Azure B2B and Guest Management Best Practices

June 23, 2022

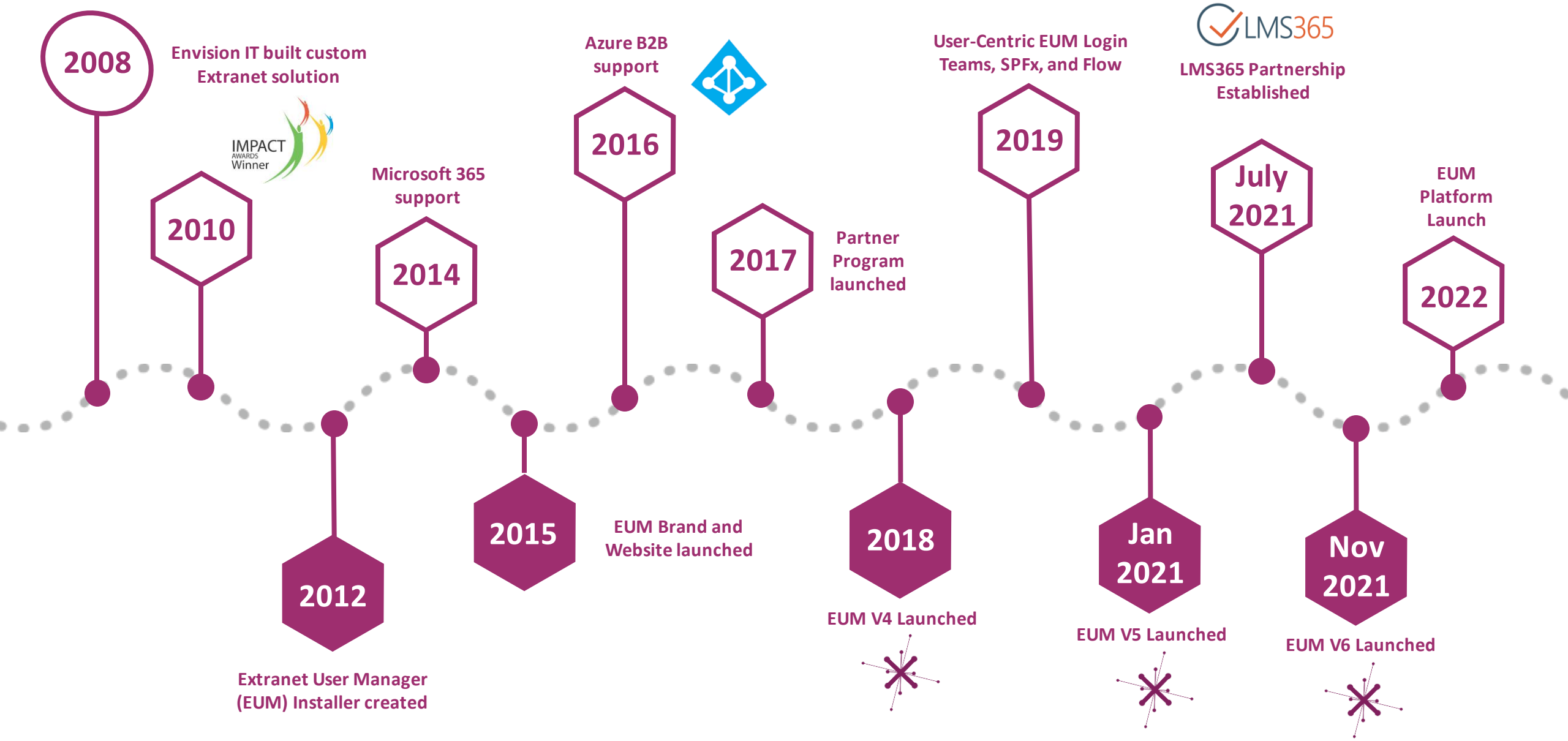
12 – 1 PM EDT

Logan Guest

- Sales and Marketing Manager, Extranet User Manager
- logan.guest@extranetusermanager.com
- www.extranetusermanager.com

Teams Meeting Etiquette

- This is a regular Teams meeting.
- Chat is open throughout the webinar.
- Feel free to ask questions or make comments through chat at any time.
- Please stay on mute. If you'd like to join the conversation, please ask on chat and wait for an invitation.
- Welcome, enjoy, and learn!


2008
Envision IT built custom Extranet solution
IMPACT AWARDS Winner
2010
2012
Extranet User Manager (EUM) Installer created
Microsoft 365 support
2014
2015
EUM Brand and Website launched
Azure B2B support
2016
2017
Partner Program launched
2018
EUM V4 Launched
User-Centric EUM Login Teams, SPFx, and Flow
2019
Jan 2021
EUM V5 Launched
LMS365
LMS365 Partnership Established
July 2021
Nov 2021
EUM V6 Launched
EUM Platform Launch
2022

Customers around the Globe

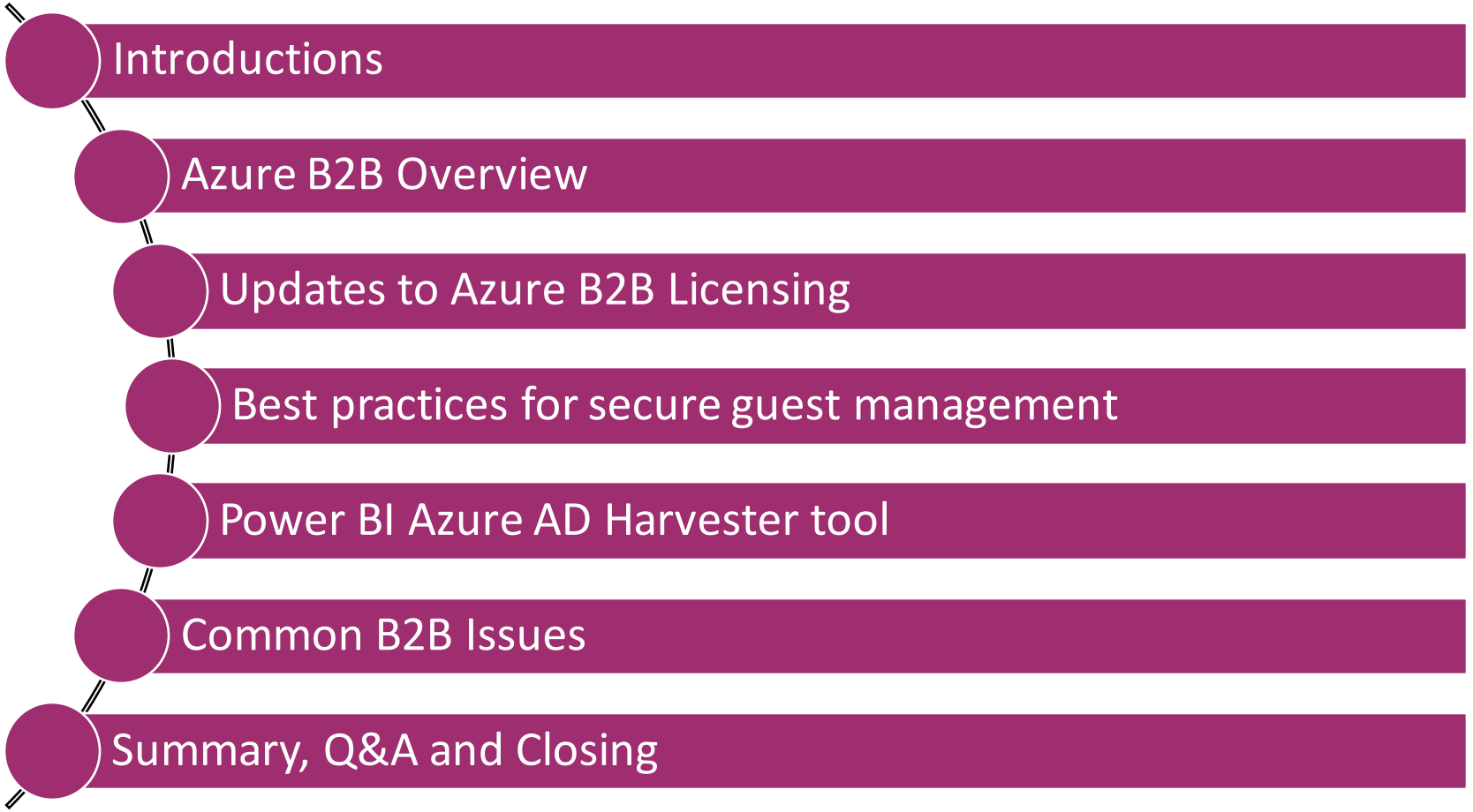
100+ Customers Deployed Globally

Peter Carson

- President, Extranet User Manager
- Office Apps and Services Microsoft MVP
- President Toronto SharePoint User Group

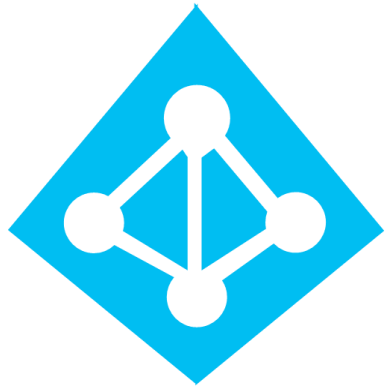
- Contact & Social:
  - peter.carson@extranetusermanager.com
  - blog.petercarson.ca
  - www.extranetusermanager.com
  - twitter.com/carsonpeter

Agenda


Introductions
Azure B2B Overview
Updates to Azure B2B Licensing
Best practices for secure guest management
Power BI Azure AD Harvester tool
Common B2B Issues
Summary, Q&A and Closing

Azure AD B2B Overview

- Azure Active Directory Business to Business
- **External (Guest) users** can access Microsoft 365 and any other system exposed through AAD
- No cost for guest users in Azure AD
- Completely free for certain Microsoft 365 workloads for external users
  - SharePoint
  - Teams
  - Planner
  - Office Online (Word, Excel, PowerPoint)
- Others have specific external licensing
  - Power Platform
    - Power BI
    - Power Apps
- Invite as many external users as you'd like



External Users in Microsoft 365

Microsoft Definition:

- "**External Users** means users that are not employees, onsite contractors or onsite agents of Customer or its Affiliates."
  - Refer to Commercial Licensing Terms (microsoft.com)
  - Typically includes subsidiary and franchisee staff
- Internal employee users are not eligible
  - Consider Microsoft 365 F1

Single Sign-On with Azure AD B2B

- No password management for guests
- Not just for signing into Microsoft properties
- Azure AD is a full Open ID Connect identity provider
  - Also supports OAuth 2.0 and SAML 2.0
- Any client (application) that can federate with these can use Azure AD for SSO
- Once a user is authenticated once to Azure AD, they don't need to authenticate again for other apps
- User can sign into their corporate SharePoint Online portal and authenticate, and then launch a shared site or link as a guest and not have to re-authenticate

Guest Sign-In Experience

Azure Active Directory

- User exists in an External Azure Active Directory
- Seamless login with organizational credentials

Microsoft Account

- Social accounts including Outlook, Hotmail, etc.

Email One-Time Passcode

- Non-licensed or non-recognized social identity
- 8 digit passcode sent to inbox each login

Google

- Direct federation to Google
- Works for @gmail.com accounts

Facebook

- Direct federation to Facebook

SAML/WS-Fed IdP

- Guest user is redirected to their Idp to sign in
- If SSO is enabled in Idp, user will experience SSO after initial sign in

[Configuring Identity Providers in Azure B2B | Extranet User Manager]

Azure AD Premium P1 vs. P2

Azure AD Premium P1	Azure AD Premium P2
• Multi-factor authentication with Conditional Access • Hybrid Identities • Password protection (custom banned passwords) • Advanced Security and Usage Reports • Conditional Access based on group, location, and device status • Azure Information Protection integration • And Much More • $6 USD user/month for staff	• Everything offered in P1 • Identity Protection • Privileged Identity Management • Access reviews • Entitlement Management (Preview) • $9 USD user/month for staff

Azure AD External Identity Licensing

- Only applies to Azure AD Premium features
  - Free for all users if not using premium features
  - Staff also need to be licensed for the same Premium features
- Price based on Monthly Active Users (MAU)
  - Replaces 1:5 billing ratio
- First 50,000 MAUs are free for both Premium P1 and Premium P2 features

	Premium P1	Premium P2
First 50,000 MAU	$0/Monthly Active Users	$0/Monthly Active Users
More than 50,000 MAU	$0.00416/Monthly Active Users	$0.020800/Monthly Active Users

https://docs.microsoft.com/en-us/azure/active-directory/external-identities/external-identities-pricing
https://azure.microsoft.com/en-us/pricing/details/active-directory/external-identities/

Azure Portal B2B Links

Company Branding

Identity Providers

- Microsoft
- One-Time Passcode
- Google
- Facebook
- Custom SAML / WS-Federation

Security

- Conditional Access
- Terms of Use

External Collaboration Settings

- Access, invite, and collaboration restrictions

Self-Service Sign Up

- User Attributes
- API Connectors
- User Flows

Lifecycle Management

- Terms of Use
- Access Reviews

Monitoring

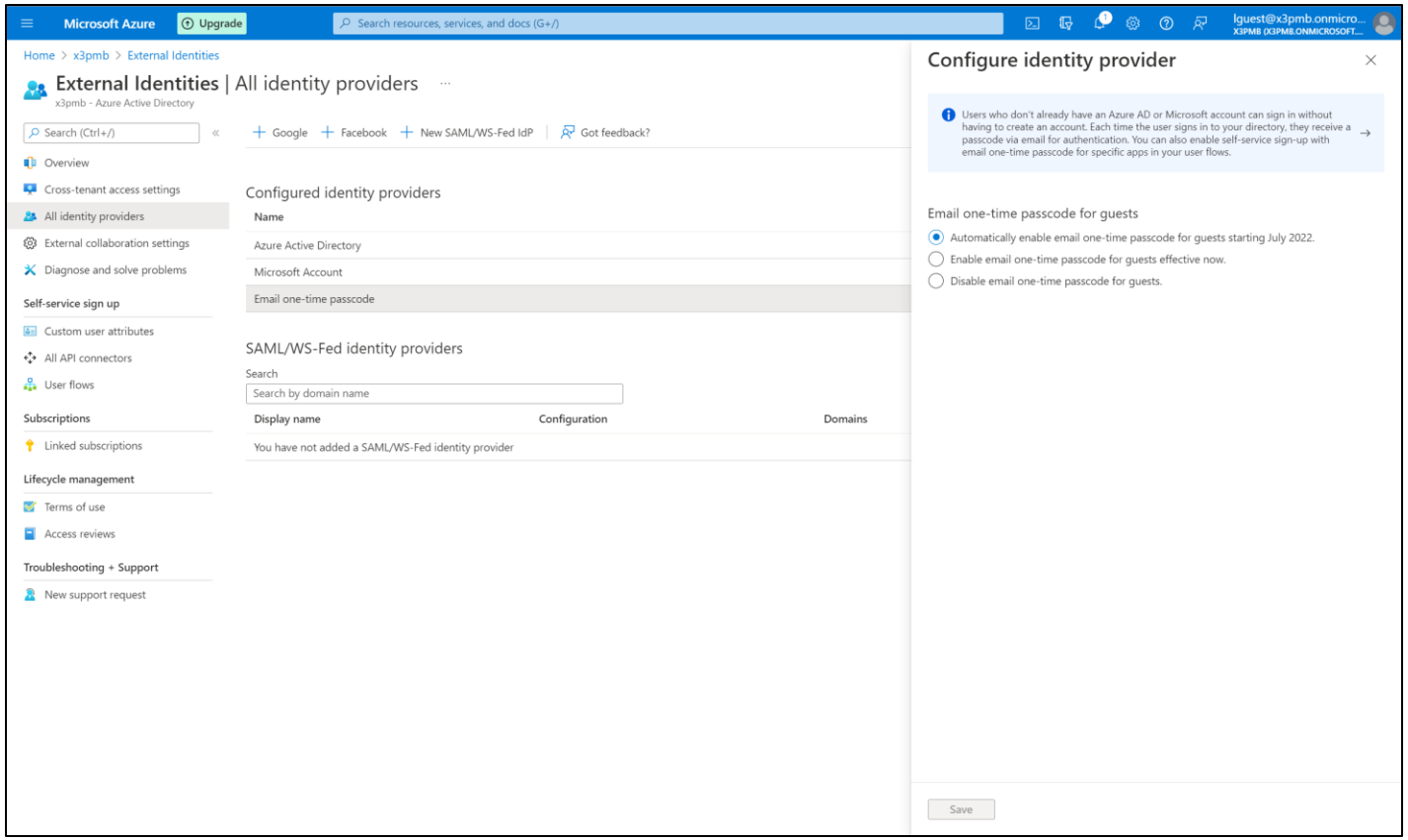
- Sign-In Logs
- Audit Logs
- Diagnostic Logs

Cross Tenant Settings

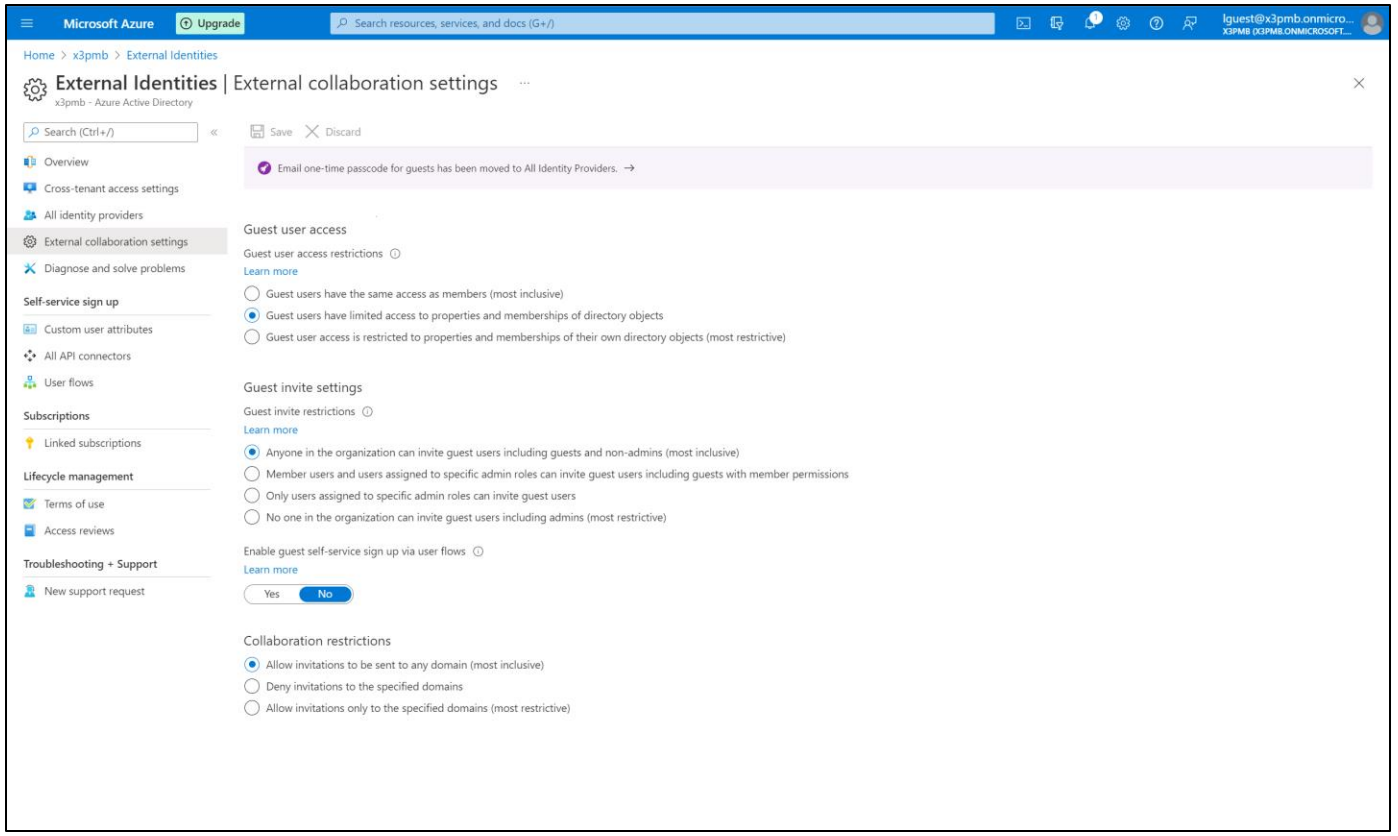
- B2B Collaboration
- B2B Direct Connect
- Trust Settings

Configuring Azure AD B2B for External Users | Extranet User Manager

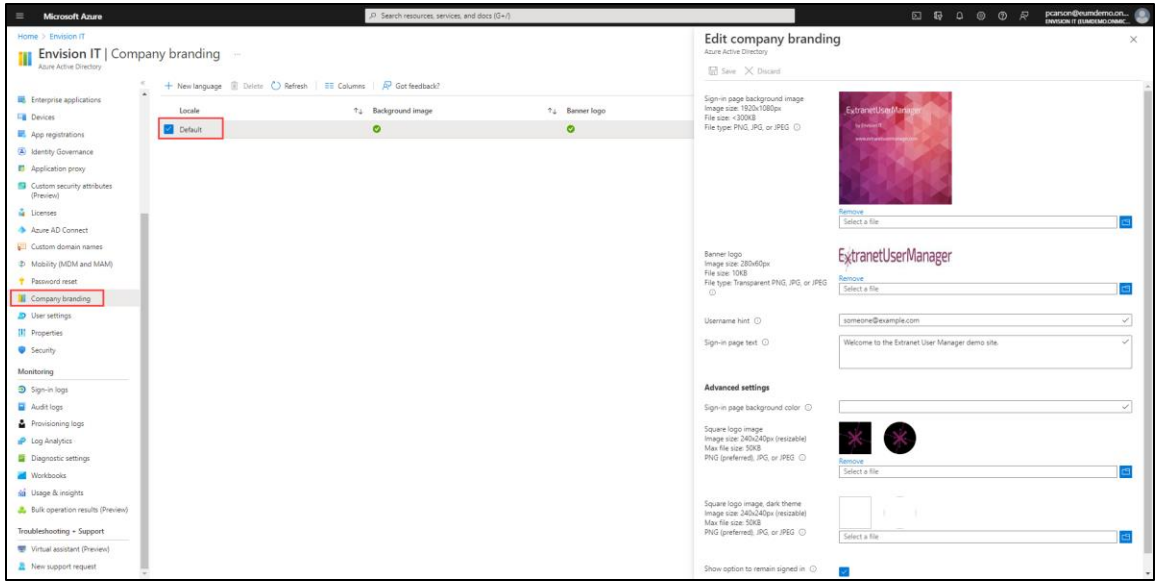
Identity Providers

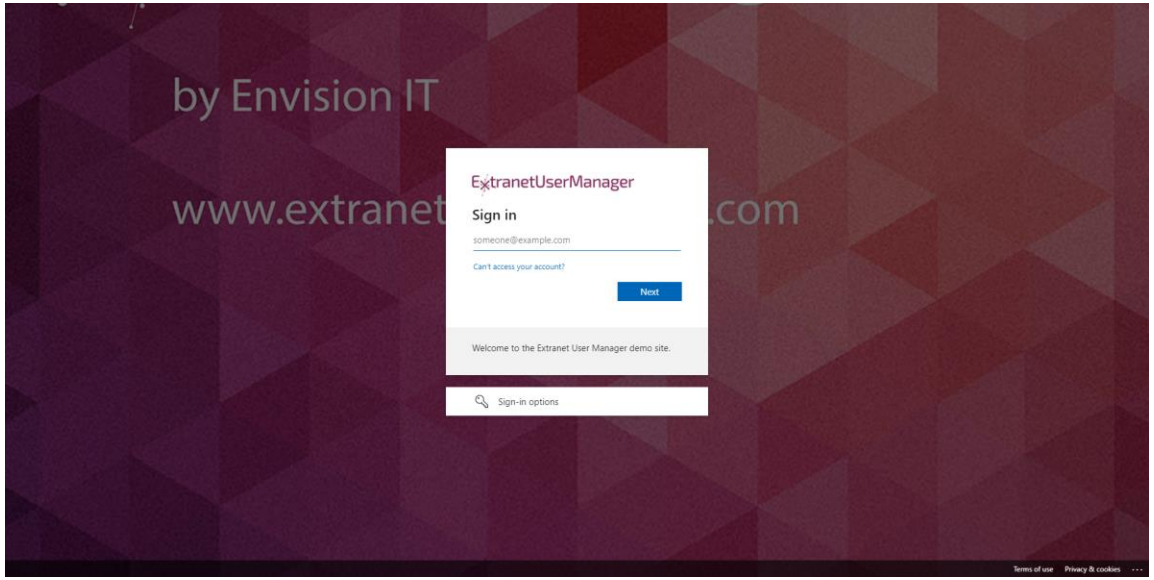


External Collaboration Settings



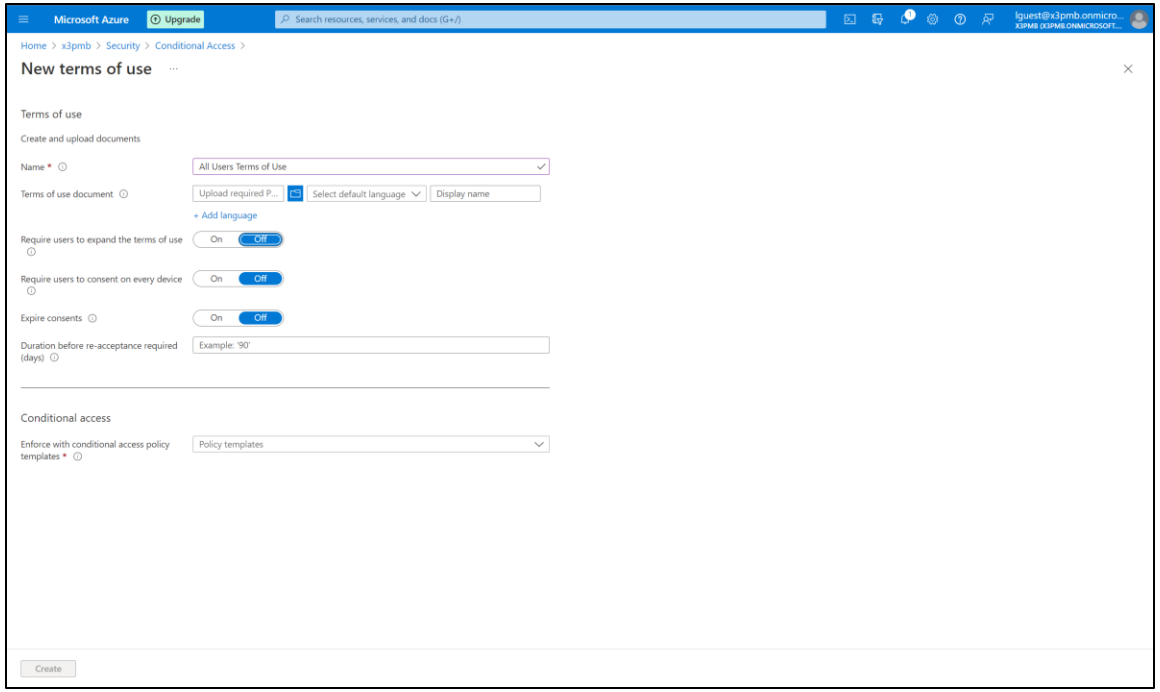
Azure AD Company Branding



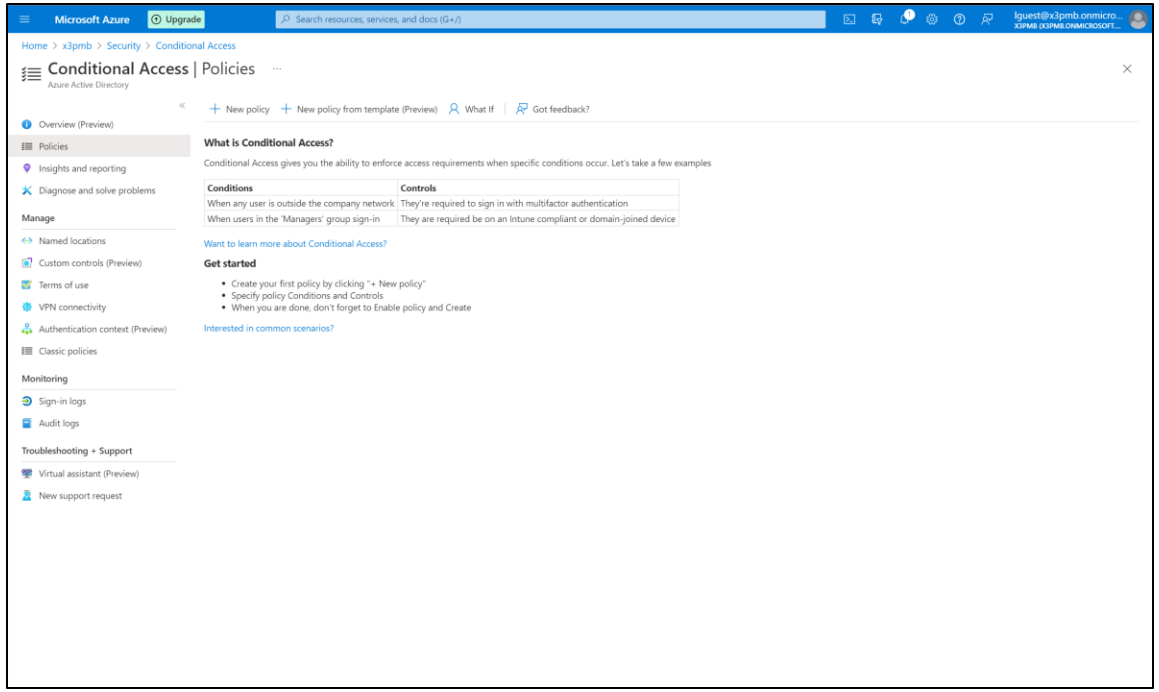


Security

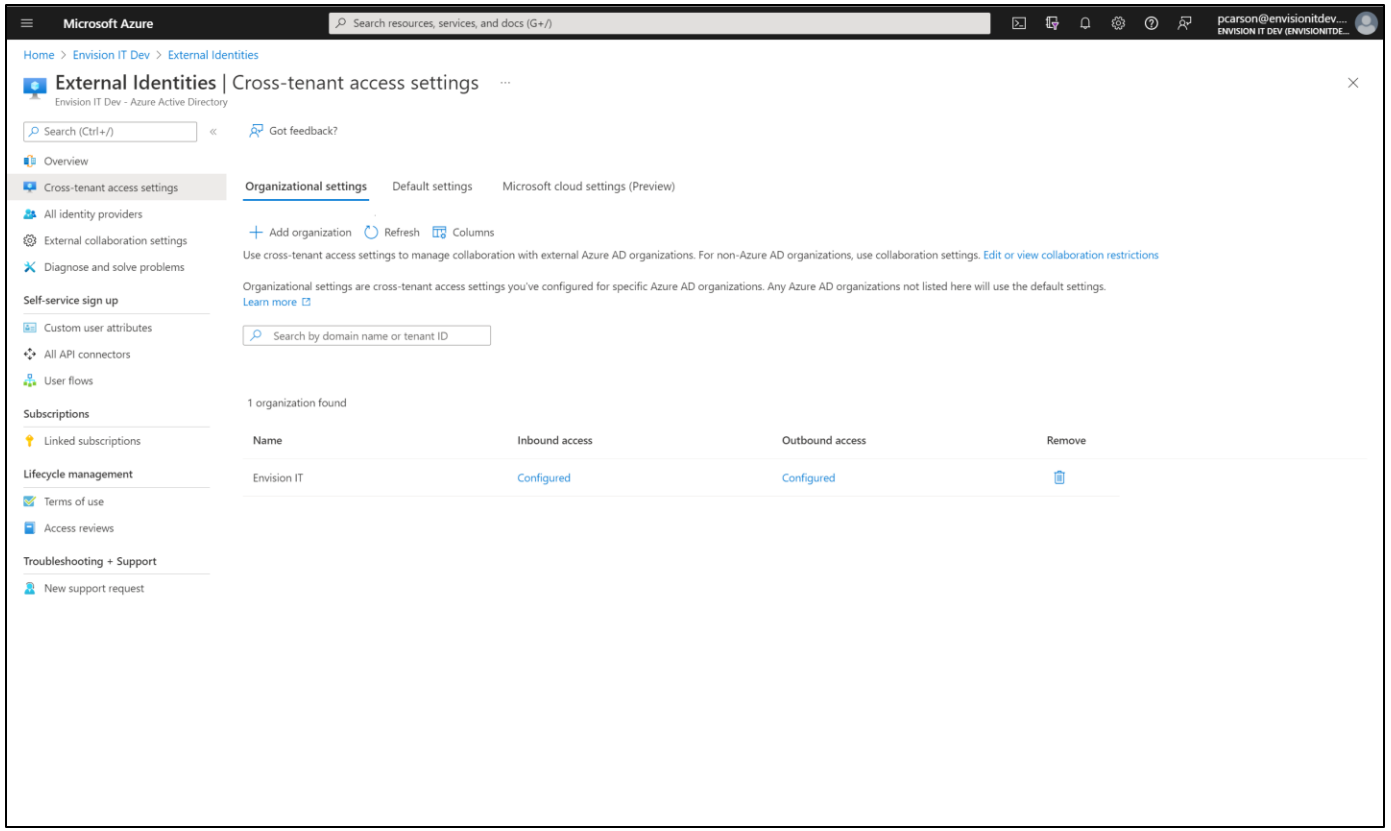
Terms of Use



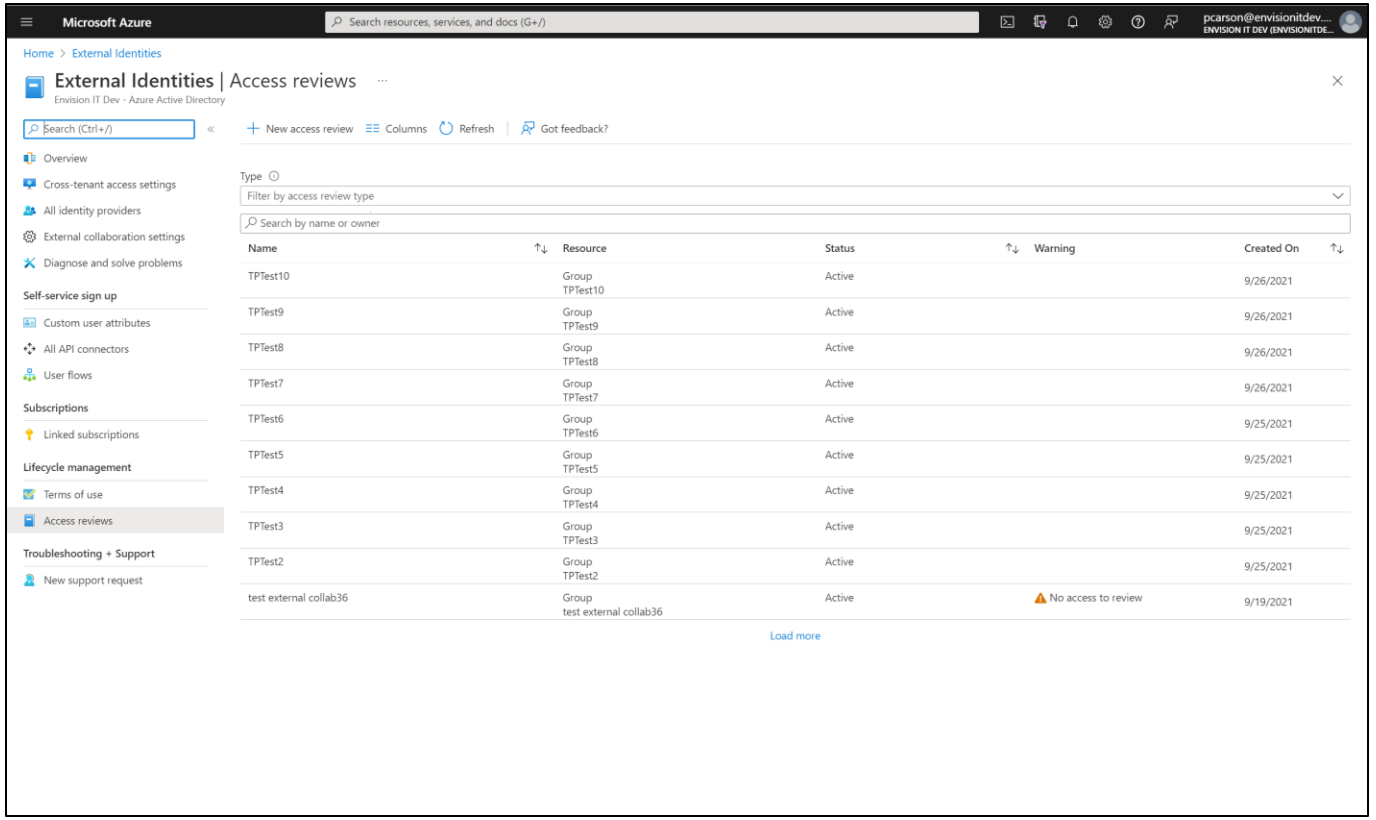
Conditional Access



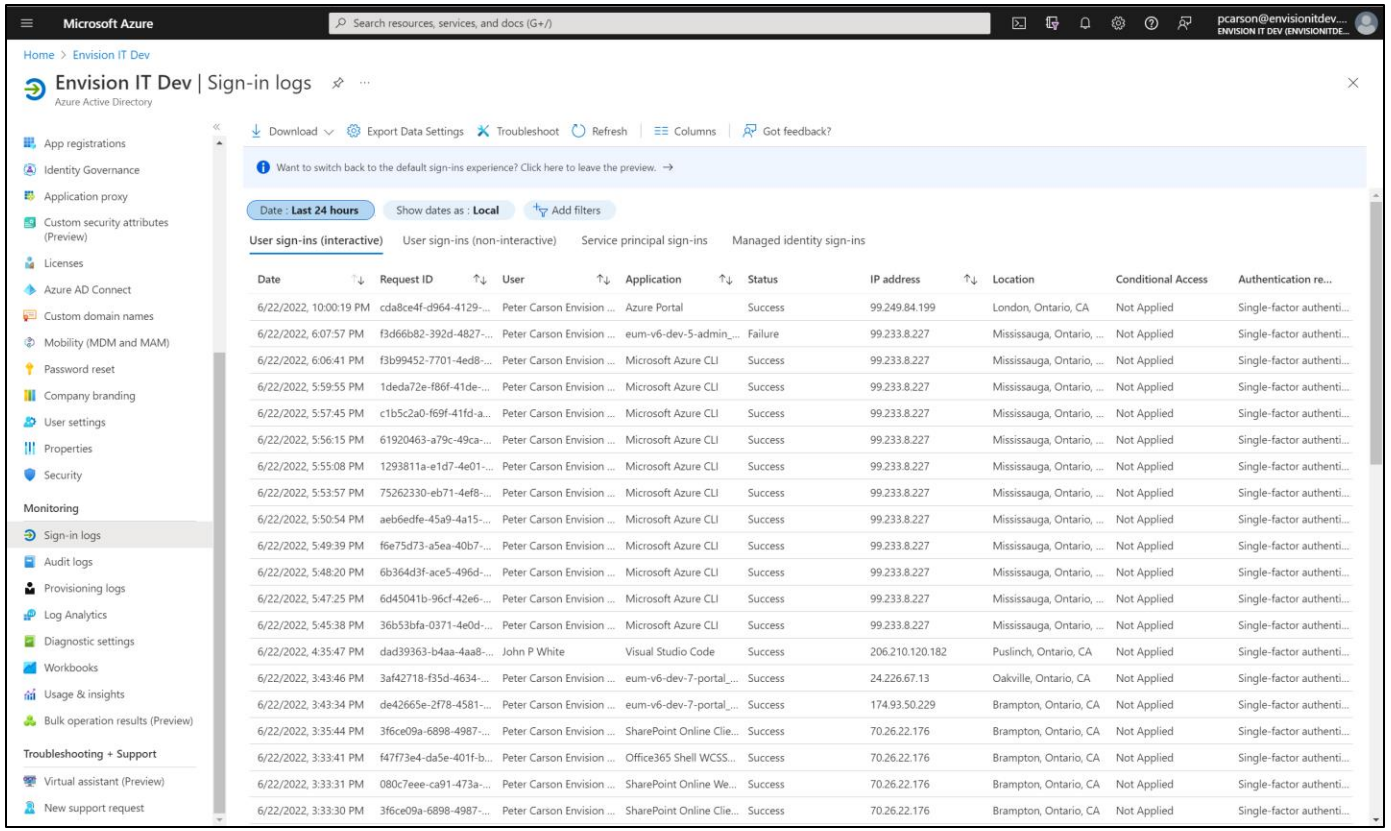
Cross Tenant Settings



Lifecycle Management



Monitoring

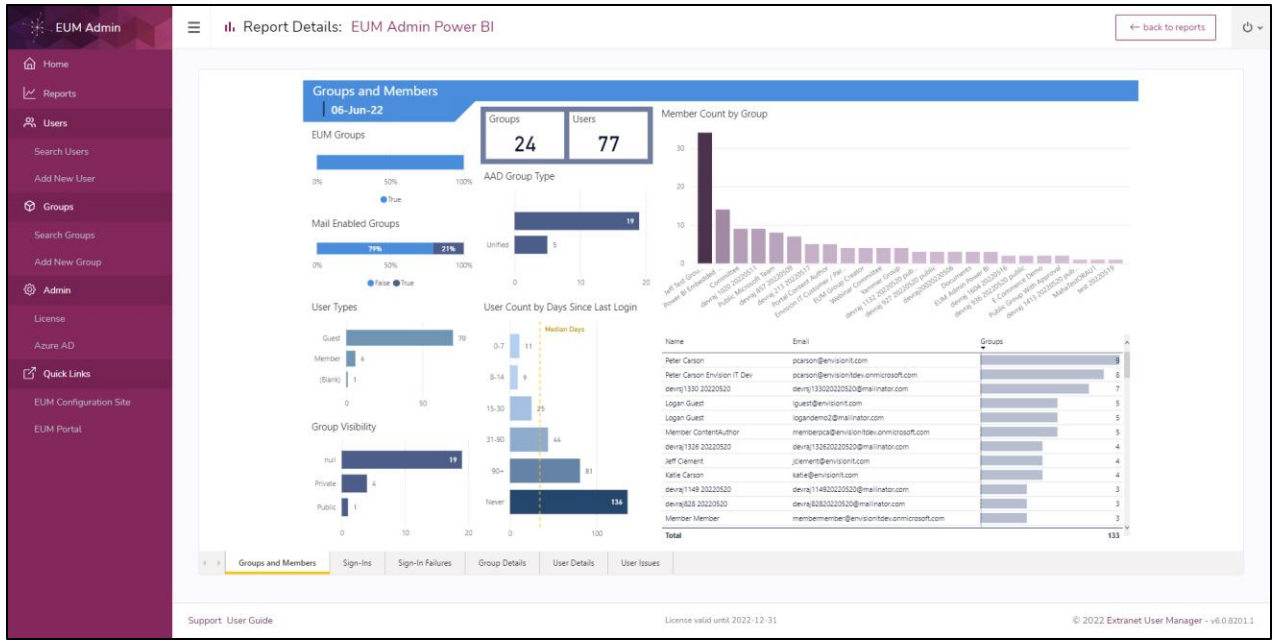

Microsoft Azure
Search resources, services, and docs (G+/)
pcarson@envisionitdev....
ENVISION IT DEV (ENVISIONITDE...
Home > Envision IT Dev
Envision IT Dev | Sign-in logs
Azure Active Directory
Download
Export Data Settings
Troubleshoot
Refresh
Columns
Got feedback?
Want to switch back to the default sign-ins experience? Click here to leave the preview.
Date : Last 24 hours
Show dates as : Local
Add filters
User sign-ins (interactive)
User sign-ins (non-interactive)
Service principal sign-ins
Managed identity sign-ins
App registrations
Identity Governance
Application proxy
Custom security attributes (Preview)
Licenses
Azure AD Connect
Custom domain names
Mobility (MDM and MAM)
Password reset
Company branding
User settings
Properties
Security
Monitoring
Sign-in logs
Audit logs
Provisioning logs
Log Analytics
Diagnostic settings
Workbooks
Usage & insights
Bulk operation results (Preview)
Troubleshooting + Support
Virtual assistant (Preview)
New support request
Date
Request ID
User
Application
Status
IP address
Location
Conditional Access
Authentication re...
6/22/2022, 10:00:19 PM cda8ce4f-d964-4129-... Peter Carson Envision ... Azure Portal Success 99.249.84.199 London, Ontario, CA Not Applied Single-factor authenti...
6/22/2022, 6:07:57 PM f3d66b82-392d-4827-... Peter Carson Envision ... eum-v6-dev-5-admin_... Failure 99.233.8.227 Mississauga, Ontario, ... Not Applied Single-factor authenti...
6/22/2022, 6:06:41 PM f3b99452-7701-4ed8-... Peter Carson Envision ... Microsoft Azure CLI Success 99.233.8.227 Mississauga, Ontario, ... Not Applied Single-factor authenti...
6/22/2022, 5:59:55 PM 1deda72e-f86f-41de-... Peter Carson Envision ... Microsoft Azure CLI Success 99.233.8.227 Mississauga, Ontario, ... Not Applied Single-factor authenti...
6/22/2022, 5:57:45 PM c1b5c2a0-f69f-41fd-a... Peter Carson Envision ... Microsoft Azure CLI Success 99.233.8.227 Mississauga, Ontario, ... Not Applied Single-factor authenti...
6/22/2022, 5:56:15 PM 61920463-a79c-49ca-... Peter Carson Envision ... Microsoft Azure CLI Success 99.233.8.227 Mississauga, Ontario, ... Not Applied Single-factor authenti...
6/22/2022, 5:55:08 PM 1293811a-e1d7-4e01-... Peter Carson Envision ... Microsoft Azure CLI Success 99.233.8.227 Mississauga, Ontario, ... Not Applied Single-factor authenti...
6/22/2022, 5:53:57 PM 75262330-eb71-4ef8-... Peter Carson Envision ... Microsoft Azure CLI Success 99.233.8.227 Mississauga, Ontario, ... Not Applied Single-factor authenti...
6/22/2022, 5:50:54 PM aeb6edfe-45a9-4a15-... Peter Carson Envision ... Microsoft Azure CLI Success 99.233.8.227 Mississauga, Ontario, ... Not Applied Single-factor authenti...
6/22/2022, 5:49:39 PM f6e75d73-a5ea-40b7-... Peter Carson Envision ... Microsoft Azure CLI Success 99.233.8.227 Mississauga, Ontario, ... Not Applied Single-factor authenti...
6/22/2022, 5:48:20 PM 6b364d3f-ace5-496d-... Peter Carson Envision ... Microsoft Azure CLI Success 99.233.8.227 Mississauga, Ontario, ... Not Applied Single-factor authenti...
6/22/2022, 5:47:25 PM 6d45041b-96cf-42e6-... Peter Carson Envision ... Microsoft Azure CLI Success 99.233.8.227 Mississauga, Ontario, ... Not Applied Single-factor authenti...
6/22/2022, 5:45:38 PM 36b53bfa-0371-4e0d-... Peter Carson Envision ... Microsoft Azure CLI Success 99.233.8.227 Mississauga, Ontario, ... Not Applied Single-factor authenti...
6/22/2022, 4:35:47 PM dad39363-b4aa-4aa8-... John P White Visual Studio Code Success 206.210.120.182 Puslinch, Ontario, CA Not Applied Single-factor authenti...
6/22/2022, 3:43:46 PM 3af42718-f35d-4634-... Peter Carson Envision ... eum-v6-dev-7-portal_... Success 24.226.67.13 Oakville, Ontario, CA Not Applied Single-factor authenti...
6/22/2022, 3:43:34 PM de42665e-2f78-4581-... Peter Carson Envision ... eum-v6-dev-7-portal_... Success 174.93.50.229 Brampton, Ontario, CA Not Applied Single-factor authenti...
6/22/2022, 3:35:44 PM 3f6ce09a-6898-4987-... Peter Carson Envision ... SharePoint Online Clie... Success 70.26.22.176 Brampton, Ontario, CA Not Applied Single-factor authenti...
6/22/2022, 3:33:41 PM f47f73e4-da5e-401f-b... Peter Carson Envision ... Office365 Shell WCSS... Success 70.26.22.176 Brampton, Ontario, CA Not Applied Single-factor authenti...
6/22/2022, 3:33:31 PM 080c7eee-ca91-473a-... Peter Carson Envision ... SharePoint Online We... Success 70.26.22.176 Brampton, Ontario, CA Not Applied Single-factor authenti...
6/22/2022, 3:33:30 PM 3f6ce09a-6898-4987-... Peter Carson Envision ... SharePoint Online Clie... Success 70.26.22.176 Brampton, Ontario, CA Not Applied Single-factor authenti...

Guest Management Best Practices

- **Every tenant should really have Azure AD P1 for all their members**
- **If not, license at least one, and you get P1 for up to 50,000 monthly active external users for free**
  - Gets you sign in activity tracking and conditional access policies
- **Turn on One Time Passcode if not already**
- **Apply company branding**
- **Determine if there should be a Terms of Use**
- **Setup logging and auditing**
- **Define sensitivity of content being shared**
- **Determine MFA requirements and conditional access policies for guests**
- **Determine if trust settings should be configured for key partners**

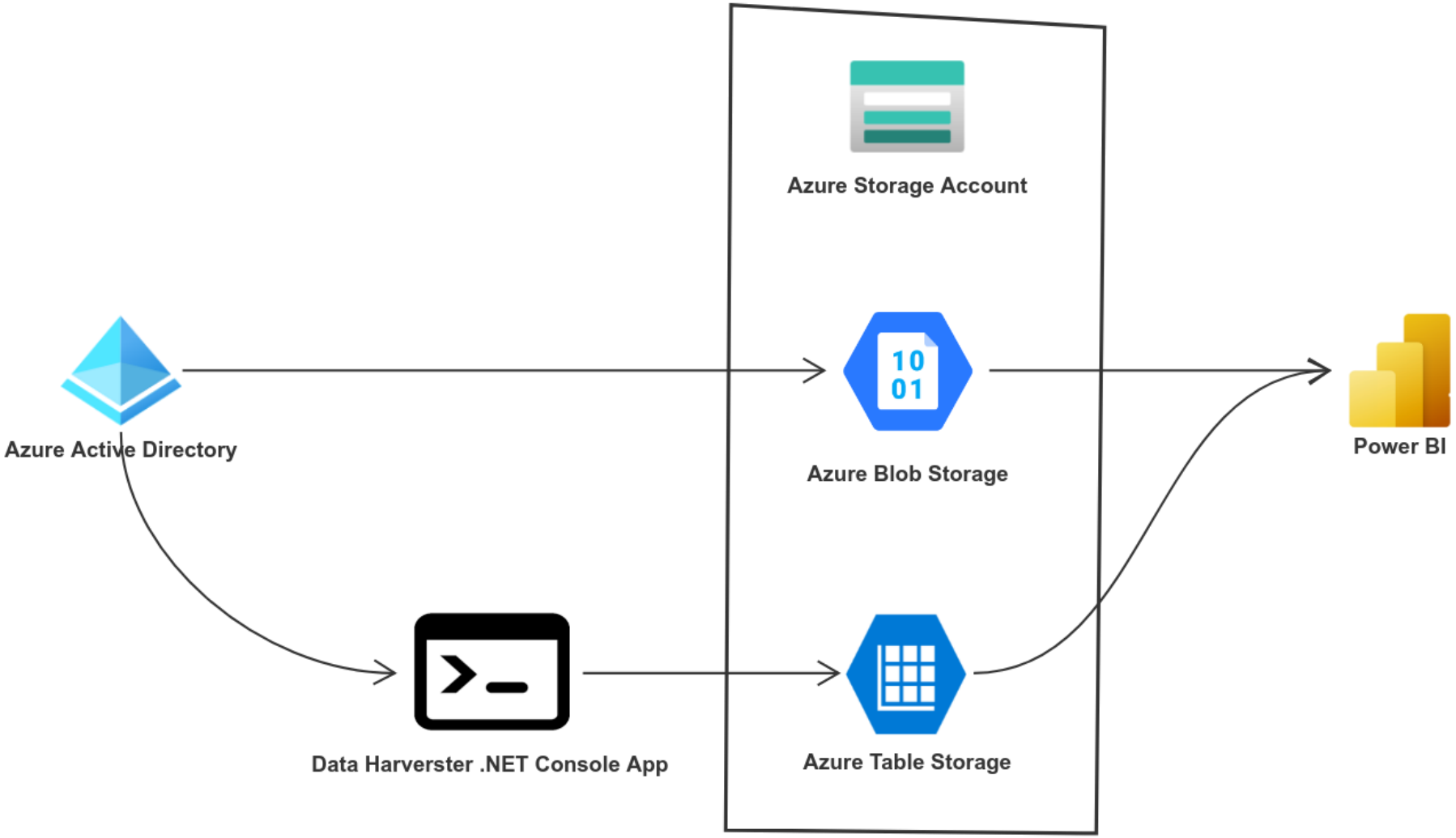
Power BI Azure AD Permissions Harvester tool

- Open source solution
- Provides insight into groups and users within Azure AD
- Ships audit logs to table storage
  - Groups and Users
  - Sign-Ins
  - Sign-In Failures
  - Group & User Details
  - User Issues
- Solution components include:
  - Harvester Console Application
  - Azure Storage Account
  - Power BI Dashboard template



ExtranetUserManager

Power BI Data Harvester



Common B2B Issues

User Type Not Populated	•Tenant may pre-date the release of Azure B2B •If user type is not populated and you use conditional access policies, they will not be properly applied to these users
Mismatch Between Email and UPN	•When email address does not match User Principal Name due to organizational change •Users get stuck during login as they sign in with their email but were invited with UPN
Missing Email	•Email is not a requirement in Azure AD for member accounts •Users who login as guests to your tenant would not receive the Microsoft issued invite •Less of an issue now as invite is no longer a requirement
Unaccepted Invitations	•Invitations are no longer required however users that were invited before this feature was introduced and did not accept the invitation cannot sign in •New preview feature allows you to reset the invitation which can be done without sending anything to guest user
Conflicting Microsoft Account	•Previously you were able to create a Microsoft account using the same email address as your organization Microsoft 365 account •Users are often unsure of what account to login with and if the wrong is chosen, they receive a sign in error

Azure AD B2B Health | Extranet User Manager

Guest Governance

User not in Any Groups

User Never Signed In

User Hasn’t Signed In X Days

[Azure AD B2B Health | Extranet User Manager]

Power BI Harvester Demo

Key Takeaways

- **Review the guest management best practices in this deck**
- **Review common issues**
- **Setup the open source Azure AD harvester to gain insight into your Azure AD**
- **Define your guest governance plan**

Relevant Articles

[Azure AD Company Branding Setup](#)
June 22, 2022

[Configuring Identity Providers in Azure B2B | Extranet User Manager](#)
June 16, 2022

[Azure AD B2B vs B2C | Extranet User Manager](#)
June 15, 2022

[Azure AD Conditional Access Policies Base Recommendations | Extranet User Manager](#)
April 11, 2022

[Azure AD B2B Health | Extranet User Manager](#)
April 10, 2022

[Microsoft Power BI Versions and Licensing | Envision IT](#)
December 15, 2021

[Five Considerations for Successful External Sharing in Microsoft 365 | Extranet User Manager](#)
November 3, 2020

Relevant Webinar Sessions

[Effective Board and Committee Management with Microsoft 365]
May 3, 2022

[Deploy Power BI Dashboards Internally and Externally without User Licensing]
March 22, 2022

[Create a Custom Learning Portal for Your External Users]
January 25, 2022

[Engaging with External Users at Scale with Microsoft 365 and Branded Portals]
November 2, 2021

[New Azure AD External Identities Features]
July 27, 2021

[Microsoft 365 Unstructured and Structured External Sharing | Extranet User Manager]
July 13, 2021

Upcoming Events

Taking a break from live webinars for July and August… You should too!

Stay tuned for upcoming events at http://eum.co/resources/events

Thank you!

Questions?