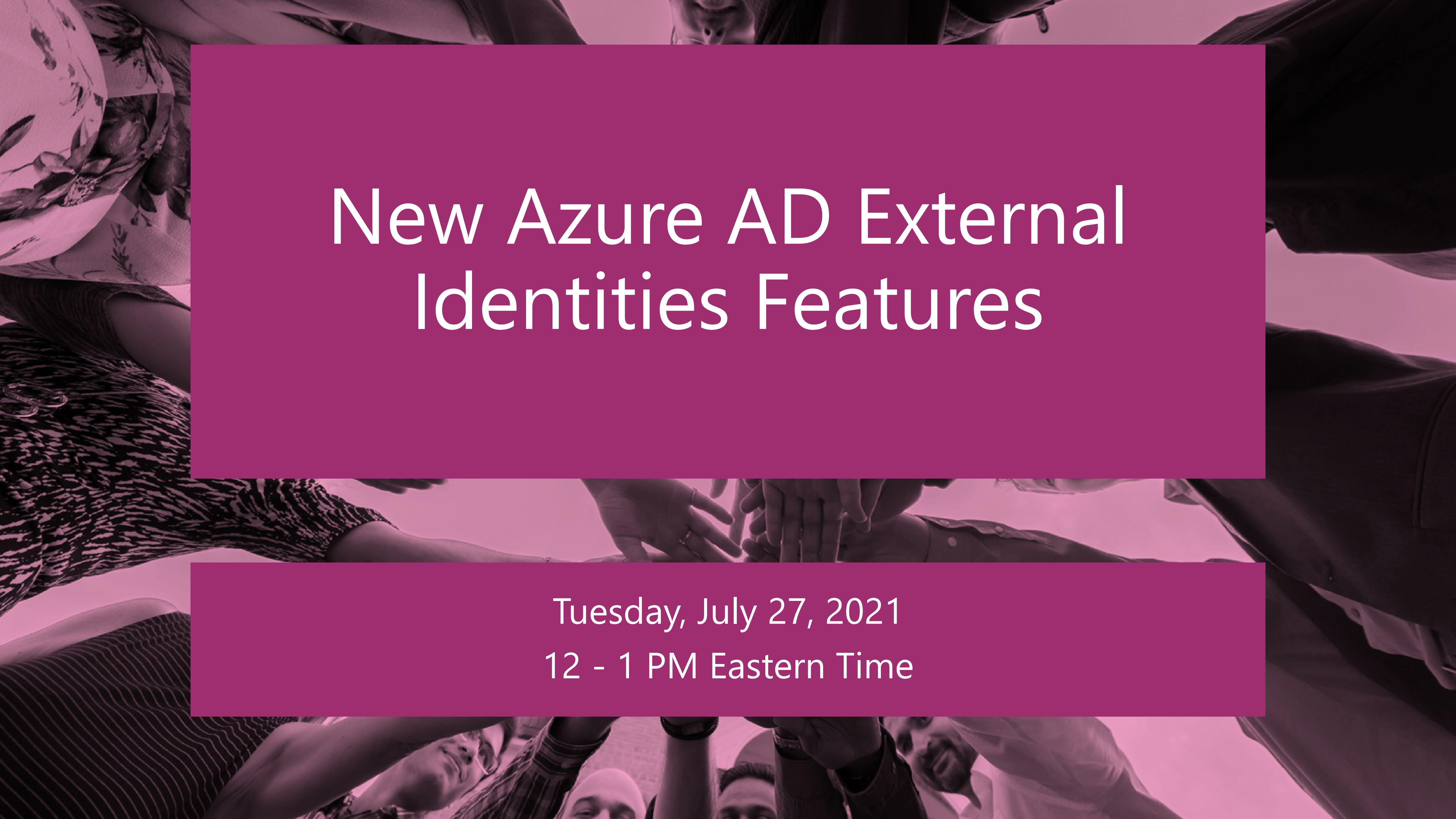


New Azure AD External Identities Features

Tuesday, July 27, 2021

12 - 1 PM Eastern Time

Peter Carson

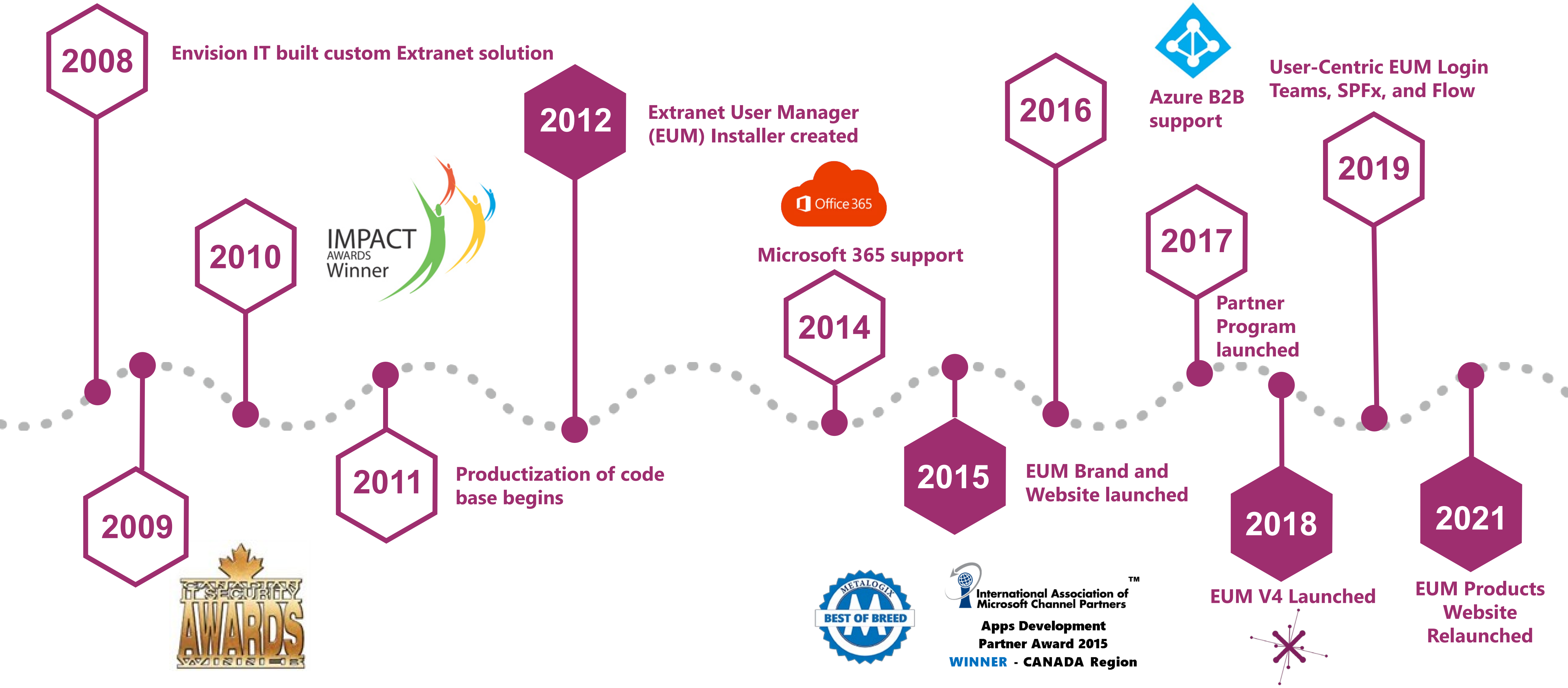
- President, Extranet User Manager
- Office Apps and Services Microsoft MVP
- peter.carson@extranetusermanager.com
- blog.petercarson.ca
- www.extranetusermanager.com
- Twitter @carsonpeter
- President Toronto SharePoint User Group

MVP Microsoft Most Valuable Professional

Logan Guest

Sales & Marketing Manager

- e: logan.guest@extranetusermanager.com
- p: (647) 265-8256



2008

Envision IT built custom Extranet solution

2009

IT SECURITY AWARDS

2010

IMPACT AWARDS Winner

2011

Productization of code base begins

2012

Extranet User Manager (EUM) Installer created

2014

Office 365

Microsoft 365 support

2015

EUM Brand and Website launched

METALOGIX BEST OF BREED

International Association of Microsoft Channel Partners™

Apps Development Partner Award 2015 WINNER - CANADA Region

2016

Azure B2B support

2017

Partner Program launched

2018

EUM V4 Launched

2019

User-Centric EUM Login Teams, SPFx, and Flow

2021

EUM Products Website Relaunched

Customers around the Globe

Grant Thornton
KINROSS
ivari
MARCH OF DIMES CANADA
JOHNSON OUTDOORS THE SPIRIT OF ADVENTURE
Boys & Girls Clubs of Canada Clubs Garçons et Filles du Canada
OntarioMD
ONTARIO POWER GENERATION
Trax emro
Ontario Association of Children's Aid Societies The voice of child welfare in Ontario
LoyaltyOne
Lassonde
camh Centre for Addiction and Mental Health
Technip
MAJEDIE Asset Management
Los Angeles World Airports
Public Health Ontario
Santé publique Ontario
G2G MARKET PLACE
CADTH Evidence Driven.
AÉROPORTS DE MONTRÉAL
ORTHOFIX
Northwestern Health Unit www.nwhu.on.ca
OAKLAND COUNTY MICHIGAN
ORAU
Russel Metals
KingSett CAPITAL
PVH
Associated Engineering
NPL National Physical Laboratory
Human-Etisk Forbund
LandSecurities
ISLINGTON
PAPYRUS
Ultra ELECTRONICS
babcock
BARNSLEY Metropolitan Borough Council
SONY make.believe
هيئة كهرباء ومياه دبي
Dubai Electricity & Water Authority
DRDGOLD LIMITED
SUPREME COURT VICTORIA

100+ Customers Deployed Globally

Agenda

- Introductions
- Azure Active Directory B2B Background
- Licensing Updates
- Self Service Sign Up
- Terms of Use
- Entitlement Management
- Summary, Q&A and Closing

Azure AD External Identities Solutions

External user collaboration (B2B)

- Externally sharing in Microsoft 365, Teams or your own applications
- Collaboration with suppliers, partners, vendors
- Users exist as Guest users in your directory

Access to Consumer-facing Apps (B2C)

- IAM for SaaS and custom developed Apps excluding Microsoft first-party apps
- Collaboration with consumers of your product
- Users are managed in a separate Azure AD directory

Azure AD B2B and Microsoft 365

- Azure Active Directory Business to Business
- **External users** can access Microsoft 365 and any other system exposed through AAD
- Completely free for certain Microsoft 365 workloads for external users
  - SharePoint
  - Teams
  - Planner
  - Office Online
- Others have specific external licensing
  - 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)
- Internal employee users are not eligible
  - Consider Microsoft 365 F1

Single Sign-On with Azure AD B2B

- **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**

Azure AD B2B Onboarding Experiences

Existing Microsoft 365

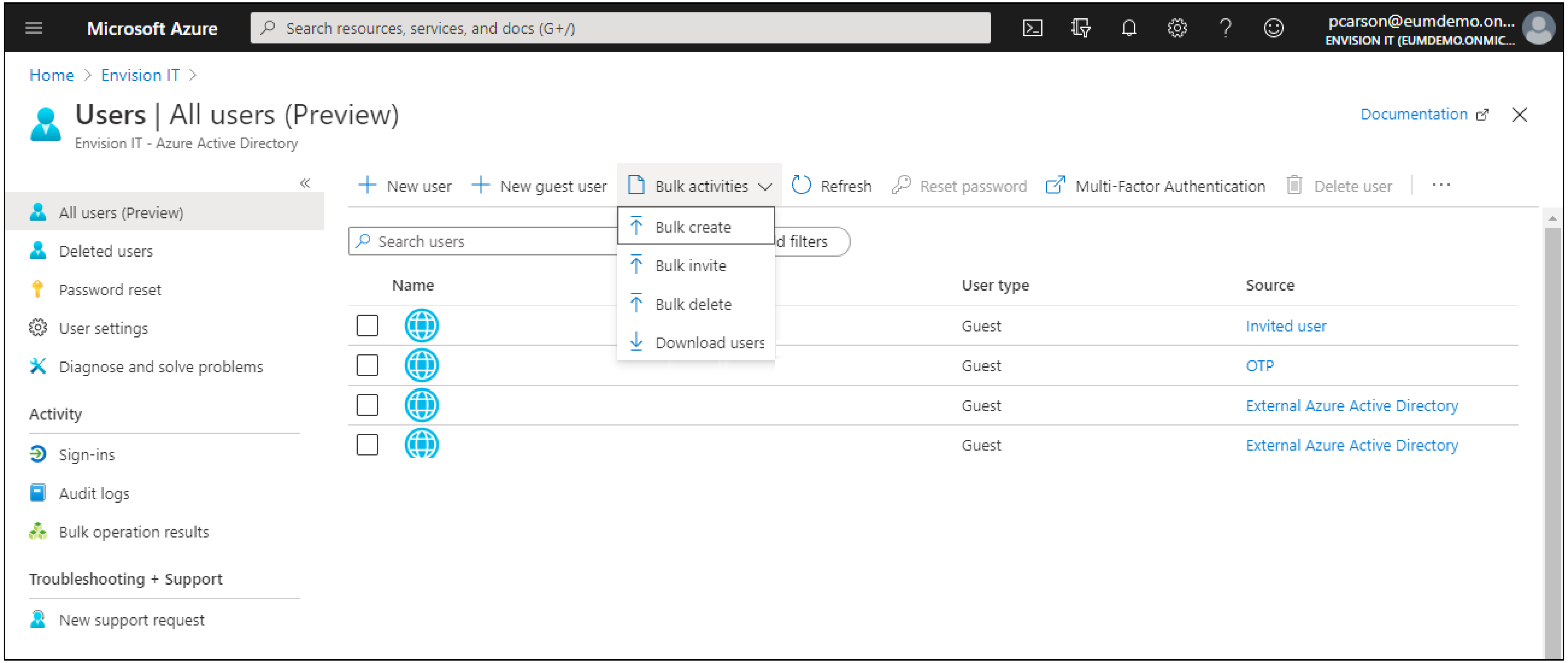
- Logs in with their Azure AD credentials
- Seamless experience
- Single sign-on if already signed into Microsoft 365
- Also works for Microsoft accounts

No Azure AD Account

- One time passcode
- Emailed at sign-in
- Valid for 30 minutes
- Low friction, no new account to setup or password to remember
- Validates at each sign in that they still own the email address

Social User

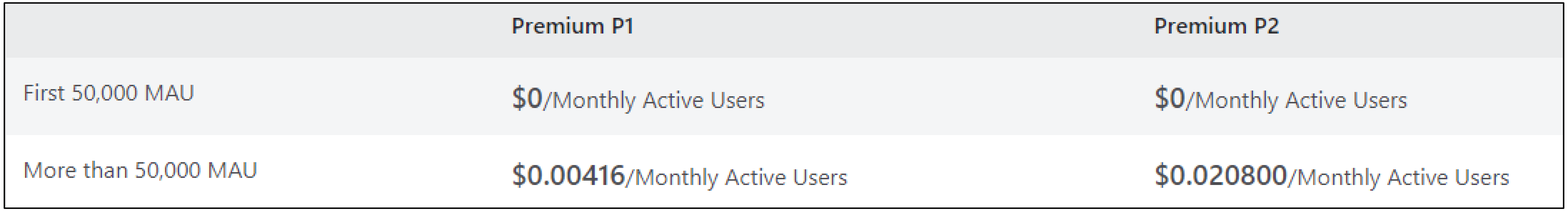
- Federation with Google and Facebook accounts now also supported
- Same seamless login experience as Microsoft 365
- Need to be an @gmail.com address for Google Federation



	Name	User type	Source
□		Guest	Invited user
□		Guest	OTP
□		Guest	External Azure Active Directory
□		Guest	External Azure Active Directory

Updates to 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 AD P1 vs. P2

Azure AD Premium P1

- **Conditional Access**
  - Multi-factor authentication
  - **Terms of Use**
- 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

Azure AD Premium P2

- Everything offered in P1
- Identity Protection
- **Privileged Identity Management**
- **Access reviews**
- **Entitlement Management (Preview)**

Azure Information Protection

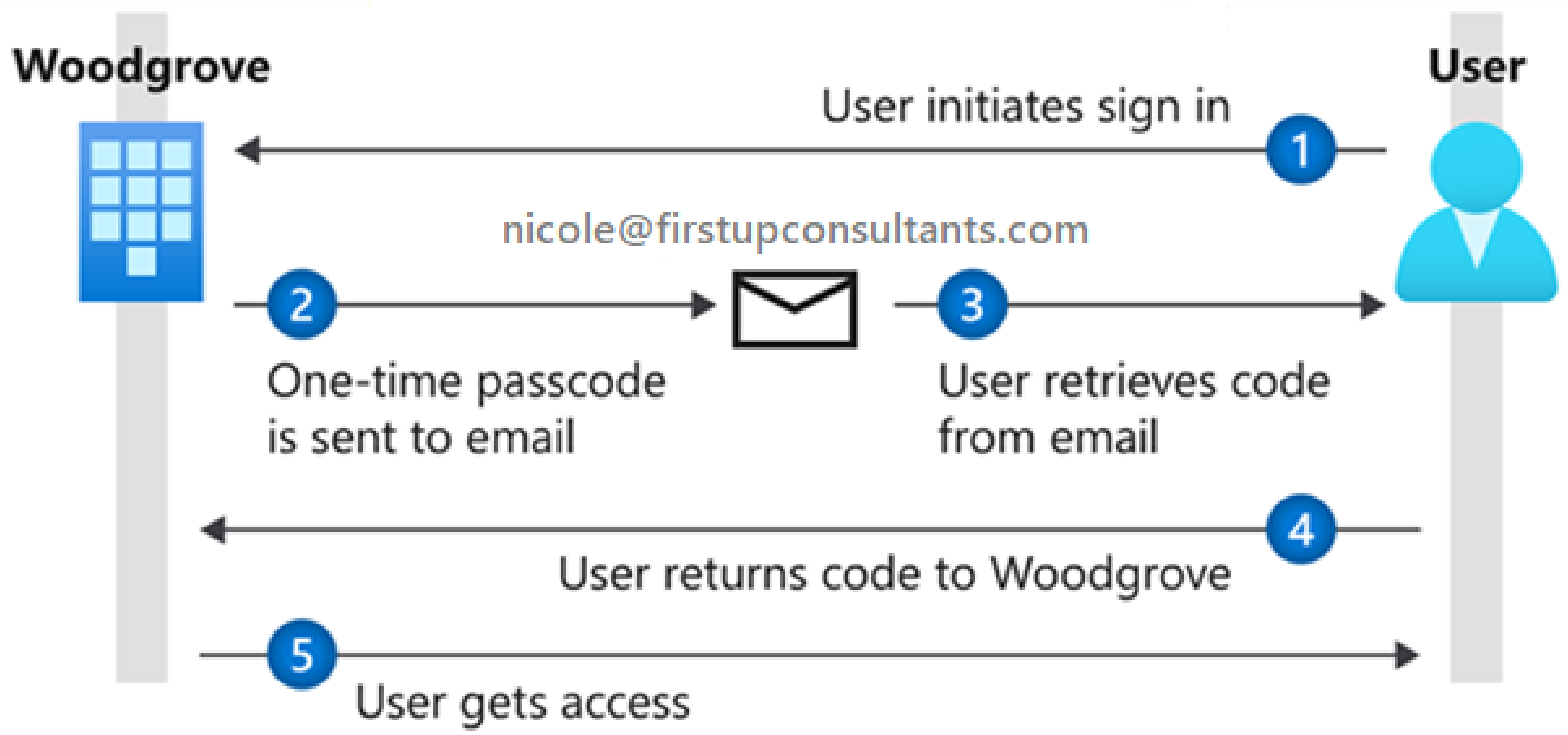
- **Used to classify and protect content**
- **More granular permissions can be applied**
  - AIP uses Azure Rights Management to encrypt and protect the documents regardless of where the document is
  - Block download, edit, copy
  - You could allow download, but for anyone to access the downloaded document they would still need to have the AIP rights assigned to them
  - Maintains control of the documents regardless of where they go
  - Permissions can be revoked for documents regardless of where they are
- **Can be used with Conditional Access to determine policy**
  - Could require MFA before accessing sensitive documents or sites
- **Can also be applied to the sharing rules**
  - Don't allow sharing of content with certain sensitivity labels applied
- **Can be manually or automatically applied (AIP P1 or P2)**

New External Identities Features

Email One-Time Passcode Authentication

- **New way to authenticate Guest users without:**
  - Azure AD account
  - Microsoft account
  - Social provider - Google or Facebook
- **Temporary passcode is sent to email address**
- **Passcode is entered to sign in**
- **One-time passcode is valid for 30 minutes**
- **Next user session will send a new passcode to the user**

Email One-Time Passcode Authentication



Woodgrove

User

1 User initiates sign in

nicole@firstupconsultants.com

2 One-time passcode is sent to email

3 User retrieves code from email

4 User returns code to Woodgrove

5 User gets access

Demo

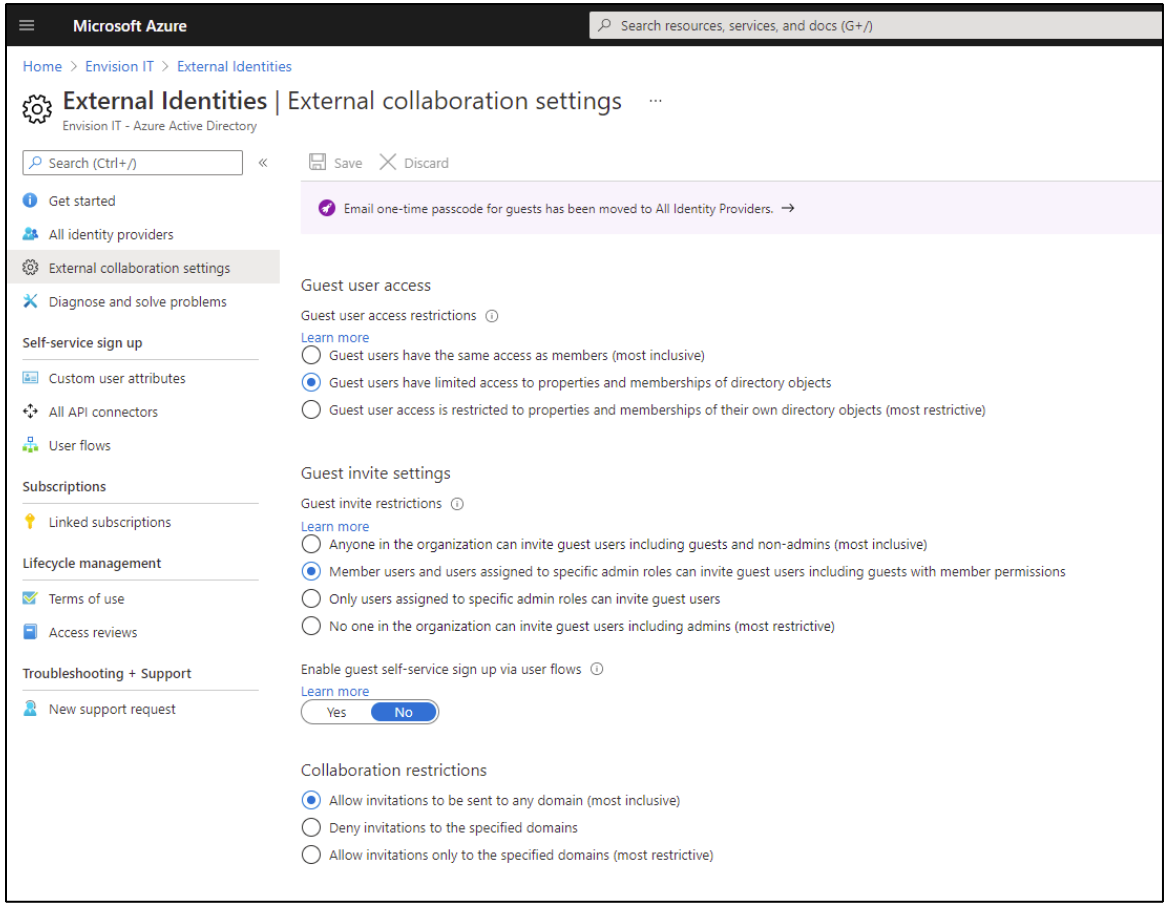
One Time Passcode

Email One-Time Passcode Authentication

- **Starting October 2021, the email one-time passcode feature will be turned on for all existing tenants**
- **Will be enabled by default for new tenants**
- **Un-managed Azure AD accounts will no longer be supported**
- **Envision IT has been using for 1.5 yrs +**
- **Very positive experience versus the previous unmanaged account setup process**

Azure AD External Identities (B2B)

- Self-service sign up
  - Custom attributes
  - API connectors
- Lifecycle management
  - Terms of use
  - Access reviews



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Envision IT > External Identities

External Identities | External collaboration settings ...

Envision IT - Azure Active Directory

Email one-time passcode for guests has been moved to All Identity Providers. →

Guest user access

Guest user access restrictions ⓘ

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

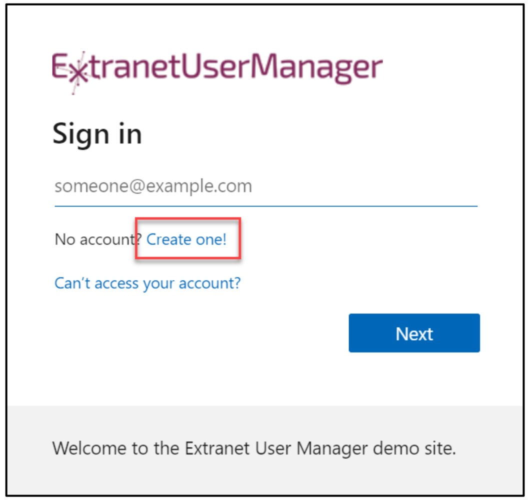
○ Allow invitations only to the specified domains (most restrictive)

External Identities documentation | Microsoft Docs

Demo

Self-Service Sign-Up

https://azureregistration.azurewebsites.net/



ExtranetUserManager

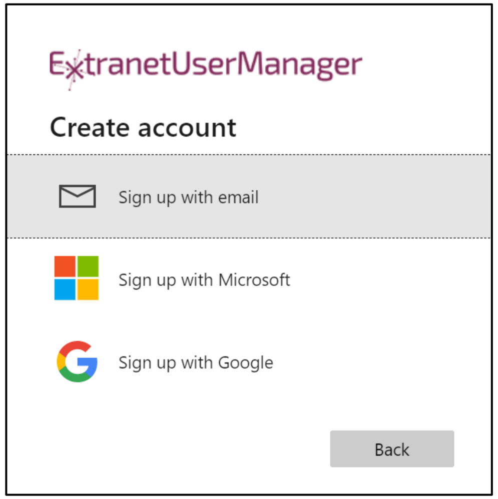
Sign in

someone@example.com

No account? Create one!

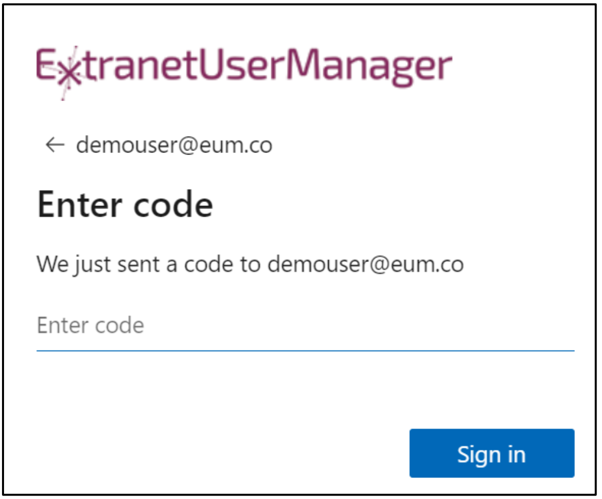
Can't access your account?

Welcome to the Extranet User Manager demo site.



ExtranetUserManager

Create account



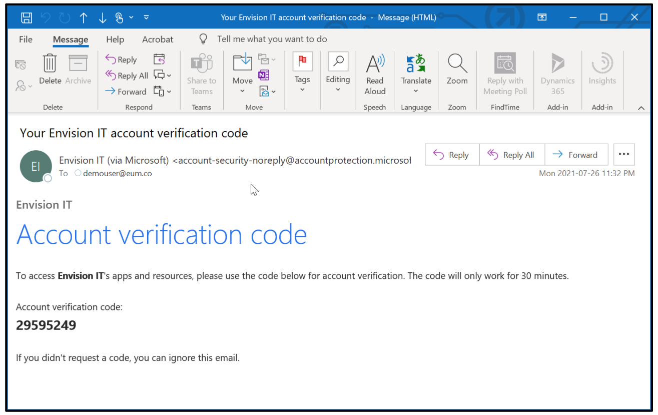
ExtranetUserManager

← demouser@eum.co

Enter code

We just sent a code to demouser@eum.co

Enter code



Your Envision IT account verification code

Envision IT (via Microsoft) <account-security-noreply@accountprotection.microsof

To demouser@eum.co

Mon 2021-07-26 11:32 PM

Envision IT

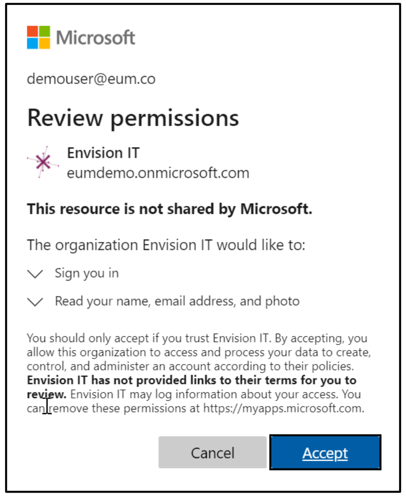
Account verification code

To access **Envision IT**'s apps and resources, please use the code below for account verification. The code will only work for 30 minutes.

Account verification code:

29595249

If you didn't request a code, you can ignore this email.



Microsoft

demouser@eum.co

Review permissions

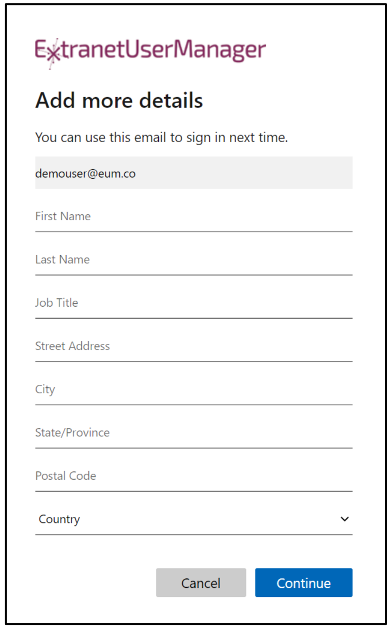
Envision IT
eumdemo.onmicrosoft.com

This resource is not shared by Microsoft.

The organization Envision IT would like to:

- Sign you in
- Read your name, email address, and photo

You should only accept if you trust Envision IT. By accepting, you allow this organization to access and process your data to create, control, and administer an account according to their policies. **Envision IT has not provided links to their terms for you to review.** Envision IT may log information about your access. You can remove these permissions at https://myapps.microsoft.com.



ExtranetUserManager

Add more details

You can use this email to sign in next time.

demouser@eum.co

First Name

Last Name

Job Title

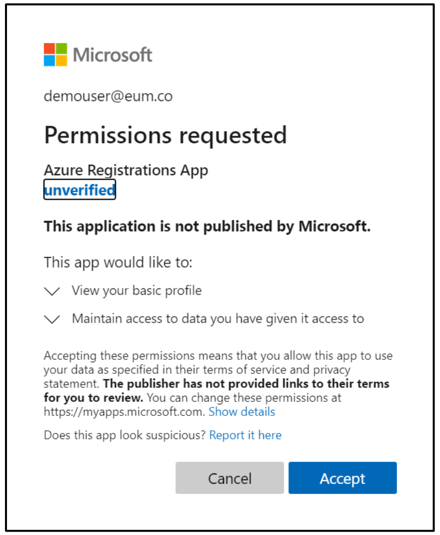
Street Address

City

State/Province

Postal Code

Country



Microsoft

demouser@eum.co

Permissions requested

Azure Registrations App
unverified

This application is not published by Microsoft.

This app would like to:

- View your basic profile
- Maintain access to data you have given it access to

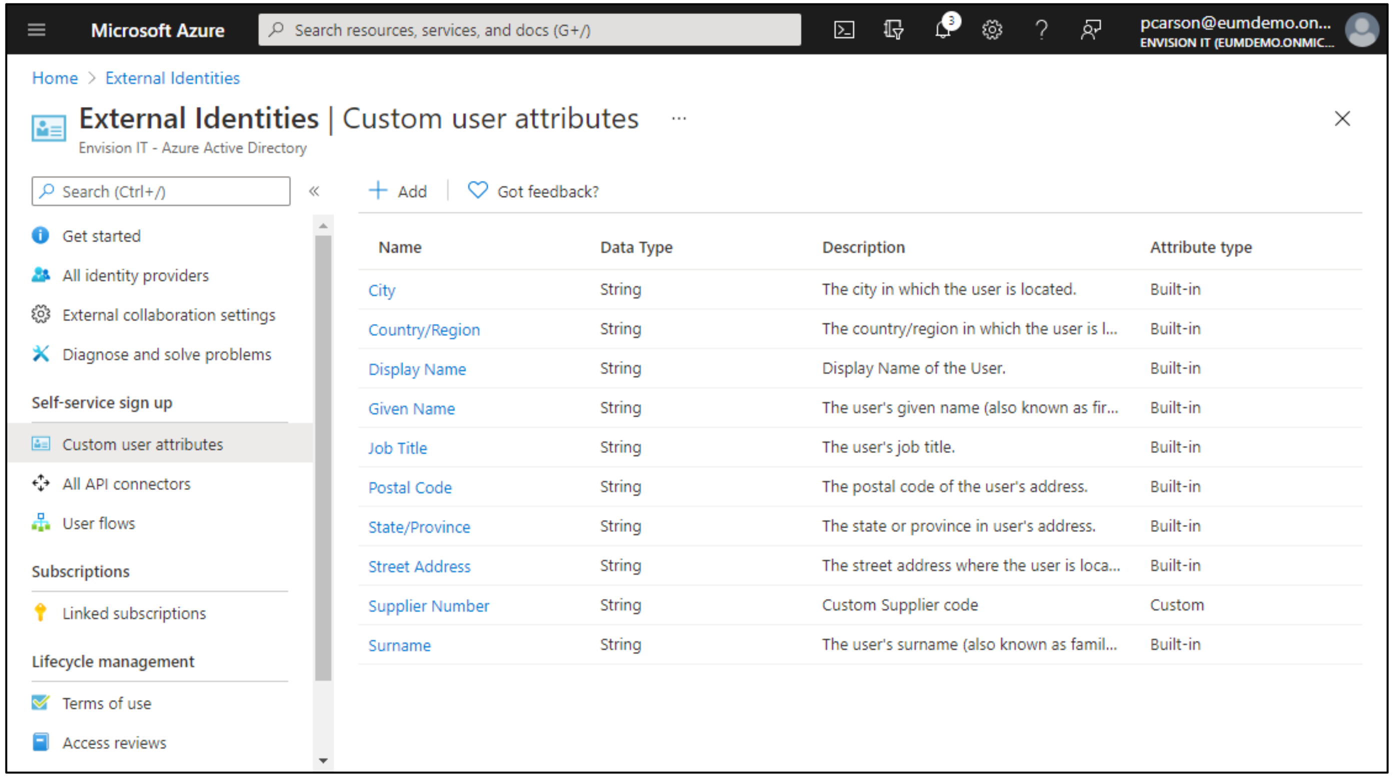
Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

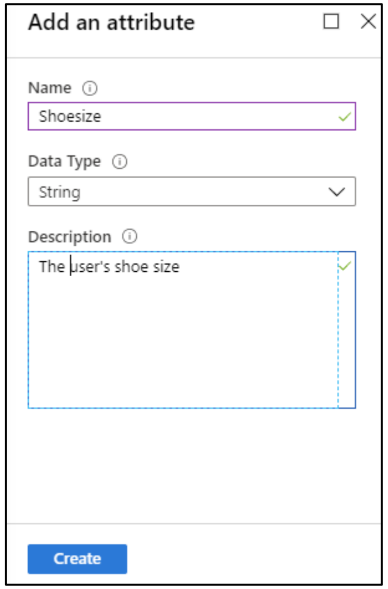
Self-Service User Sign-Up – Attributes

- **Choose what user information you require to provide access to Application**
- **Both built-in and custom attributes**
- **Steps to configure**
  - Define any custom attributes
  - Assign the attributes to a user flow
  - Define the page layout
  - Define any additional languages

Define the Attributes



Name	Data Type	Description	Attribute type
City	String	The city in which the user is located.	Built-in
Country/Region	String	The country/region in which the user is l...	Built-in
Display Name	String	Display Name of the User.	Built-in
Given Name	String	The user's given name (also known as fir...	Built-in
Job Title	String	The user's job title.	Built-in
Postal Code	String	The postal code of the user's address.	Built-in
State/Province	String	The state or province in user's address.	Built-in
Street Address	String	The street address where the user is loca...	Built-in
Supplier Number	String	Custom Supplier code	Custom
Surname	String	The user's surname (also known as famil...	Built-in

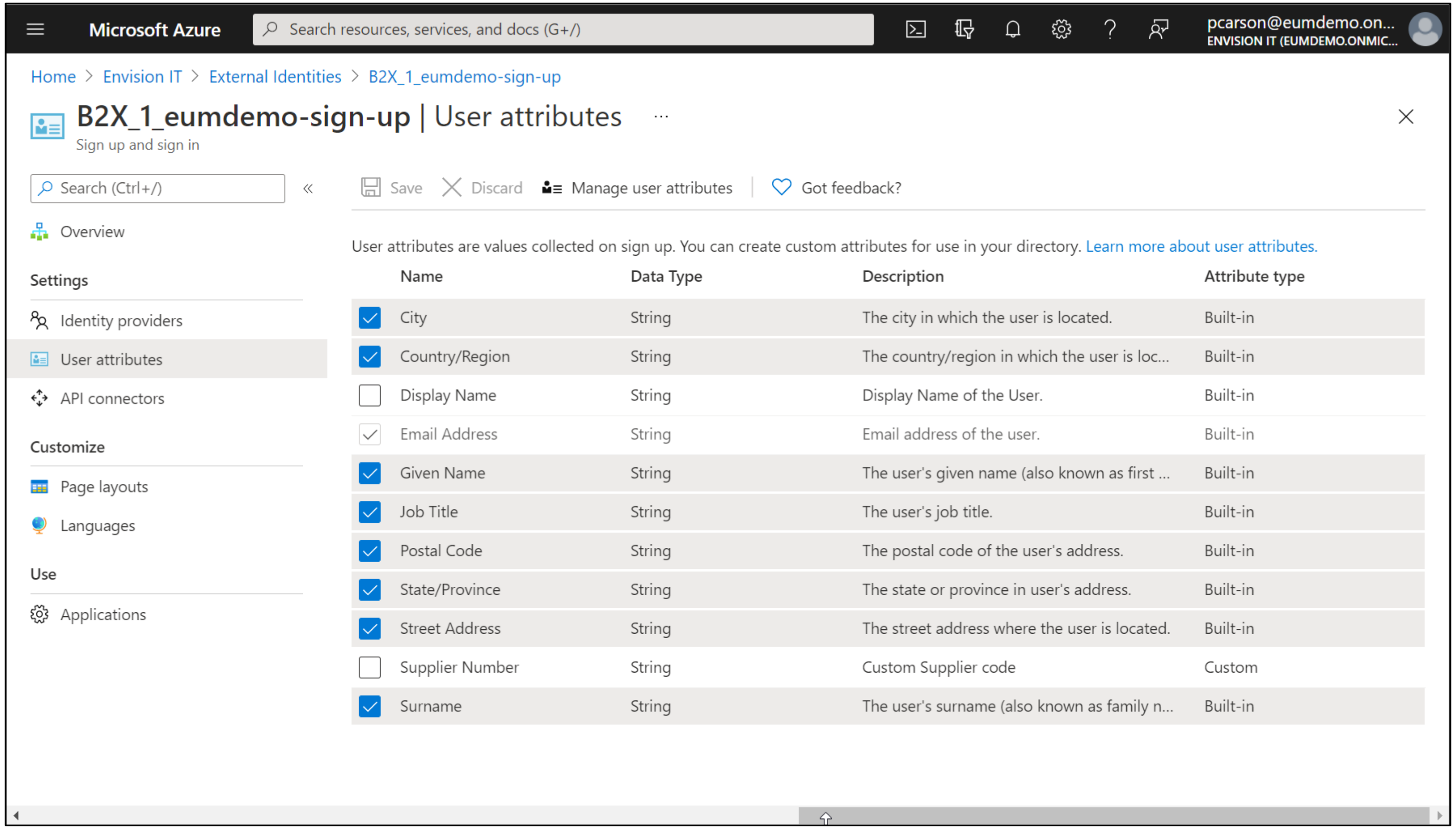


Name: Shoesize

Data Type: String

Description: The user's shoe size

Assign the Attributes to a User Flow



Microsoft Azure
Search resources, services, and docs (G+/)
pcarson@eumdemo.on...
ENVISION IT (EUMDEMO.ONMIC...
Home > Envision IT > External Identities > B2X_1_eumdemo-sign-up

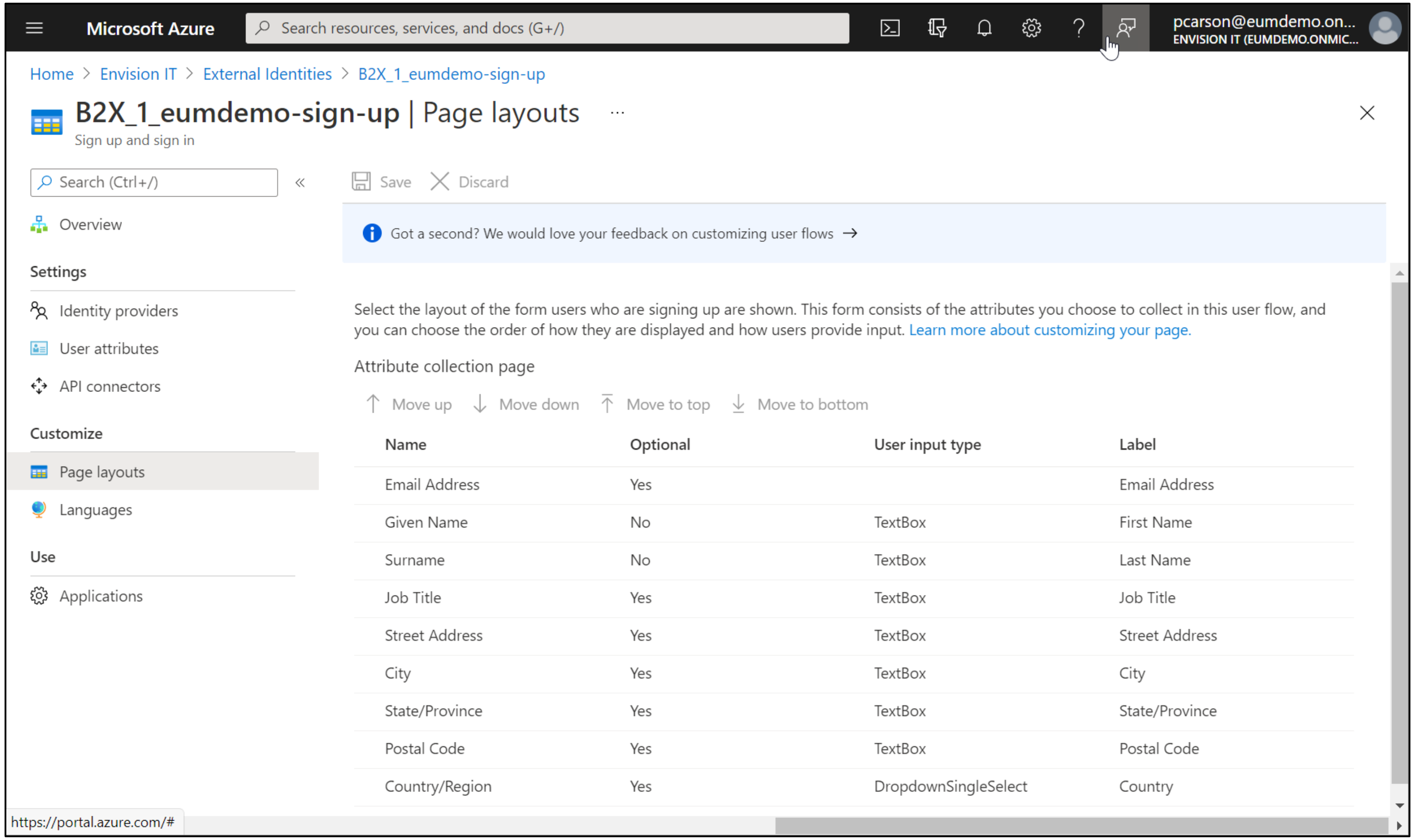
B2X_1_eumdemo-sign-up | User attributes

Sign up and sign in

User attributes are values collected on sign up. You can create custom attributes for use in your directory. Learn more about user attributes.

	Name	Data Type	Description	Attribute type
☑	City	String	The city in which the user is located.	Built-in
☑	Country/Region	String	The country/region in which the user is loc...	Built-in
☐	Display Name	String	Display Name of the User.	Built-in
✓	Email Address	String	Email address of the user.	Built-in
☑	Given Name	String	The user's given name (also known as first ...	Built-in
☑	Job Title	String	The user's job title.	Built-in
☑	Postal Code	String	The postal code of the user's address.	Built-in
☑	State/Province	String	The state or province in user's address.	Built-in
☑	Street Address	String	The street address where the user is located.	Built-in
☐	Supplier Number	String	Custom Supplier code	Custom
☑	Surname	String	The user's surname (also known as family n...	Built-in

Define the Page Layout



Microsoft Azure
Search resources, services, and docs (G+/)
pcarson@eumdemo.on...
ENVISION IT (EUMDEMO.ONMIC...
Home > Envision IT > External Identities > B2X_1_eumdemo-sign-up

B2X_1_eumdemo-sign-up | Page layouts

Sign up and sign in

Got a second? We would love your feedback on customizing user flows →

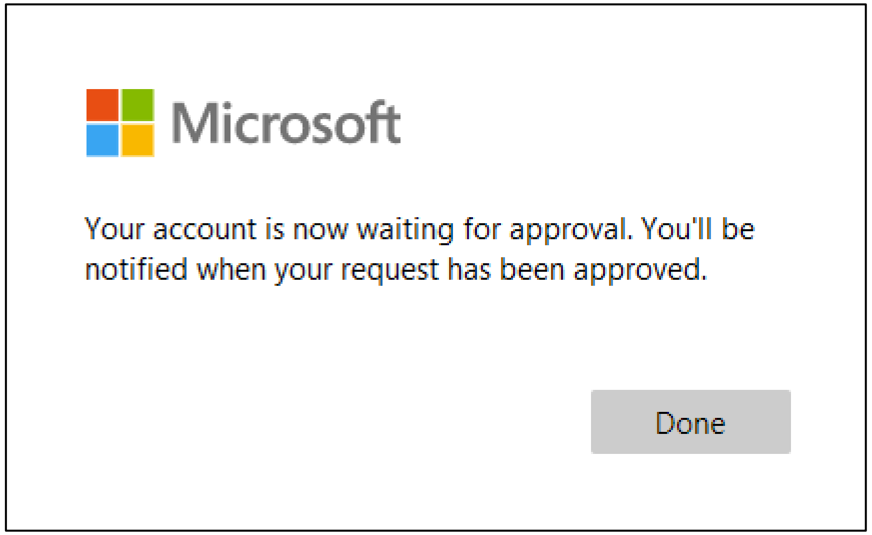
Select the layout of the form users who are signing up are shown. This form consists of the attributes you choose to collect in this user flow, and you can choose the order of how they are displayed and how users provide input. Learn more about customizing your page.

Attribute collection page

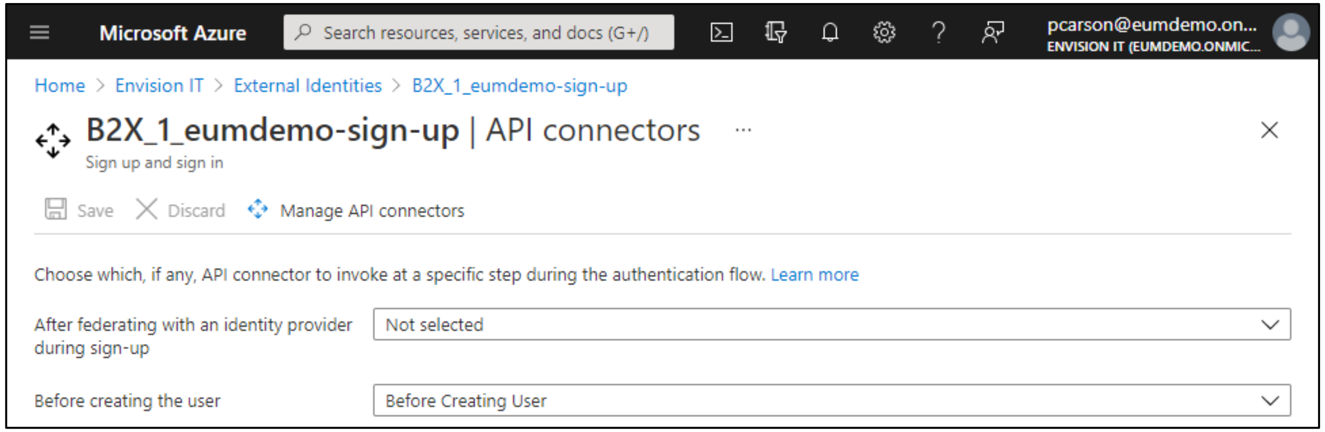
Name	Optional	User input type	Label
Email Address	Yes		Email Address
Given Name	No	TextBox	First Name
Surname	No	TextBox	Last Name
Job Title	Yes	TextBox	Job Title
Street Address	Yes	TextBox	Street Address
City	Yes	TextBox	City
State/Province	Yes	TextBox	State/Province
Postal Code	Yes	TextBox	Postal Code
Country/Region	Yes	DropdownSingleSelect	Country

Custom Approval Workflows

- **API connectors allow you to integrate custom approval workflows into the self-service sign up**



Your account is now waiting for approval. You'll be notified when your request has been approved.



Microsoft Azure
Search resources, services, and docs (G+/)
pcarson@eumdemo.on...
ENVISION IT (EUMDEMO.ONMIC...
Home > Envision IT > External Identities > B2X_1_eumdemo-sign-up
Save
Discard
Manage API connectors

B2X_1_eumdemo-sign-up | API connectors

Sign up and sign in

Choose which, if any, API connector to invoke at a specific step during the authentication flow. Learn more

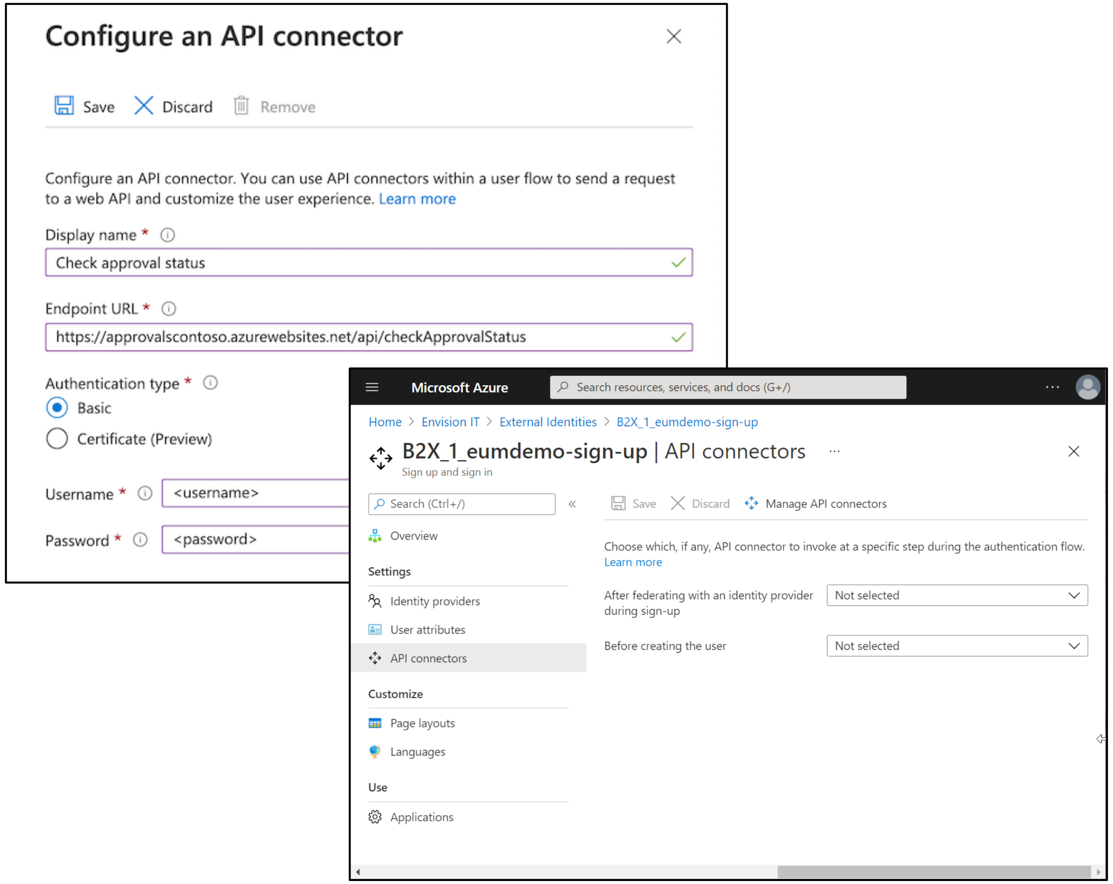
After federating with an identity provider during sign-up: Not selected

Before creating the user: Before Creating User

[Add custom approvals to self-service sign-up flows - Azure AD | Microsoft Docs]

Custom Approval Workflows

- **Preferred approach to building a full custom API is to use Logic Apps**
- **Use Azure API Management in front of Logic App to handle the security**
    - Basic auth or certificate



Configure an API connector

Configure an API connector. You can use API connectors within a user flow to send a request to a web API and customize the user experience. Learn more

Display name * : Check approval status

Endpoint URL * : https://approvalscontoso.azurewebsites.net/api/checkApprovalStatus

Authentication type *
● Basic
○ Certificate (Preview)

Username * : <username>

Password * : <password>

Microsoft Azure
Search resources, services, and docs (G+/)
Home > Envision IT > External Identities > B2X_1_eumdemo-sign-up

B2X_1_eumdemo-sign-up | API connectors

Sign up and sign in

Choose which, if any, API connector to invoke at a specific step during the authentication flow. Learn more

After federating with an identity provider during sign-up: Not selected

Before creating the user: Not selected

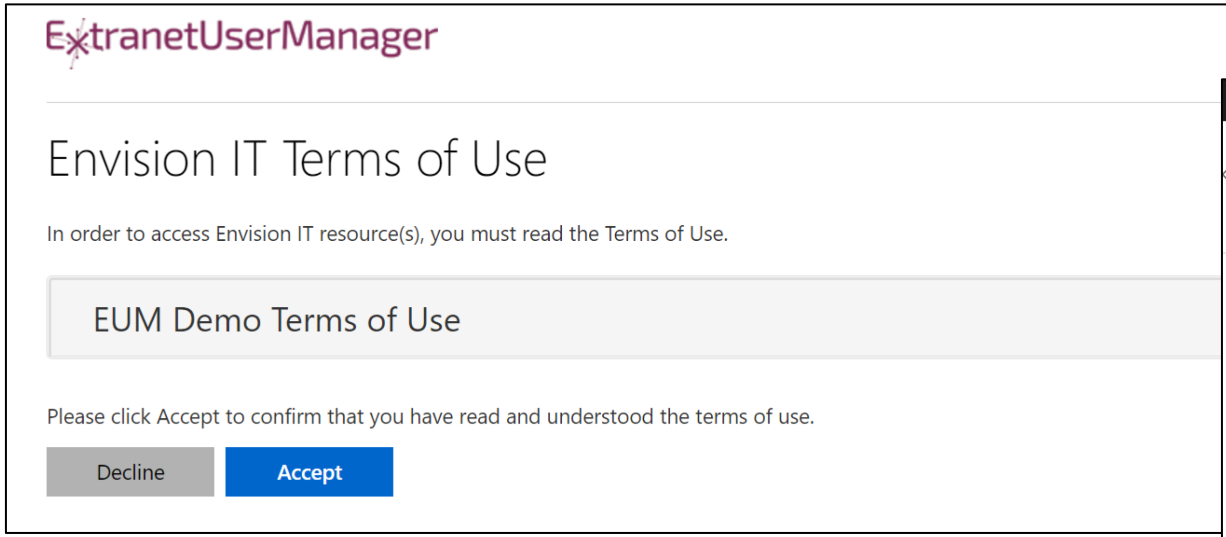
[Add custom approvals to self-service sign-up flows - Azure AD | Microsoft Docs]

Demo

Terms of Use

https://azureregistration.azurewebsites.net/

External Identities Terms of Use



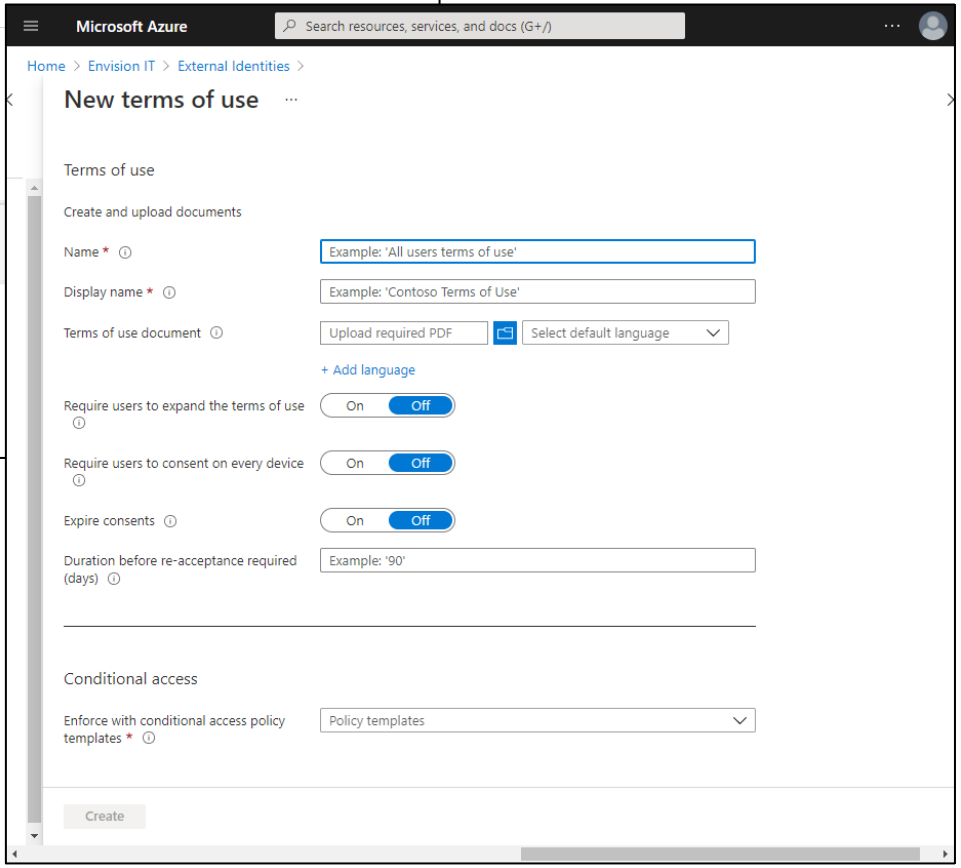
ExtranetUserManager

Envision IT Terms of Use

In order to access Envision IT resource(s), you must read the Terms of Use.

EUM Demo Terms of Use

Please click Accept to confirm that you have read and understood the terms of use.



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Envision IT > External Identities >

New terms of use

Terms of use

Create and upload documents

Name * Example: 'All users terms of use'

Display name * Example: 'Contoso Terms of Use'

Terms of use document Upload required PDF Select default language

+ Add language

Require users to expand the terms of use: On [✓ Off]

Require users to consent on every device: On [✓ Off]

Expire consents: On [✓ Off]

Duration before re-acceptance required (days) Example: '90'

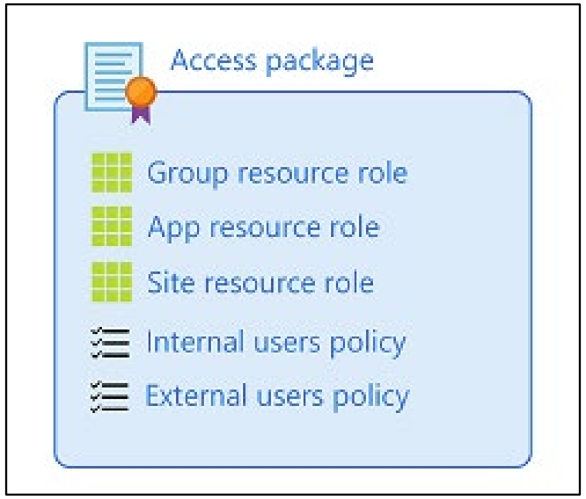
Conditional access

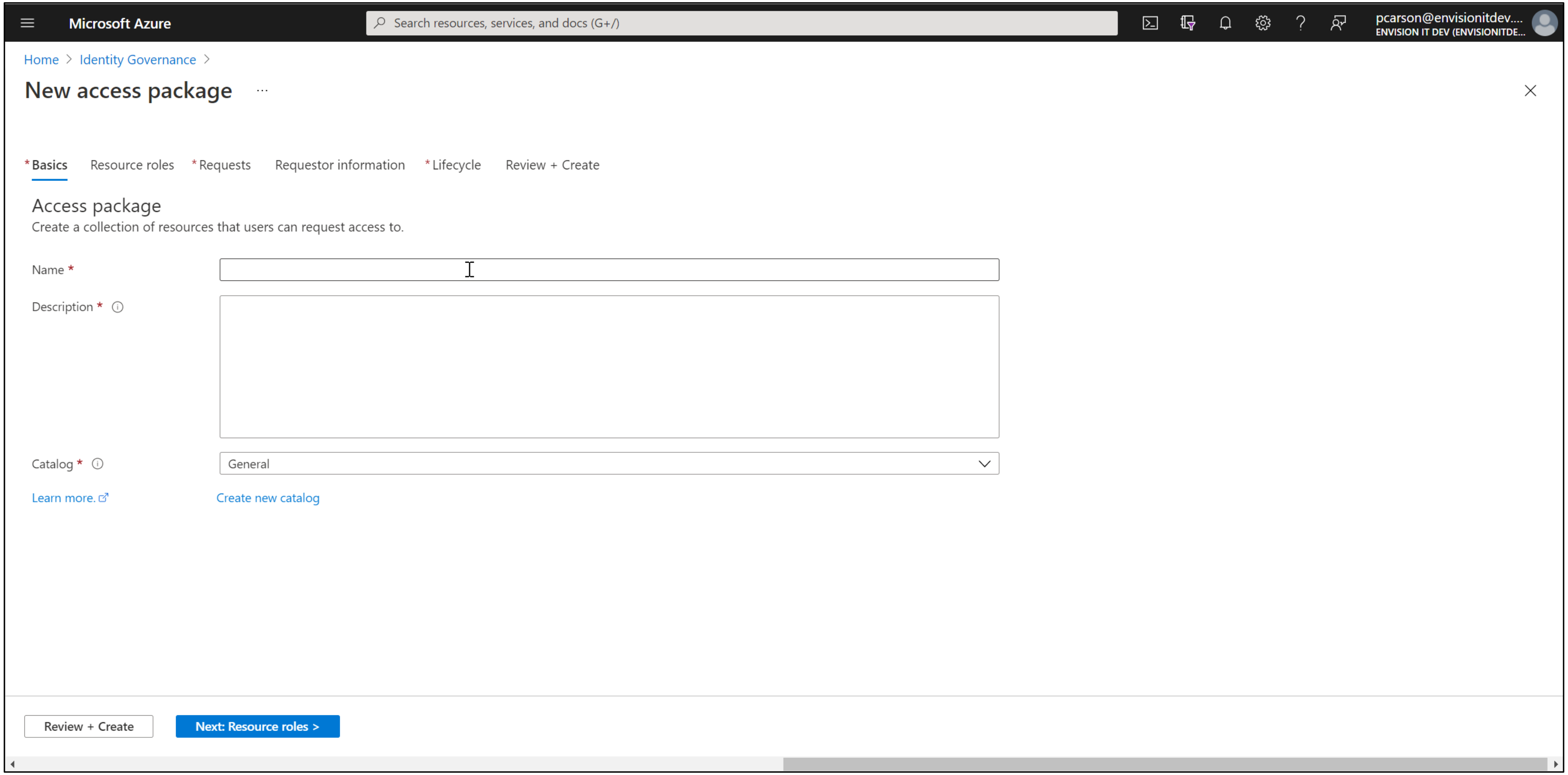
Enforce with conditional access policy templates * Policy templates

- **Also need to define a conditional access policy to enforce the Terms of Use**

Azure Entitlement Management

- **Delegate to non-administrators the ability to create access packages**
- **Access package is a bundle of resources a user needs access to**
- **Can consist of:**
  - Membership of Azure AD security groups, Microsoft 365 Groups and Teams
  - Assignment of Azure AD applications
    - SaaS and custom integrated apps supporting federation/SSO
  - Membership of SharePoint Online sites
- **Policies define the rules for the access package**
- **Within each policy, admin defines:**
  - Users or organizations who can request access
  - Approval process and who can approve/deny access
  - Duration of users access





New access package

Access package

Create a collection of resources that users can request access to.

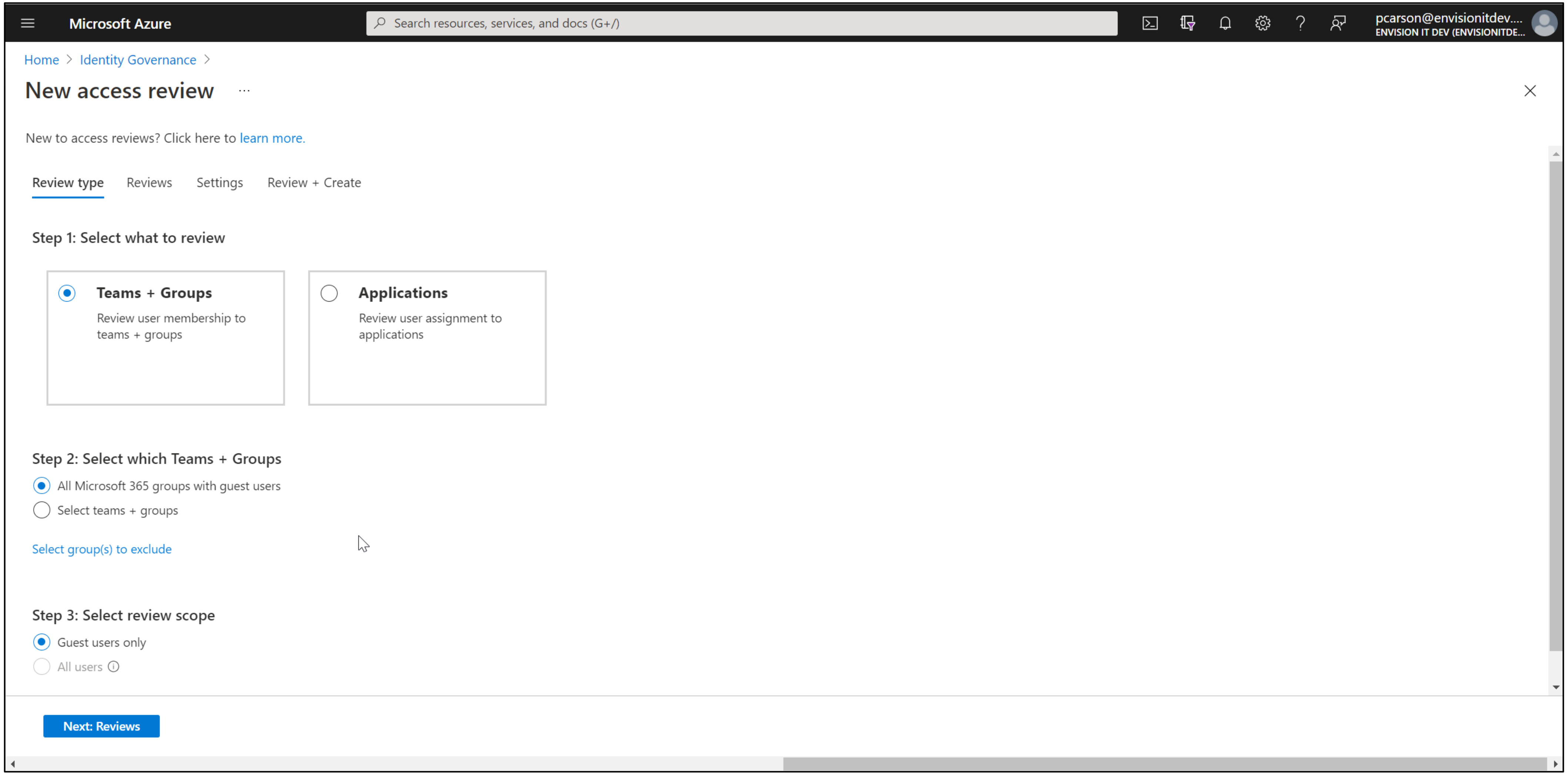
Name *

Description *

Catalog * General

Learn more.

Create new catalog



Microsoft Azure
Search resources, services, and docs (G+/)
pcarson@envisionitdev....
ENVISION IT DEV (ENVISIONITDE...
Home > Identity Governance >

New access review

New to access reviews? Click here to learn more.

Review type
Reviews
Settings
Review + Create

Step 1: Select what to review

● **Teams + Groups**
Review user membership to teams + groups

○ **Applications**
Review user assignment to applications

Step 2: Select which Teams + Groups

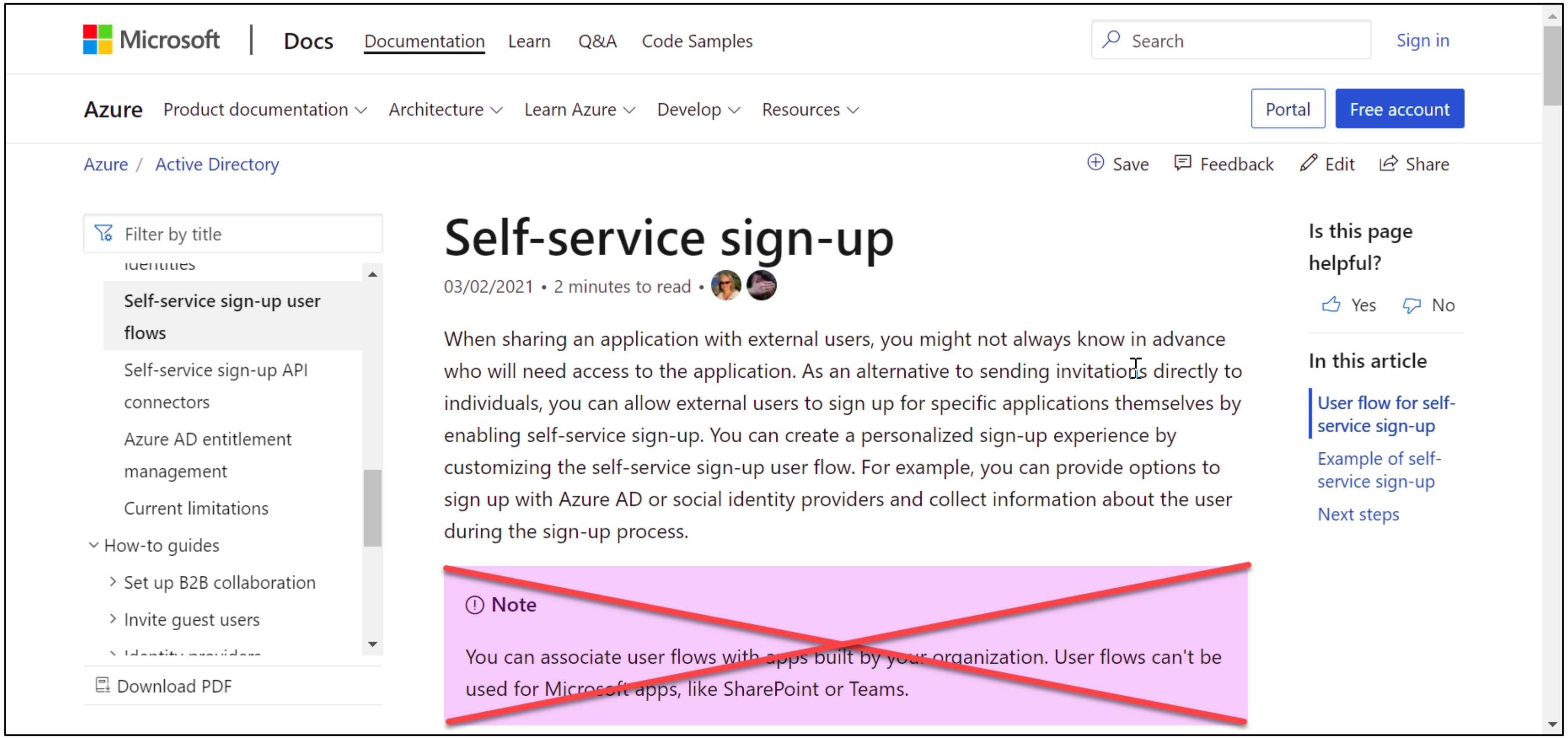
● All Microsoft 365 groups with guest users
○ Select teams + groups

Select group(s) to exclude

Step 3: Select review scope

● Guest users only
○ All users

User Flows with SharePoint or Teams



Self-service sign-up

03/02/2021 • 2 minutes to read •

When sharing an application with external users, you might not always know in advance who will need access to the application. As an alternative to sending invitations directly to individuals, you can allow external users to sign up for specific applications themselves by enabling self-service sign-up. You can create a personalized sign-up experience by customizing the self-service sign-up user flow. For example, you can provide options to sign up with Azure AD or social identity providers and collect information about the user during the sign-up process.

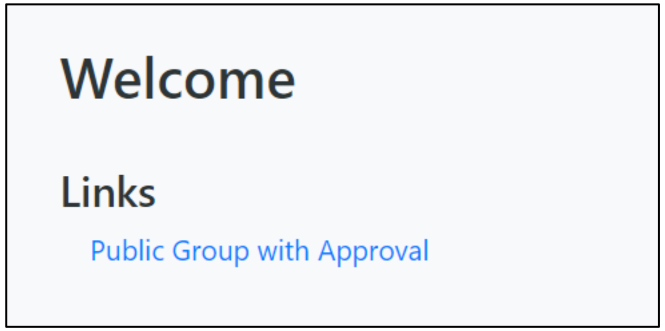
~~ⓘ Note~~

~~You can associate user flows with apps built by your organization. User flows can't be used for Microsoft apps, like SharePoint or Teams.~~

[Self-service sign-up for External Identities - Azure AD | Microsoft Docs]

Custom Portal Page to Access Package

https://azureregistration.azurewebsites.net/

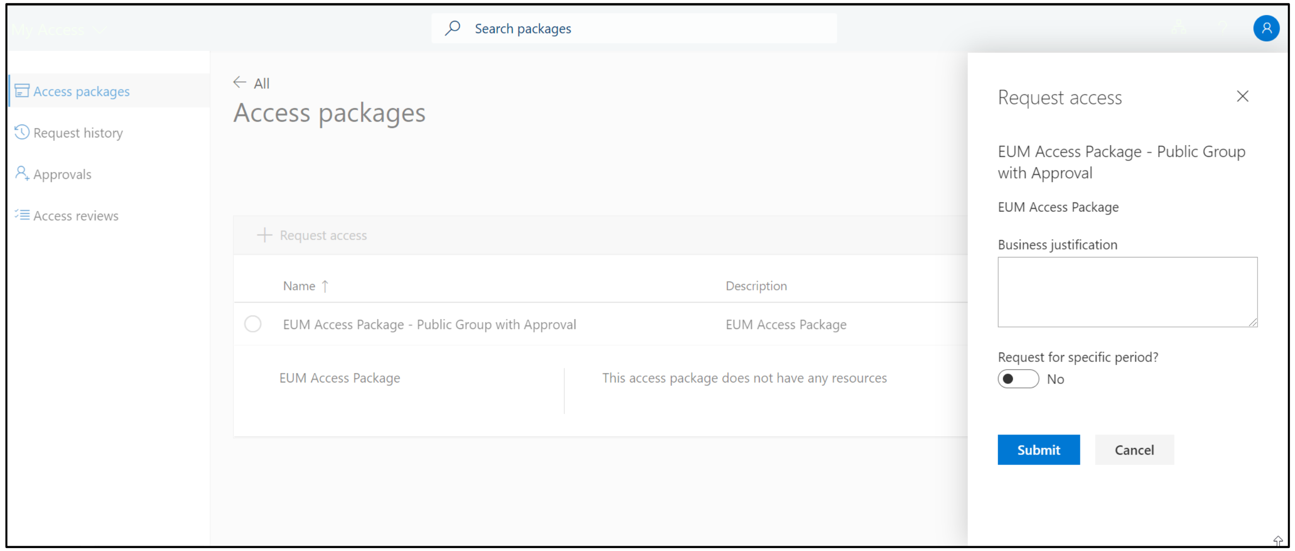


Welcome

Links

Public Group with Approval

- Azure App Service
- Registered as an Azure AD Application
- Associated with the External Identity User Flow



Access packages

＋ Request access

Name ↑	Description
○ EUM Access Package - Public Group with Approval	EUM Access Package

EUM Access Package | This access package does not have any resources

Request access ✕

EUM Access Package - Public Group with Approval

EUM Access Package

Business justification

Request for specific period? ● No

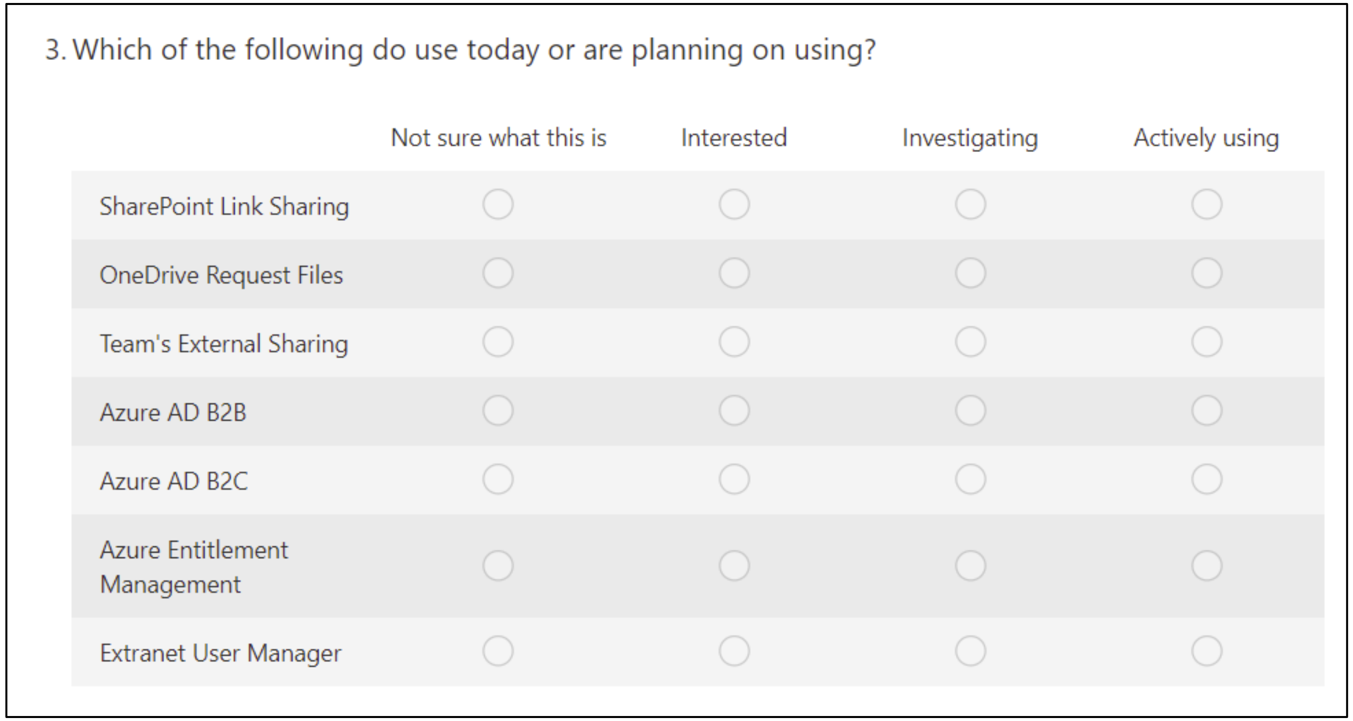
Submit Cancel

Demo

Entitlement Package

https://azureregistration.azurewebsites.net/

Microsoft Forms Poll



3. Which of the following do use today or are planning on using?

	Not sure what this is	Interested	Investigating	Actively using
SharePoint Link Sharing	○	○	○	○
OneDrive Request Files	○	○	○	○
Team's External Sharing	○	○	○	○
Azure AD B2B	○	○	○	○
Azure AD B2C	○	○	○	○
Azure Entitlement Management	○	○	○	○
Extranet User Manager	○	○	○	○

https://bit.ly/2ULk2VD

Upcoming Webinars

Taking a break for August and Early September... You should too!

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

Want to join the Envision IT / Extranet User Manager Team?

- Currently hiring for Content Marketing Specialist role
- Careers | Envision IT for more details!

Thank you!

Questions?