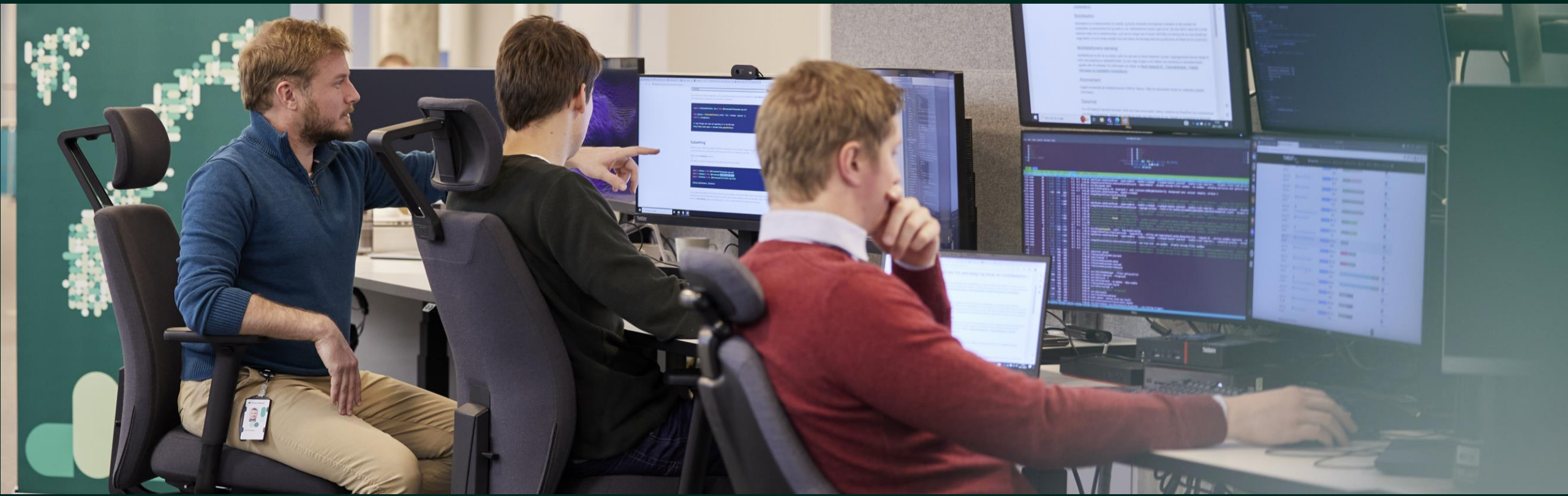
Norsk helsenett

HelseCERT

Webinaret starter snart…

Webinar – Herding Microsoft Entra ID

Mars 2024

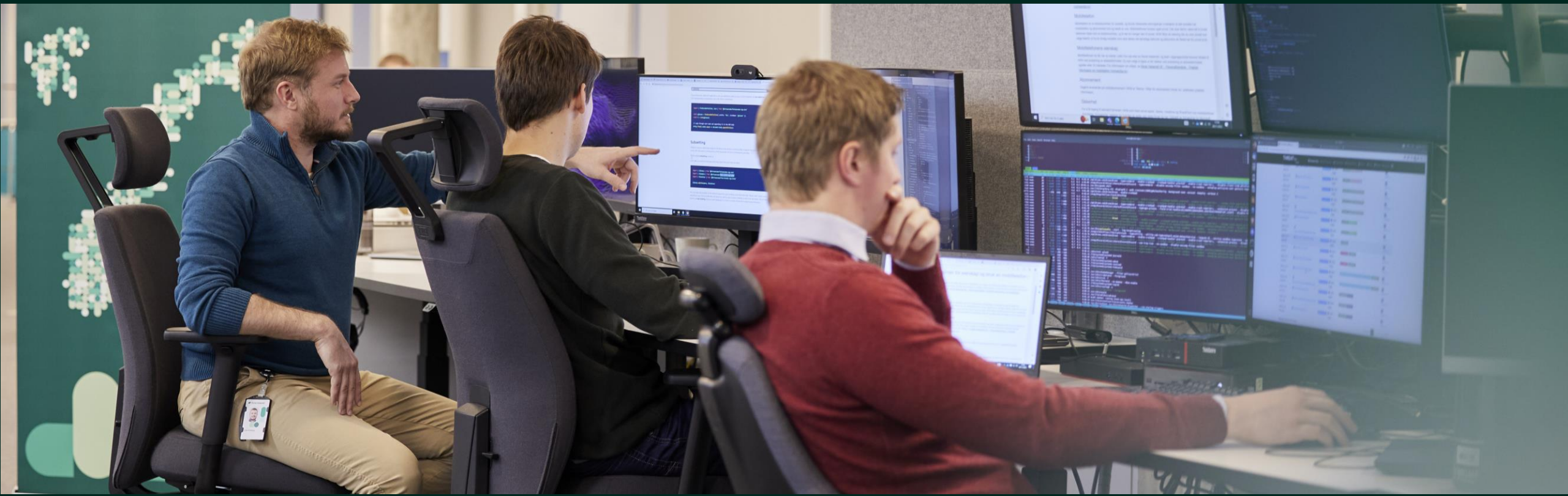


Norsk helsenett

HelseCERT
Herding Microsoft Entra ID

Webinar

Mars 2024

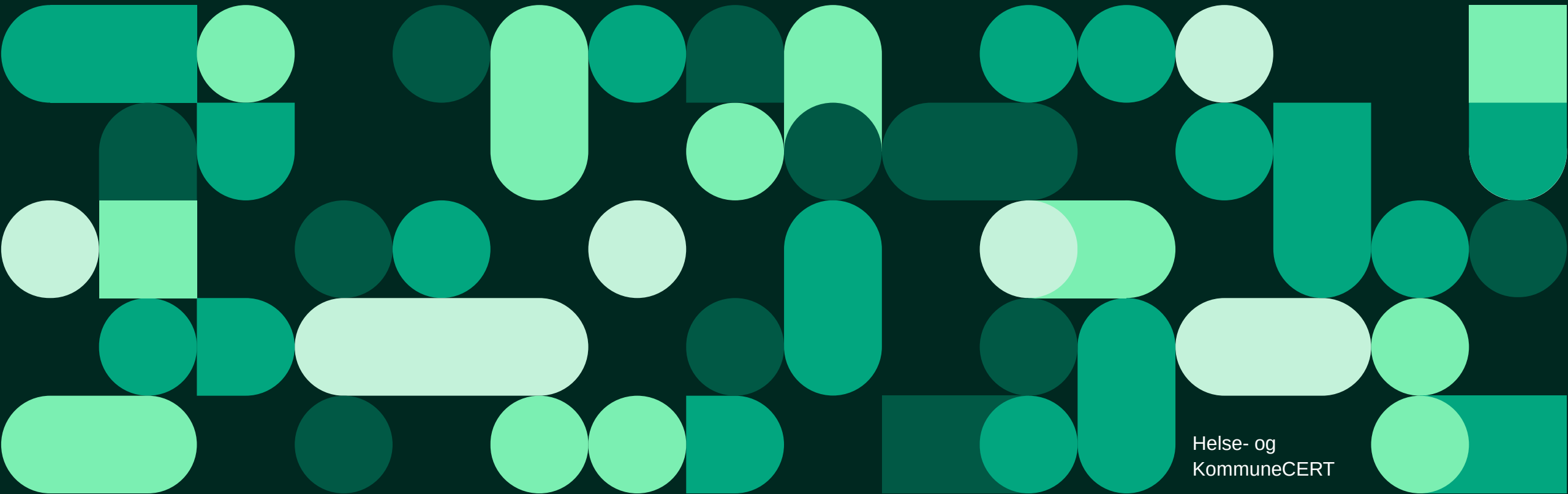


Norsk helsenett

(Intro)
Herding Microsoft Entra ID

Mars 2024

Hans Kristian Strømme



Helse- og
KommuneCERT

Agenda

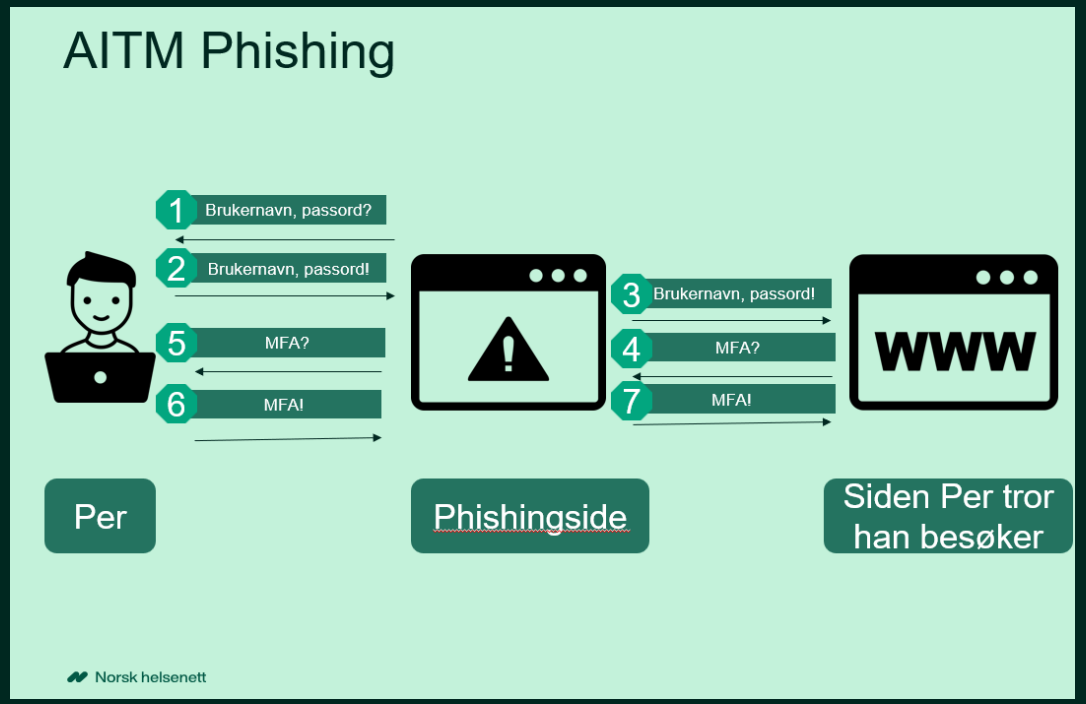
- Hvorfor
- Hvordan
  - Sikre administratorer
  - Begrens e-post
  - Conditional access
    - Geofiltrering
    - Bruk blokkeringslister

- Lenker deles i chat og med webinar-opptak

Hvorfor

Alle kan bli lurt av phishing

Bevisstgjøring hjelper

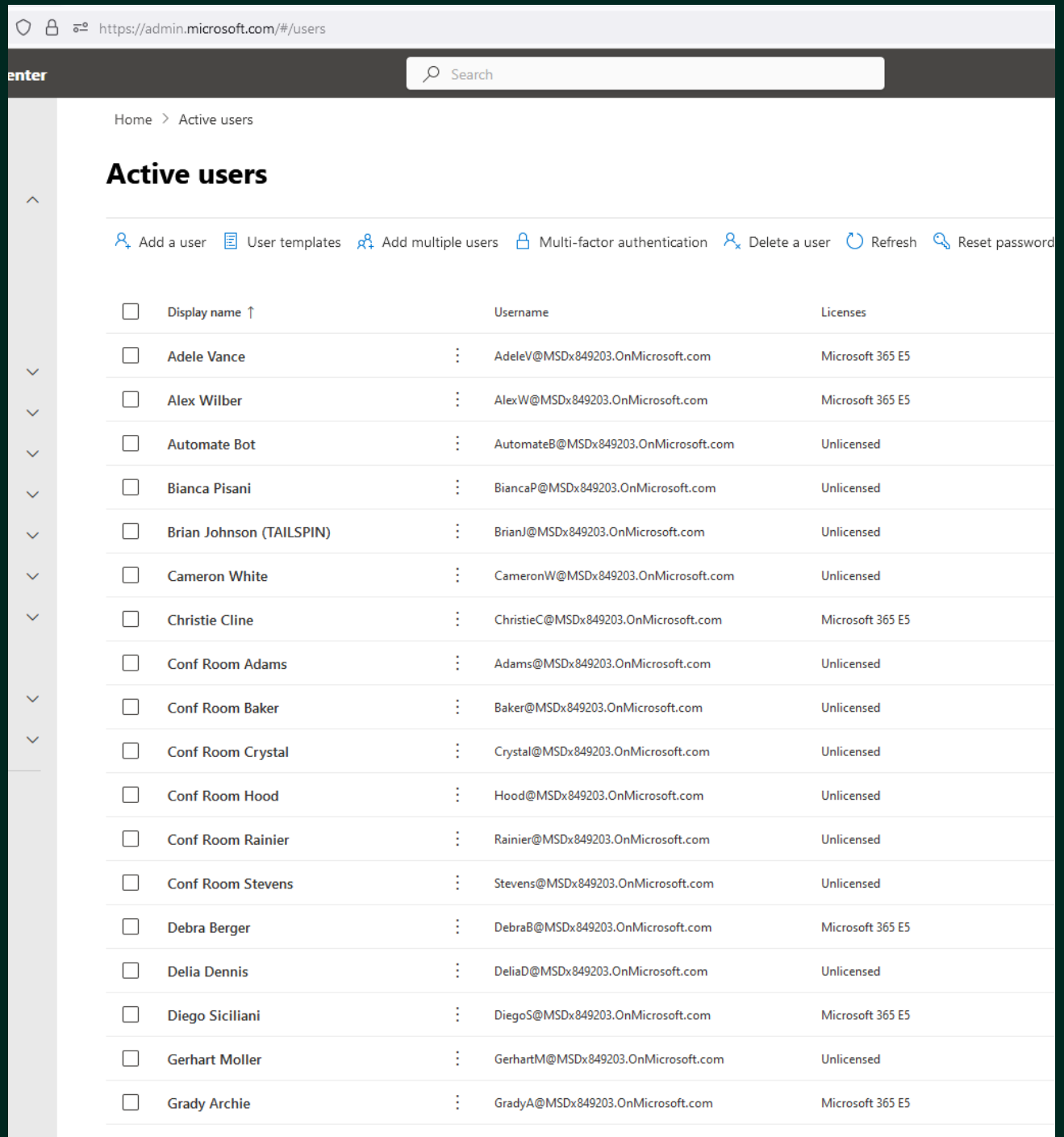


Administratorer

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

Administratorer

Fjern unødvendige



Admini

Fje

Home > Active users

Enable Dark mode

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

Global ad...

Display name ↑	Username
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

Choose columns

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

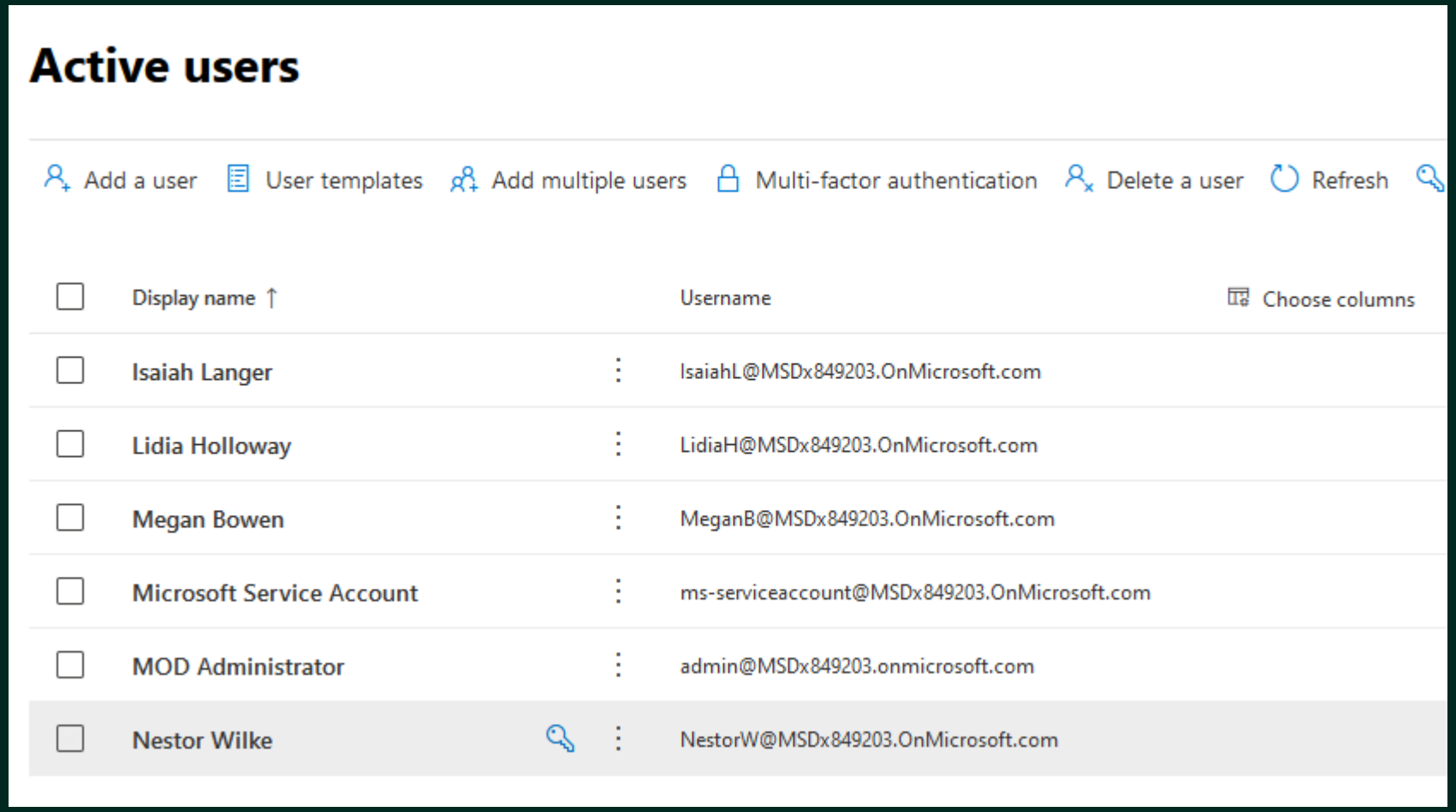
Unlicensed users

User admins

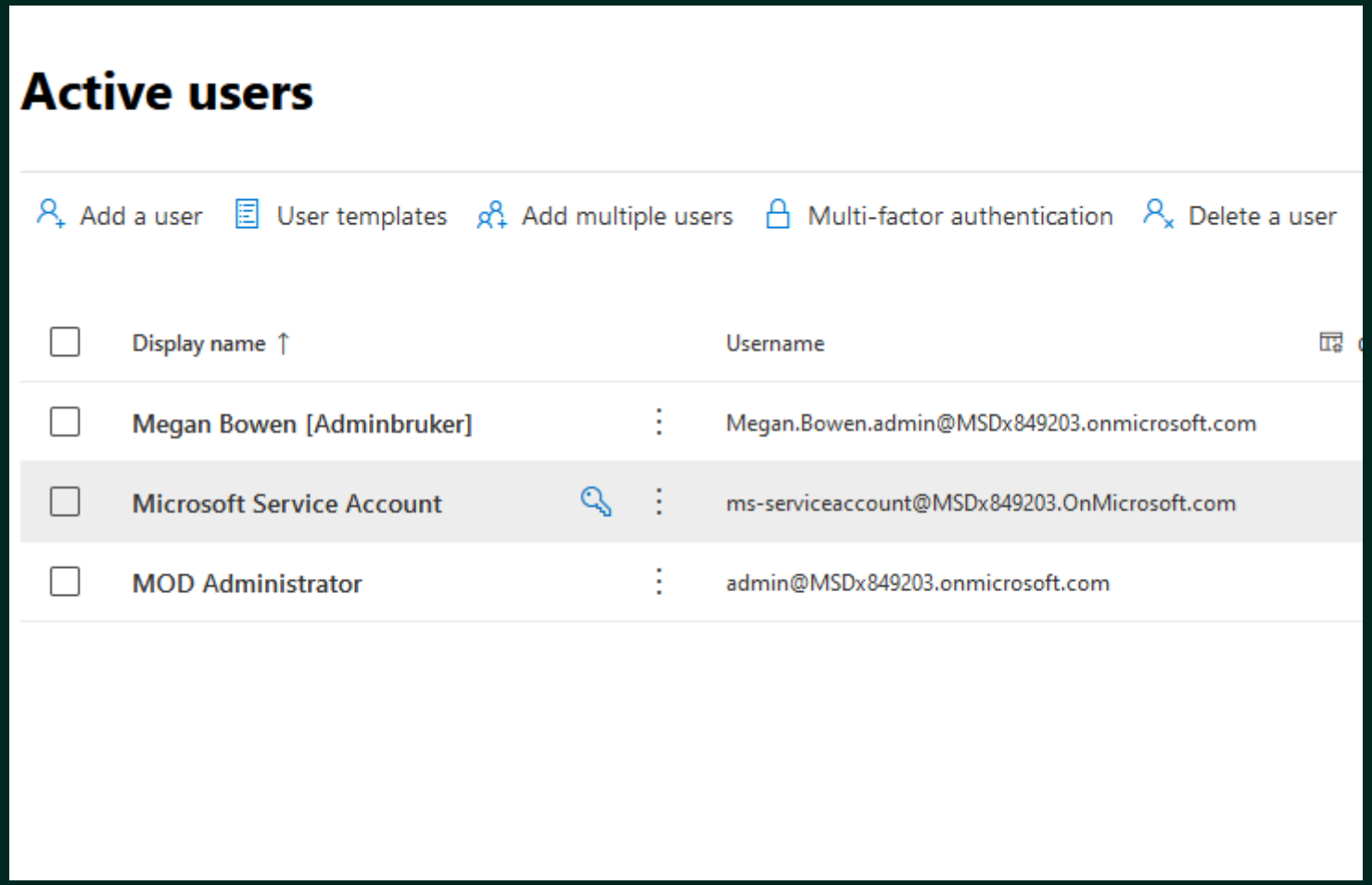
Users with errors

Norsk

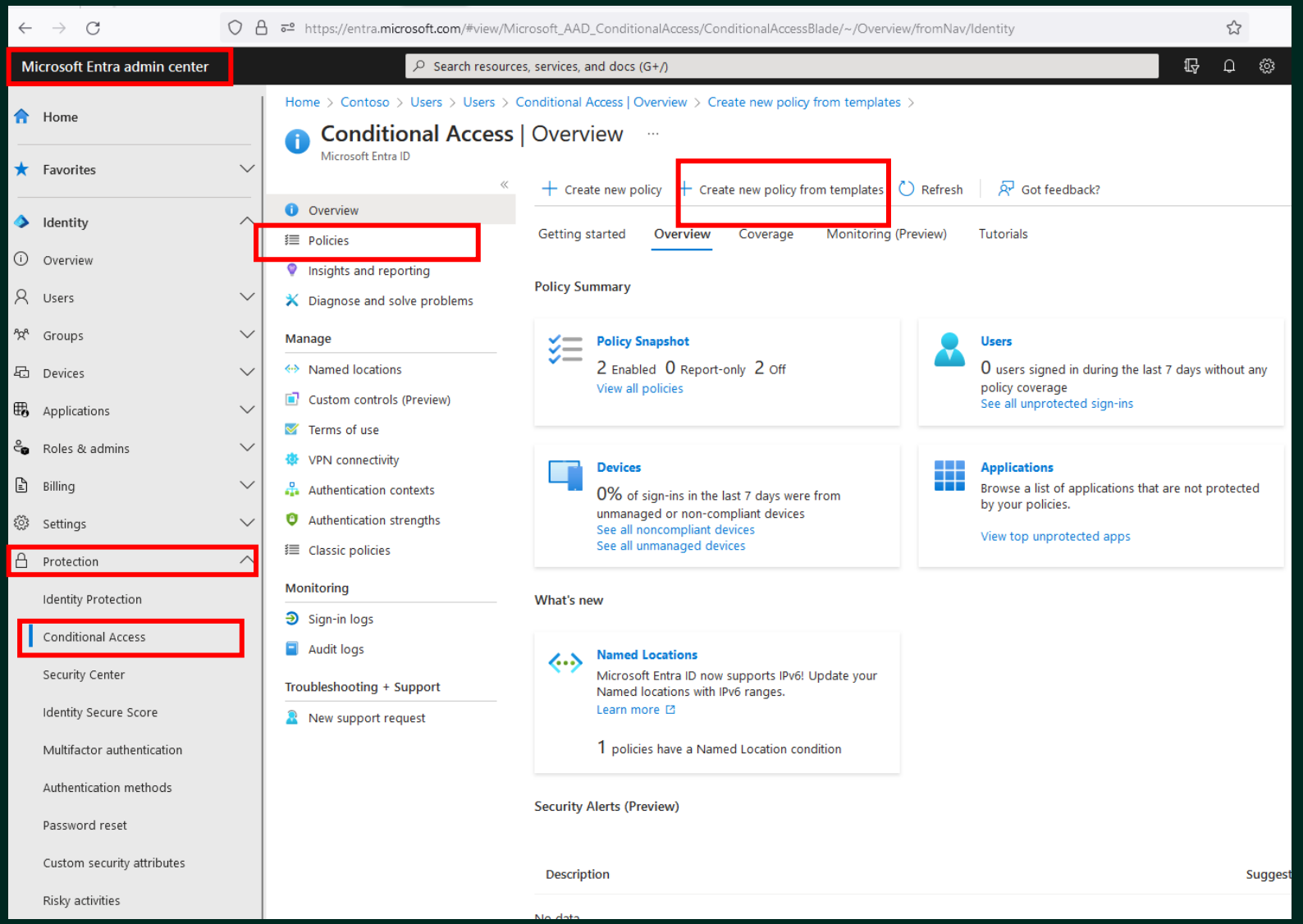
Fjern unødvendige



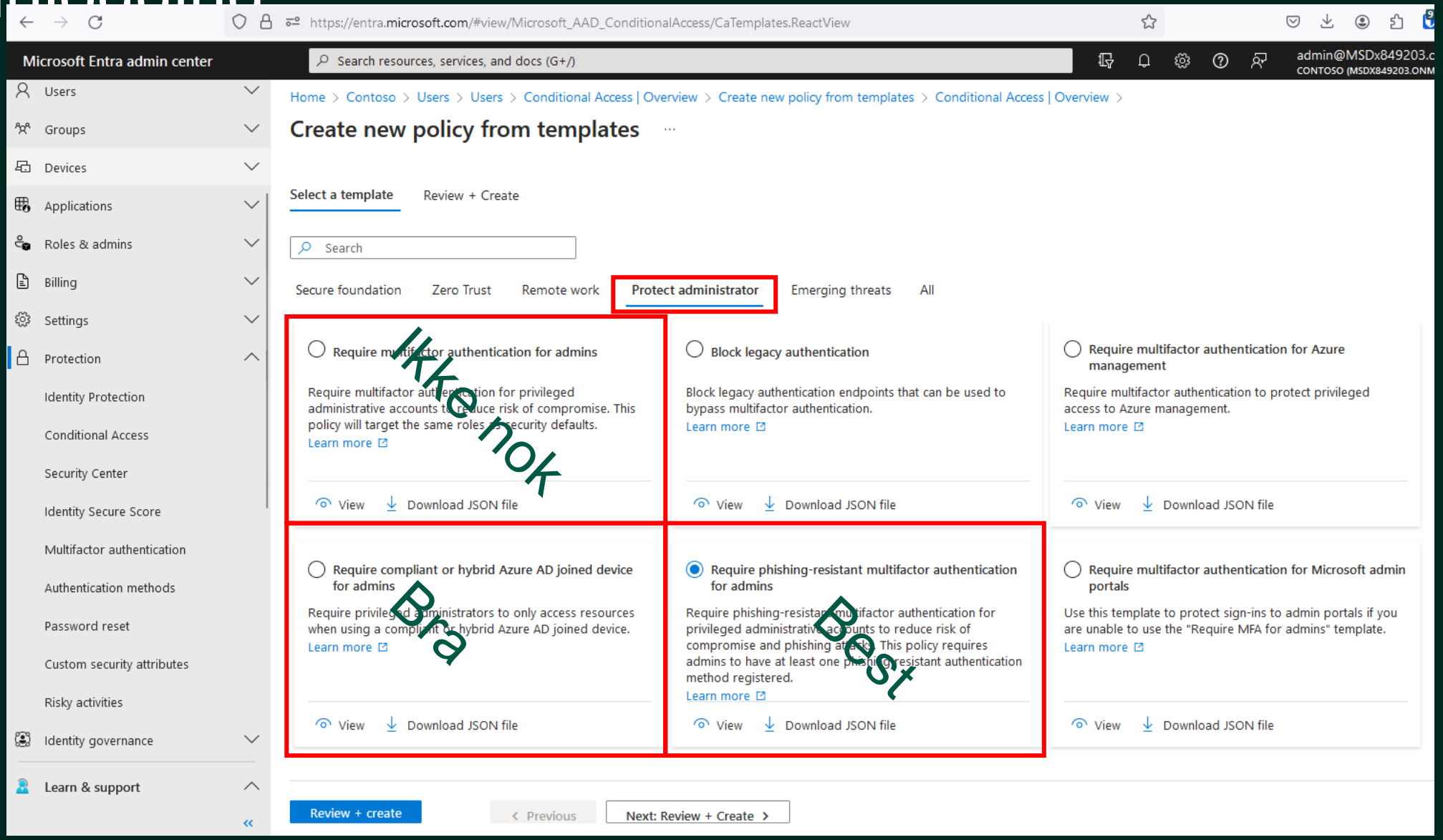
Fjern unødvendige | Ikke kjør admin i det daglige



Sikre innlogging

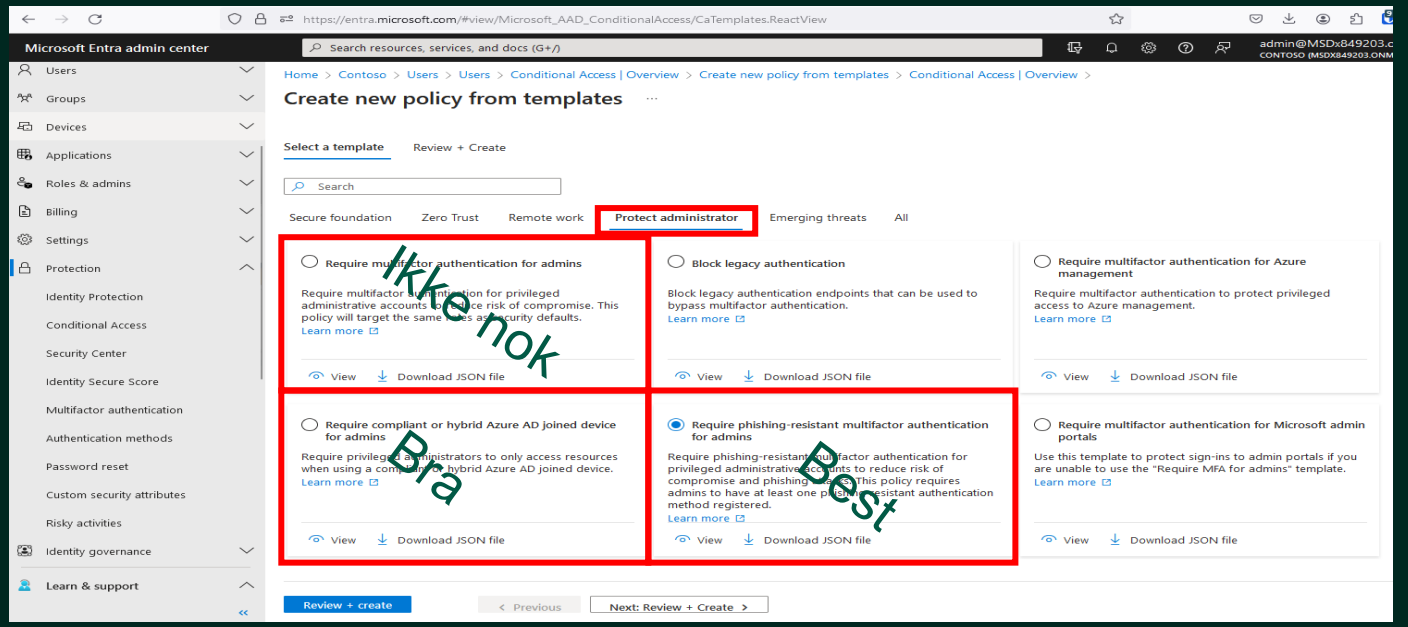


Sikre innlogging



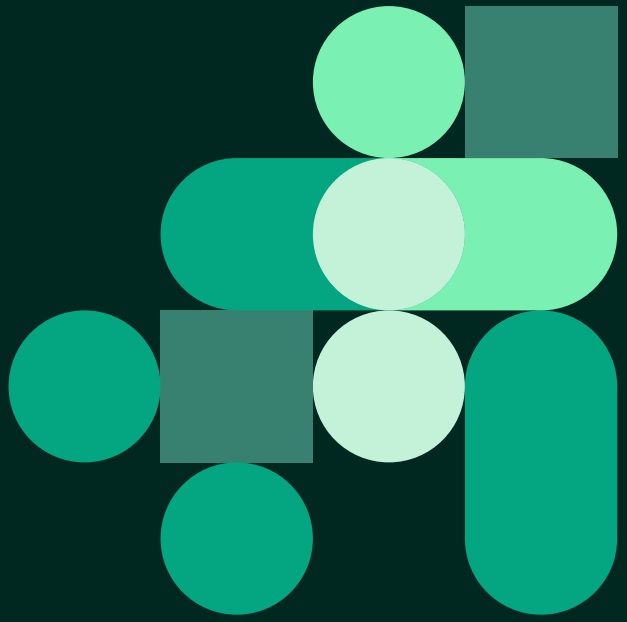
Sikre innlogging

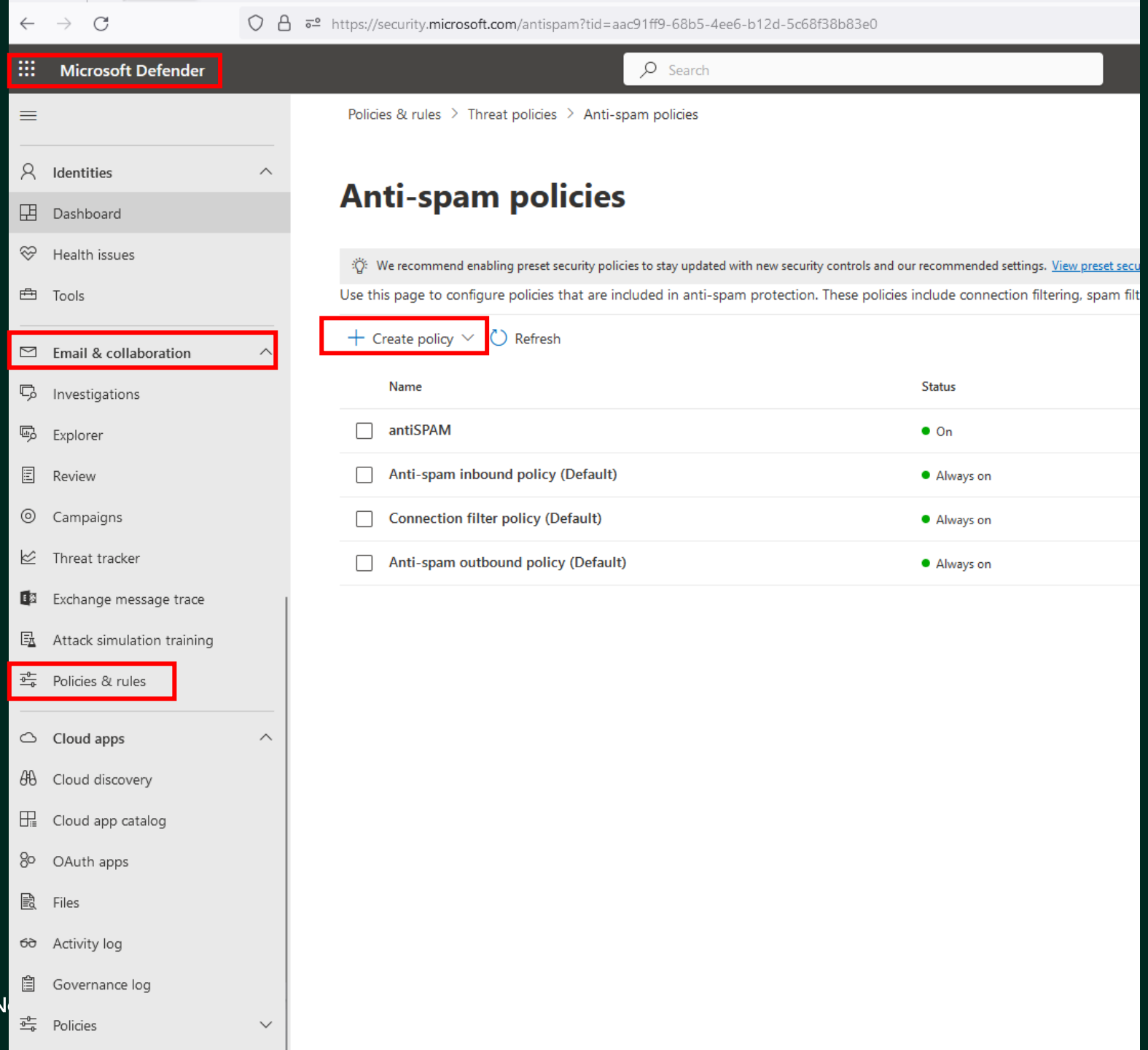
- Innrullering av enheter
- Utrulling av policy

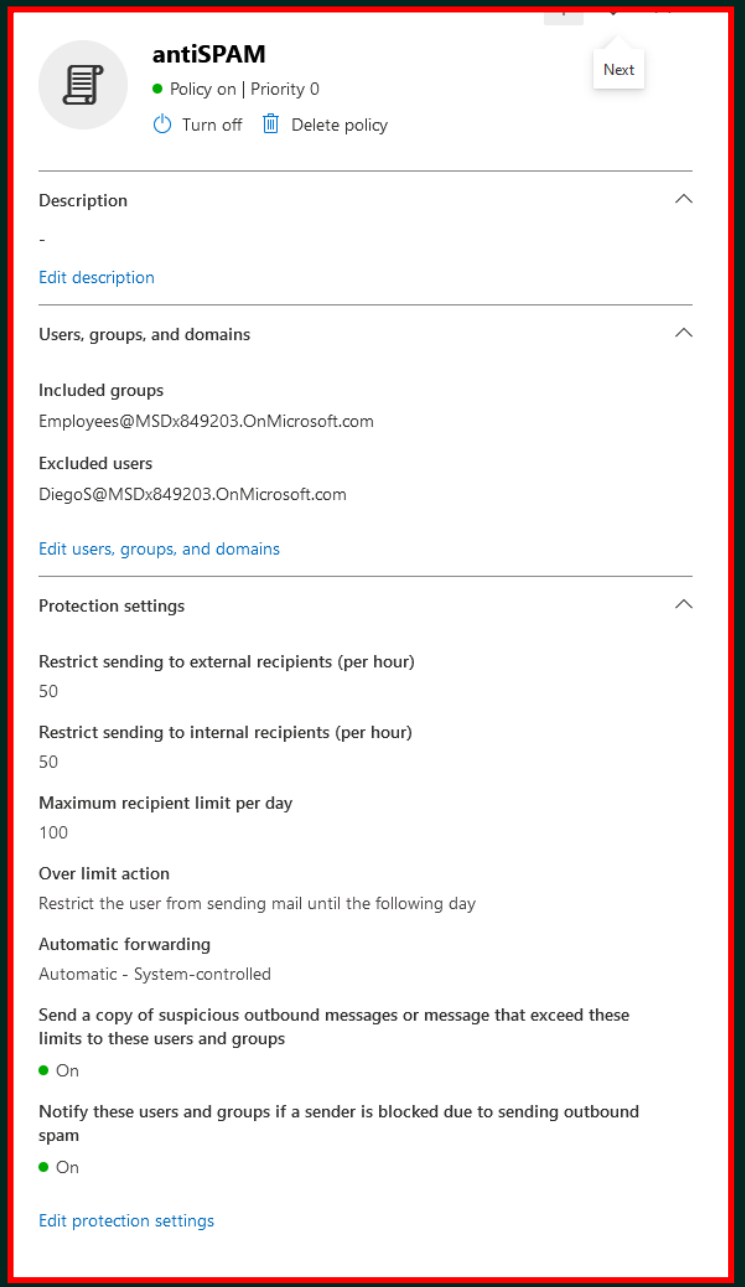


Anti-spam

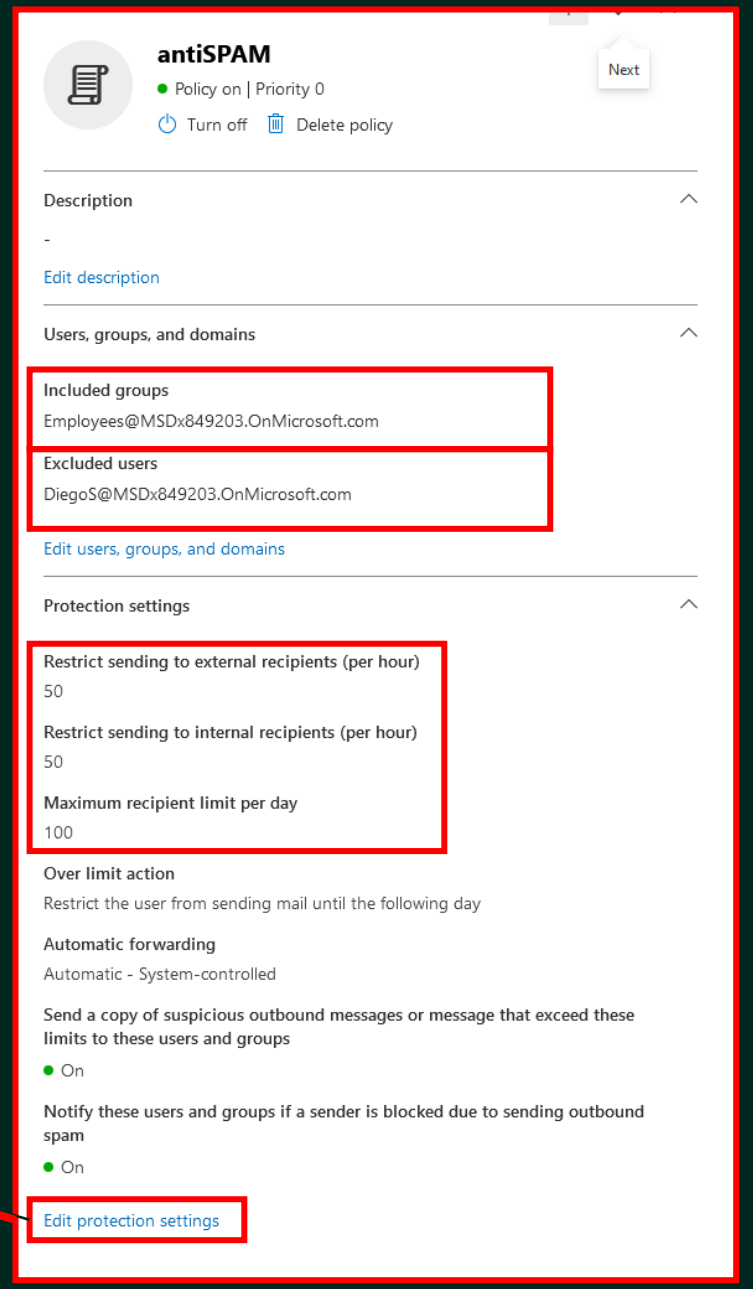
Hvorfor sende ut mye spam om du ikke må?




https://security.microsoft.com/antispam?tid=aac91ff9-68b5-4ee6-b12d-5c68f38b83e0
Microsoft Defender
Search
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
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 secu
Use this page to configure policies that are included in anti-spam protection. These policies include connection filtering, spam filt
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

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

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

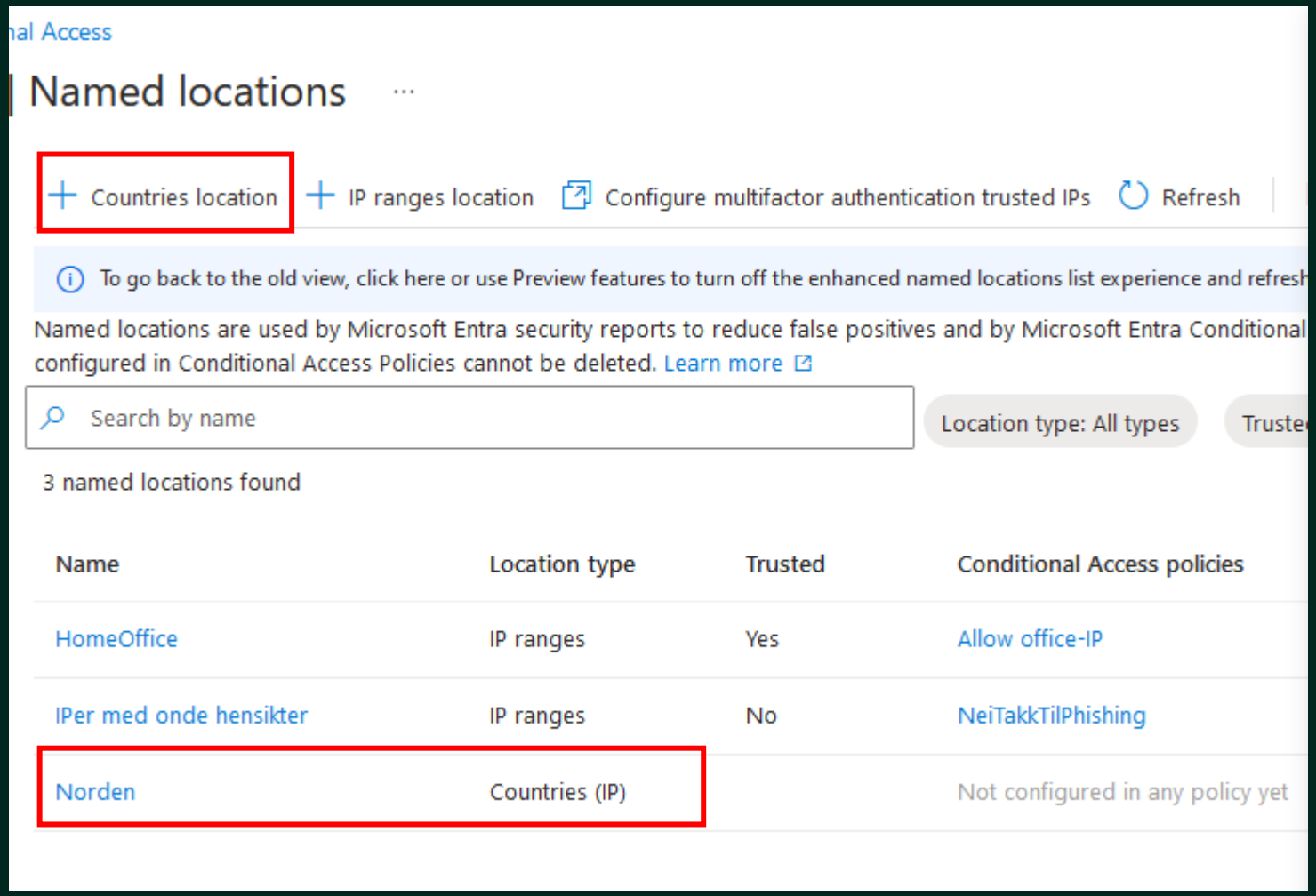
What's new

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

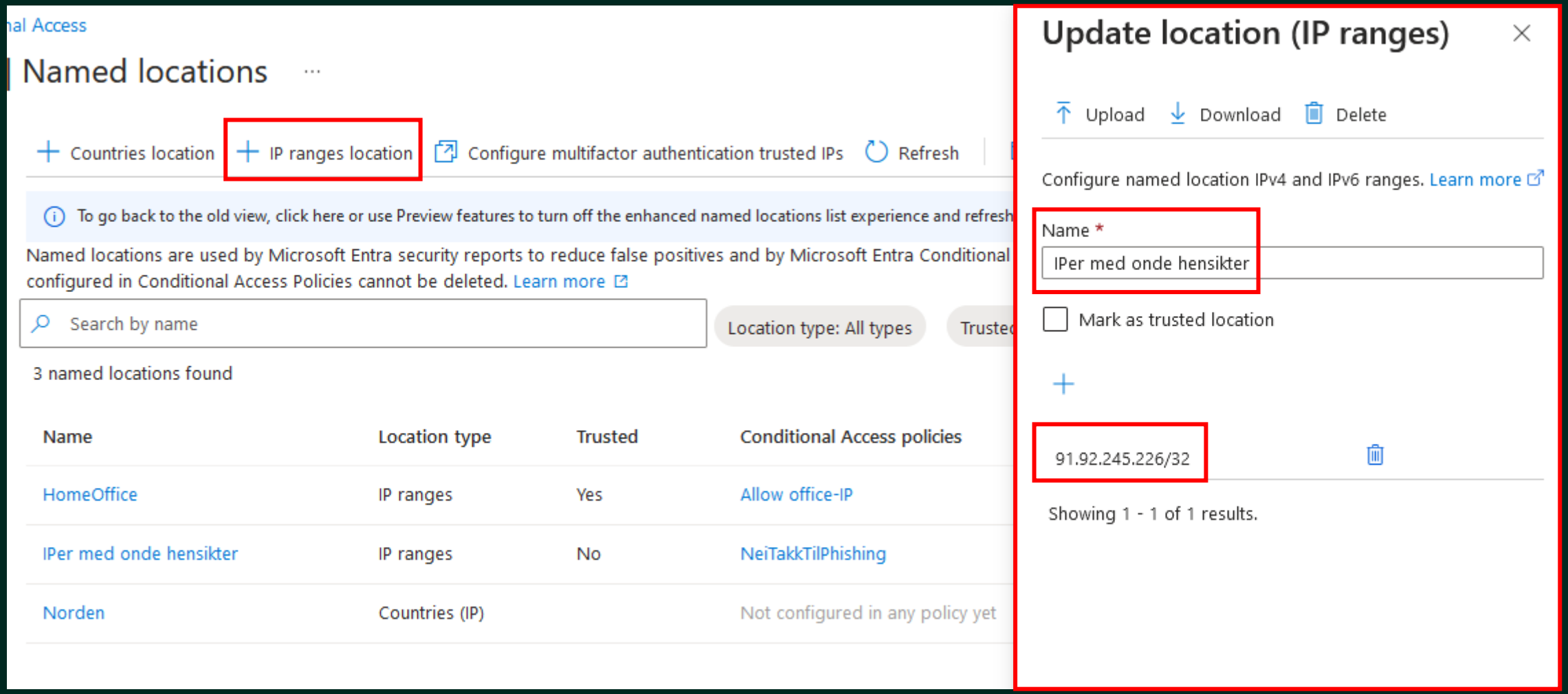
1 policies have a Named Location condition

Security Alerts (Preview)

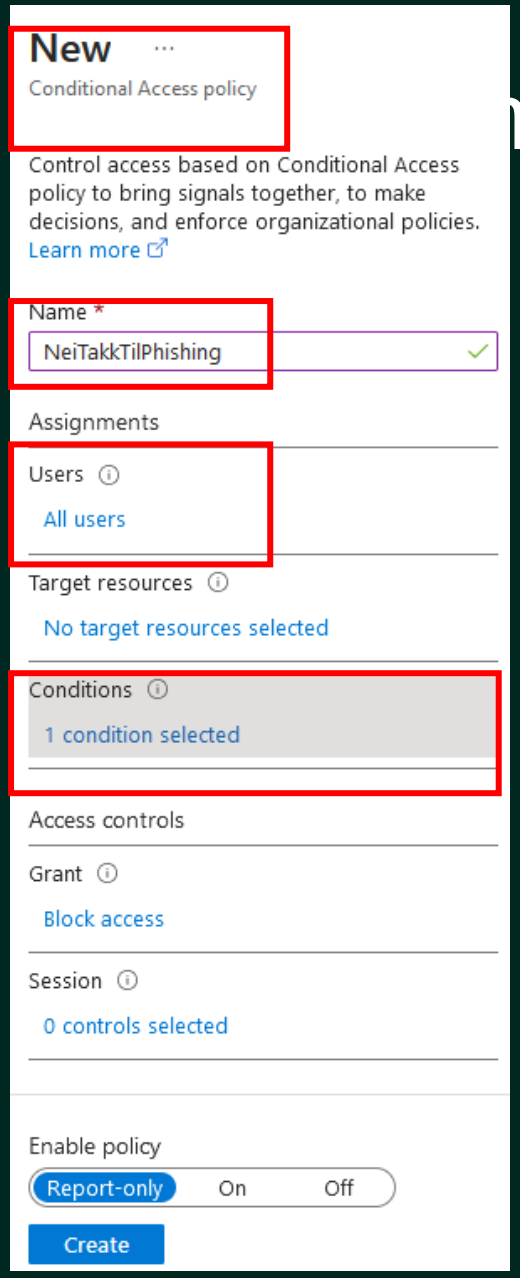
Geofiltrering



Blokkere PhishingIPer



hishingIPer



Home > hanskr | Audit logs > Conditional Access | Policies >

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

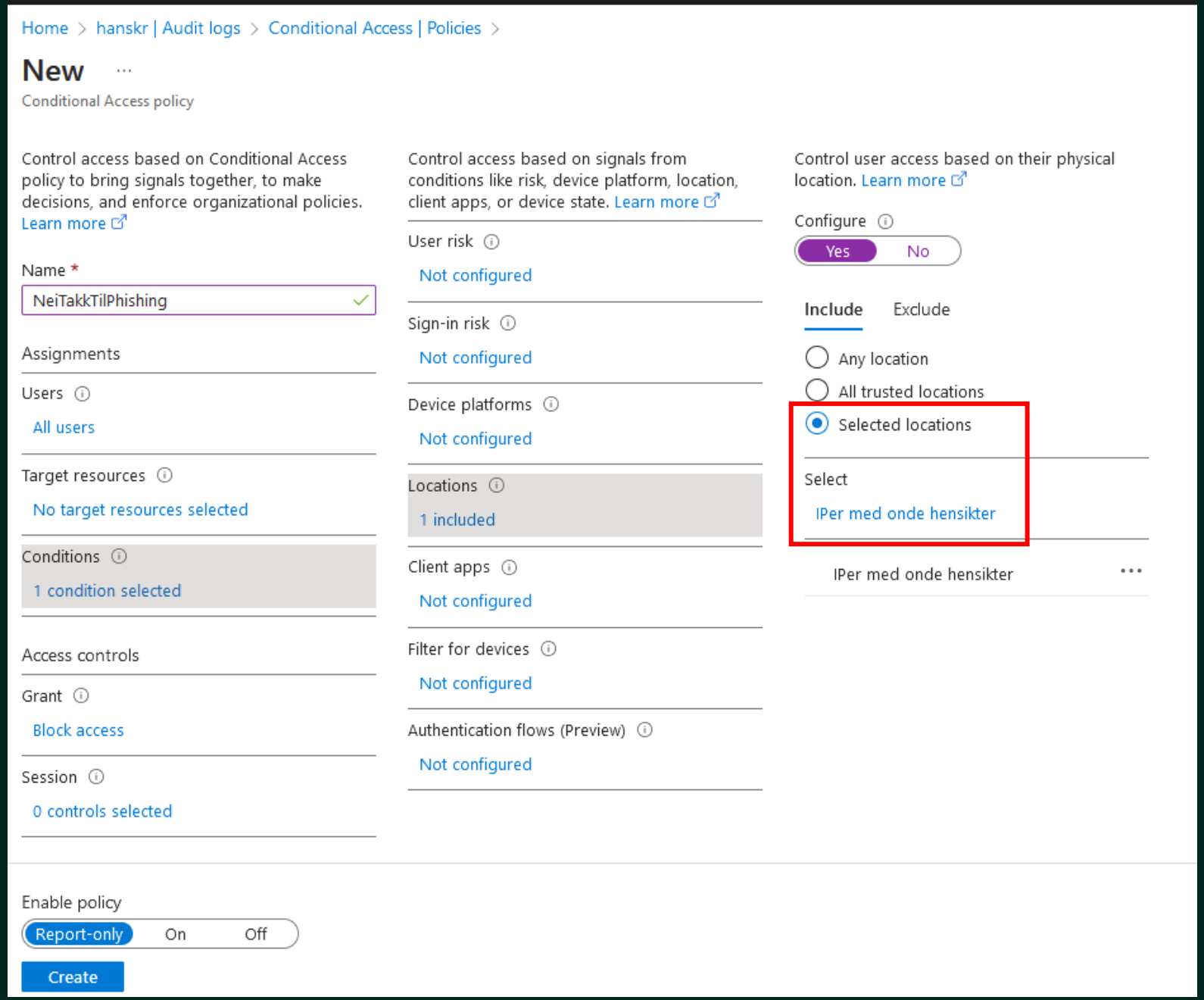
Authentication flows (Preview)

Not configured

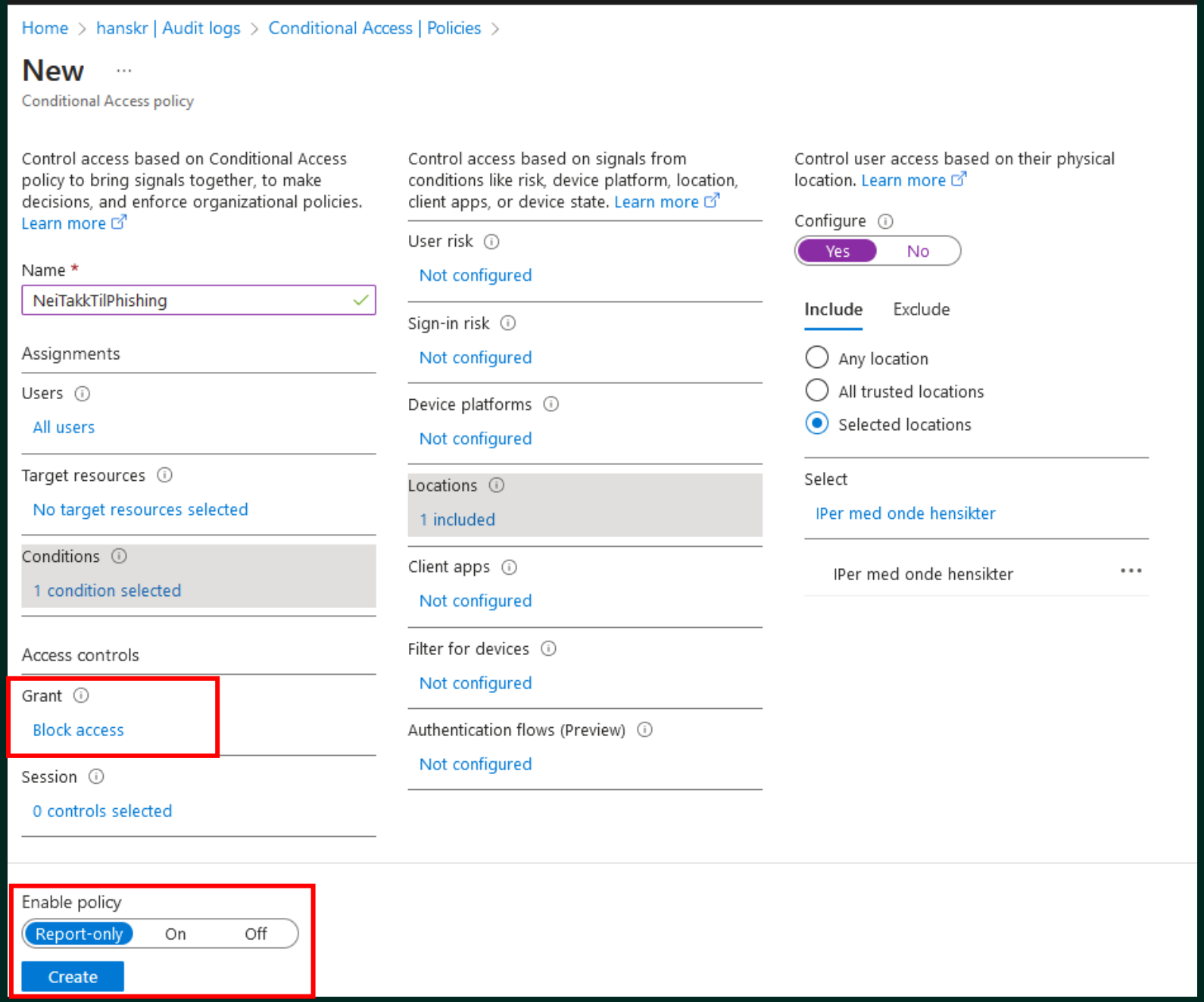
Enable policy

Report-only | On | Off

Create

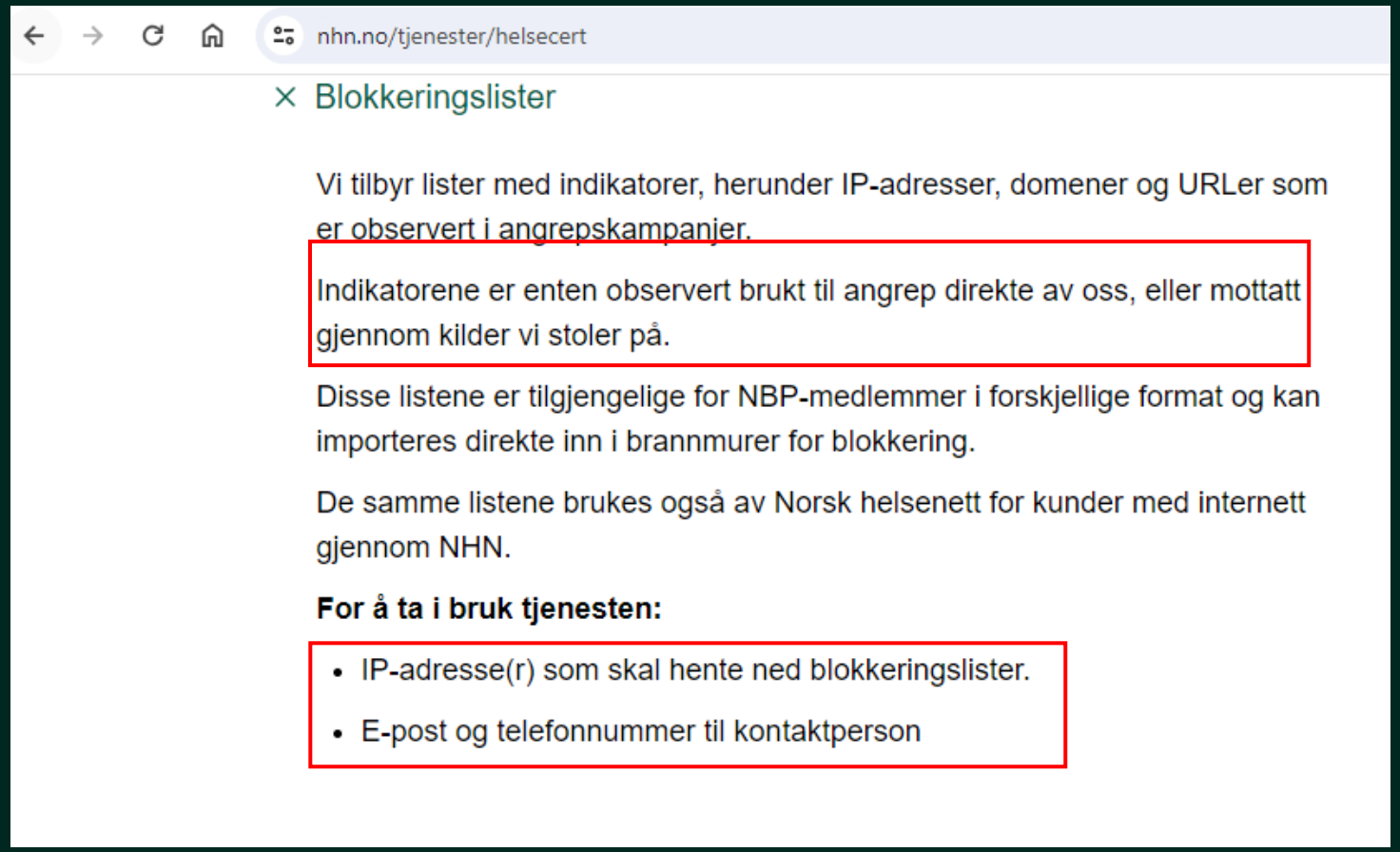


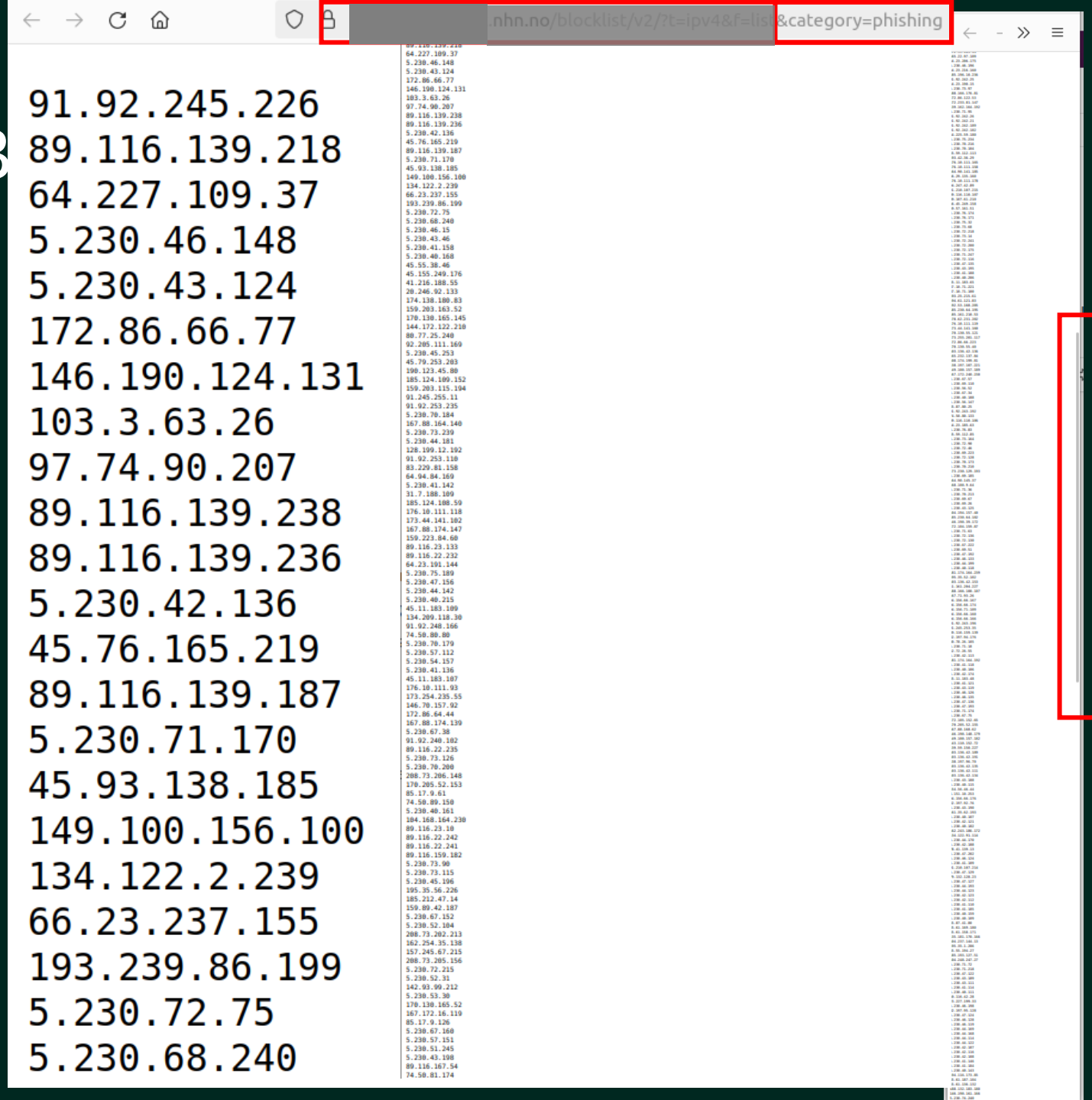
Norsk helsenett



Norsk helsenett

Oppdag kjente angrep





- 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

```powershell
$NBPuser = "Virksomhet" # Brukernavn for NBP

$smtpserver = "X.X.X.X" # IP til SMTP server
$smtpto = "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"


# Variablar 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: Variablar 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