

Surprising ways to escalate privileges in Entra ID

Marius Solbakken Mellum
Co-founder and Principal Cloud Engineer @ Fortytwo

Fortytwo
BY AMESTO

Marius Solbakken Mellum

- Co-founder and Principal Cloud Engineer @ Fortytwo
- Microsoft MVP Security
- Working with Microsoft identity for 15 years
- <https://goodworkaround.com>



What we will talk about



Misconfigurations and patterns leading to unintentional possibilities for privilege escalation



What to avoid and what to do as a developer

What we will NOT talk about



Phishing



Brute force attacks

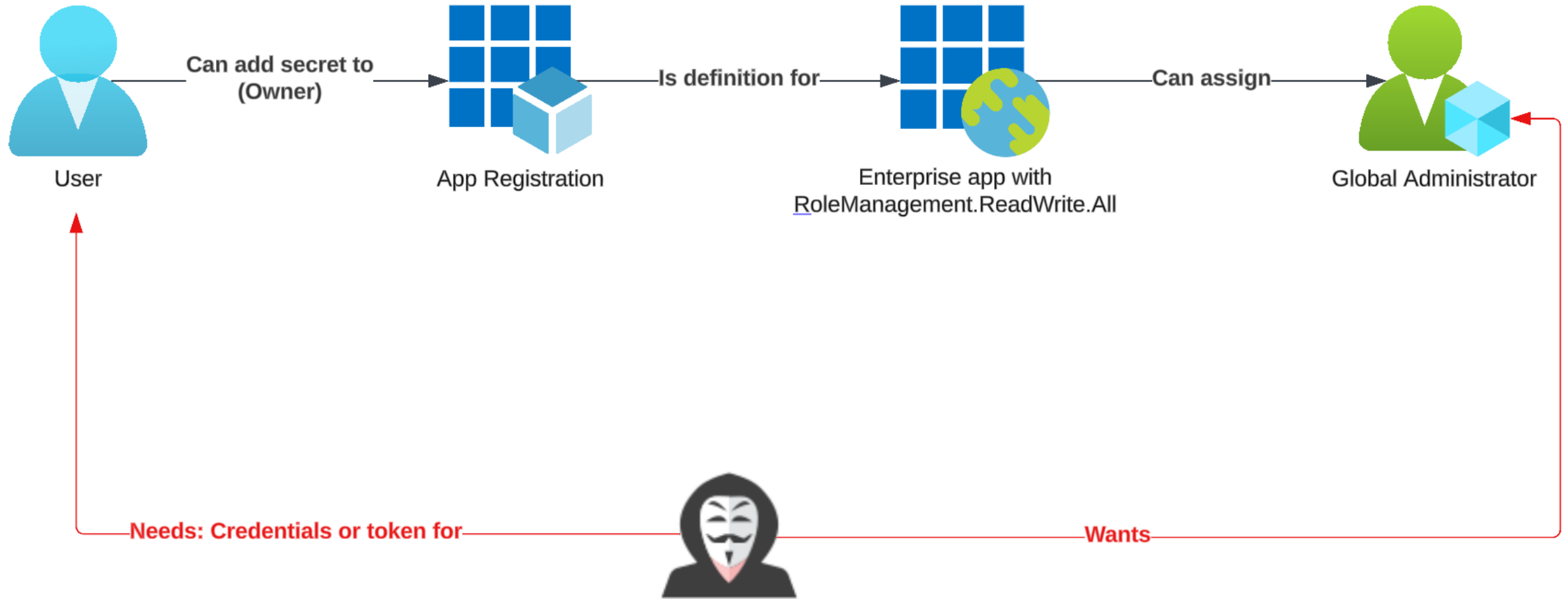


Abusing SSO features (PRT, Seamless SSO, etc.)

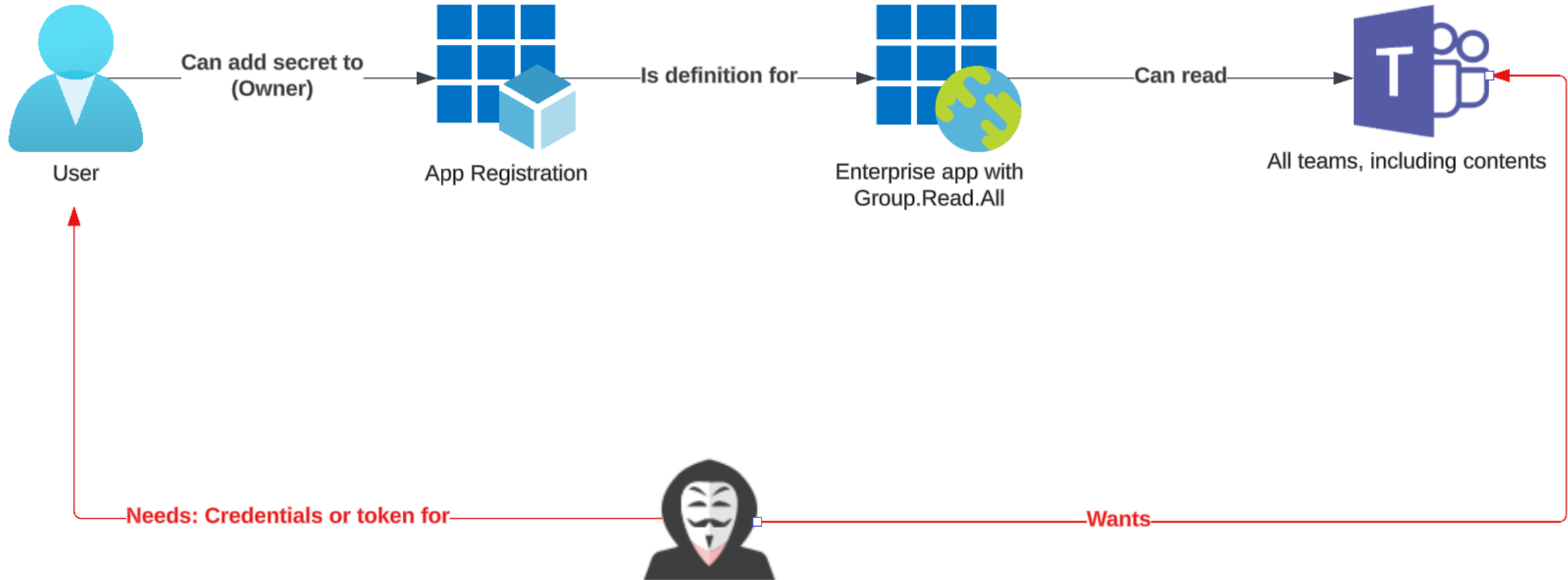


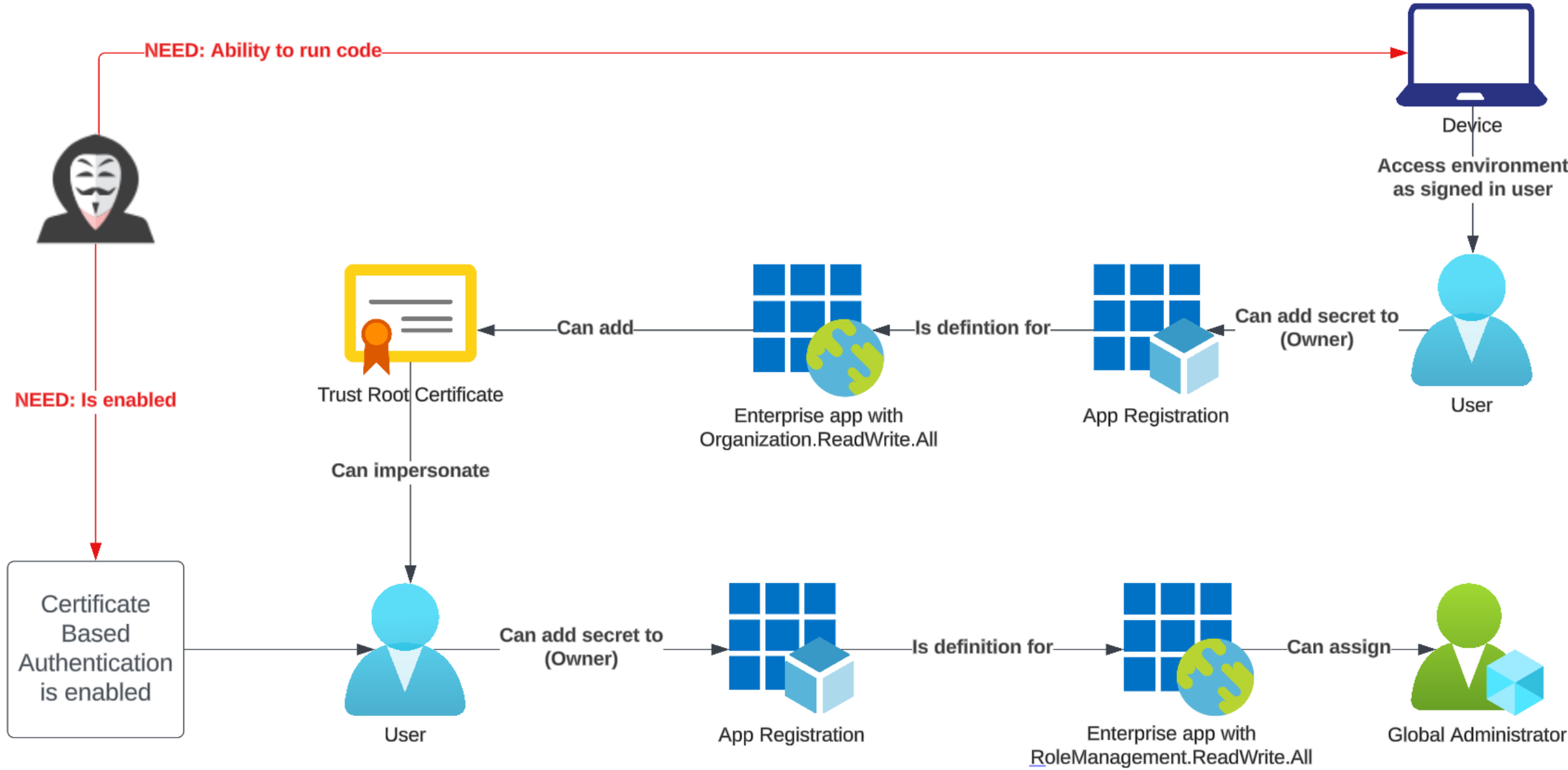
Social engineering

What is an attack path?



Not necessarily Global Admin





Entra ID Roles

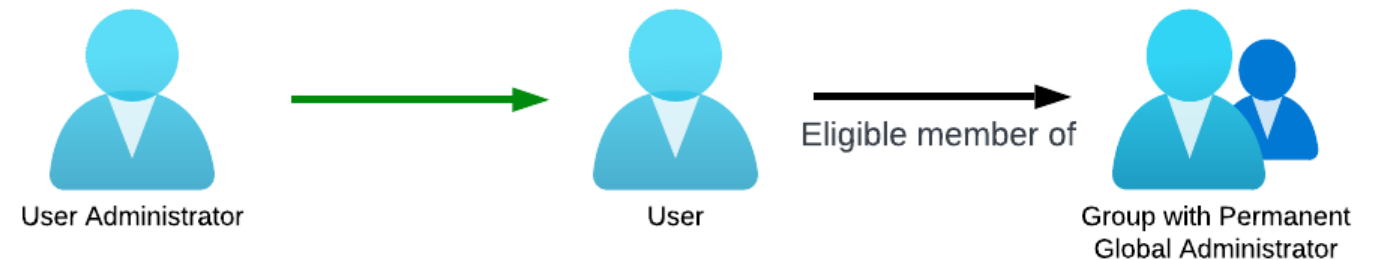
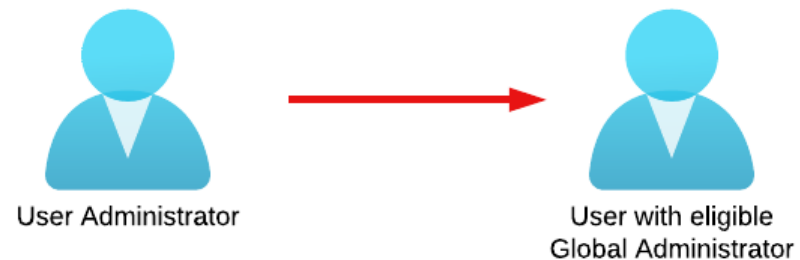
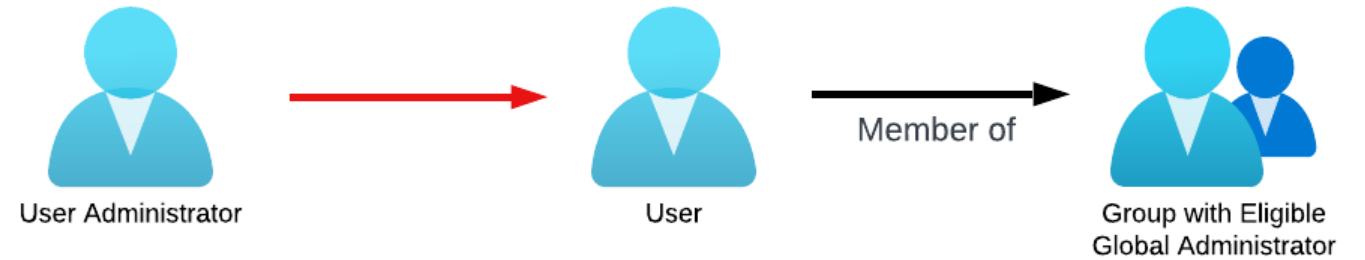
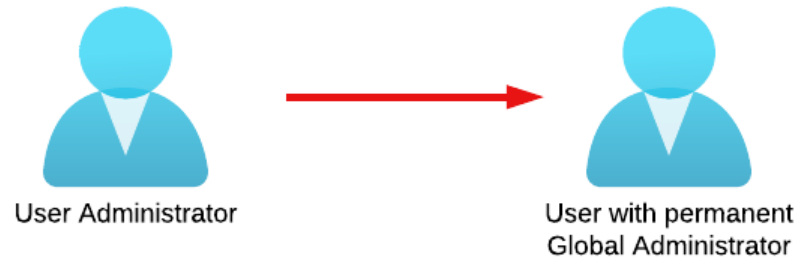
- 105 different roles
 - **Global Administrator** - a.k.a. God
 - **Privileged Role Administrator** - can assign global admin
 - **Privileged Authentication Administrator** - can reset credentials for global admins
 - **User Administrator** - Can CRUD users, except high privileged roles + reset passwords + manage groups
 - **Authentication Administrator** – Can reset MFA, create TAP
 - **Group Administrator** - Can manage all aspects of groups
 - **(Cloud) Application Administrator** - Can modify all app registrations and enterprise apps
- Privileged Identity Management – Active vs Eligible



DEMO TIME

- PROTECTED ROLES -

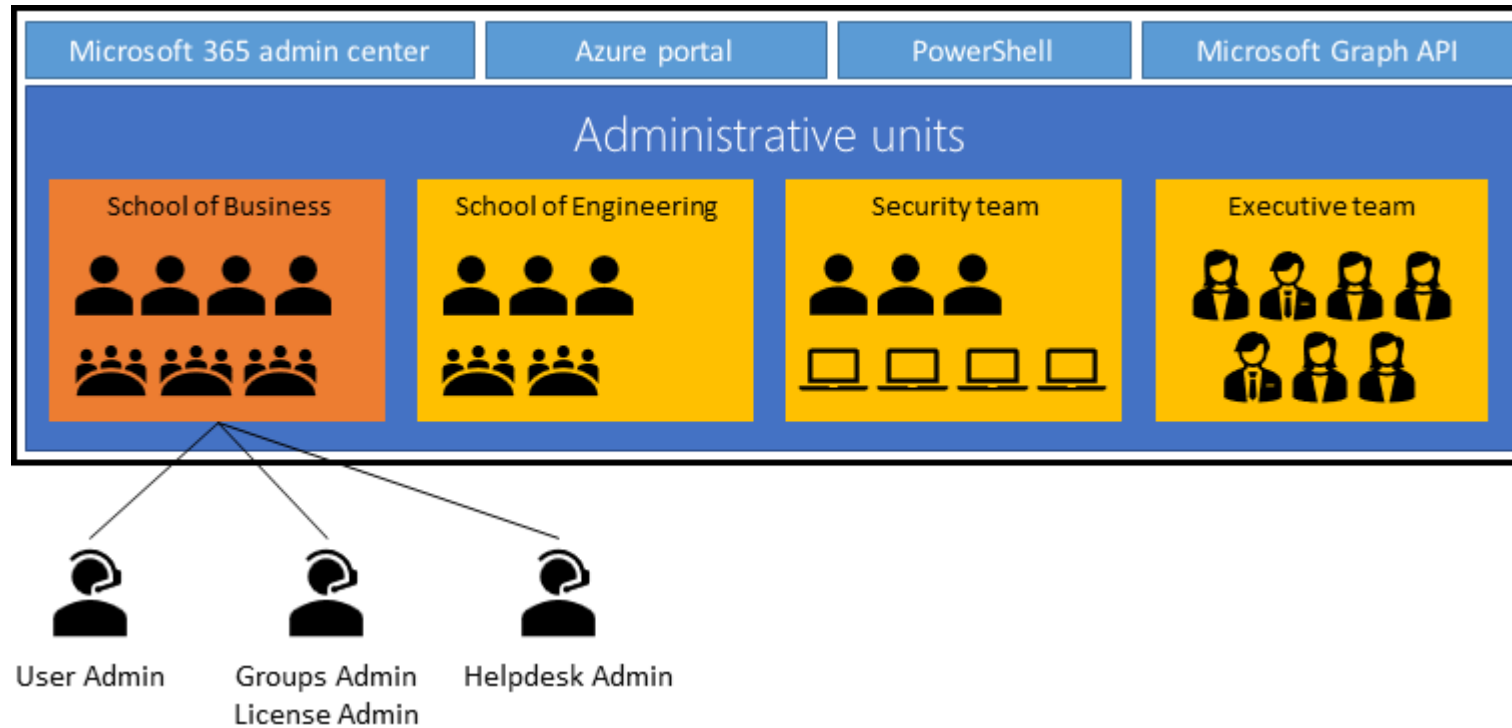
In summary – Password resets



DO NOT USE GROUPS TO PIM ONCE FOR ACTIVATING MULTIPLE ROLES AT THE SAME TIME

Scoped role assignments

- Administrative units
 - Restricted Management





DEMO TIME

- ADMINISTRATIVE UNITS -

How about applications?

- App registrations and enterprise apps

- Credentials

- Secrets
 - Certificates
 - Federated

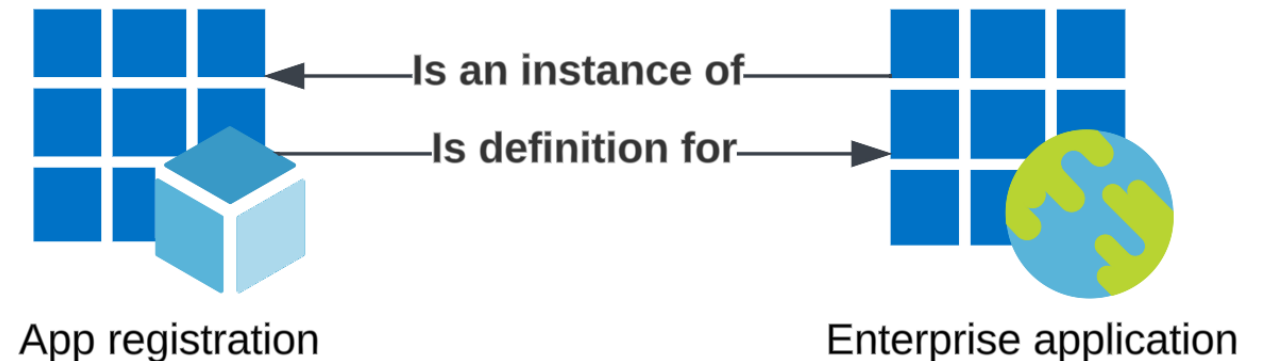
- Managed service identities

- Application owner

- App scoped directory roles

- Currently no protection mechanism

- Recommendation: Do not use owners to apps with application permissions

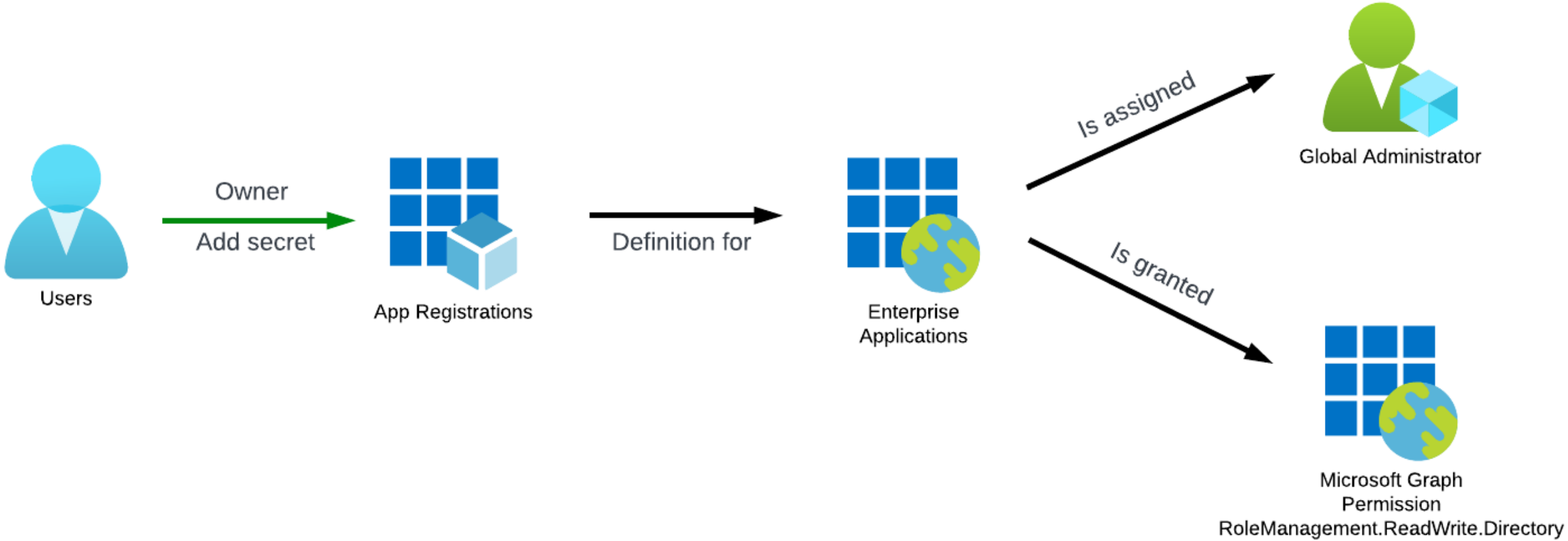




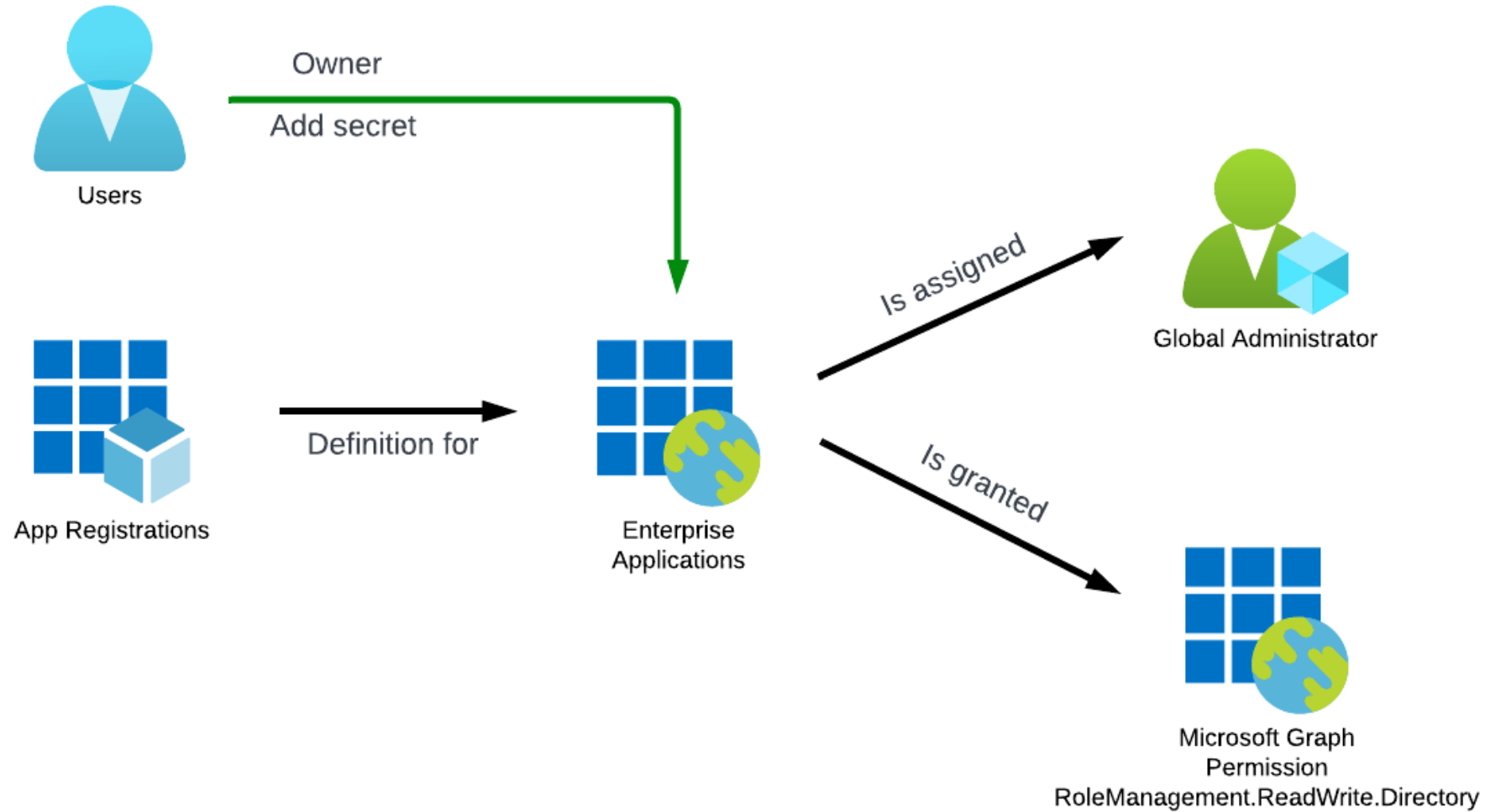
DEMO TIME

- NO PROTECTION FOR APPS -

In summary – No protection for apps



One more thing

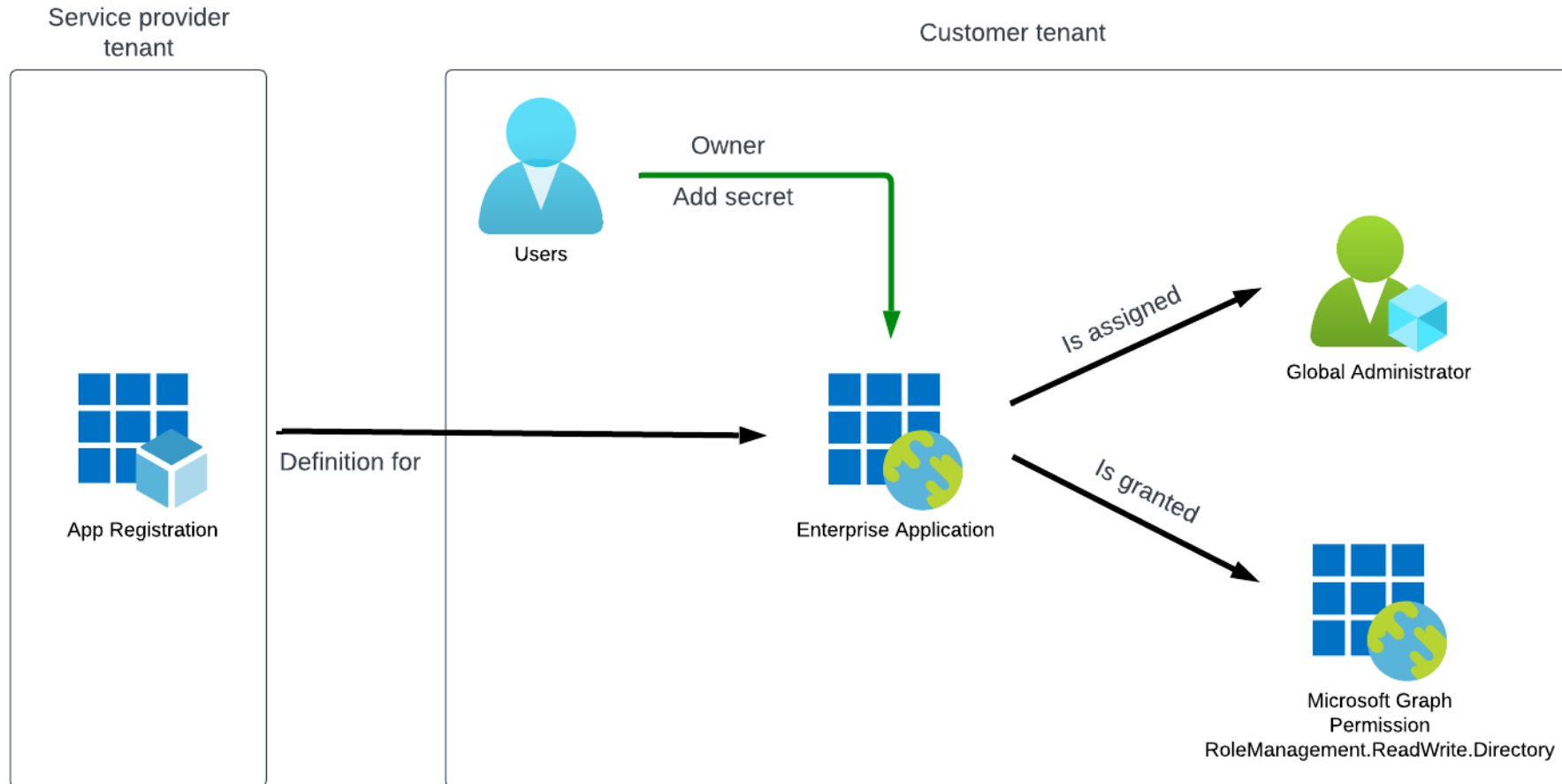




DEMO TIME

- SECRET ON ENTERPRISE APPS -

Also works for Multi-tenant applications!



High privileged app 1 | Authentication

Got feedback?

+ Add a platform

- Overview
- Quickstart
- Integration assistant

Manage

- Branding & properties
- Authentication**
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (Contoso only - Single tenant)
- Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

[Help me decide...](#)

⚠ Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft accounts for an existing registration. If you need to enable personal accounts, you can do so using the manifest editor. [Learn more about these restrictions.](#)

Advanced settings

Allow public client flows ⓘ

Enable the following mobile and desktop flows:

Yes **No**

- App collects plaintext password (Resource Owner Password Credential Flow) [Learn more](#)
- No keyboard (Device Code Flow) [Learn more](#)
- SSO for domain-joined Windows (Windows Integrated Auth Flow) [Learn more](#)

App instance property lock ⓘ

Configure the application instance modification lock. [Learn more](#)

Configure

Save Discard

App instance property lock

High privileged app 1

Prevent malicious attacks by blocking the modification of sensitive properties on instances of this application.

Enable property lock

Locked properties

4 selected

- All properties
- Credentials used for verification
- Credentials used for signing tokens
- Token Encryption KeyId

Save Discard

Microsoft Graph scopes

- <Object>.<Action>.<Scope>
- RoleManagement.ReadWrite.Directory
 - Able to assign all Entra ID roles, such as Global Administrator
- Application.ReadWrite.All
 - Able to add credentials to any app
- User.ReadWrite.All
 - Can CRUD all users except protected ones
 - Can update users to match dynamic group criteria, thus adding them to a group
 - Cannot update user passwords

Organization.ReadWrite.All

Category	Application	Delegated
Identifier	292d869f-3427-49a8-9dab-8c70152b74e9	46ca0847-7e6b-426e-9775-ea810a948356
DisplayText	Read and write organization information	Read and write organization information
Description	Allows the app to read and write the organization and related resources, without a signed-in user. Related resources include things like subscribed skus and tenant branding information.	Allows the app to read and write the organization and related resources, on behalf of the signed-in user. Related resources include things like subscribed skus and tenant branding information.
AdminConsentRequired	Yes	Yes

enabled, you can impersonate any user, including **Global Administrators**

AppRoleAssignment.ReadWrite.All



“Ah, a useful scope that let’s my service principal assign app roles”



It also gives you access to grant **any application, any Microsoft Graph permission**, effectively being able to grant itself **Global Admin** through **RoleManagement.ReadWrite.Directory**

Group.ReadWrite.All



“A useful permission for automating creation of Entra ID groups”



It also gives **you access to contents of all Teams and Microsoft 365 groups**

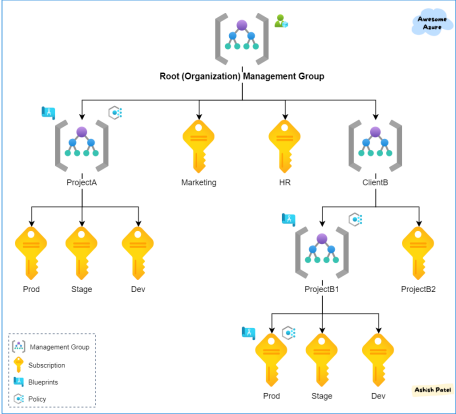
So what are we supposed to do?

- Utilize the least privileged scopes
 - Group.Create
 - GroupMember.ReadWrite.All – Or simply owner
 - Application.ReadWrite.OwnedBy
- Monitor application credentials
- As an Entra ID admin, question whether permissions are needed
- Regularly review granted permissions

Managed service identities

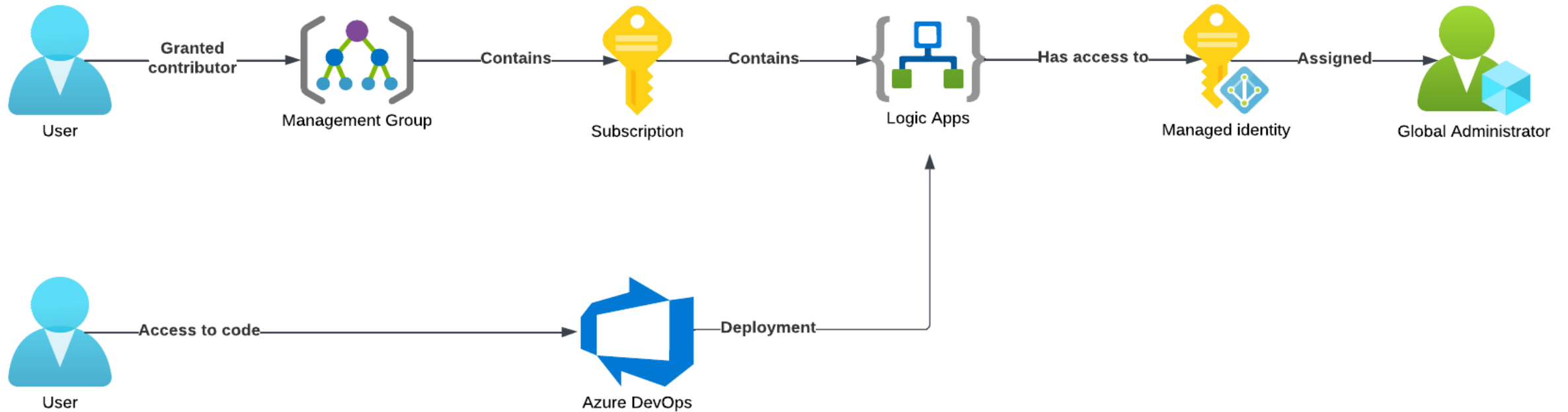


Service principal linked to an Azure resource, with no credentials to handle



Azure RBAC is critical to security

New attack paths!





DEMO TIME

AZURE CONTRIBUTOR
TO
ENTRA ID PERMISSIONS

Key takeaways

- Do not combine PIM for groups with role assignable groups
- Enable property lock on your app registrations
- Monitor app credentials
- Audit Microsoft Graph application consents
- Application owner can add credentials
- Least privilege
 - Scoped directory roles
 - 105 Entra ID roles
 - 400+ Azure RBAC roles
 - Something.ReadWrite.All may give you more than you thing
- Use Managed Service Identity, but watch out for RBAC based attack paths

Questions?

marius.solbakken@fortytwo.io

fortytwo.io / goodworkaround.com

Fortytwo
BY AMESTO

Thank you

marius.solbakken@fortytwo.io

fortytwo.io / goodworkaround.com

Fortytwo
BY AMESTO