AX Exception Installation Guide

Contents

AX Exception Installation Guide

Contents

1. AX Exception installation overview

This guide provides detailed information about installing and performing the initial configuration for AX Exception. It is intended for ACL Analytics Exchange administrators, system administrators, and database administrators responsible for implementing AX Exception.

AX Exception can either be installed on the same server as AX Server, or on a separate server. The option your organization should select depends on multiple factors including resources available on the server, the number of users accessing the system, and the overall usage of the system. Installing AX Exception on a separate server from AX Server is recommended because it simplifies future application maintenance and upgrades.

The following installation scenarios are described in this guide:

- Upgrading from version 4.x to version 5 – If you are upgrading an existing version 4.x installation on a separate server from AX Server, the setup wizard can update the application files to the latest version and migrate your configuration settings. For details, see Upgrading to version 5 on a separate server.
- Installing AX Exception on a separate server – Use this option if you want to install AX Exception on a separate server from AX Server. This is the recommended configuration. For details, see Installing AX Exception on a separate server.
- Installing AX Exception on AX Server – Use this option if you want to install AX Exception on the same server as AX Server. For details, see Installing AX Exception on the same server as AX Server.

AX Exception can use either Microsoft SQL Server or Oracle as the database platform. In most cases you database administrator will need to complete some, or all, of the database configuration before you run the installer.

- If you are using Microsoft SQL Server, the setup wizard can create and configure the AX Exception database if you have access to a database account or Windows user account that has system administration rights for the Microsoft SQL Server instance. Otherwise, you need to have your Microsoft SQL Server database administrator create an AX Exception database and database user, and provide you with the necessary password and connection settings.
- If you are using Oracle, your Oracle database administrator needs to create the required tablespace and database user, and provide you with the necessary password and connection settings. The AX Exception setup wizard does not provide the option to create the user during installation.

For information on configuring your database and running the database scripts, see ConfiguringtheAXException database.

Section contents

1.1. Downloading AX Exception server installers

The installers for AX Exception server can be downloaded from the ACL Launchpad (https://aclgrc.com). If you cannot log in to ACL Launchpad, contact your organization’s account administrator to ensure you have a valid ACL GRC account.

To download the installer:

1. Using your web browser, navigate to the ACL Launchpad (https://aclgrc.com) and log in to your ACL GRC account.
2. Download the installer file to your computer.

2. Upgrading AX Exception

This section provides instructions for upgrading AX Exception from version 4.x to version 5. The upgrade steps you need to complete depend on whether AX Exception and AX Server are installed on the same server, or on separate servers. If both applications are installed on the same server, you need to uninstall the previous version of AX Exception and install the new version after you have upgraded AX Server to version 5. If AX Exception is installed on a separate server, the upgrade process is automated by the setup wizard. You should read through the section and any referenced documents and before starting to upgrade your system.

If you need to upgrade AX Exception from a version prior to 4.0, you need to upgrade your system to version 4.0.3 before you can upgrade to version 5. Contact ACL Support Services for additional instructions, and the required installation files and documentation.

Section contents

2.1. Upgrading to version 5 on a separate server

The following procedure outlines the steps you need to complete to upgrade your server from version 4.x to version 5 when AX Exception is installed on a separate server from AX Server.

Before you begin, you need to download the AX Exception installer from the ACL Launchpad and save it on the Windows server where you want to install it.

Important

You must upgrade AX Server to version 5.0 or later before you upgrade AX Exception.

Before you begin the upgrade process you should back up your existing configuration in case you need to restore your version 4.x installation. The AX Exception setup wizard transfers most of your settings during the upgrade, but you should maintain your original settings in case the upgrade process is interrupted. You should shut down AX Exception and complete the following backup steps:

- Ensure that you have a current backup of the AX Exception database.
- Ensure that you have backed up and can restore any custom configuration settings you have made in the properties files. After the upgrade, you should update the new configuration files with your settings, rather than overwriting them with the old configuration files. These files are stored in the `geronimo\var\config` and `geronimo\var\log` subfolders where AX Exception is installed.
- If your organization has customized the workflow XML file or escalation email templates, you need to restore your customized files after the upgrade. By default, these files are stored in the `geronimo\var\config` subfolder.

After you complete the backup steps, you need to restart the AX Exception service before proceeding with the upgrade.

For information on stopping and starting the AX Exception service, see Administering the AX Exceptionservice. For information on backing up your database, see the documentation for your SQL Server or Oracle database engine.

To upgrade your AX Exception installation:

1. Double-click the AX Exception installer file. The file is named `ACLAX<version>_Exception.exe`.
2. In the **Setup Extraction Location** page, select the location to extract the files to or accept the default location, and click **Install**.

   The default extraction folder is the following subfolder in the Windows `Program Files` folder, or `Program Files (x86)` folder on 64-bit servers:
   `ACL Software\Installers\ACLAX<version>_Exception`

   Important

   The upgrade setup wizard automatically runs an upgrade script (`DBUpgrade_R400_to_R500.sql`) on the AX Exception database. If you prefer to run this script manually, you need to run it before proceeding with the upgrade. For instructions for the SQL Server platform, see Running the database upgrade script for SQL Server. For instructions for the Oracle platform, see Running the database upgrade script for Oracle.
3. If any prerequisites are missing, the **AX Exception Prerequisite Setup** page is displayed listing the prerequisites that will be installed. Click **Install** to start installing the required applications, and follow the prompts on screen to complete each of the setup wizards.
4. The installer will detect the previous 4.x version of AX Exception if it is installed on the server, and display a message indicating that the existing version will be upgraded. Click **Yes** in the **AX Exception** dialog box to proceed with the upgrade.
5. In the **Welcome** page, click **Next**.
6. In the **License Agreement** page, select **I accept the terms in the license agreement** and click **Next**.
7. In the **Destination Folder** page, click **Next**.
8. In the **AX Exception Database** page, select one of the following options and click **Next**:
   - **Run the AX Exception database scripts and configure connection settings.** – Select this option to have the setup wizard create the database and the AX Exception schema (tables, stored procedures, etc.) and configure the database connection string.
   - **Configure connection settings only.** – Select this option to have the setup wizard update the AX Exception properties file with the connection string required to access an existing AX Exception database. A database created with the AX Exception schema (tables, stored procedures, etc.) must already exist. Use this option if you ran the database scripts manually, or if you previously ran the setup wizard and created the database (that is, you are reinstalling AX Exception).
9. In the **AX Exception Database Page** verify the connection settings and click **Next**.
10. A dialog box is displayed indicating that the database will be upgraded, and that you must ensure that there are no active connections to the AX Exception database before you proceed with the upgrade. Click **OK** to continue. If you do not want to continue with the upgrade, click **Cancel** on the next page.
11. In the **ACL Analytics Exchange Geronimo Service Account** page, complete the following steps:
    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, for the setup wizard to present the appropriate list of available user accounts.
    b. Enter the **Password** for the account.
    c. Click Next.

    For information on the options for configuring service accounts, see "Understanding service account configuration" in the *ACL Analytics Exchange Server Administrator Guide*.
12. Click **Install** to begin the installation process.

13. When the installation process is complete, you can optionally select the **Show the Windows Installer log** checkbox to view a detailed log of the files that changed during the installation. Click **Finish** to exit the setup wizard.
14. If you have customized your version 4.x AX Exception installation in any of the following ways, you need to make the appropriate changes to enable the same customizations in the upgraded version and restart the ACL Analytics Exchange Geronimo service.
    a. If your organization has customized the workflow XML filename and/or content, you need to restore the file after you reinstall AX Exception, and the specify the correct path and filename in the *exceptionmgmt.workflow.file* property in the `axException.xml` configuration file.
    b. If your organization has customized the escalation email templates, you can restore them after you reinstall AX Exception by restoring your backed up template files and adjusting the *escalation.velocity* properties and *escalation.mail.format.html* property as necessary in the `axException.xml` configuration file.
    c. Verify that the hostname specified in the *useradministration.exceptionmgmt.url* property in `axExceptionAdmin.xml` matches the hostname specified in your security certificate and update the property, if necessary. If the values do not match, entities will not be displayed in the AX Exception Administration web application.

2.2. Upgrading AX Exception to version 5 on AX Server

The following procedure outlines the steps you need to complete to upgrade your server from version 4.x to version 5 when AX Exception is installed on the same server as AX Server.

Before you upgrade to the latest versions of AX Server and AX Exception, you need to uninstall AX Exception 4.x, upgrade AX Server from version 4.x to version 5, and then reinstall AX Exception version 5. Because you are completely removing AX Exception from the computer, you need to ensure that you have identified any configuration settings you need to maintain and have backed up your system.

To upgrade AX Server and AX Exception:

1. Identify any AX Exception configuration changes you want to maintain in the upgraded version. You will need to enter the main settings, such as the database connection and the mail server settings, in the AX Exception setup wizard, but you will also need to restore any information you have customized that the setup wizard does not prompt for. This includes the following:
    - Settings in `wrapper.conf`, your workflow .xml file, and the email template files (.vm). The default location for these files is the `geronimo/var/config` subfolder.
    - Settings in `DataloaderCommon.properties`, which is stored in the `App/dataloader/sessions/template/conf` subfolder.
2. Back up all AX Server and AX Exception data and configuration settings.
3. Uninstall AX Exception version 4.x
4. Restart the ACL Analytics Exchange Geronimo service to ensure that the service is still running correctly after removing AX Exception.
5. Run the AX Server version 5 installer and complete the upgrade. For information on the upgrade process, see "Upgrading to ACL Analytics Exchange version 5" in the *ACL Analytics Exchange Server Installation Guide*.
6. Download the AX Exception version 5 installer on the server where you want to install AX Exception.
7. Run the AX Exception version 5 installer. For information on the installation process, see Installing AX Exception on the same server as AX Server.

8. Make any additional changes to the AX Exception configuration files that are required and have not been completed by the installer. You should update the configuration files created by the AX Exception installer with the necessary changes, rather than replacing them with the previous versions, to ensure that any properties added in this version are present.
9. Verify that the hostname specified in the *useradministration.exceptionmgmt.url* property in `axExceptionAdmin.xml` matches the hostname specified in your security certificate. If the values do not match, entities will not be displayed in the AX Exception Administration web application. If they are different, you need to update the property and restart the ACL Analytics Exchange Geronimo service.
10. If your organization has customized the workflow XML filename and/or content, you need to restore the file after you reinstall AX Exception, and the specify the correct path and filename in the *exceptionmgmt.workflow.file* property in the `axException.xml` configuration file. If they are different, you need to update the property and restart the ACL Analytics Exchange Geronimo service.
11. If your organization has customized the escalation email templates, you can restore them after you reinstall AX Exception by restoring your backed up template files and adjusting the *escalation.velocity* properties and *escalation.mail.format.html* property as necessary in the `axException.xml` configuration file.

2.3. Running the database upgrade script for SQL Server

If you are upgrading AX Exception from version 4.x to version 5, you need to upgrade the AX Exception SQL Server database. The following procedure outlines the steps for running these scripts manually using the SQL Server administration tools. Manually running these scripts is only necessary if you want to complete the database schema update before you upgrade the application files using the AX Exception setup wizard. The setup wizard will run the upgrade scripts automatically if it detects that the database is at version 4.x.

The required upgrade SQL script is included in the folder where you extracted the AX Exception setup wizard files. The default location is: `C:\Program Files\ACL Software\Installers\ACLAX<version>_Exception\DBScripts\MSSQL\Upgrade`

To upgrade the database using SQL Server Management Studio:

1. Start **SQL Server Management Studio** (**Start** > **All Programs** > **Microsoft SQL Server <version>** > **SQL Server Management Studio**).
2. If you are prompted to log in, enter the required information to connect to the AX Exception database in the **Connect to Server** dialog box and click **Connect**.
3. Open the `DBUpgrade_R400_to_R500.sql` file and press F5 to run the script.

   If the script runs without errors, the **Messages** panel will display the message "Command(s) completed successfully." If you are prompted to save your changes to the script, you can but it is not required.
4. Exit **SQL Server Management Studio**.

2.4. Running the database upgrade script for Oracle

If you are upgrading AX Exception from version 4.x to version 5, you need to upgrade the AX Exception Oracle database. The following procedure outlines the general steps for running these scripts manually

using your preferred Oracle database administration tools. Manually running these scripts is only necessary if you want to complete the database schema update before you upgrade the application files using the AX Exception setup wizard. The setup wizard will run the upgrade scripts automatically if it detects that the database is at version 4.x.

The required upgrade SQL script is included in the folder where you extracted the AX Exception setup wizard files. The default location is: `C:\Program Files\ACL Software\Installers\ACLAX<version>_Exception\DBScripts\Oracle\Upgrade`

To upgrade the Oracle database:

1. Copy the upgrade SQL script file to the Oracle server, or a location you can run the scripts from.
2. Run the `DBUpgrade_R400_to_R500.sql` script on the AX Exception Oracle database using an account running under the SYSDBA role.

3. Installing AX Exception on a separate server

This section provides detailed instructions for installing and configuring AX Exception on a separate server from AX Server. You should read through the section before starting the installation.

You need to complete the following steps to install AX Exception on a separate server:

1. Configure, or have your database administrator configure, an Oracle or SQL Server database server to host the AX Exception database. For information about the required configuration, see the *AX Exception Administrator Guide*.
2. Download the AX Exception installer from the ACL Launchpad and save it on the Windows server where you want to complete the installation.
3. Ensure that the server meets the minimum software and hardware requirements. For details, see the *ACL Analytics Exchange System Requirements* document.
4. Check to ensure that the required ports are available on the server.
5. Run the AX Exception setup wizard.
6. Change the default Geronimo application server password to secure the server.
7. Configure the server security certificate.
8. Complete all of the post-installation tasks in Post-installation instructions.

Section contents

3.1. Configuring ports for AX Exception

In order for the ACL Analytics Exchange Geronimo service to start successfully on the AX Exception server, you must ensure that the ports required by the application server are not being used by other services or applications. Depending on your network configuration, your system administrator may also need to configure your firewall to allow connections using HTTPS.

Ports required by the Geronimo application server

AX Exception is installed with the default port settings used by the ACL Analytics Exchange Geronimo service. Table 1 lists the default ports used by Geronimo application server components that are required for the ACL Analytics Exchange Geronimo service to start successfully. These ports must not be in use when you run the AX Exception setup wizard. The reason each port is required is briefly described.

Table 1. ACL Analytics Exchange Geronimo default ports

Port Number	Component Name	Description
1099	RMI Naming	Port used by Geronimo for finding internal structures managed by the application.
1527	Derby Connector	Port used to connect to the Derby database included with and used by the Geronimo framework.
4201	OpenEJB Daemon	Port used by Geronimo for communication with the application modules.
8009	Tomcat Connector AJP	Port used to connect to the Tomcat web server that is integrated into the Geronimo framework.
80	Tomcat Connector HTTP	Port used for unencrypted HTTP communication with the server.
443 or 8443	Tomcat Connector HTTPS	Port used for encrypted HTTP (HTTPS) communication with the server. If you are performing a new installation of AX Server, the default port is 443. If you are upgrading an earlier version of AX Server, the default port is 8443.
9999	JMX Remoting Connector	Port used for managing the Geronimo services and installed modules.
61613	ActiveMQ-Stomp	Port used for the asynchronous messaging system Geronimo uses.
61616	ActiveMQ Transport Connector	Port used for the asynchronous messaging system Geronimo uses.

Confirming the availability of the required ports

If you are installing AX Exception for the first time on a separate server from AX Server, you should verify that the ports required by Geronimo are not already in use before you run the installer.

To determine which ports are in use, type the following command on the command line and review the port numbers displayed:

```
NETSTAT -a
```

If any of the required ports are being used by another service, you need to either reconfigure the service to use a different port, or temporarily disable the service in Windows Services while you install AX Exception. If necessary, you can modify some of the ports used by AX Exception after the installation process is complete. For information on configuring port settings, see "Configuring Ports used by AX Exception" in the *AX Exception Administrator Guide*.

Configuring your firewall to allow connections

If users are going to connect to AX Exception from outside the firewall, you must configure the firewall to allow inbound connections on the HTTPS port. The default HTTPS port used by AX Exception version 5.0 and later is 443. This port is used to enable encrypted HTTPS connections between the user's web browser and the Geronimo application server for the AX Exception and AX Exception Administration web applications.

Note
The default HTTPS port used by AX Server and AX Exception version 5.0 and later is 443. In earlier versions, the default HTTPS port was 8443. Installations upgraded from versions earlier than 5.0 maintain 8443 as the default HTTPS port.

3.2. Installing AX Exception on a separate server for SQL Server

The following procedure outlines the steps you need to complete to install AX Exception on a separate server from AX Server using Microsoft SQL Server 2008 as the AX Exception database platform. You must install AX Server version 5, or higher, on a separate server before you can install AX Exception.

Before you begin, download the AX Exception installer from ACL Launchpad (https://aclgrc.com) and save it on the Windows server where you want to install it.

The setup wizard can either create a new AX Exception database, or configure the connection information for an existing AX Exception database that your SQL Server database administrator has created by running the supplied SQL scripts. To successfully create the AX Exception database using the setup wizard, the user account used must be assigned to the SQL Server "sysadmin" role. If you use Windows Authentication, you must run the setup wizard as a user that belongs to the Administrators group on the server where SQL Server is installed, or as a user that has been specifically assigned to the "sysadmin" server role for the SQL Server instance. If you use SQL Server authentication, you must specify the built-in "sa" account or an equivalent account that belongs to the "sysadmin" server role.

To install AX Exception on a separate server:

1. Double-click the AX Exception installer file. The file is named `ACLAX<version>_Exception.exe`.
2. In the **Setup Extraction Location** page, select the location to extract the files to or accept the default location, and click **Install**.

   The default extraction folder is the following subfolder in the Windows `Program Files` folder, or `Program Files (x86)` folder on 64-bit servers:
   `ACL Software\Installers\ACLAX<version>_Exception`
3. In the **AX Exception Setup Options** page, select **Microsoft SQL Server** as the AX Exception database platform, select **PostgreSQL** as the ACL Analytics Exchange database platform, and click **Next**.
4. If any prerequisites are missing, the **AX Exception Prerequisite Setup** page is displayed listing the prerequisites that will be installed. Click **Install** to start installing the required applications, and follow the prompts on screen to complete each of the setup wizards.
5. In the **Welcome** page, click **Next**.

6. In the **License Agreement** page, select **I accept the terms in the license agreement** and click **Next**.
7. In the **Destination Folder** page, specify the location where AX Exception should be installed. Accept the default location, or click **Change** and select a new folder, and click **Next**.
8. In the **AX Exception Database** page, select **Microsoft SQL Server** as the database platform.
9. Select one of the following options:
    - **Run the AX Exception database scripts and configure connection settings.** – Select this option to have the setup wizard create the database and the AX Exception schema (tables, stored procedures, etc.) and configure the database connection string.
    - **Configure connection settings only.** – Select this option to have the setup wizard update the AX Exception properties file with the connection string required to access an existing AX Exception database. A database created with the AX Exception schema (tables, stored procedures, etc.) must already exist. Use this option if you ran the database scripts manually, or if you previously ran the setup wizard and created the database (i.e. you are reinstalling AX Exception).
10. Click **Next**.
11. If you selected the **Run the AX Exception database scripts and configure connection settings** complete the following steps in the **SQL Server Settings** page:
    a. In the **SQL Server Settings** page, enter the IP address or hostname for the AX Exception database server in the **Database Server** field. You can click **Browse** to locate all of the SQL Server database servers located within your network, and then select the database server to use for AX Exception and click **OK**.
    b. If the user account you are using to run the AX Exception setup wizard has the SQL Server "sysadmin" role assigned, select **Windows authentication credentials of current user**. If the user account does not have the appropriate rights, select **Server authentication using the Login ID and password below** and enter the following information for a database user account that belongs to the SQL Server "sysadmin" role:
        - **Login ID** – Enter the database account name to use to connect to the database server.
        - **Password** – Enter the password for the database account name.
    c. Click **Next**.
12. In the **AX Exception Database Settings** page, specify the following properties for the AX Exception database:
    - **Database server** – Enter the hostname or IP address for the SQL Server instance where the existing AX Exception database is located. This text box only needs to be completed if you chose the **Configure connection settings only** option in the **AX Exception Database** page.
    - **Database name** – Enter the name for the AX Exception database the setup wizard will create. If you are creating a new database, there cannot already be an existing database with the same name.
    - **Port** – Enter the port to use to connect to the database.
    - **Database User** – Enter the database user account used to access the AX Exception database. If the setup wizard is creating the database, you must enter a new account name that does not already exist in the list of SQL Server users. If the setup wizard is only configuring connection settings, you must enter a database user account that already exists and has been configured as the AX Exception database owner.
    - **Password** – If the setup wizard is creating the database, enter the password for the database user account the setup wizard will create. If the setup wizard is only configuring connection settings, enter the password for the existing database user account configured as the AX Exception database owner.
    - **Confirm Password** – Enter the same password value you entered in **Password**.
13. Click **Next**.
14. In the **SSL certificate information** page, enter the following information to create a self-signed security certificate to secure HTTPS connections to the AX Exception server:

- **Server Name** – The hostname of the server users will use to access AX Exception and AX Exception Administration. For example: exception.acl.com
- **Department or division name** – The division or business unit 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.
- **Private Key Password** – Enter the same password again. The **Keystore Password** and the **Private Key Password** must be identical.

For information on how this certificate is used, and for configuration options, see "Understanding security certificate configuration" in the *AX Exception Administrator Guide*.

15. Click **Next**.
16. In the **ACL Analytics Exchange Authentication** page, enter the following information:
    - **Host name** – Specify the hostname of the server where AX Server is installed. For example: AX.ACL.COM
    - **Port** – Specify the port to use for encrypted connections to AX Server. The default value is 443. In earlier versions, the default port was 8443.
    - **Default Domain** – Specify the default Active Directory Domain to use to authenticate users.
17. Click **Next**.
18. In the **ACL Analytics Exchange database platform** page, ensure that PostgreSQL is selected.
19. The **Encrypt database communications** setting is selected by default. You should leave this option selected unless the servers are transferring data in a secure network environment where encryption is unnecessary.
20. Click **Next**.
21. In the **ACL Analytics Exchange PostgreSQL database connection settings** page, enter the following information to connect to the PostgreSQL database:
    - **Server IP address** – Specify the IP address or hostname of the server where the PostgeSQL database server is installed.
    - **Database name** – Displays the name of the PostgreSQL database used to store ACL Analytics Exchange data. This field is not editable.
    - **Port** – Specify the port to use to connect the PostgreSQL database engine.
    - **AX Database User** – Specify the username to use to connect to the ACL Analytics Exchange database. The username required is the ACL Analytics Exchange database user account. The default username is "AclAuditExchangeRole".
    - **Password** – Specify the password to use to connect to the ACL Analytics Exchange database.
22. Click **Next**.
23. In the **Data publishing security** page, select one of the following options:
    - **Do not restrict data publishing. Allow Data Publishing from any IP address.** – Select this option if you do not want to restrict the location that data can be published from to specific servers.
    - **Restrict data publishing to specific IP addresses.** – Select this option for enhanced security if you want to ensure that exception data copied to the AX Exception database can only originate from AX Server, or from servers running AX Engine Node. Enter the IP address

of each server you want to allow data publishing from. Separate the IP addresses with semicolons if you are entering multiple IP addresses. If data publishing information is sent from any other IP address, the system will reject it and the data publishing process will fail.

24. Click **Next**.
25. In the **ACL Analytics Exchange Geronimo Service Account** page, complete the following steps:
    a. In **User name**, 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, for the setup wizard to present the appropriate list of available user accounts.
    b. Enter the **Password** for the account.
    c. Click **Next**.

    If the account you specified does not have the "Log on as a service" permission assigned, you will be prompted to confirm that this permission can be assigned to the account automatically by the setup wizard. The "Log on as a service" permission is required for AX Exception to operate correctly.

    For information on the options for configuring service accounts, see "Understanding service account configuration" in the *AX Exception Administrator Guide*.
26. In the **Escalation Settings** page, enter the following information:
    - **Escalation Time Zone** – Select the appropriate time zone from the list of available options.
    - **IP address or hostname** – Specify the IP address or host name of the mail server to use to send escalation emails. The mail server you specify must support the Simple Mail Transfer Protocol (SMTP) standard.
    - **From Address** – Specify the email address to list as the sender for outgoing escalation emails.
    - **Username** – Specify a user account with the appropriate security permissions on the mail server to send escalation emails.
    - **Password** – Specify the password for the user account.
    - **Port** – Specify the port to connect to the mail server on. The default value is 25.
27. Click **Next**.
28. Click **Install** to begin the installation process.
29. When the installation process is complete, you can optionally select the **Show the Windows Installer log** checkbox to view a detailed log of the files that changed during the installation. Click **Finish** to exit the setup wizard.
30. If you are using the self-signed certificate created by the AX Server setup wizard on AX Server, you need to export this certificate from the AX Server keystore and import it into the AX Exception keystore. For information on this process, see Exporting and importing the AX Server certificate.
31. Complete the post-installation tasks outlined in Post-installation instructions.

Related tasks

Exporting and importing the AX Server certificate

Changing the default Geronimo administrator password

3.3. Installing AX Exception on a separate server for Oracle

The following procedure outlines the steps you need to complete to install AX Exception on a separate server from AX Server using Oracle 10g or 11g as the AX Exception database platform. You must install

AX Server version 5, or higher, on a separate server before you can install AX Exception.

Before you begin, download the AX Exception installer from ACL Launchpad (https://aclgrc.com) and save it on the Windows server where you want to install it.

To install AX Exception on a separate server:

1. Double-click the AX Exception installer file. The file is named `ACLAX<version>_Exception.exe`.
2. In the **Setup Extraction Location** page, select the location to extract the files to or accept the default location, and click **Install**.

   The default extraction folder is the following subfolder in the Windows `Program Files` folder, or `Program Files (x86)` folder on 64-bit servers:
   `ACL Software\Installers\ACLAX<version>_Exception`
3. In **AX Exception Setup Options**, select **Oracle** as both the AX Exception database platform and the ACL Analytics Exchange database platform, and click **Next**.
4. If any prerequisites are missing, the **AX Exception Prerequisite Setup** page is displayed listing the prerequisites that will be installed. Click **Install** to start installing the required applications, and follow the prompts on screen to complete each of the setup wizards. If the correct version of the Oracle Instant Client is not already installed the **Oracle Instant Client for ACL Analytics Exchange** setup wizard runs. Complete the following steps to install this prerequisite:
   a. In the **Welcome** page, click **Next**.
   b. In the **License Agreement** page, select **I accept the terms in the license agreement** and click **Next**.
   c. In the **Destination Folder**page, specify where the Oracle Instant Client will be installed and click **Next**. If necessary, click **Change** to modify the default location.
   d. Click **Install** to begin the installation process.
   e. When the installation process is complete, click **Finish**.
5. In the **Welcome** page, click **Next**.
6. In the **License Agreement** page, select **I accept the terms in the license agreement** and click **Next**.
7. In the **Destination Folder** page, specify the location where AX Exception should be installed. Accept the default location, or click **Change** and select a new folder, and then click **Next**.
8. In the **AX Exception Database** page, select **Oracle** as the AX Exception database platform.
9. Select or deselect the **Encrypt database communications** checkbox as appropriate. This option should only be selected if the Oracle database server has been configured for SSL connections and data is being transferred between the database server and application server over an unsecure network.
10. Select one of the following options:
    - **Run the AX Exception database scripts and configure connection settings.** – Select this option to have the setup wizard create the AX Exception schema (tables, stored procedures, etc.) and configure the database connection string.
    - **Configure connection settings only.** – Select this option to have the setup wizard update the AX Exception properties file with the connection string required to access an existing AX Exception database. The AX Exception schema (tables, stored procedures, etc.) must already exist.
11. Click **Next**.
12. In the **AX Exception Database Settings** page, enter the following information:
    - **Server name or IP address** – The IP address or hostname of the Oracle database server where the AX Exception database is located.
    - **Service name** – The Global Database Name of the Oracle database instance for AX Exception.
    - **Non-SSL port** – The port to use for unencrypted communications with the database server. You must specify the port that is configured for the Oracle Listener. The default value is 1521.

- **SSL port**– The port to use for encrypted communications with the database server. You must specify the port that is configured for the Oracle Listener. The default value is 2484. This field is only displayed if you selected **Encrypt database communications** checkbox on the previous page in the setup wizard.
- **Username** – The Oracle username required to access the AX Exception database.
- **Password** – The Oracle password required to access the AX Exception database.

13. In the **SSL certificate information** page, enter the following information to create a self-signed security certificate to secure HTTPS connections to the AX Exception server:
    - **Server Name** – The hostname of the server users will use to access AX Exception and AX Exception Administration. For example: axexception.acl.com
    - **Department or division name** – The division or business unit 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.
    - **Private Key Password** – Enter the same password again. The **Keystore Password** and the **Private Key Password** must be identical.

    For information on how this certificate is used, and for configuration options, see "Understanding security certificate configuration" in the *AX Exception Administrator Guide*.
14. In the **ACL Analytics Exchange Authentication** page, enter the following information:
    - **Hostname** – Specify the hostname of the server where AX Server is installed. For example: AX.ACL.COM
    - **Port** – Specify the port to use for encrypted connections to AX Server. The default value is 443. In earlier versions, the default port was 8443.
    - **Default Domain** – Specify the default Active Directory Domain to use to authenticate users.
15. In the **ACL Analytics Exchange Database Info** page, select Oracle as the database platform, and select the Oracle version you are using.
16. The **Encrypt database communications** setting is not selected by default. You should select this option if the Oracle database server and the AX Exception server are transferring data in an unsecured network environment where encryption is required, and the Oracle database engine is configured to support SSL connections.
17. Click **Next**.
18. In the **ACL Analytics Exchange Oracle Database Info** page, enter the following information to connect to the Oracle database on AX Server:
    - **Server IP address** – The IP address of the Oracle database server where the ACL Analytics Exchange database is located.
    - **Service name** – The Global Database Name of the Oracle database instance for AX Server.
    - **Non-SSL port** – The port to use for unencrypted communications with the database server. You must specify the port that is configured for the Oracle Listener. The default value is 1521.
    - **SSL port**– The port to use for encrypted communications with the database server. You must specify the port that is configured for the Oracle Listener. The default value is 2484. This field is only displayed if you selected **Encrypt database communications** checkbox on the previous page in the setup wizard.
    - **User name** – The Oracle username required to access the ACL Analytics Exchange database.

- **Password** – The Oracle password required to access the ACL Analytics Exchange database.

19. Click **Next**.
20. In the **Publish Security** page, select one of the following options:
    - **Do not restrict data publishing. Allow Data Publishing from any IP address.** – Select this option if you do not want to restrict the location that data can be published from to a single server.
    - **Restrict data publishing to specific IP addresses.** – Select this option for enhanced security if you want to ensure that exception data copied to the AX Exception database can only originate from AX Server or from servers running AX Engine Node. Enter the IP address of each server you want to allow data publishing from. Separate the IP address with semicolons if you are entering multiple IP addresses. If data publishing information is sent from any other IP address, the system will reject it.
21. Click **Next**.
22. In the **ACL Analytics Exchange Geronimo Service Account** page, complete the following steps:
    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, for the setup wizard to present the appropriate list of available user accounts.
    b. Enter the **Password** for the account.
    c. Click **Next**.

    If the account you specified does not have the "Log on as a service" permission assigned, you will be prompted to confirm that this permission can be assigned to the account automatically by the setup wizard. The "Log on as a service" permission is required for AX Exception to operate correctly.

    For information on the options for configuring service accounts, see "Understanding service account configuration" in the *AX Exception Administrator Guide*.
23. In the **Escalation Settings** page, enter the following information:
    - **Escalation Time Zone** – Select the appropriate time zone from the list of available options.
    - **IP address or hostname** – Specify the IP address or host name of the mail server to use to send escalation emails. The mail server you specify must support the Simple Mail Transfer Protocol (SMTP) standard.
    - **From Address** – Specify the email address to list as the sender for outgoing escalation emails.
    - **Username** – Specify a user account with the appropriate security permissions on the mail server to send escalation emails.
    - **Password** – Specify the password for the user account.
    - **Port** – Specify the port to connect to the mail server on. The default value is 25.
24. Click **Next**.
25. Click **Install** to begin the installation process.
26. When the installation process is complete, you can optionally select the **Show the Windows Installer log** checkbox to view a detailed log of the files that changed during the installation. Click **Finish** to exit the setup wizard.
27. If you are using the self-signed certificate created by the AX Server setup wizard on AX Server, you need to export this certificate from the AX Server keystore and import it into the AX Exception keystore. For information on this process, see Exporting and importing the AX Server certificate.
28. Complete the post-installation tasks outlined in Post-installation instructions.

Related tasks

Exporting and importing the AX Server certificate

Changing the default Geronimo administrator password

3.4. Exporting and importing the AX Server certificate

If you are using the default self-signed certificate created during AX Server installation, you need to import this certificate into the AX Exception keystore as a trusted certificate. This is required for ACL Analytics Exchange authentication to work on the AX Exception server. This configuration is only required if AX Exception and AX Server are installed on different servers and AX Server uses a self-signed certificate.

In order to use the **keytool** command without specifying the full path each time you use it, you need to add the Java `bin` subdirectory to your path. You can do this permanently by updating the *Path* Environment Variable to include the full path to the Java `bin` subdirectory on both servers, or add it temporarily on the command line using the following syntax:

```
Set PATH=<java_bin_path>;%PATH%
```

For example:

```
Set PATH=C:\Program Files\Java\jdk1.7.0_67\bin\;%PATH%
```

To export and then import the AX Server certificate:

1. Complete the following steps on AX Server to export the self-signed certificate:
    a. Open a command prompt and switch to the Geronimo keystores subfolder. The default location is the `geronimo\var\security\keystores` subfolder where AX Server is installed.
    b. Type the following command and press **Enter**:

    ```
    keytool -export -alias axcorekeystore -file filename -keystore keystore_name
    ```

    Example:

    ```
    keytool -export -alias axcorekeystore -file "C:\axkeystore.crt" -
    keystore MyKeyStore
    ```

    c. Type the password for the keystore at the prompt and press **Enter**.
2. Copy the certificate file specified in the *-file* parameter above (i.e. axkeystore.crt) from the AX Server to the AX Exception server.
3. Complete the following steps on the AX Exception server to import the self-signed certificate:
    a. Open a command prompt and switch to the Geronimo `keystores` subfolder. The default location is the `geronimo\var\security\keystores` subfolder where AX Exception is installed.
    b. Type the following command and press **Enter**:

    ```
    keytool -import -alias axcorekeystore -file filename -keystore keystore_name
    ```

    Example:

    ```
    keytool -import -alias axcorekeystore -file "C:\axkeystore.crt" -
    keystore MyKeyStore
    ```

    c. Type the password for the keystore at the "Password" prompt and press **Enter**.
    d. Type 'y' at the "Trust this certificate?" prompt and press **Enter**.
4. Optional. To verify the contents of the keystore type the following command and press **Enter**, and enter the password for the keystore at the prompt and press **Enter**:

    ```
    keytool -list -v -keystore keystore_name
    ```

    Example:

    ```
    keytool -list -v -keystore MyKeyStore
    ```

    The information displayed should include the AX Server certificate information.
5. Restart the ACL Analytics Exchange Geronimo service on the AX Exception server.

3.5. Changing the default Geronimo administrator password

The Geronimo application server is installed with a default administrator account you can use to access the Geronimo Console and manage the ACL Analytics Exchange Geronimo service. You should change the default password for this account as soon as you complete the installation.

To change the Geronimo Console administrator password:

1. Open the Geronimo Console web application in your web browser and log in.

   The location of the Geronimo Console is http://<*server_name*>/console, where <*server_name*> is the hostname or IP address of the AX Exception server.
2. Enter the default username (`system`) and password (`manager`) for the Geronimo Console and click **Login**.
3. Click the **Users and Groups** link in the **Console Navigation** panel.
4. Click the **Edit** link beside the **system** username.
5. Enter the new password in **Password** and **Confirm Password** and click **Update**.
6. Log out from the Geronimo Console.

4. Installing AX Exception on the same server as AX Server

This section provides detailed instructions for installing and configuring AX Exception on a server where AX Server is already installed, or will be installed prior to installing AX Exception. You should read through the section before starting the installation.

You need to complete the following steps to install AX Exception with AX Server:

1. Configure, or have your database administrator configure, an Oracle or SQL Server database server to host the AX Exception database. For information about the required configuration, see the *AX Exception Administrator Guide*.
2. Download the AX Exception installer from the ACL Launchpad and save it on the Windows server where you want to complete the installation.
3. Install AX Server. For instructions, see the ACL Analytics ExchangeServer Installation Guide.
4. Have your system administrator provide you with the connection details for a mail server to use to send escalation emails. The required information includes the mail server hostname and port, and the user account and password to use to log in to the mail server.
5. Run the Setup Wizard for AX Exception.
6. Complete all of the post-installation tasks in Post-installation instructions.

Section contents

4.1. Installing *AX* Exception with AX Server for SQL Server

The following procedure outlines the steps you need to complete to install AX Exception on the same server as AX Server. You must install AX Server version 5.0 before you can install AX Exception.

Before you begin, you need to download the AX Exception installer from the ACL Launchpad and save it on the Windows server where you want to install it.

The setup wizard can either create a new AX Exception database, or configure the connection information for an existing AX Exception database that your SQL Server database administrator has created by running the supplied SQL scripts. In order to successfully create the AX Exception database using the setup wizard, the user account used must be assigned to the SQL Server "sysadmin" role. If you use Windows Authentication, you must run the setup wizard as a user that belongs to the Administrators group on the server where SQL Server is installed, or as a user that has been specifically assigned to the "sysadmin" server role for the SQL Server instance. If you use SQL Server authentication, you must specify the built-in "sa" account or an equivalent account that belongs to the "sysadmin" server role.

To install AX Exception on AX Server:

1. Double-click the AX Exception installer file to extract the setup wizard files. The file is named `ACLAX<version>_Exception.exe`.
2. In the **Setup Extraction Location** page, select the location to extract the files to or accept the default location, and click **Install**.

   The default extraction folder is the following subfolder in the Windows `Program Files` folder, or `Program Files (x86)` folder on 64-bit servers:
   `ACL Software\Installers\ACLAX<*version*>_Exception`
3. In the **Welcome** page, click **Next**.
4. In the **License Agreement** page, select **I accept the terms in the license agreement** and click **Next**.
5. In the **Destination Folder** page, the default location specified is the location where AX Server is installed. You cannot change the value if you are installing AX Exception on the same server where AX Server is installed. Click **Next** to continue.
6. In the **AX Exception Database** page, select **Microsoft SQL Server** as the database platform.
7. Select one of the following options:
   - **Run the AX Exception database scripts and configure connection settings.** – Select this option to have the setup wizard create the database and the AX Exception schema (tables, stored procedures, etc.) and configure the database connection string.
   - **Configure connection settings only.** – Select this option to have the setup wizard update the AX Exception properties file with the connection string required to access an existing AX Exception database. A database created with the AX Exception schema (tables, stored procedures, etc.) must already exist. Use this option if you ran the database scripts manually, or if you previously ran the setup wizard and created the database (that is, you are reinstalling AX Exception).
8. Click **Next**.
9. If you selected the **Run the AX Exception database scripts and configure connection settings** complete the following steps in the **SQL Server Settings** page:
   a. In the **Database Server** field, enter the IP address or hostname of the AX Exception database server. You can type the IP address or hostname, or you can click **Browse** to locate all of the SQL Server database servers located within your network, and then select the database server to use for AX Exception and click **OK**.
   b. If the user account you are using to run the AX Exception setup wizard has the SQL Server "sysadmin" role assigned, select **Windows authentication credentials of current user**. If the user account does not have the appropriate rights, select **Server authentication using the Login ID and password below** and enter the following information for a database user account that belongs to the SQL Server "sysadmin" role:
      - **Login ID** – Enter the database account name to use to connect to the database server.

- **Password** – Enter the password for the database account name.

c. Click **Next**.

10. In the **AX Exception Database Settings** page, specify the following properties for the AX Exception database:
    - **Database server** – Enter the hostname or IP address for the SQL Server instance where the existing AX Exception database is located. This text box only needs to be completed if you chose the **Configure connection settings only** option in the **AX Exception Database** page.
    - **Database name** – Enter the name for the AX Exception database the setup wizard will create. If you are creating a new database, there cannot already be an existing database with the same name.
    - **Port** – Enter the port to use to connect to the database.
    - **Database User** – Enter the database user account used to access the AX Exception database. If the setup wizard is creating the database, you must enter a new account name that does not already exist in the list of SQL Server users. If the setup wizard is only configuring connection settings, you must enter a database user account that already exists and has been configured as the AX Exception database owner.
    - **Password** – If the setup wizard is creating the database, enter the password for the database user account the setup wizard will create. If the setup wizard is only configuring connection settings, enter the password for the existing database user account configured as the AX Exception database owner.
    - **Confirm Password** – Enter the same password value you entered in **Password**.
11. Click **Next**.
12. In the **Data publishing security** page, select one of the following options:
    - **Do not restrict data publishing. Allow Data Publishing from any IP address.** – Select this option if you do not want to restrict the locations that AX Exception data can be published from.
    - **Restrict data publishing to specific IP addresses.** – Select this option for enhanced security if you want to ensure that exception data copied to the AX Exception database can only originate from AX Server or from servers running AX Engine Node. Enter the IP address of each server you want to allow data publishing from. Separate the IP address with semicolons if you are entering multiple IP addresses. If data publishing information is sent from any other IP address, the system will reject it.
13. Click **Next**.
14. In the **Escalation settings** page, enter the following information:
    - **Escalation Time Zone** – Select the appropriate time zone from the list of available options.
    - **IP address or hostname** – Specify the IP address or host name of the mail server to use to send escalation emails. The mail server you specify must support the Simple Mail Transfer Protocol (SMTP) standard.
    - **From Address** – Specify the email address to list as the sender for outgoing escalation emails.
    - **Username** – Specify a user account with the appropriate security permissions on the mail server to send escalation emails.
    - **Password** – Specify the password for the user account.
    - **Port** – Specify the port to connect to the mail server on. The default value is 25.
15. Click **Next**.
16. Click **Install** to begin the installation process.

Important

Before the installation process completes you are required to wait for about a minute while the Geronimo application server becomes fully

functional. The command window may appear intermittently during this period. **Do not cancel the installation.**

17. When the installation process is complete, you can optionally select the **Show the Windows Installer log** checkbox to view a detailed log of the files that changed during the installation. Click **Finish** to exit the setup wizard.
18. Complete the post-installation tasks described in Post-installation instructions.

4.2. Installing AX Exception with AX Server for Oracle

The following procedure outlines the steps you need to complete to install AX Exception on the same server as AX Server. You must install AX Server version 5.0 or higher before you can install AX Exception.

Before you begin, download the AX Exception installer from the ACL Launchpad and save it on the Windows server where you want to install it.

To install AX Exception on AX Server:

1. Double-click the AX Exception installer file. The file is named `ACLAX<version>_Exception.exe`.
2. In the **Setup Extraction Location** page, select the location to extract the files to or accept the default location, and click **Install**.

   The default extraction folder is the following subfolder in the Windows `Program Files` folder, or `Program Files (x86)` folder on 64-bit servers:
   `ACL Software\Installers\AXException_<version>`
3. In the **Welcome** page, click **Next**.
4. In the **License Agreement** page, select **I accept the terms of the license agreement** and click **Next**.
5. In the **Destination Folder** page, the default location specified is the location where AX Server is installed. You cannot change the value if you are installing AX Exception on the same server where AX Server is installed. Click **Next** to continue.
6. In the **AX Exception Database** page, select **Oracle (10g, 11g)**.
7. Select or deselect the **Encrypt database communications** checkbox as appropriate. This option should only be selected if the Oracle database server has been configured for SSL connections and data is being transferred between the database server and application server over an unsecure network.
8. Select one of the following options:
   - **Run the AX Exception database scripts and configure connection settings.** – Select this option to have the setup wizard create the AX Exception schema (tables, stored procedures, etc.) and configure the connection string.
   - **Configure connection settings only.** – Select this option to have the setup wizard update the AX Exception properties file with the connection string required to access an existing AX Exception database. The AX Exception schema (tables, stored procedures, etc.) must already exist.
9. Click **Next**.
10. In the **AX Exception Database Settings** page, specify the following properties for the AX Exception database:
    - **Server name or IP address** – The IP address or hostname of the Oracle database server where the AX Exception database is located.
    - **Service name** – The Global Database Name of the Oracle database instance for AX Exception.

- **Non-SSL port** – The port to use for unencrypted communications with the database server. You must specify the port that is configured for the Oracle Listener. The default value is 1521.
- **SSL port**– The port to use for encrypted communications with the database server. You must specify the port that is configured for the Oracle Listener. The default value is 2484. This field is only displayed if you selected **Encrypt database communications** checkbox on the previous page in the setup wizard.
- **User name** – The Oracle username required to access the AX Exception database.
- **Password** – The Oracle password required to access the AX Exception database.

11. Click **Next**.
12. In the **Publish Security** page, select one of the following options:
    - **Do not restrict data publishing. Allow Data Publishing from any IP address.** – Select this option if you do not want to restrict the locations that AX Exception data can be published from.
    - **Restrict data publishing.** – Select this option for enhanced security if you want to ensure that exception data copied to the AX Exception database can only originate from AX Server or from servers running AX Engine Node. Enter the IP address of each server you want to allow data publishing from. Separate the IP address with semicolons if you are entering multiple IP addresses. If data publishing information is sent from any other IP address, the system will reject it.
13. Click **Next**.
14. In the **Escalation Settings** page, enter the following information:
    - **Escalation Time Zone** – Select the appropriate time zone from the list of available options.
    - **IP address or hostname** – Specify the IP address or host name of the mail server to use to send escalation emails. The mail server you specify must support the Simple Mail Transfer Protocol (SMTP) standard.
    - **From Address** – Specify the email address to list as the sender for outgoing escalation emails.
    - **Username** – Specify a user account with the appropriate security permissions on the mail server to send escalation emails.
    - **Password** – Specify the password for the user account.
    - **Port** – Specify the port to connect to the mail server on. The default value is 25.
15. Click **Next**.
16. Click **Install** to begin the installation process.

Important

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

---

17. When the installation process is complete, you can optionally select the **Show the Windows Installer log** checkbox to view a detailed log of the files that changed during the installation. Click **Finish** to exit the setup wizard.
18. Complete the post-installation tasks outlined in Post-installation instructions.

5. Post-installation instructions

This section provides information about additional configuration tasks you may need to complete after AX Exception is installed. The tasks you need to complete depend on you configuration, and some tasks are optional.

Section contents

5.1. Verifying that AX Exception is running

After you complete the installation, you should ensure that the required service is running and that the server components have been deployed successfully in the Geronimo application server.

Checking Windows service statuses

You can verify that the ACL Analytics Exchange Geronimo service was successfully installed by checking the status of the service in Windows Services.

To check that status of the service:

1. Log on to the server where AX Exception is running.
2. Select **Start** > **Control Panel** > **Administrative Tools** > **Services**.
3. Check that the ACL Analytics Exchange Geronimo service is listed as "Started" or "Running" in the **Status** column.
4. If the service has not started, you can attempt to start it by right-clicking the service and selecting **Start**. If the service still doesn't start, check the log files to determine the cause of the problem or contact ACL Support Services.

Checking the ACL Analytics Exchange Geronimo service log

You can view detailed information about the status of the ACL Analytics Exchange Geronimo service by checking the `geronimo_service.log` file in the `geronimo/var/log` subfolder where AX Exception is installed. The level of detail in the log depends on the value specified in the *wrapper.logfile* property in the `wrapper.conf` configuration file. By default, a new log file is created each time the service is restarted, or when it grows beyond the specified maximum size. You can check the log to verify that the service started successfully, and to view any errors that were encountered.

Checking server component statuses

You should also verify that AX Exception and AX Exception Administration have been successfully deployed and started by the Geronimo application server. You can use the Geronimo Console to view the status of the installed applications.

To check the status of installed applications:

1. Open the Geronimo Console in your web browser and log in.

   The location of the Geronimo Console is http://<server_name>/console, where <*server_name*> is the hostname or IP address of the server where you want to check the status of the AX Exception components.

Note
In earlier versions of AX Exception, the default port value of the Geronimo Console was 8080. As a result, of your AX Exception installation has been upgraded from a previous earlier, you may need to specify port 8080 in the address bar of your web browser. For example, `http://<server_name>:8080/console`.

2. Enter the username and password you use to access the Geronimo Console and click **Login**. The default username is `system`, and the default password is `manager`.
3. In the **Console Navigation** panel, click **Applications** > **Web App WARs**.
4. Confirm that the following components are listed and that their state is "running":
    - com.acl/ax-em_admin/<*version number*>/car
    - com.acl/exceptionmgmt/<*version number*>/car
5. If any of the components have not started, you can attempt to start them by clicking the **Start** link for the component in the **Commands** column. If the service still does not start, check the `geronimo_service.log` file, in the `geronimo\var\log` subfolder to determine the cause of the problem, or contact ACL Support Services.
6. Log out from the Geronimo Console.

5.2. Changing the keystore used by the Dataloader

The setup wizard configures the Dataloader to use the self-signed certificate it creates by default. If you want to use a different keystore, you need to update the certificate settings used by the Dataloader. The Dataloader is installed on AX Server and on each instance of AX Engine Node you have configured.

To configure the Dataloader to use your certificate:

1. Update the `wrapper.conf` file by completing the following steps:
    a. Locate `wrapper.conf` in the `geronimo\var\config` subfolder on AX Server or AX Engine Node and open it in a text editor.
    b. Update the *-Djavax.net.ssl.trustStore*, *-Djavax.net.ssl.trustStoreType*, and *-Djavax.net.ssl.trustStorePassword* settings with the values required for your keystore.
    c. Save the `wrapper.conf` file and restart the ACL Analytics Exchange Geronimo service.
2. Locate the `dataloaderCommon.properties` file and open it in a text editor. The default location is the `DataLoader\sessions\template\conf` subfolder where AX Server or AX Engine Node is installed.
3. Update the following properties:
    - **trustStoreFile** – Enter the path and name of the keystore file you want to use. For example: `C:/ACL/App/geronimo/var/security/keystores/ACLKeystore`
    - **trustStorePass** – Enter the password for your keystore.
4. Save and close the file.

5.3. Configuring the Dataloader upload location

You need to manually configure the upload location for the Dataloader. This value is set in the AX Server Configuration web application, and it must specify the URL for the AX Exception web application. After this procedure is completed, AX Client users will have the option to publish their results to AX Exception when they schedule analytics.

To set the upload location:

1. Open the AX Server Configuration web application in Internet Explorer and log in. Use the same username and password that you use to log in to the Geronimo Console.

   Note
   Internet Explorer is the only web browser supported for opening the AX Server Configuration web application.

   The default location is https://<*server_name*>/aclconfig, where <*server_name*> is the hostname or IP address of your AX Server.

   For example: https://axserver.acl.com/aclconfig.

   Note
   If your AX Server installation has been upgraded from a previous version, you may need to specify port 8443 in the address bar of your web browser. For example, `https://axserver.acl.com:8443/aclconfig`.

2. Enter "system" as the username and the account password and click **Login**.
3. In the Server column, locate the AX Exception panel, and enter the URL for AX Exception in the **Data upload URL** textbox. The URL should be in the following format: `https://<server_name>/exceptionmgmt` where <*server_name*> is the hostname of the server where AX Exception is installed.

   Note
   If your AX Exception server has been upgraded from a previous version, you may need to specify port 8443 in the **Data upload URL** textbox. For example, `https://exception.acl.com:8443/exceptionmgmt`.

4. Click **Update Server Settings**.

5.4. Verifying that the Dataloader is working

To verify that the Dataloader is working correctly, you need to schedule an analytic in AX Client that publishes a results table to AX Exception. The basic process is outlined in the procedure below.

To verify that the Dataloader is working:

1. Log in to AX Client and select an analytic that creates at least one results table that can be selected for publishing to AX Exception.
2. Schedule the analytic to run, and enter the entity and analytic to publish the exceptions to in the **Publish to AX Exception** page.
3. Check the status of the analytic in AX Client.
4. If AX Client shows the analytic ran successfully, you can assign a user rights to the entity in AX Exception Administration and then log in to AX Exception to view the exceptions.
5. If AX Client shows that the analytic did not run successfully, complete the following troubleshooting steps:

- If a result set was created in AX Client check the log file to see if there is a problem with the analytic.
- If the analytic ran successfully but the AX Exception data was not published, check for a job folder created at the time the analytic ran. This folder is created in the `App\Dataloader\sessions` subfolder where AX Server, or the AX Engine Node that ran the analytic, is installed. Check the `dataloader.log` file in the job root directory, and the `ACLProject.log` file in the `output\ACL` subfolder for errors.
- If you are still unable to determine the cause of the problem, check the other logs produced by AX Exception. For more information, see Viewing the service logs.

5.5. Installing self-signed security certificates in Internet Explorer

To avoid encountering certificate error messages when accessing the AX Exception web applications, you can install the self-signed security certificate in Internet Explorer. This task needs to be completed on each computer used to access one or more of the AX Exception applications. The self-signed security certificate is created by the AX Exception setup wizard during installation of AX Exception.

If you have configured a certificate from a Certificate Authority (CA), such as VeriSign, on the AX Exception server you do not need to complete this configuration.

To install the self-signed certificate in Internet Explorer:

1. Open Internet Explorer and navigate to one of the AX Exception web applications:
   - The AX Exception address is https://<*server_name*>/exceptionmgmt
   - The AX Exception Administration address is https://<*server_name*>/ax-em_admin

   Note
   Internet Explorer is the only web browser supported for opening the AX Exception Administration web application.

   You must specify the <*server_name*> as the hostname of the server. For example: https://axexception.acl.com/axadmin

   Note
   If your AX Exception server has been upgraded from a previous version, you may need to specify port 8443 in the address. For example, `https://axexception.acl.com:8443/exceptionmgmt`.
2. Click **Continue to this website (not recommended)**.
3. Click the **Certificate Error** button next to the browser address bar.
4. Click the **View certificates** link.
5. In the **Certificate** dialog box, click **Install Certificate**.
6. Complete the following steps in the **Certificate Import Wizard**:
   a. In the **Welcome** page, click **Next**.
   b. Select **Place all certificates in the following store**, and click **Browse**.
   c. In **Select Certificate Store**, select **Trusted Root Certification Authorities** and click **OK**.
   d. Click **Next**.
   e. Click **Finish** to import the certificate.

f. In the **Security Warning** dialog box, click **Yes** to install the certificate.

g. Click **OK** in the confirmation dialog box to complete the wizard.

7. Click **OK** to close the **Certificate** dialog box.
8. Restart Internet Explorer and navigate to the one of the AX Exception web applications.

   If the certificate is configured correctly, the web application will load without displaying the certificate error page.

6. Uninstalling AX Exception

When you uninstall AX Exception, all of the application files are removed from the server, but the AX Exception database is left in place. You need to manually remove the AX Exception database from Oracle or Microsoft SQL Server.

To uninstall AX Exception from Windows Server 2008 or 2012:

1. Log in to the server you want to uninstall AX Exception from as an Administrator.
2. Navigate to the Windows **Control Panel**, and select **Uninstall a Program**.
3. Select the AX Exception entry in the list and click **Uninstall** in the toolbar.
4. Click **Yes** in the confirmation dialog box.
5. If you are prompted to restart your computer during the uninstall process, click **OK** in the message box and restart your computer after the uninstall process completes.