KROLL

KROLL LLC

Adding a User to Alation

Standard Operating Procedures

Table of Contents

1.0   Overview (Adding a User to Alation)

This should be an overview of what this SOP is about. What is the history here and some background?

This SOP provides a general initial process of how a new user will request and then be added to the Alation site. The requestor will fill out a form, submit the form and upon approval, receive access to Alation with the appropriate role. This process will evolve as usage of the data catalog increases.

2.0   Adding a User to Alation

2.1   Purpose

Include a simple statement regarding why you are writing this document. It may also be helpful to describe the purpose of the subject matter in the SOP.

2.2   Scope

This describes to whom or under what circumstances (or both) the document applies.

This document will apply to the requestor whether the person is from a Business Unit or from Internal Firm Services.

2.3   Primary Roles & Responsibilities

Position	Description of Responsibilities
DL.Alationsupport@kroll.com	Data Management Group email under VP, Data Analytics, Technology
Alation Server Admin	MANAGE USERS, ASSIGN ROLES, MANAGE SYSTEM SETTINGS, MONITOR TASKS AND USER ACTIVITY and all capabilities of the Alation Catalog Admin

This should be populated with Job Titles – not individual names.

2.4   Definitions/Acronyms

If the definition is standard (accepted throughout the industry) and published, cite the publication (or website).

2.5   Standard Operating Procedure

- **(pre-req) Requestor to view list of Alation roles and the role capabilities to determine what to choose**
- **(pre-req) Requestor to fill out add new user form (found on SharePoint site)**
- Requestor sends the form to DL.Alationsupport@kroll.com email group
- Member of DL.Alationsupport@kroll.com email group will acknowledge receipt
  - Automated response email
- Member of DL.Alationsupport@kroll.com email group will (temporarily as requested by Infrastructure) submit a OnePoint ticket to "Server Database Requests" to add the new user to Azure Active Directory. (**Note:** see Exceptions section 3.3 for more details)
  - (use this link) Server Database Requests | Onepoint (service-now.com)

- Fill in questions with the following information:
  - **Requested For**: left blank?
  - **Select the type of database request**: choose **ACCESS**
  - **List the Server Name**: enter the URL for desired Alation instance
    - https://alation-dev.kroll.com (development instance)
    - https://alation.kroll.com (production instance)
  - **List the Database name**: leave blank
  - **Are you a DIF (Data Insights and Forensics) employee**: No

Adding a User to Alation

- **Explain your request**: name of the person or people you want added and the alation role you want them added to:

Alation Role
Viewer
Composer
Steward
Users
Catalog Admin
Source Admin
Server Admin

- Click Submit

- <mark>Note: Confirm with Shai the turnaround time to add user to security group</mark>
- Approval of OnePoint ticket received
- Member of DL.Alationsupport@kroll.com email group will send the Alation link instance for new user to perform initial authentication
    - Please let the new user know to disregard the message to check their email
        - **Note**: emails will not be sent from Alation to users until the email server has been configured completely
- Member of DL.Alationsupport@kroll.com email group with Alation Server Admin rights will go to:
    - Admin Settings → Users (tab) – User Signup Requests to "Skip Email Confirmation"
        - **Note:** This is only until the email server has been configured completely
- Alation Server Admin will assign the new user to the requested role
- New User will receive an email from Member of DL.Alationsupport@kroll.com email group that the request has been completed

Here is where the user begins to document the process. This SOP may be part of the process. It should begin with that process. Other SOP's can be noted at the end of this SOP that can refer to the process before and the process that follows.

The reader of this SOP should be able to perform the process by reading thru the steps of this document.

Workflows and screenshots may also be included. Samples of data may be used. An example of a Tableau Report may also be used if it is part of the process.

If an email is used in the communication of the process…. a sample email may be included.

Roles and Responsibilities should only be referred to as their job title and not the individual's name.

3.0 Exceptions

3.1 SAML or LDAP Authentication

- Based on pending conversations with members of Infrastructure, the current use of SAML authentication through our identity provider for Single Sign-On may be changed to LDAP authentication. This change may remove the need for opening the OnePoint ticket to add a user to the Azure Active Directory Security Group
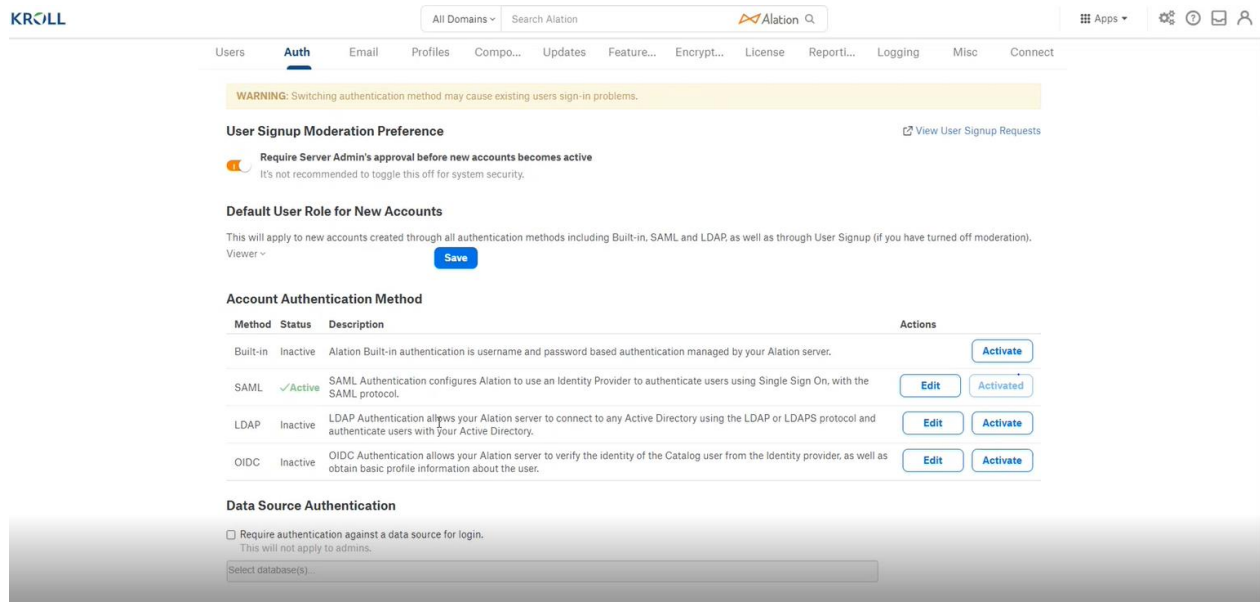
3.2 Pending Email Server Configuration

- Once the email server is fully configured, the new user will receive an email from Alation upon their initial sign-on. From there, the user will be automatically authenticated by the Alation settings. This may eliminate the Alation Server Admin from having to manually confirm to "Skip Email Confirmation" in Admin Settings
  - o Admin Settings → Users (tab) – User Signup Requests to "Skip Email Confirmation"
  - o Alation Technical Support and Kroll Infrastructure is to be scheduled to work together to complete email configuration

3.3 Updates Steps for Submitting a Request

- Once the "Existing Group Names" have been established in OnePoint, the "Add New Users to Existing Security Group | One point" page can be used instead of the Server Database Requests page. Therefore, the steps to submit a ticket for a new Alation user will be updated to include these changes such as:

  - Requestor to view list of Alation roles and the role capabilities to determine what to choose
    - o Found on the SharePoint site
  - Requestor to fill out add new user form
    - o Found on the SharePoint site
  - Requestor sends the form to DL.Alationsupport@kroll.com email group
  - Member of DL.Alationsupport@kroll.com email group will acknowledge receipt

Adding a User to Alation

- o Automated response email
- Member of DL.Alationsupport@kroll.com email group will submit a OnePoint ticket to "Add New User to Existing Security Group" in Azure Active Directory – (use this link) Add New Users to Existing Security Group | Onepoint (service-now.com)

- The "Existing Group Name" will depend on the role for the user:

Alation Role	Existing Group Name
Catalog Admin	DPSA.Alation.CatalogAdmin
Composer	DPSA.Alation.Composer
Steward	DPSA.Alation.Steward
Users	DPSA.Alation.Users
Viewer	DPSA.Alation.Viewer
Source Admin	DPSA.Alation.SourceAdmin
Server Admin	DPSA.Alation.ServerAdmin

- Search for available user
- Click on the name
- Click on **>** to Add name to "Selected box
- Click Submit

- Note: Confirm with Shai the turnaround time to add user to security group
- Approval of OnePoint ticket received
- Member of DL.Alationsupport@kroll.com email group will send the Home | Alation (kroll.com) (Alation Production site) for new user to perform initial authentication
  - Please let the new user know to disregard the message to check their email
    - **Note**: emails will not be sent from Alation to users until the email server has been configured completely
- Member of DL.Alationsupport@kroll.com email group with Alation Server Admin rights will go to:
  - Admin Settings → Users (tab) – User Signup Requests to "Skip Email Confirmation
    - **Note:** This is only until the email server has been configured completely)
- Alation Server Admin will assign the new user to the requested role
- New User will receive an email from Member of DL.Alationsupport@kroll.com email group that the request has been completed

This defines any deviation from this Standard Operating Procedure and that must be documented and approved by the document's owner. Where a situation within this process is ambiguous as to direction, those executing the process confirms their interpretation with the document owner. The document owner has the responsibility to determine where compliance/security/data governance also approve deviation or interpretation.

All events, including incidents and potential incidents, related to the privacy and/or security of sensitive information within this process shall be immediately reported to Compliance and Security. It is the responsibility of all roles described in this document, not just the document owner or manager to escalate situations that could potentially impact security and/or privacy.

4.0   Change Control Log for this Procedure

All modifications to the process must be updated in this document and approved by the document owner. The document owner as the responsibility to determine where compliance and/or security also approve the change

Date	Brief Description of Change	Author	Approver

5.0   References

List all citations and references to other documents/tools. If none, include "None" herein.

6.0   Appendices

Use appendices sparingly. If forms or other items are included as appendices, consider identifying them as EXAMPLES if it is acceptable to edit them when they are used. If no appendices are included, delete this section