Installation Guide

Axiom

Version 2022.3

Syntellis
10 S. Wacker Dr., Suite 3375
Chicago, Illinois 60606
847.441.0022
www.syntellis.com

Table of Contents

Introduction

This guide contains information on how to:

- Prepare your environment for installation of Axiom
- Install Axiom server and client components
- Configure required and optional system settings

Installation of Axiom is typically managed by your organization's Information Technology department. This guide assumes that your organization has internal expertise on network, server, and database administration. Axiom Support and your implementation consultant are available to assist you with the installation.

This guide references the Axiom Help file for additional information on certain topics. You can access Axiom Help from within Axiom.

NOTE: This guide only applies to customers who are installing Axiom on premise. If you are an Axiom Cloud client, see the separate *Cloud Technical Guide* for information on installing software for use with Axiom Cloud systems.

2

Installation Checklist

The following installation checklist applies to new installations. The checklist is provided to give you a quick step-by-step overview of the installation process. Detailed information is provided in the referenced sections.

If you are upgrading an existing installation, see Upgrading Axiom before performing any installation steps.

	Step	More Information
☐	Plan the installation and server configuration	Planning the Installation
☐	Prepare the database server	Microsoft SQL Server
☐	Prepare the Axiom database: • Create/restore the database • Upgrade the database	Preparing the Axiom database
☐	Prepare the application server: • Install IIS • Install .NET • Obtain and install Axiom certificate	Microsoft IIS Microsoft .NET Framework Installing the Axiom certificate
☐	Install the Axiom Application Server and (if needed) the Axiom Update Service	Installing the Axiom Application Server Installing Axiom Update Service
☐	Prepare the Scheduler server(s): • Install VSTO • Install .NET	Microsoft VSTO Microsoft .NET Framework
☐	Install the Axiom Scheduler Server	Installing Axiom Scheduler Service
☐	Prepare the client workstations • Install .NET • Install Excel (for Excel Client only) • Install VSTO (for Excel Client only)	Microsoft .NET Framework Microsoft Excel Microsoft VSTO

	Step	More Information
☐	Install the Axiom Desktop Client	Installing the Axiom Client on client workstations
☐	Configure Axiom: • Complete the system configuration settings • Set up Scheduler • Set up users in Security	Configuring Axiom

3

Planning the Installation

This section provides the information you need to understand the deployment options, technical requirements, and prerequisites for Axiom. Before installing Axiom, you should prepare the server and client environments as needed.

Technical requirements

Before installing Axiom, make sure that you understand the supported software versions and minimum hardware requirements. For more information, see the separate documents *Server Technical Requirements* and *Client Technical Requirements*. These documents are maintained separately so that we can provide you with the most up-to-date technical requirements. Copies of these documents are available in Axiom Help. If you do not have access to Axiom Help, Axiom Support can provide these documents to you on request.

Component overview

Axiom consists of the following server and client components.

Server components

Axiom has the following server components:

Component	Description
Application Server	The Axiom Application Server controls server-side operations for Axiom, including web services for the Web Client. It operates as a Microsoft IIS application.

Component	Description
Scheduler Service	The Axiom Scheduler Service processes Axiom tasks on a server instead of the individual client machines. Tasks can be scheduled for processing or run on demand. The application server install includes installation of a System Scheduler on the application server to handle system tasks. To handle user-scheduled tasks, you must manually install the service on one or more Scheduler servers.
Database	Axiom uses Microsoft SQL Server to store all data and files for the Axiom application. Users interact with these managed files using the Axiom virtual file system, which simulates a familiar Windows Explorer file system for accessing documents. Each Axiom system consists of two databases: an application database that holds all files, tables, and other data for the system, and a corresponding audit database to track changes made to that system.
Update Service	The Axiom Update Service is used to apply updates to certain Axiom products.

Once the application server has been installed and the Axiom database has been configured, you can access the Axiom Web Client to install the Desktop Client and perform certain administrative functions. For more information, see Installing the Axiom Client on client workstations.

Client components

Users interact with Axiom using the following clients:

Client Name	Description
Excel Client	The Excel Client provides access to all Axiom features within a Microsoft Excel interface.
Windows Client	The Windows Client emulates the spreadsheet environment without requiring Microsoft Excel. It provides full access to Axiom features, but certain spreadsheet features are limited.
Web Client	The Web Client provides browser-based access to Axiom, limited to certain web-enabled features. For end users, the Web Client provides access to web-based input forms, reports, and dashboards. For administrators, the Web Client provides access to certain administration features, such as system auditing.

Administrators can choose to use either the Excel Client or the Windows Client. End users can use any client, depending on your organization's deployment preferences and template/report design. The Excel Client and Windows Client require installation on the client machine via ClickOnce; whereas the Web Client is accessible within a browser and does not require separate installation.

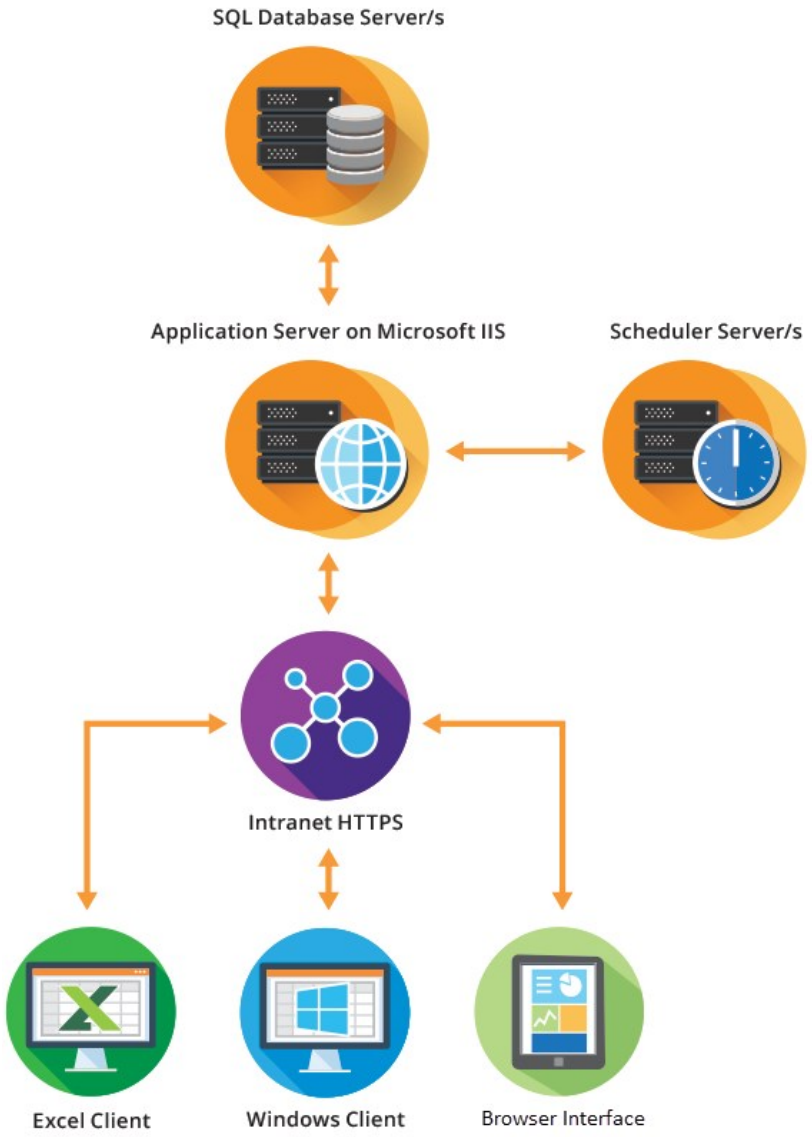
Because the Windows Client does not use Microsoft Excel, it has some limitations in regard to spreadsheet functionality. For more information, see Axiom Help: **Axiom file setup > Additional design considerations > Windows Client design considerations for Axiom files** (or search for AX2289).

The Excel Client and the Windows Client are referred to collectively as the Desktop Client. Any references to Desktop Client means use of either client.

Server configurations

Axiom can be deployed in a number of server configurations, depending on factors such as the size of your user base, the number of active plan files, and anticipated Scheduler activity.

For detailed information on server configurations, including specific hardware requirements, see the separate *Server Technical Requirements* document. Server information is summarized here for reference.



For medium, large, and enterprise deployments, server components must be hosted on separate servers for optimal performance. Additionally, for larger deployments, we recommend multiple Scheduler servers.

- The medium footprint assumes 25-50 concurrent users, fewer than 500 plan files, and moderate Scheduler activity. In this scenario, one Scheduler server should be sufficient.
- The large footprint assumes more than 50 concurrent users, more than 500 plan files, and heavy Scheduler activity. We recommend two load-balanced Scheduler servers to support this configuration.
- The enterprise footprint assumes 500-1000 concurrent users, more than 500 plan files, and heavy Scheduler activity. We recommend four load-balanced Scheduler servers to support this configuration.

Account and file permissions

User rights

Users do not require any special file permissions on your organization's network in order to work with Axiom. All Axiom managed files are stored within the Axiom database, and access to those files is controlled within the system. All users must be set up within Axiom Security, and the number of allowed users is subject to your licensing agreement with Syntellis.

Application Server—Service account rights

When setting up imports in Axiom, the import source files must be accessible to either the Network Service account or Computer account used by the Axiom Application Server. By default, the application server runs using the Network Service account.

If you are importing from a network share that is local to the application server, the share and security permissions must be configured to grant the Network Service account at least read permission. If you are importing from a network share that is not local to the application server, the share and security permissions must be configured to grant the application server Computer account at least read permission.

This applies when the import file location is fixed, or when the import is run via Scheduler. If users are running imports interactively, you can use the file prompt option to import any file, regardless of whether the application server account can access it directly.

Scheduler Server(s)—Service account rights

Scheduler supports certain tasks that can save files to specified folder locations, or process files at specified folder locations. These folder locations must be accessible to the user account for the Scheduler service.

By default, the Scheduler service runs using the local system account. If you want Scheduler to be able to access file shares on other network servers, then you must change this so the Scheduler service runs using a domain service account, and then grant this account read/write share and security permissions to the desired folders.

Software prerequisites

The following software prerequisites are required for Axiom:

Prerequisite	Database Server	Application Server	Scheduler Service	Client Workstations (Excel)	Client Workstations (Windows)
Microsoft SQL Server	X				
Microsoft IIS		X			
Microsoft .NET		X	X	X	X
Microsoft Excel				X	
Microsoft Visual Studio Tools for Office (VSTO)				X	
Web browser (Microsoft Internet Explorer and others)				X	X

Microsoft SQL Server

If you are doing a new installation of SQL Server for use with Axiom, you can use the default settings. Note the following:

- For **Feature Selections** to install, make sure that the following components are selected: **Database Engine Services**, **Client Tools Connectivity**, and **Management Tools - Complete**.
- For the **Service Account**, select **Use the built-in System account**.
- For **Authentication Mode**, select **Mixed Mode**. The sa password can be anything that meets your organization's requirements.

After installing SQL Server, make sure to install the latest service pack for the release. See the separate *Server Technical Requirements* document for a list of the currently supported SQL Server versions.

NOTE: The SQL Server version and drivers must support TLS 1.2.

Syntellis strongly recommends enabling parallelism for SQL Server. For more information on configuring parallelism, you can consult the following resources from Microsoft:

- Configure the max degree of parallelism Server Configuration Option
- Configure the cost threshold for parallelism Server Configuration Option

Microsoft IIS

Microsoft Internet Information Services (IIS) is required to be installed on the Windows Server that will host the Axiom Application Server.

The following IIS features are required:

- Under **Web Server > Common HTTP Features**, select **Default Document** and **Static Content**.
- Under **Web Server > Performance**, select **Static Content Compression** and **Dynamic Content Compression**.
- Under **Web Server > Application Development**, select **.NET Extensibility 4.6** and **ASP.NET 4.6**.
- Under **Web Server > Management Tools**, select **IIS Management Console**.
- Under **.NET Framework 4.6 Features**, select **.NET Framework 4.6**, **ASP.NET 4.6** and **WCF Services > HTTP Activation**.

Microsoft .NET Framework

Microsoft .NET Framework 4.8 or higher is required on all Axiom servers and client workstations, except for computers and devices that will only use the Axiom Web Client.

After installing IIS on the Axiom Application Server, run Windows Update on the server, and then select **Custom** to access the full list of updates. Select every available update that is related to .NET. Make sure to check the **Software, Optional** section in addition to the **High Priority** section.

If the required version of .NET is not already present on client machines, it can be installed from Microsoft's website, or from the Axiom Web Client after the application server has been installed.

Microsoft Excel

A supported version of Microsoft Excel is required to be installed on all client workstations that will use the Axiom Excel Client. Please see the separate document *Client Technical Requirements* for a full list of supported Excel versions.

When installing Excel, the following components must be included:

- Visual Basic for Applications
- .NET Programmability Support

After installing, make sure to install the latest service pack for the release.

If your organization has configured Excel to require add-ins to be digitally signed, then you must install the publisher certificate for Axiom to the Trusted Publisher area on client machines. Axiom Support can provide this certificate to clients on request.

Microsoft VSTO

Microsoft Visual Studio Tools for Office (VSTO) is required to be installed on all client workstations that will use the Axiom Excel Client. You can install this program from the Axiom Web Client after the application server has been installed.

Web browser

Use of the Web Client requires a current version of an HTML5-compliant browser. Various browsers are supported, based on the platform where the Web Client will be viewed. For full details on supported browsers, see the separate document *Client Technical Requirements*.

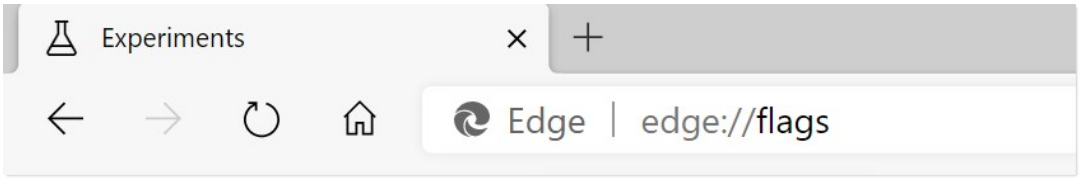
If you will be using Axiom forms exclusively within the Desktop Client (meaning users will not open forms in a separate browser), then the embedded browser within the application provides native support for form functionality. There are no additional browser requirements for Axiom forms used within the Desktop Client environment.

Requirements to install and launch the Desktop Client from the browser

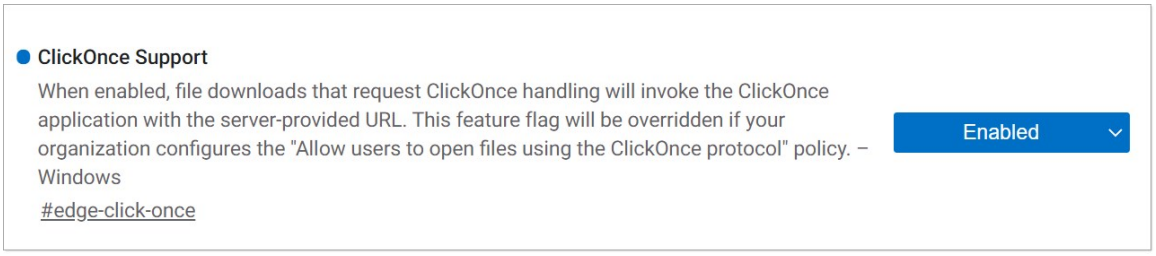
Axiom uses Microsoft ClickOnce technology to install and launch the Axiom Desktop Client (Excel or Windows) from the Web Client browser. Your chosen browser must be ClickOnce compliant, either by enabling ClickOnce support in the browser configuration settings, or by installing a ClickOnce extension for the browser.

If you are using Microsoft Edge, you can enable ClickOnce support in the browser configuration settings as follows:

1. Launch the Edge browser. In the address bar, type `edge://flags`.



2. Scroll down until you locate the item named **ClickOnce Support**. Select **Enabled** from the drop-down list.



3. Close Edge and then reopen it. You should now be able to install or launch the Axiom Windows

Client or the Axiom Excel Client from the browser.

Authentication methods

Axiom supports several different ways to perform user authentication into Axiom. Axiom can be the sole method of authentication, or you can integrate with other methods of authentication used at your organization. Axiom supports the following authentication options:

- Axiom Prompt Authentication
- Windows Authentication
- LDAP Authentication
- OpenID Authentication

Axiom Prompt Authentication is always available and does not need to be explicitly enabled. All other authentication options must be enabled during the Axiom Application Server installation if you want to use them. You can also modify authentication options post-installation using the Axiom Software Manager: **Installation Manager > Configure Authentication Methods**.

When you set up users in Axiom security, you specify which method of authentication should be used for each user. If an integrated authentication option is enabled for your system, that method is the default method.

Axiom Prompt Authentication

When using Axiom Prompt Authentication, users are authenticated based on their Axiom credentials. When the Axiom login screen displays, users must type their Axiom user name and password. In Axiom security, users must be assigned to the **Axiom Prompt** authentication type.

Axiom Prompt Authentication is always available and applies to all components of Axiom. You can use Axiom Prompt Authentication as the primary authentication method for your installation (meaning no other authentication method is enabled), or you can use it in conjunction with another authentication method. If you are also using another authentication method, then the Axiom Prompt behavior is as follows:

- If LDAP Authentication or Windows Authentication is enabled, Axiom Prompt users simply enter their Axiom user name and password at the Axiom login prompt. If the login screen is configured to show the domain selector, Axiom Prompt users must select **Axiom Named User**.
- If OpenID Authentication is enabled, Axiom Prompt users must go to a special area of the web site in order to log in. For example:

  `https://ServerName/Axiom/Home/Login`

Windows Authentication

When using Windows Authentication, users are authenticated based on their Windows credentials. When the Axiom login screen displays, users must enter their Windows user name, domain, and password. If the current domain is an allowed domain and the Windows user name matches a user name in Axiom, then the credentials are passed to Windows for authentication into Axiom. Windows Authentication applies to all components of Axiom.

Users must be set up in Axiom security using their Windows user names and assigned to the **Windows User** authentication type. This can be done manually, or you can optionally import and synchronize users from Active Directory using a Scheduler task.

Windows Authentication is enabled during the Axiom Application Server installation. When enabling Windows Authentication, you must specify allowed domains for authentication. You can modify this configuration later as needed using the Axiom Software Manager, or by using a Save Type 4 utility to the system configuration table.

If the Windows Authentication configuration only allows one domain, then that domain is assumed for authentication and users do not need to specify it when logging in. If multiple domains are allowed, then the domain must be specified in one of the following ways:

- The user must include the domain with their user name, such as: *DomainName**UserName*.
- The user must specify the appropriate domain using the **Domain** selection list on the login screen. This is an optional setting that can be enabled for your installation. For more information, see Domain prompt.

Users must enter their credentials each time they log in, unless they select **Remember me** to store their credentials for future login. For more information, see Remember me.

The Cloud Integration Service is required when using Windows Authentication in Axiom Cloud systems. For more information, see the *Cloud Technical Guide*.

LDAP Authentication

When using LDAP Authentication, users are authenticated based on their LDAP credentials. When the Axiom login screen displays, users must enter their LDAP user name (with or without the suffix) and their LDAP password. If the LDAP user name matches a user name in Axiom, then the credentials are passed to LDAP for authentication into Axiom. LDAP Authentication applies to all components of Axiom.

Users must be set up in Axiom security using their LDAP user names and assigned to the **LDAP Prompt** authentication type. The user name can contain the LDAP suffix or not as desired. Note that the user name must include the suffix if there is a user name conflict with another user that is configured with a different authentication type (or with a different LDAP suffix). For example, if you have an Axiom Prompt user jdoe, and you have an LDAP user jdoe, then the LDAP user must include the suffix on their user name to differentiate the two users.

LDAP Authentication is enabled during the Axiom Application Server installation. When enabling LDAP you must specify the connection information to the LDAP server, as well as the allowed LDAP suffixes. You can modify this configuration later as needed using the Axiom Software Manager, or by using a Save Type 4 utility to the system configuration table.

If only one LDAP suffix is allowed by the configuration, then that suffix will be used for all LDAP authentication. The user can include the suffix or not when logging in, and the Axiom user name can contain the suffix or not. Axiom will automatically append the suffix as needed when sending the credentials to LDAP for authentication. However, if multiple suffixes are allowed, then the suffix must be specified using any of the following approaches:

- The Domain selector must be enabled for login, and the user must select the appropriate suffix.
- The user must include the suffix as part of their user name when logging in.
- The user names in Axiom must include the appropriate suffix for each user.

Users must enter their credentials each time they log in, unless a user chooses to select **Remember me** to store their credentials for future login. For more information, see Remember me.

OpenID Authentication

When using OpenID Authentication, users are authenticated based on their credentials for the designated OpenID provider (such as Google OpenID Connect). OpenID Authentication is a web-based authentication method. Users access Axiom by going to the Axiom Web Client, where they must enter their user name and password for their OpenID provider. Once a user is authenticated, if the user name matches a user name in Axiom, then the user can access the Web Client and launch the Axiom Excel Client or Windows Client from the web page.

Users must be set up in Axiom using their OpenID user names, and assigned to the **OpenID** authentication type. This user name must exactly match the OpenID user name, including the @suffix.

Users assigned to OpenID Authentication can only access Axiom from the web. The Excel Client and Windows Client cannot subsequently be launched using a shortcut on the user's computer; the user must continue to log into the Axiom Web Client in order to start the Desktop Client. When using OpenID Authentication, you may want to configure the Axiom Application Server installation so that no shortcuts are placed on user computers during the client installation, since users will not be able to use these shortcuts.

OpenID Authentication is enabled during the Axiom Application Server installation. When enabling OpenID Authentication, you must specify the Client ID and Client Secret for the OpenID provider. You can modify this configuration later as needed by performing a Repair on the installation.

OpenID Authentication may require additional configuration steps for IIS, the Axiom Application Server, and the OpenID provider. These steps may vary depending on your particular environment. At minimum, you must configure the OpenID provider with the redirect URI to the Axiom login page (such as `<URLtoAxiom>/openid/login`). Please contact Axiom Support for assistance if you are interested in enabling OpenID Authentication.

Logging in as an Axiom Prompt user when OpenID Authentication is enabled

You can set up **Axiom Prompt** users when OpenID Authentication is enabled, such as to allow Axiom Support to access the system without using OpenID credentials. These users must go a special area of the web site in order to log in:

`https://ServerName/Axiom/Home/Login`

Where *ServerName* is the name of your Axiom Application Server and Axiom is the name of the virtual directory.

Login behavior

This section details some options for the Axiom login behavior. These options apply to all authentication types except OpenID.

Domain prompt

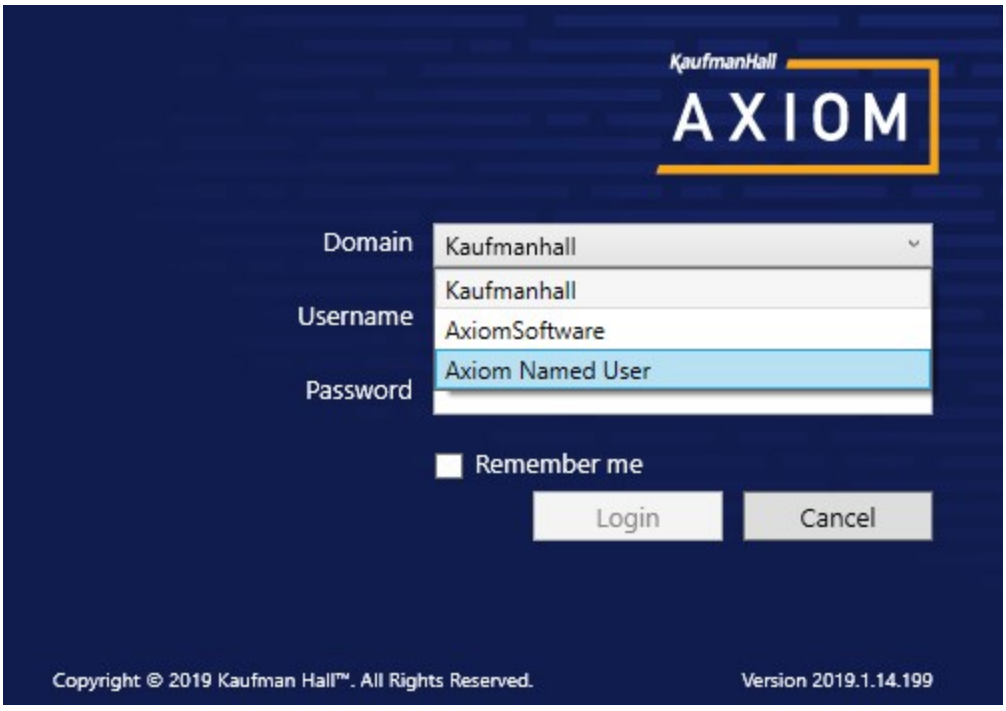
When a user logs in, Axiom looks for a matching user name within Axiom security and applies the specified authentication type for that user. For LDAP Authentication and Windows Authentication, if only one allowed domain or suffix is specified, that information can be assumed and the user does not need to include it when logging in. If multiple domains or suffixes are specified, then the user must include that information as part of their user name. For example: *DomainName**UserName* for Windows Authentication.

Alternatively, you can configure your system so that all users must specify their authentication type / domain when logging into Axiom, using the **Domain** selection list. The Domain selection list displays the following:

- **Axiom Named User** (for Axiom Prompt login)
- Each allowed Windows Authentication domain (if Windows Authentication is enabled for the installation)
- Each allowed LDAP suffix (if LDAP Authentication is enabled for the installation)

When the Domain selection list is enabled, the user must make the appropriate selection in order to log in. For example, a Windows Authentication user must select their Windows domain name. Because it is specified separately, the domain or suffix does not need to be added to the user name, even when there are multiple allowed domains or suffixes.

The following screenshot shows an example of the Domain selection list. In this example, the installation has enabled Windows Authentication with two allowed domains. The two domain names display on the selection list as well as the choice to log in as an Axiom Named User.



The Domain selection list can be enabled or disabled using the **AuthenticationDomainSelectionListRequired** system configuration setting. By default this is set to False, which means the Domain selection list only displays if your system contains duplicate user names that require the domain to be specified to differentiate those users. If you set this to True, then the Domain selection list displays at all times.

If the Domain selection list is enabled, and if Windows Authentication is enabled for the installation, then by default the user's current domain will be selected in the list (if that domain is one of the allowed domains). Otherwise, the first option in the list is selected by default. Options are ordered as follows: LDAP suffixes, Windows domains, Axiom Named User.

Remember me

Users can optionally select **Remember me** at the login screen to store their Axiom authentication for future use. This information is encrypted and only applies to the current user for the current machine. The next time the user starts Axiom on the current machine, they will not be prompted to log in.

Although all Axiom clients have a Remember Me check box on the login screen, note that the remembered status is stored separately for access to the Web Client versus the Desktop Client. For example, a user can choose Remember Me when logging into the Excel Client, and then that user will not be prompted when subsequently accessing either the Excel Client or the Windows Client. However, if the user attempts to access the Web Client, they will be prompted for credentials (and can then choose to be separately remembered for the Web Client).

NOTE: Logging out of a client will clear the remembered status for that client type. Although the Excel Client and Windows Client do not have an explicit log out feature, logging out of the Word or PowerPoint add-in will clear the remembered status for the Desktop Client (but only if you are not also currently logged into another instance of the Desktop Client).

If you do not want users to have access to the Remember Me option, so that they must log in each time, then you can disable the feature by setting the system configuration setting **ShowRememberMe** to **False**. This will hide the option from the various login screens. Keep in mind that if a user has already used the Remember Me option, hiding the setting will not clear the user's stored credentials. The user will continue to be remembered until they log out and cause their credentials to be cleared.

Using SSL

You can set up the Axiom Application Server to use Secure Socket Layer (SSL) security, assuming that you have provided a certificate and configured IIS appropriately to support it.

When installing the application server, specify the URI as HTTPS if you will be using SSL. Additionally, if you want the site to require SSL, you can select the **Require SSL** option for the application server. Please see Installing the Axiom Application Server for more information, and contact Axiom Support if you need assistance configuring SSL for your Axiom implementation.

NOTE: Syntellis does not support self-signed certificates for on-premise installations. The Axiom code does not explicitly prevent these certificates from working, however, Axiom Support will not provide assistance for any issues arising from self-signed certificates.

4

Installing Axiom Server Components

This section discusses the installation process for the Axiom server components, including:

- Creating or restoring the Axiom database
- Installing the Axiom Application Server
- Installing the Axiom Scheduler Service
- Installing the Axiom Update Service

IMPORTANT: This process is for new installations. If you are upgrading an existing installation, see Upgrading Axiom before performing any installation steps.

Before you install

Before beginning the server installation process, make sure the following prerequisites have been completed:

- Microsoft SQL Server is installed on the database server. See Microsoft SQL Server.
- Microsoft IIS is installed on the application server. See Microsoft IIS.
- Microsoft .NET updates have been performed on all servers that will host an Axiom server component. See Microsoft .NET Framework.
- The signed Axiom certificate has been placed on the application server. See the following section.

Installing the Axiom certificate

In order to install the Axiom Application Server on your on-premise server, a signed Axiom certificate must be present on the server. This is a one-time step that must be performed before the initial installation.

The certificate causes various installation and configuration options to become available within the Axiom Software Manager, including the ability to install the Axiom Application Server. If a signed certificate is not present on the server, these options are hidden.

The certificate is only required to be present on the server(s) where you want to install the Axiom Application Server. The certificate is *not* required to install the Axiom Scheduler Service.

The general steps for this process are:

1. Create/install a certificate on the server.
2. Send the certificate file to Axiom Support so that an encrypted key file can be generated for you.
3. Place the encrypted key file on the server.

Generally speaking, new releases of Axiom do not require new certificates or key files. Once this process is complete, the certificate and key file can be used indefinitely. If a future architecture change or policy change requires clients to obtain a new certificate or key file, this will be communicated in the release notes for the affected version.

Creating a certificate on the server

On the server where you want to install Axiom Application Server, create a certificate with a private key. One way to create an appropriate certificate is to use the following PowerShell script.

```
$cert = New-SelfSignedCertificate -DnsName 'Axiom Software
Manager Encryption' -CertStoreLocation "Cert:\LocalMachine" -
KeyUsage  KeyEncipherment,DataEncipherment,KeyAgreement -Type
DocumentEncryptionCert -NotAfter (Get-Date).AddYears(100) -
KeySpec KeyExchange

Export-Certificate -Cert $cert  -FilePath \temp\certificate.cer

$pwd = ConvertTo-SecureString -String "your-strong-password-here"
-Force -AsPlainText

Export-PfxCertificate -Cert $cert  -FilePath
\temp\certificate.pfx -Password $pwd
```

This script should be updated as follows:

- Replace "your-strong-password-here" with a password that meets your organization's security requirements.
- You can change the export file location for the certificate and key files if desired.
- The certificate store location can be either LocalMachine (default) or CurrentUser.
    - If LocalMachine, then the certificate will be available to any user that is able to log on to the server.
    - If CurrentUser, then the certificate must be installed (possibly through group policy) for each user account that needs to use the Axiom Software Manager on the application server.

- By default, the name of the certificate is assumed to be 'Axiom Software Manager Encryption'. If you use this name, then no registry configuration is required for the certificate. However, if you use a different name, then the following registry key must be configured for the change: `HKEY_CURRENT_USER\Software\Axiom EPM\Axiom Software Manager\EncryptionCertificateName`

NOTES:

- The same certificate should be used for all of your on-premise Axiom Application Servers (for example, production and test). The exported certificate.pfx file and password can be used to install the certificate on additional servers.
- The exported certificate.pfx file is a backup of your private key. It should be stored, along with the password, in a safe and secure location.
- None of the exported files or your password are required at run time by the Axiom Software Manager or the Axiom Application Server.

Obtaining the encrypted key file from Axiom Support

Once you have generated the certificate, send the exported **certificate.cer** file to Axiom Support. If you are not already in contact with Axiom Support about the installation, you can create a new case using the Syntellis Central client portal.

Axiom Support will use this certificate file to generate a **symmetrickeys.enc** file. They will deliver this generated file back to you, so that you can place it on the application server for use with the Axiom Software Manager.

Placing the encrypted key file on the server

Once you have obtained the **symmetrickeys.enc** file from Axiom Support, copy it to a local folder on the server where you want to install Axiom Application Server. By default, the assumed location for this key file is:

```
C:\Program Files\Axiom EPM\symmetrickeys.enc
```

If you use the default location for the key file, then no registry configuration is required. However, if you change this location, then the following registry key must be configured for the change: `HKEY_CURRENT_USER\Software\Axiom EPM\Axiom Software Manager\SymmetricKeyFilePath`

You should now be able to start the Axiom Software Manager on this machine and install the Axiom Application Server. For more information, see:

- Axiom Software Manager
- Installing the Axiom Application Server

Axiom Software Manager

The Axiom Software Manager is used to install and configure all Axiom server components and the Axiom database. To obtain a copy of the Axiom Software Manager, contact Axiom Support.

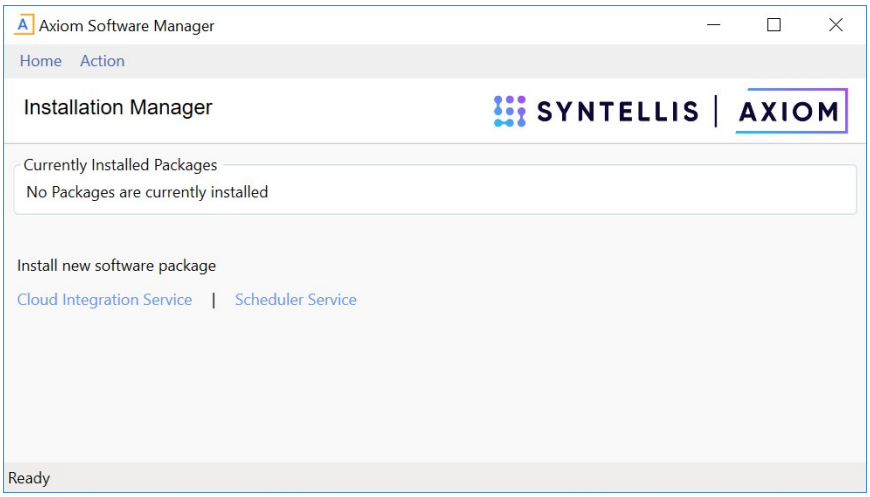
As a first step to installing Axiom on any server, you should extract the contents of the installation ZIP to a folder such as `C:\AxiomFiles\Axiom 2022.3`. The Software Manager executable `AxiomSoftwareManager.exe` will be extracted to that folder.

We recommend keeping the Software Manager on the server after the installation is complete, since the Software Manager can also be used to view installation details, configure the database, and uninstall the software if needed. Each version of Axiom, including patch updates, will have a new Software Manager that can be used to install or manage that version.

The options available in the Software Manager differ depending on whether a signed certificate is present on the server. If a certificate is present, the full Software Manager functionality is available, including the ability to restore and upgrade the Axiom database, and install or upgrade the Axiom Application Server.

Example Axiom Software Manager with certificate

If a certificate is not present on the server, then the functionality is limited to installing the Axiom Scheduler Service. The other available option in this mode—installing the Axiom Cloud Integration Service—does not apply to on-premise installations.



Example Axiom Software Manager without certificate

Preparing the Axiom database

Use the Axiom Software Manager to create or restore the Axiom database. For more information on the Software Manager, see Axiom Software Manager.

The database management features of the Axiom Software Manager require a signed certificate to be present on the server. This means that the Axiom Software Manager should be run on the server hosting the Axiom Application Server, because this server already requires a certificate.

When you perform an action in the Axiom Software Manager that requires a database connection, you must enter database administrator credentials. The credentials only need to be entered once per session for each database that you try to connect to.

NOTE: If you need to clear the stored database administrator credentials so that you can re-enter them, click **Action > Clear DBA Credentials**.

Creating or restoring the database

You can create a new blank Axiom database, or you can restore a copy of an existing Axiom database. For new customers, eventually you will be restoring a database provided by your implementation consultant, but the blank database can be used for installation in the meantime.

NOTE: The blank database contains one admin user that you can use to log into the Axiom system. You can use the Reset Axiom User Password utility to change the password for this user so that you can log in. Once real users have been set up for your implementation, you can delete this user.

If you are restoring a database, the backup file must first be placed on the database server. The restore file path is local to the database server.

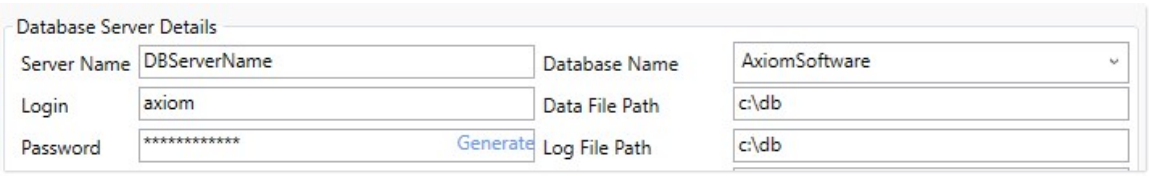
To create or restore the Axiom database:

1. In the Software Manager, click **Database Manager > Restore Databases**. (You can also click **Create/Restore** from the home screen.)

   IMPORTANT: If you do not see this option, then the server does not have a signed Axiom certificate. See Installing the Axiom certificate.

2. Complete the **Database Server Details** section with the information necessary to connect to the database server and create the Axiom database.

Item	Description
Server Name	The server name of the SQL database server. If you are not using the default instance, append the instance name with a backward slash (Server\Instance).
Login Password	The login name and password for the database. If you are creating a new database, you can set the name and password as necessary to meet your organization's requirements. If you are restoring an existing database, the name and password must match the existing name and password on the database.
Database Name	The name of the database.
Data File Path Log File Path	The location to place the data files and the log files on the database server. Paths are relative to the database server.



Example Database Server Details

3. In the **Restore System** section, select the check box for **Application Database**, and then select one of the following:
   - **Create New**: Create a system starting with an entirely blank database.
   - **Restore**: Create a system from a backup copy of an existing database.

   All paths are local to the database server.

Example Restore System database

4. By default, when you select the Application Database, the **Audit Database** is also selected. In most cases you want to leave this selected and use **Create New - Standalone** to create a separate audit database for the system. Alternatively, the **Create New - Embedded** option will create the audit database tables within the application database. This embedded configuration is intended for use with Axiom Cloud systems.

   IMPORTANT: Do not select the embedded database option unless you are instructed to do so by Axiom Support.

   The **Restore** option for the audit database is typically only used when restoring an entire system from backup in a production environment, and only when the audit database is a standalone database. If the audit database is embedded within the application database, then it will be restored when the application database is restored.

5. When all database settings are complete, click **Restore** at the bottom of the screen.
6. If you have not previously entered database administrator credentials, you are prompted to enter them. Enter the credentials (or use Trusted Authentication if you have database administrator rights) and then click **OK**.

A confirmation message displays when the process is complete. When you click **OK** to dismiss the confirmation message, the Software Manager automatically opens the **Upgrade Databases** screen. In all cases, you must upgrade the database after creating a new database or restoring an existing database. See the following section for more details.

Upgrading the database

After creating or restoring the database, it must be upgraded to the current Axiom version. The **Upgrade Databases** screen will automatically open after using the **Restore Databases** screen to create or restore a database, with the information for the database pre-populated. In most cases you can simply click **Upgrade** on this screen. However, the full instructions are provided below in case you ever need to manually perform this action.

To upgrade the database:

1. In the Software Manager, click **Database Manager > Upgrade Databases**.

IMPORTANT: If you do not see this option, then the server does not have a signed Axiom certificate. See Installing the Axiom certificate.

2. In the **Database Server Details** section, complete the following:
   - **Server Name**: Enter the database server name. If you are not using the default instance, append the instance name with a backward slash (Server\Instance).
   - **Database Name**: Enter the database name.

   Once a database server and name have been specified, the details display in the **System Database Details** section. Note that the Axiom user name for the database is the login name as currently specified on the **Restore Databases** screen. If you have come to the Upgrade Databases screen directly and you need to specify a different user name for the database that you want to upgrade, you can enter the correct user name into the **Axiom User Login** field.
3. Click **Upgrade** to upgrade the specified database.

A confirmation message box displays when the upgrade is complete.

Installing the Axiom Application Server

Use the Axiom Software Manager to install the Axiom Application Server. The following requirements apply to the Axiom Application Server installation:

- You must have administrator rights on the server to run the installation.
- A signed Axiom certificate must be present on the server to run the installation.
- During the installation, you will be prompted for a valid Axiom license file, as well as the connection information for the Axiom database. The installation cannot be completed without this information.
- The server must have Internet access in order to successfully complete the installation. This access is necessary to validate the Kaufman Hall signed publisher certificate to be used for ClickOnce installations of the client. If it is not possible to enable Internet access to the server, additional workarounds are available, as detailed in this Microsoft Support article.

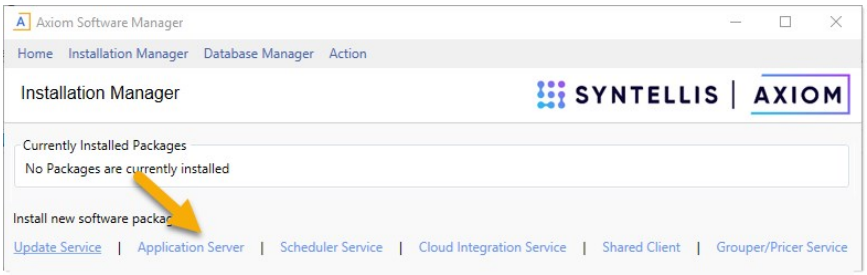
NOTE: Once you enter the installation screens, there is no Cancel button. To cancel an installation, move to a different location within the Axiom Software Manager, or close the Software Manager.

To install the Axiom Application Server:

1. Navigate to the location on the server where you have saved the Axiom Software Manager, and then double-click `AxiomSoftwareManager.exe`. For more information, see Axiom Software Manager.
2. From the **Home** screen of the Software Manager, click **Manage Software**.

TIP: You can also click **Installation Manager > Manage Software Packages** on the menu bar.

3. On the **Installation Manager** screen, under **Install new software package**, click **Application Server**.



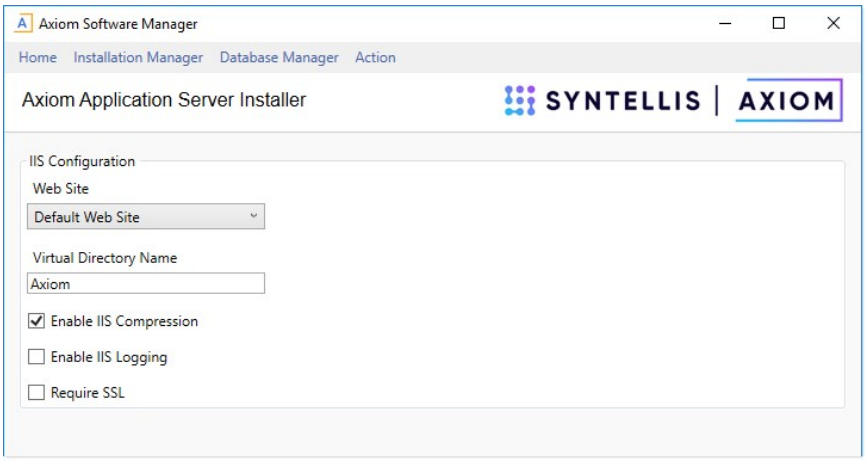
IMPORTANT: If you do not see this option, then the server does not have a signed Axiom certificate. See Installing the Axiom certificate.

The Axiom Application Server Installer begins. The installation is performed within the Software Manager—a separate installer program is not launched. While using the installer, do not use the menu to move to other locations in the Software Manager, unless you want to cancel the installation.

4. On the **License Agreement** screen, click **I accept** and then click **Next**.
5. On the **IIS Configuration** screen, complete the following settings and then click **Next**:

Item	Description
Web Site	By default, this is set to **Default Web Site**. This should not be changed.
Virtual Directory Name	By default, the virtual directory name is **Axiom**. You can change the name if desired. The virtual directory name defines how the system is accessed via the web. All examples in the documentation assume the default virtual directory name.
Enable IIS Compression	This option enables HTTP compression for the IIS application pool. This may improve performance, especially in environments where network bandwidth is an issue. If you do not want to enable compression, clear the check box. We recommend discussing the need for compression with Axiom Support before disabling the option.

Item	Description
Enable IIS Logging	This option enables IIS logging for the application. This is disabled by default because in most cases it is not necessary and does not provide useful information. However, it can be enabled if it is needed to help diagnose a particular issue.
Require SSL	This option configures the Axiom virtual directory to require SSL. You should select this option if you want all access to this web site to use SSL. Selecting this option will require the application server URI to be in HTTPS format. **NOTE:** This option does not configure the web site to require SSL; you must manually configure this for the specified web site within IIS. It simply configures the Axiom virtual directory as appropriate for environments where SSL is required.



6. On the **Installation Folder** screen, specify the location where the Axiom files will be installed, and then click **Next**.

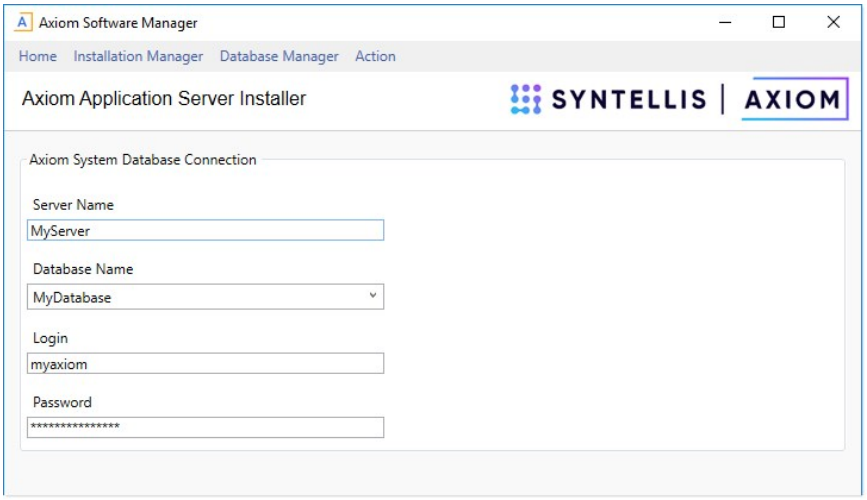
   By default, the installation location is `C:\Inetpub\wwwroot\Axiom` (where Axiom is the default virtual directory name). This location should not be changed (except to account for differences in the virtual directory name).

7. On the **System Database Connection** screen, configure the connection from the application server to the Axiom database, and then click **Next**.

To configure the connection string, complete the following settings:

Item	Description
Server Name	The server name of the SQL database server that hosts the Axiom database.
Failover Partner	Optional. The server name of the database server to be used in failover situations. This only applies to Axiom Cloud systems; otherwise it should be left blank.
Database Name	The name of the database for Axiom.
Login	The login name for the Axiom database.
Password	The password for the Axiom database. **NOTE:** The last-entered password will be remembered when using the one-click upgrade, but the password must be typed in when performing new installations or repairs of existing installations.

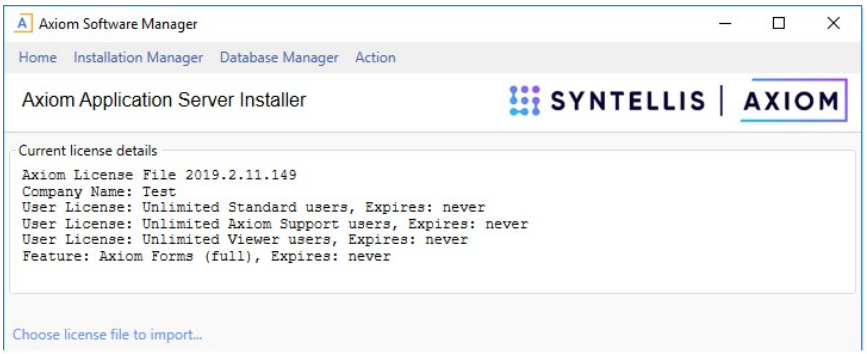
This is the same database information that was used when creating or restoring the Axiom database (Creating or restoring the database).



This information must be provided in order to continue with the install. The connection information can be changed later by using the **Configure Connections** page of the Software Manager.

8. On the **License File** screen, upload your Axiom license file, and then click **Next**.

   Click **Choose license file to import**, then navigate to the location where you have saved the license file provided by Axiom. Once you have uploaded the file, the license details display on this screen, as shown in the following screenshot.

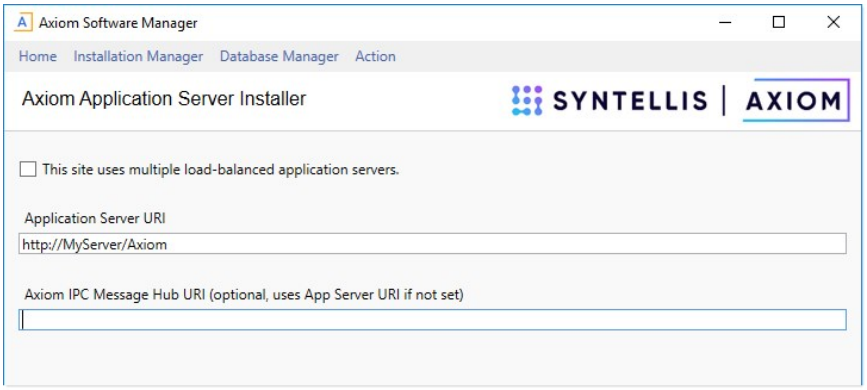


A valid license file must be provided in order to continue with the install. The license file can be updated later by using the **License Manager** page of the Software Manager. You can also update your license using the administration features of the Axiom Web Client.

9. On the **Application Server URI** screen, specify the URI to the application server, and then click **Next**.

   By default, the **Application Server URI** is `http://<servername>/Axiom`. If you changed the web site or the virtual directory name in the prior screen, then you must update this URI to match.

   In most cases you will leave the **Axiom IPC Message Hub URI** blank, so that it uses the default URI (the application server URI).



Example Application Server URI screen

NOTE: The option **This site uses multiple load-balanced application servers** is provided for legacy configurations. You should not enable this option unless instructed to by Axiom Support.

Configuring SSL

If you selected **Require SSL** on the previous installation screen, then the URI is in HTTPS format by default. If you want to use SSL for the Axiom virtual directory but not require SSL for the web site, then you can manually change the URI to use HTTPS. This will configure the virtual directory to support SSL in a mixed-mode environment.

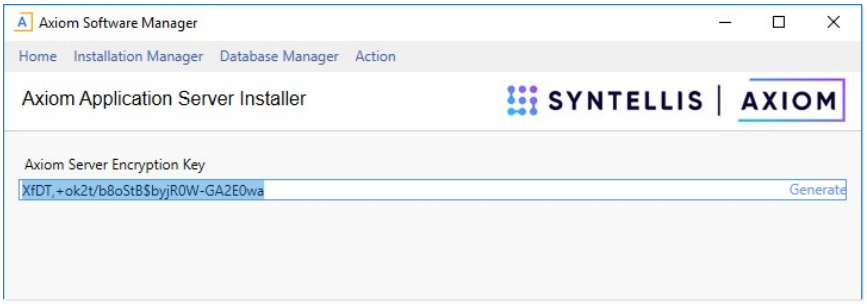
10. On the **Axiom Server Encryption Key** screen, enter an encryption key and then click **Next**.

    The encryption key is for security purposes. It is used by the Axiom Application Server to authenticate requests from the Axiom Scheduler Service. There are two options to specify the key:

    - Click **Generate** to randomly generate an encryption key. If you generate a key, be sure to copy and paste the key to a temporary location so that you can use it when you subsequently install the Axiom Scheduler Service. Once you have used the key in your application server installation and your Scheduler service installation, it will be remembered by the installer so you have no further need to save the key.

      NOTE: If you move your cursor out of the encryption key field, the key will become masked (meaning it displays as asterisks). You can place your cursor back in the field to read the key.

    - Alternatively, you can type in your own key. Axiom does not enforce any rules on the key string. If you choose to use your own key, it is your responsibility to ensure that the key is of an adequate strength for your organization's security requirements.

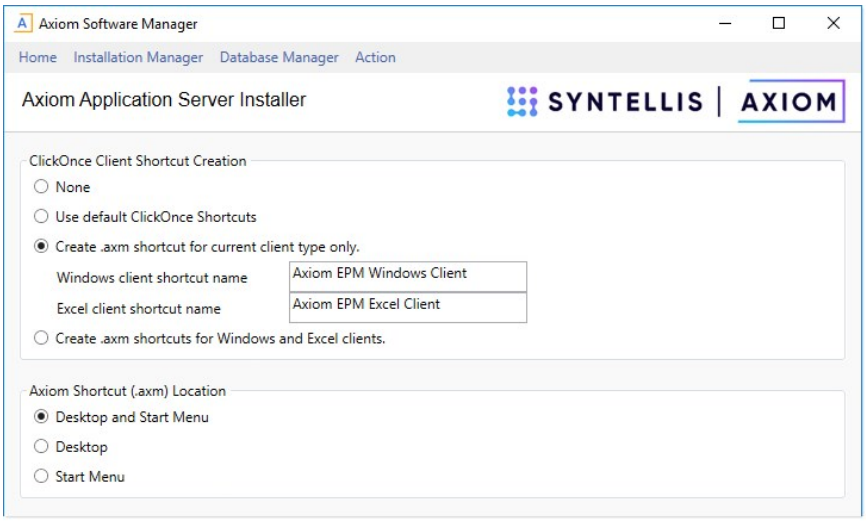


11. On the **ClickOnce Client Shortcut** screen, complete the following settings and then click **Next**.

    These settings determine whether and where shortcuts will be created on client workstations when using the ClickOnce installer to install the Axiom Windows Client and Axiom Excel Client.

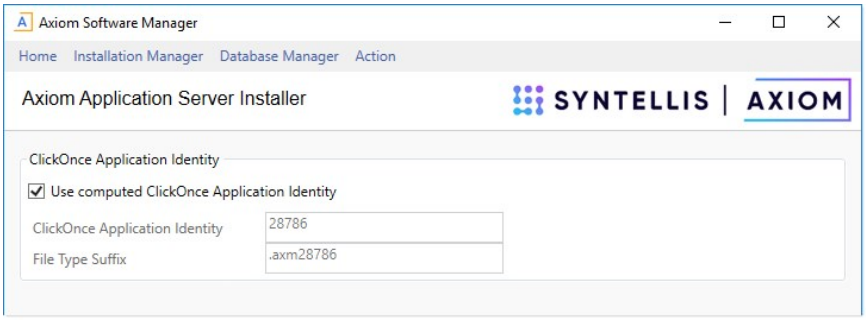
Item	Description
ClickOnce Client Shortcut Creation	Select one of the following: • **None**: No shortcuts will be created on client workstations. • **Use default ClickOnce Shortcuts**: One shortcut will be created on the client workstation, which launches the last-launched client version (Excel Client or Windows Client). If a user wants to launch the other client version, they must use the Web Client to switch back and forth. • **Create .axm shortcut for current client type only** (Default): An AXM shortcut will be created when you install/launch a particular client type (Excel Client or Windows Client). Users who only use one client type will only see the shortcut for that type. The other shortcut will only be created if you launch the other client type. If desired, you can change the default name for each shortcut. • **Create .axm shortcuts for Windows and Excel clients**: AXM shortcuts will be created for both client types when a user installs the Axiom client. If desired, you can change the default name for each shortcut.
Axiom Shortcut Location	If the prior option is set to anything other than **None**, then select one of the following options to specify where the client shortcuts will be created: • **Desktop and Start Menu** (Default) • **Desktop** • **Start Menu** In very controlled IT environments, users may not have permission to create desktop shortcuts, therefore causing the installation to fail. In these environments you can select **Start Menu** so that users are able to complete the installation and still have access to a shortcut.

NOTE: AXM shortcuts are special Axiom files that can be used to launch specific client versions using the ClickOnce protocol. From a user's perspective the shortcut is the same, except that AXM shortcuts are not automatically removed if the client program is uninstalled. ClickOnce shortcuts are automatically removed when the client is uninstalled.



12. On the **ClickOnce Application Identity** screen, specify the identity code for this particular Axiom installation, and then click **Next**.

    The ClickOnce Application Identity is used to uniquely identify this particular Axiom installation for purposes of future client updates and for launching this installation via AXM shortcut. You can leave the default settings to use the automatically-computed number for the identity (recommended), or you can clear the check box and enter a number. (If you manually enter a number, you should put the same number on the file type suffix.) You can also choose to disable use of the identity, but this is not recommended.



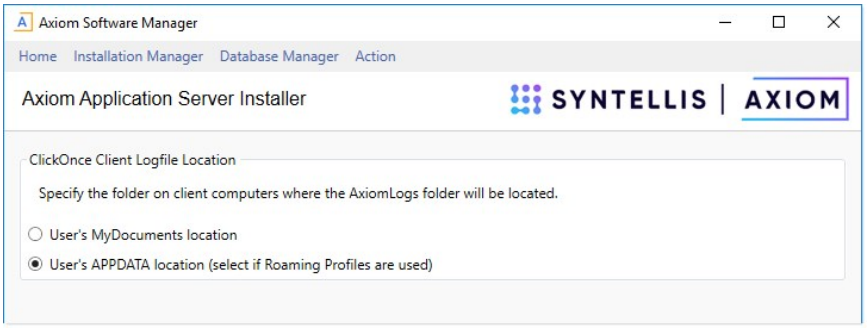
13. On the **Default Proxy Configuration** screen, specify whether to allow use of the default proxy when accessing the Axiom Application Server, and then click **Next**.

    If **Disable use of the default proxy for application server access** is selected (the default behavior), then users cannot use the default proxy to access the application server. In most environments this will improve performance.

    However, in some environments disabling proxy access may prevent clients from being able to access the application server. For these environments, the check box should be cleared to allow use of the default proxy.

14. On the **ClickOnce Client Logfile Location** screen, specify the location where the AxiomLogs folder will be created on client machines, and then click **Next**.

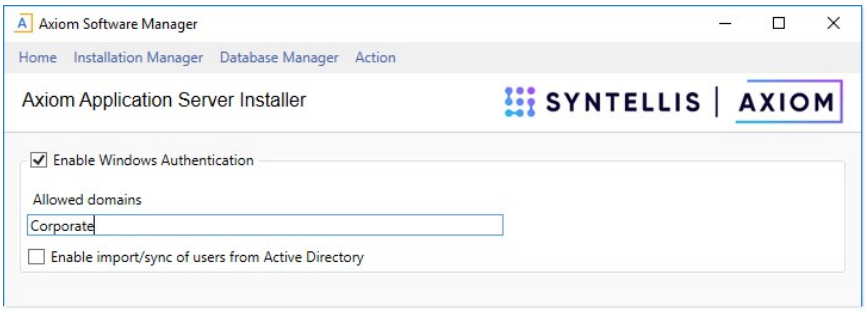
    By default, the folder is created in the user's APPDATA folder. If desired, you can change the location to the user's My Documents folder.



15. On the **Enable Windows Authentication** screen, choose whether to enable Windows Authentication, and then click **Next**.

    If you want to use Windows Authentication, then leave the **Enable Windows Authentication** option checked and complete the following settings. If you do not want to use Windows Authentication, then clear the check box. For more information, see Authentication methods.

Item	Description
Allowed domains	The recognized domains for Windows Authentication. Enter one or more domain names. Separate multiple domain names with commas. Users will be authenticated against the specified domains.
Enable import/sync of users from Active Directory	If selected, then the installation will allow use of the Active Directory Import Scheduler task to import and synchronize Active Directory users into Axiom security. Selecting this option simply enables the ability to use the Scheduler task. You must set up the Scheduler task within a system and schedule it for execution in order to import and synchronize users. If this option is not selected, then the Scheduler task can be configured but it will not execute.



NOTE: You can change these settings for the installation later by using **Installation Manager > Configure Authentication Methods**.

16. On the **Enable LDAP Authentication** screen, choose whether to enable LDAP Authentication, and then click **Next**.

    If you want to use LDAP Authentication, select **Enable LDAP Authentication** and then complete the following settings. For more information, see Authentication methods.

Item	Description
LDAP server connection string	The connection string for the LDAP directory that you want to authenticate users against.
LDAP connection user name	The user identity under which the application server will access the LDAP directory, for the purposes of passing user credentials for authentication.
LDAP connection password	The password for the designated user name.
Allowed suffixes	Recognized suffixes for use with LDAP authentication, such as: `@mydomain.local`. Including the @ sign in the suffix is optional (if it is omitted, it will be automatically included when submitting credentials for authentication). If needed, separate multiple suffixes with commas.

    NOTE: You can change these settings for the installation later by using **Installation Manager > Configure Authentication Methods**.

17. On the **SAML Authentication** screen, click **Next**.

    SAML Authentication is not supported for use with on-premise installations. It is only present in the installer for legacy installations.

18. On the **OpenID Authentication** screen, choose whether to enable OpenID Authentication, and then click **Next**.

    If you want to use OpenID Authentication, select **Use OpenID for user authentication** and then complete the following settings.

Item	Description
OpenID provider API client ID	The client ID for the OpenID provider.
OpenID provider API client secret	The client secret for the OpenID provider.

    For example, if using Google OpenID Connect, the client ID and client secret can be obtained from the Google Developers Console, within the project you are using for authentication.

NOTE: Additional setup is required to fully enable the OpenID Authentication. For more information, see Authentication methods and contact Axiom Support for assistance as needed.

19. On the **Ready to install** screen, click **Install** to begin the installation.

A status bar displays the progress of the installation. When the installation is complete, click **Done** to exit the installer. You are returned to the **Installation Manager** screen, where you can see the details of the newly installed application server.

Installing Axiom Scheduler Service

Use the Axiom Software Manager to perform the Axiom Scheduler Service installation on each server that you want to use for Scheduler task processing. Larger installations may need multiple dedicated Scheduler servers. The logged in user must have administrator rights on the server to run the installation.

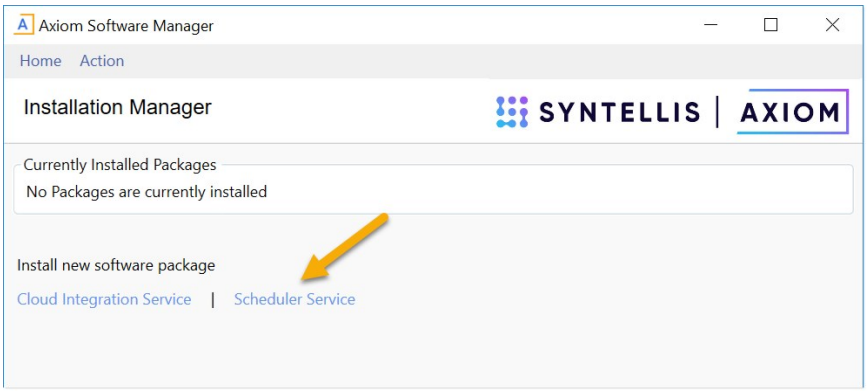
NOTES:

- Scheduler does not direct task traffic to other machines, it performs processing on the machines where it is installed.
- Once you enter the installation screens, there is no Cancel button. To cancel an installation, move to a different location within the Axiom Software Manager, or close the Software Manager.

To install the Axiom Scheduler Service:

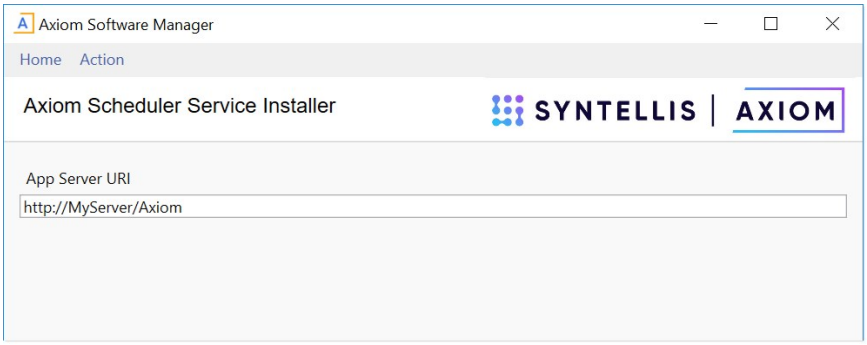
1. Navigate to the location on the server where you have saved the Axiom Software Manager, and then double-click `AxiomSoftwareManager.exe`. For more information, see Axiom Software Manager.
2. From the **Home** screen of the software manager, under **Install new software package**, click **Scheduler Service**.

NOTE: This instruction assumes that there is no signed Axiom certificate on the server and therefore the Axiom Software Manager is in "limited" mode. The certificate is *not* required in order to install the Scheduler Service. However, if a certificate is present on the machine, then you can reach this screen by selecting **Installation Manager > Manage Software Packages** from the menu bar (or by clicking the **Manage Software** icon on the Home screen).



The Axiom Scheduler Service Installer begins. The installation is performed within the Software Manager—a separate installer program is not launched. While using the installer, do not use the menu to move to other locations in the Software Manager, unless you want to cancel the installation.

3. On the **License Agreement** screen, click **I accept** and then click **Next**.
4. On the **App Server URI** screen, specify the URI to the Axiom Application Server, and then click **Next**.



This is the URI that the Scheduler service will use to access the Axiom Application Server. By default, this is `http://<APPSERVER>/Axiom`. You must edit the URI to specify the name of the server where the application server component was installed. If you changed the name of the virtual directory for the application server, then you must edit that too.

5. On the **Installation Folder** screen, specify the installation location for the Scheduler program files, and then click **Next**.

   You can accept the default installation location, or click **Browse** to select a different location. By default, the location is:

   `C:\Program Files (x86)\Axiom EPM\Axiom EPM Scheduler Service`

6. On the **Service Name** screen, specify the name of the Scheduler service, and then click **Next**.

The default name is **Axiom EPM Scheduler Service**. We recommend leaving the default name unless you will be installing multiple versions of the service on this machine and you need to be able to differentiate them.

7. On the **Axiom Server Encryption Key** screen, enter the encryption key that was used in the Axiom Application Server installation, and then click **Next**.

   The key must match the key used by the application server. The key is used to encrypt traffic between the Scheduler service and the application server.

   > **TIP:** If you do not know the encryption key that was used for the Axiom Application Server installation, you can look it up. Open the Axiom Software Manager on the Axiom Application Server, then select **Installation Manager > Configure Service Encryption**. Place your cursor in the field to read the encryption key.

8. On the **Application server** screen, specify whether to use the embedded application server, and then click **Next**.

   By default, the Scheduler installation includes an embedded application server instance that can be used to poll for queued Scheduler jobs, service requests as a result of job processing, and report the status of the Scheduler service to the system.

   It is recommended for most configurations to leave **Use embedded application server** enabled, for improved system performance. However, in some situations you may wish to disable this option. For example, if a firewall prevents direct contact between the Scheduler server and the database server, then you should disable this option.

   The second option on this screen, **Install EdiDev runtime components**, only applies to Contract Management installations. This option must be left unchecked unless you are instructed to enable it as part of a Contract Management implementation.

9. On the **Ready to Install** screen, click **Install** to begin the installation.

A status bar displays the progress of the installation. When the installation is complete, click **Done** to exit the installer. You are returned to the **Installation Manager** screen, where you can see the details of the newly installed package.

Post-installation steps

Axiom will attempt to automatically start the Scheduler service after the installation. If you discover that the service is not running, you can start it manually as follows:

1. In Windows **Administrative Tools**, go to **Services**.
2. Right-click **Axiom EPM Scheduler Service** and then select **Start**.

Installing Axiom Update Service

If necessary, use the Axiom Software Manager to install the Axiom Update Service on the Axiom Application Server. The Axiom Update Service may be required if your Axiom implementation needs to install product packages on an ongoing basis, to apply the latest version of Axiom products. Custom implementations and implementations with non-upgradable products do not need to install the update service.

NOTES:

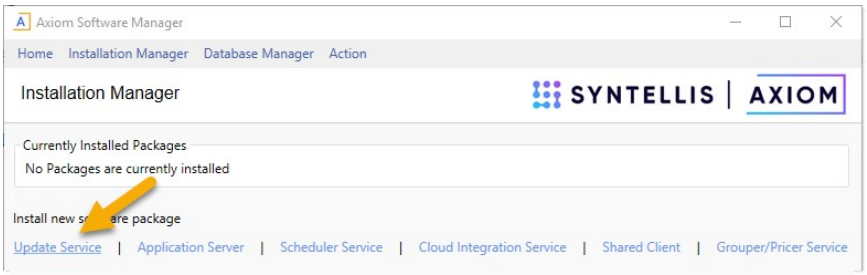
- Only certain product installations require the update service to install the product package. If you are not sure whether it is required, check the documentation for your products.
- Once you enter the installation screens, there is no Cancel button. To cancel an installation, move to a different location within the Axiom Software Manager, or close the Software Manager.

To install the Axiom Update Service:

1. Navigate to the location on the server where you have saved the Axiom Software Manager, and then double-click `AxiomSoftwareManager.exe`. For more information, see Axiom Software Manager.
2. From the **Home** screen of the software manager, click **Manage Software**.

   TIP: You can also click **Installation Manager > Manage Software Packages** on the menu bar.

3. On the **Installation Manager** screen, under **Install new software package**, click **Update Service**.



   IMPORTANT: If you do not see this option, then the server does not have a signed Axiom certificate. See Installing the Axiom certificate.

   The Axiom Update Service Installer begins. The installation is performed within the Software Manager—a separate installer program is not launched. While using the installer, do not use the menu to move to other locations in the Software Manager, unless you want to cancel the installation.

4. On the **License Agreement** screen, click **I accept** and then click **Next**.

5. On the **Installation Folder** screen, specify the installation location for the Update Service program files, and then click **Next**.

   You can accept the default installation location, or click Browse to select a different location. By default, the location is:

   `C:\Program Files (x86)\Axiom EPM\Axiom EPM Update Service\`

6. On the **Service Name** screen, specify the name of the update service, and then click **Next**.

   The default name is **Axiom EPM Update Service**. We recommend leaving the default name unless you will be installing multiple versions of the service on this machine and you need to be able to differentiate them.

7. On the **Ready to Install** screen, click **Install** to begin the installation.

A status bar displays the progress of the installation. When the installation is complete, click **Done** to exit the installer. You are returned to the **Installation Manager** screen, where you can see the details of the newly installed package.

Uninstalling server components

The Axiom server components can be uninstalled by using the Axiom Software Manager.

NOTE: These server components do not display in the Windows program manager and cannot be uninstalled from that location.

To uninstall a server component:

1. On the server where you want to uninstall a component, navigate to the location where you saved the Software Manager, and then double-click `AxiomSoftwareManager.exe`. For more information on the Software Manager, see Axiom Software Manager.

   If you did not save a copy of the Software Manager on the server, then you will need to obtain a copy in order to perform the uninstall. You can download Axiom installation packages from Axiom Help, or you can request a copy from Axiom Support. In order to uninstall a component, you can use the same version that is currently installed or a higher version.

2. If you are on a server with a signed Axiom certificate and therefore using the "full" version of the Software Manager, click **Manage Software** from the Home screen. (Alternatively, you can click **Installation Manager > Manage Software Packages** on the menu bar.) This step is not necessary when using the "limited" version of the Software Manager, because the Home screen of the limited version is the Installation Manager screen.

3. In the **Installation Manager** screen, in the **Currently Installed Packages** section, locate the component that you want to uninstall, and then click **Uninstall**.

4. At the first uninstall confirmation screen, click **Next** to continue.

5. At the **Local Content** screen, specify whether to preserve locally modified files, or delete all package files, and then click **Next**.

   By default, **Preserve locally modified files and logs** is selected. This means that any file that was modified after installation, such as log files and .config files, will not be deleted as part of the uninstall. If later you want to reinstall to this same folder location, you will need to manually delete these files and the installation folder.

   If you know that you do not need these files, you can select **Remove package folder and all files**. In this case the entire installation folder will be deleted.

6. Click **Uninstall**.

Repairing or modifying server components

You can repair and modify server components using the Software Manager. When you repair a component, the component is basically reinstalled. You can change any of the installation options.

During the repair process, all configuration files are replaced with the deployment versions, even if they have been locally modified. This is different than the upgrade process, which preserves locally modified configuration files.

To repair or modify a server component:

1. On the server where you want to repair a component, navigate to the location where you saved the Software Manager, and then double-click `AxiomSoftwareManager.exe`. For more information on the Software Manager, see Axiom Software Manager.

   If you did not save a copy of the Software Manager on the server, then you will need to obtain a copy in order to perform the repair. You can download Axiom installation packages from Axiom Help, or you can request a copy from Axiom Support. In order to repair a component, you must use the same version that is currently installed (if you use a higher version, the component will be upgraded as part of the repair).

2. If you are on a server with a signed Axiom certificate and therefore using the "full" version of the Software Manager, click **Manage Software** from the Home screen. (Alternatively, you can click **Installation Manager > Manage Software Packages** on the menu bar.) This step is not necessary when using the "limited" version of the Software Manager, because the Home screen of the limited version is the Installation Manager screen.

3. In the **Installation Manager** screen, in the **Currently Installed Packages** section, locate the component that you want to repair, and then click **Repair**.

Progress through the installation screens and modify any options as desired.

5

Installing the Axiom Client

This section discusses the installation process for the Axiom Excel Client and Axiom Windows Client on individual client workstations using ClickOnce deployment. Both the Excel Client and the Windows Client are installed using the same installer. Once the installer has been run, either client can be launched on the machine. The term *Desktop Client* is often used to refer to both of these clients.

The Axiom Web Client operates within a browser and does not require any installation. The only requirement is a browser that meets the technical requirements. For information on these requirements, see the separate document *Client Technical Requirements*.

NOTE: Certain system configuration settings should be completed before the client is deployed to end users. However, at least one client installation must occur before you can set up users in Security and finish configuring the default system Scheduler jobs. You may also want to deploy the client to a handful of users for system testing before finalizing the configuration settings. For more information on configuration, see Configuring Axiom.

Before you install

Before beginning the client installation process, make sure the following prerequisites have been completed on the client workstations:

- A supported browser with ClickOnce support is present on the client machines. See Web browser.
- Microsoft .NET Framework is installed. See Microsoft .NET Framework.
- Microsoft Excel is installed on any machine where you want to use the Excel Client. See Microsoft Excel.
- Microsoft VSTO is installed on any machine where you want to use the Excel Client. See Microsoft VSTO.

The only installer prerequisite is .NET. If the minimum required version of .NET is not present, the installer displays a message about the missing requirement and cancels the installation. If the other prerequisites are not present, then the client program will still be installed on the machine, but it may not be able to be launched until the remaining prerequisites are installed.

Installing the Axiom Client on client workstations

This section explains the installation of the Axiom Desktop Client on individual client workstations using ClickOnce.

Use of ClickOnce for client installations

Axiom takes advantage of the Microsoft ClickOnce technology that is included with the Microsoft .NET Framework. This technology allows for the installation and launch of the Axiom Excel Client or Windows Client software with minimal interaction from the user.

The IT department, which is responsible for the implementation of Axiom along with the maintenance of the servers that Axiom resides on, benefits from the ClickOnce technology in three major ways:

- **The Axiom Client is easy to update.** When upgrading to a new version of Axiom, the upgrade software is only run on the Axiom server components. When a user launches the Axiom Client, the software immediately recognizes that a new version has been installed, prompts the user to install it, downloads and installs the update, and then launches the application.
- **Minimal impact to user computers and other installed applications.** Traditional applications are installed using Windows Installer deployment and often rely on shared components, which can create potential versioning conflicts. By utilizing the ClickOnce deployment technology, the Axiom Client is completely self-contained and does not interfere with other applications.
- **No changes to end user permissions.** Applications deployed using Windows Installer often require “local administrator” permissions, which can present problems when users do not have such access. Non-administrative users can install and launch the Axiom Client without elevated permissions.

Performing the client installation

You can perform the Desktop Client installation from any page of the Axiom Web Client, using the **Quick Launch** menu. The current browser must support ClickOnce in order to directly install or launch the client. For more information, see Requirements to install and launch the Desktop Client from the browser.

Users must log in to Axiom in order to install the Desktop Client from the Web Client. Anonymous access is not allowed. Users cannot install the client and then obtain login credentials later.

To install the Axiom Desktop Client:

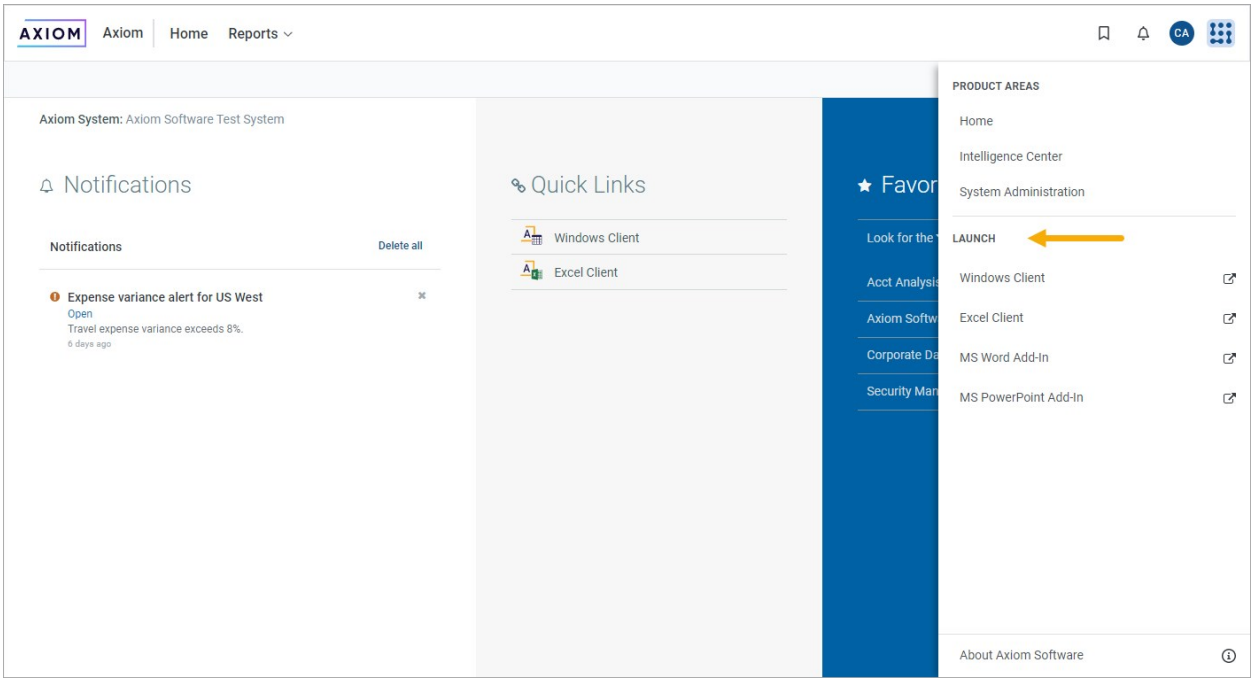
1. Open the Axiom Web Client in your browser, using the following URL:

   `https://<servername>/Axiom`

   Where *<servername>* is the name of the application server and Axiom is the default name of the virtual directory. If you specified a different virtual directory name during the application server installation, you must use that.

2. Enter your user name and password to access Axiom.
3. Once you have logged in, click the Syntellis icon in the top right of the Navigation bar.
4. In the Launch menu, click on one of the following:
    - **Windows Client**
    - **Excel Client**

> **TIP:** If you see the default home page when you log in (as shown in the following screenshot), you can also install and launch the client using the links in the **Quick Links** section.



Example Quick Launch menu to install and launch the Desktop Client

The first time that a user launches the client from a specific workstation, the following occurs:

1. The installer verifies that required prerequisites are present. As previously noted, the installer only checks for the minimum required version of .NET. The absence of other prerequisites does not stop the installation.
2. The installer downloads the client installation package and installs both clients (Excel and Windows).
3. When the installation is finished, the client type (Excel or Windows) that was specified in the link is launched.

Each subsequent time that the user launches the client from a specific workstation, the following occurs:

1. The installer checks the application server for any system updates. If any updates are found, they are downloaded and installed. Otherwise, no installation activity occurs on subsequent visits.

2. The client type (Excel or Windows) that was specified in the link or shortcut is launched.

For example, if a user first clicks on the link to launch the Excel Client, it will install the client program and then launch the Excel Client. If the user subsequently clicks on the link to launch the Windows Client, then the program does not need to be installed again, and the link will simply launch the Windows Client.

NOTE: If your end users will be using the Windows Client exclusively, you can optionally hide the Excel Client icon from the Quick Launch menu. To do this, set the system configuration setting **AllowShowExcel** to **False**. If you have a handful of users who need to install the Excel Client, those users can install it before you hide the icon, or you can use an installation URL to directly install/launch the Excel Client.

Prerequisite downloads

If a user does not have the necessary prerequisites to install the Axiom Desktop Client, these prerequisites can be installed from the Web Client as needed. Generally, installation of prerequisites requires administration privileges on the client machine.

To access the prerequisite download page:

1. Click the Syntellis icon in the Navigation bar across the top of the page to open the Area menu.
2. Click **About Axiom Software** at the bottom of the Area menu.
3. In the About Axiom Software dialog, under **Download**, click **Necessary software tools for running Axiom desktop client applications**.

This takes you to the prerequisite download page. From here, you can download prerequisites such as Microsoft .NET and VSTO.

Installation URLs

If desired, you can provide users with a link to install and launch the appropriate client, instead of having them launch it through the Web Client. The following are some common launch URLs:

Launch Action	URL
Excel Client	`http://<servername>/Axiom/c1/Axiom.UI.Start.application?client=Excel`
Windows Client	`http://<servername>/Axiom/c1/Axiom.UI.Start.application?client=Windows`
Use a language override	`http://<servername>/Axiom/c1/Axiom.UI.Start.application?client=Excel&lang=FR-fr` Substitute the desired client and language code.

Contact Axiom Support if you need assistance determining the correct URL to provide to your users for direct install/launch.

Client shortcuts

Shortcut creation for the Axiom Desktop Client depends on the selections initially made during the application server installation. These shortcut options can be changed later by using Repair on the application server installation, or by modifying the system configuration settings.

The default behavior is to create shortcuts on both the desktop and the Start menu as needed—meaning, when a particular client version is launched (Excel Client or Windows Client), a shortcut is created for that specific version. For example, if a user only ever launches the Excel Client, then they will only have a shortcut to the Excel Client. If a user launches both clients, then they will have separate shortcuts for each client.

There are several shortcut options for the ClickOnce deployment, including placing shortcuts for both clients by default, or placing no shortcuts, or using the default ClickOnce shortcut that always launches the last-launched client. You can also specify whether shortcuts are created on the desktop, the Start menu, or both. For more details on the available options, see Installing the Axiom Application Server.

NOTE: Some authentication methods, such as OpenID, do not support launching the Axiom Desktop Client via shortcut.

Uninstalling or repairing client components

▶ Uninstalling the ClickOnce Client

The Axiom ClickOnce Client can be uninstalled by using the program manager in the Windows Control Panel (**Uninstall or change a program**). Select **Axiom EPM Client**, and then select **Remove** or **Uninstall**. At the prompt, select **Remove the application from this computer**.

NOTE: If you used either of the AXM shortcut options for the ClickOnce installation, then those shortcuts will not be automatically removed from the desktop and/or the Start menu when the client is uninstalled. You must manually remove these shortcuts.

The uninstall process does not remove any files that have been modified after installation, such as log files. You can manually delete these files in the user's Windows document directory after uninstalling.

Repairing the ClickOnce Client

The Axiom ClickOnce Client can be repaired by using the program manager in the Windows Control Panel (**Uninstall or change a program**). Select **Axiom EPM Client**, and then select **Remove** or **Uninstall**. At the prompt, select **Restore the application to its previous state**.

6

Configuring Axiom

This section provides information on the initial Axiom system setup and configuration.

Editing system configuration settings

Axiom has a number of configuration settings that can be set on a per system basis. These settings are managed by using the Software Manager. For the purposes of editing system configuration settings, the Software Manager must be run on the Axiom Application Server.

NOTE: The system configuration settings can also be edited within Axiom itself, if desired. To do this, you must set up an Axiom file to use Save Type 4. For more information, see the following topic in Axiom Help: **Updating system configuration settings using Save Type 4** (AX2346).

To edit system configuration settings:

1. In the Software Manager, click **Installation Manager > Configure System Properties**.

   IMPORTANT: If you do not see this option, then the server does not have a signed Axiom certificate. See Installing the Axiom certificate.

2. If necessary, from the **Application Server** list, select the application server installation.

   In most cases, only one instance of the Axiom Application Server is present on the machine, and you do not need to change anything. This option is for situations where multiple application servers may be installed on the same machine.

3. Edit any of the configuration settings as desired. For more information on the available configuration settings, see System Configuration Settings.

   For example, you may want to edit the **Scheduler_FromEmailAddress** property, to specify an email address to use as the "From" address for Axiom email notifications. By default, this is set to `noreply@axiomepm.com`. This address will be used in all cases where a separate "From" address is not specified.

4. Click **OK**.

Resetting the application server cache

The edited configuration settings will not be recognized until the application server cache is reset. The Software Manager will attempt to reset the cache automatically when you save changes to the system configuration settings. (Using Save Type 4 in the software will also automatically reset the cache as part of the save process.)

However, if you ever need to reset the cache manually, you can do so as follows:

1. In the Software Manager, click **Installation Manager > Reset Server Cache**.

   IMPORTANT: If you do not see this option, then the server does not have a signed Axiom certificate. See Installing the Axiom certificate.

2. If necessary, from the **Application Server** list, select the application server installation.

   In most cases, only one instance of the Axiom Application Server is present on the machine, and you do not need to change anything. This option is for situations where multiple application servers may be installed on the same machine.

3. Click **Reset**.

TIP: You can also reset the application server cache in the Axiom Web Client, from **System Administration > Infrastructure Section > Reset Services**.

Setting up Scheduler

Axiom's Scheduler services manage certain system tasks and can also be used to automate user-defined tasks. After Axiom is installed, you must complete the Scheduler setup.

This setup is performed using the **Scheduler** dialog in the Axiom Desktop Client (Excel or Windows). You must have installed at least one client instance in order to perform these setup steps.

To access the Scheduler dialog:

1. Launch the Axiom Excel Client or the Windows Client. You must log in as a user that has system administrator rights.

   If you started with a new blank database, you can log into the system using the built-in admin user (user name: admin, password: admin). You should change the password of this user after logging in. Once real users have been set up for your implementation, you can delete this user.

2. On the **Axiom** tab, in the **Administration** group, click **Manage > Scheduler**.

   NOTE: In systems with installed products, this feature may be located on the **Admin** tab. In the **System Management** group, click **Scheduler**.

Enabling Scheduler services

Each system has a system Scheduler service that runs on the Axiom Application Server, and one or more manually installed Scheduler services.

The system Scheduler service is installed and activated automatically as part of the Axiom Application Server installation. No special setup steps apply. This service is only used to process system jobs.

The manually-installed Scheduler services must be explicitly enabled within the Scheduler dialog. Even though the service itself is started as part of the Scheduler services installation, these services must be enabled in Scheduler in order to begin processing tasks.

To enable Scheduler services:

1. In the **Scheduler** dialog, on the **Service** tab, click **Servers**.

   You should see at least two entries in the **Servers** tab:

   - *<AppServerName>*-System: This is the system Scheduler service.
   - *<SchedulerServerName>*: This is a manually installed Scheduler service. You will have an entry for each server where you manually installed Scheduler.

2. For each manually-installed Scheduler service, select the service in the list. In the **Configuration details** section, select the **Processing Enabled** check box, and then click **Update**.

   NOTE: The **Configuration details** section also contains several configuration settings for the Scheduler service. We recommend leaving the default settings unless you are instructed to change them by Axiom Support. For more information, see Axiom Help: **Scheduler > Scheduler administration > Managing Scheduler servers** (or search for AX2542).

These Scheduler servers are now available to process Scheduler jobs.

Configuring Scheduler system jobs

Scheduler provides several system jobs that should be configured as part of your system setup activities. These jobs are created automatically by the Scheduler service when it is started. These jobs control email notifications for Scheduler and other system processes, and cleanup processes for the database.

NOTE: The SMTP Message Delivery job must be configured in order to enable email notifications for Axiom. If this job is not configured, then email notifications will be created and saved in the database, but they will not be sent.

To configure the Scheduler system jobs:

1. In the **Scheduler** dialog, on the **Service** tab, click **Scheduled Jobs**. You should see the following scheduled jobs where the name starts with **System**:

   - **System.ProcessNotification**

- **System.SystemDataPurge**
- **System.IndexMaintenance**

2. Double-click a job to open it for editing. Once you have modified the job as needed, click **Save**.
   - In the **Tasks** section, select the task name to access the task settings, and then edit the **Task Details** as necessary. See the following section for more details on the specific task settings.
   - In the **Notifications** section, configure the email notifications for the job as desired. By default, the jobs are configured to send notifications on error, however, you must specify a valid email address to receive these notifications (such as the email address of a system administrator).
3. On the **Service** tab, click **Event Handlers** and then locate the **System.SMTPMessageDelivery** event in the list. Double-click the event to open the associated job (with the same name), then configure the task settings. For more information, see Axiom Help: **Scheduler > Scheduler setup > Setting up email delivery for Axiom** (or search for AX1769).

The changes will apply the next time the job is executed.

System job overview

The following list provides a brief description of the purpose of each job and its task settings.

SMTPMessageDelivery

Description	This job enables email notifications for Scheduler jobs and other system processes, such as process management notifications. Email notifications are stored in the database until the job picks them up and sends them.
Configuration	This task is not operational until you specify the name of a valid SMTP server in your environment. Once you have completed the SMTP server settings, make sure to disable **Test Mode** so that email notifications will be sent.
Schedule	This job is not a scheduled job. Instead, it uses an event handler so that the job is triggered for execution whenever there are email messages ready to be sent.

ProcessNotification

Description	This job enables reminder notifications for process management. These are notifications to remind users of upcoming due dates and overdue tasks.
Configuration	This task does not have any editable settings.
Schedule	By default, this job is set to execute once per hour. You should not change the frequency of this job.

SystemDataPurge

Description	This job purges old data from the system, such as old Scheduler job results, old email notifications, old temp table data, and old audit data. This task should be run regularly to help keep old and unnecessary data from impacting system performance.
Configuration	This task is configured to delete items that are older than a specified number of days (by default, 15 days). You can change the default settings for this task if desired.
Schedule	By default, this job is set to run every ten minutes from midnight to 4:00 AM. The task is operational as soon as it is created by the Scheduler service, using the default settings.

IndexMaintenance

Description	This job maintains the indexes on your Axiom databases (system database and audit database). It reports the current index fragmentation and then reorganizes or rebuilds the indexes as needed, depending on the current level of fragmentation. It also updates table statistics.
Configuration	Any changes made to the SQL statements in this system job should only be made with the guidance of Axiom Support and/or your SQL database administrator.
Schedule	By default, this task is set to run once per day, at 5:15 AM. The task is operational as soon as it is created by the Scheduler service, using the default settings.

Email notifications for system jobs

By default, most system jobs are configured to send notifications on error, however, you must edit the job to specify a valid email address for the notifications (such as the email address of a system administrator). In the **Notifications** section for the job, edit the email notification settings as desired. The default setting of `{CurrentUser.EmailAddress}` cannot be used because the job is run by the system and therefore does not resolve to a user email address.

NOTE: It is recommended to leave the SMTPMessageDelivery job at the default notification behavior of None. If this job experiences an issue attempting to send email, it likely will be unable to send you an email notification about this error.

Setting up security

This section provides an overview to security setup considerations for Axiom.

Creating users in Axiom

All users must be set up in Axiom security in order to access the system. User setup is performed within the Axiom Client.

To access the Security Management dialog:

1. Launch the Axiom Excel Client or the Windows Client. You must log in as a user that has system administrator rights.

   If you started with a new blank database, you can log into the system using the built-in admin user (user name: admin, password: admin). You should change the password of this user after logging in. Once real users have been set up for your implementation, you can delete this user.

2. On the **Axiom** tab, in the **Administration** group, click **Manage > Security > Security Manager**.

   NOTE: In systems with installed products, this feature may be located on the **Admin** tab. In the **System Management** group, click **Security > Security Manager**.

You must have installed at least one client instance in order to perform these setup steps. For more information on how Axiom security works, and details on specific security settings, see Axiom Help: **Security**.

Configuring security options for the installation

Enabling or changing authentication methods

During the application server installation, you had the option to enable various authentication options for use with Axiom. If you did not enable these options during the installation but you would like to do so later, or if you need to change any of the configuration settings for these options, you can do so in the Software Manager using **Installation Manager > Configure Authentication Methods**. The Software Manager must be run on the Axiom Application Server to modify the authentication options.

Configuring a user lockout threshold

If desired, you can configure a user lockout threshold for Axiom, so that user accounts are locked out of the system if they exceed a specified number of failed login attempts. By default, no lockout threshold is defined (unlimited attempts). You can define a user lockout threshold using the **MaxLoginAttempts** system configuration setting. For information on editing system configuration settings, see Editing system configuration settings.

Resetting a user password

You can reset a user's password from within the Software Manager. You might use this functionality if the user has been locked out or has forgotten their password, and you cannot access the Axiom Client to change the password using the Security Management dialog.

To change a user's password, select **Installation Manager > Reset Axiom User Password**. The Software Manager must be run on the Axiom Application Server to access this feature. When specifying the user name, you must preface it with the domain name if applicable (for example: domain\username). Changing the user's password using this method also clears the user lockout, if applicable.

Updating your license file

When you first installed Axiom, you imported a license file into your system database. You can update this license file using the Software Manager or using the administration features of the Axiom Web Client. For example, you may need to update your license file if you purchase additional licensed users, or if your current license file is about to expire.

As long as your license has not yet expired, you can update it from the Axiom Web Client:

1. In a web browser, open the Axiom Web Client and go to the license update page. For example:

   `http://servername/Axiom/admin/license`

   Where *servername* is the name of your Axiom Application Server, and Axiom is the default virtual directory name.

   You can also access this feature from the System Administration area of the Web Client.

   TIP: You can also access this web page from within the Axiom Excel Client or Axiom Windows Client. From the **Axiom** or **Admin** tab, click **Help > About Axiom Software**, and then click the **Update License** link at the top of the dialog.

2. On the Update Axiom Licenses page, click **Choose license file to import**.
3. Navigate to the license file, and then click **Open**.

The new license has been imported into your system. You can see the license details listed on the page.

You can also update your license file from the Software Manager, using **Installation Manager > License Manager**. You must use this method if your license file has expired, because in that case you will not be able to log into the Web Client. The Software Manager must be run on the Axiom Application Server to access the License Manager.

Configuring the service encryption key

Each installation has a service encryption key which was defined as part of the Axiom Application Server installation. If desired, you can change this encryption key later using the **Configure Service Encryption** screen.

1. In the Software Manager, click **Installation Manager > Configure Service Encryption**. The Software Manager must be run on the Axiom Application Server to access this option.
2. If necessary, from the **Application Server** list, select the application server installation.

   In most cases, only one instance of the Axiom Application Server is present on the machine, and you do not need to change anything. This option is for situations where multiple application servers may be installed on the same machine.
3. In the **Axiom Server Encryption Key** field, do one of the following:
   - Click **Generate** to generate a new random encryption key. This is the recommended approach.
   - Type your own key. Axiom does not enforce any rules on the key string. If you choose to use your own key, it is your responsibility to ensure that the key is of an adequate strength for your organization's security requirements.
4. Click **Update**.

The encryption key is changed for the installation.

TIP: You can use this screen to find out the encryption key if you need it for an installation but you did not retain a record of it. For example, if you installed the Axiom Application Server but forgot to record the key for use in the Axiom Scheduler Service installation. You can come to this screen and place your cursor in the field to read the encryption key.

Reloading system documents

Axiom has a number of system documents and templates that are added automatically to new blank systems the first time the new database is upgraded. This includes control sheets for various features, the new report template, the default home file, standard task panes and ribbon tabs, and other documents.

Subsequent document updates are handled as follows:

- The following documents are always updated when a database is upgraded: control sheets, sample task panes and ribbon tabs, and support utilities.
- All other documents can be manually updated as desired using the **Reload System Documents** screen in the Software Manager.

To reload system documents:

1. In the Software Manager, click **Installation Manager > Reload System Documents**. The Software Manager must be run on the Axiom Application Server to reload system documents.
2. If necessary, from the **Application Server** list, select the application server installation.

   In most cases, only one instance of the Axiom Application Server is present on the machine, and you do not need to change anything. This option is for situations where multiple application servers may be installed on the same machine.
3. Select the documents that you want to update. When the update is processed, the selected documents will be added to the target system, replacing any existing version of the document.
4. Click **Update**.

The selected documents are updated.

Editing the connection string to the Axiom database

The connection string to the Axiom database must be defined during the Axiom Application Server installation. If necessary, you can modify the connection string later using the **Configure Connections** screen.

NOTE: The Configure Connections screen can only be used to modify application servers that are at the same version as the Software Manager.

To edit the connection string:

1. In the Software Manager, click **Installation Manager > Configure Connections**. The Software Manager must be run on the Axiom Application Server to access this option.
2. If necessary, from the **Application Server** list, select the application server installation.

   In most cases, only one instance of the Axiom Application Server is present on the machine, and you do not need to change anything. This option is for situations where multiple application servers may be installed on the same machine.
3. Edit the **Database Server Details** as appropriate:

Item	Description
Server Name	The server name of the database server that hosts the Axiom database.
Failover Partner	Optional. The server name of the database server to be used in failover situations. This only applies to Axiom Cloud systems; otherwise it should be left blank.

Item	Description
Database Name	The name of the database for Axiom.
Login	The login name for the Axiom database.
Password	The password for the Axiom database.
Update Database user and password	Select this option if you want to change the login name and password to what you have entered in this screen. Otherwise, you must enter the login name and password as they were originally defined.

4. Click **Update**.

Backing up and restoring the Axiom database

The Axiom database should be backed up regularly using SQL Server backup functionality. Your IT department and/or database administrator should manage this backup as part of their regular backup processes. In addition to regular backups, you should make sure to take a backup before performing any system activity that may result in major database or system changes, such as before upgrading the installation.

The Axiom Software Manager can also be used to take a backup of the database, but the Software Manager's backup feature is only for "one-off" backups, not for regular ongoing backups.

Both related Axiom databases—the application database and its corresponding audit database (if standalone)—must be backed up as a set so that they remain in sync.

Managed files are stored in the Axiom application database. As long as all Axiom files are managed, then there is no need for any additional network folder or file backups in order to back up Axiom systems. If users are saving report files as non-managed files to their local drives or to a network share, these files should be backed up according to your normal file system backup processes.

If you need to restore the database, make sure to restore both related databases from the same backup “set.” The only time that you should restore only an application database is when directed to do so by Axiom Support, to troubleshoot or resolve a specific issue, or when the audit database is embedded in the application database. If the audit database is a standalone database, both database components should be restored together.

You can use standard SQL Server functionality to restore an existing database, or you can use the Axiom Software Manager. The only time that you *must* use the Software Manager to restore a database is when you are creating a new installation or a new system.

After restoring a database, you must always perform a database upgrade (even if you are restoring a database that was using the latest database version). If you restored the database using the Software Manager, the System.SMTPMessageDelivery Scheduler job is automatically set to test mode, so that the newly-restored system does not instantly start sending email notifications. To restore email functionality, you must edit the job in Scheduler and turn off test mode.

Backing up a database using the Software Manager

1. Open the Software Manager on the Axiom Application Server, then click **Database Manager > Backup Databases**. (You can also click **Backup** from the home screen.)
2. In the **Database Server Details** section, complete the following settings:

Item	Description
Database Server	The server name of the database server. If you are not using the default instance, append the instance name with a backward slash (Server\Instance).
Database Name	The name of the database.

3. In the **Options** section, complete the following settings:

Item	Description
Backup Folder	Specify the location for the backup. Paths are relative to the database server. **NOTE:** The Browse button does not apply unless the application server is also the database server.
Include Audit Database	Select this check box if you want to back up the corresponding audit databases for the selected system databases.

4. Click **Create Backup**.

The backup files are saved to the location specified in the backup settings. The backup process creates a SQL backup (.BAK) that is the same as a manual backup using SQL Management Studio.

Restoring a database using the Software Manager

For details on using the Axiom Software Manager to restore a database from backup, see Creating or restoring the database.

Enabling in-memory tables

Axiom supports in-memory tables. In-memory tables are stored in the main memory of the database server versus on disk (a "backup" version of the table is stored on disk for recovery purposes). Reading data from memory and writing data to memory can result in significant performance gains over disk-based table access.

Currently, this feature is limited to document reference tables (driver tables and other tables created using Save Type 3). Storing document reference tables in-memory may improve performance for systems with large document reference tables. Systems with smaller document reference tables are less likely to realize any noticeable performance benefit, as these smaller tables are cached on the client by default regardless.

In-memory tables are not audited. If the in-memory feature is enabled, auditing is disabled for document reference tables.

To enable in-memory tables:

1. In the Software Manager, click **Database Manager > Advanced Options**. The Software Manager must be run on the Axiom Application Server in order to access this option.
2. In the **Database Server Details**, verify that the **Server Name** and the **Database Name** are correct for the Axiom database that you want to configure. If not, enter the appropriate information.

   NOTE: You may be prompted to enter credentials for the specified database server, if those credentials have not already been stored in the Software Manager.

3. Select the check box for **Enable In-Memory Tables**.
4. Click **Apply**.

Enabling this option causes the following changes to be made to your database server:

- The Axiom database is enabled for Memory Optimized Data.
- A portion of the database server's memory is dedicated for use of in-memory tables. Currently this percentage is set at 3%.

After enabling the feature in the Software Manager, you must recycle the Axiom application pool so that the Axiom system recognizes the change. This is done on the Axiom Application Server, using the IIS Manager.

Document reference tables will be created in-memory the next time they are saved after enabling the feature.

Viewing system logs

Axiom maintains several logs that can be used to troubleshoot technical issues.

Component	Log file (default location)
Application Server	`C:\Inetpub\wwwroot\Axiom\logs` General application server activity is logged in AxiomServer.log, and Axiom form activity is logged in AxiomWebClient.log. These logs can also be accessed using the Axiom Web Client, in the **Application Server Administration > Logging** section.
Scheduler Service	`C:\Program Files(x86)\Axiom EPM\Axiom EPM Scheduler Service\logs` AND `C:\Inetpub\wwwroot\Axiom\scheduler\logs` (for the system Scheduler service)
Client Integration Service	`C:\Program Files (x86)\Axiom EPM\Axiom EPM Cloud Integration Service\logs`
Update Service	`C:\Program Files (x86)\Axiom EPM\Axiom EPM Update Service\logs`

Client	`C:\<WindowsUserDirectory>\<UserName>\AppData\Local\AxiomLogs`
	
	OR
	
	`C:\<WindowsUserDirectory>\<UserName>\My Documents\AxiomLogs`
	
	The client log can also be accessed from within the Axiom Client, from the **Help** menu.

Scheduler warnings

The application server checks the Scheduler schedule periodically, and logs any warning conditions to the event log for the application server machine. This logging is intended to warn about events that may indicate that one or more Scheduler servers are not running, or that a job has gotten "stuck." You can monitor for these events using any event log monitoring tool. The event source is Axiom.

Changing the logging level

You can temporarily change the logging level for the Axiom Application Server or the Axiom Client. You may want to change the logging level to help troubleshoot a specific issue. For assistance in determining the appropriate level of logging to troubleshoot your issue, please contact Axiom Support.

Changing the logging level for the Axiom Application Server

You can change the logging level for the application server using the Axiom Web Client.

1. In a web browser, open the Axiom Web Client and go to the logging page. For example:

   `http://<servername>/Axiom/admin/logging`

   Where *<servername>* is the name of the server hosting Axiom, and Axiom is the default virtual directory name.

   You can also access this feature from the System Administration area of the Web Client.

2. On the Logging page, select the check box to **Enable verbose logging for application server**. You can also enable verbose logging for the web client from this location.

Changing the logging level for the Axiom Client

You can change the logging level for the Axiom Excel Client or the Axiom Windows Client using the Log Analyzer tool.

1. On the **Axiom** tab, in the **Help** group, click the arrow underneath the Help icon, and then select **Log File Analyzer**.

   NOTE: If you are using an Axiom packaged product, you can access this feature from the **Admin** tab.

2. In the **Log Analyzer** window, click **Log Level** and then select the desired logging level.

Alternatively, the function AxLoggingLevel can also be used to temporarily change the logging level of the Axiom Client. To change the logging level, start the client and then type the following function into any file within the client:

`=AxLoggingLevel("LogLevel")`

The client log will return to the default setting the next time that you start the client.

Upgrading Axiom

This section details upgrade considerations and the upgrade process for Axiom.

Before you upgrade

Certain steps should always be performed before proceeding with any Axiom upgrade.

- **Review the release notes.** Make sure you understand the changes in the current release and any documented upgrade considerations. If you are upgrading from an older version, make sure to review the release notes for each interim version as well.

  IMPORTANT: Although Syntellis strives to maintain backward-compatibility with each release, any upgrade has the potential to interrupt system functionality. The *Upgrade Considerations* section of the release notes details known impacts to existing functionality, however, other impacts may be unforeseen at the time of release, or may be particular to your system. We strongly recommend performing the upgrade first on a test sandbox and then testing critical system functionality.

- **Perform the database pre-upgrade check.** The Axiom Software Manager provides a tool to check your database for potential backwards-compatibility issues before upgrade. If issues are found, they must be addressed before performing the upgrade.
- **Back up your database.** It is always a good idea to make a backup before performing any major system changes, such as an upgrade. For more information, see Backing up and restoring the Axiom database.
- **Make sure users are logged out of the system.** All users should be logged out of the system before performing the upgrade. You can communicate the planned upgrade time to users, and you can also use the System Access feature in the Windows Client or Excel Client to lock out non-admin users.

Performing the database pre-upgrade check

The Pre-Upgrade Check scans your database for known upgrade issues. Keep in mind that this check is not all-encompassing and does not guarantee that no backward-compatibility issues will exist in your system. It tests for known critical issues that can be detected in the database. Other issues may not be detectable with this kind of test or may not be known at this time.

1. Open the version 2022.3 Software Manager on the Axiom Application Server, and then click the **Upgrade** icon on the home screen.
2. Confirm the **Database Server Details** at the top of the upgrade screen.
3. Click **Pre-Upgrade Check**.

If the check finishes successfully, then you can continue with the upgrade process. If the check detects any issues, these issues should be addressed before proceeding with the upgrade. Please contact Axiom Support as needed for assistance in resolving these issues.

Upgrade considerations

The following upgrade considerations apply when moving from the most recent Axiom release of 2022.2 to the new release of 2022.3. If you are upgrading from an earlier version, please also see the release notes for the interim versions for any additional upgrade considerations.

Removal of support for in-memory document reference tables	
Description	The ability to store document reference tables as in-memory tables has been removed. This feature was primarily intended as a proof-of-concept, and we do not believe it was ever implemented at a client site. It is being removed now because the feature does not align with our current performance optimization efforts and roadmap. Additionally, use of document reference tables has been increasingly de-emphasized over time, to the extent that many clients do not use document reference tables at all. **IMPORTANT:** The in-memory feature was only available to on-premises installations. This upgrade consideration does not apply to cloud systems. In the extremely unlikely event that any on-premise client has this feature enabled, it must be disabled before upgrading to 2022.1 or later. The upgrade to 2022.x does not support upgrading memory optimized tables.
Notes for testing and review	We do not believe this feature was ever implemented at a client site. If you are an on-premise client and you believe this feature might be enabled, please contact Axiom Support for assistance.

Some filters will not migrate in web reports	
Description	Version 2022.1 introduces a new Filter Wizard for web reports. Due to the back-end changes necessary to support the new Filter Wizard, some existing filters in web reports will not migrate to the new structure.
Notes for testing and review	Please see the discussion in Upgrade considerations for web report filters for more details.

Removal of duplicative process columns in the Report Builder	
Description	When creating a web report that includes Process Management columns, it was previously necessary to include the step name and step number columns separately. Going forward, these columns have been combined into a single step column that can be used to display the step name and number in various formats. • In the **Process Status Columns** node, the previous columns **Current Step** and **Current Step Number** are combined into a single column **Current Step**. • In the **Process Step Columns** node, the previous columns **Step Name** and **Step Number** are combined into a single column **Process Step**. When using Current Step or Process Step, you can use the **Show description** and **Description display format** options in the Column Configuration panel to display just the step name, step number, or some combination of both. If you have existing reports that use the old columns, these reports will continue to work and the columns will return just the name or number as applicable.
Notes for testing and review	Nothing to test or review for this item.

Removal of unnecessary items from System Administration menu	
Description	As part of the Web Client navigation updates introduced in 2022.1, a couple of unnecessary items were removed from the System Administration menu: • **Home**: The Home menu item is not necessary as part of the System Administration menu, because it is available elsewhere. You can use the Area menu to navigate to your home page (custom systems) or to a product home page (systems with installed products). • **Forms Explorer**: The Forms Explorer has been superseded by the Intelligence Center. Although the Forms Explorer page has not been removed from the application, it is a deprecated feature and may be removed in a future release.
Notes for testing and review	Nothing to test or review for this item.

References to raw table and column names no longer work	
Description	Version 2022.1 changes the underlying table and column names in the database. If you have an import or an Execute SQL Command Scheduler task that references the raw table and column names from the database, these references will no longer work after upgrade to 2022.x. In previous versions, raw table and column names used a naming convention such as tb### or col###, where ### is the table or column ID number. The use of raw table and column names in SQL statements was and remains unsupported, however, the application did not prevent the execution of SQL statements that used these raw names. Therefore, in some cases, these raw names may be present in client systems. If your system uses supported syntax to reference tables and columns in SQL statements, then the database naming changes will not affect the operation of your system. When using supported syntax in previous versions, tables were referenced as `{tablename}`, and columns were referenced as the column name or as `{tablename.columnname}`. These references will continue to work after upgrade. Going forward, the supported syntax for tables has additional nuance that should be adopted when creating new SQL statements or editing existing SQL statements. This syntax works as follows: • `{Read:Tablename}`: This syntax should be used when reading data from the table, which should be true for the vast majority of references. • `{Write:Tablename}`: This syntax should be used when writing data to the table. • `{Table:Tablename}`: This syntax should be used to return the underlying table object name in statements such as TRUNCATE or when seeding an identity value. Existing `{tablename}` references will continue to work in SQL Server database environments.
Notes for testing and review	When your upgrade to 2022.1 or later is scheduled, the upgrade process will include a scan of your system to identify whether your system uses any of these unsupported table and column references. If any of these references are found, we will work with you to fix the references in the affected assets.

Upgrade considerations for web report filters

Version 2022.1 introduced a new Filter Wizard for web reports. Due to the back-end changes necessary to support the new Filter Wizard, some existing filters in web reports will not migrate to the new structure. If a filter cannot be migrated, the report will display an error about the problem filter. You can edit the report to delete the filter and then re-create it using the new Filter Wizard as applicable.

Additionally, some existing filters will migrate and continue to work, but due to syntax issues these filters cannot be edited in the new Filter Wizard going forward. In this case you can leave the filter as-is or delete the filter, but you cannot edit the filter or create a new version of the same filter going forward.

The following sections provide more information on these filter migration issues. If your organization has created web reports in version 2021.1, 2021.2 or 2021.3, please review these sections to determine if any of your reports may be affected.

Unsupported or invalid filter syntax

The previous Filter Wizard allowed input of any text string. This means that it was possible to create filters using invalid or unsupported syntax. Although in most cases an invalid filter would cause an error, in some cases it might have been silently ignored.

Filters using unsupported syntax may have had the intended effect in particular configurations, but are unsupported because they may not work in all configurations. For example, in the previous Filter Wizard it was possible to manually input a filter string that used math operators against multiple columns, and the report may have refreshed without error with this filter, but this is not supported filter syntax in Axiom.

If a filter statement is invalid or unsupported, the full statement will be carried over as-is to 2022.x. The report will return an error message about a filter that could not be migrated. In the new Filter Wizard, the filter statement will display as a non-editable block and will be flagged as invalid. To clear the error message, you can delete the filter and save the report.

KNOWN EXCEPTIONS:

- Filters that compare two columns using greater-than or less-than syntax are not officially supported, but will migrate as working filter statements if the rest of the filter uses valid and supported syntax. These filters will be applied to the report in the same way as previous versions. Once these filters are migrated, they cannot be edited, but they can be deleted. We may provide full support for this syntax in a future version, at which point the Filter Wizard will also be enhanced to allow creation of new column comparison filters.
- Filters that use greater-than, less-than, or BETWEEN syntax on string columns were not officially supported in previous versions, but are now supported and will migrate as working filter statements. These filters will be applied to the report in the same way as previous versions.

The new Filter Wizard does not allow creation of free-form filter statements. Therefore, these types of invalid or unsupported filter statements cannot be created going forward. Future versions of the Filter Wizard may provide official support for some of these currently unsupported filter statements.

Filters on calculations or groups that use columns from multiple tables

In previous versions, if a calculation or group used columns from multiple tables, the Filter Wizard did not consistently constrain the list of valid tables for the context. In some cases you could create filters that were not valid on all of the tables referenced by the calculation or group, or were not valid in the context of the primary table specified as the Data Context for the report. Although some of these invalid filters would cause an error, in other cases the invalid filter was silently ignored on the tables where it could not be applied.

Starting with 2022.1, the Filter Wizard correctly constrains the valid list of tables based on the tables referenced by the calculation or group, and based on what is allowed by the primary table specified as the Data Context for the report. Going forward, it should not be possible to create a filter that is invalid based on the current configuration of the report.

If your report contains a filter on a calculation or group that does not follow these rules, the migrated filter will cause an error in the report. You can resolve the error as follows:

- Review the filter to determine the desired effect of the filter, then delete it from the calculation or group.
- If you can achieve the same filter result by following the valid table rules in the new Filter Wizard, you can simply create a new filter on the calculation or group.
- If the old filter is not possible using the new rules, you should evaluate what you were attempting to achieve and determine whether there is a better way to achieve it. For example, if you had a group with columns from two different data tables, and the group had a filter defined on one of the data tables, this filter is not valid because it cannot be applied to the second data table. In this situation, you may need to define the filter directly on the column instead of on the group, or perhaps separate the columns into two different groups.

Column-only filters

In some cases, the previous Filter Wizard may have created filters that did not use fully qualified Table.Column syntax. It was also previously possible to manually input filters that did not use fully qualified syntax.

Going forward, all filters created in the new Filter Wizard use fully qualified syntax. Generally speaking, this means that all filters must begin on the affected table or on a dimension table of the affected tables.

Although column-only filters cannot be created in 2022.x, existing column-only filters will migrate and will work without error as long as the filter can be applied unambiguously to all affected tables. In the

vast majority of cases, this means that if you had a working column-only filter in a previous version, that filter will migrate and work in 2022.x. The primary reasons that a migrated column-only filter would not work are:

- If the filter was on a calculation or group with multiple tables, and the filter cannot be applied to all of the tables, then the filter is invalid and will cause an error. A different filtering approach may be needed to achieve the desired effect (as discussed in the previous section).
- If the report was created in 2021.1 and never upgraded, and had a column-only filter defined in the Grid Configuration settings, this will be migrated as a General filter. If the column cannot be applied to all tables referenced in the report, the filter will cause an error. In this case you should evaluate whether the filter was intended as a General filter or a Table-Specific filter, and attempt to re-create it using fully qualified syntax in the new Filter Wizard.

If the migrated column-only filter works, and you later need to edit this filter, keep in mind that the new Filter Wizard is unable to show specific values in the column due to the unqualified column reference. In this case you can delete the existing filter and re-create it using the new Filter Wizard, which will allow you to select specific values in the column.

Other filter migration notes

- If you have a dimension-level filter where the name of the validated column does not match the name of the lookup table, this filter will migrate and work. However, if you later need to edit this filter to select specific values in the column, the new Filter Wizard is unable to show these values due to the name mismatch. In this case you can delete the existing filter and re-create it using the new Filter Wizard, which will allow you to select specific values in the column.
- If you have an existing filter that references an empty string value, this filter will migrate and work. However, the new Filter Wizard does not currently have support for creating empty string filters such as `Request.Status<>''`. Future versions of the Filter Wizard may add this support.
- If you have an existing filter against null values, this filter will migrate and work. However, the new Filter Wizard does not currently have support for creating null value filters such as `Request.StartDate IS NULL`. Future versions of the Filter Wizard may add this support.

Upgrading an existing Axiom installation

This section explains the process of upgrading an existing Axiom installation to version 2022.3. Please contact Axiom Support to obtain a copy of the 2022.3 version of the Axiom Software Manager.

Upgrade requirements

- All customers upgrading from version 2020.3 or earlier must install a signed Axiom certificate on the Axiom Application Server in order to upgrade to 2022.3. See Installing the Axiom certificate for instructions. If you are already running 2020.4 or later, your existing certificate can be used for the upgrade.
- In order to upgrade to version 2022.3, your Axiom database must be at version 2020.4 or higher. Therefore if your system is 2020.3 or earlier, you must first use the Axiom Software Manager to upgrade your database to version 2020.4 or higher. After that, you can use the 2022.3 Software Manager to upgrade your system as normal.

Upgrading the Axiom database

▶ Upgrading the database to 2020.4 or higher

In order to upgrade to version 2022.3, your Axiom database must be at version 2020.4 or higher. If your database is version 2020.3 or lower, then you must obtain a copy of any Axiom Software Manager that is 2020.4 or higher, and upgrade your database before proceeding with the 2022.3. Please contact Axiom Support as needed to obtain a copy of the necessary Axiom Software Manager.

If your system is already running 2020.4 or higher, then you can skip this step and upgrade directly to 2022.3. The following instructions assume that you are upgrading your database to 2021.3, however, you can upgrade your database to any version from 2020.4 to 2021.3.

1. Extract the contents of the version 2021.3 installation package to the Axiom Application Server, and run `AxiomSoftwareManager.exe`.
2. In the 2021.3 Software Manager, click the **Upgrade** icon on the home screen.
3. Verify and complete the following properties on this screen:
    - Confirm that the **Database Type** and **Server Name** are correctly configured and pointing to the server where your Axiom application database is stored.
    - From the **Database Name** list, select the name of the application database to upgrade. If the server only has one Axiom application database, then that database will be selected by default.
4. Click **Upgrade**.

Once you have upgraded the database to version 2021.3 (or any version that is 2020.4 or higher), you can move on to the 2022.3 Software Manager. It is not necessary to upgrade the server or client components before proceeding with the 2022.3 installation.

Upgrading the database to 2022.3

Before upgrading the Axiom server software, you must upgrade the database.

1. Extract the contents of the version 2022.3 installation package to the Axiom Application Server, and run `AxiomSoftwareManager.exe`.
2. In the Software Manager, click the **Upgrade** icon on the home screen.
3. Verify and complete the following properties on this screen:
    - Confirm that the **Database Type** and **Server Name** are correctly configured and pointing to the server where your Axiom application database is stored.
    - From the **Database Name** list, select the name of the application database to upgrade. If the server only has one Axiom application database, then that database will be selected by default.
4. Click **Upgrade**.

When the upgrade is complete, a confirmation message displays.

Upgrading Axiom server components

Once the database has been upgraded, you can use the Software Manager to upgrade Axiom server components to version 2022.3.

NOTE: When installing a patch update, it is typically not necessary to upgrade the Axiom Update Service (unless it is specifically called out as a requirement for the patch).

1. Upgrade the Axiom Update Service (if applicable):
    - Run `AxiomSoftwareManager.exe` as an administrator on the Axiom Application Server.
    - On the home page of the Software Manager, click **Manage Software**.
    - In the **Currently Installed Packages** section, locate the entry for the Update Service, and then click **Upgrade**.
    - On the Axiom Update Service Installer screen, click **Upgrade**.
2. Upgrade the Axiom Application Server:
    - Run `AxiomSoftwareManager.exe` as an administrator on the Axiom Application Server.
    - On the home page of the Software Manager, click **Manage Software**.
    - In the **Currently Installed Packages** section, locate the entry for the Application Server, and then click **Upgrade**.
    - On the Axiom Application Server Installer screen, click **Upgrade**.
3. Upgrade the Axiom Scheduler Service (on each server where Scheduler is installed):
    - Run `AxiomSoftwareManager.exe` as an administrator on the Axiom Scheduler Server.
    - On the home page of the Software Manager (Installation Manager), locate the entry for

the Scheduler Service, and then click **Upgrade**.

- On the Axiom Scheduler Service Installer screen, click **Upgrade**.

Before proceeding with client installations and post-upgrade setup, verify that you can access the Axiom Web Client. If you are not able to load this web page, contact Axiom Support for assistance.

Upgrading individual client workstations

Individual client workstations will be upgraded automatically the next time the Axiom client is launched on that workstation. No special setup is required.

For more information on deployment using the ClickOnce installer, see Installing the Axiom Client on client workstations.

Upgrading Axiom add-ins for PowerPoint and Word

The Axiom add-ins for Word and PowerPoint will be upgraded automatically when the Axiom client is upgraded.

System Configuration Settings

The Axiom database stores several system configuration settings that can be edited if needed. For more information on how to change these settings, see Editing system configuration settings.

The following system configuration settings are available:

ADONetBatchSize

Default True	100
Description	Specifies the batch size for update statements. This should only be changed on the advice of Axiom Support.

AllowAmbiguousAlternateAggregationAndColumnFilterFieldDefinitions

Default value	False
Description	This configuration setting is no longer relevant, since the limitations affecting use of certain alternate aggregations with column filters have been removed.

AllowBlanksToBeDataRowSeparators InAQDataUpdate

Default value	True
Description	Specifies whether blank rows cause duplicate records in an Axiom query data range to be treated as contiguous or not (True/False). This is for purposes of determining update behavior for duplicate records. By default, blank rows are treated as data separators and each duplicate row will be updated. If disabled, then blank rows are ignored and the duplicate records are treated as contiguous, which means only the first row in the contiguous block will be updated.

AllowShowExcel

Default value	True
Description	Specifies whether the icon to install / launch the Axiom Excel Client shows in the Axiom Web Client (True/False). By default the icon is available if the user has the necessary security permission to launch the Excel Client. If disabled, the icon will be hidden, regardless of the user's permission. This setting can be modified using the System Configuration page in the Web Client. **NOTE:** This is a legacy setting that should no longer be needed for any system. Access to the Excel Client is now controlled by security, and the icon will show and hide automatically depending on each user's security permissions.

AllowShowPowerPoint

Default value	True
Description	Specifies whether the icon to install / launch the PowerPoint Add-In shows in the Axiom Web Client (True/False). By default the icon is available if the user has the necessary security permission to launch the add-in. If disabled, the icon will be hidden, regardless of the user's permission. This setting can be modified using the System Configuration page in the Web Client. **NOTE:** This is a legacy setting that should no longer be needed for any system. Access to the PowerPoint add-in is now controlled by security, and the icon will show and hide automatically depending on each user's security permissions.

AllowShowWord

Default value	True
Description	Specifies whether the icon to install / launch the Word Add-In shows in the Axiom Web Client (True/False). By default the icon is available if the user has the necessary security permission to launch the add-in. If disabled, the icon will be hidden, regardless of the user's permission. This setting can be modified using the System Configuration page in the Web Client. **NOTE:** This is a legacy setting that should no longer be needed for any system. Access to the Word add-in is now controlled by security, and the icon will show and hide automatically depending on each user's security permissions.

AuthenticationDomainSelectionListRequired

Default value	False
Description	Specifies whether the authentication domain selection list always displays on the login screen (True/False). By default, the selection list only displays when it is necessary (meaning only when there are duplicate user names defined in Axiom that use different domains). If you want the domain selection list to always show, then set this to True.

AutoCastFloatColumnsDuringAggregation

Default value	False
Description	Specifies treatment of numeric columns when data is aggregated by a query to the database. This should only be changed on the advice of Axiom Support.

AutoUpdateProcessTaskPane

Default value	True
Description	Specifies whether the Process task pane automatically refreshes in response to process updates that affect the user (True/False). By default the task pane automatically refreshes. If disabled, then the Process task pane does not automatically refresh. Instead, a message displays at the top of the task pane to inform the user that the process has updates and the user should refresh the task pane to see them. The user can click the message to refresh. This setting should only be changed to False if system performance is being affected by the automatic process updates, which should be rare.

AxiomSignalRServerAddress

Default value	<Blank>
Description	The URI of the server used to control IPC traffic for Axiom. By default, when no value is specified here, the Axiom Application Server for the installation is used. This option is initially configured during the Axiom Application Server installation, and can be subsequently changed using the system configuration settings or by repairing the installation.

BatchedAQsEnabled

Default value	True
Description	Specifies whether Axiom queries assigned to a batch are run using batch processing (True/False). By default, this is enabled so that queries run in their configured batches. If disabled, then batch processing is not performed and all queries are run in their normal sequential order, whether or not they are assigned to a batch. This setting is meant to be used as a stopgap in case batched Axiom queries are not configured correctly, so that the file(s) can be used while the configuration is evaluated and corrected.

BI_FiscalyearStartMonth

Default value	1
Description	The starting month of the fiscal year for purposes of fiscal year measures in visualization reports. This setting only applies in systems with an Axiom Business Intelligence license. This setting does not affect the fiscal year date parts used in Axiom queries and web reports; see ClientFiscalYearEndMonth instead.

ClickOnceClientNameExcel

Default value	Axiom Excel Client
Description	The name of the shortcut for the Excel Client when using ClickOnce installations. This option is initially configured during the Axiom Application Server installation, and can be subsequently changed using the system configuration settings or by repairing the installation.

ClickOnceClientNameWindows

Default value	Axiom Windows Client
Description	The name of the shortcut for the Windows Client when using ClickOnce installations. This option is initially configured during the Axiom Application Server installation, and can be subsequently changed using the system configuration settings or by repairing the installation.

ClickOnceShortcutLocation

Default value	DesktopAndStartMenu
Description	The location where Axiom shortcuts will be placed when using ClickOnce installations. This option is initially configured during the Axiom Application Server installation, and can be subsequently changed using the system configuration settings or by repairing the installation. Available options are: **DesktopAndStartMenu**, **DesktopOnly**, **StartMenuOnly**.

ClickOnceShortcutType

Default value	CurrentClient
Description	Specifies whether shortcuts are created when using ClickOnce installations, and if so what type. This option is initially configured during the Axiom Application Server installation, and can be subsequently changed using the system configuration settings or by repairing the installation. Available options are: **None**, **Generic**, **CurrentClient**, **Both**. See the *Installation Guide* for more information on what these options mean.

ClientFiscalYearEndMonth

Default value	12
Description	The number of the month representing the client's fiscal year end. This value is used in web reports and Axiom queries to calculate the date parts relating to the fiscal year.

CreateKeyIndexesOnTemporaryTables

Default value	True
Description	Specifies whether indexes are created for key columns of temporary tables (True/False). This should only be disabled on the advice of Axiom Support.

CreateNonKeyIndexesOnTemporaryTables

Default value	True
Description	Specifies whether indexes are created for non-key columns of the import temp table. This should only be disabled on the advice of Axiom Support.

CriticalErrorRegularExpression

Default value	Object reference not set
Description	Defines error text to match on for purposes of flagging critical errors in server logs. By default, any error messages containing this text are considered critical. This should only be changed on the advice of Axiom Support.

DefaultColumnValue_Boolean

Default value	0 (meaning False)
Description	Defines the default value for Boolean columns. You can change this to 1 for True, or blank for null. It is not recommended to use null as the default for Boolean columns unless you have a particular use case that requires it. If changed, the new value only applies to new columns created going forward. Existing columns will continue to use the default value that was set when they were created.

DefaultColumnValue_Date

Default value	<Blank> (meaning null)
Description	Defines the default value for Date columns. You can change this to any valid default value for Date columns. If changed, the new value only applies to new columns created going forward. Existing columns will continue to use the default value that was set when they were created.

DefaultColumnValue_DateTime

Default value	<Blank> (meaning null)
Description	Defines the default value for DateTime columns. You can change this to any valid default value for DateTime columns. If changed, the new value only applies to new columns created going forward. Existing columns will continue to use the default value that was set when they were created.

DefaultColumnValue_Number

Default value	0
Description	Defines the default value for Integer columns (all types) and Numeric columns. You can change this to any valid default value, including blank for null. It is not recommended to use null as the default for number-based columns unless you have a particular use case that requires it. If changed, the new value only applies to new columns created going forward. Existing columns will continue to use the default value that was set when they were created.

DefaultColumnValue_String

Default value	''
Description	Defines the default value for String columns. You can change this to any valid string value. If a value is specified, it must be enclosed in single quote marks. **NOTE:** Although it is possible to set the String column default to blank for null, Axiom does not differentiate between null values and empty string values in String columns within the spreadsheet environment. Therefore it is strongly recommended to leave the default of empty string if you do not want to use a specific string. If changed, the new value only applies to new columns created going forward. Existing columns will continue to use the default value that was set when they were created.

DefaultDBMSTarget

Default value	SQLServer
Description	Specifies the default database target for the system. Relates to a pre-release feature that is not yet generally available.

DefaultEmailClientName

Default value	Outlook
Description	Specifies a custom name for the default email client, as displayed when using the **Email Workbook** feature. If desired, you can change this name to a different email client used by your organization, or you can clear out the setting and leave it blank. If blank, then the text "Default E-Mail Client" will display in the dialog for this option.

DefaultFilterType

Default value	Includes
Description	Specifies the default comparison method for filtering "simple view" pick lists, such as when using Choose Data Element. Available options are: **BeginsWith** or **Includes**.

DefaultGetDataNoValueErrorMessage

Default value	<Blank>
Description	Specifies the return value when the parameters of a GetData function use valid syntax but the function does not return any data. You can change this to any text that you want to display in this situation. This return value can be overridden within each individual GetData function.

DefaultGetDataSQLErrorMessage

Default value	#ERR
Description	Specifies the return value when the parameters of a GetData function use invalid syntax, resulting in a SQL error. You can change this to any text that you want to display in this situation. This return value can be overridden within each individual GetData function.

DefaultOracleFetchSizeKB

Default value	1024
Description	Specifies the fetch size, in kilobytes, when importing data from an Oracle database. The fetch size determines the number of rows returned from Oracle in each batch of data. If this value is changed, IIS should be reset on the Axiom Application Server server to ensure that the cached value is not used.

DisableHashBytesCheck

Default value	False
Description	Specifies whether the hashbytes check is disabled. This should only be changed on the advice of Axiom Support.

DisableSMTPClientSSL

Default value	False
Description	Specifies whether encryption is disabled when emails are relayed from Axiom to the configured SMTP email server for delivery (True/False). This should only be disabled on the advice of Axiom Support, in order to temporarily bypass email issues caused by an incorrectly configured on-premise SMTP email server.

EllucianEnabled

Default value	False
Description	Specifies whether Ellucian is available as an import source in the Import Wizard. If enabled, you can create imports that read data directly from a specified Ellucian Banner system, using an Ellucian Ethos key. By default, this is disabled. The intent is that the setting is enabled as needed when a higher education client wants to import data from Ellucian. This setting is not returned when querying Axiom.SystemConfiguration. The Axiom Software Manager can be used to view and edit the setting.

EmailDistributionAllowedDomainList

Default value	<Blank>
Description	Defines a list of allowed email domains for Axiom. If a list is defined, then emails can only be sent from Axiom if the recipients are in the allowed domains. If any recipients are not in the allowed domains, then the email is flagged as blocked and is not sent by the System.SMTPMessageDelivery Scheduler job. By default, the list is blank, which means all email domains are allowed.

EnableFreeThreadingInUserFunctions

Default value	True
Description	Specifies locking behavior for Axiom functions. This should only be disabled on the advice of Axiom Support.

EnableLegacyAQMode

Default value	False
Description	Specifies whether to use the legacy method for creating database queries for Axiom queries (True/False). This is for backward-compatibility only and should never be manually enabled. If enabled, then the database queries for Axiom queries are created using the rules in place prior to version 5.1. When you upgrade from a pre-5.1 system to the current version, your system will be automatically set to this mode if the upgrade script detects that your system has the potential for a certain type of query ambiguity (where a specified lookup column potentially exists on more than one lookup table). In order to disable legacy mode, you must modify any affected files to use fully qualified syntax to specify the intended lookup table. Please contact Axiom Support for more information.

EnableODataAPI

Default value	False
Description	Specifies whether the OData API is enabled for use (True/False). If False, the OData API is not available and the associated URIs will return 404 errors. If True, the OData API is enabled and available for use as normal.

EnablePasswordPolicy

Default value	True
Description	Specifies whether password rules are enforced (True/False). By default, passwords must meet the rules defined in the PasswordRegularExpression setting. If disabled, then any password is valid. **NOTE:** If enabled, password rules are only enforced when defining new passwords. If the system contains existing passwords that do not meet the rules when this setting is enabled, these existing passwords will continue to be valid.

ETLAccessibleFolders

Default value	<Blank>
Description	Specifies whether the Axiom Application Server is limited to accessing a specific folder or folders in your organization's network, when performing import operations. You can leave this blank to allow the application server to access any folder (as permitted by your network file system permissions), or you can list one or more specific folder paths. Separate multiple folder paths with semi-colons. If you list specific folders, you must use the same file path format when configuring features that will access the folders. For example, if the file processing configuration specifies the file as `\\Server\Folder\filename.xls`, then you must specify `\\Server\Folder` in this setting. This setting is not returned when querying Axiom.SystemConfiguration. The Axiom Software Manager can be used to view and edit the setting. **NOTE:** This setting only applies to on-premise installations. The Axiom Cloud Integration Service used by Axiom Cloud systems has a similar setting that can be configured during installation of the service.

ETLMaxRows

Default value	500
Description	Defines the maximum number of temp table rows that will be displayed to the user when running an import using the Allow Pauses option. This setting should only be changed on the recommendation of Axiom Support. The value cannot be higher than 5,000.

ExcelAddinStartupTimeout

Default value	00:01:00 (meaning one minute)
Description	Defines the timeout value when starting up the Excel Client and the Windows Client. If the client does not start within this length of time, the startup routine is canceled and an error message displays to the user. This should only be changed on the advice of Axiom Support.

ExcelWorksheetPasswordProtectionEnabled

Default value	True
Description	Specifies whether or not worksheet protection is applied with a password (True/False). By default, when a sheet is designated as protected via the Control Sheet, the protection requires a password to remove it manually (Axiom-controlled features can be used to remove the protection without entering a password). If disabled, then the sheet is still protected but the protection can be removed manually without a password.

ExtendedDBCommandTimeout

Default value	216000
Description	Defines the timeout value, in seconds, before terminating an attempt to execute a SQL command. This should only be changed on the advice of Axiom Support.

FileProcessingSaveDataDefaultBatchSize

Default value	7000
Description	Defines the number of records to process at a time when performing a save-to-database using file processing. This setting should only be changed on the advice of Axiom Support.

FileWatcherEnabled

Default value	False
Description	Specifies whether File Watcher features are available in the Scheduler dialog. This should only be set to True for backward-compatibility purposes, for clients who are actively using the feature and have not yet had a chance to implement a different solution. The feature is deprecated for new installations.

GetCachedDataEnabled

Default value	False
Description	Specifies whether a pre-release feature is enabled in the system for testing purposes. This setting should only be changed on the advice of Axiom Support.

ImportErrorsDocumentRetentionDays

Default value	15
Description	Specifies the number of days that import error files are retained before being automatically deleted.

ImportSaveBatchSize

Default value	25000000
Description	Defines the number of rows to save in each batch when importing data. This setting applies when inserting or updating rows in the destination table. This setting should only be changed on the advice of Axiom Support.

IncludeNonKeysColumnsOnTemporaryTable Index

Default value	True
Description	Specifies whether non-key columns are included in the non-clustered index on temporary tables. This setting should only be changed on the advice of Axiom Support.

IntacctPageSize

Default value	500
Description	This feature has been deprecated. Defines the number of records to be processed per batch when importing data from Intacct. The value can be set from 100 to 1000. This setting should only be changed on the advice of Axiom Support.

InvalidPasswordErrorMessage

Default value	<Blank>
Description	Defines the message to display when creating a new password if that password does not meet the rules. This should be left blank to use the default message which details the default password rules. If the rules have been customized with the assistance of Axiom Support, then you can define a custom message that details these rules.

IsPackageIntegrationServer

Default value	False
Description	This setting relates to an internal Axiom tool and is not for client use.

LDAPAllowedSuffixes

Default value	<Blank>
Description	Defines the allowed suffixes for LDAP Authentication, used if LDAP Authentication is enabled. This option is initially configured during the Axiom Application Server installation, and can be subsequently changed using the system configuration settings or by repairing the installation.

LDAPAuthEnabled

Default value	False
Description	Specifies whether LDAP Authentication is enabled for the system (True/False). If enabled, then the LDAPConnectionString must be specified. This option is initially configured during the Axiom Application Server installation, and can be subsequently changed using the system configuration settings or by repairing the installation.

LDAPConnectionString

Default value	<Blank>
Description	Defines the connection string to the LDAP server, used if LDAP Authentication is enabled. This option is initially configured during the Axiom Application Server installation, and can be subsequently changed using the system configuration settings or by repairing the installation.

LimitOpenPlanFilesDialogToSingleSelection

Default value	True
Description	Specifies whether the Open Plan Files dialog is limited to opening a single plan file at a time (True/False). The intent of this setting is to prevent end users from accidentally or intentionally opening many plan files at once, which may take a long time to open and tie up the application in the meantime. If your system has smaller plan files and you want to allow end users to open multiple plan files at once, you can change this setting to False.

MapF9ToAxiom

Default value	True
Description	Specifies whether F9 performs an Axiom refresh in addition to calculating the workbook. By default, F9 will refresh all sheets in the workbook, and Shift+F9 will refresh the current sheet. If disabled, then the native F9 behavior of the Microsoft Excel version or the Windows Client applies.

MaxAQRows

Default value	10000
Description	Defines the maximum number of rows to return for an Axiom query. This setting is intended to prevent users from accidentally bringing in an extremely large number of rows, potentially resulting in excessive processing times or system errors. If the number of rows in the query exceeds the MaxAQRows setting, the user is warned of this and asked if they want to continue. **NOTES:** • The only user options are to cancel the query or continue with the full number of rows. This setting defines the threshold for the warning, it does not limit the query to the specified number of rows. • The warning only applies when users manually refresh Axiom queries. If the query is processed by Scheduler, then processing will fail if the query exceeds the threshold. This setting can be overridden on a per query basis, on the Control Sheet.

MaxChooseValueRows

Default value	1000
Description	Defines the maximum number of rows that can be displayed in the Choose Value dialog. This dialog is used by several features to present a list of values for user selection, such as the GetDataElement function and refresh variables. The limit only applies when the dialog is showing the "full grid view"—meaning, the dialog shows more columns than just the key column and description.

MaxConsecutiveCutnPasteWithoutWaiting

Default value	50
Description	Defines how many consecutive cut and paste actions can occur before the system stops and pauses for a second. This setting has to do with system-controlled cut and paste actions such as when creating snapshot copies. Too many consecutive actions may cause certain environments to experience memory quota errors. This setting should only be changed on the advice of Axiom Support.

MaxDegreeOfParallelism_Application

Default value	0
Description	Relates to processing for the application server. This setting should only be changed on the advice of Axiom Support.

MaxDegreeOfParallelism_Scheduler

Default value	0
Description	Relates to processing for the Scheduler server. This setting should only be changed on the advice of Axiom Support.

MaxExcelCellsToProcessInAQBatch

Default value	10000
Description	Defines the maximum number of cells to process at a time when refreshing a vertical Axiom query. This setting should only be changed on the advice of Axiom Support.

MaxExcelCellsToProcessInSingleArray

Default value	100000
Description	Defines the number of cells in a workbook that are processed at a time when saving to the database. This setting should only be changed on the advice of Axiom Support.

MaxFileAttachmentSizeKB

Default value	10000
Description	Defines the maximum size for a single file attachment. This limit is enforced when users upload attachments for plan files. When uploading multiple attachments at a time in the Web Client, the total size of all attachments must be less than 50MB. This can be configured separately if needed by using the maxRequestLength property in the web.config file for the Axiom Application Server.

MaxHierarchyRowSize

Default value	50000
Description	Defines the maximum row size for a hierarchy. If a hierarchy is created for a table with greater than 50,000 rows, then the hierarchy name will display in the Filter Wizard and Quick Filter, but when expanded a message will display to the user explaining that the hierarchy has too many rows and therefore the individual elements cannot be displayed. If needed you can change this setting to a larger row size, however, large numbers of rows in a hierarchy may cause out-of-memory errors on the client.

MaximumErrorsToReturnFromSaveOperations

Default value	10000
Description	Defines the maximum number of errors to return when a save-to-database operation occurs. This setting should only be changed on the advice of Axiom Support.

MaximumRowsAllowedThroughCopyTableData

Default value	250000
Description	Defines the maximum number of rows that can be copied when using the Copy Table Data feature. Copying tables with larger numbers of rows may cause performance issues. This setting should only be changed on the advice of Axiom Support.

MaxLoginAttempts

Default value	0 (meaning unlimited)
Description	Defines the maximum number of login attempts before a user is locked out. By default, users have unlimited login attempts. You can change this to a set number of login attempts to comply with your organization's security policies.

MaxRecursionCount

Default value	10
Description	Defines the maximum number of recursive calculations for GetData functions. This setting should only be changed on the advice of Axiom Support.

MaxSaveDataRowsInClientMemory

Default value	34000
Description	Defines the maximum number of save data rows that are stored in memory on the client. If the maximum is reached, the data rows are sent to the server and cleared from the client, and then the save process continues. The intent of this setting is to prevent out of memory errors on the client when saving very large sets of data. This setting should only be changed on the advice of Axiom Support.

MaxSaveDataToOutputSheetRowsInClient Memory

Default value	250000
Description	Defines the maximum number of save data rows that are stored in memory on the client, for purposes of placing them on an output sheet in the file. This setting only applies when using multipass file processing with the **Save to Output Sheet** option. If Axiom determines that the total number of rows for the process will exceed this limit, a message is presented to the user and the process is stopped. This setting should only be changed on the advice of Axiom Support.

MaxSystemCurrentPeriod

Default value	12
Description	Defines the maximum number that the system current period can be set to. Individual tables can be set to higher current periods if necessary. For example, most tables may use 12 periods, but you may have a table with payroll data that uses 26 periods.

MaxTableColumnNameLength

Default value	0 (meaning use system default)
Description	Defines the maximum length of table and column names. The system default is 50 characters. You can specify a different maximum size if needed. However, these names will be used in Axiom queries and Axiom functions to query data, so they should be descriptive and short.

MaxTableRowsToOpenInSpreadsheet

Default value	50000
Description	Defines the maximum number of records to be returned within Open Table in Spreadsheet. This can be set to a larger number if desired, however, returning larger amounts may result in significant performance issues.

MsSqlOptimizerRowGoalEnabled

Default value	False
Description	Specifies whether RowGoal optimization is enabled for purposes of obtaining a count of records in the Filter Wizard. This setting should only be changed on the advice of Axiom Support.

NumberOfPrincipalFiltersToValidateForBulkSave

Default value	5
Description	Specifies the number of filters that are validated when saving user permissions in bulk via Open Security in Spreadsheet. This setting should only be changed on the advice of Axiom Support.

ODataPageSize

Default value	100000
Description	Defines the number of records per page when querying data using the OData API. If data is paged, OData results include nextpage links to read all of the returned data.

OpenIDAuthenticationEnabled

Default value	<Blank>
Description	Specifies whether OpenID Authentication is enabled for the system (True/False). This option is initially configured during the Axiom Application Server installation, and can be subsequently changed by repairing the installation.

PackageIntegrationServerURL

Default value	<Blank>
Description	This setting relates to an internal Axiom tool and is not for client use.

PackageManagerAutoIntegrationNotificationsEmailList

Default value	<Blank>
Description	This setting relates to an internal Axiom tool and is not for client use.

PackageManagerDefaultValuesThreshold

Default value	0
Description	This setting relates to an internal Axiom tool and is not for client use.

ParallelSaveEnabled

Default value	TRUE
Description	Specifies whether parallel processing of save-to-database blocks is enabled (True/False). It is recommended to leave this enabled for improved performance. If you identify a particular file configuration that does not operate as expected with parallel saves enabled, you can disable the behavior on a per file basis by setting **Enable Parallel Save Data** to **Off**.

PasswordRegularExpression

Default value	<Custom string used to define default rules>
Description	Defines the password rules to be enforced if **EnablePasswordPolicy** is set to **True**. The built-in rules are as follows: • Must be at least 8 characters long • Must contain at least 1 upper-case letter and at least 1 lower-case letter • Must contain at least 1 non-alphabetic character (a number or a symbol) Axiom does not provide functionality for clients to change these rules. If you need to enforce password rules and use different rules, please contact Axiom Support for assistance.

PlatformUpdateURL

Default value	<URL to software support portal>
Description	This setting has been deprecated. Defines the URL to check for platform updates. This value should not be manually changed except as directed by Axiom Support.

ProductUpdateURL

Default value	<Blank>
Description	This setting has been deprecated. Defines the URL to check for product updates. This value should not be manually changed except as directed by Axiom Support.

ReleaseJobLocksOnMIAScheduler

Default value	False
Description	Specifies whether Axiom can break a Scheduler Server's lock on a job if that server reports as MIA (True/False). This should only be changed on the advice of Axiom Support.

RemoteDataConnectionBatchSize

Default value	10000
Description	Defines the number of rows to be sent in each batch between the Axiom Application Server and the Axiom Cloud Integration Service. This setting should only be changed on the advice of Axiom Support.

RestrictSaveAsLocalForManagedDocs

Default value	False
Description	Specifies whether **Save As (Local)** is available for managed documents (True/False). By default, Save As (Local) is available for eligible documents. If you want to remove this option for Axiom managed documents, change this setting to True. When a managed document is active, the Save As (Local) option will no longer appear on the **Save** menu of the Axiom ribbon, or when right-clicking the file tab in the navigation pane. Administrators can still save a file locally by using the **Export** option in Axiom Explorer.

SAMLAuthenticationEnabled

Default value	False
Description	Specifies whether SAML Authentication is enabled for the system (True/False). If enabled, then the SAMLUserNameHeader must be specified. This option is initially configured during the Axiom Application Server installation, and can be subsequently changed by repairing the installation.

SAMLUsernameHeader

Default value	HTTP_EPPN
Description	Specifies the user name header for SAML when SAML Authentication is enabled. This option is initially configured during the Axiom Application Server installation, and can be subsequently changed using the system configuration settings or by repairing the installation.

SAMLUsernameSuffixPreserved

Default value	False
Description	Specifies whether user names defined in Axiom include an @suffix for the SAML identity provider (True/False). By default, it is assumed that Axiom user names do not include a suffix. Set this to True if Axiom user names include a suffix. This option is initially configured during the Axiom Application Server installation, and can be subsequently changed using the system configuration settings or by repairing the installation.

SaveRetryCountOnDeadlock

Default value	3
Description	Specifies how many times the system will attempt to save data to the database after encountering a deadlock error. This setting should only be changed on the advice of Axiom Support.

Scheduler_AutomationEngine

Default value	WebAlways
Description	Because it is no longer supported to run Microsoft Excel on the Scheduler server for spreadsheet processing tasks, this setting should always be set to WebAlways. This means that spreadsheet processing tasks will be performed using the same spreadsheet emulation engine as the Windows Client.

Scheduler_ContainerIdleLinger

Default value	120
Description	How long (in seconds) a Scheduler container waits in an idle state for more jobs before it shuts down. This value only applies to Axiom Cloud systems and is configured by Axiom Support.

Scheduler_ContainerLoggingLevel

Default value	Warning
Description	The logging level for Scheduler containers. This value only applies to Axiom Cloud systems and is configured by Axiom Support.

Scheduler_ContainerPollRate

Default value	60
Description	The rate (in seconds) at which Scheduler polls the job queue. This value only applies to Axiom Cloud systems and is configured by Axiom Support.

Scheduler_ContainerProcessorWorkerThreads

Default value	2
Description	The number of worker threads per Scheduler container. This value only applies to Axiom Cloud systems and is configured by Axiom Support.

Scheduler_FailedContainerRetentionCount

Default value	0
Description	The number of failed Scheduler containers to retain within the Scheduler container. This value only applies to Axiom Cloud systems and is configured by Axiom Support.

Scheduler_FromEmailAddress

Default value	noreply@axiomepm.com
Description	Defines the "From" email address to use for any email notifications that do not have a separate specified "From" email address (for example, process management email notifications). This email address must be specified in order to enable these email notifications. If no email address is specified, the SMTP Email Delivery task will experience an error when attempting to deliver the notifications. **NOTE:** For installations that are using subsystems, the system variable `{Scheduler.FromEmailAddress}` may resolve to a subsystem administrator email address instead of the Scheduler "from" email address.

Scheduler_MaxContainerInstances

Default value	0
Description	The number of Scheduler containers that can run concurrently. This value only applies to Axiom Cloud systems and is configured by Axiom Support.

Scheduler_ServiceAgentPool

Default value	<Blank>
Description	The name of the service cluster for Scheduler processing. This value only applies to Axiom Cloud systems and is configured by Axiom Support.

SchedulingBehaviorTimezone

Default value	<Blank>
Description	The time zone used when determining the next execution of a scheduled job. By default, if this setting is left blank, the local time zone of the Scheduler server is used. This setting is primarily for use in Axiom Cloud systems and will be configured by Axiom Support. For on-premise installations, you may want to set the SchedulingBehaviorTimezone if your Scheduler Server and your client workstations are not on the same time zone. For example, if client workstations are on Pacific Standard Time but the Scheduler Server is on UTC, then job execution times will be scheduled using UTC. In this case you can set the SchedulingBehaviorTimezone to Pacific Standard Time, so that job execution times are set using the same time zone as client workstations.

SessionTimeout_DesktopClient

Default value	0
Description	The number of minutes of inactivity before a Desktop Client session expires. If set to 0, then sessions do not time out.

SessionTimeout_WebClient

Default value	0
Description	The number of minutes of inactivity before a Web Client session expires. If set to 0, then sessions do not time out.

SessionTimeoutWarning_DesktopClient

Default value	3
Description	The warning period, in minutes, before the Desktop Client session expires. If defined, then a warning message will be shown to the user to let them know that the session is about to expire. If set to 0, then no warning message displays. This setting only applies if the SessionTimeout_DesktopClient is set to a value greater than 0.

SessionTimeoutWarning_WebClient

Default value	3
Description	The warning period, in minutes, before the Web Client session expires. If defined, then a warning message will be shown to the user to let them know that the session is about to expire. If set to 0, then no warning message displays. This setting only applies if the SessionTimeout_WebClient is set to a value greater than 0.

ShowCopyPlanFilesActionInProcess

Default value	False
Description	Specifies whether the Copy Plan Files action is an available option in plan file processes (True/False). This action can be used to automatically copy plan files to a target file group when a step is completed in the process. This feature is hidden by default because most installations do not need to use it. If your installation needs to use this feature, you can expose it by changing the setting to True.

ShowRememberMe

Default value	True
Description	Specifies whether the Remember Me option is present on login screens (True/False). By default, this option is available. If disabled, then Remember Me will be hidden on login screens, meaning that users must enter their credentials each time they launch Axiom. If you disable this option after users have already used Remember Me, their current settings will not be cleared. Each user's credentials will continue to be remembered until they clear the credentials by logging out. Credentials are stored separately for the Web Client versus the Desktop Client, so if a user has saved credentials for both environments then they must log out of both. For the Desktop Client, the only way to log out is to use the Word or PowerPoint add-in, because the Excel and Windows Clients do not have a log out feature. This setting can be modified using the System Configuration page in the Web Client.

ShowWarningIfMissingAQTags

Default value	True
Description	Specifies whether missing `[aq#]` tags for active Axiom queries trigger a warning on refresh (True/False). The False setting is intended for backward-compatibility only. If warnings are being triggered in many existing files, you can disable this setting until you are able to correct the Axiom query configuration within the affected files. If the [aq#] tag was deliberately hidden using a formula as a means of dynamically disabling a query, the file should be updated to instead use the Active setting for the query. Please contact Axiom Support for assistance as needed.

ShowWarningOnGetDataProcessingFailure

Default value	True
Description	Specifies whether the circular reference warning displays when Axiom detects a failure in processing GetData functions. If disabled, then no warning message displays. This setting should only be changed on the advice of Axiom Support.

SignalRClientInvalidationLagTime

Default value	1000
Description	Specifies the lag time, in milliseconds, before performing a SignalR cache invalidation. This setting should only be changed on the advice of Axiom Support.

SqlCountQueryExpression

Default value	*
Description	Specifies the query expression for row counts in areas such as the Filter Wizard. This should only be changed on the advice of Axiom Support. This setting is not returned when querying Axiom.SystemConfiguration. The Axiom Software Manager can be used to view and edit the setting.

SqlGeneratorTempTableStrategy

Default value	On
Description	Specifies whether temp tables are used for SQL queries (On/Off/Auto). This should only be changed on the advice of Axiom Support. This setting is not returned when querying Axiom.SystemConfiguration. The Axiom Software Manager can be used to view and edit the setting.

SqlGenerator539RetryCount

Default value	2
Description	Specifies how many times a particular query will be retried after encountering a schema change. The number of retries is capped at 10. This setting is not returned when querying Axiom.SystemConfiguration. The Axiom Software Manager can be used to view and edit the setting.

SqlGeneratorUseInnerSelect

Default value	True
Description	Specifies whether to use inner selects for certain SQL query configurations (True/False). This should only be changed on the advice of Axiom Support. This setting is not returned when querying Axiom.SystemConfiguration. The Axiom Software Manager can be used to view and edit the setting.

SqlParserMaxRecursionDepth

Default value	1000
Description	Specifies the recursion depth when parsing SQL for data queries. This setting should only be changed on the advice of Axiom Support.

SubsystemsEnabled

Default value	False
Description	Specifies whether the security subsystem feature is enabled (True/False). By default, security subsystem features do not appear in the user interface, and subsystems cannot be created. If enabled, then the security subsystem features become available in the user interface. **NOTE:** If you set this option to True, create subsystems and make user assignments, and then set it back to False, the existing subsystem restrictions will still apply to assigned users. This option simply hides the feature in the user interface; it does not stop any existing subsystems from being enforced. If you do not want to use subsystems anymore, you should remove all user assignments and delete the subsystems before disabling the feature.

SuspendDrawingWhileScreenUpdatingOff

Default value	False
Description	This configuration setting is used to assist in troubleshooting screen drawing issues. This setting should only be changed on the advice of Axiom Support.

SystemCurrencySymbol

Default value	<Blank>
Description	Defines the currency symbol used by columns that are configured as Currency numeric type. If left blank, the currency symbol for the current locale is used. The Numeric Type is defined in the column properties.

SystemCurrentPeriod

Default value	1
Description	Defines the current period for the system. To change the current period, you can use the user interface in the software (**Administration > Tables > Table Administration > System Current Period / Year**).

SystemCurrentYear

Default value	1
Description	Defines the current year for the system. To change the current year, you can use the user interface in the software (**Administration > Tables > Table Administration > System Current Period / Year**).

SystemName

Default value	Axiom
Description	Defines the name of the system. You can change this name as desired. This setting can be modified using the System Configuration page in the Web Client.

TableRepartitioningRowLimit

Default value	2000000
Description	Specifies the row limit for repartitioning a table as part of saving the table properties. If the table data exceeds this row limit, then the table will not be repartitioned and instead you will be prompted to process the table repartitioning using Scheduler.

TablesRestrictedFromReportWriter

Default value	<Blank>
Description	A comma-separated list of tables to restrict from use in the web Report Builder. Any tables listed here will not be available for selection as the data context for the report, and will not display as related tables or dimension tables. By default this is blank, which means all tables are available for use in the Report Builder.

TiePlanFileSaveToProcessSubmit

Default value	True
Description	Specifies whether users can complete tasks for plan file processes when saving plan files (True/False). By default, when a user saves a file for which they have an active process task, the user is given the option to complete the task as part of the save. The "complete on save" option only applies when the user opens the file as read/write. If disabled, then no process prompt displays on save.

TranslateFrenchKeyboardDecimalSeparator

Default value	False
Description	Specifies whether special decimal translation behavior applies to the Web Client and Windows Client (True/False). If enabled, then pressing the decimal key on a numeric keypad is interpreted as a comma when the following are true: the current locale's number format is comma, and the number format for the cell is one of Number, General, Percent, Scientific, or Currency. Note that the number format only applies to the Web Client; in the Windows Client, the behavior applies regardless of the number format.

UpdateStatisticsDuringSave

Default value	False
Description	Specifies whether statistics are rebuilt as part of save-to-database processes (True/False). This applies to both the temporary table (if saving more than 10,000 rows) and the destination table. This should only be enabled on the advice of Axiom Support.

UseLegacyColumnAggregation

Default value	False
Description	Specifies whether to use the legacy default aggregation behavior for Integer and Numeric columns in data queries. This should only be enabled on the advice of Axiom Support.

UseLegacyInnerJoins

Default value	False
Description	Specifies whether to use the legacy SQL inner join strategy for lookups (True/False). This should only be enabled on the advice of Axiom Support. This setting is not returned when querying Axiom.SystemConfiguration. The Axiom Software Manager can be used to view and edit the setting.

UseLegacySQLJoinStrategy

Default value	False
Description	Specifies whether to use the legacy SQL join strategy (True/False). This should only be enabled on the advice of Axiom Support.

UseLegacySQLParser

Default value	False
Description	Specifies whether to use the legacy SQL parser (True/False). This should only be enabled on the advice of Axiom Support.

UseRestrictedWebModeForNonAdmins

Default value	True
Description	Specifies whether to use a special restricted mode in the Windows Client for non-admin users (True/False). If enabled, then certain file features are explicitly tied to read-write rights. For more information please contact Axiom Support. This setting exists for backward-compatibility only and should not be manually enabled in systems where it is not already enabled.

UseStickSessionServerHash

Default value	False
Description	Specifies how sticky sessions are handled for Axiom Cloud systems. This setting should only be changed on the advice of Axiom Support.

UseXlfnSingleUdf

Default value	True
Description	Specifies whether Axiom applies special behavior in the Windows Client (True/False), intended to prevent issues when formulas in a worksheet use a mix of dynamic array functions and implicit intersection operators.

VBA_RunMacroDisabled

Default value	True
Description	Specifies whether VBA custom solutions can be run while in the Axiom Excel Client (True/False). By default, the system does not check for VBA custom solutions, and AxiomVBA.xlam is not loaded when the system is run. If set to False, then the system uses the designated event handlers to check for VBA custom solutions, and runs them if found. This setting should only be changed to False if your system is specifically designed to use VBA custom solutions. Enabling custom solutions may unnecessarily impact system performance for systems that do not use VBA.

WebClientSkin

Default value	<Blank>
Description	Specifies the default skin to be applied to Axiom forms. If the **Skin** property for a form is blank, the default skin defined here is used. By default, this setting is blank, which means the default **Axiom** skin is used. If desired, you can specify any skin that is available to be selected for an Axiom form, including any custom skin defined for your organization. For the list of available skin names, check the **Skin** property on an Axiom form. If you have defined a specific skin name and then want to return to using the default Axiom skin, clear this setting so that it is blank again.

WebPageTabItemBackground

Default value	#FFFFFF
Description	Specifies the background color of web tabs and form dialogs while the "loading" spinner displays. You can specify a different color using a hexadecimal code.

WindowsAuthAllowedDomains

Default value	<Blank>
Description	Specifies the allowed domains for Windows Authentication, if enabled. Separate multiple domain names with a comma. This option is initially configured during the Axiom Application Server installation, and can be subsequently changed using the system configuration settings or by repairing the installation. This setting can be modified using the System Configuration page in the Web Client.

WindowsAuthEnabled

Default value	True
Description	Specifies whether Windows Authentication is enabled for the system (True/False). By default this is enabled, which means that the allowed domains must be specified using WindowsAuthAllowedDomains. This option is initially configured during the Axiom Application Server installation, and can be subsequently changed using the system configuration settings or by repairing the installation. If disabled, then Windows Authentication is not used.

WindowsAuthUserSyncEnabled

Default value	False
Description	Specifies whether Active Directory Synchronization is enabled for the system (True/False), allowing users to be imported from and synchronized with Active Directory. This option is only applicable if Windows User Authentication is enabled for the system. This option is initially configured during the Axiom Application Server installation, and can be subsequently changed using the system configuration settings or by repairing the installation.

EtlCompressRelayFileDataImport

Default value	True
Description	Indicates data coming from CIS over Azure Relay should be compressed.

EtlCompressRelayFileDataExport

Default value	False
Description	Indicates data coming from CIS over Azure Relay should be compressed.

EtlUseBlobStorageForFileUpload

Default value	False
Description	Instructs CIS to upload files to blob storage instead of using Azure Relay Service. The default was changed to false because EtlCompressRelay is more of an improvement. **NOTE:** Ensure you update CIS when installing Axiom 2022.3 to see this performance improvement.

NOTE: Systems may use additional configuration settings that are not listed here. Typically these settings are product-specific or meant to be configured by Axiom representatives only.

Index

V

W