POWER PLATFORM COMMUNITY CONFERENCE

“Copilot, Reset My Password!”

Building a secure self-service IVR with Copilot Studio & Entra ID

Peter Ruiter

MVP, Principal Solution Architect
Microsoft CX CTO, Capgemini

Capgemini

Introducing the Power Platform Community Conference App

STAY IN THE KNOW

- Get access to live event updates & notifications
- Build a personalized agenda
- Connect with other attendees
- Network with Sponsor & Exhibitors
- Join meet-ups
- Access event documents

Event Invitation Code:
5thAnnual2026

Session Feedback Surveys

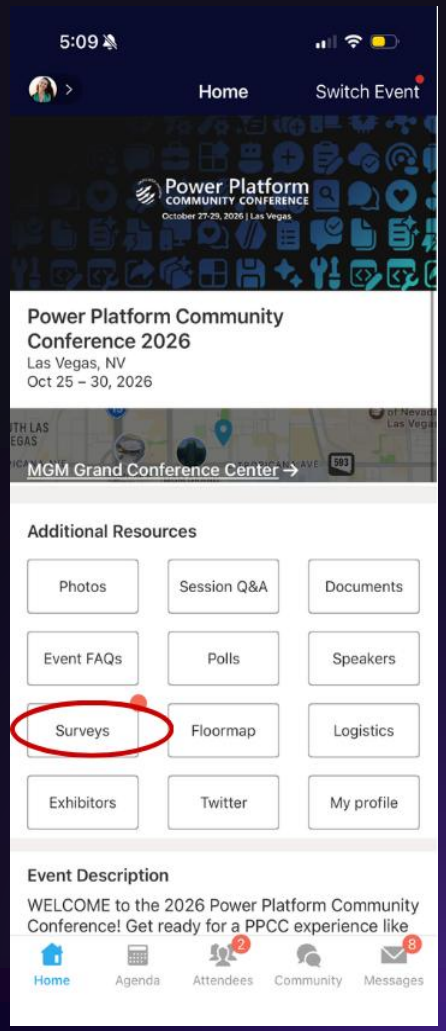
We really want to hear from YOU!

In the pursuit of making next year's Power Platform Community Conference even better, we want to hear your feedback about this session.

Here's How -

- *Simply go to the Whova App on your smartphone*
- *Scroll down on the Power Platform Community Conference Homepage to 'Additional Resources' to click "Surveys'.*
- *Click Session Feedback.*
- *Scroll down to find this session title.*
- *Complete the session feedback survey.*
- *Finally, click 'Submit'*

It's just that easy!



Agenda

01 The quiet killer of productivity
02 The vision and the architecture
03 Step 1 - Identifying the user
04 Step 2 - The secure handshake
05 Step 3 - The Golden Key (TAP)
06 Guardrails - enabling TAP safely with Entra ID
07 New conversational hardness
08 Results, demo and resources

POWER PLATFORM COMMUNITY CONFERENCE

“Copilot, Reset My Password!”

Building a secure self-service IVR with Copilot Studio & Entra ID

Peter Ruiter

MVP, Principal Solution Architect
Microsoft CX CTO, Capgemini

Capgemini

Peter Ruiter

- MVP, Principal Solution Architect
- Microsoft CX CTO @ Capgemini NL
- Microsoft Certified Trainer
- Contact center nerd

- powerpete.com
- youtube.com/@pruiter
- linkedin.com/in/peterruiter

- Peter.Ruiter@capgemini.com

Microsoft **Most Valuable Professional**

FastTrack Recognized **Solution Architect**

The quiet killer of productivity

40% of helpdesk calls are password resets. At $70 each.

40%

of all helpdesk calls are password-related. At USPS, 220,000 employees placed 30,000 reset calls a month.

$70	average cost per reset ticket in technician time and lost productivity
30,000	reset calls a month from 220,000 USPS employees
$2.1M	lost every month at that volume and cost per ticket

Sources: Gartner, via ZDNet, "40% of helpdesk calls are related to password problems"; Infosecurity Magazine, Password management webinar

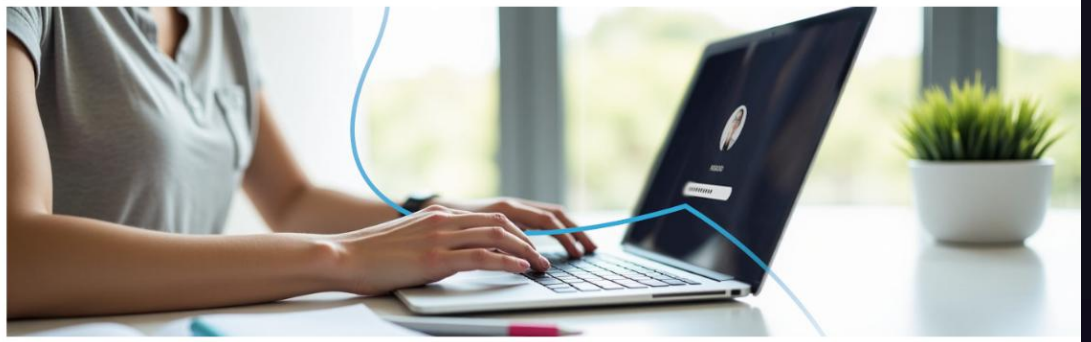
Meet the MVP who forgot his own password

Locked out at 8:55, customer keynote at 9:00. New laptop, old password, no idea which one.

My only option: call my own helpdesk and wait in the queue.

The email everyone ignores

Your Capgemini password will expire soon – change it now



Hello Peter,

Your Capgemini password (CORP) will expire soon. To avoid losing access to Capgemini services and applications, please change it before **2026-04-04 13:39:53 GMT+0200** .

Change your password easily – on your computer or mobile

Simply visit the Password Self-Service portal and follow the on-screen instructions to update your Capgemini password.

Please note: even if you use passwordless sign-in methods, such as fingerprint, facial recognition, or PIN, you are still required to reset your corporate password to avoid account lockout.

And if you get locked out of your computer, you can also update it using your mobile, in exactly the same way.

The vision: intelligent self service

One agent, voice and chat, that verifies who you are and gets you back in.

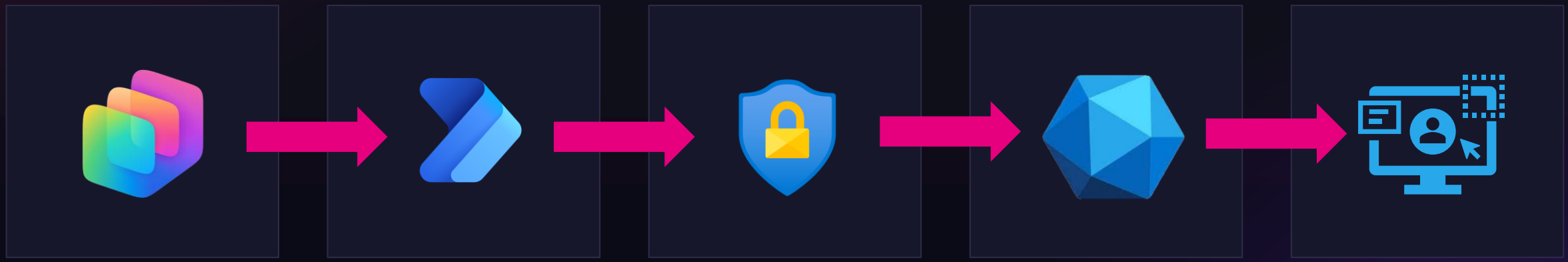
No ticket, no queue, no password read out over the phone.

The architecture: the how

Copilot Studio, Agent Flows, Entra ID and Microsoft Graph in one chain.

Each step hands the caller to the next with a stronger proof of identity.

The architecture: five hops from call to access



Copilot Studio
(Voice / Chat)

Power Automate
(Lookup user in Dynamics 365)

Entra ID
(Step-up Auth)

MS Graph
(Generate TAP)

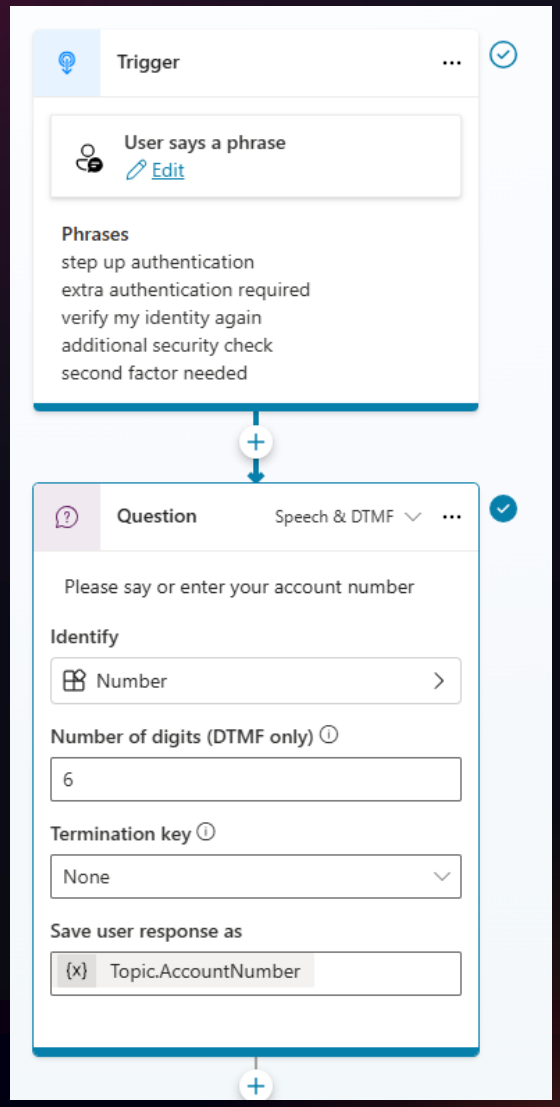
User
(Access Restored)

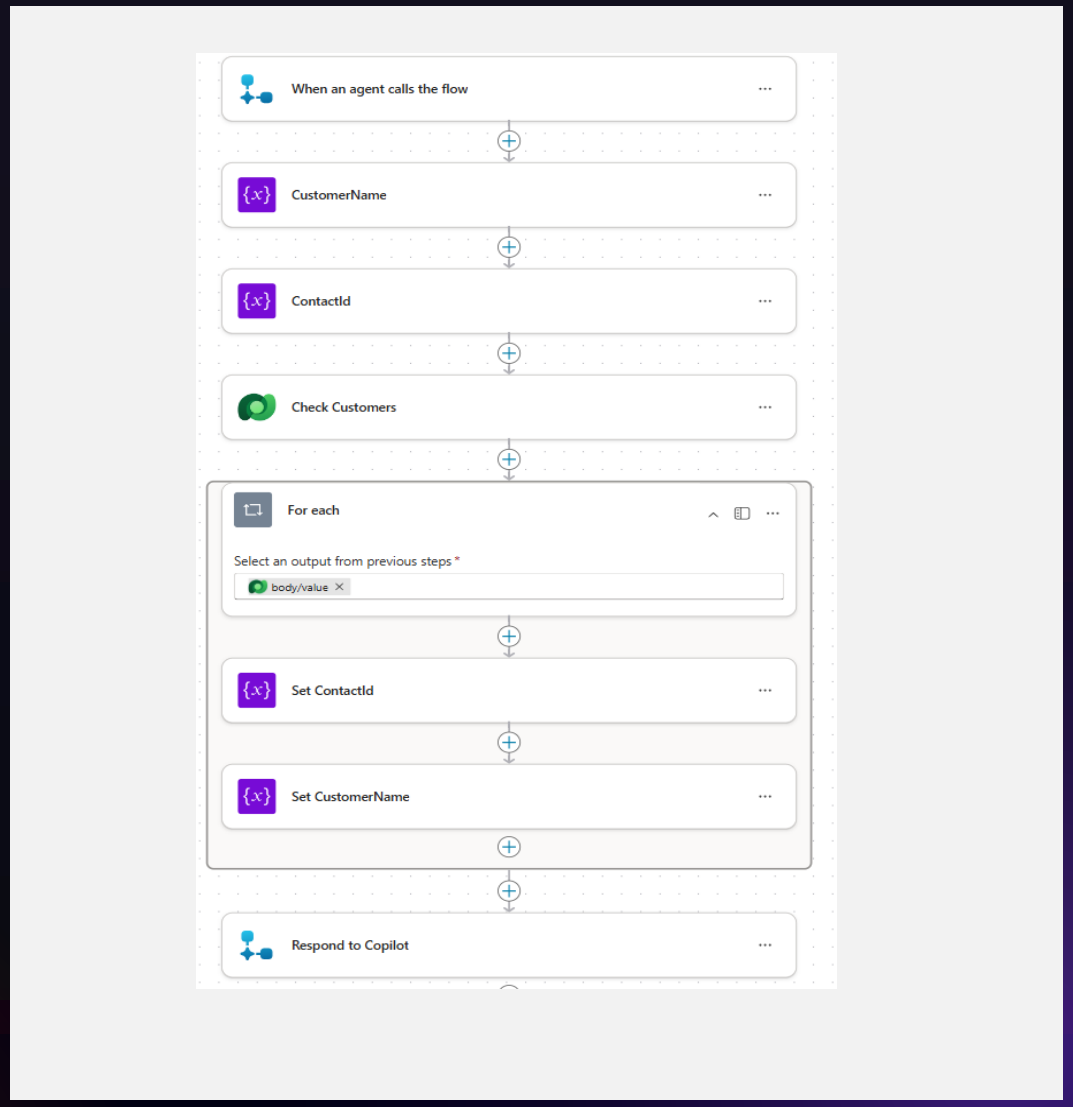
Step 1 - Identify the user

Caller ID plus a Dynamics 365 lookup finds the account before anyone types a thing.

Unknown number? The agent asks for a second identifier.

Demo - Step 1: identify the caller

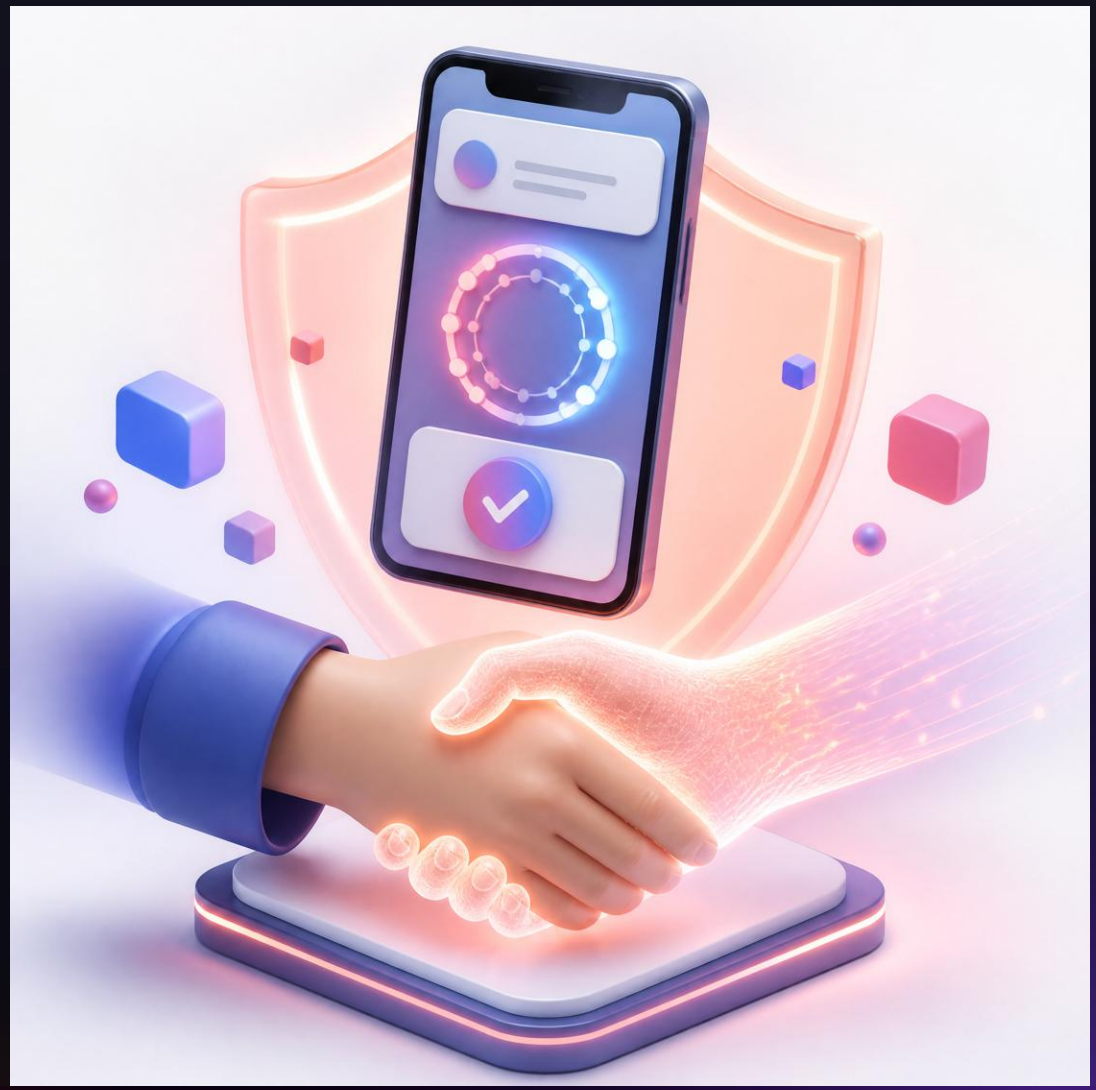




Step 2 - The secure handshake

The agent triggers a Microsoft Authenticator push; the user approves on their phone.

Nobody reads a password, PIN or secret question over the line.



Prerequisites: service principal for the MFA client

```
install-module Microsoft.Graph.Applications

Connect-MgGraph -Scopes 'Application.ReadWrite.All'

# Get ID of 'Entra Id MFA Notification Client' Service Principal
$servicePrincipalId = (Get-MgServicePrincipal -Filter "appid eq '981f26a1-7f43-403b-a875-f8b09b8cd720'").Id

$params = @{
                passwordCredential = @{
                                displayName = "Step-Up Authentication"
                }
}

# Create Client Secret onto client
$secret = Add-MgServicePrincipalPassword -ServicePrincipalId $servicePrincipalId -BodyParameter $params
```

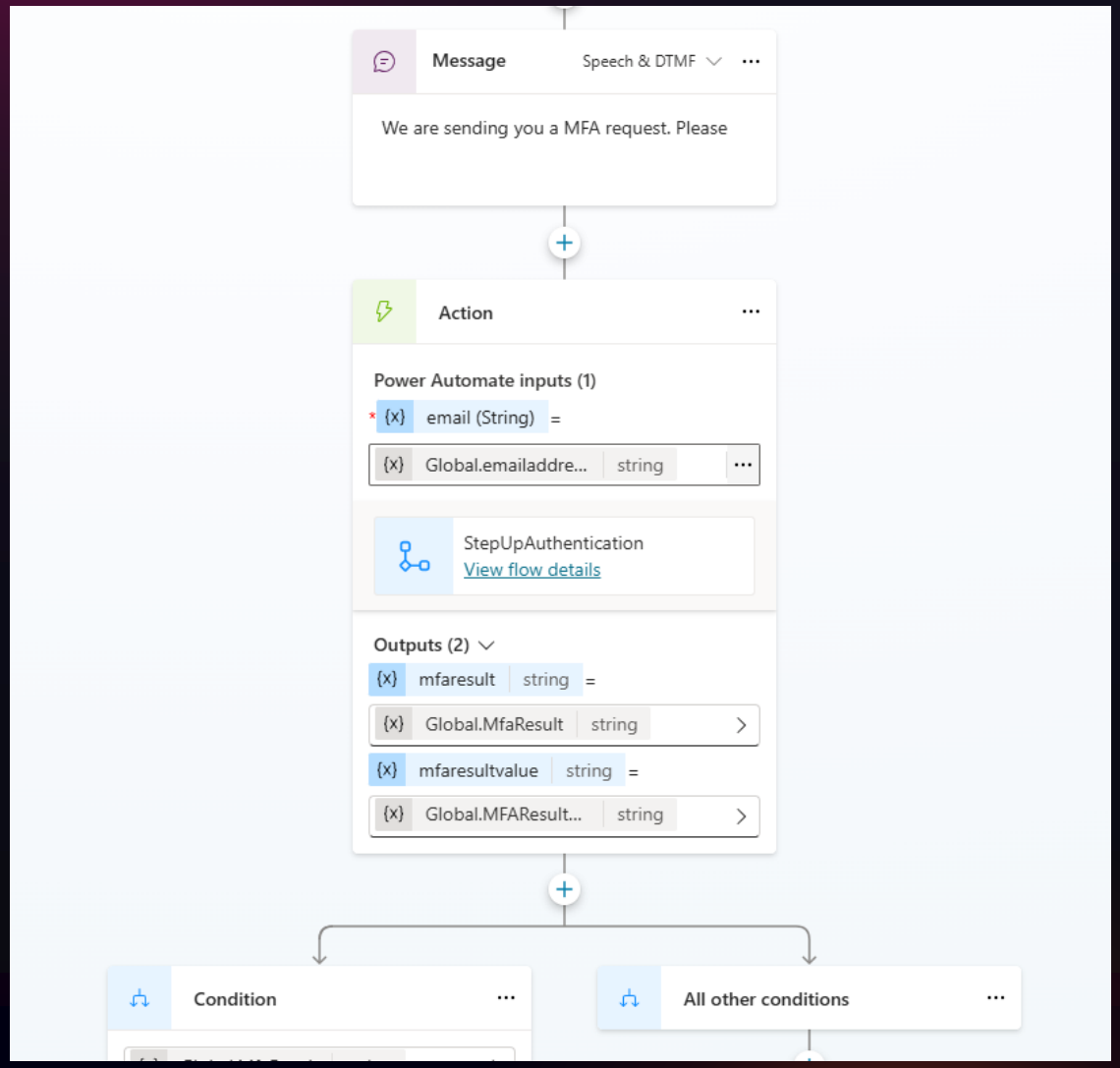
Get an MFA client access token

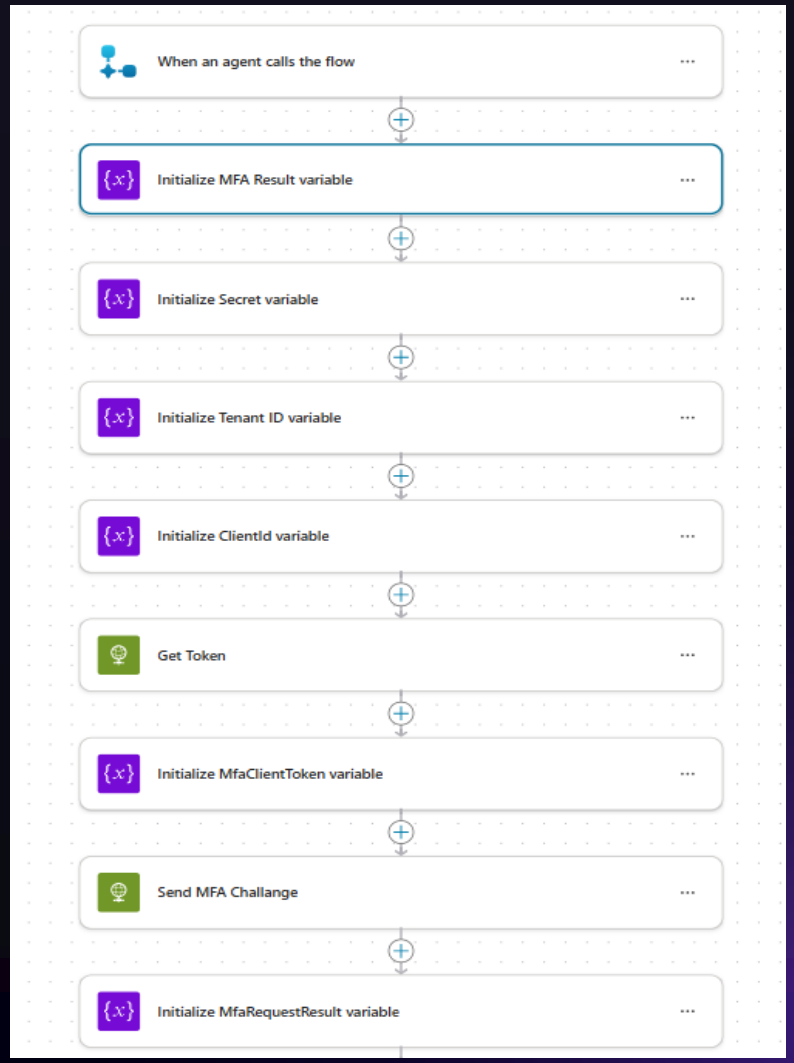
```
$secret = “xxx~xxxxxxxxx~-xxxxxxxxx-"
$email = "peter@powerpete.com"
$tenantId = “xxxxxxx-xxxxxx-xxxxxxxxxx"
$clientId = "981f26a1-7f43-403b-a875-f8b09b8cd720" # this is the same for everyone

Write-Host "Get MFA Client Access Token"
$body = @{
    'resource'      = 'https://adnotifications.windowsazure.com/StrongAuthenticationService.svc/Connector'
    'client_id'     = $clientId
    'client_secret' = $secret
    'grant_type'    = "client_credentials"
    'scope'         = "openid"
}

$mfaClientToken = Invoke-RestMethod -Method post -Uri "https://login.microsoftonline.com/$tenantId/oauth2/token" -Body $body
Write-Host "Done."
```

Send the MFA challenge to the user

```
Write-Host "Send MFA challenge to the user"
$XML = @"
<BeginTwoWayAuthenticationRequest><Version>1.0</Version>
                <UserPrincipalName>$email</UserPrincipalName><Lcid>en-us</Lcid>
                <AuthenticationMethodProperties xmlns:a="http://schemas.microsoft.com/2003/10/Serialization/Arrays">
                                <a:KeyValueOfstringstring>
                                                <a:Key>OverrideVoiceOtp</a:Key><a:Value>false</a:Value>
                                </a:KeyValueOfstringstring>
                </AuthenticationMethodProperties>
                <ContextId>bb07a24c-e5dc-4983-afe7-a0fcdc049cf7</ContextId>
                <SyncCall>true</SyncCall><RequireUserMatch>true</RequireUserMatch>
                <CallerName>radius</CallerName><CallerIP>UNKNOWN:</CallerIP>
</BeginTwoWayAuthenticationRequest>
"@

$headers = @{ "Authorization" = "Bearer $($mfaClientToken.access_token)" }
$mfaResult = Invoke-RestMethod -uri
'https://strongauthenticationservice.auth.microsoft.com/StrongAuthenticationService.svc/Connector//BeginTwoWayAuthentication' -Method POST -
Headers $Headers -Body $XML -ContentType 'application/xml'
Write-Host "Done”
```

Demo - Step 2: the secure handshake





Step 3 - The Golden Key (TAP)

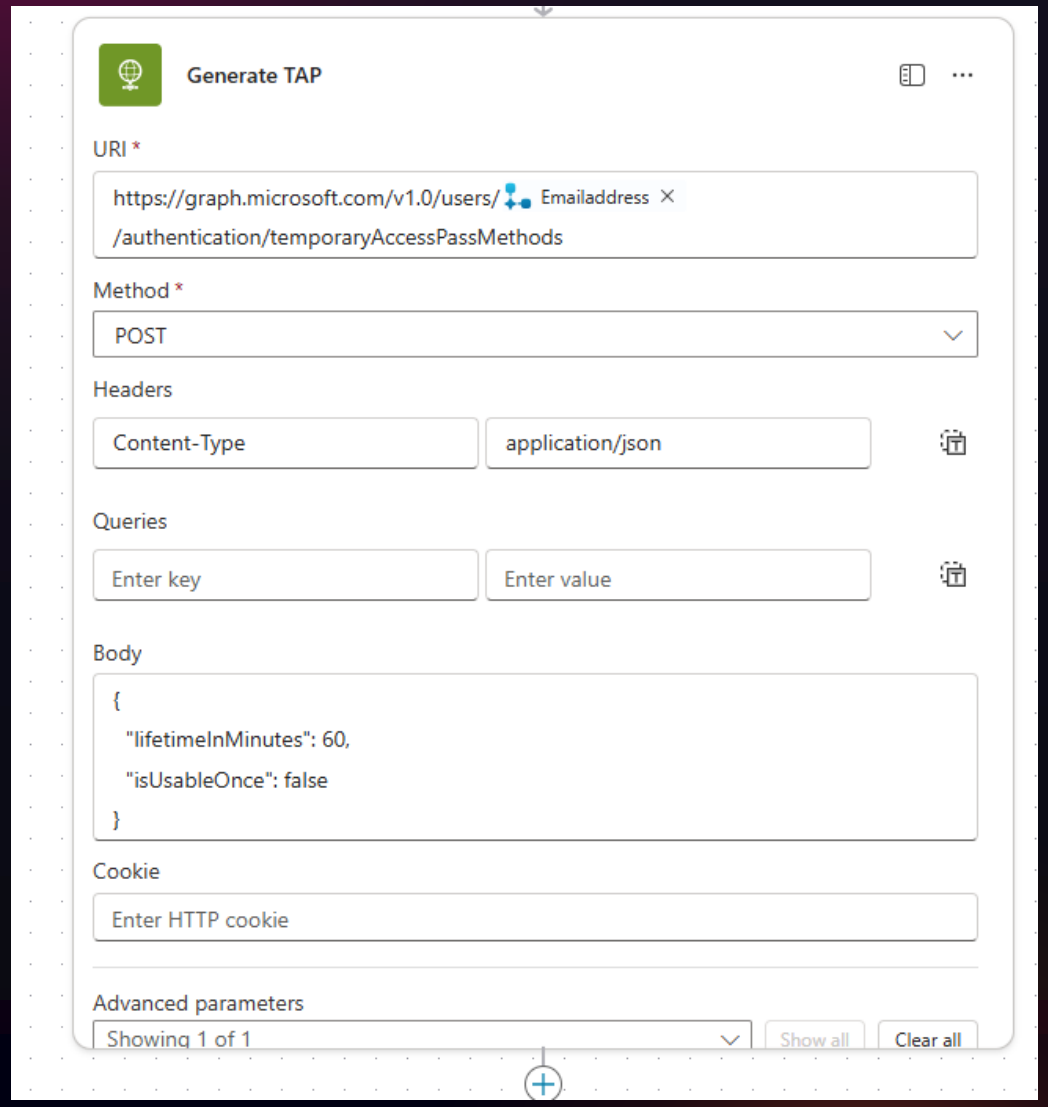
The agent generates a Temporary Access Pass through Microsoft Graph and reads it back once.

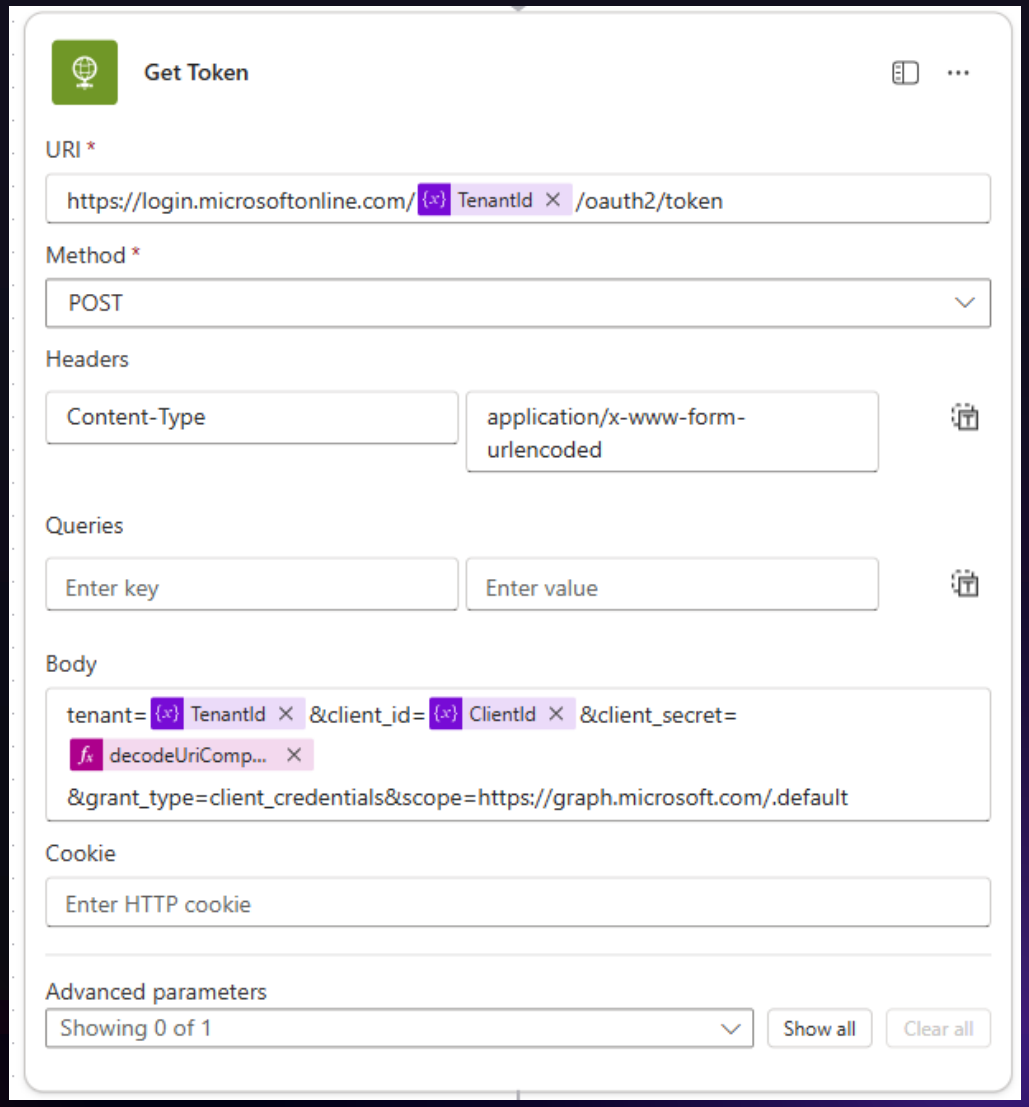
Short-lived, one-time, and the user sets a new password themselves.

Prerequisites: app registration permissions

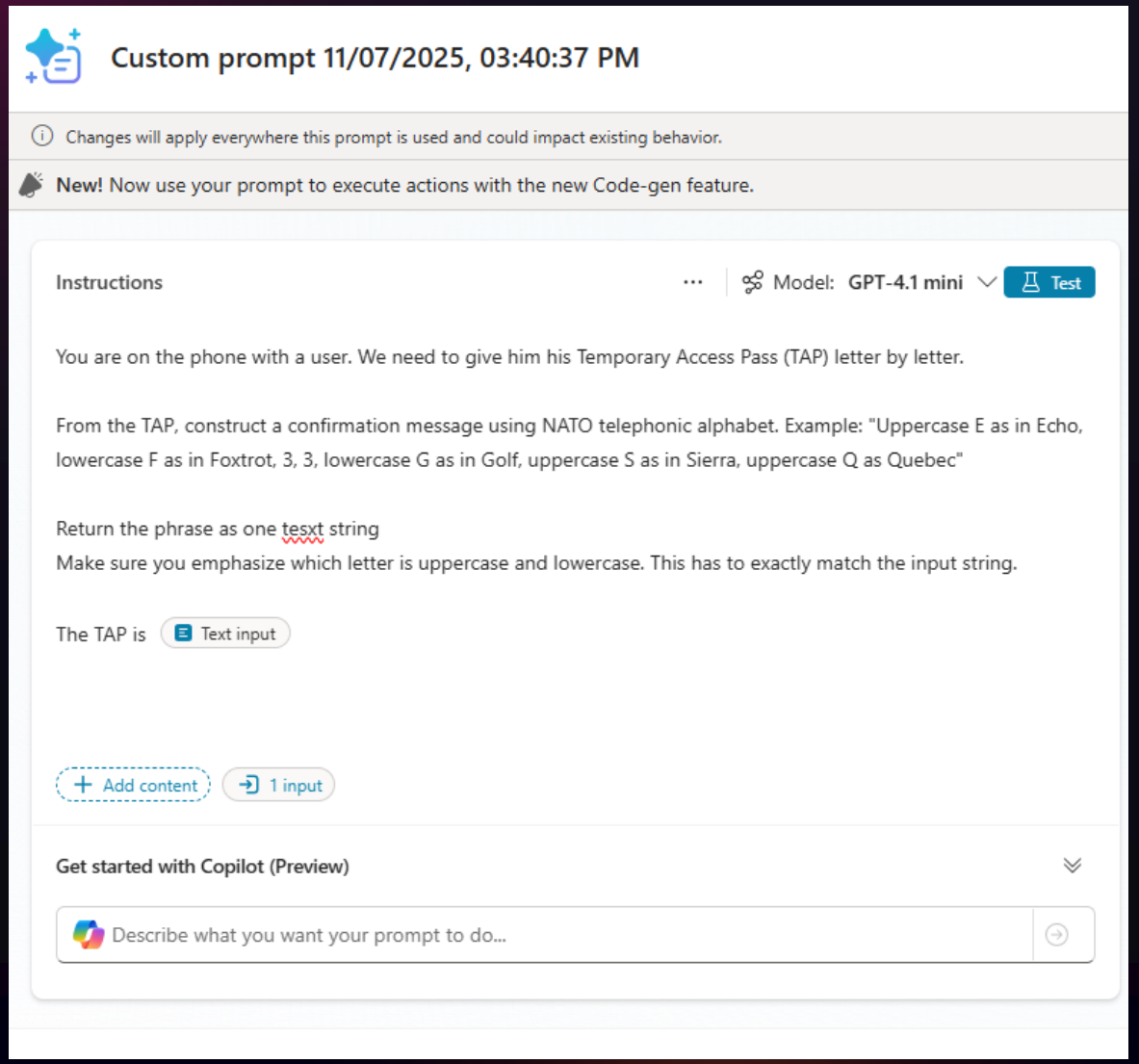
Naam API/machtigingen	Type	Beschrijving	Beheerd...	Status
Microsoft Graph (4)				
User.Read	Gedelegeerd	Aanmelden en gebruikersprofiel lezen	Nee	Verleend voor PowerPete
UserAuthenticationMethod.ReadWrite.All	Gedelegeerd	Read and write all users' authentication meth...	Ja	Verleend voor PowerPete
UserAuthMethod-TAP.ReadWrite.All	Gedelegeerd	Read and write all users' Temporary Access Pa...	Ja	Verleend voor PowerPete
UserAuthMethod-TAP.ReadWrite.All	Toepassing	Read and write all users' Temporary Access Pa...	Ja	Verleend voor PowerPete

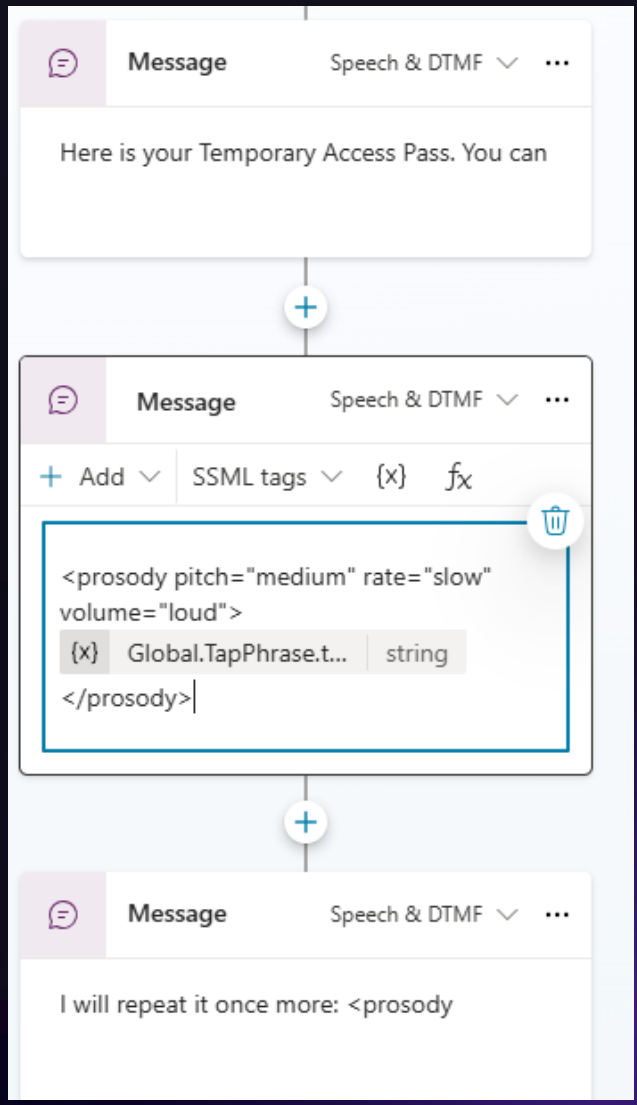
Generate a Temporary Access Pass



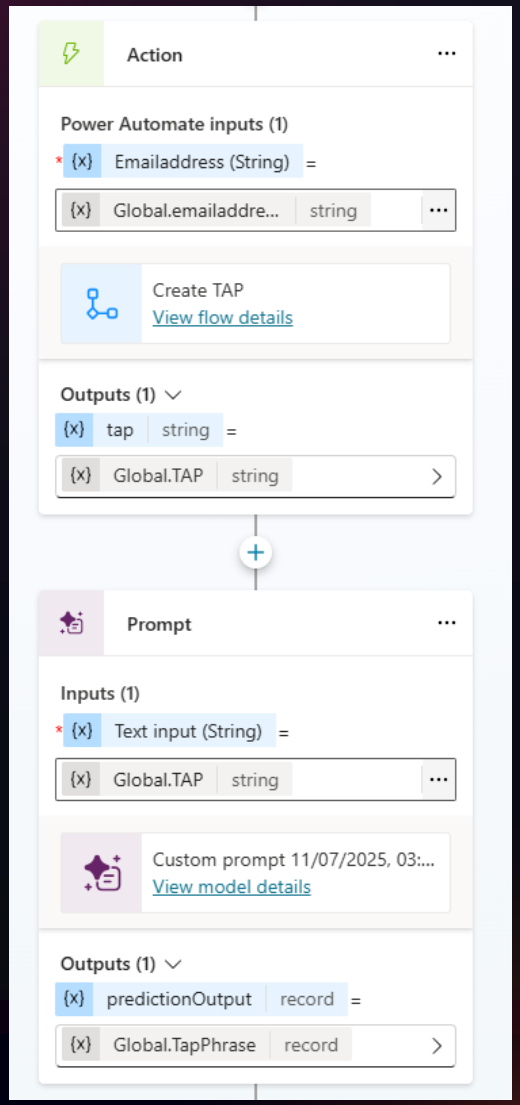


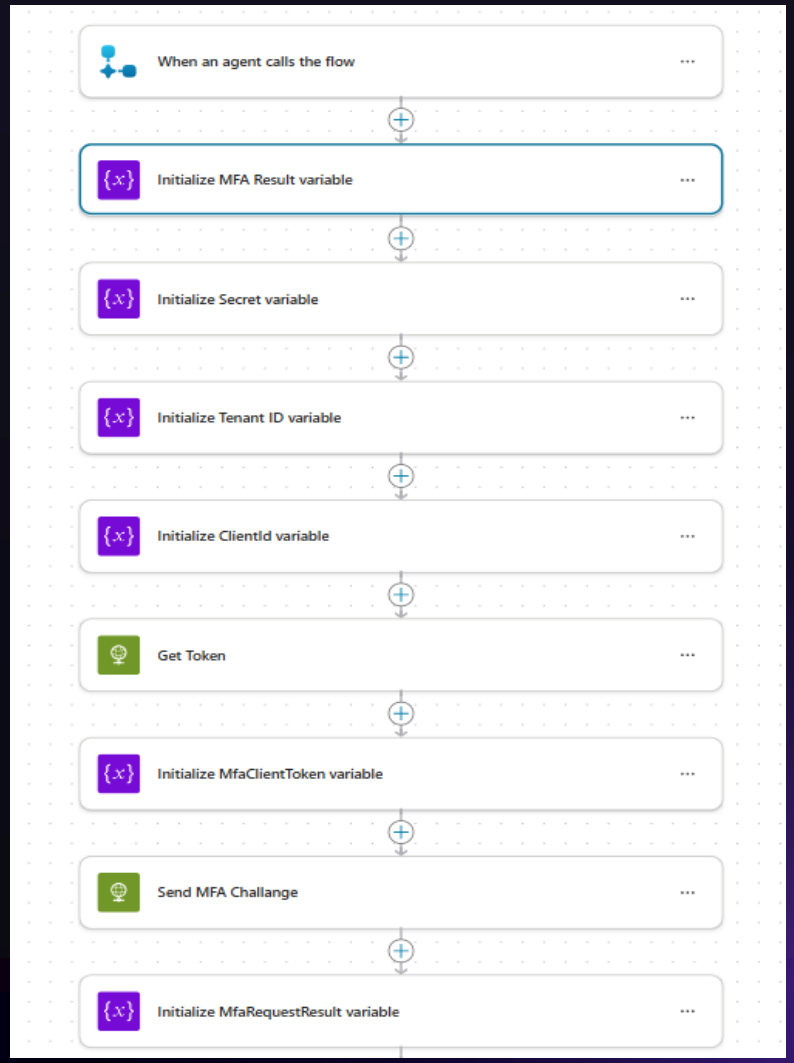
Return the TAP to the caller



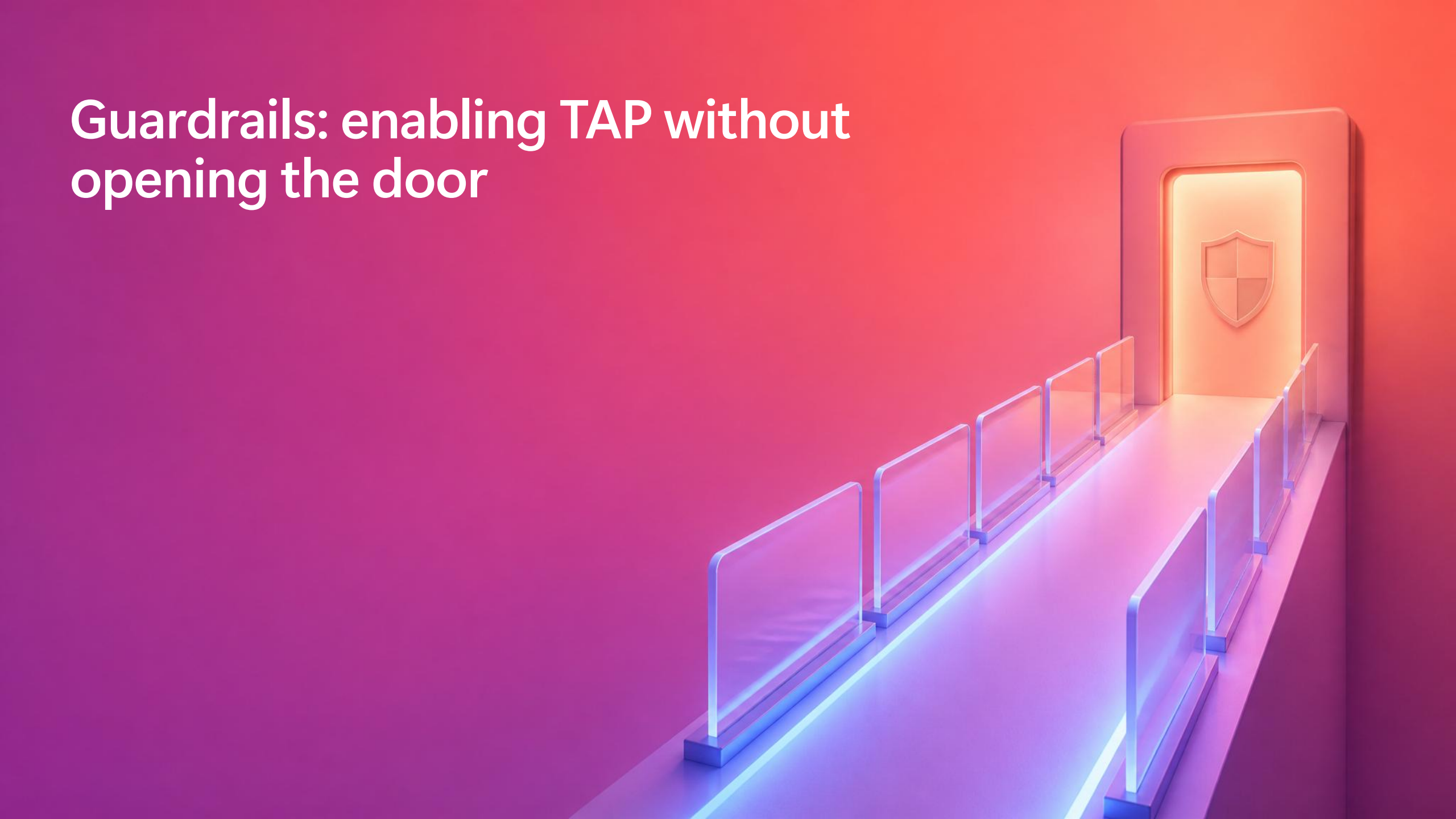


Demo - Step 3: the Golden Key





Guardrails: enabling TAP without opening the door



Scope the TAP policy before anyone can mint one

WHO

A pilot group, not all users

Target a security group in the authentication methods policy.

Exclude admins and anyone holding a privileged role.

HOW LONG

10 to 15 minutes

Policy allows 10 minutes to 30 days; defaults are 1 hour and 8 hours.

The agent sets the lifetime per pass, within the policy.

HOW OFTEN

One-time use

Enforce one-time use so a replayed or overheard pass is dead after first sign-in.

Pass expires on its own, nothing to clean up.

HOW STRONG

12+ characters, generated

Policy allows 8 to 48; let Microsoft Graph generate it.

Read it back with SSML spelling, never store it in the transcript.

Conditional Access decides where a TAP works

Trusted networks and devices

- **Named locations:** mark office IP ranges and the corporate VPN as trusted.
- **Untrusted location:** block the sign-in, or require a compliant or hybrid-joined device before the TAP counts.
- **Block legacy authentication** so the pass can never be replayed through an old protocol.
- **Sign-in frequency:** force a fresh sign-in once the new password and Authenticator are set.

Auth strengths and privileged users

- **Custom authentication strength** without TAP for admin portals and privileged roles: no pass gets anyone into Entra admin.
- **Privileged users excluded** from the TAP target group; they still go through the human helpdesk.
- **Workload identity policy** for the agent's service principal: trusted locations only.
- **Report-only first:** run the policies in report-only mode for a week, then enforce.

Lock down the agent that hands out the keys

LEAST PRIVILEGE

Scoped role, not a global one

The Graph permission (UserAuthenticationMethod.ReadWrite.All) is tenant-wide: pair it with the Authentication Administrator role scoped to an administrative unit.

Never Privileged Authentication Administrator: the agent must not be able to reset admins.

SECRETS

No credentials in the flow

Client secret or certificate in Azure Key Vault, referenced through environment variables.

Rotate on a schedule; a managed identity for the connector where it is supported.

Environment DLP policy so only this flow can call Graph.

AUDIT

Every pass leaves a trace

TAP creation is written to the Entra audit log; stream it to Sentinel.

Alert on volume spikes, out-of-hours activity and any admin target.

Email or text the user after every reset so they can shout if it wasn't them.

Defense in depth: the checklist before you go live

Layer	Control	Setting that makes it safe
Authentication methods policy	TAP enabled for a pilot group	One-time use, 10-15 min lifetime, 12+ characters, admins excluded
Conditional Access	Named locations	Office and VPN ranges trusted; elsewhere blocked or compliant device required
Conditional Access	Authentication strength	TAP not accepted for admin portals or privileged roles
Agent identity	Scoped role and Graph permission	Authentication Administrator on an administrative unit, secret in Key Vault
Caller verification	Step-up before any pass	Authenticator push with number matching, no SMS or voice fallback
Monitoring	Audit log and alerts	Every TAP creation logged; alert on spikes and admin targets; user notified

The results: happy IT, happy me

I am back in within minutes, 24/7, without admitting to a colleague that I forgot my password again.

IT loses its most boring ticket and keeps full control over who gets a pass, where and for how long.

Demo: end to end

I call, approve on my phone and get my Temporary Access Pass

Copilot Studio voice agent, Agent Flows, Entra ID, Microsoft Graph

Ready to build your own?

Everything you saw today is in a sample solution you can import this week.

Start with chat, add voice when the guardrails are in place.

POWER PLATFORM COMMUNITY CONFERENCE

Thank you

Peter Ruiter
powerpete.com | linkedin.com/in/peterruiter |
Peter.Ruiter@capgemini.com

Introducing the Power Platform Community Conference App

STAY IN THE KNOW

- Get access to live event updates & notifications
- Build a personalized agenda
- Connect with other attendees
- Network with Sponsor & Exhibitors
- Join meet-ups
- Access event documents

Event Invitation Code:
5thAnnual2026

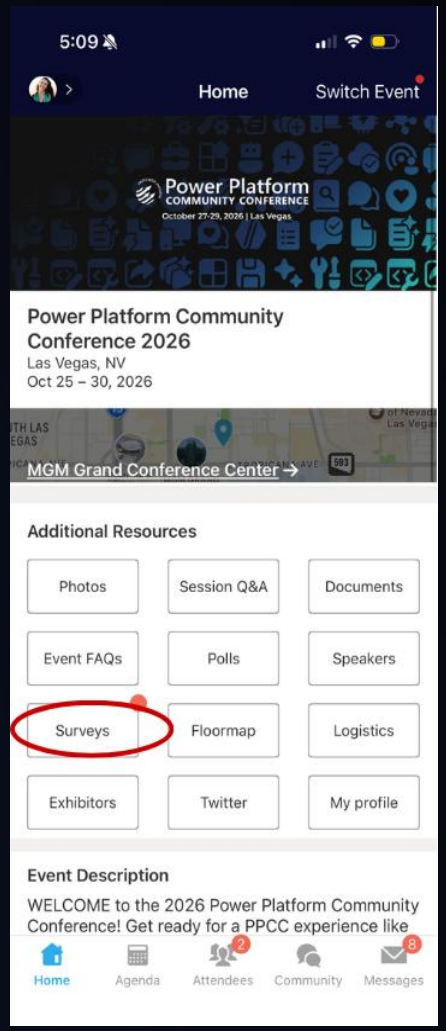
POWER PLATFORM COMMUNITY CONFERENCE

Session Feedback Surveys

We really want to hear from YOU!

In the pursuit of making next year's Power Platform Community Conference even better, we want to hear your feedback about this session.

Here's How -

- *Simply go to the Whova App on your smartphone*
- *Scroll down on the Power Platform Community Conference Homepage to 'Additional Resources' to click "Surveys'.*
- *Click Session Feedback.*
- *Scroll down to find this session title.*
- *Complete the session feedback survey.*
- *Finally, click 'Submit'*

It's just that easy!