NIC Cloud Connect

Oslo Spektrum
November 7 - 9

nic Cloud Connect

WINDOWS 11

MICROSOFT INTUNE

MICROSOFT DEFENDER FOR ENDPOINT

nic Cloud Connect

QUESTIONS?

RESOURCES?

SLIDES?

@ahlbergNicklas

@pierreThoor

Nicklas Ahlberg
Pierre Thoor

Enhancing Security with **Windows 11**: Leveraging Intune and **Defender**, for Ongoing Protection

Windows 10 end of life date: 2025-10-14

Important

Windows 10 will reach end of support on **October 14, 2025**. The current version, **22H2**, will be the **final** version of Windows 10, and all editions will remain in support with monthly security update releases through that date.


THIS
IS FINE


“Windows 11 is the best version of Windows 10!”

NIC Cloud Connect

Windows 11

RAM
4 GB

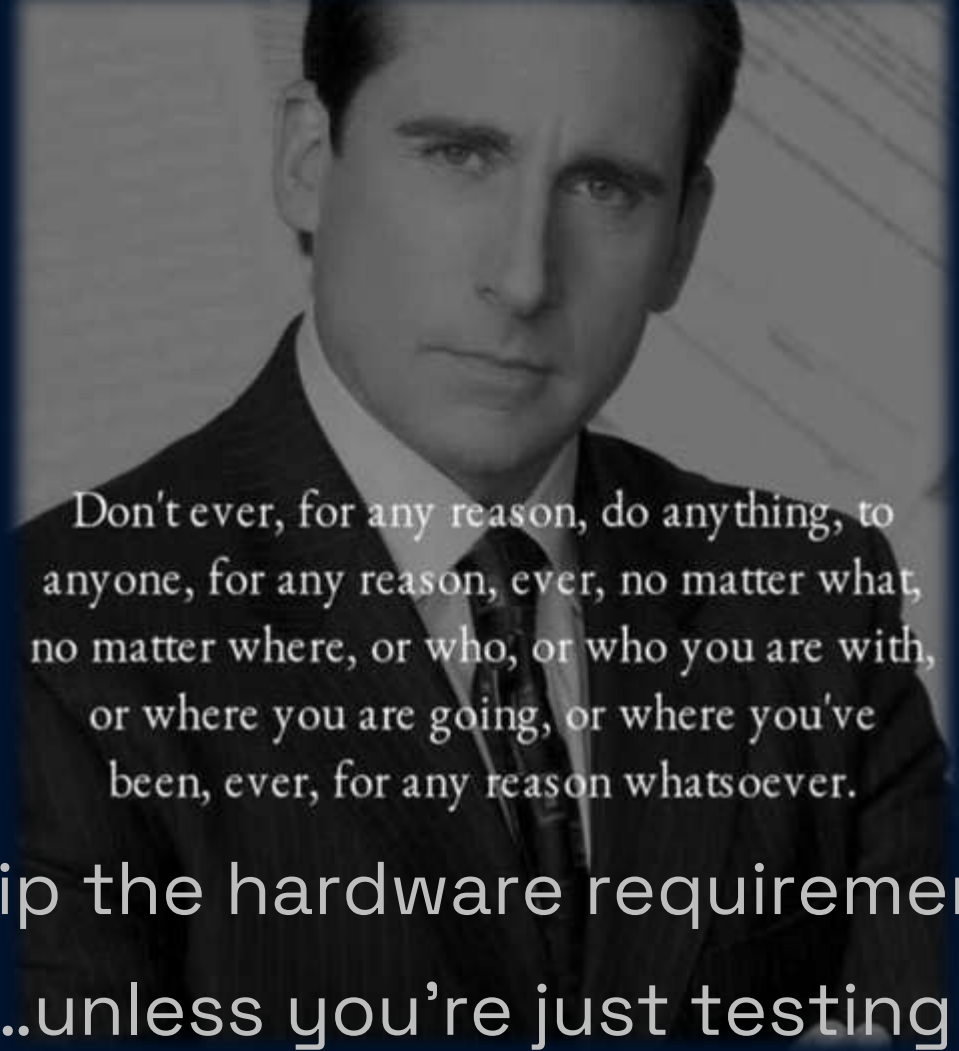
Diskspace
64 GB

CPU
1GHz, 2 cores 64-bit

System firmware
UEFI and Secure Boot capable

TPM
2.0

Display
720p



...skip the hardware requirements!

...unless you're just testing =)

Your device might malfunction due to these compatibility or other issues. Devices that do not meet these system requirements will no longer be guaranteed to receive updates, including but not limited to security updates.

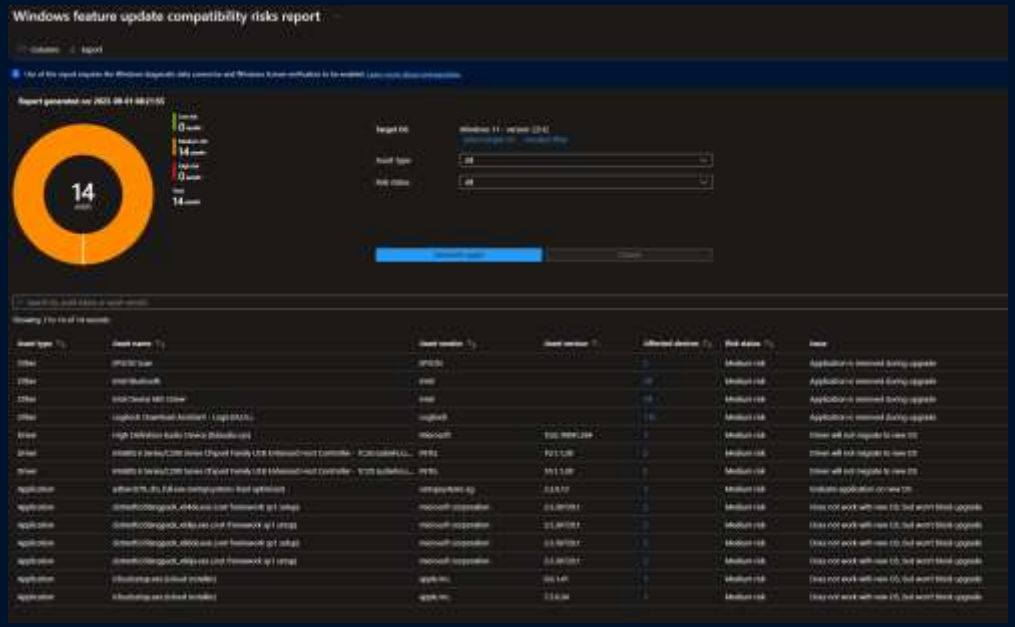
The following disclaimer applies if you install Windows 11 on a device that doesn't meet the minimum system requirements:

This PC doesn't meet the minimum system requirements for running Windows 11 - these requirements help ensure a more reliable and higher quality experience. Installing Windows 11 on this PC is not recommended and may result in compatibility issues. If you proceed with installing Windows 11 your PC will no longer be supported and won't be entitled to receive updates. Damages to your PC due to lack of compatibility aren't covered under the manufacturer warranty.

Installing Windows 11 on devices that don’t meet minimum system requirements - Microsoft Support

How to get there: risk-based approach

- 99,9% app compatibility, but the app lifecycle should be followed!
- Identify your 10 most critical apps and systems, focus on these!
- Test, but trust your OEM (drivers and firmware).
- Do not wait too long, start testing today to have time to solve critical findings.
- Gradual rollout, start with the easy picks.
    - Intelligent rollouts



Windows feature update compatibility risks report

Columns | Export

Use of this report requires the Windows diagnostic data connector and Windows license verification to be enabled. Learn more about prerequisites.

Report generated on: 2023-09-01 08:21:55

Low risk
0 assets

Medium risk
14 assets

High risk
0 assets

Total
14 assets

Target OS: Windows 11 - version 22H2
Select target OS | Unselect filter

Asset Type: All

Risk status: All

Generate again | Cancel

Search by asset name or asset vendor

Showing 1 to 14 of 14 records

Asset type	Asset name	Asset vendor	Asset version	Affected devices	Risk status	Issue
Other	EPSON Scan	EPSON		2	Medium risk	Application is removed during upgrade
Other	Intel Bluetooth	Intel		39	Medium risk	Application is removed during upgrade
Other	Intel Device MEI Driver	Intel		24	Medium risk	Application is removed during upgrade
Other	Logitech Download Assistant - LogiLDA.DLL	Logitech		113	Medium risk	Application is removed during upgrade
Driver	High Definition Audio Device (hdaudio.sys)	Microsoft	10.0.19041.264	1	Medium risk	Driver will not migrate to new OS
Driver	Intel(R) 6 Series/C200 Series Chipset Family USB Enhanced Host Controller - 1C26 (usbehci.s...	INTEL	10.1.1.38	2	Medium risk	Driver will not migrate to new OS
Driver	Intel(R) 6 Series/C200 Series Chipset Family USB Enhanced Host Controller - 1C2D (usbehci.s...	INTEL	10.1.1.38	2	Medium risk	Driver will not migrate to new OS
Application	adberdr70_chs_ful.exe (netopsystems fwad optimizer)	netopsystems ag	2.3.0.12	1	Medium risk	Evaluate application on new OS
Application	dotnetfx35langpack_x64de.exe (.net framework sp1 setup)	microsoft corporation	3.5.30729.1	2	Medium risk	Does not work with new OS, but won't block upgrade
Application	dotnetfx35langpack_x64ja.exe (.net framework sp1 setup)	microsoft corporation	3.5.30729.1	2	Medium risk	Does not work with new OS, but won't block upgrade
Application	dotnetfx35langpack_x86de.exe (.net framework sp1 setup)	microsoft corporation	3.5.30729.1	2	Medium risk	Does not work with new OS, but won't block upgrade
Application	dotnetfx35langpack_x86ja.exe (.net framework sp1 setup)	microsoft corporation	3.5.30729.1	2	Medium risk	Does not work with new OS, but won't block upgrade


Cloud
Protecting your work information
Microsoft Entra ID (formerly AAD)
Modern Device Management (MDM)
Microsoft Security baseline
Microsoft Intune
Local Admin Password solution
Endpoint Privilege Management
Remote Wipe
Microsoft Azure Attestation Service
Windows Update for Business
Windows Autopatch
Windows Autopilot
Enterprise State Roaming with Azure
Universal Print
OneDrive for work or school
MDM enrollment certificate attestation
Protecting your personal information
Microsoft Account
User reauthentication before password disablement
Find my device
OneDrive for personal
OneDrive Personal Vault
Identity
Passwordless sign-in
Window Hello
Window Hello for Business
Windows Hello PIN
Windows Hello biometric - fingerprint recognition
Windows Hello biometric - facial recognition
Windows Hello biometric - enhanced sign-in security (ESS)
Window Hello for Business multi-factor unlock
Passkeys
Windows presence sensing
FIDO support
Microsoft Authenticator app
Smart cards for Windows Service
Federated Sign-in
Advanced credential protection
Microsoft Defender SmartScreen enhanced phishing protection
Local Security Authority (LSA) protection
Credential Guard
Remote Credential Guard
Token Protection
Account Lockout policy
Access management and control
Privacy
Privacy dashboard and report
Privacy transparency and controls
Privacy resource usage
Windows diagnostic data processor configuration
Application
Application and driver control
Smart App Control
App Control for Business
User Account Control
Microsoft vulnerable driver blocklist
Application isolation
Win 32 app isolation
App containers
Windows Sandbox
Operating System
Encryption and data protection
BitLocker drive encryption
BitLocker To Go
Device Encryption
Encrypted hard drive
Personal data encryption (PDE)
Email encryption
Network security
Transport Layer Security (TLS)
Domain Name System (DNS) security
Bluetooth protection
Securing Wi-Fi connections
5G and eSIM
Windows Firewall
Virtual Private Network (VPN)
Server Message Block (SMB) file services
Virus and threat protection
Microsoft Defender SmartScreen
Microsoft Defender Antivirus
Attack surface reduction
Tamper protection
Exploit protection
Controlled folder access
Microsoft Defender for Endpoint
System security
Trusted Boot
Cryptography
Certificates
Code signing and integrity
Device health attestation
Windows security policy settings and auditing
Kiosk Mode (aka Assigned Access)
Config Refresh
Windows Security Settings
Hardware (Chip)
Hardware root-of-trust
Trusted Platform Module (TPM) 2.0
Microsoft Pluton security processor
Silicon-assisted security
Secured kernel
Hardware-enforced stack protection
Kernel Direct Memory Access (DMA) protection
Secured-core PC
Firmware protection
Secured-core configuration lock
Security Foundation
Offensive research
Microsoft Security Development Lifecycle (SDL)
OneFuzz service
Microsoft Offensive Research and Security Engineering (MORSE)
Windows Insiders and Bug Bounty program
Certification
Federal Information Processing Standard (FIPS)
Common Criteria certifications (CC)
Secure supply chain
Software Bill of Materials (SBOM)
Windows application software development kit (SDK)

Local account lockout

- Windows 11-22H2 does protect against brute force accounts through RDP or physical presence.
- Will interfere with WLAPS.

Account Lockout Policy - Windows Security | Microsoft Learn

KB5020282—Account lockout available for built-in local administrators - Microsoft Support

Network List Manager

- Location awareness to properly apply Windows Firewall rules.

```
$URL = "https://myhost.local"
Invoke-WebRequest -Uri $URL -Method get -UseBasicParsing -MaximumRedirection 0
```

NetworkListManager Policy CSP - Windows Client Management | Microsoft Learn

New security features in Windows 11 protect users and empower IT teams | Microsoft Security Blog

Enhanced phishing protection

- Ensure that enterprise credentials are not used for malicious or unintended purposes.

🤩Related user activity is logged in the Microsoft Defender for Endpoint portal.

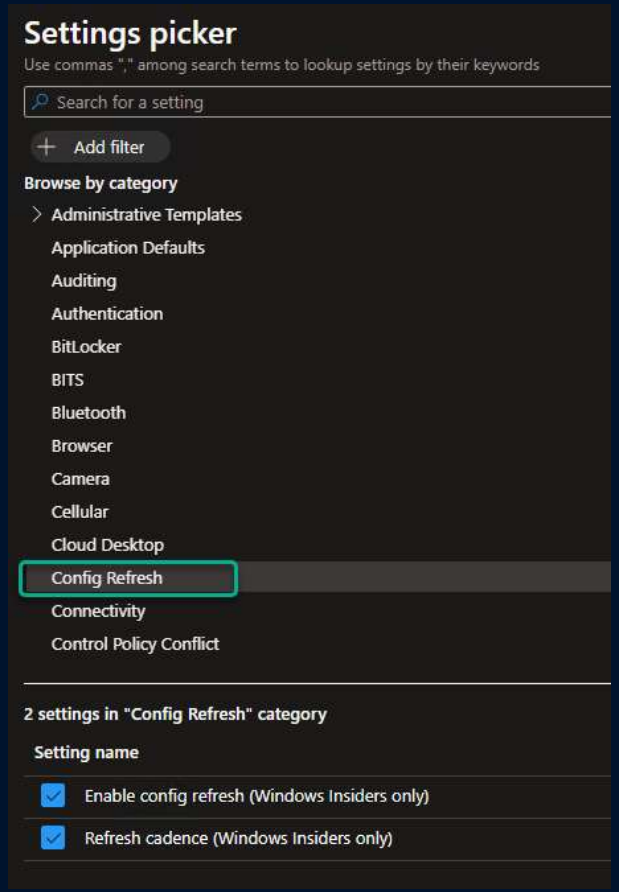
```
DeviceEvents
| where ActionType
has_any('SmartScreenAppWarning',
'SmartScreenUrlWarning')
| extend TriggerReason =
parse_json(AdditionalFields).Exp
erience
```

Enhanced Phishing Protection in Microsoft Defender SmartScreen - Windows Security

Config Refresh

- Ensure that your settings are retained in the way IT configured them.

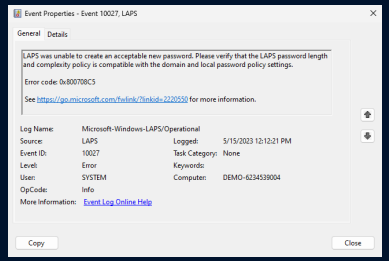
- Insider Release Preview (no 23H2 as for now)
- Settings catalog or CSP
- Enabled/Cadence/PausePeriod

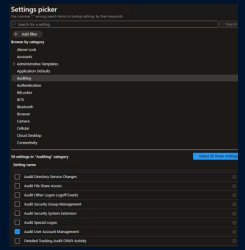


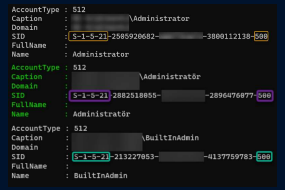
[New security features in Windows 11 protect users and empower IT teams | Microsoft Security Blog]

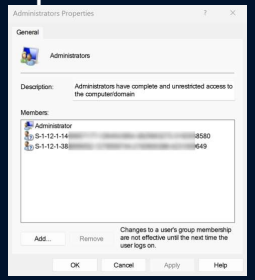
Windows LAPS

- ⭐ Windows LAPS with Entra ID is GA!
- Supports AD & AAD (one at a time)
- Built-in to 2023 April's CU, but works best with 2023-July (and later) update
- Important to have a good rollout strategy
  - **Overlapping/mismatch in password complexity policies!**
  - Rename built-in account!
  - Enable "Audit User Account Management"!
  - Take control of the local administrators group!

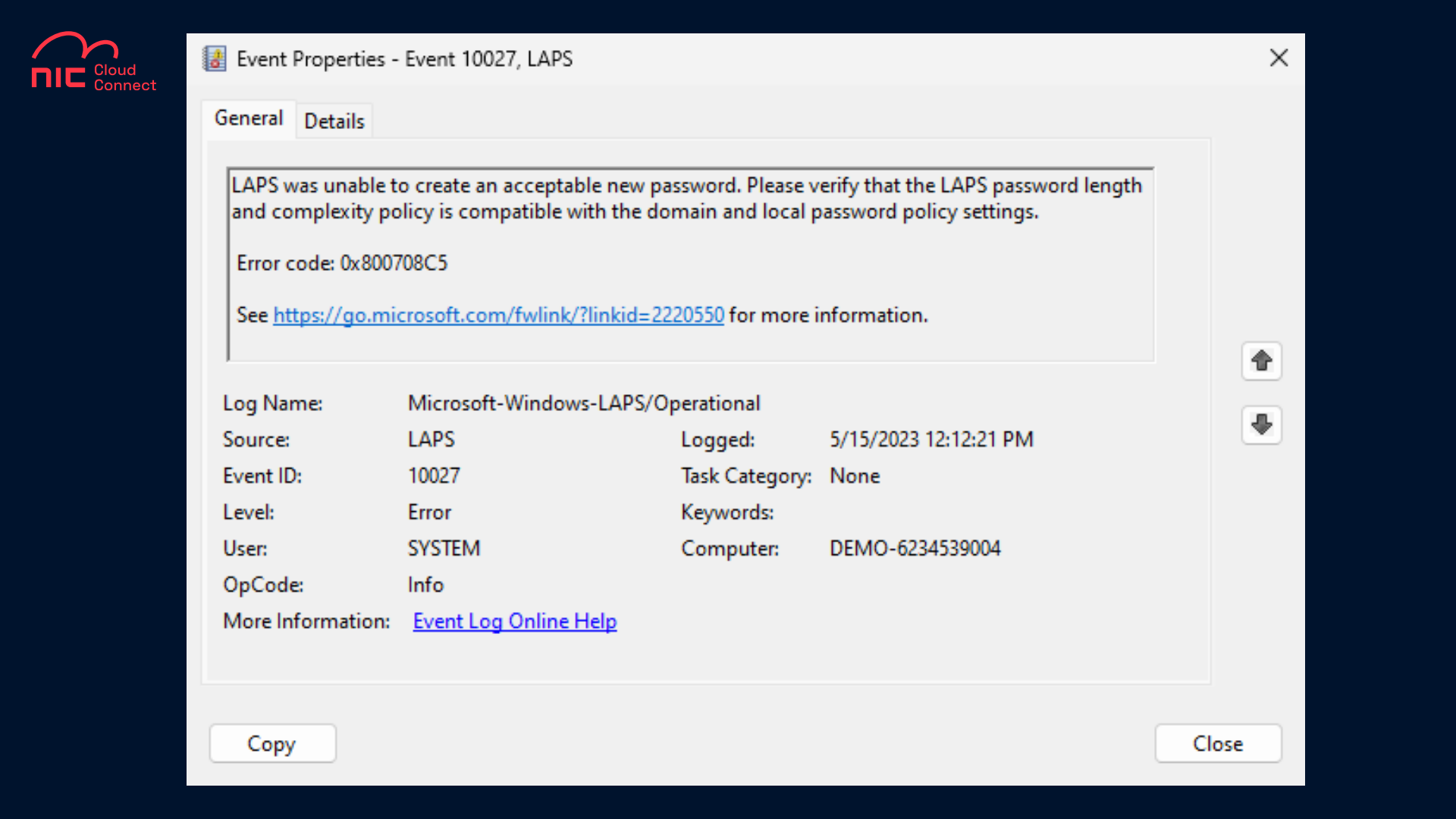




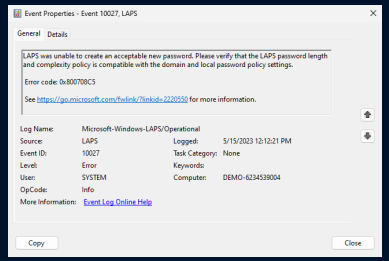


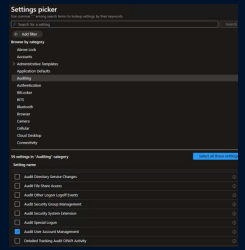


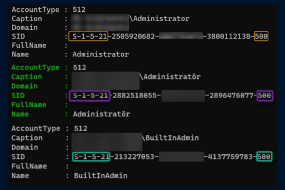
https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-concepts

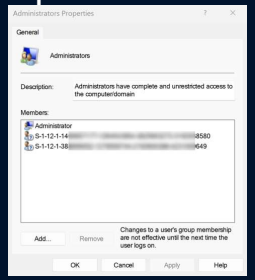

Event Properties - Event 10027, LAPS
General
Details
LAPS was unable to create an acceptable new password. Please verify that the LAPS password length and complexity policy is compatible with the domain and local password policy settings.
Error code: 0x800708C5
See https://go.microsoft.com/fwlink/?linkid=2220550 for more information.
Log Name: Microsoft-Windows-LAPS/Operational
Source: LAPS
Logged: 5/15/2023 12:12:21 PM
Event ID: 10027
Task Category: None
Level: Error
Keywords:
User: SYSTEM
Computer: DEMO-6234539004
OpCode: Info
More Information: Event Log Online Help
Copy
Close

- Windows LAPS was a big challenge, but now in public preview
- Supports AD & AAD (one at a time)
- Built-in to 2023 April's CU
- Important to have a good rollout strategy
  - Overlapping/mismatch in password complexity policies!
  - **Rename built-in account!**
  - Enable "Audit User Account Management"!
  - Take control of the local administrators group!

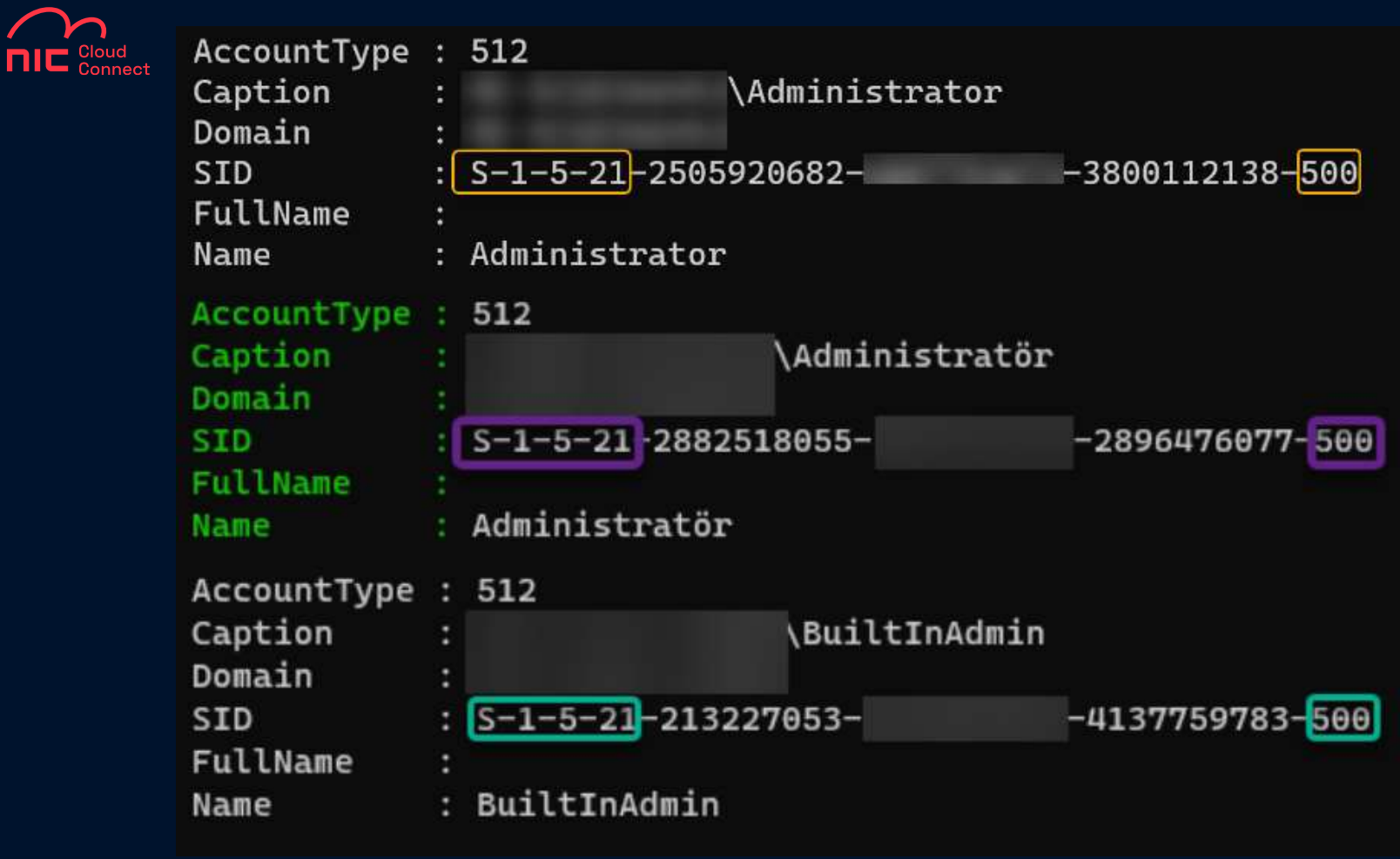




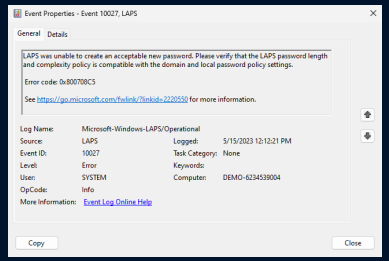


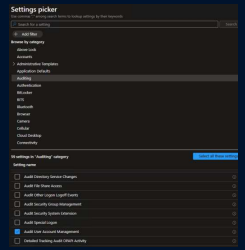


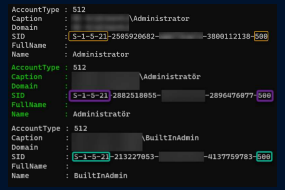
https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-concepts

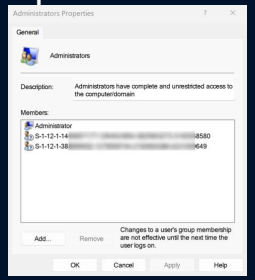

AccountType : 512
Caption : [redacted]\Administrator
Domain : [redacted]
SID : S-1-5-21-2505920682-[redacted]-3800112138-500
FullName :
Name : Administrator
AccountType : 512
Caption : [redacted]\Administratör
Domain : [redacted]
SID : S-1-5-21-2882518055-[redacted]-2896476077-500
FullName :
Name : Administratör
AccountType : 512
Caption : [redacted]\BuiltInAdmin
Domain : [redacted]
SID : S-1-5-21-213227053-[redacted]-4137759783-500
FullName :
Name : BuiltInAdmin

- Windows LAPS was a big challenge, but now in public preview
- Supports AD & AAD (one at a time)
- Built-in to 2023 April's CU
- Important to have a good rollout strategy
  - Overlapping/mismatch in password complexity policies!
  - Rename built-in account!
  - **Enable "Audit User Account Management"!**
  - Take control of the local administrators group!

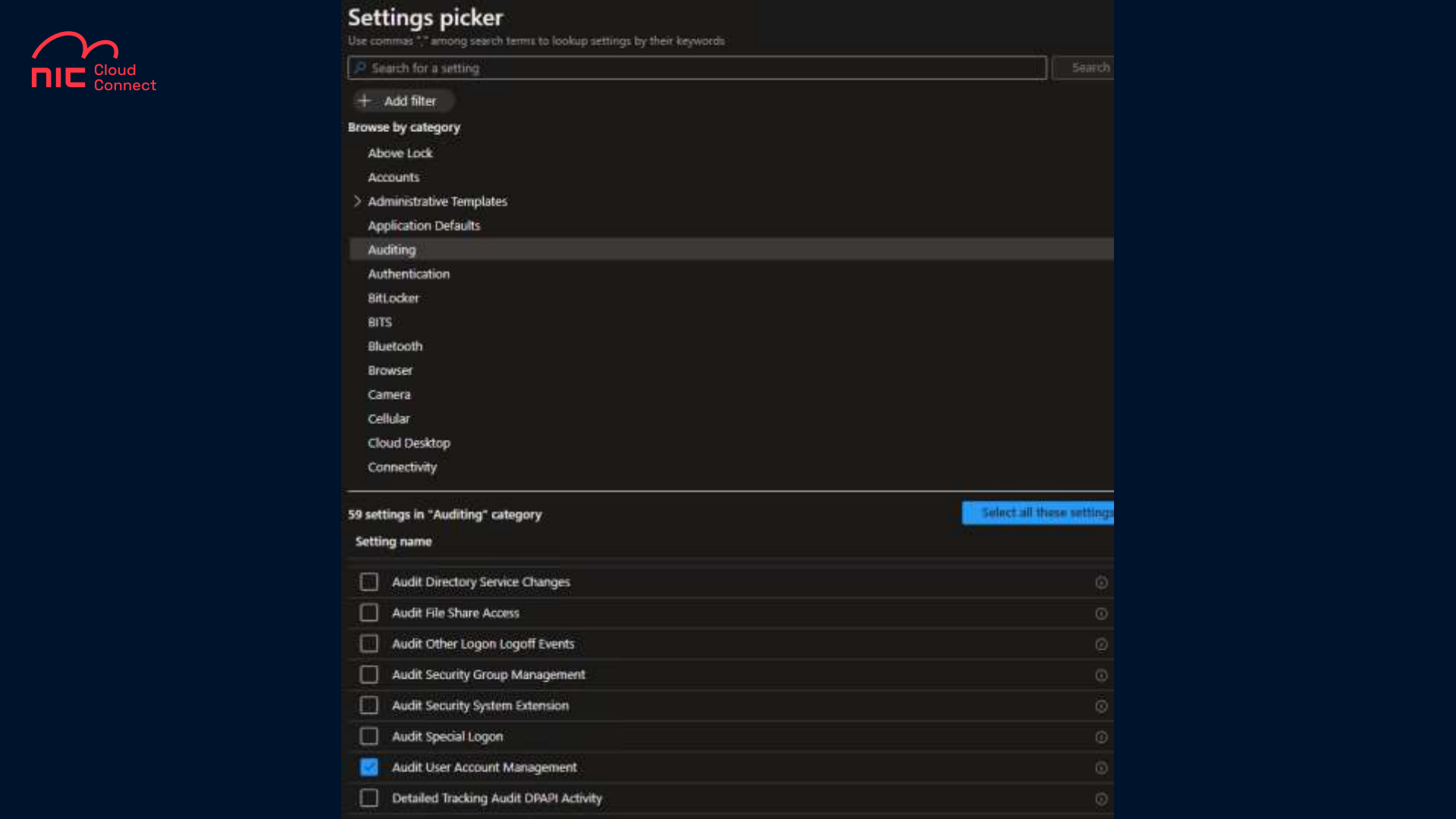




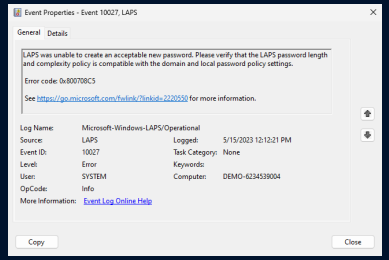


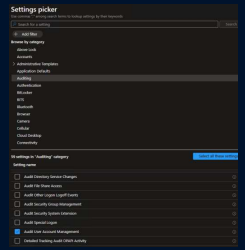


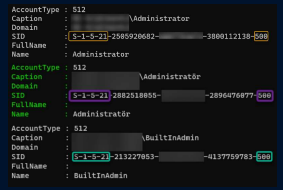
https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-concepts

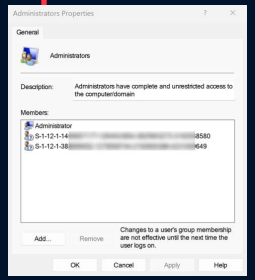

Settings picker
Use commas "," among search terms to lookup settings by their keywords
Search for a setting
Search
Add filter
Browse by category
Above Lock
Accounts
Administrative Templates
Application Defaults
Auditing
Authentication
BitLocker
BITS
Bluetooth
Browser
Camera
Cellular
Cloud Desktop
Connectivity
59 settings in "Auditing" category
Select all these settings
Setting name
Audit Directory Service Changes
Audit File Share Access
Audit Other Logon Logoff Events
Audit Security Group Management
Audit Security System Extension
Audit Special Logon
Audit User Account Management
Detailed Tracking Audit DPAPI Activity

- Windows LAPS was a big challenge, but now in public preview
- Supports AD & AAD (one at a time)
- Built-in to 2023 April's CU
- Important to have a good rollout strategy
  - Overlapping/mismatch in password complexity policies!
  - Rename built-in account!
  - Enable "Audit User Account Management"!
  - **Take control of the local administrators group!**









https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-concepts

Administrators Properties

General

Administrators

Description: Administrators have complete and unrestricted access to the computer/domain

Members:

Administrator
S-1-12-1-14[redacted]8580
S-1-12-1-38[redacted]649

Add... Remove

Changes to a user's group membership are not effective until the next time the user logs on.

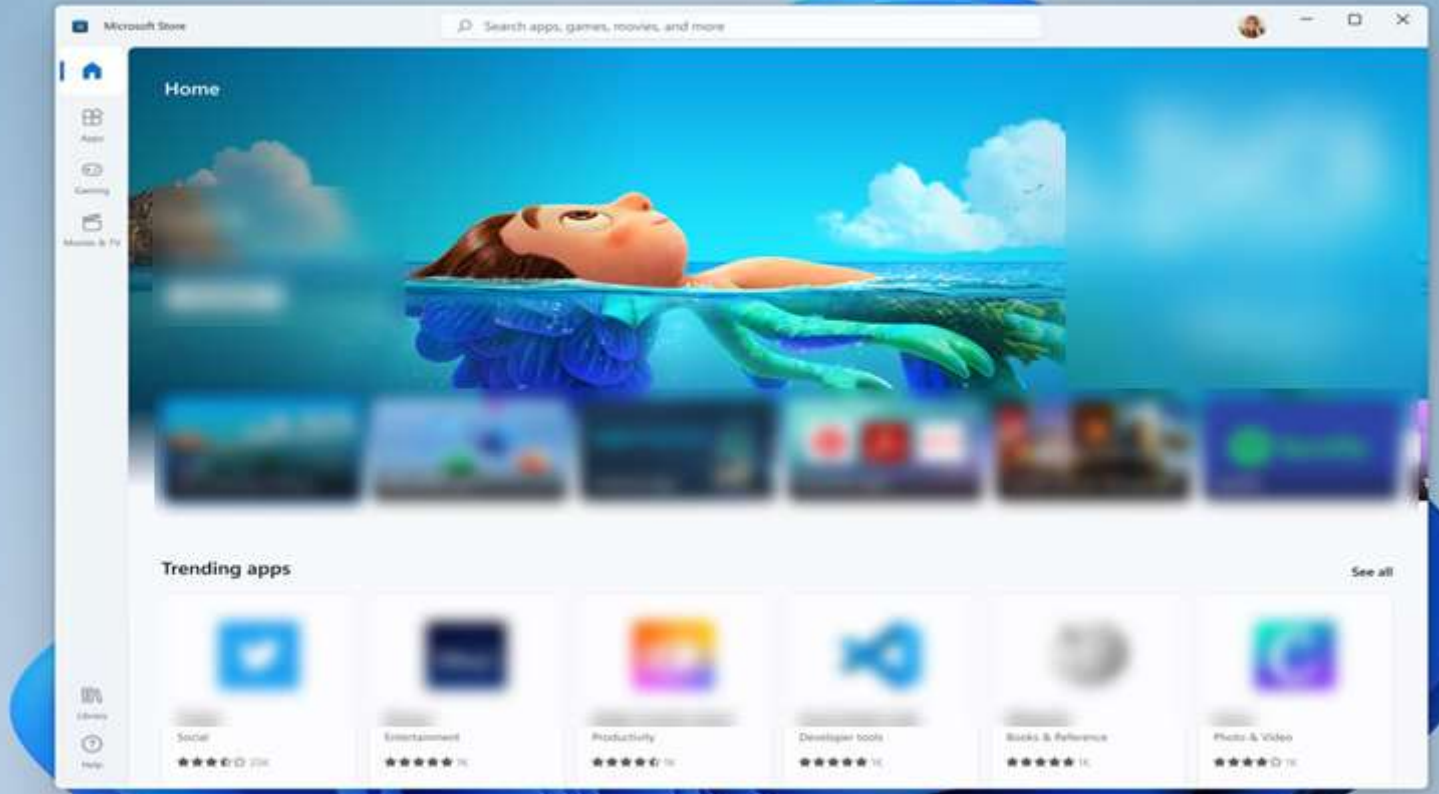
OK Cancel Apply Help

Windows LAPS: More than just a policy (rockenroll.tech)

Passwordless

- Starting in Windows 11, version 22H2 with KB5030310, *Windows passwordless experience* is a security policy that promotes a user experience without passwords on Microsoft Entra joined devices.

Windows passwordless experience - Windows Security | Microsoft Learn


Microsoft Store
Search apps, games, movies, and more
Home
Trending apps
See all

Bitlocker PIN

nic Cloud Connect

MDE onboarding

Defender for Endpoint security settings management

- For devices not being managed by Intune.
- Will allow you to push security settings from intune.

Use Intune to manage Microsoft Defender security settings management on devices not enrolled with Microsoft Intune | Microsoft Learn

Windows 10, Windows 11, and Windows Server

To support use with Microsoft Defender security settings management, your policies for Windows devices must use the *Windows 10, Windows 11, and Windows Server* platform. Each profile for the *Windows 10, Windows 11, and Windows Server* platform can apply to devices that are managed by Intune and to devices that are managed by security settings management.

Endpoint security policy	Profile	Defender for Endpoint security settings management	Microsoft Intune
Antivirus	Microsoft Defender Antivirus	✅	✅
Antivirus	Microsoft Defender Antivirus exclusions	✅	✅
Antivirus	Windows Security Experience	*Note 1*	✅
Attack Surface Reduction	Attack Surface Reduction Rules	✅	✅
Endpoint detection and response	Endpoint detection and response	✅	✅
Firewall	Firewall	✅	✅
Firewall	Firewall Rules	✅	✅

1 - The *Windows Security Experience* profile is available in the Defender portal but only applies to devices managed by Intune. It isn't supported for devices managed by Microsoft Defender security settings management.

What is advanced hunting and why should I care?

nic Cloud Connect

KQL fundamentals

Kusto Query Language (KQL)

- During 2014, Microsoft's Israeli R&D center started the development
- "Kusto" inspired by Jacques Cousteau
  - Reference to "exploring the ocean of data"
- Open-source, available on GitHub
- Used in Azure Data Explorer, Log Analytics, Microsoft Sentinel, and more

NIC Cloud Connect

Common query operators

Operator	Description
`where`	Filter a table to a subset of rows
`summarize`	Aggregates the content
`join`	Merge the rows of two tables to form a new table
`count`	Return the number of records
`top`	Return the first N records
`limit`	Return up to the specified number of rows
`project`	Select the columns to include
`extend`	Create calculated columns
`find`	Find rows that match the predicate

KQL Structure

```
Table
| where Column operator 'Value’

StormEvents
| where StartTime between (datetime(2007-11-01) .. datetime(2007-12-01))
| where State == "FLORIDA"
| count
```

Query best practices

- Get to know your data
  - `Limit / Take / Count`
- Apply filters early
  - `Where`
- `Has` beats `contains`
- Use == not =~
  - == Case sensitive
  - =~ Not case sensitive
- Parse, don't extract

Smartscreen

```
DeviceEvents
| where ActionType has_any('SmartScreenAppWarning','SmartScreenUrlWarning')
| extend TriggerReason = parse_json(AdditionalFields).Experience
// Find Smartscreen URLs
DeviceNetworkEvents
| where RemoteUrl matches regex
@'.*urs\.microsoft\.com.*|.*smartscreen.*\.microsoft\.com.*'
| where RemoteUrl != ''
| where InitiatingProcessFileName != "powershell.exe"
| summarize count() by RemoteUrl,RemotePort
| order by count_ desc
```

Table to query: DeviceEvents

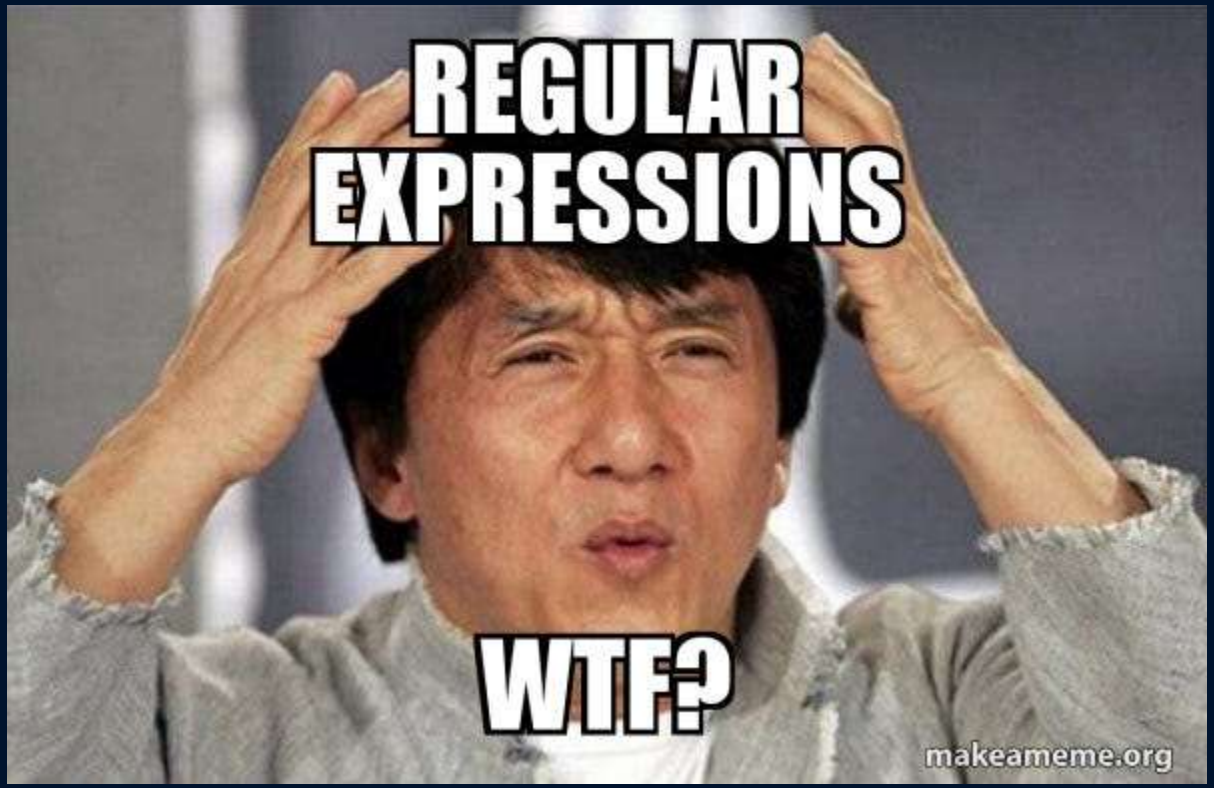
Action Type Values:

- SmartScreenAppWarning
- SmartScreenExploitWarning
- SmartScreenUrlWarning
- SmartScreenUserOverride

Endpoint/URL	Endpoint/URL Description	Required / Optional	Windows 11 / Windows 10 / Server 2022 / 2019 / Server 2016 (Unified Agent) / Server 2012 R2 (Unified Agent)
*.smartscreen-prod.microsoft.com	Used for Microsoft Defender SmartScreen protection, reporting, and notifications. MDAV Network Protection and custom URL indicators	Required	Yes
*.smartscreen.microsoft.com	Used for Microsoft Defender SmartScreen protection, reporting, and notifications. MDAV Network Protection and custom URL indicators	Required	Yes
*.checkappexec.microsoft.com	Used for Microsoft Defender SmartScreen to check application execution for trusted apps	Optional	Yes
*.urs.microsoft.com	Used for Microsoft Defender SmartScreen to check application execution for trusted apps	Optional	Yes

NIC Cloud Connect

/(reg)ex/



Our first query (use case/hunt)

```
// Finds PowerShell execution events that could involve a download
union DeviceProcessEvents, DeviceNetworkEvents
| where Timestamp > ago(7d)
// Pivoting on PowerShell processes
| where FileName in~ ("powershell.exe", "powershell_ise.exe")
// Suspicious commands
| where ProcessCommandLine has_any("WebClient",
 "DownloadFile",
 "DownloadData",
 "DownloadString",
 "WebRequest",
 "Shellcode",
 "http",
 "https")
| project Timestamp, DeviceName, InitiatingProcessFileName, InitiatingProcessCommandLine,
FileName, ProcessCommandLine, RemoteIP, RemoteUrl, RemotePort, RemoteIPType
| top 100 by Timestamp
```

Visualizing data

Summarize

- The summarize operator enables you to perform a variety of calculations on data

[DATA CAN DECEIVE]

```
Table
| summarize count() by Column
```

nic Cloud Connect

Broaden your view

Microsoft 365 Defender

- Microsoft Defender for Endpoint
- Microsoft Defender for Office 365
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Identity

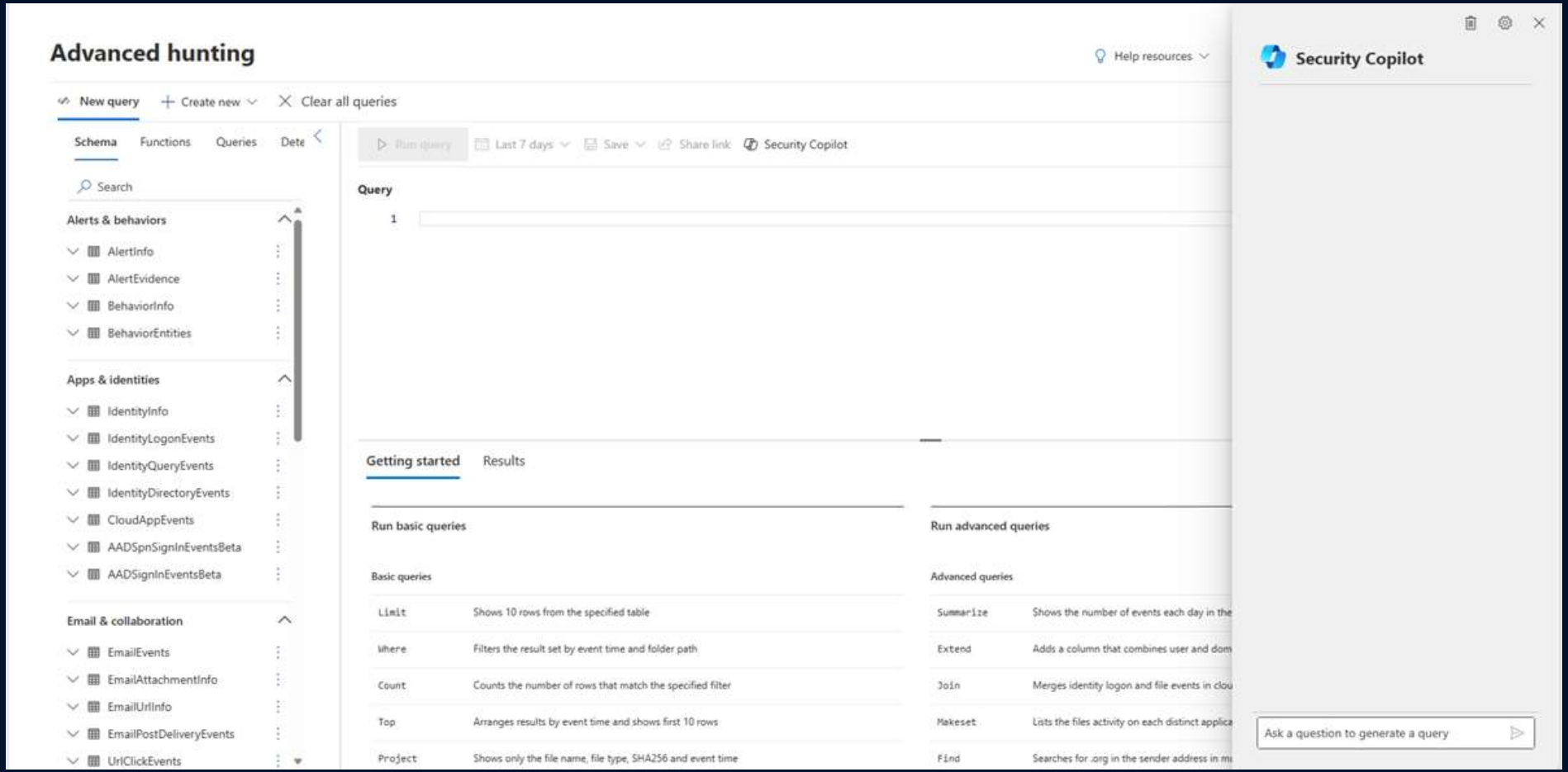
nic Cloud Connect

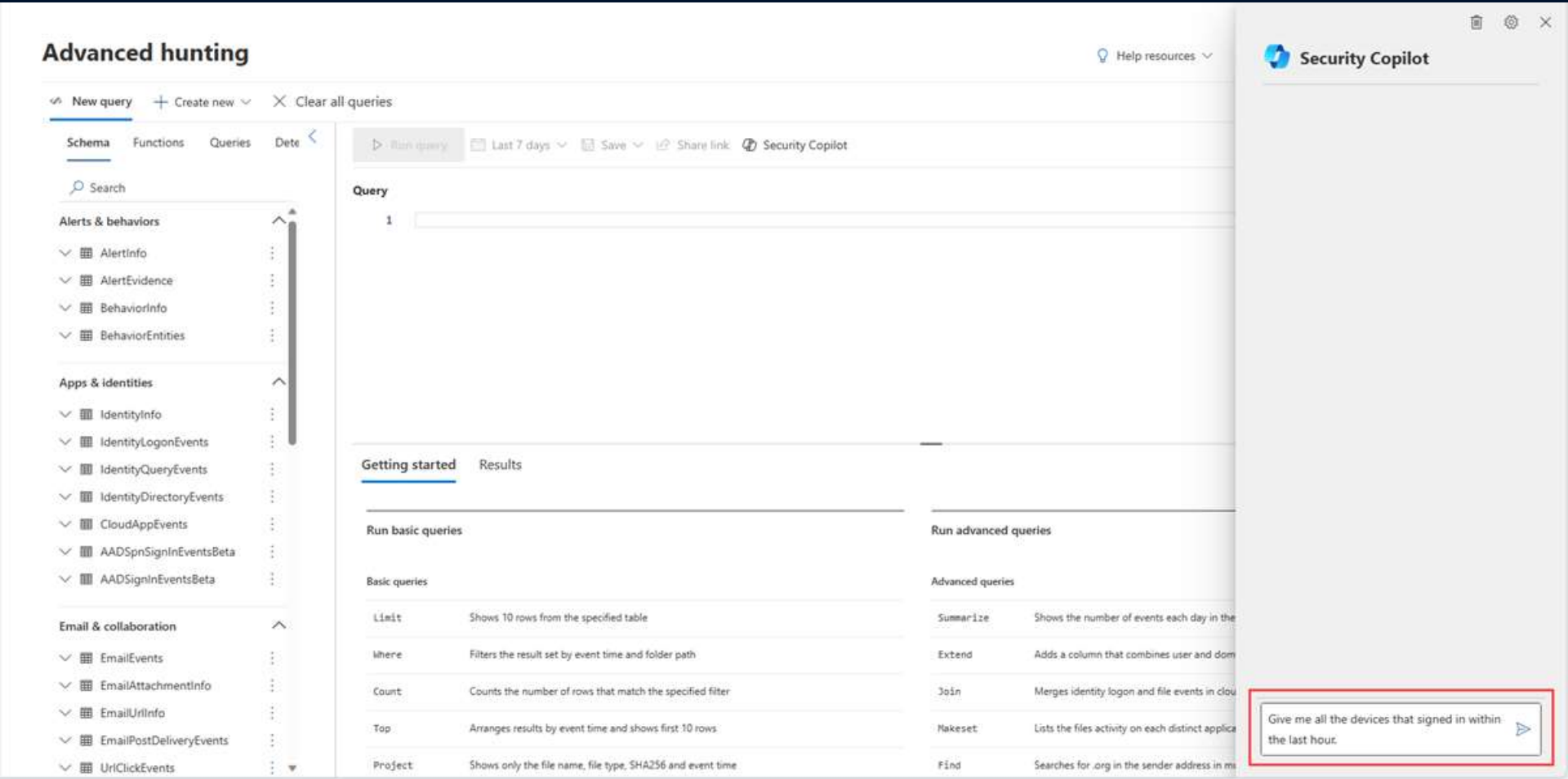
Hunt!

#HappyHunting!

nic Cloud Connect

Security Copilot


Advanced hunting
Help resources
New query
Create new
Clear all queries
Schema
Functions
Queries
Dete
Search
Alerts & behaviors
AlertInfo
AlertEvidence
BehaviorInfo
BehaviorEntities
Apps & identities
IdentityInfo
IdentityLogonEvents
IdentityQueryEvents
IdentityDirectoryEvents
CloudAppEvents
AADSpnSignInEventsBeta
AADSignInEventsBeta
Email & collaboration
EmailEvents
EmailAttachmentInfo
EmailUrlInfo
EmailPostDeliveryEvents
UrlClickEvents
Run query
Last 7 days
Save
Share link
Security Copilot
Query
1
Getting started
Results
Run basic queries
Basic queries
Limit
Shows 10 rows from the specified table
Where
Filters the result set by event time and folder path
Count
Counts the number of rows that match the specified filter
Top
Arranges results by event time and shows first 10 rows
Project
Shows only the file name, file type, SHA256 and event time
Run advanced queries
Advanced queries
Summarize
Extend
Join
Makeset
Find
Security Copilot
Ask a question to generate a query


Advanced hunting
Help resources
New query
Create new
Clear all queries
Schema
Functions
Queries
Dete
Search
Alerts & behaviors
AlertInfo
AlertEvidence
BehaviorInfo
BehaviorEntities
Apps & identities
IdentityInfo
IdentityLogonEvents
IdentityQueryEvents
IdentityDirectoryEvents
CloudAppEvents
AADSpnSignInEventsBeta
AADSignInEventsBeta
Email & collaboration
EmailEvents
EmailAttachmentInfo
EmailUrlInfo
EmailPostDeliveryEvents
UrlClickEvents
Run query
Last 7 days
Save
Share link
Security Copilot
Query
1
Getting started
Results
Run basic queries
Basic queries
Limit
Shows 10 rows from the specified table
Where
Filters the result set by event time and folder path
Count
Counts the number of rows that match the specified filter
Top
Arranges results by event time and shows first 10 rows
Project
Shows only the file name, file type, SHA256 and event time
Run advanced queries
Advanced queries
Summarize
Shows the number of events each day in the
Extend
Adds a column that combines user and dom
Join
Merges identity logon and file events in clou
Makeset
Lists the files activity on each distinct applica
Find
Searches for .org in the sender address in m
Security Copilot
Give me all the devices that signed in within the last hour.


Security Copilot
Oct 18, 2023 4:28 PM
Give me all the devices that signed in within the last hour.
Generating response...
Cancel

Security Copilot

Oct 18, 2023 4:28 PM

Give me all the devices that signed in within the last hour.

Oct 18, 2023 4:29 PM

Here's a query you can use to find what you need:

```
DeviceLogonEvents
| where Timestamp > ago(1h)
| summarize count() by DeviceName
```

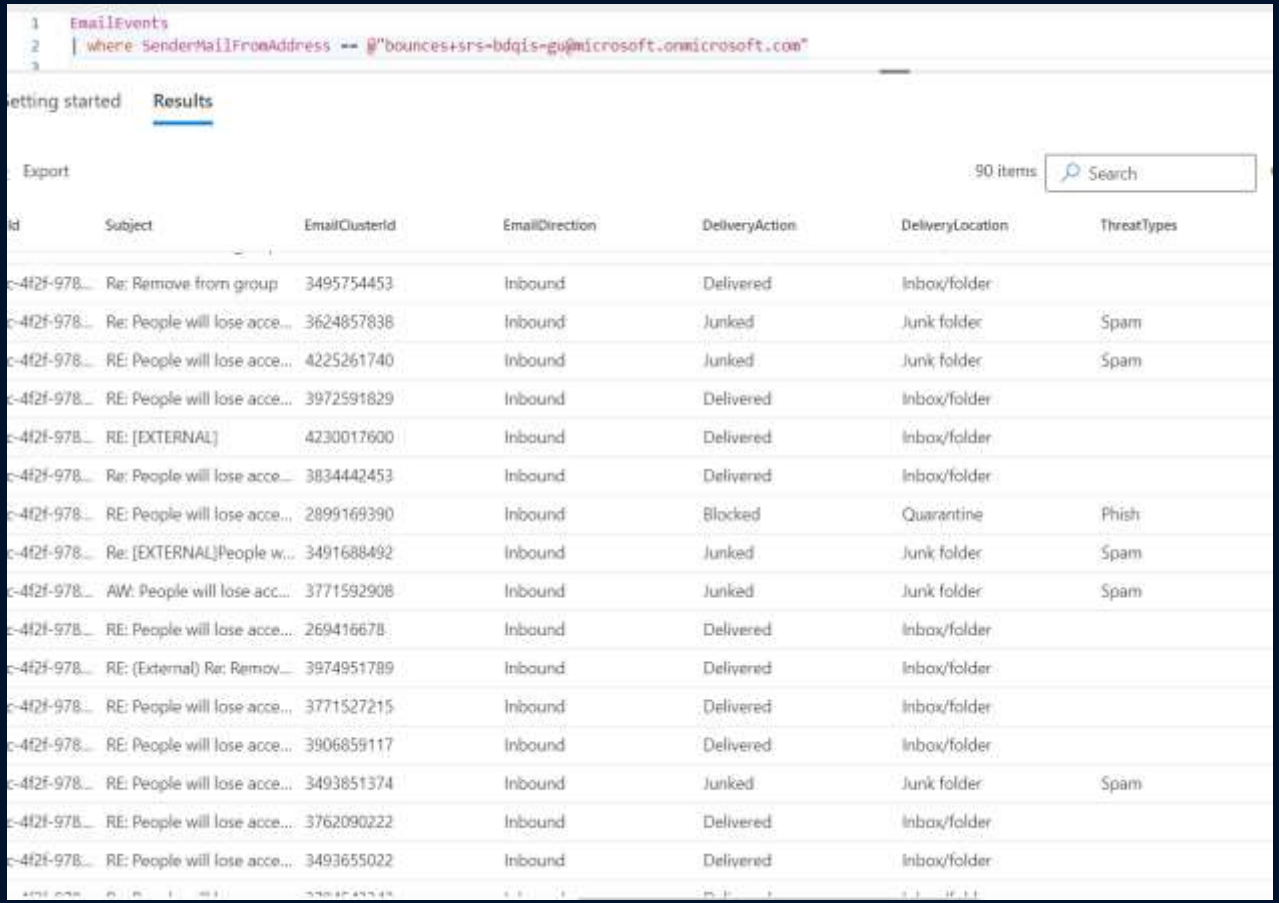
Add and run

AI generated. Verify for accuracy.

Are you a member of the Customer Connection Program (CCP)?

Member of the CCP?

```
EmailEvents
| where
SenderMailFromAddress ==
@"bounces+srs=bdqis=gu@m
icrosoft.onmicrosoft.com
"
```



```
EmailEvents
| where SenderMailFromAddress == @"bounces+srs=bdqis=gu@microsoft.onmicrosoft.com"
```

Getting started | Results

Export | 90 items | Search

Id	Subject	EmailClusterId	EmailDirection	DeliveryAction	DeliveryLocation	ThreatTypes
c-4f2f-978...	Re: Remove from group	3495754453	Inbound	Delivered	Inbox/folder	
c-4f2f-978...	Re: People will lose acce...	3624857838	Inbound	Junked	Junk folder	Spam
c-4f2f-978...	RE: People will lose acce...	4225261740	Inbound	Junked	Junk folder	Spam
c-4f2f-978...	RE: People will lose acce...	3972591829	Inbound	Delivered	Inbox/folder	
c-4f2f-978...	RE: [EXTERNAL]	4230017600	Inbound	Delivered	Inbox/folder	
c-4f2f-978...	Re: People will lose acce...	3834442453	Inbound	Delivered	Inbox/folder	
c-4f2f-978...	RE: People will lose acce...	2899169390	Inbound	Blocked	Quarantine	Phish
c-4f2f-978...	Re: [EXTERNAL]People w...	3491688492	Inbound	Junked	Junk folder	Spam
c-4f2f-978...	AW: People will lose acc...	3771592908	Inbound	Junked	Junk folder	Spam
c-4f2f-978...	RE: People will lose acce...	269416678	Inbound	Delivered	Inbox/folder	
c-4f2f-978...	RE: (External) Re: Remov...	3974951789	Inbound	Delivered	Inbox/folder	
c-4f2f-978...	RE: People will lose acce...	3771527215	Inbound	Delivered	Inbox/folder	
c-4f2f-978...	RE: People will lose acce...	3906859117	Inbound	Delivered	Inbox/folder	
c-4f2f-978...	RE: People will lose acce...	3493851374	Inbound	Junked	Junk folder	Spam
c-4f2f-978...	RE: People will lose acce...	3762090222	Inbound	Delivered	Inbox/folder	
c-4f2f-978...	RE: People will lose acce...	3493655022	Inbound	Delivered	Inbox/folder	

Table: DeviceEvents | Field: ActionType

ActionType	Description
SmartScreenAppWarning	SmartScreen warned about running a downloaded application that is untrusted or malicious.
SmartScreenExploitWarning	SmartScreen warned about opening a web page that contains an exploit.
SmartScreenUrlWarning	SmartScreen warned about opening a low-reputation URL that might be hosting malware or is a phishing site.
SmartScreenUserOverride	A user has overridden a SmartScreen warning and continued to open an untrusted app or a low-reputation URL.

```
DeviceEvents
| where ActionType has_any('SmartScreenAppWarning','SmartScreenUrlWarning')
| extend TriggerReason = parse_json(AdditionalFields).Experience
| summarize count() by tostring(TriggerReason)

DeviceEvents
| where ActionType contains "SmartScreen"
| extend TriggerReason = parse_json(AdditionalFields).Experience
| summarize count() by ActionType
```

Advanced hunting

New query | New query | New query | New query | New query | New query

Run query | Last 7 days | Save | Share link | Create detection rule

Query

```
1  DeviceEvents
2  | where ActionType has_any('SmartScreenAppWarning','SmartScreenUrlWarning')
3  | extend TriggerReason = parse_json(AdditionalFields).Experience
4  | summarize count() by tostring(TriggerReason)
5
6  DeviceEvents
7  | where ActionType contains "SmartScreen"
8  | extend TriggerReason = parse_json(AdditionalFields).Experience
9  | summarize count() by ActionType
```

Getting started | Results

Export | 3 items | Search | 0:0.154 | Low | Chart type | Customize columns

TriggerReason	count_
CustomPolicy	293
Untrusted	7
TechScam	6

Advanced hunting

New query | New query | New query | New query | New query | New query

Run query | Last 7 days | Save | Share link | Create detection rule

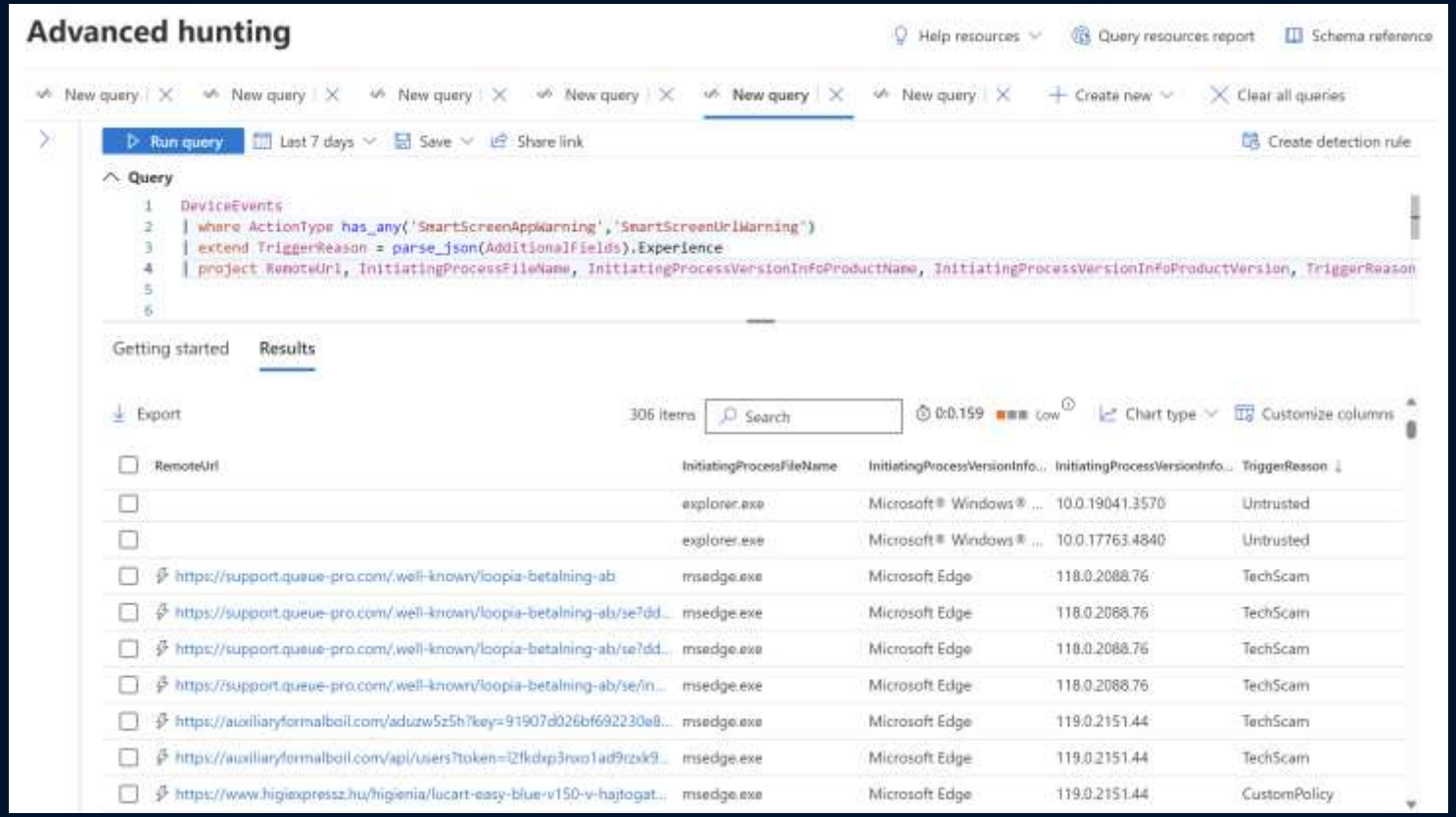
Query

```
1  DeviceEvents
2  | where ActionType has_any('SmartScreenAppWarning','SmartScreenUrlWarning')
3  | extend TriggerReason = parse_json(AdditionalFields).Experience
4  | summarize count() by tostring(TriggerReason)
5
6  DeviceEvents
7  | where ActionType contains "SmartScreen"
8  | extend TriggerReason = parse_json(AdditionalFields).Experience
9  | summarize count() by ActionType
```

Getting started | Results

Export | 3 items | Search | 0:0.169 | Low | Chart type | Customize columns

ActionType	count_
SmartScreenUrlWarning	300
SmartScreenAppWarning	6
SmartScreenUserOverride	1


Advanced hunting
Help resources
Query resources report
Schema reference
New query
New query
New query
New query
New query
New query
Create new
Clear all queries
Run query
Last 7 days
Save
Share link
Create detection rule
Query
1 DeviceEvents
2 | where ActionType has_any('SmartScreenAppWarning','SmartScreenUrlWarning')
3 | extend TriggerReason = parse_json(AdditionalFields).Experience
4 | project RemoteUrl, InitiatingProcessFileName, InitiatingProcessVersionInfoProductName, InitiatingProcessVersionInfoProductVersion, TriggerReason
5
6
Getting started
Results
Export
306 items
Search
0:0.159
Low
Chart type
Customize columns
RemoteUrl
InitiatingProcessFileName
InitiatingProcessVersionInfo...
InitiatingProcessVersionInfo...
TriggerReason
explorer.exe
Microsoft® Windows® ...
10.0.19041.3570
Untrusted
explorer.exe
Microsoft® Windows® ...
10.0.17763.4840
Untrusted
https://support.queue-pro.com/.well-known/loopia-betalning-ab
msedge.exe
Microsoft Edge
118.0.2088.76
TechScam
https://support.queue-pro.com/.well-known/loopia-betalning-ab/se?dd...
msedge.exe
Microsoft Edge
118.0.2088.76
TechScam
https://support.queue-pro.com/.well-known/loopia-betalning-ab/se?dd...
msedge.exe
Microsoft Edge
118.0.2088.76
TechScam
https://support.queue-pro.com/.well-known/loopia-betalning-ab/se/in...
msedge.exe
Microsoft Edge
118.0.2088.76
TechScam
https://auxiliaryformalboil.com/aduzw5z5h?key=91907d026bf692230e8...
msedge.exe
Microsoft Edge
119.0.2151.44
TechScam
https://auxiliaryformalboil.com/api/users?token=l2fkdep3nxo1ad9rzxk9...
msedge.exe
Microsoft Edge
119.0.2151.44
TechScam
https://www.higiexpressz.hu/higienia/lucart-easy-blue-v150-v-hajtogat...
msedge.exe
Microsoft Edge
119.0.2151.44
CustomPolicy

Advanced hunting

New query | New query | New query | New query | New query | New query

Run query | Last 7 days | Save | Share link | Create detection rule

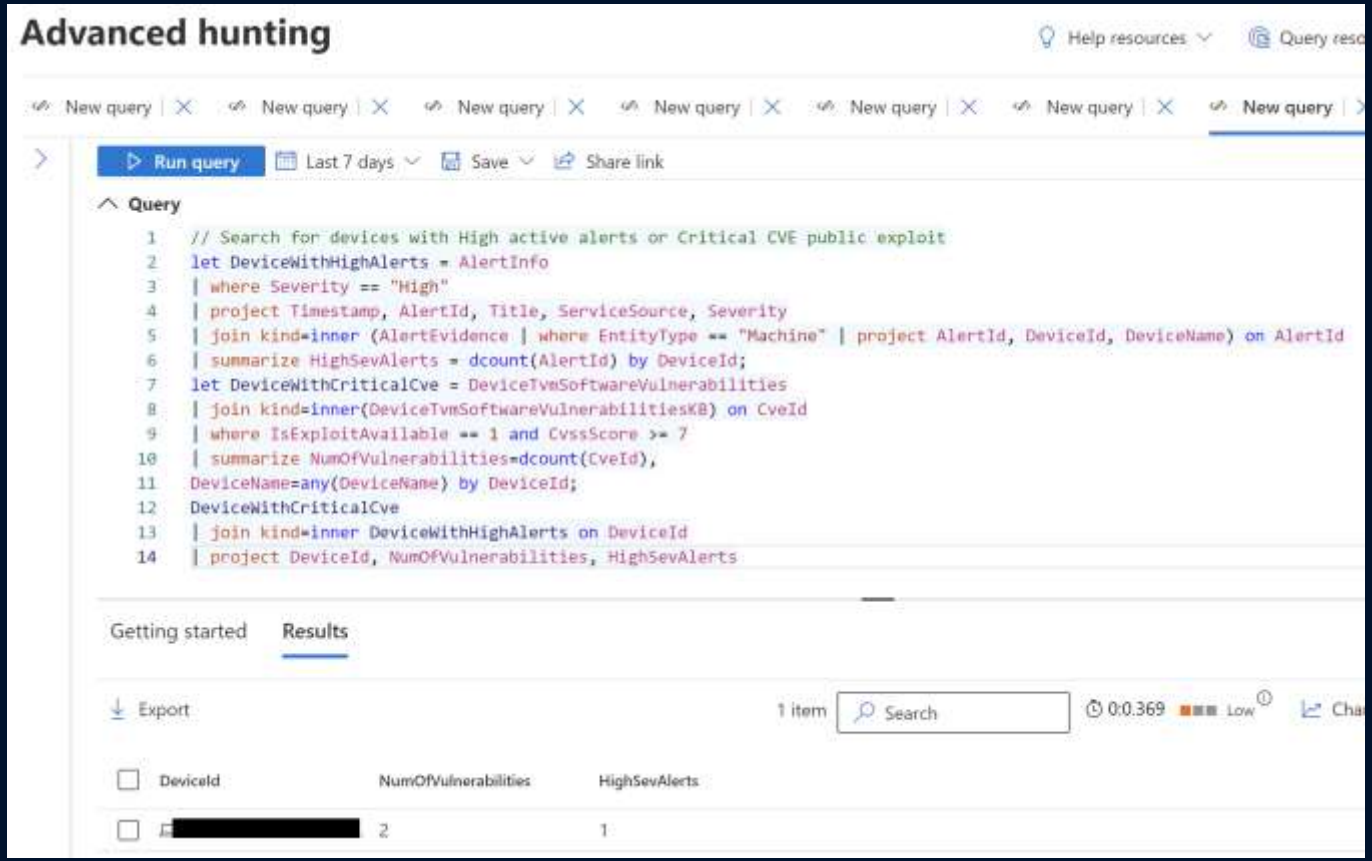
Query

```
8
9   find in (DeviceEvents, DeviceNetworkEvents)
10  where RemoteUrl contains "https://support.queue-pro.com"
11  project RemoteUrl, ActionType, FileName, Timestamp
12
```

Getting started | Results

Export | 5 items | Search | 0:0.179 | Low | Chart type | Customize columns

source_	RemoteUrl	ActionType	FileName	Timestamp
DeviceEvents	https://support.queu...	SmartScreenUrlWarning		Nov 6, 2023 3:22:23 PM
DeviceEvents	https://support.queu...	SmartScreenUrlWarning		Nov 6, 2023 3:22:26 PM
DeviceEvents	https://support.queu...	SmartScreenUrlWarning		Nov 6, 2023 3:22:26 PM
DeviceEvents	https://support.queu...	SmartScreenUrlWarning		Nov 6, 2023 3:22:26 PM
DeviceNetworkEvents	https://support.queu...	ConnectionSuccess		Nov 6, 2023 3:22:23 PM


Advanced hunting
Help resources
Query resc
New query
New query
New query
New query
New query
New query
New query
Run query
Last 7 days
Save
Share link
Query
1 // Search for devices with High active alerts or Critical CVE public exploit
2 let DeviceWithHighAlerts = AlertInfo
3 | where Severity == "High"
4 | project Timestamp, AlertId, Title, ServiceSource, Severity
5 | join kind=inner (AlertEvidence | where EntityType == "Machine" | project AlertId, DeviceId, DeviceName) on AlertId
6 | summarize HighSevAlerts = dcount(AlertId) by DeviceId;
7 let DeviceWithCriticalCve = DeviceTvmSoftwareVulnerabilities
8 | join kind=inner(DeviceTvmSoftwareVulnerabilitiesKB) on CveId
9 | where IsExploitAvailable == 1 and CvssScore >= 7
10 | summarize NumOfVulnerabilities=dcount(CveId),
11 DeviceName=any(DeviceName) by DeviceId;
12 DeviceWithCriticalCve
13 | join kind=inner DeviceWithHighAlerts on DeviceId
14 | project DeviceId, NumOfVulnerabilities, HighSevAlerts
Getting started
Results
Export
1 item
Search
0:0.369
Low
DeviceId
NumOfVulnerabilities
HighSevAlerts
2
1

Other use cases

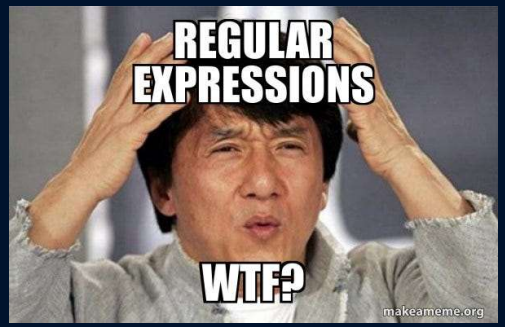
```
let KnownNames = dynamic(["teamviewer","anydesk"]);
let RATProcess =
DeviceProcessEvents
| where ProcessVersionInfoCompanyName has_any(KnownNames)
| extend DetectionMethod = "Process";
let RATNetwork =
DeviceNetworkEvents
| extend DNSRequest = (parse_json(AdditionalFields)).query,
         DNSResponse = (parse_json(AdditionalFields)).answers,
         HTTP = (parse_json(AdditionalFields)).host
| where (
        RemoteUrl has_any (KnownNames)  or
        RemotePort == 5938 or
        DNSRequest has_any (KnownNames) or
        DNSResponse has_any (KnownNames)
        )
    | extend DetectionMethod = "Network";
union RATNetwork,RATProcess
```

Other use cases

```
let minTimeRange = ago(7d);
let smartscreenAppBlocks =
    DeviceEvents
    | where ActionType == "SmartScreenAppWarning" and Timestamp > minTimeRange
    | extend ParsedFields=parse_json(AdditionalFields)
    | project Timestamp, DeviceName, BlockedFileName=FileName, SHA1, Experience=tostring(ParsedFields.Experience), ActivityId=tostring(ParsedFields.ActivityId), InitiatingProcessFileName;
// Query for UserDecision events - each one means the user has decided to ignore the warning and run the app.
let userIgnoredWarning=
    DeviceEvents
    | where ActionType == "SmartScreenUserOverride" and Timestamp > minTimeRange
    | project DeviceName, ActivityId=extractjson("$.ActivityId", AdditionalFields, typeof(string));
// Join the block and user decision event using an ActivityId
let ignoredBlocks =
    smartscreenAppBlocks
    | join kind=leftsemi (userIgnoredWarning) on DeviceName, ActivityId
    | project-away ActivityId;
ignoredBlocks
// Select only blocks on "Malicious" files.
// To hunt over Unknown/Untrusted files, remove the following where clause, but then you might want to join with additional signals.
| where Experience == "Malicious"
```

Other use cases

```
let MgmtPorts = dynamic([3389,22,5985]); //Add mgmt. ports
let PAWNetwork = dynamic(["10.10.10","10.10.11"]); //PAWs
DeviceNetworkEvents
| where ActionType == "InboundConnectionAccepted"
| where LocalPort in(MgmtPorts)
| extend RemoteSubnet = extract(@"\d{1,3}\.\d{1,3}\.\d{1,3}",0,RemoteIP),
LocalSubnet = extract(@"\d{1,3}\.\d{1,3}\.\d{1,3}",0,LocalIP)
| where RemoteSubnet !in(PAWNetwork)
```



Other use cases

```
let MgmtPorts = dynamic([3389,22,5985]);
let UnexpectedNetwork = dynamic(["10.10.10","10.10.11"]); //Type in networks
DeviceNetworkEvents
| where LocalPort in(MgmtPorts)
| extend RemoteSubnet = extract(@"\d{1,3}\.\d{1,3}\.\d{1,3}",0,RemoteIP),
LocalSubnet = extract(@"\d{1,3}\.\d{1,3}\.\d{1,3}",0,LocalIP)
| where RemoteSubnet in(UnexpectedNetwork)
```

nic Cloud Connect

WINDOWS 11

MICROSOFT INTUNE

MICROSOFT DEFENDER FOR ENDPOINT

NIC Cloud Connect

Thank you!

Please submit feedback on this session