



NTNU

Kunnskap for en bedre verden

DEPARTMENT OF INFORMATION SECURITY AND
COMMUNICATION TECHNOLOGY

INFT2504 SKYTJENESTER SOM ARBEIDSFLATE (2024 HØST)

Oblig 03

Author:

Nga Van Phung (10087)

Date: 22. November 2024

Table of Contents

List of Figures	i
List of Tables	i
1 Innledning	1
2 Beskrivelse, Tekniske Spesifikasjoner og Implementeringsdetaljer	1
2.1 Tilgangskontroll og sikkerhet	1
2.1.1 Tilgangskontroll basert på geolokasjon, tidspunkt og enhetsstatus	1
2.1.2 Sikkerhetsnivåer for ulike brukergrupper og datatyper	1
2.1.3 Sikkerhet for eksterne konsulenter og gjester	2
2.2 Mobile enheter og applikasjoner	2
2.2.1 Standardisering av operativsystemer og versjoner	2
2.2.2 Definering av godkjente applikasjoner	2
2.2.3 Isolering av bedriftsdata på mobile enheter	3
2.2.4 Sikring av sensitive data	3
2.3 Håndtering av skygge-IT (kun teori)	3
2.3.1 Kartlegging av omfanget av skygge-IT	4
2.3.2 Implementering av kontrolltiltak for å begrense bruken av ikke-godkjente tjenester	4
2.3.3 Godkjente alternativer som møter de ansattes behov	4
2.3.4 Etablering av rutiner for å oppdage og håndtere nye skygge-IT-tjenester . .	5
3 Risikovurdering og begrunnelser for valgte tiltak	5
4 Konklusjon	5
References	6

List of Figures

1 Risikovurdering og begrunnelser for valgte tiltak	5
---	---

List of Tables

1 Innledning

NyTech AS står overfor flere sikkerhetsutfordringer etter implementeringen av Microsoft 365. Blant disse utfordringene finner jeg kompleks tilgangskontroll for en mobil arbeidsstyrke, sikring av data på mobile enheter, og håndtering av såkalt “shadow-IT” hvor ansatte bruker uautoriserteapper og tjenester. Denne rapporten presenterer en sikkerhetsstrategi som adresserer disse problemstillingene ved å utnytte Microsoft 365 sine verktøy som Microsoft Endpoint Manager, Conditional Access, Microsoft Cloud App Security (MCAS), og Data Loss Prevention (DLP). Målet er å skape en balansert løsning som både ivaretar sikkerheten og tilrettelegger for en fleksibel arbeidsplass.

2 Beskrivelse, Tekniske Spesifikasjoner og Implementerings-detaljer

2.1 Tilgangskontroll og sikkerhet

2.1.1 Tilgangskontroll basert på geolokasjon, tidspunkt og enhetsstatus

a). Tiltak:

Jeg brukte betinget tilgang (Conditional Access) i Microsoft Azure AD til å sette regler basert på:

- Geografisk tilgangskontroll: Jeg antar at selskapet er nyetablert i Norge og ikke har noen kontorer i andre land, så jeg tillater kun innlogging i Norge. Jeg kan også blokkere et spesifikt land i Sør-Amerika, for eksempel Chile.

- Tidspunktbasert kontroll: jeg vil implementere policyer som begrenser pålogging utenom arbeidstiden, spesielt for utviklere med tilgang til sensitive data men dessverre finner jeg **ikke** hvor jeg kan implementere den.

- Enhetsstatus: jeg har konfigurert policyer som kun tillater tilgang fra kompatible, registrerte enheter som oppfyller kravene til sikkerhet og oppdateringer.

b). Implementering:

Jeg har opprettet policyer i Azure AD Conditional Access som definerer spesifikke krav til geografisk tilgang, tidspunkt, og enhetsstatus. (**Se vedlegg 2.1.1**)

Jeg tror at vi kan kombinere med Microsoft Endpoint Manager for å sikre at enhetene overholder kravene til oppdateringer, kryptering, og sikkerhetsinnstillinger.

Testing: (Se vedlegg 2.1.1)

c). Måling av effekt:

Overvåk påloggingsforsøk i Azure AD for å analysere mislykkede pålogginger fra blokkerte regioner og tidspunkter.

Gjennomgå rapporter om enhetsstatus i Microsoft Endpoint Manager for å sikre compliance.

2.1.2 Sikkerhetsnivåer for ulike brukergrupper og datatyper

a). Tiltak:

Forhindre deling av sensitive data via personlige e-postkontører eller skyløsninger, brukte jeg Data Loss Prevention (DLP).

Jeg har brukt MAM-policyer (Mobile Application Management) for å beskytte bedriftsdata på mobile enheter uten full administrasjon over enheten (spesielt viktig i BYOD-scenarioer).

b). Implementering:

Jeg settet opp DLP-regler og sensitivitetsetiketter i Microsoft 365 Security og Compliance Center. (**Se vedlegg 2.1.2**)

Jeg har brukt app-beskyttelsespolicyer i Endpoint Manager for å sikre bedriftsdata på BYOD-enheter. (**Se vedlegg 2.1.2**)

Testing: (Se vedlegg 2.1.2)

c). Måling av effekt:

Spor hendelser der DLP-regler utløses for å identifisere forsøk på uautorisert deling.

Overvåk etterlevelsen av app-beskyttelsespolicyer på mobile enheter.

2.1.3 Sikkerhet for eksterne konsulenter og gjester

a). Tiltak:

- Jeg vil aktivere Multi-Factor Authentication (MFA) for alle eksterne brukere, inkludert gjester.
- Jeg bruker Conditional Access for å begrense tilgang til sensitive prosjekter og data basert på enhetsstatus og geolokasjon.
- Jeg vil også konfigurere egne Teams-kanaler for eksterne som gir begrenset tilgang.

b). Implementering:

Jeg har aktiver MFA i Azure AD for gjester og eksterne konsulenter. (**Se vedlegg 2.1.3**)
Jeg opprettet Conditional Access-policyer for gjestebrukere og eksterne for å sikre at de oppfyller kravene til kompatible enheter. (**Se vedlegg 2.1.3**)

Testing: Jeg hoppet over denne testingen fordi alle må ha MFA for å logge inn (Authenticator app)

c). Måling av effekt:

Gjennomgå MFA-bruksrapporter for eksterne brukere for å sikre compliance.
Bruk rapporter fra Teams og SharePoint for å overvåke delingsaktivitet.

2.2 Mobile enheter og applikasjoner

2.2.1 Standardisering av operativsystemer og versjoner

a). Tiltak:

Jeg har brukt Endpoint Manager til å definere krav til operativsystemversjoner som støttes (jeg antar at de bruker kun iOS/iPadOS men selvfølgelig kan det være flere forskjellige f.eks Android). På denne måten kan IT-avdelingen sikre at alle enheter oppfyller minimumskravene til sikkerhet og ytelse.

Sett opp krav til både iOS- og Android-versjoner og konfigurer policyer for å blokkere enheter med utdatert eller usikker programvare.

b). Implementering:

I Endpoint Manager, konfigurerer compliance policyer for å spesifisere akseptable operativsystemversjoner for iOS. (**Se vedlegg 2.2.1**)

Vi kan også sette varsler for ikke-kompatible enheter som trenger oppdatering.

c). Måling av effekt:

Overvåk compliance-status i Endpoint Manager for å sikre at alle mobile enheter oppfyller standardkravene.

Analyser rapporter om blokkerte enheter og eventuelle sikkerhetshendelser relatert til utdatert programvare.

2.2.2 Definering av godkjente applikasjoner

a). Tiltak:

Jeg må først og frem definere en liste over godkjente apper App-beskyttelsespolicyer (MAM) i Microsoft Endpoint Manager for e-post, dokumenthåndtering og samarbeid (f.eks., Outlook for e-post, OneDrive for dokumenthåndtering, og Teams for samarbeid).

Vi bør blokkes bruk av ikke-godkjente apper som lagrer data lokalt eller mangler nødvendige sikkerhetsfunksjoner.

b). Implementering:

Jeg har bruk MAM-policyer i Endpoint Manager til å begrense tilgang til bedriftsdata kun gjenom godkjente applikasjoner. (**Se vedlegg 2.2.2**)

Vi må huske å konfigurere Conditional Access-policyer for å sikre at brukere kun får tilgang til bedriftsressurser via disse applikasjonene.

c). Måling av effekt:

Overvåk rapporter om app-bruk for å sikre at ansatte kun bruker godkjente apper til å få tilgang til bedriftsdata.

Gjennomgå bruksstatistikk for godkjente apper i Endpoint Manager for å evaluere etterlevelse.

2.2.3 Isolering av bedriftsdata på mobile enheter

a). Tiltak:

Microsoft Intune MAM uten MDM (Mobile Application Management): Implementer MAM-policyer for å isolere bedriftsdata på enheter uten å måtte administrere hele enheten. Dette er nyttig i BYOD-situasjoner.

Aktiver funksjoner som forhindrer dataoverføring fra bedriftsapper til personlige apper, og krypter bedriftsdata på enheten.

b). Implementering:

I Endpoint Manager, har jeg opprettet app-beskyttelsespolicyer som skiller bedriftsdata fra personlig data og aktivert kryptering for bedriftsdata og forhindrer kopiering og liming mellom bedrifts- og personlige apper.(Se vedlegg 2.2.3)

For som bruker private enheter, begrens deling av bedriftsdata utenfor godkjente apper.

c). Måling av effekt:

Spor hendelser der app-beskyttelsespolicyer utløses, som forsøk på å overføre data til personlige apper.

Analyser sikkerhetsloggene i Endpoint Manager for å sikre at bedriftsdata er beskyttet på mobile enheter.

2.2.4 Sikring av sensitive data

a). Tiltak:

Jeg brukte Conditional Access med App Enforced Restrictions for å sikre at sensitive data kun kan åpnes i godkjente applikasjoner og implementert restriksjoner som sikrer at filer kun kan åpnes og redigeres i godkjente apper som Outlook, Teams, og SharePoint.

Jeg har også satt opp DLP-regler for å hindre at sensitiv informasjon kan lastes opp til personlige skylagringstjenester.

b). Implementering:

Jeg brukte Conditional Access-policyer for å håndheve at spesifikke apper er nødvendige for å få tilgang til bedriftsressurser.(Se vedlegg 2.2.4)

Og DLP-policyer i Microsoft 365 Compliance Center for å hindre at ansatte kan dele sensitive filer gjennom ikke-godkjente applikasjoner. (Se vedlegg 2.2.4)

c). Måling av effekt:

Overvåk hendelser der DLP-policyer blokkerer deling av sensitive data via ikke-godkjente kanaler. Gjennomgå Conditional Access-rapporter for å sikre at kun godkjente applikasjoner brukes til tilgang til sensitive data.

2.3 Håndtering av skygge-IT (kun teori)

For å sikre seg mot utilsiktet Shadow IT kan organisasjoner implementere flere tekniske kontrolltiltak som:

- **Single Sign-On (SSO):** Løsninger som Okta eller EntraID kan fungere som et sentralt kontrollpunkt for all applikasjonstilgang.
- **Data Loss Prevention (DLP):** Systemer kan konfigureres til å overvåke og kontrollere dataoverføringer til eksterne tjenester.
- **DNS-filtrering og web gateway-løsninger:** DNS-filtrering og verktøy som Cisco Umbrella kan blokkere tilgang til kjente risikable tjenester og applikasjoner.

-
- **API-sikkerhetsverktøy:** API-sikkerhetsverktøy kan overvåke og kontrollere integrasjoner mellom applikasjoner.

2.3.1 Kartlegging av omfanget av skygge-IT

a). Tiltak:

Jeg vil bruke Microsoft Cloud App Security (MCAS) til å identifisere og analysere alle skyløsninger og apper som ansatte bruker uten godkjenning.

I tillegg vil jeg også konfigurere MCAS til å oppdage bruk av ikke-godkjente tjenester som Dropbox, WhatsApp, Gmail, og gratisversjoner av design- og kodeverktøy.

b). Implementering:

Vi bør aktivere Cloud Discovery i MCAS for å kartlegge all skyaktivitet og identifisere apper basert på bruksmønstre.

Og opprette et policy-rammeverk i MCAS for å varsle om bruk av uautoriserte apper og tjenester.

c). Måling av effekt:

Overvåk rapportene fra MCAS for å se hvilke uautoriserte apper som brukes, antall brukere, og hyppigheten av bruken.

Analyser månedlige rapporter for å identifisere trender og gjøre nødvendige justeringer.

2.3.2 Implementering av kontrolltiltak for å begrense bruken av ikke-godkjente tjenester

a). Tiltak:

Jeg vil bruke Conditional Access i Azure AD for å begrense tilgangen til bedriftsressurser når ikke-godkjente tjenester som personlige Dropbox eller Gmail benyttes.

Jeg vil også implementere DLP-regler for å hindre deling av sensitive data til uautoriserte tjenester og apper.

b). Implementering:

Vi bør opprette Conditional Access-policyer for å hindre brukere fra å laste opp data til uautoriserte tjenester ved å bruke spesifikke IP- og app-baserte regler.

I Microsoft 365 Compliance Center, kan vi opprette DLP-policyer som identifiserer og blokkerer deling av sensitive data til ikke-godkjente e-postadresser og skylagringstjenester.

c). Måling av effekt:

Spor hendelser der Conditional Access blokkerer tilgang fra ikke-godkjente tjenester.

Overvåk rapporter om DLP-hendelser som viser forsøk på deling av sensitive data til uautoriserte kanaler.

2.3.3 Godkjente alternativer som møter de ansattes behov

a). Tiltak:

Jeg anbefaler å buke OneDrive som et sikkert alternativ for fil-lagring og -deling, og Teams som det foretrukne samarbeidsverktøyet for kodeversjonering og prosjekter.

Bedriften bør også tilby Microsofts 365 apper design- og redigeringsverktøy som godkjente alternativer for markedsføringsavdelingen, inkludert PowerPoint, Publisher og tilgjengelige apper i Power Platform.

b). Implementering:

Vi kan opprette en bedriftsomfattende policy for bruk av OneDrive og Teams, og tilgjengeliggjør apper gjennom Microsoft 365 Company Portal.

Jeg tror at bedriften bør tilby opplæring og onboarding for brukere som trenger tilgang til disse verktøyene og veilede dem i sikkerhetsfordelene ved de godkjente alternativene.

c). Måling av effekt:

Overvåk bruken av OneDrive og Teams gjennom rapportene i Microsoft 365 Admin Center for å se om ansatte bytter til de godkjente løsningene.

Mål adopsjon av Microsoft 365-designverktøy ved å analysere bruksstatistikk i markedsføringsavdelingen.

2.3.4 Etablering av rutiner for å oppdage og håndtere nye skygge-IT-tjenester

a). Tiltak:

Jeg vil konfigurere MCAS for kontinuerlig overvåking og varsling om nye tjenester og apper som ikke er godkjent, og bruk AI-funksjoner for å oppdage nye mønstre av skygge-IT.

I tillegg planlegger jeg kvartalsvise gjennomganger av skygge-IT-rapporter og hold regelmessige møter med teamene for å diskutere IT-behov.

b). Implementering:

Jeg vil sette opp automatiserte arbeidsflyter i MCAS for å sende varsler til IT-administrasjon ved oppdagelse av nye ikke-godkjente apper.

Og også implementerer en gjennomgangsprosess hvor IT-avdelingen vurderer sikkerhetsrisikoen ved eventuelle nye apper som ansatte ønsker å bruke.

c). Måling av effekt:

Analyser MCAS-rapporter for å se frekvensen av nye skygge-IT-applikasjoner og deres brukere.

Evaluer resultatene fra de kvartalsvise gjennomgangene og dokumenter nødvendige endringer i godkjente apper og policyer.

3 Risikovurdering og begrunnelser for valgte tiltak

Område	Risiko	Tiltak	Begrunnelse
Tilgangskontroll og sikkerhet	<ul style="list-style-type: none">- Uautoriserte pålogginger fra ukjente lokasjoner og kompromitterte enheter.- Manglende differensiering i sikkerhet for ulike brukergrupper.- Gjestebrukere uten MFA.	<ul style="list-style-type: none">- Bruk Conditional Access for tilgang basert på geolokasjon, tidspunkt, og enhetsstatus.- Implementer MFA for eksterne brukere og gjester.	<ul style="list-style-type: none">- Conditional Access sikrer at kun autoriserte brukere og enheter får tilgang.- MFA hindrer uautorisert tilgang selv om påloggingsinformasjon er kompromittert.
Mobil sikkerhet og applikasjonsadministrasjon	<ul style="list-style-type: none">- Usikre private enheter kan eksponere bedriftsdata.- Bedriftsdata kan kopieres til personlige apper.- Fragmentert appbruk skaper ineffektivitet.	<ul style="list-style-type: none">- Standardiser støttede OS-versjoner gjennom Endpoint Manager.- Bruk app-beskyttelsespolicyer for å sikre bedriftsdata.- Sett opp godkjente apper.	<ul style="list-style-type: none">- Standardisering sikrer at kun kompatible enheter får tilgang.- App-beskyttelsespolicyer beskytter data uten å påvirke personlige apper.- Effektiviserer IT-drift.
Håndtering av skygge-IT	<ul style="list-style-type: none">- Uautoriserte skylagringstjenester kan føre til datalekkasje.- Gratisverktøy uten sikkerhetsgaranti eksponerer bedriftsdata.- Kundesupport bruker WhatsApp.	<ul style="list-style-type: none">- Overvåk bruk av uautoriserte tjenester med MCAS.- Bruk DLP-policyer for å begrense deling av sensitiv data.- Tilby godkjente alternativer som Teams.	<ul style="list-style-type: none">- MCAS gir innsikt i bruksmønstre og blokkerer uautoriserte apper.- DLP hindrer deling av sensitiv data.- Teams og OneDrive tilfredsstiller ansattes behov sikkert.

Figure 1: Risikovurdering og begrunnelser for valgte tiltak

4 Konklusjon

Strategien som er foreslått for NyTech AS, kombinerer betinget tilgang, mobil sikkerhet, og shadow-IT-håndtering. Forventede resultater inkluderer forbedret databeskyttelse, høyere compliance, og redusert risiko for sikkerhetsbrudd. Gjennom implementering av Microsoft 365-verktøy tenker jeg at bedriften kan opprettholde en sikker og fleksibel arbeidsplass som også møter de ansatte sitt behov for effektivitet. Testing og evaluering gjennom rapporter og varsler vil sikre at tiltakene fungerer som forventet og kan tilpasses etter behov.

References

- [1] Microsoft, “Conditional Access Overview,” *Microsoft Learn*, 2024. Available: <https://learn.microsoft.com/en-us/entra/identity/conditional-access/overview>. Accessed: Nov. 22, 2024.
- [2] Microsoft, “Create app-based Conditional Access policies in Intune,” *Microsoft Learn*, 2024. Available: <https://learn.microsoft.com/en-us/mem/intune/protect/app-based-conditional-access-intune-create>. Accessed: Nov. 22, 2024.
- [3] Microsoft, “App protection policies in Microsoft Intune,” *Microsoft Learn*, 2024. Available: <https://learn.microsoft.com/en-us/mem/intune/apps/app-protection-policies>. Accessed: Nov. 22, 2024.
- [4] Microsoft, “Control access from unmanaged devices in SharePoint and OneDrive,” *Microsoft Learn*, 2024. Available: <https://learn.microsoft.com/en-us/sharepoint/control-access-from-unmanaged-devices>. Accessed: Nov. 22, 2024.

Fra fagets pensum:

- Uke 45: 10-ssa-CA-Template.pdf, 10-ssa-shadow-IT.pdf
- Uke 46: 11-ssa-EndpointProtection-v2.pdf

Filene fra Blackboard of INFT2504 Skytjenester som arbeidsflate (2024 HØST):

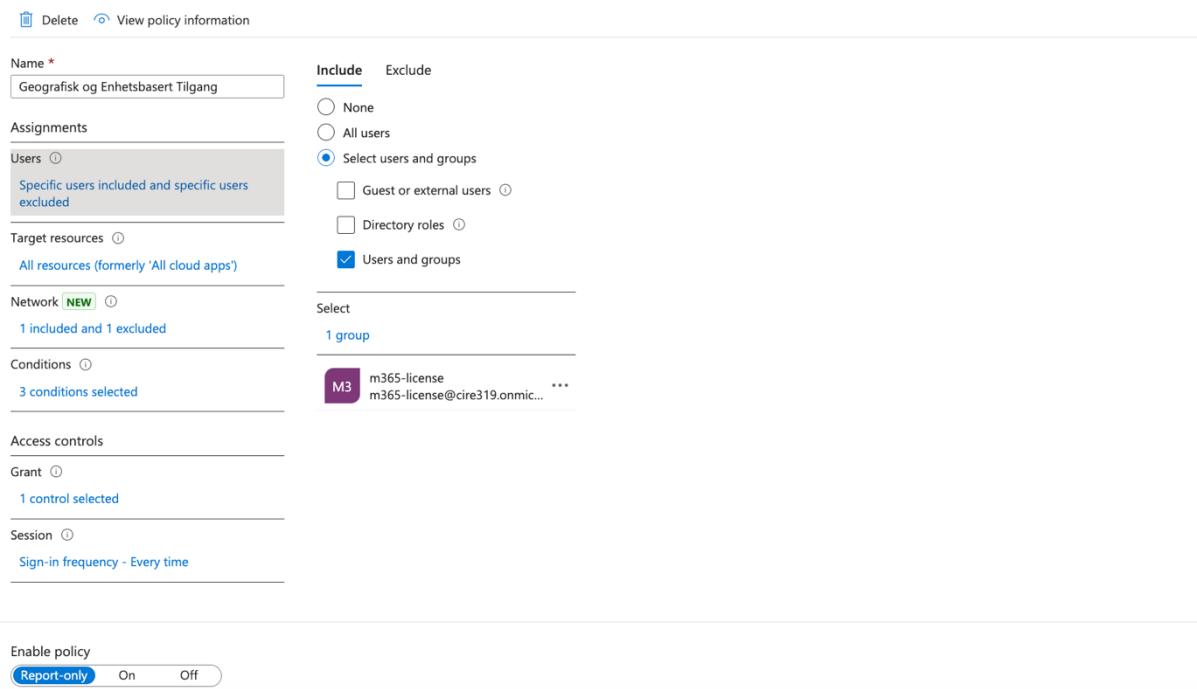
- Uke 45: 10-ssa-CA-Template.pdf

2.1.1

Her kan jeg velge kun for utvikling avdeling men jeg har bestemt meg å bruke den for alle brukere i m365-lisense gruppe:

Geografisk og Enhetsbasert Tilgang ...

Conditional Access policy



Name *
Geografisk og Enhetsbasert Tilgang

Assignments

Users ⓘ Specific users included and specific users excluded

Target resources ⓘ All resources (formerly 'All cloud apps')

Network NEW ⓘ 1 included and 1 excluded

Conditions ⓘ 3 conditions selected

Access controls

Grant ⓘ 1 control selected

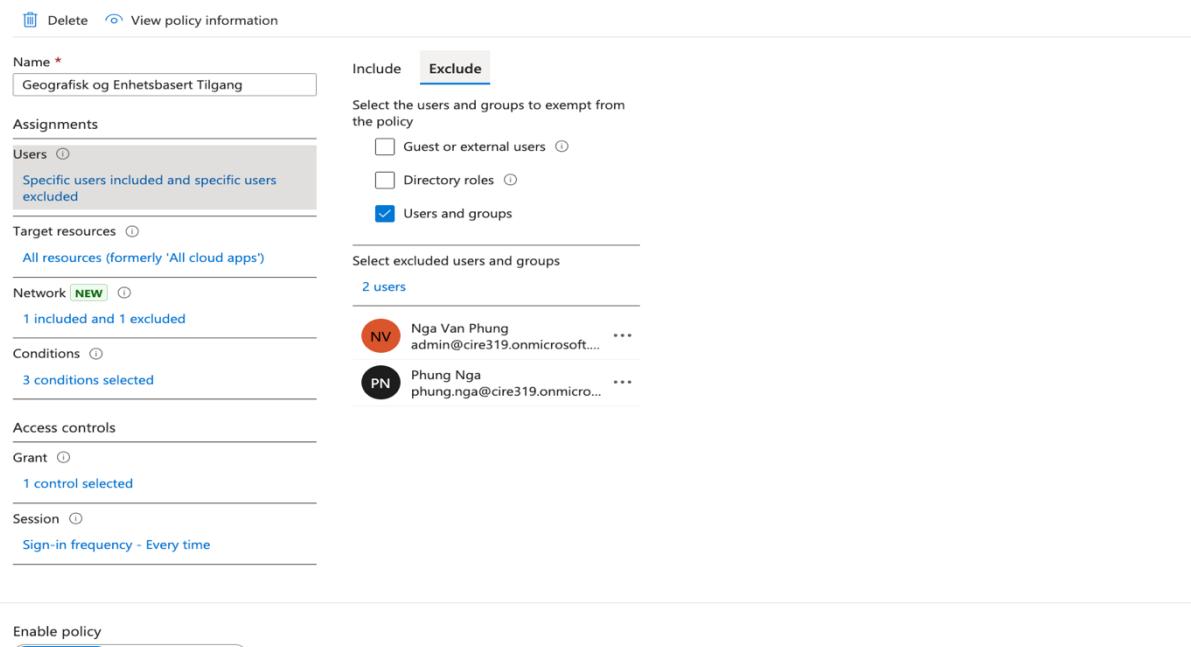
Session ⓘ Sign-in frequency - Every time

Enable policy Report-only On Off

Jeg har også opprettet en egen Global Administrator-bruker som ekskluderes fra Conditional Access-testing for å unngå å låse IT-avdelingen ute og sikre meg selv «admin» som også ekskluderes:

Geografisk og Enhetsbasert Tilgang ...

Conditional Access policy



Name *
Geografisk og Enhetsbasert Tilgang

Assignments

Users ⓘ Specific users included and specific users excluded

Target resources ⓘ All resources (formerly 'All cloud apps')

Network NEW ⓘ 1 included and 1 excluded

Conditions ⓘ 3 conditions selected

Access controls

Grant ⓘ 1 control selected

Session ⓘ Sign-in frequency - Every time

Enable policy Report-only On Off

For alle cloud apper:

Geografisk og Enhetsbasert Tilgang

Conditional Access policy

[Delete](#) [View policy information](#)

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

Assignments

Users [\(1\)](#)
[Specific users included and specific users excluded](#)

Target resources [\(1\)](#)
[All resources \(formerly 'All cloud apps'\)](#)

Network [\[NEW\]](#) [\(1\)](#)
[1 included and 1 excluded](#)

Conditions [\(1\)](#)
[3 conditions selected](#)

Access controls

Grant [\(1\)](#)
[1 control selected](#)

Enable policy
[Report-only](#) [On](#) [Off](#)

Control access based on all or specific apps, internet resources, actions, or authentication context. [Learn more](#)

Select what this policy applies to
[Resources \(formerly cloud apps\)](#)

[Include](#) [Exclude](#)

None
 All internet resources with Global Secure Access
 All resources (formerly 'All cloud apps')
 Select resources

⚠ Don't lock yourself out! This policy impacts the Azure portal. Before you continue, ensure that you or someone else will be able to get back into the portal.
Disregard this warning if you are configuring persistent browser session policy that works correctly only if "All resources" are selected. [Learn more](#)

ℹ To create a Conditional Access policy targeting members in your tenant with Global Secure Access (GSA) as a resource, make sure GSA is deployed in

Jeg har valgt kun Norge som land kan få tilgang:

Geografisk og Enhetsbasert Tilgang

Conditional Access policy

[Delete](#) [View policy information](#)

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

Assignments

Users [\(1\)](#)
[Specific users included and specific users excluded](#)

Target resources [\(1\)](#)
[All resources \(formerly 'All cloud apps'\)](#)

Network [\[NEW\]](#) [\(1\)](#)
[1 included and 1 excluded](#)

Conditions [\(1\)](#)
[3 conditions selected](#)

Access controls

Grant [\(1\)](#)
[1 control selected](#)

Enable policy
[Report-only](#) [On](#) [Off](#)

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

Configure [\(1\)](#)
[Yes](#) [No](#)

[Include](#) [Exclude](#)

Any network or location
 All trusted networks and locations
 All Compliant Network locations
 Selected networks and locations

Select
[Norway](#) [...](#)

ℹ To create a Conditional Access policy ensuring your tenant's members are coming from their compliant network, make sure Global Secure Access (GSA) is deployed and Adaptive Access Signaling in GSA is enabled in your tenant. Learn more on how to [enable GSA Adaptive Access Signaling](#).

Og ekskluderes Chile (eller jeg kan også opprette en separat policy for den men det har jeg ikke gjort):

Geografisk og Enhetsbasert Tilgang

Conditional Access policy

Delete View policy information

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.
[Learn more](#)

Name *

Geografisk og Enhetsbasert Tilgang

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

Configure

Yes No

Include Exclude

Select the locations to exempt from the policy

- All trusted networks and locations
- All Compliant Network locations
- Selected networks and locations

Assignments

Users

Specific users included and specific users excluded

Target resources

All resources (formerly 'All cloud apps')

Network

1 included and 1 excluded

Conditions

3 conditions selected

Access controls

Grant

1 control selected

To create a Conditional Access policy ensuring your tenant's members are coming from their compliant network, make sure Global Secure Access (GSA) is deployed and Adaptive Access Signaling in GSA is enabled in your tenant. Learn more on how to [enable GSA Adaptive Access Signaling](#).

Enable policy

Report-only On Off

Jeg har definert noen kondisjoner for device platform, locations og client apps:

Home > Conditional Access | Overview > Policies >

Geografisk og Enhetsbasert Tilgang

Conditional Access policy

Delete View policy information

Policy to bring signals together, to make decisions, and enforce organizational policies.
[Learn more](#)

Name *

Geografisk og Enhetsbasert Tilgang

like risk, device platform, location, client apps, or device state. [Learn more](#)

Configure

Yes No

Include Exclude

- Any network or location
- All trusted networks and locations
- All Compliant Network locations
- Selected networks and locations

Assignments

Users

Specific users included and specific users excluded

Target resources

All resources (formerly 'All cloud apps')

Network

1 included and 1 excluded

Conditions

3 conditions selected

Access controls

Grant

1 control selected

Session

Sign-in frequency - Every time

To create a Conditional Access policy ensuring your tenant's members are coming from their compliant network, make sure Global Secure Access (GSA) is deployed and Adaptive Access Signaling in GSA is enabled in your tenant. Learn more on how to [enable GSA Adaptive Access Signaling](#).

'Locations' condition is moving!

Enable policy

Report-only On Off

Home > Conditional Access | Overview > Policies >

Geografisk og Enhetsbasert Tilgang

Conditional Access policy

Delete View policy information

device state. [Learn more](#)

decisions, and enforce organizational policies. [Learn more](#)

Name *

Assignments

Users Specific users included and specific users excluded

Target resources All resources (formerly 'All cloud apps')

Network NEW 1 included and 1 excluded

Conditions 3 conditions selected

Access controls

Grant 1 control selected

Session Sign-in frequency - Every time

Enable policy Report-only On Off

Device platforms

Apply policy to selected device platforms. [Learn more](#)

Configure Yes No

Include Exclude

- Any device
- Select device platforms
 - Android
 - iOS
 - Windows Phone
 - Windows
 - macOS
 - Linux

Home > Conditional Access | Overview > Policies >

Geografisk og Enhetsbasert Tilgang

Conditional Access policy

Delete View policy information

policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

Assignments

Users Specific users included and specific users excluded

Target resources All resources (formerly 'All cloud apps')

Network NEW 1 included and 1 excluded

Conditions 3 conditions selected

Access controls

Grant 1 control selected

Session Sign-in frequency - Every time

Enable policy Report-only On Off

Client apps

Control user access to target specific client applications not using modern authentication. [Learn more](#)

Select the client apps this policy will apply to

Modern authentication clients

- Browser
- Mobile apps and desktop clients

Legacy authentication clients

- Exchange ActiveSync clients
- Other clients

Aktiverte MFA under Access Controls > Grant > Require MFA:

Home > Conditional Access | Overview > Policies >

Geografisk og Enhetsbasert Tilgang

Conditional Access policy

Delete View policy information

Name *

Assignments

Users Specific users included and specific users excluded

Target resources All resources (formerly 'All cloud apps')

Network NEW 1 included and 1 excluded

Conditions 3 conditions selected

Access controls

Grant 1 control selected

Session Sign-in frequency - Every time

Enable policy Report-only On Off

Grant

Control access enforcement to block or grant access. [Learn more](#)

Block access Grant access

Require multifactor authentication

Consider testing the new "Require authentication strength". [Learn more](#)

Require authentication strength

"Require authentication strength" cannot be used with "Require multifactor authentication". [Learn more](#)

Require device to be marked as compliant

Require Microsoft Entra hybrid joined device

Require approved client app See list of approved client apps

Require app protection policy See list of policy protected client apps

Select

Vi kan sette policyen til On for testing, eller Report-only for å overvåke effekten før full utrulling:

Policies ...

+ New policy + New policy from template ✎ Upload policy file 🤔 What if ⏪ Refresh | 🌐 Preview features | 🗣 Got feedback?

Microsoft Entra Conditional Access policies are used to apply access controls to keep your organization secure. [Learn more](#)

All policies	Microsoft-managed policies
5	4
Total 5 out of 5 policies found	
<input type="button" value="Search"/> Add filter	
Policy name	Tags
Block legacy authentication	MICROSOFT-MANAGED
Multifactor authentication for Azure Management	MICROSOFT-MANAGED
Multifactor authentication for admins	MICROSOFT-MANAGED
Multifactor authentication for all users	MICROSOFT-MANAGED
Geografisk og Enhetsbasert Tilgang	Report-only
	Creation date
	Modified date
	11/23/2024, 1:28:05 PM
	11/23/2024, 1:28:08 PM
	11/23/2024, 1:28:04 PM
	11/23/2024, 1:28:06 PM
	11/24/2024, 3:02:38 PM
	11/24/2024, 4:27:50 PM

Kompatibel enhet som jeg har satt opp for eksampel:

The screenshot shows the configuration for a mobile device compliance policy named 'Kompatibel enhet for iOS/iPadOS'. It includes sections for Basics (Name: Kompatibel enhet for iOS/iPadOS, Description: --, Platform: iOS/iPadOS, Profile type: iOS compliance policy), Compliance settings (Edit), Device Properties (Minimum OS version: 14.0.1, Maximum OS version: 18.0.1), and Device Security (Require a password to unlock mobile devices: Required, Simple passwords: Block, Minimum password length: 6, Required password type: At least alphanumeric, Number of non-alphanumeric characters in password: 4, Maximum minutes after screen lock before password is required: 5minutes, Maximum minutes of inactivity until screen locks: 15minutes, Password expiration (days): 90 Days, Number of previous passwords to prevent reuse: 3).

Testing: så lenge du er i Norge, så man helt sikkert får tilgang:

Home > cire1313 > Conditional Access	Conditional Access Sign-in logs	...
Microsoft Entra ID		
Conditional Access Sign-in logs	Download	Export Data Settings
Overview	Request ID	User
Policies	Date	Application
Insights and reporting	↓	User
Diagnose and solve problems	↑	Application
Manage	↓	Status
Named locations	↑	IP address
Custom controls (Preview)	↓	Location
Terms of use	↑	Conditional Access
VPN connectivity	↓	Authentication re...
Authentication contexts	↓	
Authentication strengths	↓	
Classic policies	↓	
Monitoring	↓	
Sign-in logs	↓	
Audit logs	↓	
Troubleshooting + Support	↓	
New support request	↓	
Columns		
Got feedback?		
11/25/2024, 4:32:26 PM	78ecc600d-2bda-49ff-...	Nga Van Phung
11/25/2024, 4:38:26 PM	96884ee5-fa23-41b2-...	Nga Van Phung
11/25/2024, 4:37:36 PM	c37ee03e-d711-4eb4-...	Nga Van Phung
11/25/2024, 2:58:33 PM	10a260de-e97e-4b6d-...	Nga Van Phung
11/25/2024, 2:58:33 PM	c1cef584-9489-4327-...	Nga Van Phung
11/25/2024, 2:58:33 PM	60daaf3a-23b3-4985-...	Nga Van Phung
11/25/2024, 2:58:29 PM	65bf57cb-f6f0-4c9b-...	Nga Van Phung
11/25/2024, 2:57:04 PM	6deab20-03a2-4a2b-...	Nga Van Phung
11/25/2024, 2:34:32 PM	362de678-3ff5-41b4-...	Nga Van Phung
11/25/2024, 2:34:32 PM	91b4e5b9-6bab-450d...	Nga Van Phung
11/25/2024, 2:34:32 PM	d3fe45eb-db80-4d1f-...	Nga Van Phung
11/25/2024, 2:34:28 PM	5b948236-f34a-414e-...	Nga Van Phung
11/25/2024, 2:34:17 PM	5b948236-f34a-414e-...	Nga Van Phung
11/25/2024, 8:10:39 AM	ad1d4f6-3020-48ca-...	Nga Van Phung
11/25/2024, 5:51:30 AM	a82b02b9-71f7-46f3-...	Nga Van Phung
11/25/2024, 4:48:07 AM	f6cbc9db-6775-442c-...	Nga Van Phung
11/24/2024, 7:41:20 PM	87e10bb8-93fc-4a0f-...	Nga Van Phung
11/24/2024, 7:41:15 PM	5b948236-f34a-414e-...	Nga Van Phung
11/24/2024, 7:41:15 PM	4e06ebb6-e9f1-47fc-...	Nga Van Phung
11/24/2024, 7:41:15 PM	86f7b5f1-825e-4d27-...	Nga Van Phung
11/24/2024, 7:40:07 PM	d6632a46-c7a0-44ec-...	Nga Van Phung

På datamaskinen, fordi jeg ikke bruker VPN, bestemmer den at jeg er i Norge og fortsatt kan bruke det normalt.

Home > Conditional Access

Conditional Access | Sign-in logs

Microsoft Entra ID

Download Export Data Settings Troubleshoot Refresh Columns Got feedback?

Date	Request ID	User	Application	Status	IP address	Location	Conditional Acc...	Authenticat...
11/26/2024, 8:55:21 ...	ccde32b3-67b0-489...	Nga Van Phung	Microsoft Office 365 ...	Failure	89.187.160.77	Tokyo, Tokyo, JP	Not Applied	Single-factor
11/26/2024, 8:49:58 ...	8d496788-831d-40c...	Nga Van Phung	Microsoft Authentica...	Success	149.88.23.205	Singapore, Central Si...	Not Applied	Single-factor
11/26/2024, 8:39:17 ...	459a86e2-926a-481...	Nga Van Phung	Azure Portal	Success	2001:700:300:411a:c...	Trondheim, Sor-Tron...	Success	Multifactor au...
11/26/2024, 8:39:14 ...	837ceebc-89d4-4ba...	Nga Van Phung	Office365 Shell WCS...	Success	2001:700:300:411a:c...	Trondheim, Sor-Tron...	Success	Multifactor au...
11/26/2024, 8:39:14 ...	5b548236-f34a-414e...	Nga Van Phung	Office365 Shell WCS...	Success	2001:700:300:411a:c...	Trondheim, Sor-Tron...	Success	Multifactor au...
11/26/2024, 8:39:13 ...	269e4524-2271-498...	Nga Van Phung	Office365 Shell WCS...	Success	2001:700:300:411a:c...	Trondheim, Sor-Tron...	Success	Multifactor au...
11/26/2024, 8:39:09 ...	be68bb35-45f3-40c9...	Nga Van Phung	Office365 Shell WCS...	Success	2001:700:300:411a:c...	Trondheim, Sor-Tron...	Success	Multifactor au...
11/26/2024, 8:39:09 ...	5b548236-f34a-414e...	Nga Van Phung	Office365 Shell WCS...	Success	2001:700:300:411a:c...	Trondheim, Sor-Tron...	Success	Multifactor au...
11/26/2024, 8:39:09 ...	e716cc69-efda-43da...	Nga Van Phung	Office365 Shell WCS...	Success	2001:700:300:411a:c...	Trondheim, Sor-Tron...	Success	Multifactor au...
11/26/2024, 8:39:04 ...	53278e89-6276-482...	Nga Van Phung	Microsoft Office 365 ...	Success	2001:700:300:411a:c...	Trondheim, Sor-Tron...	Success	Multifactor au...
11/26/2024, 8:36:56 ...	5a939f4c-52bc-4d7d...	Nga Van Phung	Microsoft Authentica...	Success	149.88.23.205	Singapore, Central Si...	Not Applied	Single-factor
11/26/2024, 8:36:55 ...	0b0d4bd7-b654-473...	Nga Van Phung	Outlook Mobile	Success	149.88.23.205	Singapore, Central Si...	Success	Multifactor au...
11/26/2024, 8:36:36 ...	84921891-dffa-445...	Nga Van Phung	Microsoft Authentica...	Success	149.88.23.205	Singapore, Central Si...	Not Applied	Single-factor
11/26/2024, 8:34:32 ...	a7d07150-9ed1-47a...	Nga Van Phung	Azure Portal	Success	2001:700:300:411a:c...	Trondheim, Sor-Tron...	Success	Multifactor au...
11/25/2024, 9:12:30 ...	de57ed6-d247-45a...	Nga Van Phung	Azure Portal	Success	188.124.133.152	Bergen Kommune, H...	Success	Multifactor au...
11/25/2024, 6:20:30 ...	55f793cc-a5a2-4fd7...	Nga Van Phung	Office365 Shell WCS...	Success	2001:700:300:411a:c...	Trondheim, Sor-Tron...	Success	Multifactor au...
11/25/2024, 6:20:30 ...	f151cd4d-eae0-4d47...	Nga Van Phung	Office365 Shell WCS...	Success	2001:700:300:411a:c...	Trondheim, Sor-Tron...	Success	Multifactor au...

Jeg opprettet en ny CA for å blokkere tilgang fra Asia, spesielt Singapore og Japan (fordi VPN-en på telefonen min bruker gratisversjonen og den ikke har søramerikanske land).

Conditional Access | Policies

Microsoft Entra ID

New policy New policy from template Upload policy file What if Refresh Preview features Got feedback?

Microsoft Entra Conditional Access policies are used to apply access controls to keep your organization secure. [Learn more](#)

All policies	Microsoft-managed policies				
8	4				
Total	out of 8				
Search Add filter					
8 out of 8 policies found					
Policy name	Tags	State	Alert	Creation date	Modified date
Block legacy authentication	MICROSOFT-MANAGED	On		11/23/2024, 1:28:05 PM	
Multifactor authentication for Azure Management	MICROSOFT-MANAGED	On		11/23/2024, 1:28:08 PM	
Multifactor authentication for admins	MICROSOFT-MANAGED	On		11/23/2024, 1:28:04 PM	
Multifactor authentication for all users	MICROSOFT-MANAGED	On		11/23/2024, 1:28:06 PM	
Blokkere tilgang fra Asia land		On		11/26/2024, 8:47:53 AM	11/26/2024, 9:14:40
Geografisk og Enhetsbasert Tilgang		Report-only		11/24/2024, 3:02:38 PM	11/24/2024, 4:27:50
Kun spesifikke apper		Report-only		11/25/2024, 6:25:14 PM	
MFA for gjester og eksterne		Report-only		11/25/2024, 1:43:12 PM	

Der, når jeg endrer VPN til Singapore eller Japan på telefonen min, mister jeg umiddelbart tilgangen til m365.

Home > Conditional Access

Conditional Access | Sign-in logs

Microsoft Entra ID

Download Export Data Settings Troubleshoot Refresh Columns Got feedback?

Date : Last 24 hours Show dates as : Local Add filters

User sign-ins (interactive) User sign-ins (non-interactive) Service principal sign-ins Managed identity sign-ins

Date	Request ID	User	Application	Status	IP address	Location	Conditional Acc...	Authenticat...
11/26/2024, 9:13:57 ...	300886ff-e778-4437...	Bente Gundersen	Outlook Mobile	Failure	149.88.23.208	Singapore, Central Si...	Failure	Multifactor au...
11/26/2024, 9:13:52 ...	459a86e2-926a-481...	Bente Gundersen	Microsoft Authentica...	Success	149.88.23.208	Singapore, Central Si...	Not Applied	Single-factor
11/26/2024, 9:12:47 ...	274bf0f1-a5a9-419c...	Bente Gundersen	Outlook Mobile	Failure	149.88.23.208	Singapore, Central Si...	Failure	Multifactor au...
11/26/2024, 9:12:43 ...	b31c1423-df95-4202...	Bente Gundersen	Microsoft Authentica...	Success	149.88.23.208	Singapore, Central Si...	Not Applied	Single-factor
11/26/2024, 9:11:35 ...	a82b02b9-7f17-46f3...	Bente Gundersen	Outlook Mobile	Failure	149.88.23.208	Singapore, Central Si...	Failure	Multifactor au...
11/26/2024, 9:11:29 ...	77e1cd82-4c71-443...	Bente Gundersen	Microsoft Authentica...	Success	149.88.23.208	Singapore, Central Si...	Not Applied	Single-factor

09:13 Outlook

Avbryt

Microsoft

bente.gundersen@cire319.onmicrosoft.com

Du har ikke tilgang til dette akkurat nå

Du ble pålogget, men du oppfyller ikke kriteriene for å få tilgang til denne ressursen. Det kan for eksempel hende du logger deg på fra en nettleser, app eller et sted som administratoren din har begrenset.

[Flere detaljer](#)

09:17 Home Enable Dark mode



You don't have permission to access this page

Access has been blocked by Conditional Access policies. The access policy does not allow token issuance. If this is unexpected please contact your administrator.

[Return to home](#) [Log out](#)

09:17



Det oppstod et problem.

[Prøv på nytt](#)

Hvis det ikke fungerer, prøv [å logge av](#) og logg inn igjen.

2.1.2

Jeg har implementert av DLP-regler i Microsoft 365 Security & Compliance Center:

The screenshot shows the Microsoft Purview Data Loss Prevention Policies page. On the left, there's a sidebar with 'Data Loss Prevention' selected under 'Solutions'. The main area is titled 'Policies' and contains a table with four rows. The columns are 'Name', 'Priority', 'Last modified', and 'Status'. The policies listed are: PCI Data Security Standard (PCI DSS) (Priority 0, Oct 31, 2024 7:56 PM, Test without notifications); GDPR (Priority 1, Oct 31, 2024 7:58 PM, In simulation without notifications); Norway Financial Data (Priority 2, Nov 24, 2024 7:24 PM, In simulation without notifications); and Norway Access to Medical Reports Act (Priority 3, Nov 24, 2024 7:30 PM, In simulation without notifications).

Jeg har opprettet sensitivitetsetiketter:

The screenshot shows the Microsoft Purview Information Protection Sensitivity labels page. On the left, there's a sidebar with 'Information Protection' selected under 'Solutions'. The main area is titled 'Sensitivity labels' and contains a table with three rows. The columns are 'Name', 'Priority', 'Scope', 'Created by', and 'Last modified'. The sensitivity labels listed are: cire319 AS confidential (Priority 0 - lowest, Files & other data assets, E..., Nga Van Phung, Oct 31, 2024 8:53:19 PM); Intern bruk (Priority 1, Files & other data assets, E..., Nga Van Phung, Oct 31, 2024 8:53:20 PM); and Offentlig (Priority 2 - highest, Files & other data assets, E..., Nga Van Phung, Nov 24, 2024 7:52:56 ...).

Implementering av App-beskyttelsespolyer i Endpoint Manager og jeg har også aktivert alternativer for å blokkere kopiering av data fra bedriftsapper til personlige apper, krev PIN-kode eller biometrisk autentisering for å åpne apper, også flere:

The screenshot shows the Microsoft Intune Admin Center. On the left, there's a sidebar with 'Apps' selected under 'All services'. The main area is titled 'Intune App Protection | Properties' and shows the 'Properties' tab. Under 'Help and support', there's a 'Diagnose and solve problems' section. Under 'Data protection', there's a table with two columns: 'Prevent backups' and 'Send org data to other apps'. The 'Send org data to other apps' row has a 'Default' value of 'skype:app-settings:calshow:itmss:itmss:itmss-apps:itmss-appss:itmss-services:' followed by a list of URLs: http://facetime.apple.com, http://maps.apple.com, https://facetime.apple.com, https://maps.apple.com, http://appsplatform.us/*, and http://onedrive.com/*.

Testing:

Jeg brukte e-post og sender ut sensitiv sikkerhetsinformasjon:

The screenshot shows the Microsoft Outlook interface. On the left, the ribbon navigation bar includes Home, View, Help, and a search bar. Below the ribbon, the left sidebar lists Favorites (Inbox, Sent Items, Drafts), Folders (Inbox, Drafts), and a Sent Items folder containing two messages. The main pane displays the 'Sent Items' folder with a message from 'Bente Gundersen' to 'External Auditor'. The message subject is 'Confidential' and contains sensitive information: 'My personal number: 29109125366 ...' and 'and credit card information: 4112 4633 1923 5444'. The message was sent at 9:48 AM on Tuesday, November 26, 2024.

Da fikk jeg denne:

The screenshot shows a Gmail inbox. The left sidebar includes options like Compose, Starred, Snoozed, Important, Sent, Drafts, and Categories (Social, Updates, Forums, Promotions). The main area shows an incoming message from 'Bente Gundersen <Bente.Gundersen@cire319.onmicrosoft.com> to me' at 9:49AM (3 minutes ago). The message subject is 'Confidential'. A blue button labeled 'Read the message' is visible. Below the message, there is a note about Microsoft Purview Message Encryption.

Bente.Gundersen@cire319.onmicrosoft.com has sent you a protected message



Sign in to view the message



Sign in with a One-time passcode

Need Help?

[Privacy Statement](#)

2.1.3

MFA i Azure AD for gjester og eksterne konsulenter:

Policies ...

+ New policy + New policy from template ⚡ Upload policy file 🤔 What if ⏪ Refresh | 🌐 Preview features | 🗣 Got feedback?

Microsoft Entra Conditional Access policies are used to apply access controls to keep your organization secure. [Learn more](#)

All policies Microsoft-managed policies

5 4 Total out of 5

🔍 Search ⚡ Add filter

5 out of 5 policies found

Policy name	Tags	State	Alert	Creation date	Modified date
Block legacy authentication	MICROSOFT-MANAGED	On		11/23/2024, 1:28:05 PM	
Multifactor authentication for Azure Management	MICROSOFT-MANAGED	On		11/23/2024, 1:28:08 PM	
Multifactor authentication for admins	MICROSOFT-MANAGED	On		11/23/2024, 1:28:04 PM	
Multifactor authentication for all users	MICROSOFT-MANAGED	On		11/23/2024, 1:28:06 PM	

Policies ...

+ New policy + New policy from template ⚡ Upload policy file 🤔 What if ⏪ Refresh | 🌐 Preview features | 🗣 Got feedback?

Microsoft Entra Conditional Access policies are used to apply access controls to keep your organization secure. [Learn more](#)

All policies Microsoft-managed policies

6 4 Total out of 6

🔍 Search ⚡ Add filter

6 out of 6 policies found

Policy name	Tags	State	Alert	Creation date	Modified date
Block legacy authentication	MICROSOFT-MANAGED	On		11/23/2024, 1:28:05 PM	
Multifactor authentication for Azure Management	MICROSOFT-MANAGED	On		11/23/2024, 1:28:08 PM	
Multifactor authentication for admins	MICROSOFT-MANAGED	On		11/23/2024, 1:28:04 PM	
Multifactor authentication for all users	MICROSOFT-MANAGED	On		11/23/2024, 1:28:06 PM	
Geografisk og Enhetsbasert Tilgang		Report-only		11/24/2024, 3:02:38 PM	11/24/2024, 4:27:50 PM
MFA for gjester og eksterne		Report-only		11/25/2024, 1:43:12 PM	

MFA for gjester og eksterne ...

Conditional Access policy

>Delete View policy information

Learn more

Name *

MFA for gjester og eksterne

Include Exclude

None

All users

Select users and groups

Guest or external users

2 selected

Specify external Microsoft Entra organizations

All

Select

Directory roles

Users and groups

Select

1 user

EA External Auditor vannga1129@gmail.com

...

Enable policy

Report-only On Off

Opprett Conditional Access-policyer for gjestebrukere og eksterne for å sikre at de oppfyller kravene til kompatible enheter Conditions > Device state: Velg Require compliant device eller bruker Microsoft Itune for å sette opp.

Policies Overview

Policy name	Platform or OS	Policy type	Last modified	Scope tags
Default compliance policy for Andri	Android device administrator	Android compliance policy	10/28/2024 5:31 PM	Default
Kompatibel enhet for iOS/iPadOS	iOS/iPadOS	iOS compliance policy	11/25/2024 1:31 PM	Default

2.2.1

Compliance polcyer for å spesifisere akseptable operativsystem-versjoner for iOS:

Properties

Basics

Name	Kompatibel enhet for iOS/iPadOS
Description	--
Platform	iOS/iPadOS
Profile type	iOS compliance policy

Compliance settings

Device Properties

Minimum OS version	14.0.1
Maximum OS version	18.0.1

Device Security

Require a password to unlock mobile devices	Required
Simple passwords	Block

Policies Overview

Policy name	Platform or OS	Policy type	Last modified	Scope tags
Default compliance policy for Andri	Android device administrator	Android compliance policy	10/28/2024 5:31 PM	Default
Kompatibel enhet for iOS/iPadOS	iOS/iPadOS	iOS compliance policy	11/25/2024 1:31 PM	Default

2.2.2

App-beskyttelsespolicyer (MAM) i Microsoft Endpoint Manager:

The screenshot shows two views of the Microsoft Intune admin center. The top view is the 'Apps | App protection policies' page, which lists policies by platform (Windows, iOS/iPadOS, macOS, Android) and management type (All app types). One policy is shown: 'App-beskyttelsespolicyer (Outlook, OneDrive and Teams)' with status 'Yes'. The bottom view is the 'Intune App Protection | Properties' page for the same policy, showing details like name, description, platform (iOS/iPadOS), and target apps (all device types, no specific device types, public apps like Microsoft Outlook, Microsoft OneDrive, Microsoft Teams, and no custom apps). It also shows data protection settings like prevent backups (block), send org data to other apps (none), and select apps to exempt (Default: skype;app-settings;calshow;itmss;itmss;apps;itmss;appss;itmss;services).

2.2.3

Isolering av bedriftsdata på mobile enheter (BYOD)

The screenshot shows the 'Apps | App protection policies' page again. A new policy has been added: 'Bedriftsdatabeskyttelse - BYOD' with status 'Yes'. This policy is listed alongside the previous ones for 'App-beskyttelsespolicyer (Outlook, OneDrive and Teams)' and 'Office 365-applikasjoner som sk...'. The table includes columns for Policy, Deployed, Updated, Platform, Management type, and Apps.

Beskyttelsesinnstillinger som jeg har gjort under Data protection:

Data kryptering: aktiverte Encrypt work files for å kryptere bedriftsdata på enheten.
Jeg har satt restrict cut, copy, and paste between apps til: Policy managed apps: Tillat kun kopiering og liming mellom godkjente bedriftsapper.
Aktiverte Require PIN for access for å sikre tilgang til apper.

Deaktiverte Backup org data to iCloud (iOS) eller Backup org data to Android Backup Service (Android). Aktiverte Block screen capture and printing of org data.

The screenshot shows the Microsoft Intune Admin Center interface. The left sidebar includes Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled 'Intune App Protection | Properties' under 'Bedriftsdatasbeskyttelse - BYOD'. It displays various policy settings:

Setting	Action
Save copies of org data	Allow
Allow user to save copies to selected services	No Allow user to save copies to selected services
Transfer telecommunication data to	Any dialer app
Dialer App URL Scheme	No Dialer App URL Scheme
Transfer messaging data to	Any messaging app
Messaging App URL Scheme	No Messaging App URL Scheme
Receive data from other apps	All Apps
Open data into Org documents	Allow
Allow users to open data from selected services	OneDrive for Business SharePoint Camera Photo Library Policy managed apps
Restrict cut, copy, and paste between other apps	0
Cut and copy character limit for any app	Block
Third party keyboards	Require
Encrypt org data	Block
Sync policy managed app data with native apps or add-ins	Block
Printing org data	Block
Restrict web content transfer with other apps	Any app
Unmanaged browser protocol	No Unmanaged browser protocol

2.2.4

Jeg brukte Conditional Access-polyer for å håndheve at spesifikke apper er nødvendige for å få tilgang til bedriftsressurser: (apper som Microsoft Teams, SharePoint Online og Exchange Online)

The screenshot shows the Microsoft Conditional Access Policies page. The left sidebar includes Overview, Policies (selected), 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), and Troubleshooting + Support. The main content area shows 7 policies in total, with 4 Microsoft-managed policies:

Policy name	Tags	State	Alert	Creation date
Block legacy authentication	MICROSOFT-MANAGED	On		11/23/2024, 1:28
Multifactor authentication for Azure Management	MICROSOFT-MANAGED	On		11/23/2024, 1:28
Multifactor authentication for admins	MICROSOFT-MANAGED	On		11/23/2024, 1:28
Multifactor authentication for all users	MICROSOFT-MANAGED	On		11/23/2024, 1:28
Geografisk og Enhetsbasert Tilgang		Report-only		11/24/2024, 3:02
Kun spesifikke apper		Report-only		11/25/2024, 6:25
MFA for gjester og eksterne		Report-only		11/25/2024, 1:45

Jeg har implementert av DLP-regler i Microsoft 365 Security & Compliance Center:

The screenshot shows the Microsoft Purview Data Loss Prevention Policies interface. The left sidebar includes links for Home, Solutions (Data Loss Prevention, Learn, Settings), Information Protection (Classifiers, Explorers), and Related solutions (Information Protection, Insider Risk Management). The main content area is titled 'Policies' and contains a table of existing policies:

Name	Priority	Last modified	Status
PCI Data Security Standard (PCI DSS)	0	Oct 31, 2024 7:56 PM	Test without notifications
GDPR	1	Oct 31, 2024 7:58 PM	In simulation without notifications
Norway Financial Data	2	Nov 24, 2024 7:24 PM	In simulation without notifications
Norway Access to Medical Reports Act	3	Nov 24, 2024 7:30 PM	In simulation without notifications

At the top of the main content area, there is a note: "Use data loss prevention (DLP) policies to help identify and protect your organization's sensitive info. For example you can set up policies to help make sure information in email and docs isn't shared with the wrong people. [Learn more about DLP](#)" and a message about role group permissions: "If your role group permissions are restricted to a specific set of users or groups, you'll only be able to manage policies for those users or groups. [Learn more about role group permissions](#)". A "View role groups" button is also present.

***Jeg har satt opp alle policyene til «Report-only» for testing og overvåke effekten før vi aktiverer policyen fullstendig. Når vi har verifisert at policyen fungerer som forventet, kan vi aktivere den ved og klikk på On og deretter Create for å lagre og starte policyen.