Secure your Intune Automation with Managed Identities

by Jan Ketil Skanke and Sandy Zeng

Sponsors

onedeploy
Windows Deployment Reimagined

ZERO TOUCH

Insight

control up

PATCH MY PC

robopack

numecent

Microsoft

eido

Rimo3

That’s me

MODERN ENDPOINT MANAGEMENT SUMMIT 2026

Jan Ketil Skanke

Jan Ketil Skanke
Microsoft MVP · Security
Intune | Identity & Access Managment

Role
Principal Cloud Architect

Focus
Intune · Identity · Security

Blog, Hobbies and more
Fotball, F1, Speaking, Coding

Intune Guardian

PIM Portal
Policy Management Tool

Sandy Zeng

Sandy Zeng
Microsoft MVP Security
Intune | Windows

Role
Senior Cloud Architect

Focus
Intune · Identity· Security

Blog, Hobbies and more
Blogging, Speaking, Coding

From Finland, Happiest Country in the world

"When we move the workloads to the cloud, we should also move our operations and automations"

Why do we automate?

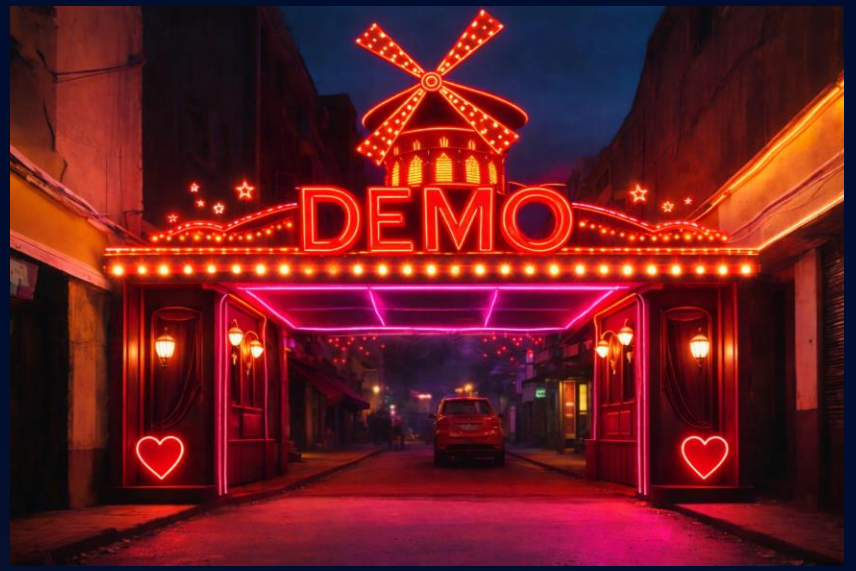
- Event driven tasks
  - Triggered by monitoring
- Repeated tasks
  - Human triggered
- Governance
  - Workflows and Desired State
  - Configurations by code
- Other

The problem with Apps & Secrets

- Credential leakage
- Misuse
- Lateral movement
- Management overhead

App Takeover

Lateral Movement risks



What are Managed Identities

Managed Identities in Microsoft Entra

- Credential-Free Authentication
  - Azure resources can securely access other services without storing secrets or credentials in code.

- Entra ID Integration
  - Managed identities are registered in Microsoft Entra ID, enabling RBAC and policy enforcement like any other identity.
- Two Identity Types
  - System Assigned
  - User Assigned

User-Assigned Managed Identity

- Created as a standalone Azure resource
- Can be assigned to one or more resources
- Lifecycle independent of any specific resource
- Multiple identities can be assigned to a single resource
- Requires manual creation and assignment
- RBAC in Azure

System-Assigned Managed Identity

- Created with an Azure resource (e.g., Azure Function, Logic App)
- Lifecycle tied to the resource
  - (deleted when the resource is deleted)
- Only one per resource
- No manual management required

Key Differences

System-Assigned

- Lifecycle Tied to resource
- One per resource
- No sharing
- Automatic management
- Deleted with resource
- Simple, resource-scoped

User-Assigned

- Independent lifecycle
- Many per resource
- Can be shared
- Manual management
- Manual deletion
- Shared and reusable

Usage

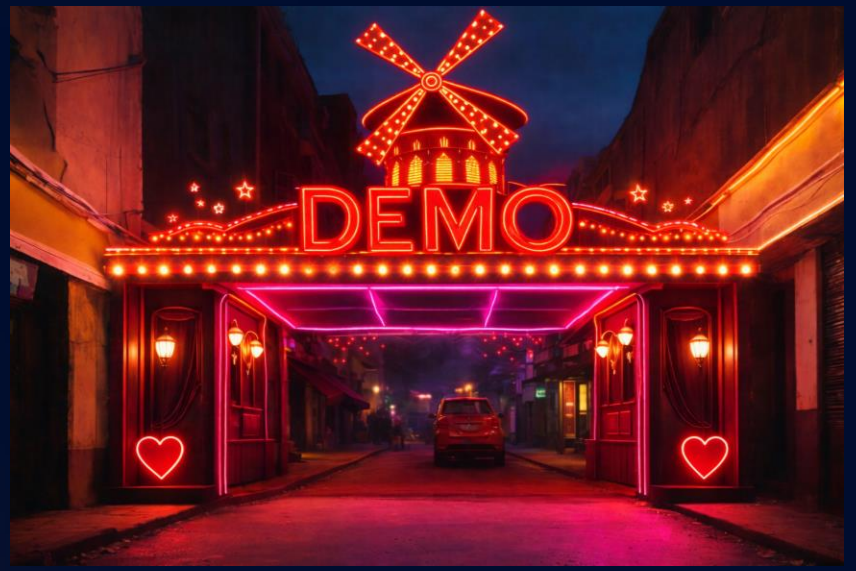
- Use system-assigned for simple, resource-specific scenarios
- Use user-assigned for sharing identities across resources or when you need more control

- Follow least privilege principle
- Remember to assign correct permissions’
- Watch for “dangling” user-assigned identities after resource deletion

Managed Identities in Action

How to setup and configure Managed Identities in Logic Apps, Azure Functions and Azure Automation

Assign Graph API Permissions and authenticate



MODERN ENDPOINT MANAGEMENT SUMMIT 2026

Best Practices & Pitfalls

- Always think least privilege
- Control your RBAC in both Azure and Entra ID

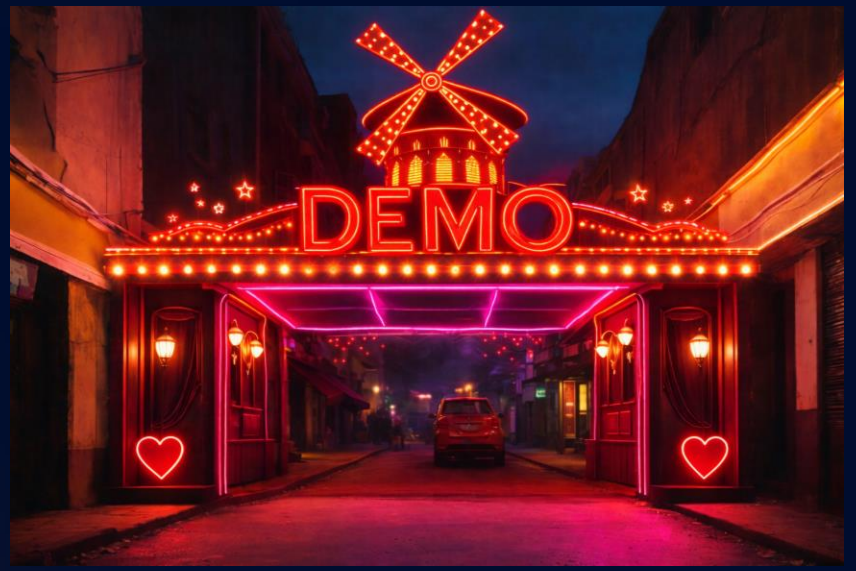
- Some common mistakes
  - Impatience when assigning new permission (Token Lifetime)
  - Permission Spree on User Assigned

Complete samples

Logic App

Azure Function App

Azure Automation



Github:

Remove Primary User:
https://github.com/sandytsang/MSIntune/tree/d55c66b3759433b4b2a32939ecd266577c3b5c6f/AzureFunctionApp/Remove%20Primary%20User

Change Primary User based on SignIn Logs:
https://github.com/sandytsang/MSIntune/tree/d55c66b3759433b4b2a32939ecd266577c3b5c6f/AzureAutomationAccount/Change-PrimaryUser

Please rate this session on Sched.com

We would love to hear what you liked and how we could improve!

Thanks!