ELECTRICITY AUTHORITY
TE MANA HIKO

Single sign-on Registry integration

18 May 2024

Contents

1. Feature overview

Registry Single Sign-On is designed to facilitate single sign-on (SSO) access to the Registry, enabling the automatic synchronization of Users and Security groups between the Registry and a participants AzureAD system.

To utilize SSO, it is essential for a participant to employ AzureAD as their Identity and Access Management (IAM) system. This requirement ensures access to the Microsoft Authentication Flow.

A participant will be able to:

a) maintain users of the Registry inside their own AzureAD system

b) maintain user access permissions on the Registry by synchronising user assignment to Security groups with equivalent security groups held by the Registry using SCIM API calls.

c) Logon to the Registry using a SSO link which will authenticate using the participants AzureAD credential.

Security group

- A security group, consisting of a unique name and a set of permissions, is an identifier existing in the Registry and in a participants own AzureAD system.
- Security group name uniqueness is enforced in the Registry via a naming convention.
- A Registry Participant maintains security group(s) within the Registry and assigns to each security group the security resources (aka *permissions*) that users assigned to the security group may access.
- Inside their own AzureAD system a participant creates *equivalently named* security groups and maintains users in those security groups (User Group assignment)
- Users and user security group assignment are synchronised with the Registry via SCIM APIs.

Security group implementation – important note

In the context of an SSO implementation, it is typically standard to handle permissions through the IAM system. Nevertheless, the Registry diverges from this norm by internally managing permissions to cater for participants who *do not* utilize SSO and would otherwise have no visibility to permissions.

Consequently, this requires participants utilizing SSO to:

a. Manually establish security groups in the Registry and assign permissions to these groups within the Registry.

b. Create security groups with identical names within their AzureAD system.

Users

- Participants do not explicitly create user accounts within the Registry.
- Users are maintained within a participant's own AzureAD and uniquely identified to the Registry by their email address. These are sent to the Registry via a SCIM API.

- Where a SCIM update creates a new user; that is a user with an email address that is not assigned to an existing user, a new user is created in the Registry and provided with a unique identifier, the unique identifier must be provided if the user is subsequently updated.
- When a user is assigned to a security group (within a Participants AzureAD system) the user is synchronised with the Registry via a SCIM API, and then has access to the permissions for that security group.

Accessing the Registry using SSO

- A user accessing the Registry website may select to login using SSO (via a link in the Registry login page). At that point, the user will enter the Microsoft Authentication Flow.
- The user enters their email address and are re-directed to their own AzureAD system where they supply their corporate credentials (and any additional authentication as prescribed by the participant).
- The user is returned to the Registry with an authentication (bearer) token, and their email address as a claim inside the token.
- The Registry validates the token and locates the Registry User from the email claim. The user is granted access to the Registry with the permissions for their assigned Security Group(s).

Developer portals

The Registry provides developer portals for UAT and production to allow developers to understand, integrate and consume the SCIM APIs.

SCIM API security

As part of initial configuration, the Registry help desk provides a Long-Term Access token (LTA). The LTA is required as a bearer token for all SCIM API calls made to the Registry.

The LTA is valid for a Registry environment; that is, a separate LTA is provided for access to UAT and Production.

2. Key concepts

Security group maintenance within the Registry and AzureAD

- Maintenance of security groups is performed independently in the Registry and in the participants AzureAD system.
- A participant creates security groups within the Registry and assign permissions to each security group.
- A participant must create *equivalently named* security groups within their own AzureAD systems.

Users security group access is not maintained within the Registry

- A participant using SSO is not required to maintain users in the Registry. User maintenance is entirely inside a participants AzureAD system.

- The user is assigned to one or more security groups and inherits all the permissions associated with those security groups.
- A user not assigned at a security group retains inquiry only access to the Registry.

AzureAD and Registry synchronisation

- Users and user security group assignment is synchronised with the Registry via SCIM APIs with each call supplying the Environment specific Long-Term Access Token (LTA) as a bearer token.

3. How the feature works

There are several steps involved in setting up SSO, these include registering your AzureAD instance within the Registry, setting up security groups, configuring SCIM interface within AzureAD using the supplied LTA, and finally synchronising users and user security goup assignments.

Requesting access to AzureAD Registry Application

1. Contact the Registry help desk and request access to Registry SSO.
    a. You must provide your unique AzureAD identifier (/tenant ID) which uniquely identifies your instance of AzureAD, the help desk will register the tenant id against your Registry participant identifier.
    b. If you have more than one participant identifier within the Registry using the same AzureAD instance, then each will need to be configured by the help desk to point to that instance. This will allow the authentication flow to direct each user logon to the correct participant AzureAD to complete their login.
2. Jade help desk will respond with:
    a. a long-term access token (LTA) for the Registry environment in which it will be used (UAT or Production), The LTA specific to the Registry environment must be provided by the participant when they call any of the SCIM APIs
        i. The LTA will be delivered via a secure mechanism
        ii. The LTA *must not be shared*
        iii. The LTA has a limited life span; however, the Registry helpdesk will inform the participant when the LTA is within 3 weeks of expiry allowing time to either generate a new token or extend the life of the existing token
    b. The SCIM API endpoints (which must be configured in your AzureAD system)
    c. Links to the UAT and production developer portals
    d. Optional pre-generation and population of security groups and user security group assignments (refer *Automatic Security Group Creation*)

Long term access token

The LTA must be provided for all SCIM API calls and match the LTA recorded for the Registry environment (UAT or production).

Creating unique security groups within the Registry

A supervisor user must access the Registry browser interface and on the security group maintenance screen maintain unique security group names and the permissions assigned to each security group.

The Registry will enforce a security group naming convention of <*Participant identifier*>_<*free text description*>, for example:

- RETA_TraderSwitching

A security group can be removed or have its *free text description* modified as desired.

Automatic security group creation

For initial setup, the Registry can automatically generate security group names based on permissions assigned to existing users and populate the security groups with users that have current access to the permissions.

Inquiry security group

By default, an inquiry only security group with no permissions is created.

We recommend the inquiry only security group contains users that have no permissions assigned; that is, users with *inquiry only* access to the Registry. Assigning users to this group provides clarity in identifying users with inquiry only access, however the Registry does not mandate this and a user with no security groups assignments retains inquiry only access.

The *free text description* will be *Inquiry*, for example "*RETA_Inquiry*." For clarity it is recommended this security group name is not changed.

Supervisor security group

By default, a supervisor security group will always be created.

This security group will contain users that have supervisor access the Registry.

The *free text description* will be *Supervisor*, for example "*RETA_Supervisor*." For clarity it is recommended this group name is not changed.

Non-inquiry security groups

Security groups that contain specific permissions are created with a naming convention containing Functional Specification process identifiers, for example:

a) Users with access to trader maintenance only will be placed in a security group named *RETA_RM010*. Where RM010 is the functional specification process identifier for trader maintenance

b) Users with access to trader maintenance and audit compliance report will be placed in a security group named *RETA_RM010AC020*

c) Users with access to trader maintenance, audit compliance report and (all) trader switching will be placed in a security group named *RETA_RM010AC020RS010RS020RS050RW010RW020*

(note: colour used in above examples for effect only)

We recommend the default naming convention is amended to clearly identify the purpose of the security group, for example:

- *“RETA_RM010AC020RS010RS020RS050RW010RW020”* might become
- *“RETA_TraderMaintAuditAndSwitching”*

(note: The SCIM max length for security group name is restricted to 75 characters, this may result in shorthand names being generated; that is, names ending in “….”)

Configuring SCIM interface

The SCIM interface must be configured within your IAM system using the endpoints supplied by the Jade help desk (and as described in the developer portal).

Each SCIM API call must include the LTA token as a bearer token.

Creating security groups within your AzureAD system

Once all security groups have been created and verified in the Registry, security groups with the exact same name as those in the Registry must be setup in your AzureAD system.

Updating SSO users onto the Registry

The Registry must be made aware of the users that will sign on using SSO.

For each user you wish to enable SSO call the SCIM Create User API.

Updating users to the security groups in your AzureAD system

Once all users have been updated onto the Registry and all security groups have been setup in your AzureAD system start assigning users to security group(s).

For each assignment AzureAD must call the SCIM Update Group API.

Manually updating users to security groups in the Registry

(If there are issues with maintaining Users via the SCIM interface, in the first instance contact the Registry helpdesk to assist in resolving the issue).

Users can be manually assigned to security groups using Registry supervisor functions. However, this is not recommended, unless there is an issue with the SCIM synchronising process that cannot be easily or quickly resolved.

Updates from your IAM system are sent to the Registry, manual updates to security group assignments entered directly to the Registry are not sent back to you; that is, synchronisation is a one-way process.

Appendix A SCIM API calls (summary)

Refer to the developer portal for further information and examples

Verb	Name	Description
POST	Create User	Create a user
DEL	Delete user	Delete a user, requires a parameter of User Id
GET	All groups	Get all security groups in the Registry
GET	All users	Get all users in the Registry
GET	Group	Get a specific group, requires a parameter of Group Id
GET	User	Get a specific user requires a parameter of User Id
PATCH	Update Group	Update a security group; that is assign or remove a user from a group, requires a parameter of Group Id
PATCH	Update User	Update information on a specific user, requires a parameter of User Id

Appendix B Registry process identifiers

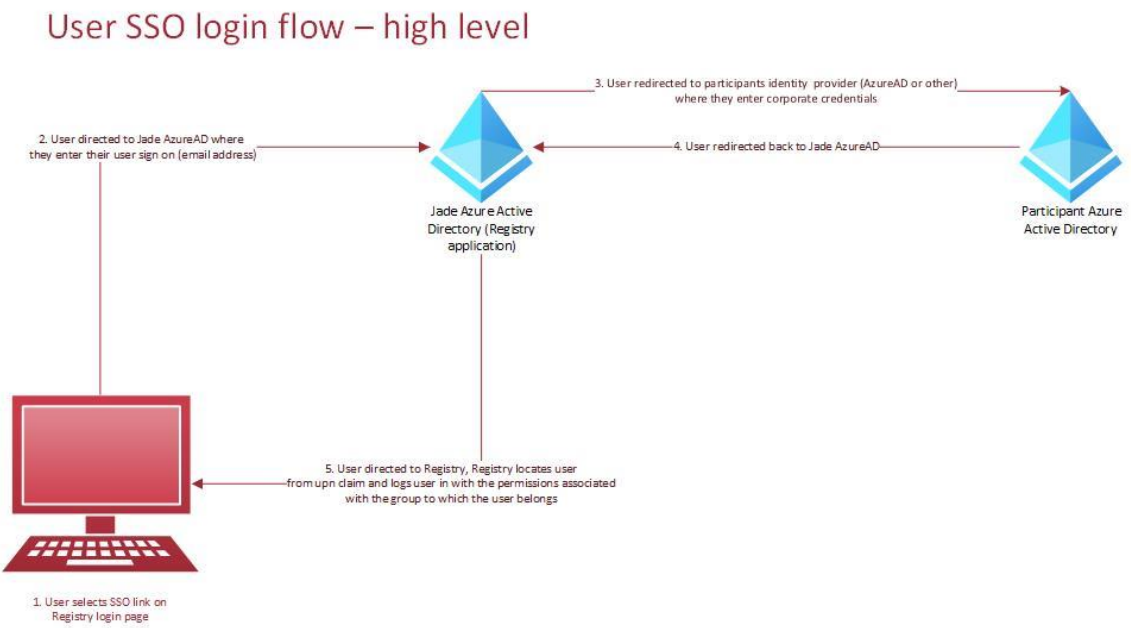
Process Id	Description
DC-010	Create and ICP (Installation Control Point)
DC-020	Make a new ICP ready
DC-030	Make a new ICP distributor
DM-010	Change initial ICP creation date
DM-020	Add additional Distributor information
DM-030	Correct Distributor information
DM-040	Reverse Distributor information
RA-010	Trader becomes responsible for an ICP – Initial Assignment
RM-010	Trader cancels the initial assignment
RM-020	Add new Trader information
RM-030	Correct Trader information
RM-040	Reverse Trader information
MM-010	Add new metering information
MM-020	Correct metering information
MM-030	Reverse metering information

Process Id	Description
MM-040	Missing MEP (Metering Equipment Providers) Ownership Historical Insertion
RS-010	Make switch request (NT (Notice of Transfer))
RS-020	Acknowledge switch request (AN)
RS-050	Complete switch or replace switch reading (CS and RR)
RW-010	Make withdrawal request (NW)
RW-020	Acknowledges withdrawal request (AW)
RC-020	Acknowledge switch read change (AC)
MN-010	Accept or decline MEP responsibility for ICP (MN)
PR-010	Produce ICP list (on demand)
PR-015	Produce current details report
PR-030	Produce ICP event detail audit report
PR-035	Produce ICP Attribute Changes
PR-040	Produce switch compliance reports
PR-060	Produce audit log
PR-065	Request file handler status
PR-090	Produce active NSPs (Network Supply Point) report
PR-100	Produce loss factors report
PR-110	Produce maintenance compliance report
PR-120	Produce NSP (Network Supply Point) mapping table report
PR-130	Produce monthly activity and status summary report
PR-140	Produce monthly switch completion report
PR-210	Missing Metering Data
PR-220	Uncertified Metering Installations
PR-230	Electrical Connection Misalignment
PR-240	Profiles Misalignment
PR-250	Produce Trader Default General Information
PR-255	Produce Metering Installation Information
PR-270	Produce report of Traders in a trader default situation by NSP
PR-280	Responsibility outside Participant Role
PR-290	Produce Trader Default Situation Market Share Report

Process Id	Description
PR-300	Report Trader Default tender and mandatory assignment
PR-310	Report Trader Default allocation results
PR-320	Monitor switch saving protection scheme
PR-330	Produce Distributor Annual Levy report
PR-340	Produce Trader Annual Levy report
PR-350	Produce Trader Default Status
PR-360	ATH (Approved Test House) and MEO (Metering Equipment Owner) Metering Report
AC-020	Produce Audit compliance report
NP-040	Re-send switching messages
NP-050	Re-send notifications
SD-010	Maintain NSP data
SD-030	Maintain Distributor Loss Category Codes
SD-040	Maintain Distributor Price Category Codes
SD-050	Maintain email Groups
SD-060	Maintain contact Groups
SU-010	Add and maintain new Users
SU-020	Disable and re-enable logons
SU-040	Assign agent
SU-060	Assign Participant audit agent
EI-010	Configure EIEP (Electricity Information Exchange Protocols) Transfer Settings
EI-020	Upload and Download EIEP via the browser
EI-030	Transfer EIEP Files
TD-020	Maintain Trader ICP Allocation Exclusion List
TD-060	tender and mandatory assignment allocation results

Appendix C High level integration

SSO login



Maintaining User Group Assignment