



# Mastering Azure AD B2B Guests



**Jan Vidar Elven**

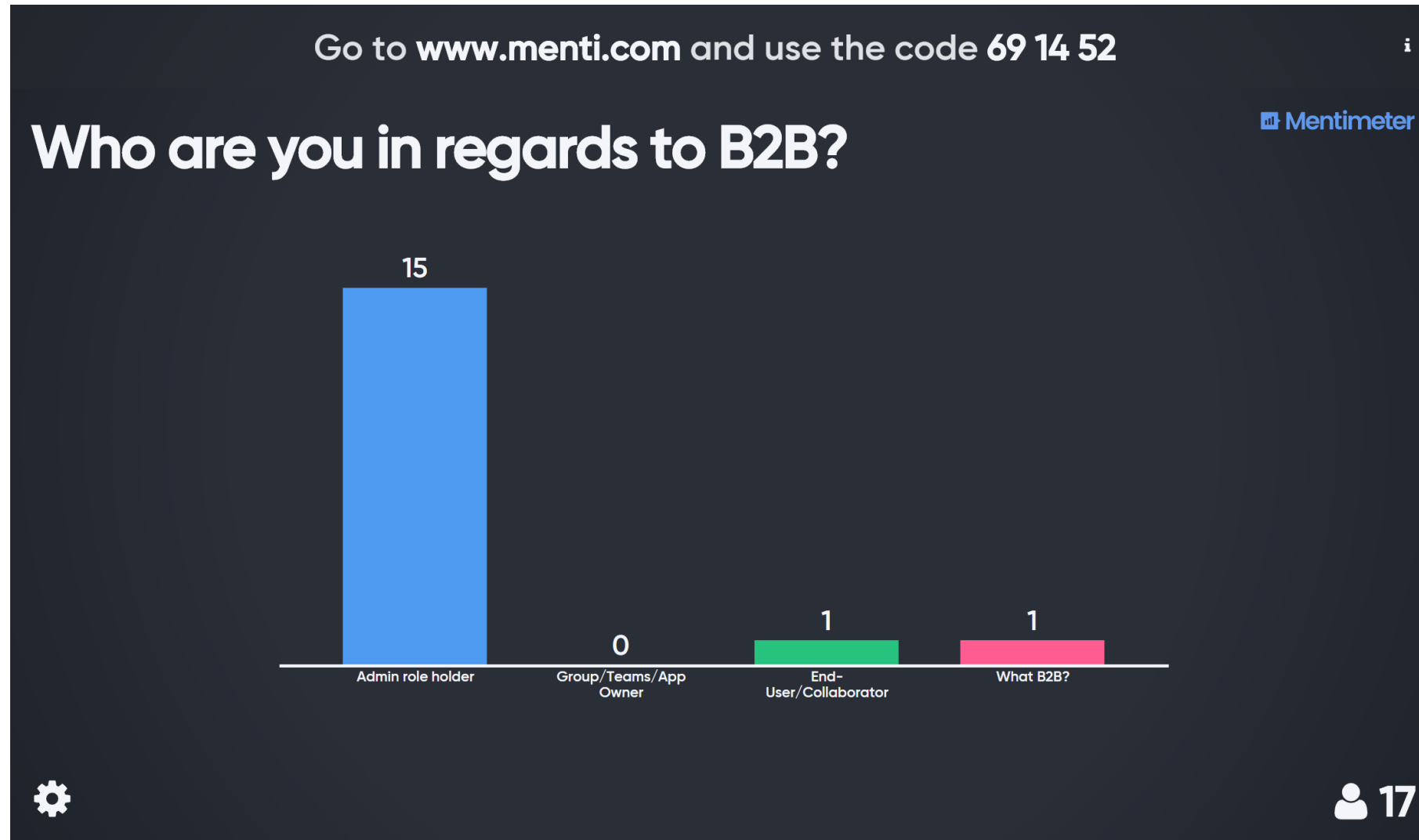
MVP Enterprise Mobility

   @JanVidarElven

Headline Sponsors:  CoreView  audiocodes Anywhere365  UltimateMigrator  
Manage Migrate Rehydrate



# Azure AD B2B Poll



# About Azure Active Directory and Guests

- Guest accounts will be created as User Objects in your Azure AD!
- Default UserType = Guest (as opposed to Member)
- Source: From Invited User to:
  - External Azure Active Directory
  - Microsoft Account
  - Windows Server Active Directory
  - Azure Active Directory
  - Google\*

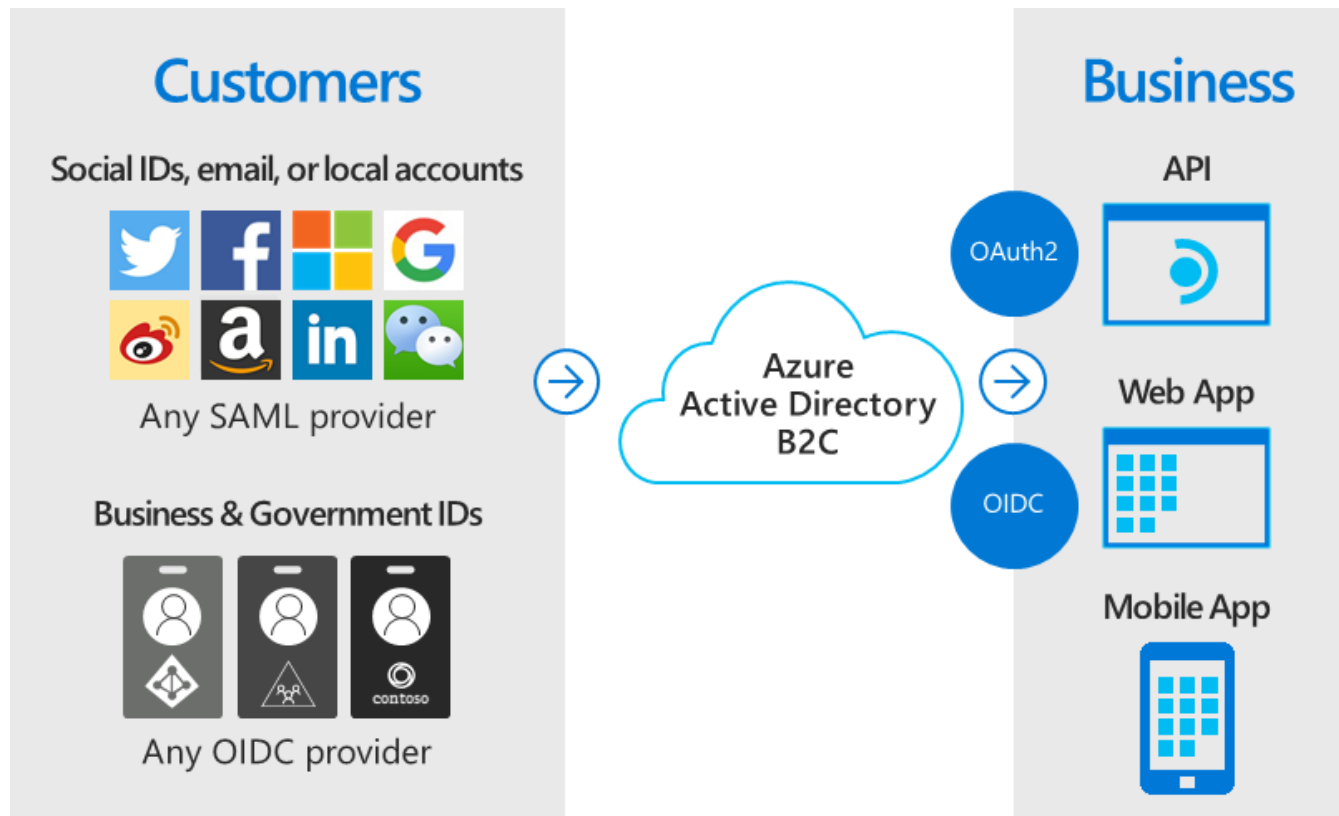
# What is really B2B?

- For Collaboration
- Business Partner
  - own identity management solution
  - no external administrative overhead for your organization
- The partner uses their own identities and credentials
  - They don't require Azure AD on their own.
- You don't need to manage external accounts or passwords.
- You don't need to sync accounts or manage account lifecycles.(\*)



# How is B2C different from B2B?

- B2B -> business collaboration and sharing of resources like files and apps
- B2C for customer/consumer facing apps



# Who can Invite?

- Normally only Admins can invite
- Inviting Guest Users to your Azure AD tenant can be delegated
  - Groups (& Teams)
  - Applications
- Group Owners
- Self Service

# Permissions & Restrictions for Guest Invites

Guest users permissions are limited ⓘ

☒ Yes ☐ No

Admins and users in the guest inviter role can invite ⓘ

☒ Yes ☐ No

Members can invite ⓘ

☒ Yes ☐ No

Guests can invite ⓘ

☐ Yes ☒ No

Enable Email One-Time Passcode for guests (Preview) ⓘ

[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)

# How to invite B2B Guests?

- For Admins and Users with Guest Inviter Role:
  - Manually in Azure AD Portal
  - Automation/Customization with PowerShell & Microsoft Graph
- For Application or Group Owners:
  - Teams
  - Groups/Apps



# What About Office 365 External Sharing?

- OneDrive/SharePoint Online different invitation manager
  - OneDrive/SharePoint Online adds users to the directory AFTER invitation redemption.
  - Different redemption experience.
  - Azure AD B2B collaboration invited users can be picked from OneDrive/SharePoint Online sharing dialog boxes. OneDrive/SharePoint Online invited users also show up in Azure AD after they redeem their invitations.

# B2B Invites with PowerShell

- Requirement:
  - Admin Role
  - AzureAD PowerShell Module

```
New-AzureADMSInvitation -InvitedUserDisplayName "Name  
(Company)" -InvitedUserEmailAddress "alias@domain.com"  
-InviteRedirectUrl "https://myapps.microsoft.com" -  
SendInvitationMessage $true
```

# B2B Invites with Microsoft Graph

POST <https://graph.microsoft.com/v1.0/invitations>

```
{
  "invitedUserDisplayName": "Display Name",
  "invitedUserEmailAddress": "alias@domain.com",
  "invitedUserMessageInfo": {
    "messageLanguage": "en-US",
    "customizedMessageBody": "custom string"
  },
  "sendInvitationMessage": false,
  "inviteRedirectUrl": "string"
}
```

# DEMO

## User Invitation Scenarios

# Organizational Relationships & Federation

- Social Identity Providers
  - Organizational Relationships
    - WS-FED, SAML
  - Google
    - Not GCP

Home > Elven Azure AD > Organizational relationships - Identity providers

## Organizational relationships - Identity providers

Elven Azure AD - Azure Active Directory

Search (Ctrl+ /)

Users from other organizations

Identity providers

Settings

Lifecycle management

Terms of use

Access reviews

Activity

Bulk operation results (Preview)

Troubleshooting + Support

Troubleshoot

New support request

+ Google + New SAML/WS-Fed IdP

Got a second? We would love your feedback on identity providers →

Invited users who own an Azure Active Directory account or a Microsoft Account can automatically sign in without further configuration.

### Social identity providers

Name
Google

### SAML/WS-Fed identity providers

Search

Search by domain name of a provider

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

# One-Time Passcode

- Support for any e-mail account
- Great for users that don't belong to:
  - Another Azure Active Directory
  - Google
  - Direct Federation via WS-FED or SAML
- .. or don't have or want to create a Microsoft Account



# Multi-Factor Authentication for Guests

- MFA
  - Enforce on a Per-User level
  - Via Conditional Access Policies
- Apply the same Conditional Access policies for Guests as for Normal Users, for
  - MFA
  - Location
  - Terms of Use

# Terms of Use

## Conditional Access - Terms of use

Azure Active Directory

« Policies

Manage

Named locations

Custom controls (preview)

Terms of use

VPN connectivity

Classic policies

Troubleshooting + Support

Troubleshoot

New support request

+ New terms    Edit terms    Delete terms    View audit logs    View selected audit logs

Search for a terms of use

NAME	ACCEPTED	DECLINED
Azure AD B2B Guest Terms of Use	6	0

Azure AD B2B Guest Terms of Use

Details Languages

Name	Azure AD B2B Guest Terms of Use
Display name	Azure AD B2B Guest Terms of Use for Elven Org
Require end user to expand	On
Require consent per device	Off
Users accepted	6
Users declined	0

# What about licensing?

- Free for Basic Azure AD features
- 1:5 for paid features
  - Conditional Access
  - Azure AD PIM

# DEMO

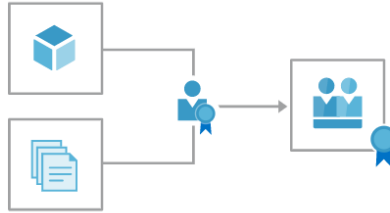
Guests and Conditional Access

# Identity Governance for Guests

- Identity Governance solution consists of:
  - Entitlement Management
  - Access Reviews
  - Privileged Identity Management
  - Terms of Use

Ensure the right people have the right access at the right time

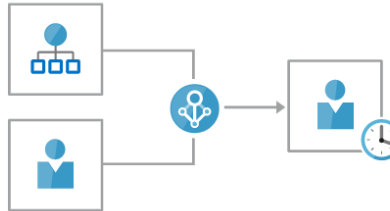
Azure AD Identity Governance helps you to protect, monitor, and audit access to critical assets while ensuring employee productivity



## Entitlement management

Govern the lifecycle of access to groups, applications, and SharePoint Online sites for both employees and guests.

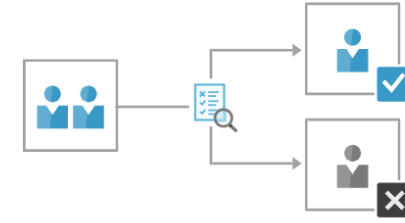
Create an access package



## Privileged Identity Management

Make users eligible for roles, so that they only have privileged access when necessary.

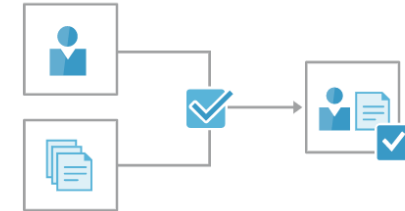
Manage role assignments



## Access reviews

Enable organizations to recertify group memberships, application access, and privileged role assignments.

Create an access review



## Terms of use

Ensure users see relevant disclaimers for legal or compliance requirements.

Publish a Terms of use

# Monitoring B2B Guests

- Sign-ins logs
- Audit logs
- Integration with Azure Monitor

## Monitoring



Sign-ins



Audit logs



Provisioning logs (Preview)



Logs



**Diagnostic settings**



Workbooks



Usage & insights



# Integrate Azure AD Activity Logs



# DEMO

## Identity Lifecycle and Governance

# Review

- Official Docs:
  - <https://docs.microsoft.com/en-us/azure/active-directory/b2b/>
- Blog Articles:
  - <https://gotoguy.blog/category/azure/azure-ad-b2b/>
- B2B PowerShell and Graph Samples Demo'ed:
  - <https://github.com/JanVidarElven/AzureADB2B-Samples>



## Headline Sponsors



Anywhere**365**



## Sponsors



**Pure IP**

