

Conditional Access policies

Valtteri Aho

Vaasa

Vanhempi konsultti, Personal coach ja Microsoft Certified Trainer

Sulava Oy, osa The Digital Neighborhoodia

Yli 15 vuotta kokemusta kouluttajana, järjestelmänvalvojana ja monipuolisena helpdesk/datacenter-asiantuntijana. Ajan saatossa kerääntynyt mittavasti tietoa on-prem Microsoft teknologioista, Microsoftin Azure/M365 sekä Modernista laitehallinnasta SCCM:ää unohtamatta. Yli 5 vuotta Sulavalla keskittyen puhtaasti laitehallinnan modernisointi- ja kehitysprojekteihin sekä tottakai kouluttamiseen.

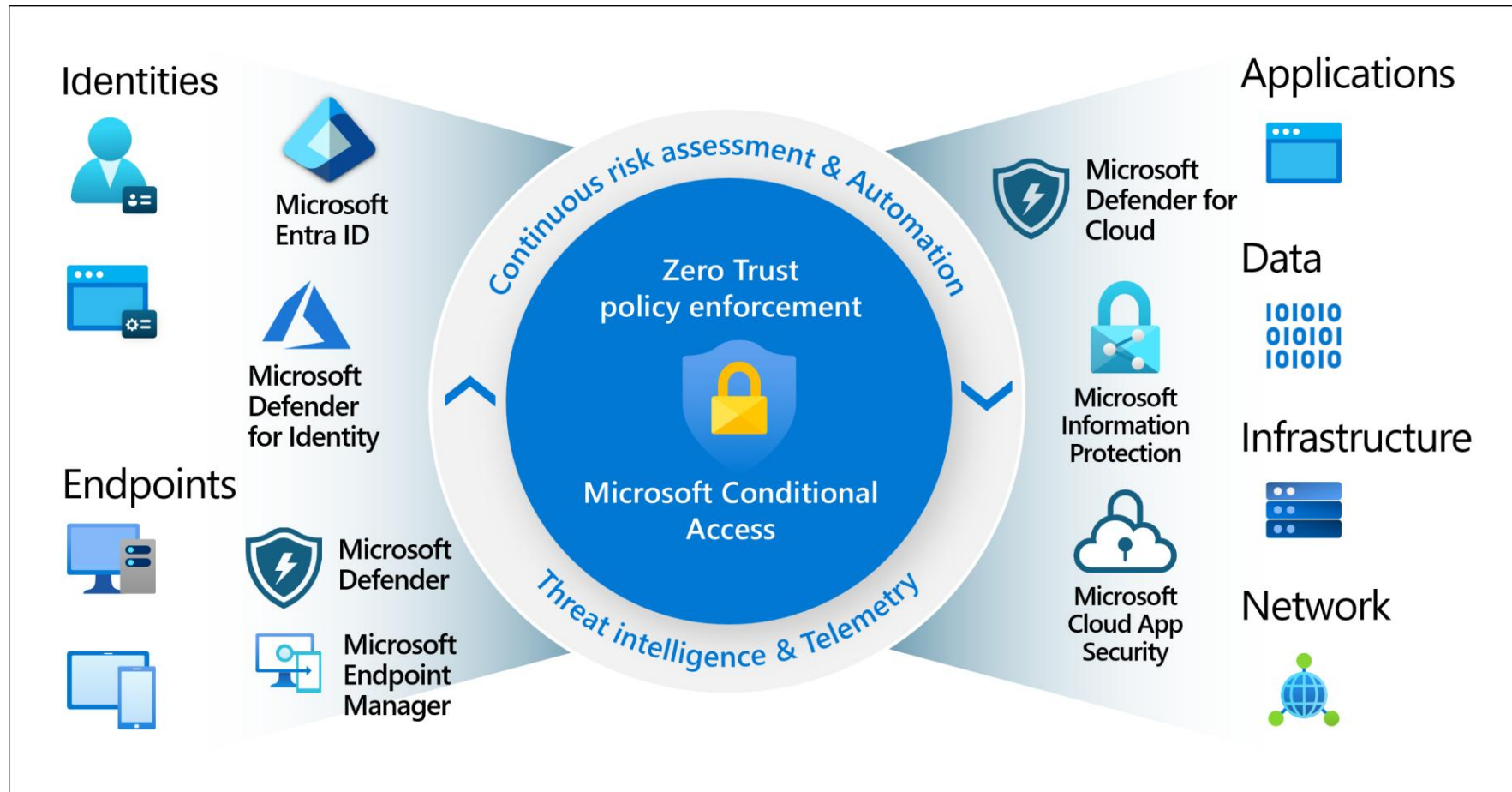
 <https://bsky.app/profile/wallopro.bsky.social>

 <https://www.linkedin.com/in/valtteri-aho/>

 <https://wallo.pro/>




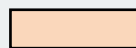




CA-policyt?



CA-policyjen nimeämiskäytäntö

- Vaikka johdonmukaisuus on tärkeää, nimeämiskäytäntöjen tulisi olla tarpeeksi joustavia mukautumaan organisaation muuttuviin tarpeisiin.
- Valitse käytettävä kieli, Englanti suositeltavaa
- Suunnittele CA-policy ryhmittely ja jätä reilusti tilaa
 - Tyypillisesti CA-policyjen määrä on alle 50, mutta myös yli 100 policyn organisaatioita on 😊

Tärkeimmät CA policyjen nimeämisessä käytetyt elementit

-  Käytä aina samaa etuliitettä, esim "CA". Voit käyttää myös "CAG" ja "CAB", Grant ja Block policyille. Etuliitteen jälkeen seuraa juokseva numero
-  Kohdistuksessa oleva pilviresurssi, usein "All" mutta jos useampi niin "selected".
-  Mitä vaaditaan jotta kirjautuminen on sallittua? MFA, Compliant device jne.
-  Kenelle/mille kohdistetaan, usein "All" mutta tässä voi käyttää myös rooleja, esim Admins.
-  Ehdoilla ohjataan policyjä, Alustat, selain, appi, käytetäänkö device filtteriä jne.
-  Viimeisenä kerrotaan policyn versio, jolla kerrotaan missä kehitysversiossa policyjä mennään, esim. V1.0, v1.1 jne. Täysin vapaaehtoinen arvo ja yleensä liittyy CA policyjen jatkokehitykseen.

Prefix:	Cloud resources	Requirements	For Who	When conditions	Version number
---------	-----------------	--------------	---------	-----------------	----------------

Esimerkkejä

CAB001: All non-supported platforms v1.0

CAB002: All for Break Glass Accounts when other than Trusted Locations v1.0

CAG001: All require compliant device for All users when Browser v1.0

CAG002: All require MFA for all users when browser on non-compliant devices v1.0

CAG003: All require compliant device for All users when mobile apps and desktop clients on Windows v1.0

CAG004: M365 and require MFA and App Protection Policy for all users when mobile apps and desktop clients on unmanaged Android and iOS v1.0

CA-policyjen ryhmittely

- CAB001-CAB100: Yleiset blokattavat
- CAG001-CAG010: Admin roolit/portaalit, Break-glass
- CAG011-CAG020: Yleiset, Security info registration, muu
- CAG021-CAG030: Käyttäjät
- CAG031-CAG040: Externals/Guests
- CAG041-CAG050: Partnerit
- CAG051-CAG090: Laitepohjaiset
- CAG091-CAG100: Appipohjaiset

Entra ID – ryhmien nimeämiskäytäntö

- Koska kohdistukset tehdään Entra ID ryhmillä, syytä miettiä ryhmien nimeämiset
- Entra ID ryhmiä käytetään joko sisältämään tai pois sulkemiseksi (include/exclude)
- Käytä etuliitettä, jolla tunnistat Entra ID ryhmät joita käytetään CA-policyissä
 - Voit nestata tarvittavat ryhmät!
- Esimerkkejä:
 - CA-CAG001-Excluded
 - CA-CAB001-Excluded
 - CA-Partner-accounts
 - CA-Service-accounts

Perusperiaatteet CA-policyissä

- Ajattele CA-policyjä kuin palomuuuri sääntöjä, jokaisen kirjautumisen PITÄÄ osua CA policyyn!
 - Tarkkana pois sulkemisten kanssa, vältä niin paljon kuin mahdollista.
- Vaadi MFA, ihan kaikilta käyttäjiltä.
 - Paitsi palvelutilit! (näitähän ei pitäisi olla) ☺
- Vaadi Phishing resistant MFA admineilta ja admin portaaleilta.
- Luo poikkeuksia varten omat CA-policyt.
- Luo poikkeusryhmät per CA-policy, mutta mieti tarkkaan miten yläpidetään.
- Vältä report-only modea mobiilialustoilla, aiheuttaa turhia sertifikaatti ilmoituksia.
- Huomio kun käyttäjän kirjautuminen osuu moneen CA-policyyn, kaikkien ehdot pitää täyttyä.
 - Block kaikista voimakkain.

Esimerkki policyjä

- Seuraavat policyt perustuvat osittain Microsoftin suosituksiin, mutta sisältää "mausteita" ja hyväksi havaittuja käytäntöjä.
- Vastaavia CA-policyjä olen rakennellut vuosia 100-25000 käyttäjän tenantteihin.
- Sopivat lähes sellaisenaan eri kokoisille organisaatiolle.
- Tyypillinen käyttöönotto näille policyille on 6-9kk.
- Muistakaa että CA-policyjen kanssa aina sattuu ja tapahtuu!
- Jäätävämpää settiä: [MSUG - Nykyaikainen Conditional Access Policy identiteetin suojaukseen by Matti Väliniemi - YouTube](#)

CA policyt joita kaikki tarvitsevat!

Yleiset
blokattavat

Admin roolit /
Admin portaalit

Security info
registration

Yleiset sallitut

Käyttäjät

External/Guest

Partnerit

Yleiset blokattavat

Blokkaa legacy auth

- Vaikka Microsoft jo blokkaa suurinta osaa, osa saadaan auki. powershellillä, syytä itse kontrolloida.

Blokkaa ei-tuetut alustat

- Blokkaa ne alustat pois joita organisaatio ei käytä/tue.
- Samalla policyllä blokkat myös tuntemattomat alustat.

Blokkaa Break-Glass tilit ja palvelutilit
tuntemattomista sijainneista

- Kahdella eri policyllä, käyttäen "network location" toimintoa joko trusted tai ihan valitsemalla.

Admin roolit/portaalit

Vaadi Phishing resistant
MFA kaikilta Admin rooleilta

- Vaihtoehtoisesti vain “privileged roles” joita on jo 26kpl!
- Aktivoituu viimeistään PIM käytettäessä

Vaadi Phishing resistant
MFA kaikilta Admin
portaaleilta

- Erityisesti Azure Admin portaali joka ei käytä Entran rooleja. (Paitsi GA!)
- Kootut Pilviresurssit: **Microsoft Admin Portals, Windows Azure Service Management API** katat kaiken tarvittavan.

Yleiset

Vaadi laitteiden rekisteröinnissä
MFA:ta

- Tämä vaikuttaa jokaisen laitteen rekisteröintiin Entrassa.
- Voit vaatia tämän lisäksi MFA:ta Intune Enrollmentissa.
- Huomioi Autopilot!

Vaadi MFA ja SSPR rekisteröinnissä
Device Compliance tai Temporary
Access Pass (TAP)

- Rajataan MFA ja SSPR rekisteröinti organisaation laitteille
- Tarvittaessa organisaation prosessien mukaisesti myös TAPilla.

Yleiset Käyttäjät, Guestit, Externalit ja partnerit

Vaadi MFA jokaiselta käyttäjältä

- Pois sulje Palvelutilit ja Break-Glass tilit.
- Pois sulje Guestit ja External accounts.

Vaadi MFA jokaiselta guest / external -käyttäjältä sekä uudelleenkirjautuminen 14 päivän välein

- Kahdella eri policyllä = Helpompi säätää jälkikäteen

Vaadi MFA jokaiselta partner-käyttäjältä sekä uudelleenkirjautuminen 14 päivän välein

- Lisämausteena MFA "TAI" device compliance.
- Riippuu organisaation politiikoista partnerien laitteiden suhteen.
- Windows 365 FTW!

Kehittyneemmät policyt



Riskipohjaiset (vaatii Entra ID P2)

Vaadi MFA kun käyttäjän kirjautumisen riskitaso on riittävän korkea

- Suositus kirjautumisen riskitasolle medium to high.
- Kohdistetaan lisenssin omaaville käyttäjille.

Vaadi MFA ja Salasanan vaihto kun käyttäjän riskitaso riittävän korkea

- Suositus käyttäjän riskitasolle medium to high.
- Vaatii että käyttäjällä on SSPR rekisteröinti tehty ja palvelu on aktiivinen.
- Kirjautumismäärä on joka kerta, jotta salasana vaihto tulee eteen joka kirjautumiskerralla.
- Entrassa asetuksia, joilla saadaan riskitaso poistetaan myös hybrid ympäristössä AD:sta salasana vaihdolla.

Laitepohjaiset, Selain

Vaadi Device compliance selaimella

- Kaikille alustoille policy per alusta, kaikille käyttäjille, Paitsi guestit, externalit, ehkä jopa partnerit.
- Vaatii aina Selainkonffia! Chrome, Firefox, Safari!
- Myös mobiilialustoilla!

Vaadi Device compliance sekä MFA
selaimella ja uudelleenkirjautuminen
14 päivän välein

- Kaikille alustoille policy per alusta, kaikille käyttäjille, Paitsi guestit, externalit, ehkä jopa partnerit.
- Valituille pilviresursseille, jotka osaavat "välittää" Device compliance tietoa Entra kirjautumisessa.
- Pois suljetaan device filtterillä compliantit laitteet.
- Nämä policyt toimivat yhdessä, näin ei muodostu aukkoja!

Laitepohjaiset, Mobile apps and desktop clients

Vaadi Device compliance Mobile apps
and desktop clients

- Kaikille alustoille policy per alusta, kaikille käyttäjille, Paitsi guestit, externalit, ehkä jopa partnerit.

Vaadi Device compliance sekä MFA
mobile apps and desktop clients ja
uudelleenkirjautuminen 14 päivän
välein

- Kaikille alustoille policy per alusta, kaikille käyttäjille, Paitsi guestit, externalit, ehkä jopa partnerit.
- Valituille pilviresursseille, jotka osaavat "välittää" Device compliance tietoa Entra kirjautumisessa.
- Pois suljetaan device filtterillä compliantit laitteet.
- Nämä policyt toimivat yhdessä, näin ei muodostu aukkoja!

Device code flow

Blokataan Device code flow

- Pois suljetaan ainakin Teams rooms laitteet ja joskus jopa devaajat.
- Hyvä aloittaa ensin report-only moodissa.

Appi pohjaiset (App Protection Policies, (APP))

Vaadi APP hallituilta laitteilta

- Kohdistetaan joko kaikkiin pilviresursseihin tai vain rajattuihin, riippuu paljon käytettävistä Appeista ja niiden APP kyvykkyyksistä
- Device filtterillä mukaan vain hallitut laitteet (MDMAppID)
- Jos kaikki pilviresurssit, rajataan pääsy resursseihin jo APP asetuksissa.
- Poikkeuksien rakentaminen tuskallista, toki tehtävissä!

Vaadi APP ei-hallituilta laitteilta

- Kohdistus riippuu organisaation politiikasta ei-hallituille laitteille (MAM-WE).
- Device filtterillä pois suljetaan hallitut laitteet (MDMAppID).
- Jos kaikki pilviresurssit, rajataan pääsy resursseihin jo APP asetuksissa.
- Käyttöskenaariot oltava selkeät!

Admin rooli/portaali kovennot

Vaadi Device compliance
kaikilta Admin rooleilta, pois
sulje sijainnit

- Admin roolien käyttö vaatii Device compliance TAI tunnetun/luotetun sijainnin.
- Pois sulkemalla sijainti, varmistetaan että Admin käyttäjä voi kirjautua pilviresursseihin myös palvelimilta.
- Voidaan myös rajata vain haluttuihin Admin rooleihin (PRIVILEGED!)

Vaadi Device compliance
kaikilta Admin portaaleilta,
pois sulje sijainnit

- Admin portaalien käyttö vaatii Device compliance TAI tunnetun/luotetun sijainnin.
- Pois sulkemalla sijainti, varmistetaan että Admin portaaliin voi kirjautua myös palvelimilta.
- Kootut Pilviresurssit: **Microsoft Admin Portals, Windows Azure Service Management API** katat kaiken tarvittavan.

Lopputulokset

35 CA-policyä

Policy name	State
CAB001 All block legacy authentication for all users v1.0	On
CAB002 All block unknown platforms for all users v1.0	On
CAB003 All block networks other than selected for Break-glass accounts v1.0	On
CAB004 All block networks other than selected for service accounts v1.0	On
CAB005 All block Authentication flow for all users excluding managed devices v1.0	Report-only
CAG001 All require Phishing-resistant MFA for All Admin roles v1.0	On
CAG002 Admin Portals require phishing-resistant MFA for all users v1.0	On
CAG003 All require device compliance for privileged admin roles excluding named locations v1.0	On
CAG004 Admin portals require device compliance for All users excluding named locations v1.0	On
CAG011 Security info registration require TAP or compliant device for All Internal users v1.0	On
CAG012 Device registration require MFA for All Users v1.0	On
CAG013 All require MFA for All User when Sign-in risk is medium to high v1.0	On
CAG014 All require MFA and password change for All Users when User risk is medium to high with SIF every time v1.0	On
CAG021 All require MFA for all users v1.0	On
CAG031 All require MFA for Guest accounts with SIF 14 days v1.0	On
CAG032 All require MFA for External accounts with SIF 14 days v1.0	On
CAG041 All require MFA for Partner accounts with SIF 14 days v1.0	On
CAG051 All require device compliance for All users when browser on Windows v1.0	On
CAG052 All require device compliance for All Users when browser on iOS/Android v1.0	On
CAG053 All require device compliance for All Users when browsers on MacOS v1.0	On
CAG054 All require device compliance for All Users when browser on Linux v1.0	On
CAG061 All require MFA for All users when browser on Windows excluding compliant devices with SIF 14 days v1.0	On
CAG062 All require MFA for All users when browser on iOS/Android excluding compliant devices with SIF 14 days v1.0	On
CAG063 All require MFA for All users when browser on MacOS excluding compliant devices with SIF 14 days v1.0	On
CAG064 All require MFA for All users when browser on Linux excluding compliant devices with SIF 14 days v1.0	On
CAG071 All require device compliance for All users when Mobile apps and desktop clients on Windows v1.0	On
CAG072 All require device compliance for All users when Mobile apps and desktop clients on iOS/Android v1.0	On
CAG073 All require device compliance for All users when Mobile apps and desktop clients on MacOS v1.0	On
CAG074 All require device compliance for All users when Mobile apps and desktop clients on Linux v1.0	On
CAG081 All require MFA for All users when Mobile apps or desktop clients on Windows excluding compliant devices with SIF 14 days v1.0	On
CAG082 All require MFA for All users when Mobile apps or desktop clients on iOS/Android excluding compliant devices with SIF 14 days v1.0	On
CAG083 All require MFA for All users when Mobile apps or desktop clients on MacOS excluding compliant devices with SIF 14 days v1.0	On
CAG084 All require MFA for All users when Mobile apps or desktop clients on Linux excluding compliant devices with SIF 14 days v1.0	On
CAG091 All require app protection policy for All users on managed iOS/Android when Mobile app or desktop client v1.0	On
CAG092 All require app protection policy for All users on unmanaged iOS/Android when Mobile apps and desktop clients v1.0	On

Kiitos!



<https://wallo.pro/>