Installing AX Server with PostgreSQL (multi-server)

Version: 6.5

Published: Friday, September 1, 2017

Table of contents

Introduction

This guide is designed to walk you through the process of installing AX Server with a PostgreSQL database server. The contents of this guide are limited to installation and initial setup.

For additional information about AX Server maintenance and using Analytics Exchange, visit the online ACL Help Docs.

Intended audience

This guide is written for AX Server administrators who are responsible for the installation and setup of Analytics Exchange for their organizations.

Pre-installation tasks

Gathering installation resources

Before you begin installing or upgrading AX Server, identify the key contacts you need to provide assistance and information for the installation process.

ACL Support Services

Contact ACL Support Services if you encounter problems that you cannot solve during the installation or upgrade. Before you contact ACL Support, ensure that you have the following information:

- The specific version of AX Server that you are installing or upgrading
- Details about the database (PostgreSQL or Oracle) that you are using with AX Server
- Any error or warning messages that you are encountering

You can contact ACL Support Services in a number of different ways:

- submitting a support ticket online (preferred method)
- live chat
- email (support@acl.com)
- telephone

Primary ACL contact

To download the AX Server installation package from Launchpad, you must have a valid Launchpad account.

- If you are the primary contact at your organization, you should have received a welcome email from ACL with instructions for signing in to your account. If you have not received the email or need further assistance, contact ACL Support Services.
- If you are not the primary contact, you should have received instructions by email when the primary contact added you to Launchpad. If have not received instructions, contact your organization's primary contact or ACL account administrator.

Database administrator

If your organization has a database administrator, he or she will have important information you require to install and configure AX Server.

IT staff

If your organization has IT staff who administer services such as network access, file storage, and security policies, they may have information you need to complete the installation. They may also need to complete tasks such as creating Active Directory user accounts and modifying firewall rules.

AX Server ports

For the Analytics Exchange Service to start successfully on the AX Server server or AX Engine Node, you must ensure that the ports required by the TomEE application server are not being used by other services or applications.

Checking ports in use

From a command prompt, use the NETSTAT command to display in-use ports:

```
NETSTAT -a
```

If required ports are being used by another service, you must do one of the following:

- reconfigure the service to use a different port
- temporarily disable the service in Windows Services while you install AX Server

If necessary, you can modify some of the ports used by AX Server after the installation process is complete.

> **Note**
>
> If you are installing AX Server or AX Engine Node for the first time on a server, you should verify that the ports required by the TomEE application server are not in use before you run the installer.

Ports required by the AX Server

AX Server and AX Engine Node are installed with the default port settings used by the Analytics Exchange Service.

Port	Component	Encryption	Description
8009	Tomcat Connector AJP	Non-SSL	Port used to connect to the TomEE application server. This is a unidirectional port. It is used for internally by AX Server and does not need to be opened for outside communication.
80	Tomcat Connector HTTP	Non-SSL	Port used for unencrypted HTTP communication with the server. This is a unidirectional port. It should be opened for outside communication on AX Server and AX Engine Node.
443	Tomcat Connector HTTPS	SSL	Port used for encrypted HTTP (HTTPS) communication with the server. This is a bidirectional port. It must be opened on AX Server for com-

Port	Component	Encryption	Description
			munication with AX Client. If you are upgrading an earlier version of AX Server, the default port is 8443.
5432	PostgreSQL	Supported	You can specify a different port that is not in use in the AX Server installer. **Note** If you are configuring a dual-server installation, you must ensure that the PostgreSQL and AX Server and AX Engine Node can communicate on this port.
10000	AX Connector	TwoFish 128 bit	If this port is in use, you can specify a different port that is not in use in the AX Server installer. This service is used primarily to access AX Server tables that have been exported to ACL Analytics projects. It must be opened on AX Server for inbound communication.
4201	AX Engine Node	Non-SSL	Used to connect AX Engine Node to the master AX Server. If the AX Engine Node and AX Server are communicating across a firewall, you must open this port.
1521	Oracle database	Non-SSL	Port used for unencrypted Oracle database communication. It must be opened on AX Server and AX Engine Node for communication with the Oracle database. **Note** Your IT team will stipulate which port is required when Oracle is used as the AX Server database server. The port can be changed after the installation is completed, if necessary.
5432	Oracle database	SSL	Port used for encrypted Oracle database communication. It must be opened on AX Server and AX Engine Node for communication with the Oracle database if you are encrypting the connection. **Note** Your IT team will stipulate which port is required when Oracle is used as the AX Server database server. The port can be changed after the installation is completed, if necessary.
1543	ACL Connector for Analytics Exchange	SSL	Port used for establishing an ODBC connection to analytic results. This port is only required if you install the optional ACL Connector for Analytics Exchange service. It must be opened for inbound communication on AX Server.

Firewall configuration

To connect to AX Server from outside your network firewall, you must allow inbound connections on the following ports:

Port	Component	Description
443	Tomcat Connector HTTPS	Used to enable HTTPS connections to the web server for the AX Web Client and AX Server Configuration web applications, and for secure file transfers to and from AX Server. **Note** The default value for servers upgraded from versions prior to 5.0.0 is 8443.
10000	AX Connector	Used to enable access to AX Server tables from client computers through ACL Analytics.
4201	AX Engine Node	Used to connect AX Engine Node to the master AX Server. If the AX Engine Node and AX Server are communicating across a firewall, you must open this port.

Each client computer that connects to AX Server must also have the corresponding ports open for outbound communication.

Download the Analytics Exchange installers

Download the installers from Launchpad so you can install Analytics Exchange.

> **Note**
>
> You must be able to sign in to an Launchpad account (www.aclgrc.com) in order to download Analytics Exchange installers, and activate AX Server.

Available installers

Installers for the following Analytics Exchange applications are available on Launchpad:

- AX Server (contains installers for both AX Server and the PostgreSQL)
- AX Engine Node
- ACL Analytics compatibility upgrade for AX Server (if currently applicable)
- AX Client
- Direct Link

Download steps

> **Note**
>
> The installer download page provides the latest version of Analytics Exchange. If you require an installer for a previous version, you must contact ACL Support Services for a copy of the installer for that version

1. Sign in to Launchpad (www.accounts.aclgrc.com) and click **Analytics Exchange**.

   An email with sign in instructions is sent from notifications@aclgrc.com to your company's ACL account administrator. If you are unable to sign in to your Launchpad account, contact your company's ACL account administrator or ACL Support Services for assistance.

2. From the **Select software package to download** list, select the installer you want to download.

   > **Note**
   >
   > Ensure that you download the correct edition (non-Unicode or Unicode) as all installed applications must use the same edition.

3. Click **Download *<Version>*** and save the installer to the computer that you plan to install the application on.

Installation

Install the PostgreSQL database server

Run the AX Server installer on the database server machine to install PostgreSQL on a separate physical machine. Once the database is installed, cancel the installer and run the AX Server portion of the installation on the application server machine.

> **Note**
>
> You must install PostgreSQL before installing AX Server.

Install PostgreSQL

Run the installer and select your database configuration

1. Double-click the installation package and if a security warning dialog box appears, verify the information listed and click **Yes**.
2. Select the setup language and click **OK**.
3. In the **Setup Extraction Location** page, specify the folder where the installation files will be extracted, and click **Install**.

   > **Tip**
   >
   > Click **Browse** to select a folder or accept the default location: `C:\Program Files (x86)\ACL Software\Installers\ACLAX<version>_Server_<edition>`.

4. Click **Yes** in the dialog box with the message about the database engine.
5. In the **Analytics Exchange Server Setup Options** page, select **PostgreSQL** and click **Install**.
6. To run the PostgreSQL setup wizard, click **Yes**.
7. If you are prompted to install prerequisites, click **Install** and wait while the prerequisites are installed.

   Follow any on-screen instructions to complete the prerequisite setup.

Configure the database connection and security

1. In the **Welcome** page, click **Next** and in the **License Agreement** page, select **I accept the terms in the license agreement** and click **Next**.
2. In the **Destination Folder** page, accept the default PostgreSQL install location or click **Change** to modify the location, and click **Next**.

If you modify the installation location, the path you specify must not include any spaces.

3. In the **Configure your Analytics Exchange PostgreSQL database server** page select **New Installation** and click **Next**.

   The PostgreSQL database server is installed and during the subsequent AX Server installation process, a new Analytics Exchange database is created.

4. In the **Service configuration** page, enter the following information to configure the PostgreSQL database service and then click **Next**:

Field	Description
Account name	The name of the Windows user account that will run the service. Keep the default account name "postgres" unless you have a reason for changing it. If the account does not already exist, it will be created as a local user account. You cannot use accounts that belong to the Administrators group on the server. If you use an existing account, the required file system permissions and the "Log on as a service" right are assigned to the account.
Account domain	The name of the Active Directory domain the user account belongs to. If you are using a local user account, keep the default value of the computer name.
Account password	The password for the user account. If the user account already exists, you must enter the correct password. If the installer is creating a new account, enter the password you want to use. The password must meet any password complexity requirements that are enforced by the Windows operating system. Additionally, the password must not include backslashes (\) or apostrophes (').
Verify password	Enter the password again to verify it.

5. If the user account does not exist, click **Yes** to create the account.
6. In the **Database configuration** page, enter the following information and then click **Next**:

Field	Description
Port number	The port number used for communications to and from the PostgreSQL. The default port is 5432.
Superuser name	The name of the PostgreSQL Superuser account. The default value is `postgres` and it cannot be changed.
Password	The password for the PostgreSQL Superuser account. Your password must not include backslashes (\) or apostrophes ('). **Note** For security reasons, do not use the same password that you used for the Windows user account that runs the PostgreSQL database service.

Field	Description
Password (again)	Enter the password again to confirm it.

> **Note**
>
> Make a note of the PostgreSQL Superuser account name and password. You need to enter them when you create the Analytics Exchange database during the AX Server portion of the installation.
>
> For information about configuring service accounts, see "Service account configuration" on page 73.

7. In the **SSL certificate information** page, enter the following information to create a self-signed security certificate to secure HTTPS connections between the PostgreSQL and AX Server (and AX Exception if it is installed) and then click **Next**:

Field	Description
Server name	The hostname of the database server. For example: `ax.acl.com`.
Department or division name	The division or business unit that the certificate is being issued for. For example: `Development`.
Organization Name	The name of your company or organization. For example: `ACL Services Ltd.`.
City Name	The city or locality where your company or organization is located. For example: `Vancouver`.
State/Province Name	The state or province where your company or organization is located. For example: `BC`.
Country code	The two-character country code for the country where your company or organization is located. For example: `CA`.
Password	Enter a password of at least 6 characters.
Verify password	Enter the same password again.

   For information about how this certificate is used, and for configuration options, see "Security certificates" on page 51.

8. Click **Install** and when the installation is complete, click **Finish**.

   The AX Server installation process automatically starts when the PostgreSQL installation is complete.

9. Cancel the installer by clicking **Cancel** as soon as the **Cancel** button is available.

Postrequisites

Now that PostgreSQL is installed, copy the installer to the application server machine and install AX Server. For more information, see "Install standalone AX Server for PostgreSQL" on the next page.

Install standalone AX Server for PostgreSQL

Install AX Server without PostgreSQL if your database server is on a separate physical machine.

Prerequisites

The PostgreSQL database must already be installed on a separate server before you install AX Server. For more information, see "Install the PostgreSQL database server" on page 18.

Install AX Server

> **Caution**
>
> You must install the KB2919355 Windows Updates before starting your Analytics Exchange installation on Windows Server 2012 R2. If you do not install this update, your Analytics Exchange installation cannot succeed.

Run the installer and select your database configuration

1. Double-click the installation package and if a security warning dialog box appears, verify the information listed and click **Yes**.
2. Select the setup language and click **OK**.
3. In the **Setup Extraction Location** page, specify the folder where the installation files will be extracted, and click **Install**.

   > **Tip**
   >
   > Click **Browse** to select a folder or accept the default location: `C:\Program Files (x86)\ACL Software\Installers\ACLAX<version>_Server_<edition>`.

4. Click **Yes** in the dialog box with the message about the database engine.
5. In the **Analytics Exchange Server Setup Options** page, select **PostgreSQL** and click **Install**.
6. To cancel the PostgreSQL setup wizard, click **No**.
7. If you are prompted to install prerequisites, click **Install** and wait while the prerequisites are installed.

Follow any on-screen instructions to complete the prerequisite setup. You may be required to restart your computer after installing prerequisites.

Configure your Analytics Exchange services

1. If you are prompted to install prerequisites, click **Install** and wait while the prerequisites are installed.

   Follow any on-screen instructions to complete the prerequisite setup. You may be required to restart your computer after installing prerequisites. If you do need to restart the computer, continue the installation by double-clicking the installer then and selecting the appropriate language, installation destination, and database server.

   > **Note**
   >
   > You may be prompted to accept the terms and conditions for the .NET Framework when installing prerequisites. In this case, the terms and conditions dialog box may appear hidden behind the Analytics Exchange installer dialog box. When installing the .NET Framework, ensure that the installer is not waiting for your input.

2. In the **Welcome** page, click **Next** and in the **License Agreement** page, select **I accept the terms in the license agreement** and click **Next**.
3. In the **Destination Folders and Settings** page, specify where the AX Server application files will be installed and the location where AX Server data will be stored.

   If necessary, click **Change** to modify either, or both, of the default locations. The paths you specify must not include any spaces, and the location you specify for AX Server data must have sufficient disk space available.

   > **Note**
   >
   > If you want to store AX Server data on a dedicated file server or other network location, you need to configure the shared folder after you complete the installation. The shared folder cannot be specified in the AX Server installer.

4. In the **Analytics Exchange Connector port number** panel, enter the port number for the AX Connector to use, or accept the default value of 10000.

   The AX Connector service is used primarily to access *ACL* tables on AX Server from ACL Analytics.

5. In the **Analytics Exchange Tomcat Service Account** panel, do the following:
   a. Enter the domain and username for the account in the format `domain\username`, or click **Browse** to locate the required domain and username.

      If you browse for the account name, you must enter or select the domain or server name first in the **Browse for a User Account** dialog box in order for the installer to present the appropriate list of available user accounts.

> **Note**
>
> Using a local user account to run the TomEE service is not supported. These accounts do not have the appropriate privileges to run some *ACL* commands.

b. Enter the **Password** for the account.
c. Click **Next**.
d. If you are prompted to grant the "Log on as a service" right to the Tomcat service account, click **Yes** and then **OK**.

For information on the options for configuring service accounts, see "Service account configuration" on page 73.

Configure your database connection settings

1. In the **Configure your Analytics Exchange database** page, ensure that **PostgreSQL** is selected, and do one of the following:
   - If you are installing AX Server and PostgreSQL on the same physical server, deselect **Encrypt database communications**.
   - If you are installing AX Server and PostgreSQL on separate physical servers, select **Encrypt database communications** to encrypt the connection.

     > **Tip**
     >
     > Encryption slows performance somewhat, so you should enable it only if data is being transferred between the database server and the application server over an unsecure network.

2. In the **Analytics Exchange database connection settings** page, enter the following information to configure the connection string:

Field	Description
Database Server	The IP address or server name of the server where the database server is located. If you are installing AX Server on the same physical server as PostgreSQL, keep the default value of `localhost` unless you have a reason to change it.
Port	The port to use to connect to the PostgreSQL database. The default port is 5432.
Superuser	The name of the PostgreSQL Superuser account. Leave the default value of `postgres` unless you have a reason to change it.
Password	The password for the Super user account.

3. In the **New PostgreSQL user for Analytics Exchange database** panel, enter the following information and then click **Next**:
   - **Username**: The name of the PostgreSQL database user account to use to access the Analytics Exchange database. The installer creates this user account when it creates the database.
   - **Password**: The password for the PostgreSQL database user account.

- **Password (again)**: Enter the password for the PostgreSQL database user account again to confirm it.

Configure security and authentication

1. In the **Microsoft Active Directory Connection Details** page, verify that the value in the **Default Domain** text box is correct, or enter the correct value, and click **Next**.

   > **Note**
   >
   > The default domain value is the domain end users are authenticated against if they do not specify a domain when they log in using form-based authentication. For example, if an end user enters `jsmith` as their username, and the default domain is ACL, it is equivalent to entering `acl\jsmith`.

2. In the **Analytics Exchange Authentication** page, select the appropriate authentication method:
   - **Form Based Authentication**: Select this option if you want users to be prompted to enter their username and password each time they start a new session with Analytics Exchange. A session is created when a new web browser window is opened, or when AX Client is started.
   - **Integrated Windows Authentication**: Select this option if you want users to be silently authenticated by Analytics Exchange applications based on the user account used to log in to Windows. User accounts that belong to the configured Active Directory domain will not need to enter their username and password information when they access Analytics Exchange applications.

   For more information about the authentication options and the required configuration, see "Analytics Exchange authentication" on page 76.

3. Specify the AX Server authentication configuration details by doing one of the following and then click **Next**:
   - If you selected **Form Based Authentication**, specify the hostname of the server where AX Server is installed. For example: `AX.ACL.COM`.
   - If you selected **Integrated Windows Authentication**, enter the following information:
     - **Analytics Exchange Server Hostname**: Specify the hostname of the server where AX Server is installed. For example: `AX.ACL.COM`
     - **Active Directory Domain** – Specify the Active Directory Domain to use to authenticate users
     - **Kerberos Domain Controller IP Address** – The IP address where your organization's Active Directory Domain Controller is located
     - **Kerberos Service Password** – The password for the Service Principal Name (SPN) account created in Active Directory
4. If you have an existing SSL security certificate, do the following in the **SSL certificate information** page:
   a. Select **Use existing keystore file** and browse to the keystore file on your computer.
   b. Enter the existing **Keystore password**.

5. In the **SSL certificate information** page, enter the following information and then click **Next**:

Field	Description
Server name	The hostname of the database server. For example: `ax.acl.com`.
Department or division name	The division or business unit that the certificate is being issued for. For example: `Development`.
Organization Name	The name of your company or organization. For example: `ACL Services Ltd.`.
City Name	The city or locality where your company or organization is located. For example: `Vancouver`.
State/Province Name	The state or province where your company or organization is located. For example: `BC`.
Country code	The two-character country code for the country where your company or organization is located. For example: `CA`.
Keystore password	Enter a password of at least 6 characters. **Note** If you are using an existing keystore file, this instance of the **Keystore password** text box is disabled.
Private key password	Enter the same password again. The **Keystore password** and the **Private key password** must be identical.

   For information about how this certificate is used, and for configuration options, see "Security certificates" on page 51.

6. In the **Enter Tomcat console username and password** page, enter the following information and then click **Next**:
   - **Username**: Enter the username you want to use to access and administer the Tomcat Web Application Manager and the AX Server Configuration web application
   - **Password**: Enter a password for the username
   - **Confirm password**: Enter the password again to confirm it

Finish the installation

1. Click **Install**.

   Note

   Before the installation process completes you are required to wait for about a minute while the TomEE application server becomes fully functional. The command window may appear intermittently during this period. **Do not cancel the installation.**

2. When the installation process is complete, click **Finish** to exit the installer.

The AX Server Configuration web application opens in the default web browser after the installer finishes. You must complete post-installation tasks in the web application in order for AX Server to be fully functional. For more information, see "Post-installation tasks" on page 29.

> **Note**
>
> If the AX Server Configuration web application displays an error in the web browser, wait for 2 -3 minutes before reloading the page. Depending on your server hardware, the required services may take a few minutes to be fully functional.

If you close the AX Server Configuration web application before completing all the post-installation tasks, you can access the web application again in a web browser. The default location is `https://<servername>/aclconfig`, where <*servername*> is the hostname or IP address of your AX Server. For example: `https://axserver.acl.com/aclconfig`.

Post-installation tasks

Complete the following tasks to finalize your AX Server installation.

> **Note**
>
> Depending on your AX Server configuration, some of these tasks may be optional. If you have components on multiple physical servers, you may need to complete the tasks on each machine.

AX Server tasks

1. Verify that AX Server is running.

   For more information, see "Verify that AX Server is running" on the next page.
2. Activate AX Server.

   For more information, see "Activate AX Server" on page 32.
3. Add an AX Server administrator.

   For more information, see "Add an AX Server administrator" on page 34.
4. Configure the Archive and Restore data directory.

   For more information, see "Configure the Archive and Restore data directory" on page 35.
5. Optional. Install and configure Python on AX Server and any instances of AX Engine Node if you intend to use Python integration in Analytic scripts.

   For more information, see "Configuring Python for use with AX Server" on page 38.

AX Client tasks

1. Verify client application connections.

   For more information, see "Verifying client application connections" on page 36.
2. Optional. From the AX Server machine, configure the application timeout setting for AX Client.

   By default, the application times out after sitting idle for 30 minutes. You can change this maximum idle time setting in the `aclAuditExchange.xml` configuration file. For more information, see "aclAuditExchange.xml" on page 83.

Verify that AX Server is running

Verify AX Server is running by checking the service log, services, and the Tomcat Web Application Manager.

Check the Analytics Exchange Service log

To check that the Analytics Exchange Service is running, in the `TomCat/logs` sub-directory of AX Server, open the `TomEE.date.log` file and review the log entries.

A new log file is created each time the service is started/restarted or when the file exceeds the maximum file size.

Check the AX Server services

The status of each AX Server Windows service should be “Started” or “Running”. If you have installed AX Server components on more than one server, make sure to check the services on all servers.

1. On to the server where the services are running, navigate to the Windows **Control Panel**, select **Administrative Tools**, and then open **Services**.
2. In the **Services** window, check that the following services are listed as “Started” or “Running” in the **Status** column:
   - **Analytics Exchange Service**: runs on AX Server and each instance of AX Engine Node
   - **AX Connector**: runs only on AX Server
   - **Analytics Exchange Database <*version number*>**: runs on the server where the PostgreSQL is installed

     This service may run on the same server as AX Server, or on a separate server. The service is present only if PostgreSQL is the database server for AX Server

   If any of the services have not started, you can try to start them by right-clicking the service and selecting **Start**. If the service still does not start, check the log file to determine the cause of the problem or contact ACL Support Services.

Checking the AX Server applications

Check the deployment status of the AX Server applications from the Tomcat Web Application Manager.

1. From a web browser, navigate to `http://server_name/manager` and log in to the Tomcat Web Application Manager.

Replace *server_name* with the hostname or IP address of the server hosting AX Server or the AX Engine Node instance.

> **Note**
>
> Your Tomcat Web Application Manager credentials are specified during the AX Server installation. If you cannot remember your credentials, reset them.

2. Confirm that the following applications display the **Running** status as **true** on AX Server:
   - Analytics Exchange (AX) Server *<version number>*
   - AX Webclient *<version number>*
   - AX System Admin *<version number>*
   - AX Core Server *<version number>*
   - AX Central Authentication System (CAS) *<version number>*
   - AX Gateway Mapper *<version number>*
   - AX Light Client *<version number>*
   - Tomcat Host Manager Application
   - Tomcat Manager Application
   - AX Core REST Interface *<version number>*
   - Apache TomEE

   If any of the applications have not started, in the **Commands** column, click **Start**.
3. Exit the Tomcat Web Application Manager.

Activate AX Server

You can activate your AX Server online using the AX Server Configuration or offline using Launchpad.

> **Note**
>
> You must have a valid Launchpad account with the appropriate permissions to activate AX Server. If you do not have an Launchpad account, contact your ACL account administrator.

Renewing a subscription?

If you are renewing an expired subscription, you must deactivate and then reactivate your instance of AX Server to complete the renewal process. For information about deactivating the server, see Deactivate AX Server.

Online activation

1. Sign in to the AX Server Configuration web application (`https://<server-name>/aclconfig`) and locate the **Activation** panel.
2. From the **Server Type** list, select one of the following:
   - **Production**: the primary production server
   - **Non-Production**: the server used for non-production purposes such as testing and staging
   - **Disaster Recovery**: the server designated for disaster recovery or failover
3. In **Activation**, enter your Launchpad credentials and click **Select Org**.
4. From the **Organizations** list, select the organization the server belongs to and click **Activate Server**.

   Result: After the identification file imports, `The server has been activated` displays.

Offline activation

1. Sign in to the AX Server Configuration (`https://<servername>/aclconfig`) web application and locate the **Activation** panel.
2. From the **Server Type** list, select one of the following:
   - **Production**: the primary production server
   - **Non-Production**: the server used for non-production purposes such as testing and staging
   - **Disaster Recovery**: the server designated for disaster recovery or failover
3. In **Offline Activation**, click **Generate** and save the machine identifier file `AXOfflineActivation.mif` on your local workstation.

Your local workstation must have an Internet connection to access Launchpad and complete the rest of the activation.

4. Sign in to Launchpad (www.aclgrc.com) and select your organization.
5. Select **Options > Activations** and on the left-hand side, click **Offline Activation**.
6. Upload your activation file:
   a. Click **Choose File**, browse to your server machine identifier file `AXOffLineActivation.mif` and click **Open**.
   b. From the Application drop-down list, select the AX Server installation type.
   c. From the **User** drop-down list, select your name and then click **Upload**.

      Result: Once the machine identifier file uploads, the machine name of the server appears in the Activations list.
7. Next to the name of the activated server, click **Download Activation File** and save the activation file `analytics_exchange_server.oaf` on your local workstation.
8. From the AX Server Configuration web application, in the Offline Activation section, browse to the activation file that you downloaded from Launchpad and click **Import**.

   Result: After the identification file imports, `The server has been activated` displays.

Add an AX Server administrator

Use the AX Server Configuration web application to add an administrative user. The user is granted the Administrator role.

> **Note**
>
> You must add at least one administrative account after installing AX Server to use AX Client. Once you add the first user, you can use AX Client to add more users.

1. In a web browser, navigate to `https://<servername>/aclconfig` and log in to the AX Server Configuration web application.

   Use the same credentials that you use to log in to the Tomcat Web Application Manager.

2. Locate the **Add AX administrator** panel, and enter the name of the Windows user account to add:
   - If the user account belongs to the default Active Directory domain for your Analytics Exchange implementation, you can enter the user name without specifying the domain.

     The default domain for AX Server is specified in the **Settings** section of the **Server** panel.
   - If the user account does not belong to the default Active Directory domain, you need to specify the domain and the user name using the following format: **`Domain\username`**
   - If the user account is a local Windows user account on the server where AX Server is installed, you need to specify the computer name and the user name using the following format: **`ComputerName\UserName`**
3. Click **Add Administrator**.

Configure the Archive and Restore data directory

Configure the Archive and Restore data directory to make the Archive and Restore commands available to end-users with application Administrator rights in AX Client.

> **Note**
>
> If the directory is not configured, the Archive and Restore commands are disabled in AX Client.

1. In a web browser, navigate to `https://<servername>/aclconfig` and log in to the AX Server Configuration web application.

   Use the same credentials that you use to log in to the Tomcat Web Application Manager.

2. In the **Server** section, in the **Archive and restore data directory** field, enter the file path or UNC path to the directory where you save archived collections.

   You must specify a folder that already exists. A UNC path is a shared folder that is specified using the following format: `\\<server_name>\<shared_folder>`.

   The user account used to run the Analytics Exchange Service must have Full Permissions for the folder you configure as the Archive and Restore data directory. You must manually assign the required security rights in Active Directory.

   > **Note**
   >
   > The data directory can either be located locally on AX Server, or on a remote file server or storage-area network (SAN). You must ensure that the specified location has enough disk space allocated to store your archived collections based on the size of collections stored in AX Server, including analytic job results, and your organization's archiving policies.

3. To save your changes, click **Update** at the bottom of the **Server** section.

Verifying client application connections

Check that local and any remote users can connect to AX Server using AX Client, ACL Analytics, and AX Web Client after installing AX Server and any instances of AX Engine Node.

Prerequisites

At the locations that users will connect from:

- install AX Client
- install ACL Analytics

Application connection checks

Check	Details
Start AX Client and connect to AX Server.	If you are unable to log in, confirm the following settings: ◦ If the user account you are logging in with does not belong to the default Active Directory domain specified for AX Server, you must specify the domain when you log in. For example: `DomainName\Username` ◦ The **Server** settings specified in the **Options** dialog box must match the settings required by AX Server. ◦ If a firewall is present on the client computer where AX Client is running, ensure that the required ports are open for outbound communication. By default, the required port is 443 (Tomcat Connector HTTPS). Port 10000 (AX Connector) must also be open if ACL Analytics is being used.
Export a table from AX Server that has a source data file stored on AX Server.	a. When you select the table, check that the **Data source** property specifies "Data source is managed by AX Server". b. In the **Export** dialog box, make sure that **Work with the exported file(s)** is selected, and **Export data files along with selected definitions** is deselected (the default settings). c. If you are able to open the table in ACL Analytics after entering the server profile password, then AX Connector is configured correctly. d. If you are not able to open the server table, see "Assigning rights for the AX Connector service" on page 77 for instructions on completing the additional security configuration that may be necessary. When you import an *ACL* project or an analytic into AX Server, and select **Import source data files (.fil files)**, any tables in the project are converted into server tables and the associated *ACL* data files (.fil) are copied to AX Server. Server tables are accessed using AX Connector.
Launch the Help	If HTTP requests from the client computer are redirected to a proxy server, attempts to access the

Check	Details

system by selecting **Help > Contents**.	Help system may fail. You can specify the correct IP address and port for the proxy server by adding the following two lines to the `ACLAnalyticsExchange.ini` file in the folder where AX Client is installed. The default location is `C:\Program Files\ACL Software\ACL Analytics Exchange Client`.
	`-Dhttp.proxyHost=<proxy_server_hostname_or_ip>`
	`-Dhttp.proxyPort=<proxy_server_port>`
	For example:
	`-Dhttp.proxyHost=192.168.5.190`
	`-Dhttp.proxyPort=3128`

Configuring Python for use with AX Server

To configure Python to work with AX Server, you must install the correct version of Python, add the Python executable to your system PATH environment variable, and set the PYTHONPATH system environment variable on each machine that hosts an instance of AX Server or AX Engine Node.

How it works

To run Python scripts, Analytics Exchange must be able to call the Python executable and find the scripts it is instructed to run. AX Server uses the PATH environment variable to locate Python and the PYTHONPATH environment variable to locate scripts.

Install Python version 3.5.x (32-bit)

> **Note**
>
> You must complete these steps on every machine that hosts an instance of AX Server or AX Engine Node.

1. From the Python downloads page, download the latest version of Python 3.5 to your machine.
2. On your machine, double-click the installer.
3. In the installer, select **Add Python *versionNumber* to PATH**.
4. Click **Install** and follow the on-screen instructions.
5. Reboot the machine before running any Python scripts from ACL.

Set the PYTHONPATH environment variable

> **Note**
>
> You must complete these steps on every machine that hosts an instance of AX Server or AX Engine Node. The user account that runs the Analytics Exchange Service must have permission to access the folder(s) in your PYTHONPATH environment variable.

1. In your Windows operating system, create one or more folders to house your Python scripts.

   Example –`C:\python_scripts`.

2. From your Windows operating system, open the **System Properties** dialog box and click **Environment Variables**.
3. In the **System variables** section, click **New** and enter the following:
   - **Variable name** –**`PYTHONPATH`**
   - **Variable value** – enter the full path to the folder(s) you created to house the Python scripts

     Separate multiple folder paths with a semi-colon: `C:\python_scripts;C:\dev;C:\tmp`.

4. To save the variable, click **OK** and then in the **System Properties** dialog box, click **OK**.

Installing AX Engine Node (optional)

Install AX Engine Node for PostgreSQL

Install AX Engine Node to increase the analytic processing capability of Analytics Exchange. AX Engine Node is hosted on a separate server from AX Server.

Install AX Engine Node

> **Caution**
>
> You must install the KB2919355 Windows Updates before starting your Analytics Exchange installation on Windows Server 2012 R2. If you do not install this update, your Analytics Exchange installation cannot succeed.

Run the installer and select your database configuration

1. Double-click the installation package and if a security warning dialog box appears, verify the information listed and click **Yes**.
2. Select the setup language and click **OK**.
3. In the **Setup Extraction Location** page, specify the folder where the installation files will be extracted, and click **Install**.

   > **Tip**
   >
   > Click **Browse** to select a folder or accept the default location: `C:\Program Files (x86)\ACL Software\Installers\ACLAX<version>_EngineNode_<edition>`.

4. In the **Analytics Exchange Server Setup Options** page, select **PostgreSQL** and click **Next**.
5. If you are prompted to install prerequisites, click **Install** and wait while the prerequisites are installed.

   Follow any on-screen instructions to complete the prerequisite setup.

Configure your database service

1. In the **Welcome** page, click **Next** and in the **License Agreement** page, select **I accept the terms in the license agreement** and click **Next**.
2. In the **Destination Folders** page, specify where the AX Engine Node application files will be installed and the working directory for analytic processing, and then click **Next**.

   If necessary, click **Change** to modify either, or both, of the default locations. The paths you specify must not include any spaces.

3. In the **ACL Analytics Exchange server information** page, enter the IP address of the server where AX Server is installed and click **Next**.

4. In the first **Analytics Exchange Server database connection settings** page, select **PostgreSQL** from the **Database Platform** options.
5. To encrypt the database connection, select **Encrypt database communications** and then click **Next**.

   To encrypt the connection, your database server must be configured for SSL connections.

   > **Tip**
   >
   > Encryption slows performance somewhat, so you should enable it only if data is being transferred between the database server and the application server over an unsecure network.

6. In the second **Analytics Exchange Server database connection settings** page, enter the following information:

Field	Description
Database Server	The IP address or server name of the server where the database server is located. If you are installing AX Server on the same physical server as PostgreSQL, keep the default value of `localhost` unless you have a reason to change it.
Port	The port to use to connect to the PostgreSQL database. The default port is 5432.
Superuser	The name of the PostgreSQL Superuser account. Leave the default value of `postgres` unless you have a reason to change it.
Password	The password for the Super user account.

Configure the application service account and security

1. In the **Analytics Exchange Tomcat Service Account** panel, do the following and click **Next**:
   a. Enter the domain and username for the account in the format `domain\username`, or click **Browse** to locate the required domain and username.

      If you browse for the account name, you must enter or select the domain or server name first in the **Browse for a User Account** dialog box in order for the installer to present the appropriate list of available user accounts.

      > **Note**
      >
      > Using a local user account to run the TomEE service is not supported. These accounts do not have the appropriate privileges to run some *ACL* commands.

   b. Enter the **Password** for the account.
   c. Click **Next**.
   d. If you are prompted to grant the "Log on as a service" right to the Tomcat service account, click **Yes** and then **OK**.

For information on the options for configuring service accounts, see "Service account configuration" on page 73.

2. In the **SSL certificate information** page, enter the following information to create a self-signed security certificate to secure HTTPS connections to the AX Engine Node and then click **Next**:

Field	Description
Server name	The hostname of the database server. For example: `ax.acl.com`.
Department or division name	The division or business unit that the certificate is being issued for. For example: `Development`.
Organization Name	The name of your company or organization. For example: `ACL Services Ltd.`.
City Name	The city or locality where your company or organization is located. For example: `Vancouver`.
State/Province Name	The state or province where your company or organization is located. For example: `BC`.
Country code	The two-character country code for the country where your company or organization is located. For example: `CA`.
Keystore password	Enter a password of at least 6 characters. **Note** If you are using an existing keystore file, this instance of the **Keystore password** text box is disabled.
Private key password	Enter the same password again. The **Keystore password** and the **Private key password** must be identical.

For information about how this certificate is used, and for configuration options, see "Security certificates" on page 51.

Finish the installation

1. Click **Install**.

> **Note**
>
> Before the installation process completes you are required to wait for about a minute while the TomEE application server becomes fully functional. The command window may appear intermittently during this period. **Do not cancel the installation.**

2. When the installation process is complete, click **Finish** to exit the installer.

Postrequisites

- "Configuring a shared data folder" on the next page
- "Configuring AX Engine Nodes" on page 47

Configuring a shared data folder

To store data files on a separate server from AX Server or to support AX Engine Node on one or more servers you must provide access to AX Server data files through a shared folder.

Using shared data folders

There are two common use cases for shared data folders:

- **external data storage** – you can store the data files on a server where there is more hard disk space available or on a network file server
- **AX Engine Node** – installations require a shared folder so that the analytic servers and AX Server can access data files.

Shared folder location

The shared folder must be accessible through a Windows UNC path with the following format: `\\ComputerName\SharedFolder` and be located either in a shared Windows folder or a Storage Area Network (SAN).

Required folder permissions

The Windows user account used to run the TomEE application server service on the AX Server and each AX Engine Node must have read and write permissions for the folder.

Any users that access AX Server tables using ACL Analytics must have read access permissions for the folder.

Configure a shared folder on Windows 2008

1. In Windows Explorer, right-click the folder you want to share and select **Share**.
2. In the **File Sharing** dialog box, select the users or groups you want to share the folder with.
3. Check the permissions assigned to each user or group, and click the drop-down list beside each entry you want to modify the permissions for and select the appropriate permissions.
4. Click **Share** and then click **Done**.

Configuring AX Engine Nodes

Use one or more instances of AX Engine Node to run analytics across multiple servers and increase processing power.

How it works

Increasing processing power

By default, analytics are processed directly on AX Server. Although this works in most cases, you may require more processing power when:

- you want to run anlaytics requiring high processing power
- you want to run a number of analytics in a short span of time

To increase processing power, you can configure one or more instances of AX Engine Node and run your analytics on these separate servers.

Balancing multiple nodes

When a node has space in its queue, it notifies AX Server that it can process jobs and the server then assigns jobs to that node. As a result, running multiple AX Engine Nodes that are allowed to handle several jobs simultaneously can cause one node to handle multiple jobs while others sit idle.

To ensure jobs are balanced across nodes, configure the maximum number of jobs each node can process as `1` and schedule analytic jobs accordingly.

Setting up AX Engine Nodes

Prerequisites

Before you add and configure an AX Engine Node in the AX Server Configuration web application, you must:

- configure your system so that AX Server data files are stored in a shared folder which is accessible using a UNC path (e.g. `\\server_name\shared_folder`). For more information, see "Configuring a shared data folder" on the previous page
- physically install and configure each instance of AX Engine Node on a server

Add an AX Engine Node

1. Sign in to the AX Server Configuration web application and locate the **Engine Nodes** panel.

2. In the **Add Engine Node** panel, enter the following information:
   - **New Engine Node IP address or computer name**: the hostname or IP address of the server where the AX Engine Node is installed
   - **Jobs (max)**: the maximum number of analytic jobs that the engine node can process at one time

     > **Note**
     >
     > Jobs are queued until the number of concurrently running jobs falls below the maximum.

3. Click **Add Engine Node**.
4. Click **Update Engine Node Settings**.

Result: The AX Engine Node is used to process analytics. If it is the first AX Engine Node, processing is transferred from AX Server to the new node. If you added multiple AX Engine Nodes, scheduled jobs are distributed among them.

Configuring AX Engine Nodes

From the **Engine Nodes** panel of the AX Server Configuration web application, you can edit the configuration settings of any AX Engine Node you have added.

When you edit a value, click **Update** to save the change.

Individual AX Engine Node settings

- Enabled/disable an engine node
- Change the Hostname or IP address
- Change the max jobs
- Remove an engine node

Global AX Engine Node settings

> **Note**
>
> These settings apply to all instances of AX Engine Node and all analytics that run on the server(s).

You can copy data files to each AX Engine Node instance before analytics are processed using the **Copy analytic data to engine node** setting:

- **Yes**: data files from the analytic folder of AX Server are copied to the analytic job directory of the AX Engine Node before processing starts
- **No**: data files remain in the analytic folder of AX Engine Node and are not copied to the job directory of the AX Engine Node before processing starts

Copy data files	Do not copy data files
Improves performance when data files are repeatedly accessed across the network	Improves performance when a small number of analytics run simultaneously
Improves performance when running multiple analytics simultaneously or if a single analytic runs several commands on large data files	Improves performance when the time to copy data files outweighs the time you can save by by writing your analytics so that, whenever possible, analytic commands are run locally on the AX Engine Node. For example: a. Write a command to select only the required records from the table the script opens remotely. b. Use the `EXTRACT` command with the `LOCAL` parameter specified to extract the records into a new table on the AX Engine Node instance. c. Run any additional commands on the local table.

Security certificates

Analytics Exchange installations require SSL security certificates. By default, a self-signed security certificate is installed, however you may replace this default certificate with a certificate issued by a third-party *certificate authority* (CA).

How it works

SSL certificates are used to establish a trusted, secure, encrypted connection between client applications and AX Server.

Both self-signed certificates and CA-issued certificates ensure that the data transferred between AX Server and client applications cannot be easily accessed by a third party, however when you purchase a CA certificate you gain additional trust because an independent, trustworthy certificate authority validates the server's authenticity.

Using self-signed certificates for AX Server

If you choose to use a self-signed certificate, each user that accesses the server encounters a warning page indicating that the security certificate was not issued by a trusted certificate authority. To stop this warning, each client user must verify that the certificate is issued by a trusted source by doing the following:

- install the self-signed certificate in their browser when connecting with AX Web Client
- select **Trust self-signed certificates** during installation or on the **Tools** menu in AX Client

> **Tip**
>
> Certificate installation is not typically required if you replace the self-signed certificate with a certificate purchased from a CA because Internet Explorer supports certificates issued by most CAs automatically. Using a CA certificate can therefore improve end user interaction with the server.

Replacing the certificate

To replace the default self-signed certificate, you must create a keystore, import the certificate, and then configure the TomEE application server to use the certificate. For more information, see "Installing security certificates for AX Server" on page 54.

> **Note**
>
> If the *Common Name* (CN) value specified in the security certificate changes when you replace the self-signed certificate, you must change the `cas.securityContext.casServerHost` property in the `aclCasClient.xml` configuration file to match the updated CN value on every server where Analytics Exchange server components are installed.
>
> If you used Integrated Windows Authentication and the CN value changes, you must also update the Internet Explorer settings on each client computer. For more information, see "Configuring Integrated Windows Authentication" on page 79.

AX Engine Node certificates

The certificate configured on each AX Engine Node is used to encrypt communications between the AX Engine Node and the Analytics Exchange database.

The self-signed certificate can be replaced with a certificate purchased from a CA, but because end-users do not access the AX Engine Node replacing the certificate is typically not required.

PostgreSQL connections

The certificate configured for PostgreSQL is used to encrypt communications between the database server and any Analytics Exchange servers that connect to the database:

- AX Server
- AX Engine Node
- AX Exception

When to use SSL for database connections

The certificate is only used if the applications connecting to the database have SSL turned on. Because of the performance cost associated with SSL, it should be turned off if it is not required. For example, if AX Server and the PostgreSQL are installed on the same computer, SSL should be turned off for the components installed on AX Server.

Replacing the certificate

The security certificate created by the PostgreSQL setup wizard during installation is a self-signed certificate. The server certificate must be in place for SSL connections to work, but the specific information in the certificate, such as the server name, is not validated. For this reason, replacing the installed self-signed certificate with a CA-issued certificate is typically not required.

ACL Connector for Analytics Exchange connections

The ACL Connector for Analytics Exchange does not require an SSL connection, however it does support SSL encryption if you choose to enable it.

The connector relies on different technology and protocols than AX Server, and therefore does not use the same security certificate configuration or tool set that is required when encrypting other AX Server communication.

To support SSL encryption, you must generate and install a set of security certificates on the AX Server machine using OpenSSL. When SSL is enabled, the connector uses OpenSSL to encrypt all data moving across the network connection.

For more information, see "Installing security certificates for the ACL Connector for Analytics Exchange" on page 58.

Installing security certificates for AX Server

Install a certificate from a *Certificate Authority* (CA) to replace the default self-signed certificate used to secure the SSL connection between AX Server and client applications.

Tools and prerequisite knowledge

This task requires you use Oracle's keytool utility for managing keys and certificates. For more information about the keytool utility, see the Oracle keytool documentation.

To successfully complete this task, you should also be comfortable working with *security certificates* and Java *KeyStore* technology:

- **Security certificate** – an electronic document used to prove the ownership of a public key. The certificate includes information about the key, information about its owner's identity, and the digital signature of an entity that has verified the certificate's contents are correct. For more information, see "Security certificates" on page 51
- **Java KeyStore** – a repository of security certificates plus corresponding private keys used for in SSL encryption. For more information, see Oracle: Creating a KeyStore

Backup the TomEE application server configuration before you start

1. In Windows Explorer, open the `TomCat\conf` sub-folder in the directory where you installed the Analytics Exchange server application you are updating the keystore configuration for.
2. Copy the `conf\tomee.xml`, `conf\server.xml`, and `conf\system.properties` files to a safe backup location.

   If you run into any issues while you are configuring the security certificate, you can restore your original configuration by stopping the Analytics Exchange Service, restoring these files, and then restarting the service.

Server-side process

> **Tip**
>
> Add the Java `bin` subdirectory to your OS PATH environment variable so that you can use the keytool command without specifying the full path. To add the subdirectory to the path for your session, execute `Set PATH=<java_bin_path>;%PATH%`.

Create a new keystore

1. Open a command prompt on the server.
2. Use the following syntax to create the new keystore:

   keytool -genkeypair -alias <*alias*> -keyalg RSA -keystore <*keystore_filename*>

   Example – keytool -genkeypair -alias AX_store -keyalg RSA -keystore myAxKeystore
3. Answer each question when prompted:

Field	Example
What is your first and last name? **Note** You must enter the hostname of your AX Server instance for this question.	axserver.ax.com
What is the name of your organizational unit?	Purchasing
What is the name of your organization?	ExampleCompany
What is the name of your City or Locality?	Cupertino
What is the name of your State or Province?	CA
What is the two-letter country code for this unit?	US
Is <CN=axserver.ax.com, OU=Purchasing, O=ExampleCompany, L=Cupertino, ST=CA, C=US> correct?	y

   Press **Enter** to use the same password as the keystore or specify a new password and press **Enter**.

Generate a Certificate Signing Request (CSR) on the new keystore

> **Note**
> Skip this section if you are using an existing certificate.

If you purchased your security certificate from a commercial CA, such as VeriSign, consult the documentation they provide for information on configuring your keystore. Create a CSR using the following syntax:

keytool -certreq -alias <alias> -keyalg RSA -file <csr_output_file> -keystore <*keystore_filename*>

Result – You now have a file that you can use to request a certificate from a certificate authority.

Import your CA certificate into the keystore

If your certificate is in a format such as PKCS12 that cannot be imported into a keystore, and you cannot convert it to the PEM format, contact ACL Support Services for assistance with configuring the

certificate in Tomcat.

1. Depending on the CA you are using you may need to import an intermediate certificate and/or root certificate into your keystore. Use the following syntax to import one or both of these certificates:

   `keytool -import -alias <alias> -keystore <keystore_filename> -trustcacerts -file <certificate_filename>`

   If you are importing both certificates the *alias* specified for each certificate should be unique. You need to first import the root certificate, and then run the `keytool` command again to import the intermediate certificate.

2. Use the following syntax to import your security certificate:

   `keytool -import -alias <alias> -keystore <keystore_filename> -trustcacerts -file <certificate_filename>`

   The *alias* specified must be the same value specified when you generated the keystore. The imported certificate will replace the default self-signed certificate created in the keystore.

3. Copy the keystore file to the `App\keystores` sub-folder.

Configure the TomEE application server to use the certificate

1. Locate `server.xml` in the `TomCat\conf` sub-folder and open it in a text editor.
2. Update the following settings and then save and close `server.xml`:
   - **keystoreFile** – the name and path to the keystore file you created in the following format: `C:\ACL\App\keystores\<your_keystore_name>`
   - **keystorePass** – the password you specified for the keystore when you created it. The password must be enclosed in double quotation marks (" ").
3. Locate `system.properties` in the `TomCat\conf` sub-folder and open it in a text editor.
4. Update the following settings and then save and close `system.properties`:
   - **javax.net.ssl.trustStore** – the name and path to the keystore file you created in the following format: `C:/ACL/App/keystores/<your_keystore_name>`

     > **Note**
     >
     > You must use the forward slash '/' character in the keystore path. If you use the backslash character '\' as is common in Windows environments, you will encounter server errors when logging in.

   - **javax.net.ssl.trustStorePassword** – the password you specified for the keystore when you created it
5. Restart the Analytics Exchange Service.

Client-side process

Import certificates into the AX Client machine Java cacerts file

This configuration must be completed on each end-user computer where AX Client is installed if you are using a certificate without a root certificate in the `cacerts` file by default.

1. Open Windows Explorer and navigate to the `cacerts` file in the `jre\lib\security` sub-folder where AX Client is installed.

   The default location is `C:\Program Files (x86)\ACL Software\ACL Analytics Exchange Client\jre\lib\security`

2. Create a backup copy of the file before making any changes.
3. Depending on the certificates you receive from the Certificate Authority you are using, you may need to import an intermediate certificate and/or root certificate into the `cacerts` file. Use the following syntax to import one or both of these certificates:

   keytool -import -alias <*alias*> -keystore <cacerts_file> -trustcacerts -file <certificate_filename>

   If you are importing both certificates the *alias* specified for each certificate should be unique.

4. Type the password for the keystore at the **Password** prompt and press **Enter**.

   The default Java password for the `cacerts` file is **`changeit`**.

5. Enter **`y`** at the **Trust this certificate?** prompt and press **Enter**.

If necessary, install the certificate in the web browser on each computer that will access Analytics Exchange web applications.

> **Note**
>
> This is not necessary if the certificate is provided by a CA listed in the Trusted Root Certification Authorities list in Internet Explorer. Large commercial CAs, such as VeriSign, are included in this list.

Installing security certificates for the ACL Connector for Analytics Exchange

The ACL Connector for Analytics Exchange supports Secure Sockets Layer (SSL) encryption on the connections between client machines and AX Server. If SSL is enabled, the connector uses OpenSSL to encrypt all data moving across the network connections between client machines and the server.

To configure SSL using certificates, you must generate a set of SSL certificates on the server machine. You can generate one of the following certificate types for the SSL connection:

- Self-signed certificate
- Certificate Authority (CA) certificate

Before you begin

Download and install OpenSSL and then add the path to the `openssl.exe` executable to your `PATH` environment variable.

> **Note**
>
> Like many open source software projects, the OpenSSL project does not distribute any code in binary form. Instead you must download the project source code and build the binary or locate a binary that is distributed for your operating system from a third-party source.
>
> For more information, see the OpenSSL documentation.

Generating an SSL certificate for self-signing

Use OpenSSL to generate a key file and certificate file on the server machine. Self-signed certificates are useful during development or testing, when you do not need to purchase a commercial certificate.

Show me how

1. Open a command prompt and then create the `C:\newcerts` directory.

   ```
   md C:\newcerts
   ```

2. Change to the new directory and generate a server key file and server certificate file.

```
cd C:\newcerts
openssl req -x509 -newkey rsa:4096 -keyout server-key.pem -out server-cert.pem -days 365 -
nodes
```

You are prompted for information which is incorporated into the certificate, such as Country, City, Company Name, and so on. Make a note of the information you enter as you may get prompted for this information again at a later stage.

> **Note**
>
> The `-nodes` argument removes password-protection for the private key so you do not need to enter a password when you restart the server.

Result – the self-signed certificate is created. You require `server-key.pem` and `server-cert.pem` during the installation of the ACL Connector for Analytics Exchange on the AX Server machine. Client users do not require a certificate file when using this option.

Generating an SSL certificate with a Certificate Authority (CA)

Like self-signed certificates, Certificate Authority (CA) certificates ensure no third-party can easily access the connection. However, CA certificates provide additional trust because an independent, trustworthy certificate authority validates the server's authenticity.

Show me how

Create the server private key

1. Open a command prompt and then create the `C:\newcerts` directory.

   ```
   md C:\newcerts
   ```

2. Change to the new directory and generate a new key.

   ```
   cd C:\newcerts
   openssl genrsa -out server-key-withPass.pem
   ```

3. Generate a certificate signing request.

   ```
   openssl req -new -key server-key-withPass.pem -out signingReq.csr
   ```

   You are prompted for information which is incorporated into the certificate, such as Country, City, Company Name, and so on. Make a note of the information you enter as you may get prompted for this information again at a later stage. When asked for an email address, provide a valid email address so that the Certificate Authority can send the certificate via this address.

4. Verify the information in the `signingReq.csr` file and then send the file to the Certificate Authority as a request.

Result – if the request is successful, the Certificate Authority sends you a certificate using the email address you provided in the signing request. The email you receive includes an encrypted CA certificate and a link to an encrypted CA intermediate certificate.

Copy both certificates to a text file, with the non-intermediate certificate followed by the intermediate certificate and then save the file as `CA-cert.pem`. You require this file for the following section.

Create and sign the server certificate

1. Gather the following files that were generated in the previous section and copy the three files to `C:\newcerts`:
   - `server-key-withPass.pem`
   - `signingReq.csr`
   - `CA-cert.pem`
2. Open a command prompt and change to `C:\newcerts`:

   ```
   cd C:\newcerts
   ```

3. Create the server certificate:

   ```
   openssl CA -in signingReq.csr -out server-cert.pem -keyfile server-key-withPass.pem -days 365 -cert CA-cert.pem
   ```

4. Remove the password from `server-key-withPass.pem` so that you are not required to enter a password when restarting the server, and generate the final server key file (`server-key.pem`).

   ```
   openssl rsa -in server-key-withPass.pem -out server-key.pem
   ```

   > **Caution**
   >
   > Once you remove the requirement for the password, the certificate can be copied and used elsewhere. Therefore, once you remove the password requirement, you must take adequate precautions when storing the file. Ensure that the permissions are set to only allow access to those who need it.

Result – the server certificate is created and signed.

Distributing the SSL certificates

Once you generate a self-signed or CA certificate, you have a full set of SSL certificates that you can distribute:

- **the CA-cert.pem file** – required by any client to connect to the ACL Connector for Analytics Exchange over SSL using a Certificate Authority certificate
- **the Server Key file (server-key.pem) and the Server Certificate file (server-cert.pem)** – required when you run the ACL Connector for Analytics Exchange installer on AX Server if you want to enable SSL

Appendix

This appendix contains additional topics you may need to complete the procedures in this document.

AX Server requirements

For best AX Server performance, ensure your hardware and software meets the minimum requirements. Satisfactory production environment performance may require greater resources than the minimum specification.

Hardware

Processor, memory, and hard disk requirements for production systems depend on the following factors:

- the number of concurrent users and their usage profiles
- the size of the data payload
- the desired response time

Component	Minimum	Recommendation
Processor	2.5 gigahertz (GHz)	Quad-core processor (or two Dual-core processors) at 3.5 GHz or higher
Memory (RAM)	8 GB	16 GB or higher
Hard disk	100 GB This is the approximate amount of disk space required to download, extract, and install the pre-requisites. (AX Server is 4.5 GB)	200 - 500 GB Data storage requirements vary by the number of types of audit tests performed and the volume of transactions. Smaller implementations typically require 50GB per year, while larger implementations may require up to 500GB per year. For use in production, high-speed disk access and throughput is recommended.
Other	TCP/IP connectivity. The ability to connect to Launchpad is required during online server activation.	

Software

> **Caution**
>
> You must install the KB2919355 Windows Updates before starting your Analytics Exchange installation on Windows Server 2012 R2. If you do not install this update, your Analytics Exchange installation cannot succeed.

Software requirement	Minimum	Recommendation
Operating system		
◦ Windows Server 2016 ◦ Windows Server 2012 R2 ◦ Windows Server 2008 R2 Enterprise Edition (64 bit) **Note** Apply all critical Windows updates before installing AX Server. Running Windows Server 2012 using the Server Core (no GUI) option is not supported.	Windows Server 2008 R2 Enterprise Edition (64 bit)	Windows Server 2016
Web browser		
◦ Chrome ◦ Firefox ◦ Internet Explorer	Internet Explorer version 11	Latest version of Chrome
Optional integrated programming languages		
◦ Python programming language ◦ R scripting language When installing Python, you must also configure it to run on your system. For more information, see "Configuring Python for use with AX Server" on page 38. Depending on the R CRAN packages you intend to use, you may need to add the R `i386` 32-bit binary folder to your `PATH` environment variable. **Note** You must install the requirements to use integrated Python or R functions in your analytics. If you do not intend to use these languages, you do not need to install them.	◦ Python 3.5.x (32-bit) ◦ R 3.3.1 (32 or 64-bit depending on Operating System)	◦ Python 3.5.x (32-bit) ◦ R 3.2.3 or 3.2.5 (32 or 64-bit depending on Operating System)
To use the *ACL* Connector for Oracle, you must install: ◦ Oracle Instant Client 11g or 12c	◦ You do not need to install Oracle Instant Client if you do not intend to use the *ACL* Connector for Oracle ◦ The bitness of Oracle Instant Client must match your operating system's bitness. If the 32-bit Instant Client is installed on a 64-bit machine, the connection fails	N/A

Software requirement	Minimum	Recommendation
	◦ If you install the Oracle Instant Client after AX Server, you must restart the Analytics Exchange Service before you can use the connector ◦ If you are using Oracle as the database server for AX Server, you must also install Instant Client on the machine that hosts the database server, see "Database server" on the facing page	

Automatically installed prerequisites

The following prerequisites are automatically installed by the AX Server setup wizard if the required software is not detected:

- Oracle Java Runtime Environment 8 (JRE 8u121)
- Apache TomEE 7.0.2
- Java Cryptography Extension for Java 8
- Microsoft Access Database Engine 2010 SP2
- Microsoft .NET Framework 4.6.2

> **Note**
>
> If your computer already has .NET 4.6.0 or NET 4.6.1, the application uses the installed version of .NET and does not install 4.6.2.

- Microsoft Visual C++ 2015 Redistributable (x64 and x86)
- MSXML SDK 2.5

ACL data connectors

The ODBC drivers listed below are installed for use as ACL data connectors:

Driver name	File name	Version
ACL Connector for Amazon Redshift	`AmazonRedshiftODBC_sb64.dll`	1.1.6.1009
ACL Connector for Cassandra	`CassandraODBC_sb64.dll`	2.4.1.1001
ACL Connector for Concur	`ConcurODBC_sb64.dll`	1.1.1.1002
ACL Connector for Couchbase	`CouchbaseODBC_sb64.dll`	1.1.0.1000
ACL Connector for Drill	`DrillODBC_sb64.dll`	1.2.4.1004
ACL Connector for DynamoDB	`DynamoDBODBC_sb64.dll`	1.0.1.1000

Driver name	File name	Version
ACL Connector for Google BigQuery	GoogleBigQueryODBC_sb64.dll	2.0.2.1005
ACL Connector for HBase	HBaseODBC_sb64.dll	1.1.0.1000
ACL Connector for Hive	HiveODBC_sb64.dll	2.1.5.1006
ACL Connector for Impala	ImpalaODBC_sb64.dll	1.2.5.1005
ACL Connector for MongoDB	MongoDBODBC_sb64.dll	2.2.1.1001
ACL Connector for Oracle	OracleODBC_sb64.dll	1.1.1.1019
ACL Connector for Salesforce	SFODBC_sb64.dll	1.2.5.1017
ACL Connector for Spark	SparkODBC_sb64.dll	1.1.5.1005
ACL Connector for SQL Server	SQLServerODBC_sb64.dll	1.3.6.1022
ACL Connector for Teradata	tdataodbc_sb64.dll	1.0.0.1003
	Note The 32-bit versions of the drivers have `32` instead of `64` in the file name.	

Prerequisites included in Windows server

The following prerequisites are included in a default Windows server installation. The versions listed are the minimum requirement and most OS installations include later versions:

- Microsoft Core XML Services (MSXML) 6.0
- Microsoft Data Access Components (MDAC) 2.8
- Microsoft Jet 4.0

Database server

AX Server supports two database platforms, Oracle and PostgreSQL.

If your organization is implementing both AX Server and AX Exception the supported configurations are:

- both application databases using Oracle
- configuring the AX Server to use PostgreSQL as the database and Microsoft SQL Server as the AX Exception database

Software requirement	Minimum	Recommendation
One of the following Oracle versions if Oracle is selected as the Analytics Exchange database platform: ◦ Oracle 12c ◦ Oracle 11gR2 **Note** The server Oracle is installed on must meet the hardware requirements specified by the database vendor. You must also install Oracle Instant Client 12.1 if you intend to use AX Connector direct database access.	Oracle 11gR2	Oracle 12c
PostgreSQL 9.3.9 if PostgreSQL is selected as the Analytics Exchange database platform. **Note** • If PostgreSQL is installed on the same server as AX Server, meeting the AX Server hardware requirements is sufficient. If PostgreSQL is installed on a separate server a 64-bit dual CPU, 64-bit operating system, and 2 GB of memory are recommended for production use. • The PostgreSQL version included with the AX Server setup wizard is 9.3.9, however PostgreSQL is tested and supported up to version 9.3.13.	PostgreSQL 9.3.9	PostgreSQL 9.3.9

AX Engine Node requirements

For best AX Engine performance, ensure your hardware and software meets the minimum requirements. Satisfactory production environment performance may require greater resources than the minimum specification.

Hardware

Processor, memory, and hard disk requirements for production systems depend on the following factors:

- the number of concurrent users and their usage profiles
- the size of the data payload
- the desired response time

Component	Minimum	Recommendation
Memory (RAM)	8 GB	16 GB or higher
Hard disk	3.5 gigabytes (GB) This is the approximate amount of disk space required to download, extract, and install the prerequisites and AX Engine Node.	10 GB or higher For use in production, high-speed disk access and throughput is recommended.
Other	Network connectivity to AX Server.	

Software

Software requirement	Minimum	Recommendation
◦ Windows Server 2016 ◦ Windows Server 2012 R2 ◦ Windows Server 2008 R2 Enterprise Edition (64 bit)	Windows Server 2008 Enterprise Edition R2 (64 bit)	Windows Server 2016

Software requirement	Minimum	Recommendation
Note You must install the **Windows Server 2012 R2 Update (KB2919355)** as a pre-requisite to installing the .NET Framework. Apply all critical Windows updates before installing AX Server. Running Windows Server 2012 using the Server Core (no GUI) option is not supported.		
Optional integrated programming languages		
◦ Python programming language ◦ R scripting language When installing Python, you must also configure it to run on your system. For more information, see "Configuring Python for use with AX Server" on page 38. Depending on the R CRAN packages you intend to use, you may need to add the R `i386` 32-bit binary folder to your `PATH` environment variable. **Note** You must install the requirements to use integrated Python or R functions in your analytics. If you do not intend to use these languages, you do not need to install them.	◦ Python 3.5.x (32-bit) ◦ R 3.3.1 (32-bit)	◦ Python 3.5.x (32-bit) ◦ R 3.2.3 or 3.2.5 (32-bit)
To use the *ACL* Connector for Oracle, you must install: ◦ Oracle Instant Client 11g or 12c	◦ You do not need to install Oracle Instant Client if you do not intend to use the *ACL* Connector for Oracle ◦ The bitness of Oracle Instant Client must match your operating system's bitness. If the 32-bit Instant Client is installed on a 64-bit machine, the connection fails ◦ If you install the Oracle Instant Client after AX Engine Node, you must restart the Analytics Exchange Service before you can use the connector ◦ If you are using Oracle as the database server for AX Server, you must also install Instant Client on the machine that hosts the database server, see "Database server" on page 67	N/A

Automatically installed prerequisites

The following prerequisites are automatically installed by the AX Server setup wizard if the required software is not detected:

- Oracle Java Runtime Environment 8 (JRE 8u121)
- Apache TomEE 7.0.2
- Java Cryptography Extension for Java 8
- Microsoft Access Database Engine 2010 SP2
- Microsoft .NET Framework 4.6.2

> **Note**
>
> If your computer already has .NET 4.6.0 or NET 4.6.1, the application uses the installed version of .NET and does not install 4.6.2.

- Microsoft Visual C++ 2015 Redistributable (x64 and x86)
- MSXML SDK 2.5

ACL data connectors

The ODBC drivers listed below are installed for use as ACL data connectors:

Driver name	File name	Version
ACL Connector for Amazon Redshift	AmazonRedshiftODBC_sb64.dll	1.1.6.1009
ACL Connector for Cassandra	CassandraODBC_sb64.dll	2.4.1.1001
ACL Connector for Concur	ConcurODBC_sb64.dll	1.1.1.1002
ACL Connector for Couchbase	CouchbaseODBC_sb64.dll	1.1.0.1000
ACL Connector for Drill	DrillODBC_sb64.dll	1.2.4.1004
ACL Connector for DynamoDB	DynamoDBODBC_sb64.dll	1.0.1.1000
ACL Connector for Google BigQuery	GoogleBigQueryODBC_sb64.dll	2.0.2.1005
ACL Connector for HBase	HBaseODBC_sb64.dll	1.1.0.1000
ACL Connector for Hive	HiveODBC_sb64.dll	2.1.5.1006
ACL Connector for Impala	ImpalaODBC_sb64.dll	1.2.5.1005
ACL Connector for MongoDB	MongoDBODBC_sb64.dll	2.2.1.1001
ACL Connector for Oracle	OracleODBC_sb64.dll	1.1.1.1019

Driver name	File name	Version
ACL Connector for Salesforce	`SFODBC_sb64.dll`	1.2.5.1017
ACL Connector for Spark	`SparkODBC_sb64.dll`	1.1.5.1005
ACL Connector for SQL Server	`SQLServerODBC_sb64.dll`	1.3.6.1022
ACL Connector for Teradata	`tdataodbc_sb64.dll`	1.0.0.1003
	Note The 32-bit versions of the drivers have `32` instead of `64` in the file name.	

Prerequisites included in Windows server

The following prerequisites are included in a default Windows server installation. The versions listed are the minimum requirement and most OS installations include later versions:

- Microsoft Core XML Services (MSXML) 6.0
- Microsoft Data Access Components (MDAC) 2.8
- Microsoft Jet 4.0

Service account configuration

AX Server uses three Windows services to perform most of the application functions on the server: Analytics Exchange Service, Analytics Exchange Connector, and Analytics Exchange Database.

Service names

Display name of the service	Service name
Analytics Exchange Service	TomEE
Analytics Exchange Connector	AXConnector
Analytics Exchange Database (AX Server installations that use a PostgreSQL database only)	ACL_AXDatabase

Analytics Exchange Service

The Analytics Exchange Service is installed on the AX Server and each AX Engine Node you configure.

Analytics Exchange Service user account

To assign a user account to run the Analytics Exchange Service, you must do one of the following:

- select an existing domain account
- create a new domain account

> **Note**
>
> Using a local user account to run the TomEE service is not supported. These accounts do not have the appropriate privileges to run some *ACL* commands.

Directory permissions for service account

The user account you choose must be able to access the **Data directory** and **Archive and restore data directory** folders specified in the AX Server Configuration web application.

The following permissions are required:

- **Data directory**: read and write permissions
- **Archive and restore data directory**: full permissions

> **Note**
>
> The AX Server installer assigns the required local permissions on the server to run the service. However, the permissions must be configured manually if the folder is on a different server, or if the user account does not have rights to the specified folder by default.

User accounts for multiple instances of Analytics Exchange Service

If your installation has multiple instances of the Analytics Exchange Service running on different servers, you should create a domain account with the rights required to run the service and access AX Server data before you perform any installation.

During each installation, specify that account to run the Analytics Exchange Service.

User accounts for Analytics Exchange Service with Direct Link

If the machine hosting AX Server or an instance of AX Engine Node also has a Direct Link installation, the user account must have permission to run the following executables:

- `saplogon.exe`
- `sapgui.exe`

> **Note**
>
> Without permission to run these executables, analytics that include Direct Link commands fail. You can assign Full Control permissions to the folder containing the executables. By default, the executables are at `C:\Program Files\SAP\FrontEnd\SAPgui`.

Analytics Exchange Connector

The AX Server installer configures the Analytics Exchange Connector service to use the Local System account. It is recommended that you use this default configuration.

Analytics Exchange Database

The PostgreSQL setup wizard configures the Analytics Exchange Database service with the local permissions on the server required to run the service.

During the installation, you can:

- use an existing local user account on the server
- have the installer create a new local user account
- specify a domain account

By default, the group that the PostgreSQL user account is part of is granted access to the program that controls the database (`pg_ctl.exe`), however you may restrict access to this program to just the specific account that runs the database service.

> **Note**
>
> You cannot use the built-in Local System account to run the service because the database server must access network resources, which the Local System account does not permit.

The Analytics Exchange Database service is installed on the server where PostgreSQL is installed, and it is only present if you use PostgreSQL as the database server.

Analytics Exchange authentication

Use form-based or integrated Windows authentication to validate user identity when logging in to Analytics Exchange applications.

Authentication types

Form-based authentication

For each new session in the Analytics Exchange client applications, users must enter a username and password into a login form:

- AX Client
- AX Web Client
- AX Exception

> **Note**
>
> A new session is established each time the AX Client is started or the AX Web Client is accessed from a new browser window.

Integrated Windows authentication

Analytics Exchange client application authentication is handled silently by the Windows operating system without prompting users for credentials. When an application launches, it uses the account credentials entered when the user logged into the operating system. If the authentication fails, the user is prompted for credentials on a login form.

> **Tip**
>
> Integrated authentication requires more setup work, but is ultimately more convenient for client application users.

Choosing an authentication method

Choose the type of authentication you are going to use when you set up AX Server. You can switch between the two authentication options at any time.

Assigning rights for the AX Connector service

If you are unable to open the table in ACL Analytics after entering the server profile password, and you have confirmed that the server profile is configured correctly, assign rights for the AX Connector service on the machine where AX Server is installed.

Each Analytics Exchange user must have these rights assigned. You can assign rights to individual user accounts or groups.

Assign read and write access to the AX Connector installation folder

1. Open Windows Explorer and navigate to the folder where AX Connector is installed.

   The default location is `C:\ACL\App\analytic_engine\aclse`.
2. Right-click the folder and select **Properties**.
3. Click the **Security** tab.
4. Add the user accounts or groups that will access AX Server and assign them the **Read** and **Write** permissions by selecting the appropriate checkbox in the **Allow** column.
5. Click **OK**.

Assign full control rights to the AX Connector executable (aclse.exe)

1. Open Windows Explorer and navigate to the folder where AX Connector is installed.

   The default location is `C:\ACL\App\analytic_engine\aclse`.
2. Right-click the `aclse.exe` file and select **Properties**.
3. Click the **Security** tab.
4. Add the user accounts or groups that will access AX Server and assign them the **Full Control** permission by selecting the checkbox in the **Allow** column.
5. Click **OK**.

Allow log on locally rights

1. To open the security policy settings, do one of the following:
   - If the server is not the domain controller, select **Start > Control Panel > Administrative Tools > Local Security Policy**.

- If the server is the domain controller, select **Start > Control Panel > Administrative Tools > Domain Security Policy** .

2. In the **Security Settings**, double-click **Local Policies > User Rights Assignment > Allow log on locally**.
3. If the server is a domain controller, ensure that the **Define these policy settings** checkbox is selected.
4. Add the user accounts or groups that will access AX Server.

Configuring Integrated Windows Authentication

Setup the Active Directory Domain Controller server, AX Server, and the desktop environment for each client application end user to configure Integrated Windows Authentication. Integrated Windows Authentication enables single sign-on access control for AX Client users.

> **Note**
>
> Integrated Windows Authentication is not supported for instances of AX Client running on the server's operating system. You must be connecting from a client operating system otherwise the application defaults to form-based authentication.

How it works

Integrated Windows Authentication uses the security features of Windows clients and servers. It does not prompt users for a user name and password, and the current Windows user information on the client computer is supplied by the web browser through a cryptographic exchange. The following protocols are used to manage authentication:

- **SPNEGO** – AX Client connections
- **Kerberos** – server profile connections to ACL Analytics

If the authentication exchange initially fails to identify the user, the web browser will prompt the user for a Windows user account user name and password.

Create an SPN account

Create a new Windows *Service Principal Name* (SPN) account in Active Directory to map the AX Server authentication service to an Active Directory account.

Show me how

1. On the Active Directory Domain Controller server, click **Start > All Programs > Administrative Tools > Active Directory Users and Computers**.
2. Right-click the domain entry in the treeview where you want to create the new SPN account and select **New > User**.
3. Enter the requested information and click **Next**.
4. Configure the user password and click **Next**:
   a. Enter the account password.
   b. Deselect **User must change password at next logon**.
   c. Select **Password never expires**.
5. Click **Finish**.

Map the authentication service to the SPN account

Map the AX Server authentication service to the Active Directory SPN account using the **ktpass** command.

Show me how

1. On the Active Directory Domain Controller server, open a command prompt and change directories to the directory where `ktpass.exe` is located.

   The default location is `c:\Program Files\Support Tools`.

2. To map the authentication service to the SPN account, enter the following keypass command:

   ```
   ktpass /out filename /princ name /pass password /mapuser local_username /ptype principal_type /crypto encryption_type
   ```

For ktpass syntax, see Microsoft Ktpass reference.

Example

The following example maps the authentication service to the SPN account using the **ktpass** command:

```
ktpass /out 'C:\ax.keytab' /princ HTTP/axserver.ax.com@AX.COM /pass pass1234 /mapuser AXSSO /ptype KRB5_NT_PRINCIPAL /crypto RC4-HMAC-NT
```

Register an SPN for the AX Connector service

Register an SPN for the AX Connector service using the **setspn** command.

Show me how

1. On the Active Directory Domain Controller server, open a command prompt and change directories to the directory where `setspn.exe` is located.

   The default location is `c:\Program Files\Support Tools`.

2. To register the SPN, enter the following setspn command:

   ```
   setspn -A ACLSE/full_domain_and_servername computer_name
   ```

   > **Note**
   >
   > ACLSE is the required value to identify AX Connector and must be entered in all caps. The *computer_name* value can be entered as name or domain\name.

3. Optional. To verify the mapping of the SPN account, use the following setspn command:

```
setspn -L computer_name
```

Example

The following example uses the setspn command to register the SPN:

```
setspn -A ACLSE/axserver.acl.com axserver
```

Test the SPN account mapping

Optionally, copy the keytab file to the AX Server instance and use the **kinit** command to test your SPN account mapping.

Show me how

Prerequisite: Add the Java `bin` subfolder to your *path* environment variable to use the **klist** command without specifying the full path.

```
set PATH=java_bin_path;%PATH%
```

1. On the Active Directory Domain Controller server, copy the `.keytab` file you created with the ktpass command and paste it in the `Windows` directory of AX Server.
2. In the `Windows` directory of AX Server, create a file called `krb5.ini`.
3. From the command prompt, usethe following command to verify that the keytab file can be read:

   ```
   klist -k
   ```

4. To attempt to authenticate, use the following command:

   ```
   kinit username@REALM.COM
   ```

5. Enter the user's password and press **Enter**.

Example

The following is an example of a krb5.ini file:

```
[libdefaults]
ticket_lifetime = 24000
```

```
default_realm = <domain>
default_keytab_name = <path_to_keytab_file>
dns_lookup_realm = false
dns_lookup_kdc = false
default_tkt_enctypes = rc4-hmac
default_tgs_encrypes = rc4-hmac [realms]
<domain> = {
 kdc = <adserver.domain.com>:88
}
[domain_realm]
<.domain> = <DOMAIN>
<domain> = <DOMAIN>
```

Enable Integrated Windows Authentication from Internet Explorer

Enable Integrated Windows Authentication from Internet Explorer in each end user's desktop environment. Users must be connecting from a client operating system, Integrated Windows Authentication is not supported for instances of AX Client running on the server's operating system.

Show me how

1. In Microsoft Internet Explorer, click **Tools > Internet Options > Advanced**.
2. Under the **Security** group, select **Enable Integrated Windows Authentication** and then click **Apply**.
3. Click the **Security** tab.
4. Select the **Local Intranet** icon and then click **Sites**.
5. In the **Local Intranet** dialog box, click **Advanced** and then enter the HTTPS URL for your AX Server instance and click **Add**.

   Example: `https://axserver.ax.com`.
6. Click **Close**, click **OK** in each open dialog box until the **Internet Options** dialog box closes and restart Internet Explorer.

The updated settings take effect the next time Internet Explorer is launched.

aclAuditExchange.xml

Stores global settings for AX Server.

Settings can be modified using the AX Server Configuration web application.

> **Note**
>
> You can modify most of these values from the AX Server Configuration web application. You should use the web application whenever possible to change AX Server settings because the values are validated before the `aclAuditExchange.xml` file is re-saved.

File settings

Key	Description	Corresponding Field in AX Server Configuration Web Application
allowExecCommand	Specifies how the scripting engine handles the EXECUTE command when encountered in an analytic: ◦ **yes**: the EXECUTE command is processed when encountered ◦ **no** (default): the EXECUTE command is ignored when encountered, a message is written to the log, but analytic does not fail > **Note:** The EXECUTE command is available in ACL Analytics version 10, or higher.	**Allow execute command?**
aclsePortNumber	The port number used to connect to the AX Connector service.	**Port Number**
allowExportData	Specifies whether AX Client users can download data files from AX Server to their workstation: ◦ **yes**: data export options in AX Client are enabled ◦ **no**: data export options in AX Client are disabled > **Note** This property is set to "yes" by default and should not be changed.	
AXHttpsPort	Specifies the port used for encrypted communications with the AX Server. The default value is 8443.	

Key	Description	Corresponding Field in AX Server Configuration Web Application
aclsePrefixPath	The file path where temporary files created by the AX Connector service are stored.	**Connector working directory**
AXHostname	Specifies the hostname of the AX Server. The value must be entered with uppercase characters. **Example:** `AXSERVER.ACL.COM`	**Server IP address or computer name**
aclseProfileName	The name of the server profile used to connect to AX Server server tables. **Note:** Use this field's default value unless you have a specific reason for changing it. By default, version 4.0.2 or higher uses `Analytics Exchange`. Version 4.0.0 uses `AuditExchange`.	
EmDataLoadUrlRoot	The web address used to connect to AX Exception.	**Data Upload URL**
useWhiteList	Specifies whether the file extension whitelist is enabled: ◦ **yes**: only files with specified white-listed file extensions can be uploaded or imported to AX Server ◦ **no** (default setting): files with any extension can be uploaded or imported to AX Server	**Enable whitelist**
mailHostServer	The IP address of the mail server to use to relay messages to specified users when an analytic chain fails.	**SMTP server address**
copyDataFiles	Specifies whether data files will be copied before analytic processing starts: ◦ **yes**: data files for the folder where the analytic is located will be copied to the analytic job subfolder before analytic processing starts ◦ **no**: analytics will be processed without copying data files **Note:** This setting is only applicable if you are using one or more engine nodes in your AX Server environment.	**Copy analytic data**
databaseLoadJobsPath	Specifies the location where temporary files are created before being uploaded to the database.	

Key	Description	Corresponding Field in AX Server Configuration Web Application
dataFilePath	The folder where AX Server data files are stored on the server. The default location is `C:\ACL\Data\repository\datafiles`.	**Data directory**
mailHostPassword	The password for the user account that can be used to send messages.	**SMTP password**
doesLinkSecurityUseMasterLocation	Specifies the type of application permissions that AX Client and AX Web Client users need to access linked tables, linked layouts, and linked analytics. Users always require permission to the folder containing the linked item and to the parent collection. This setting specifies the permission requirement for the master item: ◦ **yes**: users need permissions to the master item and its parent collection or collections ◦ **no**: users do not need permissions to the master item and its parent collection or collections	
mailHostUsername	Optional. The username of a user with the appropriate rights on the mail server to send email messages. **Note:** Depending on the configuration of the server this account may or may not need to be specified.	**SMTP user name**
fileTransferPath	The folder where data files are stored during file transfers.	**Server file transfer directory**
archiveRestorePath	Specifies the location where archived collections are stored.	**Archive and restore data directory**
emailOnFailureAddress	The email address to use as the "From" address in emails sent to users.	**sender email address**
trustETLserver	This property is not used in this release.	
resultsCleanupStartDate	Specifies a cutoff date for the results cleanup feature. No analytic jobs or associated results are deleted prior to the specified date, regardless of the **Results Cleanup** settings for an analytic. This property is set to 01/01/1900 by default.	**Start date for results cleanup**
useResultsCleanup	Specifies whether the **Results Cleanup** setting is enabled	**Enable results**

Key	Description	Corresponding Field in AX Server Configuration Web Application
	on the **Configuration** tab in AX Client: ◦ **yes**: users with full permissions for an analytic can configure auto-deletion of analytic jobs and associated results ◦ **no** (default): the **Results Cleanup** setting is disabled	**cleanup**
DefaultDomain	The Active Directory domain to use by default if a user does not specify a domain when they log in.	**Default Active Directory domain**
ServerType	Specifies the type of server activation.	**Server Type**
fileExtensionWhiteList	The list of file types that are allowed to be uploaded or imported to AX Server if the file extension whitelist is enabled.	**File extension whitelist**
mailHostPort	The port required to communicate with the mail server. **Note:** If you are using the default port of 25, this field may be left unset.	**SMTP port**
attachLogFiles	Whether or not to attach log files to the analytic fail notification email: ◦ **yes**: analytic log files are attached to email notifications of analytic failure ◦ **no** (default): analytic log files are not attached to email notifications of analytic failure **Note:** In the case of a failed analytic chain, the log for the specific analytic that fails is attached to the email.	**Attach log files to email notification**
attachmentSizeLimitInMB	The maximum total attachment size for analytic failure notification emails. By default, this is set to 10 MB. **Note:** If the total file attachment size exceeds the specified limit, no log files are attached to the email and the email notification indicates that the system omitted the logs due to a size constraint.	**Maximum total attachment size (in MB)**
axClientIdleLogoutInMinutes	The maximum number of minutes that AX Client can sit idle before the session is ended and the user is logged out. By default, this is set to **30**.	

Key	Description	Corresponding Field in AX Server Configuration Web Application
	The value must be an integer or null. When set to null or 0, the application does not time out when idle. **Note** If the application is completing a large import or export with processing time that exceeds the timeout, the timeout counter starts after the process completes. The import or export does not fail due to the maximum idle time setting. If a dialog that is not related to importing and exporting files is open when the timeout expires, the application and all associated dialogs close.	