

NIC **REBEL**
EDITION

Jan Ketil Skanke

Master Your Intune Automation with Managed Identities

Jan Ketil Skanke

- Principal Cloud Architect - CloudWay
- Microsoft MVP in Security (10 years)
- Star Wars, Lego and Formula 1 Geek



“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
- Other

The problem with App Secrets

- Credential leakage
- Misuse
- Lateral movement
- Management overhead

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

Feature	System-Assigned	User-Assigned
Lifecycle	Tied to resource	Independent
Number per resource	One	Many
Sharing	No	Yes
Management	Automatic	Manual
Deletion	With resource	Manual
Use Case	Simple, resource-scoped	Shared, 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



Graph API Integration

- Assign Graph API Permissions and authenticate



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 Apps
- Runbook



