

External Identities - Self-Service Sign Up, Governance and all that Jazz!

- Jan Vidar Elven
- Architect @ Skill AD
- Twitter @JanVidarElven
- MVP Enterprise Mobility

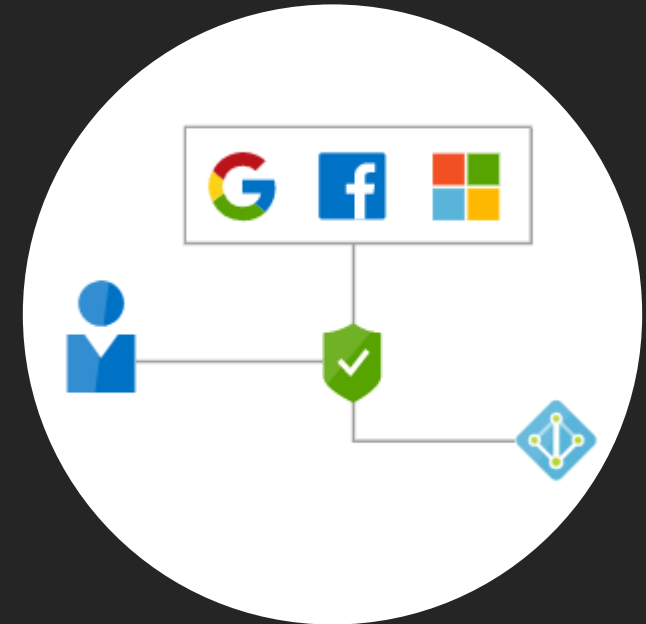


NORDIC

— VIRTUAL SUMMIT —

External Identities

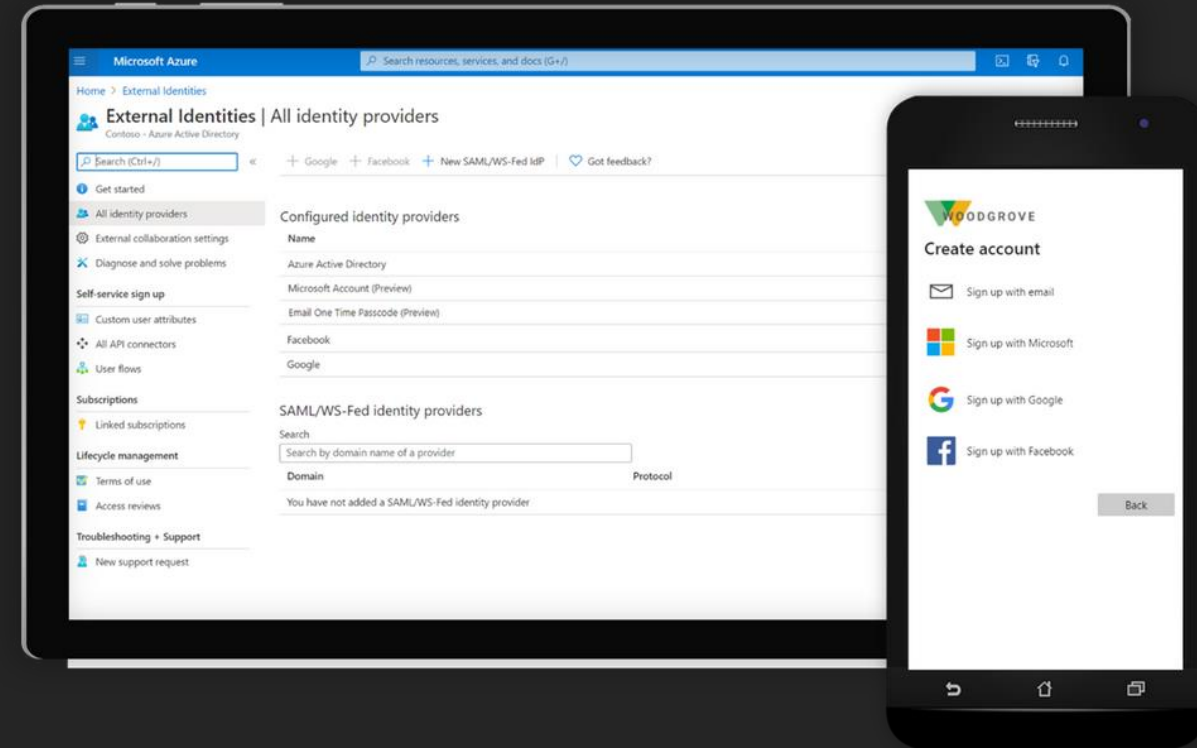
– Beyond the Invitation Process



So, what's new?

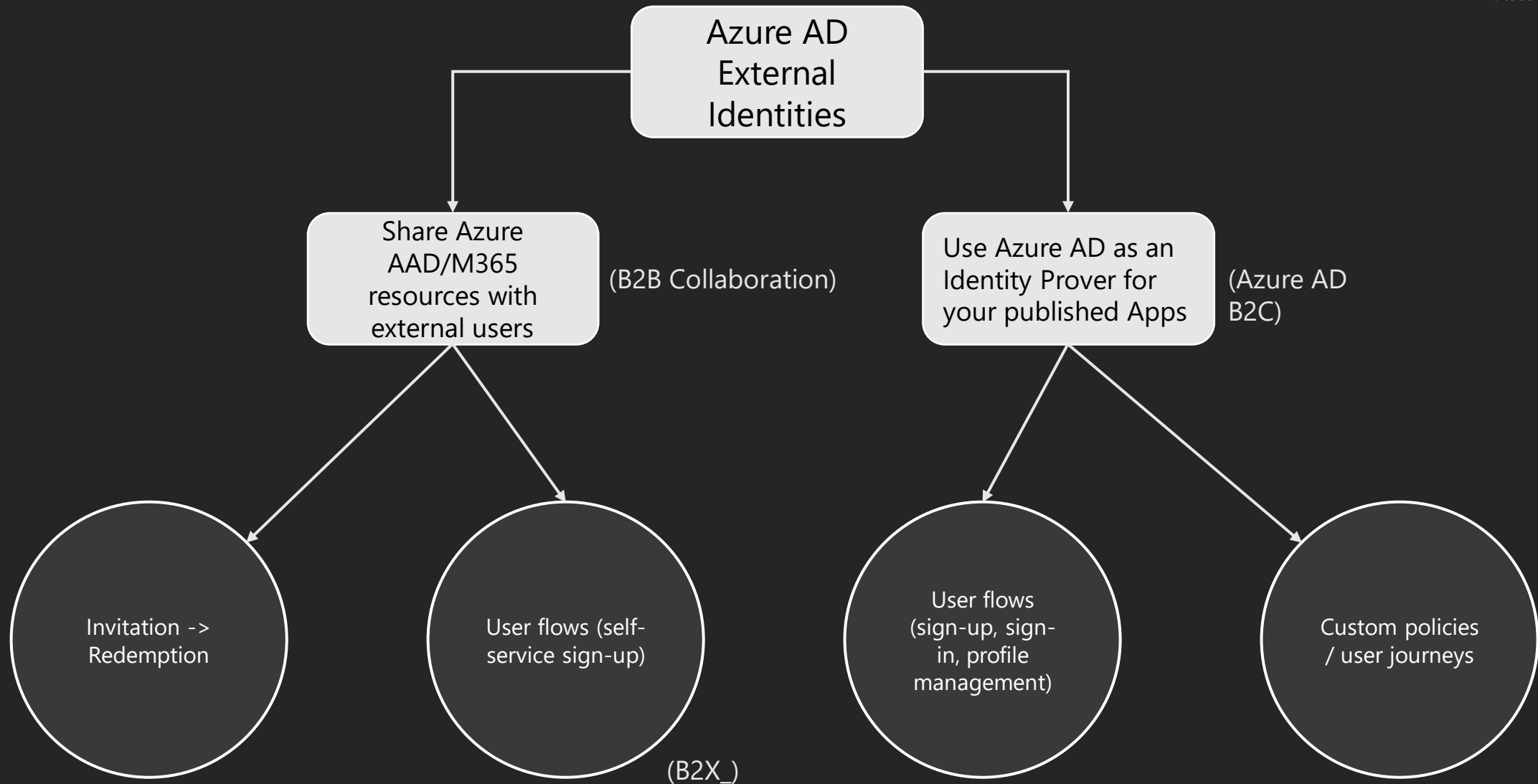
Breaking
news!

- March 2021: Azure Active Directory External Identities GA
 - Self-Service Sign-Up User Flows
 - Next generation User Flows with B2C
- Identity Protection with risk-based Conditional Access to Azure AD B2C
- Scalable lifecycle & user management
- External Identities SLA -> 99.99%



<https://techcommunity.microsoft.com/t5/azure-active-directory-identity/azure-active-directory-external-identities-is-generally/ba-p/2147080>

Scenarios for External Identities



Sign your self up as a Guest user

User flows (self-service sign-up)

- Only for Azure AD Apps (not M365)
 - But available for M365 after!
- Attributes
 - Standard & Custom
- API Connector
 - After sign-in
 - Before user is created
- User Flow
 - Identity Provider
 - Attributes, Language & Layout
 - API Connectors
 - Applications

Configure External collaboration settings

External collaboration settings

Diagnose and solve problems

Self-service sign up

Custom user attributes

All API connectors

User flows

Subscriptions

Linked subscriptions

Lifecycle management

Terms of use

Access reviews

Troubleshooting + Support

New support request

Guest user access

Guest user access restrictions (Preview) ⓘ

[Learn more](#)

☐ Guest users have the same access as members (most inclusive)

☒ Guest users have limited access to properties and memberships of directory objects

☐ Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

Guest invite settings

Guest invite restrictions ⓘ

[Learn more](#)

☐ Anyone in the organization can invite guest users including guests and non-admins (most inclusive)

☒ Member users and users assigned to specific admin roles can invite guest users including guests with member permissions

☐ Only users assigned to specific admin roles can invite guest users

☐ No one in the organization can invite guest users including admins (most restrictive)

Enable guest self-service sign up via user flows ⓘ

[Learn more](#)

☒ Yes

☐ No

Collaboration restrictions

☒ Allow invitations to be sent to any domain (most inclusive)

☐ Deny invitations to the specified domains

☐ Allow invitations only to the specified domains (most restrictive)

If only self-service sign-up?


Configure Microsoft 365 Groups External Sharing

Microsoft 365 Groups


Choose how guests from outside your organization can collaborate with your users in Microsoft 365 Groups. [Learn more about guest access to Microsoft 365 Groups](#)


- ☒ Let group owners add people outside your organization to Microsoft 365 Groups as guests
- ☒ Let guest group members access group content
If you don't select this, guests will still be listed as members of the group, but they won't receive group emails or be able to access any group content. They'll only be able to access files that were directly shared with them.


Configure Identity Providers: Who can sign up?


 **External Identities** | All identity providers ...
Elven Azure AD - Azure Active Directory

[«](#) [+ Google](#) [+ Facebook](#) [+ New SAML/WS-Fed IdP](#) | [Got feedback?](#)


 Get started


 All identity providers


 External collaboration settings

 Diagnose and solve problems


Self-service sign up

 Custom user attributes


 All API connectors


 User flows

Subscriptions

 Linked subscriptions

Lifecycle management

 Terms of use

 Access reviews

Configured identity providers

Name
Azure Active Directory
Microsoft Account (Preview)
Email one-time passcode (Preview)
GoogleElvenPrivate

SAML/WS-Fed identity providers

Search

Domain
You have not added a SAML/WS-Fed identity provider

Linking Azure Subscription: 1:5 -> MAU

[Link subscription](#) [Edit](#) | [Got feedback?](#)

By switching to pricing based on Monthly Active Users (MAU), you will no longer be limited to a 1:5 Azure AD to guest license ratio. Save with your first 50,000 MAU free and pay only for what you use. [Learn more](#)

Your tenant's subscription

Tenant	Directory type	Status	Subscription	Resource group
<input checked="" type="checkbox"/> Elven Azure AD	Azure AD	✓ Linked	Microsoft Azure Sponsorship	rg-external-identities

 microsoft.azureactive

Provider	Status
Microsoft.AzureActiveDirectory	✓ Registered
Custom user attributes	
Billing unit	Monthly active users (MAU)

Demo

User Flow for Self Service Sign Up with Approvals



Identity Governance

Managing the Lifecycle & Access of External Identities



External Identities Lifecycle Scenarios



Self-service onboarding with access packages & approvals



Access reviews of guests in Teams & Groups



Automatic disable and remove guest users



Terms of Use for legal or compliance requirements

Featured Previews in Governance




- Ignite Nov 2021:
 - Custom Entitlement Workflows based on Azure Logic Apps
- Preview Sep 2021:
 - Onboard partners more easily with new Azure AD entitlement management features: Custom questions & attributes
- Preview Jul 2021:
 - Ensure compliance using separation of duties checks in access requests



Configure Lifecycle of External Users

[Home](#) > [Identity Governance](#)

 **Identity Governance** | Settings ...

Getting started

Entitlement management

Access packages

Catalogs

Connected organizations

Reports

Settings

<< Save Cancel

Manage the lifecycle of external users

Select what happens when an external user, who was added to your directory through an access package request, loses their last assignment to any access package.

Block external user from signing in to this directory

Yes

No

Remove external user

Yes

No

Number of days before removing external user from this directory

30

Demo

External Identities Governance – Self Service Sign Up and
Workflow Customizations



Summary & Resources

Bringing it all together

Resources

- Repositories for Demo resources:
 - Self Service Sign-Up:
<https://github.com/JanVidarElven/SelfServiceSignUpApprovals>
 - Identity Governance External User Sign Up:
<https://github.com/JanVidarElven/ExternalIdentitiesGovernance>
- Docs:
 - [Add a custom approval workflow to self-service sign-up](#)
 - [Trigger custom Logic Apps with Azure AD entitlement management](#)
- Connect:
 - @JanVidarElven
 - gotoguy.blog

