AD Administration Tab — Standard Operating Procedure (SOP)

For Organizational Stakeholders, Security Leadership, and Systems Integrators

Purpose

The AD Administration tab provides a unified interface for performing high-impact Active Directory operations with forensic clarity and zero ambiguity. It is designed for organizations that require controlled, auditable, and efficient directory administration without relying on scattered MMC consoles, PowerShell scripts, or tribal knowledge.

This module centralizes user, group, and OU administration into a single operational pane, ensuring consistency, accountability, and compliance across the enterprise.

Capabilities Overview

User Administration

- **Find User**: Rapidly locate any AD user by name, SAM account, or partial match.
- **Create User**: Launches a guided creation workflow enforcing naming standards, OU placement rules, password policies, and attribute completeness.
- **Modify User**: Update attributes, enable/disable accounts, reset passwords, unlock accounts, and manage group membership.
- **User History**: Displays a full audit trail of attribute changes, group membership modifications, and account control events.

Group Administration

- **Find Group**: Search for security or distribution groups across the domain.
- **Create Group**: Enforces organizational naming conventions, scope selection, and type selection.
- **Manage Membership**: Add or remove members with immediate audit logging.
- **Group Properties**: View scope, type, description, and membership count at a glance.

OU Administration

- **Find OU**: Navigate the directory structure to locate organizational units.
- **Create OU**: Enforce structural standards and apply baseline GPO links automatically.
- **Move Objects**: Relocate users, groups, or computers with full audit tracking.

Object Recovery

- **Resurrect Object**: Restore deleted AD objects using tombstone reanimation or AD Recycle Bin (if enabled).
- **Attribute Preservation**: RDAM attempts to restore original attributes, group memberships, and OU placement when possible.

Operational Workflow

1. Identity or Object Selection

Operators begin by selecting a user, group, or OU. RDAM immediately loads:

- **Distinguished Name**
- **Object type**
- **Attribute summary**
- **Membership or child objects**

This eliminates the need for multiple MMC snap-ins.

2. Action Execution

Once an object is selected, operators can:

- **Modify attributes**
- **Adjust group membership**
- **Move the object**
- **Reset passwords**
- **Enable/disable accounts**

All actions are validated before execution to prevent misconfiguration.

3. Audit Logging

Every action is logged with:

- **Operator identity**
- **Timestamp**
- **Before/after values**
- **Affected object DN**

This supports compliance frameworks such as:

- **NIST 800-53**

- **CMMC**
- **ISO 27001**

Organizational Benefits

For ISSMs & ISSOs

- **Centralized governance**: All AD changes flow through a single, auditable interface.
- **Reduced insider risk**: Eliminates unauthorized or undocumented AD modifications.
- **Compliance alignment**: Provides evidence for access control and identity management controls.

For CIOs & IT Directors

- **Operational efficiency**: Reduces administrative overhead and training requirements.
- **Standardization**: Enforces consistent workflows across teams and contractors.
- **Visibility**: Provides real-time insight into identity operations.

For System Integrators

- **Rapid deployment**: No need to build custom scripts or consoles.
- **Repeatable workflows**: Ensures consistent AD administration across client environments.
- **Reduced error surface**: Guided workflows prevent misconfigurations.

For Security & Incident Response Teams

- **Immediate access to identity data**
- **Fast rollback of changes**
- **Object recovery capabilities**

Summary

The AD Administration tab transforms Active Directory management from a fragmented, error-prone process into a unified, auditable, and secure operational workflow. It empowers organizations to enforce identity governance, reduce administrative risk, and maintain compliance with industry standards — all while dramatically improving efficiency.