

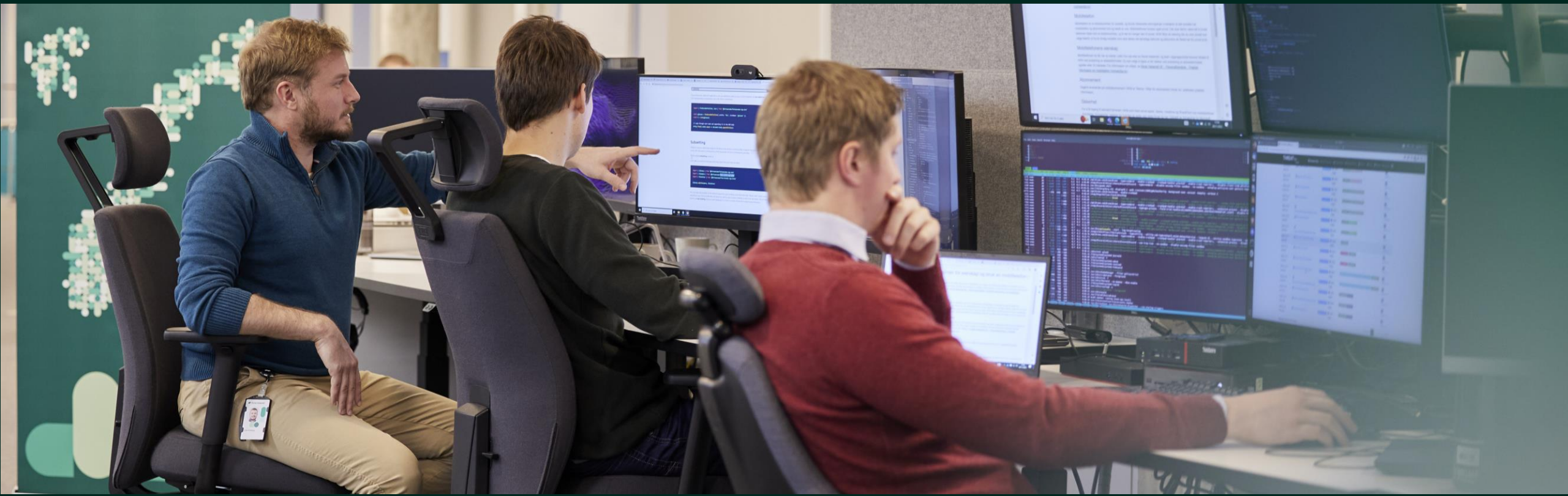


HelseCERT

Webinaret starter snart...

Webinar – Herding Microsoft
Entra ID

Mars 2024



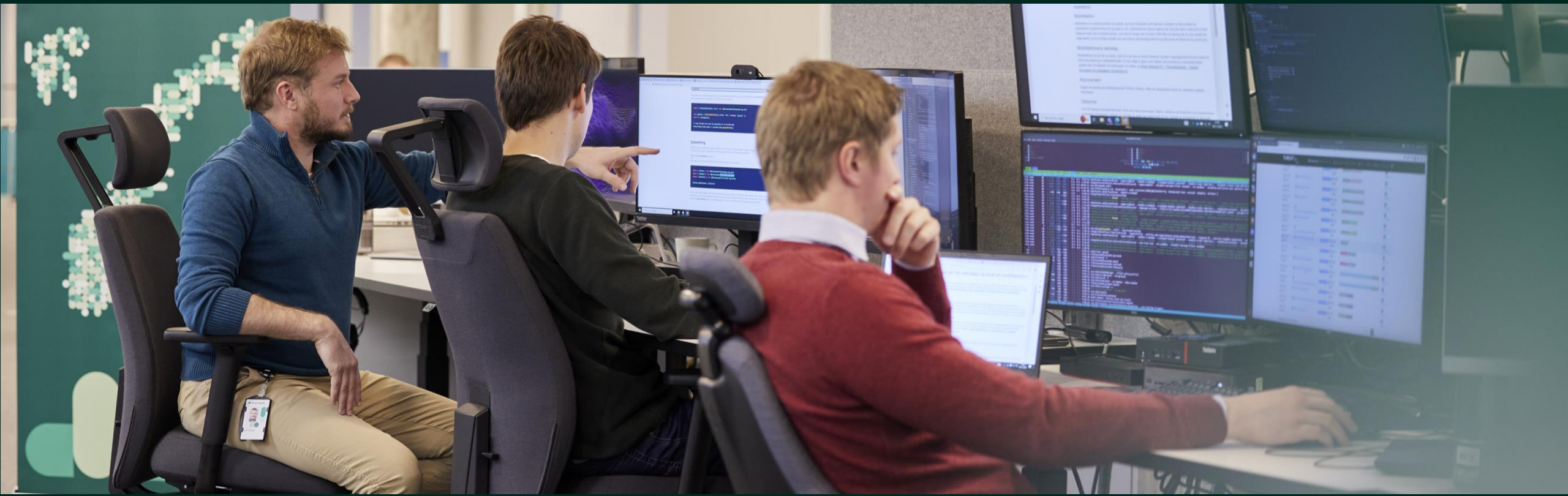


HelseCERT

Herding Microsoft Entra ID

Webinar

Mars 2024



(Intro) Herding Microsoft Entra ID

Mars 2024

Hans Kristian Strømme

Agenda

➤ Hvorfor

➤ Hvordan

- Sikre administratorer
- Begrens e-post
- Conditional access
 - Geofiltrering
 - Bruk blokkeringslister

➤ Lenker deles i chat og med webinar-opptak

Hvorfor

Alle kan bli lurt av phishing

Bevisstgjøring hjelper



AITM Phishing



Administratorer

- Fjerne unødvendige
- Ikke kjør admin til daglig
- Sikre innlogging
 - MFA: ikke lengre nok
 - Innrullerte enheter: Bra
 - Phishingresistent: Best

Fjern unødvendige

https://admin.microsoft.com/#/users

enter Search

Home > Active users

Active users

[Add a user](#) [User templates](#) [Add multiple users](#) [Multi-factor authentication](#) [Delete a user](#) [Refresh](#) [Reset password](#)

☐	Display name ↑		Username	Licenses
☐	Adele Vance	:	AdeleV@MSDx849203.OnMicrosoft.com	Microsoft 365 E5
☐	Alex Wilber	:	AlexW@MSDx849203.OnMicrosoft.com	Microsoft 365 E5
☐	Automate Bot	:	AutomateB@MSDx849203.OnMicrosoft.com	Unlicensed
☐	Bianca Pisani	:	BiancaP@MSDx849203.OnMicrosoft.com	Unlicensed
☐	Brian Johnson (TAILSPIN)	:	BrianJ@MSDx849203.OnMicrosoft.com	Unlicensed
☐	Cameron White	:	CameronW@MSDx849203.OnMicrosoft.com	Unlicensed
☐	Christie Cline	:	ChristieC@MSDx849203.OnMicrosoft.com	Microsoft 365 E5
☐	Conf Room Adams	:	Adams@MSDx849203.OnMicrosoft.com	Unlicensed
☐	Conf Room Baker	:	Baker@MSDx849203.OnMicrosoft.com	Unlicensed
☐	Conf Room Crystal	:	Crystal@MSDx849203.OnMicrosoft.com	Unlicensed
☐	Conf Room Hood	:	Hood@MSDx849203.OnMicrosoft.com	Unlicensed
☐	Conf Room Rainier	:	Rainier@MSDx849203.OnMicrosoft.com	Unlicensed
☐	Conf Room Stevens	:	Stevens@MSDx849203.OnMicrosoft.com	Unlicensed
☐	Debra Berger	:	DebraB@MSDx849203.OnMicrosoft.com	Microsoft 365 E5
☐	Delia Dennis	:	DeliaD@MSDx849203.OnMicrosoft.com	Unlicensed
☐	Diego Siciliani	:	DiegoS@MSDx849203.OnMicrosoft.com	Microsoft 365 E5
☐	Gerhart Moller	:	GerhartM@MSDx849203.OnMicrosoft.com	Unlicensed
☐	Grady Archie	:	GradyA@MSDx849203.OnMicrosoft.com	Microsoft 365 E5

Active users

 Add a user  User templates  Add multiple users  Multi-factor authentication  Delete a user  Refresh  Reset password  Export users

 Search active users list ...

☐	Display name ↑		Username		Choose columns
☐	Isaiah Langer	⋮	IsaiahL@MSDx849203.OnMicrosoft.com		
☐	Lidia Holloway	⋮	LidiaH@MSDx849203.OnMicrosoft.com		
☐	Megan Bowen	⋮	MeganB@MSDx849203.OnMicrosoft.com		
☐	Microsoft Service Account	⋮	ms-serviceaccount@MSDx849203.OnMicrosoft.com		
☐	MOD Administrator	⋮	admin@MSDx849203.onmicrosoft.com		
☐	Nestor Wilke	⋮	NestorW@MSDx849203.OnMicrosoft.com		

-  Global ad...
-  New filter
-  Clear filter
- Standard filters
 - All users
 - Billing admins
 - ☒ Global admins
 - Guest users
 - Helpdesk admins
 - Licensed users
 - Service support admins
 - Sign-in allowed
 - Sign-in blocked
 - Unlicensed users
 - User admins
 - Users with errors

Fjern unødvendige

Active users

 Add a user  User templates  Add multiple users  Multi-factor authentication  Delete a user  Refresh 

☐	Display name ↑		Username	 Choose columns
☐	Isaiah Langer	⋮	IsaiahL@MSDx849203.OnMicrosoft.com	
☐	Lidia Holloway	⋮	LidiaH@MSDx849203.OnMicrosoft.com	
☐	Megan Bowen	⋮	MeganB@MSDx849203.OnMicrosoft.com	
☐	Microsoft Service Account	⋮	ms-serviceaccount@MSDx849203.OnMicrosoft.com	
☐	MOD Administrator	⋮	admin@MSDx849203.onmicrosoft.com	
☐	Nestor Wilke	 ⋮	NestorW@MSDx849203.OnMicrosoft.com	

Fjern unødvendige | Ikke kjør admin i det daglige

Active users

 Add a user  User templates  Add multiple users  Multi-factor authentication  Delete a user

☐	Display name ↑		Username	
☐	Megan Bowen [Adminbruker]	⋮	Megan.Bowen.admin@MSDx849203.onmicrosoft.com	
☐	Microsoft Service Account	 ⋮	ms-serviceaccount@MSDx849203.OnMicrosoft.com	
☐	MOD Administrator	⋮	admin@MSDx849203.onmicrosoft.com	

Sikre innlogging

The screenshot displays the Microsoft Entra admin center interface. The left navigation pane shows the 'Protection' section expanded, with 'Conditional Access' selected. The main content area shows the 'Conditional Access | Overview' page. The 'Policies' link in the left navigation pane is highlighted. The 'Create new policy from templates' button is highlighted in the top right area. The page includes a 'Policy Summary' section with cards for 'Policy Snapshot', 'Users', 'Devices', and 'Applications'. The 'Policy Snapshot' card shows 2 Enabled, 0 Report-only, and 2 Off policies. The 'Users' card shows 0 users signed in during the last 7 days without any policy coverage. The 'Devices' card shows 0% of sign-ins in the last 7 days were from unmanaged or non-compliant devices. The 'Applications' card shows a list of applications that are not protected by your policies. The 'What's new' section includes a 'Named Locations' update. The 'Security Alerts (Preview)' section is partially visible at the bottom.

Sikre innlogging

Microsoft Entra admin center

Search resources, services, and docs (G+)

admin@MSDx849203.c
CONTOSO (MSDX849203.ONM)

Home > Contoso > Users > Users > Conditional Access | Overview > Create new policy from templates > Conditional Access | Overview >

Create new policy from templates

Select a template Review + Create

Search

Secure foundation Zero Trust Remote work **Protect administrator** Emerging threats All

☐ 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 defaults.

[Learn more](#)

[View](#) [Download JSON file](#)

☐ Block legacy authentication

Block legacy authentication endpoints that can be used to bypass multifactor authentication.

[Learn more](#)

[View](#) [Download JSON file](#)

☐ Require multifactor authentication for Azure management

Require multifactor authentication to protect privileged access to Azure management.

[Learn more](#)

[View](#) [Download JSON file](#)

☐ Require compliant or hybrid Azure AD joined device for admins

Require privileged administrators to only access resources when using a compliant or hybrid Azure AD joined device.

[Learn more](#)

[View](#) [Download JSON file](#)

☒ Require phishing-resistant multifactor authentication for admins

Require phishing-resistant multifactor authentication for privileged administrative accounts to reduce risk of compromise and phishing attacks. This policy requires admins to have at least one phishing-resistant authentication method registered.

[Learn more](#)

[View](#) [Download JSON file](#)

☐ Require multifactor authentication for Microsoft admin portals

Use this template to protect sign-ins to admin portals if you are unable to use the "Require MFA for admins" template.

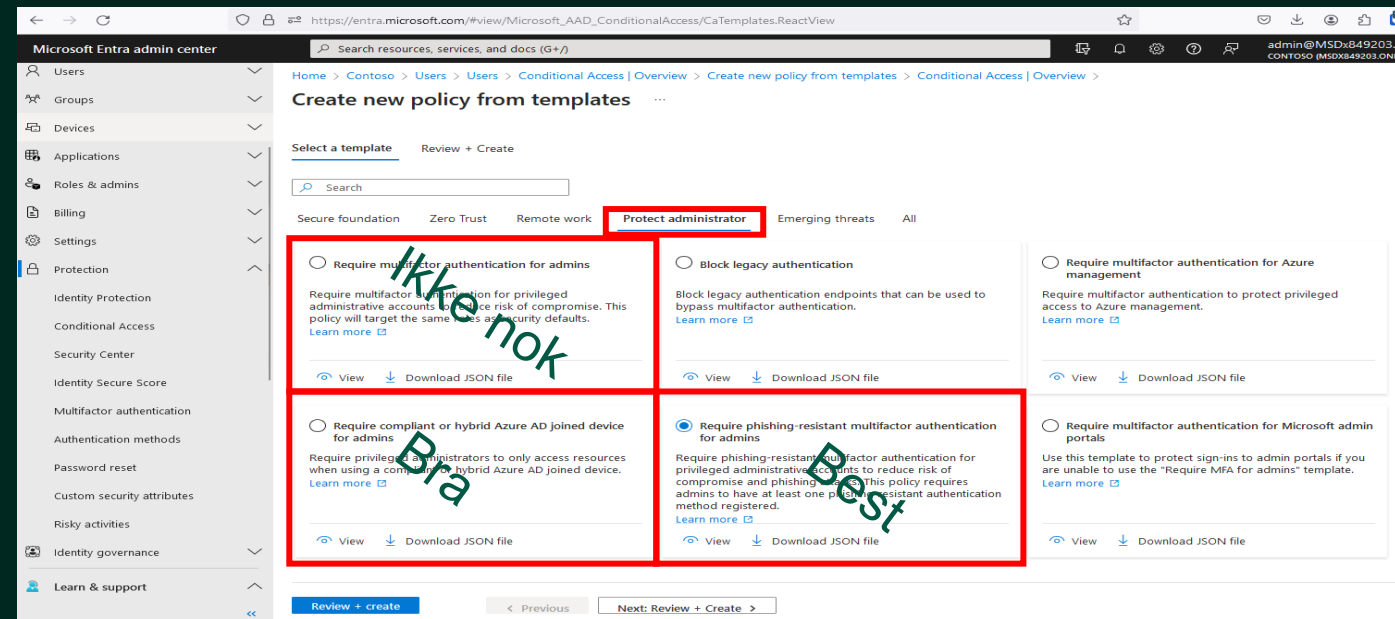
[Learn more](#)

[View](#) [Download JSON file](#)

[Review + create](#) [< Previous](#) [Next: Review + Create >](#)

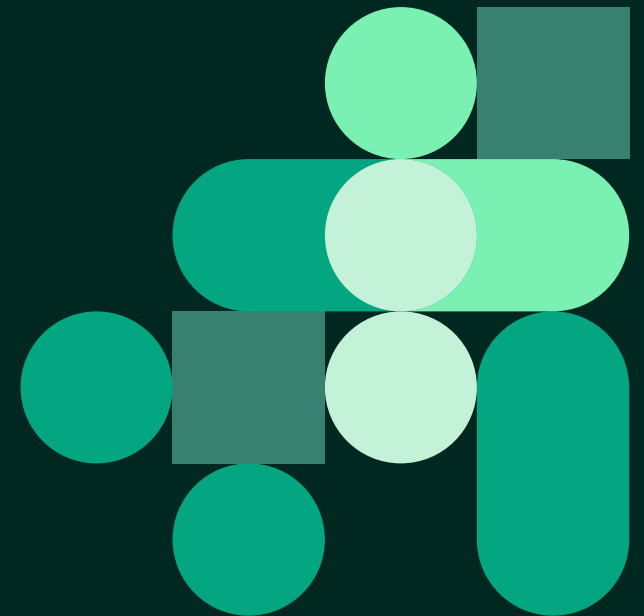
Sikre innlogging

- Innrullingering av enheter
- Utrulling av policy



Anti-spam

Hvorfor sende ut mye spam om du ikke må?



Microsoft Defender

Identities

Dashboard

Health issues

Tools

Email & collaboration

Investigations

Explorer

Review

Campaigns

Threat tracker

Exchange message trace

Attack simulation training

Policies & rules

Cloud apps

Cloud discovery

Cloud app catalog

OAuth apps

Files

Activity log

Governance log

Policies

Search

Policies & rules > Threat policies > Anti-spam policies

Anti-spam policies

We recommend enabling preset security policies to stay updated with new security controls and our recommended settings. [View preset security policies](#)

Use this page to configure policies that are included in anti-spam protection. These policies include connection filtering, spam filtering, and more.

+ Create policy Refresh

Name	Status
☐ antiSPAM	On
☐ Anti-spam inbound policy (Default)	Always on
☐ Connection filter policy (Default)	Always on
☐ Anti-spam outbound policy (Default)	Always on

antiSPAM

Policy on | Priority 0

Turn off Delete policy

Next

Description

-

[Edit description](#)

Users, groups, and domains

Included groups

Employees@MSDx849203.OnMicrosoft.com

Excluded users

DiegoS@MSDx849203.OnMicrosoft.com

[Edit users, groups, and domains](#)

Protection settings

Restrict sending to external recipients (per hour)

50

Restrict sending to internal recipients (per hour)

50

Maximum recipient limit per day

100

Over limit action

Restrict the user from sending mail until the following day

Automatic forwarding

Automatic - System-controlled

Send a copy of suspicious outbound messages or message that exceed these limits to these users and groups

On

Notify these users and groups if a sender is blocked due to sending outbound spam

On

[Edit protection settings](#)

Notifications

- ☒ Send a copy of suspicious outbound messages or message that exceed these limits to these users and groups

Please enter the full email address

 SOCTeam@MSDx849203.onmicroso... 

- ☒ Notify these users and groups if a sender is blocked due to sending outbound spam

Please enter the full email address

 SOCTeam@MSDx849203.onmicroso... 



antiSPAM

● Policy on | Priority 0

 Turn off  Delete policy

Next

Description

-

[Edit description](#)

Users, groups, and domains

Included groups

Employees@MSDx849203.OnMicrosoft.com

Excluded users

DiegoS@MSDx849203.OnMicrosoft.com

[Edit users, groups, and domains](#)

Protection settings

Restrict sending to external recipients (per hour)

50

Restrict sending to internal recipients (per hour)

50

Maximum recipient limit per day

100

Over limit action

Restrict the user from sending mail until the following day

Automatic forwarding

Automatic - System-controlled

Send a copy of suspicious outbound messages or message that exceed these limits to these users and groups

● On

Notify these users and groups if a sender is blocked due to sending outbound spam

● On

[Edit protection settings](#)

Microsoft Entra admin center

Identity

Overview

Users

Groups

Devices

Applications

Protection

Identity governance

External Identities

Show more

Protection

Identity Protection

Conditional Access

Authentication methods

Password reset

Custom security attributes

Risky activities

Learn & support

Home > hanskr | Audit logs >

Conditional Access | Overview

Microsoft Entra ID

Overview

Policies

Insights and reporting

Diagnose and solve problems

Manage

Named locations

Custom controls (Preview)

Terms of use

VPN connectivity

Authentication contexts

Authentication strengths

Classic policies

Monitoring

Sign-in logs

Audit logs

Troubleshooting + Support

New support request

Create new policy

Create new policy from templates

Refresh

Got feedback?

Getting started

Overview

Coverage

Monitoring (Preview)

Tutorials

Policy Summary

Policy Snapshot

2 Enabled 0 Report-only 2 Off

View all policies

Users

1 user signed in during the last 7 days without any policy coverage

See all unprotected sign-ins

Devices

100% of sign-ins in the last 7 days were from unmanaged or non-compliant devices

See all noncompliant devices

See all unmanaged devices

Applications

Browse a list of applications that are not protected by your policies.

View top unprotected apps

What's new

Named Locations

Microsoft Entra ID now supports IPv6! Update your Named locations with IPv6 ranges.

Learn more

1 policies have a Named Location condition

Security Alerts (Preview)

Geofiltrering

Conditional Access

Named locations

+ Countries location

+ IP ranges location

Configure multifactor authentication trusted IPs

Refresh

To go back to the old view, click here or use Preview features to turn off the enhanced named locations list experience and refresh

Named locations are used by Microsoft Entra security reports to reduce false positives and by Microsoft Entra Conditional Access Policies configured in Conditional Access Policies cannot be deleted. [Learn more](#)

Search by name

Location type: All types

Trusted

3 named locations found

Name	Location type	Trusted	Conditional Access policies
HomeOffice	IP ranges	Yes	Allow office-IP
IPer med onde hensikter	IP ranges	No	NeiTakkTilPhishing
Norden	Countries (IP)		Not configured in any policy yet

Blokkere PhishingIPer

Conditional Access

Named locations

+ Countries location

+ IP ranges location

Configure multifactor authentication trusted IPs

Refresh

To go back to the old view, click here or use Preview features to turn off the enhanced named locations list experience and refresh

Named locations are used by Microsoft Entra security reports to reduce false positives and by Microsoft Entra Conditional Access Policies configured in Conditional Access Policies cannot be deleted. [Learn more](#)

Search by name

Location type: All types Trusted

3 named locations found

Name	Location type	Trusted	Conditional Access policies
HomeOffice	IP ranges	Yes	Allow office-IP
IPer med onde hensikter	IP ranges	No	NeiTakkTilPhishing
Norden	Countries (IP)		Not configured in any policy yet

Update location (IP ranges)

Upload

Download

Delete

Configure named location IPv4 and IPv6 ranges. [Learn more](#)

Name *

IPer med onde hensikter

☐ Mark as trusted location

+ 91.92.245.226/32

Showing 1 - 1 of 1 results.

Norsk helsennett

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 *

NeiTakkTilPhishing 

Assignments

Users 

[All users](#)

Target resources 

[No target resources selected](#)

Conditions 

[1 condition selected](#)

Access controls

Grant 

[Block access](#)

Session 

[0 controls selected](#)

Enable policy

[Report-only](#)

On

Off

Create

PhishingIPer

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 *

NeiTakkTilPhishing

Assignments

Users ⓘ

[All users](#)

Target resources ⓘ

[No target resources selected](#)

Conditions ⓘ

[1 condition selected](#)

Access controls

Grant ⓘ

[Block access](#)

Session ⓘ

[0 controls selected](#)

Enable policy

[Report-only](#)

On

Off

Create

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 ⓘ

[1 included](#)

Client apps ⓘ

[Not configured](#)

Filter for devices ⓘ

[Not configured](#)

Authentication flows (Preview) ⓘ

[Not configured](#)

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 *

NeiTakkTilPhishing

Assignments

Users ⓘ

All users

Target resources ⓘ

No target resources selected

Conditions ⓘ

1 condition selected

Access controls

Grant ⓘ

Block access

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 ⓘ

1 included

Client apps ⓘ

Not configured

Filter for devices ⓘ

Not configured

Authentication flows (Preview) ⓘ

Not configured

Control user access based on their physical location. [Learn more](#)

Configure ⓘ

Yes

No

Include

Exclude



Any location



All trusted locations



Selected locations

Select

IPer med onde hensikter

IPer med onde hensikter



Enable policy

Report-only

On

Off

Create

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 *

NeiTakkTilPhishing

Assignments

Users ⓘ

All users

Target resources ⓘ

No target resources selected

Conditions ⓘ

1 condition selected

Access controls

Grant ⓘ

Block access

Session ⓘ

0 controls selected

Enable policy

Report-only

On

Off

Create

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 ⓘ

1 included

Client apps ⓘ

Not configured

Filter for devices ⓘ

Not configured

Authentication flows (Preview) ⓘ

Not configured

Control user access based on their physical location. [Learn more](#)

Configure ⓘ

Yes

No

Include Exclude

☐

Any location

☐

All trusted locations

☒

Selected locations

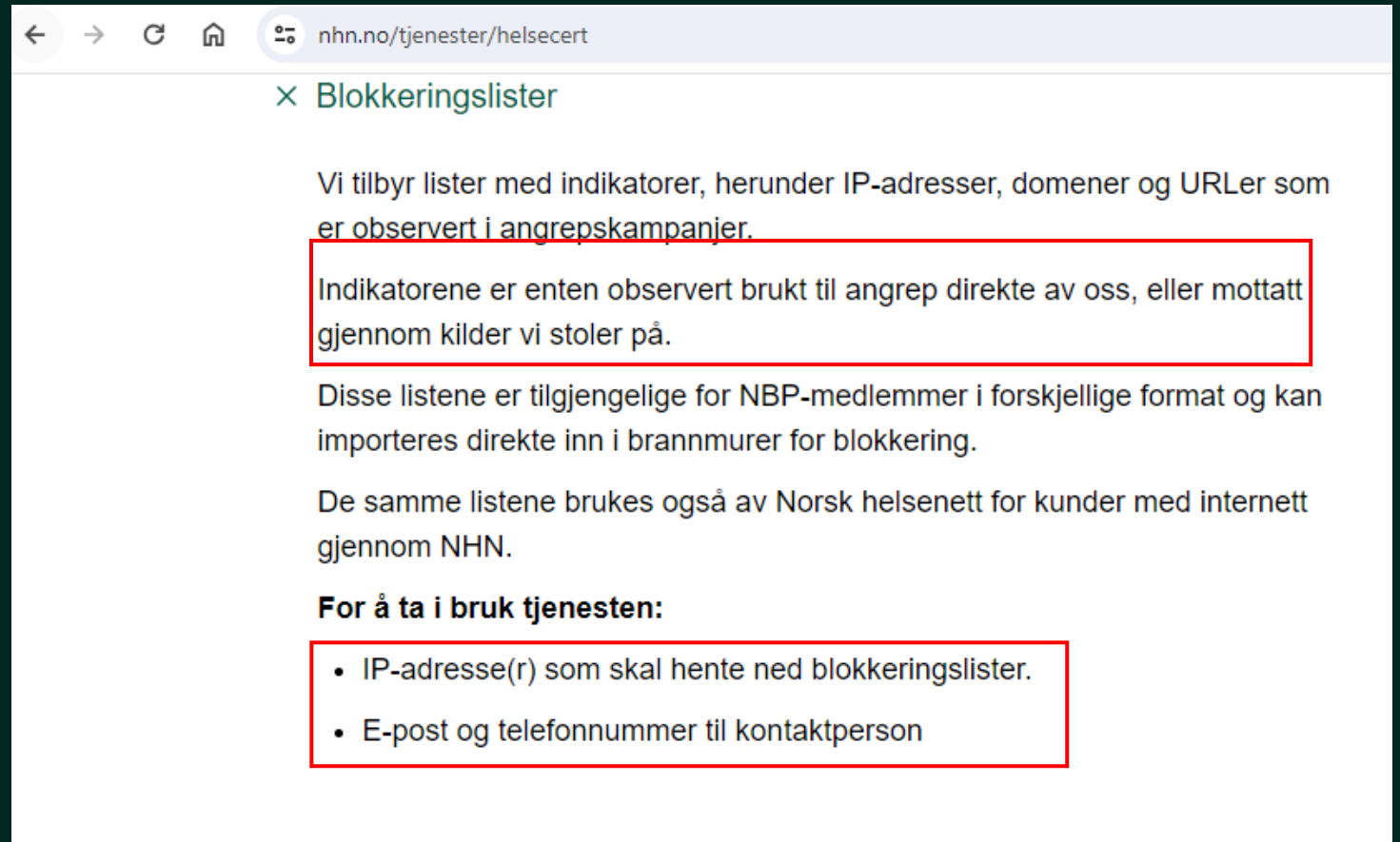
Select

IPer med onde hensikter

IPer med onde hensikter

...

Oppdag kjente angrep



The screenshot shows a web browser window with the address bar displaying 'nhn.no/tjenester/helsecert'. The page title is 'Blokkeringslister'. The main content explains that the service provides lists of indicators (IP addresses, domains, and URLs) observed in attack campaigns. It states that these indicators are either observed used directly by the service or received from trusted sources. The lists are available for NBP members in various formats and can be imported directly into firewalls for blocking. It also mentions that the same lists are used by the Norwegian Health Network for customers with internet access through NHN. A section titled 'For å ta i bruk tjenesten:' (To use the service:) lists two requirements: having an IP address to download the blocking lists, and having an email and phone number for the contact person.

← → ↻ 🏠 🌐 nhn.no/tjenester/helsecert

× Blokkeringslister

Vi tilbyr lister med indikatorer, herunder IP-adresser, domener og URLer som er observert i angrepskampanjer.

Indikatorene er enten observert brukt til angrep direkte av oss, eller mottatt gjennom kilder vi stoler på.

Disse listene er tilgjengelige for NBP-medlemmer i forskjellige format og kan importeres direkte inn i brannmurer for blokkering.

De samme listene brukes også av Norsk helsenett for kunder med internett gjennom NHN.

For å ta i bruk tjenesten:

- IP-adresse(r) som skal hente ned blokkeringslister.
- E-post og telefonnummer til kontaktperson

B



91.92.245.226
89.116.139.218
64.227.109.37
5.230.46.148
5.230.43.124
172.86.66.77
146.190.124.131
103.3.63.26
97.74.90.207
89.116.139.238
89.116.139.236
5.230.42.136
45.76.165.219
89.116.139.187
5.230.71.170
45.93.138.185
149.100.156.100
134.122.2.239
66.23.237.155
193.239.86.199
5.230.72.75
5.230.68.240
5.230.46.15
5.230.43.46
5.230.41.158
5.230.40.168
45.55.38.46
45.155.249.176
41.216.188.55
20.246.92.133
174.138.180.83
159.203.163.52
176.130.165.145
144.172.122.210
88.77.25.240
92.205.111.169
5.230.45.253
45.79.253.203
190.123.45.88
185.124.109.152
159.203.115.194
91.245.255.11
91.92.253.235
5.230.70.184
167.88.164.140
5.230.73.239
5.230.44.181
128.199.12.192
91.92.253.110
83.229.81.158
64.94.94.169
5.230.41.142
31.7.188.109
185.124.108.59
176.10.111.118
173.44.141.182
167.88.174.147
159.223.84.60
89.116.23.133
89.116.22.232
64.23.191.144
5.230.75.189
5.230.47.156
5.230.44.142
5.230.40.215
45.11.183.189
134.209.118.30
91.92.248.166
74.58.80.89
5.230.70.179
5.230.57.112
5.230.54.157
5.230.41.136
45.11.183.187
176.10.111.93
173.254.235.55
146.70.157.92
172.86.64.44
187.88.174.139
5.230.67.38
91.92.248.182
89.116.22.235
5.230.73.126
5.230.70.200
208.73.206.148
179.205.52.153
85.17.9.61
74.58.80.150
5.230.40.161
184.160.164.238
89.116.23.19
89.116.22.242
89.116.22.241
89.116.159.182
5.230.73.90
5.230.73.115
5.230.45.196
195.35.56.236
185.212.47.14
159.89.42.187
5.230.67.152
5.230.52.104
208.73.202.213
182.254.35.138
157.245.87.215
208.73.205.156
5.230.72.215
5.230.52.31
142.93.99.212
5.230.53.30
179.130.165.52
167.172.16.119
85.17.9.126
5.230.67.160
5.230.57.151
5.230.51.245
5.230.43.198
89.116.167.54
74.58.81.174

89.116.139.218
64.227.109.37
5.230.46.148
5.230.43.124
172.86.66.77
146.190.124.131
103.3.63.26
97.74.90.207
89.116.139.238
89.116.139.236
5.230.42.136
45.76.165.219
89.116.139.187
5.230.71.170
45.93.138.185
149.100.156.100
134.122.2.239
66.23.237.155
193.239.86.199
5.230.72.75
5.230.68.240
5.230.46.15
5.230.43.46
5.230.41.158
5.230.40.168
45.55.38.46
45.155.249.176
41.216.188.55
20.246.92.133
174.138.180.83
159.203.163.52
176.130.165.145
144.172.122.210
88.77.25.240
92.205.111.169
5.230.45.253
45.79.253.203
190.123.45.88
185.124.109.152
159.203.115.194
91.245.255.11
91.92.253.235
5.230.70.184
167.88.164.140
5.230.73.239
5.230.44.181
128.199.12.192
91.92.253.110
83.229.81.158
64.94.94.169
5.230.41.142
31.7.188.109
185.124.108.59
176.10.111.118
173.44.141.182
167.88.174.147
159.223.84.60
89.116.23.133
89.116.22.232
64.23.191.144
5.230.75.189
5.230.47.156
5.230.44.142
5.230.40.215
45.11.183.189
134.209.118.30
91.92.248.166
74.58.80.89
5.230.70.179
5.230.57.112
5.230.54.157
5.230.41.136
45.11.183.187
176.10.111.93
173.254.235.55
146.70.157.92
172.86.64.44
187.88.174.139
5.230.67.38
91.92.248.182
89.116.22.235
5.230.73.126
5.230.70.200
208.73.206.148
179.205.52.153
85.17.9.61
74.58.80.150
5.230.40.161
184.160.164.238
89.116.23.19
89.116.22.242
89.116.22.241
89.116.159.182
5.230.73.90
5.230.73.115
5.230.45.196
195.35.56.236
185.212.47.14
159.89.42.187
5.230.67.152
5.230.52.104
208.73.202.213
182.254.35.138
157.245.87.215
208.73.205.156
5.230.72.215
5.230.52.31
142.93.99.212
5.230.53.30
179.130.165.52
167.172.16.119
85.17.9.126
5.230.67.160
5.230.57.151
5.230.51.245
5.230.43.198
89.116.167.54
74.58.81.174

nhn.no/blocklist/v2/?t=ipv4&f=list&category=phishing

89.116.139.218
64.227.109.37
5.230.46.148
5.230.43.124
172.86.66.77
146.190.124.131
103.3.63.26
97.74.90.207
89.116.139.238
89.116.139.236
5.230.42.136
45.76.165.219
89.116.139.187
5.230.71.170
45.93.138.185
149.100.156.100
134.122.2.239
66.23.237.155
193.239.86.199
5.230.72.75
5.230.68.240
5.230.46.15
5.230.43.46
5.230.41.158
5.230.40.168
45.55.38.46
45.155.249.176
41.216.188.55
20.246.92.133
174.138.180.83
159.203.163.52
176.130.165.145
144.172.122.210
88.77.25.240
92.205.111.169
5.230.45.253
45.79.253.203
190.123.45.88
185.124.109.152
159.203.115.194
91.245.255.11
91.92.253.235
5.230.70.184
167.88.164.140
5.230.73.239
5.230.44.181
128.199.12.192
91.92.253.110
83.229.81.158
64.94.94.169
5.230.41.142
31.7.188.109
185.124.108.59
176.10.111.118
173.44.141.182
167.88.174.147
159.223.84.60
89.116.23.133
89.116.22.232
64.23.191.144
5.230.75.189
5.230.47.156
5.230.44.142
5.230.40.215
45.11.183.189
134.209.118.30
91.92.248.166
74.58.80.89
5.230.70.179
5.230.57.112
5.230.54.157
5.230.41.136
45.11.183.187
176.10.111.93
173.254.235.55
146.70.157.92
172.86.64.44
187.88.174.139
5.230.67.38
91.92.248.182
89.116.22.235
5.230.73.126
5.230.70.200
208.73.206.148
179.205.52.153
85.17.9.61
74.58.80.150
5.230.40.161
184.160.164.238
89.116.23.19
89.116.22.242
89.116.22.241
89.116.159.182
5.230.73.90
5.230.73.115
5.230.45.196
195.35.56.236
185.212.47.14
159.89.42.187
5.230.67.152
5.230.52.104
208.73.202.213
182.254.35.138
157.245.87.215
208.73.205.156
5.230.72.215
5.230.52.31
142.93.99.212
5.230.53.30
179.130.165.52
167.172.16.119
85.17.9.126
5.230.67.160
5.230.57.151
5.230.51.245
5.230.43.198
89.116.167.54
74.58.81.174

89.116.139.218
64.227.109.37
5.230.46.148
5.230.43.124
172.86.66.77
146.190.124.131
103.3.63.26
97.74.90.207
89.116.139.238
89.116.139.236
5.230.42.136
45.76.165.219
89.116.139.187
5.230.71.170
45.93.138.185
149.100.156.100
134.122.2.239
66.23.237.155
193.239.86.199
5.230.72.75
5.230.68.240
5.230.46.15
5.230.43.46
5.230.41.158
5.230.40.168
45.55.38.46
45.155.249.176
41.216.188.55
20.246.92.133
174.138.180.83
159.203.163.52
176.130.165.145
144.172.122.210
88.77.25.240
92.205.111.169
5.230.45.253
45.79.253.203
190.123.45.88
185.124.109.152
159.203.115.194
91.245.255.11
91.92.253.235
5.230.70.184
167.88.164.140
5.230.73.239
5.230.44.181
128.199.12.192
91.92.253.110
83.229.81.158
64.94.94.169
5.230.41.142
31.7.188.109
185.124.108.59
176.10.111.118
173.44.141.182
167.88.174.147
159.223.84.60
89.116.23.133
89.116.22.232
64.23.191.144
5.230.75.189
5.230.47.156
5.230.44.142
5.230.40.215
45.11.183.189
134.209.118.30
91.92.248.166
74.58.80.89
5.230.70.179
5.230.57.112
5.230.54.157
5.230.41.136
45.11.183.187
176.10.111.93
173.254.235.55
146.70.157.92
172.86.64.44
187.88.174.139
5.230.67.38
91.92.248.182
89.116.22.235
5.230.73.126
5.230.70.200
208.73.206.148
179.205.52.153
85.17.9.61
74.58.80.150
5.230.40.161
184.160.164.238
89.116.23.19
89.116.22.242
89.116.22.241
89.116.159.182
5.230.73.90
5.230.73.115
5.230.45.196
195.35.56.236
185.212.47.14
159.89.42.187
5.230.67.152
5.230.52.104
208.73.202.213
182.254.35.138
157.245.87.215
208.73.205.156
5.230.72.215
5.230.52.31
142.93.99.212
5.230.53.30
179.130.165.52
167.172.16.119
85.17.9.126
5.230.67.160
5.230.57.151
5.230.51.245
5.230.43.198
89.116.167.54
74.58.81.174

- Data fra hendelser i NBP
- Dere har varslet oss
 - Fortsett med det
- Angripere gjenbruker IP
- Varsel i innboksen hjelper ingen

Blokklister

- SYSIKT automatiserte løsningen
 - Blokklist automatisk inn i M365
 - Blokklist-IPer søkes etter siste 30 dagene
- Krever:
 - NBP blocklist
 - Microsoft P1 – lisens
- Skriptet kjøres fra maskin i Windows task scheduler

```
$NBPUser = "Virksomhet" # Brukernavn for NBP

$smtpserver = "X.X.X.X" # IP til SMTP server
$smtppto = "sikkerhetsansvarlig@virksomhet.no", "support@virksomhet.no" # Epost mottakere
$smtpfrom = "noreply@virksomhet.no" # Epost avsender

# Lokasjon for csv fil
$NamedLocations = "C:\Scripts\_Task scheduler\HelseCertBlocklistIPv4.csv"

# lokasjon for signins fra blocklista
$Signinslog = "C:\Scripts\_Task scheduler\SigninLogs.txt"

# lokasjon for signins fra blocklista
$Keysfil = "C:\Scripts\_Task scheduler\keys.txt"

# Variabler som må endrast for å koble til Microsoft Graph og oppdatere Named Location
$TenantId = "12345678-abcd-1234-abcd-0123456789abcd" # Tenant ID til Azure AD
$AppId = "12345678-1234-abcd-1234-0123456789abcd" # App ID til app registrert i Azure AD
$CertificateThumbprint = "AA123456ABC12345ABC41B4F20E4B2D1" # Thumbprint til sertifikat som er lasta opp i Azure AD
#####
# Slutt: Variabler som må endrast
#####

# Henter inn nøkkeldata fra filen nokler.txt
Get-Content ./keys.txt | ForEach-Object {
    $key, $val = $_ -split '='
    if ($key -eq 'NBPPass') { $NBPPass=$val }
    elseif ($key -eq 'TenantId') { $TenantId=$val }
    elseif ($key -eq 'AppId') { $AppId=$val }
    elseif ($key -eq 'CertificateThumbprint') { $CertificateThumbprint=$val }
}
```

Tilgjengelig på:

- <https://github.com/helsecert/blocklist>
- Ser du noe som kan forbedre?
 - Vi tar gjerne
 - pull request
 - Forbedringsforslag

|| Oppsummert



Sikre administratorer



Sett spam-policy



Bruk blokkeringslister

Microsoft 365

Stort tema

Takk for oppmerksomheten

