IMPROVE IDENTITY SECURITY IN AZURE AD

JAN BAKKER

DUTCH CLOUD MEETUP

10.11.2022

AKA.MS/JANBAKKER

- Identity & Access Management | Security
- MVP Enterprise & Mobility

WHAT'S ON THE AGENDA?

The problem with passwords

Live phishing demo!

Tips for better identity security in Azure AD

“IDENTITY IS THE NEW PERIMETER”

ZERO TRUST

WHAT IS ZERO TRUST?

VERIFY EXPLICITLY

ASSUME BREACH

LEAST PRIVILIGE

PhaaS, cybercriminals offer multiple services within a single subscription. In general, a purchaser needs to take only three actions:

Microsoft Digital Defense Report 2022

1. Select a phishing site template/design from among the hundreds offered.
2. Provide an email address to receive credentials obtained from phishing victims.
3. Pay the PhaaS merchant in cryptocurrency.

Once these steps are completed, the PhaaS merchant creates services with three or four layers of redirect and

10 TIPS TO IMPROVE YOUR IDENTITY SECURITY IN AZURE AD

1. BLOCK LEGACY AUTHENTICATION

More than **99 %** of password spray attacks use legacy authentication protocols

More than **97 %** of credential stuffing attacks use legacy authentication

Azure AD accounts in organizations that have disabled legacy authentication experience **67 %** fewer compromises than those where legacy authentication is enabled

Effective October 1, 2022, we will begin to permanently disable Basic Authentication for Exchange Online in all Microsoft 365 tenants regardless of usage, except for SMTP Authentication.

Create new policy from templates (Preview)

Got feedback?

Customize your build | **Select template** | Review + create

We recommend the following templates based on your response

- Require multifactor authentication for admins
  Require multifactor authentication for privileged administrative accounts to reduce risk of compromise. This policy will target the same roles as Security Default.
  View policy summary
- Securing security info registration
  Secure when and how users register for Azure AD multifactor authentication and self-service password.
  View policy summary
- **Block legacy authentication** (selected)
  Block legacy authentication endpoints that can be used to bypass multifactor authentication.
  View policy summary
- Require multifactor auth all users
  Require multifactor auth all user accounts to redu compromise.
  View policy summary
- Require multifactor authentication for Azure management
  Require multifactor authentication to protect privileged access to Azure resources.
  View policy summary
- Require multifactor authentication for risky sign-ins
  Require multifactor authentication if the sign-in risk is detected to be medium or high. (Requires an Azure AD Premium 2 License)
  View policy summary
- Require password change for high-risk users
  Require the user to change their password if the user risk is detected to be high. (Requires an Azure AD Premium 2 License)
  View policy summary

Name your policy

CA003: Block legacy authentication

Policy state

Off | On | Report-only

Policy summary

Policy template

Basics

Template category	Identities
Policy template	CA003: Block legacy authentication

Assignments

Users and groups

Included users	All Users
Excluded users	Current user

Cloud apps or actions

Cloud apps	All apps

Conditions

Client apps

Legacy authentication clients	Exchange ActiveSync clients Other clients

Access controls

Block access	Selected

2. REQUIRE MFA FOR ALL USERS

Your password doesn't matter, but MFA does! Based on our studies, your account is more than **99.9%** less likely to be compromised if you use MFA.

Bad: Password	**Good:** Password and...	**Better:** Password and...	**Best:** Passwordless
123456	SMS	Authenticator (Push Notifications)	Authenticator (Phone Sign-in)
qwerty	Voice	Software Tokens OTP	Window Hello
password		Hardware Tokens OTP (Preview)	FIDO2 security key
iloveyou			**Certificates**
Password1			

Create new policy from templates (Preview)

Got feedback?

Customize your build | **Select template** | Review + create

We recommend the following templates based on your response

- Require multifactor authentication for admins
  Require multifactor authentication for privileged administrative accounts to reduce risk of compromise. This policy will target the same roles as Security Default.
  View policy summary
- Securing security info registration
  Secure when and how users register for Azure AD multifactor authentication and self-service password.
  View policy summary
- Block legacy authentication
  Block legacy authentication endpoints that can be used to bypass multifactor authentication.
  View policy summary
- **Require multifactor authentication for all users** (selected)
  Require multifactor authentication for all user accounts to reduce risk of compromise.
  View policy summary
- Require multifactor authentication for guest access
  Require guest users perform multifactor authentication when accessing your company resources.
  View policy summary
- Require multifactor authentication for Azure management
  Require multifactor authentication to protect privileged access to Azure resources.
  View policy summary
- Require multifactor authentication for risky sign-ins
  Require multifactor authentication if the sign-in risk is detected to be medium or high. (Requires an Azure AD Premium 2 License)
  View policy summary
- Require password change for high-risk users
  Require the user to change their password if the user risk is detected to be high. (Requires an Azure AD Premium 2 License)
  View policy summary

Name your policy

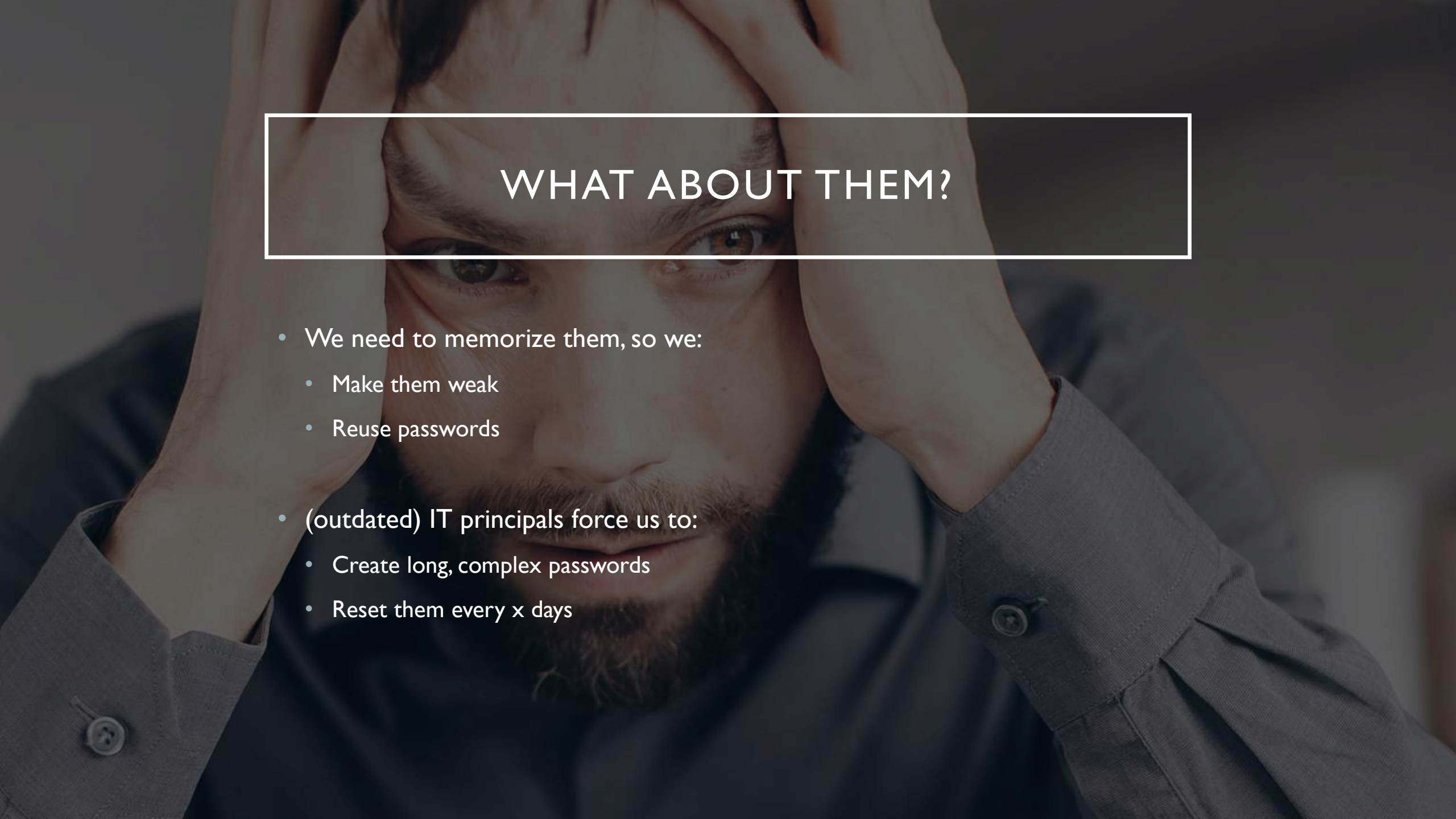
CA004: Require multifactor authentication for all users

Policy state

Off | On | Report-only

EVILGINX DEMO

3. LET'S TALK ABOUT PASSWORDS



WHAT ABOUT THEM?

- We need to memorize them, so we:
  - Make them weak
  - Reuse passwords
- (outdated) IT principals force us to:
  - Create long, complex passwords
  - Reset them every x days

BAN COMMON PASSWORDS, TO KEEP THE MOST VULNERABLE PASSWORDS OUT OF YOUR SYSTEM

Azure AD Password Protection

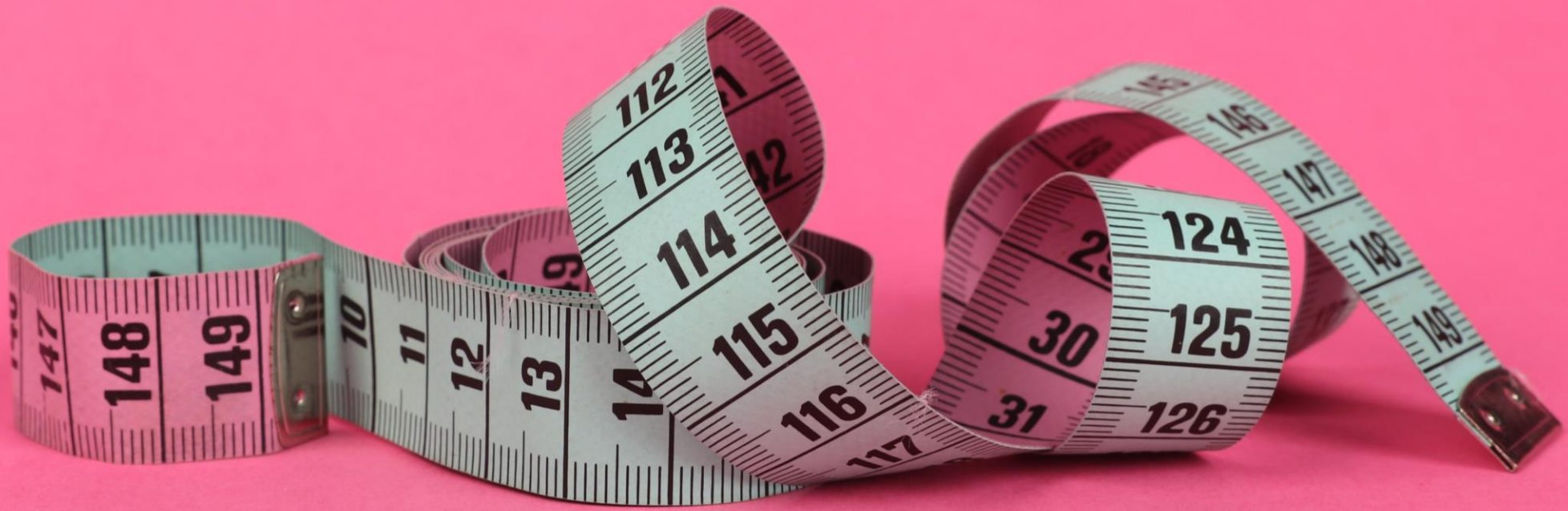
- Default global passwords
- Custom password (up to a 1000)

DON'T REQUIRE CHARACTER COMPOSITION REQUIREMENTS. FOR EXAMPLE, *&(^%$

Some complexity requirements even prevent users from using secure and memorable passwords, and force them into coming up with less secure and less memorable passwords.

DON'T REQUIRE MANDATORY PERIODIC PASSWORD RESETS FOR USER ACCOUNTS

TO ENCOURAGE USERS TO THINK ABOUT A UNIQUE PASSWORD, WE RECOMMEND KEEPING A REASONABLE **14-CHARACTER** MINIMUM LENGTH REQUIREMENT.



Flower-country

bus-Corn-fleet

4. ENABLE PASSWORD HASH SYNC

Password Hash Sync also enables **leaked credential detection** for your hybrid accounts. Microsoft works alongside dark web researchers and law enforcement agencies to find publicly available username/password pairs. If any of these pairs match those of our users, the associated account is moved to high risk.

5. CONSENT PHISHING ATTACKS

Consent and permissions | User consent settings

Manage

User consent settings

Permission classifications

Save | Discard | Got feedback?

Control when end users and group owners are allowed to grant consent to applications, and when they will be required to request administrator review and approval. Allowing users to grant apps access to data helps them acquire useful applications and be productive, but can represent a risk in some situations if it's not monitored and controlled carefully.

User consent for applications

Configure whether users are allowed to consent for applications to access your organization's data. Learn more

- Do not allow user consent
  An administrator will be required for all apps.
- Allow user consent for apps from verified publishers, for selected permissions (Recommended)
  All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.

  2 permissions classified as low impact
- Allow user consent for apps
  All users can consent for any app to access the organization's data.

Group owner consent for apps accessing data

Configure whether group owners are allowed to consent for applications to access your organization's data for the groups they own. Learn more

- Do not allow group owner consent
  Group owners cannot allow applications to access data for the groups they own.
- Allow group owner consent for selected group owners
  Only selected group owners can allow applications to access data for the groups they own.
- Allow group owner consent for all group owners
  All group owners can allow applications to access data for the groups they own.

Enterprise applications | User settings

Contoso - Azure Active Directory

Overview
Overview
Diagnose and solve problems
Manage
All applications
Application proxy
User settings
Collections
Security
Conditional Access
Consent and permissions
Activity
Sign-in logs
Usage & insights
Audit logs
Provisioning logs

Save | Discard | Got feedback?

Admin consent requests

Users can request admin consent to apps they are unable to consent to: Yes / No

Who can review admin consent requests

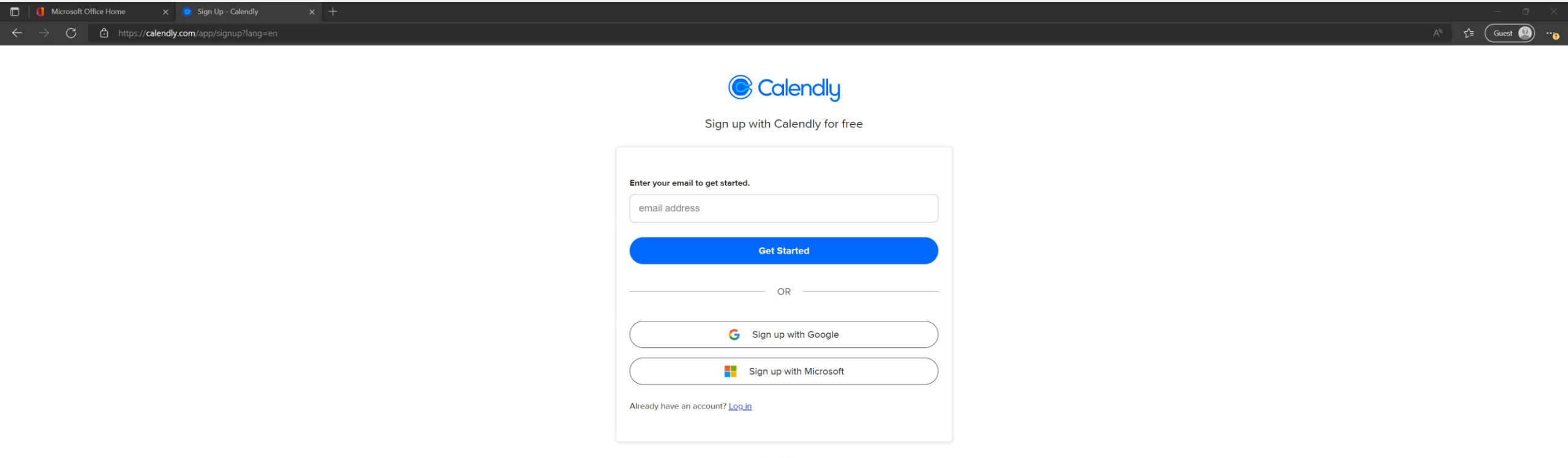
Reviewer type	Reviewers
Users	+ Add users
Groups (Preview)	+ Add groups
Roles (Preview)	1 role selected.

Selected users will receive email notifications for requests: Yes / No

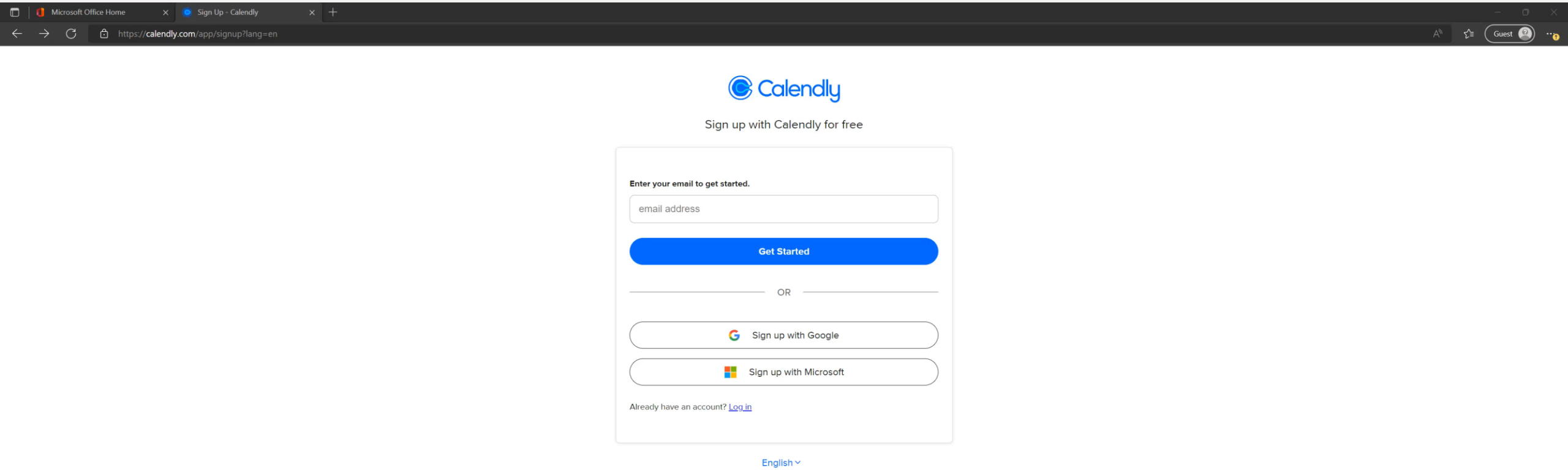
Selected users will receive request expiration reminders: Yes / No

Consent request expires after (days): 30

Office 365 Settings



App consent with admin approval



App consent without admin approval

6. AUTHENTICATION CONTEXT & NUMBER MATCHING

Microsoft Authenticator settings

The Microsoft Authenticator app is a flagship authentication method, usable in passwordless or simple push notification approval modes. The app is free to download and use on Android/iOS mobile devices. Learn more.

Basics Configure

Note: Users must be included as part of the Microsoft Authenticator targeted groups under the 'Basics' tab.

Require number matching for push notifications 1

Note: If the feature status is set to Microsoft-managed, it will be enabled by Microsoft at an appropriate time after the preview. Learn more

Status Enabled

Target Include Exclude

- (•) All users
- ( ) Select group

Show application name in push and passwordless notifications 2

Note: If the feature status is set to Microsoft-managed, it will be enabled by Microsoft at an appropriate time after the preview. Learn more

Status Enabled

Target Include Exclude

- (•) All users
- ( ) Select group

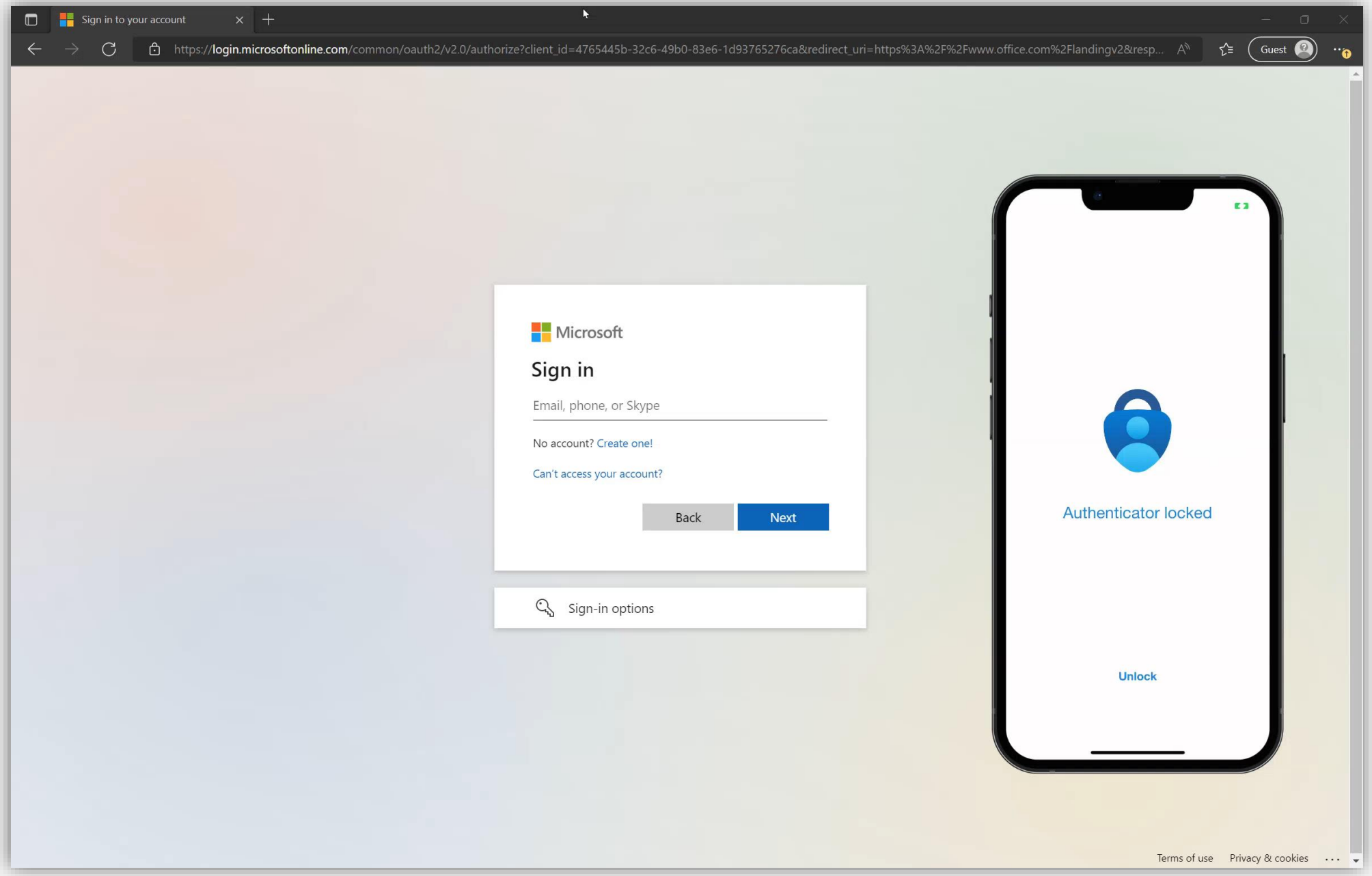
Show geographic location in push and passwordless notifications 3

Note: If the feature status is set to Microsoft-managed, it will be enabled by Microsoft at an appropriate time after the preview. Learn more

Status Enabled

Target Include Exclude

- (•) All users
- ( ) Select group


Sign in to your account
https://login.microsoftonline.com/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d93765276ca&redirect_uri=https%3A%2F%2Fwww.office.com%2Flandingv2&resp...
Guest
Microsoft
Sign in
Email, phone, or Skype
No account? Create one!
Can't access your account?
Back
Next
Sign-in options
Authenticator locked
Unlock
Terms of use
Privacy & cookies

7. CONDITIONAL ACCESS

REQUIRE DEVICE TO BE MARKED AS COMPLIANT OR HYBRID AZURE AD JOINED DEVICE

New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

Example: 'Device compliance app policy'

Assignments

Users or workload identities

0 users or workload identities selected

Cloud apps or actions

No cloud apps, actions, or authentication contexts selected

Conditions

0 conditions selected

Access controls

Grant

0 controls selected

Session

0 controls selected

Enable policy

Grant

Control access enforcement to block or grant access. Learn more

- Block access
- Grant access

- [ ] Require multifactor authentication
- [ ] Require authentication strength (Preview)
- [x] Require device to be marked as compliant

Don't lock yourself out! Make sure that your device is compliant.

- [x] Require Hybrid Azure AD joined device

Don't lock yourself out! Make sure that your device is Hybrid Azure AD Joined.

- [ ] Require approved client app
  See list of approved client apps
- [ ] Require app protection policy
  See list of policy protected client apps
- [ ] Require password change

New tab

Search or enter web address

Guest

You're browsing as a guest

As a guest, your browsing data is kept separate from the profiles on this device. Here's what happens when you close all windows you browsed as a guest:

Microsoft Edge **won't save**:

- Your browsing history
- Your download history
- Cookies and site data

Microsoft Edge **will save**:

- Files you download

Windows PowerShell

```
root@vps8874:~# evilginx
```

- -- Gone Phishing -- -

by Kuba Gretzky (@mrgretzky) version 2.4.2

```
[07:55:04] [inf] loading phishlets from: /usr/share/evilginx/phishlets/
[07:55:04] [inf] loading configuration from: /root/.evilginx
[07:55:05] [inf] blacklist: loaded 8 ip addresses or ip masks
[07:55:05] [inf] setting up certificates for phishlet 'o365'...
[07:55:05] [+++] successfully set up SSL/TLS certificates for domains: [login.miicrosoftonliine.com www.miicrosoftonliine.com login.m
iicrosoftonliine.com]
```

phishlet	author	active	status	hostname
citrix	@424f424f	disabled	available	
instagram	@charlesbel	disabled	available	
linkedin	@mrgretzky	disabled	available	
okta	@mikesiegel	disabled	available	
onelogin	@perfectlylog...	disabled	available	
outlook	@mrgretzky	disabled	available	
wordpress.org	@meitar	disabled	available	
amazon	@customsync	disabled	available	
coinbase	@An0nud4y	disabled	available	
facebook	@charlesbel	disabled	available	
reddit	@customsync	disabled	available	
twitter	@white_fi	disabled	available	
booking	@Anonymous	disabled	available	
o365	@jamescullum	enabled	available	miicrosoftonl...
paypal	@An0nud4y	disabled	available	
protonmail	@jamescullum	disabled	available	
twitter-mobile	@white_fi	disabled	available	
github	@audibleblink	disabled	available	
tiktok	@An0nUD4Y	disabled	available	
airbnb	@AN0NUD4Y	disabled	available	

:

REQUIRE TRUSTED LOCATIONS

New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

Example: 'Device compliance app policy'

Assignments

Users or workload identities

0 users or workload identities selected

Cloud apps or actions

No cloud apps, actions, or authentication contexts selected

Conditions

1 condition selected

Access controls

Grant

0 controls selected

Session

0 controls selected

Control access based on signals from conditions like risk, device platform, location, client apps, or device state. Learn more

User risk

Not configured

Sign-in risk

Not configured

Device platforms

Not configured

Locations

Any location and all trusted locations excluded

Client apps

Not configured

Filter for devices

Not configured

Control user access based on their physical location. Learn more

Configure

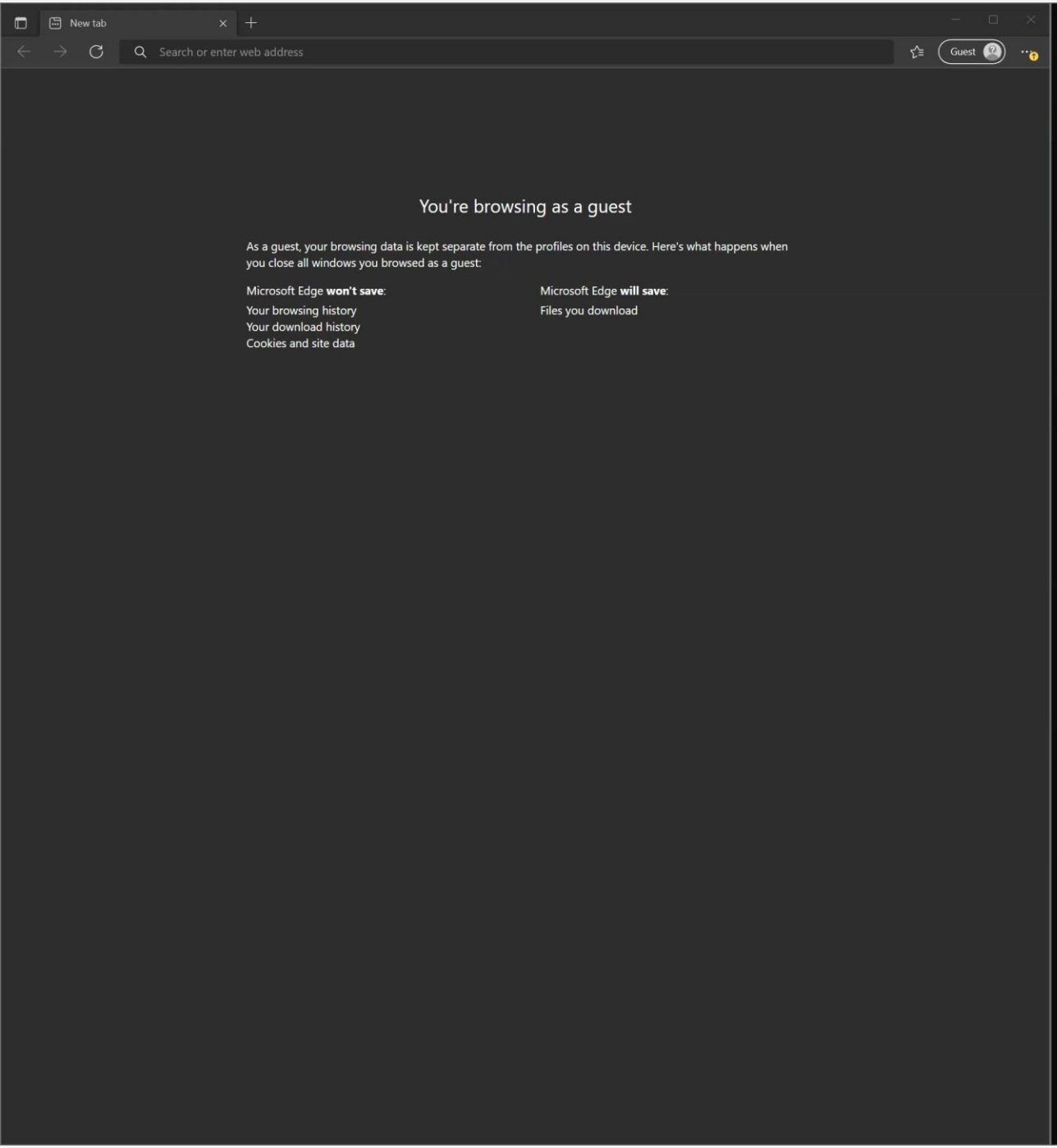
Yes No

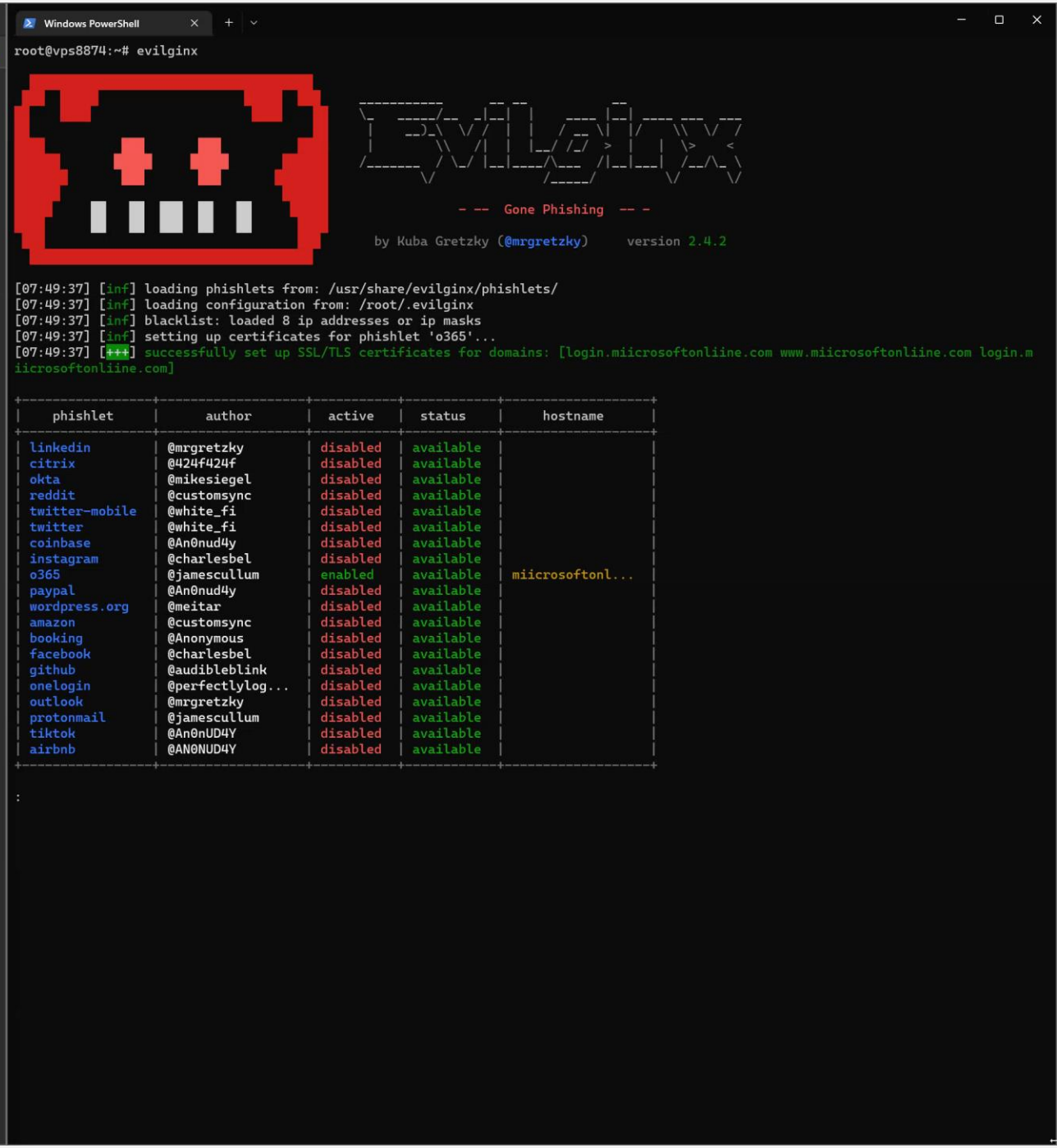
Include Exclude

Select the locations to exempt from the policy

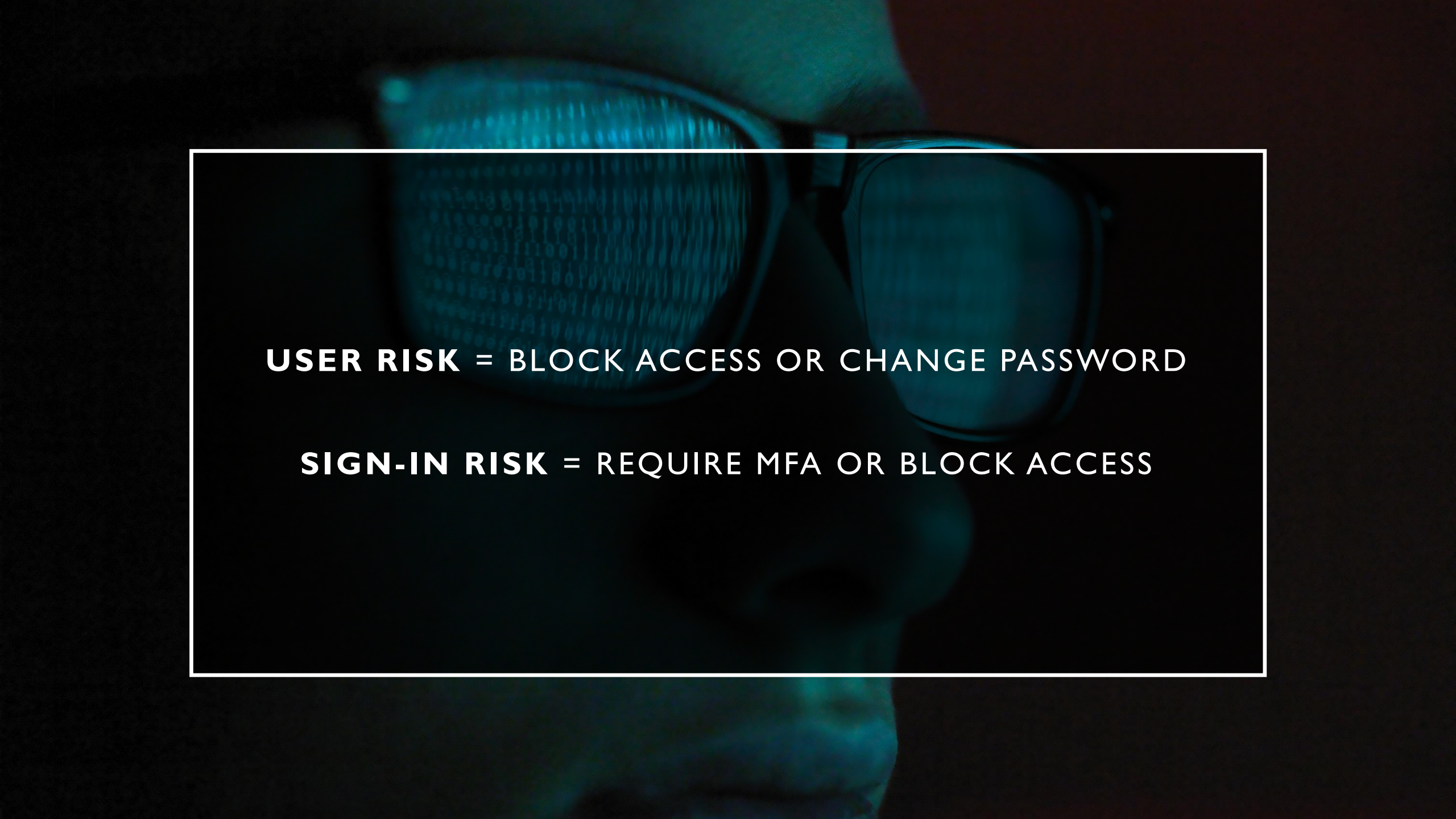
- (•) All trusted locations
- ( ) Selected locations

Enable policy


New tab
Search or enter web address
Guest
You're browsing as a guest
As a guest, your browsing data is kept separate from the profiles on this device. Here's what happens when you close all windows you browsed as a guest:
Microsoft Edge won't save:
Your browsing history
Your download history
Cookies and site data
Microsoft Edge will save:
Files you download


Windows PowerShell
root@vps8874:~# evilginx
Gone Phishing
by Kuba Gretzky (@mrgretzky) version 2.4.2
[07:49:37] [inf] loading phishlets from: /usr/share/evilginx/phishlets/
[07:49:37] [inf] loading configuration from: /root/.evilginx
[07:49:37] [inf] blacklist: loaded 8 ip addresses or ip masks
[07:49:37] [inf] setting up certificates for phishlet 'o365'...
[07:49:37] [+++] successfully set up SSL/TLS certificates for domains: [login.miicrosoftonliine.com www.miicrosoftonliine.com login.miicrosoftonliine.com]
phishlet | author | active | status | hostname
linkedin | @mrgretzky | disabled | available
citrix | @424f424f | disabled | available
okta | @mikesiegel | disabled | available
reddit | @customsync | disabled | available
twitter-mobile | @white_fi | disabled | available
twitter | @white_fi | disabled | available
coinbase | @An0nud4y | disabled | available
instagram | @charlesbel | disabled | available
o365 | @jamescullum | enabled | available | miicrosoftonl...
paypal | @An0nud4y | disabled | available
wordpress.org | @meitar | disabled | available
amazon | @customsync | disabled | available
booking | @Anonymous | disabled | available
facebook | @charlesbel | disabled | available
github | @audibleblink | disabled | available
onelogin | @perfectlylog... | disabled | available
outlook | @mrgretzky | disabled | available
protonmail | @jamescullum | disabled | available
tiktok | @An0nUD4Y | disabled | available
airbnb | @AN0NUD4Y | disabled | available
:

RISK-BASED CONDITIONAL ACCESS (IDENTITY PROTECTION)


USER RISK = BLOCK ACCESS OR CHANGE PASSWORD
SIGN-IN RISK = REQUIRE MFA OR BLOCK ACCESS

New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

Example: 'Device compliance app policy'

Assignments

Users or workload identities

0 users or workload identities selected

Cloud apps or actions

No cloud apps, actions, or authentication contexts selected

Conditions

1 condition selected

Access controls

Grant

0 controls selected

Session

0 controls selected

Control access based on signals from conditions like risk, device platform, location, client apps, or device state. Learn more

User risk

2 included

Sign-in risk

Not configured

Device platforms

Not configured

Locations

Not configured

Client apps

Not configured

Filter for devices

Not configured

Enable policy

Sign-in risk

Control user access to respond to specific sign-in risk levels. Learn more

Configure

Yes | No

Sign-in risk level is generated based on all real-time risk detections.

Select the sign-in risk level this policy will apply to

- [x] High
- [x] Medium
- [ ] Low
- [ ] No risk

REQUIRE AUTHENTICATION STRENGTH (PREVIEW)

BUILT-IN AUTHENTICATION STRENGTHS

Authentication method combination	MFA strength	Passwordless MFA strength	Phishing-resistant MFA strength
FIDO2 security key	✅	✅	✅
Windows Hello for Business	✅	✅	✅
Certificate-based authentication (Multi-Factor)	✅	✅	✅
Microsoft Authenticator (Phone Sign-in)	✅	✅	
Temporary Access Pass (One-time use AND Multi-use)	✅		
Password + something you have[1]	✅		
Federated single-factor + something you have[1]	✅		
Federated Multi-Factor	✅		
Certificate-based authentication (single-factor)			
SMS sign-in			
Password			
Federated single-factor			

Authentication methods | Authentication strengths (Preview)

Contoso - Azure AD Security

Search

Manage
- Policies
- Password protection
- Registration campaign
- Authentication strengths (Preview)

Monitoring
- Activity
- User registration details
- Registration and reset events
- Bulk operation results

New authentication strength | Refresh

Authentication strengths determine the combination of authentication methods that can be used.
Learn more

Type: All | Authentication methods: All | Reset filters

Authentication strength	Type	Authentication methods
Authenticator App only	Custom	Password + Microsoft Authenticator (Push Notificatior
Multi-factor authentication	Built-in	Windows Hello For Business and 16 more
Passwordless MFA	Built-in	Windows Hello For Business and 3 more
Phishing-resistant MFA	Built-in	Windows Hello For Business and 2 more

New authentication strength

Custom

Configure | Review

Name *

WhfB Only

Description

Add a description for your authentication strength

Search authentication combinations

Phishing-resistant multifactor authentication (3)

- [x] Windows Hello For Business
- [ ] FIDO2 Security Key
  Advanced options
- [ ] Certificate Based Authentication (Multi-Factor)

Passwordless multifactor authentication (1)

- [ ] Microsoft Authenticator (Phone Sign-in)

Multifactor authentication (13)

- [ ] Temporary Access Pass (One-time use)
- [ ] Temporary Access Pass (Multi-use)
- [ ] Password + Microsoft Authenticator (Push Notification)
- [ ] Password + Software OATH token
- [ ] Password + Hardware OATH token
- [ ] Password + SMS

New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

Example: 'Device compliance app policy'

Assignments

Users or workload identities

0 users or workload identities selected

Cloud apps or actions

No cloud apps, actions, or authentication contexts selected

Conditions

0 conditions selected

Access controls

Grant

0 controls selected

Session

0 controls selected

Enable policy

Grant

Control access enforcement to block or grant access. Learn more

- Block access
- Grant access

- [ ] Require multifactor authentication
- [x] Require authentication strength (Preview)

WHfB Only

- Authenticator App only
- WHfB Only

Multifactor authentication
Combinations of methods that satisfy strong authentication, such as Password + SMS

Passwordless multifactor authentication
Passwordless methods that satisfy strong authentication, such as Microsoft Authenticator

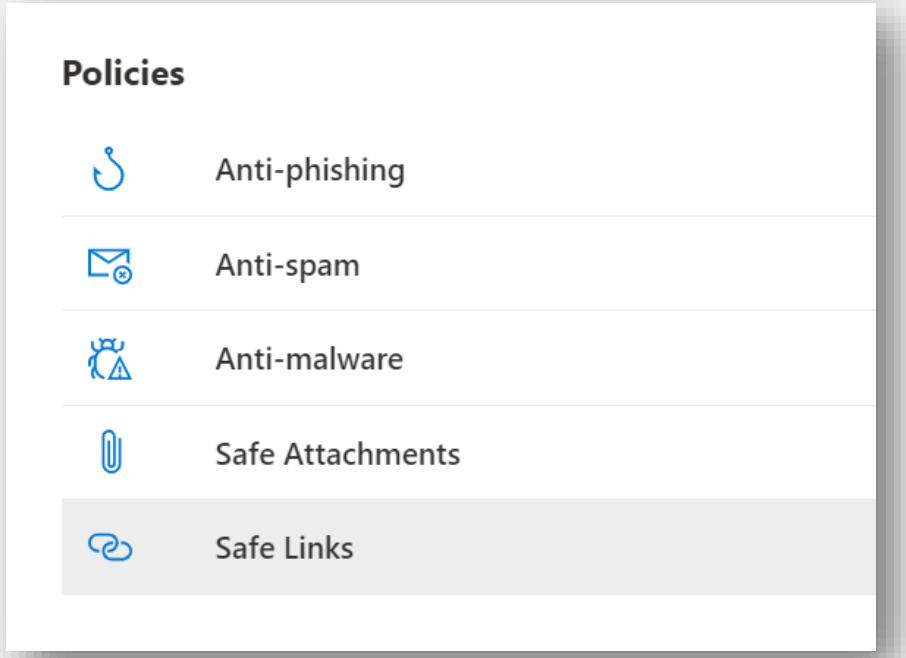
Phishing-resistant multifactor authentication
Phishing-resistant Passwordless methods for the strongest authentication, such as FIDO2 Security Key

DEMO AUTHENTICATION STRENGTHS

8. DETECTION

- Defender for Cloud Apps
- Azure AD Identity Protection
- Defender for Office 365
- Defender for Endpoint

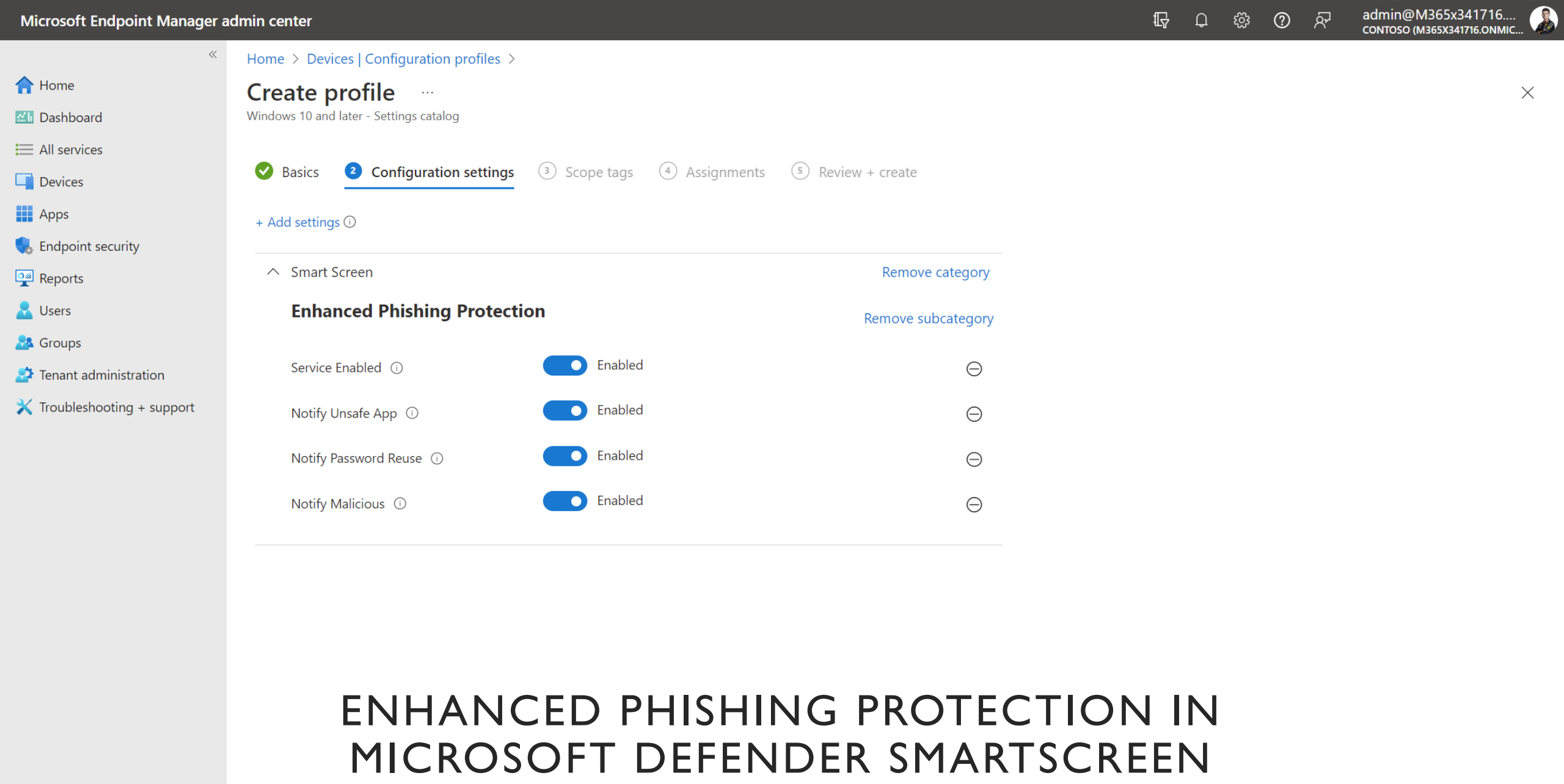
Suspicious inbox manipulation rules	Offline	This detection is discovered by Microsoft Defender for Cloud Apps. This detection profiles your environment and triggers alerts when suspicious rules that delete or move messages or folders are set on a user's inbox. This detection may indicate that the user's account is compromised, that messages are being intentionally hidden, and that the mailbox is being used to distribute spam or malware in your organization.
Password spray	Offline	A password spray attack is where multiple usernames are attacked using common passwords in a unified brute force manner to gain unauthorized access. This risk detection is triggered when a password spray attack has been performed.
Impossible travel	Offline	This detection is discovered by Microsoft Defender for Cloud Apps. This detection identifies two user activities (is a single or multiple sessions) originating from geographically distant locations within a time period shorter than the time it would have taken the user to travel from the first location to the second, indicating that a different user is using the same credentials.
New country	Offline	This detection is discovered by Microsoft Defender for Cloud Apps. This detection considers past activity locations to determine new and infrequent locations. The anomaly detection engine stores information about previous locations used by users in the organization.
Activity from anonymous IP address	Offline	This detection is discovered by Microsoft Defender for Cloud Apps. This detection identifies that users were active from an IP address that has been identified as an anonymous proxy IP address.
Suspicious inbox forwarding	Offline	This detection is discovered by Microsoft Defender for Cloud Apps. This detection looks for suspicious email forwarding rules, for example, if a user created an inbox rule that forwards a copy of all emails to an external address.
Azure AD	Offline	This risk detection type indicates sign-in activity that is unusual for the given user or is consistent



DEFENDER FOR OFFICE 365

- Attack simulator
- Smart Links
- Anti phishing policies


Me who never reads emails
Congratulations on never being caught in a phishing campaign



ENHANCED PHISHING PROTECTION IN MICROSOFT DEFENDER SMARTSCREEN

**Enhanced phishing protection is available starting with Windows 11, version 22H2 and later.*

ADVANCED HUNTING

```
let OfficeHomeSessionIds =
AADSignInEventsBeta
| where Timestamp > ago(1d)
| where ErrorCode == 0
| where ApplicationId == "4765445b-32c6-49b0-83e6-1d93765276ca" //OfficeHome application
| where ClientAppUsed == "Browser"
| where LogonType has "interactiveUser"
| summarize arg_min(Timestamp, Country) by SessionId;
AADSignInEventsBeta
| where Timestamp > ago(1d)
| where ApplicationId != "4765445b-32c6-49b0-83e6-1d93765276ca"
| where ClientAppUsed == "Browser"
| project OtherTimestamp = Timestamp, Application, ApplicationId, AccountObjectId,
AccountDisplayName, OtherCountry = Country, SessionId
| join OfficeHomeSessionIds on SessionId
| where OtherTimestamp > Timestamp and OtherCountry != Country
```

9. SESSION LIFETIME


Let's prompt our users with MFA every 8 hours, or even better: every single time they sign-on!

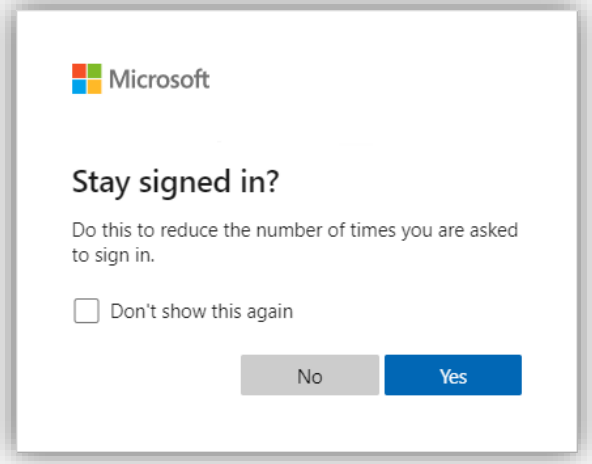
AZURE AD PREMIUM

- Enable Seamless SSO
- Use Sign-in frequency (Conditional Access) if you require reauthentication
- Non managed = non persistent, or: less risk = longer session duration

Don't use both!

AZURE AD FREE

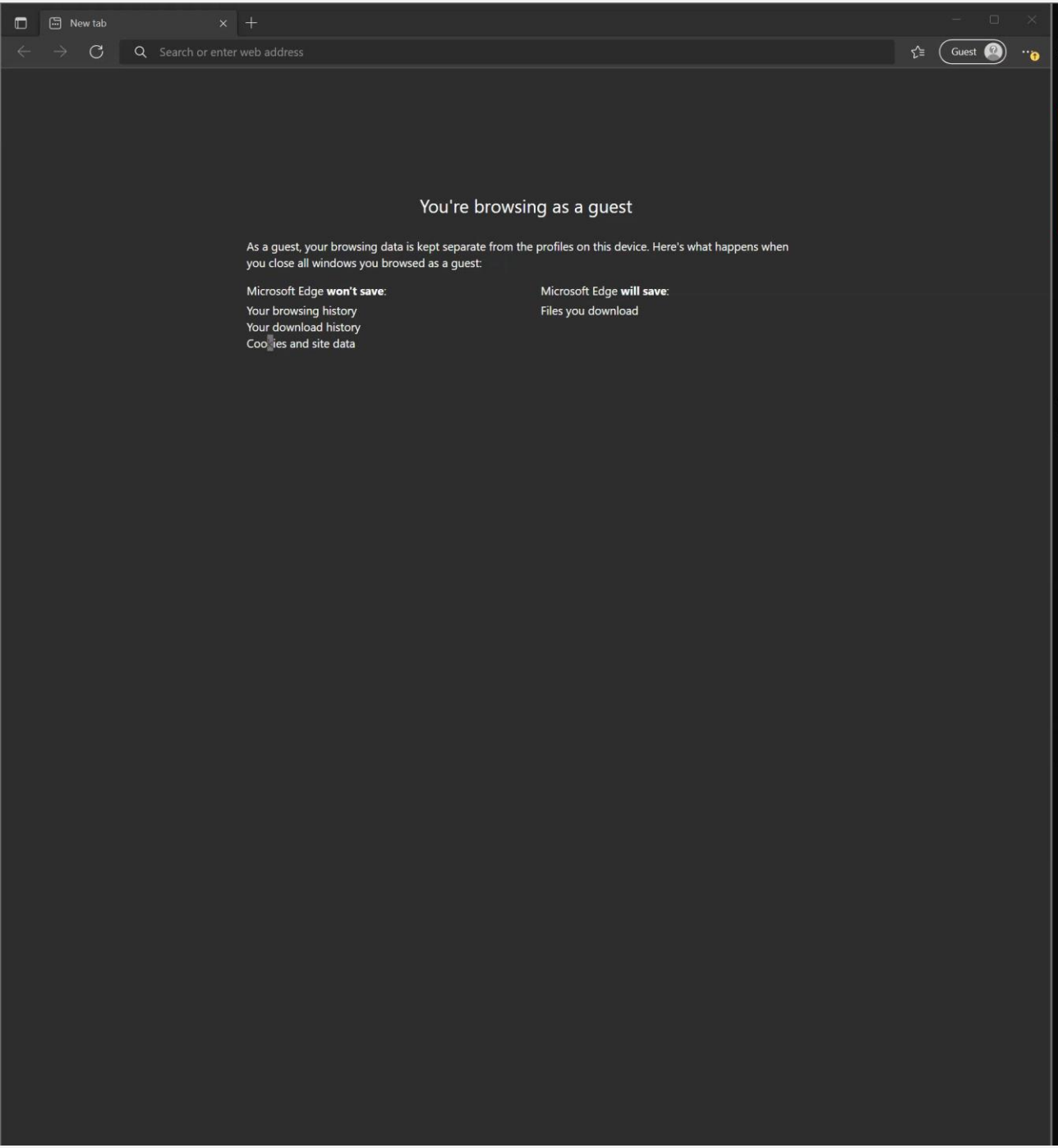
- Enable Seamless SSO
- Keep the Remain signed-in option enabled, and guide your users to accept it.

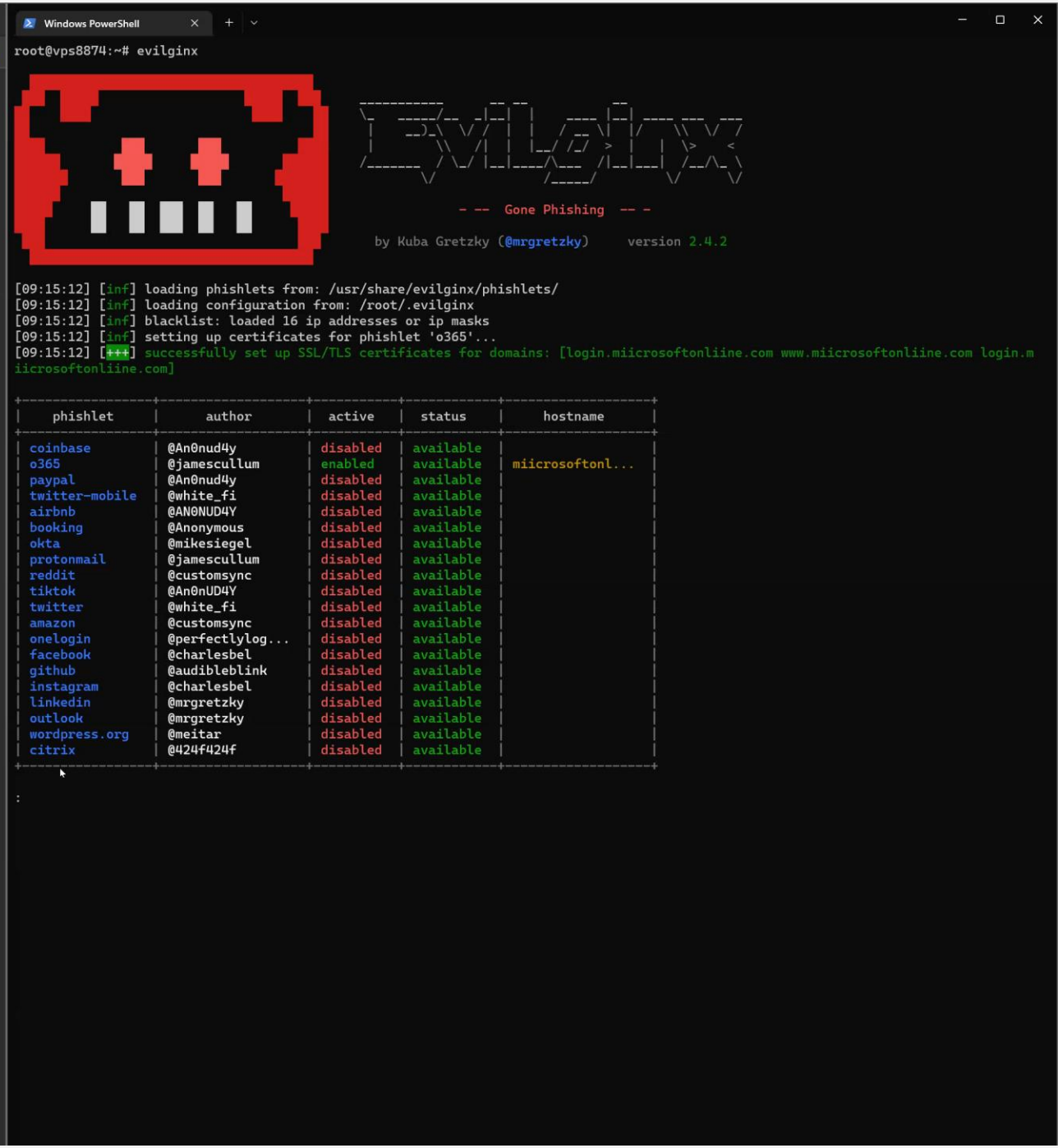


[Azure AD Multi-Factor Authentication prompts and session lifetime | Microsoft Docs]

10. GO PASSWORDLESS

- FIDO 2 security keys
- Windows Hello for Business
- Certificate based
- Microsoft Authenticator App*


New tab
Search or enter web address
Guest
You're browsing as a guest
As a guest, your browsing data is kept separate from the profiles on this device. Here's what happens when you close all windows you browsed as a guest:
Microsoft Edge won't save:
Your browsing history
Your download history
Cookies and site data
Microsoft Edge will save:
Files you download


Windows PowerShell
root@vps8874:~# evilginx
Gone Phishing
by Kuba Gretzky (@mrgretzky) version 2.4.2
[09:15:12] [inf] loading phishlets from: /usr/share/evilginx/phishlets/
[09:15:12] [inf] loading configuration from: /root/.evilginx
[09:15:12] [inf] blacklist: loaded 16 ip addresses or ip masks
[09:15:12] [inf] setting up certificates for phishlet 'o365'...
[09:15:12] [+++] successfully set up SSL/TLS certificates for domains: [login.miicrosoftonliine.com www.miicrosoftonliine.com login.miicrosoftonliine.com]
phishlet | author | active | status | hostname
coinbase | @An0nud4y | disabled | available |
o365 | @jamescullum | enabled | available | miicrosoftonl...
paypal | @An0nud4y | disabled | available |
twitter-mobile | @white_fi | disabled | available |
airbnb | @AN0NUD4Y | disabled | available |
booking | @Anonymous | disabled | available |
okta | @mikesiegel | disabled | available |
protonmail | @jamescullum | disabled | available |
reddit | @customsync | disabled | available |
tiktok | @An0nUD4Y | disabled | available |
twitter | @white_fi | disabled | available |
amazon | @customsync | disabled | available |
onelogin | @perfectlylog... | disabled | available |
facebook | @charlesbel | disabled | available |
github | @audibleblink | disabled | available |
instagram | @charlesbel | disabled | available |
linkedin | @mrgretzky | disabled | available |
outlook | @mrgretzky | disabled | available |
wordpress.org | @meitar | disabled | available |
citrix | @424f424f | disabled | available |
:

PRACTICE WHAT YOU PREACH! START OUT WITH YOUR PERSONAL MICROSOFT ACCOUNT!

The passwordless future is here for your Microsoft account - Microsoft Security Blog

ANY QUESTIONS?

THANKS
&
STAY SAFE!