AX Exception Administration User Guide

Contents

AX Exception Administration User Guide

Contents

Accessing AX Exception Administration

About AX Exception security

Viewing users and their role assignments

Adding users

Modifying user rights

Deleting users

1. Accessing AX Exception Administration

Users that belong to the AX Server Administrator group can log in to the AX Exception Administration web application and administer users and permissions for AX Exception.

Note

Internet Explorer is the only web browser supported by the AX Exception Administration web application.

To access the AX Exception Administration web application:

1. Open Internet Explorer and navigate to the home page for AX Exception Administration. You must belong to the AX Server Administrator group to log in.

   The default location is https://<*server_name*>/ax-em_admin, where <*server_name*> is the hostname or IP address of your AX Exception server. The default HTTPS port is 443 for new AX Server version 5 installations. However, if your AX Server has been upgraded from version 4.x, HTTPS is likely using port 8443, which was the default port used in earlier versions. If the HTTPS port is 8443, you must specify it in the URL.

   For example: https://exception.acl.com:8443/ax-em_admin
2. If you are prompted to log in, enter your username and password and click **Login**.

Related concepts

About AX Exception security

Related tasks

Viewing users and their role assignments

Adding users

Modifying user rights

Deleting users

2. About AX Exception security

The **Users** page displays the users that currently have access to the AX Exception, AX Web Client, and AX Client applications, the roles they belong to, and the entities they have been assigned rights to. The **Users** page displays user rights in a table with the following three columns:

- **Username** – Lists the domain and user account of each user that has been added to ACL Analytics Exchange. The list of users is stored in the ACL Analytics Exchange database, and each user must be assigned rights to access AX Exception, AX Client, and AX Web Client. Rights for AX Client and AX Web Client are administered in AX Client, but are also displayed in AX Exception Administration.
- **AX Exception** – Lists the AX Exception roles the user belongs to. If the role requires that specific entities be assigned, the entities assigned to the user are displayed in brackets after the role. The user can be assigned to one or more of the following roles:
  - **Primary Reviewer** – Users that belong to this role can work with new exceptions in the system for entities that they have been assigned rights for. New exceptions are automatically assigned to the "Assigned to Primary Reviewer" workflow state. The Primary Reviewer can either assign the exception to the Secondary Reviewer, or they can close the exception.
  - **Secondary Reviewer** – Users that belong to this role can work with exceptions in the "In Review" state for entities that they have been assigned rights for.
  - **EM Admin** – Users that belong to this role have access to the purge commands in the **Exception Details** page. They can delete exceptions from the system for the entities they have been assigned rights to using other roles that give them write access to the entities (that is, not the "Read Only EM" role or any custom roles you add that only provide read-only access). For example, if they have been assigned the "Primary Reviewer" role for five entities, they can purge exceptions from these entities based on their combined "EM Admin" and "Primary Reviewer" rights. They cannot purge exceptions from any other entities in the system.
  - **Show All Entities EM** – Users that belong to this role have read-only access to all entities in the system. They can view exceptions for all entities, but cannot edit them or move them to new workflow states. Users that belong to other user groups that give them rights to modify particular entities will still be able to modify those entities, and they will have read-only access to all other entities.
  - **Access All Entities EM** – Users that belong to this role can view and edit all entities in the system.
  - **Read Only EM** – Users that belong to this role have read-only access to entities they have been assigned rights for. They can view the exceptions for these specific entities, but cannot edit them or move them to new workflow states.

  AX Exception can be customized to support additional roles. If additional roles have been created, they will be displayed in the list of roles a user belongs to when they are assigned.
- **AX Server** – Lists the AX Server roles the user belongs to. If no roles are listed, the user cannot log in to AX Client or AX Web Client. AX Server roles cannot be modified in AX Exception Administration.

Related tasks

Accessing AX Exception Administration
Viewing users and their role assignments
Adding users
Modifying user rights
Deleting users

3. Viewing users and their role assignments

To view user rights:

- Open the AX Exception Administration application in your web browser.

  The **Users** page lists all of the users that have access to the system and their role assignments.

Related concepts
About AX Exception security

Related tasks
Accessing AX Exception Administration
Adding users
Modifying user rights
Deleting users

4. Adding users

You can use AX Exception Administration to add users and grant them security rights to access AX Exception.

To add a user:

1. Click the **Add** link in the navigation panel.
2. Enter the following information for the user you want to add:
   - **Active Directory username** – Enter a username exactly as it appears in the user’s Active Directory or local Windows account and click **OK**.

     Note
     For users who belong to an Active Directory domain other than the default domain specified for your ACL Analytics Exchange installation, or for users with a local Windows account, you must include the name of the user’s domain, or the machine name of the AX Server, using the following format: `<domain name>\<username>` or `<server name>\<username>`. For example: BranchOffice\john_smith, or AXServer\ann_wilson.
   - **First name** – Enter the user’s first name.
   - **Last name** – Enter the user’s last name.
   - **Email address** – Enter the user’s email address.

3. To assign the user rights to AX Exception, complete the following steps:
    a. Click **Add Role**.
    b. Select the role to assign from the **AX Exception roles** drop-down list.
    c. If you selected the “Primary Reviewer”, “Secondary Reviewer”, or “Read only EM” role you must add the entities the role is valid for. Select the entity, or entities, you want to assign the user rights to and click **Add Entities** ➕. You can **Ctrl+click** to select multiple entities in the list.
    d. Click **OK**.
4. Click **Save** to add the user.

    If the user is successfully added, a confirmation page is displayed.

Related concepts

About AX Exception security

Related tasks

Accessing AX Exception Administration

Viewing users and their role assignments

Modifying user rights

Deleting users

5. Modifying user rights

You can use the AX Exception Administration application to modify the roles and entities assigned to users.

To modify a user’s rights:

1. In the **Users** page, click the link in the **Username** column for the user you want to update.
2. Modify the following information as necessary:
    - **First name** – The user’s first name.
    - **Last name** – The user’s last name.
    - **Email address** – The user’s email address.
3. To assign the user rights to AX Exception, complete the following steps:
    a. Click **Add Role**.
    b. Select the role to assign from the **AX Exception roles** drop-down list.
    c. If you selected the “Primary Reviewer”, “Secondary Reviewer”, or “Read only EM” role you must add the entities the role is valid for. Select the entity, or entities, you want to assign the user rights to and click **Add Entities** ➕. You can **Ctrl+click** to select multiple entities in the list.
    d. Click **OK**.
4. To remove a user’s AX Exception role assignments, or entities from a role, click the **remove** link beside the role or entity you want to remove.
5. To add additional entities to an existing role, complete the following steps:
    a. Click the **Add Entity** link for the role.
    b. Select the entity, or entities, you want to assign the user rights to and click **Add Entities** ➕. You can **Ctrl+click** to select multiple entities in the list.
    c. Click **OK**.

6. Click **Save** to update the user’s rights.

   If the user is successfully updated, a confirmation page is displayed.

Related concepts

About AX Exception security

Related tasks

Accessing AX Exception Administration
Viewing users and their role assignments
Adding users
Deleting users

6. Deleting users

You can use AX Exception Administration to delete users if the only roles they have been assigned are AX Exception roles. The **Delete** button is disabled in AX Exception Administration if a user account cannot be deleted because there are AX Server roles assigned to the account.

If you want to delete a user that has both AX Server roles and AX Exception roles assigned, you must first remove their AX Exception roles in AX Exception Administration. After the AX Exception roles have been removed you, or another user with AX Server Administrator rights, can delete the user from the system using AX Client.

To delete a user:

1. In the **Users** page, click the link in the **Username** column for the user you want to delete.
2. Click **Delete**.

Related concepts

About AX Exception security

Related tasks

Accessing AX Exception Administration
Viewing users and their role assignments
Adding users
Modifying user rights