==========

==========

CATEGORY: AzureAD / Entra ID

==========

==========

SOP 1 – Get Entra ID User Details

Script Name: Get Entra ID User Details **Category:** AzureAD / Entra ID **Version:** 1.0 **Approved By:** IT Operations / Security

1. Purpose

This script retrieves detailed information about an Entra ID (Azure AD) user account, including identity attributes, licensing, and status. It provides a standardized, auditable method for cloud identity inspection.

2. Scope

- **Systems:** Any RDAM-authorized workstation with Entra ID connectivity.
- **Directory:** Microsoft Entra ID tenant(s) authorized for RDAM.
- **Authorized Personnel:**
    - IAM engineers
    - Cloud administrators
    - Security analysts

3. Definitions

- **Entra ID User:** Cloud identity object representing a person or service.
- **UPN:** User Principal Name (user@domain.com).
- **Object ID:** Unique GUID assigned to the identity.

4. Preconditions

- Operator must have read permissions in Entra ID.
- RDAM must be authenticated to Entra ID via delegated or app-based permissions.

- Network access to Microsoft Graph endpoints.

5. Required Inputs

- User identifier (UPN, Object ID, or email).

6. Procedure Steps

1. **Input Collection**
    - Wizard prompts for user identifier.
    - Validate non-empty.
2. **Identity Resolution**
    - Query Microsoft Graph for the user.
    - If multiple matches, return ambiguity warning.
3. **Attribute Retrieval**
    - Retrieve:
        - DisplayName
        - UserPrincipalName
        - ObjectId
        - AccountEnabled
        - AssignedLicenses
        - AssignedPlans
        - Sign-in status
        - Directory roles (if permitted)
4. **Output Formatting**
    - Present structured results (JSON/table).
5. **Logging**
    - Log operator, user identifier, timestamp.

7. Expected Output

- Full user profile details from Entra ID.

8. Post-Execution Validation

- IAM may compare results with Microsoft 365 Admin Center.

9. Error Handling

- User not found.
- Access denied.
- Graph API unreachable.

10. Security Considerations

- Cloud identity data is sensitive; restrict access.
- Do not export results outside approved channels.

11. Audit Logging Requirements

- Operator ID
- User identifier
- Timestamp
- Success/Failure

12. Organizational Benefit Statement

This script provides a consistent, auditable method for retrieving cloud identity details, supporting troubleshooting, governance, and compliance.

SOP 2 – List User’s Entra ID Groups

Script Name: List User’s Entra ID Groups **Category:** AzureAD / Entra ID

1. Purpose

This script retrieves all Entra ID groups a user belongs to, including direct and optionally transitive memberships. It supports access reviews and troubleshooting.

2. Scope

- All Entra ID groups (security, Microsoft 365, dynamic).
- Used by IAM and security teams.

3. Definitions

- **Transitive Membership:** Group membership inherited through nested groups.
- **Security Group:** Used for access control.
- **M365 Group:** Used for collaboration.

4. Preconditions

- Operator must have read access to group membership.
- Graph API connectivity.

5. Required Inputs

- User identifier (UPN/Object ID).
- Optional: Include transitive memberships.

6. Procedure Steps

1. **Input Collection**
    - Wizard prompts for user identifier and transitive flag.
2. **User Resolution**
    - Query Graph to locate user.
3. **Group Enumeration**
    - Retrieve direct memberships.
    - If transitive enabled, expand nested groups.
4. **Output Formatting**
    - List group names, IDs, types.
5. **Logging**
    - Log user and group count.

7. Expected Output

- List of groups the user belongs to.

8. Post-Execution Validation

- IAM may compare with Access Reviews or PIM.

9. Error Handling

- User not found.
- Access denied.

10. Security Considerations

- Group membership reveals privilege level; restrict access.

11. Audit Logging Requirements

- Operator ID
- User identifier
- Group count
- Timestamp

12. Organizational Benefit Statement

This script supports identity governance by providing a clear, auditable view of user group memberships in Entra ID.

SOP 3 – Get Entra ID Group Members

Script Name: Get Entra ID Group Members **Category:** AzureAD / Entra ID

1. Purpose

This script retrieves all members of an Entra ID group, supporting access reviews, troubleshooting, and compliance audits.

2. Scope

- Security groups
- Microsoft 365 groups
- Dynamic groups

3. Definitions

- **Group Member:** User, device, or service principal assigned to the group.

4. Preconditions

- Operator must have read access to group membership.
- Group must exist.

5. Required Inputs

- Group identifier (name/Object ID).

6. Procedure Steps

1. **Input Collection**
    - Wizard prompts for group identifier.

2. **Group Resolution**
    - Query Graph to locate group.
3. **Membership Retrieval**
    - Retrieve all members.
    - Handle pagination if large group.
4. **Output Formatting**
    - List members with type and ID.
5. **Logging**
    - Log group and member count.

7. Expected Output

- Full list of group members.

8. Post-Execution Validation

- IAM may compare with M365 Admin Center.

9. Error Handling

- Group not found.
- Access denied.

10. Security Considerations

- Group membership may reveal privileged identities.

11. Audit Logging Requirements

- Operator ID
- Group identifier
- Member count
- Timestamp

12. Organizational Benefit Statement

This script provides a controlled, auditable method for reviewing group membership, supporting compliance and access governance.

SOP 4 – Add User to Entra ID Group

Script Name: Add User to Entra ID Group **Category:** AzureAD / Entra ID

1. Purpose

This script adds a user to an Entra ID group in a controlled, logged manner, supporting access provisioning workflows.

2. Scope

- Security and M365 groups.
- Used by IAM and helpdesk with delegated rights.

3. Definitions

- **Group Assignment:** Adding a user to a group for access or collaboration.

4. Preconditions

- Operator must have write access to group membership.
- Group and user must exist.
- Action must align with approved access request.

5. Required Inputs

- User identifier
- Group identifier

6. Procedure Steps

1. **Input Collection**
    - Wizard prompts for user and group.
2. **Resolution**
    - Resolve both objects via Graph.
3. **Membership Check**
    - If user already in group, return informational message.
4. **Add Operation**
    - Add user to group via Graph API.
5. **Verification**

    - Requery group to confirm membership.
6. **Logging**
    - Log operator, user, group, timestamp.

7. Expected Output

- Confirmation of successful membership addition.

8. Post-Execution Validation

- IAM may verify via M365 Admin Center.

9. Error Handling

- User/group not found.
- Access denied.
- Group type not supported.

10. Security Considerations

- Adding users to privileged groups must follow strict approval workflows.

11. Audit Logging Requirements

- Operator ID
- User
- Group
- Timestamp

12. Organizational Benefit Statement

This script ensures access provisioning is consistent, auditable, and aligned with governance policies.

SOP 5 – Remove User from Entra ID Group

Script Name: Remove User from Entra ID Group **Category:** AzureAD / Entra ID

1. Purpose

This script removes a user from an Entra ID group, supporting de-provisioning and access cleanup.

2. Scope

- Security and M365 groups.

- Used by IAM and security teams.

3. Definitions

- **De-provisioning:** Removal of access when no longer required.

4. Preconditions

- Operator must have write access to group membership.
- Action must align with approved request.

5. Required Inputs

- User identifier
- Group identifier

6. Procedure Steps

1. **Input Collection**
    - Wizard prompts for user and group.
2. **Resolution**
    - Resolve both objects.
3. **Membership Check**
    - If user not in group, return informational message.
4. **Remove Operation**
    - Remove user via Graph API.
5. **Verification**
    - Confirm removal.
6. **Logging**
    - Log operator, user, group, timestamp.

7. Expected Output

- Confirmation of removal.

8. Post-Execution Validation

- IAM may verify via M365 Admin Center.

9. Error Handling

- User/group not found.
- Access denied.

10. Security Considerations

- Removing users from critical groups may impact access; ensure approvals.

11. Audit Logging Requirements

- Operator ID
- User
- Group
- Timestamp

12. Organizational Benefit Statement

This script ensures access removal is consistent, auditable, and aligned with least-privilege principles.

SOP 6 – List Entra ID Devices

Script Name: List Entra ID Devices **Category:** AzureAD / Entra ID

1. Purpose

This script retrieves all devices registered in Entra ID, supporting inventory, compliance, and troubleshooting.

2. Scope

- Entra ID registered and joined devices.
- Used by IAM, security, and endpoint teams.

3. Definitions

- **Registered Device:** Device registered for SSO or conditional access.
- **Joined Device:** Device joined to Entra ID for full management.

4. Preconditions

- Operator must have read access to device objects.
- Graph API connectivity.

5. Required Inputs

- Optional: Filter (OS, join type, enabled state).

6. Procedure Steps

1. **Input Collection**
    - Wizard prompts for optional filters.
2. **Device Enumeration**
    - Query Graph for devices.
3. **Filtering**
    - Apply filters if provided.
4. **Output Formatting**
    - List devices with:
        - Name
        - Object ID
        - OS
        - Join type
        - Enabled state
5. **Logging**
    - Log count and operator.

7. Expected Output

- List of devices matching criteria.

8. Post-Execution Validation

- Endpoint team may cross-check with Intune.

9. Error Handling

- Access denied.
- Graph API unreachable.

10. Security Considerations

- Device inventory is sensitive; restrict access.

11. Audit Logging Requirements

- Operator ID
- Filter used
- Device count
- Timestamp

12. Organizational Benefit Statement

This script provides a centralized, auditable view of cloud-registered devices, supporting compliance and asset management.

SOP 7 – Get Conditional Access Policies

Script Name: Get Conditional Access Policies **Category:** AzureAD / Entra ID

1. Purpose

This script retrieves all Conditional Access (CA) policies in Entra ID, supporting security audits, troubleshooting, and compliance.

2. Scope

- All CA policies in the tenant.
- Used by IAM and security teams.

3. Definitions

- **Conditional Access Policy:** Rule controlling authentication and access conditions.

4. Preconditions

- Operator must have read access to CA policies.
- Graph API connectivity.

5. Required Inputs

- None (unless filtering is implemented).

6. Procedure Steps

1. **Policy Enumeration**
    - Query Graph for all CA policies.
2. **Attribute Retrieval**

- Retrieve:
    - Name
    - State (enabled/disabled)
    - Conditions
    - Grant controls
    - Session controls

3. **Output Formatting**
    - Present structured policy list.
4. **Logging**
    - Log operator and policy count.

7. Expected Output

- Full list of CA policies with details.

8. Post-Execution Validation

- Security team may compare with portal.

9. Error Handling

- Access denied.
- Graph API unreachable.

10. Security Considerations

- CA policies define security posture; restrict access strictly.

11. Audit Logging Requirements

- Operator ID
- Policy count
- Timestamp

12. Organizational Benefit Statement

This script provides a controlled, auditable method for reviewing CA policies, supporting compliance and security governance.

SOP 8 – Get Sign-In Logs

Script Name: Get Sign-In Logs **Category:** AzureAD / Entra ID

1. Purpose

This script retrieves Entra ID sign-in logs for users, supporting security investigations, access troubleshooting, and compliance reporting.

2. Scope

- User sign-ins
- Application sign-ins
- Conditional Access results

3. Definitions

- **Sign-In Log:** Record of authentication attempts.

4. Preconditions

- Operator must have read access to sign-in logs.
- Graph API connectivity.

5. Required Inputs

- User identifier (optional).
- Time range.
- Optional filters (status, app, location).

6. Procedure Steps

1. **Input Collection**
    - Wizard prompts for filters.
2. **Query Construction**
    - Build Graph query with filters.
3. **Log Retrieval**
    - Retrieve sign-in logs.
    - Handle pagination.
4. **Output Formatting**

- Present logs with:
    - Timestamp
    - User
    - App
    - IP
    - Result
    - Conditional Access outcome

5. **Logging**
    - Log operator and query parameters.

7. Expected Output

- List of sign-in events matching criteria.

8. Post-Execution Validation

- Security team may correlate with SIEM.

9. Error Handling

- Access denied.
- API throttling.
- Invalid filters.

10. Security Considerations

- Sign-in logs contain sensitive authentication data; restrict access.

11. Audit Logging Requirements

- Operator ID
- Filters used
- Log count
- Timestamp

12. Organizational Benefit Statement

This script provides a controlled, auditable method for retrieving authentication logs, supporting incident response and compliance.