# Automating AD User Management from HR Workflows Using ServiceNow ITOM

# Overview

Onboarding and offboarding are two of the most sensitive IT processes in any organization. A delay in creating an Active Directory (AD) user account can leave new hires without system access for hours or even days. Worse, failing to promptly disable or remove AD users during offboarding can lead to serious **security risks, license misuse,** and **compliance violations.**

In many organizations, this process remains **manual, ticket-driven,** and dependent on multiple teams (HR, IT, Security).

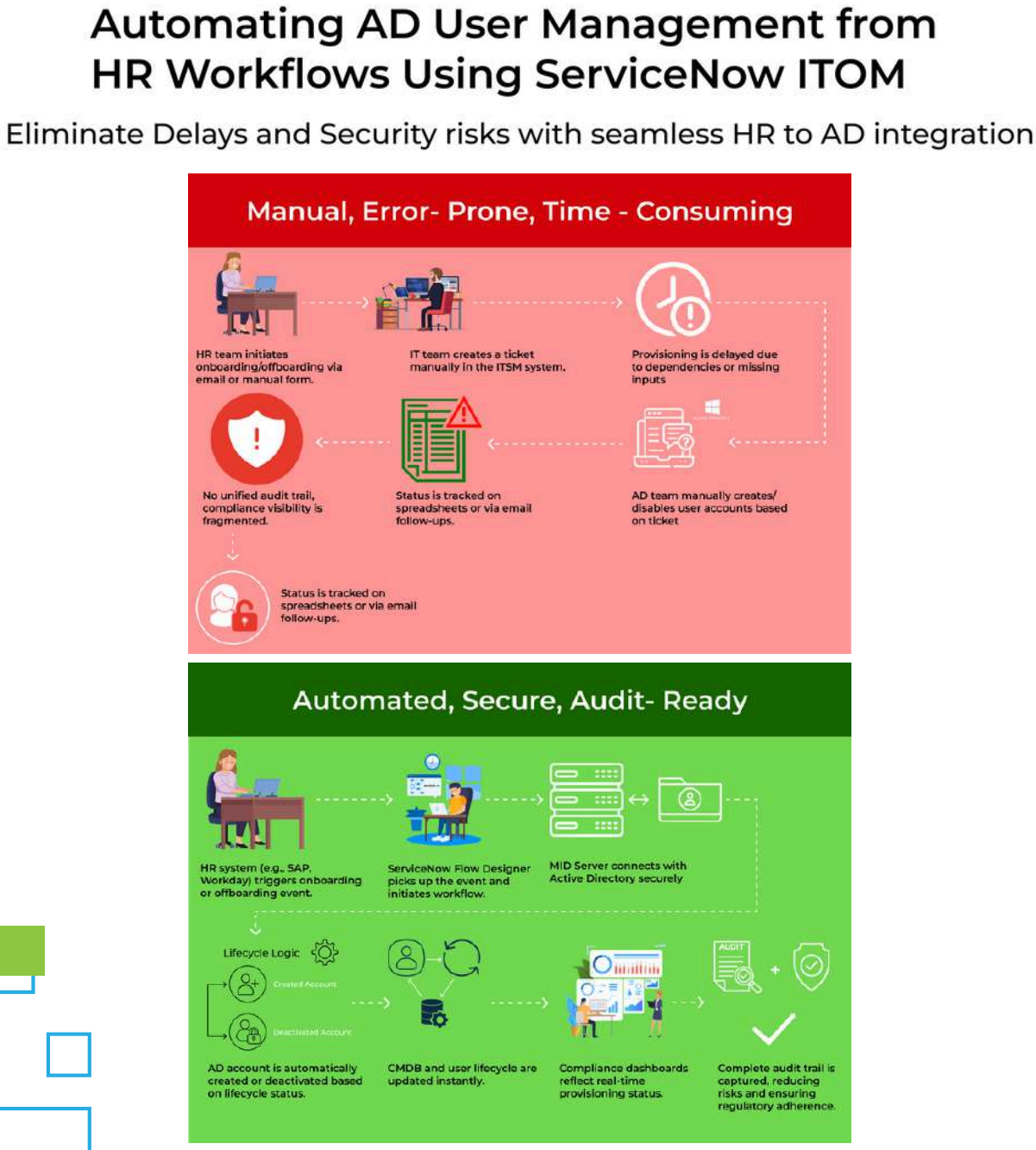
But with **ServiceNow ITOM,** specifically the **Orchestration, Flow Designer,** and **MID Server** capabilities, you can build a reliable, repeatable, and automated pipeline that connects your **HR platform** with **Active Directory**, ensuring:

- Timely account provisioning and deactivation
- Real-time visibility for audits and compliance
- Reduction in manual effort and error
- Seamless integration with CMDB and lifecycle events

# Overview

This guide walks developers through building an **automated workflow** to:

*Add or delete a user in Active Directory whenever a corresponding onboarding or offboarding event is triggered from ServiceNow HR or any integrated HCM system.*



# What You'll Need (Technical Prerequisites)

| Requirement | Details |
|---|---|
| **ServiceNow Version** | Washington (Q2 2024 release) or Xanadu (Early Access) |
| **ITOM Orchestration Plugin** | Must be activated (Orchestration Core + PowerShell activities) |
| **HRSD or Catalog Workflow** | Either ServiceNow HRSD or a custom catalog item triggers the flow |
| **MID Server** | Installed and connected to the on-prem AD network |
| **AD PowerShell Access** | Admin credentials with rights to create/disable users |
| **ServiceNow Roles Required** | admin, x_orch_admin, flow_designer, mid_server |
| **ServiceNow Roles Required** | Available via IntegrationHub if not using custom scripts |

# Key Terms to Know

- **HR Lifecycle Events** – Pre-defined events in ServiceNow HRSD (e.g., New Hire, Termination) that trigger automation
- **Ownership Confusion** – Secure bridge between ServiceNow and on-prem systems like AD.
- **Flow Designer**– No-code/low-code automation builder with orchestration support.
- **Credential Alias** – A secure credential storage and reference mechanism in MID Servers.

# What You'll Learn

By the end of this guide, you will be able to:

- Automate user creation and deletion in AD from ServiceNow flows
- Integrate HRSD workflows with infrastructure-level orchestration
- Use Flow Designer, PowerShell scripts, and the MID Server to control AD
- Capture errors, perform logging, and ensure secure execution

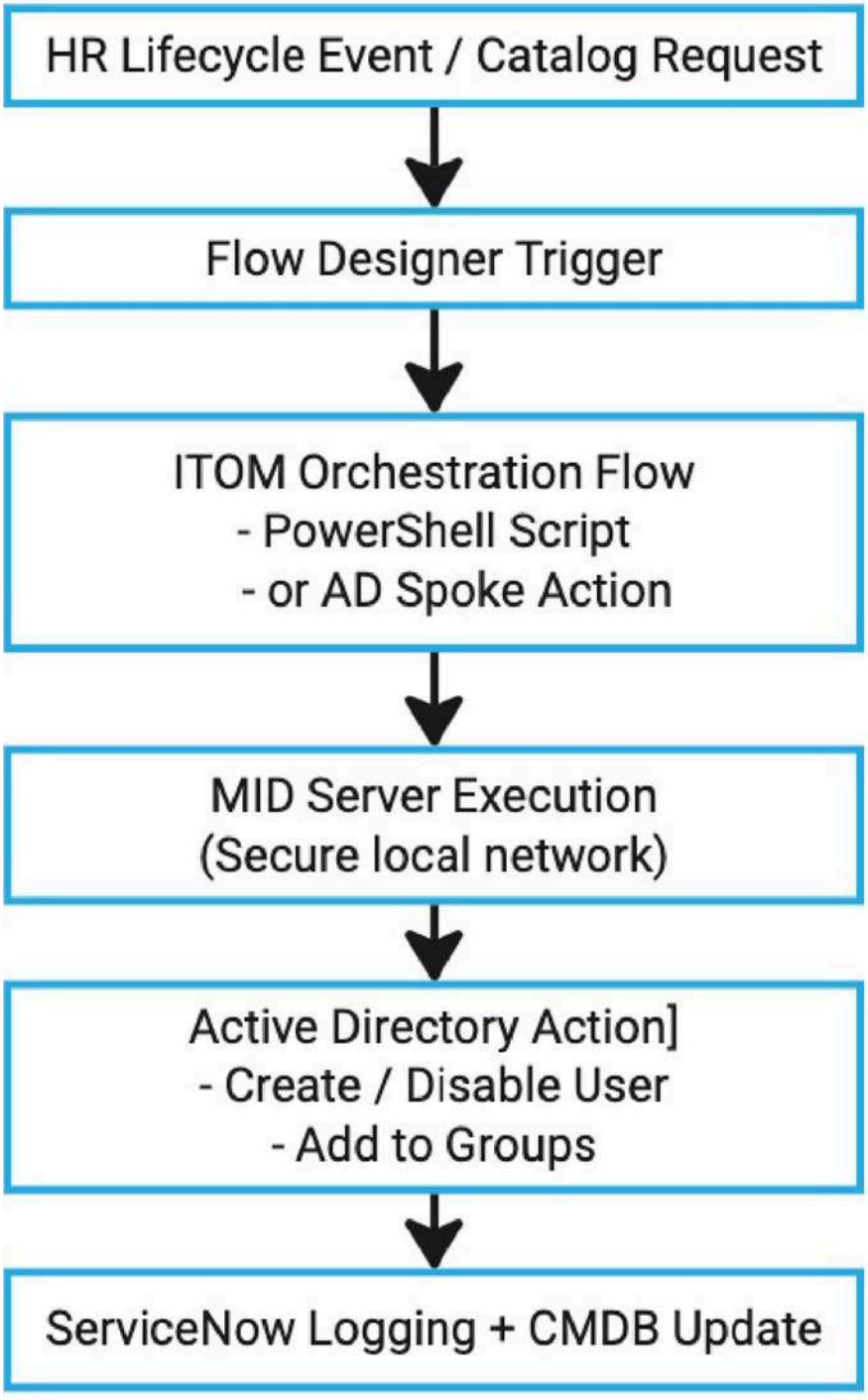
# System Architecture and Toolset

## How It Works: From HR Action to Active Directory Execution

The core idea behind this automation is **orchestrating infrastructure-level actions** (like creating or disabling users in Active Directory) **based on HR lifecycle events** (such as onboarding or termination).
With ServiceNow ITOM's Orchestration capabilities, you can securely connect your ServiceNow instance to on-premises systems like AD, without compromising control or auditability.

# System Architecture and Toolset

## Here's a simplified end-to-end flow



# Core ServiceNow Components Used

| Component | Description |
|---|---|
| **Flow Designer** | The low-code engine is where the automation logic is created. It reacts to HR requests or catalog items. Supports conditional logic and MID Server orchestration. |
| **ITOM Orchestration** | Provides the necessary PowerShell orchestration activities to interact with AD (used when AD Spoke is not available). Enables secure, script-based remote execution via MID Server. |
| **MID Server** | A secure bridge between ServiceNow (cloud) and your on-prem infrastructure (like Active Directory). Ensures no direct external access to internal resources. |
| **HRSD Lifecycle Events** | Used to trigger flows based on events like onboarding, role change, or termination. These are linked to employee records in HR. |
| **AD Spoke (Optional)** | A plug-and-play option from IntegrationHub that provides ready-made actions (e.g., Create AD User, Disable AD User) if scripting is to be avoided. Requires IntegrationHub licensing. |
| **Credential Aliases** | Secures the username/password used for AD operations. Stored once and referred to safely within flows. |

# Use Case Flow

**Event** – HR triggers "New Hire – Full-Time"

**Automation Flow:**

- HR creates a request or a Lifecycle Event that triggers onboarding.
- Flow Designer kicks in and runs an orchestration flow.
- Flow passes user details (first name, email, group) to AD via MID Server.
- PowerShell script (or Spoke) creates the user and assigns them to groups.
- Flow updates the CMDB or HR case notes with confirmation.
- An email notification is sent to HR and IT.

# What You Achieve with This Setup

- **Secure execution** without exposing AD to the internet
- **End-to-end automation** across business and infrastructure layers
- **Auditable and traceable** logs of every provisioning action
- **Easily extendable** to cover software access, group memberships, and mailbox creation

# Developer Walkthrough – Create AD User on Onboarding

In this section, we'll walk through the **technical implementation** of automatically **creating a user in Active Directory** when an onboarding request is triggered via ServiceNow—either through **HR Lifecycle Events** (in HRSD) or a **custom Service Catalog item**. This flow will run securely through a **MID Server** using either **PowerShell scripts** or the **AD Spoke** in IntegrationHub.

This guide assumes you're using **ServiceNow Washington or Xanadu**, with updated Flow Designer and Orchestration capabilities.

## Scenario: Automate New Hire AD Account Creation

**Trigger:** Identify all current asset sources and validate data quality.
**Goal:** Automatically create the user account in Active Directory with relevant attributes and group memberships

### Step-by-Step Developer Guide

**Step 1: Configure the MID Server**

- Ensure the MID Server is installed on a Windows machine within the same network as the AD server.
- Assign proper permissions to the MID Server user (typically, a service account with rights to create/modify AD objects).
- Test connectivity in **ServiceNow → MID Server → Status = Up.**

# Scenario: Automate New Hire AD Account Creation

**Washington or later Update:** MID Server log visibility now supports real-time diagnostics during orchestration.

**Step 2: Create a Credential Alias**

- Navigate to **Orchestration > Credentials > Credential Aliases**
- Create a new alias (e.g., AD_Service_Account)
- Link it to a Windows credential record with AD access
- Set the access policy to restrict use only to the relevant flow

**Tip:** Don't hardcode credentials in scripts—use aliases for secure execution and rotation.

**Step 3: Build the Flow in Flow Designer**

- Go to **Flow Designer > New Flow**
- Name it: Onboarding - Create AD User
- **Trigger:** Select "HR Lifecycle Event" or "Catalog Item submitted"

# Scenario: Automate New Hire AD Account Creation

**Add Actions:**

1. **Get Record:** Fetch employee details (first name, last name, email, department, etc.)
2. **If condition** (optional): Check if user already exists in AD
3. **Script Step** or **AD Spoke Action:**

- If using **PowerShell via Orchestration:**
- Use the “Run PowerShell Script” action
- Write a script to create the AD user with dynamic input (see sample below)

If using **AD Spoke:**

- Action: “Create Active Directory User”
- Map employee fields to AD attributes (e.g., sAMAccountName, mail, displayName)

4.Update Record / Log Output: Add comments to the HR case or update the CMDB
5.Send Notification: Notify HR and IT of success or failure

# Scenario: Automate New Hire AD Account Creation

**Sample Snippet**

```
$Username = "$($inputs.firstname).$($inputs.lastname)"
$UserPrincipalName = "$Username@yourdomain.com"
$Password = "P@ssword123!"     #Ideally, randomized and stored securely
$OU = "OU=Employees,DC=yourdomain,DC=com

New-ADUser `
 -Name "$($inputs.firstname) $($inputs.lastname)" `
 -GivenName $inputs.firstname `
 -Surname $inputs.lastname `
 -SamAccountName $Username `
 -UserPrincipalName $UserPrincipalName `
 -AccountPassword (ConvertTo-SecureString $Password -AsPlainText -Force) `
 -Path $OU `
 -Enabled $true
```

# Scenario: Automate New Hire AD Account Creation

**Step 4: Test and Validate**

- Use test HR records to run the flow
- Validate that the user appears in AD with the correct attributes
- Check ServiceNow logs (Flow Designer + MID Server logs)
- Ensure the HR case is updated with a success message

**Extend with Optional Logic**

- Assign user to specific security groups (e.g., based on department)
- Create a home folder or mailbox using additional PowerShell steps
- Store generated credentials in a vault or email them to the manager

**Real-World Result**

A mid-size healthcare provider automated the creation of 150+ AD users annually with zero manual intervention, reducing onboarding time by **80%**, and ensuring strict compliance with user access policies.

# Automating AD User Deactivation on Offboarding

**Why Offboarding Automation Matters:**
Offboarding is often overlooked but is just as critical—if not more—than onboarding. When user accounts are not promptly disabled or removed from Active Directory (AD), it creates significant risks:

- **Unauthorized access to critical systems**
- **Violation of compliance frameworks (HIPAA, SOX, GDPR)**
- **Inaccurate license usage and audit penalties**
- **Data leakage from lingering access to email or file shares**

This section walks through how ServiceNow ITOM can **automatically disable AD users and revoke access** when an offboarding event is triggered, ensuring speed, security, and traceability.

**Scenario: Automate AD Account Deactivation**

**Trigger:** HR initiates a "Termination" lifecycle event
**Goal:** Automatically disable the user in AD, revoke group memberships, and log results in the HR case or CMDB

# Automating AD User Deactivation on Offboarding

**Step-by-Step Developer Guide**

**Step 1: Create the Termination Flow**

- Go to **Flow Designer > New Flow**

- Name: Offboarding – Disable AD User

- **Trigger:** HR Lifecycle Event = "Termination" (or last working date reached)

**Add Actions:**

1. **Look Up Record:** Fetch user's email, sAMAccountName, and AD DN from HR or CMDB
2. **Script Step or AD Spoke Action:**
    - If using Orchestration PowerShell Script:
        - Disable account
        - Remove from security groups
    - If using **AD Spoke:**
        - Action: "Disable Active Directory User"
3. **Log Output:** Write a note in the HR task record
4. **Notify Security/HR:** Email or create a task if deactivation fails

# Automating AD User Deactivation on Offboarding

**Sample Snippet**

```
Disable-ADAccount -Identity $inputs.samAccountName

# Optional: Remove from all groups
$groups = Get-ADUser $inputs.samAccountName -
Properties MemberOf | Select-Object -ExpandProperty
MemberOf
foreach ($group in $groups) {
    Remove-ADGroupMember -Identity $group -
Members $inputs.samAccountName -Confirm:$false
}
```

**Step 2: Secure Credential Alias and MID Server**

- Reuse the **same credential alias** (AD_Service_Account)
- The MID Server must have the right to disable accounts and remove memberships
- Test credential validity in **Credential Test Tool**

# Automating AD User Deactivation on Offboarding

| Feature | Description |
|---|---|
| **Access Revocation Workflow** | Extend the flow to revoke access to applications like email, VPN, and file shares |
| **Last Day Automation** | Use Scheduled Flow logic to trigger deactivation at the end of the employee's last working day. |
| **Ticket Escalation** | If AD is unreachable, auto-create a task for IT Security for manual action. |
| **Audit Trail** | Write all activity (timestamp, user, outcome) to an audit log table or CMDB for compliance. |

# Best Practices and Smart Extensions

Now that you've walked through how to automate both onboarding and offboarding with ServiceNow ITOM, let's look at how to **optimize, secure,** and **scale** this implementation across your organization.

# Best Practices and Smart Extensions

## Best Practices for Developers

1. Use Flow Variables & Reusable Subflows

- Modularize PowerShell steps or AD Spoke actions into reusable subflows.
- Helps when scaling to multiple employee types (e.g., contractors vs. FTEs).

2. Test in Non-Prod Environments

- Always validate PowerShell scripts using a staging domain or sandbox AD setup.
- Leverage MID Server logs and debug mode in Flow Designer for diagnostics.

3. Credential Management

- Use Credential Aliases with restrictive access policies.
- Schedule credential rotation with built-in ServiceNow credential policies or integrate with a Vault.

4. Maintain a Rollback Plan

- Always include rollback logic in case of partial failures (e.g., user created but not added to groups).
- Use flags or conditions to skip duplicate actions.

5. Audit & Alert

- Write success/failure logs to a centralized audit table.
- Create exception alerts or incident tasks for failed executions.

# Best Practices and Smart Extensions

## Read our Blog:

1. ServiceNow ITOM vs Traditional Tools – A Comparison in 2025
2. 5+ ServiceNow ITOM Use Cases by Industry – From Data Centers to License Management

## Conclusion

ServiceNow ITOM is no longer just about servers and infrastructure. With modern releases like **Washington** and **Xanadu,** ITOM now acts as a powerful **automation backbone** for business-driven workflows like HR onboarding and offboarding.
By securely connecting your HR events to Active Directory operations through **Flow Designer, Orchestration,** and **MID Server,** you can:

- Cut down manual effort and provisioning delays
- Securely manage user access throughout the lifecycle
- Achieve better compliance and audit readiness
- Integrate business logic with infrastructure automation

This guide has given you a real-world, technical playbook to implement a highly requested automation in the ITOM space. It's designed to be developer-friendly, easy to scale, and tightly aligned with modern ServiceNow capabilities.