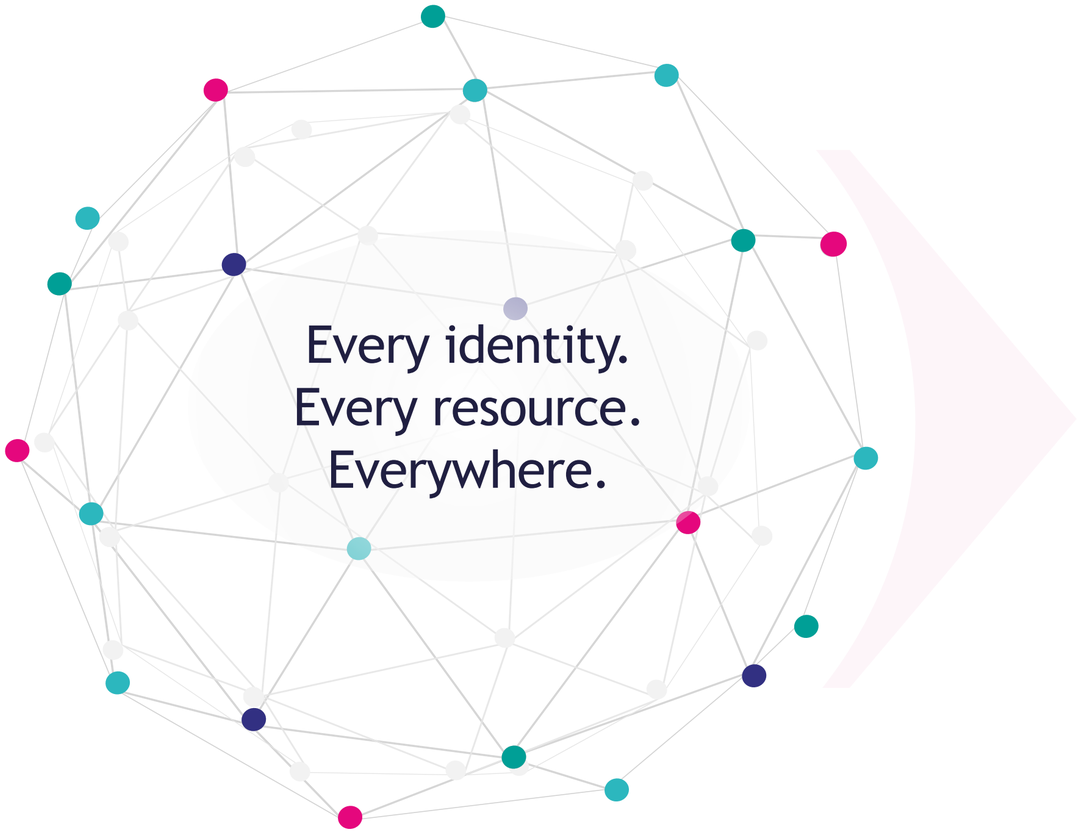
Secure & govern your applications with Entra ID

Identity has become the perimeter..



Accelerated growth of identities and apps, on and off the corporate network, requiring secure, user-friendly access

Massive rise in identity attacks—more than 4,000 password attacks per second—increasing risk of compromised accounts

Evolving regulations and compliance requirements for protecting identities and auditing access rights

- Guus van Berge
- Amsterdam is home
- Consultant at InSpark
- 20 years+ experience with Microsoft solutions
- Focus on Secure Identity
- Identity Governance connoisseur

“I help organizations embrace proactive security with Zero Trust Identity implementations”

“Automatically ensure that the right people have the right access to the right resources at the right time”

Identity lifecycle

- Source of truth
- JML

Access lifecycle

- Delegate access
- Review access

Privileged access lifecycle

- Entra/Azure roles
- Other scenarios

“Automatically ensure that the right people have the right access to the right resources at the right time”

Identity lifecycle

- Source of truth
- JML

Access lifecycle

- Delegate access
- Review access

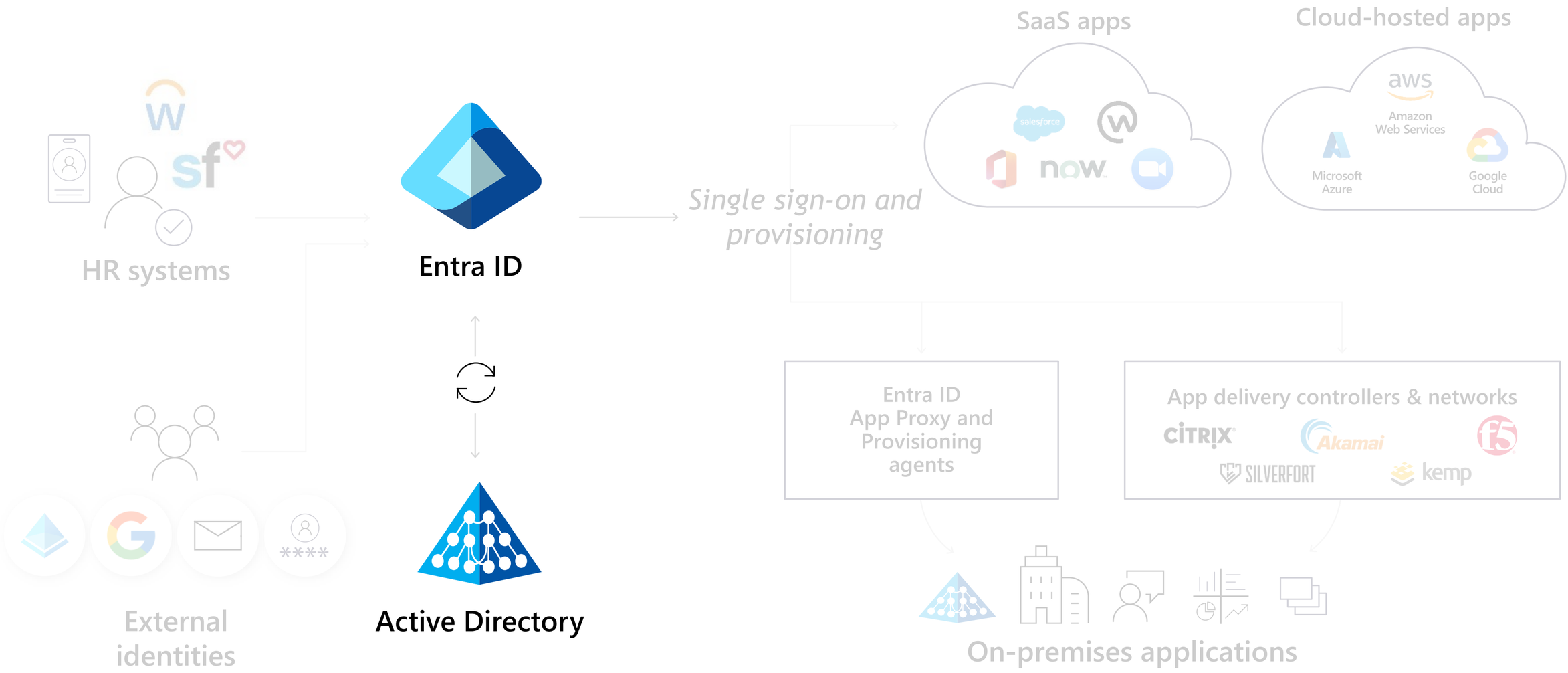
Privileged access lifecycle

- Entra/Azure roles
- Other scenarios

What to expect today

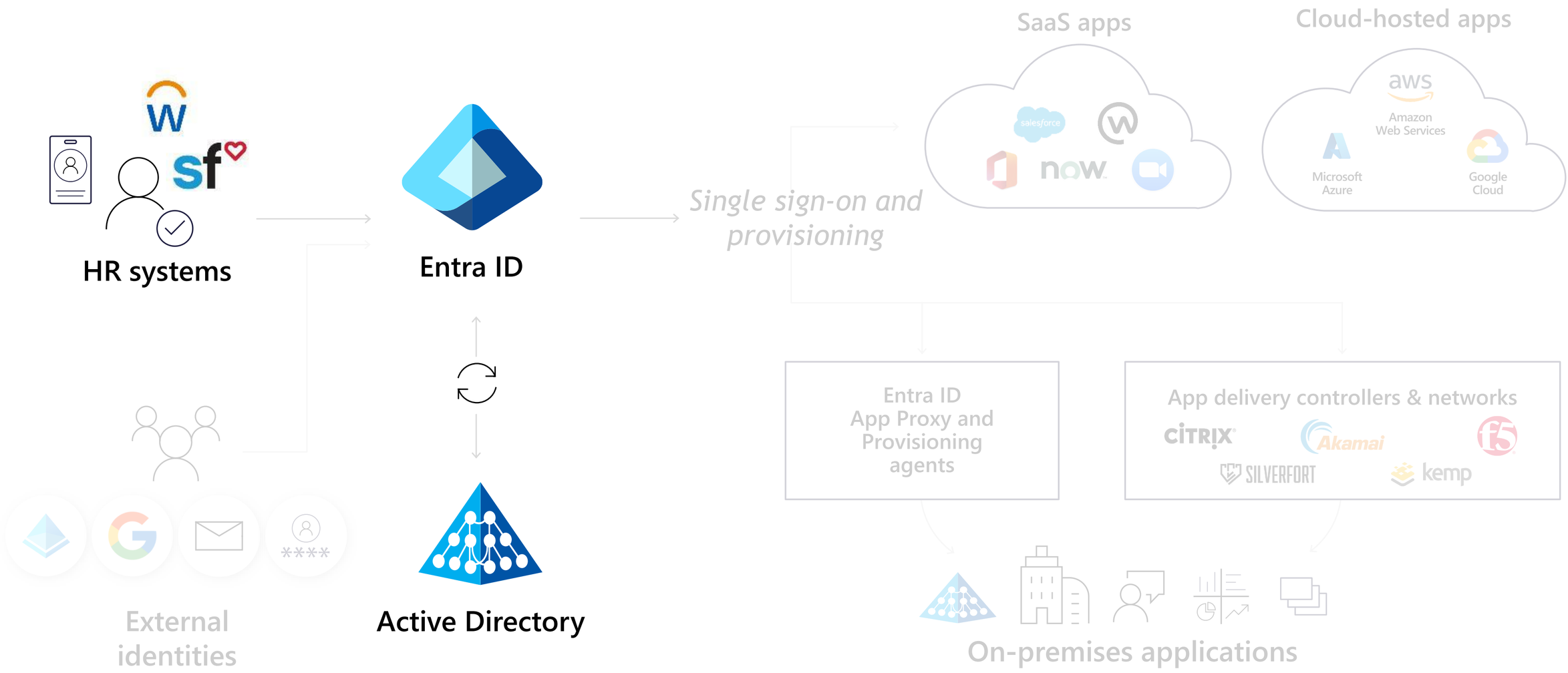
- App provisioning
- Access Packages
- Access reviews
- PIM

Provisioning



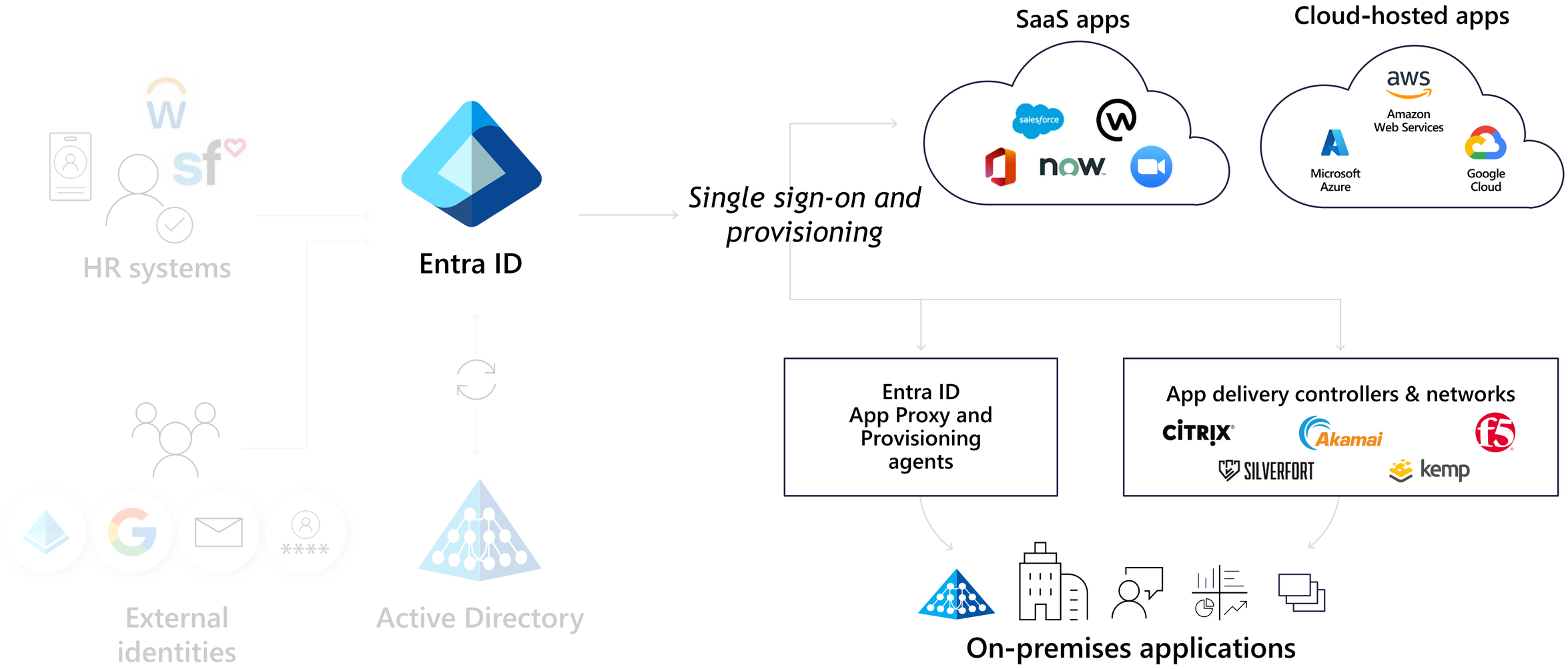
Provisioning

Inbound provisioning



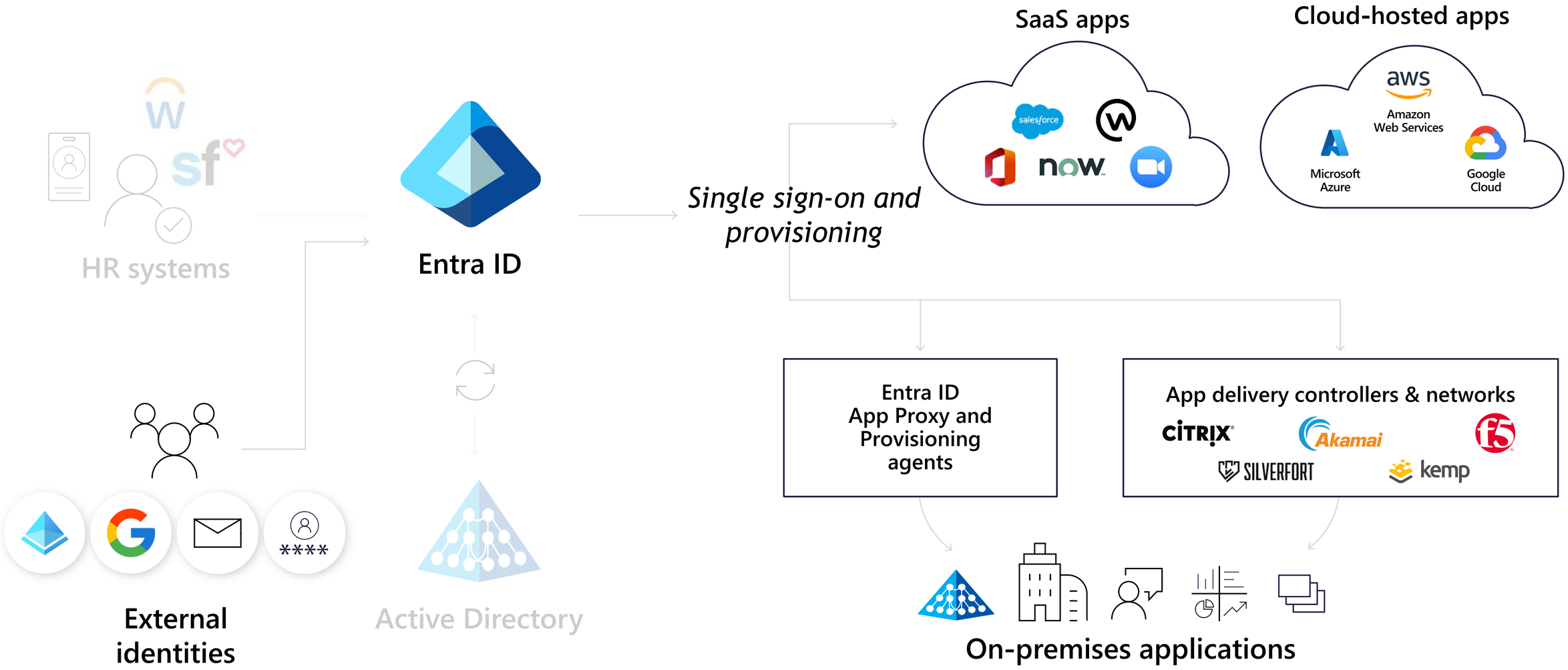
Provisioning

App provisioning



Provisioning

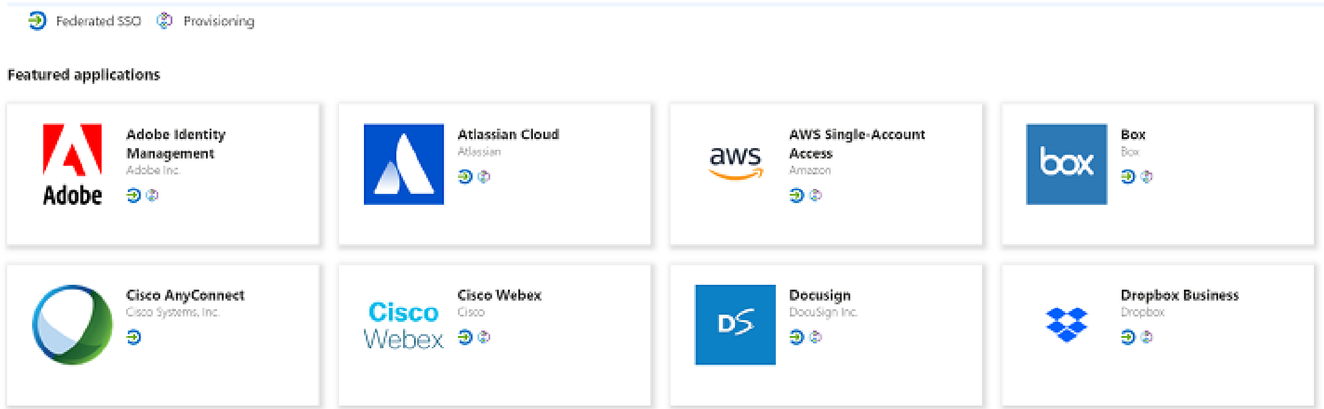
App provisioning

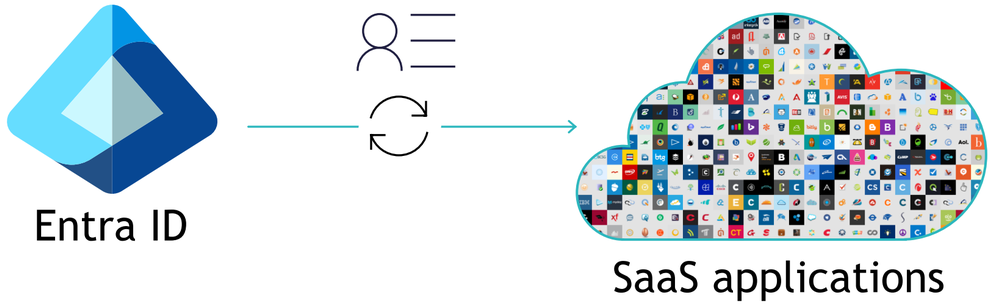


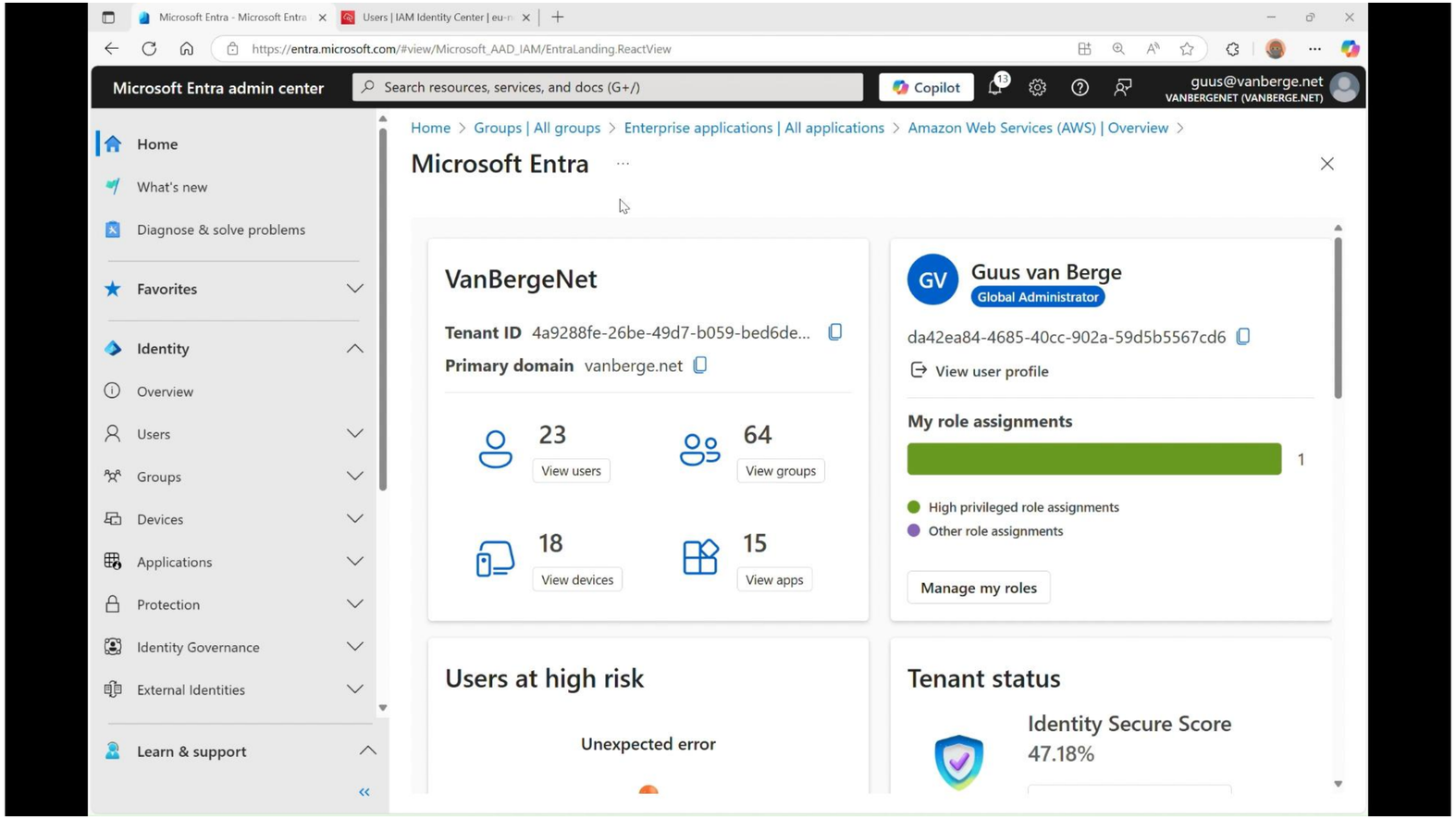
What Is

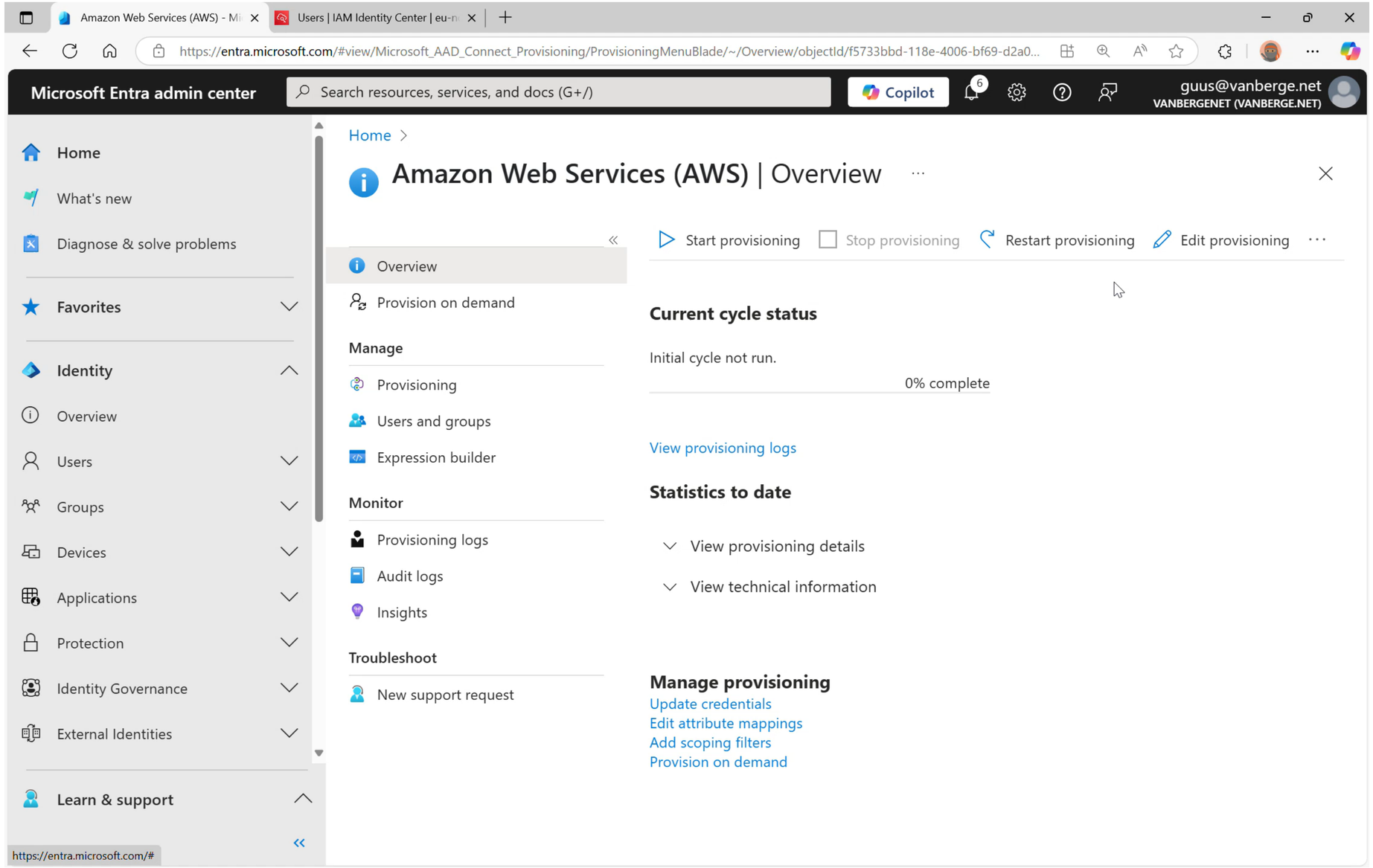
Provisioning to SaaS Apps

- Selected apps support provisioning of groups.
- Customizable attribute mappings.
- Out of the box tools for monitoring and auditing.
- Custom alerts using Log Analytics.
- Easily implemented in a brown field scenario!





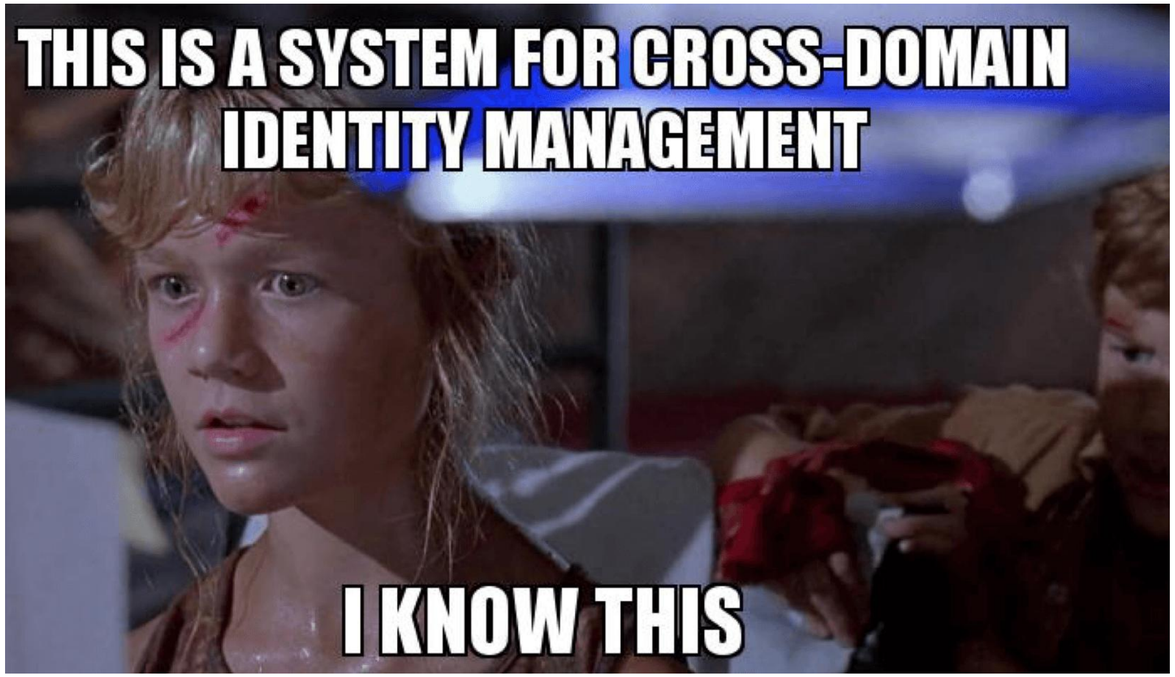

Microsoft Entra - Microsoft Entra
Users | IAM Identity Center | eu-
https://entra.microsoft.com/#view/Microsoft_AAD_IAM/EntraLanding.ReactView
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
guus@vanberge.net
VANBERGENET (VANBERGE.NET)
Home
What's new
Diagnose & solve problems
Favorites
Identity
Overview
Users
Groups
Devices
Applications
Protection
Identity Governance
External Identities
Learn & support
Home > Groups | All groups > Enterprise applications | All applications > Amazon Web Services (AWS) | Overview >
Microsoft Entra
VanBergeNet
Tenant ID 4a9288fe-26be-49d7-b059-bed6de...
Primary domain vanberge.net
23
View users
64
View groups
18
View devices
15
View apps
GV
Guus van Berge
Global Administrator
da42ea84-4685-40cc-902a-59d5b5567cd6
View user profile
My role assignments
1
High privileged role assignments
Other role assignments
Manage my roles
Users at high risk
Unexpected error
Tenant status
Identity Secure Score
47.18%

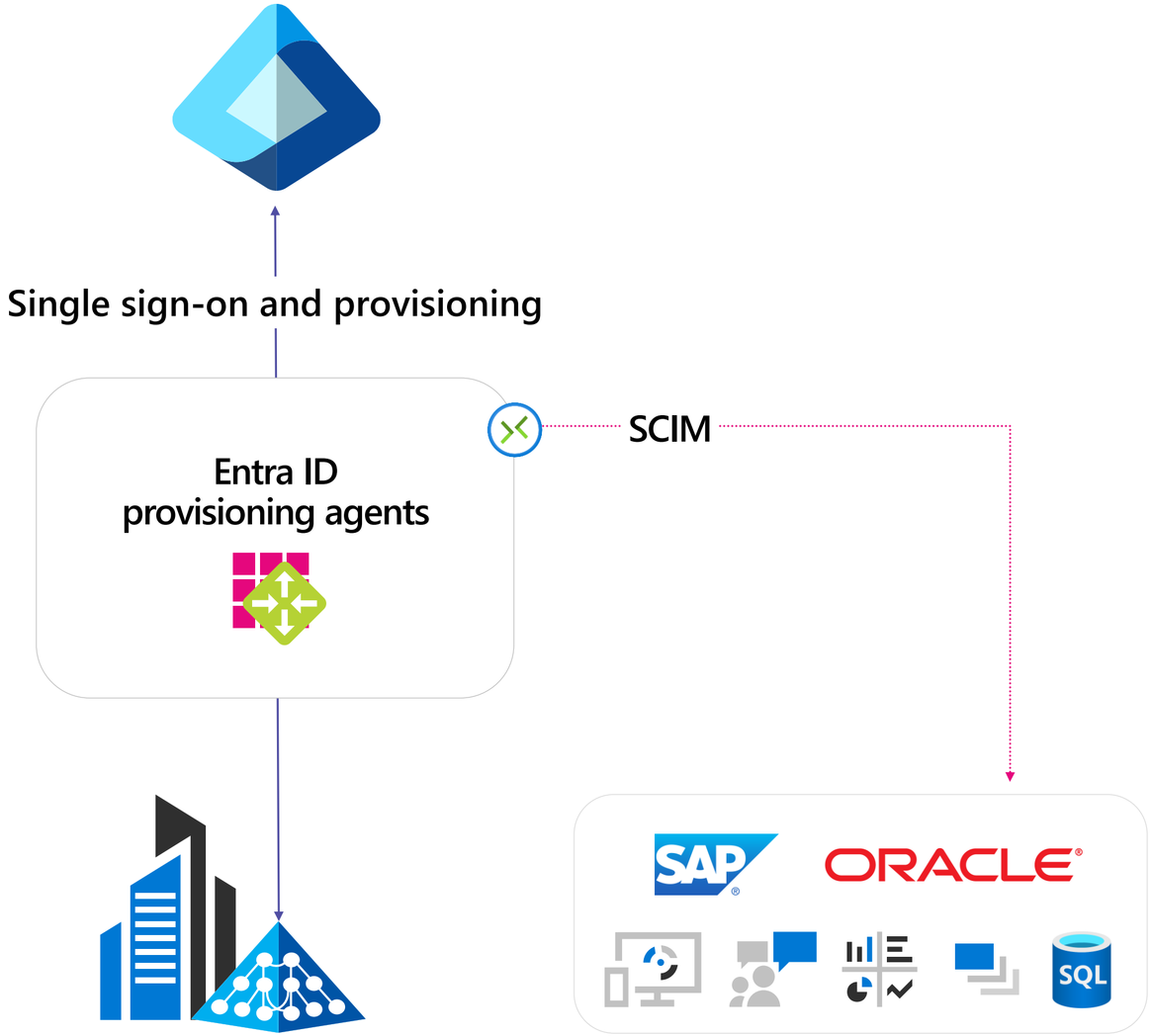

Amazon Web Services (AWS) - Mi
Users | IAM Identity Center | eu-n
https://entra.microsoft.com/#view/Microsoft_AAD_Connect_Provisioning/ProvisioningMenuBlade/~/Overview/objectId/f5733bbd-118e-4006-bf69-d2a0...
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
6
guus@vanberge.net
VANBERGENET (VANBERGE.NET)
Home
What's new
Diagnose & solve problems
Favorites
Identity
Overview
Users
Groups
Devices
Applications
Protection
Identity Governance
External Identities
Learn & support
https://entra.microsoft.com/#
Home
Amazon Web Services (AWS) | Overview
Overview
Provision on demand
Manage
Provisioning
Users and groups
Expression builder
Monitor
Provisioning logs
Audit logs
Insights
Troubleshoot
New support request
Start provisioning
Stop provisioning
Restart provisioning
Edit provisioning
Current cycle status
Initial cycle not run.
0% complete
View provisioning logs
Statistics to date
View provisioning details
View technical information
Manage provisioning
Update credentials
Edit attribute mappings
Add scoping filters
Provision on demand

Provisioning

On-premises Apps

The **Entra provisioning service** supports **SCIM** enabled apps to provision users into **applications** hosted **on-premises** or in a virtual machine.





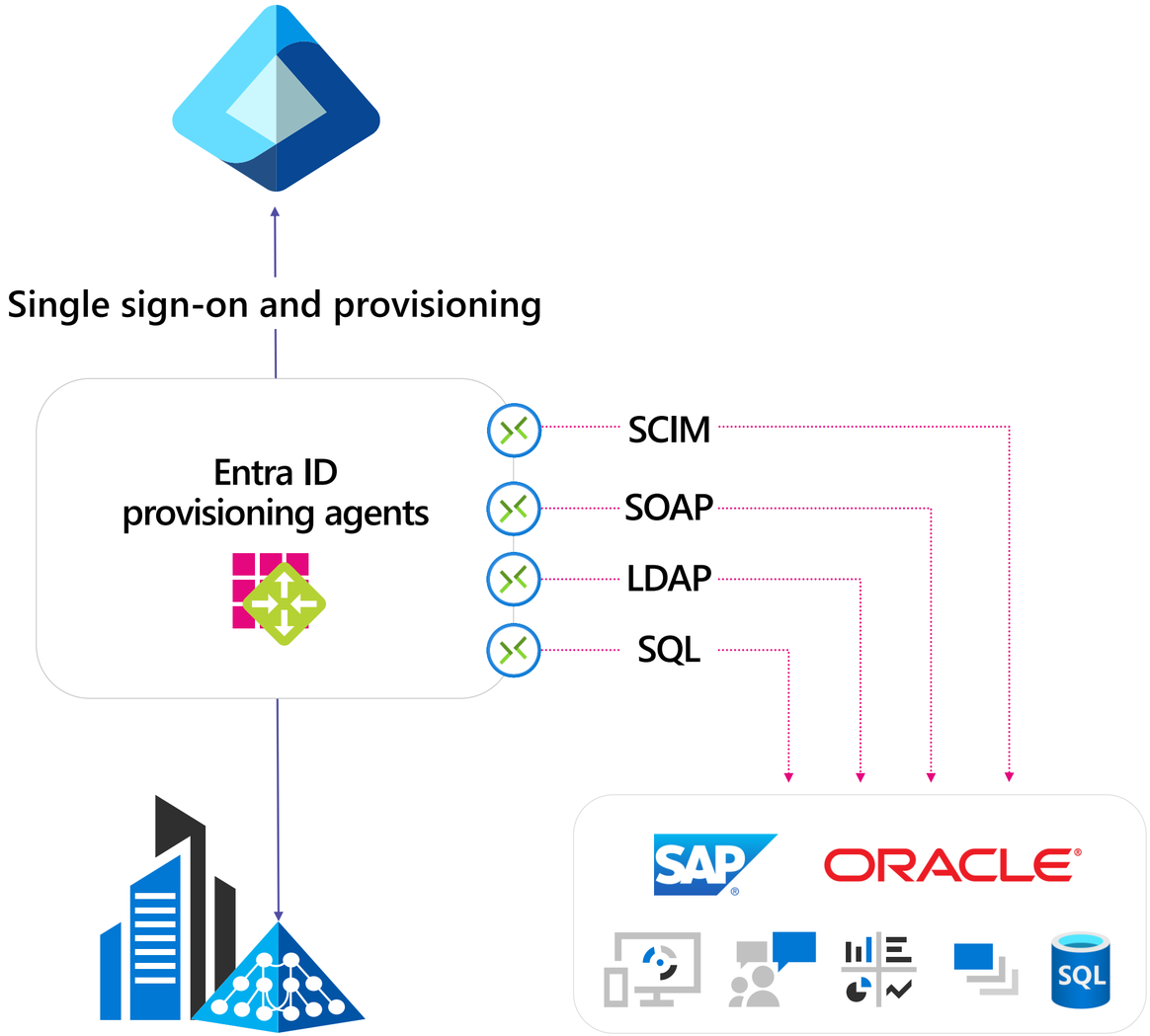
Legacy Apps

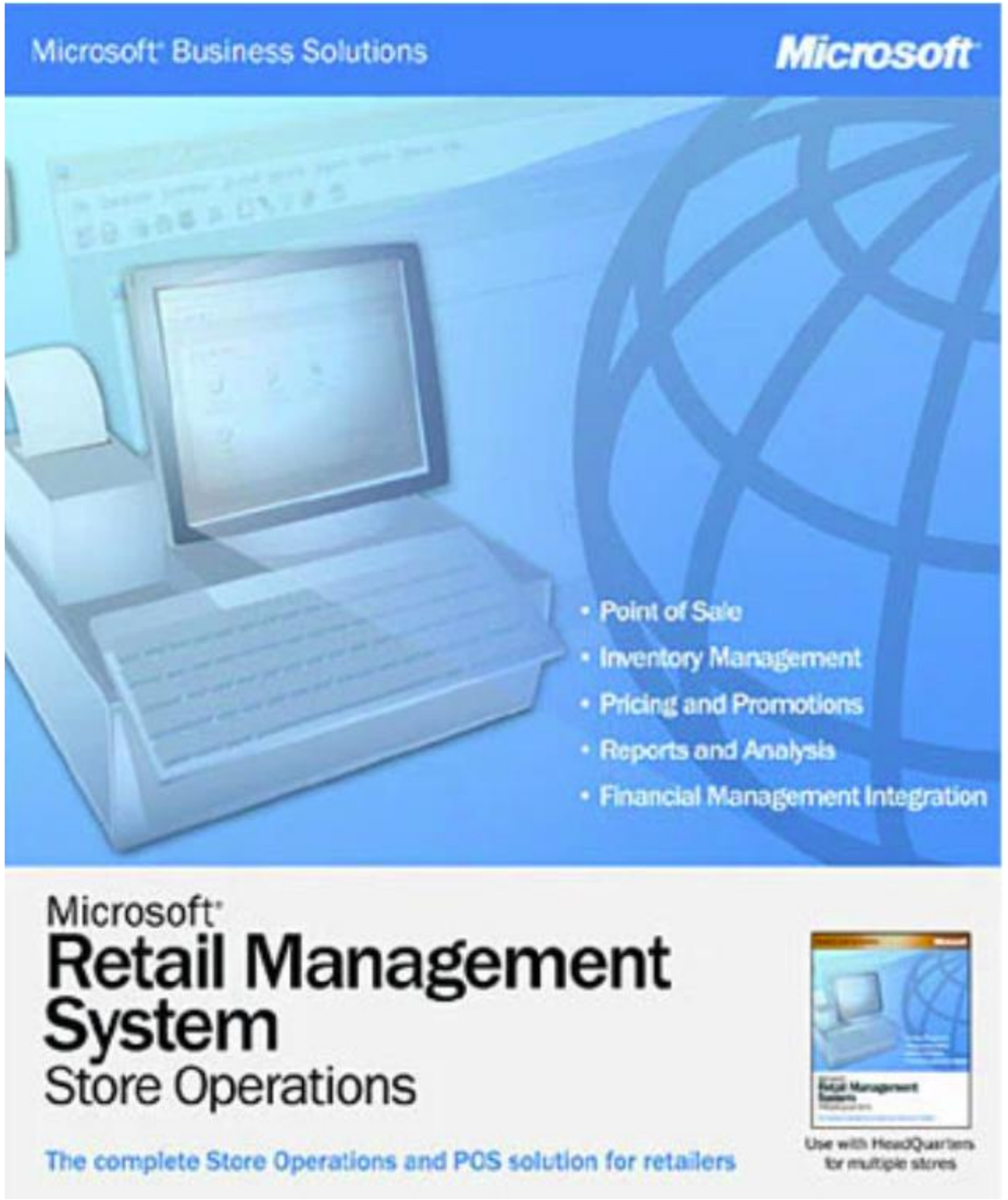
The **ECMA Connector** host converts **provisioning** requests from Entra ID to requests into **legacy applications.**

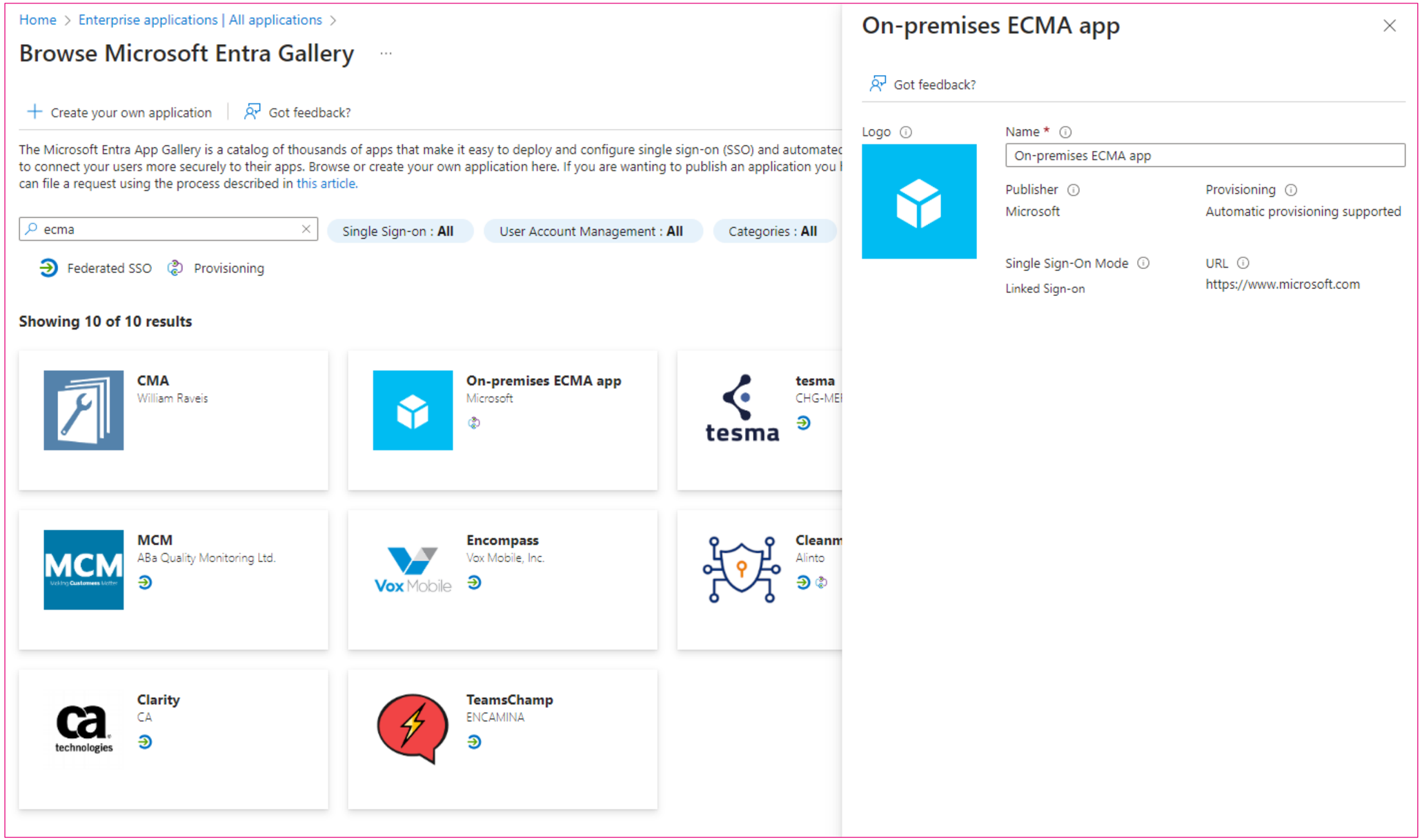
Microsoft-delivered connectors:

- **LDAP**
- **SQL** (MS SQL, Azure SQL, IBM DB2 9/10, Oracle 10g/11g/12c/18c, MsQL 5/8, Postgres)
- **Web** (REST/SOAP)
- **PowerShell** (Flat-file)

Re-use your existing MIM configuration!

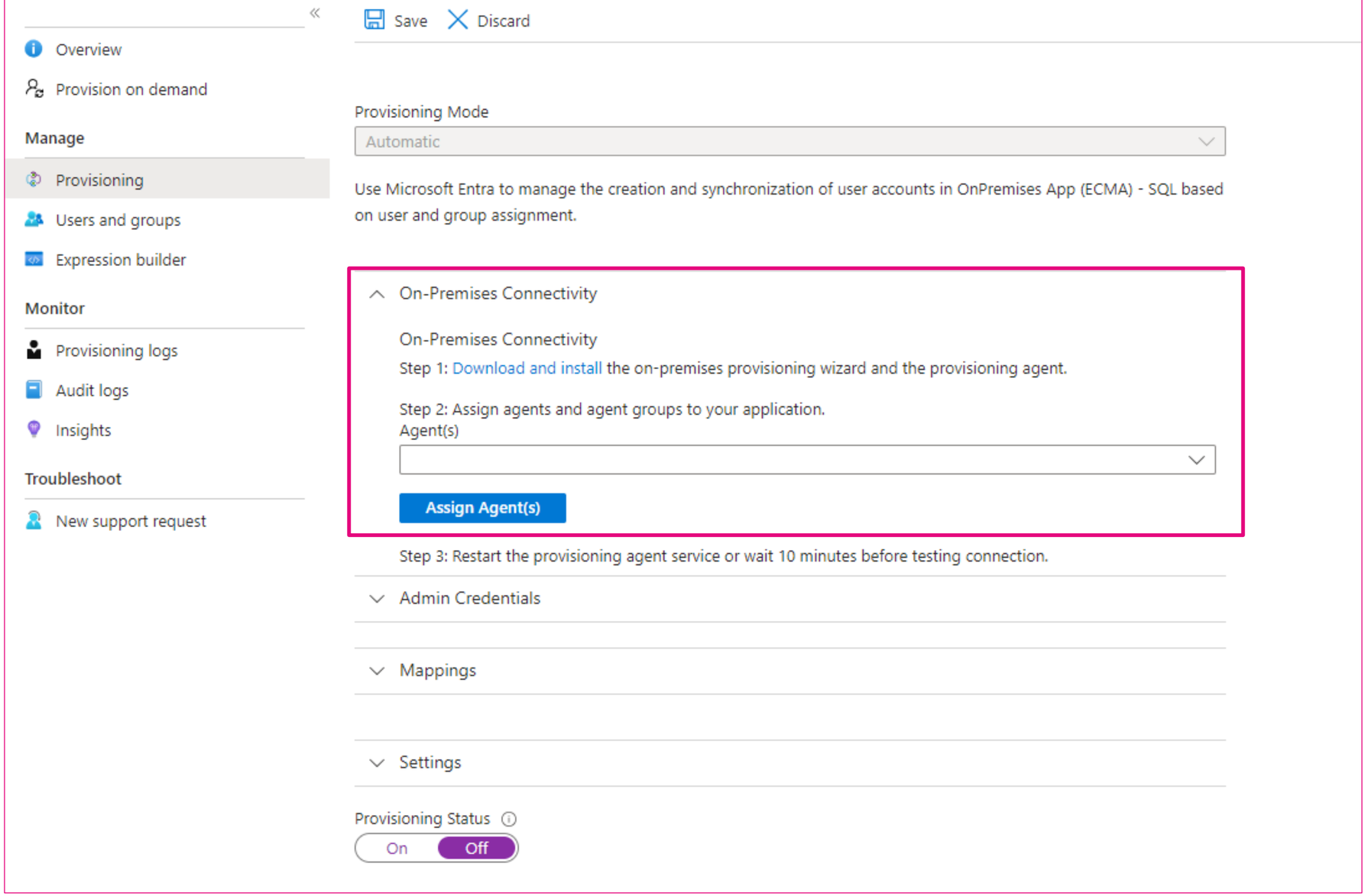


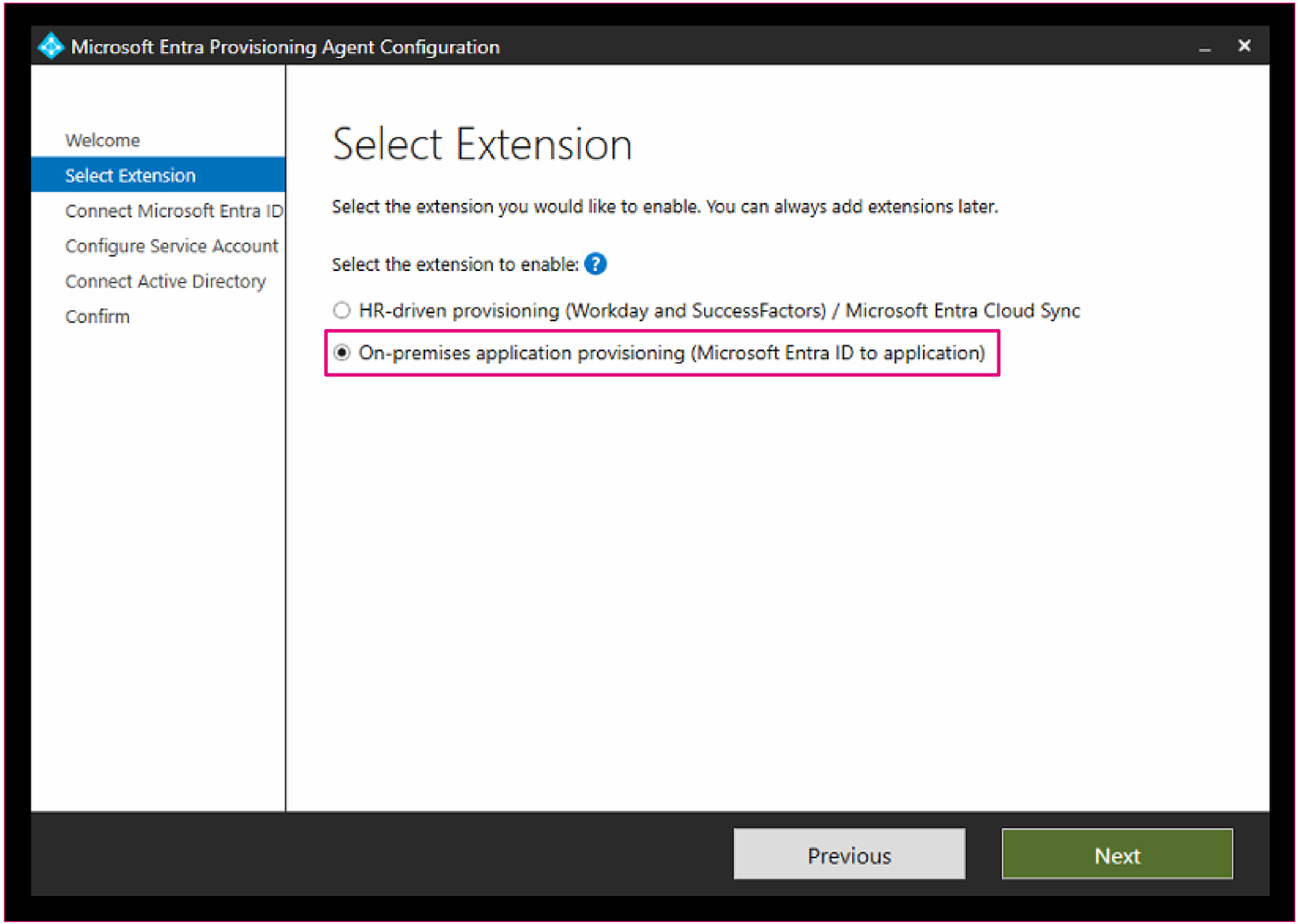

Microsoft® Business Solutions
Microsoft
• Point of Sale
• Inventory Management
• Pricing and Promotions
• Reports and Analysis
• Financial Management Integration
Microsoft®
Retail Management System
Store Operations
The complete Store Operations and POS solution for retailers
Use with HeadQuarters for multiple stores

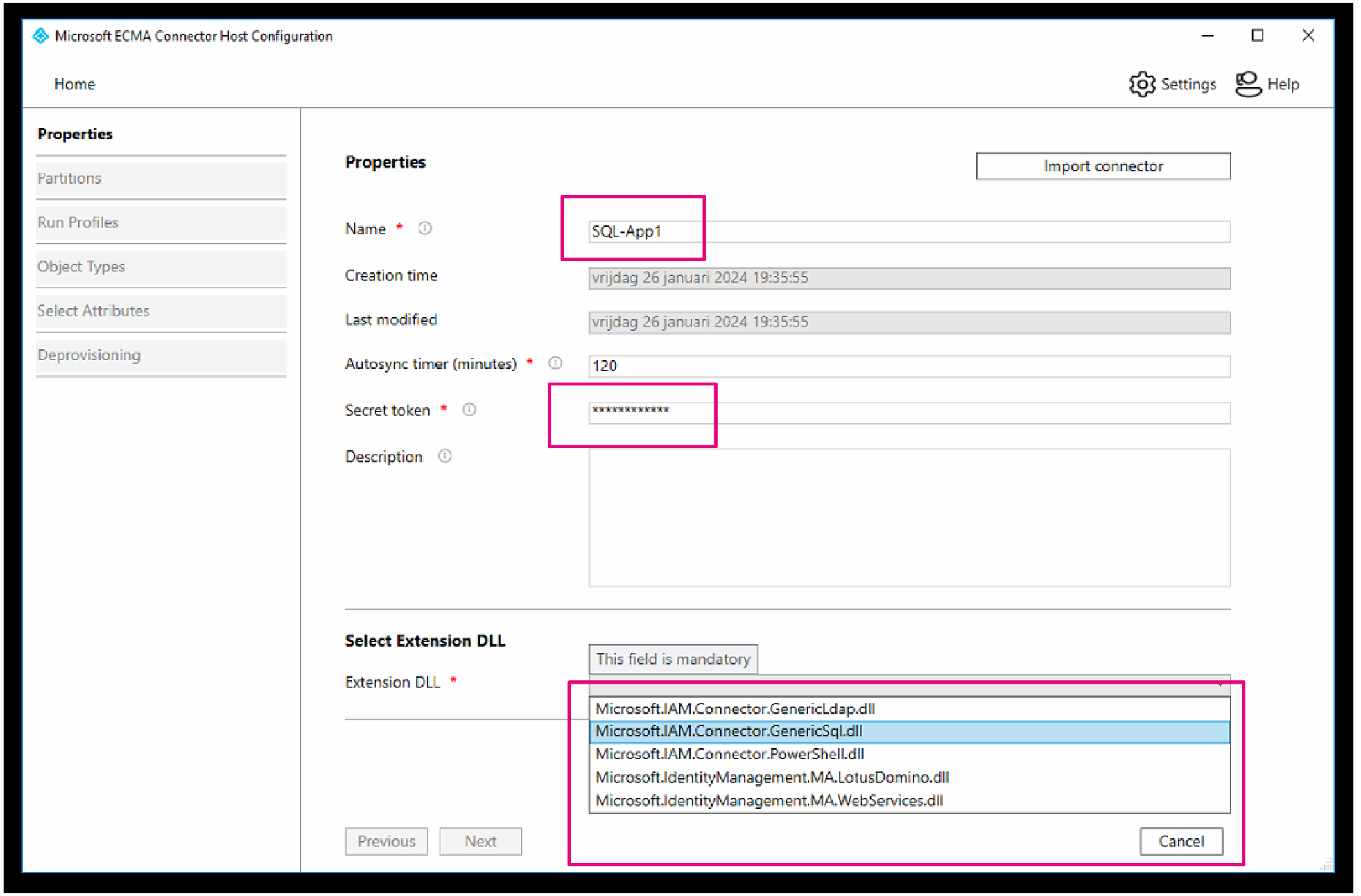

Home > Enterprise applications | All applications >
Browse Microsoft Entra Gallery
Create your own application
Got feedback?
The Microsoft Entra App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated
to connect your users more securely to their apps. Browse or create your own application here. If you are wanting to publish an application you
can file a request using the process described in this article.
ecma
Single Sign-on : All
User Account Management : All
Categories : All
Federated SSO
Provisioning
Showing 10 of 10 results
CMA
William Raveis
On-premises ECMA app
Microsoft
tesma
MCM
ABa Quality Monitoring Ltd.
Encompass
Vox Mobile, Inc.
Clarity
CA
TeamsChamp
ENCAMINA
On-premises ECMA app
Got feedback?
Logo
Name *
On-premises ECMA app
Publisher
Microsoft
Provisioning
Automatic provisioning supported
Single Sign-On Mode
Linked Sign-on
URL
https://www.microsoft.com

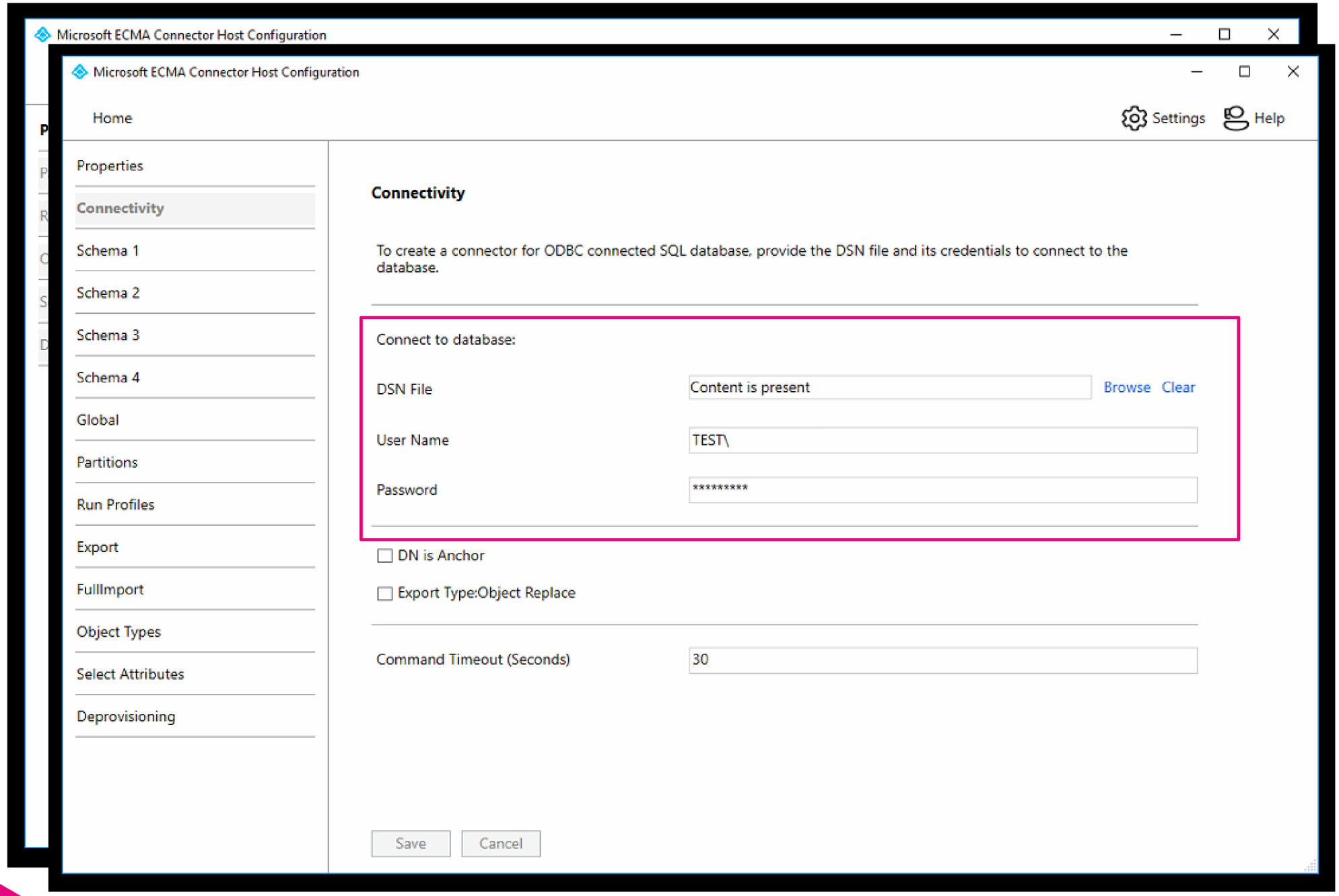
Home > Enterprise applications | All applications > OnPremises App (ECMA) - SQL | Provisioning > OnPremises App (ECMA) - SQL

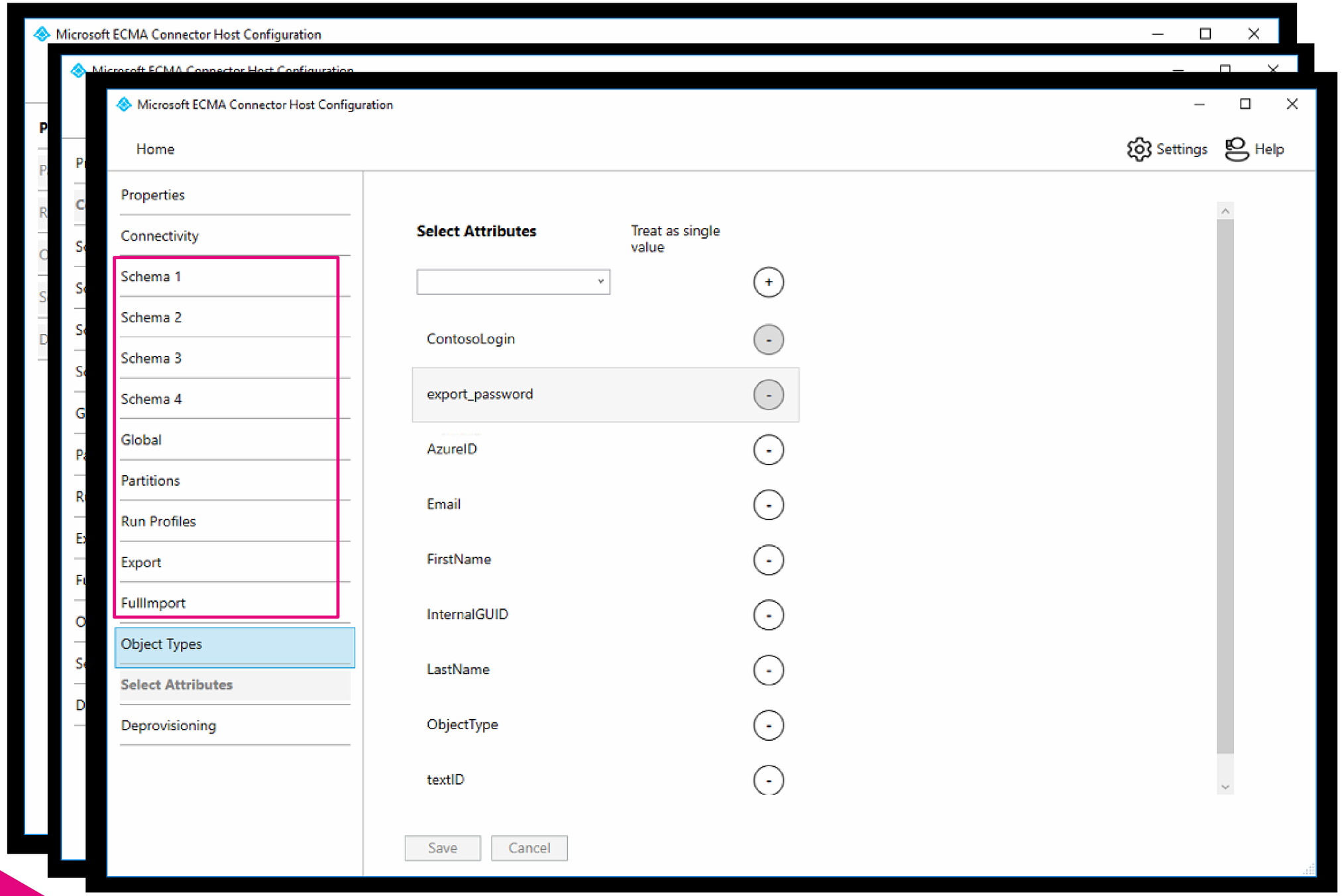
OnPremises App (ECMA) - SQL | Provisioning ...




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)
Previous
Next


Microsoft ECMA Connector Host Configuration
Home
Settings
Help
Properties
Partitions
Run Profiles
Object Types
Select Attributes
Deprovisioning
Properties
Import connector
Name *
SQL-App1
Creation time
vrijdag 26 januari 2024 19:35:55
Last modified
vrijdag 26 januari 2024 19:35:55
Autosync timer (minutes) *
120
Secret token *
Description
Select Extension DLL
This field is mandatory
Extension DLL *
Microsoft.IAM.Connector.GenericLdap.dll
Microsoft.IAM.Connector.GenericSql.dll
Microsoft.IAM.Connector.PowerShell.dll
Microsoft.IdentityManagement.MA.LotusDomino.dll
Microsoft.IdentityManagement.MA.WebServices.dll
Previous
Next
Cancel


Microsoft ECMA Connector Host Configuration
Microsoft ECMA Connector Host Configuration
Home
Settings
Help
Properties
Connectivity
Schema 1
Schema 2
Schema 3
Schema 4
Global
Partitions
Run Profiles
Export
FullImport
Object Types
Select Attributes
Deprovisioning
Connectivity
To create a connector for ODBC connected SQL database, provide the DSN file and its credentials to connect to the database.
Connect to database:
DSN File
Content is present
Browse
Clear
User Name
TEST\
Password
****
DN is Anchor
Export Type:Object Replace
Command Timeout (Seconds)
30
Save
Cancel


Microsoft ECMA Connector Host Configuration
Microsoft ECMA Connector Host Configuration
Home
Settings
Help
Properties
Connectivity
Schema 1
Schema 2
Schema 3
Schema 4
Global
Partitions
Run Profiles
Export
FullImport
Object Types
Select Attributes
Deprovisioning
Select Attributes
Treat as single value
ContosoLogin
export_password
AzureID
Email
FirstName
InternalGUID
LastName
ObjectType
textID
Save
Cancel

OnPremises App (ECMA) - SQL | Provisioning

- Overview
- Provision on demand

Manage

- Provisioning
- Users and groups
- Expression builder

Monitor

- Provisioning logs
- Audit logs
- Insights

Troubleshoot

- New support request

Save Discard

Provisioning Mode

Automatic

Use Microsoft Entra to manage the creation and synchronization of user accounts in OnPremises App (ECMA) - SQL based on user and group assignment.

On-Premises Connectivity

Admin Credentials

Admin Credentials

Microsoft Entra needs the following information to connect to OnPremises App (ECMA) - SQL's API and synchronize user data.

Tenant URL *

https://localhost:8585/ecma2host_SQL/scim

Secret Token

•

Test Connection

Mappings

Mappings

Mappings allow you to define how data should flow between Microsoft Entra ID and ScimOnPremises.

Name	Enabled
Provision Azure Active Directory Users	Yes

Restore default mappings

Settings

Provisioning Status

On Off

OnPremises App (ECMA) - SQL | Provisioning

Overview
Provision on demand

Manage
Provisioning
Users and groups
Expression builder

Monitor
Provisioning logs
Audit logs
Insights

Troubleshoot
New support request

Save Discard

Provisioning Mode

Automatic

Use Microsoft Entra to manage the creation and synchronization of user accounts in OnPremises App (ECMA) - SQL based on user and group assignment.

On-Premises Connectivity

Admin Credentials

Admin Credentials

Microsoft Entra needs the following information to connect to OnPremises App (ECMA) - SQL's API and synchronize user data.

Tenant URL *

https://localhost:8585/ecma2host_SQL/scim

Secret Token

•

Test Connection

Mappings

Mappings

Mappings allow you to define how data should flow between Microsoft Entra ID and ScimOnPremises.

Name	Enabled
Provision Azure Active Directory Users	Yes

Restore default mappings

Settings

Provisioning Status

On Off

Edit Attribute ...

A mapping lets you define how the attributes in one class of Microsoft Entra object (e.g. Users) should flow to and from this application.

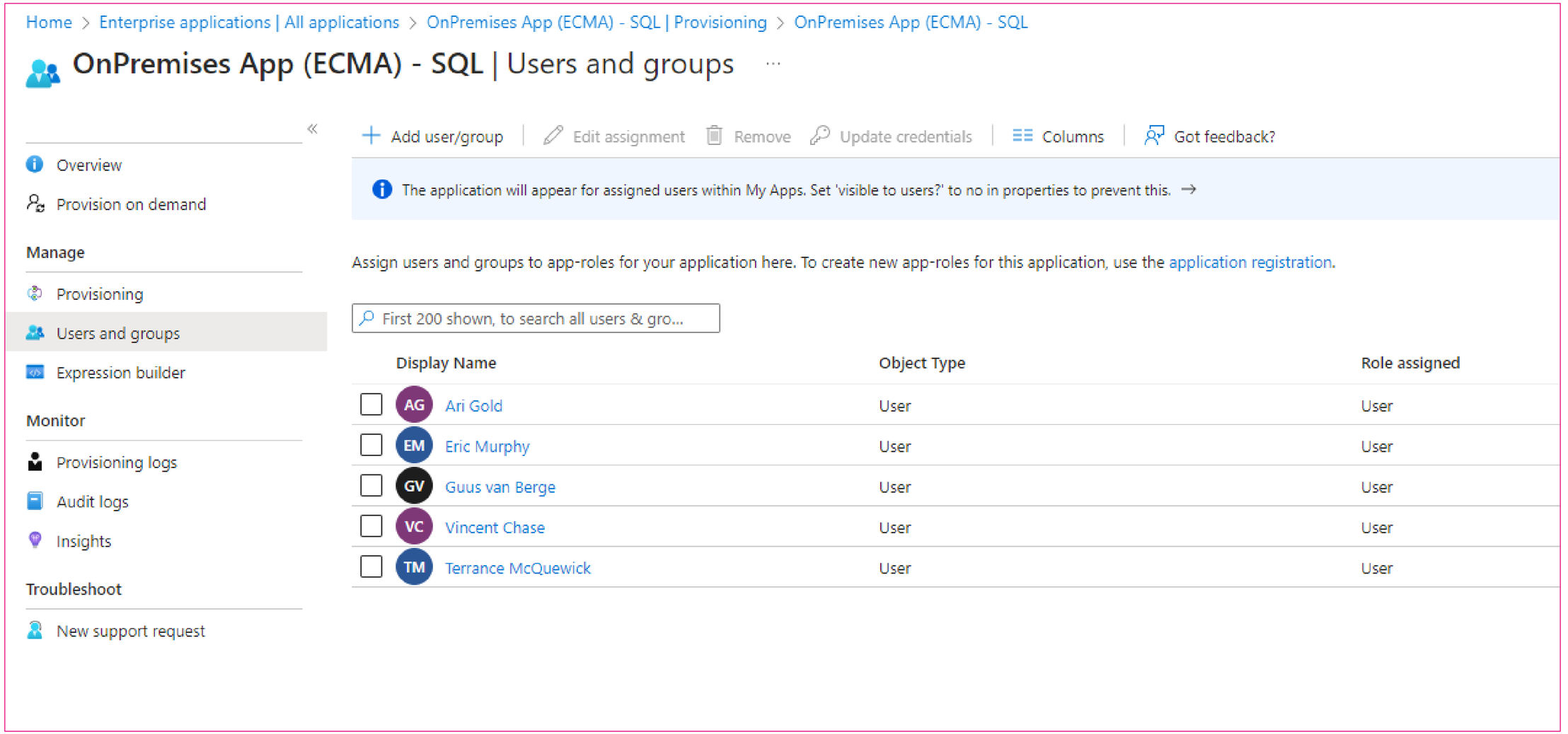
Mapping type
Direct

Source attribute *
userPrincipalName

Default value if null (optional)

Target attribute *
urn:ietf:params:scim:schemas:extension:ECMA2Host:2.0:User:ContosoLogin

- active
- id
- PLACEHOLDER
- urn:ietf:params:scim:schemas:extension:ECMA2Host:2.0:User:AzureID
- urn:ietf:params:scim:schemas:extension:ECMA2Host:2.0:User:ContosoLogin
- urn:ietf:params:scim:schemas:extension:ECMA2Host:2.0:User:Email
- urn:ietf:params:scim:schemas:extension:ECMA2Host:2.0:User:export_password
- urn:ietf:params:scim:schemas:extension:ECMA2Host:2.0:User:FirstName
- urn:ietf:params:scim:schemas:extension:ECMA2Host:2.0:User:InternalGUID
- urn:ietf:params:scim:schemas:extension:ECMA2Host:2.0:User:LastName
- urn:ietf:params:scim:schemas:extension:ECMA2Host:2.0:User:ObjectType
- urn:ietf:params:scim:schemas:extension:ECMA2Host:2.0:User:textID


Home > Enterprise applications | All applications > OnPremises App (ECMA) - SQL | Provisioning > OnPremises App (ECMA) - SQL
OnPremises App (ECMA) - SQL | Users and groups
Overview
Provision on demand
Manage
Provisioning
Users and groups
Expression builder
Monitor
Provisioning logs
Audit logs
Insights
Troubleshoot
New support request
Add user/group
Edit assignment
Remove
Update credentials
Columns
Got feedback?
The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this.
Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the application registration.
First 200 shown, to search all users & gro...
Display Name
Object Type
Role assigned
AG Ari Gold User User
EM Eric Murphy User User
GV Guus van Berge User User
VC Vincent Chase User User
TM Terrance McQuewick User User

OnPremises App (ECMA) - SQL | Provision on demand

- Overview
- Provision on demand

Manage
- Provisioning
- Users and groups
- Expression builder

Monitor
- Provisioning logs
- Audit logs
- Insights

Troubleshoot
- New support request

Learn More | Got feedback?

Provision on-demand for a subset of users or groups before rolling it out broadly to your organization. When provisioning a group you can select 5 members at a time.

No user or group will be provisioned on-demand that would not have been provisioned through the regular provisioning cycles.

Selected user: Terrance McQuewick

OnPremises App (ECMA) - SQL | Provision on demand

Overview
Provision on demand

Manage
Provisioning
Users and groups
Expression builder

Monitor
Provisioning logs
Audit logs
Insights

Troubleshoot
New support request

Learn More | Technical details | Got feedback?

User

TM Terrance McQuewick

1. Import user

This step shows the user retrieved from the source system and the properties of the user in the source system.

Success | View details

2. Determine if user is in scope

This step shows the scoping conditions that were evaluated and which ones the user passed or failed.

Success | View details

3. Match user between source and target system

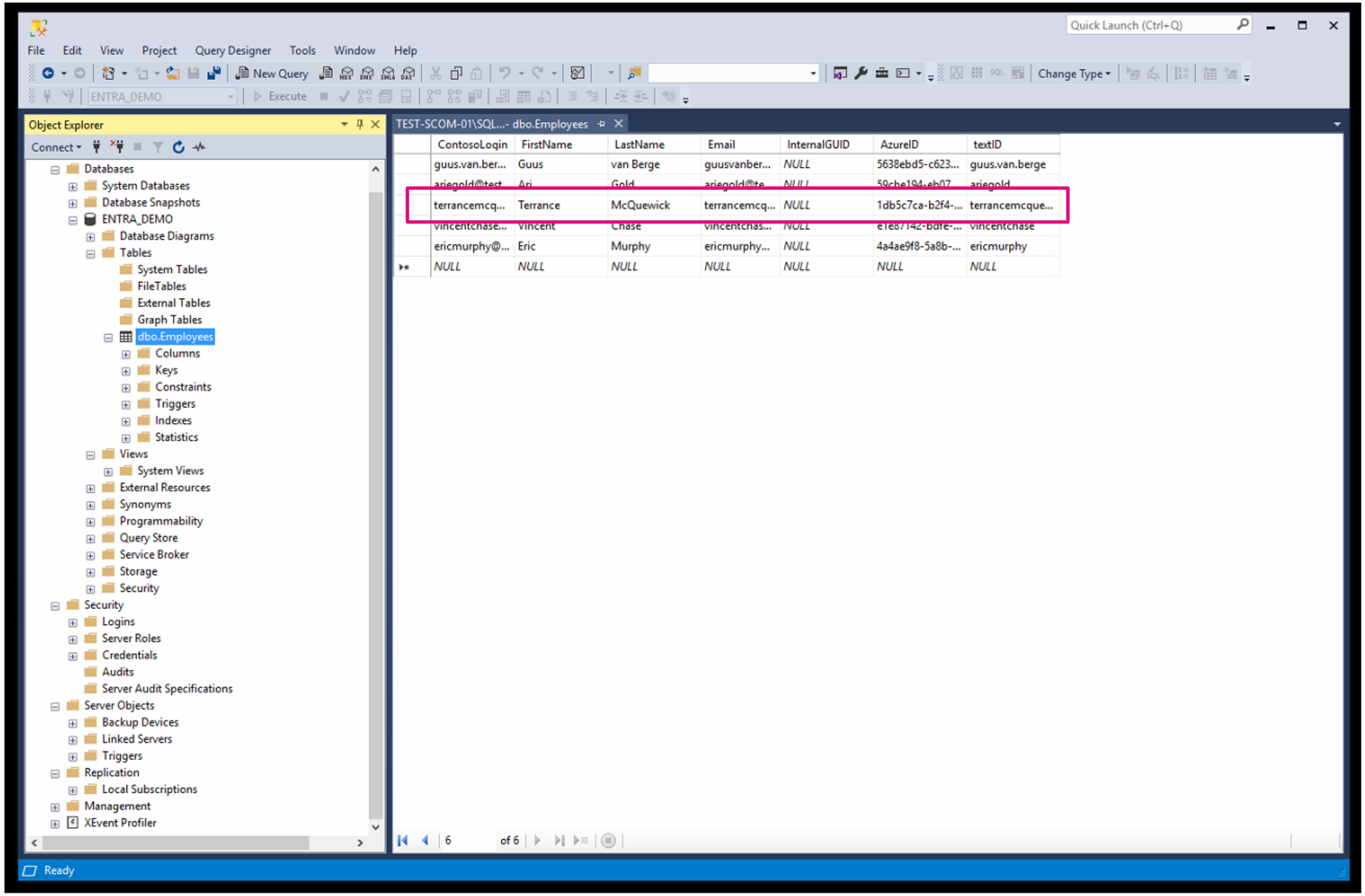
This step shows whether the user was found in the target system as well as the properties of the user in the target system.

Success | View details

4. Perform action

This step shows the action that was performed in the target application, such as creating a user or updating a user.

Success | View details


File Edit View Project Query Designer Tools Window Help
New Query
Change Type
ENTRA_DEMO
Execute
Quick Launch (Ctrl+Q)
Object Explorer
Connect
Databases
System Databases
Database Snapshots
ENTRA_DEMO
Database Diagrams
Tables
System Tables
FileTables
External Tables
Graph Tables
dbo.Employees
Columns
Keys
Constraints
Triggers
Indexes
Statistics
Views
System Views
External Resources
Synonyms
Programmability
Query Store
Service Broker
Storage
Security
Security
Logins
Server Roles
Credentials
Audits
Server Audit Specifications
Server Objects
Backup Devices
Linked Servers
Triggers
Replication
Local Subscriptions
Management
XEvent Profiler
TEST-SCOM-01\SQL...- dbo.Employees
ContosoLogin FirstName LastName Email InternalGUID AzureID textID
guus.van.ber... Guus van Berge guusvanber... NULL 5638ebd5-c623... guus.van.berge
terrancemcq... Terrance McQuewick terrancemcq... NULL 1db5c7ca-b2f4-... terrancemcque...
ericmurphy@... Eric Murphy ericmurphy... NULL 4a4ae9f8-5a8b-... ericmurphy
NULL NULL NULL NULL NULL NULL NULL
6 of 6
Ready

Govern your Apps

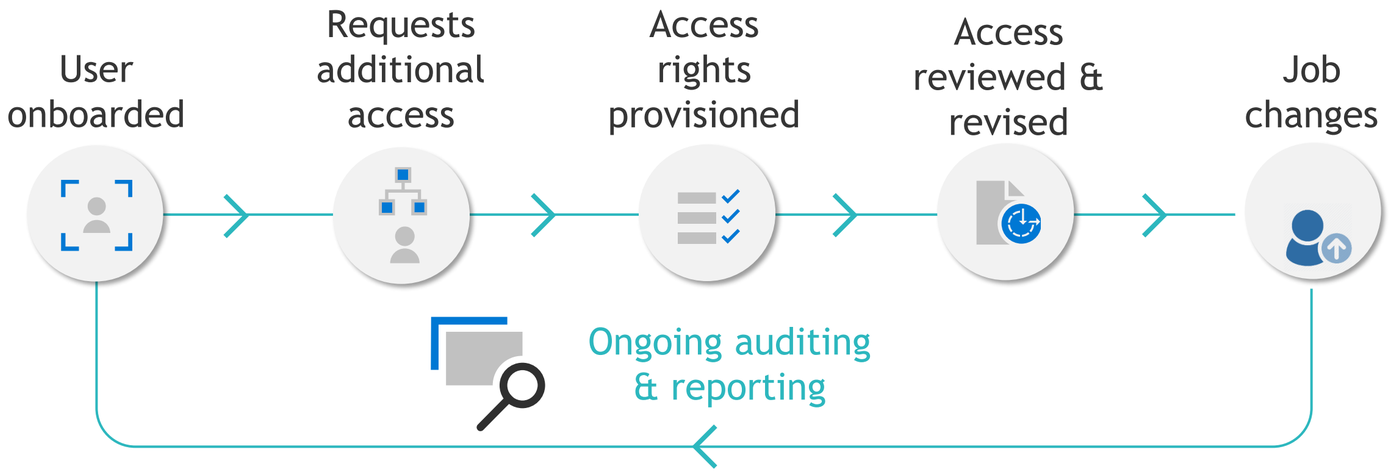
Access Packages

Let users **request access** and **automate** access assignments, approval, workflows, reviews for **all human identity types**.

Multi-stage approval workflow, separation of duties and **access recertification.**

Self-service policy and workflow can be defined by app, **group or site owners.**

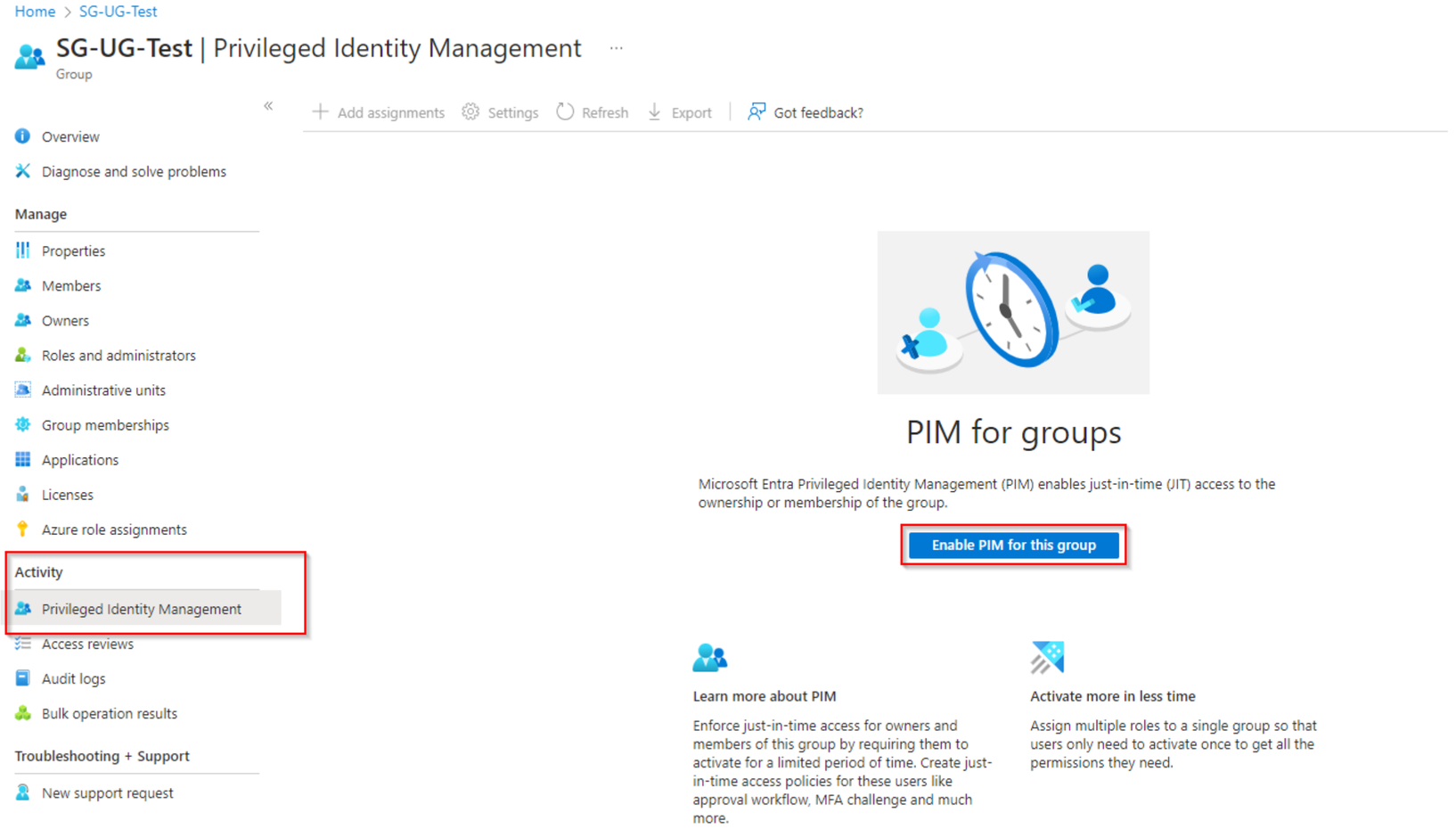
Supports custom workflows for access lifecycle (**through Logic Apps integration**)

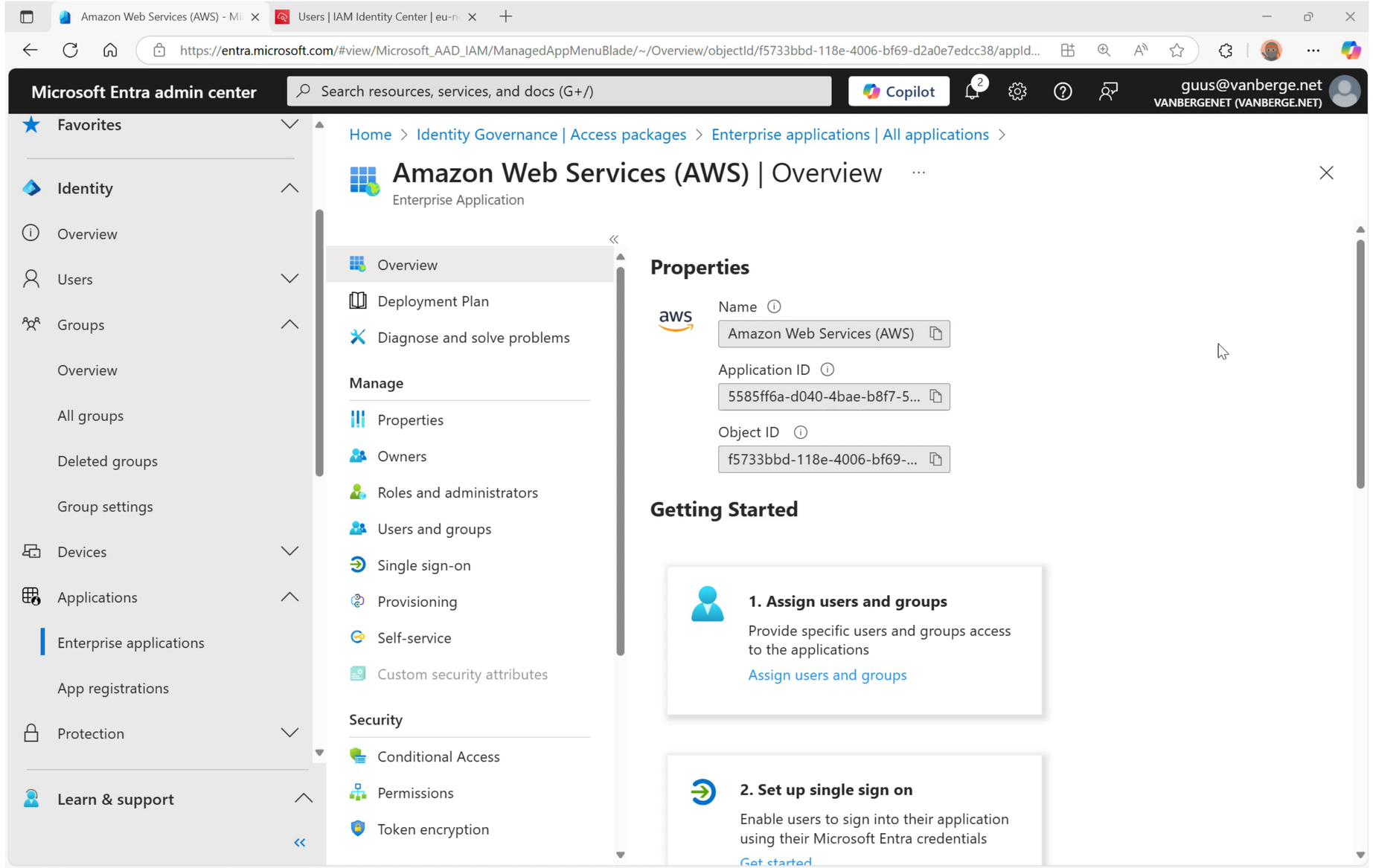


Protect your Apps

PIM for Groups

- Just-in-time membership and ownership of groups through Privileged Identity Management
- Control access to connected applications and permissions or roles inside the apps.
- Require approval for activation, enforce MFA, require justification, limit the activation time and more.
- Apply on on-premises resources with Group Writeback.




Amazon Web Services (AWS) - Mi
Users | IAM Identity Center | eu-n
https://entra.microsoft.com/#view/Microsoft_AAD_IAM/ManagedAppMenuBlade/~/Overview/objectId/f5733bbd-118e-4006-bf69-d2a0e7edcc38/appId...
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
guus@vanberge.net
VANBERGENET (VANBERGE.NET)
Favorites
Identity
Overview
Users
Groups
Overview
All groups
Deleted groups
Group settings
Devices
Applications
Enterprise applications
App registrations
Protection
Learn & support
Home > Identity Governance | Access packages > Enterprise applications | All applications >
Amazon Web Services (AWS) | Overview
Enterprise Application
Overview
Deployment Plan
Diagnose and solve problems
Manage
Properties
Owners
Roles and administrators
Users and groups
Single sign-on
Provisioning
Self-service
Custom security attributes
Security
Conditional Access
Permissions
Token encryption
Properties
Name
Amazon Web Services (AWS)
Application ID
5585ff6a-d040-4bae-b8f7-5...
Object ID
f5733bbd-118e-4006-bf69-...
Getting Started
1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups
2. Set up single sign on
Enable users to sign into their application using their Microsoft Entra credentials
Get started

How to move forward from here..

Source of truth & JML

Low-hanging Apps

Entitlement & reviews

Keep doing what you're doing

How to move forward from here..

Source of truth & JML

Low-hanging Apps

Entitlement & reviews

Keep doing what you're doing

How to move forward from here..

Source of truth & JML

Low-hanging Apps

Entitlement & reviews

Keep doing what you're doing

How to move forward from here..

Source of truth & JML

Low-hanging Apps

Entitlement & reviews

Keep doing what you're doing

Thanks for comming to my session!

Time for Q&A

Find me after for feedback and more info