Cloud Technical Guide

Axiom
Version 2022.3

AXIOM

Contents

Introduction

Welcome to the Axiom Cloud! Your Axiom Cloud system is hosted and maintained by Syntellis in a dynamically scalable, secure, and geo-distributed Microsoft Azure datacenter. Before your users can get started with this system, there are a few minor setup and installation tasks that need to be performed by your organization.

Use of your Axiom Cloud system requires the following:

- Installation of the Axiom Desktop Client and its prerequisites on user workstations. The Desktop Client is required in order to access and use your Axiom Cloud system.

- Installation of the Axiom Cloud Integration Service on a Windows server at your organization. This service is used to facilitate certain secured data communications between your Axiom Cloud system and servers in your organization's network, such as for data imports/exports and user authentication. Although this service is not absolutely required in order to use your Axiom Cloud system, most customers choose to install it in order to gain access to the features it enables.

Axiom Cloud technical requirements

This section details the technical requirements for use of the Axiom Cloud.

▶ Client technical requirements

For information on technical requirements for use of the Axiom Client with the Axiom Cloud, see the separate document *Axiom Client Technical Requirements*.

▶ Network bandwidth requirements

All Internet connections to the Axiom Cloud must be at least 3 Mbps for data download and upload. Syntellis will work with you to validate the Internet connection performance of your desired usage environment.

▶ Firewall requirements

- **Axiom Desktop Client**: Your organization's corporate firewall must allow communication via port 443 using the TLS 1.2 protocol between the client workstation and the Axiom Cloud. In addition, the following domains must be added to your "allow list": **https://*.axiom.cloud**, **https://*.powerbi.com**, and **https://*.analysis.windows.net**.

- **Axiom Cloud Integration Service**: The Axiom Cloud Integration Service must be able to establish outbound connections on ports 443 and 5671, as well as port range 9350-9354. If this recommendation cannot be met, the minimum requirement is to allow outbound traffic for these ports to the Microsoft Azure Datacenter IP Range list for your geographic region, which is subject to change on a weekly basis.

  The Axiom Cloud Integration Service must be able to accept a validated SSL certificate from the following domains: **https://*.axiom.cloud** and **https://*.servicebus.windows.net**.

For clients on the legacy **axiomepmcloud.com** and **khaempcloud.com** domains, we will be deprecating those domains starting with version 2020.1 of Axiom. Please work with your Information Technology department to ensure that **https://*.axiom.cloud** is added to your "allow list" prior to upgrading to version 2020.1 or later.

▶ Email delivery requirements

The Axiom Cloud is configured to email alerts and other information via standard email messages to your end users. Your organization's corporate email system must allow Axiom Cloud emails to be delivered to your SMTP endpoint without being blocked. Please add the SMTP email server ***.sendgrid.net** or the email address ***@axiom.cloud** to your "allow list" according to your email server best practices.

Axiom Client

Installation of the Axiom Desktop Client is required to access your Axiom Cloud system. There are two versions of the desktop client:

- **Windows Client.** The Windows Client is typically used by standard Axiom end users. It does not require Microsoft Excel to be installed on the workstation.

- **Excel Client.** The Excel Client is typically used by Axiom administrators and report writers. It requires Microsoft Excel to be installed on the workstation.

For information regarding the Axiom Client technical requirements and prerequisites, see the separate document *Axiom Client Technical Requirements*.

Axiom provides a third client, the Web Client, for browser-based access of certain web-enabled files and features. Use of the Web Client does not require any installation. Users who will access Axiom only via the Web Client can simply navigate to the appropriate URL using a supported browser.

Installing the Axiom Client

This section explains the installation of the Axiom Desktop Client (Windows Client and Excel Client) on individual client workstations.

▶ Requirements to install and launch the Desktop Client from the browser
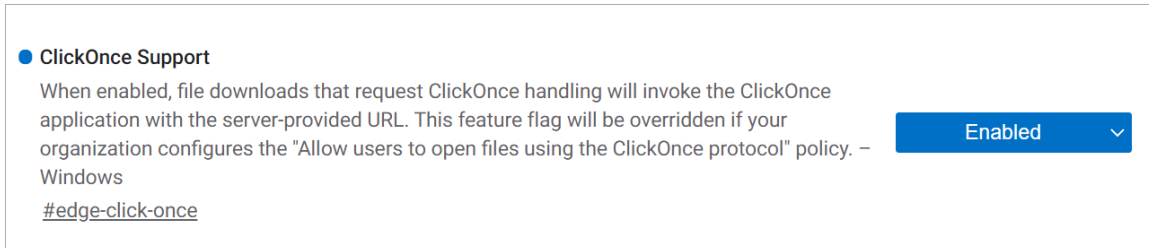
Axiom uses Microsoft ClickOnce technology to install and launch the Axiom Desktop Client (Excel or Windows) from the Web Client browser. Your chosen browser must be ClickOnce compliant, either by enabling ClickOnce support in the browser configuration settings, or by installing a ClickOnce extension 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`.
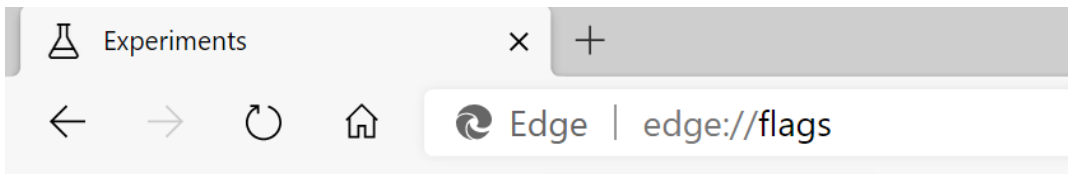
2. Scroll down until you locate the item named **ClickOnce Support**. Select **Enabled** from the drop-down list.

● ClickOnce Support

When enabled, file downloads that request ClickOnce handling will invoke the ClickOnce application with the server-provided URL. This feature flag will be overridden if your organization configures the "Allow users to open files using the ClickOnce protocol" policy. – Windows

#edge-click-once

Enabled ⌄

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.

▶ Before you install

Before beginning the client installation process, make sure you have installed the necessary prerequisites for the particular Axiom Client you intend to use.

1. Log into your workstation as a local administrator.

2. Open your browser and navigate to the following URL:

   `https://<customername>.axiom.cloud`

   Where *<customername>* is your assigned system name for the Axiom Cloud.

3. Click the Syntellis icon ⠿ in the right side of the navigation bar across the top of the page. At the bottom of the menu, click **About Axiom Software**.

4. In the About Axiom dialog, under **Download**, click **Necessary software tools for running Axiom desktop client applications**.

   AXIOM ✖

   System Name
   Axiom Software Test System

   Download
   Necessary software tools for running Axiom desktop client applications
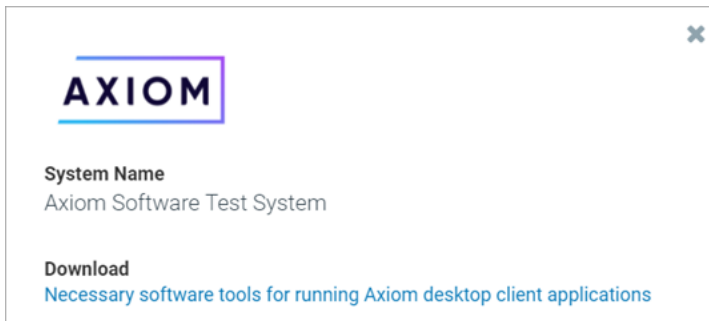
5. From the Download page, install the necessary prerequisites for the Axiom Client that you intend to use.

   See the separate document *Axiom Client Technical Requirements* for more information on which prerequisites to install.
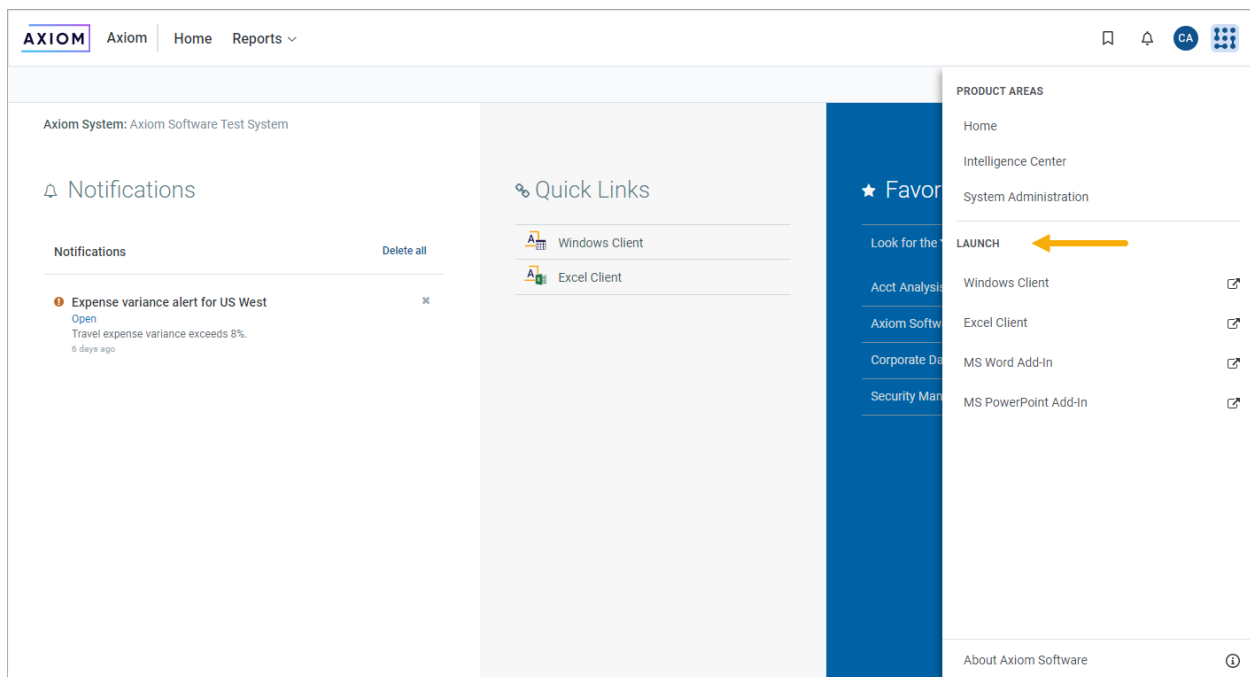
▶ Install the Axiom Client

1. Log into your workstation as yourself.

2. Open your browser and navigate to the following URL:

   `https://<customername>.axiom.cloud`

   Where *<customername>* is your assigned system name for the Axiom Cloud.

   The browser used must support ClickOnce in order to directly install and launch the application. See Requirements to install and launch the Desktop Client from the browser.

3. Click the Syntellis icon ⠿ in the right side of Navigation bar across the top of the page. In the Launch menu, click on one of the following to install that client:

   - **Windows Client**
   - **Excel Client**

Example Quick Launch menu to install the Axiom client

▶ Client shortcuts

Depending on the selected user authentication method for your system, the Axiom Client installation may create shortcuts on your desktop and in your Start menu. If these shortcuts are present, then you can launch the Axiom Client directly via these shortcuts, without needing to access the Axiom web page. If you are using SAML or OpenID Authentication, then you must always go to the Axiom web page in order to launch the system.

► Upgrading the Axiom Client

Going forward, under normal circumstances you should not need to manually upgrade the Axiom Client. Your Axiom Cloud system can be upgraded by Axiom Support at your organization's request. Once the Axiom Cloud system is upgraded, your client installations will be automatically upgraded as needed the next time a user attempts to log into Axiom on that workstation.

User Authentication

Login credentials are required to access Axiom. The specific credentials depend on the user authentication method enabled for your system.

The Axiom Cloud supports the following authentication methods:
- **Windows Authentication**: Users are authenticated by your Windows Active Directory.
- **SAML Authentication**: Users are authenticated by a designated SAML identity provider.
- **OpenID Authentication**: Users are authenticated by a designated OpenID provider.

Axiom Support will enable your organization's preferred authentication method in your Axiom Cloud system. The following sections provide a brief overview of each method and the information needed from your organization to enable it.

► Windows Authentication

When using Windows Authentication, users are authenticated by your Windows Active Directory. To access Axiom, users log in with their Windows user names and passwords. A "remember me" option is available so that users do not have to enter their credentials every time they start Axiom.

The user names defined in Axiom must match the Windows user names in Active Directory. Users can be manually created in Axiom, or imported from Active Directory.

To enable this option for your Axiom Cloud system, you must provide Axiom Support with the allowed domain names for authentication. Additionally, to facilitate the user authentication you must install the Axiom Cloud Integration Service in your environment, to enable secured communication between your cloud system and your network domain. For more information on this process, see Axiom Cloud Integration Service.

► SAML Authentication

SAML Authentication (Security Assertion Markup Language) is a web-based authentication method. Users are authenticated by a designated identity provider, such as Windows Active Directory Federation Services. To access Axiom, users go to the web page for your Axiom Cloud system, where they must log in using their credentials for the identity provider. Once the user is authenticated, they can access the Axiom Web Client or install/launch the Windows Client or Excel Client.

The user names defined in Axiom must match the user names for the designated identity provider. Users must log in using the web each time they want to start Axiom—desktop shortcuts cannot be used to directly launch the Windows Client or Excel Client.

To enable this option for your Axiom Cloud system, you must provide Axiom Support with the following information:

- The URL to your identity provider
- The metadata URL for your identity provider
- The URN attribute for the authenticated user name (as provided to Axiom from your identity provider)

Additionally, the following setup steps must be completed in your environment. Axiom Support is available to assist with these steps as needed.

- Add the metadata URL for your Axiom Cloud system (provided by Support) to your identity provider so that it is recognized as a service provider. For example, in Active Directory Federation Services, the metadata URL must be added as a Relying Party Trust.
- For Active Directory Federation Services, add a Claim Rule to send the Active Directory **SAM-Account-Name** as the **Name-ID**.
- Other setup steps may be necessary, depending on your identity provider.

▶ OpenID Authentication

OpenID Authentication is a web-based authentication method. Users are authenticated by a designated OpenID provider, such as Google OpenID Connect. To access Axiom, users go to the web page for your Axiom Cloud system, where they must log in using their credentials for the OpenID provider. Once the user is authenticated, they can access the Axiom Web Client or install/launch the Windows Client or Excel Client.

The user names defined in Axiom must match the user names for the designated OpenID provider, including the @suffix. Users must log in using the web each time they want to start Axiom—desktop shortcuts cannot be used to directly launch the Windows Client or Excel Client.

To enable this option for your Axiom Cloud system, you must provide Axiom Support with the following information:

- The client ID for your OpenID provider
- The client secret for your OpenID provider

Additionally, the following setup steps must be completed in your environment. Axiom Support is available to assist with these steps as needed.

- Configure the OpenID provider with the redirect URI to the Axiom login page (such as `https://CustomerSite.axiom.cloud/openid/login`).
- Other setup steps may be required, depending on your OpenID provider.

Axiom Cloud Integration Service

The Axiom Cloud Integration Service is used to facilitate certain data communications between your Axiom Cloud system and servers in your organization's network. Normally, the Axiom Cloud would not be able to communicate with these servers due to firewall restrictions and other security controls. The Cloud Integration Service provides a secure bridge between the Axiom Cloud and your organization's network.

The Cloud Integration Service uses 256-bit HTTPS for this communication, using a Shared Access Signature (SAS) authentication protocol involving a 256-bit primary cryptographic key in Base64 representation and a token generated using the HMAC-SHA256 of a resource string.

Although installation of the Cloud Integration Service is technically optional, it is required if you want to use any of the following features:

- **Windows Authentication.** In order to use Windows Authentication for login to Axiom, your Axiom Cloud system needs to validate users against your organization's Windows domain. This validation is accomplished using the Cloud Integration Service.

- **Import/Export of local data.** If you want to be able to import data from a database hosted in your network or from a file residing on your network, your Axiom Cloud system must be able to access the local database or local file. The same principles apply when exporting data from your cloud system to a local database or delimited file. This access is accomplished using the Cloud Integration Service.

- **File Processing to a local folder.** If you want to be able to generate snapshot or export files using file processing and then save the file output locally, your Axiom Cloud system must be able to access the local folder location. This access is accomplished using the Cloud Integration Service.

Server technical requirements

The Axiom Cloud Integration Service must be installed on a Windows Server in your organization's network environment. The server technical requirements are as follows:

Requirement	Cloud Integration Service
CPU	Dual core 2.0Ghz or higher
RAM	2GB
Disk	150MB available disk
OS	Windows Server 2019
Other Software	.NET Framework 4.8 or higher

Other requirements depend on the usage of the service:

- When used for Windows Authentication, the server must be able to access the Windows domain(s) used for authentication.

- When used for import of data from source files, or for file processing to a local folder location, the user identity of the service must have permission to the appropriate file shares and files.
- When used for import/export of data from a database, the server must be able to see the appropriate database server, so that the credentials in the import/export package can be used to access it.

You can install and use more than one Cloud Integration Service as needed. For example, one service could be used for authentication, while another service could be used for import/export.

For information on networking and firewall requirements, see Axiom Cloud technical requirements.

Installing the Axiom Cloud Integration Service

In order to perform the installation, you must have obtained a copy of the Axiom installation package (ZIP file) and extracted the contents of this package to the server where you want to install the Cloud Integration Service. The installation package can be obtained from Axiom Support.

The logged in user must have administrator rights on the server to run the installation.

> **IMPORTANT:** In order to complete the install, you must know the encryption key for your Axiom Cloud system. If you do not know this key, contact Axiom Support for assistance.

> **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.

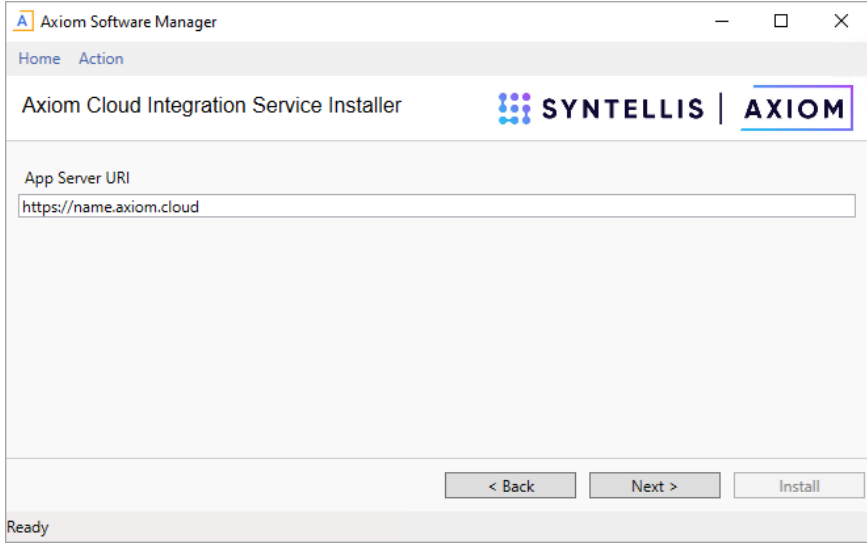**To install the Axiom Cloud Integration Service:**

1. Navigate to the location where you extracted the Axiom installation package, and then run `AxiomSoftwareManager.exe` as an administrator.

2. On the **Installation Manager** screen, under **Install new software package**, click **Cloud Integration Service**.
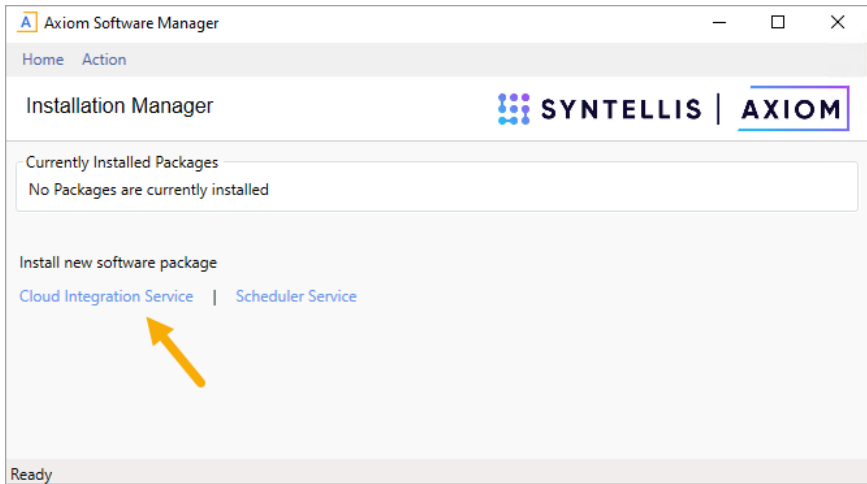
The Axiom Cloud Integration Service installation begins. The installation is performed within the Software Manager—a separate installer program is not launched. While using the installer, do not use the menu to move to other locations in the Software Manager, unless you want to cancel the installation.

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 you use to access the web page for your Axiom Cloud system.

5. On the **Installation Folder** screen, specify the installation location for the Cloud Integration 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 Cloud Integration Service\
    ```

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

    The default name is **Axiom EPM Cloud Integration Service**.

7. On the **Axiom Server Encryption Key** screen, specify the encryption key for your Axiom Cloud system, and then click **Next**.

    This key is used by your Axiom Cloud system to authenticate requests from the Cloud Integration Service. The key must match the key defined for your cloud system. If you do not know the key, contact Axiom Support for assistance.

8. Optional. Specify whether to enable **Restrict to HTTPS connection mode**:
    - If enabled, then the Cloud Integration Service can only use port 443.
    - If disabled (default), then the Cloud Integration Service can use other supported ports.

9. Optional. On the **Accessible Folders** screen, specify the folders that the Cloud Integration Service can access, and then click **Next**.

    This setting can be used to limit the service to accessing a specific folder or folders in your organization's network. You can leave this blank to allow the service to access any folder (as permitted by the network file system permissions for the service), 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 used by the Axiom feature that you intend to run using the Cloud Integration Service. For example, if an import utility specifies the file as `\\Server\Folder\filename.xlsx`, then you must specify `\\Server\Folder` in this setting. If instead you specify `N:\Sharename\Folder`, the service will not be able to access the file for the import.

    > **NOTE:** After installation, the list of accessible folders can be viewed in the remote data connection properties, in Scheduler. However, the accessible folders cannot be defined or modified from Scheduler. If you need to edit the accessible folders after installation, you must repair the Cloud Integration Service.

10. 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 Cloud Integration 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 Cloud Integration Service** and then select **Start**.

If you will be using the Cloud Integration Service to access files on your network, then the account used to run the service must have the appropriate network security permissions to access these files. Please contact Axiom Support for assistance in configuring this access for the service account as needed.

▶ Saving a copy of the Software Manager

It is recommended to leave the Software Manager file on the machine where you installed the Cloud Integration Service, so that it is available in case you later need to repair or uninstall the service. The Windows Control Panel cannot be used to perform these activities. If you have deleted the Software Manager file and you need to perform a repair or uninstall, you can obtain a copy of the installation package from Axiom Support or from the Axiom help files.

Setting up the remote data connection

In order to use the Axiom Cloud Integration Service with Axiom features such as imports or user authentication, you must create a *remote data connection*. The remote data connection links the Cloud Integration Service with your Axiom Cloud system.

Remote data connections are created in Scheduler, using the Axiom Excel Client or Windows Client. You must install the Desktop Client before you can perform this activity. For more information, see Axiom Client.

Once you have logged into the client, go to **Manage > Scheduler** on the Axiom tab. (If you are using an Axiom packaged product, you can access Scheduler from the **Admin** tab.)

Setting up the remote data connection is a three-part process:

1. Axiom Support must create a namespace for your Axiom Cloud system and provide you with the connection string to this namespace. Make sure you have this information before proceeding with the steps in the following sections.

2. The Cloud Integration Service must be enabled in Scheduler so that it is available to process requests from the remote data connection.

3. The remote data connection must be created in Scheduler.

Steps 2 and 3 are discussed in the following sections. Only administrators can perform these actions.

▶ Enabling the Cloud Integration Service

After the Axiom Cloud Integration Service is installed on a local server, you must enable this server for use in Scheduler.

To enable the Cloud Integration Service:

1. On the **Service** tab of the Scheduler dialog, click **Servers**.

2. In the list of servers, select the server hosting the Cloud Integration Service. The name of this server is *ServerName*-**CIS**.

3. At the bottom of the dialog, under **Configuration details**, select the check box for **Cloud Integration Service Enabled** and then click **Update**.

The server is now enabled and ready for use. You can refresh the page to see the updated server status.

If you installed the Cloud Integration Service on multiple servers to use for different purposes, then you must enable each server separately.

▶ Creating the remote data connection

In order to use the Axiom Cloud Integration Service with Axiom features, you must create a remote data connection in Scheduler.

The remote data connection links the Axiom Cloud Integration Service to your Axiom Cloud system, using a namespace created specifically for this purpose by Axiom Support. You must have the connection string to this namespace in order to create the remote data connection.

To create a remote data connection:

1. On the **Service** tab of the Scheduler dialog, click **Remote Data Connections**.

2. At the bottom of the dialog, click **New Connection**.

   A set of empty fields displays in the **Configuration details** section.

3. Complete the following settings:

Item	Description
Name	The name of the remote data connection.
Description	Optional. The description of the remote data connection.
Connection String (SAS)	The connection string to the namespace that was created by Axiom Support in the Microsoft Azure environment for your Axiom Cloud system. If you do not have this connection string, contact Axiom Support.

Item	Description
Use for authentication service	Specifies whether the remote data connection is used for Windows Authentication. This only applies if Windows Authentication is enabled for your Axiom Cloud system. If enabled, this remote data connection will also be used for any Active Directory Import tasks set up for your system.
Cloud Integration Server	The name of the Axiom Cloud Integration Service installed in the local network environment. The name of this server is *ServerName*-**CIS**.

4. Click **Save Connection**.

The connection now displays in the list of remote data connections.
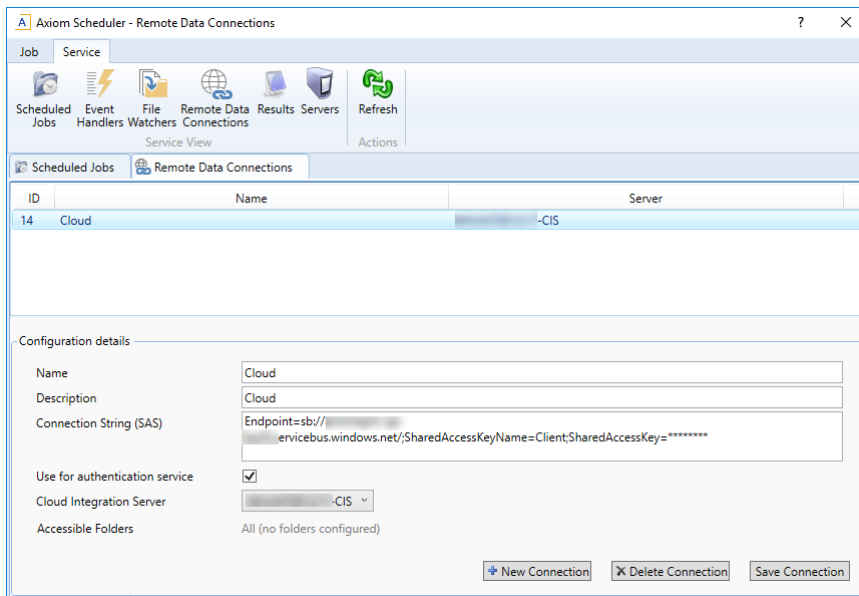
Example remote data connection

If you later want to edit this connection you can come back to this screen, select the connection and make the necessary edits, then click **Save Connection** to save the changes. To delete a connection that you no longer need, use **Delete Connection**.

If you installed the Cloud Integration Service on multiple servers, you should create a remote data connection for each server. For example, you could set up one remote data connection for user authentication and another for import/export. For the import/export connection, you would disable the option **Use for authentication service**.

Using a remote data connection with Axiom features

Once a remote data connection has been set up for your installation, you can use this connection with Windows Authentication, import and export utilities, and file processing. For more information on setting up these features, see Axiom Help.

▶ Windows Authentication

In order to use Windows Authentication with the Axiom Cloud, you must have a remote data connection defined with the option **Use for authentication service** enabled (as discussed in the previous section). All other setup requirements for Windows Authentication still apply—see the Axiom Help files for more information.

When a user attempts to log into your Axiom Cloud system using Windows Authentication, their credentials are verified by your Windows domain using the remote data connection. This means that the remote data connection configuration in Scheduler must remain intact, and the server hosting the Cloud Integration Service must remain up and running. If the remote data connection or the Cloud Integration Service are unavailable, users will be unable to log in.

If you are using the Active Directory Import task in Scheduler to synchronize users in Axiom with your Active Directory, this task will automatically use the remote data connection that is enabled for user authentication.

▶ Import/Export utilities

When you set up the **Source** for an import or the **Destination** for an export, you have the option to specify a remote data connection. If a remote data connection is specified, then the import or export utility will use that connection to transfer data or a file between the Axiom Cloud and your local network.
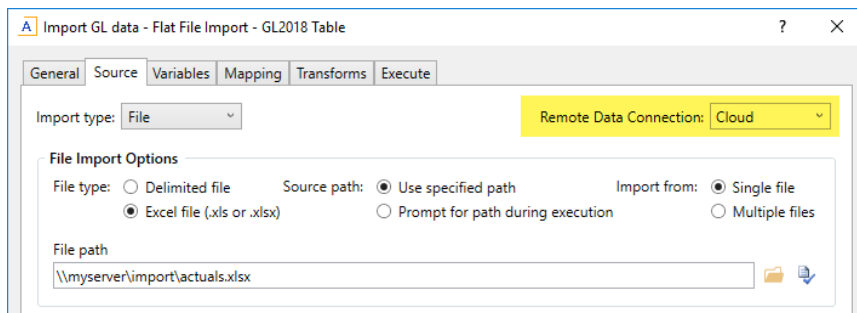
Example import source using a remote data connection

▶ File processing

When you select **Local File System** as the output location for snapshot or export file processing, you have the option to specify a remote data connection. This connection is required if you plan to perform the file processing via Scheduler.
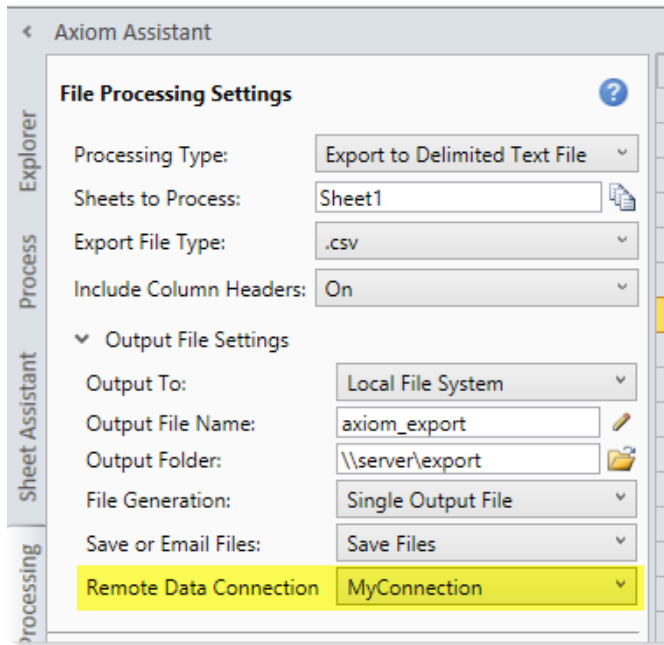
Example file processing configuration using a remote data connection

You can also use a remote data connection with the File Collect option of file processing. In this case, the setting is located on the File Collect Configuration sheet.

Output File Settings	
Output location (local file or Axiom)	Local File System
Output file purge setting (Axiom files only) - can be a static purge date or number of days	
Output folder path	\\server\folder\monthlyreports
Remote Data Connection Name	MyRDC
Output file name (no extension)	MonthlyReportsPackage_North
Output file type	.xlsx
Save or email generated files	Save File and Send Email

Example File Collect configuration using a remote data connection

Upgrading the Axiom Cloud Integration Service

It is required to upgrade the Axiom Cloud Integration Service when upgrading to version 2022.3.

> **NOTE:** The minimum .NET version requirement is 4.8. Make sure your server meets this requirement before upgrading the service.

In order to perform the upgrade, you must have obtained a copy of the Axiom installation package (ZIP file) and extracted the contents of this package to the server where the Cloud Integration Service is installed. The installation package can be obtained from Axiom Support. You must have administrator rights on the server to run the installation.

To upgrade the Axiom Cloud Integration Service:

1. Navigate to the location where you extracted the Axiom installation package, and then run

`AxiomSoftwareManager.exe` as an administrator.

2. On the **Installation Manager** screen, in the **Currently Installed Packages** section, locate the entry for the Cloud Integration Service and then click **Upgrade**.

3. On the Axiom Cloud Integration Service screen, click **Upgrade**.

The upgrade occurs automatically with no further prompts. All installation settings are remembered from the original install.

> **NOTE:** If you are upgrading from a much older version of the service, it may be necessary to perform a Repair to provide values for required settings that did not exist when you performed the original installation. For more information on these settings, see Installing the Axiom Cloud Integration Service, and contact Axiom Support for assistance as needed.

Uninstalling the Axiom Cloud Integration Service

The Axiom Cloud Integration Service can be uninstalled by using the Axiom Software Manager.

To uninstall the Cloud Integration Service:

1. Navigate to the location where you extracted the Axiom installation package, and then run `AxiomSoftwareManager.exe` as an administrator.

2. On the **Installation Manager** screen, in the **Currently Installed Packages** section, locate the entry for Cloud Integration Service and then click **Uninstall**.

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

4. 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.

5. Click **Uninstall**.

> **NOTE:** The Cloud Integration Service does not display in the Windows program manager and cannot be uninstalled from that location.