

Microsoft 365 turvaline kasutuselevõtt

Sisukord

Sisukord 2

1	Sissejuhatus	5
2	Äriliste vajaduste defineerimine	8
2.1	Eesmärgid ja vajadused	9
2.2	Microsoft 365 projekti elemendid.....	9
3	Riskide hindamine	10
4	Olukorra kaardistamine.....	17
4.1	Taristu kaardistamine.....	18
5	Litsentsid ja kulupõhised teenused	20
5.1	Pilveteenuste paketid.....	21
5.2	Kulupõhised teenused.....	24
6	Identiteedihalduse disain ja juurutus	25
6.1.1	„Pilv ainult“ identiteedi mudel	27
6.1.2	Sünkroniseeritud identiteedi mudel	27
6.1.3	Federeeritud identiteedi mudel.....	29
6.1.4	Pass-Through Authentication	29
6.2	Hübriididentiteedi mudeli valimine.....	30
6.3	Hübriididentiteedi seadistamine	31
6.3.1	Ettevõtte domeeni lisamine Entra ID teenuses	31
6.3.2	Active Directory lokaalse domeeni nimede kontroll ja muutmine	32
6.3.3	TLS 1.2 seadistamine Entra Connect serveris	33
6.3.4	Active Directory haldustööriistade paigaldamine.....	34
6.3.5	Teenustekontode loomine Entra Connect teenusele	34
6.3.6	Entra Connect paigaldamine ja seadistamine.....	36
6.3.7	Entra Connect õiguste seadistamine	39
6.3.8	Grupipoliitika seadistamine	39
6.3.9	Entra Connect serveri täiendav turvamine	40
6.3.10	Teise Entra Connect serveri seadistamine	40
7	Pilvepõhiste infoturvelahenduste juurutamine.....	42
7.1	Lahenduste ülevaade	43
7.1.1	Teenused	43
7.1.2	Teenuste asukoht	44
7.1.3	Nimede standard	45
7.1.4	Teenuste sildistamine	45
7.2	Õiguste ja Azure Subscription kontrollimine	46
7.3	Ressursigruppide loomine	47
7.4	Azure Log Analytics teenuskeskkonna paigaldamine	47
7.4.1	Log Analytics teenuskeskkonna paigaldamine	47
7.4.2	Logide säilitamise muutmine	48
7.5	Azure Automation konto loomine.....	49
7.6	Microsoft Defender for Cloud teenuse seadistamine	50
7.6.1	Microsoft Defender for Cloud subscriptioni seadistamine	50
7.6.2	Microsoft Defender for Cloud Log Analytics Workspace seadistamine.....	52
7.7	Microsoft Sentineli teenuse aktiveerimine	52
7.8	Microsoft Sentineli teenuse seadistamine	53
7.8.1	Tasuta andmete hoidlad Sentinelis.....	53
7.8.2	Andmehoidlate seadistamine	53
7.8.3	Entity Behavior Analytics seadistamine	55
8	Küberintsidentide haldus pilveteenustes.....	57

8.1	Oluline	58
8.1.1	Analüütika reeglid	58
8.1.2	Analüütika reeglite mallid	58
8.2	Küberintsidentide teavitamise seadistamine	59
8.2.1	Ressursigrupi loomine	59
8.2.2	Logic Apps rakenduse loomine	60
8.2.3	Logic Apps õiguste delegeerimine	60
8.2.4	Logic Apps töövoos seadistamine	61
8.2.5	Automaatika töövoos seadistamine Sentinelis	63
8.3	Analüütika reeglite seadistamine	65
8.4	Intsidentide käsitlemine	66
9	Administratiivmudeli määratlemine ja kasutuselevõtt	69
9.1	Entra ID infoturbe teenused	70
9.1.1	Entra ID Multi-factor Authentication	70
9.1.2	Entra ID Conditional Access	70
9.1.3	Entra ID Identity Protection	71
9.1.4	Entra ID Privileged Identity Management	71
9.2	Põhimõtete defineerimine	71
9.2.1	Administratiivmudeli disain	72
9.3	Analüüsi läbiviimine	74
9.3.1	FIDO2 turvavõtmed	74
9.3.2	PIM õiguste grupid ja seadistused	74
9.3.3	Koolitus	75
9.3.4	Õiguste kaardistamine ja rollide jaotamine	75
9.4	Entra ID infoturbe sätete seadistamine	79
9.4.1	Gruppide loomine	79
9.4.2	Infoturbe sätete seadistamine	79
9.5	Avariikontode seadistamine	81
9.5.1	Avariikontode loomine	81
9.5.2	Gruppidesse lisamine	82
9.5.3	Kombineeritud infoturbe info registreerimine	83
9.5.4	Parooli poliitika seadistamine	83
9.5.5	Turvavõtmete seadistamine	83
9.5.6	Avariikontode objekti ID´de tuvastamine	84
9.5.7	Monitooringu seadistamine Sentinel teenuses	85
9.6	Administraatorite kontode seadistamine	86
9.6.1	Litsentside määramine	86
9.6.2	Konto loomine	87
9.6.3	Parooli poliitika seadistamine	87
9.6.4	Turvavõtmete seadistamine	88
9.6.5	Gruppide loomine	89
9.6.6	Gruppide seadistamine	90
9.6.7	Entra ID Gruppide PIM rollide seadistamine	91
9.6.8	Microsoft Entra PIM rollide seadistamine	93
9.6.9	Õiguste määramine	93
9.6.10	Konto testimine ja õiguste aktiveerimine	94
9.7	Tingimusliku ligipääsu reeglite seadistamine	95
9.7.1	Reegel 1 – Require multi-factor authentication for Azure management	97
9.7.2	Reegel 2 – Configure - Sign-in frequency	97
9.7.3	Reegel 3 – Require – Entra ID MFA registration from trusted workstation	98
9.7.4	Reegel 4 – Require compliant or hybrid Entra joined device for administrators	99
9.7.5	Reegel 5 – Block access for unknown or unsupported device platform	100
9.7.6	Reegel 6 – Require multi-factor authentication for risky sign-ins	100
9.7.7	Reegel 7 – Require password change for high-risk users	101
9.7.8	Reegel 8 – Block legacy authentication	102
9.7.9	Reegel 9 – Require approved client app for mobile devices (MAM)	102

9.7.10	Reegel 10 – Require multi-factor authentication for device registration	103
9.7.11	Reegel 11 – Access only from trusted countries	104
10	Pilvepõhiste produktiivsuslahenduste seadistamine.....	106
10.1	Põhimõtete ja kasutajate vajaduste defineerimine	107
10.1.1	Oluline meelespea	107
10.2	Entra ID seadistamine	108
10.2.1	Paroolivahetuse seadistamine	108
10.2.2	Kasutajate seadistused	108
10.2.3	Välised kasutajad	109
10.2.4	Seadmete seadistused	109
10.2.5	Rakenduste seadistused	110
10.2.6	Gruppide seadistused	110
10.2.7	Ettevõtte brändingu sätted	111
10.2.8	Mitmetasemelise kontrolli seadistused (Oluline)	111
10.3	Mobile Application Management profiilide seadistamine	112
10.3.1	Hallatud rakenduste poliitikate loomine Android seadmetele	112
10.3.2	Hallatud rakenduste poliitikate loomine iOS seadmetele	113
10.3.3	Ettevõtte emaili seadistamine Android / iOS seadmes.....	114
10.4	Office 365 turbefunktsioonide seadistamine	116
10.4.1	Üldiste failitüüpide keelustamine	116
10.4.2	Spämmipoliitikate seadistamine	116
10.4.3	Emailide automaatsed suunamised	117
10.4.4	DKIM ja SPF kirjade seadistamine.....	117
10.4.5	Exchange Online andmete andmehoiu poliitikate defineerimine	117
10.5	Exchange Online sätete seadistamine	119
10.5.1	IPv6 seadistamine	119
10.5.2	Exchange Online logide hoiu seadistamine.....	119
10.5.3	„Unified Audit Log“ logi reegli kontroll läbi PowerShell'i	120
10.5.4	E-kirjade märgistamine	120
10.5.5	Outlook Web Access kolmandate osapoolte pilveteenuste blokeerimine	121
10.5.6	Parooli aegumise poliitika	121
10.5.7	Väliste osapooltega jagamine	122
10.5.8	Customer Lockbox E5 litsentsi omanikele.....	123
10.5.9	Kalendrite jagamine	123
10.5.10	Aegunud protokollid	124
10.5.11	Aegunud protokollide välja lülitamine postkasti tasemel (Edasijõudnutele)	125
10.5.12	Microsoft Teams välised külalised	126
10.5.13	Microsoft 365 grupid ja välised kasutajad	126
10.5.14	Kasutajatoe informatsiooni lisamine	127
10.6	SharePoint Online ja Onedrive for Business sätete seadistamine	128
10.7	Microsoft Teams seadistamine	130
10.7.1	Välised kasutajad	130
10.7.2	Failide jagamise teenused Teams kaudu	130
10.8	Office 365 seadistuste auditeerimine	131
10.8.1	ORCA paigaldamine.....	131
10.8.2	Raporti loomine	131
11	Pilvepõhiste produktiivsuslahenduste kasutuselevõtt.....	132
11.1	Teenuste kasutuselevõtt	132
12	Kokkuvõte.....	134

1 Sissejuhatus

Käesolev juhend on loodud eesmärgiga võtta Microsoft 365 pilveteenused kasutusele turvaliselt ja jätkusuutlikult. Juhendit lugedes võivad ettevõttel juba erinevad Microsofti pilveteenused kasutusel olla, mistõttu on mõistlik keskkond juhendis välja toodud soovitude ja seadistuste osas üle kontrollida. Juhend ei keskendu kitsalt ainult Exchange Online ja Teamsi kasutuselevõtule, vaid toob välja kogu terviku algusest lõpuni, et pilveteenuste keskkond võetaks kasutusele edukalt. Tuleb silmas pidada, et kogu tervikut vaadates tuleb vältida tehnilise võla teket. Viimane võib väga kergesti juhtuda, kui keskendutakse väga kitsalt ainult ühele asjale.

Käesolev juhend koosneb kümnest erinevast osast luues ühtse terviku:

- Äriliste vajaduste defineerimine
- Riskide hindamine
- Olukorra kaardistamine
- Litsentsid ja kulupõhised teenused
- Identiteedihalduse disain ja juurutus
- Pilvepõhiste infoturvelahenduste juurutus
- Pilveteenuste küberintsidentide haldus
- Administratiivmudeli määratlemine ja kasutuselevõtt
- Pilvepõhiste produktiivsuslahenduste seadistamine
- Pilvepõhiste produktiivsuslahenduste kasutuselevõtt

Enne juhendi alusel tegevuste alustamist, soovime selle kõigepealt algusest lõpuni läbi töötada. Selle käigus peaks Teil tekkima erinevaid küsimusi ja mõtteid. Kui avastate, et mingid asjad on Teie ettevõtte puhul puudu või teistmoodi, siis proovige kõigpealt aru saada, mis põhjusel see nii on.

Juhendiga on kaasas järgnevad lisad:

PowerShelli skriptid:

- **Entra ID - Avariikontode-ParooliPoliitikaMuutmise.ps1**
 - Entra ID avariikontode paroolipoliitika seadistamise skript.
- **Entra ID - Connect-ADKontoLoomine.ps1**
 - Entra Connect teenusekonto loomine Active Directory lugemiseks ja muudatuste tegemiseks.
- **Entra Connect-GMSAKontoLoomine.ps1**
 - Entra Connect teenusekontode loomine.
- **Entra ID - Connect-ÕigusteSeadistamine.ps1**
 - Entra Connect teenusekonto õiguste seadistamise skript.
- **Enable-TLS1.2.ps1**
 - Seadistab TLS 1.2 Entra Connect serveris.
- **Get-TLS1.2Status.ps1**
 - Kontrollib kas TLS 1.2 on serveris seadistatud.
- **Lülita-VäljaOWA3PartyStorage.ps1**

- Lülitab välja kolmandate osapoolte failide jagamisteenused
- **Entra ID - PilveAdministraatoriteKontode-Seadistamine.ps1**
 - Seadistab pilve administraatori kontol paroolipoliitika ringi.

Dokumendid:

- **Azure Administratiivmudel.xlsx**
 - Exceli tabel mida kasutada Azure administratiivmudeli kaardistamiseks ja seadistamiseks.

Microsoft Sentinel analüütika reeglid:

- **Avariikontode kasutamine.txt**
 - Microsoft Sentineli päringu näidis avariikontode monitooringu seadistamine

1.1 Portaaliid

Microsoft on aastate jooksul ehitanud erinevaid portaale oma teenuste halduseks. Tänapäevaks on viis peamist portaali:

- **portal.azure.com**
 - Microsofti kulupõhiste teenuste haldus ja tänase seisuga veel ka Entra ID. Soovitatav on kasutada **entra.microsoft.com** portaali.
- **security.microsoft.com**
 - Microsofti infoturbe teenuste haldus nagu nt Defender for Endpoint, Defender for Identity, Defender for Cloud Apps jne.
- **intune.microsoft.com**
 - Microsofti seadmete halduse lahendused nagu nt Microsoft Intune, Autopilot, Co-Management, Mobile Application Management.
- **portal.office.com**
 - Microsofti produktiivsus-lahenduste haldus nagu nt Exchange Online, Teams, SharePoint Online jne.
- **entra.microsoft.com (UUS)**
 - Tegemist on täiesti uue portaaliga kuhu Microsoft koondab kokku kogu oma identiteedi lahenduste halduse. Microsoft plaanib edaspidi kõik täiendused ja uued teenused lisada entra.microsoft.com portaali ja uuendused ei pruugi enam portal.azure.com kaudu leitavad olla.

1.2 Azure Active Directory on nüüd Microsoft Entra

Olulise uuendusena Microsofti tootevalikus tuleb märkida, et Azure Active Directory (Azure AD), mis on olnud keskne osa Microsoft 365 identiteedihalduse ja turvalisuse infrastruktuurist, on nüüd ümber nimetatud Microsoft Entra'ks.

2 Äriliste vajaduste defineerimine

Eesmärgid:

- Äriliste vajaduste väljaselgitamine
- Projektiplaani koostamine
- Projektimeskonna komplekteerimine

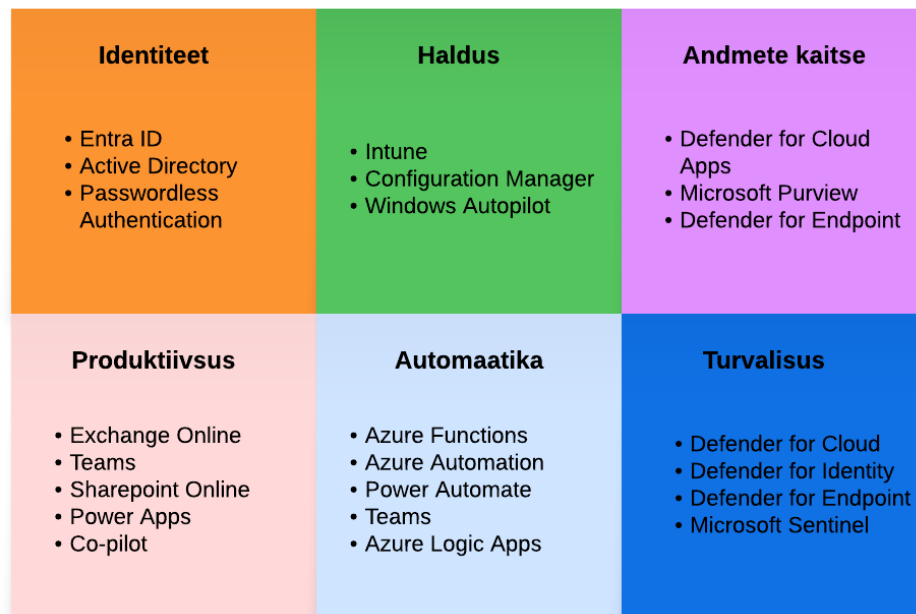
2.1 Eesmärgid ja vajadused

Enne pilveteenuste juurutamist on väga oluline sõnastada ärilised eesmärgid, mida ettevõtte soovib pilveteenuseid kasutusele võttes saavutada ja mis väärtust see loob. Äriliistest eesmärkidest peaks välja joonistuma täpsemad tehnilised eeldused ja litsentside vajadused.

Eesmärkide sõnastamisele peab järgnema mõõdikute defineerimine. Selline lähenemine annab selge arusaama, kuidas projekt aja möödudes edeneb ning kas liigutakse soovitud eesmärkide suunas. Soovitatav on ka enne suuremat juurutust viia läbi erinevad töötoad, mõistmaks paremini pilveteenuste võimekust ja kuidas uusi lahendusi kasutusele võtta. Töötubade läbiviimiseks vajadusel kaasata väliseid partnereid. Oluline on meeles pidada, et tegemist ei ole ainult tehnilise projektiga, vaid hõlmab endas palju protsesside ja inimestega seotud muudatusi. On oht, et korraka liiga palju muudatusi rakendades ei pruugi projekt soovitud eesmärki täita.

2.2 Microsoft 365 projekti elemendid

Microsoft 365 pilveteenuste juurutamine ei ole üksnes Exchange Online või Teams kasutuselevõtt. Pilveteenuste edukaks ja turvaliseks juurutuseks peavad läbi mõeldud olema järgmised teemad:



3 Riskide hindamine

Eesmärgid:

- Arusaam pilveteenuste kasutuselevõtuga seotud riskidest

Eeltingimused:

- Ärilised vajadused on välja selgitatud

3.1 Riskianalüüsi läbiviimine

Pilveteenuste kasutuselevõtmisega kaasnevad ettevõttele riskid ning sellest tulenevalt on oluline, et nendest ollakse teadlikud. Allpool tabelis on välja toodud võimalikud riskid, millega tuleks arvestada ning millele tuleks vastavalt riski mõjule koostada riskiohjeplaan.

Legend:

- **Jah** => risk eksisteerib
- **Ei** => riski ei eksisteeri

Oht	Kirjeldus	Maapealne teenus / teenused	Pilve teenus
1. Pilveteenuse pakkuja IT süsteemi avarii (tehniline viga, inimviga, loodusjõud)	Pilveteenuse pakkuja IT süsteemi avarii tõttu ei suudeta pakkuja teenust vastavalt kokkulepitud käideldavusnõuetele ja andmeid ei ole võimalik taastada kokkulepitud ulatuses.	Jah	Jah
2. Pilveteenuse pakkujaga ühepoolne lepingu lõppemine	Pilveteenuse pakkuja lõpetab omapoolselt teenuse pakkumise (pankrot, mainekahju, loodusjõud). <ul style="list-style-type: none"> • Käideldavusnõudeid pole võimalik tagada, teenus ei ole kättesaadav • Ühepoolse lepingu lõppemisega võib jääda ilma terviklikest andmetest • Andmed võivad muutuda avalikuks 	Ei	Jah
3. Pilveteenuse pakkuja valimisel ei tehta piisavat taustauuringut	Teenusepakkuja põhjaliku taustauuringu mitte tegemisel (täpsustades nt <i>security policy</i> dokumenti, auditeid) on risk andmete käideldavusele, konfidentsiaalsusele ja terviklikkusele.	Jah	Jah
4. Ettevõtte poolt äri vajadustele mittevastava pilveteenuse valik (paketi valik)	Teenuste ebapiisava valiku puhul on riskid suhteliselt madalad, kuid vale pakett võib tekitada olukorra, et keegi ei pääse andmetele ligi, sest nt kohad/litsentsid on täis või teenuse sisu puudulik jne.	Jah	Jah
5. Pilveteenuse tellimisel läbi sideettevõtte ei ole lepingu tingimused läbiräägitavad (puudused tingimustes)	Sisuliselt risk mitmekordistub, kuna toimub teenuse vahendamine. Ettevõttes peab teenuse tellimisel leppima riskiga, et SLA tingimused on ettemääratud ja need pole läbiräägitavad: <ul style="list-style-type: none"> • teenusekatkestuse kestus ja taastamise aeg (käideldavuse nõuded) • andmekadu katkestuse ajal ei taga andmete terviklikkuse nõudeid 	Jah	Jah
6. Pilveteenuse kasutuselevõtmisel ei saa lepingus pakutavates tingimustes kaasa	Ettevõttes peab teenuse tellimisel leppima riskiga, et on ilmselt kindlad ettemääratud SLA tingimused ja need pole läbiräägitavad.	Jah	Jah

rääkida (puudused tingimustes)	<ul style="list-style-type: none"> • teenusekatkestuse kestus ja taastamise aeg (käideldavuse nõuded) • andmekadu katkestuse ajal, ei taga andmete terviklikkuse nõudeid 		
7. Pilveteenuse klient eeldab teenuse pakkujalt rohkem kui lepingus kirjas (ressursside jagatud vastutuse risk)	Kliendi eelduste tõttu võib jääda mõni aspekt nõrgema kaitsega või ilma piirangut seadmata. Pole selgust kust jookseb vastutus teenuse pakkuja ja tarbija vahel (turvalisus, riskid).	Ei	Jah
8. Pilveteenuse pakkuja tugi on puudulik või halvasti kättesaadav	Tugi ei ole kättesaadav või ei ole asjakohane (võib kaasa tuua ohu andmete ja süsteemide käideldavusele, terviklusele või konfidentsiaalsusele.)	Jah	Jah
9. Pakutav teenus ise ei ole ajakohane	Ise teenust majutades on risk, et rakendus ei saa piisavalt kiirelt uuendusi. Pilveteenuse pakkujat tuleb usaldada, et pakutav teenus on kõige uuemate uuendustega.	Jah	Ei
10. Pilveteenusele üleminek ja ülalhoidmine on kulukas	<ul style="list-style-type: none"> • Ei arvestata, et ajakohased serverid ja süsteemid mis on pilveteenuse teenuse tellimise komplekti maksavad igakuiselt või aastas teatud summa. • Enne pilveteenusele üleminekut ei arvestata kulusid ja tulusid. • Varjatud kulu - Kasutajate kasvamisel tasu suureneb • Varjatud kulu - Andmemahu kasvamisel tasu suureneb <p>Rahastuse puudumisel on risk, et pannakse teenus kinni (oma andmekeskuses on teenused ja serverid olemas ehk rahastuse kohene katkemine ei ole kriitiline. Pilveteenuste kasutamise eest tuleb tasuda igakuiselt või aastaselt)</p>	Jah / Ei	Jah
11. Teenuse osutamise ebapiisav järelvalve	Pilveteenuse pakkuja poolt osutatav teenus ei vasta käideldavuse ja tervikluse nõuetele	Jah	Jah
12. Sõltuvus välisest teenusepakkujast	Lepingus tingimuste muutmise (nt omaniku vahetus, seaduse muutus jne) korral võib olla oht, et käideldavuse ja/või terviklikkuse nõuded ei ole täidetud.	Jah	Jah
13. Pilveteenuse pakkuja turvameetmete ebapiisav järelvalve	Järelvalve puudumisel muutuvad avalikuks delikaatsed andmed/info.	Jah	Jah
14. Pilveteenusest väljumine on keerukas	Pilveteenusest väljumisel on oht, et ei saada andmeid kätte või tekib andmekadu. Puudub pädevus andmete kättesaamiseks (nt kui vastavate teadmistega inimesi enam pole).	Jah	Jah
15. Pakutav pilveteenus muutub ebasobilikuks	Pilveteenuse muutumisel (nt uus versioon, mille tulemusel muutub teenuse sisu) ei ole võimalik enam soovitud teenust kasutada või	Jah	Jah

	ei saa varasemaid andmeid kätte (tuleks järgida soovitusi ja parimaid praktikaid).		
16. Pilveteenuse pakkuja rikub lepingutingimusi	Risk konfidentsiaalsuse, terviklikkuse ja käideldavuse kaole	Jah	Jah
17. Ettenägematu pilveteenuse nõudluse suurenemine	Kasvava nõudluse suurenemisel on risk, et valitud pakett ei oma piisavalt vahendeid nõudluse täitmiseks.	Jah	Jah
Organisatoorsed			
18. Pakutava pilveteenuse kasutajal ei ole piisavad turvanõuded	Ettevõtte ja tema pilves olevate andmete ühendus ei ole turvaline.	Jah	Jah
19. Pilveteenuse õiguste jagamisel tehakse viga	<ul style="list-style-type: none"> • Administraatoril liiga vähe õiguseid, kasutajal liiga palju õiguseid. • Administreerimisel tehtav inimlik viga. • Rollide jagamise protsess on puudulik (pääsuõiguste protsess). 	Jah	Jah
20. Pilveteenuse seadistamisel tehakse viga	Inimfaktor, et seadistamisel läheb midagi valesti.	Jah	Jah
21. Pilveteenust ei kasutata tõhusalt	Ei võeta kasutusele kõiki paketiiga kaasa tulevaid võimalusi (turvanõudeid, teenuseid jne). Pilveteenuse seadistamisel tuleb määrata turvanõuded, mis valitud paketi/teenusega kaasa tulevad (nt kaheastmeline autentimine (2FA), nutiseadmesse lisaparooli lisamine, FIDO2 võtmed jne).	Jah	Jah
22. Pilveteenuse kasutamine on ebamugav, keerukas	Puudub info kuidas teenust kasutada või see on keeruline. Hakatakse otsima erinevaid lihtsamaid alternatiive dokumentide jagamiseks/saatmiseks (Google, Dropbox jne)	Jah	Jah
23. Pilveteenuse teenust ei dokumenteerita	<ul style="list-style-type: none"> • Seosed teiste süsteemidega, mille tulemusel vajalik ka teiste teenuste turbeastet tõsta. • Puudub strateegia pilveteenuse kasutuselevõtmiseks. • Mitte-dokumenteerimine võib kaasa tuua andmekao riski. • Puuduvad protsessid teenuse turvaliseks kasutamiseks. 	Jah	Jah
24. Välise teenuspakkuja poolne andmete lekitamine kolmandale osapoolle.	<ul style="list-style-type: none"> • Teenusepakkuja lubab ligipääsu salajastele andmetele. 	Ei	Jah

25. Inimeste liikumine	<ul style="list-style-type: none"> Süsteemi tundev inimene lahkub, on eemal. Ei ole samade oskustega asendajat. Inimeste voolavuse tõttu on risk turvateadlikkuse ja kogemuse osas. 	Jah	Jah / Ei
26. Pilveteenuse väärkasutus	<ul style="list-style-type: none"> Tundlike dokumentide saatmisel/jagamisel sisestatakse vale inimese kontaktid, jagatakse read-only dokumente muutmisõigustega, tehakse näiteks dokument kogemata avalikuks või unustatakse dokumendid krüpteerida. Inimesed ei ole piisavalt koolitatud ja teadlikud teenust turvaliselt kasutama. 	Jah	Jah
<ul style="list-style-type: none"> Inimlik viga - dokumentide saatmisel Inimlik viga - dokumentide jagamisel Inimlik viga - dokumentide mittekrüpteerimine Inimlik viga – lisatakse vale inimene koosoleku vestlusse (üle veebi pakutav ruum) 			
27. Pilveteenuse kasutamine on piiratud	Uue teenuse kasutamisele võtmisel koos piirangutega on oht, et osade funktsioonide puudumisel või keerukuse tõttu hakatakse alternatiivseid, vähemturvalisi rakendusi kasutama.	Jah	Jah
Tehnilised			
28. Internetiühenduse katkemine	Internetiühenduse katkemine sideteenusepakkuja rikke/vea tõttu. Ei ole võimalik ligi pääseda pilveteenusele (LIVE dokumentidele).	Jah	Jah
29. Ei kasutata turvalist võrguühendust (avalike võrkude kasutamise risk)	Väljaspool võrdlemisi turvalist ettevõtte võrku, ei kasutata VPN ühendust ligipääsemiseks pilveteenusele nutiseadmes, koduarvutis, kohvikus jne	Jah / Ei	Jah / Ei
30. Pilveteenuse server ei vasta	Ei ole võimalik pilveteenusele ligi pääseda	Jah	Ei, aga võimalik
31. Ei varundata pilveteenuses hoitavaid andmeid	Varukoopiate puudumisel ei ole võimalik andmeid taastada. Kui peaks juhtuma, et pilveteenuse enda regulaarsete varukoopiate tegemisel midagi juhtub, on risk andmete kaole.	Jah	Jah
32. Ei ole võimalik ise monitoorida pilveteenust	Pilveteenuse pakkuja monitoorib ise oma süsteemi, mistõttu peab teenuse kasutaja usaldama pakkuja monitooringut	Ei	Jah

33. Ressursside jagatud kasutuse riskid	Pilveteenuse kliendid jagavad samu ressursse - servereid, võrku, salvestusruumi. Erinevate klientide eraldamine on pilveteenuse osutaja ülesanne ning sõltub tema süsteemide ja protsesside turvalisusest. On võimalik, et kliendid saavad teatud tingimustel infot teiste klientide teenuste, andmevahetuse või salvestatud andmete kohta.	Ei	Jah
34. Pilveteenuste kasutajate üheaegne koormuse tõus	Pilveteenuse pakkuja ei suuda koormuse tõttu kokkulepitud käideldavuse nõudeid tagada, mille tõttu ei ole andmed kättesaadavad.	Ei	Jah
Ründed			
35. Andmete või tarkvara manipuleerimine rünnaku tagajärjel, nt turvanõrkuste olemasolul, teenuse pahatahtlik väärkasutus, DDOS	<ul style="list-style-type: none"> Ründed pilveteenusepakkuja vastu. Avalik haldusliides (andmevahetus), paroolide lekkimisel rünnatav. Pilveteenuse pakkuja ei suuda kokkulepitud käideldavusnõudeid tagada. 	Jah, pead ise kaitsma	Jah / Ei, suuresti kaitstud
36. Välise teenuste volitamatu kasutamine	<ul style="list-style-type: none"> Pilveteenuse pakkuja kasutab väliseid teenusepakkujaid, kellele esitatud infoturbenõuded ei vasta teenuse terviklikkuse ja käideldavuse nõuetele. Lubatakse ligipääs salajastele andmetele või autentimise infole 	Jah	Jah
37. Välise teenuspakkuja sihilik käideldavuse häirimine	<ul style="list-style-type: none"> Pole võimalik andmetele ligi saada. 	Ei	Jah
38. Administraatori õiguste väärkasutus	<ul style="list-style-type: none"> Pilveteenuse pakkuja IT administraatorite õiguste volitamatu kasutamine võib kaasa tuua andmekao või andmete muutumise/hävimise. 	Jah	Jah

3.2 Pilveteenuste varundamine ja taastamine

Microsoft ei paku oma klientidele standardses mõistes Microsoft 365 varundamise teenust. Microsoft on juurutanud oma teenustesse erinevaid meetmeid, mis võimaldavad vältida andmete kadu (ning vajadusel nende taastamist).

Lähemalt soovitage tutvuda järgmiste viidetega:

- <https://docs.microsoft.com/en-us/exchange/back-up-email>
- <https://docs.microsoft.com/en-us/microsoft-365/compliance/retention-policies-sharepoint?view=o365-worldwide>
- <https://docs.microsoft.com/en-us/microsoft-365/compliance/retention-policies-teams?view=o365-worldwide>
- <https://docs.microsoft.com/en-us/microsoft-365/compliance/retention-policies-exchange?view=o365-worldwide>
- <https://docs.microsoft.com/en-us/microsoft-365/compliance/retention-limits?view=o365-worldwide>

Kui riskide analüüsi tulemusel selgub, et Microsoft poolsed meetmed ei anna soovikohaseid tulemusi, tuleks täiendavalt hankida kolmanda osapoole lahendus Microsoft 365 teenuste sisu varundamiseks teise asukohta.

4 Olukorra kaardistamine

Eesmärgid:

- Selgitada välja tänane taristu olukord ja võimalikud puudused
- Vajaliku sisendi saamine pilveteenuste juurutamiseks

4.1 Taristu kaardistamine

Pilveteenuste edukaks juurutamiseks on vaja kaardistada tänane ettevõtte taristu seis. Seda juhendit lugedes võite Te juba teada, et pilveteenuste juurutust on varem alustatud, kuid sellest puudub dokumentatsioon. On muidugi ka võimalik, et pilveteenuste juurutamist on teostatud, kuid puudub ülevaade kui hästi seda on tehtud.

Kaardistus peab hõlmama järgmisi teemasid ja punkte:

- Active Directory keskkonna analüüs
 - o OS versioon
 - o *Schema* ja *Forest* tasemed
 - o Audit poliitika domeenikontrollerites
 - Milliseid logisid salvestatakse domeenikontrollerites või teistes serverites ja tööjaamades. Kui poliitika on puudu, siis infoturbeinsidendi korral puuduvad vajalikud logid.
 - o Ettevõtte struktuur Active Directory's
 - o Sensitiivsete gruppide liikmed (Domain Admins, Administrators, Enterprise Administrators jne)
- Kas teenuste logisid kogutakse keskselt
- Kas on eelnevalt juba soetatud pilveteenuste litsentse ja mis põhjusel need soetati
- Millised pilveteenused on juba kasutusel ja kas selle kohta on olemas dokumentatsioon
 - o Exchange Online
 - o Teams
 - o Entra ID
 - o Onedrive for Business
 - o Sharepoint Online
 - o Intune
 - o jne
- Kes omab ligipääsu pilveteenustele (kasutajad, administraatorid jne)
- Milline on ettevõtte identiteedimudel
 - o Kas on tehtud liidestusi Entra ID'ga
 - o Kas on paigaldatud Entra Connect teenus
 - Entra Connect versioon
 - Entra Connect seadistused
 - Millal Entra Connecti viimati uuendati
 - o Kui palju on pilve kontosid, grupe ja arvuteid sünkroniseeritud. Kas on jäänud süsteemi vanu kontosid ja kas on sünkroniseeritud õiged objektid.
- Pilveteenuste teenuseomanikud
- Microsoft Office versioonid
- Persoonide, rollide kaardistus

- Ärilised vajadused erinevatel gruppidel, näiteks:
 - Müügimees
 - Juhtkond
 - Raamatupidamine
 - Jne
- Milliseid seadmeid erinevad grupid kasutavad ja miks
- Kellele seadmed kuuluvad. Kas töötajad kasutavad isiklike või tööandja seadmeid
- Kas kasutajad kasutavad oma isiklikes seadmetes tööandja e-maili ja muid rakendusi töö tegemiseks
- Kas töötajate palkamisel ja lahkumisel on olemas kirjeldatud vastavad protsessid
- Kas kasutusel on eraldi spämmifiltrid
- Exchange serverite analüüs
 - Versioonid
 - Arhitektuur

NB! Kui analüüsi käigus leiate, et maapealne Active Directory versioon on 2008 R2 või varasem, siis tuleb Active Directory uuendada vähemalt versioonile 2019 (soovitavalt 2022). Pilveteenuste juurutamiseks tuleb kasutada süsteeme, mis on ajakohased ja Microsofti poolt toetatud.

5 Litsentsid ja kulupõhised teenused

Eesmärgid:

- Valida välja sobiv pilveteenuste pakett, mis vastab ettevõtte vajadustele.

Eeltingimused:

- Riskianalüüs
- Taristu kaardistus
- Defineeritud ärilised eesmärgid

5.1 Pilveteenuste paketid

Pilveteenuste juurutamiseks on vaja valida litsentside pakett, mis vastab ettevõtte äriliste eesmärkidele ja infoturbe poliitikatele. Õige litsentsipaketi valimise eelduseks on ettevõtte sisemine äri- ja turbevajaduste analüüs. Kui ärilised vajadused on kaardistatud, siis tuleb need konverteerida tehnilisteks nõueteks.

Litsentse on võimalik soetada erinevate pakettidena või üksikult. Mõned näited erinevatest võimalustest:

Paketeeritud komplektid (loetelu ei ole lõplik):

- Enterprise Mobility + Security (EM+S) E3 / E5
 - o Sisaldab Intune, Entra ID P1 / P2, Defender for Cloud Apps ja Defender for Identity litsentse
 - o Täpseminfo: <https://www.microsoft.com/en-us/microsoft-365/enterprise-mobility-security/compare-plans-and-pricing>
- Microsoft 365 E3 / E5
 - o Sisaldab Office 365 ja EM+S teenuseid
- Microsoft 365 Business Basic
- Microsoft 365 Business Standard
- Microsoft 365 Business Premium
- Office 365 E3 / E5

Üksikud teenused (loetelu ei ole lõplik):

- Entra ID
 - o Entra ID P1 / Entra ID P2
- Exchange Online
 - o Exchange Online Plan 1 / Exchange Online Plan 2
- Sharepoint Online
 - o SharePoint Online Plan 1 / SharePoint Online Plan 2
- Teams

Pakettide valikuvõimalusi on palju. Paketid, mis on tähisega E5 või A5 on kõige suurema funktsionaalsusega. Microsoft on viimasel ajal üha enam oma kliente suunanud Microsoft 365 pakettide peale, sest need sisaldavad nii haldus-, infoturbe- kui ka produktiivsuslahendusi. Kui soetate ainult Office 365 või Exchange Online paketi, siis saate sellega turvalisuse vaates ainult piiratud funktsionaalsuse. Soodsamate litsentside puhul võib näiteks selguda, et logisid ei saa hoida pikemalt kui 90 päeva või ei ole võimalik seadistada mingit teist konkreetset seadistust, sest seda ei ole valitud pakettis olemas.

Erinevate litsentside soetamise puhul tuleb arvesse võtta lisaks maksumusele ka litsentsi poolt pakutava funktsionaalsuse vastavust ärinõuetele. Kui peaks juhtuma, et Te vajalikke litsentse ei saa soetada, siis suure tõenäosusega ei pruugi Te saada seadistada kõiki turvasätteid.

Litsentside soetamisel on võimalik kombineerida erinevaid pakette ja saada täpselt see, mida vaja on. Näiteks osta kõigile kasutajatele Microsoft 365 E3 ja lisada sinna juurde Defender for Office 365 infoturbe teenuste pakett. Neid võimalike kombinatsioone tuleks litsentsimisspetsialistiga analüüsida.

Kui soovite koheselt osta kõigile näiteks Microsoft 365 E5 litsentsid, siis on vaja veenduda, et olete ettevõttes valmis kogu funktsionaalsust mõistliku ajaga juurutama. Ei ole mõistlik osta litsentse, mille pakutavaid võimalusi Te ei suuda juurutada. Microsofti pilveteenuste juurutamine ei ole ainult tehniline projekt, siia on vaja kaasata kogu organisatsioon.

Käesolevas juhendis eeldatakse, et soetatud on vähemalt Entra ID P1 ja Intune litsents kõikidele kasutajatele. Neid saab soetada kas eraldi või läbi Enterprise Mobility + Security või M365 pakettide. Entra ID P1 pakett sisaldab väga olulisi infoturbe teenuseid ja sätteid, nagu näiteks tingimuslike ligipääsureeglite defineerimist, logide suunamist Sentineli jne. Intune abil on meil võimalik hallata nutiseadmed või rakendada neile hallatud rakenduste poliitikaid. Viimasel juhul pannakse ettevõtte andmed eraldi virtuaalsesse konteinerisse. Kui andmed on eraldi hallatud, siis saate neid kaugelt kustutada ja ka näiteks kasutust reguleerida (kas kasutaja saab andmeid isiklikku profiili tõsta jne).

Administraatorite osas eeldame, et on soetatud Entra ID P2 või Enterprise Mobility + Security E5 või Microsoft 365 E5 pakett. Entra ID P2 pakettis on kaks väga olulist teenust: Identity Protection ja Privileged Identity Management. Administraatorid peavad privilegeeritud õigusi kasutama ainult vajaduspõhiselt ja administratiivkontod peavad olema kaetud põhjalikumate infoturbelahendustega kui vaid mitmetasemeline kontroll. Eelpoolnimetatud teenused aitavad seda saavutada. Administratiivmudeli peatüki lugemisel näete täpsemalt, kuidas käib administraatorite kontode seadistamine.

Teenus	Entra ID P2 / Microsoft 365 E5 / Enterprise Mobility +Security E5	Entra ID P1 / Microsoft 365 E3 / Enterprise Mobility +Security E3
Conditional Access	Jah	Jah
Multi-factor Authentication	Jah	Jah
Identity Protection	Jah	Ei
Privileged Identity Management	Jah	Ei

Entra ID infoturbe teenused

5.2 Kulupõhised teenused

Litsentsitud teenuste kõrvale on vaja soetada vähemalt üks Azure subscription, et oleks võimalik kasutada kulupõhiseid teenuseid. Kulupõhised teenuste jaoks ei pea eelnevalt ostma litsentse, vaid arveldatakse kulutatud mahu järgi. Kulupõhised teenused on näiteks virtuaalmasin, veebileht, virtuaalvõrk, Microsoft Sentinel infoturbetaenus jne. Käesolevas juhendis me seadistame Azure Log Analytics ja Microsoft Sentinel kulupõhise teenuse logide hoiu jaoks. Erinevates teenustes tekib erinevates mahtudes logisid ja neid on vaja hoiustada. Infoturbe vaates on meil võimalik nende logide pealt luua erinevaid analüütika reegleid jne.

Konsulterige oma litsentsi partneriga, millised võimalusi kulupõhiste teenuste osas pakutakse. Alati on võimalik kasutada krediitkaarti, kuid see on võimalikest variantidest kõige kulukam, eriti kui teenuse mahud ajas kasvavad.

Täpsemalt saate erinevate pakkumiste kohta lugeda siit - <https://azure.microsoft.com/en-us/support/legal/offer-details/>

6 Identiteedihalduse disain ja juurutus

Eesmärgid:

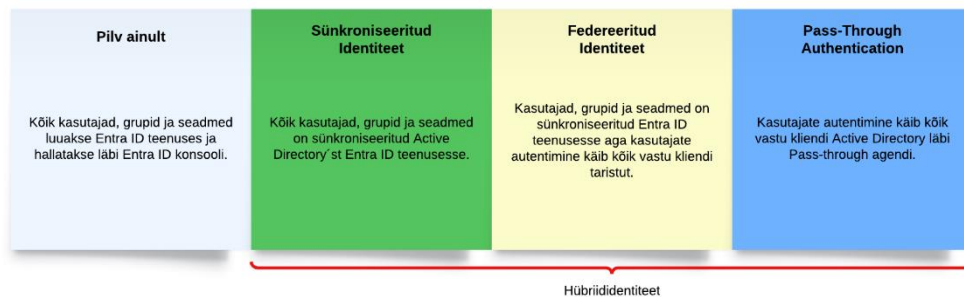
- Ettevõtte vajadustele vastav identiteedihalduse lahenduse välja valimine
- Identiteedihalduse lahenduse arhitektuuri kokkuleppimine
- Identiteedihalduse lahenduse juurutamine

Eeltingimused:

- 2 virtuaalmasinat (Windows Server 2016 või uuem)
 - Server peab olema liidestatud sisemise domeeniga
 - Server kuulub “**Tase-0**” kategooriasse
 - Server on uuendatud viimaste turvauuendustega
- Entra ID Global administraatori õigused
- Active Directory Enterprise administraatori õigused
- Ligipääs ettevõtte DNSi seadistustele
- Domeeni nimi või nimed mida soovitakse lisada Entra ID´sse

6.1 Identiteedi mudelid

Microsoft pakub ettevõtetele nelja erinevat identiteedimudelit.

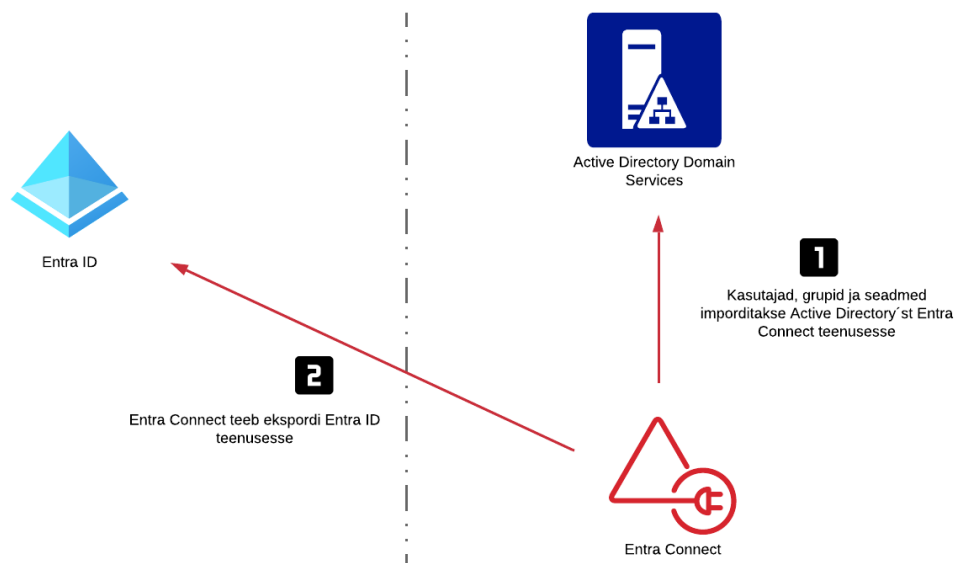


Microsofti poolt pakutavad identiteedimudelid

Ettevõtte kellel on maapealne Active Directory Domain Services, siis enamasti valitakse üks kolmest võimalikust identiteedimudelist:

- Sünkroniseeritud
- Federeeritud
- Pass-Through Authentication

Identiteetid sünnivad maapealses Active Directory teenuses ja kui kasutajal on vajadus pääseda ligi pilveteenustele, siis see konkreetne kasutaja sünkroniseeritakse Entra ID-ga. Pärast seda on võimalik kasutajal pääseda ligi ettevõtte pilveteenustele sama kontoga. Niiugust lahendust nimetatakse hübriididentiteedimudeliks.



Active Directory objektide sünkroniseerimise protsess Entra ID teenusega

Hübriididentiteedi korral on konkreetsel kasutajal ainult üks konto ja ta saab tarbida teenuseid nii pilves kui ka „maa peal“. Nagu üleval joonisel on näha, siis teenus nimega Entra Connect vastutab identiteedite sünkroniseerimise eest Active Directory' st Entra ID teenusesse. Tegemist on kohustusliku teenusega, kui soovitakse kasutada hübriididentiteeti. Entra Connecti tuleb kaitsta samal tasemel, kui Active Directory-t. Entra Connect teenus omab tavaliselt palju õigusi ja seetõttu ka ligipääsu väga sensitiivsele informatsioonile.

Maapealsest Active Directory'ist kasutajate mitte sünkroniseerimisel Entra ID'ise tuleks kasutajal hakata kasutama kahte erinevat kontot ja parooli. Selline olukord ei ole kindlasti soovitatav, kuna põhjustab kasutajate jaoks segadust

„Pilv ainult“ identiteeti kasutatakse „pilveteenuste administratiivmudeli“ juurutamisel. Lisaks luuakse Teie Entra ID keskkonda ka külaliskontod juhul, kui olete oma väliseid partnereid kutsunud koostööd tegema või on kasutajad ise mõne välise osapoollega informatsiooni jaganud. Külaliskontode sätteid on võimalik muuta ja auditeerida. Eraldi lisa federatsioone luua pole vaja ja neid kontosid ettevõtte Active Directory teenusesse tagasi ei sünkroniseerita.

6.1.1 „Pilv ainult“ identiteedi mudel

„Pilv ainult“ identiteedi puhul on tegemist kõige lihtsama identiteedi lahendusega. Sellisel juhul toimub kasutajate haldus otse veebipõhise Entra ID portaali kaudu ja ühtegi kasutajat ettevõtte maapealsest domeenist ei sünkroniseerita. „Pilv ainult“ lahendus sobib ettevõttele, millel ei ole „maapealset“ taristut või soovitakse „maapealsest“ taristust loobuda.



Pilv ainult identiteedimudel

Eelised

- Haldad kasutaja kontosid ja seadistusi otse läbi Entra ID portaali
- Pole vaja täiendavaid servereid ja teenuseid
- Lihtne hallata
- Madalad kulud

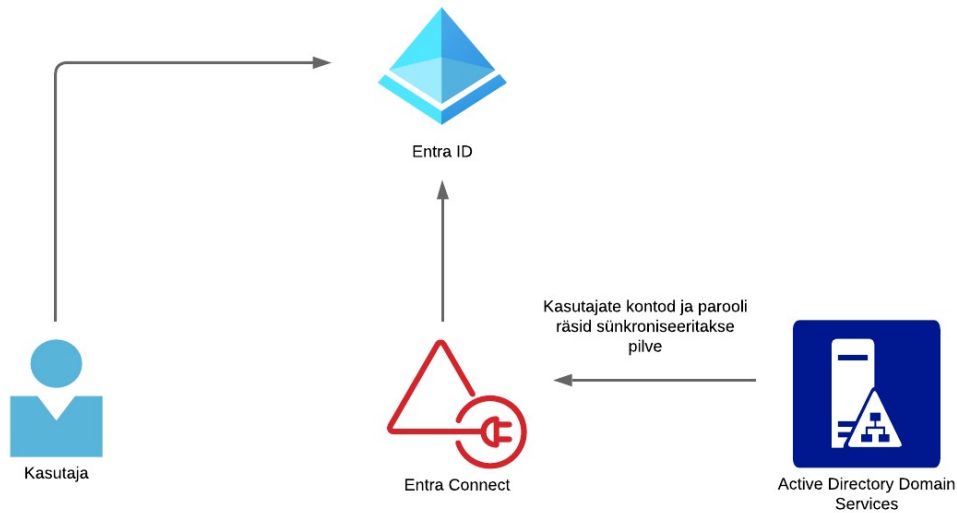
Puudused

- Nõuab kasutajatelt eraldi kontot juhul, kui ettevõttel on maapealne Active Directory teiste teenuste jaoks

6.1.2 Sünkroniseeritud identiteedi mudel

Sünkroniseeritud identiteedi puhul sünkroniseeritakse olemasolevad kasutajad majasisesest domeenikontrollerist otse Entra ID teenusesse. Selle seadistamiseks tuleb kasutusele võtta vähemalt üks täiendav server, kuhu paigaldatakse Entra Connect teenus. Parimate praktikate järgi peaks neid olema alati kaks. Juhul kui peaks midagi ühega neist juhtuma, siis on Teil võimalik lülituda ümber teisele serverile ja hoida ära pikem teenusekatkestus.

Entra Connecti on võimalik ka ühe serveriga juurutada, kuid siis on oluline, et vastavad riskid on kaardistatud.



Sünkroniseeritud identiteedimudel

Eelised

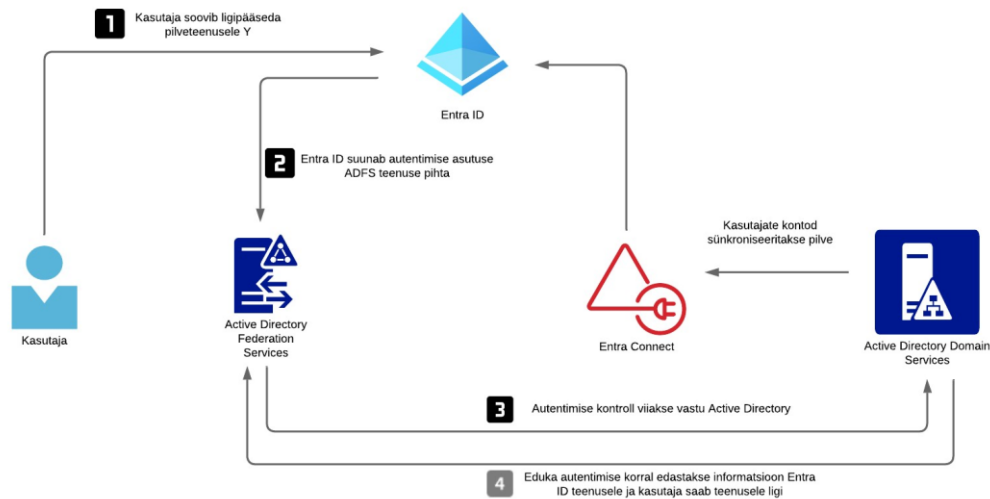
- Kasutajal on sama kasutajanimi ja parool
- Hea lahendus ettevõttele, kus on olemas oma majasisesed domeenikontrollerid, ning soovitakse kasutada sama kasutajanime ja parooli nii kohalike, kui ka pilveteenuste ressursside ligipääsemiseks ja kasutamiseks.

Miinused

- Parooli räsid tuleb sünkroniseerida Entra ID teenusesse. Tegemist ei pruugi olla miinusega, kui see risk on aktsepteerinud.
- Võrreldes pilv ainult mudeliga tuleb lisada juurde minimaalselt vähemalt üks lisa server Entra Connect jaoks

6.1.3 Federeeritud identiteedi mudel

Federeeritud identiteedi mudeli puhul on tegemist kõige kallima ja keerukama lahendusega. Federeeritud identiteedi kasutuselevõtuks on vaja nelja erinevat serverit ja koormusjaotureid. Esimese asjana tuleb seadistada Active Directory Federation Services ehk ADFS teenus ja peale seda saab sisse lülitada federeeritud identiteedi. ADFS keskkond peab olema kindlasti kõrge käideldavusega, sest selle mittetöötamise korral ei ole võimalik pilve teenustele ligi pääseda. Federeeritud identiteedi puhul puudub vajadus sünkroniseerida kasutajate parooli räsisid.



Federeeritud identiteedimudel

Eelised

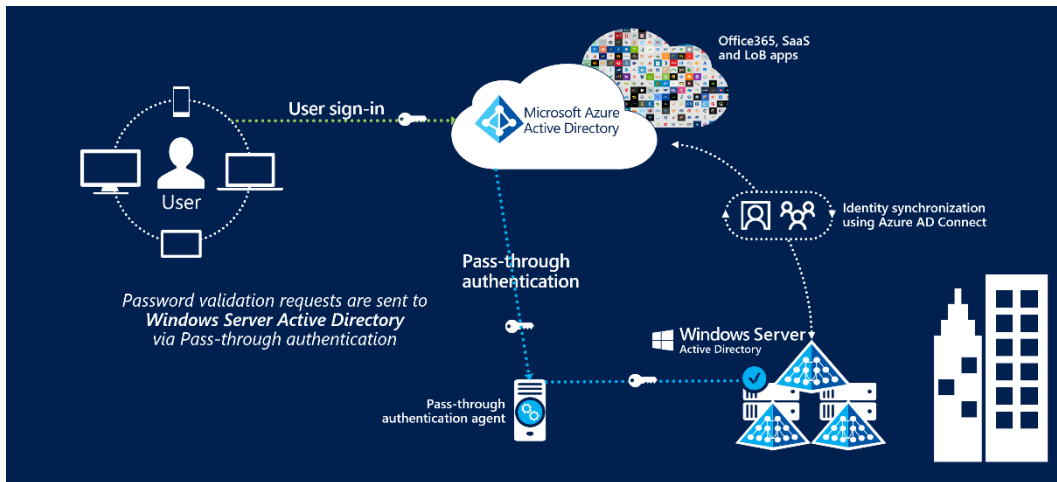
- Single Sign-On kasutamise võimalus pilveteenustele
- Pole vaja sünkroniseerida parooliräsisid pilve, kuid on soovitatav seda ikkagi teha juhuks, kui peaks midagi juhtuma ADFS taristuga
- Kasutaja parooli õigsust kontrollitakse vastu ettevõtte sisemist Active Directory-t

Miinused

- Kõige kallim identiteedi lahendus, kuna nõuab nelja lisaserveri ja koormusjaoturite paigaldust
- Nõuab palju seadistamist ja käideldavuse monitooringut
- Internetist on nähtav kõigile ettevõtte ADFS teenus. Tegemist on potentsiaalse sihtmärgiga, mida võivad küberkurjategijad soovida rünnata.

6.1.4 Pass-Through Authentication

Pass-Through Authentication ehk PTA identiteedi puhul on tegemist kõige uuema lahendusega. PTA lahenduse puhul on kasutusel hübriididentiteet, aga parooli kontrollitakse vastu ettevõtte sisemist Active Directory keskkonda, just nagu federeeritud identiteedi puhul. PTA on odavam, kui federeeritud lahendus, kuid see ei ole nii paindlik ja rohke funktsionaalsusega kui federeeritud identiteedimudel. Samas on see lihtsam ja turvalisem mudel, mida juurutada.



Pass-through Autentimise mudel

Eelised

- Lihtsam ja odavam kui federeeritud identiteet
- Võimaldab kontrollida kasutaja parooli vastu ettevõtte sisemist Active Directory teenust
- Võimaldab SSO (Seamless Single Sign-On).
- Võimalik juurutada ka tasuta Entra ID versioonide puhul

Miinused

- Ei paku 100% samasugust funktsionaalsust, kui federeeritud identiteedi mudel.

6.2 Hübriididentiteedi mudeli valimine

Analüüsisid neid nelja erinevat identiteedimudelit, mida Microsoft meile pakub, siis kõige mõistlikum oleks juurutada *Passthrough Authentication* identiteedimudelit.

Passthrough Authentication annab meile järgmised eelised

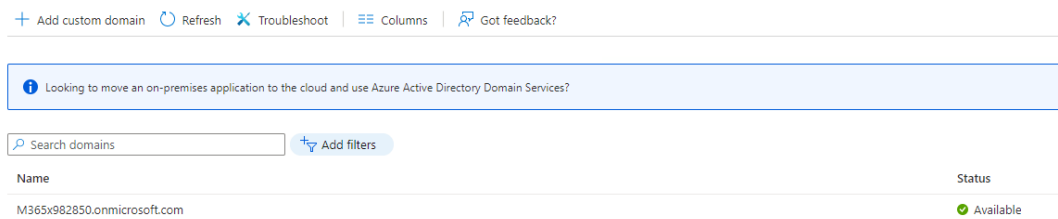
- Lihtsam ja odavam kui federeeritud identiteet
 - o Ei nõua lisa koormusjaoturite paigaldamist
 - o Koormusjaotust teeb Microsoft meie eest
- Turvaline
 - o Võimaldab kontrollida kasutaja parooli vastu ettevõtte sisemist Active Directory teenust
 - o Kasutaja kinni panek kohalikus Active Directories rakendub koheselt ka Entra ID teenuses
 - o Parooli räsivad ei pea sünkroniseerima
 - o Teenus ei ole internetist nähtav
 - o Ühildub kõigi teiste Entra ID pakutavate infoturbe teenustega
- Võimaldab SSO (Seamless Single Sign-On)

6.3 Hübriididentiteedi seadistamine

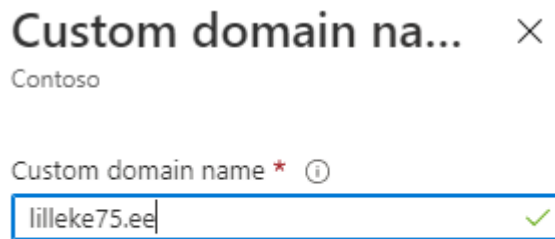
6.3.1 Ettevõtte domeeni lisamine Entra ID teenuses

Enne kui Te alustate domeeni lisamist on oluline, et Te kõigepealt lepite kokku erinevate osapooltega selle tegevuse läbiviimise. Ettevõtte domeeni lisamine Entra ID'ga eeldab, et Teil on õigusi lisada väliseid DNSi kirjeid. Entra ID's saate vastava unikaalse koodi ja kui see kood leitakse Teie ettevõtte DNSist, siis kinnitatakse vastav domeen ära.

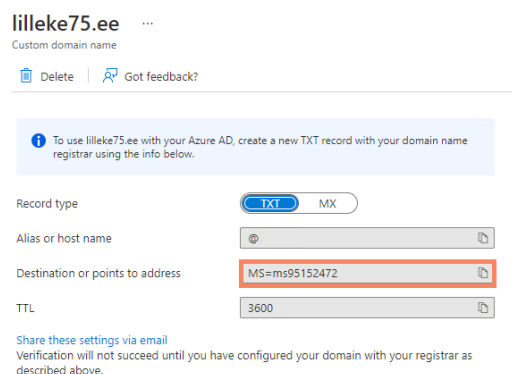
1. Ava **portal.azure.com** sulle väljastatud kontoga
2. Azure portaalis olles valige **Entra ID**
3. Entra ID konfiguratsiooni paneelist valige **Custom domain names**
4. Vaikimisi on Teie Entra ID's juba Teie ettevõtte teenuse domeeni nimi. Tegemist on unikaalse nimega.



5. Valige **+Add custom domain**
6. Sisestage oma ettevõtte domeeni nimi



7. Vajutage **Add domain**
8. Peale seda kuvatakse Teile informatsioon, mistuleb edastada välisele partnerile või kui Teil on endal vastavad õigused, siis lisage vastav **TXT** kirje oma välise domeeni DNSi. Teie keskkonnas on vastav väärtus teiste numbritega.

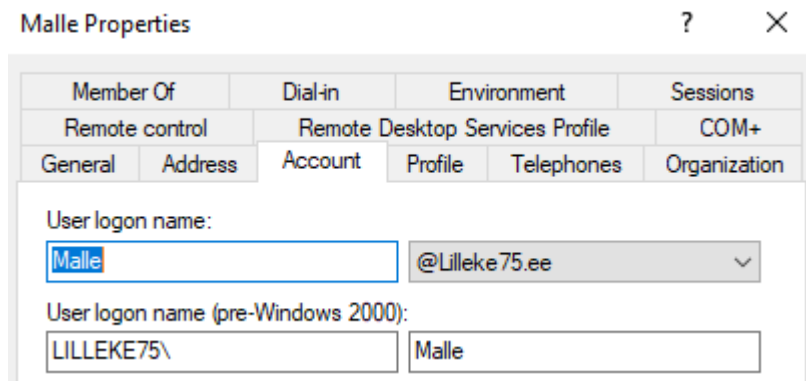


9. Kui vastav kirje on lisatud, siis oodake natuke ja vajutage **Verify**. Kui kohene kinnitus ei tööta, siis on vaja oodata kuni lisatud DNS kirjed replitseeruvad. Tehke paus ja proovige mõne aja pärast uuesti.
10. Kui Teie ettevõttel on rohkem kui üks domeen, siis järgige samasid juhiseid ka teiste domeenide puhul.

6.3.2 Active Directory lokaalse domeeni nimede kontroll ja muutmine

Selleks, et me saaksime kasutajaid sünkroniseerida Active Directorist pilve, peame me veenduma, et kasutajate domeeni nimi klapiks välise domeeniga. Kui kasutaja **User logon Name** (UPN) on täna näiteks Malle@lilleke75.local, siis seda ei ole võimalik pilve sünkroniseerida. Selleks, et seda kontot oleks võimalik ka pilvest kasutada, tuleks kasutajate **User Principal Name** muuta.

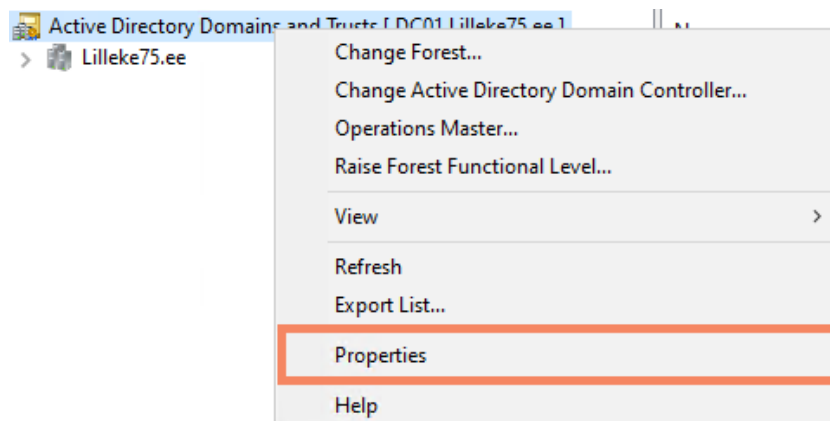
1. Avage **Active Directory Users and Computers**
2. Valige üks oma kasutajatest ja kontrollige kasutaja konto sätteid



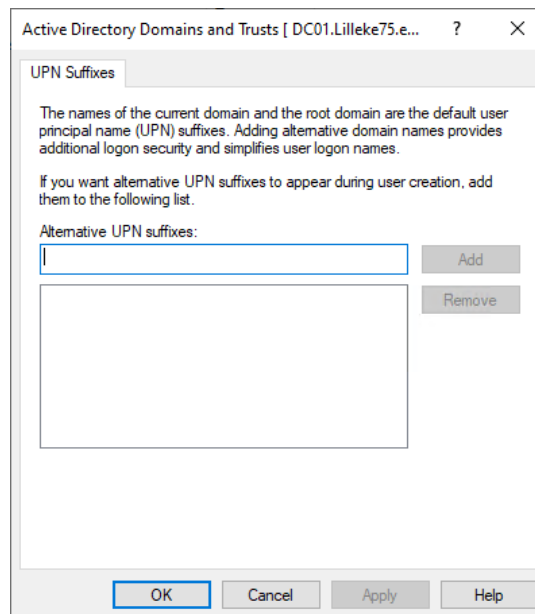
Kui kasutaja domeen kattub välise domeeniga, siis sellega muresid ei ole. Hea oleks vastav kontroll teha iga kasutaja osas, mida soovite pilve sünkroniseerida. Seda kontrolli saate teha edukalt läbi PowerShell.

Kui peaks selguma, et osadel kasutajatel on domeeniks midagi muud (näiteks **Lilleke75.local**), siis tuleb Teil väline domeen Active Directory's ära seadistada ja siis vastav muudatus teha. Selleks tuleks teha järgmised sammud:

1. Avage **Active Directory Domains and Trusts**
2. **Active Directory Domains and Trusts** tööriistas tehke parem hiireklahv ja valige **Properties**

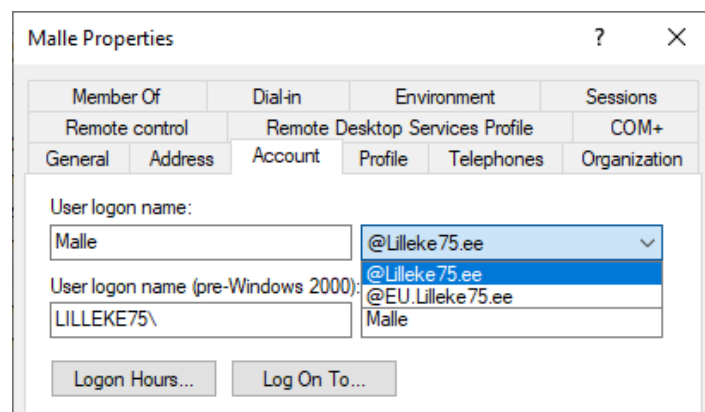


3. **UPN Suffixes** aknas sisestage kõik oma välised domeeni nimed, mida Te soovite kasutajatele määrata



4. Vajutage **OK**

Kui vastavad domeenid on lisatud, siis on Teil võimalik määrata uus domeen ka kasutajatele.



Enne kui antud muudatust tegema hakkate, siis on vaja välja selgitada kõikvõimalikud seosed selle sisemise domeeni nimega. Kui Teil on mingid vanad rakendused või teenused, mis kontrollivad ainult seda esialgset domeeni, siis võivad taolised teenused katki minna. Valmistage ette pilootgrupp, tehke muudatusi gruppide kaupa ja monitoorige. Kui avastate, et midagi läks katki, siis muudke kasutaja UPN tagasi. Sellises olukorras tuleks analüüsida, kuidas edasi saab minna. Microsoftil on ka teisi seadistamise variante, kui see variant Teie ettevõttele ei sobi.

6.3.3 TLS 1.2 seadistamine Entra Connect serveris

Järgmiste sammude puhul eeldame, et olete paigaldanud uue serveri Entra Connect teenuse jaoks. Entra Connecti ei tohi paigaldada Domeenikontrolleritesse, Active Directory Federation Services (ADFS) serveritesse, Web Application Proxy ega ka Exchange serverisse. Kasutada tuleb eraldi serverit.

Juhendis kasutame **AADC01** serveri nime Entra Connect jaoks. Entra Connect serverit tuleb kaitsta nagu kõiki Microsofti identiteedi servereid.

1. Logige sisse **Entra Connect** serverisse

2. Juhendiga kaasas olevast skriptide kataloogist võtke **Enable-TLS1.2.ps1** PowerShell skript ja kopeerige see serverisse. Tegemist on skriptiga, mis seadistab TLS 1.2
3. Avage **PowerShell** administraatori õigustega
4. Käivitage **Enable-TLS1.2.ps1** PowerShell skript. Peale seda peaksite nägema taolist teadet

```
Administrator: Windows PowerShell
PS C:\Skriptid> Get-ExecutionPolicy
RemoteSigned
PS C:\Skriptid> .\Enable-TLS1.2.ps1
TLS 1.2 has been enabled. You must restart the Windows Server for the changes to take affect.
PS C:\Skriptid>
```

5. Tehke serverile **restart**

6.3.4 Active Directory haldustööriistade paigaldamine

1. Logige sisse **Entra Connect** serverisse
2. Avage **PowerShell** administraator õigustega ja käivitage järgmine käsk
 - a. **Install-WindowsFeature -Name RSAT-AD-PowerShell,RSAT-ADDS -IncludeAllSubFeature**
3. Peale edukat paigaldust peaksite nägema taolist teadet

```
PS C:\Users\administrator.LILLEKE75> Install-WindowsFeature -Name RSAT-AD-PowerShell,RSAT-ADDS -IncludeAllSubFeature
Success Restart Needed Exit Code Feature Result
-----
True No Success {Remote Server Administration Tools, Activ...
```

6.3.5 Teenustekontode loomine Entra Connect teenusele

Entra Connect jaoks on meil vaja luua kaks erinevat kontot:

- Hallatud teenusekonto (Group Managed Service Account) Entra Connect teenuse jaoks
- Tavaline Active Directory konto informatsiooni lugemiseks, muutmiseks ja kirjutamiseks. Vastavad õigused tuleb kõik ise delegeerida. Õiguste seadistamisel tuleb lähtuda millist funktsionaalsust Te kasutusele soovite võtta.

Hallatud teenusekontod eeldavad, et Domeenikontrolleritesse on loodud peavõti (Root Key). Peavõtit kasutatakse hallatud teenusekontodele paroolide genereerimiseks ja ilma selleta ei ole võimalik ka neid kontosid luua. Peavõtme olemasolu saab kontrollida **Get-KdsRootKey** PowerShell'i käsuga. Kui vastav PowerShell'i käsk ei tagasta midagi, siis peavõtit ei eksisteeri teie Active Directory keskkonnas.

```
PS C:\Users\administrator.LILLEKE75> Get-KdsRootKey
AttributeOfwrongFormat :
KeyValue                : {219, 83, 19, 124...}
EffectiveTime           : 08.12.2021 16:43:58
CreationTime            : 09.12.2021 02:43:58
IsFormatValid           : True
DomainController        : CN=DC01,OU=Domain Controllers,DC=Lilleke75,DC=ee
ServerConfiguration     : Microsoft.KeyDistributionService.Cmdlets.KdsServerConfiguration
KeyId                   : 0f442d1b-2106-7fb5-0bdd-54d9a1a35d93
VersionNumber           : 1
```

Get-KdsRootKey väljund

Kui on selgunud, et peavõti on puudu, siis tuleb see luua vastava käsuga

1. Logige sisse **Entra Connect** serverisse

2. Avage **PowerShell** administraator õigustega ja käivitage järgmine käsk
3. **Add-KdsRootKey -EffectiveTime ((Get-Date).AddHours(10))**Nüüd tuleb oodata 10 tundi ja siis saate jätkata järgmiste tegevustega

Hallatud teenusekonto loomiseks järgige järgmisi samme

1. Logige sisse **Entra Connect** serverisse
2. Juhendiga kaasas olevast skriptide kataloogist võtke **Entra Connect-GMSAKontoLoomine.ps1** PowerShell skript ja kopeerige see serverisse.
3. Avage vastav skript **PowerShell ISE**´ga (administraator õigustes)
4. Vajadusel muutke **\$GMSATeenuseKontoNimi** muutuja väärtust. Selle skripti järgi luuakse **GMSA-AADC01** nimeline teenusekonto. Kui Teie serveri nimi on teine, siis muutke see vastavaks oma keskkonnale

```
1 #Azure AD Connect serveri nimi
2 $AzureADConnectServer1 = $env:COMPUTERNAME
3 $DomeeniNimi = (Get-ADDomain).DnsRoot
4 $GMSATeenuseKontoNimi = "GMSA-AADC01"
5
```

5. Veenduke, et kõik klappib Teie keskkonnaga
6. **Käivitage** skript
7. Käivitage järgmine käsk veendumaks, et konto loodi edukalt
 - a. **Get-ADServiceAccount -Identity "GMSA-AADC01"**
8. Järgmiseks käivitage järgnev käsk, et teenusekonto paigaldada **AADC01** serverisse
 - a. **Install-ADServiceAccount -Identity "GMSA-AADC01"**
9. Käivitage järgmine käsk veendumaks, et vastava konto paigaldamine oli edukas
 - a. **Test-ADServiceAccount -Identity "GMSA-AADC01"**

Active Directory lugemiseks, kirjutamiseks ja muutmiseks tuleb luua vastav konto. Konto loomiseks järgige järgmisi samme

1. Logige sisse **Entra Connect** serverisse
2. Juhendiga kaasas olevast skriptide kataloogist võtke **Entra ID - Connect-ADKontoLoomine.ps1** PowerShell skript ja kopeerige see serverisse.
3. Avage vastav skript **PowerShell ISE**´ga (administraator õigustes)
4. **Entra ID - Connect-ADKontoLoomine.ps1** PowerShell skript teeb järgmisi tegevusi:
 - a. Genereerib suvalise parooli
 - b. Prindib genereeritud parooli ekraanile
 - c. Loob uue tavalise Active Directory konto Teie keskkonda. Skript eeldab, et Te täpsustakse millisesse Organizationl Uniti (OU) alla see luuakse.
5. Skripti sees muutke järgmisi ridu
 - a. Rida **12, 13** ja **14**. Muutke need vastavalt Teie ettevõtte reeglitele

```

10 #Uue konto loomine
11 $ADAADKontoAndmed = @{
12     Name = "SVC-AADC" # Teenusekonto nimi. Muutke vastavalt Teie asutuse nimestandardile
13     Path = "OU=Teenusekontod,OU=Tase-0,OU=Lilleke75,DC=Lilleke75,DC=ee" #Kopeerige vastav distinguishedName oma Active Directorist.
14     SamAccountName = "SVC-AADC" # Teenusekonto nimi. Muutke vastavalt Teie asutuse nimestandardile
15     Description = "Azure AD Connect teenusekonto"
16     AccountPassword = $kontoParool
17     Enabled = $True
18 }

```

6. Veenduke, et kõik klapi Teie keskkonnaga
7. Käivitage skript
8. Peale seda peaks Teie Active Directories olema **SVC-AADC** nimeline teenusekonto

6.3.6 Entra Connect paigaldamine ja seadistamine

1. Laadige alla **Entra Connect** (vana nimega Azure AD Connect) paigaldusfail
 - a. <https://www.microsoft.com/en-us/download/details.aspx?id=47594>
2. Kopeerige **AzureADConnect.msi** Entra Connect serverisse
3. Käivitage **AzureADConnect.msi**
4. **Entra Connect Welcome** lehel kinnitage, et Te olete tingimustega nõus ja vajutage **Continue**
5. **Express Settings** lehel vajutage **Customize**. Ekspress paigaldust soovitate teha ainult laboris ja mitte tootmise keskkonnas. Ekspress paigaldus loob teenusekonto ja seadistab kõik vastavad õigused Teie eest. Tegemist on küll lihtsama viisiga, kuidas Entra Connect paigaldada aga selle tõttu ei saa te määrata konto nimesid ega ka kuidas õigusi jagatakse täpselt.
6. **Install required Components** lehelt valige „*Use an existing service account*“
 - a. Teenusekonto tüübiks valige **Managed Service Account**
 - b. Sisestage Service Account Name väljale: **lilleke75\GMSA-AADC01\$** (Teie ettevõttes on teine domeen ja kasutaja)
 - c. **Service Account Password** väli jätke tühjaks

Install required components

No existing synchronization service was found on this computer. The Azure AD Connect synchronization service will be installed. ?

Specify a custom installation location

Use an existing SQL Server

Use an existing service account

Managed Service Account

Domain Account

SERVICE ACCOUNT NAME

SERVICE ACCOUNT PASSWORD

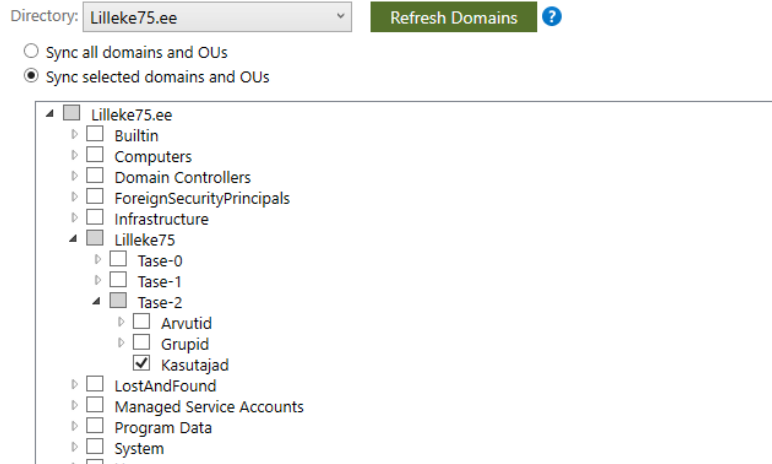
Specify custom sync groups

Import synchronization settings ?

Hallatud teenusekonto informatsiooni sisestamine

7. Vajutage **Install**
8. **User Sign-in** lehel valige Teie ettevõttes kokkulepitud identiteedi mudel. Selles juhendis me seadistame **Pass-through authentication** mudeli koos **Single Sign-On** funktsionaalsusega.
9. Lülitage sisse **Enable Single Sign-On** funktsionaalsus ja vajutage **Next**
10. **Connect to Entra ID** lehel sisestage **Entra ID Global** administraatori konto ja vajutage **Next**
11. **Connect your directories** valige oma Active Directory mets (forest) mida soovite liidestada ja vajutage **Add Directory**
12. **AD forest account** lehel valige „**Use existing AD account**“ ja sisestage eelnevalt loodud Active Directory teenusekonto informatsioon:
 - a. **Domain Username:** lilleke75\SVC-AADC
 - b. **Password:** PowerShelliga genereeritud parool
13. Vajutage **OK**
14. Vajutage **Next**
15. **Entra ID sign-in configuration** lehel kontrollige üle, et Te näete oma ettevõtte domeene ja vajutage **Next**
16. **Domain and OU filtering** lehel valige ainult need **Organizational Unitid** mida on vaja sünkroniseerida. Kogu Active Directory sisu ei pea kindlasti ega ka tohiks sünkroniseerida. Kui tänane Active Directory puu on sassis ja korrastamata, siis tuleks see eelnevalt korda teha ja siis alles jätkata.

Domain and OU filtering



17. Vajutage **Next**
18. **Uniquely identifying** your users lehel vajutage **Next**
19. **Filter users and devices** vajutage **Next**
20. **Optional features** lehel on Teil võimalik seadistada täiendavat funktsionaalsust. Nende lisade seadistamist saab alati ka hiljem teha ja kõik sõltub Teie projekti skoobist. Kindlasti soovitame juurde lugeda ka ametliku dokumentatsiooni nende lisada osas.
 - a. Exchange hybrid deployment
 - b. Exchange Mail Public Folders
 - c. Entra ID app and attribute filtering
 - d. Password hash synchronization
 - e. Password writeback
 - f. Group writeback
 - g. Device writeback
 - h. Directory extension attribute sync
21. Vajutage **Next**
22. **Enable Single Sign-On** lehel valige **Enter Credentials** ja sisestage **Active Directory** domeeniadministraatori konto

Enable single sign-on

Enter a domain administrator account to configure your on-premises forest for use with single sign-on. ?

Lilleke75.ee Enter credentials ✓

23. Vajutage **Next**
24. **Ready to configure** lehel kontrollige üle sisestatud informatsioon ja valitud sätted ja vajutage **Install**

Ready to configure

Once you click Install, we will do the following:

- Configure synchronization services on this computer
- Install Microsoft Azure AD Connect Authentication Agent for Pass-Through Authentication
- Enable Pass-through authentication
- Enable single sign-on
- Configure Source Anchor Attribute
- Configure M365x982850.onmicrosoft.com - AAD Connector
- Configure Lilleke75.ee Connector
- Disable Password hash synchronization
- Enable Azure AD Export Deletion Threshold (500)

Start the synchronization process when configuration completes.

Enable staging mode: When selected, synchronization will not export any data to AD or Azure AD.

25. Kui kõik läks edukalt siis Te peaksite nägema **Configuration complete** teadet.

26. Vajutage **Exit**

27. Logige välja ja uuesti sisse **Entra Connect** serverisse. Kui Te seda ei tee, siis Te ei saa ka Entra Connect sätteid muuta.

6.3.7 Entra Connect õiguste seadistamine

Entra Connectiga tuleb kaasa täiendav PowerShell'i moodul nimega **ADSyncConfig**. Selles moodulis on Teile ette tehtud PowerShell'i käsud, millega Te saate Entra Connect teenusekontole anda hõlpsasti õigusi. **Entra Connect** seadistamisel ei seadistatud parooli räsede sünkroniseerimist või parooli tagasi kirjutamist Entra ID'ist maapealsesse Active Directory jne. Kõigi võimaluste kasutusele võtu soovi korral tuleb delegeerida täiendavaid õigusi. Neid õigusi saab delegeerida erinevatel tasemetel. Õiguste delegeerimist kõige kõrgemal tasemel soovitatakse vältida. Kõige kõrgema tasemel tuleb delegeerida ainult üks õigus ja selleks on parooli räsede sünkroniseerimine. Seda ei saa teha madalamatel tasemetel. Kõige kõrgema tasemel on õigused nagu **Replicating Directory Changes** ja **Replicating Directory Changes All**.

Alumises skriptis on näidisedena välja toodud seadistamise võimalused. Alumisest skriptist on olulised read **11** ja **13**. **Set-ADSyncRestrictedPermissions** näiteks rakendab täiendavad turbe sätteid teenuse kontole, et ainult teatud Active Directory õigustega inimesed saavad seda kontod muuta jne. **Set-ADSyncBasicReadPermissions** annab **Entra Connect** töötamiseks miinimum õigused.

```

1 #Impordi Azure AD Connect AdSyncConfig moodul
2 Import-Module "C:\Program Files\Microsoft Azure Active Directory Connect\AdSyncConfig\AdSyncConfig.psm1"
3
4 #Get-Command -Module AdSyncConfig
5
6 #Küsime kohaliku domeeni nime ja defineerime teenusekonto nime
7 $DomeeniNimi = (Get-ADDomain).DnsRoot
8 $SADAADKonto = "SVC-AADC"
9 $SADAADKONTODN = "CN=SVC-AADC,OU=Teenusekontod,OU=Tase-0,OU=Lilleke75,DC=Lilleke75,DC=ee"
10
11 Set-ADSyncBasicReadPermissions -ADConnectorAccountName $SADAADKonto -ADConnectorAccountDomain $DomeeniNimi
12 #Käsu käivitamisel küsitakse kasutajanime ja parooli
13 Set-ADSyncRestrictedPermissions -ADConnectorAccountDN $SADAADKONTODN
14
15 #Azure AD Connect täiendav funktsionaalsuse seadistamine
16 Set-ADSyncExchangeHybridPermissions -ADConnectorAccountName $SADAADKonto -ADConnectorAccountDomain $DomeeniNimi
17 Set-ADSyncExchangeMailPublicFolderPermissions -ADConnectorAccountName $SADAADKonto -ADConnectorAccountDomain $DomeeniNimi
18 Set-ADSyncMsDsConsistencyGuidPermissions -ADConnectorAccountName $SADAADKonto -ADConnectorAccountDomain $DomeeniNimi
19 Set-ADSyncPasswordHashSyncPermissions -ADConnectorAccountName $SADAADKonto -ADConnectorAccountDomain $DomeeniNimi
20 Set-ADSyncPasswordWritebackPermissions -ADConnectorAccountName $SADAADKonto -ADConnectorAccountDomain $DomeeniNimi
21 Set-ADSyncUnifiedGroupWritebackPermissions -ADConnectorAccountName $SADAADKonto -ADConnectorAccountDomain $DomeeniNimi
22

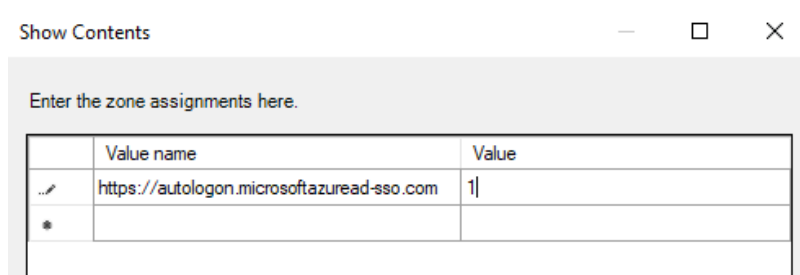
```

Juhendist leiate skripti nimega **Entra ID - Connect-ÕigusteSeadistamine.ps1**. Enne seadistamist tuleb tutvuda vastavate juhistega käskude kohta.

6.3.8 Grupipoliitika seadistamine

1. Logige sisse domeenikontrollerisse (Neid samme saate ka teha masinas, kuhu on paigaldatud grupipoliitika haldusvahendid)
2. Valige **Server Manager** ja sealt valige **Tools -> Group Policy Management**

3. **Group Policy Objects** peal tehke parem hiireklahv ja valige **New**
4. **New GPO** aknas sisestage uue grupipoliitika nimi, nt **Entra ID SSO**
5. Valige nimekirjast just loodud uus grupipoliitika **Entra ID SSO**
6. Tehke parem **hiireklahv** ja valige **Edit**
7. Avage seadistus **User Configuration -> Policies -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page**
8. Valige **Site to Zone Assignment List** seadistus
9. Lülitage sisse **Site to Zone Assignment List** seadistus ja vajutage Show
10. **Show Contents** lehel sisestage järgnev informatsioon



11. Vajutage **OK**
12. Avage seadistus **User Configuration -> Policies -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Intranet Zone**
13. Valige **Allow updates to status bar via script** seadistus ja lülitage see sisse
14. Vajutage **OK**
15. Sulgege **Entra ID SSO** grupipoliitika
16. Nüüd linkige **Entra ID SSO** grupipoliitika oma kasutajate OU'le

6.3.9 Entra Connect serveri täiendav turvamine

Entra Connect serverite turvamise osas soovime rakendada täiendavaid info turbe poliitikaid. Soovitused leiate järgmiselt lingilt:

- <https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-install-prerequisites#harden-your-microsoft-entra-connect-server>

6.3.10 Teise Entra Connect serveri seadistamine

Nüüd, mil Teil on olemas esimene Entra Connect server, soovime seadistada ka teise. Teise serveri seadistamine käib samamoodi, kuid viimases aknas tuleb valida „**Enable staging mode: When selected, synchronization will not export any data to AD or Entra ID**“. Vastava seadistusega tagatakse, et teisest Entra Connect serverist Entra ID´se midagi ei ekspordita, mis on omakorda vajalik andmekonfliktide vältimiseks.

Ready to configure

Once you click Install, we will do the following:

- Configure synchronization services on this computer
 - Install Microsoft Azure AD Connect Authentication Agent for Pass-Through Authentication
 - Enable Pass-through authentication
 - Enable single sign-on
 - Configure Source Anchor Attribute
 - Configure M365x982850.onmicrosoft.com - AAD Connector
 - Configure Lilleke75.ee Connector
 - Disable Password hash synchronization
 - Enable Azure AD Export Deletion Threshold (500)
- Start the synchronization process when configuration completes.
- Enable staging mode: When selected, synchronization will not export any data to AD or Azure AD.

Kui peaks juhtuma, et esimese serveri töös esineb tõrkeid, saate teise serveri lülitada primaarseks. Oluline on meeles pidada, et mõlemad serverid oleksid alati sama konfiguratsiooniga, mistõttu tuleb muudatused teha alati mõlemas serveris, mitte ainult peamises serveris.

7 Pilvepõhiste infoturvelahenduste juurutamine

Eesmärgid:

- Juurutada keskne pilvepõhine turbeinfo ja sündmuste haldussüsteem
- Koguda erinevate pilveteenuste logid keskselt kokku
- Suuta tuvastada anomaaliaid ja ründeid

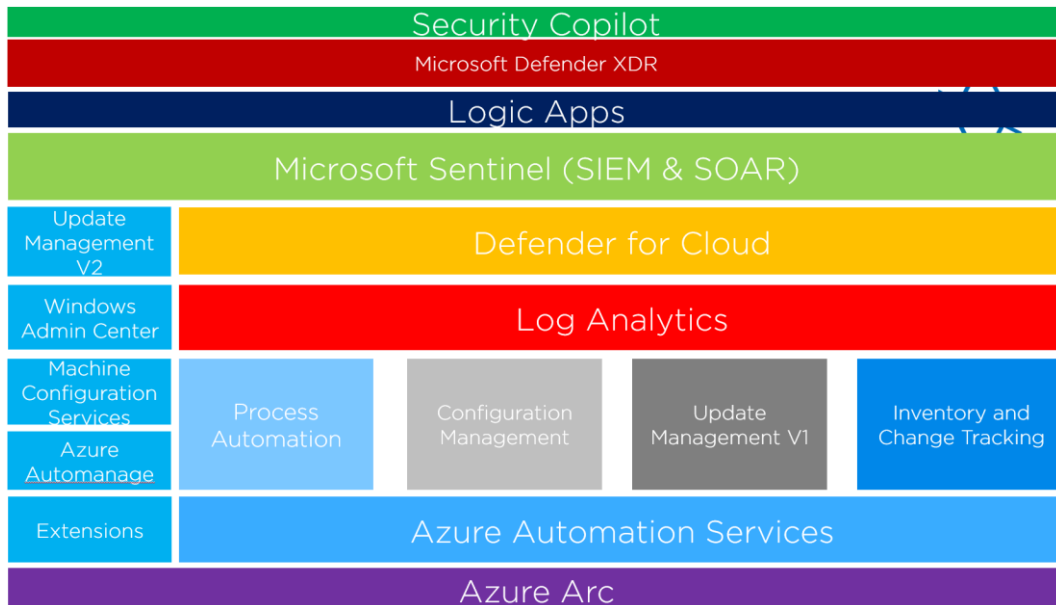
Eeltingimused:

- Ligipääs Microsoft'i Azure kulupõhiste (*consumption-based*) teenustele on olemas
 - 1 Azure subscription
- Entra ID Global administraatori õigused on olemas
- Nimede standardid ja teenuste sildid on kokku lepitud pilveteenuste objektidele
- Pilveteenuste piirkond, kuhu kulupõhiseid teenuseid võib paigaldada, on kokku lepitud
- Logide hoiu periood on kindlaks määratud
- Infoturbe emaili aadress, kuhu võib saata teavitusi, on seadistatud

7.1 Lahenduste ülevaade

Microsoft Entra ID ja Office 365 teenuste juurutamisel tuleb kasutusele võtta toetavaid infoturbe lahendusi. Nendes teenustes luuakse erinevates kogustes logisid, mida tuleb hoida ja analüüsida. Infoturbe seisukohas tulenevalt on võimalik luua erinevaid rünnakute tuvastuse reegleid, analüüsida trende ja anomaaliaid. Vajadusel saab vastata erinevatele rünnakutele automaatselt. Samuti võib logide kokku kogumine lihtsustada ettevõtte üleminekut pilveteenusele.

Infoturbe teenused:



7.1.1 Teenused

- **Azure Log Analytics**
 - o Keske teenus, kuhu on võimalik suunata ja hoiustada erinevaid pilveteenuste logisid
- **Microsoft Defender for Cloud**
 - o Pilvepõhine infoturbe teenus, mis analüüsib paigaldatud teenuste infoturbe taset ja vastavust parimatele praktikatele. Teenus suudab tuvastada ka erinevaid rünnakuid.
- **Microsoft Sentinel**
 - o Pilvepõhine turbeinfo ja sündmuste haldussüsteem (TSHS), mille kaudu on võimalik hallata küberintsidente, analüüsida trende ja logisid, visualiseerida teenuste kasutust ja vajadusel reageerida intsidentidele automaatselt.
- **Azure Automation**
 - o Azure Automation pakub nelja erinevat teenust
 - Protsessi automatika
 - Konfiguratsioonihaldus
 - Turvauuenduste haldus
 - Inventuuri ja muudatuste haldus
 - o Administraatorina on võimalik läbi protsessi automatika mooduli automatiseerida oma igapäevaseid tegevusi.
- **Microsoft Defender XDR (Extended Detection and Response)**

- Tegemist on integreeritud turvaplatvormiga, mis ühendab endas mitmeid Microsofti infoturbe lahendusi, sealhulgas Defender for Identity, Defender for Endpoint, Defender for Cloud Apps ja Defender for Office 365. Selle platvormi peamine eesmärk on pakkuda terviklikku kaitset ja paremat nähtavust läbi kogu ettevõtte digitaalse ökosüsteemi, hõlmates nii maapealseid kui ka pilvepõhiseid ressursse.
- **Azure Arc**
 - Hübridipilvedele mõeldud taristuteenus, millega on võimalik laiendada Azure funktsionaalsust erinevatesse pilvedesse.

Neid teenuseid on võimalik kasutusele võtta erinevates andmekeskustes ja / või pilvedes. Nende lahenduste kasutuselevõtt ei eelda VPN ühenduste loomist Azure ja enda andmekeskuste vahel.

Selles konkreetses juhendis keskendume eelkõige järgmistele lahendustele:

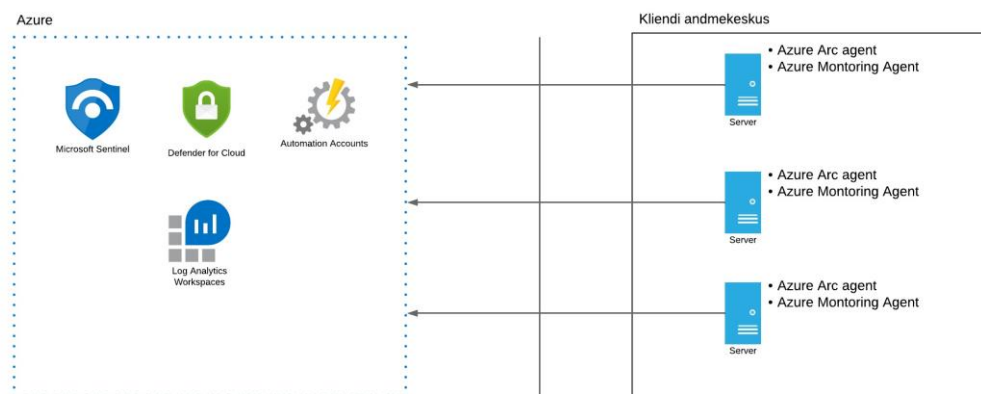
- **Azure Log Analytics**
- **Microsoft Defender for Cloud**
- **Microsoft Sentinel**
- **Azure Automation**

Kui ettevõttel on soov Entra ID, Office 365 jt logisid tuua oma andmekeskusesse, siis on soovitatav need kõigepealt suunata kõik kokku Log Analytics teenusesse ja sealt luua vajalikud ekspordi reeglid.

Ekspordi reeglite kohta saab täpsemalt lugeda siit: <https://docs.microsoft.com/en-us/azure/azure-monitor/logs/logs-data-export?tabs=portal>

Teise võimalusena saab kasutusele võtta Microsofti Sentinel keskse logihoiu teenuse ja liidestada sinna ka kriitilisemate teenuste logid, näiteks maapealne Active Directory, Exchange server jne. Sellisel juhul on võimalik saada terviklik pilt oma keskkonnast.

Microsofti Sentinel'i kasutuselevõtuks tuleks Azure Arc agent paigaldada koos vastavate laiendustega, et logid saada maapealsetest teenustest Sentineli.



Hübridpilve monitorooring

7.1.2 Teenuste asukoht

Kulupõhiste teenuste kasutuselevõtul tuleb alati määrata andmekeskuse geograafiline piirkond. Enne teenuste paigaldamist leppige kokku, millised piirkonnad on lubatud. Vaikimisi pakub Microsoft asukohale lähimat piirkonda, mis on ka soovitatav.

Juhendis paigaldakse kõik teenused ida Euroopa piirkonda (West Europe region).

7.1.3 Nimede standard

Teenuste paigaldamise ajal küsitakse erinevatele objektidele nimesid. Eelnevalt tuleks seega sisemiselt kokku leppida, kuidas Azure's erinevaid objekte nimetama hakatakse. Kui nimetused ei ole standardiseeritud, siis on keskkonda raske hallata, mis omakorda võib hiljem tekitada segadust. Kõige lihtsam on Excel'it kasutades vastavad objektid ära kirjeldada.

Järgnevalt üks näide, kuidas saab objekte nimetada. Siinkohal on tegemist ressursigrupiga

- **RG-PROD-IT-AZ-SECURITY-WE**
 - o **RG** – Ressursigrupp
 - o **PROD-IT** – IT-osakond, tootmises oleva teenusega (mitte test või arendus)
 - o **AZ-SECURITY** – Azure infoturbe lahendused
 - o **WE** – West Europe

7.1.4 Teenuste sildistamine

Kulupõhiste teenuste paigaldamisel küsitakse siltide (*tags*) lisamist. Tegemist ei ole kohustusliku väljaga, ent soovituslik on seda siiski teha. Võimalik on lisada näiteks raamatupidamise kulukoodid, teenuseomanik(ud), kas tegemist on arenduse või testiga jne. Siltide lisamine lihtsustab aruandlust ja haldust.

Basics **Tags** Review + create

Apply tags to your Azure resources to logically organize them by categories. A tag consists of a key (name) and a value. Tag names are case-insensitive and tag values are case-sensitive. [Learn more](#) ↗

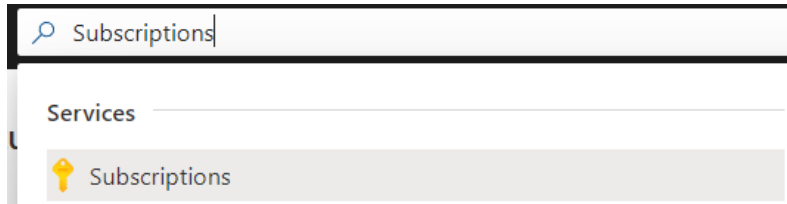
Name ⓘ	Value ⓘ	Resource
<input type="text"/>	: <input type="text"/>	Resource group

Siltide lisamine teenustele

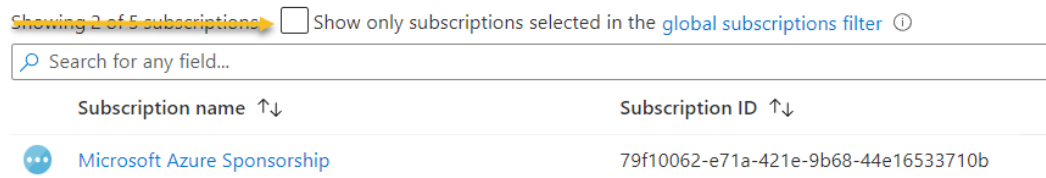
7.2 Õiguste ja Azure Subscription'i kontrollimine

Ettevõttele väljastatud Azure subscriptioni(te) olemasolu on võimalik kontrollida Azure portaali kaudu. Oluline on vältida kõigi teenuste paigaldamist ainult ühe subscriptioni alla. Erinevad teenused tuleks erinevate subscriptionite alla lisada, et oleks võimalik neid lihtsasti eristada ja saada parem ülevaade teenuste kuludest. Infoturbe lahenduste jaoks on siiski mõistlik kasutada ühte subscriptionit, sest nende toodete omavahelised seosed on väga tugevad.

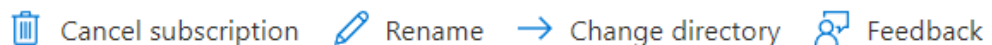
1. Ava **portal.azure.com** sulle väljastatud kontoga
2. Azure portaalis trükkige otsingusse „**Subscriptions**“



3. Valige **Subscriptions**
4. Kui **Show only subscriptions selected in the global subscriptions filter** on valitud, siis eemaldage sealt linnuke



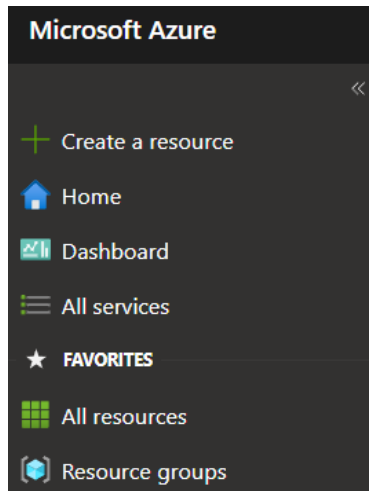
5. Vastavalt lepingule võib subscriptionil olla vaike nimi, nagu nt „**Microsoft Azure Enterprise**“. Subscription'i nimi tuleks kindlasti ära muuta. Vastasel korral järgnevate subscriptionite lisamisel on neil kõigil sama nimi.
6. Selleks valige nimetatud subscription.
7. Menüüist valige **Rename** ja andke vastav nimi, nt „**Azure infoturbe ja halduslahendused**“



7.3 Ressursigruppide loomine

Selleks, et Azure kulupõhiseid teenuseid saaks paigaldada, on vaja luua ressursigrupp. Ressursigrupp on virtuaalne konteiner, kuhu saab paigaldada erinevaid teenuseid ja vastavalt ressursigruppidele ka õigusi delegerida erinevatele inimestele. Paigalduse puhul on oluline jälgida teenuste asukohta. Azure lubab teenuseid paigaldada erinevatesse piirkondadesse ja vaike sätete puhul võivad teenused sattuda ka valesse kohta.

1. Azure portaalis olles vali **Resource Groups**

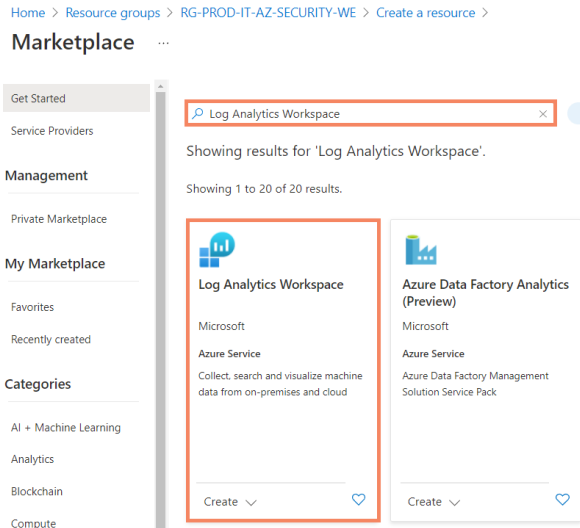


2. Vali **+Create**
3. Uue ressursigrupi loomisel täida ära järgmised väljad:
 - a. **Subscription:** Azure infoturbe ja halduslahendused
 - b. **Resource Group:** RG-PROD-IT-AZ-SECURITY-WE
 - c. **Region:** (Europe) West Europe
4. Vajuta **Next**
5. **Tags** lehel saate lisada kokkulepitud sildid. Vajutage **Next**
6. **Review +create** lehel kontrollige üle sisestatud informatsioon ja vajutage **Create**
7. Nüüd peaks teil olema **RG-PROD-IT-AZ-SECURITY-WE** ressursigrupp

7.4 Azure Log Analytics teenuskeskkonna paigaldamine

7.4.1 Log Analytics teenuskeskkonna paigaldamine

1. Azure portaalis olles vali **RG-PROD-IT-AZ-SECURITY-WE** ressursigrupp
2. Vali **+Create**
3. Pilveteenuste poest otsida teenus nimega „**Log Analytics Workspace**“

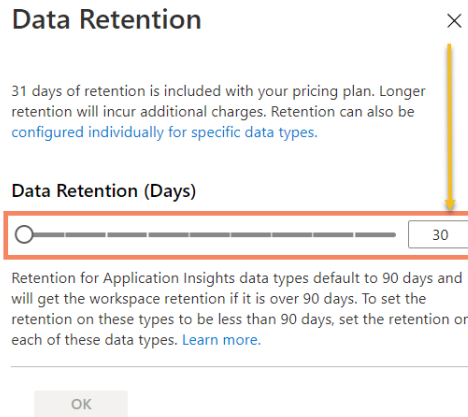


4. Vali **Create** -> **Log Analytics Workspace**
5. **Create Log Analytics workspace** lehel tuleb täita järgmised väljad:
 - a. **Subscription:** Azure infoturbe ja halduslahendused
 - b. **Resource Group:** RG-PROD-IT-AZ-SECURITY-WE
 - c. **Instance details:**
 - i. **Name:** AZ-PROD-IT-LOG-ANALYTICS-WE
 - ii. **Region:** West Europe
6. Vajutage **Next**
7. Sisestage kokkulepitud sildid ja vajutage **Next**
8. Kontrollige sisestatud informatsiooni õigsust ja vajutage **Create**
9. Nüüd peaks teil olema **AZ-PROD-IT-LOG-ANALYTICS-WE** Azure Log Analytics Workspace

7.4.2 Logide säilitamise muutmine

Vaikimisi hoitakse logisid kuni 30 päeva. Halduse ja infoturbe vaates on see liialt lühike periood. Analüüsi oma vajadusi ja seadistage vastav päevade arv.

1. Azure portaalis olles vali **RG-PROD-IT-AZ-SECURITY-WE** ressursigrupp
2. Valige **AZ-PROD-IT-LOG-ANALYTICS-WE** Log Analytics Workspace
3. **AZ-PROD-IT-LOG-ANALYTICS-WE** konfiguratsiooni paneelil valige **Usage and estimated costs**
4. Valige **Data Retention**
 - a. Sisestage kokkulepitud päevade arv.

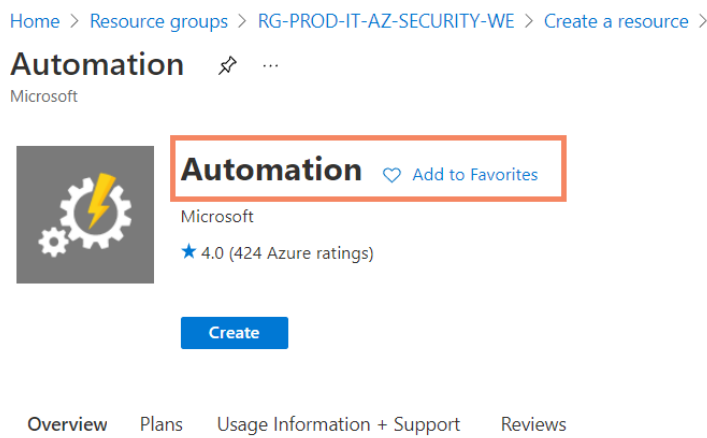


Logide hoiustamine

7.5 Azure Automation konto loomine

Samasse keskkonda tuleb paigaldada ka automaatikakonto. Automaatikakonto abil saab automatiseerida erinevaid tegevusi. Vajadusel saab kasutusele võtta ka teisi automaatikakonto teenuseid nagu Update Management, Change Tracking and Inventory ja Desired State.

1. Azure portaalis olles vali **RG-PROD-IT-AZ-SECURITY-WE** ressursigrupp
2. Vali **+Create**
3. Pilveteenuste poest otsida järgmine teenus nimega „**Automation**“



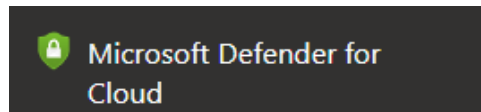
4. Vali **Create**
5. Create an Automation Account lehel täita ära järgmised väljad:
 - a. **Subscription:** Azure infoturbe ja halduslahendused
 - b. **Resource Group:** RG-PROD-IT-AZ-SECURITY-WE
 - c. **Instance details:**
 - i. **Automation Account Name:** PROD-IT-AUTOMATION-WE
 - ii. **Region:** West Europe
6. Advanced lehel jätke vaike sätted ja vajutage **Next**. Automaatikakontoga luuakse hallatud süsteemne teenusekonto. Selle kaudu on võimalik pääseda ligi teistele teenustele. Vaikimisi ei oma see teenus teistes teenustes õigusi.
7. **Networking** lehel jätke vaike sätted ja vajutage **Next**

8. Sisestage kokkulepitud sildid ja vajutage **Next**
9. Kontrollige sisestatud informatsiooni õigsust ja vajutage **Create**
10. Nüüd peaks teil olema **PROD-IT-AUTOMATION-WE** automaatikakonto

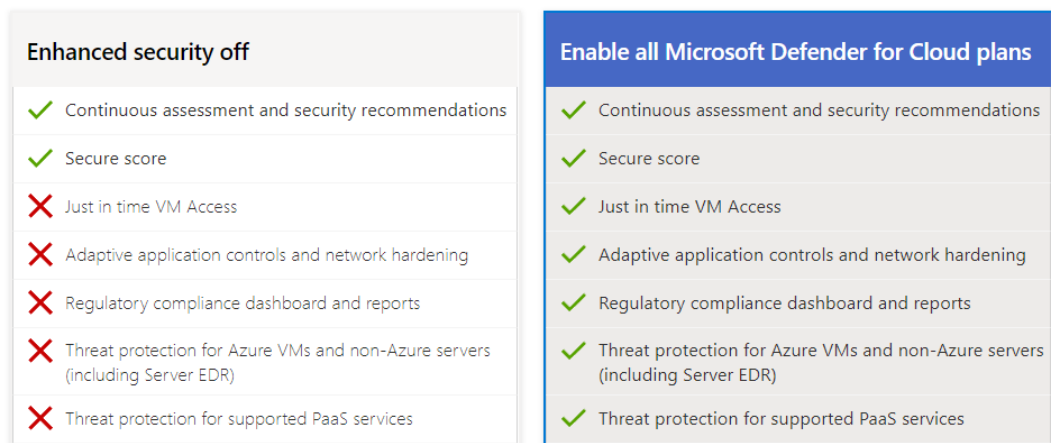
7.6 Microsoft Defender for Cloud teenuse seadistamine

7.6.1 Microsoft Defender for Cloud subscriptioni seadistamine

1. Azure portaalis olles valige Microsoft Defender for Cloud



2. **Microsoft Defender for Cloud** lehel valige **Environment settings**
3. Valige „**Azure infoturbe ja halduslahendused**“ subscription
4. Valige „**Enable All Microsoft Defender for Cloud plans**“ pakett



5. Teenuste osas jätke alles ainult **Servers** ja teised lülitage välja. Vajadusel ja võimaluste korral võite kasutusele võtta ka teised teenused

^ Select Defender plan by resource type **Enable all**

Microsoft Defender for	Resources	Pricing	Configuration	Plan
Servers	0 servers	\$15/Server/Month		On Off
App Service	0 instances	\$15/Instance/Month		On Off
Azure SQL Databases	0 servers	\$15/Server/Month		On Off
SQL servers on machines	0 servers	\$15/Server/Month \$0.015/Core/Hour		On Off
Open-source relational databases	0 servers	\$15/Server/Month		On Off
Storage	0 storage accounts	\$0.02/10k transactions		On Off
Containers	0 container registries: 0 kubernetes cores	\$7/VM core/Month		On Off
Key Vault	0 key vaults	\$0.02/10k transactions		On Off
Resource Manager		\$4/1M resource management operations		On Off
DNS		\$0.7/1M DNS queries		On Off

6. Vajutage **Save**
7. Valige **Auto provisioning** ja lülitage sisse järgmised sätted
 - a. **Log Analytics agent for Azure Arc Machines (preview)**
 - i. Valige **AZ-PROD-IT-LOG-ANALYTICS-WE** Log Analytics Workspace

- ii. Vajutage **Apply**
 - b. **Vulnerability assessment for machines**
 - i. Valige **Microsoft Threat and vulnerability management**
 - ii. Vajutage **Apply**
 8. Vajutage **Save**
 9. Valige **Email notifications**
 - a. Siin saab seadistada, keda infoturbe intsidendi korral tuleks teavitada
 10. Muudatuste tegemisel vajutage **Save**
 11. Valige **Integrations** ja veenduge, et mõlemad valikud oleksid seadistatud
 - a. Allow Microsoft Defender for Cloud Apps to access my data
 - b. Allow Microsoft Defender for Endpoint to access my data
 12. Valige **Continues Export** ja seadistage järgmised sätted
 - a. Valige **Log Analytics Workspace** paneel
 - b. Lülitage sisse järgmised eksport-reeglid
 - i. **Security recommendations**
 - ii. **Secure score**
 - iii. **Security Alerts**
 - iv. **Regulatory compliance**
 - c. Export frequency alt lülitage sisse mõlemad eksport-reeglid
 - i. **Streaming updates**
 - ii. **Snapshots (Preview)**
 - d. **Export configuration** alt valige **RG-PROD-IT-AZ-SECURITY-WE** ressursigrupp
 - e. **Export target** alt valige järgmised sätted
 - i. **Subscription**: Azure infoturbe ja halduslahendused
 - ii. **Select target workspace**: AZ-PROD-IT-LOG-ANALYTICS-WE
 13. Valige **Security policy**
 14. Vajutage **Add more standards** nupule
 15. **ISO 27001:2013** tagant valige add
 16. **ISO 27001:2013 Basic** lehel vajutage Next
 17. **Parameters** lehel vajutage Next
 18. **Remediation** lehel valige West Europe piirkond ja vajutage Next
 19. **Non-compliance messages** lehel vajutage Next
 20. **Review +create** lehel kontrollige informatsiooni õigsust ja vajutage **Create**
 21. Peale seda peaks **ISO 27001:2013** kontrollfunktsioonid keskkonda paigaldatud olema.

ISO 27001:2013

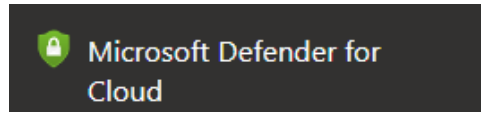
Track ISO 27001:2013 controls in the Compliance Dashboard, based on a recommended set of policies and assessments.

Manually added

Delete

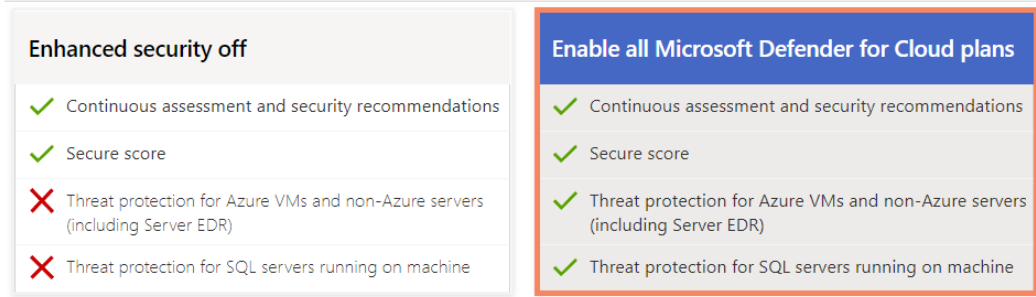
7.6.2 Microsoft Defender for Cloud Log Analytics Workspacce seadistamine

1. Azure portaalis olles valige **Microsoft Defender for Cloud**



2. **Microsoft Defender for Cloud** lehel valige **Environment settings**
3. Valige **AZ-PROD-IT-LOG-ANALYTICS-WE** workspace
4. **Defender plans** lehel valige „**Enable all Microsoft Defender for Cloud plans**“ pakett

[Enable the enhanced security features of Microsoft Defender for Cloud. Learn more >](#)



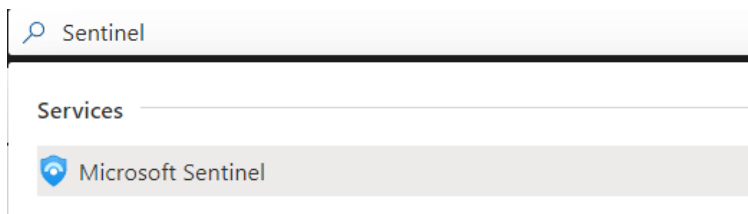
5. Lülitage teenus sisse ainult serveritele

Microsoft Defender for	Resources	Pricing	Plan
Servers	0 servers	\$15/Server/Month ⓘ	<input type="checkbox"/> On <input checked="" type="checkbox"/> Off
SQL servers on machines	0 servers	\$15/Server/Month ⓘ \$0.015/Core/Hour	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off

6. Vajutage **Save**
7. Valige **Data Collection**
8. Valige **Common** tase
9. Vajutage **Save**

7.7 Microsoft Sentineli teenuse aktiveerimine

1. Azure portaalis olles trükkige otsingusse „**Sentinel**“



2. Valige otsingust „**Microsoft Sentinel**“
3. **Microsoft Sentinel** lehel valige **Create Microsoft Sentinel**

4. **Add Microsoft Sentinel to a workspace** lehel valige **AZ-PROD-IT-LOG-ANALYTICS-WE** Log Analytics workspace
5. Vajutage **Add**
6. Mõne aja pärast peaks ilmema teade:

Microsoft Sentinel free trial activated

The free trial is active on this workspace from 12/8/2021 to 1/8/2022 at 11:59:59 PM UTC.

During the trial, up to 10 GB/day are free for **both Microsoft Sentinel and Log Analytics**. Data beyond the 10 GB/day included quantity will be billed. [Learn more.](#)

OK

Esimese 31 päeva vältel on Sentinel teenus tasuta ja andmete maht on limiteeritud 10 GB peale päevas. Log Analytics teenuse eest tuleb ikka maksta.

7.8 Microsoft Sentineli teenuse seadistamine

7.8.1 Tasuta andmete hoidlad Sentinelis

Sentineli on võimalik keskselt kokku koguda erinevat infot erinevatest andmehoidlatest. Järgmistest andmehoidlatest logide kogumise eest Microsoft raha ei küsi:

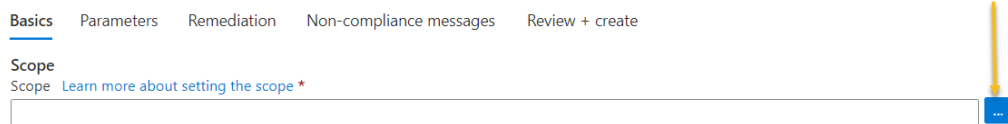
- **Azure Activity Logs**
- **Entra ID Identity Protection**
- **Office 365**
- **Microsoft Defender for Cloud**
- **Microsoft Defender for IoT**
- **Microsoft 365 Defender**
 - o Ainult intsidendid ja teavitused on tasuta
- **Microsoft Defender for Endpoint**
 - o Ainult intsidendid ja teavitused on tasuta
- **Microsoft Defender for Identity**
 - o Ainult intsidendid ja teavitused on tasuta
- **Microsoft Defender for Cloud Apps**
 - o Ainult intsidendid ja teavitused on tasuta

7.8.2 Andmehoidlate seadistamine

Vaikimisi ei koguta Sentineli mingit infot. Selleks, et Sentinel saaks tuvastada anomaaliaid ja erinevaid ründeid, on vaja seadistada andmehoidlad. Kogutud andmete põhjal on võimalik lisada erinevaid analüütika reegleid ja logisid analüüsida. Meeles tuleb pidada, et mitte kõik andmehoidlad ei ole tasuta.

1. Sentinel portaalis valige **Content Hub**
2. Otsige **Entra ID (Azure Active Directory)**.
 - a. Entra ID logide importimine Sentinelis ei ole tasuta ja selleks peab olema Entra ID 1 litsentsid kasutajatele.
3. Vajutage **Install** ja oodake natuke
4. Vajutage **Manage** nuppu

5. Valige **Entra ID** (Azure Active Directory) andmehoidla
6. Valige **Microsoft Entra ID**
7. Valige „**Open Connector Page**“
8. Lülitage sisse järgmiste logide import
 - a. **Sign-In Logs**
 - b. **Audit Logs**
 - c. **Non-Interactive User Sign-In Log (Preview)**
 - d. **Service Principal Sign-In Logs (Preview)**
 - e. **Managed Identity Sign-In Logs (Preview)**
 - f. **Provisioning Logs (Preview)**
 - g. **ADFS Sign-In Logs (Preview)**
 - h. **User Risk Events (Preview)**
 - i. **Risky Users (Preview)**
 - j. **Network Access Traffic Logs (Preview)**
 - k. **Risky Service Principals (Preview)**
 - l. **Service Principal Risk Events (Preview)**
9. Vajutage **Apply Changes** nuppu.
10. Minge tagasi „**Content Hub**“ lehele ja otsige **Microsoft 365**
11. Vajutage **Install** ja oodake natuke
12. Vajutage **Manage**
13. Valige Microsoft 365 andmehoidla
14. Vajutage **Open connector page** nuppu
15. Lülitage sisse järgmiste logide import
 - a. **Exchange**
 - b. **Sharepoint**
 - c. **Teams**
16. Vajutage **Apply Changes** nuppu
17. Minge tagasi „**Content Hub**“ lehele ja otsige **Azure Activity**
18. Vajutage **Install** ja oodake natuke
19. Vajutage **Manage**
20. Valige **Azure Activity** andmehoidla
21. Vajutage **Open connector page** nuppu
22. Vajutage **Launch Azure Policy Assignment wizard** nuppu
23. **Configure Azure Activity logs to stream to specified Log Analytics workspace** lehel valige „...“ (leitav Scope all)



24. Valige Azure infoturbe ja halduslahendused subscription ja **RG-PROD-IT-AZ-SECURITY-WE** ressursigrupp
25. Vajutage **Select**
26. Vajutage **Next**
27. **Parameters** lehel valige **AZ-PROD-IT-LOG-ANALYTICS-WE**
28. Vajutage **Next**
29. **Remediation** lehel valige **West Europe** region ja lülitage sisse **Create a remediation Task** seadistus

Create a remediation task ⓘ

Policy to remediate

Configure Azure Activity logs to stream to specified Log Analytics workspace

30. Vajutage **Next**
31. **Non-compliance** lehel vajutage **Next**
32. **Review + create** lehel kontrollige sisestatud informatsiooni õigsust ja vajutage **Create**
33. Minge tagasi andmehoidlate lehele ja valige **Microsoft Defender for Cloud**
34. Vajutage **Open connector page** nuppu
35. **Subscription** nimekirjast valige **Azure infoturbe ja halduslahendused** subscription ja ühendage see Sentineliga.



36. Minge tagasi andmehoidlate lehele ja valige **Microsoft Defender for Cloud Apps**
37. Vajutage **Open connector page** nuppu
38. Lülitage sisse **Alerts** tüüpi logide import
39. Vajutage **Apply Changes**
40. Minge tagasi andmehoidlate lehele ja valige **Azure Active Directory Identity Protection**
41. Vajutage **Connect** nuppu

7.8.3 Entity Behavior Analytics seadistamine

Entity Behavior Analytics on eraldi funktsionaalsus Sentinelis, mis tegeleb kokku kogutud informatsiooni automaatse analüüsiga. Hetkel toetab konkreetne funktsionaalsus nelja erinevat andmehoidlat.

1. **Sentinel** portaalis valige **Settings**
2. **Settings** lehelt valige **Settings**
3. **Entity behavior Analytics** alt vajutage **Set UEBA** nuppu
4. **Lülitage** UEBA funktsionaalsus sisse ja seadistage järgmised andmehoidlad:

- a. **Active Directory** (Eeldab Defender for Identity teenust)
 - b. **Entra ID**
 - c. **Audit Logs**
 - d. **Signin Logs**
 - e. **Azure Activity Logs**
 - f. **Security Events** (Logid mis tulevad ettevõtte serveritest. Vaikimisi kogutakse üldistest logidest kokku 140+ erinevat logi)
5. Vajutage **Apply**

8 Küberintsidentide haldus pilveteenustes

Eesmärgid:

- Töötada välja või täiendada küberintsidentide käsitlemise kord
- Leppida kokku vastutavad isikud ja tegevused
- Koolitada infoturbe töötajaid, kuidas uusi lahendusi kasutada

Eeltingimused:

- Pilvepõhised infoturbelahendused on paigaldatud ja seadistatud

8.1 Oluline











Vaikimisi on Sentinelis sisselülitatud mõned üksikud analüütika reeglid ja infoturbe töötajana on võimalik neid ise juurde luua. Microsoft lisab uusi analüütika reegleid jooksvalt kataloogi juurde, mida saab vastavalt vajadusele kasutusele võtta. Kui analüütika reegel pole aktiveeritud, siis intsidente nende kohta ei tehta.

8.1.1 Analüütika reeglid

Microsoft pakub täna kolme erinevat tüüpi analüütika reegleid, mida saate ise defineerida:

- **Scheduled Query Rule**
 - Ajastatud päringud vastavalt defineeritud päringutele ja sätetele.
- **Microsoft Incident Creation Rule**
 - Võimalik on luua ühendusi teiste Microsofti pilvepõhiste teenustega ja kui sealt peaks tuvastatama mingi anomaalia või rünne, siis tehakse vastav intsident Sentinelis.
 - Toetatud pilveteenused selle analüütika reegli all
 - Microsoft Defender for Cloud Apps
 - Microsoft Defender for Cloud
 - Entra ID Identity Protection
 - Microsoft Defender for IoT
 - Microsoft Defender for Office 365
 - Microsoft Defender for Endpoint
 - Microsoft Defender for Identity
- **NRT Query Rule**
 - Kõige uuem analüütika reegel, mis töötab reaalsajas

Sentinelis konsoolist nähtub, et vaikimisi on sisse lülitatud **Fusion** ja **Anomaly** tüüpi analüütika reeglid.

<input checked="" type="checkbox"/>	High	Advanced Multistage Attack Detection	 Fusion	 Enabled
<input type="checkbox"/>	Informational	(Preview) Anomalous Account Creation	 Anomaly	 Enabled
<input type="checkbox"/>	Informational	(Preview) Anomalous Azure AD sign-in sessions	 Anomaly	 Enabled
<input type="checkbox"/>	Informational	(Preview) Anomalous Azure operations	 Anomaly	 Enabled
<input type="checkbox"/>	Informational	(Preview) Anomalous Code Execution	 Anomaly	 Enabled

Seadistatud analüütika reeglid Sentinelis

8.1.2 Analüütika reeglite mallid

Ettevõtte infoturbe töötajana on võimalik sisse lülitada ka Sentineliga kaasatulevaid analüütika reeglite malle. Reeglite mallid on leitavad Sentinelis konsoolist **Content Hub** lehelt. Määrake filtri tüübiks **Content Type == Analytics Rule**.

Content title	Content source	Provider	Support	Category	Status
<input type="checkbox"/> A client made a web request to a po...	Standalone	Community	Community	Security - Others	
<input type="checkbox"/> A host is potentially running a crypt...	Standalone	Community	Community	Security - Threat Protection	
<input type="checkbox"/> A host is potentially running a hacki...	Standalone	Community	Community	Security - Threat Protection	
<input type="checkbox"/> A host is potentially running PowerS...	Standalone	Community	Community	Security - Threat Protection	
<input type="checkbox"/> Account added and removed from p...	Standalone	Community	Community	Identity, Security - Others	
<input type="checkbox"/> Account created from non-approved...	Standalone	Community	Community	Identity, Security - Others	
<input type="checkbox"/> AD account with Don't Expire Passw...	Standalone	Community	Community	Identity, Security - Others	
<input type="checkbox"/> AD FS Abnormal EKU object identifie...	Standalone	Community	Community	Identity, Security - Others	
<input type="checkbox"/> Addition of a Temporary Access Pass...	Standalone	Community	Community	Identity, Security - Threat Protection	
<input type="checkbox"/> ADFS DKM Master Key Export	Standalone	Community	Community	Identity, Security - Others	
<input type="checkbox"/> AdminSDHolder Modifications	Standalone	Community	Community	Security - Others	
<input type="checkbox"/> Anomalous login followed by Teams...	Standalone	Community	Community	Security - Others	

Analüütika reeglite mallid

Infoturbe töötajana on mõistlik need reeglid üle kontrollida ja vastavalt seadistatud andmehoidlale analüütika reeglid ka sisse lülitada. Alguses ei ole teada, kui palju müra need reeglid võivad keskkonnas tekitada. Seda saab teada, kui vastav reegel on sisse lülitatud ja on mõnda aega kasutuses olnud. Peale seda saab analüüsida konkreetse reeglite poolt tekitatud intsidente ning nende põhjuseid. Vajadusel on võimalik reegleid ise muuta ja täpsustada reegli tingimusi.

8.2 Küberintsidentide teavitamise seadistamine

Enne täiendavate reeglite seadistama asumist, tuleb seadistada näidis teavituste töövoog emailile. Intsidentide töövoog automaatika eeldab erinevate juhtumite kohta kokku lepitud protsesside olemasolu. Viimase puudumisel ning sellest tulenevalt oodatud tulemuse puudumisel on väga raske midagi automatiseerida.

Käesolevas juhendis seadistame emaili teavituse Logic Apps teenuse kaudu. Logic Apps on eraldi teenus, mis lubab automatiseerida erinevaid töövoogusid. Vastavad automaatika töövood paigaldatakse sama subscriptioni alla.

8.2.1 Ressursigrupi loomine

1. Azure portaalis olles vali **Resource Groups**
2. Vali **+Create**
3. Uue ressursigrupi loomisel täida ära järgmised väljad:
 - a. **Subscription:** Azure infoturbe ja halduslahendused
 - b. **Resource Group:** RG-PROD-IT-LOGIC-APPS-WE
 - c. **Region:** (Europe) West Europe
4. Vajuta **Next**

5. Tags lehel saate lisada kokkulepitud sildid. Vajutage **Next**
6. **Review +create** lehel kontrollige sisestatud informatsiooni õigsust ja vajutage **Create**
7. Nüüd peaks Teil olema **RG-PROD-IT-LOGIC-APPS-WE** ressursigrupp
8. Valige **RG-PROD-IT-LOGIC-APPS-WE** ressursigrupp
9. Valige **Access Control (IAM)**
10. Valige **Add -> Add Role Assignment**
11. **Add Role Assignment** lehelt valige **Owner** ja vajutage **Next**
12. **Members** lehel lisage enda konto. Ilma selle sammuta ei saa seadistada automaatika töövooge läbi Logic Apps.
13. Vajuage **Next**
14. **Review + Assign** lehel kontrollige informatsiooni õigsust ja vajutage **Review + Assign**

8.2.2 Logic Apps rakenduse loomine

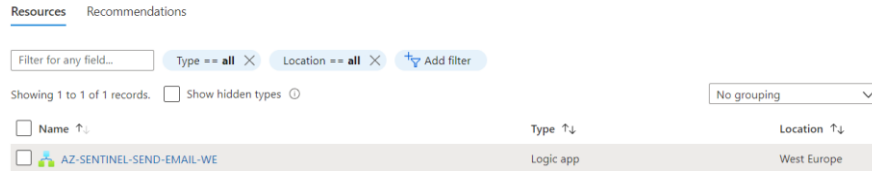
1. Azure portaalis olles sisestage otsingusse „**Logic Apps**“



2. Valige otsingust „**Logic Apps**“
3. **Logic Apps** lehel valige **+Add**
4. **Create Logic App** lehel sisestage järgnev informatsioon
 - a. **Subscription:** Azure infoturbe ja halduslahendused
 - b. **Resource Group:** RG-PROD-IT-LOGIC-APPS-WE
 - c. **Type:** Consumption
 - d. **Logic App Name:** AZ-SENTINEL-SEND-EMAIL-WE
 - e. **Enable Log Analytics:** Yes ja valige oma Log Analytics keskkond
 - f. **Region:** West Europe
5. Vajutage **Review+ Create**
6. Valige **Create**

8.2.3 Logic Apps õiguste delegerimine

1. Azure portaalis olles valige **Resource Groups -> RG-PROD-IT-LOGIC-APPS-WE**
2. Nüüd peaksite Te nägema **AZ-SENTINEL-SEND-EMAIL-WE** Logic Apps rakendust.



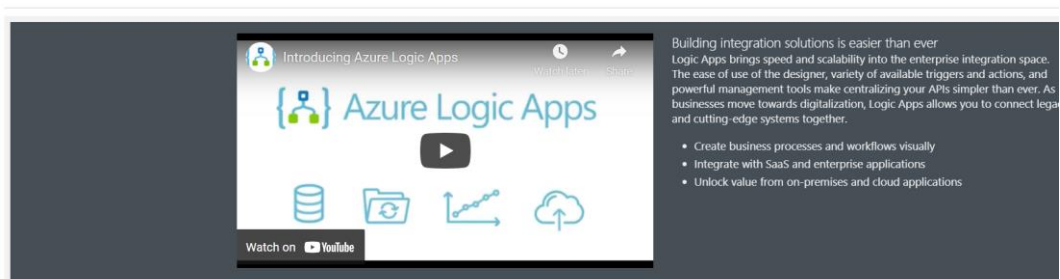
3. Valige **AZ-SENTINEL-SEND-EMAIL-WE**
4. **AZ-SENTINEL-SEND-EMAIL-WE** lehel valige Identity
5. **Identity** lehel valige **System Assigned** ja lülitage see **sisse**
6. Vajutage **Save**
7. **Enable system assigned managed identity** lehel valige **Yes**
8. Valige **Azure Role assignments**
9. Valige + **Add Role Assignments**
10. **Add Role Assignments** lehel valige järgnev informatsioon:
 - a. **Scope:** Resource Group
 - b. **Subscription:** Azure infoturbe ja halduselahendused
 - c. **Resource Group:** RG-PROD-IT-AZ-SECURITY-WE
 - d. **Role:** Microsoft Sentinel Reader
11. Vajutage **Save**

Role	Resource Name	Resource Type	Assigned To	Condition
Microsoft Sentinel Reader	RG-PROD-IT-AZ-SECURITY-WE	Resource Group	AZ-SENTINEL-SEND-EMAIL-WE	None

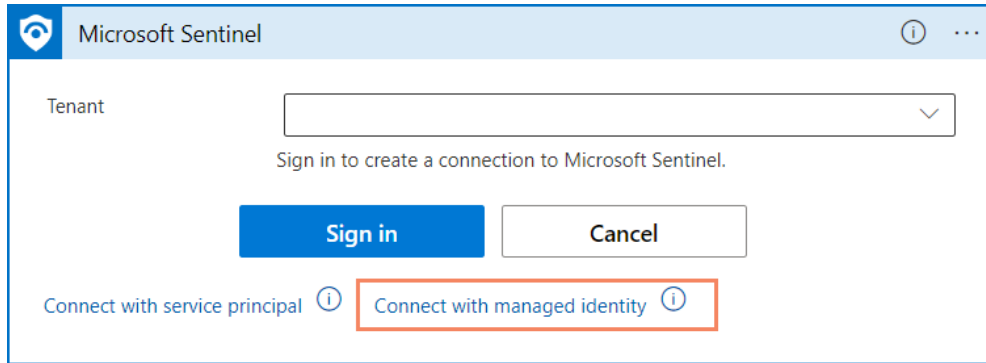
8.2.4 Logic Apps töövoos seadistamine

1. Azure portaalis olles valige **Resource Groups -> RG-PROD-IT-LOGIC-APPS-WE**
2. Valige **AZ-SENTINEL-SEND-EMAIL-WE** Logic Apps rakendus
3. Teile peaks nüüd avanema **Logic Apps Designer**

Logic Apps Designer ...

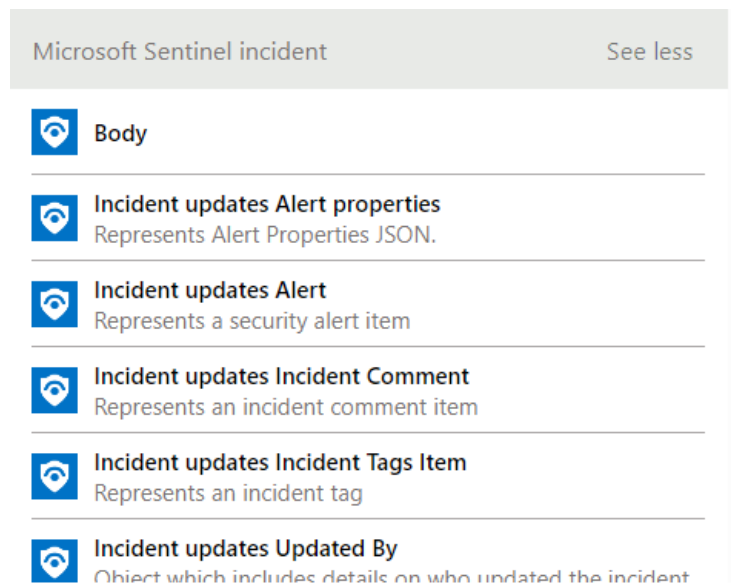


4. Valige **Blank Logic Apps**
5. Sisestage otsingusse „Sentinel“
6. Triggers alt valige „Microsoft Sentinel Incident“
7. **Sentinel** esimesel sammul vajutage **Connect with managed identity**

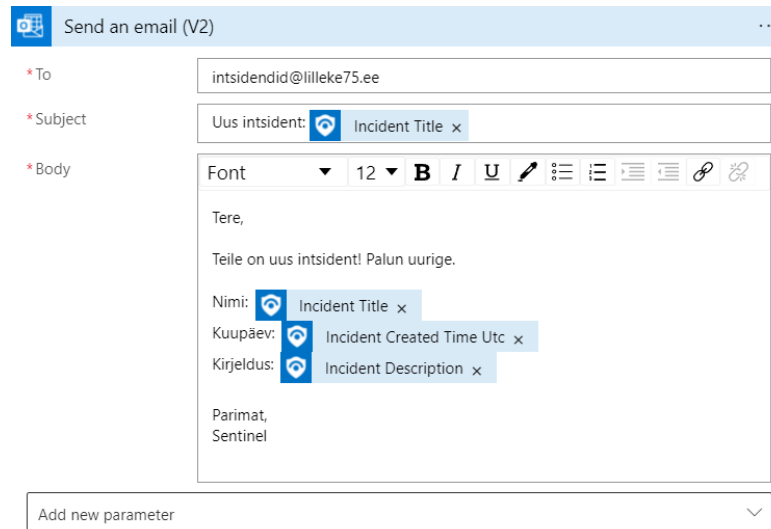


8. Järgmisena sisestage ühenduse nimi ja vajutage **Create**
9. Valige + **New Step**
10. Uue sammu tüübiks valige **Send an email(V2)**. Vastav samm kuulub Office 365 Outlook alla.
11. Valige **Sign in**. Nüüd küsitakse Teie käest millise emaili alt neid saatma hakatakse. Selleks tuleks luua vastav konto. Kui vastav konto on olemas, siis sisestage konto ja parool.
12. **Send an email (V2)** lehel saate sisestada järgneva informatsiooni:
 - a. **To:** Sisestage infoturbe osakonna emaili aadress, nt intsidendid@lilleke75.ee
 - b. **Subject:** Uus intsident: %MUUTUJA%
 - c. **Body:**

Vasakpoolses kastis leiate dünaamilised muutujad, mida saab valida oma kirja sisu jaoks.



Koos muutujatega on võimalik luua taoline kiri. Enne seadistamist tuleb kirja sisu eelnevalt kokku leppida.

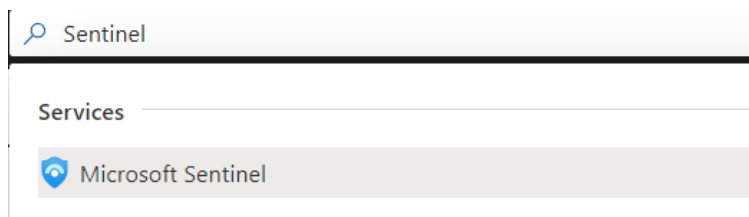


13. Vajadusel saate lisada täiendavaid parameetreid

14. Kui vastavad lüngad on täidetud, vajutage **Save**

8.2.5 Automaatika töövoogu seadistamine Sentinelis

1. Azure portaalis olles trükkige otsingusse „**Sentinel**“



2. Valige otsingust „**Microsoft Sentinel**“

3. Valige **AZ-PROD-IT-LOG-ANALYTICS-WE** keskkond

4. **Sentinel**i paneelist valige **Settings**

5. Valige **Settings** uuesti

6. Valige **Playbook permissions**

7. Valige **Configure Permissions**

8. Manage Permissions lehel valige **RG-PROD-IT-LOGIC-APPS-WE**

9. Valige **Apply**

10. Valige **Automation -> Active Playbooks**

11. Nüüd on loodud automaatika reeglid

12. Automation lehel valige **+Create -> Playbook with incident trigger**

13. **Create new Automation** lehel sisestage järgnev informatsioon

a. **Automation Rule Name:** EXECUTE AZ-SENTINEL-SEND-EMAIL-WE

b. **Conditions:** All

c. **Actions :** Run playbook

i. Valige **AZ-SENTINEL-SEND-EMAIL-WE**

d. Valige **Apply**

Vastav reegel käivitub iga uue intsidendi korral. Kui kõik sammud on läbitud vastavalt juhendile, siis uue intsidendi puhul laekub sarnane email.

Tere,

Telle on uus intsident! Palun uurige.

Nimi: [SAMPLE ALERT] Suspicious policy change and secret query in a Key Vault

Kuupäev: 2021-12-18T14:04:08.8616411Z

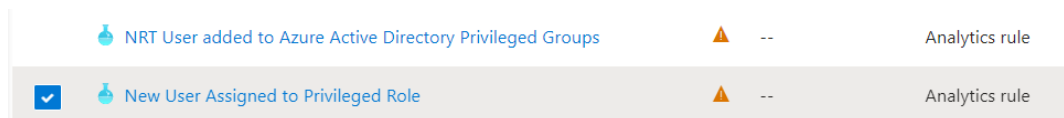
Kirjeldus: THIS IS A SAMPLE ALERT: While may be benign it could also indicate that a Key Vault policy change has been made and operations to list and/or get secrets occurred shortly thereafter. In addition, this operation pattern is not normally performed by the user on this vault. This is highly indicative that the Key Vault has been compromised and the secrets within have been stolen by a malicious actor.

Parimat,
Sentinel

8.3 Analüütika reeglite seadistamine

Sentinel andmete hoidlate seadistamisel ei käivitatud koheselt andmete hoidlate intsidentide loomist. Nüüd, mil on olemas üks vastav automaatika töövoog, mis saadab intsidendi korral emaili, saab sisse lülitada ühe näidis analüütika reegli, mida Microsoft pakub.

1. Sentinel paneelist valige **Content Hub**.
2. Valige Entra ID (Azure Active Directory) andmehoidla
3. Vajutage Manage
4. Sisestage otsingusse „user“. Otsing peaks näitama „**New User Assigned to Privileged Role**“ analüütika reeglit



5. Valige vastav reegel ja vajutage Configuration
6. Valige vastav reegel ja vajutage **Create Rule**
7. **Analytics rule wizard - Create new rule from template** lehel vajutage **Next**
8. **Set Rule Logic** lehel nähtub, et vastav reegel kasutab **AuditLogs** tabelit ja selle tabeli andmed tulevad Entra ID andmehoidlast. Vajadusel saab vajutades **Test with current data** vaadata, kui palju tulemusi keskkonnas vastav päring annab.

Define the logic for your new analytics rule.

Rule query

Any time details set here will be within the scope defined below in the Query scheduling fields.

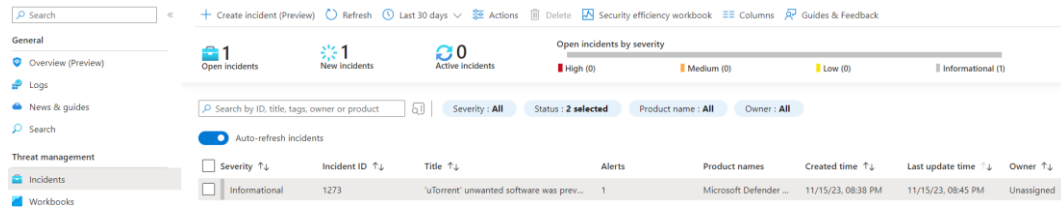
```
// Define the start and end times based on input values
let starttime = now()-1d;
let endtime = now();
// Set a lookback period of 14 days
let lookback = starttime - 14d;
// Define a reusable function to query audit logs
```

9. Samal lehel olev **Query Scheduling** näitab, kui tihti seda päringut käivitatakse ja kui pikka perioodi vaadatakse tagasi.
10. Vajutage **Next**
11. **Incident settings** lehel saate määrata, kas vastavaid intsidente grupeeritakse kokku või mitte. Kui Sentinel on Teie jaoks uus, siis on võimalik alguses erinavad võimalusi testida ja leida parim viis, kuidas intsidente näha.
12. Vajutage **Next**
13. **Automated Response** lehel on näha, millised automaatika töövood sellele reegliiga seonduvad. Eelnevalt tehtud töövoog rakendub igale intsidendile.
14. Vajutage **Next**
15. **Review and create** lehel kontrollige informatsiooni õigsust ja vajutage **Create**

Nüüd on olemas esimene Microsofti malli järgi seadistatud analüütika reegel. Järgmise sammuna on mõistlik üle kontrollida ka kõik muud reeglid ja lülitada sisse enda jaoks olulised.

8.4 Intsidentide käsitlemine

Kui vastavad analüütika reeglid on ära seadistanud koos esialgse teavitus töövooga, võidakse luua ka erinevaid intsidente. Kõik intsidendid on Sentinelis alati **Incidents** paneeli all.

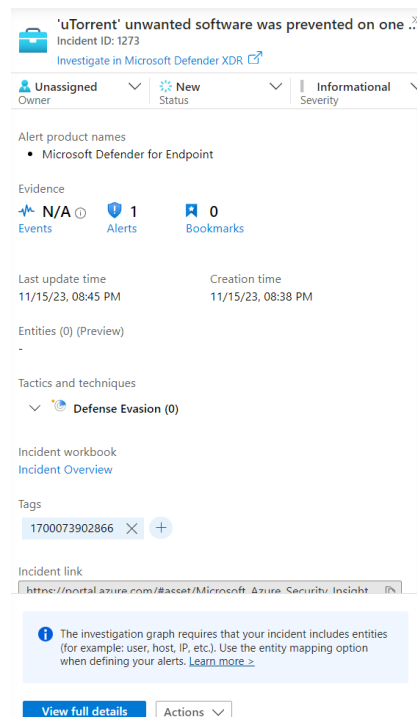


Intsidentid Sentinel teenuses

Sõltuvalt ettevõtte suuruselt ja analüütika reeglitest võib päevane intsidentide arv olla erinev. Osa intsidente võivad olla ka valepositiivsed ehk tegelikult kriitilist olukorda ette tulnud ei ole. Sellisel juhul tuleks uurida põhjusi ning vajadusel tuleks muuta vastavat reeglit. Ilmneda võib ka päris juhtumeid ja sellistes olukordades on oluline lähtuda varasemalt IT-meeskonnaga koostöös loodud juhistest, mis katavad elementaarsed punktid.

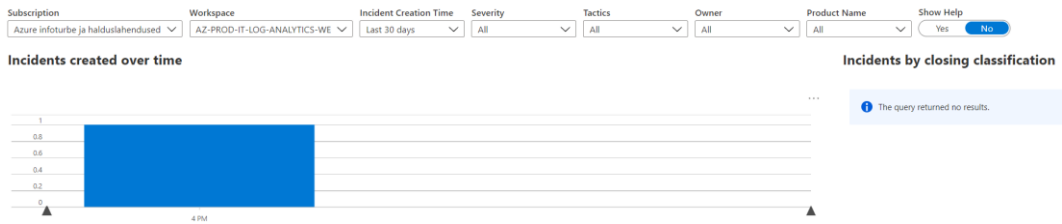
Kui intsidentide käsitlemist ei ole varasemalt IT-osakonnaga käsitletud, on tõenäoline, et kriisi olukorras astutakse samme vales järjekorras viies kokkuvõttes kogu juhtumi lahendamine tundub keerulisemale tasemele. Ülioluline on leppida kokku konkreetsed vastutused ja nii sisemine kui ka välimine kommunikatsioon.

Üleval pildilt on näha näide sisse tulnud intsidendist. Intsidenti valides kuvatakse alljärgnev informatsioon. Sõltuvalt intsidendist on sisu erinev.



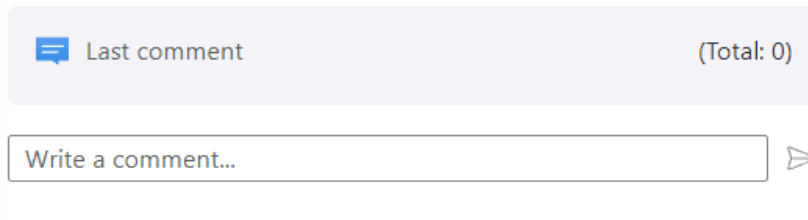
Aknas nähtub, mis on antud intsidenti tekitanud. Antud juhul näeme, et vastava ründe on tuvastanud Microsoft Defender XDR teenus. Täiendavat infot on võimalik vaadata ka otse Microsoft Defender XDR portaalist. Sentinel'i õigused ei anna automaatselt ligipääsu kõikidele teistele teenustele. Iga uue intsidenti puhul tuleks määrata vastutaja ja staatuseks panna **Active**. Nii on näha, et vastav juhtum on töösse võetud ja sellega tegeletakse. Sentinelis on **Security Efficient Workbook**, mis näitab kogu ettevõtte intsidente, sh kes on kõige rohkem neid lahendanud, kui kaua nende lahendamine on aega võtnud jne.

Security Operations Efficiency

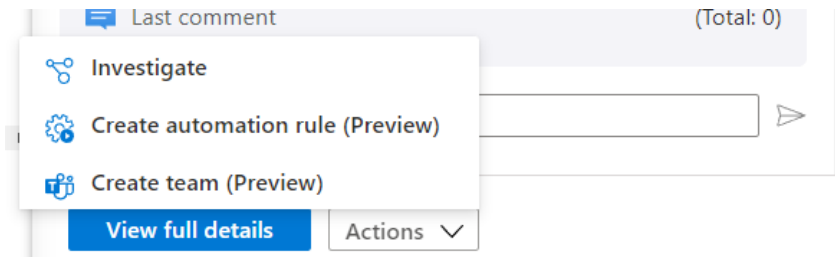


Security Efficient Workbook

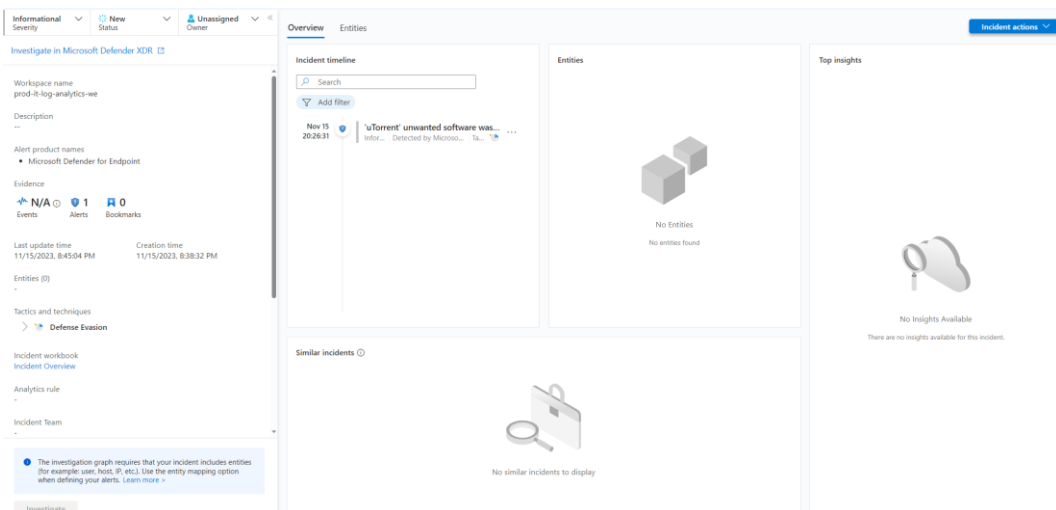
Tulles tagasi nimetatud intsidentide juurde, näeme ka isikuid ja teenuseid, millega intsident on seotud. Juhul kui peaks selguma, et mingi juhtumi lahendamine võtab rohkem aega, soovitatakse lisada vastav kommentaar.



Uute intsidentide puhul lubab Microsoft luua ka eraldi Teamsi grupi konkreetse juhtumi lahendamiseks. Suuremate intsidentide puhul võib tekkida vajadus kaasata ka väliseid eksperte.



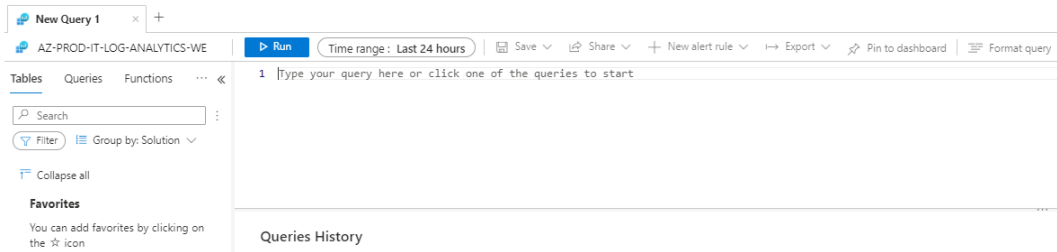
Vajutades **View Full Details** nuppu avaneb järgnev vaade.



Sellesse vaatesse tuuakse kokku kõik konkreetse ründega seotud tegevused. Teatud rünnakute puhul võib neid tegevusi olla palju.

Infoturbe töötajana on alati võimalik üle vaadata täiendavad detailed logid ja teha täiendavaid päringuid. Selleks tuleb minna Sentineli peakonsooli ja valida **Logs**.

Avanevas aknas saab päringuid sisestada ja teha vastavat analüüsi.



Päringute keeleks kasutab Microsoft KQLi, millega soovitame kindlasti täiendavalt tutvuda.

Oluline on intsidente igapäevaselt jälgida ja analüüsida. Vastasel juhul võib jääda märkamata olulisi arenguid ja kogu keskkond võidakse kompromiteerida.

9 Administratiivmudeli määratlemine ja kasutuselevõtt

Eesmärgid:

- Leppida kokku pilveteenuste administreerimise põhimõtted
- Juurutada vastavad tehnilised meetmed ja protsessid riskide maandamiseks administratiivkontodest lähtuvalt

Eeltingimused:

- Pilvepõhised infoturvelahendused on juurutatud
- Entra ID 2 või Enterprise Mobility +Security E5 või Microsoft 365 E5 litsentsid administraatoritele on olemas

9.1 Microsoft Entra infoturbe teenused

Pilveteenuste administratiivmudeli juurutamiseks on vaja võimekamaid litsentse. Kui ettevõttele on hangitud näiteks Microsoft 365 E5 või Enterprise Mobility +Security E5 litsentsid, siis on vajalikud litsentsid juba olemas. Juhul kui valisite madala taseme litsentsid (näiteks Microsoft 365 E3), tuleb administraatorite kontode kaitsmiseks teha täiendav investeering.

Microsoft Entra pakub järgmisi infoturbe teenuseid:

- Conditional Access
- Multi-factor Authentication
- Identity Protection
- Privileged Identity Management

Conditional Access ja Multi-factor Authentication on olemas ka Entra ID Premium 1 paketi. Identity Protection ja Privileged Identity Management vajavad aga Entra ID Premium 2 litsentsi. Entra ID Premium 2 litsentsid ongi just kõige olulisemad administraatorite vaates. Administraatoritele ei ole soovitatav välja anda püsivaid õigusi. Kõik vajalikud õigused aktiveeritakse vahetult enne vastavat tööülesannet ja väljastatakse ainult kindlaks perioodiks.

9.1.1 Microsoft Entra Multi-factor Authentication

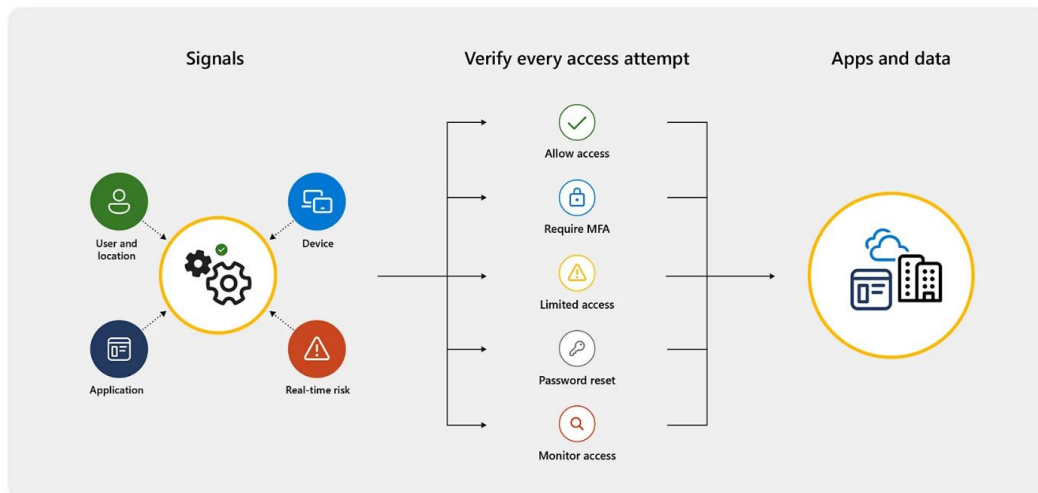
Mitmefaktoriline autentimine on protsess, kus sisselogimise ajal palutakse kasutaja tuvastamiseks täiendavalt paroolile viia läbi täiendav tuvastamise näiteks:

- Sisestada kood oma mobiiltelefoni rakendusest (Authenticator)
- Kinnitada sisselogimine oma mobiiltelefoni rakendusest (Authenticator)
- Kinnitada sisselogimine sõrmejälje skaneerimisega
- Saata telefoni numbrile SMS
- Kasutada turvavõtit

Teenuse seadistamise ajal on võimalik administraatoril määrata autentimise võimalused. Risk kontode kompromiteerimiseks ilma mitmefaktorilise autentimiseta on märkimisväärselt suur.

9.1.2 Microsoft Entra Conditional Access

Conditional Access ehk tingimuslik ligipääs on teenus, mis lubab defineerida erinevate teenuste info põhjal erinevaid ligipääsu reegleid. Administraatorid saavad näiteks luua reegleid, mis nõuavad ettevõtte ärirakenduse ligipääsuks infoturbepoliitikatele vastavuses olevat seadet. Kui seade vastab tingimustele, siis on võimalik teenust tarbida ja ülejäänud juhtudel blokeeritakse ligipääs.



Entra ID Conditional Access teenus

9.1.3 Microsoft Entra Identity Protection

Tegemist on masinõppel põhineval infoturbe teenusega, mis analüüsib kasutajate kontode kasutamist erinevates olukordades. Teenus suudab tuvastada erinevaid anomaaliaid ja kontode kompromiteerimisega seotud tegevusi:

- Sisselogimine TOR veebilehitseja kaudu
- Sisselogimine riigist, kust pole kasutaja kunagi sisse loginud
- Kasutaja parool on varasemalt juba lekkinud

Teenuse seadistamisel on võimalik paika panna, kuidas käituda erinevate kahtlaste juhtumite korral. Näiteks nõuda parooli vahetust, blokeerida ligipääs jmt.

9.1.4 Microsoft Entra Privileged Identity Management

Suurte õigustega kasutajad nagu Globaalsed administraatorid, Exchange Online administraatorid on küberründajate sihtgrupp. Nimetatud õigustes on võimalik väga kiirelt ja väga palju kahju tekitada. Privileged Identity Management lubab sensitiivsemate tegevuste jaoks administraatoritel või teistel osapooltel kinnitusprotsessi kaudu ajutiselt õigusi taotleda. See tähendab, et administraatorid ei pea omama pidevalt suuri õigusi, vaid saavad need ainult siis, kui neid on vaja tööde teostamiseks või intsidentide lahendamiseks.

9.2 Põhimõtete defineerimine

Enne pilveteenuste administratiivmudeli juurutamise alustamist on väga oluline ettevõtte sees põhimõtted kokku leppida ja selgitada, et miks see on oluline. Vaadates Microsofti poolt välja antud raporteid on näha, et erinevatel ettevõtetel on väga palju suurte õigustega kasutajad ilma igasuguse kaitseta. Pole rakendatud mitmetasemelist kontrolli või on ka liialt palju kasutajaid Globaalsete administraatorite grupis.

Mõned näited ettevõtte administratiivmudeli põhimõtete dokumendis sisalduva kohta:

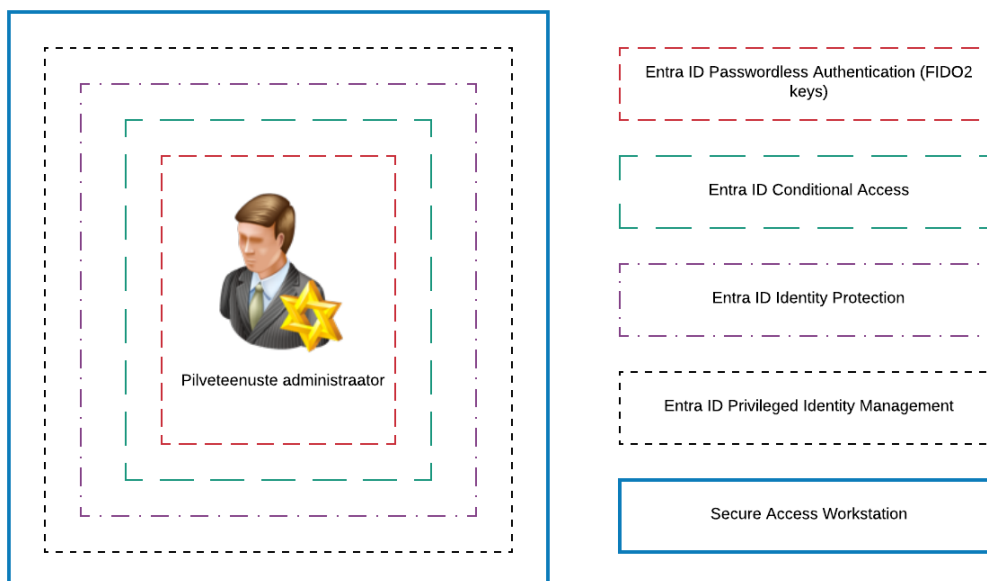
- Tegevused, mis nõuavad tavakasutajast rohkem õigusi, viiakse läbi ainult selleks ette nähtud administratiivtegevusteks mõeldud seadmetest.
- Servereid ja teenuseid on võimalik hallata ainult ettevõtte poolt välja antud ja hallatud seadmetest.
- Igale administraatorile on ette nähtud erinev arv administratiivkontosid. Konkreetne arv sõltub ametikohast ja kohustustest.

- Administratiivtööjaamad on ainult kasutatavad selleks ettenähtud asukohast ja võrgust.
- Pilveteenuste halduse jaoks kasutatakse „pilv ainult“ (cloud-only) kontot. Tegemist on kontoga, mida ei sünkroniseerita ettevõtte kohaliku Active Directory keskkonnaga.
- Igal pilveteenustega seotud administratiivkontol peab olema seadistatud turvavõti. Turvavõti väljastatakse IT-osakonnast ja võtme seadistamise peab läbi viima administraator iseseisvalt vastavalt juhendile. Iga väljastatud võti tuleks registreerida ettevõtte infosüsteemis.
- Pilveteenuste haldusega seotud administraatoritele rakendatakse „Tingimusliku Ligipääsu“ (Conditional Access) poliitikad, mis defineerivad ära, mis tingimustel on üldse võimalik teenustele ligi pääseda.
- Pilveteenuste haldusega seotud administraatoritel rakendatakse Entra ID Identity Protection poliitikad, mis peaksid takistama ja tuvastama kontode kompromiteerimisi.
- Pilveteenuste haldusega seotud administraatoritel rakendatakse Entra ID Privileged Identity Management poliitikad. Administratiiv õiguste saamine tuleb eraldi küsida ja kinnitada. Kontodel administratiivõigused vaikumisi puuduvad.

Sarnaste põhimõtete defineerimisega peab suutma tagada ja veenduda, et ettevõtte sensitiivsemad administratiivkontodega seotud riskid on võimalikult hästi leevendatud. Siinkohal rakendame erinevaid tehnilisi kontrole, kuid on väga oluline rangelt pidada kinni ka kokku lepitud protsessidest. On oluline, et kogu IT-meeskond protsesse järgivad, sest vastasel korral kaob usaldus kogu administratiivmudeli vastu.

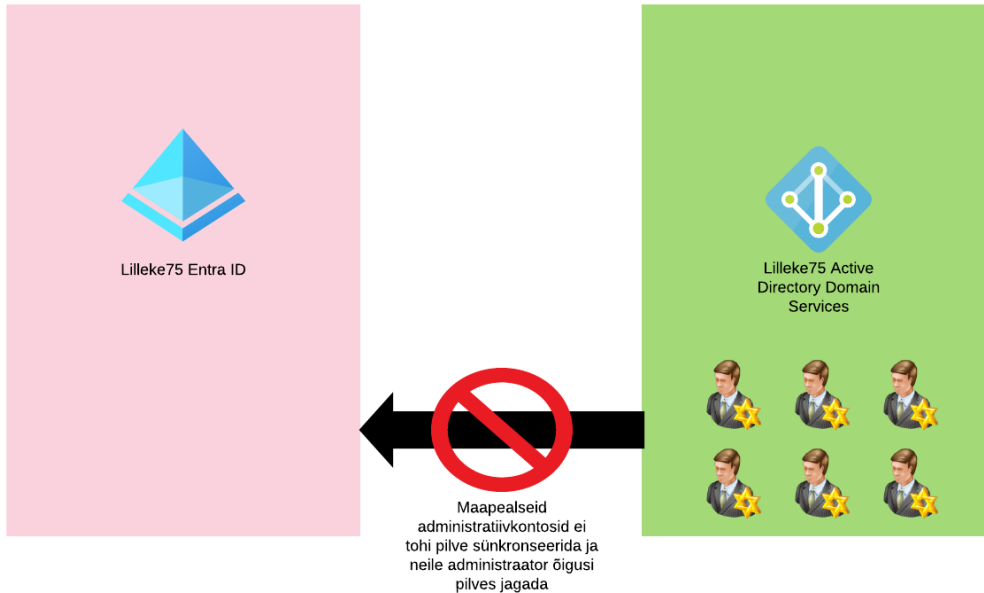
9.2.1 Administratiivmudeli disain

Pilvepõhine administratiivmudel koosneb 5 erinevast meetmest koos täiendavate protsessidega.



Pilveteenuste administratiivmudel

Kui ettevõttel on maapealne Active Directory Domain Services, siis selle teenuse administratiivkontosid ei tohiks pilve sünkroniseerida ja teiseks ei tohi ka neile pilves administratiivõigusi jagada. Kui Te kasutate pilves ja maapeal samu kontosid, siis maapealse Active Directory kompromiteerimine tähendab ka administratiiv õiguste saamist pilveteenustes. Oluline on siin administratiivmodelid lahku lüüa ja ka lahus hoida.



Erinevad administratiivmodelid pilves ja maapeal

Igale administraatorile väljastatakse FIDO2 turvavõti koos „pilv ainult“ kontoga. FIDO2 turvavõtmete kasutamisel ei pea administraator sisestama kasutajanime ja parooli.

Sellise lähenemisega ei ole võimalik administraatori kontot „õngitseda“ (phishing), sest konto seadistamisel ei väljastatud kordagi administraatorile parooli. Teiseks ei tohiks lasta administraatoritel seadistada ja kasutada telefonipõhiseid kinnitusmeetodeid.

Teise meetmena rakendame administraatorite kontodele erinevaid tingimusliku ligipääsu reegleid Entra ID'st. Näiteks:

- Mitmetasemeline kontroll on nõutud kõikidele administraatoritele
- Mitmetasemeline kontroll on nõutud pilveteenuste administreerimiseks
- Administraatori sessiooni pikkus on sätestatud
- Tor veebilehitsejad ja ühenduste anonümiseerijad on keelatud

Kolmanda meetmena aktiveeritakse administraatori kontodel Entra ID Identity Protection teenus. Selle teenusega saab tuvastada kasutajakontoga seotud anomaaliaid ja vajadusel keelata sisse logimine üldse. Taolisi reegleid saab ka defineerida tingimusliku ligipääsu kaudu.

Neljanda meetmena rakendatakse kasutajale Entra ID Privileged Identity Management teenus. Selle teenusega kaetud administraatorid ei oma vaikimisi mitte ühtki õigust pilveteenustes. Kõik õigused tuleb eelnevalt küsida ja vastavalt seadistustele saada vastav kinnitus. Õiguste küsimuse kinnitust on võimalik edastada ka kellegile teisele, kes peab selle kinnitama ja alles siis väljastatakse vastavad õigused. Erinevatele rollidele rakendatakse erinevad sätted.

Kõige viimasena meetmena siin nimekirjas on „**Secure Access Workstation**“. Tegemist on eraldi tööjaamaga, mis on mõeldud ainult administratiivtegevuste läbiviimiseks. Kahjuks eksitakse sageli selle reegli vastu. Sama arvutit kasutatakse ka mitmete muude kõrvaliste mitteadministratiivsete tegevuste teostamiseks sh koosolekud, internetis surfamine, emailide lugemine. Probleemiks võib ka see, et tavakasutajate ja administraatorite seadmed on kõik sama keskhalduslahendusega seotud ja ei pruugi olla isegi võrgu tasemel eraldatud.

Administratiivtegevuste läbiviimisel peab alati tagama, et tegevusi alustatakse turvalisest keskkonnast, mis ei ole kompromiteeritud. Samasid põhimõtteid tuleb ka jälgida majasisese Active Directory halduses.

9.3 Analüüsi läbiviimine

Enne pilveteenuste õiguste jagama asumist, on oluline eelnevalt läbi viia õiguste analüüs. Siinkohal tuleb analüüsida nii Entra ID rolle, kui ka kulupõhiste teenuste õigusi (subscriptions, ressurssigrupid jne). Kui pilveteenused on juba mõnda aega kasutuses olnud, siis on vaja ära kaardistada ka kõik eelnevalt seadistatud õigused. Peale õiguste kaardistamist ja seadistamist on võimalik administraatoritele välja anda uus „pilv ainult“ administraatori konto koos turvavõtmega. Vanad kontod tuleks kõik sulgeda ja õigused eemaldada. Eesmärk on teha kogu õiguste süsteemile taaskäivitus ja täiendavate protsesside kaasabil veenduda, et õiguste jagamine ja teenuste paigaldamine käib kõik vastavalt kokkulepitud põhimõtete järgi. Enne analüüsi tegemist on vaja kokku leppida, kes hakkab õiguste delegeerimise ja monitooringu eest vastutama. Hea oleks määrata vähemalt kaks inimest – üks on primaarne ja teine sekundaarne administraator.

Kui õigusi saab seadistada rohkem kui üks inimene, võib see viia negatiivse tulemini. Vajadusel määrata sekundaarne administraator, kui peadministraator peaks olema majast väljas või puhkusel.

Siinkohal räägime ainult administraatorite ja mitte lõppkasutajate õiguste haldusest.

9.3.1 FIDO2 turvavõtmed

Administratiivmudeli juurutamiseks on vaja tellida FIDO2 võtmeid. Entra ID toetab erinevate tootjate tooteid ja võimaluse korral tuleks testida erinevaid võtmeid. Turul on saadaval nii soodsamaid, kui ka kallimaid võtmeid. Kallimaid võtmeid on võimalik kasutusele võtta samaaegselt ka teistes teenustes.

Toetatud võtmete nimekirja leiate siit - <https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless#fido2-security-key-providers>

9.3.2 PIM õiguste grupid ja seadistused

Microsoft lubab õigusi defineerida kahel erineval moel. Need on:

- **Eligible:** Sellel juhul peab administraator privilegeeritud õigused endale eelnevalt küsima. Õigused ei ole kaasas koheselt ja neid saab küsida ainult ajutiseks kasutamiseks. Tegemist on ka soovitatud lahendusega, kuidas Entra PIM kaudu õigusi jagada.
- **Active:** Privilegeeritud õigused on pidevalt aktiivsed ja administraator ei pea tegema lisa tegevusi õiguste saamiseks.

9.3.3 Koolitus

Iga administraator peab saama vastava koolituse teenuste administreerimise osas ja tuleb ka veenduda, et vastav isik omab teadmisi, kuidas mingeid teenuseid tuleb administreerida jne. Koolitamata inimeste kohene tööle rakendamine võib kaasas tuua konfiguratsioonivigu või halvimal juhul küberintsidendi. Võimaluse korral saata administraatorid peale koolitust sertifitseerimise eksamit tegema. Vastavad eksamid näitavad, kas administraatorid on koolitusel omandanud vastavad teadmised.

9.3.4 Õiguste kaardistamine ja rollide jaotamine

Käesoleva juhendiga on kaasas Azure Administratiivmudel Exceli dokument. Antud Exceli dokument hakkab olema õiguste ja rollide süsteemi alusdokument. Vajadusel saate kasutusele võtta ettevõttele sobivama vahendi või formaadi.

Azure Administratiivmudeli dokumendis on järgmised lehed:

- **Kasutajad**
 - o Avariikontod ja pilveteenuste administraatorite kontode nimed ja sätted.
- **Grupid**
 - o Administratiivmudelis kasutatavad grupid.
- **Entra ID PIM Rollid**
 - o Entra ID Privileged Identity Management rollide sätted.
- **Ettevõtte PIM Rollid**
 - o Koondtabel mis toob kokku Entra ID ja kulupõhiste teenuste rollid.
- **Entra ID Rollid**
 - o Entra ID rollide nimekiri ja nendega seotud administraatorid.
- **Conditional Access Reeglid**
 - o Rakendatavad Conditional Access reeglid.
- **Azure Subscriptions**
 - o Kulupõhised teenused ja nende subscriptionid.

Tabeli täitmist tuleb teha täpselt eelpool loetletud järjekorras. Enne tabeli täitmist on vaja defineerida erinevatele objektitele vastavad standardid. Kui nimede standardit ei defineerita, siis on tunduvalt raskem keskkonda hallata ja automatiseerida. Kaasasolevas Exceli tabelis on välja toodud mõned näited, mida palume üks-ühele oma keskkonnas mitte seadistada. Näidete eesmärk on tuua välja, kuidas õiguste kaardistamist ja analüüsi selle Exceli tabeli kaudu teha.

Kasutajad

Kasutajate tabelis tuleb ära kirjeldada kõik pilveteenuste administraatorid ja need kontod hakkavad kasutama Teie Entra ID teenuse domeeni nime. Nendel kontodel ei kasutata ettevõtte domeeni nime nagu Lilleke75.ee jne. Selles tabelis tuleks ära täita ka Entra ID avariikontod. Avariikontodest räägime täpsemalt allpool.

Nimi	Kirjeldus	Kommentaariid	Azure AD Roll	Turvavõti	Juhendi näidis
AADBA-289858086761	Entra ID avariikonto 1	Monitoring peab olema seadistatud. Mitte kasutada samu nimesid päris tootmises. Genereerige oma kontod vastavalt oma poliitikate järgi. Tegemist on näidis nimega.	Global Administrator	JAH	JAH
AADBA-815895247538	Entra ID avariikonto 2	Monitoring peab olema seadistatud. Mitte kasutada samu nimesid päris tootmises. Genereerige oma kontod vastavalt oma poliitikate järgi. Tegemist on näidis nimega.	Global Administrator	JAH	JAH
Malle.Puu_CA@M365x982850.onmicrosoft.com John.Wood@Contoso.onmicrosoft.com	Pilve administraator		Valkimisi ei oma mitte ühtki õigust Valkimisi ei oma mitte ühtki õigust	JAH JAH	JAH JAH

Grupid

Administratiivmudeli juurutamisel tuleb luua mitmeid gruppe. Osa gruppe kasutame teatud Entra ID funktsioonide jaoks, näiteks FIDO2 turvavõtmed jne ja teised grupid tulenevad ettevõtte ametikohtade rollide jaotuse järgi.

Grupi nimi	Grupi tüüp	Kirjeldus	Entra ID Rollid	Seadistatud	Juhendi näidis
AAD-AR-SEC-TEMPORARY-ACCESS-PASS	Security	Lubab kasutajatel kasutada Entra ID's ajutisi autentimise passe	EI		JAH
AAD-AR-SEC-FIDO2-SECURITY-KEYS	Security	Lubab kasutajatel kasutada FIDO2 turvavõtmeid	EI		JAH
AAD-AR-SEC-EXCLUDED-FROM-CA	Security	Kontod millele ei rakendu mitte ükski tingimuslik ligipääsu reegel	EI		JAH
AAD-AR-SEC-CLOUD-ADMINISTRATORS	Security	Kõik pilve administraatorid	EI		JAH
AR-SEC-PIM-SECURITY-ENGINEER	Security	Lilleke75 infoturbe töötajad	JAH		JAH
AR-SEC-PIM-HELPDESK	Security	Lilleke75 helpdeski töötajad	JAH		JAH
AR-SEC-PIM-INFRA-ENGINEER	Security	Lilleke75 taristu haldusega seotud inimesed	JAH		JAH
AR-SEC-PIM-GLOBAL-ADMIN	Security	Lilleke75 Entra ID Globaalsed administraatorid. Siin peaks olema maksimaalselt kuni kaks inimest	JAH		JAH
AR-SEC-PIM-EXCHANGE-ADMIN	Security	Lilleke75 Exchange Online administraatorid. Siin peaks olema maksimaalselt kuni kaks inimest	JAH		JAH

Näidis Exceli tabelis on kirjeldatud nelja erineva osakonna grupi nimed:

- AR-SEC-PIM-SECURITY-ENGINEER
- AR-SEC-PIM-HELPDESK
- AR-SEC-PIM-INFRA-ENGINEER
- AR-SEC-PIM-GLOBAL-ADMIN
- AR-SEC-PIM-EXCHANGE-ADMIN

Erinevaid õigusi hakatakse määrama vaid kokkulepitud gruppidele. Tuleb mees pidada, et õigusi ei anta kunagi otse kontole. Gruppide loomisel on oluline silmas pidada, et superadministraatori gruppe luua ei tohi. Superadministraatori grupid on need, mis sisaldavad kõiki olulisi õigusi. Erinevad küberintsidendid on näidanud, et taolised grupid teevad küberkurjategijatele elu väga lihtsaks ja ründe läbi viimise kiireks. Nagu gruppide näites nähtub, on kaks eraldi gruppi nimedega AR-SEC-PIM-GLOBAL-ADMIN ja AR-SEC-PIM-EXCHANGE-ADMIN. Mõlemad omavad ainult ühte õigust. Taolised suurte õigustega grupid eeldavad, et keegi teine peab enne nende õiguste küsimise aktsepteerima. Ilma täiendava nõusolekuta ei tohi olla võimalik aktiveerida Entra ID Global administraatori või Exchange Online administraatori õigust.

Entra PIM Rollid

Entra PIM rollide lehel on ära kirjeldatud absoluutselt kõik Entra ID rollid. Iga roll tuleb vastavalt ettevõtte poliitikatele ära seadistada.

Seadistus	Nõuab 2FA kinnitust	Teavitus	Intsidendi ID	Nõuab eraldi kinnitust	Kinnitaja(d)	Aktiveerimise kestus	Alalised administraatorid	Kommentaar	Seadistatud
Entra ID Roll									
Application Administrator	JAH	JAH	JAH	EI	Ei ole kedagi	4 tundi	Ei ole kedagi		11.12.2023
Application Developer	JAH	JAH	JAH	EI	Ei ole kedagi	4 tundi	Ei ole kedagi		01.12.2023
Attack Payload Author									
Attack Simulation Administrator									

Entra Privileged Identity Management rollide sätted

Iga rolli kohta tuleb märkida järgmine info:

- Kas mitmetasemeline kontroll on nõutud
- Kas rolli aktiveerimisel teavitatakse kedagi
- Kas rolli aktiveerimisel tuleb sisestada intsidendi ID
- Kas rolli aktiveerimisel tuleb kellegi käest kinnitust küsida
- Kes on konkreetse rolli õiguste kinnitajad
- Kui pikaks ajaks õigusi välja antakse

- Kas vastavas rollis on alalisi administraatoreid
- Kommentaarid, märkused
- Konkreetse rolli seadistamise kuupäev

Kokku on tabelis üle 100 rolli, mida tuleb vastavalt sätetele määrata ja alles siis seadistamisega Entra ID portaalis jätkata. Meie soovitus on anda enamus õigusi maksimaalselt välja neljaks tunniks ja suuremaid õigusi nagu Global administraator ja Exchange Online administraatori rolle kuni üheks tunniks. Enne kui keegi soovib taolisi õigusi küsida, peaks taolised muudatused olema eelnevalt kokkulepitud ja õiguste kinnitajatega läbi räägitud ning dokumenteeritud.

Entra ID Rollid

Asutuse enda rollinimi	AR-SEC-PIM-SECURITY-ENGINEER	AR-SEC-PIM-HELPDESK	AR-SEC-PIM-INFRA-ENGINEER	AR-SEC-PIM-GLOBAL-ADMIN	AR-SEC-PIM-EXCHANGE-ADMIN
Entra ID Roll					
Application Administrator			JAH		
Application Developer					
Azure AD Joined Device Local Administrator					
Azure DevOps Administrator					
Azure Information Protection Administrator					
Attack Payload Author					
Attack Simulation Administrator					
Attribute Assignment Administrator					
Attribute Assignment Reader					
Attribute Definition Administrator					
Attribute Definition Reader					
Authentication Administrator					
Authentication Policy Administrator					
B2C IEF Keyset Administrator					
B2C IEF Policy Administrator					
Billing Administrator			JAH		

Ettevõtte PIM Rollid

Ettevõtte PIM Rollid tabel koondab endamisi kokku kõik seadistatud Entra ID rollid koos kulupõhiste rollidega. Vasakul on märgitud sinisega Entra ID rollid ja tumerohelisega kulupõhised teenused nagu Sentinel jne. Eelnevalt seadistatakse pilvepõhised infoturbe lahendused, mida saab Privileged Identity Management teenuse kaudu hallata. Kui paigaldada oma keskkonda lisanduvaid teenuseid, tuleb vastavasse tabelisse ridu juurde lisada.

Login	Rolli tüüp	Subscription ID	Subscriptioni nimi	Ressursigrupp	AR-SEC-PIM-SECURITY-ENGINEER
Rollid					JAH
Global Reader	Entra ID				JAH
Security Reader	Entra ID				JAH
Security operator	Entra ID				JAH
Security Administrator	Entra ID				
Azure Sentinel Reader	Azure Resource	Azure infoturbe ja halduslahendused	79f10062-e71a-421e-9b68-44e16533710b	RG-PROD-IT-AZ-SECURITY-WE	JAH
Azure Sentinel Responder	Azure Resource	Azure infoturbe ja halduslahendused	79f10062-e71a-421e-9b68-44e16533710b	RG-PROD-IT-AZ-SECURITY-WE	JAH
Azure Sentinel Contributor	Azure Resource	Azure infoturbe ja halduslahendused	79f10062-e71a-421e-9b68-44e16533710b	RG-PROD-IT-AZ-SECURITY-WE	JAH
Log Analytics Contributor	Azure Resource				
Log Analytics Reader	Azure Resource				
Logic Apps Contributor	Azure Resource				
Logic Apps Operator	Azure Resource				
Helpdesk Administrator	Entra ID				
Authentication Administrator	Entra ID				
User Administrator	Entra ID				
Billing Administrator	Entra ID				
Desktop Analytics Administrator	Entra ID				
Cloud Device Administrators	Entra ID				
Intune Administrator	Entra ID				
License Administrator	Entra ID				
Privileged Role Administrator	Entra ID				
Service Support Administrator	Entra ID				
SharePoint Administrator	Entra ID				
Teams Administrator	Entra ID				
Global Administrator	Entra ID				
Grupi Omanik					Andrus Toru
Kasutajad					Malle Puu, Kalle Maasikas
Märkmed					

Conditional Access Reeglid

Tingimusliku ligipääsu reeglite tabelis peab ära kirjeldama kõik reeglid ja sihtrühmad, mida planeeritakse rakendada. Need reeglid reguleerivad ära kõige olulisemad tingimused teenuste tarbimiseks.

Poliitika	Kirjeldus	Sihtrühm	Seadistatud
GRANT - Require 2FA for Administrators	Mitmetasemeline kontroll on alati nõutud administraatoritel	Administraatorid	
GRANT - Require 2FA for Azure Management	Mitmetasemeline kontroll on alati nõutud Azure halduse	Kasutajad / Administraatorid	
CONFIGURE - Sign-in frequency control	Kasutaja sessiooni pikkus	Administraatorid	
REQUIRE - Entra ID MFA registration from registered workstation	Mitmetasemeline kontroll lubatakse seadistada ainult usaldatud asukohtades	Kasutajad / Administraatorid	
GRANT - Require 2FA for M365 Licensed Users	Mitmetasemeline kontroll on nõutud Microsoft 365 teenustel	Kasutajad	
GRANT - Require approved client app for mobile devices (MAM)	Nutiseadmetes saab pilveteenuseid tarbida ainult asutuse hallatud rakendustest	Kasutajad	
GRANT - Require compliant device for supported platforms	Seade peab vastama asutuse infoturbe standardile	Kasutajad	
REQUIRE - Terms of use	Teenuste kasutustingimused	Kasutajad	

Azure Subscriptions

Ettevõtte kõik paigaldatud kulupõhised teenused.

Subscriptioni Nimi	Subscription ID	Kirjeldus
Azure infoturbe ja halduslahendused	79f10062-e71a-421e-9b68-44e16533710b	Pilvepõhised infoturbe teenused nagu Microsoft Sentinel, Azure Log Analytics jne

9.4 Entra ID infoturbe sätete seadistamine

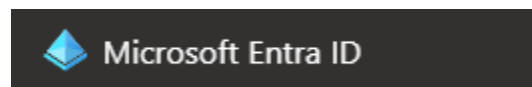
9.4.1 Gruppide loomine

Vastavalt Administratiivmodeli Exceli tabelile on vaja luua neli erinevat gruppi teatud infoturbe meetmete kasutamiseks:

- AAD-AR-SEC-TEMPORARY-ACCESS-PASS
- AAD-AR-SEC-FIDO2-SECURITY-KEYS
- AAD-AR-SEC-EXCLUDED-FROM-CA
- AAD-AR-SEC-CLOUD-ADMINISTRATORS

Kõik need grupid on **Security** tüüpi grupid ja Entra ID rolle ei pea saama neile määrata.

1. Azure portaalis olles valige **Microsoft Entra ID**



2. Valige **Groups**

3. Valige **New Group**

4. **New Group** lehel täita ära järgmised väljad:

- a. **Group Type:** Security
- b. **Group Name:** AAD-AR-SEC-TEMPORARY-ACCESS-PASS
- c. **Group Description:** Lubab kasutajatel kasutada Entra ID ajutisi autentimise passe
- d. **Microsoft Entra roles can be assigned to the Group:** No
- e. **Membership type:** Assigned
- f. Omanikud ja liikmed jätta tühjaks

5. Vajuta **Create**

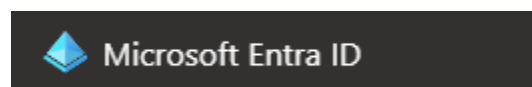
6. Nüüd järgi samu samme ja loo ülejäänud kolm gruppi.

7. Peale nende sammude järgimist peaks olema neli erinevat Entra ID gruppi

<input type="checkbox"/>	Name ↑	Object Id	Group Type	Membership Type
<input type="checkbox"/>	AA AAD-AR-SEC-CLOUD-ADMINISTRATORS	7a649bf8-a8b8-49e0-9f19-ff49aa66c561	Security	Assigned
<input type="checkbox"/>	AA AAD-AR-SEC-EXCLUDED-FROM-CA	39ce5bd6-f552-43bc-bd00-44b1d22a9146	Security	Assigned
<input type="checkbox"/>	AA AAD-AR-SEC-FIDO2-SECURITY-KEYS	3a8aafbf-11ea-4749-8e72-d0f5cdc8f62e	Security	Assigned
<input type="checkbox"/>	AA AAD-AR-SEC-TEMPORARY-ACCESS-PASS	ac1a58b6-9a59-460d-8e5e-1b29c319068a	Security	Assigned

9.4.2 Infoturbe sätete seadistamine

1. Azure portaalis olles valige **Microsoft Entra ID**



2. Entra ID konfiguratsiooni paneelil valige **Security**

3. Valige **Authentication Methods**

4. **Authentication Policies** lehel valige **FIDO2 Security Key**

5. **FIDO2 Security Key** settings lehel lülitage **FIDO2** võtmete kasutamine sisse
6. Sihtrühmaks valige **Select Users** ja valige **AAD-AR-SEC-FIDO2-SECURITY-KEYS** grupp

FIDO2 Security Key settings ...

Basics Configure

ENABLE

Yes No

USE FOR:

- Sign in
- Strong authentication

TARGET

All users Select users

Add users and groups

Name

AAD-AR-SEC-FIDO2-SECURITY-KEYS

7. Vajutage **Save**
8. **Authentication Policies** lehel valige **Temporary Access Pass**
9. **Temporary Access Pass** lehel lülitage funktsionaalsus sisse
10. Sihtrühmaks valige **Select Users** ja valige **AAD-AR-SEC-TEMPORARY-ACCESS-PASS** grupp
11. Valige **Configure** leht ja vajutage **Edit** nuppu
12. **Temporary Access Pass** seadistuste lehel saate täpsustada ajutiste koodide keerukuse ja kui mitu korda konkreetset genereeritud koodi saab kasutada. Oma ettevõtte siseselt leppige vastavad reeglid kokku. Siin juhendis tõstetakse koodi pikkust kuni 16 täheni ja lubatakse koodi kasutada ainult ühe korra. Ajutisi koode kasutatakse turvavõtmete seadistamisel.

Temporary Access Pass settings ×

Temporary Access Pass is a time-limited passcode that serves as strong credentials and allow onboarding of passwordless credentials. The Temporary Access Pass authentication method policy can limit the duration of the passes in the tenant between 10 minutes to 30 days. [Learn more](#)

Minimum lifetime

Minutes
 Hours
 Days

hour

Maximum lifetime

Minutes
 Hours
 Days

hours

Default lifetime

Minutes
 Hours
 Days

hour

Length (characters)

✓

Require one-time use

Yes
 No

13. Vajutage **Update**

14. Vajutage **Save**

9.5 Avariikontode seadistamine

Enne teiste seadistamisega jätkamist on vaja luua kaks Entra ID avariikontot. Avariikontosid kasutatakse ainult juhul, kui me oleme kogemata ennast ära lukustanud tingimusliku reeglite tõttu või mingil põhjusel ei suudeta tingimuslikke reegleid töödelda. Avariikontod lisame **AAD-AR-SEC-EXCLUDED-FROM-CA** gruppi ja neile tingimuslikke reegleid ei rakendata. Mõlemad kontod peaksid olema seadistatud turvavõtmetega, mis omakorda peavad olema füüsiliselt seifi pandud. Mõlemaid kontosid tuleks regulaarselt kord kvartalis testida. Kontode monitooring seadistatakse eraldi Sentinelis.

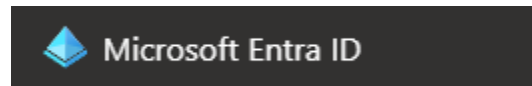
Avariikontode loomisel ei tohi kindlasti kasutada üldlevinud nimesid nagu breakaccount, breaktheclassaccount jne. Kontode loomisel kasutage kokkulepitud eesliideste tähti ja suvaliselt genereeritud numbreid. Siin juhendis on meil eesliideseks **AADBA** ja peale seda 12 suvaliselt genereeritud numbrit:

- AADBA-289858086761
- AADBA-815895247538

Oma keskkonna seadistamisel palume avariikontod nimetada teisiti. Avariikontosid tuleks igapäevaseks kasutamiseks mõeldud seadmest mitte kasutada. Avariikontode ligipääs peab olema eraldi reguleeritud. Avariikontod hakkavad olema ainukesed alalised Entra ID Globaalsed administraatorid. Kõik teised kontod on hallatud läbi Privileged Identity Management teenuse.

9.5.1 Avariikontode loomine

1. Azure portaalis olles valige **Microsoft Entra ID**



2. Valige **Users**
3. Valige **+New User**
4. New user lehel täita järgmised väljad:
 - a. **User Name:** AADBA-289858086761. Domeeniks jätta ettevõtte Entra ID teenuse nimi.
 - b. **Name:** AADBA-289858086761
 - c. **Password:** Genereerida pikk ja keeruline parool. Parooli maha salvestada ei ole vaja. Kontode kasutus saab olema ainult läbi turvavõtmete.
 - d. **Roles**
 - i. Global Administrator
 - e. **Usage location:** Estonia

Identity

User name * @

The domain name I need isn't shown here

Name *

First name

Last name

Password

Auto-generate password

Let me create the password

Initial password *

5. Peale seda on loodud esimene Entra ID avariikonto

<input type="checkbox"/>	AADBA-289858086761	AADBA-289858086761@m365x982850.onmicrosoft.com	Member
--------------------------	--------------------	--	--------

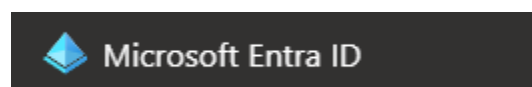
6. Nüüd järgige samu samme ja looge juurde teine avariikonto

7. Peale kõikide sammude järgimist peaks nüüd olema kaks avariikontot

<input type="checkbox"/>	AADBA-289858086761	AADBA-289858086761@m365x982850.onmicrosoft.com	Member	No
<input type="checkbox"/>	AADBA-815895247538	AADBA-815895247538@m365x982850.onmicrosoft.com	Member	No

9.5.2 Gruppidesse lisamine

1. Azure portaalis olles valige **Microsoft Entra ID**



2. Valige **Groups**
3. Lisage mõlemad avariikontod järgmistesse gruppidesse:
 - a. AAD-AR-SEC-TEMPORARY-ACCESS-PASS
 - b. AAD-AR-SEC-FIDO2-SECURITY-KEYS
 - c. AAD-AR-SEC-EXCLUDED-FROM-CA
4. Valige **AAD-AR-SEC-TEMPORARY-ACCESS-PASS** grupp

5. Valige **Members**
6. Valige **+Add Members**
7. Lisage mõlemad avariikontod
8. Vajutage **OK**
9. Järgige nüüd samu samme teiste gruppide puhul

9.5.3 Kombineeritud infoturbe info registreerimine

1. Azure portaalis olles valige **Microsoft Entra ID**



2. Valige **User settings**
3. Valige **Manage user feature settings**
4. Lülitage sisse **Users can use the combined security information registration experience**. Vastav poliitika peab olema rakendatud kõikidele kasutajatele.

9.5.4 Parooli poliitikate seadistamine

1. Kopeerige oma haldus masinasse **Entra ID - Avariikontode-ParooliPoliitikateMuutmise.ps1** PowerShell'i skript. Vastav skript on kaasas koos juhendiga.
2. Avage skript administraator õigustega **PowerShell ISE**'s. Käskude edukaks kasutamiseks on vaja paigaldada Microsoft Graph PowerShell'i moodul. Moodul laetakse automaatselt alla <https://www.powershellgallery.com/> lehelt.
3. Skript võtab maha paroolide muutmise nõude avariikontodel. Vastavas skriptis on vaja muuta rida **15** ja **16**. Sisestage sinna oma avariikontode nimed.

```

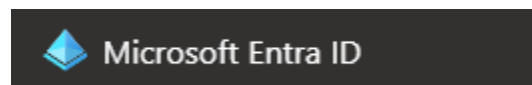
1 #Microsoft Graph PowerShell'i mooduli paigaldamine
2 Install-Module -Name Microsoft.Graph -Force -Verbose
3
4 #Ühenda Microsoft Graph külge. Erinevad tegevused nõuavad erinevaid õigusi. Palun loe dokumentatsioonist vajadusel juurde,
5 #kui soovid muid muudatusi teha.
6 $Scopes = @(
7     "user.Readwrite.All",
8     "user.Read.All",
9     "Directory.AccessAsUser.All"
10 )
11
12 Connect-MgGraph -Scopes $Scopes
13
14 #Avariikontode nimed
15 $Avariikonto1 = "SIESTA SIIA OMA AVARIIKONTO 1 UPN"
16 $Avariikonto2 = "SIESTA SIIA OMA AVARIIKONTO 2 UPN"
17
18 $Parameetrid = @{}
19     "passwordProfile" = @{
20         "forceChangePasswordNextSignIn" = $false
21     }
22 }
23 Update-MgUser -UserId $Avariikonto1 -BodyParameter $Parameetrid
24 Update-MgUser -UserId $Avariikonto2 -BodyParameter $Parameetrid

```

4. Kui vastavad muudatused on tehtud, siis käivitage skript.

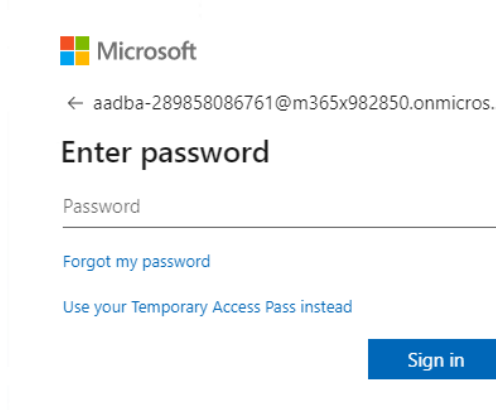
9.5.5 Turvavõtmete seadistamine

1. Azure portaalis olles valige **Microsoft Entra ID**



2. Valige **Users**
3. Valige üks oma avariikontodest
 - a. AADBA-289858086761@m365x982850.onmicrosoft.com

4. Avariikonto profiili lehel valige **Authentication Methods**
5. Kui näete teadet „**Switch to the new user authentication methods experience! Click here to use it now**“, siis vajutage selle peale
6. Valige **+Add Authentication Method**
7. **Add Authentication Method** lehel valige **Temporary Access Pass**
8. Vajutage **Add** ja salvestage informatsioon
9. Vajutage **OK**
10. Avage veebilehitsejaga uus aken ja avage <https://aka.ms/mysecurityinfo> aadress
11. Sisestage avariikonto nimi ja vajutage **Next**
12. **Enter Password** lehel valige „**Use your Temporary Access Pass instead**“



13. Sisestage **Temporary Access Pass** ja vajutage **Sign In**
14. Security Info lehel valige **+Add Method**
15. Add a method lehel valige **Security Key**
16. Vajutage **Add**
17. **Security Key** lehel valige **Next**
18. Valige **USB device** tüüpi seade
19. Sisestage turvavõti **USB** või **USB-C** pessa
20. **Security Key setup** lehel valige **OK**
21. **Continue Setup** lehel valige **OK**
22. Sisestage 8-12 kohaline PIN kood ja vajutage **OK**
23. Peale seda peaks turvavõti edukalt lisatud olema
24. Eemaldage eelnevalt lisatud **Temporary Access Pass** avariikonto alt
25. Nüüd järgige samu samme ka teisel avariikontol. Peale seda peaks mõlemad avariikontod olema seadistatud turvavõtmetega,

9.5.6 Avariikontode objekti ID´de tuvastamine

1. Azure portaalis olles valige **Microsoft Entra ID**



2. Valige **Users**
3. Valige üks oma avariikontodest
4. Avariikonto profiili lehel peaksite nägema **Object ID** välja

Identity

Name

AADBA-289858086761

User Principal Name

AADBA-289858086761@m365x982850.onmicrosoft.com

Object ID

6a5e6ed9-d986-4506-9f43-bcf3a672fc32

5. Kopeerige vastav **ID** Notepadi
6. Tehke sama ka teise kontoga
7. Nüüd peaks Teil olema mõlema avariikonto objekt ID´d. Neid sammuseid ID´sid kasutatakse Sentinelis analüütika reegli defineerimisel. Kui keegi peaks neid kontosid kasutama, siis luuakse Sentineli automaatselt kõrge taseme intsident.

9.5.7 Monitooringu seadistamine Sentinel teenuses

1. Azure portaalis olles trükkige otsingusse **Sentinel**



2. Valige **Microsoft Sentinel**
3. Valige oma Sentineli keskkond
4. Sentineli konfiguratsiooni paneelilt valige Analytics
5. Analytics lehel valige **Create** ja määrake uue analüütika reegli tüübiks **NRT Query rule**.
6. **Analytics rule wizard - Create a new NRT rule General** lehel täitke ära järgmised väljad
 - a. **Name:** Entra ID avariikontode kasutamine
 - b. **Description:** Keegi on proovinud kasutada või on edukalt loginud sisse Entra ID avariikontoga
 - c. **Severity:** High
 - d. **Status:** Enabled
7. Vajutage **Next: Set rule logic**
8. **Set rule logic** lehel sisestage analüütika reegel. Juhendiga on kaasas näidis analüütika reegel Entra ID avariikontode jaoks. Avage fail nimega Avariikontode kasutamine.txt ja muutke objekti ID´d vastavalt ettevõtte keskkonna järgi. Punasega märgitud objekti ID´d asendage oma ID´dega.

```

SigninLogs
| where UserId == "6a5e6ed9-d986-4506-9f43-bcf3a672fc32" or UserId == "b4158701-d788-4891-bfee-d047d2dadca8"
| where Status.errorCode == 0
| extend AccountCustomEntity = Identity
| extend IPCustomEntity = IPAddress
| extend HostCustomEntity = SourceSystem

```

Rule query

The rule will run once every minute, and will capture events with an ingestion time in the past minute ⓘ

```

SigninLogs
| where UserId == "6a5e6ed9-d986-4506-9f43-bcf3a672fc32" or UserId == "b4158701-d788-4891-bfee-d047d2dadca8"
| where Status.errorCode == 0
| extend AccountCustomEntity = Identity
| extend IPCustomEntity = IPAddress
| extend HostCustomEntity = SourceSystem

```

[View query results >](#)

Your query is limited to a single table and to watchlists.

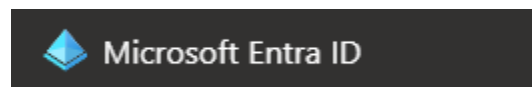
9. Vajutage **Next: Incident Settings**
10. **Incident Settings** lehel jätkake vaike väärtused ja valige **Next**
11. **Automated Response** lehel valige **Next**
12. **Review and create** lehel kontrollige vastav informatsioon üle ja vajutage **Create**
13. Peale vastavaid samme peaks olema analüütika reegel, mis kontrollib avariikontode kasutamist.

9.6 Administraatorite kontode seadistamine

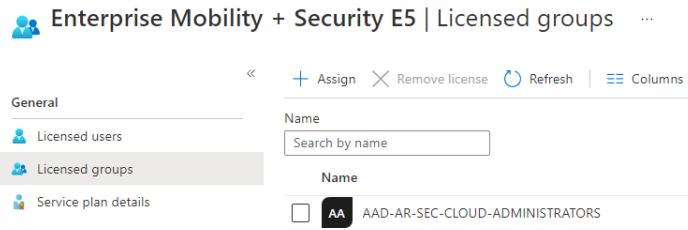
Avariikontod on seadistatud ja saab jätkata kõigi teiste kontode ja gruppide loomisega. Administraatorite kontosid tuleb luua täpselt nii palju, kui on vaja. Selles juhendis luuakse näidiseks üks näidis roll algusest lõpuni koos administraator kontoga. Oma keskkonnas tuleb suure tõenäosusega luua neid rohkem. Administraatorikontode loomiseks on oluline, et oleks olemas vastav nimede standard.

9.6.1 Litsentside määramine

1. Azure portaalis olles valige **Microsoft Entra ID**

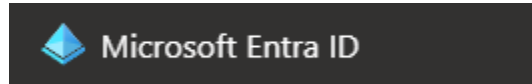


2. Valige **Licenses**
3. Valige **All Products**
4. Valige oma litsentsid mida Te olete administraatoritele soetanud. Siin juhendis on soetatud Enterprise Mobility + Security E5 litsentsid.
5. Valige **Licensed groups Enterprise Mobility + Security E5** lehel
6. Valige **Assign**
7. Assign **License** lehel **+add users and groups**
8. Otsige **AAD-AR-SEC-CLOUD-ADMINISTRATORS** pilve administraatorite grupp
9. Vajutage **Select**
10. Vajutage **Review + Assign**
11. Vajutage **Assign**



9.6.2 Konto loomine

1. Azure portaalis olles valige **Microsoft Entra ID**



2. Valige **Users**
3. Valige **+New User**
4. New user lehel ära täita järgmised väljad:
 - a. **User Name:** Malle.Puu.CA. Domeeniks jätta ettevõtte Entra ID teenuse nimi.
 - b. **Name:** Malle.Puu.CA
 - c. **Password:** Genereerida pikk ja keeruline parool. Parooli maha salvestama ei pea. Kontode kasutus saab olema ainult läbi turvavõtmete.
 - d. **Groups:**
 - i. Lisage kasutaja järgmistesse grupidesse
 1. AAD-AR-SEC-TEMPORARY-ACCESS-PASS
 2. AAD-AR-SEC-FIDO2-SECURITY-KEYS
 3. AAD-AR-SEC-CLOUD-ADMINISTRATORS
 - e. **Usage location:** Estonia

Identity

User name *	Malle.Puu.CA ✓	@	m365x982850.onmicroso... ✓	
<small>The domain name I need isn't shown here</small>				
Name *	Malle.Puu.CA ✓			
First name	Malle ✓			
Last name	Puu ✓			

5. Peale seda peaks olema üks uus pilve administraatori konto

<input type="checkbox"/>	Malle.Puu.CA	Malle.Puu.CA@m365x982850.onmicrosoft.com	Member	No
--------------------------	--------------	--	--------	----

9.6.3 Parooli poliitikate seadistamine

1. Kopeerige oma haldus seadmesse **Entra ID - PilveAdministraatoriteKontode-Seadistamine.ps1** PowerShell'i skript. Vastav skript on kaasas koos juhendiga.
2. Avage skript administraator õigustega PowerShell ISE's. Käskude edukaks kasutamiseks on vaja paigaldada Microsoft Graph PowerShell'i moodul. Moodul laetakse automaatselt alla <https://www.powershellgallery.com/> lehelt.

- Skript võtab maha paroolide muutmise nõude administraator kontodel. Vastavas skriptis on vaja muuta rida **15**. Sisestage sinna administraatori konto UPN (User Principal Name).

```

1 #Microsoft Graph Powershelli mooduli paigaldamine
2 Install-Module -Name Microsoft.Graph -Force -Verbose
3
4 #Ühenda Microsoft Graph külge. Erinevad tegevused nõuavad erinevaid õigusi. Palun loe dokumentatsioonist vajadusel juurde,
5 #kui soovid muid muudatusi teha.
6 $Scopes = @(
7     "User.Readwrite.All",
8     "User.Read.All",
9     "Directory.AccessAsUser.All"]
10 )
11
12 Connect-MgGraph -Scopes $Scopes
13
14 #Avariikontode nimed
15 $Administraatorikonto = "SISESTA SIIA PILVE ADMINISTRAATORI KONTO UPN"
16
17 $Parameetrid = @{
18     "passwordProfile" = @{
19         "forceChangePasswordNextSignIn" = $false
20     }
21 }
22 Update-MgUser -UserId $Administraatorikonto -BodyParameter $Parameetrid

```

- Kui vastavad muudatused on tehtud, siis käivitage skript.

9.6.4 Turvavõtmete seadistamine

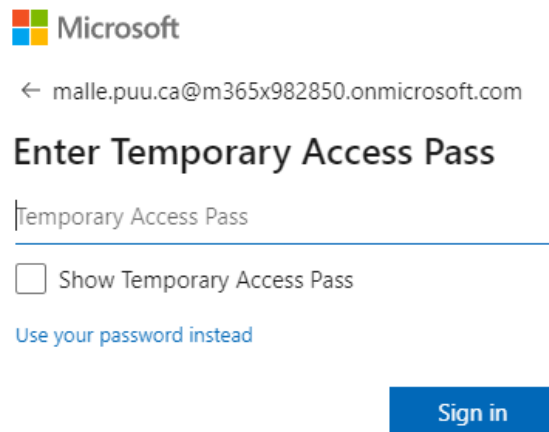
- Azure portaalis valige **Microsoft Entra ID**



- Valige **Users**
- Valige vastloodud pilve administraatori konto
- Konto profiili lehel valige **Authentication Methods**
- Kui Te näete teadet „**Switch to the new user authentication methods experience! Click here to use it now**“, vajutage selle peale
- Valige **+Add Authentication Method**
- Add Authentication Method** lehel valige **Temporary Access Pass**
- Vajutage **Add** ja salvestage informatsioon
- Vajutage **OK**

Vastav informatsioon tuleb edastada administraatorile, kes seadistab oma kontole turvavõtme. Avariikontode puhul tegite kõik sammud ise, nüüd tuleb väljastada teistele administraatorile võtme aktiveerimiseks turvavõti ja ajutine pass. Hea oleks luua juhend, kuidas võtmeid kasutada ja aktiveerida.

- Avage veebilehitsejaga uus aken ja avage <https://aka.ms/mysecurityinfo> aadress
- Sisestage nimi ja vajutage **Next**
- Enter Password** lehel valige „**Use your Temporary Access Pass instead**“



The screenshot shows the Microsoft 365 login interface. At the top left is the Microsoft logo. Below it is a back arrow and the email address 'malle.puu.ca@m365x982850.onmicrosoft.com'. The main heading is 'Enter Temporary Access Pass'. There is a text input field containing 'Temporary Access Pass'. Below the input field is a checkbox labeled 'Show Temporary Access Pass'. A link 'Use your password instead' is visible below the checkbox. At the bottom right is a blue 'Sign in' button.

4. Sisestage **Temporary Access Pass** ja vajutage **Sign In**
5. **Security Info** lehel valige **+Add Method**
6. **Add a method** lehel valige **Security Key**
7. Vajutage **Add**
8. **Security Key** lehel valige **Next**
9. Valige **USB device** tüüpi seade
10. Sisestage turvavõti **USB** või **USB-C** pessa
11. **Security Key setup** lehel valige OK
12. **Continue Setup** lehel valige OK
13. Sisestage 6-8 kohaline PIN kood ja vajutage OK
14. Peale seda peaks turvavõti edukalt lisatud olema
15. Eemaldage eelnevalt lisatud **Temporary Access Pass**
16. Nüüd peaks võti olema kasutatav

9.6.5 Gruppide loomine

Juhendi järgi on *Malle Puu* määratud infoturbe osakonda, selleks tuleb luua AR-SEC-PIM-SECURITY-ENGINEER Entra ID grupp.

1. Azure portaalis valige **Microsoft Entra ID**



2. Valige **Groups**
3. Valige **New Group**
4. New Group lehel täida järgmised väljad:
 - a. **Group Type:** Security
 - b. **Group Name:** AR-SEC-PIM-SECURITY-ENGINEER
 - c. **Group Description:** Lilleke75 infoturbe töötajad
 - d. **Entra roles can be assigned to the Group:** Yes. Siin oluline saada nendele gruppidele määrata rolle

e. **Membership type:** Assigned

f. Omanikud ja liikmed jätta tühjaks

Group type * ⓘ
Security

Group name * ⓘ
Enter the name of the group

Group description ⓘ
Enter a description for the group

Microsoft Entra roles can be assigned to the group ⓘ
Yes No

Membership type ⓘ
Assigned

Owners
No owners selected

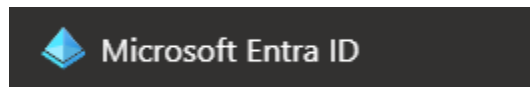
Members
No members selected

Roles
No roles selected

5. Vajutage **Create**

6. Nüüd peaks olema vajalik grupp Lilleke75 infoturbe töötajatele. Samasid samme kasuta ka teiste gruppide loomiseks teiste osakonna töötajate jaoks.

9.6.6 Gruppide seadistamine

1. Azure portaalis valige **Microsoft Entra ID**2. Valige **Groups**

3. Valige AR-SEC-PIM-SECURITY-ENGINEER grupp

4. AR-SEC-PIM-SECURITY-ENGINEER grupi lehelt valige **Privileged Access**5. Vali **Enable Privileged Access**

Enable Privileged Access

Privileged Access Groups enable just-in-time (JIT) access to the Owner or Member role of this group. JIT access by Azure AD PIM provides enhanced security for owners with delegated administrative tasks.

Enable privileged access

6. **Privileged Access** lehel valige **Eligible Assignments** paneel

+ Add assignments Settings Refresh Export | Got feedback?

Eligible assignments Active assignments Expired assignments

7. Valige + **Add assignments**8. **Add assignment** lehel määrata **Select Role** tüübiks **Member**9. Vajuta **No member selected** peal10. **Select a member Group** lehel valige Malle Puu11. Vajutage **Select**

12. Vajutage **Next**

13. **Setting** lehel määratakse, kui kaua saab Malle Puu olla selle grupi liige. Hetkel jääb selleks 1 aasta. Vastavalt ettevõtte poliitikatele on õigus määrata erinevaid perioode. Kui aeg saab läbi, siis kasutaja saab küsida pikendust. Tegemist on hea järelvalve meetoditega vältimaks õiguste aegumist. Vastavalt poliitikatele tuleb õigused regulaarselt üle vaadata.

14. Vali **Assign**

15. Nüüd on Malle Puule antud õigus küsida ennast Lilleke75 infoturbe töötajate gruppi. Vastav grupp ei anna Mallele õigusi koheselt vaid selle grupi kaudu hakkab ta nägema talle väljastatud õigusi.

Eligible assignments		Active assignments	Expired assignments
<input type="text" value="Search by member name or principal name"/>			
Name	Principal name		
Member			
Malle.Puu.CA	Malle.Puu.CA@m365x982850.onmicrosoft.com		

9.6.7 Entra ID Gruppide PIM rollide seadistamine

Järgmised gruppide sätted tuleb vastavalt ettevõtte analüüsile seadistada. Samu seadistusi saab ka seadistada Entra ID rollidele ja Excelis on need defineeritud „**Entra ID PIM Rollid**“ lehel.

1. Azure portaalis valige **Microsoft Entra ID**



2. Valige **Groups**

3. Valige AR-SEC-PIM-SECURITY-ENGINEER grupp

4. AR-SEC-PIM-SECURITY-ENGINEER grupi lehelt valige **Privileged Access**

5. **Privileged Access** lehel valige **Settings**

6. Valige **Member**

7. **Role setting details – Member** lehel valige **Edit**

8. **Role setting details – Member activation** lehel lisage järgmine info

- Activation maximum duration (hours):** näiteks 4 tundi. Sensitiivsemad grupid ja õigused võiksid olla kuni 1 tund.
- On activation, require:** Azure MFA kindlasti igale rollile
- Require justification on activation:** Jah kindlasti. Põhjendus peaks olema juures igas aktivatsioonis. Selle järgi on hiljem hea teha õiguste küsimuste analüüsi.
- Require ticket on activation.** Seda oleks hea küsida suuremate õiguste küsimusel.
- Require approval to activate.** See peaks olema seadistatud kindlasti Entra ID Global Administrator ja Exchange Administrator rollidele. Vajadusel saab ka lisada teistele.

Activation Assignment Notification

Activation maximum duration (hours)

----- 4

On activation, require

None

Azure MFA

[Learn more](#)

Require justification on activation

Require ticket information on activation

Require approval to activate

Select approver(s)

No approver selected

9. Valige **Assignment** leht. Siin saate ära defineerida, kui pikalt keegi saab mingis rollis olla.

Edit role setting - Member ...

Privileged Identity Management | Privileged access groups (Preview)

Activation Assignment Notification

Allow permanent eligible assignment

Expire eligible assignments after

1 Year

Allow permanent active assignment

Expire active assignments after

6 Months

Require Azure Multi-Factor Authentication on active assignment

Require justification on active assignment

10. Valige **Notification** leht. Õiguste aktiveerimisel ja rollide muudatuste puhul on võimalik defineerida erinevaid lisa emaili aadresse. Sisestage kõik need kontaktid, kellele tuleks vastavaid teavitusi saata.

Activation Assignment Notification

Send notifications when members are assigned as eligible to this role:

Type	Default recipients	Additional recipients	Critical emails only
Role assignment alert	<input checked="" type="checkbox"/> Admin	<input type="text" value="Email IDs separated by semicolon"/>	<input type="checkbox"/>
Notification to the assigned user (assignee)	<input checked="" type="checkbox"/> Assignee	<input type="text" value="Email IDs separated by semicolon"/>	<input type="checkbox"/>
Request to approve a role assignment renewal/extension	<input checked="" type="checkbox"/> Approver	<input type="text" value="Email IDs separated by semicolon"/>	<input type="checkbox"/>

Send notifications when members are assigned as active to this role:

Type	Default recipients	Additional recipients	Critical emails only
Role assignment alert	<input checked="" type="checkbox"/> Admin	<input type="text" value="Email IDs separated by semicolon"/>	<input type="checkbox"/>
Notification to the assigned user (assignee)	<input checked="" type="checkbox"/> Assignee	<input type="text" value="Email IDs separated by semicolon"/>	<input type="checkbox"/>
Request to approve a role assignment renewal/extension	<input checked="" type="checkbox"/> Approver	<input type="text" value="Email IDs separated by semicolon"/>	<input type="checkbox"/>

Send notifications when eligible members activate this role:

Type	Default recipients	Additional recipients	Critical emails only
Role activation alert	<input checked="" type="checkbox"/> Admin	<input type="text" value="Email IDs separated by semicolon"/>	<input type="checkbox"/>
Notification to activated user (requestor)	<input checked="" type="checkbox"/> Requestor	<input type="text" value="Email IDs separated by semicolon"/>	<input type="checkbox"/>
Request to approve an activation	<input checked="" type="checkbox"/> Approver	<input type="text" value="Only designated approvers can receive this email"/>	<input type="checkbox"/>

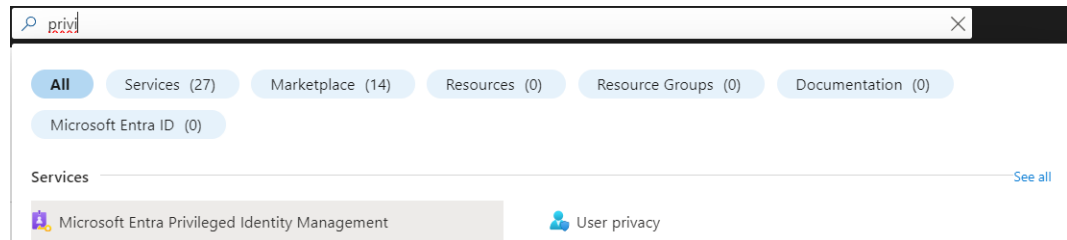
11. Vajutage **Update**

12. Valige **Owner** ja seadistage samad sätted.

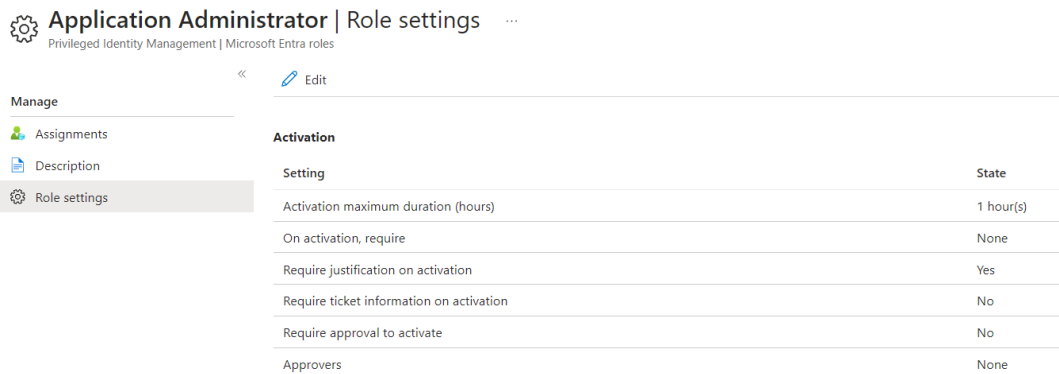
13. Taolisi seadistusi tuleb teha iga Entra ID rolli grupi kohta, mida oma ettevõtte loote.

9.6.8 Microsoft Entra PIM rollide seadistamine

1. Azure portaalis olles trükkige otsingusse „Privi“

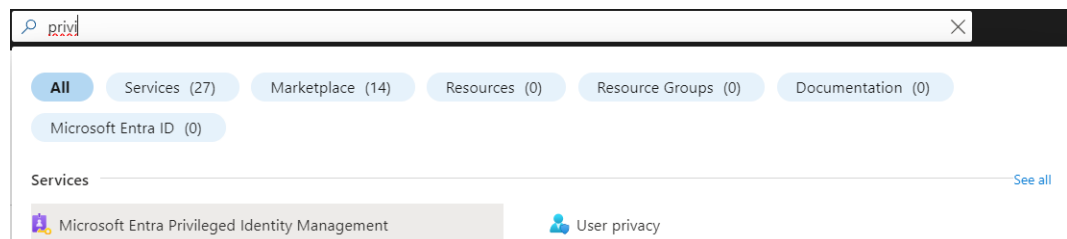


2. Valige **Microsoft Entra Privileged Identity Management**
3. Valige **Entra Roles**
4. Valige **Roles**
5. Nüüd peaks näitama nimekirja kõikidest rollidest, mis on ettevõtte Entra ID keskkonnas.
6. Valige näiteks **Application Administrator**
7. Valige **Role Settings**
8. Nüüd peaksite nägema juba tuttavaid küsimusi. Ettevõtte pead administraatorina peaksite kõik need rollid seadistama vastavalt kokkulepitud poliitikatele. Samu seadistused tehti eelnevalt ka oma loodud PIM gruppidele.



9.6.9 Õiguste määramine

1. Azure portaalis olles trükkige otsingusse „Privi“



2. Valige **Microsoft Entra Privileged Identity Management**
3. Valige **Entra Roles**
4. Valige **Roles**
5. Rollide nimekirjast valige **Global Reader**

6. **Global Reader** konfiguratsiooni paneelis veenduge, et oleks valitud **Eligible Assignments** leht
7. Valige + **Add Assignment**
8. Valige **no member selected** ja lisage AR-SEC-PIM-SECURITY-ENGINEER grupp
9. Valige **Select**
10. Valige **Next**
11. Valige **Assign**
12. AR-SEC-PIM-SECURITY-ENGINEER grupi liikmed saavad küsida nüüd Global Reader õigusi.
13. Järgige samu samme ja delegeerige **AR-SEC-PIM-SECURITY-ENGINEER** grupile järgmised õigused:
 - a. Security Administrator
 - b. Security Operator
 - c. Security Reader
14. Nüüd peaks AR-SEC-PIM-SECURITY-ENGINEER grupp omama järgmisi õigusi

+ Add assignments | Refresh | Got feedback?

Eligible assignments | Active assignments | Expired assignments

Search by role

Role	↑↓	Principal name	Scope	↑↓	Membership
Global Reader			Directory		Direct
Security Operator			Directory		Direct
Security Reader			Directory		Direct
Security Administrator			Directory		Direct

Neid samme järgides on loodud Malle Puule „pilv ainult“ administraatori konto, infoturbe administraatorite privilegeeritud haldusega seotud grupp ja määratud sellele grupile nelja erineva õiguse küsimise võimalus.

9.6.10 Konto testimine ja õiguste aktiveerimine

1. Sisestage turvavõti **USB** või **USB-C** pessa
2. Avage veebilehitseja ja avage **portal.azure.com**
3. Valige **Sign-in options**
4. Valige **Sign in with a security key**
5. Sisestage PIN kood ja vajutage OK. Osade võtmete puhul tuleb neid ka peale PIN koodi sisestamist puudutada.
6. Eduka sisselogimise korral peaks avanema Azure portaal.
7. Azure portaalis olles otsige otsingust „Privi“ ja valige otsingust „**Privileged Identity Management**“
8. **Privileged Identity Management | Quick start** lehelt valige **My Roles**
9. **My Roles** lehelt valige **Privileged Access Groups**

10. My roles | Privileged access groups lehel peaks nägema oma rolli gruppi.

Eligible assignments						Active assignments		Expired assignments	
Search by role or group									
Role	Group	Group type	Membership	End time	Action				
Member	AR-SEC-FIM-SECURITY-ENGINEER	Security	Direct	12/12/2022, 9:16:59 PM	Activate Extend				

11. Valige **Activate**

12. Sisestage põhjendus ja kui kauaks õigusi soovite saada.

13. Vajutage **Activate**

14. Nende sammude peale aktiveeritakse ainult vastava grupi liikmelisus. Õigusi veel nende sammudega ei väljastata.

15. Nüüd peakite nägema ka teadet „**You have just activated a role. Click here to view your Active roles**“

16. My roles | Microsoft Entra roles lehelt valige **Entra Roles**

17. Nüüd peaksite nägema nelja erinevat **Entra ID** rolli, mis on sellele grupile määratud.

Eligible assignments				Active assignments		Expired assignments	
Search by role							
Role	Scope	Membership					
Global Reader	Directory	Group					
Security Operator	Directory	Group					
Security Reader	Directory	Group					
Security Administrator	Directory	Group					

18. Valige vastav roll ja vajutage **Activate**

19. Sisestage põhjendus ja kui kauaks õigusi soovite saada

20. Vajutage **Activate**

21. Kui kõik läks hästi, siis väljastati vajalikud õigused ja saate jätkata teenuste administreerimisega.

9.7 Tingimusliku ligipääsu reeglite seadistamine

Administraatorite kontod koos õigustega on nüüdseks seadistatud, aga hetkel saavad administraatorid oma kontosid kasutada igast seadmest ja asukohast. Selleks, et seda kõike reguleerida on vaja seadistada Entra Conditional Access reeglid. Conditional Access reeglid lubavad defineerida erinevates komponentidest koosnevaid poliitikaid, nagu seade, kasutaja, asukoht jne. Sõltuvalt ettevõtte enda riskide hindamisest, on võimalik teha poliitikaid erineva tasemega. Mõni ettevõtte võib blokeerida kõik kõrge taseme logimised, või neid siiski lubada, kuid nõuda mitmetasemelise kontrolli kinnitust või paroolivahetust.

Oluline ongi enne nende poliitikate seadistamist täpselt ära kaardistada, mis tingimustel saab pilve teenuseid administreerida ja kasutajatel andmeid tarbida.

Antud juhendis on välja toodud kõige olulisemad reeglid, mis on soovitatav rakendada.

Oluline!

Iga reegli seadistamisel veenduge, et kasutaksite **Report-Only** funktsionaalsust koos test grupiga. Kui olete veendunud, et kõik töötab soovikohaselt, siis lülitage test grupil Report-Only funktsionaalsus välja ja korrake katset. Kui koheselt rakendada uusi poliitikaid ilma

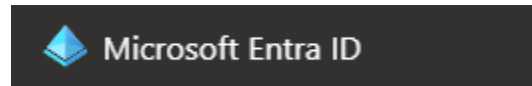
testimata, võivad konfiguratsiooni vea tõttu kõik teenused lukku minna ja kasutajatel tekib teenuste kasutamisel katkestus.

9.7.1 Reegel 1 – Require multi-factor authentication for Azure management

Loome poliitika, mis küsib alati Azure portaali sisenedes kasutajatelt või administraatoritelt mitmetasemelist kontrolli. Tingimusliku reegli defineerimisel on oht ennast täiesti pilvest välja lukustada. See tähendab, et mitte keegi ei saa enam pilve resurssidele ligi. Enne reeglite defineerimist veenduge, et avariikontod on olemas ja AAD-AR-SEC-EXCLUDED-FROM-CA gruppi lisatud. Enne igat reegli rakendamist on võimalik seadistada raporteerimise funktsionaalsus, et saada aru kuidas reegel töötab. Vajadusel tehke täiendavaid teste test kasutajate peal.

Vastavalt riskide analüüsi tulemusest on võimalus lisada juurde tingimused **Require Hybrid Entra joined device**, ehk seade peab tulema ettevõtte maapealsest Active Directory' st või **Require device to be marked as compliant**, ehk siis seade peab vastama ettevõtte infoturbe poliitikatele. Kui seadistate sarnaseid poliitikaid esmakordselt, alustage samm haaval ja tooge tingimusi järk-järgult juurde.

1. Azure portaalis valige **Microsoft Entra ID**



2. Valige **Security**
3. Valige **Conditional Access**
4. Valige **New Policy -> Create New Policy**
5. Uue **Conditional Access** reegli lehel lisage järgmine info:
 - a. Name: **Require multi-factor authentication for Azure management**
 - b. Users or workload identities
 - i. **Include**: All users
 - ii. **Exclude**: Valige AAD-AR-SEC-EXCLUDED-FROM-CA grupp, kus on avariikontod
 - c. Cloud apps or actions
 - i. **Include**: Microsoft Azure Management
 - d. Grant
 - i. Valige **Require multi-factor authentication** valik
6. **Enable policy** valige On.
7. Vajutage **Create**

Nüüd on loodud poliitika, mis nõuab alati mitmetasemelist kontrolli Azure portaali sisenedes.

9.7.2 Reegel 2 – Configure - Sign-in frequency

Järgmiseks seadistage poliitika, mis seadistab administraatorite sessiooni pikkuse ja määrab, millal peab mitte aktiivse sessiooni korral uuesti ennast autentima.

1. Azure portaalis olles valige **Microsoft Entra ID**



8. Valige **Security**
9. Valige **Conditional Access**
10. Valige **New Policy -> Create New Policy**
11. Uue Conditional Access reegli lehel lisage järgnev:
 - a. Name: **Configure - Sign-in frequency control**
 - b. Users or workload identities
 - i. **Include:** Valige AAD-AR-SEC-CLOUD-ADMINISTRATORS grupp
 - c. Cloud apps or actions
 - i. **Include:** All cloud apps
12. Session
 - a. Lülitage sisse **Sign-in frequency** ja määrake pikkuseks **1 tund**
 - b. Lülitage sisse **Persistent browser session** ja määrake selle seadistuse väärtuseks **Never persistent**
13. **Enable policy** valige On.
14. Vajutage **Create**

9.7.3 Reegel 3 – Require – Entra ID MFA registration from trusted workstation

Järgnev poliitika nõuab mitmetasemelise kontrolli seadistamist ainult läbi ettevõtte maapealsest Active Directory seadme, mis on sünkroniseeritud Entra ID'sse. Taoline poliitika aitab kaitsta juhtudel, mil kasutaja konto on lekkinud ja küberkurjategija proovib kasutaja eest ise mitmetasemelise kontrolli seadistada.

1. Azure portaalis olles valige **Microsoft Entra ID**




2. Valige **Security**
3. Valige **Conditional Access**
4. Valige **New Policy -> Create New Policy**
5. Uue Conditional Access reegli lehel lisage järgnev:
 - a. Name: **Entra ID MFA registration from trusted Workstation**
 - b. Users or workload identities
 - i. **Include:** All users
 - ii. **Exclude:** Valige AAD-AR-SEC-EXCLUDED-FROM-CA grupp kus on meil avariikontod, All guest and external users
 - c. Cloud apps or actions
 - i. Valige **Cloud apps** asemel **User Actions** ja lülitage sisse **Register Security Information**
 - d. Conditions

- i. **Client Apps**
 1. Valige kõik rakendused **Browser, Mobile Apps and Desktop Clients, Exchange ActiveSync Clients, Other clients**
- e. **Grant**
 - i. Valige **Require multifactor Authentication** ja **Require Microsoft Entra hybrid joined device**
 - ii. Täiendava tingimusena lülitage sisse „**Require all the selected controls**“ seadistus.
6. **Enable policy** valige On.
7. Vajutage **Create**

9.7.4 Reegel 4 – Require compliant or hybrid Entra joined device for administrators

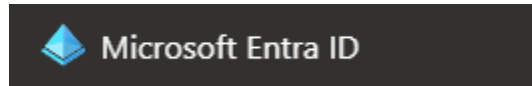
Järgnev poliitika nõuab administraatoritelt infoturve poliitikatele vastavat seadet või maapealsest Active Directory’st sünkroniseeritud seadet Entra ID’sse.

1. Azure portaalis olles valige **Microsoft Entra ID**

2. Valige **Security**
3. Valige **Conditional Access**
4. Valige **New Policy -> Create New Policy**
5. Uue **Conditional Access** reegli lehel lisage järgnev:
 - a. Name: **Require compliant or hybrid Entra joined device for administrators**
 - b. Users or workload identities
 - i. **Include:** Valige AAD-AR-SEC-CLOUD-ADMINISTRATORS
 - c. Cloud apps or actions
 - i. **Include:** All cloud apps
 - d. Grant
 - i. Valige **Grand Access** ja lülitage sisse
 1. Require device to be marked as compliant
 2. Require Hybrid Entra joined device
 - ii. **For Multi control** seadistuseks valige **Require one of the selected controls**
6. **Enable policy** valige On.
7. Vajutage **Create**

9.7.5 Reegel 5 – Block access for unknown or unsupported device platform

Järgnev poliitika blokeerib kõik mittetoetatud seadmed. Võimalik on ka antud poliitika rakendada ainult administraatoritele.

1. Azure portaalis olles valige **Microsoft Entra ID**

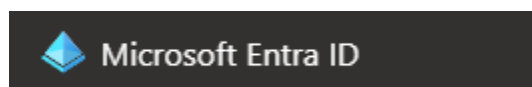


2. Valige **Security**
3. Valige **Conditional Access**
4. Valige **New Policy -> Create New Policy**
5. Uue Conditional Access reegli lehel lisage järgnev:
 - a. Name: **Block access for unknown or unsupported device platform**
 - b. Users or workload identities
 - i. **Include:** All Users
 - ii. **Exclude:** Valige AAD-AR-SEC-EXCLUDED-FROM-CA grupp, kus on avariikontod
 - c. Cloud apps or actions
 - i. **Include:** All cloud apps
 - d. Conditions
 - i. **Device Platforms**
 1. Lülitage funktsionaalsus sisse
 - a. **Include:** Any device
 - b. **Exclude** alt valige Android, iOS, Windows, macOS
 - e. Grant
 - i. Valige **Block Access**
6. **Enable policy** valige On.
7. Vajutage **Create**

9.7.6 Reegel 6 – Require multi-factor authentication for risky sign-ins

Järgnev reegel kontrollib kasutaja sisselogimise riski. Kui tegemist on keskmise või kõrgema riskiga, küsitakse mitmetasemelist kontrolli. Muidugi võib ka selliste juhtumite korral üldse pilveteenuste kasutamine keelata. Vastav reegel nõuab Entra ID Premium 2 paketti.

1. Azure portaalis olles valige **Microsoft Entra ID**



2. Valige **Security**
3. Valige **Conditional Access**
4. Valige **New Policy -> Create New Policy**

5. Uue Conditional Access reegli lehel lisage järgnev:
 - a. Name: **Require multi-factor authentication for risky sign-ins**
 - b. Users or workload identities
 - i. **Include:** All Users
 - ii. **Exclude:** Valige AAD-AR-SEC-EXCLUDED-FROM-CA grupp, kus on avariikontod
 - c. Cloud apps or actions
 - i. **Include:** All cloud apps
 - d. Conditions
 - i. **Sign-in risk**
 1. Lülitage vastav poliitika sisse ja valige Medium ja High tasemed
 - e. Grant
 - i. Valige **Grant Access** ja veenduge, et **Require multi-factor authentication** oleks valitud
6. **Enable policy** valige On.
7. Vajutage **Create**

9.7.7 Reegel 7 – Require password change for high-risk users

Vastav reegel sunnib kõiki kasutajaid muutma parooli, kui tegemist on kõrgema taseme kasutaja riskiga. Vastav reegel nõuab Entra ID Premium 2 paketti.

1. Azure portaalis olles valige **Microsoft Entra ID**



2. Valige **Security**
3. Valige **Conditional Access**
4. Valige **New Policy -> Create New Policy**
5. Uue Conditional Access reegli lehel lisage järgnev:
 - a. Name: **Require password change for high-risk users**
 - b. Users or workload identities
 - i. **Include:** All Users
 - ii. **Exclude:** Valige AAD-AR-SEC-EXCLUDED-FROM-CA grupp, kus on avariikontod
 - c. Cloud apps or actions
 - i. **Include:** All cloud apps
 - d. Conditions
 - i. **User Risk**
 1. Lülitage vastav poliitika sisse ja valige **High** tase
 - e. Grant

- i. Valige **Grant Access** ja veenduge, et **Require Password Change** oleks valitud

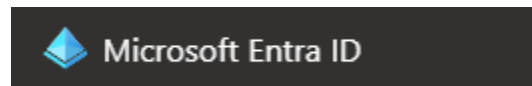
6. **Enable policy** valige On.

7. Vajutage **Create**

9.7.8 Reegel 8 – Block legacy authentication

Vastav reegel keelustab ebaturvaliste protokollide kasutamise. Enne reegli rakendamist tuleks analüüsida, mis põhjustel vanu protokolle kasutatakse ja kas see võib kaasa tuua mingi teenuse katkestuse.

1. Azure portaalis olles valige **Microsoft Entra ID**



2. Valige **Security**

3. Valige **Conditional Access**

4. Valige **New Policy -> Create New Policy**

5. Uue Conditional Access reegli lehel lisage järgnev:

- a. Name: **Block legacy authentication**
- b. Users or workload identities
 - i. **Include:** All Users
 - ii. **Exclude:** Valige AAD-AR-SEC-EXCLUDED-FROM-CA grupp, kus on avariikontod
- c. Cloud apps or actions
 - i. **Include:** All cloud apps
- d. Conditions
 - i. **Clients Apps**
 1. Lülitage vastav poliitika sisse ja valige Exchange ActiveSync clients Other clients
- e. Grant
 - i. Valige **Block Access**

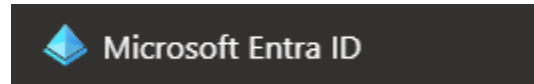
6. **Enable policy** valige On.

7. Vajutage **Create**

9.7.9 Reegel 9 – Require approved client app for mobile devices (MAM)

Vaikimisi saavad kasutajad andmeid tarbida igast seadmest ja rakendusest. Infoturbe seisukohast ei ole see soovitatav. Vastav poliitika määrab, et ettevõtte andmeid saab tarbida lubatud rakenduste kaudu nagu Microsoft Outlook jne. Selliste poliitikate rakendamisel ei saa kasutajad andmeid tõsta sinna, kuhu pole lubatud ning vajadusel saab ettevõtte andmeid kaitsta kaug-kustutamise teel jne.

1. Azure portaalis olles valige **Microsoft Entra ID**

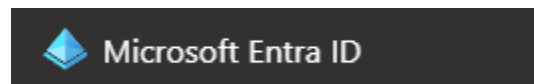


2. Valige **Security**
3. Valige **Conditional Access**
4. Valige **New Policy -> Create New Policy**
5. Uue Conditional Access reegli lehel lisage järgmine:
 - a. Name: **Require approved client app for mobile devices (MAM)**
 - b. Users or workload identities
 - i. **Include:** All Users
 - ii. **Exclude:** Valige AAD-AR-SEC-EXCLUDED-FROM-CA grupp, kus on avariikontod
 - c. Cloud apps or actions
 - i. **Include:** All cloud apps
 - d. Conditions
 - i. **Device Platforms**
 1. Lülitage funktsionaalsus sisse ja valige **iOS** ja **Android**
 - e. Grant
 - i. Valige **Grant Access** ja veenduge, et **Require approved client app** ja **Require app protection policy** oleksid valitud.
 - ii. For multiple controls tüübiks valige **Require one of the selected controls**
6. **Enable policy** valige **On**.
7. Vajutage **Create**

9.7.10 Reegel 10 – Require multi-factor authentication for device registration

Uute seadmete registreerimisel on nõutud mitmetasemeline kontroll.

1. Azure portaalis olles valige **Microsoft Entra ID**



2. Valige **Security**
3. Valige **Conditional Access**
4. Valige **New Policy -> Create New Policy**
5. Uue Conditional Access reegli lehel lisage järgnev:
 - a. **Name:** Require multi-factor authentication for device registration
 - b. Users or workload identities
 - i. **Include:** All users
 - ii. **Exclude:** Valige AAD-AR-SEC-EXCLUDED-FROM-CA grupp, kus on avariikontod, All guest and external users

- c. Cloud apps or actions
 - i. Valige **Cloud apps** asemel **User Actions** ja lülitage sisse **Register or join devices**
 - d. Grant
 - i. Valige **Grant Access** veenduge, et **Require multi-factor authentication** oleks valitud
6. **Enable policy** valige On.
 7. Vajutage **Create**

9.7.11 Reegel 11 – Access only from trusted countries

Kontode arv mida igapäevaselt kompromiteeritakse on äärmiselt suur ja teenuste ning andmete kaitsmiseks on vaja erinevaid meetmeid. Kasutajad võivad langeda erinevate rünnakute ohvriks (nt kalastus) ja kergekäeliselt oma parooli välja anda. Selleks, et vähendada riske taoliste rünnakute puhul, on oluline defineerida äritegevuse asukoha riigid ja kõik teised blokeerida. Erinevate rünnete puhul on tuvastatud küberkurjategijate katseid kasutajatelt kuritegelikult moel välja petetud paroolide abil koheselt ettevõtte andmetele ja teenustele ligi pääseda.

NB! Enne reegli rakendamist, tuleb reeglit hoolikalt testida väiksema grupi peal.

1. Azure portaalis olles valige **Microsoft Entra ID**



2. Valige **Security**
3. Valige **Named locations**
4. Valige **+Countries location**
5. **New location (Countries)** lehel täitke järgmised väljad:
 - a. **Name:** Blokeeritud riigid
 - b. **Countries:** valige kõik riigid, kus Teil täna tegevust ei ole
6. Vajutage **Create**
7. Valige **Conditional Access**
8. Valige **+New policy**
9. **New Conditional Access Policy** lehel täitke ära järgmised väljad:
 - a. **Name:** Access only from trusted countries
 - b. **Users or workload identities**
 - i. **Include:** All users
 - ii. **Exclude:** Valige AAD-AR-SEC-EXCLUDED-FROM-CA grupp, kus on avariikontod
 - c. **Conditions**
 - i. Valige **Locations** ja lülitage reegel sisse
 - ii. Valige **Selected Locations** ja valige eelnevalt loodud „**Blokeeritud riigid**“ grupp
 - iii. Vajutage **Select**

d. Grant

i. Valige **Block Access**

10. **Enable policy** valige On

11. Vajutage **Create**

10 Pilvepõhiste produktiivsuslahenduste seadistamine

Eesmärgid:

- Viia Entra ID seadistus vastavusse parimatele praktikatele
- Seadistada Office 365 teenuste infoturbe sätteid ja reguleerida ettevõtte andmete töötlemist, loomist ja jagamist

Eeltingimused:

- Ettevõtte ärivajadused on analüüsitud
- Taristu on kaardistatud
- Administreerimismudel on juurutatud ja kokku lepitud
- Hübrididentiteet on disainitud ja juurutatud

10.1 Põhimõtete ja kasutajate vajaduste defineerimine

10.1.1 Oluline meelespea

Microsofti pilveteenuste juurutamisel tõstatub ühe olulisema küsimusena, kuidas toimub informatsiooni ja andmete jagamine väliste osapooltega. Seda on võimalik seadistada leebemalt või väga kindlalt reguleeritud domeenide vastu. Mida suuremat kontrolli soovite omada, seda rohkem on administratiivset tööd ja kasutajate rahulolu võib olla madalam. Enne kui otsustate, milline tee valida, veenduge, et olete need põhimõtted ja vajadused ettevõttes läbi arutanud. Sisemise kokkuleppe olemasolu korral on oluline seda ka kasutajatele kommunikeerida ja selgitada. Kui antud teema jääb tähelepanuta, siis suure tõenäosusega lähevad teenused kasutusele vaikeseadistustega, mis omakorda võib tähendada riski infoturbe seisukohast.

Projekti käigus tõstatub ka küsimus erinevat tüüpi seadmete ja nende omanike osas. Võimalik on luua erinevaid profiile ja sätteid vastavalt kasutajatele ja seadmetele. Mõnel kasutajal võib olla rohkem kui üks seade. Näiteks Juhanil võib olla ettevõtte laptop, isiklik Androidi telefon ja isiklik macOS või juhtub, et mõni kasutaja ei soovigi ettevõtte seadet kasutada. Ehk sellisel juhul tuleks osata vastata küsimusele, kas töötajal on luba infotarbida kõikidel erinevates seadmetes või otsustate teha ka piiranguid?

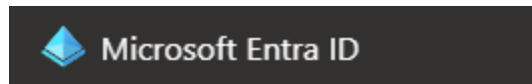
Kui otsustate lubada kasutajatel kasutada isiklikke seadmeid, on oluline kokku leppida seadmete kasutustingimused ja kommunikeerida, millist infot mingitel juhtudel keskselt kogutakse (nt kasutaja asukoht jne). Peaadministraatorina on võimalik näiteks näha, millisest riigist kasutajad teenuseid tarbivad jne. Samuti tuleb selgelt kokku leppida, kes vastutab isiklike seadmete turvalisuse eest. Juhul, kui kasutaja seade nakatub või on langeb küberrünnaku ohvriks, siis peab olema selge, kuidas sellises olukorras käituda.

10.2 Entra ID seadistamine

10.2.1 Paroolivahetuse seadistamine

Administraatorina on võimalik seadistada iseteenindus parooli vahetamiseks. Kui sünkroniseerite kasutajaid maapealsest Active Directory´st, siis oleks mõistlik lubada ka parooli tagasi kirjutamine maapealsesse Active Directory. Parooli tagasi kirjutamine maapealsesse Active Directory eeldab ka Entra Connecti vastavast seadistamist. Vaikimisi on see välja lülitatud ja seda saab ka kontrollida Entra ID portaali kaudu. Antud iseteeninduse seadistamine ei ole kohustuslik, aga on soovituslik.

1. Azure portaalis olles valige **Microsoft Entra ID**

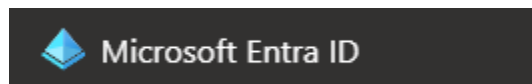


2. Valige **Users**
3. Valige **Password reset**
4. **Properites** lehel saate valida kellel Te lubate parooli muuta
5. Valige **Authentication Methods**. Siin saate öelda mitu erinevat autentimist meetodid kasutaja peab kasutama parooli vahetamiseks.
6. Valige **Registration**. Vaikimisi küsitakse kasutaja käest 180 päeva pärast informatsiooni üle kontrollimist
7. Valige **Notification**. Siin saate öelda kas parooli vahetuse korral teavitatakse kasutajat ja kas administraatorikonto parooli vahetuse korral teavitatakse ka teisi administraatoreid
8. Valige **Customizaton**. Siin saate seadistada oma ettevõtte IT toe veebilehe koos kontaktidega
9. Valige **on-premises integration**. Siin saate öelda, kas parool kirjutatakse tagasi maapealsesse Active Directory. Pidage meeles selle seadistamisel, et Entra Connecti serverit on vaja selle jaoks ka seadistada.

10.2.2 Kasutajate seadistused

Vaikimisi saavad kasutajad vaadata kogu Entra ID sisu, aga infoturbe seisukohast lähtuvalt ei ole see soovitatav. Kasutaja konto kompromiteerimisel on küberkurjategijal samadele andmetele ligipääs ja see võib teha kättesaadavaks liialt palju olulist informatsiooni. Teiseks ei ole soovitatav, et kasutajad saavad ise Entra ID külge lisada erinevaid rakendusi.

1. Azure portaalis olles valige **Microsoft Entra ID**



2. Valige **Users**
3. Valige **User Settings**
4. Lülitage välja **Users can register applications** funktsionaalsus.
5. Lülitage sisse **Restrict access to Entra ID administration portal**
6. Lülitage välja **LinkedIn account connections**.
7. Vajutage **Save**

10.2.3 Välised kasutajad

Vaikimisi on kasutajatel ja Teie Entra ID külalistel palju õigusi. Nad saavad ise kutsuda uusi külalisi ja lisaks näha ka kogu Teie Entra ID sisu. Entra ID külaliskontod peaks olema rangema kontrolli all. Tehke valikud vastavalt ettevõtte poliitikatele.

1. Azure portaalis olles valige **Microsoft Entra ID**



2. Valige **Users**
3. Valige **User Settings**
4. Valige **External Collaboration Settings**
5. Manage **External Collaboration Settings** lehel tehke järgmised valikud
 - a. **Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)**
 - i. See on oluline säte. Külalised ei tohiks kindlasti saada näha kogu teie Entra ID sisu.

Järgmise kahe sättega saab reguleerida, kui palju kasutajatel on vabadust ise külalisi lisada ja kas kutseid saab saata igale domeenile.

Guest invite settings

Guest invite restrictions ⓘ

[Learn more](#)

Anyone in the organization can invite guest users including guests and non-admins (most inclusive)

Member users and users assigned to specific admin roles can invite guest users including guests with member permissions

Only users assigned to specific admin roles can invite guest users

No one in the organization can invite guest users including admins (most restrictive)

Enable guest self-service sign up via user flows ⓘ

[Learn more](#)

Yes No

Collaboration restrictions

Allow invitations to be sent to any domain (most inclusive)

Deny invitations to the specified domains

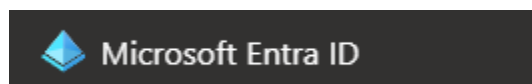
Allow invitations only to the specified domains (most restrictive)

6. Muudatuste järel vajutage **Save**

10.2.4 Seadmete seadistused

Seadmete lisamise poliitikaid seadistades on küsimus, millist tüüpi seadmed on lubatud. Kas kasutajad peaksid saama lisada isiklike seadmeid Entra ID'sse? Kui jah, siis tuleb see sisse lülitada. Võimalik on ka lubada seda teha mingil konkreetsel grupil.

1. Azure portaalis olles valige **Microsoft Entra ID**




2. Valige **Devices**
3. Valige **Device settings**
4. Vastavalt kokkulepitud poliitikatele seadistage **Users may join devices to Entra** poliitika

5. **Require Multi-Factor Authentication to register or join devices with Microsoft Entra** poliitikat seadistama ei pea, kuna seda reguleerime Entra ID Conditional Access reeglite kaudu
6. Vaikimisi saab kasutaja lisada kuni 50 seadet. Seadistage see number väiksemaks, kui see on ettevõtte vaates liialt palju
7. Peale muudatuste tegemist vajutage **Save**
8. Valige Enterprise State Roaming menüüst. Vaikimisi on see välja lülitatud. Enterprise State Roaming lubab teatud informatsioonil seadmetevahelist liikumist. Täpsemalt saate lugeda siit - <https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-faqs>

10.2.5 Rakenduste seadistused

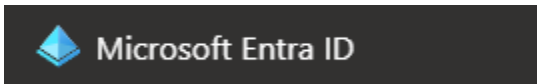
Entra ID rakendustele on võimalik anda väga palju õigusi ja seda teavad ka küberkurjategijad. Entra ID teenuses olevad rakendused peaksid olema rangema kontrolli all ja tuleks veenduda, et kolmandad osapooled ei omaks kogemata liialt palju õigusi. Üks levinumaid ründeid küberkurjategijate poolt on kutsed, mis on justkui päris ja mille aktsepteerimisel delegeeritakse teisele poolele palju õigusi.

1. Azure portaalis olles valige **Microsoft Entra ID**
-  Microsoft Entra ID
2. Valige **Enterprise applications**
 3. Valige **User Settings**
 4. Veenduge et järgmised sätted oleksid välja lülitatud:
 - a. **Users can add gallery apps to My Apps**
 - b. **Users can request admin consent to apps they are unable to consent to**
 5. Valige **Consent and permissions**
 6. **User consent settings** veenduge, et kasutajad ja gruppide omanikud ei saaks anda ise erinevatele teenustele ligipääse.
 - a. **Do not allow user consent**
 - b. **Do not allow group owner consent**
 7. Valige **Save**

10.2.6 Gruppide seadistused

Vaikimisi saavad kasutajad luua ise erinevaid tüüpe gruppe. Soovitatav on antud seadistused välja lülitada ja paika panna protsess, kuidas gruppide tellimine käib. Kui lubate näiteks Teamsis kasutajatel ise töögruppe lisada, siis lõpuks ei pruugi enam keegi aru saada, mis millegi jaoks on kasutusel ja kui inimesed lahkuvad, siis on oht, et need jäävad tähelepanuta.

1. Azure portaalis olles valige **Microsoft Entra ID**



2. Valige **Groups**

3. Valige **General**

4. Lülitage välja järgmised seadistused

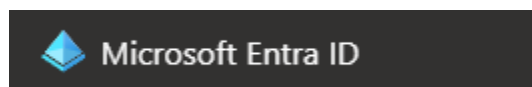
- a. Users can create security groups in Azure portals, API or PowerShell seadistus
- b. Users can create Microsoft 365 groups in Azure portals, API or PowerShell

5. Vajutage Save

10.2.7 Ettevõtte brändingu sätted

Selleks et kasutaja saaks aru, milline on päriselt Teie ettevõtte pilveteenuse keskkond, siis on hea lisada oma ettevõtte logod ja tekstid.

1. Azure portaalis olles valige **Microsoft Entra ID**



2. Valige **Company branding**

3. Valige **Default**

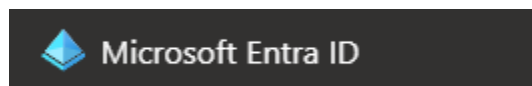
4. Sisestage ettevõtte informatsioon ja logod.

10.2.8 Mitmetasemelise kontrolli seadistused (Oluline)

Microsoft on mitmetasemelise kontrolli teenust oluliselt täiendanud. Nüüd on võimalik näidata kasutajale, kust riigist kasutaja logimine toimub. Lisaks peab kasutaja logimisel sisestama telefonis näidatud koodi. Varem piirduti vaid kasutaja telefoni edastatud logimise kinnitamise teatega. Üha enam kasutavad aga küberkurjategijad seda nõrkust ära ning „pommitavad“ kasutajat nende teavitustega, mistõttu Microsoft rakendas ka täiendavad meetmed.

Seepärast on oluline üle minna uuele konfiguratsioonile

1. Azure portaalis olles valige **Microsoft Entra ID**



2. Valige **Security**

3. **Security** lehelt valige **Authentication Methods**

4. Valige **Microsoft Authenticator**

5. **Microsoft Authenticator settings** lehelt valige **Configure** ja lülitage sisse järgmised sätted:

- a. **Require number matching for push notifications**
- b. **Show application name in push and passwordless notifications**
- c. **Show geographic location in push and passwordless notifications**

6. Vajutage **Save**

7. Vajadusel on võimalik uusi sätteid testida väiksema grupi peal ja alles peale testimist rakendada kõigile.

10.3 Mobile Application Management profiilide seadistamine

Vaikimisi saavad kasutajad lisada erinevatesse seadmetesse ettevõtte emaili ja samas saavad nad kasutusele võtta ka teisi emaili rakendusi. Viimane ei ole kindlasti soovitatav, sest nii kaob kontroll oma ettevõtte andmete üle.

Järgmisena seadistame kaks erinevat profiili, millest üks on mõeldud Android seadmetele ja teine iOS seadmetele. Nende poliitikate kaudu tagame, et ettevõtte informatsioon oleks seadmetes eraldi konteinerisse pandud ja loob võimaluse kaugelt tööprofiil kustuda. Tingimusliku ligipääsu reegel number 9 ütleb, et kasutajad saavad andmeid tarbida ainult hallatud rakenduste kaudu ja kõik teised on blokeeritud. Profiilide loomisel küsitakse päris palju erinevat infot, seega on oluline et see oleks korralikult läbi mõeldud. Enne poliitikate rakendamist kõikidele kasutajatele, veenduge et poliitikad oleksid korrektselt testitud. Lõppkasutajatele on vaja kirjutada ka juhend, kuidas ettevõtte emaili oma seadmes seadistada.

NB! Vastavate poliitikate seadmisel ei saa kasutaja töö emaili jaoks kasutada seadme vaike emaili rakendust, vaid selleks tuleb kasutada Microsoft Outlooki. Teiseks oleks ka hea kasutajate isiklike Android põhiste seadmetele rakendada Android tööprofiil. Tööprofiili rakendamisel pannakse tööga seotud andmed ja rakendused eraldi konteinerisse.

10.3.1 Hallatud rakenduste poliitikate loomine Android seadmetele

1. Avage **intune.microsoft.com**
2. **Microsoft Intune Admin Center** portaalist valige **Apps**
3. Apps lehelt valige **App Protection Policies**
4. Valige **+Create Policy -> Android**
5. Create Policy lehel sisestage järgnev informatsioon:
 - a. **Name:** APP-PROTECTION-ANDROID-V01
 - b. **Description:** Hallatud rakenduste poliitikad Android seadmetele
6. Vajutage **Next**
7. Apps lehel valige järgmised sätted
 - a. **Target to apps on all device types**
 - i. Siin saate valida Jah või Ei. Kui ütlete Jah, siis rakendatakse vastavad poliitikad erinevalt hallatud või mitte hallatud seadmetele. Seadmete halduses on variante mitmeid. Te võite seadme täiesti halduse alla võtta ja siis rakendada lisaks hallatud rakenduste poliitikaid, või kui tegemist on isikliku seadmega, siis seadet ei võeta halduse alla ja kasutaja isiklikus seadmes pannakse töö asjad eraldi konteinerisse. Suure tõenäosusega kasutajad ei soovi, et saaksite täis kontrolli nende isiklike seadmete üle.
 - b. **Target policy to** poliitika osas on järgmised valikud
 1. Selected Apps
 2. All Apps
 3. All Microsoft Apps
 4. Core Microsoft Apps

- ii. Sõltuvalt projekti eesmärgist tehke oma valik. Minimaalset võiks valida Core Microsoft Apps.

8. Valige **Next**

9. **Data protection** lehel küsitakse väga palju sisendit erinevate poliitikate kohta. Võimalik on seadistada, mida täpselt kasutaja teha saab, nt kas kasutaja saab tõsta andmeid ettevõtte konteinerist välja või mitte jne. Enne suuremat paigaldmist veenduge, et seadistused vastaksid ettevõtte poliitikatele ja et vastavad testid oleksid tehtud. Selles juhendis teeme järgmised valikud:

- a. **Backup org data to Android backup services:** Block
- b. **Send org data to other apps:** Policy managed apps
- c. **Restrict cut, copy, and paste between other apps:** Policy managed apps with paste in
- d. **Screen capture and Google Assistant:** Block
- e. **Encrypt org data:** Required
- f. **Encrypt org data on enrolled devices:** Required
- g. **Sync policy managed app data with native apps or add-ins:** Block
- h. **Printing org data:** Block
- i. **Restrict web content transfer with other apps:** Microsoft Edge

10. Vajutage **Next**

11. **Access Requirements** lehel küsitakse, kuidas toimub ettevõtte andmetele ligipääs. Kas on ainult PIN lubatud, või ka näpujälje lugeja. Kindlasti me ei soovita eemaldada PINi küsimust kasutajate isiklikes seadmetes. Tehke vajalikud muudatused.

12. Vajutage **Next**

13. **Conditional Access** lehel küsitakse, et kuidas tuleks käituda, kui seade on kaua kinni olnud või mitte aktiivne. Tehke vajalikud muudatused.

14. Vajutage **Next**

15. Assignments lehel valige grupp kasutajaid, kellele on määratud vastavad litsentsid.

16. Vajutage **Next**

17. **Review +Create** lehel kontrollige oma seaded ja vajutage Create

10.3.2 Hallatud rakenduste poliitikate loomine iOS seadmetele

- 1. Avage **intune.microsoft.com**
- 2. **Microsoft Intune Admin Center** portaalist valige Apps
- 3. Apps lehelt valige **App Protection Policies**
- 4. Valige **+Create Policy -> iOS / iPadOS**

1. Create Policy lehel sisestage järgnev informatsioon:

- a. **Name:** APP-PROTECTION-IOS-V01
- b. **Description:** Hallatud rakenduste poliitikad iOS seadmetele

2. Vajutage **Next**

3. **Apps** lehel valige järgmised sätted

a. **Target to apps on all device types**

- i. Siin saate valida Jah või Ei. Kui ütlete Jah, siis rakendatakse vastavad poliitikad erinevalt hallatud või mitte hallatud seadmetele. Seadmete halduses on variante mitmeid. Seadme võib täiesti halduse alla võtta ja siis rakendada lisaks hallatud rakenduste poliitika, või kui tegemist on isikliku seadmega, siis seadet ei võeta halduse alla ja kasutaja isiklikus seadmes pannakse töö asjad eraldi konteinerisse. Suure tõenäosusega kasutajad ei soovi, et saaksite täis kontrolli nende isiklike seadmete üle.

b. **Target policy to** poliitika osas on Teil järgmised valikud

1. Selected Apps
2. All Apps
3. All Microsoft Apps
4. Core Microsoft Apps

- ii. Sõltuvalt projekti eesmärgist tehke oma valik. Minimaalset võiks valida Core Microsoft Apps.

4. Valige **Next**

5. **Data Protection** lehel täitke ära järgmised valikud

1. **Backup org data to iTunes and iCloud backups:** Block
2. **Send org data to other apps:** Policy managed apps
3. **Sync policy managed app data with native apps or add-ins:** Block
4. **Printing org data:** Block

6. Valige **Next**

7. **Access requirements** lehel küsitake sarnast informatsiooni nagu Android seadmete puhulgi. Tehke oma valikud ja veenduge, et PIN küsimine oleks kindlasti sees.

8. Valige **Next**

9. Kontrollige üle **Conditional Launch** reeglid ja vajutage **Next**

10. Assignments lehel valige grupp kasutajaid, kellele on määratud vastavad litsentsid.

11. Vajutage **Next**

12. **Review +Create** lehel kontrollige oma seaded ja vajutage **Create**

10.3.3 Ettevõtte emaili seadistamine Android / iOS seadmes

1. Oma test või päris seadmes avage rakenduste pood
2. Otsige poest **Intune Company Portal**
3. Vajutage **Install**
4. Otsige poest **Outlook**
5. Vajutage **Install**
6. Avage **Outlook** ja valige **Add Account**

7. Sisestage oma emaili aadress ja vajutage **Continue**
8. Valige konto tüübiks **Office 365**
9. Vajutage **Next**
10. Sisestage parool ja vajutage **Next**
11. Valige **Register Device**
12. **Get Access** lehel valige **Continue**
13. Järgmisena küsitakse PIN koodi sisestamist. Sisestage PIN kood kaks korda
14. Vajutage **Done**
15. Nüüd peaksite saama ligi ettevõtte emailile.

10.4 Office 365 turbefunktsioonide seadistamine

Office 365 teenuste komplektis on väga palju erinevaid sätteid, mida on võimalik seadistada. Paljude seadistuste juures on väga olulisel kohal just organisatsiooni taseme küsimused, mis defineerivad, kuidas töötatakse, mida lubatakse, palju lubatakse jne. Sellele lisaks kõik infoturbe seotud küsimused. Mainime siinkohal ära, et Microsoft pakub oma kliendile täiendavaid infoturbe teenuseid ka Office 365 teenustele. Kui leiate, et midagi pole vaikumisi valitud paketi olemas, siis võib-olla on võimalik soovitud funktsionaalsus saada Defender toodetega.

Microsoft Defender for Office 365 Plan 1	Microsoft Defender for Office 365 Plan 2
<ul style="list-style-type: none"> - Safe Attachments - Safe Links - Safe Attachments for SharePoint, OneDrive, and Microsoft Teams - Anti-phishing in Defender for Office 365 protection - Real-time detections 	<ul style="list-style-type: none"> - Microsoft Defender for Office 365 Plan 1 funktsionaalsus, pluss lisaks <ul style="list-style-type: none"> o Threat Trackers o Threat Explorer o Automated investigation and response o Attack simulation training o Campaign Views

Microsoft Defender for Office 365 paketid

10.4.1 Üldiste failitüüpide keelustamine

Emailide vahendusel liigub väga palju pahavara ja administraatorina on võimalik teatud tüüpi manuseid blokeerida. Microsoft on defineerinud vaike nimekirja, kuid neid on võimalik juurde lisada.

1. Avage **security.microsoft.com**
2. Valige **Policies and Rules**
3. Valige **Threat Policies**
4. Valige **Anti-malware**
5. Valige **Default** poliitika
6. **Default** poliitika lehel valige **Edit protection settings**
7. **Edit protection** lehel lülitage sisse **Enable the common attachments filter** poliitika. Vajadusel võite ise ka juurde lisada failide tüüpe, mis pole ettevõttes lubatud. Teiseks saate täiendavalt seadistada ka teavituste saajaid jne.
8. Vajutage **Save**

10.4.2 Spämmipoliitikate seadistamine

Sõltuvalt mahtudest on võimalik seadistada erinevaid piiranguid emailide mahtude osas. Teatud mahtude saavutamisel märgitakse kasutajad kahtlasteks ja nad ei pruugi enam saada emaili saata. Mahtude kontrolliks soovitame tutvuda vaike sätetega - <https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/exchange-online-limits#sending-limits-1>

1. Avage **security.microsoft.com**
2. Valige **Policies and Rules**
3. Valige **Threat Policies**

4. Valige **Anti-spam** poliitika
5. Valige **Anti-spam outbound policy**
6. **Anti-spam** poliitika lehel vajutage edit protection settings
7. Lülitage sisse **Send a copy of outbound messages that exceed these limits to the users and groups** poliitika ja täpsustage keda peaks teavitama.
8. Vajutage **Save**

10.4.3 Emailide automaatsed suunamised

Kontode kompromiteerimisel võivad küberkurjategijad sisse lülitada emailide automaatse suunamise. Ettevõtte administraatorina on võimalik selles osas erinevaid sätteid muuta. Järgneva poliitika seadistamise eelduseks on arusaam, kas sellise funktsiooni kasutamine on kooskõlas andmekaitse poliitikatega.

1. Avage <https://admin.exchange.microsoft.com/>
2. Valige **Mail Flow -> Remote Domains**
3. **Remote Domains** lehel valige **Default**
4. **Default** akna paneelil valige **Edit Reply types**
5. **Email reply types** lehel saate öelda, kas automaatne kirjade edasi suunamine on lubatud või mitte

10.4.4 DKIM ja SPF kirjete seadistamine

DKIM lisab emailile digitaalse templi, mis võimaldab saajal kontrollida, kas saatjal on õigust taolist domeeni kasutada. Enne kui Te alustate DKIM kirjete lisamist oma DNSi ja seadistama Office 365, siis me soovime esmalt läbi lugeda ametlik dokumentatsioon - <https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/use-dkim-to-validate-outbound-email?view=o365-worldwide>

1. Avage <https://security.microsoft.com/dkimv2>
2. Nüüd peaks avama kõik lisatud domeenid Entra ID teenusega
3. Valige domeen, millele soovite lisata **DKIM**
4. Kindla domeeni nime peal lülitage sisse **Sign messages for this domain with DKIM signatures** poliitika
5. Poliitika sisse lülitamisel kontrollitakse, kas vastavad **CNAME** kirjed on DNSi lisatud või mitte. Kui ei ole, kuvatakse vastavad kirjed, mille peaksite lisama.
6. Sender Policy Framework ehk SPF kirjete lisamiseks järgige Microsofti juhendit
 - a. <https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-spf-in-office-365-to-help-prevent-spoofing?view=o365-worldwide>

10.4.5 Exchange Online andmete andmehoiu poliitikate defineerimine

Uute töötajate tööle tulemine ja lahkumine peaksid olema tagatud väga hästi väljatöötatud protsessidega. Töötajate lahkumisega võib kasutajakonto ja ligipääsud erinevatesse süsteemidesse lahti jääda jne. Teiseks tekib küsimus, mis saab kasutajate andmetest: kui kaua neid alles hoitakse, kui kaua litsentse kasutajaga seome, kui palju tal erinevaid Teams gruppe on jne. Neid kõiki küsimusi peaks pilveteenuste juurutamise käigus analüüsima ja arvesse võtma. Office 365 lubab siinkohal defineerida erinevaid andmehoiu poliitikaid.

Enne kui alustate andmehoiu sätteid seadistama, on oluline, et need oleks kokku lepitud ning dokumenteeritud. Siinkohal soovime täiendavalt lugeda Microsofti enda dokumenti: <https://docs.microsoft.com/en-us/microsoft-365/compliance/create-retention-policies?view=o365-worldwide>

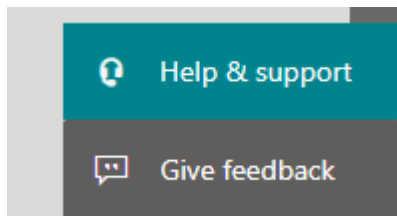
1. Avage <https://compliance.microsoft.com/>
2. Valige **Policies -> Retention**
3. Valige + **Retention Policy**
4. **Retention Policy** lehel sisestage poliitika nimi ja kirjeldus
5. **Choose the type of retention policy to create** lehel valige, kas reegel on dünaamiline või staatiline. Dünaamilise reegli loomiseks on vaja esmalt luua eesmärk (scope) ja siis on võimalik seda tüüpi poliitika luua. Staatilise reegli puhul seda nõuet ei ole. Enne poliitika tüübi valikut selgitage välja oma täpsemad valikud.
6. **Choose locations to apply the policy** lehel küsitake, millistele teenustele see poliitika kehtib. Valige välja teenused.
7. Vajutage **Next**
8. **Decide if you want to retain content, delete it, or both** lehel küsitakse, kui kaua soovite vastavat informatsiooni hoida. Seadistage poliitika vastavalt kokkulepitud numbritega
9. Vajutage **Next**
10. **Review and Finish** lehel kontrollige informatsioon üle ja vajutage **Submit**
11. Vajutage **Done**

10.5 Exchange Online sätete seadistamine

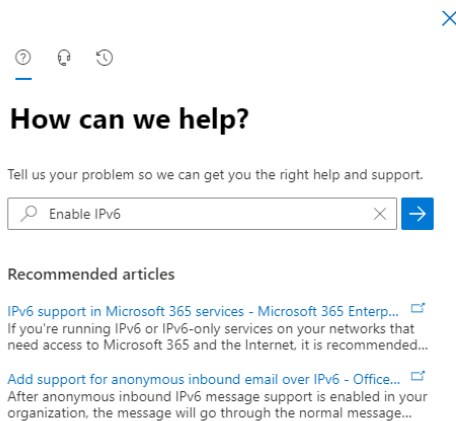
10.5.1 IPv6 seadistamine

Vaikimisi ei ole IPv6 sisselülitatud. Selle seadistamiseks tuleb klienditoega eraldi ühendust võtta.

1. Avage <https://admin.microsoft.com/>
2. Valige nurgast **Help ja Support**



3. **How can we help** lehel sisestage „*Enable IPv6*“ ja vajutage sinisele noole peale



4. Vajutage **Contact Support**

5. **Contact Support** lehel

- a. **Title**

- b. **Description**

- i. Kirjeldusse lisage, et soovite IPv6 tuge ja millisele domeenile seda soovite

- c. **Contact Number and Email**

6. Vajutage **Contact me**

10.5.2 Exchange Online logide hoiu seadistamine

Küberintsidentide puhul on olulised just logid. Ilma logideta on väga raske leida vastuseid küsimustele: kes, kus, millal ja mida. Võib juhtuda, et avastate intsidendi alles mitmeid kuid hiljem ja kui vastavaid logisid pole, ei ole enam midagi teha.

Vaikimisi hoitakse audit logisid kuni 90 päeva. Kui Teie organisatsiooni vajadusi see ei kata, siis on vaja soetada täiendavaid litsentse. Enne poliitikate seadistamist lugege täpsemalt veel Microsofti ametliku artiklit - <https://docs.microsoft.com/en-us/microsoft-365/compliance/audit-log-retention-policies?view=o365-worldwide>

1. Avage <https://compliance.microsoft.com/>
2. Valige **Audit**
3. **Audit** lehel valige **Audit retention policies**
4. Valige **Create Audit retention policy**
5. **New audit retention policy** lehel täitke ära järgmised väljad
 - a. Policy Name
 - b. Description
 - c. Users
 - d. Record Type
 - e. Duration – 90 days, 6 months, 9 months, 1 year, 10 years
 - f. Priority
6. Vajutage **Save**

10.5.3 „Unified Audit Log“ logi reegli kontroll läbi PowerShell'i

1. Paigaldage alljärgnevalt lingilt oma seadmesse PowerShell versioon 7.X, kui seda seni veel pole tehtud
 - a. <https://learn.microsoft.com/en-us/powershell/scripting/install/installing-powershell-on-windows?view=powershell-7.2>
2. Avage PowerShell versioon 7.X ja käivitage järgmine käsk:
 - a. **Install-Module -Name ExchangeOnlineManagement -Force -Verbose**
3. Peale **ExchangeOnlineManagement** mooduli paigaldamist käivitage järgmised käsud:
 - a. **Connect-ExchangeOnline**
 - i. Käsk lubab ühenduda vastu Exchange Online teenust
 - b. **Get-AdminAuditLogConfig | Select-Object -Property UnifiedAuditLogIngestionEnabled**
 - i. Kuvab ekraanile teie logimise sätte staatuse
4. Veenduge, et **UnifiedAuditLogIngestionEnabled** väärtus oleks **True**

```
Get-AdminAuditLogConfig | Select-Object -Property UnifiedAuditLogIngestionEnabled
UnifiedAuditLogIngestionEnabled
-----
True
```

10.5.4 E-kirjade märgistamine

Vaikimisi Exchange Online ei näita, kas kiri on tulnud väljastpoolt ettevõtte domeeni. Selleks, et kasutajatel oleks parem arusaam, kust kiri on tulnud, tuleb see eraldi seadistada.

1. Avage PowerShell versioon 7.X ja käivitage järgmised käsud
 - a. **Connect-ExchangeOnline**
 - b. **Get-ExternalInOutlook | Select-Object -Property Enabled**

2. Get-ExternalInOutlook käsk peaks kuvama väärtuse **True** või **False**. Kui väärtuseks on **False**, siis käivitage järgmine käsk:
 - a. **Set-ExternalInOutlook -Enabled \$true**
3. Peale seadistuse tegemist näevad kasutajad analoogset teadet igal kirjal, mis on tulnud väljastpoolt ettevõtte domeeni.

TEST



10.5.5 Outlook Web Access kolmandate osapoolte pilveteenuste blokeerimine

Vaikimisi saavad kasutajad läbi Outlook Web Accessi kasutada kolmandate osapoolte failide jagamise pilveteenuseid nagu Dropbox, Google jne. Selleks, et nad ei saaks neid kasutada, on vaja see eraldi välja lülitada PowerShell'i kaudu.

Käivitage **PowerShell ISE** administraatorina ja käivitage käsud samm sammult.

```

1 #Paigalda ExchangeOnlineManagement PowerShell'i Moodul
2 Install-Module ExchangeOnlineManagement -Force -Verbose
3
4 #Ühenda Exchange Online vastu
5 Connect-ExchangeOnline
6
7 #Lülita välja teiste pilveteenuste failide jagamise teenus
8 Set-OwaMailboxPolicy -Identity OwaMailboxPolicy-Default -AdditionalStorageProvidersAvailable $false
9
10 #Prindi välja preagune seadistus
11 Get-OwaMailboxPolicy | Select-Object -Property AdditionalStorageProvidersAvailable
12
  
```

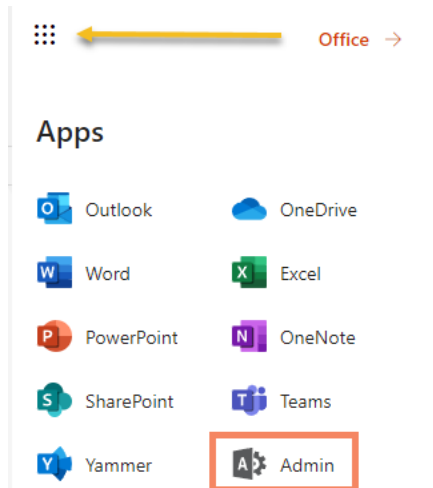
Exchange Online V2 PowerShell'i mooduli kohta saab täiendavalt lugeda siit -

<https://docs.microsoft.com/en-us/powershell/exchange/exchange-online-powershell-v2?view=exchange-ps#install-and-maintain-the-exo-v2-module>

10.5.6 Parooli aegumise poliitika

Vaikimisi palutakse paroolivahetust teha iga 90 päeva tagant, aga tänapäeval ei ole soovitatav seda enam nii tihti teha. Pilveteenuste kasutamisel ei ole kasutajanimi ja parool enam piisav meede. Nagu eelnevalt kirjeldatud, siis tingimusliku reeglite lisamisega saame määrata rohkem tingimusi pilveressurssidele ligipääsemiseks. Kui ettevõtte identiteet tuleb maapealt, siis maapealsed grupipoliitikat juba reguleerivad paroolivahetust. Ideaalis võiks töökoht olla üldse paroolivaba.

1. Avage **portal.office.com**
2. Vajutage täpikeste peale ja valige **Admin**

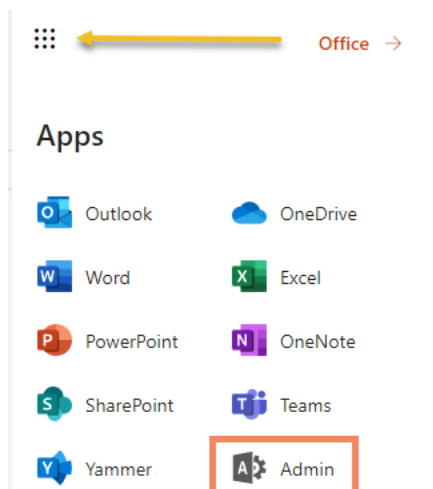


3. Valige ... **Show all**
4. Valige **Settings** ja **Org Settings**
5. Valige **Security & Privacy**
6. Valige **Password expiration policy**
7. Lülitage välja **Set user passwords to expire after a number of days** poliitika

10.5.7 Väliste osapooltega jagamine

Vaikimisi saavad kasutajad ise külalisi lisada. Vastavalt ettevõtte äri vajadustele ja riskide analüüsile on see võimalik kas sisse jätta või keelata.

1. Avage **portal.office.com**
2. Vajutage täpikeste peale ja valige **Admin**

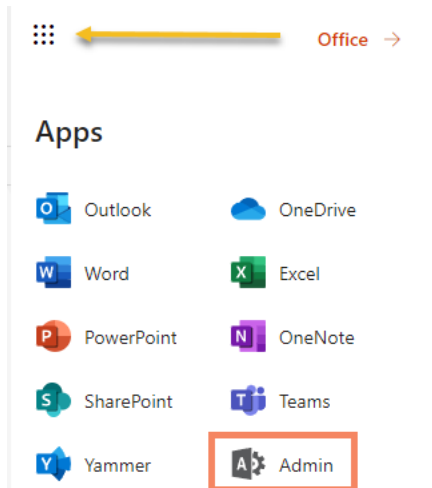


3. Valige ... **Show all**
4. Valige **Settings** ja **Org Settings**
5. Valige **Security & Privacy**
6. Valige **Sharing**
7. Seadistage poliitika vastavalt ettevõtte poliitikatele.

10.5.8 Customer Lockbox E5 litsentsi omanikele

Customer Lockbox sisselülitamisel peab Microsofti poolne tehnik alati luba küsima enne, kui nad mingi probleemi korral ettevõtte andmetele soovivad ligi pääseda.

1. Avage **portal.office.com**
2. Vajutage täpikeste peale ja valige **Admin**

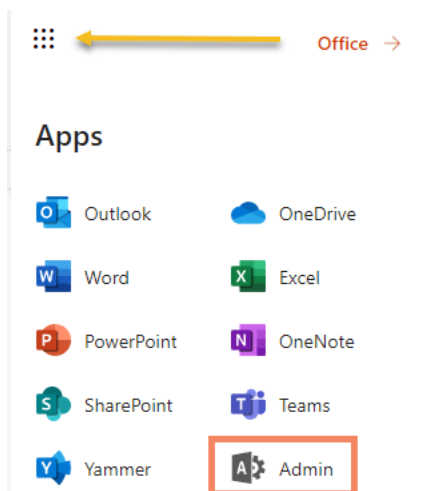


3. Valige **... Show all**
4. Valige **Settings** ja **Org Settings**
5. Valige **Security & Privacy**
6. Valige **Customer LockBox**
7. Seadistage poliitika

10.5.9 Kalendrite jagamine

Vaikimisi saavad kasutajad jagada oma kalendrid kõigiga, kes kasutavad O365 ja Microsoft Exchange teenuseid. Seadistage vastav poliitika vastavalt ettevõtte äri vajadustele ja riskide analüüsile.

1. Avage **portal.office.com**
2. Vajutage täpikeste peale ja valige **Admin**



3. Valige **... Show all**

4. Valige **Services**
5. Valige **Calender**
6. Seadistage poliitikad
7. Vajutage **Save**

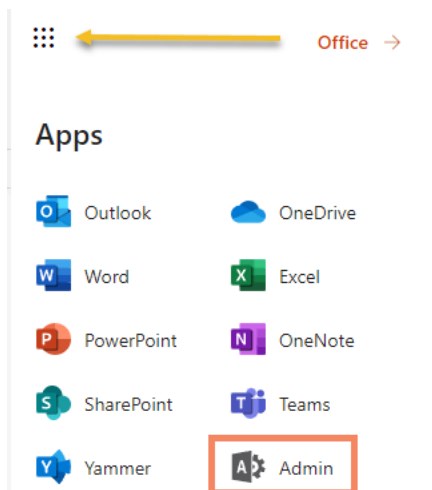
10.5.10 Aegunud protokollid

Alates 01.10.2022 plaanib Microsoft eaturvalised protokollid oma teenustes ära keelustada. Paljud küberkurjategijad kasutavad just neid protokolle, et rünnata ettevõtte keskkondi ja selle kaudu pääseda ligi ettevõtte andmetele. Administraatorina on võimalik juba täna sellega tegeleda ja veenduda, et mingid konkreetsete teenused ei kasutaks vanu protokolle.

Täpsemalt saate lugeda kogu protsessist siit -
<https://techcommunity.microsoft.com/t5/exchange-team-blog/basic-authentication-deprecation-in-exchange-online-september/ba-p/3609437>

NB! Enne, kui asute vanu protokolle kinni panema, siis kontrollige üle oma keskkonna Entra ID logid. Kui olete veendunud, et kõik on korras, siis järgige alljärgmisi samme.

1. Avage **portal.office.com**
2. Vajutage täpikeste peale ja valige **Admin**



3. Valige **... Show all**
4. Valige **Services**
5. Valige **Modern Authentication**
6. Veenduge, et järkev poliitika oleks sisselülitatud **Turn on modern authentication for Outlook 2013 for Windows and later**
7. Eemaldage tugi järgnevatelt teenustelt
 - a. Outlook Client
 - b. Exchange ActiveSync
 - c. Autodiscover
 - d. IMAP4
 - e. POP3

- f. Authenticated SMTP
- g. Exchange Online PowerShell

8. Vajutage **Save**

10.5.11 Aegunud protokollide välja lülitamine postkasti tasemel (Edasijõudnutele)

Administraatorina on veel võimalik aegunud protokolle välja lülitada ka postkasti tasemel. Teatud juhtudel on vaja need välja lülitada kõigil postkastidel, seejuures lubades teatud erandeid. Eelistatult on aegunud protokollid välja lülitatud kõigil postkastidel.

Järgnevate seadistuste puhul tuleb olla riskidest teadlik. Järgmised sätted on mõeldud edasijõudnutele ehk kogenud administraatoritele.

Vanade protokollide välja lülitamise seadistamine toimub kahes osas:

- Protokollide välja lülitamine postkastide tasemel
- Postkasti poliitikate muutmine.

Järgige järgmisi samme vastavate seadistuste tegemiseks

1. Paigaldage allolevalt lingilt oma seadmesse PowerShell versioon 7.X, kui seda pole senini veel tehtud:
 - a. <https://learn.microsoft.com/en-us/powershell/scripting/install/installing-powershell-on-windows?view=powershell-7.2>
2. Avage PowerShell versioon 7.X ja käivitage järgmine käsk:
 - a. **Install-Module -Name ExchangeOnlineManagement -Force -Verbose**
3. Peale **ExchangeOnlineManagement** mooduli paigaldamist käivitage järgmised käsud:
 - a. **Connect-ExchangeOnline**
 - i. Käsk ühendub Exchange Online teenusega
 - b. **Get-EXOCasMailbox | Select-Object -Property PrimarySmtpAddress,ImapEnabled,PopEnabled,MAPIEnabled,EwsEnabled,ActiveSyncEnabled | Format-Table**
 - i. Kuvab ekraanile e-posti aadressi ja protokollid, mis on aktiveeritud ja mis mitte
4. Kui on tuvastatud kasutajad, kelle postkastidel soovite nt IMAPi, POPi või SMTP protokollid välja lülitada, kasutage järgmisi käsked:
 - a. **Set-CASMailbox -ImapEnabled \$false**
 - b. **Set-CASMailbox -PopEnabled \$false**
 - c. **Set-CASMailbox -SmtpClientAuthenticationDisabled \$true**
5. Vastavate käskude juures tuleb määrata alati ka postkast.
6. Postkasti reeglite muutmiseks tuleb kasutada järgmisi käsked:
 - a. **Get-CASMailboxPlan**
 - i. Kuvab ekraanile postkastid ja nende sätted

```

ActiveSyncMailboxPolicy      :
ActiveSyncDebugLogging      : False
ActiveSyncEnabled           : True
ActiveSyncSuppressReadReceipt : False
DisplayName                  : ExchangeOnline
ECPEEnabled                  : True
ImapEnabled                  : False
ImapUseProtocolDefaults     : True
ImapMessagesRetrievalMimeFormat : BestBodyFormat
ImapEnableExactRFC822Size   : False
ImapProtocolLoggingEnabled  : False
ImapSuppressReadReceipt    : False
ImapForceICalForCalendarRetrievalOption : False
MAPIEnabled                  : True
MapiHttpEnabled             :
MAPIBlockOutlookNonCachedMode : False
MAPIBlockOutlookVersions   :
MAPIBlockOutlookRpcHttp    : False
PublicFolderClientAccess    : False
MAPIBlockOutlookExternalConnectivity : False
OwaMailboxPolicy            : OwaMailboxPolicy-Default
OwaEnabled                   : True
OwaForDevicesEnabled        : True
PopEnabled                   : False

```

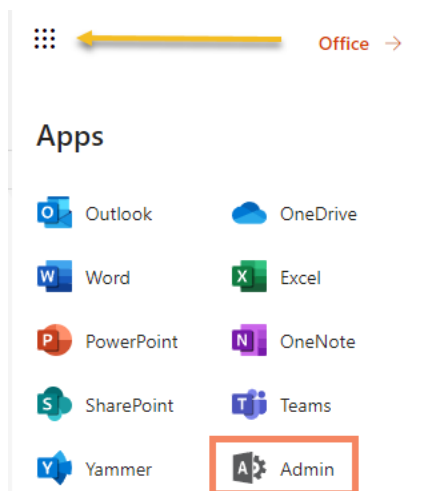
b. IMAPi ja POPi välja lülitamiseks kasutage järgmist käsku:

- i. **Get-CASMailboxPlan | Set-CASMailboxPlan -ImapEnabled \$false -PopEnabled \$false**

10.5.12 Microsoft Teams välised külalised

Vaikimisi on võimalik külalisi lisada Teamsi.

1. Avage **portal.office.com**
2. Vajutage täpikeste peale ja valige **Admin**

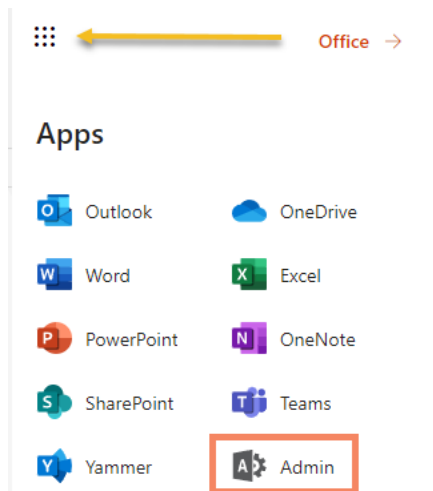


3. Valige **... Show all**
4. Valige **Services**
5. Valige **Microsoft Teams**
6. Seadistage **Allow guest Access in Teams** seadistus vastavalt kokkulepitud reeglitele

10.5.13 Microsoft 365 grupid ja välised kasutajad

Vaikimisi saavad kasutajad lisada külalisi M365 gruppidesse ja saavad ka grupiga kaasas olevatele andmetele ligi. Vajadusel muutke vastav poliitika vastavalt äri vajadustele ja riskide analüüsile.

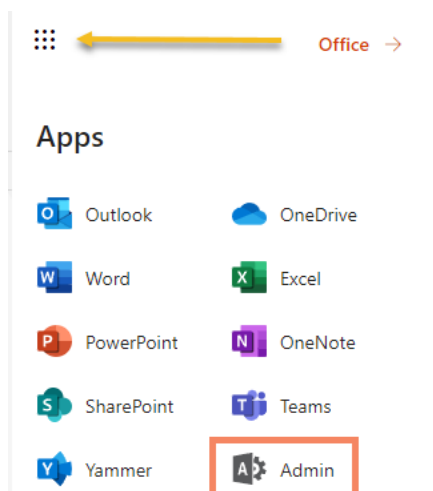
1. Avage **portal.office.com**
2. Vajutage täpikeste peale ja valige **Admin**



3. Valige **... Show all**
4. Valige **Services**
5. Valige **Microsoft 365 Groups**
6. Seadistage mõlemad poliitikad vastavalt kokkulepitud poliitikatele

10.5.14 Kasutajatoe informatsiooni lisamine

1. Avage **portal.office.com**
2. Vajutage täpikeste peale ja valige **Admin**

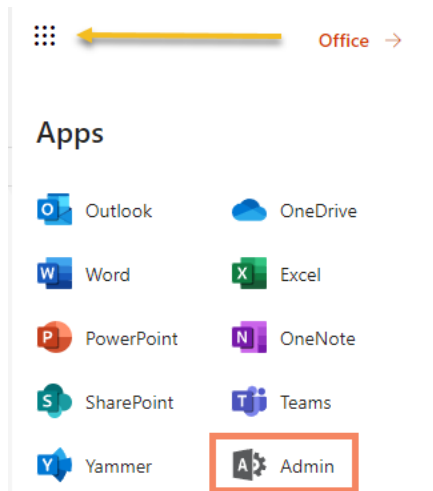


3. Valige **... Show all**
4. Valige **Organization Profile**
5. Valige **Help desk information**
6. Sisestage oma ettevõtte IT-toe informatsioon

10.6 SharePoint Online ja Onedrive for Business sätete seadistamine

SharePoint ja OneDrive saavad olema mõlemad olulised teenused, kus hakatakse hoidma väga suures mahus ettevõtte andmeid. Et säilitada andmete üle kontrolli, on vaja täpselt piiritleda lubatu ja lubamatu. Veelgi enam on see oluline seetõttu, et tekib võimalus hakata andmeid jagama väliste osapooltega.

1. Avage **portal.office.com**
2. Vajutage täpikeste peale ja valige **Admin**



3. Valige ... **Show all**
4. Valige **SharePoint administraatori** paneel
5. **SharePoint Admin Center** lehel valige **Policies -> Sharing**
6. **Sharing** lehel saate seadistada, kui rangelt soovite kontrollida informatsiooni jagamist erinevate osapooltega.
 - a. Soovitame seadistada järgmised poliitikad vastavalt ettevõtte poliitikatele
 - i. Content can be shared with
 - ii. Allow guests to share items they dont own
 - iii. Guest Access to a site or OneDrive will expire automatically after this many days
 - iv. People who use a verification code must reauthenticate after this many days
 - v. File and folder links
 - vi. These links must expire within this many days
 - b. Vajutage **Save**
 - c. Valige **Access Control**
 - d. **Access Control** lehel valige **Unmanaged devices**
 - i. **Unmanaged devices** lehel saate kinni panna andmete kasutamise mitte hallatud seadmetest või piirata kasutust. Seadistage vastav poliitika vastavalt oma ettevõtte poliitikatele.
 - ii. Vajutage **Save**

- e. **Access Control** lehel valige **Idle session sign-out**
 - i. See poliitika kontrollib, kaua säilitatakse mitteaktiivset sessiooni mittehallatud seadmetes.
- f. **Access Control** lehel valige **Apps that dont use modern authentication**
 - i. Selle poliitika seadistamisega saab keelata kõik vanad rakendused, mis ei toeta modernset autentimist.
- 7. **SharePoint Admin Center** lehel valige **Settings**
- 8. Valige **OneDrive Sync** poliitika
 - a. **Sync** lehel saate seadistada järgmised poliitikad
 - i. **Allow syncing only on Computers joined to specific domains**
 - 1. Vajadusel on võimalik defineerida, millise Active Directory domeeni osas lubatakse andmeid sünkroniseerida
 - ii. **Block upload of specific file types**
 - 1. Kui ei soovitakse kasutajad konkreetseid failitüüpe Onedrive sünkroniseerimist piirata, saate selle ise täpsustada
- 9. Valige **OneDrive Retention** poliitika
 - a. Siin saab defineerida kustutatud kasutajate informatsiooni säilitamise aega.

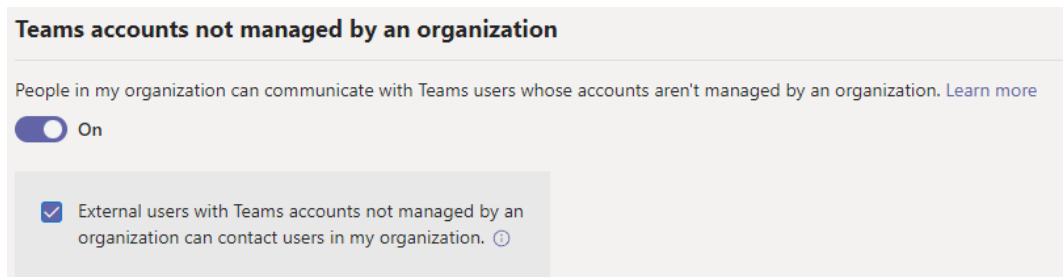
10.7 Microsoft Teams seadistamine

Microsoft Teams sätete seadistamine eeldab väga head eeltööd ettevõtte siseselt, et täpselt välja selgitada, kuidas kasutajad hakkavad täpsemalt Teamsi kasutama ja kuidas seda teha efektiivselt. Teams lubab luua väga palju erinevaid automaatika töövooge ja teha kasutajate igapäeva töö tunduvalt lihtsamaks.

Siin juhendis toome välja seadistused, mis on seotud väliste osapooltega ja failide jagamisega Teams kaudu.

10.7.1 Välised kasutajad

1. Avage <https://admin.teams.microsoft.com/>
2. Valige **Users -> Guest Access**
3. **Guest Access** lehel saate seadistada täpsemalt, mida külalised saavad teha või mitte
4. Valige **Users -> External Access**
5. **External Access** saate öelda, kas lubate ainult konkreetseid domeene või väline kasutus on täiesti keelatud.
6. Teiseks on võimalik lubada **Teams Chat** rakendusest ettevõtte töötajatele otse kirjutamine. Selle seadistuse lubamisel, ei pea Teie Entra ID keskkonnas külalisi registreerima.



7. Viimasena saate defineerida, kas kasutajate suhtlusvabadus laieneb ka Skype kasutajatega suhtlusel.

10.7.2 Failide jagamise teenused Teams kaudu

1. Avage <https://admin.teams.microsoft.com/>
2. Valige **Teams -> Teams Settings**
3. **Teams Settings** lehel lülitage välja:
 - a. Citrix files
 - b. DropBox
 - c. Box
 - d. Google Drive
 - e. Egnyte
4. Vajutage **Save**

10.8 Office 365 seadistuste auditeerimine

Office 365 teenuses on väga palju seadistusi ning nendes orienteerumine on keeruline. Selle lihtsustamiseks on Microsoft loonud tööriista nimega ORCA, mis aitab aru saada, kas teenused on turvaliselt seadistatud.

ORCA on PowerShell'i moodul, mida saab paigaldada ja käivitada oma seadmest. ORCA käivitamisel luuakse raport, mis näitab, kui hästi või halvasti Office 365 keskkond on seadistatud.

10.8.1 ORCA paigaldamine

1. Avage **PowerShell** administraatorina ja käivitage järgmine käsk:
 - a. **Install-Module ORCA -Force -Verbose**
2. PowerShell'i aken jätkke lahti

10.8.2 Raporti loomine

1. Endiselt avatud PowerShell'i aknas olles käivitage järgnev käsk:
 - a. **Get-ORCAReport**
2. Sisestage oma kasutajanimi ja parool
3. Käsu edukal lõpetamisel luuakse raport **AppData\Local\Microsoft\ORCA** kataloogi.

11 Pilvepõhiste produktiivsuslahenduste kasutuselevõtt

11.1 Teenuste kasutuselevõtt

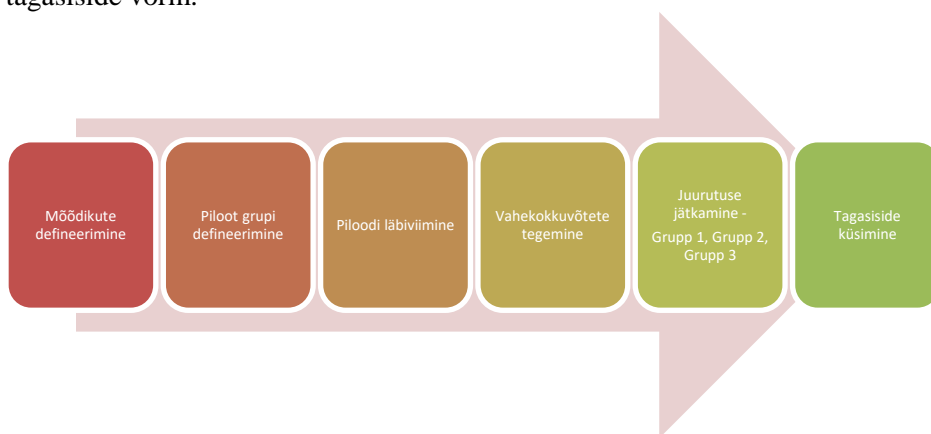
Enne teenuste kasutuselevõttu tuleb veenduda, et pilveteenused oleksid kõik seadistatud vastavalt äriliste vajadustele ja infoturbe poliitikatele. Kui vastavaid infoturbe poliitikaid pole rakendatud, võib juhtuda, et kasutaja vajutab nuppu sünkroniseeri, mistõttu olete koheselt kaotanud kontrolli oma ettevõtte andmete üle. Selle vältimiseks on oluline enne „võtmete kätte“ jagamist teha kogu projektile tagasivaade ja viia läbi täiendavad kontrollid.

Pilveteenuste kasutusevõtuks on oluline eelnevalt koolitada kogu oma IT-meeskond ja töötada läbi korduma kippuvad küsimused. Üks enamlevinumatest küsimustest on kuidas seadistada mitmetasemelise kontrolli, või kuidas toimida uue telefoniga. Selliseid küsimused oleks hea ära dokumenteerida ja lõppkasutajatele lihtsasti kättesaadavaks teha.

Uus administratiivmudel saab alguses kindlasti olema ka administraatoritele võõras, aga järk-järgult peaks see minema lihtsamaks. Muidugi on oluline vastavate juhendite olemasolu ja kohandamine administraatoritele. Uute administraatorite lisandumisel on oluline, et nad saaksid ka vastava koolituse.

Oluline on ka koolitada lõppkasutajad. Sõltuvalt ettevõtte projekti eesmärkidest on kindlasti teemasid, mida käsitleda. Kõige suurem muutus saab olema Microsoft Teamsi kasutuselevõtt. Microsoft Teams nõuab tugevamat äripoolset juhtimist ja vajab head struktuuri. Struktuuri loomine Teamsis ei ole ainult IT-osakonna töö, vaid siin on vaja sisendit äri poolelt. Teamsi juurutamisel tuleb mõista, et tegu ei ole ainult sõnumite saatmise rakendusega. Teams võimaldab kasutusele võtta erinevat tüüpi automaatikat jne. Uute lahenduste parimal viisil rakendamise osas tuleks kindlasti täiendavat tööd teha.

Suurema ettevõtte ülese juurutamise puhul on vaja esmalt läbi viia pilootprojekt. Pilootprojektis peaks olema kaastatud erinevad inimesed erinevate vajadustega. Hea oleks ka defineerida vajalikud mõõdikud ja eesmärgid. Pilootprojekti ajal on oluline koguda kasutajatelt tagasisidet, mille põhjal on võimalik analüüsida seadistuste funktsionaalsust ja kasutaja rahulolu. Selleks võib läbi viia üks-ühele vestlusi või luua kasutajatele vastav tagasiside vorm.



Pilveteenuste juurutamine etappide kaupa

Pilveteenuste juurutamisel üks osa on ka mitmetasemelise kontrolli juurutamine. Mitmetasemelise kontrolli juurutamist saab teha kahel erineval viisil. Varasemalt kasutati

selleks Entra ID mitmetasemelise kontrolli juurutamise portaali, kuid seda lähenemist ei soovitata enam kasutada. Kasutades antud portaali, lülitatakse kasutajatel sisse püsiv mitmetasemelise kontrolli poliitika.

multi-factor authentication

users service settings

Before you begin, take a look at the [multi-factor auth deployment guide](#).

View: Sign-in allowed users Multi-Factor Auth status: Any bulk update

<input type="checkbox"/>	DISPLAY NAME ▲	USER NAME	MULTI-FACTOR AUTH STATUS
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>	Alex Wilber	AlexW@M365x982850.OnMicrosoft.com	Disabled
<input type="checkbox"/>	Allan Deyoung	AllanD@M365x982850.OnMicrosoft.com	Disabled
<input type="checkbox"/>	Diego Siciliani	DiegoS@M365x982850.OnMicrosoft.com	Disabled

Vana Entra ID mitmetasemelise kontrolli seadistuste portaali

Uuem lähenemine on teha seda läbi tingimuslike reeglite, nagu me ka eelnevas peatükis tegime. Kui olete juhuslikult juba kunagi rakendanud mitmetasandilise kontrolli läbi portaali, siis võib selle üle migreerida ka uuele lahendusele. Selleks tuleb Microsofti dokumentatsioonist vastavad PowerShell'i skriptid leida ja vajalikud seadistused ümber teha. Uute kasutajate seadistamisel ei tohi siis enam vana lähenemist kasutada.

Kasutajate seast võib kõige rohkem tagasisidet tulla just mitmetasemelise kontrolli seadistamise üle. Seetõttu tuleb seda aegsasti, väga selgelt ja lihtsalt kommunikeerida. Mitmetasemelise kontrolli edukaks juurutamiseks ei piisa ainult ühekordsest teavitamisest, vaid tegu on järjepideva tööga. Oluline on, et kasutajad oskaksid seda ise kasutusele võtta ja nad saaksid aru, miks see on oluline. Kindlasti tuleks kaasata ettevõtte siseselt kommunikatsioonispetsialistid, kes aitavad seda sõnumit paremini sõnastada.

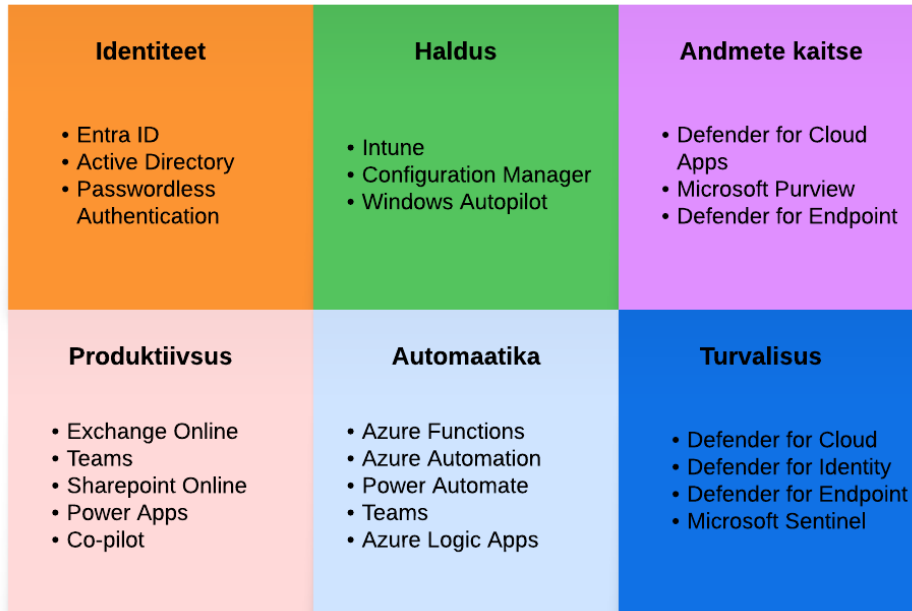
Kui kommunikatsioon on segane või eba piisav, võib juhtuda, et kasutajad ei saa seadistamisega hakkama ja koormavad Helpdeski. Võib ka juhtuda, et mitmetasemelise kontrolli juurutamise protsent jääb väga madalaks, eesmärgiks on aga 100%. Väga tihti on alahinnatud kommunikatsiooni olulisust, mistõttu kogu pilveteenuste projekt jääb edukalt lõpuni viimata. Mitmetasemelise kontrolli seadistamise juhendit tuleb testida erinevate inimeste peal, veendumaks et kasutajad saavad aru, mida neilt oodatakse.

Microsoft on loonud mitmetasemelise kontrolli juurutamiseks eraldi materjalid, mida saab ka väga edukalt kasutada kommunikeerimisel: <https://www.microsoft.com/en-us/download/details.aspx?id=57600>

Kui pilootprojekt on osutunud edukaks ja suuri vigu ei tuvastatud, võib edasi liikuda ülejäänud kasutajatega. Siin on mitmeid võimalusi: kas lähtuda osakondadest või töö spetsiifikast vms. Võimalik on muidugi ka teha kõigile üldteavitus teenuse kättesaadavuse kohta. Viimasel juhul tuleks veenduda, et IT-osakonnas on piisavalt inimesi, kes on valmis kõikide kasutajate küsimustele vastama. Isegi, kui pilootprojekt läks hästi, on hea jätkata tagasiside küsimist kasutajatelt veendumaks, et midagi olulist tähelepanuta ei jää.

12 Kokkuvõte

Office 365 teenuste juurutus ei ole ainult Exchange Online või Teams. Edukaks juurutamiseks on seda pilti vaja vaadata suuremalt ja ühtlasi veenduda, et oleks olemas kompetentne meeskond, kes suudaks seda ellu viia.



Paljude sätete seadistamise osas on oluline omada vajalikku sisendit. Kui analüüs ei ole piisav, on raske ka IT-osakonnal vajalikke seadistusi teha. Sobilike litsentside valimine võib tunduda nii lihtne kui ka keeruline samaaegselt. Võib tunduda ahvatlev hankida kõige eksklusiivsem lahendus, ent selle juurutamiseks ei pruugi ettevõttel olla piisavalt vahendeid ning kompetentsi ja valmidust. Lisaks litsentsidele on oluline veenduda, et Teil oleks ligipääs täiendavatele kulupõhiste teenustele, et küberturbe seisukohast tulenevalt oleks võimalik säilitada pilveteenuste logid ja vajadusel ka seadistada rünnakute tuvastamisi ning automaatikat. Kõige aluseks on ärivajaduste ja riskianalüüs, mis annab ülevaate võimalustest ja valmidusest.

Soovime Teile teadlikku ja tarka juurutamist!