

MICROSOFT SECURE SCORE V PRAKSI



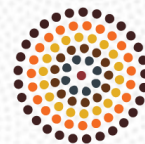
span

MATEJ KLEMENČIČ

Cyber Security Architect

- www.span.eu/si
- www.linkedin.com/company/span
- www.linkedin.com/in/matejklemencic
- matej.klemencic@span.eu
- www.matej.guru



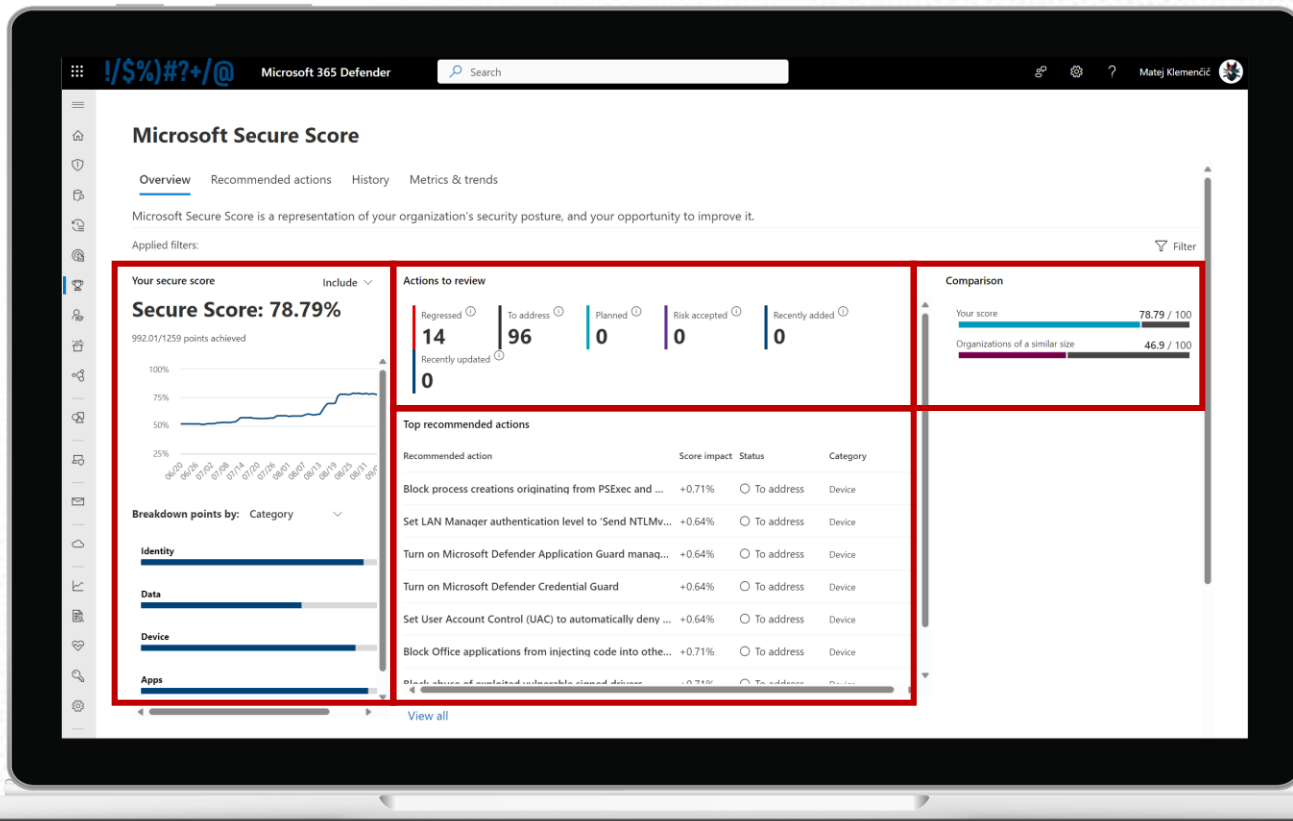


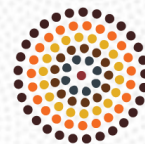
MICROSOFT SECURE SCORE

Vidljivost in smernice za krepitev kibernetске higiene

ODGOVORI NA VARNOSTNA VPRAŠANJA

- Kakšna je varnostna ocena?
- Kje začeti?
- Kako ukrepati?



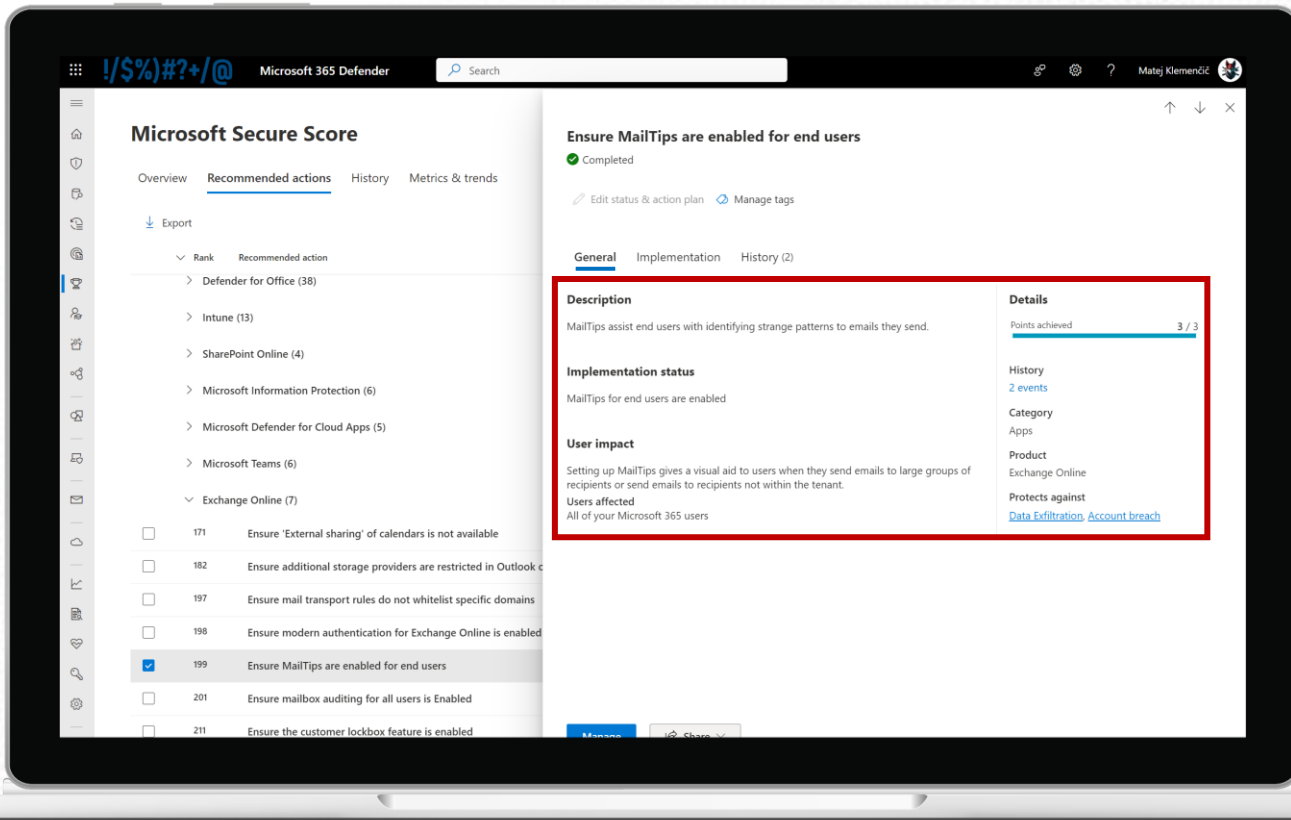


MICROSOFT SECURE SCORE

Vidljivost in smernice za krepitev kibernetске higijene

ODGOVORI NA VARNOSTNA VPRAŠANJA

- Kakšna je varnostna ocena?
- Kje začeti?
- Kako ukrepati?



Microsoft 365 Defender

Microsoft Secure Score

Overview **Recommended actions** History Metrics & trends

Export

Rank	Recommended action
>	Defender for Office (38)
>	Intune (13)
>	SharePoint Online (4)
>	Microsoft Information Protection (6)
>	Microsoft Defender for Cloud Apps (5)
>	Microsoft Teams (6)
>	Exchange Online (7)
<input type="checkbox"/>	171 Ensure 'External sharing' of calendars is not available
<input type="checkbox"/>	182 Ensure additional storage providers are restricted in Outlook
<input type="checkbox"/>	197 Ensure mail transport rules do not whitelist specific domains
<input type="checkbox"/>	198 Ensure modern authentication for Exchange Online is enabled
<input checked="" type="checkbox"/>	199 Ensure MailTips are enabled for end users
<input type="checkbox"/>	201 Ensure mailbox auditing for all users is Enabled
<input type="checkbox"/>	211 Ensure the customer lockbox feature is enabled

Ensure MailTips are enabled for end users

Completed

Edit status & action plan Manage tags

General **Implementation** History (2)

Description

MailTips assist end users with identifying strange patterns to emails they send.

Implementation status

MailTips for end users are enabled

User impact

Setting up MailTips gives a visual aid to users when they send emails to large groups of recipients or send emails to recipients not within the tenant.

Users affected

All of your Microsoft 365 users

Details

Points achieved **3 / 3**

History

[2 events](#)

Category

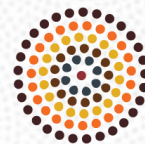
Apps

Product

Exchange Online

Protects against

[Data Exfiltration](#) [Account breach](#)

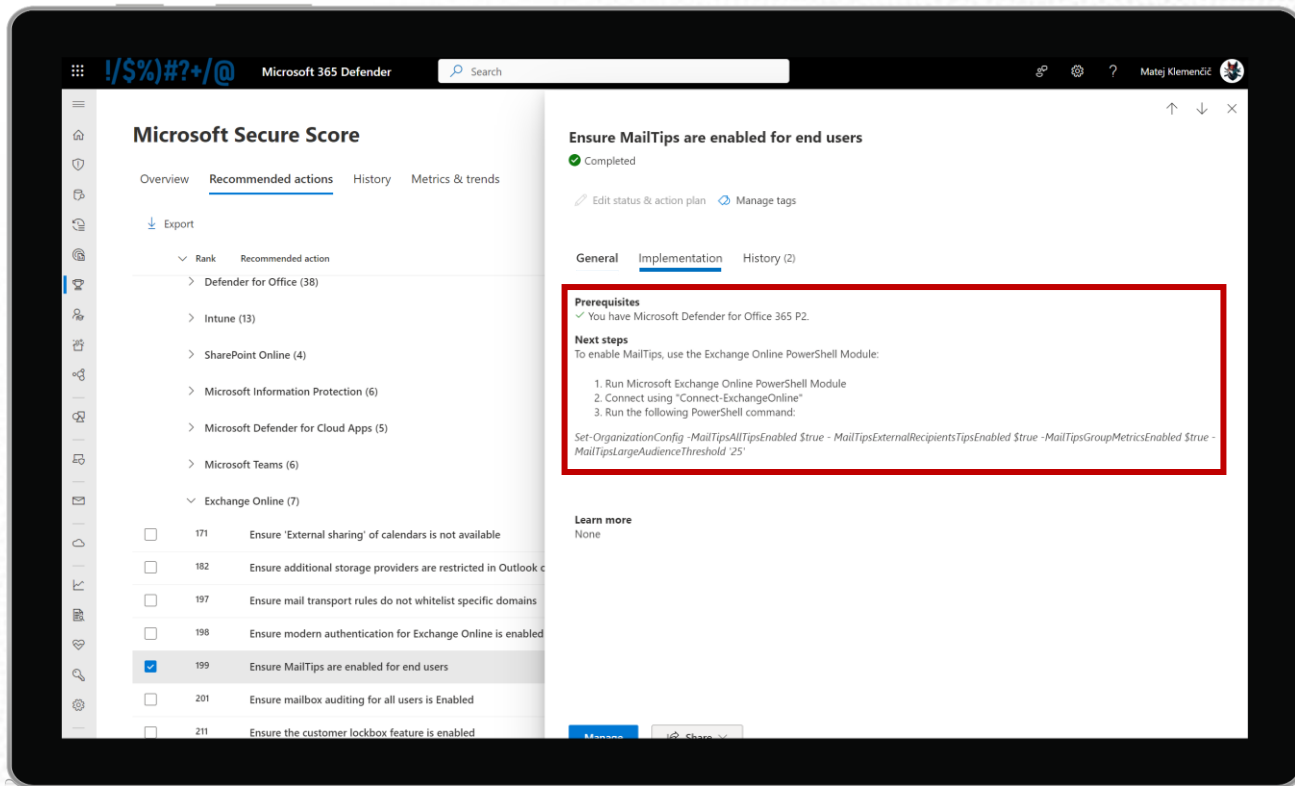


MICROSOFT SECURE SCORE

Vidljivost in smernice za krepitev kibernetске higijene

ODGOVORI NA VARNOSTNA VPRAŠANJA

- Kakšna je varnostna ocena?
- Kje začeti?
- Kako ukrepati?



The screenshot shows the Microsoft 365 Defender interface. The main section is titled "Microsoft Secure Score" and includes tabs for Overview, Recommended actions, History, and Metrics & trends. Under "Recommended actions", there is a list of services and their associated security recommendations. The "Exchange Online (7)" section is expanded, showing a list of recommendations. The recommendation "Ensure MailTips are enabled for end users" (ID 199) is highlighted with a blue checkmark, indicating it is completed. A red box highlights the "Prerequisites" and "Next steps" for this recommendation.

Microsoft Secure Score

Overview Recommended actions History Metrics & trends

Export

Rank	Recommended action
>	Defender for Office (38)
>	Intune (13)
>	SharePoint Online (4)
>	Microsoft Information Protection (6)
>	Microsoft Defender for Cloud Apps (5)
>	Microsoft Teams (6)
>	Exchange Online (7)

ID	Recommendation	Status
171	Ensure 'External sharing' of calendars is not available	Not completed
182	Ensure additional storage providers are restricted in Outlook	Not completed
197	Ensure mail transport rules do not whitelist specific domains	Not completed
198	Ensure modern authentication for Exchange Online is enabled	Not completed
199	Ensure MailTips are enabled for end users	Completed
201	Ensure mailbox auditing for all users is Enabled	Not completed
211	Ensure the customer lockbox feature is enabled	Not completed

Ensure MailTips are enabled for end users

Completed

Edit status & action plan Manage tags

General Implementation History (2)

Prerequisites

- ✓ You have Microsoft Defender for Office 365 P2.

Next steps

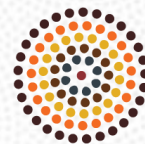
To enable MailTips, use the Exchange Online PowerShell Module:

1. Run Microsoft Exchange Online PowerShell Module
2. Connect using "Connect-ExchangeOnline"
3. Run the following PowerShell command:

```
Set-OrganizationConfig -MailTipsAllTipsEnabled $true - MailTipsExternalRecipientsTipsEnabled $true -MailTipsGroupMetricsEnabled $true -MailTipsLargeAudienceThreshold '25'
```

Learn more

None

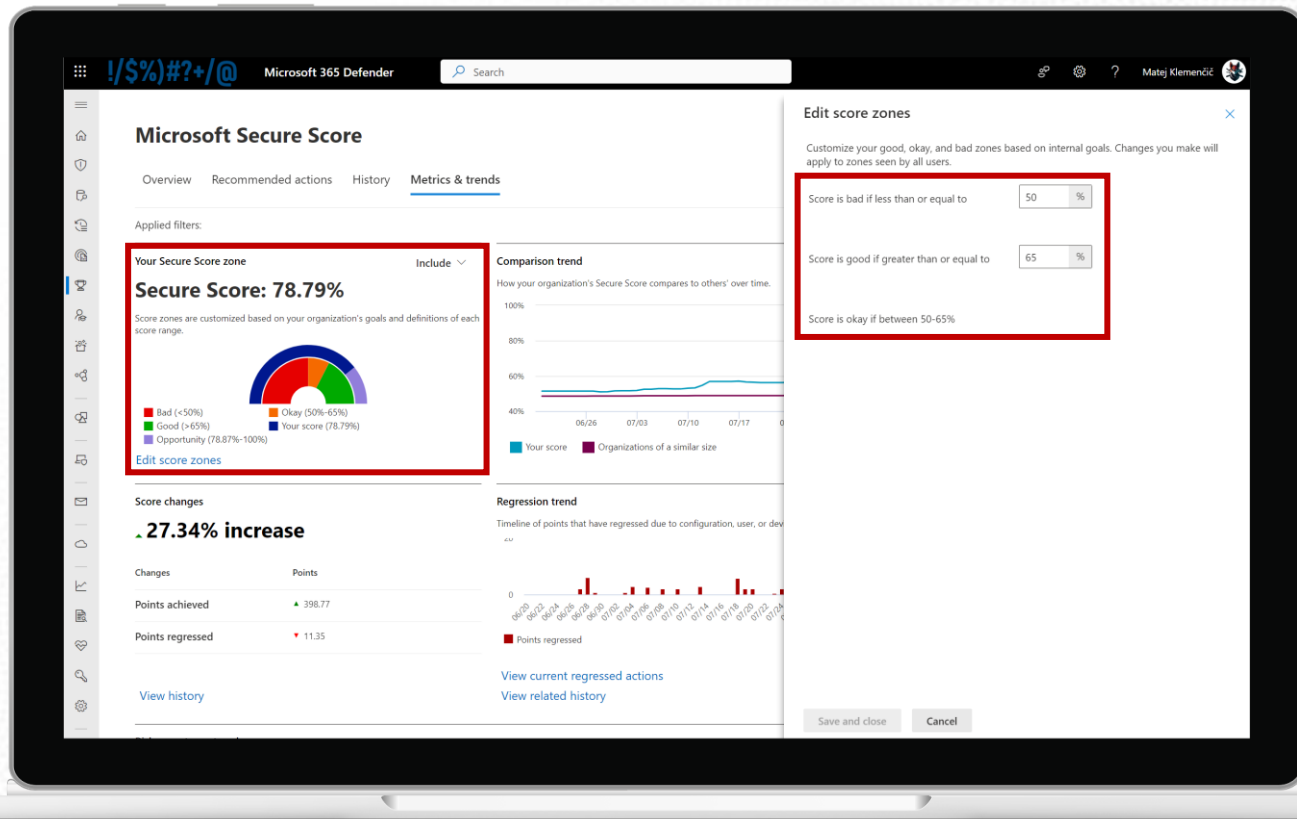


MICROSOFT SECURE SCORE

Vidljivost in smernice za krepitev kibernetске higiene

ODGOVORI NA VARNOSTNA VPRAŠANJA

- Kakšna je varnostna ocena?
- Kje začeti?
- Kako ukrepati?
- Kako spremljati rezultate?
- Kako poročati?





DEMO

Zadnje obvestilo : Plačilo je bilo preklicano



MIMOVRSSTE <bill@mimovsret.com>

Za [REDACTED]

Povezave in druge funkcije v tem sporočilu so onemogočene. Če želite o
To sporočilo smo pretvorili v golo besedilo.

<<https://www.mimovrsste.com/>>

Spoštovana stranka !

To je potrdilo, da je naš obdelovalec plačil obdelal celotno povračilo

Kliknite tukaj, če želite sprožiti vračilo. <<https://rebrand.ly/14babcb>>

Če tega postopka ne opravite v 24/48 urah, se zadeva samodejno z

[Dashboard](#) [Browse](#) [Scan Endpoints](#) [Create Pulse](#) [Submit Sample](#) [API Integration](#)

All mimovsret.com MATEJ.KLE...

DOMAIN

mimovsret.com

Add to Pulse

Submit URL Analysis

Pulses0

Passive DNS4

URLs0

Files0

Analysis Overview

IP Address

Domain Not Currently Resolving to an IP

WHOIS

Registrar: Tucows Domains Inc., Creation Date: Sep 16, 2023

Related Pulses

None

Related Tags

None

Indicator Facts

Registered recently Domain not resolving

Running webserver

External Resources

Whois, UrlVoid, VirusTotal

Analysis

Related Pulses

Comments (0)

Whois

Show 10 entries Search:

RECORD	VALUE
Emails	domainabuse@tucows.com
Name	REDACTED FOR PRIVACY
Name Servers	NS.INMOTIONHOSTING.COM
Org	REDACTED FOR PRIVACY

ENHANCES EOP/MDO POLICIES

- Configuration Analyzer for EOP and Microsoft Defender for Office 365
 - <https://security.microsoft.com/configurationAnalyzer>
- Microsoft Defender for Office 365 Recommended Configuration Analyzer (ORCA)
 - <https://github.com/cammurray/orca>
 - **Install-Module ORCA**
 - **Get-ORCAReport**
 - *Developed by Product Managers at Microsoft, however, is not an official Microsoft utility.*

PASSWORD POLICY

Ensure the 'Password expiration policy' is set to 'Set passwords to never expire (recommended)'

Completed

Edit status & action plan Manage tags

General Implementation History (1)

Description

Research has found that when periodic password resets are enforced, passwords become less secure. Users tend to pick a weaker password and vary it slightly for each reset. If a user creates a strong password (long, complex and without any pragmatic words present) it should remain just as strong in the future as it is today. It is Microsoft's official security position to not expire passwords periodically without a specific reason, and recommends that cloud-only tenants set the password policy to never expire.

Implementation status

Your current policy is set to let passwords expire.

User impact

Your users will no longer need to periodically create new passwords.

Users affected

All of your Microsoft 365 users

Details

Points achieved 8 / 8

History

1 events

Category

Identity

Product

Azure Active Directory

Protects against

[Password Cracking](#), [Account Breach](#)

The following Microsoft Entra password policy requirements apply for all passwords that are created, changed, or reset in Microsoft Entra ID. Requirements are applied during user provisioning, password change, and password reset flows. You can't change these settings except as noted.

Property	Requirements
Characters allowed	Uppercase characters (A - Z) Lowercase characters (a - z) Numbers (0 - 9) Symbols: - @ # \$ % ^ & * - _ ! + = [] { } \ ' , . ? / ` ~ " () ; < > - blank space
Characters not allowed	Unicode characters
Password length	Passwords require - A minimum of eight characters - A maximum of 256 characters
Password complexity	Passwords require three out of four of the following categories: - Uppercase characters - Lowercase characters - Numbers - Symbols Note: Password complexity check isn't required for Education tenants.
Password not recently used	When a user changes their password, the new password should not be the same as the current password.
Password isn't banned by Microsoft Entra Password Protection	The password can't be on the global list of banned passwords for Microsoft Entra Password Protection, or on the customizable list of banned passwords specific to your organization.

PASSWORD POLICY (NIST - 2022)

- ...password policy that requires all **user-created passwords** to have **at least the length of eight**, and all **auto-generated passwords** to be at least **six characters** in length.
- Passwords **should be reset once a year** in order to maintain digital security.
- Changing your password more **frequently** than necessary can actually have a **negative effect** on security since users may use **simple variations of the same password** over time instead of creating stronger ones with each resetting period.
- Passwords which are **known to be frequently used or compromised should be prohibited**.

PASSWORD POLICY (CIS - 2021)

- ...an **eight-character minimum password length** is recommended **for an MFA account**, and **14 characters for a password only account**.
- Password expiration requirements **offer no containment benefits** because attackers will often use credentials as soon as they compromise them.
- ...we also recommend **a yearly password change**. This is primarily because for all their good intentions users will share credentials across accounts.
- Organizations **should ban the use of common bad passwords**.

AZURE ACTIVE DIRECTORY PASSWORD PROTECTION

Ensure password protection is enabled for on-prem Active Directory

✓ Completed

NTK

Edit status & action plan Manage tags

General Implementation History (2)

Description

Enable Azure Active Directory Password Protection to Active Directory to protect against the use of common passwords.

Note: This recommendation applies to Hybrid deployments only, and will have no impact unless working with on-premises Active Directory.

Implementation status

Azure Active Directory Password Protection is enabled

User impact

The potential impact associated with implementation of this setting is dependent upon the existing password policies in place in the environment. For environments that have strong password policies in place, the impact will be minimal. For organizations that do not have strong password policies in place, implementation of Azure Active Directory Password Protection may require users to change passwords, and adhere to more stringent requirements than they have been accustomed to.

Users affected

All of your Microsoft 365 users

Details

Points achieved 6 / 6

History

2 events

Category

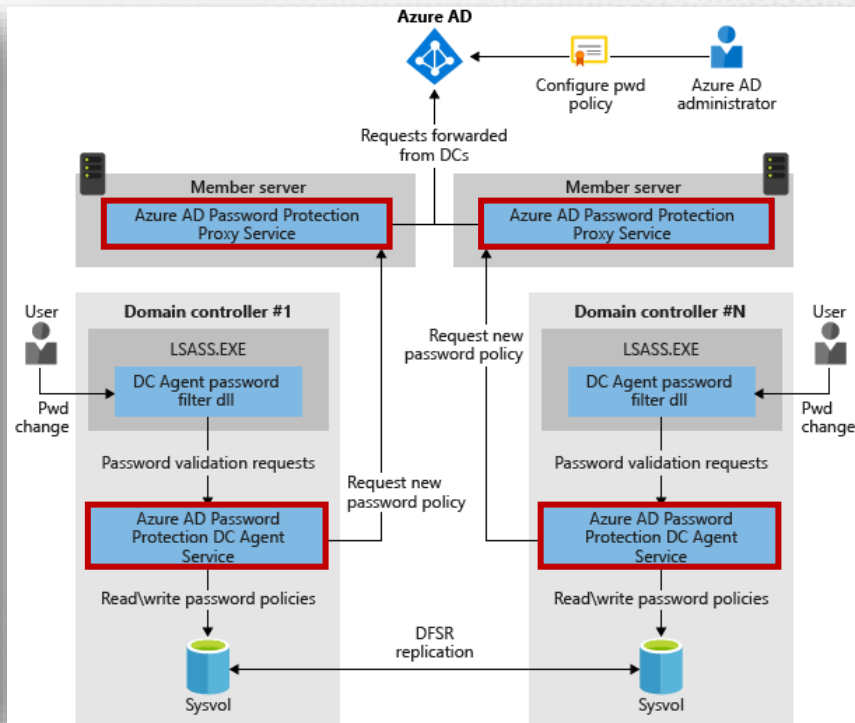
Apps

Product

Azure Active Directory

Protects against

[Data Exfiltration](#) [Password Cracking](#),
[Account breach](#)



LOCAL ADMINISTRATOR ACCOUNT

Disable the built-in Administrator account

☐ To address

NTK

[Go to threat and vulnerability management to take action](#) [Manage tags](#)

General Exposed entities Implementation History (17)

Description

Determines whether the built-in Administrator account is disabled

Implementation status

10/15 exposed devices

Details

Points achieved 2.67 / 8

History

17 events

Category

Enable Local Admin password management

☐ To address

[Go to threat and vulnerability management to take action](#) [Manage tags](#)

General Exposed entities Implementation History (16)

Description

Enables management of password for local administrator account in AD. Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all endpoints during deployment. This poses a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

Details

Points achieved 0.67 / 5

History

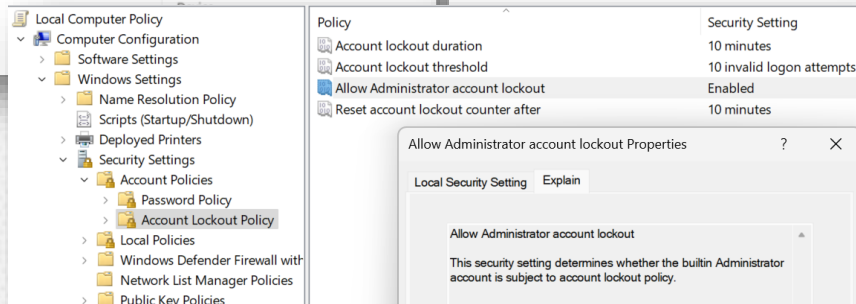
16 events

Category

Device

Product

Defender for Endpoint



IDENTITY PROTECTION

Enable Azure AD Identity Protection sign-in risk policies

☐ To address

 Edit status & action plan  Manage tags

General Implementation History (4)

Description

Turning on the sign-in risk policy ensures that suspicious sign-ins are challenged for multifactor authentication (MFA).

Implementation status

You have 1 of 31 users that don't have the sign-in risky policy turned on.

User impact

When the policy triggers, the user will need MFA to access the account. If a user hasn't registered for MFA, they're blocked from accessing their account. If account access is blocked, an admin would need to recover the account.

Users affected

All of your Microsoft 365 users

Details

Points achieved **6.77 / 7**

History

[4 events](#)

Category

Identity

Product

Azure Active Directory

Protects against

[Password Cracking](#), [Account Breach](#)

Enable Azure AD Identity Protection user risk policies

☐ To address

 Edit status & action plan  Manage tags

General Implementation History (2)

Description

With the user risk policy turned on, Azure Active Directory detects the probability that a user account has been compromised. As an administrator, you can configure a user risk Conditional Access policy to automatically respond to a specific user risk level. For example, you can block access to your resources or require a password change to get a user account back into a clean state.

Implementation status

You have 1 users out of 31 that do not have user risk policy enabled.

User impact

When the policy triggers, access to the account will either be blocked or the user would be required to use multifactor authentication and change their password. Users who haven't registered MFA on their account will be blocked from accessing it. If account access is blocked, an admin would need to recover the account. Thus, it is important to configure the MFA registration policy for all users who are a part of the user risk policy to ensure that they have registered MFA.

Users affected

All of your Microsoft 365 users

Details

Points achieved **6.77 / 7**

History

[2 events](#)

Category

Identity

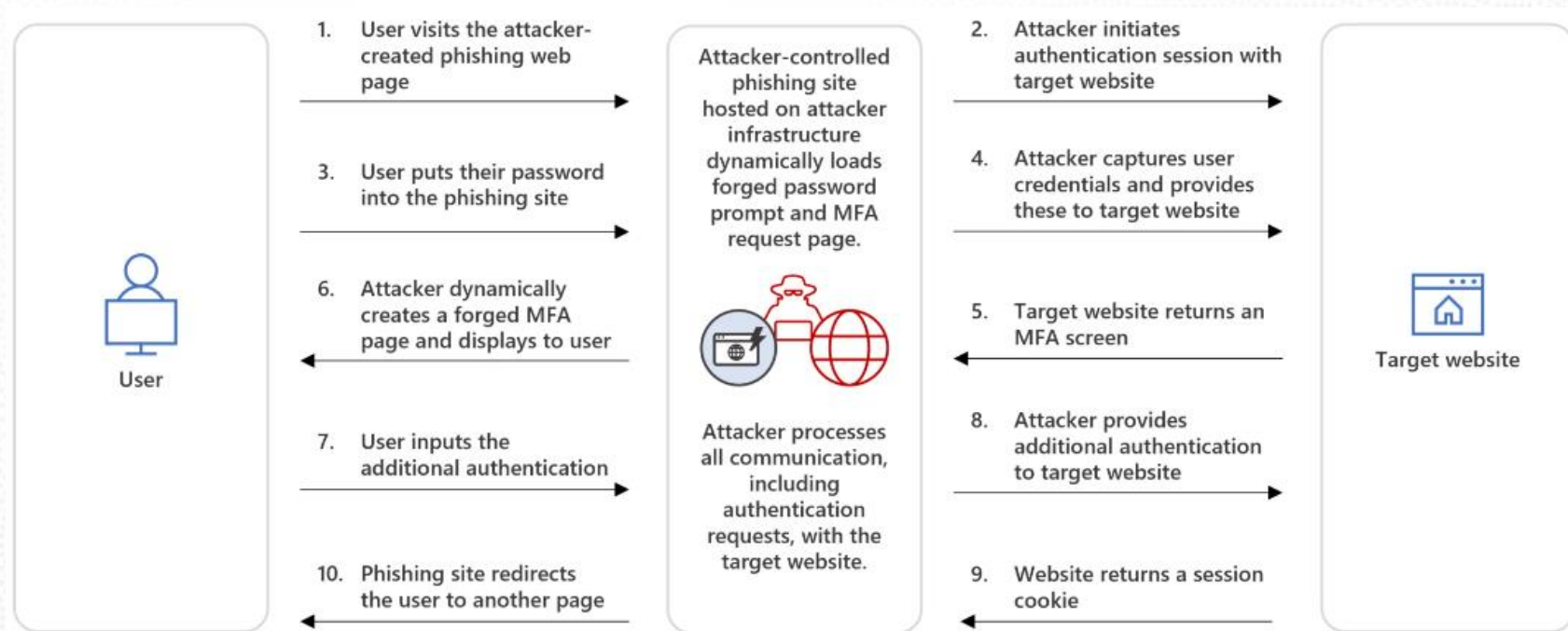
Product

Azure Active Directory

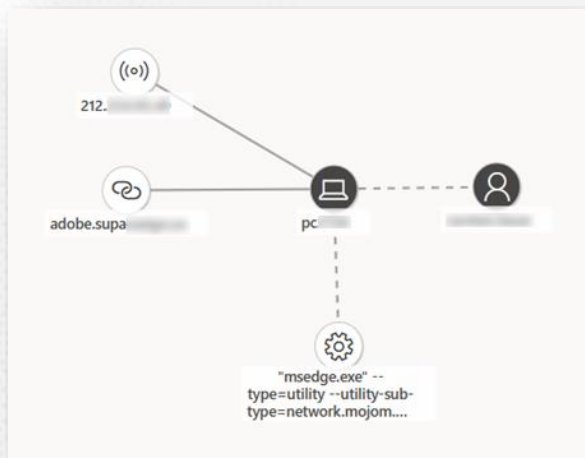
Protects against

[Password Cracking](#), [Account Breach](#)

ADVERSARY-IN-THE-MIDDLE (AiTM)



ADVERSARY-IN-THE-MIDDLE (AiTM)



5/17/2023 2:26:48 PM	✓	⚙	[10504] userinit.exe	...	▼
2:26:49 PM	✓	⚙	[10548] explorer.exe	...	▼
2:27:18 PM	✓	⚙	[7024] msedge.exe --no-startup-window --win-session-start /prefetch:5	...	▼
2:27:18 PM	✓	⚙	[13648] msedge.exe --type=utility --utility-sub-type=network.mojom....	...	▼
5/24/2023 3:36:32 PM		(oo)	Outbound connection from 10.1.10.68:63851 to 212.10.10.10:80	...	▼
<div>⚡ Connection to adversary-in-the-middle (AiTM) phishing site</div> <div>■■■ High ● Detected ● New</div>					

ADVERSARY-IN-THE-MIDDLE (AiTM)

Activity Details: Sign-ins

Basic info	Location	Device info	Authentication Details	Conditional Access	Report-only
Date		5/24/2023, 3:37:22 PM			
Request ID		35301cf2-44b0-43ae-9271			
Correlation ID		77d102aa-1dab-40f1-b0e7			
Authentication requirement		Multifactor authentication			
Status		Success			
Continuous access evaluation		No			
Additional Details		MFA requirement satisfied by claim in the token			
Troubleshoot Event		Follow these steps: Launch the Sign-in Diagnostic. 1. Review the diagnosis and act on suggested fixes.			
User					
Username					

Activity Details: Sign-ins

Basic info	Location	Device info	Authentication Details	Conditional Access	Report-only
Device ID					
Browser		Edge 113.0.1774			
Operating System		Windows 10			
Compliant		No			
Managed		No			
Join Type					

Activity Details: Sign-ins

Basic info	Location	Device info	Authentication Details	Conditional Access	Report-only
Device ID		7ec6a48f-c878-4cab-a6f7			
Browser		Edge 18.19045			
Operating System		Windows 10			
Compliant		Yes			
Managed		Yes			
Join Type		Azure AD joined			

ENTERPRISE APPLICATIONS

Ensure user consent to apps accessing company data on their behalf is not allowed

✓ Alternate mitigation

[Edit status & action plan](#) [Manage tags](#)

General Implementation History (2)

Description

To reduce the risk of malicious applications attempting to trick users into granting them access to your organization's data, we recommend that you allow user consent only for applications that have been published by a verified publisher.

Implementation status

You have marked this action as resolved through alternate mitigation.

User impact

When the consent policy is triggered, users cannot consent to unreliable apps. However, if the admin consent request is configured, it gives admins a secure way to review apps before granting access.

Users affected

All of your Microsoft 365 users

Details

Points achieved **4 / 4**

History

[2 events](#)

Category

Identity

Product

Azure Active Directory

Protects against

[Data Exfiltration](#) [Data Spillage](#)

Ensure the admin consent workflow is enabled

✓ Completed

NTK

[Edit status & action plan](#) [Manage tags](#)

General Implementation

Description

Without an admin consent workflow (Preview), a user in a tenant where user consent is disabled will be blocked when they try to access any app that requires permissions to access organizational data. The user sees a generic error message that says they're unauthorized to access the app and they should ask their admin for help. The admin consent workflow (Preview) gives admins a secure way to grant access to applications that require admin approval. When a user tries to access an application but is unable to provide consent, they can send a request for admin approval. The request is sent via email to admins who have been designated as reviewers. A reviewer acts on the request, and the user is notified of the action.

Implementation status

Admin consent workflow is: true

User impact

None.

Users affected

All of your Microsoft 365 users

Details

Points achieved **5 / 5**

History

[0 events](#)

Category

Apps

Product

Azure Active Directory

Protects against

[Data Exfiltration](#)

MICROSOFT DEFENDER ANTIVIRUS UPDATES

Update Microsoft Defender Antivirus definitions

✔ Completed

NTK

[Go to threat and vulnerability management to take action](#) [Manage tags](#)

General

Exposed entities

Implementation

History (9)

Description

This status indicates that Microsoft Defender Antivirus definitions are not up to date. Not having the latest antivirus definitions could potentially expose you to recently discovered viruses.

Implementation status

0/16 exposed devices

Details

Points achieved 9 / 9

History

[9 events](#)

Category

Device

Product

Defender for Endpoint

QUESTIONS?



span

THANK YOU

www.span.eu