SOP-HYB-001__Hybrid__AD__v1.0.0

SOP-HYB-001__Hybrid__AD__v1.0.0

SOP-HYB-001: Hybrid Active Directory Architecture and Management

Version: 1.1 **Status:** Final **Author:** OberaConnect IT **Date:** 2025-12-02

1.0 Purpose

The purpose of this Standard Operating Procedure (SOP) is to document the major components of a Hybrid Active Directory (AD) environment, which integrates on-premises Windows Active Directory with Microsoft Entra ID (formerly Azure AD) and Microsoft 365 (M365). This document provides guidance for monitoring, maintenance, and troubleshooting.

2.0 Scope

This SOP applies to the management and troubleshooting of hybrid identity infrastructure. This includes: - Microsoft Entra Connect (formerly Azure AD Connect) synchronization - Active Directory Federation Services (ADFS) - DNS configurations for federated authentication - Certificate lifecycle management

3.0 Prerequisites

- Basic understanding of Windows Server Active Directory.
- Familiarity with Microsoft 365/Entra ID administration.
- Knowledge of DNS principles and management.
- Access to Entra admin center (entra.microsoft.com).

4.0 Architecture Components

4.1 Directory Synchronization Server (Entra Connect)

Attribute	Description
Server Role	Hosts Microsoft Entra Connect (formerly Azure AD Connect)
Service Name	`Microsoft Azure AD Sync` (ADSync)
Sync Direction	On-premises AD → Entra ID (one-way by default)
Sync Frequency	Every 30 minutes (default)

Key Points: - Accounts created directly in Entra ID/M365 are NOT synchronized back to on-premises AD. - Password hash sync or pass-through authentication handles credential validation. - The sync server should NOT be a domain controller in production environments.

Example Configuration:

```
Server: DC01 (or dedicated sync server)
Domain: corp.contoso.com
Entra Tenant: contoso.onmicrosoft.com
```

4.2 ADFS Server (Federation Services)

Attribute	Description
Server Role	Active Directory Federation Services
Purpose	Federated authentication for SSO
External Access	Via Web Application Proxy (WAP)

> **NOTE:** Microsoft recommends migrating from ADFS to Entra ID cloud authentication (Password Hash Sync + Seamless SSO) for reduced complexity and improved security.

4.3 DNS Configuration for Federation

For federated authentication, Microsoft's authentication service must locate your ADFS server:

1. **Required DNS Record:**
   - Type: `A` record
   - Name: `sts` or as configured in ADFS (e.g., `sts.contoso.com`)
   - Value: External IP of ADFS/WAP server
2. **Authentication Flow:**
   - User attempts M365 login
   - Microsoft identifies federated domain
   - Redirects to organization's ADFS endpoint
   - ADFS authenticates against on-premises AD
   - Token returned to Microsoft for access

5.0 Monitoring and Health Checks

5.1 Entra Connect Health Monitoring

1. **Access Entra Connect Health:**

   - Navigate to: **entra.microsoft.com > Identity > Hybrid management > Microsoft Entra Connect > Connect Health**
   - Or: **Microsoft 365 Admin Center > Health > Directory sync status**

2. **Key Metrics to Monitor:** | Metric | Healthy State | Action if Unhealthy | |——|————|—————| | Last sync time | Within 3 hours | Check ADSync service, run manual sync | | Sync errors | 0 | Review sync error report, fix attribute conflicts | | Export errors | 0 | Check connector space, verify object permissions | | Password sync | Enabled (if used) | Verify service account, check event logs |

3. **Manual Sync Commands (PowerShell on sync server):**

   ```
   # Check sync status
   Get-ADSyncScheduler

   # Force delta sync
   Start-ADSyncSyncCycle -PolicyType Delta

   # Force full sync (use sparingly)
   Start-ADSyncSyncCycle -PolicyType Initial
   ```

4. **Event Logs to Review:**

   - Application Log: Source `Directory Synchronization`
   - Application Log: Source `ADSync`

5.2 ADFS Health Monitoring

1. **ADFS Event Logs:**

   - Event Viewer > Applications and Services Logs > AD FS > Admin

2. **Test ADFS Connectivity:** `powershell # From ADFS server Get-AdfsProperties Test-AdfsServiceHealth`

3. **External Test:**

   - Navigate to: `https://sts.contoso.com/adfs/ls/IdpInitiatedSignon.aspx`
   - Should display ADFS sign-in page

6.0 Certificate Management (CRITICAL)

6.1 ADFS Certificates Overview

Certificate	Purpose	Location	Typical Validity
Service Communications	SSL/TLS for ADFS endpoints	ADFS server	1-2 years
Token Signing	Signs SAML tokens	ADFS (auto-generated)	1 year (auto-rollover)
Token Decryption	Decrypts incoming tokens	ADFS (auto-generated)	1 year (auto-rollover)

6.2 Certificate Renewal Procedure

For Service Communications Certificate (SSL):

1. **Obtain new certificate** from CA (public or internal).
2. **Import to ADFS server:** `powershell # Import certificate to Local Machine\Personal store Import-PfxCertificate -FilePath "C:\certs\newcert.pfx" -CertStoreLocation Cert:\LocalMachine\My -Password (ConvertTo-SecureString -String "password" -AsPlainText -Force)`
3. **Update ADFS to use new certificate:**

   ```
   # Get thumbprint of new certificate
   Get-ChildItem Cert:\LocalMachine\My | Where-Object {$_.Subject -like "*sts.contoso.com*

   # Set new certificate
   Set-AdfsSslCertificate -Thumbprint "<new_thumbprint>"
   Set-AdfsCertificate -CertificateType Service-Communications -Thumbprint "<new_thumbprin
   ```

4. **Restart ADFS service:** `powershell Restart-Service adfssrv`
5. **Update WAP servers** (if applicable): `powershell Set-WebApplicationProxySslCertificate -Thumbprint "<new_thumbprint>"`

6.3 Certificate Expiration Monitoring

1. **Check current certificates:** `powershell Get-AdfsCertificate | Select-Object CertificateType, Certificate, Thumbprint | Format-Table`
2. **Set calendar reminders** 30 days before expiration.
3. **Enable auto-rollover** for token signing/decryption (enabled by default): `powershell Set-AdfsProperties -AutoCertificateRollover $true`

7.0 Troubleshooting

Issue	Symptoms	Resolution
Sync not running	Objects not appearing in Entra ID	Check ADSync service status, run `Start-ADSyncSyncCycle`
Password sync failures	Users can't sign in with new passwords	Check password hash sync status, verify service account
ADFS login fails	Redirect to ADFS times out	Check ADFS service, verify DNS, check firewall rules for 443
Certificate errors	Browser SSL warnings on ADFS page	Renew SSL certificate per Section 6.2
"User not found" in M365	Account exists on-prem but not in cloud	Check sync scope filters, verify OU is in sync
Duplicate object errors	Sync errors for specific users	Check for soft-matched objects, use `IdFix` tool

8.0 Related Documents

- SOP-AD-001: Active Directory Domain Connection Troubleshooting
- SOP-M365-001: Microsoft 365 Governance and Administration
- Microsoft Docs: https://learn.microsoft.com/en-us/entra/identity/hybrid/

9.0 Revision History

Version	Date	Author	Description
1.0	2025-12-02	OberaConnect IT	Initial document creation (Setco-specific).
1.1	2025-12-29	Jeremy Smith	SME Review: Generalized for reuse across clients. Updated terminology to Entra ID. Added Section 5.0 (Monitoring and Health Checks). Added Section 6.0 (Certificate Management). Added comprehensive troubleshooting table.