.
4. Click **Apply**.

Enabling Secure Sockets

Enabling an SSL protocol on the Accolade Web server is optional. The procedures below assume that you have obtained an SSL certificate and installed it on the Accolade Web Server.

Enabling an SSL protocol requires that you do the following:

- Set the site bindings for SSL.
- Define SSL requirements for the Accolade website.
- Set the Accolade website to use SSL in the Administration Console.

Sopheon recommends enabling HTTP Strict Transport Security (HSTS). See Microsoft's technical documentation for more information.

To set the site bindings for SSL:

1. On the web server, in Administrative Tools, open **Internet Information Services (IIS) Manager** and expand the appropriate server name.
2. Expand **Sites**, right-click **Accolade Main Website**, and click **Edit Bindings** in the menu.
3. Click **Add** in the Site Bindings dialog box.
4. In the **Type** field, select **https** and click **Edit**.
5. Set the following:

Field	Description
IP Address	Leave **All Unassigned** selected.
Port	Sopheon recommends port 443 for the Accolade website.
SSL Certificate	Select the certificate that you installed.

6. Click **OK**.
7. In the Site Bindings dialog box, do one of the following:
   - Remove the HTTP binding if you are using SSL for all traffic.
   - Leave the HTTP binding if you want to allow anonymous idea submission over http.
8. Click **Close** and continue with the next procedure.

To define SSL requirements for the Accolade website:

1. On the web server, in Administrative Tools, open **Internet Information Services (IIS) Manager** and expand the appropriate server name.
2. Expand **Sites**, click **Accolade Main Website**, and double-click **SSL Settings** in the center pane menu
3. Select the **Require SSL** check box.
4. In the Actions pane, click **Apply**.
5. In the Connections pane, expand the **Accolade website**.
6. Select the **Idea application**.
7. Double-click **SSL Settings** and clear the **Require SSL** check box.
8. In the Actions pane, click **Apply**.

To verify the Accolade website name:

1. From the Start menu, open the Accolade Administration Console, and select **Website Configuration** from the Navigation pane.
2. Ensure that the port number is the same as the number you entered in the **Port** field in IIS.
3. Click **Apply**, even if you did not update the port number.
4. In the Navigation pane, select **Standard Parameters** to display the Accolade parameters.
5. In the following parameters, verify the URLs match those you used to configure the website, using “HTTPS” and the port number.
   - **Accolade Process Manager Website URL** - HTTPS://*<fully qualified servername>*:443/
   - **Anonymous Idea Submission URL** - HTTPS://*<fully qualified servername>*:443/idea/

Translating and Modifying Accolade Text

You can translate or modify the messages and text in Accolade, including the menu names in Accolade add-ins. You can translate the text displayed in Accolade into a different language or only change some individual terms, such as "deliverable", into terms that are used in your

company. Translatable text includes labels, titles, menus, and messages—any text the user interface generates on internationalized pages.

The changes you make for translation or modifying text currently do not translate the online Help content.

For more information about this process, see the Accolade Online Help.

Working With HSTS

Accolade is compatible with HTTP Strict Transport Security (HSTS), but configuration will depend on Internet Information Services (IIS) installation. Please refer to Microsoft's technical documentation for configuration.

Improving First Load Performance

To improve the first load performance:

1. Open Command Prompt with Administrative rights, on the application server.
2. Navigate to the Accolade 'Bin' folder.
3. Run "*PrecompileWebsite.exe --loglevel Information*". This may run for a couple of minutes.

For additional flags and options, run "*PrecompileWebsite.exe --help*".

Installation Complete

The installation is complete. You are now able to access the website from a client computer running the correct browser version.

For information about configuring users' computers, see "Configuring Client Computers" on page 65.

Chapter 4

Configuring Client Computers

Before the users of a new installation start to work with Accolade, ensure that their client computers are set up correctly and that the Accolade add-ins they use are installed. When upgrading, it is not necessary to uninstall existing add-ins before installing the new versions.

Important! Users installing the Sopheon Client Service or Accolade Office Extensions add-ins must be logged on as administrators on the computers on which they are completing the installation.

Web Browser Requirements and Setup

Accolade is supported in the following web browsers:

- Microsoft Edge version 44 and higher
- Microsoft Chromium Edge version 84 and higher
- Google Chrome, version 84.0 and higher.
- Mozilla Firefox version 80.0 and higher
- Apple Safari for OS 12 and higher or MacOS version 10.13

Review the following sections for additional web browser settings and requirements to ensure that Accolade runs smoothly:

- Allowing Pop-Ups for the Accolade Web Site
- Disabling Auto-Complete Browser Features
- Launching Accolade Portfolio Optimizer from Google Chrome

Allowing Pop-Ups for the Accolade Web Site

Add the Accolade website to the list of allowed sites if the web browser's pop-up blocker is turned off.

To allow pop-ups for the Accolade web site in Microsoft Edge:

1. From the Microsoft Edge **Menu** (icon in the top right corner of the browser), select **Settings > Site permissions**.

   You can also access the Site permissions settings by navigating to the Accolade website and clicking the Lock icon next to the website link in the address bar. If you use this method, you will need to click the **Refresh** button on the site afterwords in order to apply the changes.

2. Select **Pop-ups and redirects**.
3. In the Allow field, click **Add**, enter the URL to the Accolade website and click **Add**.
4. Close the browser page, or click the **Refresh** button on the site to apply the changes.

To allow pop-ups for the Accolade web site in Chrome:

1. From the Chrome **Customize and control Google Chrome** menu, select **Settings**.
2. If necessary, click **Show advanced settings** at the bottom of the Settings page.
3. In the **Privacy** section, click **Content Settings**.

4. In the **Pop-ups** section, click **Manage Exceptions**, add the URL to the Accolade website in the **Hostname Pattern** field, and select **Allow** from the **Behavior** list.
5. Click **Done** to save your changes.
6. Close the browser page.

To allow pop-ups for the Accolade web site in Firefox:

1. From the Firefox **Settings** menu, select **Options**.
2. Click **Content** and clear the **Block pop-up windows** check box.
3. Click **Exceptions** and enter any exceptions for pop-up settings as necessary for your company.
4. Click **OK** to save your changes.

Disabling AutoComplete Browser Features

For security purposes, Sopheon recommends disabling features in any browser that automatically completes text in fields and forms. The name of this feature varies by browser.

To disable autofill in Microsoft Edge:

1. From the Microsoft Edge **Menu** (icon in the top right corner of the browser), select **Settings > Privacy and services**.
2. In the Clear browsing data section, select **Choose what to clear**.
3. Select the **Autofill form data (includes forms and cards)** check box. and click **Clear now**.
4. Close the browser page.

To disable autofill in Chrome:

1. From the Chrome **Customize and control Google Chrome** menu, select **Settings**.
2. Click **Show advanced settings** at the bottom of the Settings page.
3. In the **Passwords and Forms** section, clear the selections for both the **Enable Autofill to fill out web forms in a single click** and the **Offer to save passwords I enter on the web** options.
4. Close the browser page.

To disable auto form fill in Firefox:

1. From the Firefox **Settings** menu, select **Options**.
2. Click **Privacy**.
3. In the **History** section, select **Use custom settings for history** from the **Firefox will** field.

4. Clear the **Remember search and form history** option.
5. Click **OK** to save your changes.

Launching Accolade Portfolio Optimizer from Google Chrome

For users who access Accolade Portfolio Optimizer in Google Chrome, install the Google Chrome extension as described below.

To install the ClickOnce Google Chrome extension:

1. Start Chrome and open a new tab.
2. In the new tab, click the Apps option and select to open the Web Store.
3. In the Chrome web store search field, enter **clickonce**.
4. In the search results, select the **ClickOnce Helper**.
5. On the Web Store page, click **Add to Chrome**.
6. Click **Add Extension**.

Preventing Accolade Add-Ins from Being Disabled

If you install any of the Accolade add-ins you can install the Sopheon Client Service, which prevents the Microsoft application from disabling the Accolade add-in. The service automatically re-enables the add-in if it becomes disabled. To re-enable the add-ins, the service updates Accolade registry keys to ensure that they load properly when the Microsoft application starts.

To install the Sopheon Client Service:

1. In the Accolade installation software, open the **Client Installation (Add-ins)** folder.
2. Run **Sopheon Client Service v17.1.msi**.

Integrating with Microsoft Applications

The Accolade Office Extensions add-in provides an integration between Accolade and the desktop versions of Microsoft 365 applications. Users can download documents directly to a Microsoft application, open and complete the necessary information, and then save the documents directly to Accolade without having to navigate back to Accolade. To enhance reporting functionality, Accolade Office Extensions allows users to create global or project-level reports in Excel that pull data from Accolade. These reports can be saved locally and accessed for individual use, or uploaded to Accolade for reporting purposes.

In addition, the Accolade Office Extensions add-in provides an integration that allows Microsoft Project Professional or Project Standard users to create Microsoft Project plan templates and use them to manage projects in conjunction with a related Accolade project.

The Accolade Office Extensions add-in is compatible with the following Microsoft applications:

- Excel
- Outlook
- PowerPoint
- Project Professional or Standard
- Word

Note: If your company's Accolade users are using these applications as part of the Microsoft 365 suite, they must have the applications installed locally. Accolade Office Extensions will not integrate with Microsoft 365 accessed solely online via subscription.

See the *Sopheon Accolade 17.1 Software and Hardware Requirements* document for the current Microsoft 365 version requirements.

The Accolade Office Extensions add-in must be installed on every user's computer in order to use any or all of the integration functionality.

To install the Accolade Office Extensions add-in:

1. In the Accolade installation software, open the **Client Installation (Add-ins)** folder.
2. Run **Accolade Office Extensions.msi**.
3. Open each application and ensure that the Accolade menu items are visible.

   If the menus are not visible after you run the installation, ensure that the Accolade add-ins are trusted.

Important! Use of the Microsoft Project functionality requires the MS Project Integration Key, and may require additional licensing. Contact Sopheon Customer Support for more information.

Installing all Microsoft Windows Important Updates

Ensure that each user installs all currently required Windows important updates from Microsoft Update after installing the add-ins.

Chapter 5

Configuring Authentication

This chapter describes how to setup authentication and how to setup Dashboards for Accolade for use with SSO. The content of this chapter assumes you have a working knowledge of server management and the Accolade server setup for a customer.

Important! Due to the complexity of configuring authentication, Sopheon recommends working with Sopheon Client Services to ensure correct setup and support.

Setting Up Authentication

This section describes the steps and settings required on the Accolade Server to set up Authentication. Each is described in more detail in the sections below.

- Accolade Administration Console settings
- Configure the Client Computer
- Testing the setup

Accolade Administration Console Settings

1. Open the Accolade Administration Console and select **Authentication Configuration** in the navigation pane.
2. Review the default settings for the Service Credentials and make changes as necessary for your configuration.

Field	Description
Task Service User Name	Enter the name of the user to be authenticated. These are the credentials task services use to validate connections Accolade.
Task Service Password	Enter the password of the user to be authenticated. These are the credentials task services use to validate connections to Accolade.

3. Select the Authentication Type.
4. Review the default settings and make changes as necessary for your configuration.

SopheonID

Field	Description
Client ID*	Unique identifier for your registered application. Enter the saved value of the Client ID for the app you registered with the OpenID Provider.
Client Secret*	Required if Accolade is configured as a confidential client. This will use the Hybrid Flow (aka Implicit Flow with Form Post and Authorization Code Flow) to sign in the user.
Region*	The AWS region of the target User Pool, for example: us-east-2
User Pool ID*	The ID of the target User Pool, for example: us-east-2_9mcupUb61
Name Claim Type	The claim type to identify the user's login name. Defaults to: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name if omitted. For example: preferred_username.
Prompt	A space-delimited list of string values that specifies whether the author-

Field	Description
	ization server prompts the user for reauthentication and consent. For example, select_account.
Max Age	Maximum Authentication Age. Specifies the allowable elapsed time since the last time the end-user was actively authenticated by the OpenID Provider. If the elapsed time is greater than this value, the OpenID Provider must attempt to actively re-authenticate the enduser. For example: 3600 (60 minutes).

OpenID Connect

Field	Description
Client ID*	Unique identifier for your registered application. Enter the saved value of the Client ID for the app you registered with the OpenID Provider.
Client Secret*	Required if Accolade is configured as a confidential client. This will use the Hybrid Flow (aka Implicit Flow with Form Post and Authorization Code Flow) to sign in the user.
Authority*	The Authority is the base address for the well-known OpenID configuration document: <Authority>/.well-known/openid-configuration. For example, for Microsoft Entra ID, this might be: https://login.microsoftonline.com/organizations/v2.0/.
Name Claim Type	The claim type to identify the user's login name. Defaults to: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name if omitted. For example: preferred_username.
Prompt	A space-delimited list of string values that specifies whether the authorization server prompts the user for reauthentication and consent. For example: select_account.
MaxAge	Maximum Authentication Age. Specifies the allowable elapsed time since the last time the end-user was actively authenticated by the OpenID Provider. If the elapsed time is greater than this value, the OpenID Provider must attempt to actively re-authenticate the enduser. For example: 3600 (60 minutes).
Scopes	Specifies the scopes for which you want to request authorization, which dictate which claims (or user attributes) you want returned. These must be separated by a space. Defaults to ‘openid profile’ if omitted.

Note: The Redirect URI to be configured in the OpenID Provider should have the path '/signin-oidc'. For example: https://<accolade-server>.company.com/signin-oidc.

For customers with legacy requirements for API token requests and as a backwards compatibility measure, the OAuth 2.0 Resource Owner Password Credentials (ROPC) Grant flow can be enabled by selecting 'Yes' for the "Enable ROPC" setting.

If enabled, the following details should be supplied:

Field	Description
Token Endpoint*	The URL of the token endpoint where clients obtain identity and access tokens in exchange for an OAuth 2.0 grant. For example: https://login.microsoftonline.com/organizations/oauth2/v2.0/token
Client ID*	Unique identifier for your registered application. Enter the saved value of the Client ID for the app you registered with the OpenID Provider.
Client Secret	Your application's Client Secret.
Client Assertion	A different form of client_secret, generated using a certificate.
Name Claim Type	The claim type to identify the user's login name. Defaults to: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name if omitted. For example: preferred_username.
Scopes	Specifies the scopes for which you want to request authorization, which dictate which claims (or user attributes) you want returned. These must be separated by a space. Defaults to 'openid profile' if omitted.
Timeout	HTTP Request timeout. Defaults to 00:01:40 (1 minute and 40 seconds) if omitted.

Note: It is mandatory to include a value for either Client Secret or Client Assertion.

WS-Federation

Field	Description
Realm	A securely configured domain to share resources securely. The realm is the uniform resource identifier (URI) of the application. For example: https://<accolade-server>.company.com
Metadata Address*	The WS-Federation identity provider metadata file location. The address to retrieve the WS-Federation metadata, for example: https://<ADFS FQDN>/FederationMetadata/200706/FederationMetadata.xml This could also be a local file, for example: file://c:/folder/federationmetadata.xml.

Field	Description
Name Claim Type	The claim type to identify the user's login name. Defaults to: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name if omitted.
Freshness	Indicates the desired maximum age of authentication specified in minutes; if specified as "0" it indicates to re-prompt the user for authentication.
Active Requestor Address	WS-Trust 1.3 endpoint to enable the ROPC grant flow in Accolade. For example: https://<ADFS FQDN>/adfs/services/trust/13/UsernameMixed

Windows

No additional settings are needed for this Authentication Type.

Basic

Field	Description
Realm	A securely configured domain to share resources securely. The realm is the uniform resource identifier (URI) of the application. For example, https://<accolade-server>.company.com
Default Domain	Enter the domain the web server is on.

Note: Different Authentication Providers use cookie names of different lengths and web infrastructure policies may need to be revised to cater for longer cookie names.

5. Click **Apply** to save your changes.

When making changes to this page in a load balanced configuration, stop the website in IIS on each application server and Windows service (not including the Cache Service) to ensure the following settings are correctly reloaded when each application server is brought back up.

Apply the authentication page configuration settings across all application servers in the load balanced configuration.

Configuring the Client Computer

Add the following sites to your trusted sites internet zone. This ensures cookies for all servers are in the same location and can be shared between the browser and the add-ins:

- Accolade Server (ex. https://abc.sopheon.com).
- WS Federation Server passive profile endpoint or OpenID Connect IdP server (ex. https://fs1.sopheon.com).
- Client Identity Provider Server.

Testing the Setup

To ensure all settings are correct, open a web browser and enter the site address, for example, https://test.sopheon.com and verify that a login page displays similar to the following:

Setting Up Dashboards for Accolade for SSO

This section describes the steps and settings required to setup Dashboards for Accolade to work with SSO. Each is described in more detail in the sections below.

- Accolade Administration Console settings
- Hosts file updates
- Qlik server setup
- Configuring the Client Computer
- Testing the setup

Accolade Administration Console Settings

Use the Accolade Administration Console to set the system parameters that are specific to Dashboards for Accolade in a single sign-on scenario.

To update system parameters specific to Dashboards for Accolade:

1. On the Accolade server, open the Accolade Administration Console and select **Standard Parameters** in the navigation pane.
2. From the **Category** list, select **Dashboards** and click **Show Advanced**.
3. Set the following parameters, if not already set:
   - **Dashboards Server URL** – Address of the Dashboards server.
   - **Dashboards User Group** – Name of the user group used for Dashboard document permissions. This must be the same name as the DMS user group you will set in Qlik for each chart.
   - **Dashboards Web Ticket Password** – Password of the user used for retrieving the Dashboards web ticket. (leave blank if you are using TrustedIP configuration)
   - **Dashboards Web Ticket User Name** – Name of the user used for retrieving the Dashboards web ticket. (leave blank if you are using TrustedIP configuration)
4. Click **Apply** to save your changes.

Option 1: Set up a Web Ticket User

We are not using this at this time, but Sopheon Product Development built it as an option as the password is stored in plain text. On the Qlik Server, add the web ticket user to the Qlik Administrators group in Windows Computer Management.

Option 2: Set up a TrustedIP Relationship Between the Accolade and Qlik Servers

Restrict the Accolade server to be the only server that calls the Qlik server to get a ticket. For a public server, route the requests straight to the Qlik server by using internal IP addresses.

Hosts File Updates

Enter the Qlik server's address and other information to update the host files.

1. On the Accolade Server, open the hosts file, located in C:\Windows\System32\drivers\etc, using Notepad.
2. At the bottom of the file, enter the Qlik server’s internal IP address, and its public name, such as abc.sopheon.com.

   ```
   10.1.1.111 abc.sopheon.com
   ```
3. Save your changes to the file.

Qlik Server TrustedIP

Add Trusted IP elements to the Qlik server.

1. On the Qlik Server, open the C:\Program Data\QlikTech\Webserver folder and open the config.xml file using Notepad.

2. In the <Authentication> section under <GetWebTicket>, ensure the <TrustedIP> parameter is set to the internal IP address of the Accolade server.

   For example:

   ```
   <GetWebTicket url="/QvAjaxZfc/GetWebTicket.aspx">
     <TrustedIP>10.1.1.110</TrustedIP>
   </GetWebTicket>
   ```

   Note: If you are supporting multiple Accolade servers with this Qlik server, you can add multiple Trusted IP elements.

3. Save the file.

Qlik Server Setup

Use the information in this section to setup the Qlik server. Setting up the Qlik server requires you to configure the IIS website and the DMS authorization.

To configure IIS Website:

Complete the following on the Qlik Server.

1. On the Qlik Server, open the IIS Management Console and change the following folders to enable Anonymous Authentication and disable Windows Authentication.
   - QVAjaxZFC
   - QlikView

To configure DMS Authorization:

Complete the following on the Qlik Server.

1. On the Qlik Server, open the Qlik Management Console and select the **System** tab.
2. Expand **Management Service > Qlik Servers** and select the server to configure.
3. Select the **Security** tab.
4. In the Authorization section, select **DMS Authentication**.

In the Qlik Management Console, set the user group that can view documents available to Dashboards for Accolade:

1. On the Qlik Server, open the Qlik Management Console and select the Documents tab.
2. Open the **Dashboard - Charts** folder and select the file you will be creating a global link for in Accolade.
3. Select the **Authorization** tab.
4. Add a user.
5. Select **Named Users** in the **User Type** drop-down field.

6. Click the **Manage Users** icon.
7. Manually input the **Dashboards User Group** that was entered into the Accolade Administration Console parameters.

8. Click **OK**.
9. Click **Apply**.
10. Repeat for each additional document that will be created in the Accolade global links.

Configuring the Client Computer

In addition to the sites in the previous section for Accolade setup, add the following sites to your trusted sites internet zone. This ensures cookies for all servers are in the same location and can be shared between the browser and the add-ins:

Qlik Server (ex. https://testqv.sopheon.com)

Testing the Dashboards for Accolade SSO Setup

To ensure all settings are correct, open a web browser and display Qlik to ensure the single sign-on implementation is correct. Once DMS is turned on, the only way to access Qlik is through the Accolade server using a /dashboards on the end of the FQDN of the Accolade server.

For example, https://abc.sopheon.com/dashboards

Once the SSO settings are verified, Dashboards for Accolade can be installed and configured. See the *Sopheon Accolade Qlik Dashboards for Accolade v17.1 Installation Guide* for more information.

Chapter 6

Upgrading Accolade

This chapter describes the process for upgrading Accolade to release 17.1.

Caution! Carefully review and understand the potential impact on your implementation of Accolade before upgrading to a new version. Sopheon expressly disclaims responsibility for any such impact. In particular, additional work may be required to upgrade Accolade if it includes customizations. If your implementation includes customizations, contact Sopheon Customer Support for assistance with your upgrade.

Preparing to Upgrade Accolade

Important! If you are running a version of Accolade prior to a major release version, you must upgrade to major release versions before upgrading to other releases. For example, if upgrading from any 12 version to 17.1, you must upgrade to 13.0 first.

Before beginning the Accolade upgrade, review the requirements in the *Sopheon Accolade v.17.1 Software and Hardware Requirements* document to ensure your system meets the requirements. To complete the upgrade, you must log on to the Accolade servers as a member of the Administrator group.

Upgrading Accolade includes the following steps:

1. Running the **Pre-Upgrade Check.sql** script, and correcting customization issues within Accolade.

   Sopheon recommends against customizing the database except by creating custom views. Running this script finds any customizations that may not run correctly after upgrading. If you have such customizations, contact Sopheon Customer Support before upgrading.
2. Stopping Accolade and backing up the current version.
3. Updating any software or hardware requirements.
4. Updating the database schema.
5. Installing the new Accolade version.
6. Configuring Accolade after installation.
7. Configuring the client computers.
8. Running the **Post Upgrade.sql** script.

Ensure that you have the **Accolade_v17.1.x_Installation.zip** file containing the installation software saved to an accessible location. The file is available for download from www.sopheon.com.

Running the Pre-Upgrade Scripts

The **Pre-Upgrade Check.sql** script must be run prior to upgrading to the latest version of Accolade to check for database customizations. If the script is not run, the Upgrade script will error and not allow you to complete the upgrade.

Note: If you have calculated metrics missing their formula configured in your system, the script will return the list of calculated metrics and uncheck the **Calculated Metric** check box in the metric configuration.

To run the pre-upgrade checks:

1. In **SQL Server Management Studio**, browse to the installation software and open the following folder:

   `Server Installation (Database)\Database Scripts\Other Scripts`

2. Select the Accolade database and run the **Pre-Upgrade Check.sql** script.

   If the script encounters issues with any of the listed items, the pre-upgrade check outputs the following:

   - Issue Type - Classification of the issue detected.
   - Issue Item - Identification of the Accolade component affected by the issue.
   - Issue Notes - Additional information to correct the issue detected.

Uninstalling Microsoft Teams Integration and/or Cloud Office Component

To uninstall the Cloud Office Component:

1. Remove the Accolade SmartDocuments for Office browser extension from Microsoft Edge, Google Chrome, and/or Mozilla Firefox.
2. Remove the Accolade SmartDocuments for Office add-ins.
3. Stop Accolade, including the following components:
   - IIS
   - All Accolade services
4. Drop all CRVP_CloudOffice_* views from the main Accolade database.
5. Cleanup `Configuration\Tasks.config` file:
   - Remove `BeforeDocumentDownload` custom event for type 'Sopheon.Apps.CloudOffice.DocumentEventHandlers.EventHandlers'
   - Remove `OnDocumentUpload` custom event for type 'Sopheon.Apps.CloudOffice.DocumentEventHandlers.EventHandlers'
6. Cleanup Website\web.config file:
   - Cleanup or remove 'cors:AllowedOrigins' app setting
   - Cleanup or remove 'auth:AllowedClientURIs' app setting
   - Remove <location> element with path 'CloudOffice'

- Remove <location> element with path ‘Plugins/CloudOffice/Embedded’
- Remove <location> element with path ‘BrowserExtensions’

7. Delete files and folders:
   - Delete folder `Bin\Plugins\`
   - Delete file `Website\App_Data\Sopheon.Apps.CloudOfficeApiHelp.xml`
   - Delete file `Website\Bin\DocumentFormat.OpenXml.dll`
   - Delete file `Website\Bin\Sopheon.Apps.CloudOffice.DocumentEventHandlers.dll`
   - Delete file `Website\Bin\System.IO.Packaging.dll`
   - Delete file `Website\Bin\Plugins\Sopheon.Apps.CloudOffice.dll`
   - Delete file `Website\Bin\Plugins\Sopheon.Apps.CloudOffice.dll.config.json`
   - Delete folder `Website\Bin\Plugins\`, if empty (this folder could still be used by other components)
   - Delete folder `Website\BrowserExtensions\`
8. Reboot the Accolade application server.
9. Navigate to Accolade and verify that the application is working as expected.

To uninstall the Microsoft Teams Integration Component:

1. Deactive or delete Quick Grid with system name ‘qgMSTeamsStageTask’.
2. Deactive or delete Layout with system name ‘layMSTeamsProject’.
3. Delete Global Link with system name ‘MSTeamsConfig’.
4. Stop Accolade, including the following components:
   - IIS
   - All Accolade services
5. Drop all C365_* stored procedures, tables, and types from the main Accolade database.
6. Cleanup `Configuration\Tasks.config` file:
   - Remove task with ID ‘BCD9E2B7-57EA-41D4-9148-6F56233AF88F’
   - Remove task with ID ‘8B587BF1-0430-4D09-A5E8-D20E142FF048’
7. Cleanup `Bin\TaskService.exe.config` file:

- Remove <probing> element

8. Cleanup `Website\web.config` file:
    - Cleanup or remove ‘cors:AllowedOrigins’ app setting
    - Cleanup or remove ‘auth:AllowedClientURIs’ app setting
    - Remove <location> element with path ‘Plugins/Sopheon.Apps.MSTeams/Embedded’
    - Remove module ‘FixContentModule’ from <system.webServer>
9. Cleanup `Website\Optimizer\web.config` file:
    - Remove module ‘FixContentModule’ from <system.webServer>
10. Delete files and folders:
    - Delete folder `Bin\Plugins\`
    - Delete file `Bin\System.Net.Http.dll`
    - Delete file `Website\App_Data\Sopheon.Apps.MSTeamsApiHelp.xml`
    - Delete file `Website\Bin\Sopheon.Apps.MSTeams.HttpModule.dll`
    - Delete file `Website\Bin\Plugins\Sopheon.Apps.MSTeams.dll`
    - Delete file `Website\Bin\Plugins\Sopheon.Apps.MSTeams.config.json`
    - Delete file `Website\Bin\Plugins\Sopheon.Shared.TaskService.dll`
    - Delete file `Website\Bin\Plugins\Sopheon.Accolade.Web.Api.dll`
    - Delete file `Website\Bin\Plugins\Microsoft.Graph.Auth.dll`
    - Delete file `Website\Bin\Plugins\Microsoft.Graph.Core.dll`
    - Delete file `Website\Bin\Plugins\Microsoft.Graph.dll`
    - Delete file `Website\Bin\Plugins\Microsoft.Identity.Client.dll`
    - Delete folder `Website\Bin\Plugins\`, if empty (this folder could still be used by other components)
11. Reboot the Accolade application server.
12. Navigate to Accolade and verify that the application is working as expected.

Stopping Accolade and Performing Backups

Stop the Accolade application and complete database backups prior to upgrading to the latest version of Accolade. If the last database backup is more than 4 hours old, the **Pre-Upgrade Script** will warn you. It is advised you create a new backup of the databases before proceeding to ensure you do not lose data changes since the last backup.

Stop Accolade, including the following components:

- IIS
- All Accolade services

Additionally, stop all scheduled tasks (such as Qlik Dashboards for Accolade reload schedules, and maintenance tasks such as reloads, system backups, index rebuilds, patch installations, etc.) for the duration of the upgrade.

Create a backup of the following Accolade components:

Component	Notes
Administration Console Configuration Settings	Record the settings from the following panels in the console: • Database Configuration • Website Configuration • Autoloader Configuration You will need to re-enter the settings after the upgrade is complete.
Custom Database Objects	Save any custom reporting views, stored procedures, functions, and triggers so they can be reapplied after the upgrade.
Process Manual	If stored in the Accolade installation, create a backup of the process model.
Customizations	Create a backup of any customizations you may have created or edited, such as .asp pages, custom DLLs, and so forth. You must back up these custom files before you proceed with the upgrade, and you can re-apply them after the upgrade is completed if they are still appropriate.
Customizations	Create a backup of any custom icon sets before you proceed with the upgrade. After the upgrade is finished, you can re-apply them. **Important!** Icons have changed to the .svg filetype in Accolade v13.0. If you are upgrading from any 11 or 12 version to 13.0.0 or later, you will need to update the icons prior to re-applying them after the upgrade. When adding custom icon sets, place the folder in the following file locations and reset IIS.

Component	Notes
	The default location for icon sets is: `C:\Program Files\Sopheon\Accolade\Etc\IconSets`
Log Files	Back up the log files if you want to restore the log files after the upgrade. Log files are stored in the following default locations: *<install location>*`\Accolade\Website\Logs` • web.config *<install location>*`\Accolade\Log` • Accolade.log • trace.log • *<timestamp>*Error.log

After backing up the Accolade components above, create backup copies of the Accolade and snapshots databases.

Note: Scenarios databases are working databases that do not store data. Therefore, they do not need to be backed up prior to completing an upgrade.

After completing full database backups, disable any scheduled backups for the duration of the upgrade. You will re-enable scheduled backups once the upgrade is complete.

Integrations with Dashboards for Accolade

If Accolade is integrated with Dashboards for Accolade you should uninstall the appropriate Qlik **Integration with Dashboards for Accolade v<version>.msi** file from the Qlik server.

To prepare for an upgrade with Dashboards for Accolade:

1. Uninstall the appropriate Qlik **Integration with Dashboards for Accolade v<*version*>.msi**.
2. On the Qlik server, install the current version of the appropriate Qlik **Integration with Dashboards for Accolade v<*version*>.msi.**

   This file is located in the appropriate Qlik **Integration with Dashboards for Accolade** folder of the Accolade installation software.

   For specific instructions, see the appropriate Qlik *Dashboards for Accolade Installation Guide* in the Accolade installation software.

Upgrading to a Later SQL Server Version

If you are upgrading the SQL Server, continue with the procedure in this section. If you are not upgrading the SQL server, continue with "Upgrading the Database Schemas" on page 90.

To upgrade the SQL Server version:

1. On the database server and new SQL Server instance, ensure the following:
   - All server specifications listed in the *Sopheon Accolade v17.1 Software and Hardware Requirements* document are met.
   - Collation for the Accolade databases is the same as for the SQL Server instance.
   - All Windows Updates have been installed.
2. Restore the databases to the new SQL Server version.
3. Run the scripts for restored databases.

   To run scripts, you must log in to SQL Server with the appropriate rights of the database owner. See "Database Prerequisites" on page 16.

   In the installation software, browse to the **Other Scripts** folder and open the script **Prepare Restored Database Script.sql**.

   `Server Installation (Database)\Database Scripts\Other Scripts`

   Replace *<NewDBOwner>* in the script with the SQL login of a user who always has the **sysadmin** and **public** roles on the SQL Server instance and whose default language is **English**.

   Run the query against the newly restored Accolade and snapshots databases.
4. Start SQL Server Management Studio and, on the Files page of the Database Properties window, ensure that the **Use full text indexing** check box is selected.

   Initial size and autogrowth values depend on Sopheon's technical requirements analysis.
5. Click **Options** and complete the following:

Field	Setting
Compatibility Level	Accolade 17.1 supports the below options. Sopheon recommends matching this with the SQL version being used. • **SQL Server 2019 (150)** • **SQL Server 2022 (160)**
Auto Update Statistics Asynchronously	Set to **True**.
Default Cursor	Set to **LOCAL**.

6. Open the Administration Console on the Application server that will be used with this database, and complete the following:
   - Open the Database Configuration tab and enter the information for the database you just restored.
   - Open the Distributed Cache configuration and set the Cache Servers and Usages for this new environment.

- Open the Website Configuration tab and update the Website configuration settings for this new environment.

To install the MS Office IFilters to enable text search in Accolade:

1. In Windows Explorer, browse to the installation software in **Accolade_v17.1.x_ Installation.zip**, and open the following folder:

   `Server Installation (Database)\MS Office Support.`

2. Open the 64-bit or 32-bit folder and run the two files that are appropriate for your database server version.

Server Version	Files
64-bit server	Run both of the following in the order listed: • FilterPackx64.exe • FilterPack64bit.exe
32-bit server	Run both of the following in the order listed: • FilterPackx86.exe • FilterPack32bit.exe

   If a secondary window flashes, displaying and immediately disappearing, when you run a FilterPack file, IFilter is already installed.

3. After installing both filter packs for your database version, install the service packs and updated filter packs available in the following locations. Run both packs even if you are not running a different version of MS Office.
   - **Office 2010 Filter Pack SP2** - https://support.microsoft.com/en-us/kb/2687447.
   - **Update for Microsoft Filter Pack 2.0** - https://support.microsoft.com/en-us/kb/2881026.
4. From **SQL Management Studio**, run both of the following scripts:
   - EXEC SP_FULLTEXT_SERVICE 'load_os_resources', 1
   - EXEC SP_FULLTEXT_SERVICE 'verify_signature', 0
5. Restart the database.

Application Server Prerequisites

See the *Sopheon Accolade v17.1 Software and Hardware Requirements* document for a full list of the hardware and software required for the application server.

Updating .NET Framework

Important! .NET Framework must be installed *after* roles, services, and features to ensure proper configuration of IIS. If the server already has .NET installed when

you install the roles, install .NET Framework again after the roles are installed.

Upgrading the Database Schemas

You must run database upgrade scripts from the Accolade installation software to update your Accolade and snapshots databases to the **Accolade 17.1** schema. You must also create at least one scenarios database.

Note: The database upgrade scripts may cause SQL Server to repeatedly display one or both of the following messages: “Caution: Changing any part of an object name could break scripts and stored procedures.” and "Nonqualified transactions are being rolled back. Estimated rollback completion <*number*>%." You can ignore both messages.

Upgrading the Accolade and Snapshots Database

Run scripts to upgrade the main Accolade database and the snapshots database and confirm that databases settings are correct.

Note: The upgrade script changes the recovery model to **Simple** to minimize the impact to the hard drive disc space and maximize performance during upgrade. The script restores the recovery model to the previous setting when complete.

To upgrade the databases:

1. Log on to the SQL Server instance using a login with the **sysadmin** and **public** server roles and with **English** as the default language.
2. If you have restored the database for this upgrade, run the following script for restored databases. Otherwise, continue with step 3.

   In the installation software, browse to the **Other Scripts** folder and open the script **Prepare Restored Database Script.sql**.

   `Server Installation (Database)\Database Scripts\Other Scripts`

   Replace <*NewDBOwner*> in the script with the SQL login of a user who always has the **sysadmin** and **public** roles on the SQL Server instance and whose default language is **English**.

   Run the query against the newly restored database.
3. Start SQL Server Management Studio, and on the **Files** page of the **Database Properties** window, ensure that the **Use full text indexing** check box is selected.

   Initial size and autogrowth values depend on Sopheon’s technical requirements analysis.
4. Click **Options** and ensure the following settings are correct:

Field	Setting
Compatibility Level	Accolade 17.1 supports the below options. Sopheon recommends matching this with the SQL version being used. • **SQL Server 2019 (150)** • **SQL Server 2022 (160)**
Auto Update Statistics Asynchronously	Set to **True**.
Default Cursor	Set to **LOCAL**.

5. In the installation software, browse to the Upgrade folder (`Server Installation (Database)\Database Scripts\Upgrade`) and open the following files in the order listed. You must run the script for the main Accolade database first.
   - **Accolade v17.1 - Main - Upgrade.sql** - Open this file to upgrade the main Accolade database. Select the main Accolade database and run the script.
   - **Accolade v17.1 - Snapshots - Upgrade.sql** - Open this file to upgrade the snapshots database. Select the snapshots database and run the script.
6. If the Accolade database had custom reporting views that were saved as a script, open and run that script on the appropriate database.
7. Repeat this procedure to update the other database.

Creating or Recreating the Scenarios Databases

Accolade includes databases to improve the performance of Accolade Portfolio Optimizer for concurrent users. When upgrading, the scripts drop the existing databases and then create the needed ones.

Important! You must create at least one database even if your company does not use Portfolio Optimizer. The upgrade replaces any existing scenarios databases with the number of databases entered in this script. Sopheon recommends that you create one scenarios database for each expected concurrent user of Portfolio Optimizer.

To create the scenarios database:

1. To create the scenarios databases, browse to the installation software and open the following folder:

   `Server Installation (Database)\Database Scripts\Create.`
2. To specify the number and size of the scenarios databases, edit the **Accolade v17.1 - Scenario - Create Database.sql** script.
3. Scroll down to a block of SET statements containing the following variables and enter the value you want.

   Each variable applies to all scenarios databases.

Variable	Description	Default Value
@NumDBs	Number of databases to create	1
@MDFFileGrowth	Autogrowth for MDF (master data) files	50 MB
@MDFFileSize	Initial size of MDF files	1 GB
@LDFFileGrowth	Autogrowth for LDF (log) files	50 MB
@LDFFileSize	Intitial size of LDF files	500 MB

Values for the “File” variables default to MB if units are not specified. Add “GB” to specify a size in gigabytes.

The number of concurrent databases you select does not limit the actual number of concurrent users of Portfolio Optimizer.

4. Run the script on the Accolade database to create the scenarios databases.

   The new databases are named: <*main database name*>_Scenarios_<*number*>.

   For example: Accolade_Scenarios_3

5. To configure the scenarios databases, browse to the installation software and open the following folder:

   `Server Installation (Database)\Database Scripts\Other Scripts`

6. Run the **Prepare Restored Database Script.sql** on each new scenarios database.

   Select the same owner for each scenarios database as the owner of the Accolade and snapshots databases.

7. To create the database schemas, browse to the installation software and open the following folder:

   `Server Installation (Database)\Database Scripts\Create`

8. Run the **Accolade v17.1 - Scenario - Create.sql** script on each new scenarios database.

9. In SQL Server Management Studio, open the properties of the user login that Accolade uses to connect to the Accolade and snapshots databases.

10. On the **User Mapping** page, map the login to each new scenarios database with the **public** and **SGM_Write** roles.

Backing Up the Databases After Upgrade

Complete a full database backup after running the necessary upgrade scripts.

Re-enable scheduled backups that were previously disabled prior to upgrading.

Installing the Accolade Application Software

Note: If your network configuration sets the Network Service to not have access across the network, also see "Secure Network Best Practices" on page 126.

Prior to installing the Accolade application, disable User Account Control (UAC). If your company policy does not allow the disabling of UAC, you must run the installation from the command line.

To install the Accolade application:

1. Browse to the installation software, open the **Server Installation (Application)** folder, and run **Accolade v17.1 Server.msi**.

   If UAC is enabled, open a command prompt and enter the following: `msiexec /i <full path and file name>`.

   The command prompt needs to be launched as a local admin.

   For example: `msiexec /i "c:\install files\server installation\Accolade v17.1 Server.msi"`

2. On the Customer Information page, ensure that the **User Name** and **Organization** information is correct.
3. In the **Serial Number** field, enter the serial number assigned to you.

   Serial numbers are case sensitive.
4. On the Destination Folder page, accept the default installation location or browse to a custom location.

   Note the location that you select. You need the location when you configure Accolade.

   The default location is: `C:\Program Files\Sopheon\Accolade\`
5. On the Ready to Install the Program page, click **Install** and wait while the installation completes.
6. On the InstallShield Wizard Complete page, click **Finish**.

   If the Accolade Application installation does not complete, even when run from the command line, navigate to the Local Policy Editor (Local Security Policy > Local policy > Security Options > User Account Control: Run All Administrators in Admin Approval Mode) and set the **User Account Control: Run All Administrators in Admin Approval Mode** setting to **Disabled** and run the installation again.
7. Install the Accolade Cache service:

   1. Browse to the installation software.
   2. Open the Server Installation (Application) folder.

3. Run "Install_Memurai_as_AccoladeCacheService.ps1".
4. Verify a service named "Accolade Cache Service" is running.

Continue with the next section to configure Accolade.

Configuring Accolade After Upgrade

To configure Accolade after completing an upgrade of the software, complete the following steps below for each application server.

To configure Accolade after upgrading:

1. Open the Accolade Administration Console on the application server. The **Configuration Wizard** will be shown.
2. On the Database Configuration tab, confirm the database connections are correct as noted in "Stopping Accolade and Performing Backups" on page 86.
3. On the Organization Information tab, confirm that the name of your organization is in the **Organization Name** field.

   Once a name is entered and saved, the information becomes read only and cannot be changed.
4. On the Organization Information tab, confirm that your organization's **Acclaim Projects URL** and **Integration ID** are in their respective fields.

   Note: These fields will only be populated if your organization has purchased integration with Acclaim Projects.
5. On the Website Configuration tab, confirm the settings are correct as noted in "Stopping Accolade and Performing Backups" on page 86.
6. On the Distributed Cache Configuration tab, confirm that the configuration settings are correct, click **Clear Cache** to clear the distributed cache, enter your password, and click **Apply**.

   Note: Cache servers must be installed prior to this step. See Setting Up Distributed Cache Servers for more.
7. *(Optional)* If you use a directory or drop box location to automatically upload reference tables into Accolade, repopulate the settings on the Autoloader Configuration tab that you noted in "Stopping Accolade and Performing Backups" on page 86.
8. *(Optional)* If you are using the Timed Task Service, see "Configuring the Accolade Timed Task Service" on page 61.

Important! The Accolade modules and components license keys were updated in version 13.0. To ensure the website works properly after the upgrade, confirm with Sopheon Customer Support that the current module keys are correct.

Improving First Load Performance After Upgrade

To improve the first load performance:

1. Open Command Prompt with Administrative rights, on the application server.
2. Navigate to the Accolade 'Bin' folder.
3. Run "*PrecompileWebsite.exe --clean --loglevel Information*". This may run for a couple of minutes.

For additional flags and options, run "*PrecompileWebsite.exe --help*".

Metrics Calculation Maintenance

Important! Complete the following procedure as part of metric calculation maintenance and to ensure metric calculations fire correctly after upgrade. Resynchronizing metric calculations is a mandatory step, and only needs to be run once per upgrade procedures.

To run metric calculation maintenance:

1. Stop IIS and all Accolade services except for cache services.

   Note: If you have a load balanced configuration, you will need to stop IIS and the above services on all servers.

2. Open the Accolade Administration Console on the application server.
3. Clear the cache by navigating to the **Distributed Cache Configuration** tab, clicking **Clear Cache** to clear the distributed cache, and click **Apply**.
4. Navigate to the **Maintenance Configuration** tab.
5. Click **Apply** to run the metric formula resynchronization, and confirm that you want to run it at this time.
6. Ensure metrics returned as successful in the Results column of the table. Click **Export** to review the error log and correct any metrics returned with error messages.

   Note: You must correct the metrics returned with error messages manually in the application. Rerun the resynchronization to display the metrics again and to ensure the corrected metrics return successfully.

7. Restart IIS and all Accolade services.

Restoring Back Up Files

Restore the files that you backed up before the upgrade.

File Type	Notes

Log Files	If you backed up your old log directories, you can copy them to the new installation directories on the application server.
	• Copy Logs data to:
	`<install location>\Sopheon\Accolade\Website\Logs`
	• Copy Log data to:
	`<install location>\Sopheon\Accolade\Log`

Custom Database Objects	If you backed up any custom views, stored procedures, functions or triggers, restore them to the database they originated from.
Other Customizations	If you backed up any custom icons before the upgrade, restore them to the **IconSets** folder where Accolade is installed: `C:\Program Files\Sopheon\Accolade\Etc\IconSets` **Important!** Icons have changed to the .svg filetype in Accolade v13.0. If you are upgrading from any 11 or 12 version to 13.0.0 or later, you will need to update the icons prior to re-applying them after the upgrade. If you backed up any custom Web pages or DLLs, restore them to their appropriate locations. Contact Sopheon Customer Support to check whether these customizations are still valid in the new Accolade version.

Configuring Client Computers After Upgrade

As part of the upgrade process, make the following changes on the computers of the employees using Accolade.

- **Install all Microsoft Windows Important Updates** - All Windows important updates must be installed from Microsoft Update.
- **Install new add-ins and complete client configuration** - Complete the configuration of client computers by installing the new versions of the Sopheon Client Service and the Accolade Office Extensions add-in. See "Configuring Client Computers" on page 65.

Note: The Accolade MS Project Integration add-in has been combined with the Accolade Office Extensions add-in as of Accolade v.13.2. Installing the new version of Accolade Office Extensions will update with the latest functionality for all Microsoft applications, and will automatically remove the old add-in components.

Running the Post-Upgrade Scripts

Run the post-upgrade scripts on the Accolade and snapshots databases. To run scripts, you must log in to SQL Server with the appropriate rights of the database owner. See "Database Prerequisites" on page 16.

To run the post-upgrade scripts:

1. In the installation software, browse to the following folder:

   `Server Installation (Database)\Database Scripts\Post Upgrade`

2. Open the **Accolade v17.1 - Main - Post Upgrade.sql** script.
3. Select the Accolade database and run the script.

   This script removes several database tables that are now obsolete.

4. In the same folder, open the **Accolade v17.1 - Snapshots - Post Upgrade.sql** script.
5. Select the snapshots database and run the script.

Upgrade Complete

This completes the Accolade upgrade. For instructions about logging in to Accolade, see "After Installation" on page 99.

Chapter 7

After Installation

This chapter describes how to log in to Accolade for the first time after the installation is complete. It also refers to other sources of information about Accolade.

Note: Accolade uses extra resources for analytics and support.

With Version 17.1 and forward, for end-users to utilize the Accolade Online Help, ensure that client-machines can access the URL: https://support.sopheon.net/.

Version 17.1 includes integration with Pendo.io for anonymous application usage statistics. Access to these URLs is required for proper analytic functionality:
https://cdn.pendo.io
https://data.pendo.io
https://app.pendo.io

If CDNs are not allowed on the server, or access to the URLs cannot be provided, turn the Product Experience parameter to *0* in the Accolade Administration Console.

Logging in to Accolade as the First User

To log on to Accolade as the very first user, you must have set up the initial administrator's user name and password correctly as described in "Running the Initial Configuration Wizard" on page 30, and you must log in as that user if you are using Basic authentication.

1. Open a web browser and enter the URL of your Accolade server.
2. Do one of the following to log in to the Accolade application:
   - If you are using Windows Authentication, either ensure that you are logged in to the Accolade server as the user that was specified in the Administration Console, or browse to the fully qualified domain name of the Accolade website and enter that user's credentials when prompted.
   - If you are using Basic authentication, enter the Administrator user name and password in the dialog box and click **OK**.

   The Accolade home screen for your assigned user role displays.

Additional Accolade Documentation

Additional information about configuring and using Accolade can be found in the following sources:

- **Accolade Administrator's Guide** - Familiarize yourself with the *Accolade Administrator's Guide* before putting Accolade into production. The guide describes configuration settings that should be considered for both functional purposes and performance tuning, and describes the actions that an administrator takes to set up and maintain Accolade.
- **Accolade Online Help** - Use the online Help accessible from within the Accolade application for information about using Accolade, including explanation of the Accolade tasks and concepts, help on getting started with Accolade, and procedural information for doing your job within Accolade.
- **Accolade Office Extensions Online Help** - Use this online Help for information about how to use the Accolade integration with Microsoft application documents and reporting. Available from within the Word, Excel, PowerPoint, and Project applications after installing the Accolade Office Extensions add-in.
- **Portfolio Optimizer Online Help** - Use the online Help available from within Portfolio Optimizer for information about how to use Optimizer to manage and evaluate a portfolio of projects.
- **Accolade Web API** - Use the online Help available directly within the Web API that describes methods used to customize Accolade using the Web API. Go to http://<server>/Help/apiHelp.

Optional Scripts

You can run optional database scripts for various reasons after upgrade or installation. Run the following scripts as needed.

Important! Running these scripts in the wrong circumstance can result in unintended changes to your data. Contact Sopheon Customer Support prior to running, to ensure that you protect the integrity of the data and don't inadvertently cause problems.

- **Comprehensive Layout Populate Script.sql** - Re-adds the Comprehensive landing page layout with pre-populated pods and formatting.
- **Constraints Resync Script (Core).sql** - Removes and recreates all constraints on the main Accolade database.
- **Constraints Resync Script (Snapshot).sql** - Removes and recreates all constraints on the Snapshots database.
- **Delete Temporary Scenarios.sql** - Removes any temporary scenario from the system.
- **Extend Metric Reporting Tables.sql** - Expands the number of metrics, matrix metrics, and reference tables that can be reported on in Accolade.
- **Focused Layout Populate Script.sql** - Re-adds the Focused landing page layout with pre-populated pods and formatting.
- **Migration Extension_AddTargetTeamLeaderAsSourceTeamMember.sql** - Adds the team leader of the target project as a team member of the source project on project migration.
- **Migration Extension_AddProjectLink.sql** - Creates a project link from the source project to the target project on project migration.
- **Migration Extension_DateMetrictoEndDate.sql** - Migrates the date named @DateMetricSystemName from the source project to the end date of the target project on project migration.
- **Migration Extension_DateMetrictoGateDate.sql** - Migrates the date named @DateMetricSystemName from the source project to the Gate Date of the gate named @GateName in the target project on project migration.
- **Migration Extension_DateMetrictoStartDate.sql** - Migrates the date named @DateMetricSystemName from the source project to the start date of the target project.
- **Migration Extension_MatrixDatesToGateDates.sql** - Migrates the gate dates defined in a matrix within the source project to the Gate dates of the target project.
- **Migration Extension_UpdateProjectCode.sql** - Appends the delimiter and string to the end of the source project code and apply it as the project code of the target project.

For example, @Delimiter =N'.' and @String Format = ' ### ' would take a source project code of 123 and make it 123.001. It will increment until the project code is unique.

- **PLN_MyProjectsGridView_Populate.sql** - Re-adds the default My Projects Gantt View if it is missing.
- **Project Gates Layout Populate Script.sql** - Creates a new default Gate layout with pre-populated pods and formatting.
- **Project Home Layout Populate Script.sql** - Re-adds the default Home system layout with pre-populated pods and formatting.
- **Project TimeView Layout Populate Script.sql** - Creates a new default Project Time View layout with pre-populated pods and formatting.
- **Recalculate Assignment Visibility By Process Model.sql** - Recalculates the visibility of all project deliverables and activities under the specified process model, using current propagation rules as though a process model update had just taken place.
- **Resync Asynchronous Data Script.sql** - Resyncs selected Reporting tables and optionally searches errors for tables needing resync. Before running this script, all connected servers should be disconnected and IIS should be shut down, and Qlik services must not be reloading.
- **Synchronize Non-Manual Deadline and Finish Dates.sql** - Updates settings and dates for all project deliverables and project activities Finish dates to match their corresponding non-manual Deadlines.
- **Vertical Tab Replacement Script.sql** - Removes all vertical tabs through the system.

To run an optional script:

Important! Sopheon recommends stopping IIS and all Accolade services on the application server prior to running any of these scripts.

---

1. Stop IIS and all Accolade services except for cache services.
2. Browse to the installation software and open the following folder:

   `Server Installation (Database)\Database Scripts\Other Scripts`
3. Select the Accolade database script(s) to run.
4. Once all scripts have been run, open the Accolade Administration Console on the application server.
5. Clear the cache by navigating to the **Distributed Cache Configuration** tab, clicking **Clear Cache** to clear the distributed cache, and click **Apply**.
6. Restart IIS and all Accolade services.

Chapter 8

Uninstalling Accolade

This chapter describes the process for uninstalling Accolade. The Accolade uninstallation is divided into the two following general steps:

1. Uninstall the Accolade application.
2. Uninstall the Accolade Cache service.

Uninstalling the Accolade Application

To uninstall the Accolade application:

1. Log on to the Application Server.
2. Open Command Prompt, and enter the following: `iisreset /stop`. This stops IIS services.
3. Open Windows Services. Locate the following services, right-click on each, and select **Stop**.
    - Accolade Active Directory Service
    - Accolade Auto Loader Service
    - Accolade Cache Service
    - Accolade Timed Task Service
4. Open Windows Apps & Features.
5. From your list of programs, locate **Accolade v17.1 Server**, and click on **Uninstall**.

You have successfully uninstalled the Accolade application. However, this process is not complete unless you uninstall Accolade Cache services as well.

Uninstalling Accolade Cache Services

Important! You must have the Accolade installation media downloaded.

To uninstall Accolade Cache services:

1. Open Windows PowerShell, as an Administrator.
2. Browse to the Accolade installation media and open the following folder:

    `MediaSkeleton1\Server Installation (Application)`
3. Select and load Uninstall_AccoladeCacheService.ps1.
4. Run the script.

You have successfully uninstalled Accolade Cache services.

Once both the Accolade Application and Accolade Cache services are successfully uninstalled, Accolade is completely uninstalled.

Appendix A

Enabling and Configuring the MSDTC Service

Enabling the MSDTC Service is required only when the Accolade databases and the application are installed on separate computers.

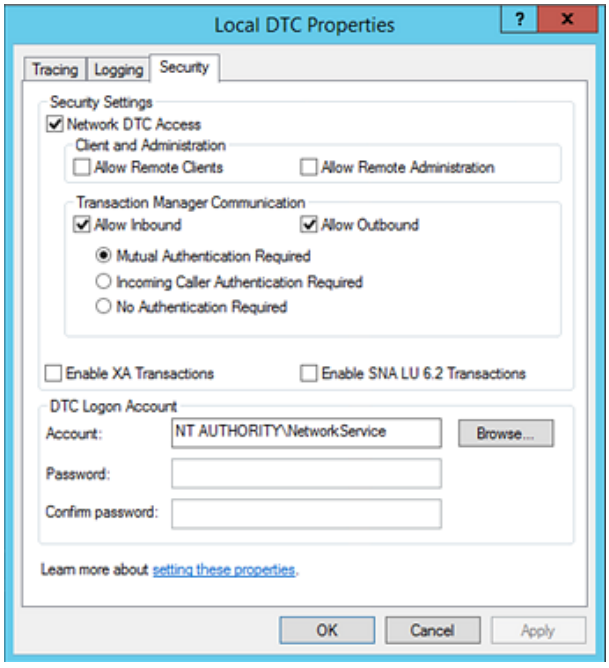
Configuring MSDTC Service on Windows Server 2019 and Windows Server 2022

To configure the MSDTC Service security settings:

Note: The MSDTC service is enabled and running by default on Windows Server 2019 and Windows Server 2022. Confirm that the MSDTC service has started and ensure that the same security settings for the MSDTC service are configured on both the database and application servers.

1. In **Administrative Tools**, open **Component Services**.
2. In the console tree, select **Services**.
3. In the list of services, ensure that the **Distributed Transaction Coordinator** is started, and its startup type is **Automatic (Delayed Start)**.

   To modify status or startup type, right-click **Distributed Transaction Coordinator**, and click **Properties**. To set the startup type, select **Automatic (Delayed Start)** in the **Startup Type** list. To start the service, click **Start**.
4. In the console tree, expand **Component Services > Computers, My Computer**, and then **Distributed Transaction Coordinator**.
5. Right-click **Local DTC** and select **Properties**.
6. In the Local DTC Properties dialog box, select the **Security** tab.



7. Ensure that the **Network DTC Access** check box is selected.
8. In the **Transaction Manager Communication** section, ensure that the **Allow Inbound** and **Allow Outbound** check boxes are selected, and then select the authentication type.

   The **Incoming Caller Authentication Required** option should only be used for Windows 2019 and 2022 servers in a clustered environment.

   Important! Ensure that the same authentication type is selected on both the application and database servers.

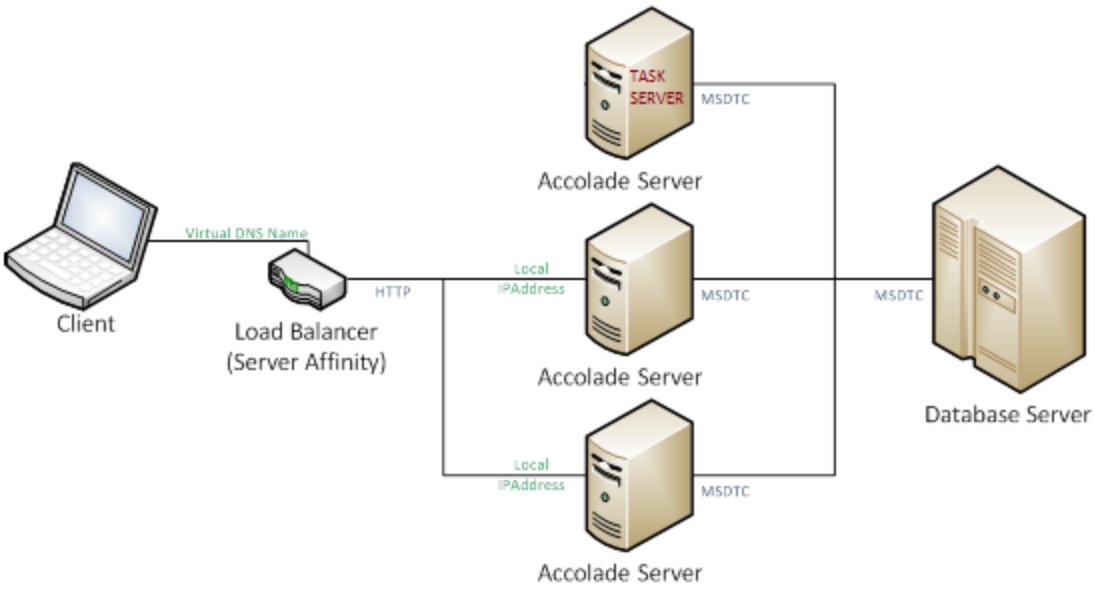
   ---

9. Click **OK** to close the Properties dialog box, right-click **Distributed Transaction Coordinator** in the list of services and select **Restart**.

Appendix B

Load Balancing - High Availability

An Accolade Server Farm consists of multiple Accolade servers accessible through a load balancer that communicates with a single Accolade database. An Accolade server farm can provide load balancing, high availability, or both.



Load Balancer Configuration

Configure the load balancer to use Source Address Persistence, routing client requests from a given source address to the same physical Accolade server each time within a given time frame. Source Address Persistence is required to support certain document upload and download operations that require multiple client requests to the same physical Accolade server. The Source Address Persistence timeout setting needs to be at least as large as the other Accolade configured timeout values, and slightly longer than the IIS Upload timeout.

Database Server Configuration

Accolade requires Microsoft Distributed Transaction Coordinator (MSDTC) communication between the database server and each of the Accolade servers in the farm. Configure MSDTC as specified in "Enabling and Configuring the MSDTC Service" on page 105. Ensure that the MSDTC on the database server can communicate with each Accolade server in the farm via the NETBIOS name and that a firewall does not block MSDTC communication.

Accolade Server Configuration

Use the following instructions and guidelines to configure the Accolade server.

1. Designate one server in the farm to install first and to become the “Main” Accolade Task server.

   This server runs all Accolade tasks, such as transform database errors, to event log entries, processes email notifications, and perform shared data cleanup operations. All other servers run a subset of these tasks. Any Accolade server in the farm can be promoted to the “Main” Task Server by re-enabling the tasks that are disabled when configuring a non-“Main” task server in the farm.

   Configure only one server in the farm as the “Main” Task Server at a time. The “Main” Task Server does not need to be included in the Web server farm.

2. For all Accolade servers in the farm, perform the preexistence installation tasks and initial installation of Accolade described, (all steps prior to the Accolade Administration Console Wizard) following the standard instructions in Chapter 3 of this guide.

3. Run the Accolade Administration Console Wizard on the first server in the farm, following the standard instructions in Chapter 3 of this guide, with the following changes:

   - Specify the virtual DNS name (load balancer name) on the Website Configuration page. This name is the same for each server in the farm.
   - Specify the local IP address of the server on the Website Configuration page. This address different for each server in the farm.

4. In the **Tasks.config** file located in *<installdir>*\Accolade\Configuration folder, comment out the task entry for each of the following shared tasks on each non-"main" Accolade

Task server in the server farm. Use standard XML comment syntax to make the requested changes. Example - <!--<Element to be commented out />-->

- ApplicationInsightsDatabaseInfoTask
- InstantNotificationTask
- StatusNotificationsTask
- ReportNotificationsTask
- RetrieveDatabaseErrorsTask
- PurgeUserAccessLogTask
- PurgeScenariosTask
- ResyncUserAccessTask
- LicenseInfoEmailTask
- ReportGeneratorExportsTask
- DARuleRunnerDailyTask
- DARuleRunnerWeeklyTask
- DARuleRunnerMonthlyTask

Also, ensure the following tasks are only running on the main Accolade server:

- DASyncSourceConnectorsTask
- ProcessPostImportEventsTask
- TimedMetricCalculationsTask
- CacheDatabaseDependencyPollingTask
- ScheduledProjectTrendingTask

Ensure that the TimedTaskService is also running on every server and enable the following tasks on every server in the farm:

- PurgeFilesTask
- ProcessPendingMetricCalculationsTask

The following task is included for support remediation and should not be run under normal circumstances:

- RedisClearCacheTask

5. Load balanced configurations using Active Directory integration should also ensure that only one server (such as the main server) is running the "Accolade Active Directory Service". On all other servers, that Windows Service should be disabled.
6. Run the Accolade Administration Console Wizard for each additional server in the farm, following the standard instructions in the *Sopheon Accolade Administrator's Guide*. The wizard automatically populates values after the database configuration page. Ensure that these values are correct before continuing.

7. Configure all servers in the farm to use a shared static machine key for the Accolade website.
   - From within IIS Manager, double-click **Machine Key** in the **ASP.Net** area.
   - In both the **Validation Key** and **Decryption Key** sections, clear the **Automatically generate at run time** option and the **Generate a Unique Key for each application** option.
   - In the Actions panel on the right, select **Generate Keys** and click **Apply**.
   - Copy and paste the generated keys into each load balancer node and click **Apply**.
8. If using the MS Project Viewer, add the public website name / vanity name of the Accolade web farm to the hosts file on each Accolade application server with IP address 127.0.0.1.

   The hosts file is usually located at C:\windows\system32\drivers\etc\. Open the file with Notepad. If, for example, the website vanity name is Accolade.Acme.net, add the following two lines to the bottom of the hosts file on each server:

   127.0.0.1 Accolade.Acme.net

   127.0.0
9. Configure the webfarm to use a shared key ring location for Data Protection.
   a. Create a network location for the shared key ring like `\\server\share\keys`; make sure the Accolade website's Application Pool identity has the full control permission on the network share; the Application Pool identity is usual the Network Service account

   b. Create a X509 Certificate to be used for data encryption; the certificate should include the private keys

   c. On all servers:

      i. Install X509 Certificate in the LocalMachine\My store; make sure the X509 certificate is readable by the Accolade website's Application Pool identity by adding the IIS_IUSRS group to the certificate's ACL in the Certificate Store.

      ii. Update the Website\web.config file with the shared key ring location and the X509 certificate thumbprint:

```
<appSettings>
     <add key="auth:Key:Path"
     value="\\server\share\keys" />
     <add key="auth:Key:CertificateThumbprint"
     value="6c8**********************************b"
     />
</appSettings>
```

iii. Update the WebsiteCore\appsettings,Production.json file with the shared key ring location and the X509 certificate thumbprint:

```
{
      "DataProtection": {
        "KeyPath": "\\server\share\keys",
        "CertificateThumbprint":
        "6c8**********************************b"
      }
}
```

When upgrading to new versions of Accolade, you will need to reestablish links between the servers in the load balanced configuration. Do this by navigating to the Distributed Cache page of the Administration Console on one of the servers and clicking **Apply**.

Ensure that each application server in the configuration is set to the same time zone.

SSL

Accolade requires that the certificate used on all endpoints match exactly. The load balancer SSL certificate must be the exact same certificate that each Accolade application server in the farm uses. See "Enabling Secure Sockets" on page 62 for more information.

SSO

Once SSL is in place, SSO can be configured. See "Setting Up Authentication" on page 72 for more information.

Note that certificates should still point to themselves and not the load balanced machine.

Runtime Operations

- Perform any changes to the Accolade website or file system on all servers in the farm.
- Parameter changes are shared across all servers in the farm.
- Manually recycle the Accolade and Accolade Services IIS Application pools whenever the Administration Console is used to change the server configuration. Restart running Accolade Windows service excluding the cache windows service.

  If the settings do not update, shut down previously running non-cache services and websites on each load balanced machine, click **Clear Cache** in the Distributed Cache page in the Administration Console, and bring websites and services back up.
- Install server patches to all servers in the farm. All servers must be taken offline for patch installation unless explicitly allowed in the patch instructions.

- There should always be only one Task server in the farm. Configure this server to act as a web server or to only handle Accolade tasks.
- The Autoloader service can run on any server in the farm but Sopheon recommends running it on one server at a time.

Fail Over Operations

If a server in the farm fails and the load balancer re-routes future requests for a client, that client may experience an error if the server transition occurred during certain file upload or download operations. In the event of this type of failure, the client may re-issue the request without compromising data integrity.

Designate a new Accolade Task server if the original Task server fails or becomes unavailable. To promote any server to the Task server, re-enable the tasks that were commented on from the **Tasks.config** file in step 4 above. If the original Task server could come back online, comment out the tasks listed to demote it. Deadlocks can occur or event log data can be lost if more than one server is configured as the Task server.

No other servers in the configuration should have the 'failed' server used as a designated cache server. If a server in the configuration is used as a 'failed' server, it will need to be switched over to use a different server for its cache provider for get requests or have no entry to default to the master. If each application server uses the cache server hosted on itself, 'failed' servers used as designated cache servers should not be a concern.

Changing Application Servers

You may need to re-purpose a server used in a load balanced configuration for another configuration, such as shifting resources between Dev and Test environments. To set up a distributed cache server in a load balanced configuration, see "Setting Up Distributed Cache Servers " on page 40.

To remove a machine from its current load balanced configuration:

1. From the Administration Console of the application server you want to remove from load balanced configuration, navigate to the Distributed Cache Configuration page.

   If the machine is hosting the current Distributed Cache master, select a different server to be the master and click **Apply** to save your changes.
2. Click the **Cache Servers** tab and select the **Remove** check box. This disconnects the cache server from the other servers in the network and any designated usages against it. Click **Apply** to save your changes.
3. Navigate to the Database Configuration page and enter the details for the database the machine should point to. Click **Apply** to save your changes.

4. Navigate to the Distributed Cache Configuration page and ensure the Cache Server tab lists the newly configured server. Machines should be able to connect to that database server.
5. Enter the machine domain name and cache port on the Cache Server tab.
6. Click the **Usages** tab and enter the machine name and its hosted cache server. Click **Apply** to save your changes.
7. Reset IIS on all application servers in the configuration.

Appendix C

Application Server Roles, Role Services, and Features

This appendix lists the roles, role services, and features in the standard installation on the application server.

Roles and Services in Windows Server 2022

Compare this list to the list shown in the Server Roles and Features sections of the Server Manager to ensure you have installed all the needed items on a Windows 2022 server.

Other roles than those listed here might also be installed. The roles and features below are required for Accolade to run successfully.

Web Server (IIS) Role

Displays in the Server Roles section of the Server Manager.

- Web Server > Common HTTP Features
  - Default Document
  - Directory Browsing
  - HTTP Errors
  - Static Content
  - HTTP Redirection
- Web Server > Health and Diagnostics

    - HTTP Logging
    - Logging Tools
    - ODBC Logging (selected if SMTP Server is selected)
    - Request Monitor
    - Tracing
- Web Server > Performance
    - Static Content Compression
    - Dynamic Content Compression
- Web Server > Security
    - Request Filtering
    - Basic Authentication
    - Client Certificate Mapping Authentication
    - Digest Authentication
    - IIS Client Certificate Mapping Authentication
    - IP and Domain Restrictions
    - URL Authorization
    - Windows Authentication
- Web Server > Application Development
    - .NET Extensibility 4.8
    - Application Initialization
    - ASP
    - ASP.NET 4.8
    - CGI
    - ISAPI Extensions
    - ISAPI Filters
    - Server Side Includes
    - WebSocket Protocol
- Management Tools
    - IIS Management Console
- Management Tools > IIS Management Compatibility
    - IIS Metabase Compatibility
    - IIS Management Console
    - IIS Scripting Tools

- IIS WMI Compatibility

Features

Displays in the Features of the Server Manager.

- .NET Framework 4.8 Features
  - .NET Framework 4.8
  - ASP .NET 4.8
  - WCF Services
    - HTTP Activation
    - Message Queuing (MSMQ Activation)
    - Named Pipe Activation
    - TCP Activation
    - TCP Port Sharing
- Management OData IIS Extension
- System Data Archiver
- Windows Process Activation Service
  - Process Model
  - Configuration APIs

Roles and Services in Windows Server 2019

Compare this list to the list shown in the Server Roles and Features sections of the Server Manager to ensure you have installed all the needed items on a Windows 2019 server.

Other roles than those listed here might also be installed. The roles and features below are required for Accolade to run successfully.

Web Server (IIS) Role

Displays in the Server Roles section of the Server Manager.

- Web Server > Common HTTP Features
  - Default Document
  - Directory Browsing
  - HTTP Errors
  - Static Content
  - HTTP Redirection
- Web Server > Health and Diagnostics
  - HTTP Logging
  - Logging Tools
  - ODBC Logging (selected if SMTP Server is selected)
  - Request Monitor
  - Tracing
- Web Server > Performance
  - Static Content Compression
  - Dynamic Content Compression
- Web Server > Security
  - Request Filtering
  - Basic Authentication
  - Client Certificate Mapping Authentication
  - Digest Authentication
  - IIS Client Certificate Mapping Authentication
  - IP and Domain Restrictions
  - URL Authorization
  - Windows Authentication

- Web Server > Application Development
  - .NET Extensibility 4.7
  - ASP
  - ASP.NET 4.7
  - ISAPI Extensions
  - ISAPI Filters
- Management Tools
  - IIS Management Console
- Management Tools > IIS Management Compatibility
  - IIS Metabase Compatibility
  - IIS Management Console
  - IIS Scripting Tools
  - IIS WMI Compatibility

Features

Displays in the Features of the Server Manager.

- .NET Framework 4.7 Features
  - .NET Framework 4.7
  - ASP .NET 4.7
  - WCF Services
    - HTTP Activation
    - Message Queuing (MSMQ Activation)
    - Named Pipe Activation
    - TCP Activation
    - TCP Port Sharing
- Management OData IIS Extension
- System Data Archiver
- Windows Process Activation Service
  - Process Model
  - Configuration APIs

Appendix D

Database and Server Management

This appendix includes procedures for several database and server management tasks for the Accolade and snapshots databases, including moving, restoring, and renaming the database. It also includes the procedure for increasing the number of scenarios databases and for updating service account passwords for Accolade and Dashboards for Accolade.

Renaming Databases

If you rename a database, for example as part of restoring it, run the stored procedure **SGM_CreateSynonyms** on the database after renaming the database.

- This procedure is not necessary if you are only upgrading your Accolade version.
- If you rename the main database name, for example from “Accolade” to “NewName”, you must also rename the snapshots database. In this example, you would rename the snapshots database to “NewName_Snapshots”.

To rename a database:

1. In **SQL Server Management Studio**, connect to the database you have renamed.
2. Run the following the statement: `exec SGM_CreateSynonyms.`
3. Re-create the scenario databases you need. See "Creating the Scenarios Databases" on page 19.

Restoring the Accolade or Snapshots Database to a Different Server

Prior to restoring the Accolade or snapshots databases to a different server, stop Accolade including:

- Accolade Autoloader Service
- Accolade Timed Tasks Service
- IIS

Ensure that the SQL server version on the new server is the same or greater than the version on the original server.

Note: The following procedure applies to the Accolade and snapshots databases. Ensure that you select the correct database as you are working through each step.

To restore a database to a different server:

1. Back up the database, copy it, and restore it on the new server.
2. In SQL Management Studio, on the **Options** page, ensure that the **Compatibility** level is equal or greater than the minimum requirement for Accolade.
3. Browse to the **Other Scripts** folder in the Server Installation (Database) software and open **Prepare Restored Database Script.sql**.
4. Replace <*NewDBOwner*> with the SQL login of the database owner and run the script.

This user should always have the **sysadmin** role on the SQL Server instance.

5. In the **Logins** folder, delete and then re-create the login of the database service account.

   You must re-create the service account login because it still has an ID from the original server. Configure the login's settings as follows:

   - Set the **Default Language** to **English**.
   - In the User Mapping page, select the database, ensure the **public** role, and assign the **SGM_Write** role.

6. If you are restoring the Accolade database, in **SQL Server Management Studio**, run the following statement against the database: `exec SGM_CreateSynonyms`.
7. In the Accolade Administration Console, click **Tools** and run the Install Wizard, entering the appropriate settings on each page.
   - Enter the correct names, URLs, and other settings in the **Database Configuration** and **Website Configuration** pages.
   - On the **Administrator Login** page, note any new logins to create or delete.
8. Create the scenario databases as needed following the instructions "Creating the Scenarios Databases" on page 19.
9. Open the Administration Console on the Application server that will be used with this database, and complete the following :
   - Open the Database Configuration tab and enter the information for the database you just restored.
   - Open the Distributed Cache configuration and set the Cache Servers and Usages for this new environment.
   - Open the Website Configuration tab and update the Website configuration settings for this new environment.

Changing the Service Account Password

As your policies require, update the service account passwords for Accolade and Dashboards for Accolade. How often you update these passwords depends on the security policies and procedures in place at your company.

To change the service account password:

1. On the application server, stop all Accolade services and all Qlik services, including the following:
   - Qlik Directory Service Connector
   - Qlik Distribution Service
   - Qlik Management Service

- Qlik Server
- Qlik Settings Service

2. Update the password for the service account(s) in the services console on the server(s) where the account is used.
   - Accolade services
   - Qlik Server services
   - Monthly Snapshot job
3. Update the pool identity password, including the following:
   - Qlik IIS application pool identity
   - Accolade application pools identify if the you change the identity as described in "Secure Network Best Practices" on page 126.
4. Update the password for the Accolade database account in the Database Configuration section of the Accolade Administration Console.
5. Change the password for the Accolade database account in SQL, or in Active Directory if you use Active Directory for authentication.
6. Restart the Accolade and Qlik services you stopped in step 1.
7. Test and verify access after the services restart.

Secure Network Best Practices

If the Network Service within your network setup does not have access across the network, set the application pools to use and the Accolade services to use a domain user and add that user to the Accolade website configuration.

When using Windows Integrated Authentication for Accolade Database Login, IIS Application Pool Identity must either be Network Service or the same Windows User as used for the Database Login.

To update the site's Application Pool Identity settings, see the Application Pool User section in Running the Initial Configuration Wizard.

To set the Accolade Application Pools Manually to Use a Domain User:

1. On the application server, open the **Internet Information Services (IIS) Manager**.
2. In the Connections tree, select **Application Pools**.
3. Right-click the **Accolade Main Web site** pool and select **Advanced Settings**.
4. In the **Process Model** section, locate the **Identity** field and click **...** to display the properties.
5. Select **Custom Account**, click **Set**, and enter the login information for a domain user that has access to the Accolade database.

6. Click **OK**.
7. Repeat these steps to assign the same domain user to the **AccoladeOptimizer** and **AccoladeServices** pools.

To set the Accolade Services to Use a Domain User:

1. On the application server, open the **Server Manager**.
2. In the Console tree, select **Configuration > Services.**
3. Right-click the **Accolade Timed Task Service** and select **Properties**.
4. Select the **Log On** tab and select **This Account**.
5. Set the login information to the same domain user you set for the Application pools.
6. Click **OK**.
7. Repeat these steps to assign the same domain user to the **Accolade Active Service** and the **AccoladeAutoloader service**.

   The procedures may vary slightly, depending on the server version.

To add the Domain User to the Accolade Website Configuration:

1. On the application server, open the Accolade Administration Console.
2. In the Navigation pane, select **Website Configuration**.
3. In the **Windows Groups** field, add the domain user defined for the Accolade application pools and services.
4. Click **Apply**.

Appendix E

Accolade System Parameters

This appendix lists and describes the Accolade parameters available in the Accolade Administration Console and explains their allowed values.

Within the console, drag the Name column (and the console itself) wider to make overlapping parameter names easier to read.

License Keys

Use the license key parameters to enter the keys for optional add-on Accolade features. Sopheon provides these license keys to you or enters them for you in the Administration Console:

- Collaborative Workflow License Key
- Data Analytics License Key
- Extended Project Edit Rights License Key
- Idea Submission License Key
- Innovation Planning License Key
- MS Project Integration Key
- Portfolio Center License Key
- Resource Planning License Key
- Time Tracking License Key

Mail and Notifications

The following parameters apply to the internal emailing capability within Accolade, including sending notifications about system events by email:

Display Name	Description	Default Value
Enable Notifications*	Enables or disables notifications through email for events such as deliverables not being ready for an upcoming date.	1
Enable Simple Email Support	Enables or disables Simple Email through Accolade.	0
Email Separator	The separator character to use for emails addressed to multiple recipients.	; (semicolon)
Send Empty Schedule Email Notification	Whether or not to send a scheduled email, even if no events have occurred.	0
Send Emails for Late Assignments in Stages Set to Conditional Go	Enables or disables sending emails for assignments that are late in stages that have a corresponding gate decision set to Conditional Go. Conditional Go is available as a gate decision if the **Disable Conditional Go Gate Decision** parameter is set to **0**.	0

Display Name	Description	Default Value
Send Scheduled HTML Report Notifications	Enable scheduled send of HTML report notifications.	1
SMTP SSL Connection Mode	SSL Setting for connection to SMTP Server: **None**: Provided for legacy compatibility. **Opportunistic**: Elevates the connection to use TLS encryption immediately after reading the greeting and capabilities of the server, but only if the server supports the STARTTLS extension. This is provided as a compatibility option. **Forced**: Elevates the connection to use TLS encryption immediately after reading the greeting and capabilities of the server. If the server does not support the STARTTLS extension, then the connection will fail. Most Secure option.	0
SMTP SSL Trusted Cert Thumbprint	The thumbprint of the SSL cert used by the SMPT server. Used for troubleshooting connection errors by removing validation against a trusted certificate with a matching thumbprint.	
Advanced Parameters		
Email Address to Send License Information	The email address to which to send license information. Typically an internal support address.	N/A
Last Status Report Send Date	The day of the month that notification status reports were last processed.	N/A
Notification Delivery Return Address*	The email address used to send notification emails from Accolade.	N/A
SMTP Connection String	*(Read Only)* The SMTP connection string for sending email notifications.	N/A
Allow usage of CallStoredProcedure	Enable usage of CalledStoredProcedure function in Metric Formulas.	0

* This parameter can also be set within Accolade in **Process > Configuration > Parameters**.

Privacy

The following parameter applies to reports generated from Accolade and Accolade Office Extensions:

Display Name	Description	Default Value
Report Privacy Warning Text*	The text included at the top of each report to indicate privacy of the report content (500 characters). Enter the warning text in the language you would like it to display.	Blank
Advanced Parameters		
Enable System Consent Prompt	Whether or not to show the User Consent prompt if users have not previously consented.	Blank

* This parameter can also be set within Accolade in **Process > Configuration > Parameters**.

Process

The following parameters apply to flow of projects from creation through their model structure:

Display Name	Description	Default Value
Allow Document Owners to Set Deadline	Enables or disables document owner's ability to set the deadline date for documents they own. When disabled, Project Managers or Process Managers can set the deadline date for documents within projects.	0
Allow Document Owners to Set Function	Enables or disables document owner's ability to set the function for document they own. When disabled, Project Managers or Process Managers must set the function for documents.	0
Allow Document Owners to Set Start Date	Enables or disables document owner's ability to set the start date for documents they own.	0

Display Name	Description	Default Value
	When disabled, Project Managers or Process can set the start date for documents within projects.	
Allow Project Owner to Set Gate Dates	Enables or disables project owner's ability to update a gate date from the progress graphic on a current or future gate that has the status of Pending Decision.	0
Allow Team Members to Share Assignments	Enables or disables team member's ability to assign themselves as a document owner within a project.	1
Auto-Generate Project IDs*	Enables or disables automatic system generated project IDs. If set to **0**, project creators enter their own project ID when creating a project.	0
Automatically Publish Submitted Ideas*	Enables or disables the automatic publication of documents attached to submitted ideas.	0
Default New Versions to Published*	Enables or disables the automatic publication of new versions of an existing document. **Important!** Process Designers can set publish options for individual deliverables and activities in process models that override this system parameter. Project deliverables and activities with different publish settings than the system parameter, respect the setting in the process model. Activities added to deliverables in projects, however, respect the system parameter.	1
Disable Conditional Go Gate Decision	Enables or disables the ability to set a gate decision to Conditional Go. When a decision is set to Conditional Go, one or more condition must be met before the next gate meeting decision. When disabled, Go is the only gate decision that provides approval to proceed to the next project stage.	0

Display Name	Description	Default Value
Disable Link to File	Enables or disables the ability to link a document's source to an external document stored outside of Accolade.	0
Disable Link to Website	Enables or disables the ability to link a document's source to a website.	0
Enforce Project Security for Add Team Member	Determines if the User Select dialog box on a project only includes users who have security access to the project through access group, security list, and security profile settings. This setting applies to adding team members and project managers to a project or planning element. The default setting of **0** allows the addition of users to a project by exception, outside their security access. **Important!** If you enable this parameter, existing projects that contain users assigned outside their security access are not automatically updated. Correct any projects with security concerns manually.	0
Number of Days for Gate Meeting Warning*	The number of days prior to a gate meeting to consider assignments incomplete.	7
Restrict Discussions Tab to Project Team	When enabled, restricts the project discussions feature to only the Project Manager and project team members.	0
Show Conditional Go Assignments as Current	Determines if gates set to Conditional Go are shown as current gate in the Word pod.	1
Show Week Number in Calendar Controls*	When enabled, the calendar selection control includes the week number as the first column, and the week starts on Monday instead of Sunday. **Note:** When changing the parameter value, clear distributed cache if you have distributed cache configured	0

Display Name	Description	Default Value
	on your system and then reset IIS to prompt the system to inherit the parameter change.	
Advanced Parameters		
Allow Last Status Report to be Deleted	Enables or disables a user's ability to delete the last status report they submitted.	0
Default Deliverable/Activity Details Dialog Main Content	*(Read Only)* The default display content when opening the Deliverable/Activity Details dialog box. The default setting displays quick grids if they are available, or versions if the deliverable or activity has no quick grid assigned.	0
Disable Workflow Decline Decision	Enables or disables the ability to decline a decision within a workflow. When set to **1**, the **Decline request to review deliverable** option is not available for workflow action owners entering decisions for their workflow actions.	0
Display Extended Fields on User Selector Default	Enables or disables the display of extended fields on the User Selector dialog. When set to **1**, the extended fields will be displayed.	1
Enable Quick Grids Protected Mode	Enables or disables grids that are set to be protected (view only).	0

* This parameter can also be set within Accolade in **Process > Configuration > Parameters**.

Product Enhancement

The following parameters apply to the product enhancement system:

Display Name	Description	Default Value
Enable Product Enhancement System	Hides or shows Product Enhancement System Icon. When set to **1**, it is enabled. When set to **0**,	1

Display Name	Description	Default Value
Icon	it is disabled.	
Product Enhancement System Visibility	Shows Product Enhancement System Icon for specific roles. Enter the role codes. A blank default value will include all roles.	Blank

* This parameter can also be set within Accolade in **Process > Configuration > Parameters**.

Organization Information

The following parameters apply to organizational information:

Display Name	Description	Default Value
Advanced Parameters		
Organization Name	When configuring Accolade or upgrading to version 14.2 or higher, this field must be populated with the name of your organization. **Important!** Once a name is entered and saved, the information becomes read-only and cannot be changed.	Blank
Integration ID	Customer integration ID for Accolade to connect to Acclaim Projects. This must only be populated if your organization has purchased integration with Acclaim Projects.	Blank
Acclaim Projects URL	Fully qualified URL to the Acclaim Projects website. This must only be populated if your organization has purchased integration with Acclaim Projects.	Blank

* This parameter can also be set within Accolade in **Process > Configuration > Parameters**.

Security

The following parameters apply to security settings:

Display Name	Description	Default Value
Advanced Parameters		
Encrypt Distributed Cache Entries	If set to **1**, values stored in the Distributed Cache will be encrypted. When changing the value, restart IIS on all application servers in the load balanced configuration then clear the cache on the Distributed Cache page of the Administration console. **Important!** Enabling this parameter impacts application performance.	0
Login Metric	The system name of the metric used for the location login selection list, if you are prompting users for a location when they log in. This metric is a list or multi-select list metric. The configuration of the metric entered here becomes read-only; therefore, Sopheon recommends using a metric whose list values are defined in a reference table, so you can update the metric's values as needed.	Blank
Restrict Administrators From Updating Their Account	If set to **1**, Administrators cannot update their account through the User Administration page or by importing users when setting up Accolade user accounts.	0
Task Service Password	*(Read Only)* Encrypted password used when the task service makes a web service call. The credentials are used for authenticating users.	Blank
Task Service User	*(Read Only)* Username used when the task service makes a web service call. The credentials are used for authenticating users.	Blank

System

The following parameters apply to system-level settings, such as database and network, and are typically set once at installation:

Display Name	Description	Default Value
Active Directory Enabled	User extended fields sync with Active Directory.	0
Enable Plug-ins	Whether users can load browser plug-ins.	0
Enable User Profile Images*	Enables the ability to add an image to a user account or user profile that displays with a user's name in various locations in Accolade.	1
Maximum Number of Recent Items	The maximum number of entries that display in the Recent Items list displayable from the Accolade title bar.	50
Maximum Searchable Extended Fields	The maximum number of extended fields can be set for user searches.	5
Metrics Recalculation Chunk Size (Integer)	The number of distinct projects to include when completing metric recalculations. Contact Sopheon Customer Support before changing this setting.	100
Number of Days to Retain Error Logs	The number of days to save logs that contain system error information.	365
Number of Days to Retain User Access Logs	The number of days to save logs that contain user access information.	390
Project Thumbnail Image Height	The height of the project thumbnail image, in pixels.	80
Project Thumbnail Image Width	The width of the project thumbnail image, in pixels.	80
Replace Empty Values	Whether or not null values in Accolade reporting results are returned with values indicating blank or empty results such as [empty]. If this parameter is set to **0**, number, date, and string metrics that contain no value display as blank in reporting results.	1
Reporting Office Extensions Record Limit	The maximum number of rows returned in a report created using Accolade Office Extensions Query. Must be set to a whole, positive number.	50,000

Display Name	Description	Default Value
Advanced Parameters		
Accolade Footer Text	The text displayed in the Accolade page footers. This may be corporate or legal directives, or any text all employees in your company need to see.	Blank
Accolade Header Text	The text displayed above the Accolade main menu bar. This may be corporate or legal directives, or any text all employees in your company need to see.	Blank
Accolade Process Manager Version	*(Read Only)* The current version and build number for Accolade Process Manager.	x.x.x
Accolade Process Manager Website URL	The website address for Accolade Process Manager.	Blank
Allow Default Landing Page	Allows personalized landing pages to be selected by users.	1
Allow Restricted Project Names to be Visible	Indicates whether project names for projects selected to be hidden, display in Resource Editor and on timesheets for all users regardless of if they are on the project team or have rights to view the project.	0
Anonymous Idea Submission URL	The website address for Idea Submission.	
Application Insights Key	Defines the resource used to aggregate telemetry data.	Blank
Cancel Snapshot in Process	*(Read Only)* Indicates 1 if a snapshot is in the process of being canceled. Use for troubleshooting purposes.	0
Currency Symbol	Corporate currency symbol displayed in AOR charts and reports. **Important!** If users upload files into Accolade that contain different currency symbols not listed here, the value in this parameter will be used instead.	$
Customization	*(Read Only)* Indicates if your instance of Accol-	0

Display Name	Description	Default Value
Installed	ade is a customized version. Standard versions display 0.	
Database Filestore Buffer Size	The database filestore buffer size, in bytes.	1024000
Default Domain for Users	The default domain for login when one is not provided.	Blank
Default Search Language ID	The Local ID (LCID) the Accolade search uses.	1033
Enable Autofit Cells on Smart Excel Download	Enables or disables Smart Excel metric/metadata fields to be autofit when downloading Smart Excel document	1
Enable Autoloader Service	*(Read Only)* Indicates whether the automatic upload service is enabled.	0
Enable Client Macro Events for MS Office Add-In	Enables or disables the support of client-side macros for the Accolade Office Extensions add-in. For example, events that happen before or after saving a document.	0
Enable Customization Extensions	Enables or disables the support for customizations that use the Extension Object.	1
Enable MS Docs Date Time Stamp	Enables or disables using a date/time stamp to distinguish versions of MS Office documents that are opened more than once.	0
Enable Smart PowerPoint Documents	Enables the "smart" functionality in MS PowerPoint documents downloaded from and uploaded to Accolade. If set to **0**, users can download and upload MS PowerPoint files; however, if the file contains Accolade data, such as field codes, those values do not update.	1
Enable Stakeholders	Whether or not to enable information to be shared with outside stakeholders.	1
Enable Windows Authentication	Enables or disables Windows for user login authentication.	1
Enforce List Value Validation	Indicates if list and multilist values should be validated before saving.	0
Event Log Types to	The types of Windows event log entries to dis-	Application

Display Name	Description	Default Value
Display on Error	play when an error is triggered.	System
Fiscal Year Start Month	The number correlating to the first month of your company's fiscal year. 1 = January, 12 = December. A value of 1 defaults time intervals to calendar year by beginning with January. **Note:** This setting does not affect metric or date calculations. It only determines the time intervals in Gantt views, allowing users to align timelines according to fiscal year or calendar year.	1
Hidden Reference Table Category Name	The name of the category that contains hidden reference tables.	
Idea Management Transfer Directory Location	*(Read Only)* The path to the directory where idea submission document transfers occur.	
Max Levels in Portfolio Center	The maximum levels of project relationships to show in Dashboards for Accolade.	3
Max Process MultiThreading	The maximum number of threads the Accolade Timed Task Server uses per application server. For example, in an implementation with three application servers, if set to **4**, up to four threads are created for each application server, for a total of 12. Set to **0** to automatically set the threads based on the number of cores in the application server. The optimum setting for your Accolade implementation is dependent on your data and your application server/database server configuration. In a load balanced configuration, all servers must be included in the value. Changing this setting can affect other applications running on the database server if the server is a shared resource. If this value is changed after the initial configuration, all application servers will need	0

Display Name	Description	Default Value
	their IIS reset, as well as the Accolade Timed Task Service restarted to update the new setting. Contact Sopheon Customer Support before changing this setting.	
Maximum File Upload Size	The maximum uploaded file size allowed (in bytes). When uploading multiple files, this limit is imposed on each file in the group upload, not the upload as whole.	209715200
Maximum Filter Metrics Allowed	The maximum number of metrics allowed to be designated as filter metrics.	3
Number of Event Logs to Display on Error	The number of Windows Event Log entries to display when an error is triggered.	20
Password Change URL	The URL to a custom web page where users are able to change their local Accolade password. Leave the parameter blank to prevent users from changing their password.	Blank
Pre-Check Office File Readability	Enables or disables the check for the readability of MS Office files before adding them to the system.	0
Project Recalculation Notification Chunk Size	Sets the amount of projects to notify users of processing pending metric calculations from the Task Service. This setting is in bytes, and determines when a project indicates that calculations are processing, and when the **Recalculate All** button within metric configuration indicates that metric calculations are still processing. Contact Sopheon Customer Support before changing this setting.	100
Related Document Import Load Schedule	*(Read Only)* The scheduled time for importing related documents using the automatic upload service.	Blank
Rich Text Size Warning	Metric Size to warn the user when they are getting close to the maximum allowed metric size (in MB).	75

Display Name	Description	Default Value
	Important! The value cannot exceed 2 GB as metrics with Rich Text enabled cannot contain more than 2 GB of data.	
SignalR Transport	The SignalR transport mechanism. Separate entries using a pipe (|) delimiter. Options include: **webSockets**, **foreverFrame**, **serverSentEvents**, and **longPolling**. Note that the capitalization must match exactly to set the parameter. This parameter is only used in cross domain environments. Contact Sopheon Customer Support before changing this setting.	Blank
System Delimiter for Lists	The character used to separate items in a list metric when stored as a string.	| (pipe)
Transfer Directory Location	*(Read Only)* The path to the directory in the file system where document transfers occur.	
User Session Data Latency	The amount of time to wait after the Web session has timed out to delete the user session data.	5

* This parameter can also be set within Accolade in **Process > Configuration > Parameters**.

Accolade Portfolio Optimizer

The following parameters apply to the Portfolio Optimizer optional component:

Display Name	Description	Default Value
Portfolio Optimizer Load Requested Demands	Enables or displays requested demands from displaying in Portfolio Optimizer, along with assigned demands.	0
Portfolio Optimizer Waterline Threshold Percent*	The percentage at which to show a warning as resource demand approaches capacity.	90
Prefix for Generic Placeholder	The prefix that begins the name of every generic resource to prevent overbooked icons from dis-	[Any

Display Name	Description	Default Value
Resources*	playing in Portfolio Optimizer.	
Warn User When Uploading Data Older than (Days)*	The number of days since data was downloaded to trigger a warning to Portfolio Optimizer users uploading changes from Portfolio Optimizer.	30
Advanced Parameters		
Portfolio Optimizer Data Contract Version	*(Read Only)* Data contract version for Portfolio Optimizer communication.	x.x
Portfolio Optimizer Minimum Client Version	*(Read Only)* Minimum Portfolio Optimizer client version compatible with the server.	x.x

* This parameter can also be set within Accolade in **Process > Configuration > Parameters**.

Resource Planning

The following parameters apply to the Resource Planning optional component for Accolade Portfolio Center.

Display Name	Description	Default Value
Allow Multiple Links for an Assigned Pool	Enables or disables whether a single assigned-only pool has links to multiple requested-only pools.	0
Disable Editing on Project Resources Tab	Enables or disables whether the **Resources** page within a project is read-only.	0
Enable Extended Demand Constraints	Enables or disables Resource Editor filters that match projects to pools when adding demands.	0
Maximum Resource Demand History	The maximum number of demands that can be shown in resource demand history.	0
Maximum Time Periods to Download	The maximum number of time periods that can be downloaded into a Resource Planning Smart Excel document.	200
Minimum Time Periods to Download	The minimum number of time periods that can be downloaded into a Resource Planning Smart Excel document.	12
Resource Planning Total Divisor	*(Read Only)* The number by which capacity and demand totals should be divided to show average	1

Display Name	Description	Default Value
	monthly capacity or demand over the entire planning period.	
Advanced Parameters		
Number of Buffered Time Periods Back from the Current Period	The number of time periods before the current period that have data loaded into resource planning pages like Resource Editor when the page loads. **Important!** Set the value equal to or less than the **Periods Back** value on the Admin Console when configuring Resource Planning time periods. See the *Accolade Installation Guide* for more information on setting Resource Planning time periods.	12
Number of Buffered Time Periods Forward from the Current Period	The number of time periods after the current period that will have data loaded into resource planning pages like Resource Editor when the page loads.	60
Resource Planning Time Interval Type	*(Read Only)* Time interval in each resource planning cell (0 = weeks, 1 = months, 2 = quarters, 3 = years).	1

DataBus - Simple Queue Service

The following parameters apply to handling the direct connection to the DataBus - Simple Queue Service (SQS):

Note: To enter these parameters, you must have an AWS User with permissions to only talk to the Simple Queue Service mentioned.

Display Name	Description	Default Value
Data Bus Access Key	Key retrieved when creating the IAM user.	N/A
Data Bus Secret Key	Key retrieved when creating the IAM user.	N/A
Data Bus Region	Indicates the region that the SQS was set up (e.g.: us-east-1).	N/A

Display Name	Description	Default Value
SQS URL	The HTTPS URL of the Simple Queue Service.	N/A

Integrations

The following parameters apply to the MS Teams Integration optional component:

Display Name	Description	Default Value
MS Teams Application (client) ID	The Application (client) ID of the application registered in Microsoft Azure Active Directory.	Blank
MS Teams Directory (tenant) ID	The Directory (tenant) ID of the application registered in Microsoft Azure Active Directory (see above). The tenant ID can be a GUID (the ID of your Azure AD instance), for single-tenant applications, or a domain name associated with your Azure AD instance (also for single-tenant applications) Placeholders can also be used as a tenant ID in place of the Azure AD authority audience enumeration: • *Organizations* for a multitenant application • *Consumers* to sign in users only with their personal accounts • *Common* to sign in users with their work and school accounts or their personal Microsoft accounts	organizations
MS Teams Prompt Type	Specifies how the user should be prompted to authenticate. The prompt parameter can be used to make sure that the End-User is still present for the current session or to bring attention to the request. Space delimited, case sensitive list of ASCII string values that specifies whether the End-User is prompted for reauthentication and consent. Defined values are:	select_account

Display Name	Description	Default Value
	• **none** - Do not display any authentication or consent user interface pages. An error is returned if an End-User is not already authenticated or the Client does not have pre-configured consent for the requested Claims or does not fulfill other conditions for processing the request. Cannot be used in combination with other values. • **login** - Prompt the End-User for reauthentication. If it cannot reauthenticate the End-User, an error is returned. • **consent** - Prompt the End-User for consent before returning information to the Client. If it cannot obtain consent, an error is returned. • **select_account** - Prompt the End-User to select a user account. This enables an End-User who has multiple accounts to select amongst the multiple accounts that they might have current sessions for. If an account selection choice made by the End-User cannot be obtained, an error is returned.	
MS Teams Domain Hint	Domain hints are directives that are included in the authentication request from an application. They can be used to accelerate the user to their federated IdP sign-in page. Or they can be used by a multi-tenant application to accelerate the user straight to the branded Azure AD sign-in page for their tenant. If included, leads to a more streamlined user experience. An example of a domain hint would be a domain name such as sopheon.com.	Empty
MS Teams URI Scheme	The default URI Scheme to use for the MS Teams integration. This indicates the user experience when transitioning between Accolade and MS Teams.	1

Display Name	Description	Default Value
	0 = use the launcher (the Microsoft intermediate step which allows the user to select whether to use the MS Teams App or the web app), 1 = msteams scheme (use the MS Teams app), 2 = https scheme (use the web app).	

MS Project Integration

The following parameters apply to the MS Project Integration optional component:

Display Name	Description	Default Value
MS Project Field for Misc Data	The name of the custom field in MS Project used to store miscellaneous data.	Text26
MS Project Field for Status	The name of the custom field in MS Project used to store status data.	Text28
MS Project Filed for Status Notes	The name of the custom field in MS Project used to store status notes data.	Text27
MS Project Field for Task ID	The name of the custom field in MS Project used to store task ID data.	Text30
MS Project Field for Task Owner	The name of the custom field in MS Project used to store task owner data.	Text29
MS Project Field for User ID	The name of the custom field in MS Project used to store user ID data.	Text24
MS Project Field for User Login	The name of the custom field in MS Project used to store user login data.	Text25

Currency

The following parameters apply to the currency in which you do business:

Display Name	Description	Default Value
Advanced Parameters		
Corporate Currency	*(Read Only)* Currently selected corporate currency code. Projects can run in a difference currency.	N/A
Corporate Currency Previously Set	*(Read Only)* Indicates if the corporate currency has been changed.	0

Timeouts

The following parameters apply the number of seconds the application waits before timing out in various scenarios. These settings are typically only changed for troubleshooting purposes or to accommodate certain hardware implementation:

Display Name	Description	Default Value
Calculated Metric Process Timeout (minutes)	The number of minutes before a running calculation process times out.	60
Web Session Timeout (minutes)*	The number of minutes of inactivity allowed before a user's Accolade session times out and requires the user to re-enter their user name and password.	60
Advanced Parameters		
Database Default Command Timeout (seconds)	The number of seconds before an ordinary database command times out.	30
Database Filestore Command Timeout (seconds)	The number of seconds before a database filestore command times out.	120
Database Import Command Timeout (seconds)	The number of seconds before a data import times out.	1200
Database Import Transaction Timeout (hh:mm:ss)	The amount of time before a data import database transaction times out.	0:20:00
Database Portfolio Optimizer Command	The number of seconds before a Portfolio Optimizer database command times out.	300

Display Name	Description	Default Value
Timeout (seconds)		
Database Reference Tables Command Timeout (seconds)	The number of seconds before a reference table database command times out.	600
Database Reference Tables Transaction Timeout (hh:mm:ss)	The number of seconds before a reference table transaction command times out.	0:20:00
Database Transaction Timeout (hh:mm:ss)	The amount of time before a database transaction times out.	0:05:00
Distributed Cache Command Timeout (seconds)	The number of seconds before a distributed cache command times out. If you change this setting reset IIS and restart the Accolade Windows Services, except for the cache service.	30
Document Refresh Timeout (seconds)	The number of seconds before the refresh of a document containing field codes times out.	1200
Report Cache Sliding Expiration Timeout (hh:mm:ss)	The amount of time a report will remain in cache after the last time it is accessed.	0:00:10
Reporting Office Extensions Database Timeout (seconds)	The number of seconds before the SQL database for reporting in Accolade Office Extensions queries time out.	30
Reporting Office Extensions Timeout (minutes)	The number of minutes before reporting in Accolade Office Extensions queries time out.	10
Save to Accolade Timeout (seconds)	The number of seconds before the document being saved via the Accolade Office Extensions times out.	1200
Web API Client Credential Session Timeout (minutes)	The number of minutes before a web API client's session will time out due to inactivity.	60
Database Data Api Command Timeout (seconds)	The number of seconds before a data API command times out.	900

* This parameter can also be set within Accolade in **Process > Configuration > Parameters**.

Time Tracking

The following parameters apply to the Time Tracking optional component:

Display Name	Description	Default Value
Advanced Parameters		
Time Tracking Max Daily Units	The maximum daily value not to be exceeded on a given day when entering time on timesheets.	0
Time Tracking Warn or Block Input Greater than Max Daily Units	Enables or disables the ability to enter time exceeding the daily limit. When set to **0**, a warning displays when users enter a value greater than the allotted max daily value. When set to **1**, the system clears cells that contain values greater than the max daily limit, and prevents users from submitting timesheets.	0
Time Tracking Warn or Block Input on Restricted Days	Enables or disables the ability to enter time on restricted days. When set to **0**, a warning displays when users enter time on restricted days. When set to **1**, the system prevents users from entering time on restricted days.	0
Weekly Restricted Days	Day(s) of the week which time cannot be entered on timesheets. 0 = Sunday, 6 = Saturday. Separate entries using a pipe (|) delimiter.	Blank
Weekly Start Day	*(Read Only)* The day of the week on which timesheets start. 0 = Sunday, 6 = Saturday.	0

Dashboards

The following parameters apply to the Dashboards for Accolade optional component:

Display Name	Description	Default Value
Dashboards Server URL	URL of the Accolade Dashboards Server	Blank
Advanced Parameters		
Dashboard Users Group	Name of the User Group used for Dashboards document permissions.	Blank
Dashboards Web	Password of the user used for retrieving the	Blank

Display Name	Description	Default Value
Ticket Password	Dashboards web ticket.	
Dashboards Web Ticket User Name	Name of the user used for retrieving the Dashboards web ticket.	Blank

Excel

The following parameters apply to downloading content such as online reports, metrics, and process model data from Accolade to MS Excel:

Display Name	Description	Default Value
Excel Header Background Color	The background color of the header rows in online reports downloaded to MS Excel.	0276FD
Excel Header Font Color	The font color of the text in header rows in online reports downloaded to MS Excel.	FFFFFF
Excel Header Is Bold	Sets whether the header text is bold or regular weight in online reports downloaded to MS Excel.	0

AutoLoader

The following parameters apply to setting the autoloader configuration, and are all read only within the Standard Parameters list. To update autoloader settings, use the Autoloader Configuration pane within the Administration Console:

Display Name	Description	Default Value
Advanced Parameters		
FTP Inbox Path	*(Read Only)* Path to the FTP inbox folder.	Blank
FTP Outbox Path	*(Read Only)* Path to the FTP outbox folder	Blank
FTP Password	*(Read Only)* Password for the FTP site.	Blank
FTP Username	*(Read Only)* Username for the FTP site.	Blank
Local Inbox Path	*(Read Only)* File path to the local inbox folder.	Blank
Local Outbox Path	*(Read Only)* File path to the local outbox folder.	Blank

Display Name	Description	Default Value
Relay Delay on Error	*(Read Only)* Length of time in seconds that the service waits before retrying on error.	Blank

Service Broker

The following parameters apply to the Microsoft SQL Server Service Broker:

Display Name	Description	Default Value
Advanced Parameters		
Service Broker Conversation Lead Time	The number of seconds, prior to the conversation lifetime, before the Service Broker stops sending messages on the conversation. Set the lead time value as less than the lifetime value, as it is intended to warn when approaching the lifetime time out.	14400
Service Broker Conversation Lifetime	The maximum number of seconds before the SQL Service Broker ends the conversation. The lifetime value must exceed the timeout value and should be significantly longer than the time out value to avoid breaching the lifetime conversation end.	86400
Service Broker Conversation Timeout	The number of seconds a conversation is allowed to run before the conversation times out and fires another conversation. For each new message sent on the conversation prior to reaching the time out, Accolade extends the allotted time for the conversation by this value.	60
Service Broker Retry Attempts	The number of retries the Service Broker attempts to complete a request after receiving an error.	10
Service Broker Retry Delay	The amount of time to wait between Service Broker retries (in hh:mm:ss format).	000:00:15

Index

Sopheon Corporation

6870 West 52nd Avenue, Suite 215

Arvada, CO 80002