Oh my... A user account is compromised!

What should we do now!?

Peter Klapwijk

𝕏 *Inthecloud_247*

Dutch
Microsoft
& Security
Meetup

About me

Peter Klapwijk
Modern Workplace
Consultant @ Wortell

Like: Football, Community stuff

Award: MVP Intune + Windows

A user account is compromised!

What should we do now!?

- Disable user account
- Reset password
- Revoke sign in sessions
- Delete authentication methods

- Disable Windows devices
- Wipe or reboot Windows devices
- Retire Android, iOS and macOS devices

- *What's needed in your environment (for example isolate a device)*

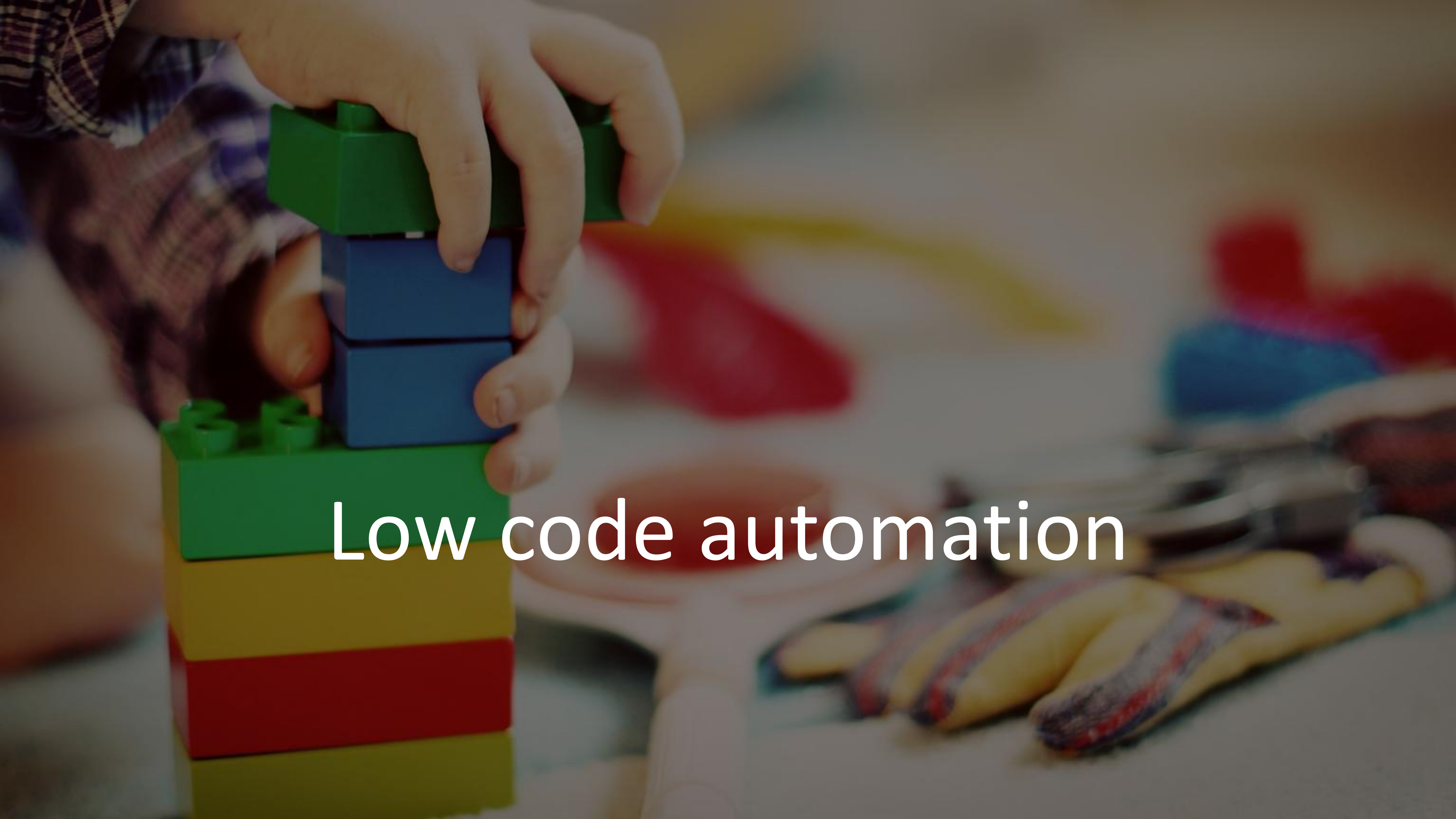
Which service are involved

- Entra ID
- Microsoft Intune

- Defender for Endpoint (optional)
- Depends on your further needs

  A lot is possible via Graph API

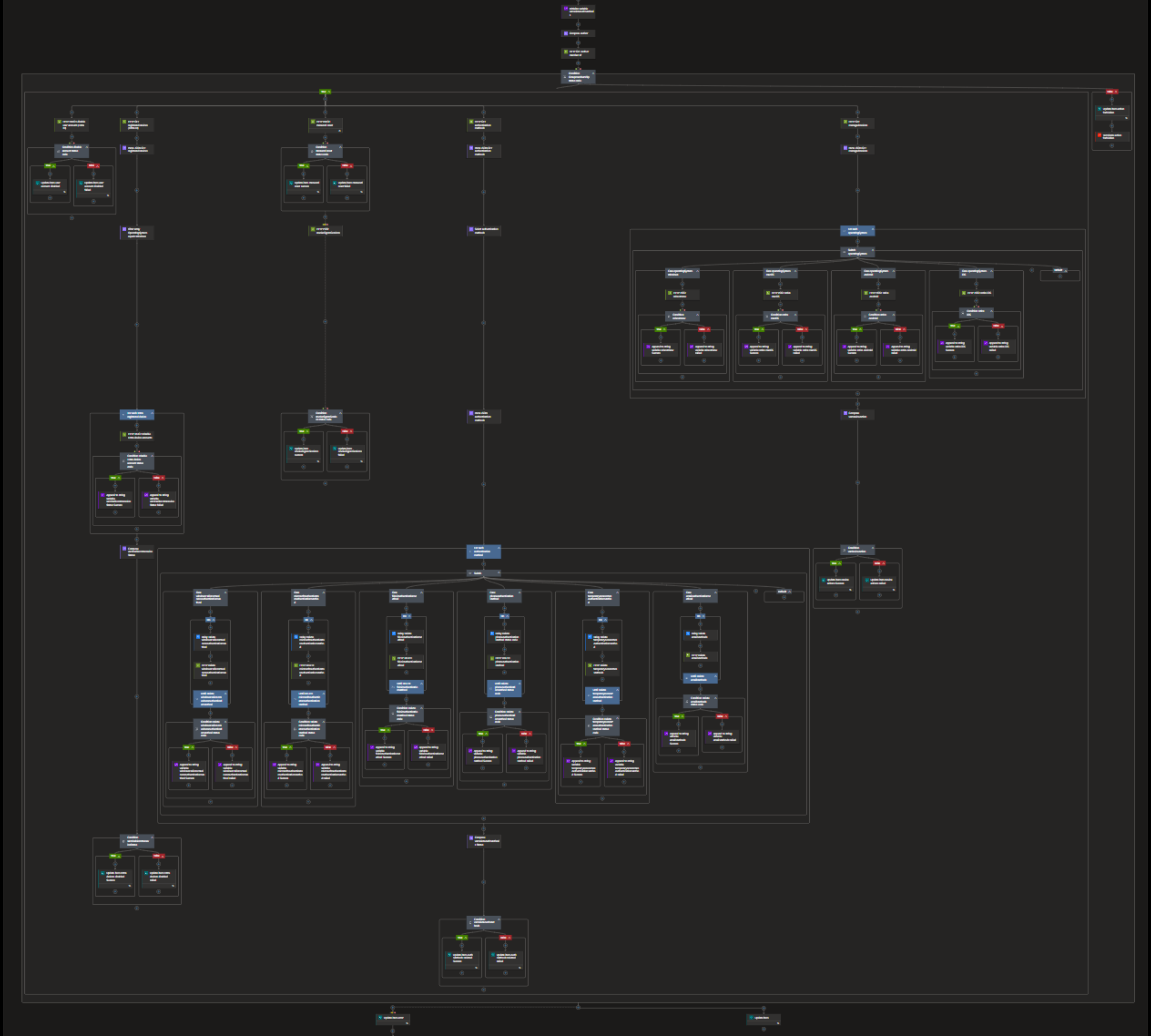
Let's automate this process



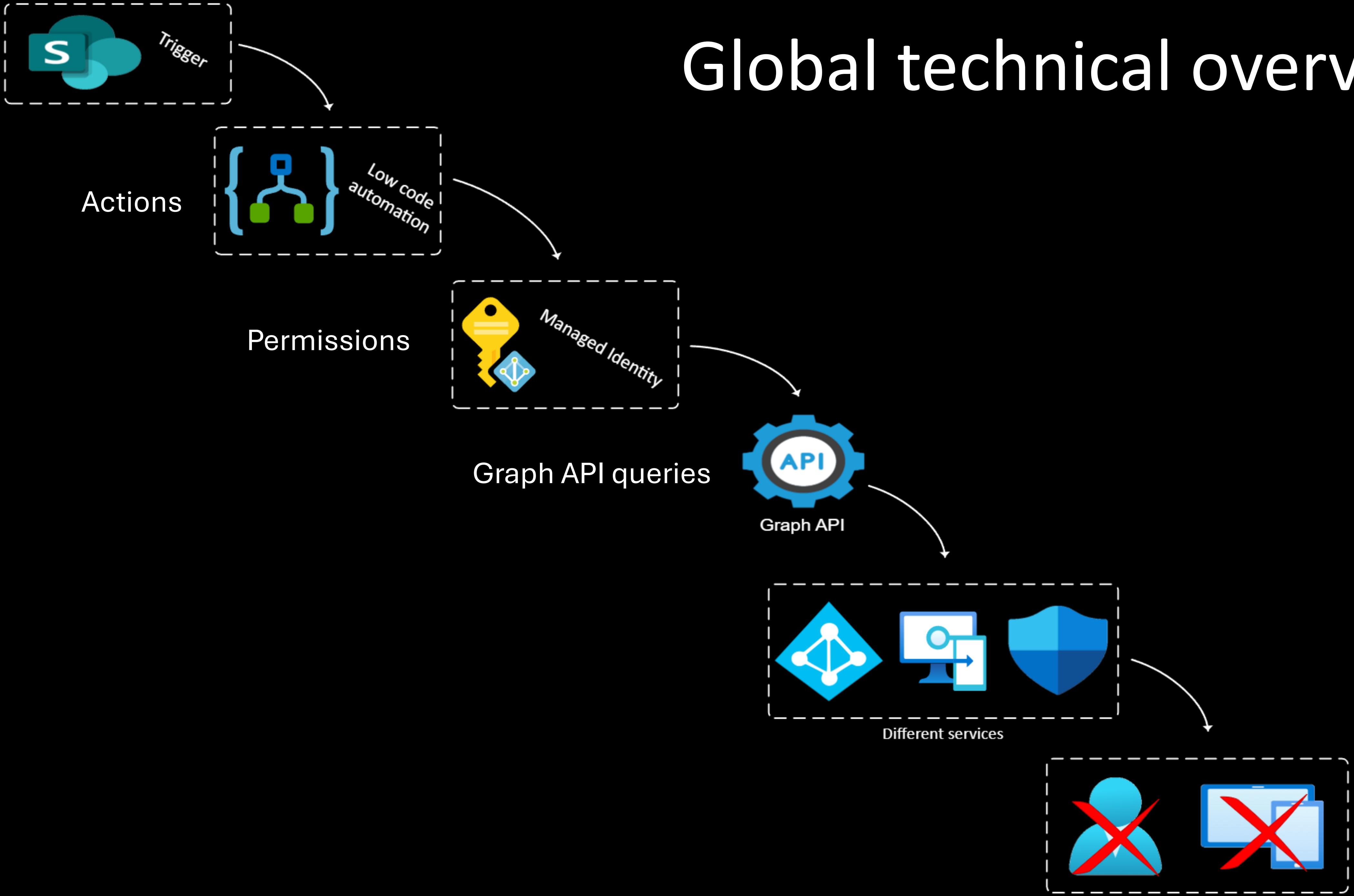
Low code automation

Power Automate vs Azure Logic Apps

Audience:	End users	IT pro, developers
Licensing:	Per user licensing (M365 suite)	Consumption-based or fixed pricing model via an Azure subscription
Use cases:	Automating everyday tasks, like managing approvals	Complex workflows, like this solution



Global technical overview



Actions

Permissions

Graph API queries

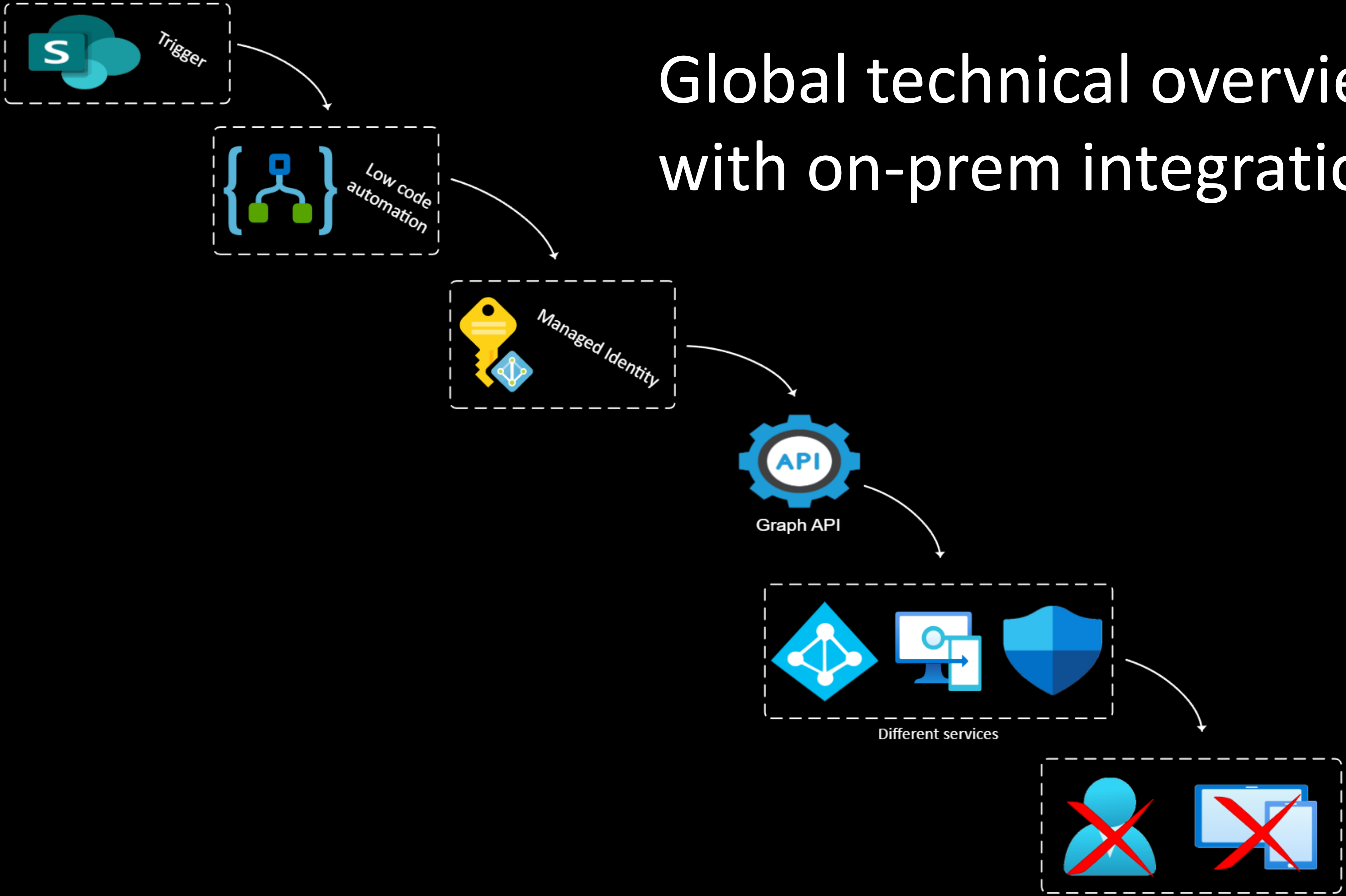
Blog post

Managed Identity

- Enterprise application
- Automatically managed to get an auth token
- No username or password
- System-assigned or user-assigned
- Application permissions + User administrator role

Demo

Global technical overview with on-prem integration



Trigger

Low code automation

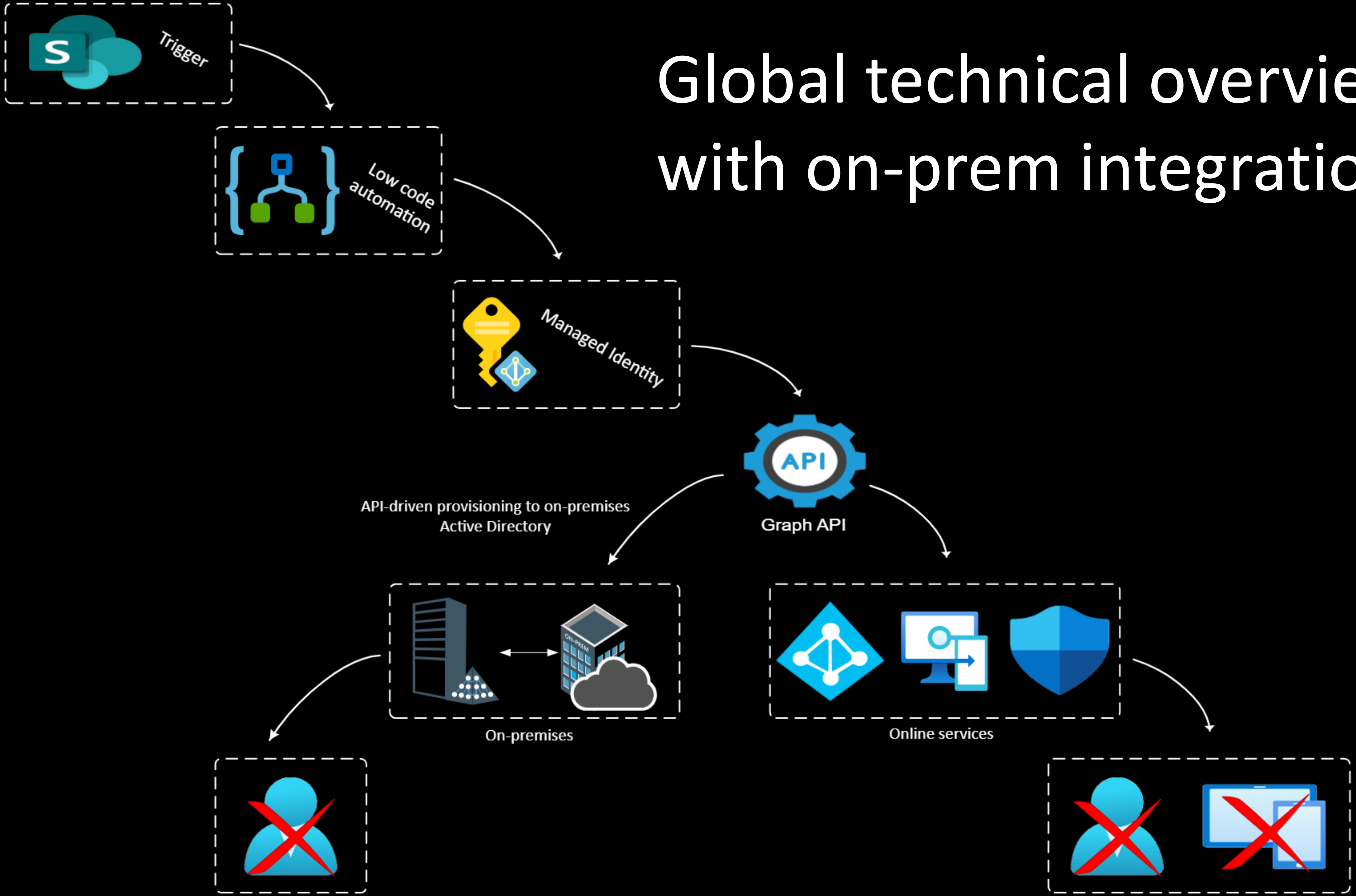
Managed Identity

Graph API

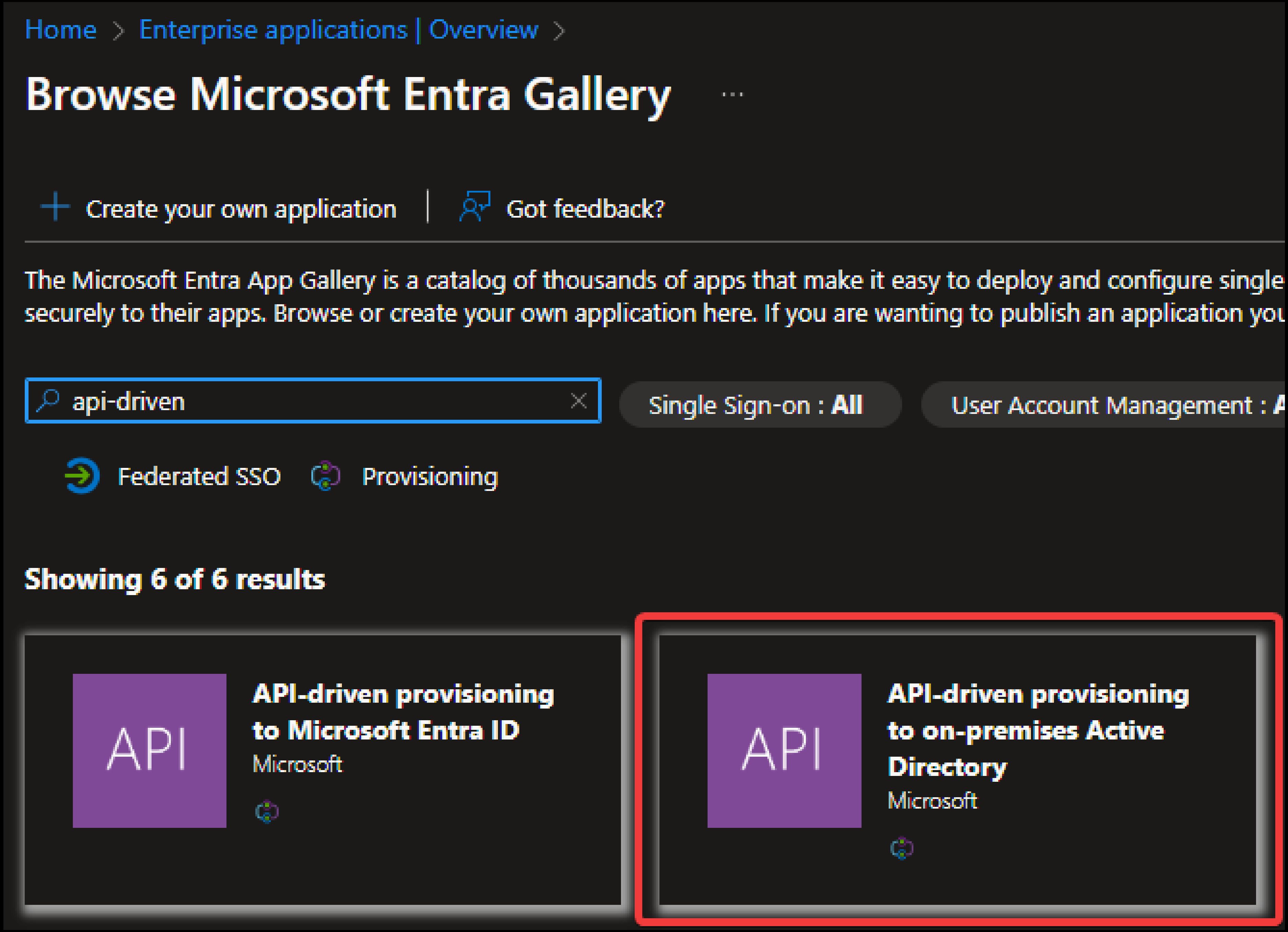
Different services

Blog post

Global technical overview with on-prem integration



Blog post


Home > Enterprise applications | Overview >
...
+ Create your own application
Got feedback?
Federated SSO
Provisioning

Browse Microsoft Entra Gallery

The Microsoft Entra App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single
securely to their apps. Browse or create your own application here. If you are wanting to publish an application you

api-driven

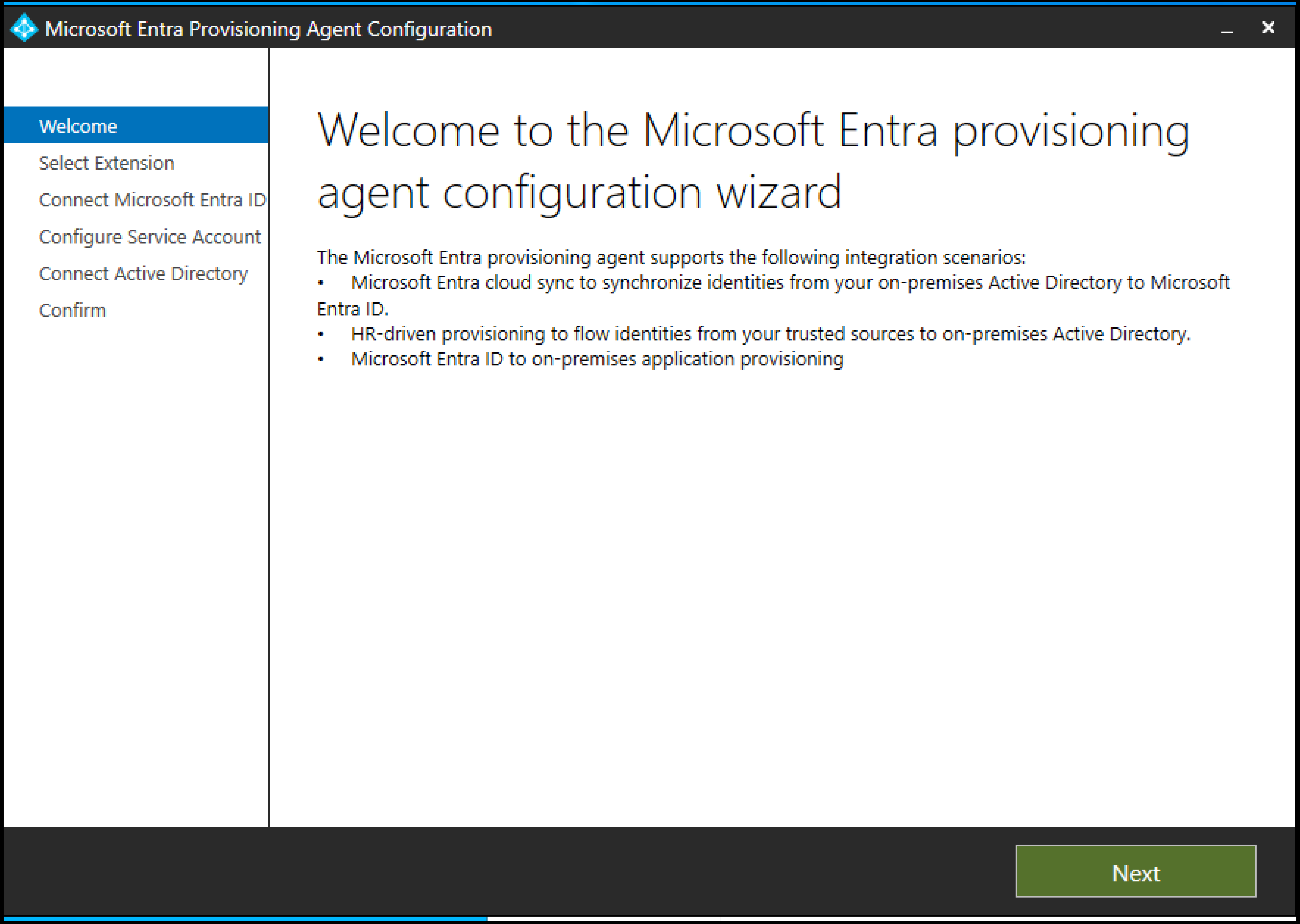
Single Sign-on : **All**

User Account Management : A

Showing 6 of 6 results

API **API-driven provisioning to Microsoft Entra ID**
Microsoft

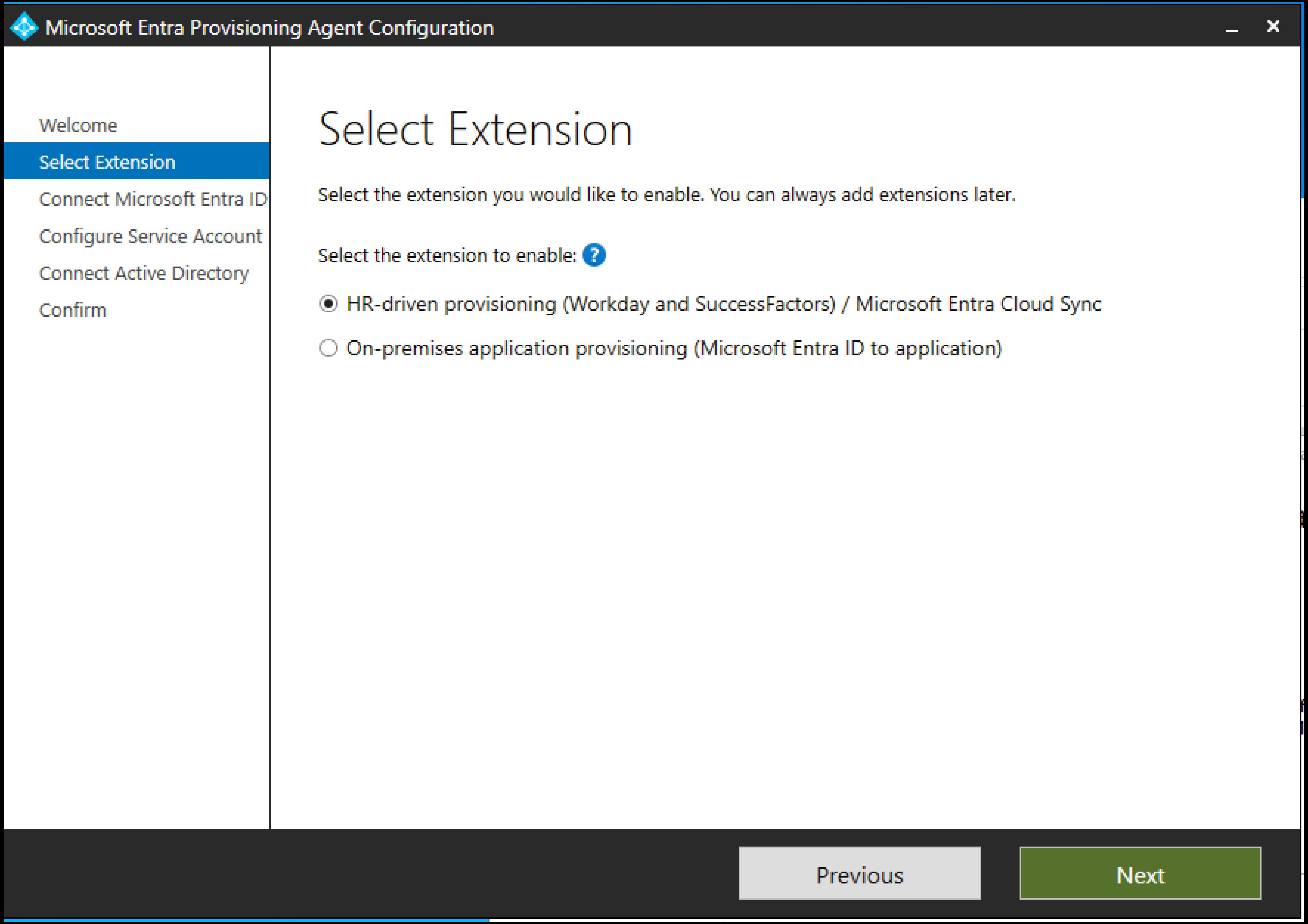
API **API-driven provisioning to on-premises Active Directory**
Microsoft


Microsoft Entra Provisioning Agent Configuration
Welcome
Select Extension
Connect Microsoft Entra ID
Configure Service Account
Connect Active Directory
Confirm
Next

Welcome to the Microsoft Entra provisioning agent configuration wizard

The Microsoft Entra provisioning agent supports the following integration scenarios:

- Microsoft Entra cloud sync to synchronize identities from your on-premises Active Directory to Microsoft Entra ID.
- HR-driven provisioning to flow identities from your trusted sources to on-premises Active Directory.
- Microsoft Entra ID to on-premises application provisioning



Microsoft Entra Provisioning Agent Configuration
Welcome
Select Extension
Connect Microsoft Entra ID
Configure Service Account
Connect Active Directory
Confirm

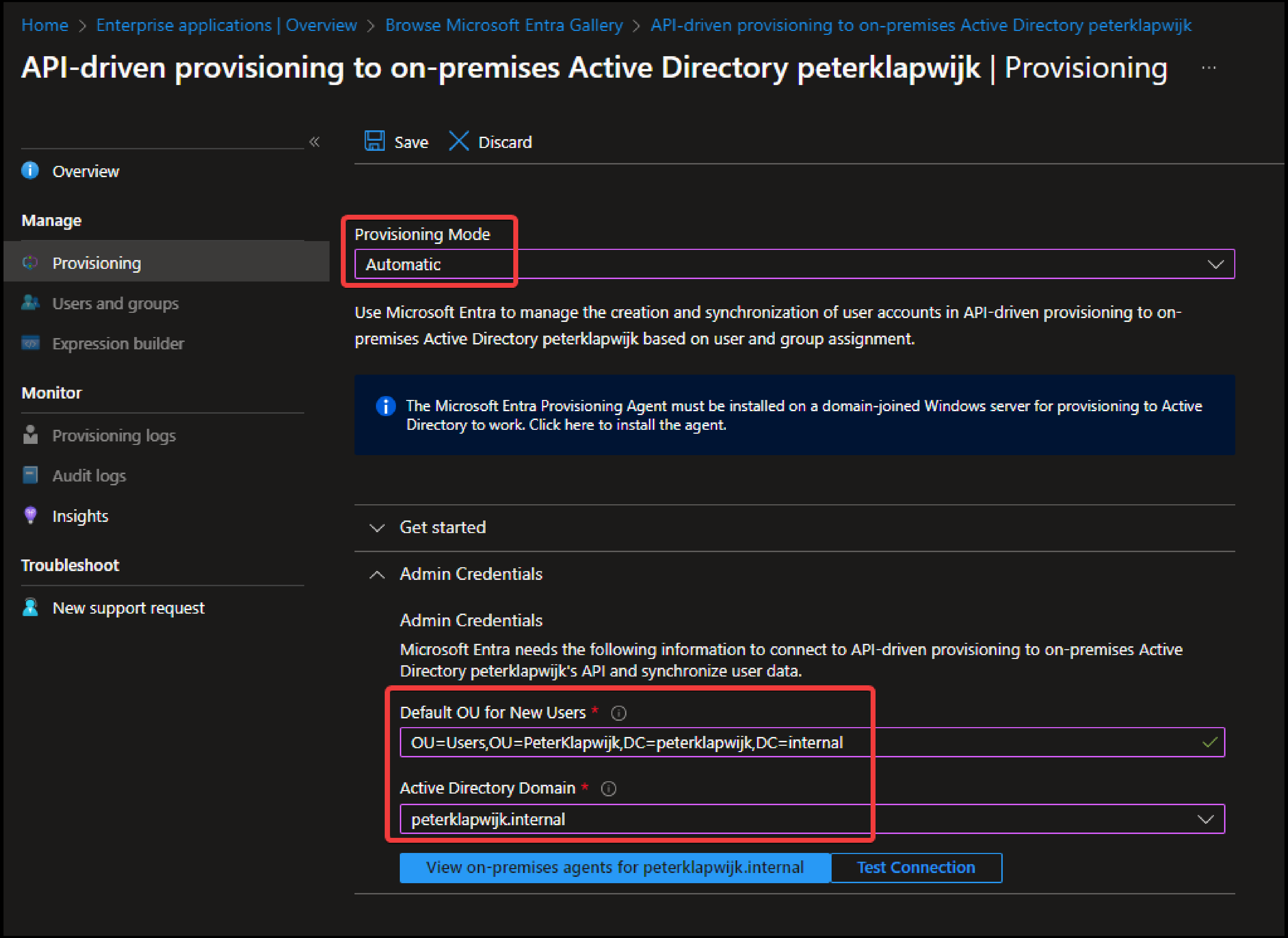
Select Extension

Select the extension you would like to enable. You can always add extensions later.

Select the extension to enable: ?

● HR-driven provisioning (Workday and SuccessFactors) / Microsoft Entra Cloud Sync

○ On-premises application provisioning (Microsoft Entra ID to application)



Home > Enterprise applications | Overview > Browse Microsoft Entra Gallery > API-driven provisioning to on-premises Active Directory peterklapwijk

API-driven provisioning to on-premises Active Directory peterklapwijk | Provisioning

Provisioning Mode: Automatic

Use Microsoft Entra to manage the creation and synchronization of user accounts in API-driven provisioning to on-premises Active Directory peterklapwijk based on user and group assignment.

The Microsoft Entra Provisioning Agent must be installed on a domain-joined Windows server for provisioning to Active Directory to work. Click here to install the agent.

Admin Credentials

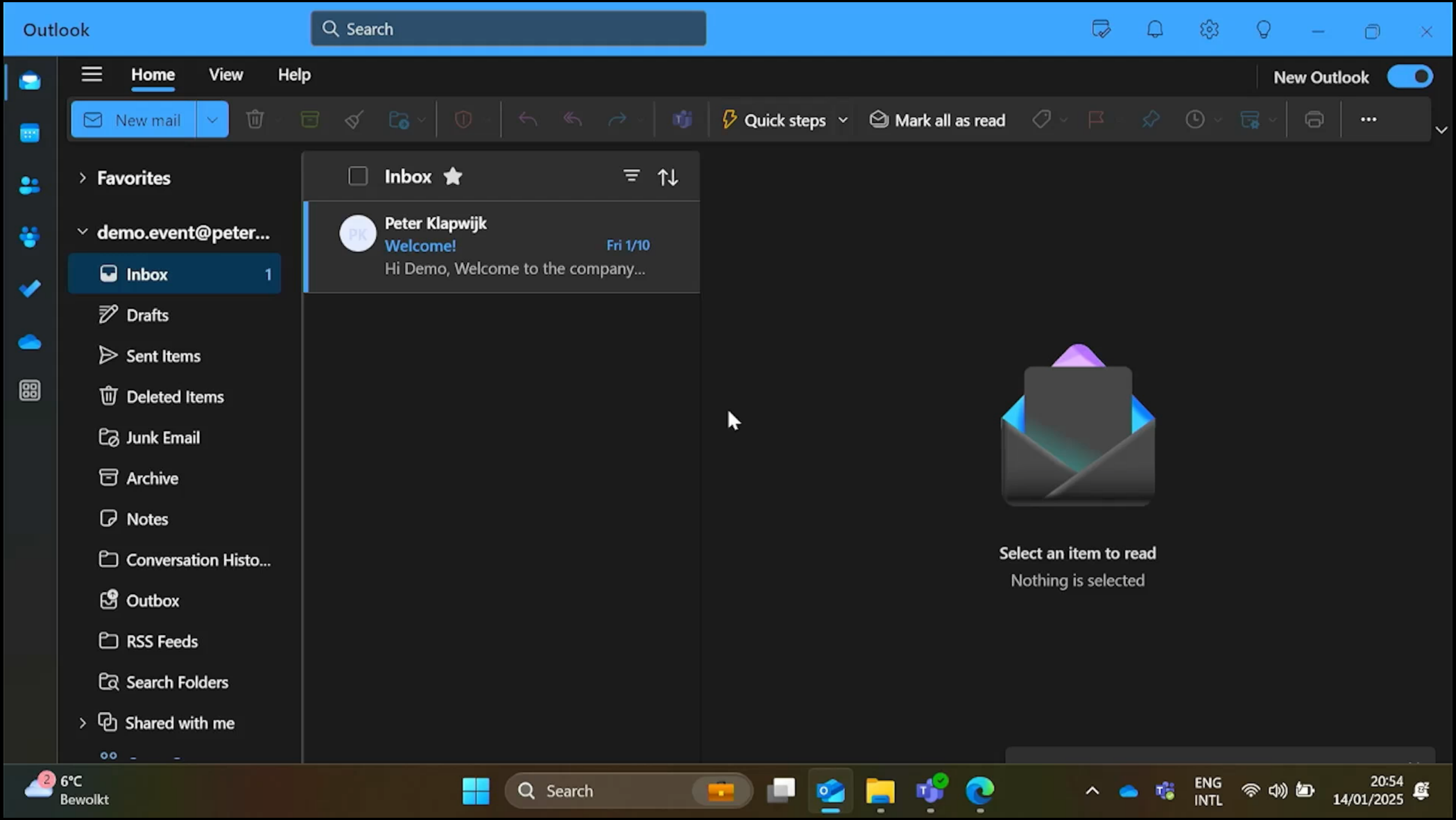
Microsoft Entra needs the following information to connect to API-driven provisioning to on-premises Active Directory peterklapwijk's API and synchronize user data.

Default OU for New Users *: OU=Users,OU=PeterKlapwijk,DC=peterklapwijk,DC=internal

Active Directory Domain *: peterklapwijk.internal

It’s that simple

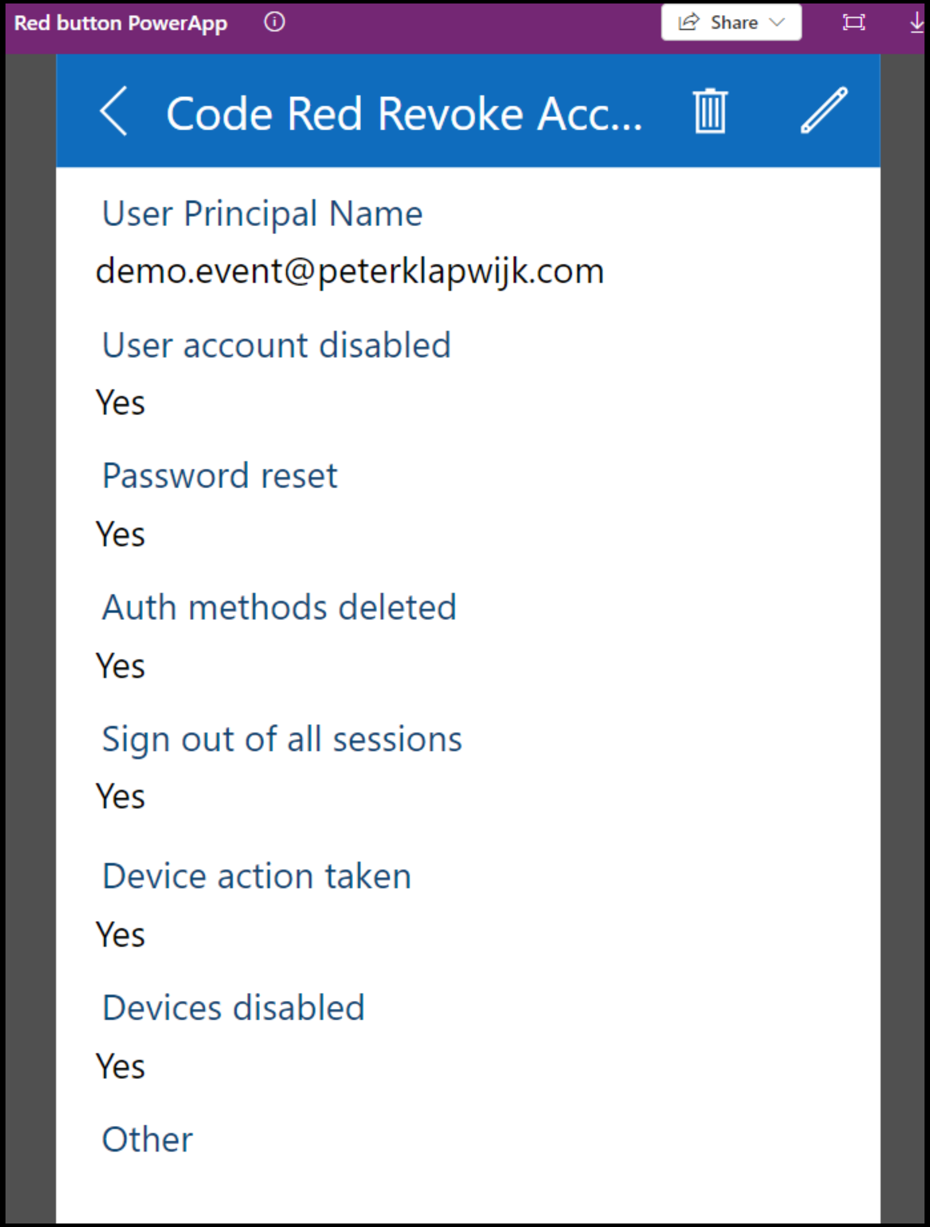
Demo



Peter Klapwijk
Welcome! Fri 1/10
Hi Demo, Welcome to the company...

Select an item to read
Nothing is selected

PowerApp



User Principal Name

demo.event@peterklapwijk.com

User account disabled

Yes

Password reset

Yes

Auth methods deleted

Yes

Sign out of all sessions

Yes

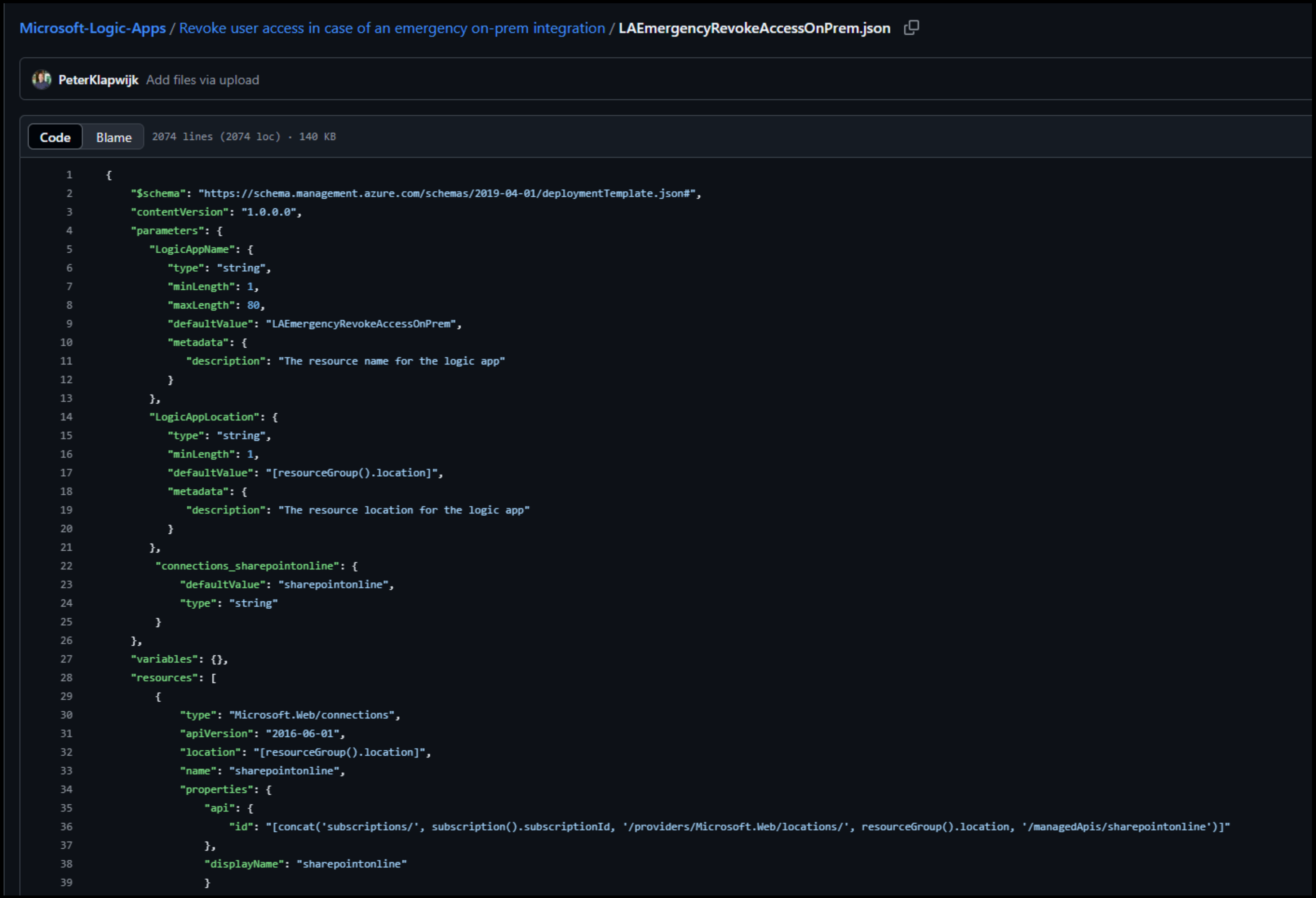
Device action taken

Yes

Devices disabled

Yes

Other



Microsoft-Logic-Apps / Revoke user access in case of an emergency on-prem integration / LAEmergencyRevokeAccessOnPrem.json

PeterKlapwijk Add files via upload

```
{
    "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "LogicAppName": {
            "type": "string",
            "minLength": 1,
            "maxLength": 80,
            "defaultValue": "LAEmergencyRevokeAccessOnPrem",
            "metadata": {
                "description": "The resource name for the logic app"
            }
        },
        "LogicAppLocation": {
            "type": "string",
            "minLength": 1,
            "defaultValue": "[resourceGroup().location]",
            "metadata": {
                "description": "The resource location for the logic app"
            }
        },
         "connections_sharepointonline": {
              "defaultValue": "sharepointonline",
              "type": "string"
         }
    },
    "variables": {},
    "resources": [
         {
              "type": "Microsoft.Web/connections",
              "apiVersion": "2016-06-01",
              "location": "[resourceGroup().location]",
              "name": "sharepointonline",
              "properties": {
                  "api": {
                      "id": "[concat('subscriptions/', subscription().subscriptionId, '/providers/Microsoft.Web/locations/', resourceGroup().location, '/managedApis/sharepointonline')]"
                  },
                  "displayName": "sharepointonline"
                  }
```

Templates on GitHub

Questions!?

Dutch
Microsoft
& Security
Meetup

Related blog post

Thank you!

Reach out to me!

Dutch
Microsoft
& Security
Meetup