



CLOUD IDENTITY SUMMIT '20

Identity Management Track

"Azure AD B2B: Notes from the Field"

Stephan Wälde (glueckkanja-gab)

Community Event by

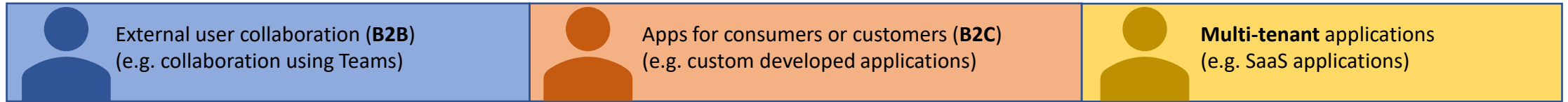


BONN

sponsored by



External Identities Overview



B2B Overview

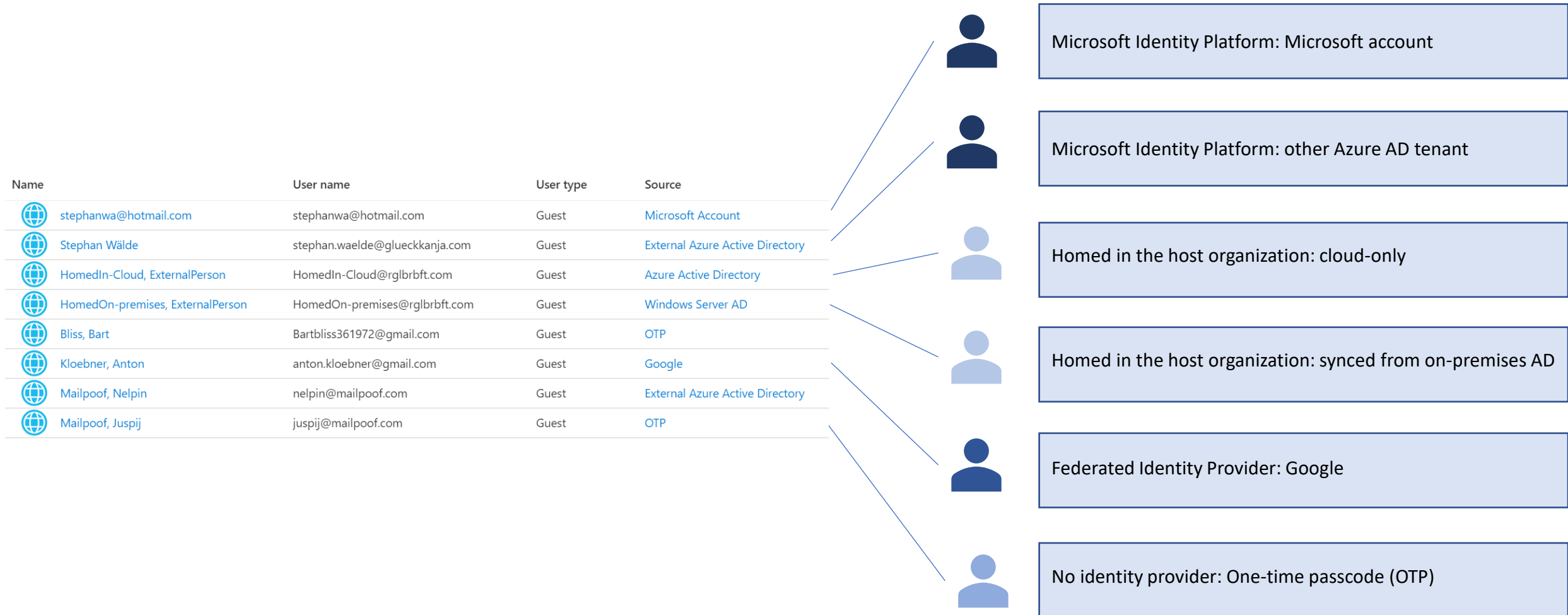
Microsoft Identity Platform: external Azure AD tenant or Microsoft account

Federated Identity Provider: Google, Facebook, Direct Federation (SAML 2.0 or WS-Fed)

No identity provider: One-time passcode (OTP)

Homed in the host organization: either synced from on-premises AD or cloud-only

External Identities Overview: B2B Guest Users



Adding B2B Users

By invitation

- Add guest user in the Azure AD portal (single invite or bulk invite)
- Add guest user using PowerShell (single invite or bulk invite)
- Redemption through the invitation Email: includes consent experience
- Redemption through a direct link to an app or portal: includes consent experience

Who can invite? This is customizable.

- By default, all users and guests in your directory can invite guests even if they're not assigned to an admin role.
- Azure AD role: Guest inviter

By script or synchronization

- Script only recommended for two tenants
- Synchronization most complex, Mesh or „Global Tenant“









By Self-service sign-up (Preview)

- You can create user flows for apps that are built by your organization.
- Only for Azure AD, Google and Facebook accounts

By account creation

- homed in the host organization

External Identities Overview

Name	User name	User type	Source
 stephanwa@hotmail.com	stephanwa@hotmail.com	Guest	Microsoft Account
 Stephan Wälde	stephan.waelde@glueckkanja.com	Guest	External Azure Active Directory
 HomedIn-Cloud, ExternalPerson	HomedIn-Cloud@rglbrbft.com	Guest	Azure Active Directory
 HomedOn-premises, ExternalPerson	HomedOn-premises@rglbrbft.com	Guest	Windows Server AD
 Bliss, Bart	Bartbliss361972@gmail.com	Guest	OTP
 Kloebner, Anton	anton.kloebner@gmail.com	Guest	Google
 Mailpoof, Nelpin	nelpin@mailpoof.com	Guest	External Azure Active Directory
 Mailpoof, Juspilj	juspilj@mailpoof.com	Guest	OTP

Home Tenant Conditional Access Bypass

Terminology

- Home Tenant, Invited Tenant: tenant that contains the regular user account object
- Resource Tenant, Inviting Tenant, Host organization: tenant that contains the guest account object and the resource(s)



abby@home-tenant.com

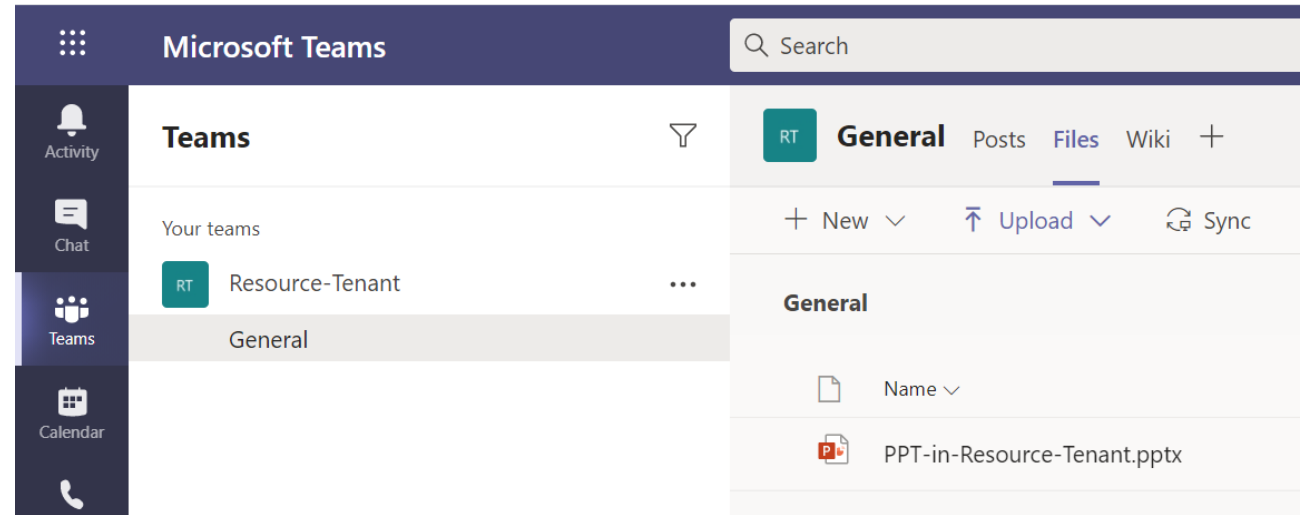
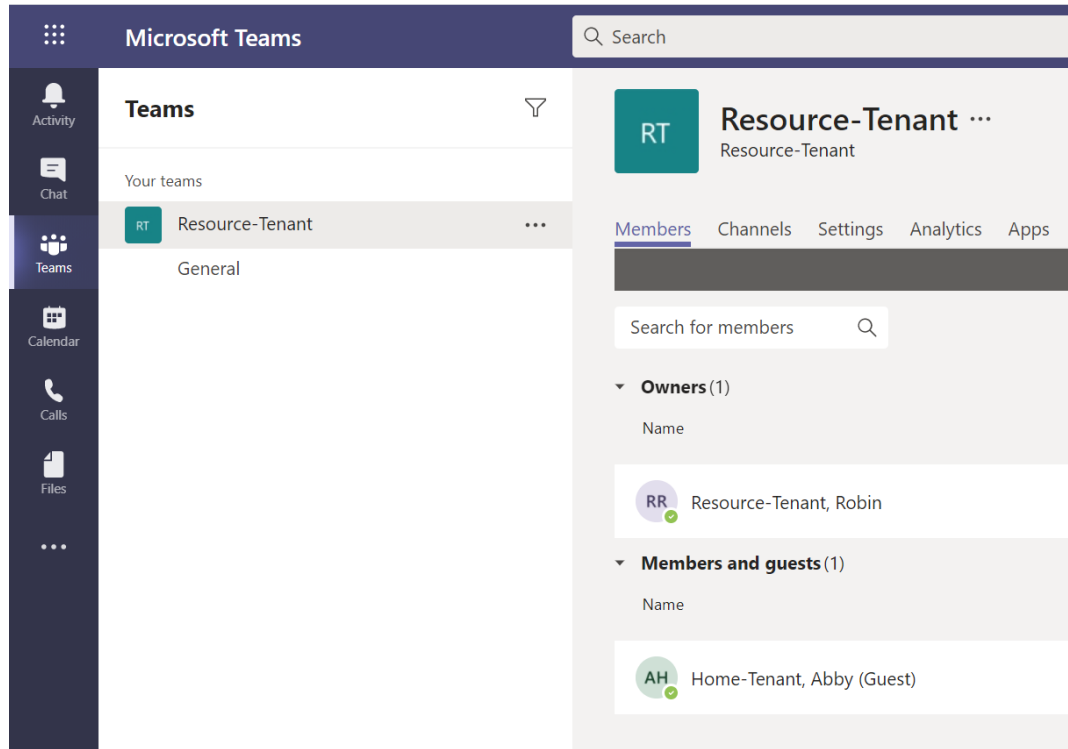


abby_home-tenant.com#EXT#@resourcetenantcom.onmicrosoft.com

Session sign-in navigation

- First sign in to Home Tenant, then sign in to Resource Tenant
- Sign in to Resource Tenant directly
 - Azure CLI: `az login --allow-no-subscriptions --tenant 9cbada80-ca8c-43b1-8fb2-492cf58bccc9`
 - Powershell: `Connect-AzureAD -TenantId 9cbada80-ca8c-43b1-8fb2-492cf58bccc9`
 - Powershell: `Connect-AzAccount -TenantId 9cbada80-ca8c-43b1-8fb2-492cf58bccc9`
 - Browser: <https://portal.azure.com/9cbada80-ca8c-43b1-8fb2-492cf58bccc9>

Home Tenant Conditional Access Bypass



Sign in to Resource Tenant directly (SharePoint)

<https://resourcetenantcom.sharepoint.com/sites/Resource-Tenant/Shared%20Documents/General/PPT-in-Resource-Tenant.pptx?web=1>

Tenant name

Teams name

Channel name

File name

Open in Browser

Home Tenant Conditional Access Bypass

Home > Home-Tenant > Users > Home-Tenant, Abby

Home-Tenant, Abby | Sign-ins

User

» 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 : 10/8/2020 to 10/8/2020 Show dates as : Local User starts with 5cd58c8c-f85c-4b94-b8b0-b894cb0b0907 Add filters

User sign-ins (interactive) User sign-ins (non-interactive)

Date	↑↓	Request ID	User	↑↓	Application	↑↓	Status	IP ...	Location	Conditional access	Authentication requirement
10/8/2020, 8:13:56 PM		c1f6f55e-7b2d-4d61-8f23-27239194a700	Home-Tenant, Abby		Microsoft Office Web Apps Service		Success	80.72....	Oberursel (Taurus),...	Not Applied	Multi-factor authentication
10/8/2020, 8:13:49 PM		6de0d3ec-b169-45ff-9117-c6efe981aa00	Home-Tenant, Abby		Office 365 SharePoint Online		Success	80.72....	Oberursel (Taurus),...	Not Applied	Multi-factor authentication

Home > Resource-Tenant > Users > Home-Tenant, Abby

Home-Tenant, Abby | Sign-ins

User

» 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 : 10/8/2020 to 10/8/2020 Show dates as : Local User starts with 5f2249d5-434d-43c6-b1bb-7eb801912b76 Add filters

User sign-ins (interactive) User sign-ins (non-interactive)

Date	↑↓	Request ID	User	↑↓	Application	↑↓	St...	I...	Locati...	Conditional access	Authentication requirement
10/8/2020, 8:13:56 PM		c1f6f55e-7b2d-4d61-8f23-27239194a700	Home-Tenant, Abby		Microsoft Office Web Apps Service		Success	8...	Oberursel...	Success	Multi-factor authentication
10/8/2020, 8:13:49 PM		6de0d3ec-b169-45ff-9117-c6efe981aa00	Home-Tenant, Abby		Office 365 SharePoint Online		Success	8...	Oberursel...	Success	Multi-factor authentication

Azure MFA for B2B Guests

Choose between ~~the good~~, the bad and the ugly

With Azure MFA for B2B Guests in the Resource Tenant

- Azure MFA the only viable option for additional factor for B2B guests
- Officially recommended by Microsoft
- There might be scenarios with double MFA
- Confusing end user experience
 - Why do I have to register again for MFA?
 - Why am I getting an MFA prompt? Which tenant is asking for MFA?
 - How do I navigate to change my MFA settings in the other tenant where I am the B2B guest?



Without Azure MFA for B2B Guests in the Resource Tenant

- Sign in to Resource Tenant directly: possible with password as a single factor



What you can see as a guest in the Resource Tenant...

What you can see as a guest (independent of guest user access restrictions)

- Some tenant details like custom domains
- Properties of your own B2B guest account

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)

```
PS C:\> (Get-AzureADTenantDetail).Verifieddomains | ft name,_default

Name                                     _Default
----
resource-tenant.onmicrosoft.com         True
resource-tenant.com                     False
```

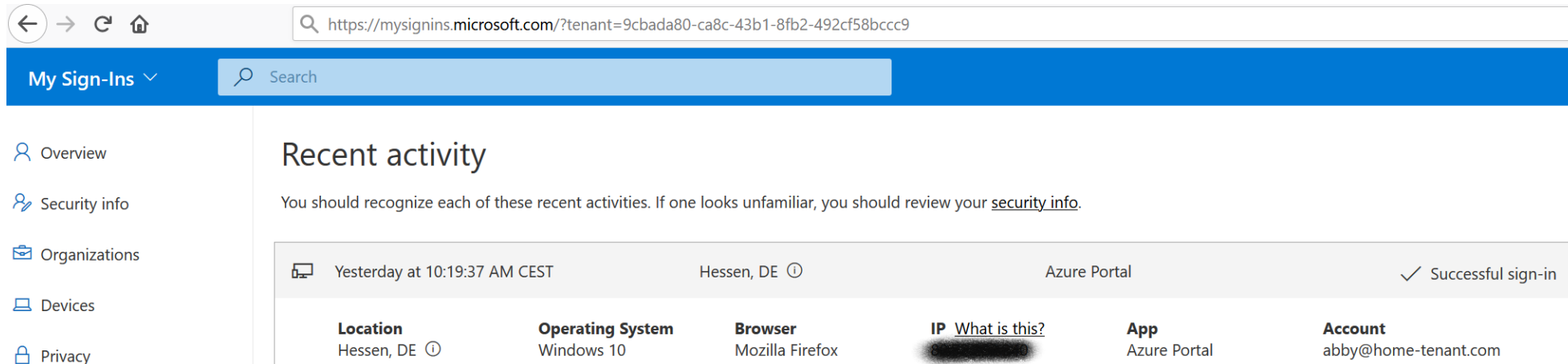
```
PS C:\> Get-AzureADUser -ObjectId 5f2249d5-434d-43c6-b1bb-7eb801912b76 | fl obj*,cre*,displ*,mail*,proxy*,user*

ObjectId       : 5f2249d5-434d-43c6-b1bb-7eb801912b76
ObjectType     : User
CreationType   : Invitation
DisplayName    : Home-Tenant, Abby
Mail           : abby@home-tenant.com
MailNickName   : abby_home-tenant.com#EXT#
ProxyAddresses : {SMTP:abby@home-tenant.com}
UserPrincipalName : abby_home-tenant.com#EXT#@resource-tenant.onmicrosoft.com
UserState      : Accepted
UserStateChangedOn : 2020-10-04T09:57:55Z
UserType       : Guest
```

What you can see as a guest in the Resource Tenant...

What you can see as a guest (independent of guest user access restrictions)

- Your own guest sign-ins to the Resource tenant
 - Browser: <https://mysignins.microsoft.com/?tenant=9cbada80-ca8c-43b1-8fb2-492cf58bccc9>
 - Graph API: [https://graph.microsoft.com/beta/auditLogs/signIns?api-version=beta&\\$filter=\(userId%20eq%20%275f2249d5-434d-43c6-b1bb-7eb801912b76%27\)](https://graph.microsoft.com/beta/auditLogs/signIns?api-version=beta&$filter=(userId%20eq%20%275f2249d5-434d-43c6-b1bb-7eb801912b76%27))



The screenshot shows the 'My Sign-Ins' page in a web browser. The address bar displays the URL: <https://mysignins.microsoft.com/?tenant=9cbada80-ca8c-43b1-8fb2-492cf58bccc9>. The page has a blue header with 'My Sign-Ins' and a search bar. On the left, there is a navigation menu with links to Overview, Security info, Organizations, Devices, and Privacy. The main content area is titled 'Recent activity' and includes a warning: 'You should recognize each of these recent activities. If one looks unfamiliar, you should review your [security info](#).' Below this, a table displays a recent sign-in event.

Location	Operating System	Browser	IP	App	Account
Hessen, DE	Windows 10	Mozilla Firefox	[REDACTED]	Azure Portal	abby@home-tenant.com

Additional details from the activity row: Yesterday at 10:19:37 AM CEST, Hessen, DE, Azure Portal, Successful sign-in.



A bit about B2B Guest Browser Sessions

Video

SharePoint Cookies:

- rtfa
- FedAuth

Web Application Open Platform Interface (WOPI) protocol authentication:

```
{
  "typ": "JWT",
  "alg": "RS256",
  "x5t": "xX1T0IJx2VBTBEyQLtkE8V6fHpg"
}.{
  "aud": "wopi/resourcetenantcom.sharepoint.com@9cbada80-ca8c-43b1-8fb2-492cf58bccc9",
  "iss": "00000003-0000-0ff1-ce00-000000000000@90140122-8516-11e1-8eff-49304924019b",
  "nbf": "1602956899",
  "exp": "1602992899",
  "nameid": "0#.f|membership|david_home-tenant.com#ext#@resourcetenantcom.onmicrosoft.com",
  "nii": "microsoft.sharepoint",
  "isuser": "true",
  "cachekey": "0h.f|membership|10032000ee905edc@live.com",
  "isloopback": "True",
  "appctx": "f1b29a9510df401e9419a9c7ee8ad9a6;CXisWLlKHVFrq2bC/aDKXSXSlNw=;Default;;1B03C431AEF;True;;0;a09d849f-d0da-2000-7274-07e1954fdcf7"
}.[Signature]
```

And now
for something
completely different...



UPN and Email Address

Email only, no UPN: helen@home-tenant.com

```
DisplayName      UserPrincipalName      ProxyAddresses
-----
Home-Tenant, Helen helensemployeenumber@home-tenant.com {smtp:helensemployeenumber@home-tenant.com, SMTP:helen@home-tenant.com}
```

```
PS C:\> New-AzureADMSInvitation -InvitedUserEmailAddress helen@home-tenant.com -SendInvitationMessage $False
-InvokeRedirectUrl "https://myapps.microsoft.com/?tenantid=9cbada80-ca8c-43b1-8fb2-492cf58bccc9"
```

Before redemption

```
DisplayName      : helen
GivenName        :
Surname          :
Mail             : helen@home-tenant.com
MailNickName     : helen_home-tenant.com#EXT#
OtherMails       : {helen@home-tenant.com}
ProxyAddresses   : {SMTP:helen@home-tenant.com}
UserPrincipalName : helen_home-tenant.com#EXT#@resourcetenantcom.onmicrosoft.com
UserState        : PendingAcceptance
UserType         : Guest
```

After redemption

```
DisplayName      : Home-Tenant, Helen
GivenName        :
Surname          :
Mail             : helen@home-tenant.com
MailNickName     : helen_home-tenant.com#EXT#
OtherMails       : {helensemployeenumber@home-tenant.com, helen@home-tenant.com}
ProxyAddresses   : {SMTP:helen@home-tenant.com}
UserPrincipalName : helen_home-tenant.com#EXT#@resourcetenantcom.onmicrosoft.com
UserState        : Accepted
UserType         : Guest
```

UPN and Email Address

UPN only, no Email: david@home-tenant.com

DisplayName	UserPrincipalName	Mail	ProxyAddresses
-----	-----	----	-----
Home-Tenant, David	david@home-tenant.com		{}

```
PS C:\> New-AzureADMSInvitation -InvitedUserEmailAddress david@home-tenant.com -SendInvitationMessage $False  
-InviteRedirectUrl "https://myapps.microsoft.com/?tenantid=9cbada80-ca8c-43b1-8fb2-492cf58bccc9"
```

Before redemption

DisplayName	: david
GivenName	:
Surname	:
Mail	: david@home-tenant.com
MailNickName	: david_home-tenant.com#EXT#
OtherMails	: {david@home-tenant.com}
ProxyAddresses	: {SMTP:david@home-tenant.com}
UserPrincipalName	: david_home-tenant.com#EXT#@resourcetenantcom.onmicrosoft.com
UserState	: PendingAcceptance
UserType	: Guest

After redemption

DisplayName	: Home-Tenant, David
GivenName	:
Surname	:
Mail	: david@home-tenant.com
MailNickName	: david_home-tenant.com#EXT#
OtherMails	: {david@home-tenant.com}
ProxyAddresses	: {SMTP:david@home-tenant.com}
UserPrincipalName	: david_home-tenant.com#EXT#@resourcetenantcom.onmicrosoft.com
UserState	: Accepted
UserType	: Guest


UPN and Email Address

UPN, Email on different objects: fredsupnandgracesemail@home-tenant.com

DisplayName	UserPrincipalName	Mail
Home-Tenant, Fred	fredsupnandgracesemail@home-tenant.com	
Home-Tenant, Grace	grace@home-tenant.com	fredsupnandgracesemail@home-tenant.com


```
PS C:\> New-AzureADMSInvitation -InvitedUserEmailAddress fredsupnandgracesemail@home-tenant.com -SendInvitationMessage $true  
-InviteRedirectUrl "https://myapps.microsoft.com/?tenantid=9cbada80-ca8c-43b1-8fb2-492cf58bccc9"
```

DisplayName	: fredsupnandgracesemail
GivenName	:
Surname	:
Mail	: fredsupnandgracesemail@home-tenant.com
MailNickName	: fredsupnandgracesemail_home-tenant.com#EXT#
OtherMails	: {fredsupnandgracesemail@home-tenant.com}
ProxyAddresses	: {SMTP:fredsupnandgracesemail@home-tenant.com}
UserPrincipalName	: fredsupnandgracesemail_home-tenant.com#EXT#@resourcetenantcom.onmicrosoft.com
UserState	: PendingAcceptance
UserType	: Guest

 Home

grace@home-tenant.com

Review permissions



Resource-Tenant resourcetenantcom.onmicrosoft.com

This resource is not shared by Microsoft.

The organization Resource-Tenant would like to:

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

DisplayName	: Home-Tenant, Grace
GivenName	:
Surname	:
Mail	: fredsupnandgracesemail@home-tenant.com
MailNickName	: fredsupnandgracesemail_home-tenant.com#EXT#
OtherMails	: {grace@home-tenant.com, fredsupnandgracesemail@home-tenant.com}
ProxyAddresses	: {SMTP:fredsupnandgracesemail@home-tenant.com}
UserPrincipalName	: fredsupnandgracesemail_home-tenant.com#EXT#@resourcetenantcom.onmicrosoft.com
UserState	: Accepted
UserType	: Guest



CLOUD IDENTITY SUMMIT '20

Your Feedback is important!

<http://feedback.identitysummit.cloud/>

Thanks to our sponsors!

