



## Tips for structuring the Active Directory infrastructure

Vivin Sathyan  
Technical Evangelist



# Agenda

- 4 aspects of Active Directory management
- Options for managing Active Directory
- Limitations of the native tools
- A better alternative
- Question and answers

## 4 aspects of Active Directory Administration

1. Retrieving information
2. Managing objects
  - Manual
  - Automation
3. Delegating and auditing actions
4. Active Directory cleanup

## Options for managing Active Directory

- Native tools
- Third party tools

## Native tools

- PowerShell
- Active Directory users and computers
- Office365 Admin center
- Skype for business
- Exchange management console
- Event viewer

## Native tools - Challenges

- Confirmation messages aren't very helpful
- Consolidate information from multiple native tools
- Ability to delegate to non-admin users
  - Learning curve involved
  - Time consuming

The background features a white rectangular area with rounded corners, centered on a light gray background. Surrounding this central area are various colorful geometric shapes: a red circle in the top-left, a yellow circle in the top-right, a red circle in the middle-right, a green circle in the bottom-right, a blue circle in the bottom-right, and a red circle in the bottom-left. There are also red and blue lines and dots scattered around the edges of the white area.

A better alternative?



## 4 aspects of Active Directory Management with ADManager Plus



# 1. Retrieving information made easy

- How many administrators do you have?
- Find out and manage permissions on confidential folders
- Query important LDAP attributes - User information
- Accounts that have never logged on - security threat



## Permission Management

Manage permissions on files, folders and shares.

[View Recent T](#)

### Modify NTFS Permissions

Select Folders:  [\[ Select \]](#)

[\[ Permission \]](#)

Select Permissions:

Account	Permission	Applies To	Type
<input type="text" value="Finance managers"/> <a href="#">[ Select ]</a>	List folder/ read data, ▼	This folder, sub- ▼	Allow ▼ <input data-bbox="1657 518 1684 540" type="button" value="+"/>

[Copy from folder](#)

- ☒ Include inheritable permissions from this object
- ☐ Remove all existing permissions and apply only
- ☐ Replace all existing inheritable permissions on a

- [\[Show Basic\]](#)
- |  |   |
|--|---|
| <input type="checkbox"/> Traverse folder/ execute file       | <input type="checkbox"/> Write Extended Attributes    |
| <input checked="" type="checkbox"/> List folder/ read data   | <input type="checkbox"/> Delete sub-folders and files |
| <input checked="" type="checkbox"/> Read Attributes          | <input type="checkbox"/> Delete                       |
| <input checked="" type="checkbox"/> Read Extended Attributes | <input type="checkbox"/> Read Permissions             |
| <input type="checkbox"/> Create file/ write data             | <input checked="" type="checkbox"/> Write Permissions |
| <input type="checkbox"/> Create folders/ append data         | <input type="checkbox"/> Take Ownership               |
| <input checked="" type="checkbox"/> Write Attributes         |   |

[\[ Preview \]](#)

## Users who have never logged on

HR

- Member of basic groups in AD
- Did not login even once
- When created: 21<sup>st</sup> of January 2018

Password: Password@123

Vendor

- Member of basic groups in AD
- Did not login even once
- When created: 3<sup>rd</sup> of December 2018

Password: Password@123

IT staff

- Member of top security groups
- Did not login even once
- When created: 1<sup>st</sup> of August 2018

Password: Password@123

# lastLogon vs. lastLogonTimestamp in Active Directory

▲ An employee left the company. I try to find out when his AD account was logged in for the last time - if it was before the dismissal or after.

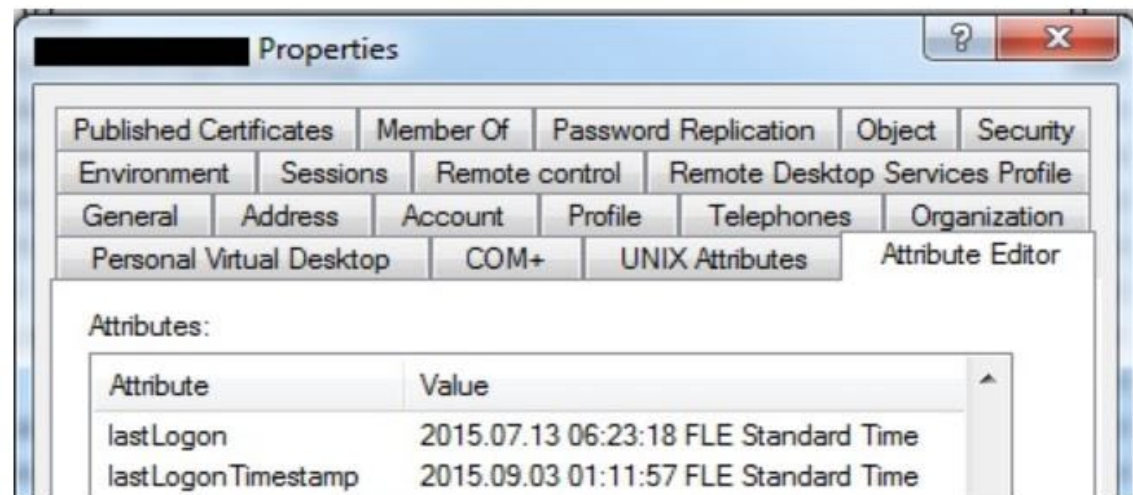
3

▼ There are these 2 attributes in user properties window: *lastLogon* and *lastLogonTimestamp*. *lastLogon* date is earlier than the dismissal date, but *lastLogonTimestamp* date is posterior to the dismissal date (so in this case we would have a security problem).



1

How to know, which one of these attributes shows the actual last AD account login time? What is the difference between them?



## 2. Effectual management of objects

- Manage the entire life cycle of an object
- Two ways
  - Manual
  - Automation



# User creation templates



Layout View



Creation Rules



Copy User Attributes



Enable Drag-n-Drop

☒ Active Directory ☒ Google Apps ☒ Office 365

General

Account

Contact

Exchange

Remote Mailbox

Terminal

OCS/Lync/Skype

Custom Attributes



## General

First name



Initials

Last name



\*Logon Name

FirstName + LastName



workshop.admanagerplus.co

eg. JohnSmith@workshop.admanagerplus.com



[Create your own naming format](#)

\*Logon name(pre-Windows 2000)

Same as logonname

eg. JohnSmith

\*Full name

Same as logonname

eg. JohnSmith

Display name

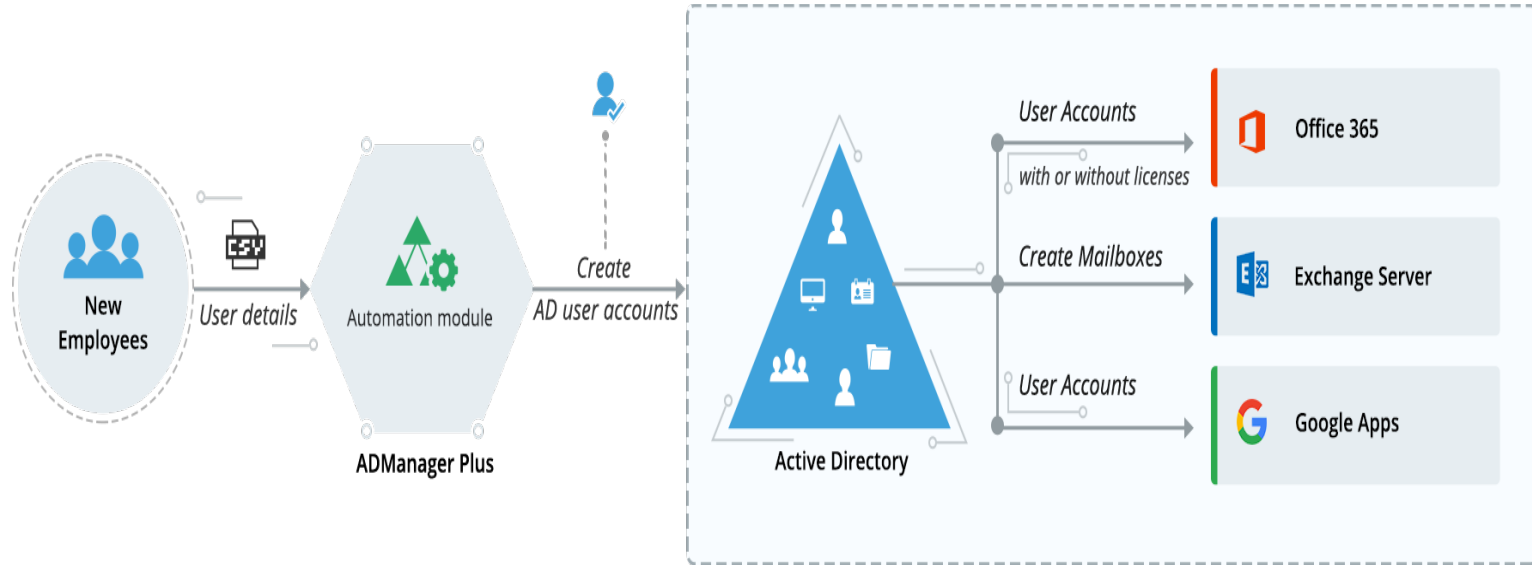
Same as logonname

eg. JohnSmith



Employee ID

# User provisioning made effective



# Automation: User creation

## Create New Automation

\* Automation Name : IT\_user account creation

Description : Basic IT accounts - Members of IT-Tech access group

Automation Category : User Automation

Select Domain : workshop.admanagerplus.com

### Tasks to automate

Specify the task you want to automate.

Automation Task/Policy : Create Users

Template to be applied: IT\_Accounts

Location of CSV: \\server\newly hired users\IT e.g. \\server\_name\share\_name\folder

☒ Select only the appended objects from the file. ?

☒ Implement Business Workflow ?

### Execution Time

Specify the time/interval at which the task should be run.

Run at : Weekly

On: Tuesday At: 10 Hrs 40 Mns

Save

Save & Run

Cancel



# ITSM-IAM Integration & more.

---

## ADManager Plus + ServiceDesk Plus

Create | Unlock | Enable | Disable | Delete | Reset passwords

## ADManager Plus + ServiceNow

Create | Unlock | Enable | Disable | Delete | Reset passwords & Add or remove from Group

## Other integrations

MS SQL and Oracle DB - user onboarding





Request Catalog



Quick Actions

Desktop Central

MDM

ADManager Plus

Advanced Analytics

AD Self Service

Zoho Creator App

Request ID Search...



Pro

Request ID : 1



Edit

Close

Assign

Actions

Reply

Work Log Timer

## User Onboarding

By SteveMartinHR on Aug 14, 2017 08:57 PM

Du

Request

Tasks (0/1)

Resolution

History

## Description

Onboard New Joinees by creating accounts in Active Direc

Status : Open

Priority : High

Stop Timer

Merge Request

Link Requests

Duplicate Request

Print Preview

Delete

Convert Incident to Service

Create Service Request

Enable User(s) in AD

Unlock User(s) in AD

Create User in AD

Reset User Password

Delete User(s) in AD

Disable User(s) in AD

Enter Resolution

Add Notes

Add Attachment

Add Work Log

Add Task

Add Task(s) from Template

View Task(s)

Add Reminder

View Reminder(s)

Add Dependency

Submit for Approval

Search Problems

Associate Change

Associate Project

Search Solutions

View Requester Details

View Requests by Requester

View Assets belonging to User

Reply

Forward

Request Details

Edit

Filter navigator



Service Catalog > ADManager Plus



## ADManager Plus

### Items



#### Create a User in AD

Create A User in AD



#### Delete Users In AD

Delete Users In AD



#### Disable Users in AD

Disable Users in AD



#### Enable Users in AD

Enable Users in AD



#### Reset User Password in AD

Reset User Password in AD



#### Unlock Users in AD

Unlock Users in AD

### Self-Service

Homepage

Dashboards

Service Catalog

Knowledge

Help the Help Desk

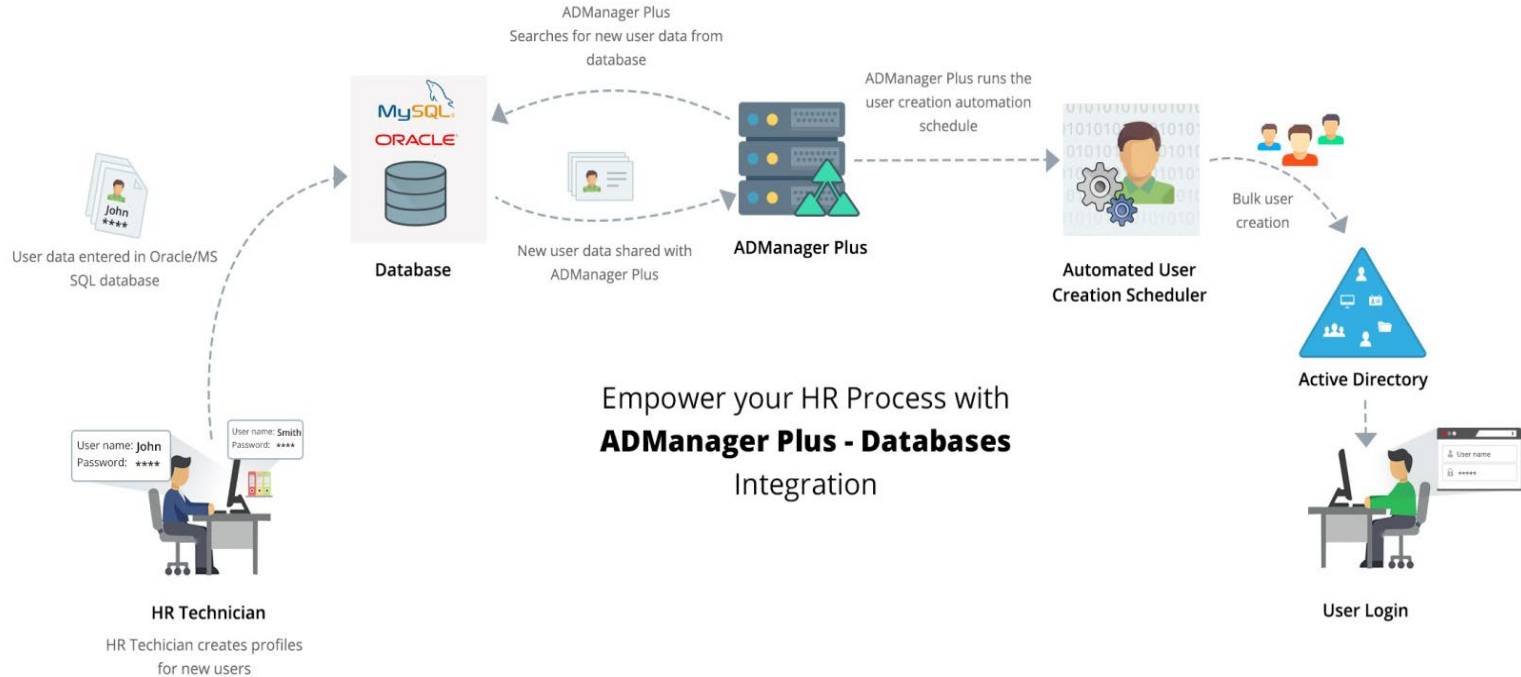
Visual Task Boards

Connect Chat

Incidents

Watched Incidents

# ADManager Plus and DB integration



### 3. Delegating and auditing actions

- Points to be remembered
  - Precise restrictions
  - Use the domain admin account only for actions that require the privilege level of this account.
  - Never use shared accounts
  - Review events and take corrective actions

# User permissions are untouched!



# Roles: Task controllers

## Create Help Desk Role

Role Name:

Description:

☒ AD Management ☐ AD Reports ☐ Administration

### User Management

Computer Management

Contact Management

Group Management

Mailbox Management

OU Management


Security Management

File Server Management

Office 365 Management

### Bulk User Management

☒ Create Users

 [User Attribute ..](#)

☒ Create Single User

☐ Create Bulk Users

☒ Modify Users ?

☒ Modify Single User

☐ Modify Bulk Users

☒ User Templates

☒ User Creation Templates

☒ User Modification Templates

### Bulk User Modification

☐ Deny Bulk Modification | ☐ Deny CS

☒ General Attributes

☒ Reset Password

☐ Group Attributes

☒ Unlock Users

☐ Move Users

☐ Delete Users

☐ Account Attributes

☐ Restore Deleted Users

☐ Exchange Attributes

☐ Create/Archive MailBox

☐ Modify SMTP Address

☐ Set MailBox Rights

☐ Delivery Options

☐ Naming Attributes

☐ Exchange Features

☐ Auto Reply

☐ Terminal Services

☐ Profile Attributes

☐ Remote Control Attributes

☐ Session Attributes

☐ Environment Attributes

☐ Move/Delete TS Home folders

☐ Dial-in

# Technician auditing

## Help Desk Delegation

Help Desk Technicians

Help Desk Roles

## Help Desk Audit Reports

Audit Report

Admin Audit Report

Help Desk Reports

Technicians Report



## Help Desk Audit Report

Lists all the actions/operations performed by help desk technicians [Learn more...](#)

[Schedule Reports](#)

Select Help Desk Technicians :  [\[choose\]](#)

Period :

[Quick Search](#)

Show Rows :    1-25 of 1758

Technician Name	Action Name ▲	Action Category	Action Time	Object Name	Object Domain	Status	
ADManager Plus Admin	Add To Group	User Modification	2017-02-02 08:00:01	RichardWills	workshop.admanagerplus.com	Add operation successful.	<a href="#">Details</a>
ADManager Plus Admin	Add To Group	User Modification	2017-02-02 08:00:01	arun.t	workshop.admanagerplus.com	Add operation successful.	<a href="#">Details</a>
ADManager Plus Admin	Add To Group	User Modification	2017-02-02 08:00:01	ralphtest	workshop.admanagerplus.com	Add operation successful.	<a href="#">Details</a>
ADManager Plus Admin	Add To Group	User Modification	2017-02-02 08:00:01	admin	workshop.admanagerplus.com	Add operation successful.	<a href="#">Details</a>
ADManager Plus Admin	Add To Group	User Modification	2017-02-02 08:00:01	Richard.Wills	workshop.admanagerplus.com	Add operation successful.	<a href="#">Details</a>
ADManager Plus Admin	Add To Group	User Modification	2017-02-02 08:00:01	testwednesday	workshop.admanagerplus.com	Add o succe	



# Request and approve methodology



Requests

Create Request

All Requests

Workflow Delegation

Requesters

Reviewers

Approvers

Executors

Requester Roles

Configuration

Business Workflow

Assigning Rules

Business Workflow

Define an order of execution for important administrative tasks. [Learn more...](#)

Workflow Name

User de-provisioning workflow

Description

Delete accounts after 180 days

Workflow Stages

Requester

The one who raises a request for a particular action.  
[\[Configure\]](#)

Reviewer

The one who assesses the request, weighs its pros and cons, and offers recommendations. [\[Configure\]](#)

No. of Reviewers: 1 ▾

Approver

The one who possesses the authority to finalize an action. [\[Configure\]](#)

No. of Approvers: 1 ▾

Executor

The one who executes the approved action. [\[Configure\]](#)

Create Workflow

Cancel

🔍

1 - 4 of 4

5 ▾

Action	Workflow Name	Description	Workflow Stages
	Default business workflow	This is a predefined workflow present in the product.	Requester → Executor
	User onboarding workflow	This workflow will be used while processing the request for user account creation.	Requester → Reviewers: 1 → Executor
	Stale accounts cleanup workflow	This workflow will be used while processing stale accounts cleanup.	Requester → Reviewers: 2 → Executor
	User password reset workflow	This workflow will be used while processing password reset requests.	Requester → Reviewers: 2 → Approver: 2 → Executor

Create Rule to assign a request to appropriate technicians. [Learn more...](#)

Rule name

Description

Business workflow

Requester > 1 Reviewer > Executor

Rule criteria

1.

Action

Is

Create Users,Bulk User Creation

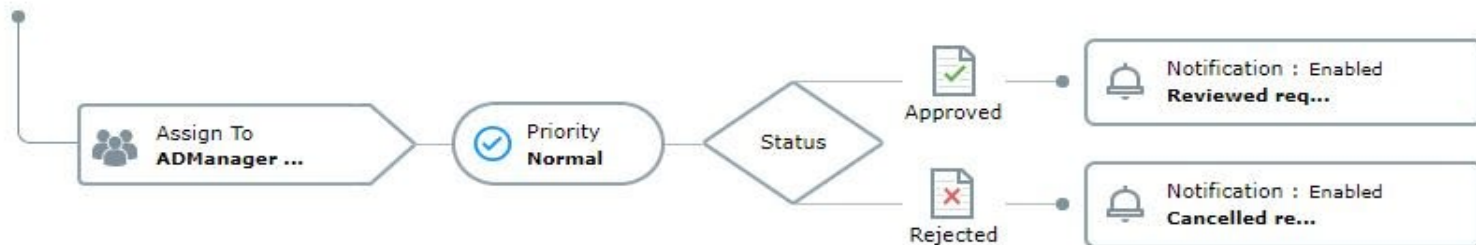
X +

Criteria : 1

Request administration

Request creation

Request reviewal



Request execution

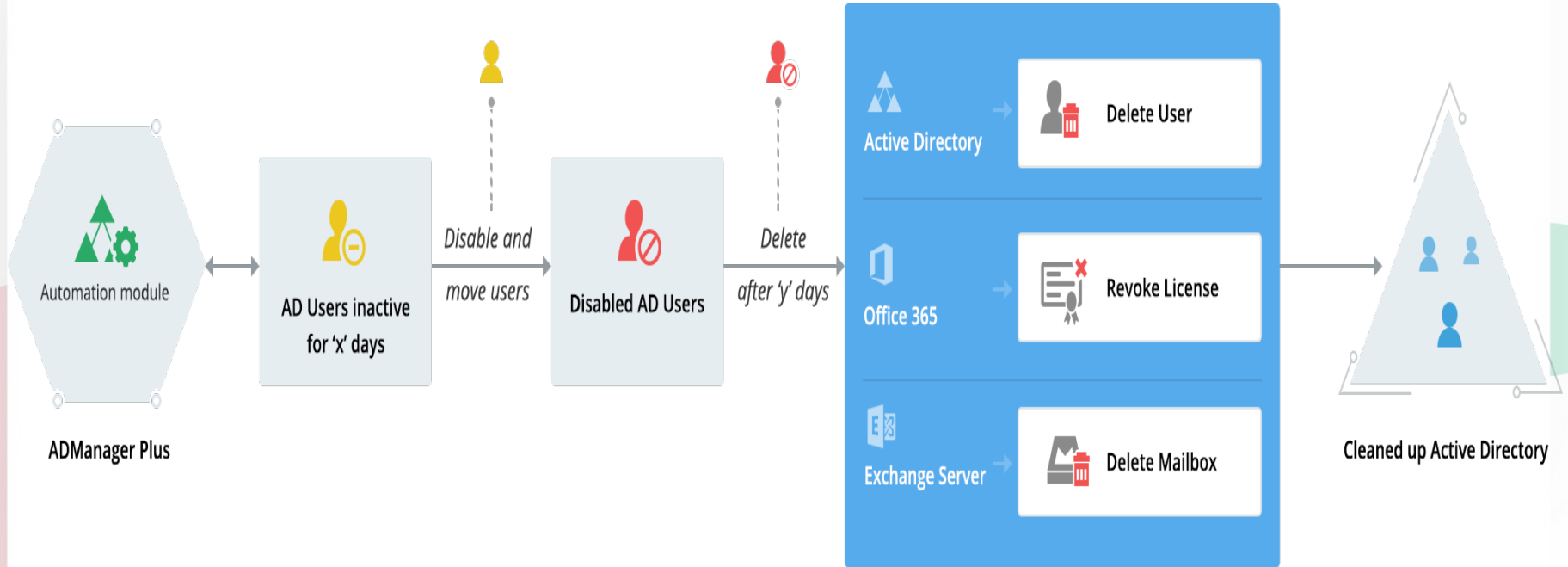
Update Rule

Cancel

## 4. Active Directory cleanup

- Users who have not logged in for more than 180 days and are still enabled
  - Enhances security
  - Effective utilization of license
- Computers that have not authenticated for more than 6 months
- Groups without any members

# Active Directory cleanup / user off boarding



# Create your own logic for automation

\* Automation Policy Name :

Description :

Automation Category :

Select Domain :

## Instant Tasks





☐ Clear all existing Group memberships

## Successive Task(s)

Task Group

[More](#)



After  days, from the time of executing the previous task

☒ Disable user mailbox

☐ Disconnect user mailbox

☐ Delete User mailbox

# Supervise and execute automations

## Create New Automation

\* Automation Name :

Inactive user objects - 180 days

Description :

Automation Category :

User Automation

Select Domain :

workshop.admanagerplus.com

All [\[Add OUs\]](#)

### Tasks to automate

Specify the task you want to automate.

Automation Task/Policy :

Policy for removing inact...

☒ Implement [Business Workflow](#) [?](#)

### Select objects

Select the objects on which the task would be performed - from report and/or CSV import.

From Report:

Inactive Users

[\[Select\]](#)

[Select More](#)

### Execution Time

Specify the time/interval at which the task should be run.

Run at : Monthly

On:

10

At:

17

Hrs

0

Mns

# ManageEngine® Thank you!

[vivin.sathyan@manageengine.com](mailto:vivin.sathyan@manageengine.com)  
[HybridCloud@realdolmen.com](mailto:HybridCloud@realdolmen.com)

[www.manageengine.com](http://www.manageengine.com)

