SOP-AD-002_Mac_AD_Integration_v1.0.0

SOP-AD-002_Mac_AD_Integration_v1.0.0

Standard Operating Procedure: SOP-AD-002

1. Document Control

- **SOP Number:** SOP-AD-002
- **Title:** Adding Mac Device to Active Directory Domain
- **Version:** 1.1
- **Effective Date:** 2025-12-02
- **Author:** Gemini Agent
- **Approval:** IT Department Head (Placeholder)

2. Purpose

This Standard Operating Procedure (SOP) outlines the step-by-step process for securely adding a macOS device to an Active Directory (AD) Domain, ensuring proper integration with organizational network services and authentication systems.

3. Scope

This SOP applies to all IT personnel responsible for configuring and managing Apple macOS devices within the organization's network environment.

4. Definitions / Acronyms

- **AD:** Active Directory
- **macOS:** Apple's proprietary operating system for its Mac line of computers.
- **Directory Utility:** A macOS application used to configure directory services, including Active Directory integration.
- **Domain Admin:** An account with administrative privileges within the Active Directory domain.

5. Responsibilities

- **IT Administrators:** Responsible for executing this procedure and ensuring the Mac device is successfully joined to the Active Directory domain.

5.1 Prerequisites (VERIFY BEFORE PROCEEDING)

Before attempting to bind to Active Directory, verify the following:

1. **Network Connectivity:**
   - Mac is connected to the corporate network (wired or VPN).
   - Mac can reach the domain controller: `ping <domain_controller_ip>`
2. **DNS Configuration:**
   - Mac's DNS must point to the domain controller(s).
   - Verify DNS: Open **System Settings > Network > [Your Connection] > Details > DNS**.
   - Test DNS resolution: `nslookup <domain_name>` should return DC IP addresses.
3. **Domain Controller Reachability:**
   - Test LDAP connectivity: `bash nc -zv <domain_controller_ip> 389`
   - Test Kerberos connectivity: `bash nc -zv <domain_controller_ip> 88`
4. **Time Synchronization:**
   - Kerberos requires time within 5 minutes of DC.
   - Verify: **System Settings > General > Date & Time** - ensure "Set time and date automatically" is enabled.
5. **Domain Admin Credentials:**
   - Have credentials ready for a Domain Admin account authorized to join computers.

6. Procedure

Follow these steps to add a Mac device to the Active Directory Domain:

1. **Open Directory Utility:**
   - Press `Command + Space` to open Spotlight Search.
   - Type "Directory Utility" and press Enter to open the application.
2. **Unlock for Changes:**
   - Click the padlock icon at the bottom-left corner of the Directory Utility window.
   - Enter the administrator password for the Mac device when prompted to allow modifications.
3. **Select Active Directory:**
   - In the Directory Utility window, select the "Active Directory" service.

- Click the pencil icon (Edit) at the bottom of the window to configure the service.

4. **Enter Domain Information:**
   - In the "Active Directory Domain" field, type the full Active Directory domain name (FQDN format, e.g., `corp.contoso.com`).
   - The "Computer ID" field will automatically populate with the Mac's hostname.
   - **IMPORTANT:** Click the disclosure triangle next to "Show Options" to configure advanced settings.
5. **Configure Advanced Options (CRITICAL):**

   User Experience Tab:
   - **Create mobile account at login:** ENABLE (allows offline login for laptop users)
   - **Require confirmation before creating a mobile account:** Optional (set based on policy)
   - **Force local home directory on startup disk:** ENABLE (recommended for laptops)

   Mappings Tab:
   - **UID/GID mapping:** Leave as default unless specific mapping is required.

   Administrative Tab:
   - **Allow administration by:** Select AD groups that should have local admin rights on this Mac.
   - Common groups: `Domain Admins`, `IT Administrators`, or a custom group like `Mac-LocalAdmins`.
   - Format: `DOMAIN\GroupName` or just `GroupName` if domain is understood.
6. **Bind to Domain:**
   - Click the "Bind" button.
7. **Provide Domain Administrator Credentials:**
   - A new window will appear, prompting for a network domain administrator login.
   - Enter the username and password for a valid Domain Admin account.
   - Click "OK."
8. **Confirm Integration:**
   - Allow a few minutes for the binding process to complete. The Mac device will connect to the Active Directory domain.

- A green indicator should appear next to "Active Directory" in Directory Utility.
- Verify the connection by checking System Settings (or System Preferences) > Users & Groups > Login Options, or by attempting to log in with a domain user account.

7. Verification

1. **Check AD Binding Status (Terminal):** `bash dsconfigad -show` Should display the Active Directory domain and forest information.
2. **Verify User Lookup:** `bash dscl /Search -read /Users/<domain_username>` Should return user attributes from Active Directory.
3. **Test Kerberos Authentication:** `bash kinit <domain_username>@<DOMAIN.COM>` `klist` Should obtain and display a Kerberos ticket.
4. **Test Domain Login:**
   - Log out of the Mac.
   - At the login window, enter domain credentials: `DOMAIN\username` or `username@domain.com`.
   - First login will create a mobile account (if configured).

8. Troubleshooting

Error	Cause	Resolution
"Invalid credentials" during bind	Wrong password or account lacks permissions	Verify Domain Admin credentials. Try `DOMAIN\username` format.
"Unable to contact domain"	DNS not pointing to DC	Verify DNS settings point to domain controller. Test with `nslookup <domain>`.
"Unknown server or domain"	FQDN not used or DNS issue	Use full FQDN (e.g., `corp.contoso.com` not just `contoso`).
Bind succeeds but login fails	Mobile account not created, or time skew	Enable "Create mobile account at login". Verify time sync.
"Authentication server could not be contacted"	Kerberos ports blocked	Verify ports 88 (Kerberos) and 389 (LDAP) are open to DC.
Login works but no admin rights	Admin group not configured	Check "Allow administration by" in Directory Utility advanced options.

Error	Cause	Resolution
Slow login or "network account unavailable"	Network issues or DC unreachable	Check network connectivity. Consider mobile account for offline login.

CLI Unbind (if needed):

```
sudo dsconfigad -remove -force -username <domain_admin> -password <password>
```

9. Related Documents

- SOP-AD-001: Active Directory Domain Connection Troubleshooting
- Apple Platform Deployment Guide: https://support.apple.com/guide/deployment/

10. Revision History

Version	Date	Description of Change	Author
1.0	2025-12-02	Initial release	Gemini Agent
1.1	2025-12-29	SME Review: Added Section 5.1 Prerequisites with connectivity checks. Added Step 5 Advanced Options (mobile account, admin groups, UID mapping). Added Section 7 Verification with Terminal commands. Added Section 8 Troubleshooting table.	Jeremy Smith