

The logo for Lou MUG consists of the word "Lou" in white, bold, sans-serif font on a red square background, and the word "MUG" in white, bold, sans-serif font on a yellow square background. A green square is partially visible behind the "Lou" square.

Lou
MUG

Microsoft Security

Upcoming Roadmap Features &
Tales Of The Wild

Friday, November 18, 2022
11:30AM - 1:00PM



Josh Gatewood

- Certs
 - Azure Admin Associate
 - Identity and Access Admin Associate
 - Security Admin Associate
 - Azure Security Engineer Associate
 - Cloud Fundamentals
 - Security, Compliance and Identity Fundamentals
 - GCP Infrastructure Admin

The Microsoft Solutions Partner logo is located in a white rounded rectangle on a purple-to-orange gradient background. It features the Microsoft logo (four colored squares: red, green, blue, yellow) to the left of the text "Microsoft" in a bold, black, sans-serif font, with "Solutions Partner" in a smaller, black, sans-serif font below it.

Microsoft
Solutions Partner

Security



My Babies

My Password is Password

Bad: Password

123456

qwerty

password

iloveyou

Password1

Good: Password and...



SMS



Voice

Better: Password and...



Authenticator
(Push Notifications)



Software
Tokens OTP



Hardware Tokens OTP
(Preview)

Best: Passwordless



Windows
Hello



Authenticator
(Phone Sign-in)



FIDO2 security key

WHfB – Hybrid Cloud Trust

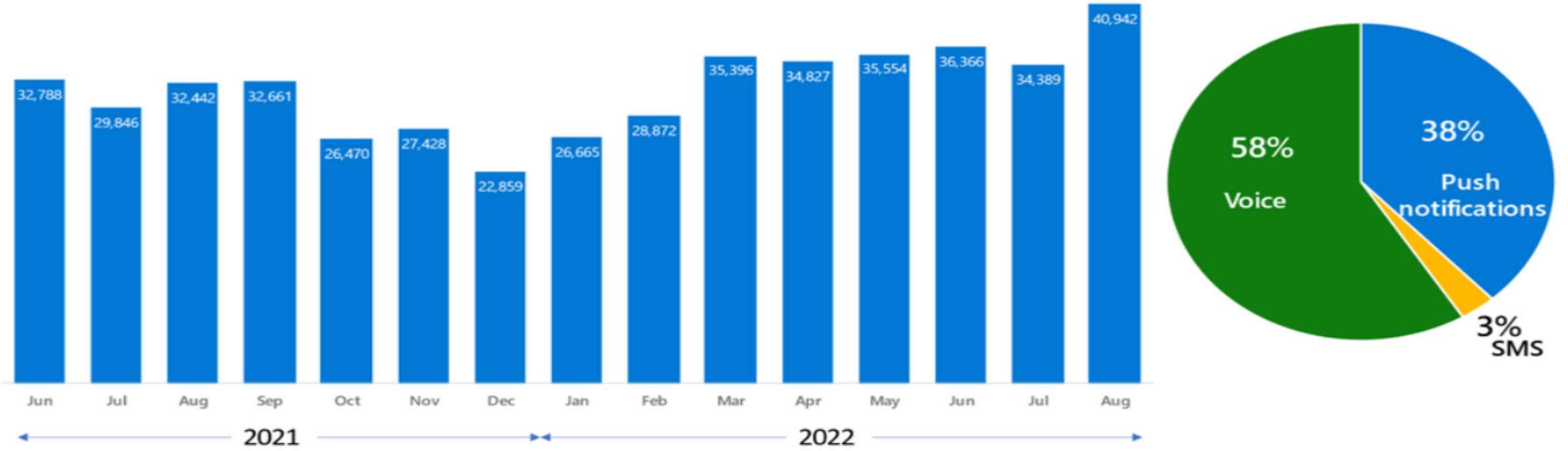
- <https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-hybrid-cloud-kerberos-trust?tabs=intune>

The goal of **Windows Hello for Business cloud Kerberos trust** is to bring the simplified deployment experience of *passwordless security key sign-in* to Windows Hello for Business, and it can be used for new or existing Windows Hello for Business deployments.

Windows Hello for Business cloud Kerberos trust uses **Azure AD Kerberos**, which enables a simpler deployment when compared to the *key trust model*:

- No need to deploy a public key infrastructure (PKI) or to change an existing PKI
- No need to synchronize public keys between Azure AD and Active Directory for users to access on-premises resources. This means that there isn't delay between the user's WHFB provisioning and being able to authenticate to Active Directory
- *Passwordless security key sign-in* can be deployed with minimal extra setup

MFA Fatigue Attacks




Source: Azure AD Identity Protection sessions at high risk with multiple failed MFA attempts

MFA Fatigue

<https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad-blog/defend-your-users-from-mfa-fatigue-attacks/ba-p/2365677>

Number Matching!

 @merill@toot.merill.net @merill · Nov 15
PSA The Microsoft Authenticator app will start enforcing number match on all tenants from Feb 27, 2023

We have some handy change comms templates for you at aka.ms/mfatemplates to inform your users of the change.

Are you trying to sign in?

Patriot Consulting Technology Group LLC.
jgatewood@patriotconsultingtech.com

Enter the number shown to sign in.

App
Azure Portal

Location
KY, United States

No, it's not me **Yes**

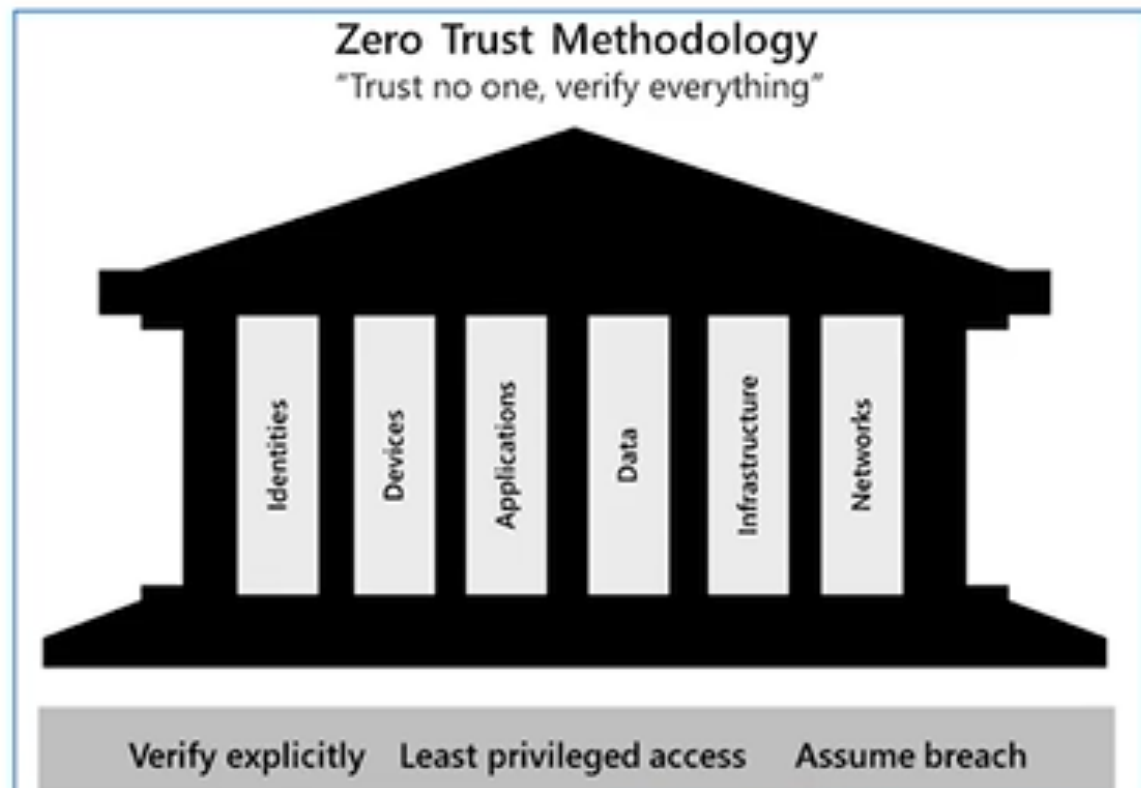
Zero-trust methodology

Zero Trust guiding principles

- Verify explicitly
- Least privileged access
- Assume breach

Six foundational pillars

- **Identities** may be users, services, or devices.
- **Devices** create a large attack surface as data flows.
- **Applications** are the way that data is consumed.
- **Networks** should be segmented.
- **Infrastructure** whether on-premises or cloud based, represents a threat vector.
- **Data** should be classified, labeled, and encrypted based on its attributes.



Mememes



Device Restrictions OLD (2 months ago)

Custom ...

Windows 10 and later

1 Configuration settings **2** Review + save

OMA-URI Settings ⓘ

Add

Export

Name ↑↓	Description ↑↓	OMA-URI ↑↓	Value
Approved	Not configured	./Vendor/MSFT/Defender/Configuration/DeviceControl/...	String (XML file)
RemovalMedia	Not configured	./Vendor/MSFT/Defender/Configuration/DeviceControl/...	String (XML file)
BlockWriteExecute	Not configured	./Vendor/MSFT/Defender/Configuration/DeviceControl/...	String (XML file)

Device Restrictions

Device Control

ID Configured

+ Add Delete

<input checked="" type="checkbox"/> Name	Included ID	Excluded ID	Entry
<input checked="" type="checkbox"/> <input style="border: 1px solid red;" type="text"/>	+ Set reusable settings	+ Set reusable settings	+ Edit Entry

The field for Name is required.

Configure Entry ✕

Name

+ Add Delete


<input type="checkbox"/>	Type * ⓘ	Options * ⓘ	Access mask * ⓘ	Sid ⓘ	Computer Sid ⓘ
<input type="checkbox"/>	Allow	None	Execute	<input checked="" type="text"/>	<input checked="" type="text"/>



- Read
- Write
- Execute

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/device-control-removable-storage-access-control?WT.mc_id=Portal-Microsoft_Intune_Workflows&view=o365-worldwide

Configure reusable settings (preview) ...

Windows 10 and later

 Please review policy.

 Basics  **Configuration settings**  Review + Add

Create an Attack surface reduction setting group that is a reusable list of one or more endpoints defined as different media types. This setting group can be referenced by one or more Device control policies. Each Device control policy can allow or block access to all endpoints in this setting. If this setting group is edited after it's been created, any changes will automatically apply to the policies that reference this setting group.

Device Control

Match type  Match any

[+ Add](#) [Delete](#)

Name Configure settings

[+ Edit instance](#)

The field for Name is required.

Previous

Next

Configure instance ✕

Device Control

Device class 

Device ID  

Friendly name  

A string uniquely identifies the device in the system, for example, USBSTOR\DISK&VEN_GENERIC&PROD_FLASH_DISK&REV_8.07\8735B611&0

[Learn more](#)

Instance ID  

Name

Primary ID  

Product ID  


Serial number  

Vendor ID  

Vendor ID and Product ID  

Save

M365maps.com

 Microsoft 365 Licensing						
By Aaron Dinnage — January, 2022						
Enterprise Mobility + Security (EMS)	Full	Simple	E3	E5	Azure AD	
Microsoft 365 Apps	Full	Business	Enterprise			
Microsoft 365 Business	Full	Basic	Standard	Premium		
Microsoft 365 Consumer	Full	Family	Office			
Microsoft 365 Education	Full	A1 (Legacy)	A1 for Devices	A3	A5	
Microsoft 365 Student Use Benefit	Venn	Simple				
Microsoft 365 Enterprise	Simple	Venn	Landscape	E3	E5	
Microsoft 365 Frontline	Full	F1	F3	F5		
Microsoft Defender	Business	Endpoint	Office 365			
Microsoft Project and Visio	Project	Visio				
Microsoft Teams Rooms	Full	Premium				
Office 365 Education	Full	Simple				
Office 365 Enterprise *	Full	Simple	E1	E3	E5	F3
Windows	Enterprise	Pro	VL	Windows 365		
Client Access License (CAL) *	CALs	Main Bridges	Other Bridges	All Bridges		

Your Speaker Coach Insights

Private

* Your Speaker Coach report is only visible to you.



Good work! Next time, try paying a bit more attention to your repetitive language and filler words.

🕒 12:09

Time spent speaking

💬 74

Suggestions to review

Suggestions from your meeting

64 Repetitive Language

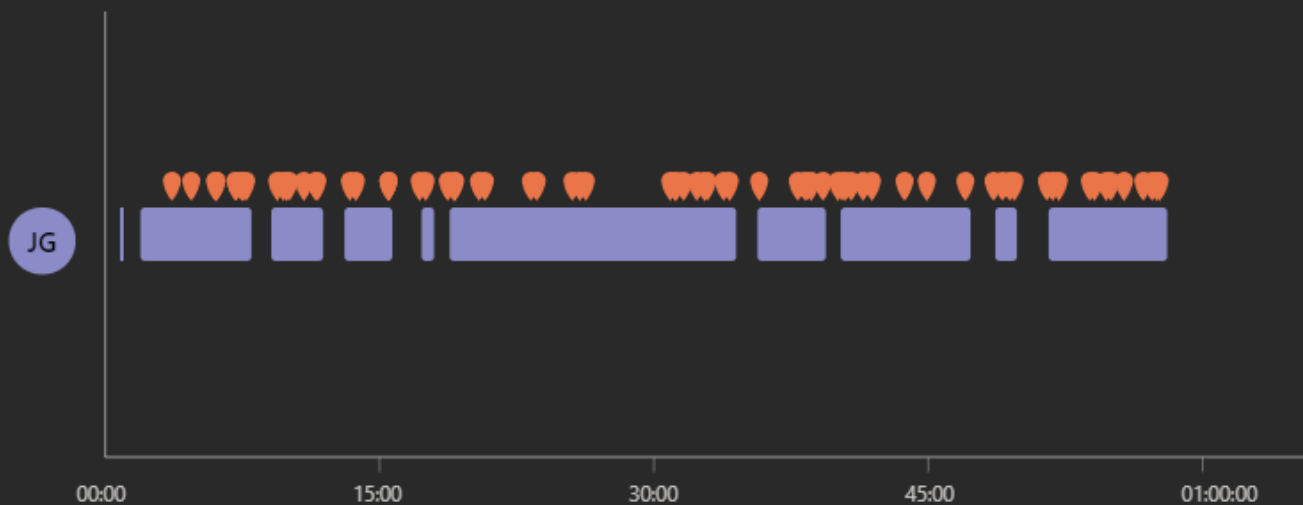
8 Filler Words

1 Pace

1 Inclusiveness

✓ Intonation

✓ Monologue



Your Speaker Coach Insights

Private

* Your Speaker Coach report is only visible to you.



Good work! Next time, try paying a bit more attention to your repetitive language and filler words.

🕒 14:13

Time spent speaking

💬 96

Suggestions to review

Suggestions from your meeting

76 Repetitive Language

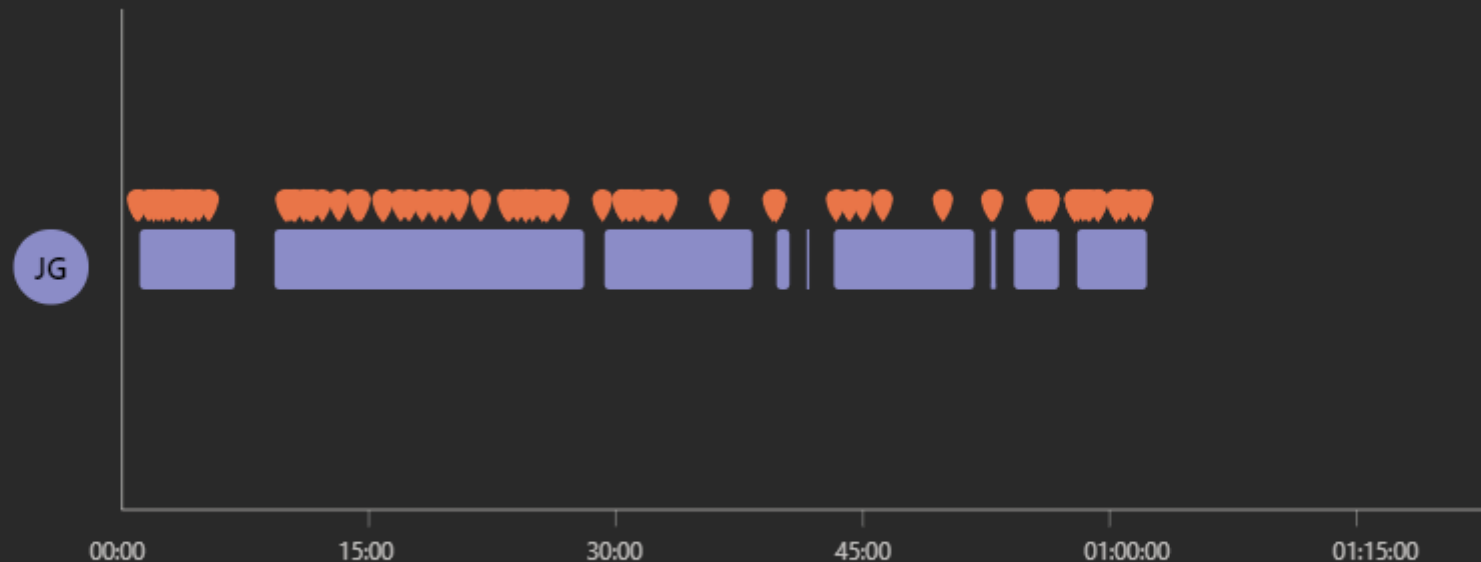
17 Filler Words

3 Inclusiveness

✓ Pace

✓ Intonation

✓ Monologue



< Inclusiveness

Consider replacing or avoiding these terms or phrases, which might offend some people.

It looks like you said:

you guys

Alternative Phrase:

→ "you all"

< 3 of 3 >

< Repetitive Language

You repeatedly used these words during the meeting:

alright 50

perfect 14

cool 12

< Filler Words

Try to avoid these filler words. (Click each word to see on the timeline)

like 9

uhh 3

umm 2

You know 2

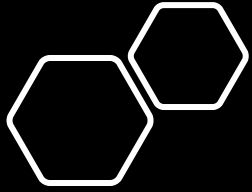
I mean 1

What you will hear me say



On the Horizon





SPAM Toast

<https://techcommunity.microsoft.com/t5/windows-it-pro-blog/deliver-organizational-messages-with-windows-11-and-microsoft/ba-p/3651011>

The screenshot shows the Microsoft Endpoint Manager admin center interface. The breadcrumb navigation is 'Home > Tenant admin'. The main heading is 'Tenant admin | Organizational messages (preview)'. A search bar is present. The left-hand navigation pane includes: Tenant status, Remote help, Microsoft Tunnel Gateway, Connectors and tokens, Filters, Roles, Azure AD Privileged Identity Management, Diagnostics settings, Audit logs, Device diagnostics, Multi Admin Approval, Premium add-ons, End user experiences, Customization, Organizational messages (preview) (highlighted), Custom notifications, and Terms and conditions. The main content area has tabs for 'Overview' and 'Message'. Under 'Overview', there is a section 'What are Organizational messages?' with a description: 'You can send messages with your organization's logo directly to your users through their Windows 11 devices. Select from a variety of common messages for display just above their taskbar, in their Notifications, or when they run the Get Started app. [Learn more about organizational messages](#)'. Below this are three columns: 'Taskbar messages' (Choose this message type to display a message on users' desktops, just above their taskbar. The message repeats with a frequency you set until the user acts on it. View button), 'Notifications area messages' (Select this message type to display a message in your users' Notifications. The message repeats with a frequency you set until the user acts on it. View button), and 'Get Started app messages' (These messages appear just once, the first time the Get Started app runs after a device is enrolled in Intune. View button). A section 'Before you create a message:' contains three numbered steps: 1. Ensure the required mobile device management (MDM) policy settings are set to Allow. [Learn more about MDM policy settings](#). 2. Decide whether to block messages directly from Microsoft, while allowing admin messages to display. [Learn more about controlling messages](#). A toggle switch is set to 'Allow'. 3. Prepare logos for your org in PNG format with a transparent background. You'll need three sizes: 48 x 48 pixels used for messages in the Notifications area, 64 x 64 pixel images used for messages attached to the Taskbar, and 50 pixels high x 50-100 pixels wide used for Get Started app messages.

Premium Intune SKU



Remote Help



Tunnel for Mobile App Management



Endpoint Privilege Management



Advanced endpoint analytics



More to come...



New LAPS – Called Windows LAPS

Benefits of using Windows LAPS

Use Windows LAPS to regularly rotate and manage local administrator account passwords and get these benefits:

- Protection against pass-the-hash and lateral-traversal attacks
- Improved security for remote help desk scenarios
- Ability to sign in to and recover devices that are otherwise inaccessible
- A fine-grained security model (access control lists and optional password encryption) for securing passwords that are stored in Windows Server Active Directory
- Support for the Azure role-based access control model for securing passwords that are stored in Azure Active Directory

<https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-overview>

Enhanced Phishing Protection in Microsoft Defender SmartScreen

Phishing protection

When you sign into Windows using a password, help protect your password from malicious apps and sites.



On

- Warn me about malicious apps and sites
- Warn me about password reuse
- Warn me about unsafe password storage

[Learn more](#)



Chromium and Win 11 22H2

Settings picker

Use commas "," among search terms to lookup settings by their keywords

🔍 phishing protection

Search

+ Add filter

Browse by category

Smart Screen\ Enhanced Phishing Protection

4 results in the "Enhanced Phishing Protection" subcategory

Select all these settings

Setting name

- | | | |
|--------------------------|-----------------------|---|
| <input type="checkbox"/> | Notify Malicious | ⓘ |
| <input type="checkbox"/> | Notify Password Reuse | ⓘ |
| <input type="checkbox"/> | Notify Unsafe App | ⓘ |
| <input type="checkbox"/> | Service Enabled | ⓘ |

<https://learn.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-smartscreen/phishing-protection-microsoft-defender-smartscreen?tabs=intune>

Trends and Observations



The background is a dark teal color with a repeating pattern of colorful speech bubbles. Each bubble is a different color (red, yellow, purple, grey) and contains a white question mark. The bubbles are scattered across the entire page, creating a textured, busy background.

Questions, Comments – Open Forum



Thanks
Everyone

Happy
Thanksgiving

