HAMK
Hämeen ammatti-
korkeakoulu

Microsoft 365 Lighthouse IT-palveluntarjoajille

Microsoft 365 Lighthouse laitehallinnan tukena

Tieto- ja viestintätekniikan opinnäytetyö

Tieto- ja viestintätekniikka

2024

Lauri Toropainen

HAMK
Hämeen ammatti-
korkeakoulu

Tieto- ja viestintätekniikka
Lauri Toropainen
Microsoft 365 Lighthouse IT-palveluntarjoajille
Teemu Järvenpää

Tiivistelmä
2024

Tämän opinnäytetyön tavoitteena oli arvioida Microsoft 365 Lighthouse -palvelun ominaisuuksia laite- ja käyttäjähallinnan tehostamisessa, erityisesti uusien asiakkaiden Microsoft 365 -ympäristöjen hallintakäytäntöjen käyttöönoton osin. Työ toteutettiin IT-palvelutalo Vetonaula Oy:n toimeksiannosta, ja sen taustalla oli tarve kartoittaa Microsoft 365 -asiakasympäristöjen laite- ja käyttäjähallinnan käyttöönotto- ja hallintaratkaisuja.

Työssä esitellään Microsoft 365 Lighthousen ja Microsoft Intune -laitehallintapalvelun keskeiset toiminnot ja ominaisuudet sekä käyttöoikeuksiin liittyvät vaatimukset. Käytännön osuudessa testattiin Microsoft 365 Lighthousen toimivuutta reaalimaailman skenaarioissa käyttämällä Vetonaulan testaustarkoitukseen luotua Microsoft 365 -ympäristöä. Microsoft 365 Lighthouse -palvelun hallintakäytäntölinjauksen luonti, kohdistaminen ja käyttöönotto toteutettiin vaiheittain, ja prosessi dokumentoitiin yksityiskohtaisesti.

Tulokset osoittivat, että Microsoft 365 Lighthouse tarjoaa tehokkaita työkaluja IT-palveluntarjoajille, mutta dokumentaation puutteellisuus ja käyttöoikeuksiin liittyvät epäselvyydet aiheuttavat haasteita. Palvelun käyttöoikeushallinnan rajoitteet aiheuttivat myös hidasteita ja ongelmia palvelun käyttöönotossa, sekä hallintakäytäntö ominaisuuksien testaamisessa.

Johtopäätöksissä todetaan, että Microsoft 365 Lighthouse -palvelun hallintakäytäntölinjaukset toimivat hyvänä mallipohjana asiakkaiden hallintakäytäntöjen käyttöönotossa. Etenkin uusien asiakkaiden Microsoft 365 -ympäristöjen käyttöönotossa palvelu voisi nopeuttaa ja selkeyttää prosessia sekä vähentää manuaalisen työn aiheuttamia inhimillisiä virheitä. Palvelun käyttöönotto kuitenkin vaatii IT-palveluntarjoajalta huolellista sisäistä testaamista sekä palvelun sovittamista omaan tuotantoonsa.

Avainsanat Microsoft 365 Lighthouse, hallintakäytännöt, laitehallinta, käyttäjähallinta
Sivut 44

HAMK
Hämeen ammatti-
korkeakoulu

Information and Communication Technology
Lauri Toropainen
Microsoft 365 Lighthouse for MSPs
Teemu Järvenpää

Abstract
2024

The objective of this thesis was to evaluate the features of the Microsoft 365 Lighthouse service in enhancing the management and deployment of device and user management policies, particularly for new customer Microsoft environments. The project was commissioned by the IT service company Vetonaula Oy, driven by the need to explore device and user management solutions for Microsoft customer environments.

The thesis presented the key functions and features of Microsoft 365 Lighthouse and the Microsoft Intune device management service, along with the associated access requirements. The practical part of the study tested the functionality of Lighthouse in real-world scenarios using Vetonaula's test Microsoft environment. The creation, targeting, and deployment of management policy baselines through the Lighthouse service were executed step-by-step, and the process was documented.

The results indicated that Lighthouse offers effective tools for IT service providers, but the lack of comprehensive documentation related to access permissions posed challenges. Restrictions in access management also caused delays and issues in deploying the service and testing the management policy features.

The conclusions suggest that Microsoft 365 Lighthouse's management policy baselines serve as a good template for regularly used management policies. Especially in the deployment of new customer Microsoft environments, the service could streamline and clarify the process. However, deploying the service requires IT service providers to conduct thorough internal testing and adapt the service to their own operations.

Keywords Microsoft Lighthouse, management policies, device management, user management
Pages 44

Sisällys

1 Johdanto 1

2 Tietoperusta 2

2.1 Microsoft 365 Lighthouse 2

2.1.1 Käyttöönoton vaatimukset 3

2.1.2 Microsoft 365 lighthouse -oikeudet 4

2.1.3 Microsoft 365 Lighthouse -portaalin yleiskatsaus 6

2.1.4 Home 7

2.1.5 Tenants 8

2.1.6 Tenant Details 9

2.1.7 Deployment 10

2.2 Microsoft Intune 13

2.2.1 Microsoft Intune -palvelun vaatimukset 13

2.2.2 Yleiskatsaus ja toiminnot 14

2.2.3 Microsoft Intune -palvelun tukemat hallintakäytännöt 15

3 Toiminnallinen osuus: hallintakäytäntöominaisuuksien testaus 17

3.1 Hallintakäytäntölinjauksen luonti ja hallintakäytäntötehtävien lisääminen linjaukseen 17

3.1.1 Vetonaula Demo -hallintakäytäntölinjauksen luonti 18

3.1.2 Hallintakäytäntötehtävien lisääminen luotuun linjaukseen 19

3.2 Hallintakäytäntölinjauksen kohdistaminen asiakasympäristöön 26

3.2.1 Vaatimukset ja vaikutukset 26

3.2.2 Hallintakäytäntölinjauksen kohdistaminen 27

3.3 Hallintakäytäntötehtävien käyttöönotto asiakasympäristöön 28

3.3.1 Käyttöoikeusvaatimukset 28

3.3.2 Hallintakäytäntötehtävien käyttöönotto asiakasympäristöön 29

3.4 Hallintakäytäntötehtävien tilan seuranta asiakasympäristössä 37

4 Tulokset ja johtopäätökset 40

4.1 Dokumentaatio 40

4.2 Microsoft 365 Lighthouse -käyttöoikeudet 40

4.3 Hallintakäytäntölinjauksen ja hallintakäytäntötehtävien luonti 41

4.4 Hallintakäytäntötehtävien käyttöönotto asiakasympäristöön 42

4.5 Johtopäätökset ja suositukset 43

Lähteet 44

Kuvat, taulukot ja kaavat

Kuva 1. Päävalikko 6

Kuva 2. Home 7

Kuva 3. Tenants 8

Kuva 4. Tenant details 9

Kuva 5. Baselines 11

Kuva 6. Deployment Insights 12

Kuva 7. Uusi hallintakäytäntölinjaus 18

Kuva 8. Uusi hallintakäytäntötehtävä 20

Kuva 9. Uusi hallintakäytäntötehtävä 20

Kuva 10. Uusi hallintakäytäntötehtävä 21

Kuva 11. Uusi hallintakäytäntötehtävä 22

Kuva 12. Hallintakäytäntötehtävän konfiguraatioasetukset 23

Kuva 13. Vetonaula Demo Baseline 25

Kuva 14. Hallintakäytäntölinjauksen kohdistaminen 27

Kuva 15. Deployment plan 29

Kuva 16. Hallintakäytäntötehtävän käyttöönoton aloitus 30

Kuva 17. Ehdollisen pääsynhallintakäytännön asiakasympäristökohtaiset konfiguraatiot 31

Kuva 18. Hallintakäytäntötehtävän käyttöönotto -tila 32

Kuva 19. Hallintakäytäntötehtävän ristiriitaiset konfiguraatiot 33

Kuva 20. Hallintakäytäntötehtävän ristiriitaiset & päällekkäiset arvot 34

Kuva 21. Confirm compliance 35

Kuva 22. Hallintakäytäntö tehtävän käyttöönoton viimeistely 36

Kuva 23. Deployment plan 37

Kuva 24. Tehtävien käyttäjien käyttöönottotila 39

1 Johdanto

Digitalisaation ja teknologisen kehityksen myötä pilvipalveluiden merkitys yritysten IT-infrastruktuurin hallinnassa on kasvanut merkittävästi viime vuosina. Tämä kehitys on tuonut, ja tuo jatkuvasti mukanaan uusia haasteita ja mahdollisuuksia IT-palveluiden tarjoajille. Vetonaula Oy, suomalainen IT-palvelutalo, pyrkii jatkuvasti kehittämään ja tehostamaan palveluitaan vastatakseen sekä nykyisten että tulevien asiakkaidensa tarpeisiin. Opinnäytetyön taustalla on tarve kartoittaa Microsoft 365 -asiakasympäristöjen laite- ja käyttäjähallinnan käyttöönotto- ja hallintaratkaisuja. Tässä kontekstissa Microsoft 365 Lighthouse saattaa tarjota arvokkaan työkalun, joka mahdollistaa uusien Microsoft -asiakasympäristöjen käyttöönoton keskitetysti ja tehokkaasti.

Microsoft 365 Lighthouse on suunniteltu pilvipohjaisen hallinnan tarpeisiin, tarjoten IT-palvelijoille työkalut asiakasympäristöjen valvontaan, hallintaan ja tietoturvan ylläpitoon. Yhdessä Microsoft Intunen kanssa, joka on laajalti käytetty laitehallintaratkaisu, Microsoft 365 Lighthouse voisi merkittävästi automatisoida ja yksinkertaistaa Microsoft 365 -asiakkuuksien hallintakäytäntöjen käyttöönottoa. Tämän opinnäytetyön tavoitteena on tutkia ja arvioida Microsoft 365 Lighthousen ominaisuuksia ja mahdollisuuksia Microsoft 365 -asiakasympäristöjen hallinnassa.

Opinnäytetyö jakautuu kolmeen osaan, jotka kattavat teoreettisen tietoperustan, käytännön testauksen, sekä lopuksi tulosten analysoinnin. Työ alkaa tietoperustalla, jossa esitellään Microsoft 365 Lighthouse - ja Microsoft Intune -palveluiden keskeiset toiminnot ja ominaisuudet. Käytännön osuudessa hyödynnetään Vetonaulan testi-Microsoft 365 -ympäristöä, jonka avulla testataan Microsoft 365 Lighthousen toimivuutta reaalimaailman skenaarioissa, painottaen hallintakäytäntöjen käyttöönoton testausta Microsoft 365 Lighthouse -palvelun avulla. Lopuksi analysoidaan saadut tulokset, esitetään johtopäätökset sekä annetaan suositukset Microsoft 365 Lighthousen laajemmasta käyttöönotosta Vetonaula Oy:ssä.

Tämän työn tulokset tarjoavat arvokasta tietoa paitsi Vetonaula Oy:lle, myös muille IT-toimijoille, jotka etsivät uusia työtapoja tehostaakseen Microsoft 365 -asiakasympäristöjen käyttöönottoa ja hallintaa. Tulosten perusteella Vetonaula Oy voi tehdä päätöksiä siitä, miten hyödyntää Microsoft 365 Lighthousen tarjoamia työkaluja tehokkaasti.

2 Tietoperusta

2.1 Microsoft 365 Lighthouse

Microsoft 365 Lighthouse hyödyntää useita siihen integroituja Microsoft-palveluita, kuten Microsoft Intune -laitehallintapalvelua ja Microsoft Defender -tietoturvapalvelua. Näiden palveluiden käyttäminen Microsoft 365 Lighthouse -portaalissa, edellyttää, että asiakasympäristöt omistavat tarvittavat palveluiden tilaukset. (Microsoft, 2023-c)

Keskeiset toiminnot:

- Asiakasympäristöjen käyttöönotto ja hallinta. Microsoft 365 Lighthouse -palvelun tarkoituksena on yksinkertaistaa uusien asiakasympäristöjen hallinnan käyttöönottoa. Microsoft 365 Lighthouse antaa suosituksia hallintakäytäntöihin, jotka soveltuvat erityisesti pienille ja keskisuurille yrityksille, mutta palvelu antaa myös mahdollisuuden IT-kumppaneille luoda omat hallintakäytäntölinjauksensa. Microsoft 365 Lighthouse -portaali tarjoaa näkymän, joka mahdollistaa kaikkien asiakasympäristöjen seurannan ja hallinnan yhdestä paikasta. (Microsoft, 2023-c)

- Riskienhallinta ja turvallisuuden valvonta. Microsoft 365 Lighthouse mahdollistaa turvallisuusuhkien tehokkaan tunnistamisen ja hallinnan. Tekoälypohjaiset työkalut analysoivat jatkuvasti toimintaa ja tarjoavat suosituksia riskeihin puuttumiseksi. Tämä auttaa IT-kumppania ylläpitämään asiakasympäristöjen turvallisuutta ja varmistamaan, että ne pysyvät suojattuina. (Microsoft, 2023-c)

- Myynti- ja asiakassuhteiden hallinta. tekoäly-ohjatut oivallukset antavat IT-kumppaneille työkaluja uusien asiakkaiden hankkimiseen, ja olemassa olevien asiakassuhteiden syventämiseen. Microsoft 365 Lighthouse tarjoaa personoituja suosituksia ja toimia, jotka mahdollisesti auttavat IT-kumppaneita kasvattamaan liiketoimintaansa. (Microsoft, 2023-c)

- Laitteiden ja palveluiden ylläpito. Microsoft 365 Lighthouse käyttää apunaan Microsoft Intune -laitehallintapalvelua ja tarjoaa yksityiskohtaisia tietoja laitteiden tilasta, sekä mahdollistaa hallintakäytäntövertailut. Tämä auttaa IT-kumppania varmistamaan, että kaikki laitteet noudattavat yhtenäisiä turvallisuusstandardeja. Lisäksi Microsoft 365 Lighthouse helpottaa yleisiä ylläpitotehtäviä, kuten salasanojen resetointia, MFA-autentikoinnin asetuksia ja itsepalvelusalasanan nollauksia (SSPR). (Microsoft, 2023-c)

2.1.1 Käyttöönoton vaatimukset

Microsoft 365 Lighthouse -palvelun vaatimusten tarkoituksena on varmistaa, että vain oikeutetut kumppanit ja heidän asiakasympäristönsä voivat hyödyntää sen tarjoamia toimintoja. Tässä luvussa käydään lävitse sekä IT-kumppanin että kumppanin asiakkuuksilta vaaditut ominaisuudet Microsoft 365 Lighthouse -palvelun käyttöönottoon.

Microsoft 365 Lighthouse on saatavilla Microsoftin Cloud Solution Provider (CSP) -ohjelmaan rekisteröityneille kumppaneille. Ohjelmaan kuuluvat sekä suorat laskuttajat (Direct-Bill) että epäsuorat jälleenmyyjät (Indirect Resellers), kuten Vetonaula Oy, joka on rekisteröitynyt epäsuoraksi jälleenmyyjäksi. Kumppanin on oltava CSP-ohjelmaan rekisteröitynyt, mutta heidän hallinnoimiensa asiakasympäristöjen ei tarvitse olla ohjelman piirissä. (Microsoft, 2024-d)

Seuraavaksi lueteltavat ehdot on täytyttävä, jotta tässä työssä esimerkkinä käytetty Vetonaulan testi-asiakasympäristö, kuten muutkin Microsoft 365 -asiakasympäristöt näkyvät niitä hallitsevan IT-kumppanin Microsoft 365 Lighthouse -portaalissa (Microsoft, 2024-d):

- Kumppanin ja asiakasympäristön välille on oltava muodostettu kumppanuussuhde, joko delegoidun järjestelmänvalvojan hajautettujen oikeuksien (GDAP) tai delegoidun järjestelmänvalvojan oikeuksien (DAP) kautta.
- Asiakasympäristön on omistettava vähintään yksi seuraavista Microsoft-tilauksista: Microsoft 365, Office 365, Exchange Online, Windows 365 Business tai Microsoft Defender for Business.
- Asiakasympäristössä saa olla korkeintaan 2500 lisensioitua käyttäjää.
- Asiakasympäristön on sijaittava samalla maantieteellisellä alueella (esimerkiksi Pohjois-Amerikka, Euroopan unioni tai Aasia) kuin kumppaniorganisaatio, joka niitä hallinnoi.

Näiden vaatimusten täyttyessä asiakasympäristöt ilmestyvät automaattisesti kumppanin Microsoft 365 Lighthouse -portaaliin, tarjoten IT-kumppanille mahdollisuuden aloittaa asiakkuuksien hallinta ja valvonta Microsoft 365 Lighthouse -portaalin avulla.

Vaikka edellä mainitut vaatimukset takaavat Microsoft 365 Lighthouse -portaalin perustoiminnallisuuden, eivät ne yksinään riitä kaikkien Lighthouse-ominaisuuksien käyttöön. Microsoft 365 Lighthousen tarjoamat edistyneemmät toiminnot, kuten tekoälypohjaiset analyysityökalut ja erityiset tietoturvapalvelut, vaativat asiakasympäristöltä tiettyjen Microsoft-palveluiden lisenssejä. (Microsoft, 2024-d)

Työssä käytettyjen Lighthouse-ominaisuuksien tarkemmat vaatimukset käsitellään myöhemmissä kappaleissa

2.1.2 Microsoft 365 lighthouse -oikeudet

Microsoft 365 Lighthouse -palvelun oikeuksia hallitaan pääasiassa kahden mekanismin kautta, roolipohjainen pääsynhallinta (RBAC) IT-kumppanin Microsoft 365 -ympäristössä, sekä delegoidun järjestelmänvalvojan hajautetut oikeudet (GDAP) asiakasympäristöissä. Näiden mekanismien on tarkoitus kontrolloida sitä, kuka pääsee käsiksi mihinkin tietoihin ja mitä muutoksia he voivat suorittaa Microsoft 365 Lighthouse -portaalissa. (Microsoft, 2024-b)

Microsoft 365 Lighthouse hyödyntää roolipohjaista pääsynhallintaa (RBAC). RBAC-roolit mahdollistavat käyttöoikeudet, joiden avulla voidaan määritellä, mitä tietoja ja toimintoja palvelun käyttäjät voivat hallita. Tämä järjestelmä on suunniteltu turvaamaan ja tehostamaan asiakasympäristöjen hallintaa antamalla IT-kumppanin teknikoille vain tarpeelliset oikeudet heidän tehtäviensä suorittamiseen. (Microsoft, 2024-b)

RBAC-rooleja hallitaan Microsoft 365 Lighthouse -permissions sivun kautta. Vain IT-kumppanin Microsoft 365 -ympäristön globaalit järjestelmänvalvojat voivat hallita näitä rooleja, mikä varmistaa, että vain valtuutetut henkilöt voivat määrittää tai muuttaa käyttöoikeuksia. (Microsoft, 2024-b)

Tällä hetkellä Microsoft 365 Lighthousessa on käytössä vain yksi RBAC-rooli: ”Lighthouse Account Manager”. Rooli antaa lukuoikeudet suurimpaan osaan Microsoft 365 Lighthouse -portaaliin ominaisuuksista.

Vain yhden RBAC-roolin tarjoaminen rajoittaa joustavuutta ja hankaloittaa käyttöoikeuksien tarkkaa kohdentamista IT-kumppanin tarpeisiin. Tämä lisää turvallisuusriskiä ja vähentää kykyä mukauttaa käyttöoikeuksia eri käyttäjäryhmien vaatimuksiin sopiviksi. Tästä syystä Microsoft 365 Lighthouse -oikeudet jaetaan pääosin GDAP-roolien avulla.

Delegoidun järjestelmänvalvojan hajautetut oikeudet (GDAP) tarjoaa tarkempaa kontrollia ja joustavuutta määrittämällä IT-kumppanin käyttäjien oikeudet asiakasympäristöihin Microsoftin sisäänrakennettujen roolien kautta. Kumppanin ja asiakkaiden välisillä kumppanuussuhteilla (GDAP) pystytään siis rajoittamaan IT-kumppanin teknikoiden suoraa hallintaa asiakasympäristöiden käyttämiin ominaisuuksiin ja tätä kautta teknikoille voidaan antaa tehtäväkohtaisesti vähiten oikeuksia sisältäviä rooleja. (Microsoft, 2024-b)

Microsoft 365 Lighthouse -palvelun käyttöoikeushallinnan ymmärtäminen on kriittisen tärkeää IT-kumppanille, jotta se voi tehokkaasti hallita ja suojata Microsoft -asiakkuuksiaan. RBAC ja GDAP tarjoavat yhdessä työkalut ja menetelmät, joiden tarkoituksena on varmistaa, että vain oikeutetut henkilöt pääsisivät käsiksi arkaluontoisiin tietoihin ja pystyisivät suorittaa toimintoja asiakasympäristöissä. Näiden järjestelmien asianmukainen konfigurointi ja ylläpito ovat avainasemassa turvallisen ja tehokkaan IT-palvelun tarjoamisessa.

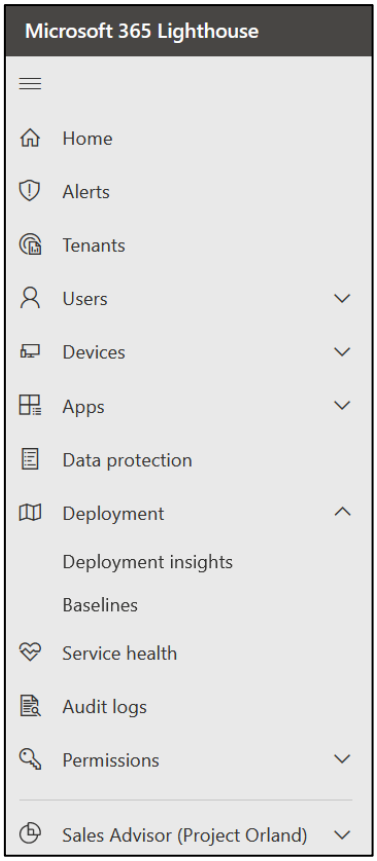
2.1.3 Microsoft 365 Lighthouse -portaalin yleiskatsaus

Alaluvuissa 2.1.3 – 2.1.7 käydään läpi Microsoft 365 Lighthouse -portaali ja sen sisältämät sivut ja välilehdet, joita hyödynnetään työn toiminnallisessa osuudessa. Lukujen tarkoituksena on hahmoitella, miltä palvelun portaali todellisuudessa näyttää, sekä käydään yleisesti läpi työssä käytettäviä ominaisuuksia.

Microsoft 365 Lighthouse -portaalin verkko-osoite on: “https://lighthouse.microsoft.com”.

Kuva 1. esittelee Microsoft 365 Lighthouse -portaalin päävalikon, jonka avulla onnistuu pääsy keskeisiin hallintatoimintoihin ja näkymiin.

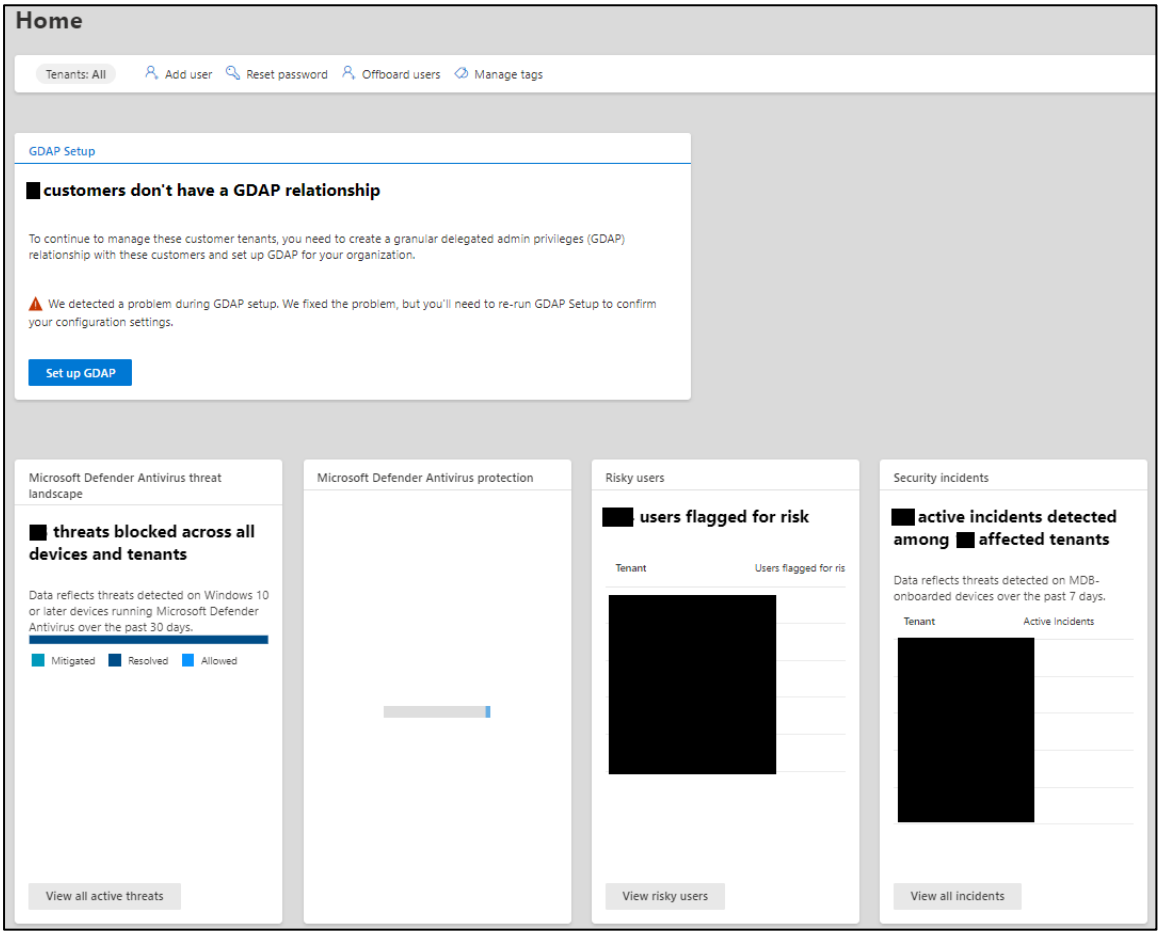
Kuva 1. Päävalikko



2.1.4 Home

Home -sivu toimii perinteiseen tapaan kotinäkymänä koko Microsoft 365 Lighthouse -portaalille. Käyttäjä pystyy itse muokkaamaan graafista käyttöliittymää joustavasti ja lisäämään siihen käyttäjälle tärkeimpiä Lighthouse-palvelun ominaisuuksia vastaavat pienoisohjelmat. Näkymän kautta siirtyminen haluttuihin ominaisuuksiin tapahtuu helposti lisättyjen pienoisohjelmien tai päävalikon kautta.

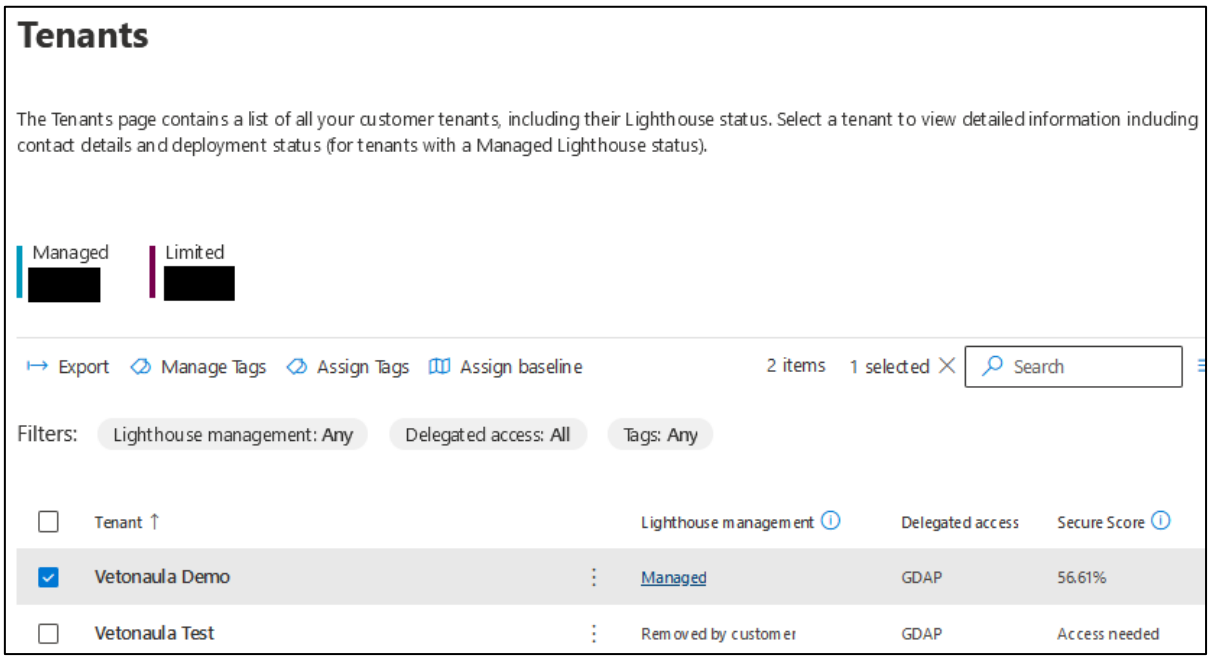
Kuva 2. Home



2.1.5 Tenants

Tenants -sivulle on listattu kaikki IT-kumppanin hallitsemat Microsoft 365 -asiakasympäristöt, jotka täyttävät asiakasympäristöjen Lighthouse-vaatimukset. Vaatimukset ovat listattu alaluvussa 2.1.1 Käyttöönoton vaatimukset.

Kuva 3. Tenants



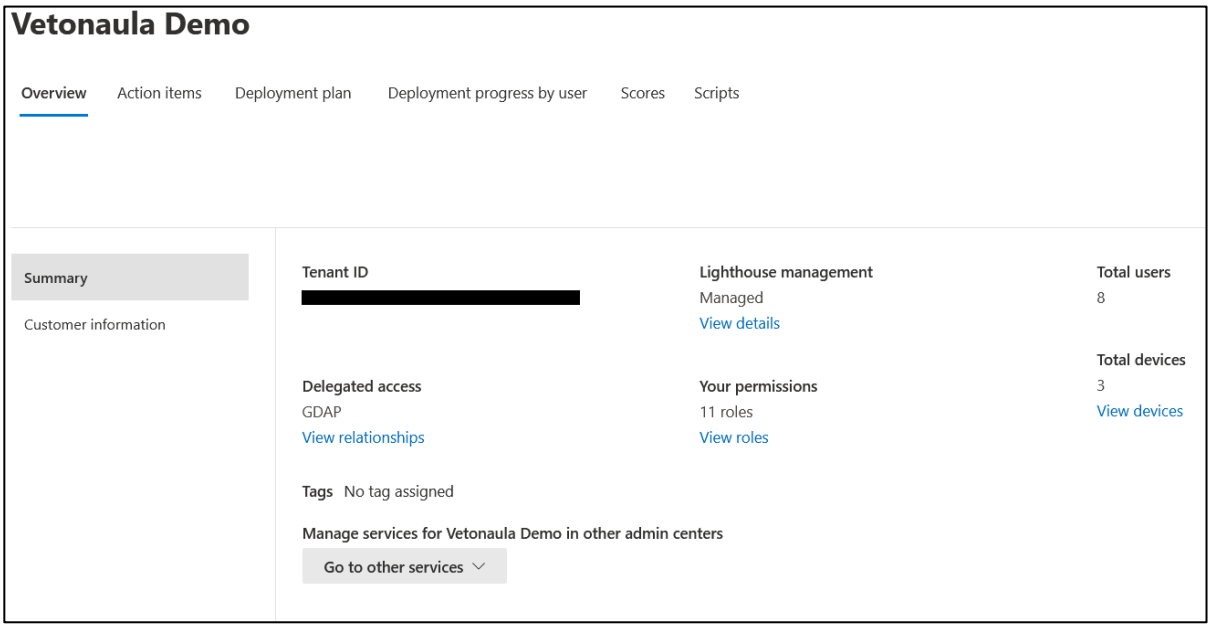
Tenants -sivulta löytyy seuraavat toiminnot:

- Export: Viedään asiakasympäristön listaus Excel CSV-tiedostoon.
- Manage Tags: Lisätään, muokataan tai poistetaan tunnisteita. Tunnisteiden avulla voidaan järjestellä asiakasympäristöjä ja suodattaa näkymiä helposti. Tunnisteiden luominen ja määrittäminen auttaa organisoimaan ja hallitsemaan asiakasympäristöjä tehokkaammin. Tunnisteita voidaan käyttää esimerkiksi asiakasympäristöjen jakamiseen IT-kumppanin eri asiakastiimeille.
- Assign Tags: Määritetään tunnisteita asiakasympäristöille.
- Assign Baseline: Määritetään hallintakäytäntölinjauksia asiakasympäristöille. Näihin linjauksiin palataan alaluvussa 2.1.7.
- Search: Etsitään tiettyjä asiakasympäristöjä avainsanojen avulla.

2.1.6 Tenant Details

Tenant details -sivu aukeaa, kun Tenants -sivun ympäristölistauksesta valitaan tietty asiakasympäristö. Sivulla on useita välilehtiä, jotka tarjoavat kattavan näkymän asiakasympäristön tilaan ja hallintaan.

Kuva 4. Tenant details



Tenant details -sivun keskeisimmät välilehdet ovat listattu alla:

- Overview -välilehti sisältää asiakasympäristön yleiset tiedot, yhteystiedot sekä graafista dataa Microsoft 365 -palveluiden käytöstä. Täältä löytyy tietoja kuten asiakkaan verkkotunnus, asiakasympäristön yksillöllinen tunniste (tenant-ID), hallintatila, GDAP-käyttöoikeus tiedot, käyttäjien ja laitteiden määrä sekä turvallisuus- ja käyttöönottoarvot.

- Deployment plan -välilehti näyttää asiakasympäristön käyttöönoton tilan, joka perustuu ympäristölle määritettyyn hallintakäytäntölinjaukseen. Täällä voidaan tarkastella linjauksen käyttöönottoaskeleita ja edistymistä.

- Deployment progress by user -välilehti tarjoaa näkymän kunkin käyttäjän käyttöönoton tilaan.

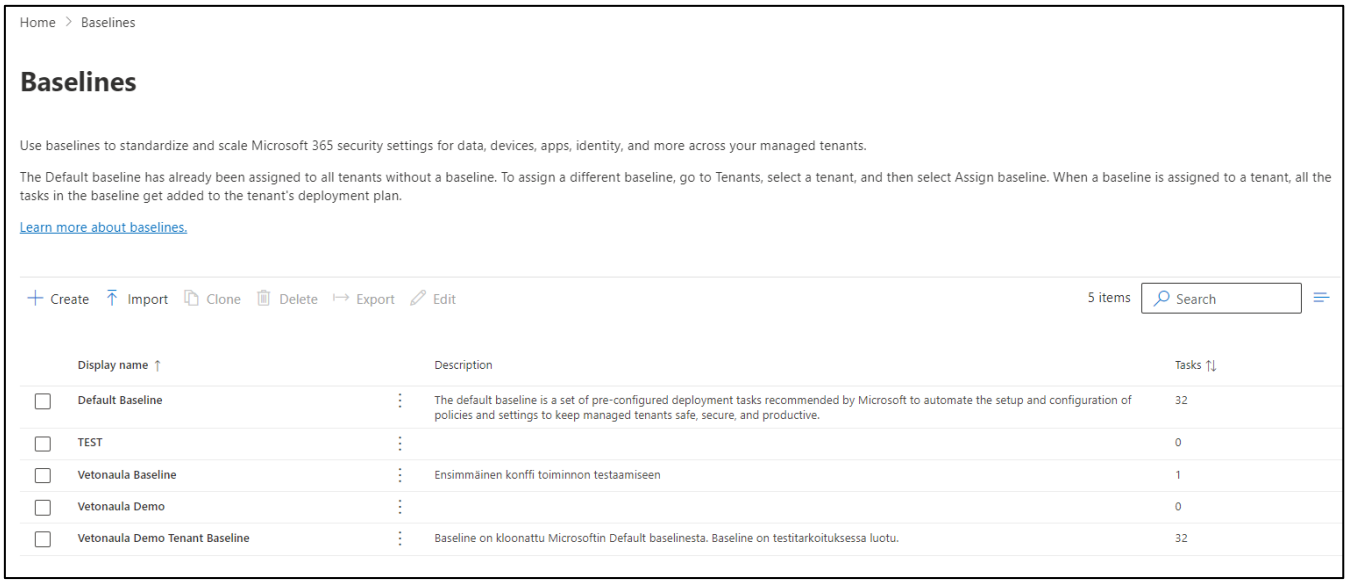
2.1.7 Deployment

Deployment -sivut tarjoavat työkalun asiakasympäristöjen käyttöönoton hallintaan. Tämä osio sisältää kaksi alisivua: "Deployment Insights" ja "Baselines". Deployment -sivut ja niiden ominaisuudet ovat tämän työn kannalta keskeisimpiä, koska ne mahdollistavat hallintakäytäntölinjausten luomisen ja niiden jakamisen asiakasympäristöihin. Käyttöönoton ominaisuudet käyttävät apunaan Microsoft 365 Lighthouse -palveluun integroitua Microsoft Intune -laitehallintapalvelua. Näiden ominaisuuksien käyttö vaatii asiakasympäristöiltä Microsoft Intune tilauksen.

Baselines

Baselines -sivulla IT-kumppani voi vakioida hallintakäytäntölinjauksiaan (baselines) keskitetysti. Tällä sivulla tapahtuu hallintakäytäntölinjausten luonti ja hallinta. Linjaukset toimivat mallipohjana, joka sisältää joukon hallintakäytäntötehtäviä (tasks). Tehtävät pitävät sisällään aina yhden hallintakäytännön, sekä sen konfiguraatioasetukset.
Tältä sivulta voidaan luoda, tuoda, monistaa, poistaa, viedä ja muokata hallintakäytäntölinjauksia.

Kuva 5. Baselines



Baselines-sivun keskeisimmät ominaisuudet ovat:

- Create**:** Luo uusi hallintakäytäntölinjaus määrittelemällä sen tehtävät ja asetukset.
- Import**:** Tuo aiemmin luotu hallintakäytäntölinjaus tiedostosta.
- Clone**:** Monista olemassa oleva hallintakäytäntölinjaus uuden perustaksi.
- Delete**:** Poista valittu hallintakäytäntölinjaus.
- Export**:** Vie hallintakäytäntölinjaus tiedostoon myöhempää käyttöä varten.
- Edit**:** Muokkaa olemassa olevaa hallintakäytäntölinjausta.

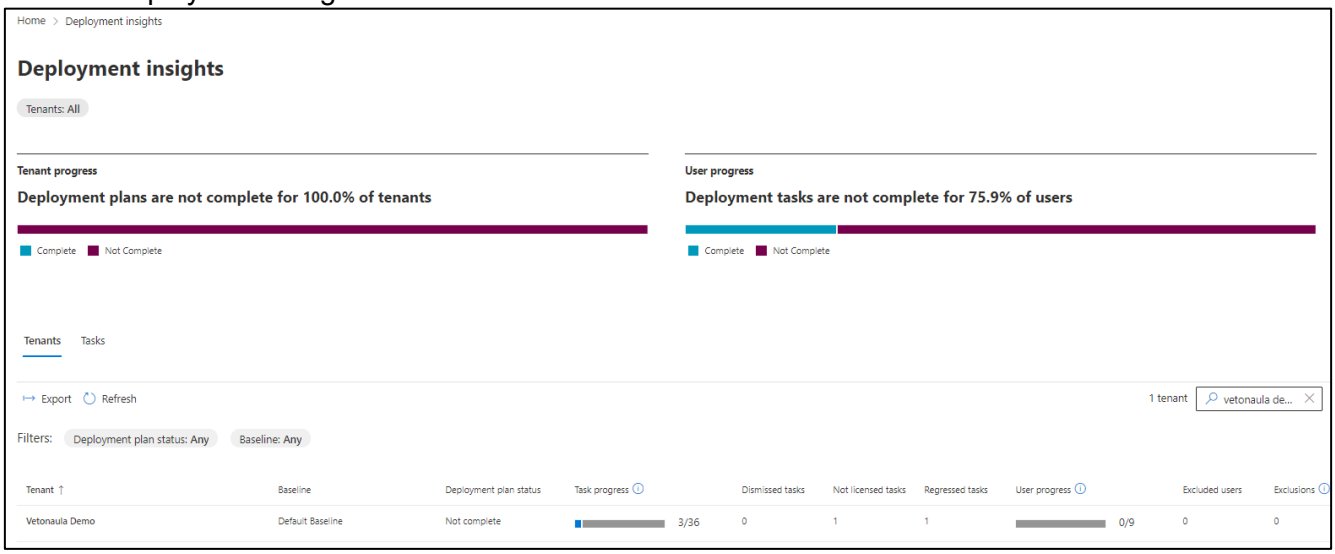
Näiden toimintojen avulla IT-kumppanit voivat hallita ja optimoida asiakasympäristöjensä hallintakäytäntöjä.

Microsoftin 365 Lighthouse -palvelun oletus hallintakäytäntölinjaus (Default Baseline) on automaattisesti määritetty kaikille asiakasympäristöille, joilla ei ole vielä määritelty omaa linjausta. (Microsoft, 2024-c)

Deployment Insights

Deployment Insights -sivu tarjoaa syvällisen näkymän asiakasympäristöjen käyttöönoton edistymiseen ja auttaa IT-kumppania seuraamaan ja optimoimaan hallintakäytäntölinjausten sekä niiden sisältämien hallintakäytäntötehtävien käyttöönottoa.

Kuva 6. Deployment Insights



Deployment Insights -sivulla voidaan tarkkailla keskitetysti kaikkien asiakkuuksien hallintakäytäntötehtävien sekä linjausten käyttöönoton tilaa. Kuvakaappauksen (Kuva 6.) mukaisesti kaaviosta voidaan nähdä, kuinka moni asiakasympäristö on suorittanut kaikki tehtävät ja kuinka monella ympäristöllä on vielä tehtäviä kesken.
Tenants-välilehdellä voidaan tarkastella kunkin asiakasympäristön, sekä ympäristön sisältämien käyttäjien yksityiskohtaisia käyttöönoton tilatietoja, mukaan lukien lisenssien tilaa ja mahdollisia poikkeamia. Tietoja voidaan suodattaa ja etsiä tarpeen mukaan.

Deployment Insights -sivun avulla IT-kumppanit voivat tunnistaa käyttöönoton tilan kaikissa asiakasympäristöissä, käyttäjissä ja tehtävissä. Kumppani voi tarkastella käyttöönoton poikkeamia, kuten hylättyjä tehtäviä ja yhteensopimattomia käyttäjiä. Sivulla voidaan tutkia hallintakäytäntötehtäviä, joiden tila-arvot ovat muuttuneet yhteensopimattomaksi tai ei-lisensoiduksi. IT-kumppani voi arvioida uhkia käyttäjien ja tehtävien käyttöönoton edistymisen perusteella sekä priorisoida käyttöönoton toimenpiteitä riskin perusteella. (Microsoft, 2023-f)

Deployment Insights tarjoaa IT-kumppaneille kattavat työkalut seurata, analysoida ja optimoida hallintakäytäntölinjausten käyttöönottoa, mikä parantaa yleistä hallintaa ja turvallisuutta kaikissa hallituissa asiakasympäristöissä.

2.2 Microsoft Intune

Microsoft Intune on pilvipalvelupohjainen laitehallintaratkaisu, joka mahdollistaa organisaatioiden erilaisten laitteiden keskitetyn hallinnan ja suojaamisen. Organisaatiot kohtaavat haasteita laitteiden hallinnassa, kun työntekijät ja opiskelijat tarvitsevat pääsyn organisaation resursseihin sijainnista riippumatta. Heidän täytyy organisaation sisäisesti pystyä tekemään yhteistyötä, työskentelemään etänä ja pääsemään turvallisesti käsiksi näihin resursseihin. Järjestelmänvalvojien tehtävänä on suojata organisaation tiedot, hallita loppukäyttäjien pääsyä ja tarjota tukea riippumatta siitä, missä käyttäjät työskentelevät.

Microsoft Intune auttaa näiden haasteiden ratkaisemisessa tarjoamalla kattavan päätepisteiden hallintaratkaisun. Se hallinnoi käyttäjien pääsyä organisaation resursseihin ja yksinkertaistaa sovellusten ja laitteiden hallintaa monilla eri laitteilla, mukaan lukien mobiililaitteilla, pöytäkoneilla ja virtuaalisilla päätepisteillä. Microsoft Intune tarjoaa laajat työkalut käyttäjien, laitteiden sekä sovellusten ja hallintakäytäntöjen hallintaan, mikä mahdollistaa tehokkaan tuen hybridi- ja etätyövoimalle. (Microsoft, 2024-a)

2.2.1 Microsoft Intune -palvelun vaatimukset

Microsoft Intune vaatii toimiakseen seuraavia asioita asiakkaan Microsoft 365 -ympäristöltä (Microsoft, 2023-b):

- Asiakasympäristön laitteiden on oltava rekisteröity Microsoft Intuneen, jotta niitä voidaan hallita. Rekisteröinti mahdollistaa laitteiden etähallinnan ja sovellusten hallinnan.

- Laitteiden on oltava yhteydessä internettiin, jotta ne voivat vastaanottaa Microsoft Intunen käskyjä sekä lähettää tilannetietoja.

- Asiakasympäristöllä on oltava tarvittavat Microsoft 365 -tilaukset, jotka kattavat Microsoft Intunen käytön. Esimerkiksi Microsoft 365 Business Premium tai Microsoft 365 E3/E5 tilaukset.

- Microsoft Intune intergroituu pilvipalvelupohjaisen identiteetti- ja pääsynhallintaratkaisu Microsoft Entra ID -palvelun kanssa, joten asiakasympäristöllä on oltava Entra ID -tilaus käyttäjien ja laitteiden todentamista sekä käyttöoikeuksien hallintaa varten.

2.2.2 Yleiskatsaus ja toiminnot

Microsoft Intune tarjoaa monipuoliset toiminnot, joiden avulla IT-kumppanit voivat hallita ja suojata asiakkaidensa laitteita, sovelluksia ja käyttäjiä. Microsoft Intune mahdollistaa laitteiden ja sovellusten keskitetyn hallinnan sekä tietoturvan varmistamisen useilla eri laitetyypeillä ja käyttöjärjestelmillä, mikä tekee siitä tehokkaan työkalun modernille IT-hallinnalle.

Microsoft Intune mahdollistaa monenlaisten laitteiden, kuten Android-, iOS/iPadOS-, Windows-, macOS- ja Linux Ubuntu Desktop -laitteiden hallinnan. Tämä yhtenäinen hallinta parantaa tietoturvaa ja hallinnan tehokkuutta kaikille organisaation laitteille. (Microsoft, 2024-a)

Microsoft Intune tarjoaa sisäänrakennetun sovellushallinnan, joka kattaa sovellusten jakelun, päivitykset ja poistot. Microsoft Intune mahdollistaa myös yrityssovellusten ja -datan suojaamisen, ilman että laitetta tarvitsee rekisteröidä hallintaan. (Microsoft, 2024-a)

Microsoft Intune sisältää työkaluja hallintakäytäntöjen luomiseen ja hallintaan. Näihin kuuluvat salausasetukset, salasanasäännöt, palomuurimääritykset sekä laitteiden yhteensopivuuden vertaus laitehallinnassa määritettyihin käytäntöihin. Näiden työkalujen avulla voidaan varmistaa, että kaikki laitteet noudattavat organisaation tietoturvastandardeja. (Microsoft, 2024-a)

Microsoft Intune integroituu saumattomasti Microsoft Entra ID -palvelun kanssa, mikä mahdollistaa yksityiskohtaisen pääsynvalvonnan ja identiteettien hallinnan. Pääsynvalvonnan tarkoitus on hallita ja suojata organisaation resursseja varmistamalla, että vain valtuutetut käyttäjät ja laitteet pääsevät käsiksi organisaation resursseihin. Pääsynvalvonnan käytäntöjen avulla voidaan varmistaa, että pääsy organisaation resursseihin perustuu laitteen tilaan, käyttäjän sijaintiin ja muihin määriteltyihin ehtoihin. (Microsoft, 2024-a)

Microsoft Intune tarjoaa myös käyttäjille mahdollisuuden hyödyntää itsepalveluominaisuuksia, mikä vähentää IT-tuen tarvetta ja parantaa käyttäjäkokemusta. Itsepalveluominaisuuksien avulla käyttäjät voivat esimerkiksi palauttaa unohtuneen tietokoneen PIN-koodin ja asentaa laitehallinnan kautta jaeltuja tarvitsemiaan sovelluksia. (Microsoft, 2024-a)

2.2.3 Microsoft Intune -palvelun tukemat hallintakäytännöt

Microsoft Intune mahdollistaa laajan valikoiman hallintakäytäntöjä, joiden avulla organisaatiot voivat hallita ja suojata laitteitaan sekä käyttäjiään tehokkaasti. Hallintakäytännöt tarjoavat keskitetyn tavan määrittää ja jaella erilaisia sääntöjä ja asetuksia laitteille, mikä parantaa tietoturvaa, yhtenäistää yrityksen toimintaa sekä tehostaa hallintatoimia.

On kolmen tyyppisiä Microsoft Intune -hallintakäytäntöjä, mukaan lukien:

1. Konfiguraatiokäytännöt: Nämä ovat Intune-palvelun versio perinteisistä ryhmäkäytännöistä (Group Policies). Niiden avulla voidaan soveltaa ennalta määritettyjä asetuksia käyttäjiin tai laitteisiin.
   Esimerkkinä Wi-Fi-asetukset: määritetään laitteiden automaattinen yhdistäminen organisaation langattomaan verkkoon.

2. Tietoturvakäytännöt: Tietoturvakäytännöt tai tietoturvatasot ovat Windows-asetuksia, joiden avulla voidaan soveltaa tunnettua asetuskokonaisuutta ja oletusarvoja, joita Microsoft suosittelee. Näiden käytäntöjen avulla voidaan nopeasti ja helposti suojata päätepisteitä ja tällä tavoin koko Microsoft 365 ympäristöä.
   Esimerkkinä salausvaatimukset: edellytetään laitteiden käyttävän salausmenetelmiä, kuten BitLocker-levynsalausta Windows-laitteissa, tietojen suojaamiseksi luvattomalta pääsyltä.

3. Yhdenmukaisuuskäytännöt: Yhdenmukaisuuskäytännöt arvioivat laitteen yhdenmukaisuutta määritetyn tason perusteella, kuten laitteen salaussääntöjen tai tietyn käyttöjärjestelmäversion minimivaatimuksien perusteella. Ne ovat hyödyllisiä poikkeamien havaitsemiseksi ja yhdessä Entra ID -palvelun käyttämien ehdollisten pääsynhallintakäytäntöjen kanssa ne voivat rajoittaa laitteen pääsyä, jos sitä pidetään yhteensopimattomana.
   Esimerkkinä salasanavaatimukset: määritetään minimivaatimukset salasanojen pituudelle, monimutkaisuudelle ja vaihtotiheydelle, mikä parantaa tilien turvallisuutta.

   Ehdolliset pääsynhallintakäytännöt ovat Entra ID -palvelun ylläpitämiä hallintakäytäntöjä, tämän takia niitä ei sisällytetä ylläolevaan listaukseen, mutta niitä voidaan hallita sekä luoda myös Microsoft Intune -palvelun kautta.

Hallintakäytännöt parantavat organisaation tietoturvaa ja hallinnan tehokkuutta keskittämällä ja automatisoimalla laite-, käyttäjä- ja sovellusasetukset. Ne mahdollistavat nopean reagoinnin tietoturvauhkien ilmetessä ja varmistavat, että kaikki laitteet noudattavat organisaation tietoturvastandardeja. Esimerkiksi, kun uusi tietoturvauhka ilmoitus julkaistaan, organisaatio voi nopeasti päivittää kaikki laitteet uusilla suojausasetuksilla yhden keskitetyn hallintaportaalin kautta.

3 Toiminnallinen osuus: hallintakäytäntöominaisuuksien testaus

Työn toiminnallisessa osuudessa testataan Microsoft 365 Lighthouse -palvelun hallintakäytäntö ominaisuuksia. Testataan hallintakäytäntölinjauksen luontia, kohdistamista sekä käyttöönottoa. Tätä varten käytetään Vetonaulan testi-Microsoft 365 -ympäristöä "Vetonaula Demo", joka toimii testeissä esimerkkiasiakkuutena, johon luotava hallintakäytäntölinjaus on tarkoitus kohdistaa ja lopuksi käyttöönottaa. Microsoft 365 Lighthouse -palvelun valmiuksia, sekä toimivuutta arvioidaan toiminnallisessa osuudessa tehtyjen testien perusteella tarkemmin luvussa 4.

Tämä osio sisältää kuvakaappauksia ja yksityiskohtaisia ohjeita, jotka helpottavat prosessin ymmärtämistä.

3.1 Hallintakäytäntölinjauksen luonti ja hallintakäytäntötehtävien lisääminen linjaukseen

Tässä osiossa luodaan "Vetonaula Demo Baseline" -niminen hallintakäytäntölinjaus. Tämän avulla havainnollistetaan, miten hallintakäytäntölinjaus luodaan ja mitä yksityiskohtia tulee ottaa huomioon sen luonnin yhteydessä.

Uuden hallintakäytäntölinjauksen voi luoda kolmella eri tavalla:

- Kopioimalla portaalissa jo olemassa olevan hallintakäytäntölinjauksen, ja sen pohjalta uuden rakentamisen.

- Tuomalla hallintakäytäntölinjauksen tiedostosta (linjaukset käyttävät “JSON” tiedostomuotoa.

- Luomalla uuden tyhjän hallintakäytäntölinjauksen.

(Microsoft, 2023-a)

3.1.1 Vetonaula Demo -hallintakäytäntölinjauksen luonti

Hallintakäytäntölinjauksen luonti tapahtuu Microsoft 365 Lighthouse -portaalin Baselines-sivulta. Tämä sivu mahdollistaa uusien hallintakäytäntölinjausten luomisen ja olemassa olevien hallinnan.

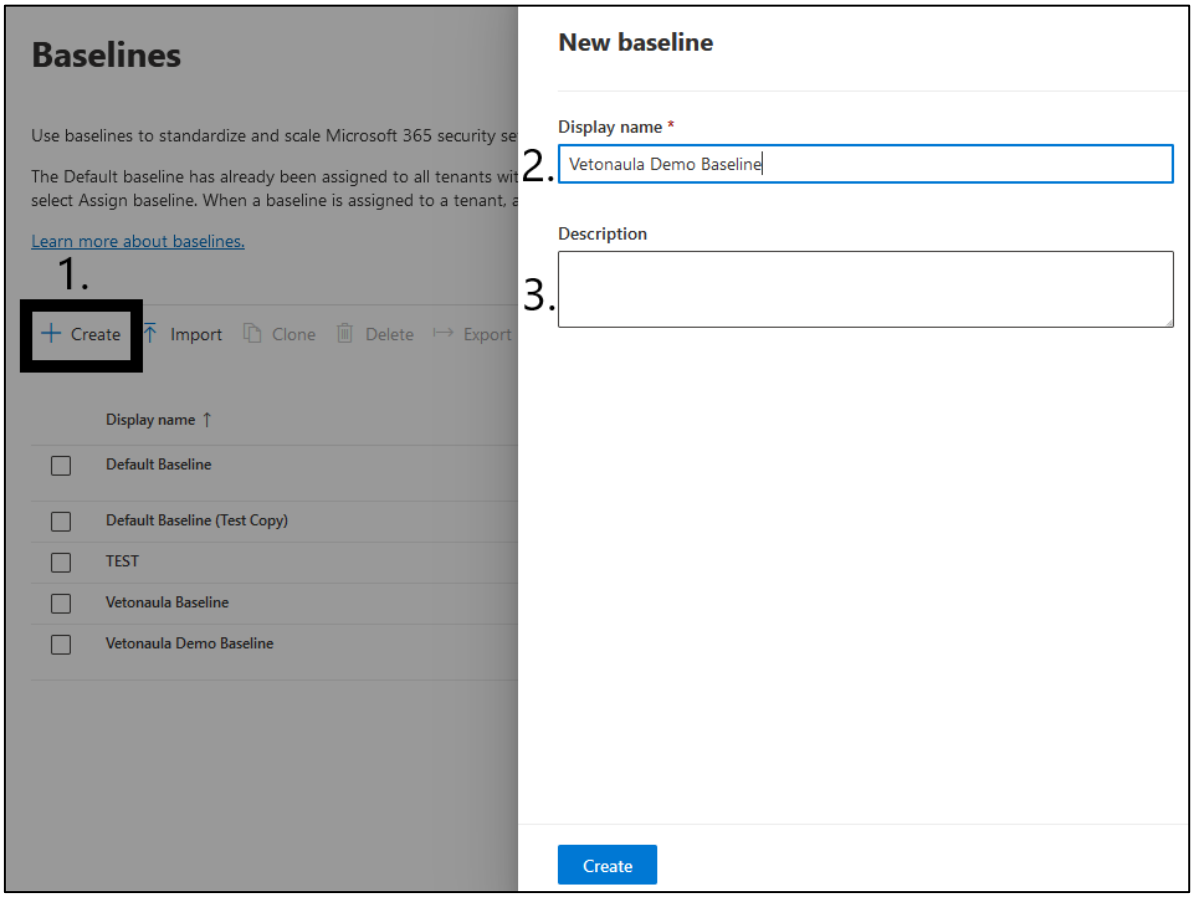
Kuvassa 7. hahmotellaan uuden linjauksen luominen seuraavilla ohjeilla:

1. Valitaan "Create", ja luodaan uusi hallintakäytäntölinjaus.

2. Annetaan hallintakäytäntölinjaukselle nimi, tässä tapauksessa: "Vetonaula Demo Baseline".

3. Lisätään kuvaus, jossa kerrotaan lyhyesti linjauksen tarkoitus ja sisältö.

Kuva 7. Uusi hallintakäytäntölinjaus



3.1.2 Hallintakäytäntötehtävien lisääminen luotuun linjaukseen

Kun uusi hallintakäytäntölinjaus, tässä tapauksessa "Vetonaula Demo Baseline", on luotu, on seuraavana vaiheena lisätä siihen hallintakäytäntötehtävät.

Hallintakäytäntötehtävien luontiin on kaksi mahdollista menetelmää:

1. Tehtävän kloonaaminen toisesta hallintakäytäntölinjauksesta

2. Kopioimalla haluttu hallintakäytäntö asiakasympäristöstä ja luomalla siitä uusi hallintakäytäntötehtävä. (Tätä menetelmää käytetään tässä työssä.)

Jälkimmäisessä menetelmässä tulee huomioida, että hallintakäytäntöön ei jää asiakasympäristökohtaisia asetuksia tai kohdistuksia, kohdistuksilla tarkoitetaan hallintakäytäntöjen sisäisiä kohdistusmääritelmiä, joilla kohdistetaan tai epäkohdistetaan käytäntö tiettyihin ryhmiin/käyttäjiin/sijainteihin/laitteisiin yms.

Kopioidessa hallintakäytäntöä asiakasympäristöstä, Microsoft ohjeistaa seuraavalla tavalla:

Microsoft 365 Lighthouse tunnistaa mahdollisuuksien mukaan hallintakäytännöt, jotka sisältävät arkaluonteista tietoa, ja poistaa asiakasympäristökohtaiset arvot hallintakäytäntötehtävästä. Joissakin hallintakäytäntö tyypeissä arkaluonteiset asetusarvot on kuitenkin tunnistettava ja poistettava manuaalisesti, jotta ne eivät sisälly hallintakäytäntötehtävään. Microsoft 365 Lighthousen järjestelmänvalvojien on tarkasteltava kopioituja hallintakäytäntötehtäviä ja poistettava kaikki asiakasympäristökohtaiset asetusarvot, joita ei tulisi soveltaa muihin hallittuihin asiakasympäristöihin.
Jokaisen lisätyn hallintakäytännön konfiguraatioasetukset tulee siis käydä lävitse, ja tarkastaa ettei asetuksissa ole arvoja, joita ei haluta käyttöönottaa muissa hallituissa asiakasympäristöissä. Hallintakäytännöt voivat esimerkiksi käyttää asiakasympäristössä sijaitsevia käyttöoikeusryhmiä käytännön kohdistamista tai epäkohdistamista varten. Hallintakäytäntötehtävät tulee luoda ilman kohdistuksia käyttäjäoikeusryhmiin, mikäli ne eivät ole Microsoftin universaaleja ryhmiä, jotka sijaitsevat kaikissa Microsoft 365 -ympäristöissä oletuksena (esim. “All Users”). (Microsoft, 2023-a)

Hallintakäytäntöjen asiakasympäristökohtaiset konfiguraatiot, sekä kohdistumiset ja epäkohdistumiset määritetään, kun hallintakäytäntötehtävät käyttöönotetaan tiettyyn Microsoft 365 -ympäristöön.

Hallintakäytäntötehtävien luonti tapahtuu Baselines-sivulta:

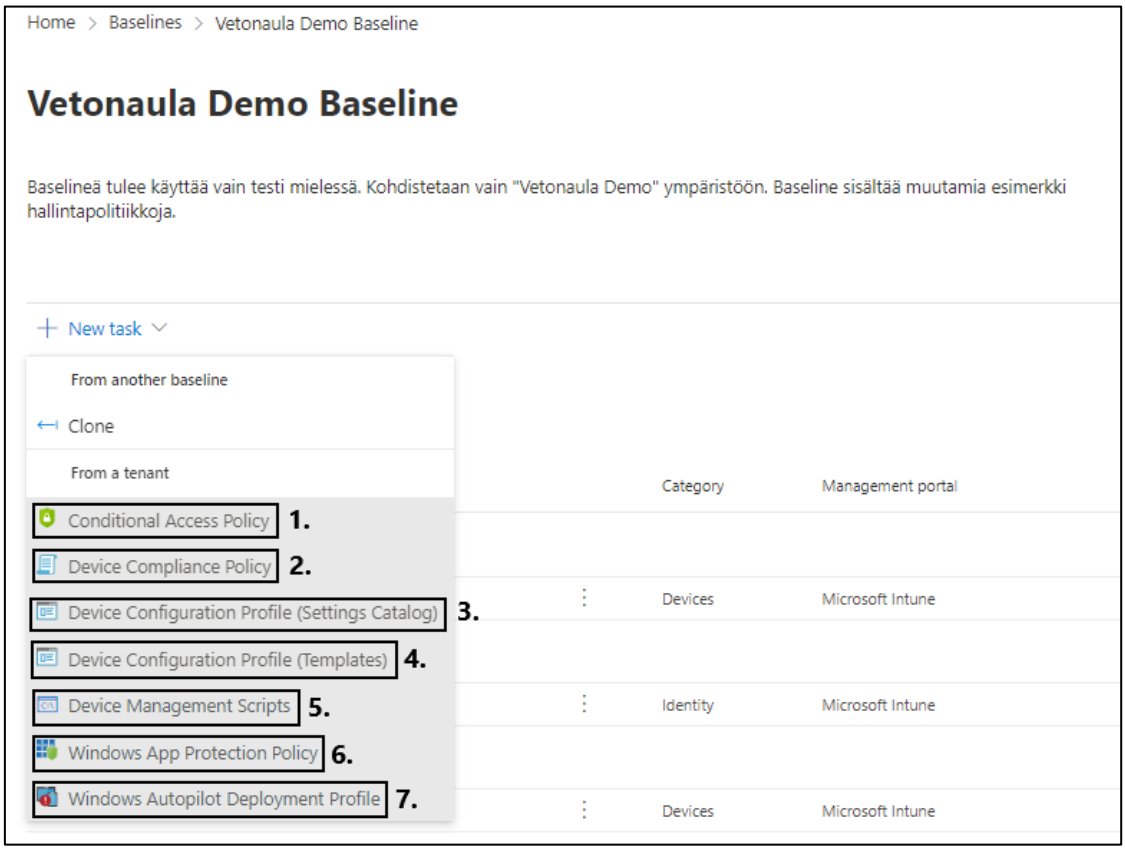
1. Valitaan hallintakäytäntölinjaus, esimerkiksi "Vetonaula Demo Baseline".

2. Valitaan "New task" uuden tehtävän lisäämistä varten.

Microsoft 365 Lighthouse -portaali mahdollistaa seitsemän erityyppisen hallintakäytännön tuomisen linjaukseen (kts. Kuva 8.). Kopioidessa hallintakäytäntöä valitaan minkä tyyppinen hallintakäytäntö halutaan kopioida.

3. Valitaan hallintakäytäntötyyppi, esimerkiksi ”Conditional Access Policy”

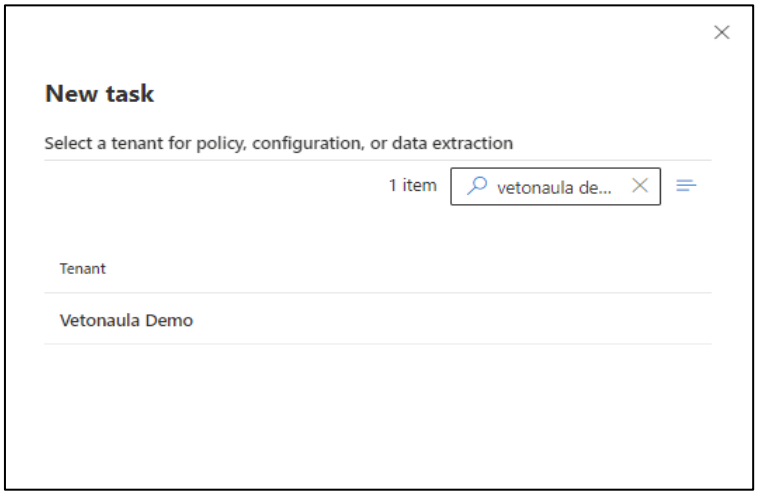
Kuva 8. Uusi hallintakäytäntötehtävä



4. Valitaan mistä asiakasympäristöstä hallintakäytäntö halutaan kopioida, ympäristöä voidaan etsiä asiakkuuden nimellä, esimerkissä hallintakäytäntö kopioidaan Vetonaula Demo ympäristöstä (Kuva 9.).

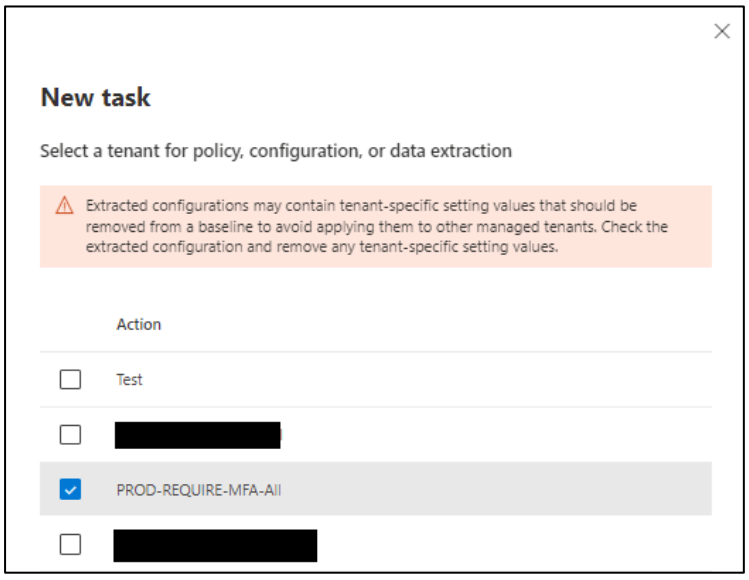
Kuva 9. Uusi hallintakäytäntötehtävä (Hallintakäytännön kopioiminen vaatii

käyttäjältä ”Global Administrator” -GDAP-roolin kopioinnin kohteena olevaan Microsoft 365 -ympäristöön.)



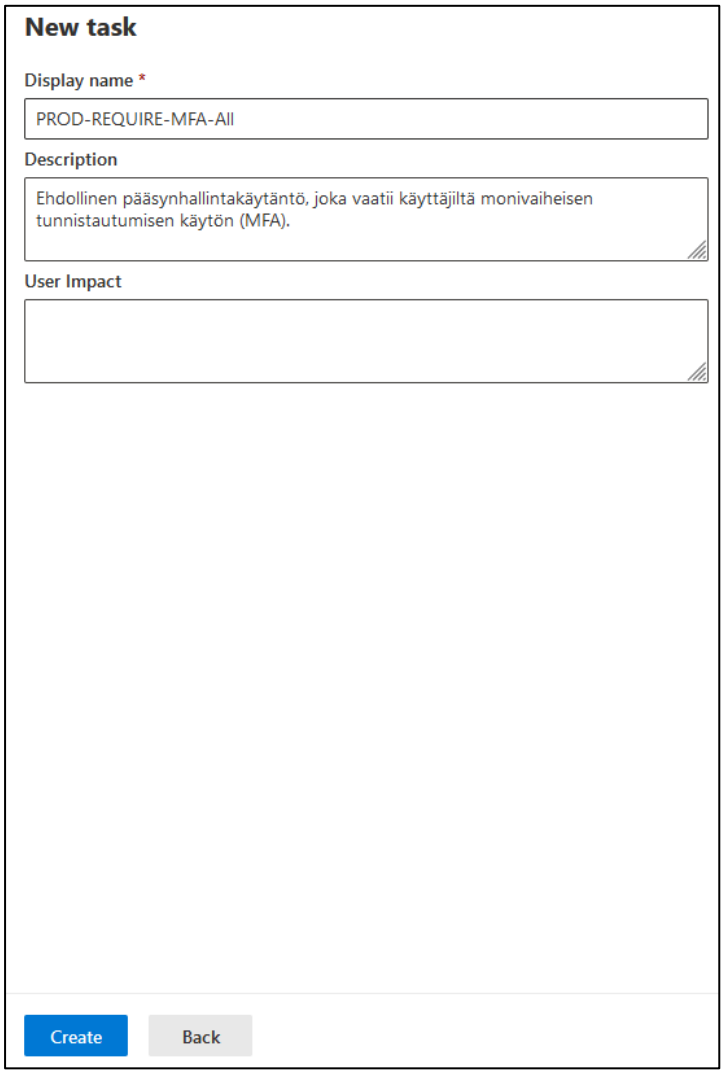
5. Valitaan haluttu kopioitava hallintakäytäntö, esimerkissä valitaan monivaiheiseen tunnistautumiseen (MFA) liittyvä ehdollisen pääsynhallinnankäytäntö. Palvelu ohjeistaa käymään hallintakäytännön konfiguraatioasetukset läpi siten, ettei hallintakäytäntötehtävään jää mitään asiakasympäristö kohtaisia arvoja (Kuva 10.). Konfiguraatioasetukset saadaan auki vasta tehtävän valmistumisen jälkeen.

Kuva 10. Uusi hallintakäytäntötehtävä



6. Viimeisessä vaiheessa määritetään hallintakäytäntötehtävän nimi, kuvaus sekä esimerkissä tyhjäksi jätetty ”käyttäjä vaikutus” kenttä (Kuva 11.). Esimerkissä on käytetty kopioidun hallintakäytännön nimeä.

Kuva 11. Uusi hallintakäytäntötehtävä

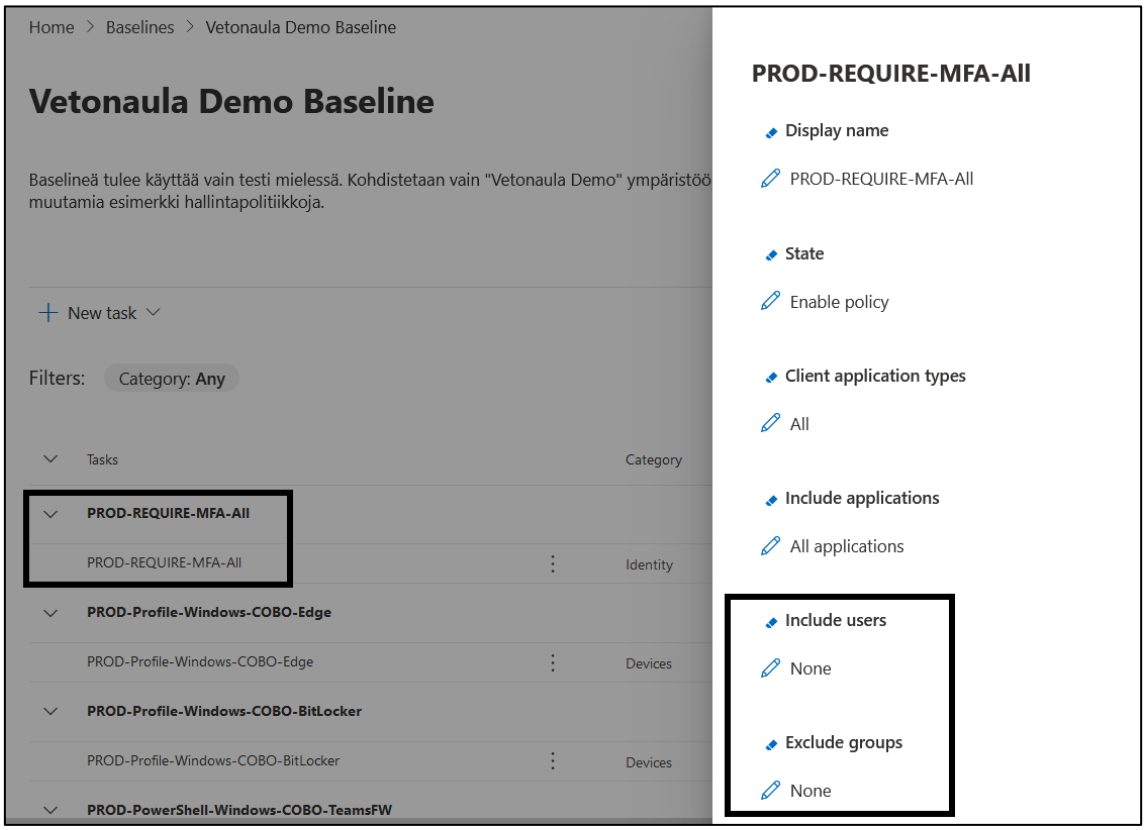


Kun hallintakäytäntötehtävä on luotu, on seuraavaksi syytä käydä läpi sen konfiguraatioasetukset, siten ettei tehtävään ole kopioinnista jäänyt mitään asiakasympäristökohtaisia arvoja tai kohdistusryhmiä. Tässä vaiheessa tulee huomioida, minkä tyyppinen hallintakäytäntötehtävä on kyseessä, ja minkä kaltaisia konfiguraatioasetuksia se sisältää. Konfiguraatioasetukset ja niiden arvot tulee asettaa niin, että hallintakäytäntötehtävän voi käyttöönottaa sen kohdeasiakasympäristöille.

Hallintakäytäntötehtävän asetukset saa näkyviin valitsemalla halutun tehtävän listauksesta, esimerkissä valitaan edellisessä vaiheessa ehdollisen pääsynhallintakäytännön pohjalta luotu tehtävä ”PROD-REQUIRE-MFA-All” (Kuva 12.).

Kun oikea tehtävä on valittu, käydään läpi tehtävän konfiguraatioasetukset. Tehtävästä on tarkoituksena poistaa kaikki asiakasympäristöön viittaavat arvot sekä kohdistukset, jotka kopioinnin pohjalta ovat jääneet asetuksiin. Varmistetaan myös, että muutenkin asetukset ja arvot ovat asianmukaisesti (Kuva 12.).

Kuva 12. Hallintakäytäntötehtävän konfiguraatioasetukset



Tässä esimerkissä asetuksen ”Include users”-asetuksen ”All users”-arvo jätettiin paikoilleen, koska kohdistettuna oleva ryhmä on Microsoftin universaali käyttöoikeusryhmä.

”Exclude groups”-epäkohdistusasetuksesta poistettiin siinä olleet käyttöoikeusryhmät, koska ne viittasivat kopioidun hallintakäytännön asiakasympäristöön. Tämän asetuksen kohdistusryhmät määritetään asiakasympäristökohtaisesti hallintakäytäntötehtävän käyttöönoton yhteydessä. Tässä esimerkissä ei ollut muita korjattavia konfiguraatioasetusten arvoja.

Samankaltaisesti Vetonaula Demo Baseline -hallintakäytäntölinjaukseen lisättiin kuusi erityyppistä hallintakäytäntötehtävää (kuva 13.):

1. Conditional Access Policy **“PROD-REQUIRE-MFA-All”**
   Ehdolliseen pääsynhallintakäytäntöön perustuva hallintakäytäntötehtävä, joka vaatii käyttäjiltä monivaiheisen tunnistautumisen (MFA) käyttämisen.

2. Device Compliance Policy **“PROD-Compliance-Windows-All Baseline”**
   Yhdenmukaisuuskäytäntöön perustuva hallintakäytäntötehtävä Windows-laitteille, joka varmistaa laitteiden noudattavan tiettyjä vaatimuksia. Käytäntö vaatii laitteilta esimerkiksi BitLocker-salaustekniikan käytön sekä asettaa minimivaatimuksen Windows-käyttöjärjestelmän versiolle.

3. Device Configuration Profile (Settings Catalog) ”**PROD-Profile-Windows-COBO-Edge”**:
   Laitekonfiguraatioprofiilin perustuva hallintakäytäntötehtävä, joka sisältää muokattavia asetuksia. Tässä tapauksessa konfiguraatioprofiili määrittää Windows-laitteiden Microsoft Edge-selaimen kirjanmerkkiasetuksia.

4. Device Configuration Profile (Templates) **“PROD-Profile-Windows-COBO-BitLocker”**:
   Laitekonfiguraatioprofiiliin perustuva hallintakäytäntötehtävä, joka perustuu valmiisiin asetusmalleihin. Tässä tapauksessa konfiguraatioprofiililla hallitaan Windows-laitteiden Bitlocker-levynsalauksen asetuksia.

5. Device Management Script **“PROD-PowerShell-Windows-COBO-TeamsFW”**:
   Laitehallintaskriptiin (PowerShell) perustuva hallintakäytäntötehtävä, joka asettaa tiettyjä palomuurisääntöjä Microsoft Teams -työpöytäohjelmaa varten.

6. Windows Autopilot Deployment Profile**” PROD_Autopilot_User_AADJ”**:
   Käyttöönoton hallintaprofiiliin perustuva hallintakäytäntötehtävä, joka hallitsee Windows-laitteiden Autopilot-provisiointiprofiilin asetuksia.

Työssä käytettävä testi-hallintakäytäntölinjaus on nyt valmis. Hallintakäytäntölinjauksen tehtäviä voidaan muokata ja tarkastella valitsemalla haluttu hallintakäytäntölinjaus Baselines-sivulta (Kuva 13.).

Baselines-sivu kertoo myös hallintakäytäntötehtäviin asiakasympäristöiltä vaaditut tilaukset. Tässä tapauksessa vaaditut tilaukset ovat Microsoft Intune ja Microsoft Entra ID P1 (Kuva 13.)

Kuva 13. Vetonaula Demo Baseline

Tasks	Category	Management portal	Required services
PROD-REQUIRE-MFA-All			
PROD-REQUIRE-MFA-All	Identity	Microsoft Intune	Microsoft Entra ID P1
PROD-Profile-Windows-COBO-Edge			
PROD-Profile-Windows-COBO-Edge	Devices	Microsoft Intune	Intune
PROD-Profile-Windows-COBO-BitLocker			
PROD-Profile-Windows-COBO-BitLocker	Devices	Microsoft Intune	Intune
PROD-PowerShell-Windows-COBO-TeamsFW			
PROD-PowerShell-Windows-COBO-TeamsFW	Devices	Microsoft Intune	Intune
PROD_Autopilot_User_AADJ			
PROD_Autopilot_User_AADJ	Devices	Microsoft Intune	Intune
PROD-Compliance-Windows-All-Baseline			
PROD-Compliance-Windows-All-Baseline	Devices	Microsoft Intune	Intune

3.2 Hallintakäytäntölinjauksen kohdistaminen asiakasympäristöön

Tässä osiossa kuvataan, kuinka luotu hallintakäytäntölinjaus kohdistetaan tiettyyn asiakasympäristöön, tässä tapauksessa Vetonaula Demo -ympäristöön. Hallintakäytäntölinjauksen kohdistaminen ei vielä käyttöönota linjauksen sisältämiä hallintakäytäntötehtäviä, vaan se tehdään työn seuraavassa vaiheessa ja on kuvattu alaluvussa 3.3.

3.2.1 Vaatimukset ja vaikutukset

Hallintakäytäntölinjauksen kohdistaminen vaatii käyttäjältä Global Administrator -GDAP -roolin IT-kumppanin Microsoft 365 -ympäristössä.

Kun hallintakäytäntölinjaus kohdistetaan asiakasympäristöön, se korvaa ympäristölle aiemmin määritetyn hallintakäytäntölinjauksen. Tässä tapauksessa Microsoftin luoma oletushallintakäytäntölinjaus "Default Baseline" korvautuu uudella linjauksella, mikä tarkoittaa, että kaikki entisen linjauksen hallintakäytäntötehtävät, tehtävien konfiguraatiot ja asetetut ympäristökohtaiset arvot pyyhkiytyvät.

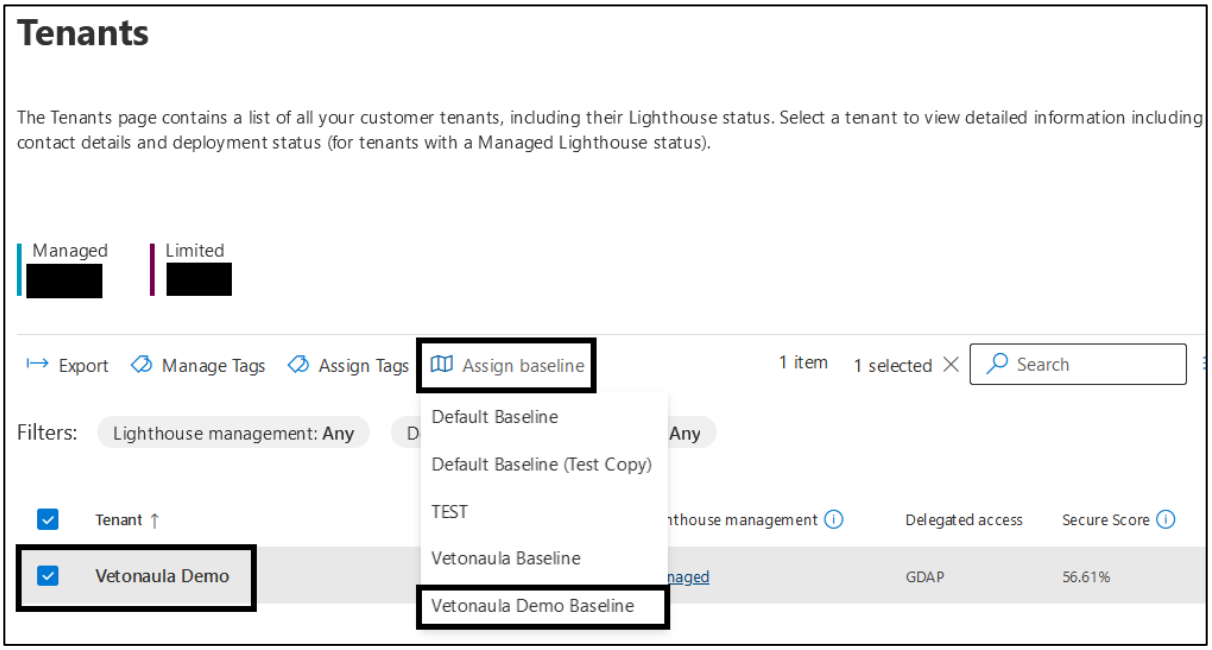
Mikäli entisen linjauksen hallintakäytäntötehtävät ovat jo käyttöönotettu asiakasympäristöön, eivät käyttöönotetut hallintakäytännöt pyyhkiydy vielä tässä vaiheessa asiakasympäristöstä, vaan ne tulee tarvittaessa poistaa ennen uusien hallintakäytäntötehtävien käyttöönottoa.

3.2.2 Hallintakäytäntölinjauksen kohdistaminen

Hallintakäytäntölinjaus kohdistetaan seuraavalla tavalla:

1. Avataan Microsoft 365 Lighthouse -portaali ja valitaan päävalikosta Tenants-sivu
2. Valitaan luettelosta asiakasympäristö, johon halutaan kohdistaa hallintakäytäntölinjaus, tässä tapauksessa "Vetonaula Demo".
3. Valitaan kohteena olevan asiakasympäristön kohdalla "Assign Baseline".
4. Valitaan avautuvasta luettelosta haluttu hallintakäytäntölinjaus, tässä tapauksessa "Vetonaula Demo Baseline".
5. Vahvistetaan valinta ja varmistetaan, että hallintakäytäntölinjaus on kohdistettu haluttuun asiakasympäristöön.

Kuva 14. Hallintakäytäntölinjauksen kohdistaminen



Kun hallintakäytäntölinjaus on kohdistettu asiakasympäristöön, tulee seuraavaksi määritellä hallintakäytäntötehtävien ympäristökohtaiset konfiguraatiotasetuksien arvot. Seuraavassa alaluvussa ohjeistetaan, miten hallintakäytäntötehtävät käyttöönotetaan asiakasympäristöön, sekä mitä kyseisessä vaiheessa tulee huomioida.

3.3 Hallintakäytäntötehtävien käyttöönotto asiakasympäristöön

Tässä alaluvussa käydään läpi hallintakäytäntötehtävien käyttöönotto. Vasta tässä vaiheessa tapahtuu muutoksia kohteena olevaan asiakasympäristöön.

3.3.1 Käyttöoikeusvaatimukset

Hallintakäytäntötehtävien käyttöönoton vaatimuksina on Global Administrator GDAP -rooli IT-kumppanin Microsoft 365 -ympäristössä (tässä tapauksessa Vetonaula Oy:n Microsoft-ympäristö), sekä tarvittavat Microsoft Intune -palvelun GDAP-käyttöoikeusroolit asiakasympäristössä. Mikäli käyttöönotettava hallintakäytäntö on Entra ID -ehdollisen pääsynhallintakäytäntö, niin tarvitaan myös vaadittu GDAP-rooli Entra ID -palveluun.

3.3.2 Hallintakäytäntötehtävien käyttöönotto asiakasympäristöön

Tässä osiossa hallintakäytäntötehtävät käyttöönotetaan asiakasympäristöön. Tämä pitää tehdä yksi tehtävä ja yhteen asiakasympäristöön kerrallaan. Hallintakäytäntötehtävät ovat olemassa vain Microsoft 365 Lighthouse -palvelussa, ja kun tehtävä käyttöönotetaan asiakasympäristöön, se luo kohdeympäristöön tehtävää vastaavan hallintakäytännön. Vasta tässä vaiheessa hallintakäytäntöön lisätään kohteena olevan asiakasympäristön halutut asetukset, arvot ja kohdennukset.

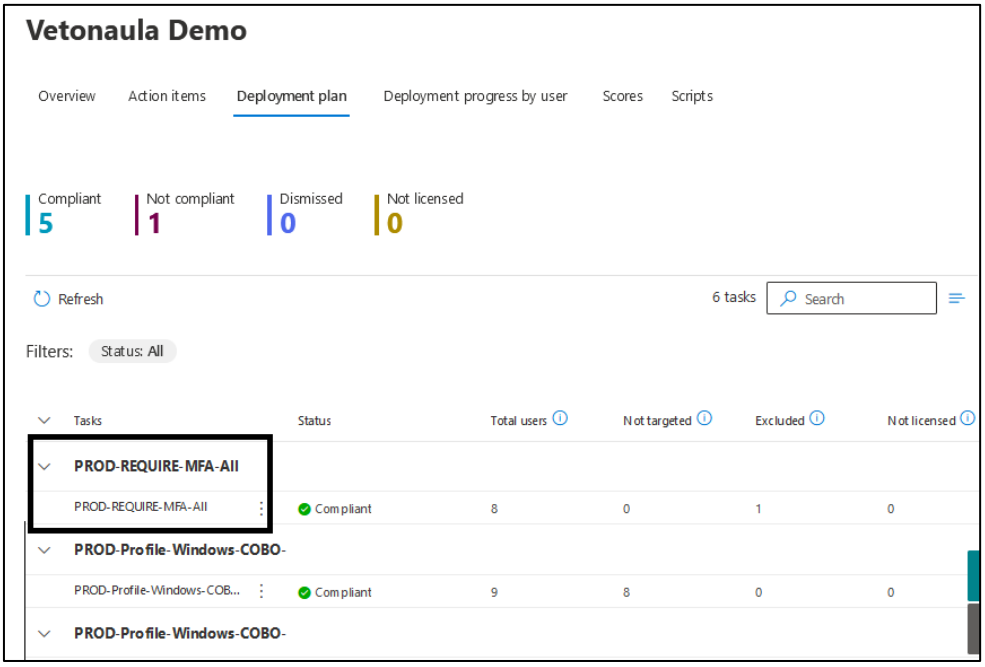
Jotta luotavilla hallintakäytännöillä saavutetaan haluttu vaikutus asiakasympäristössä, tulee hallintakäytännöt sekä niiden erinäiset konfiguraatioasetukset olla hyvin suunniteltu etukäteen. Tässä työssä esimerkkinä käytetyt hallintakäytännöt, ovat luotu Vetonaula Oy:n käytössä olevien hallintakäytäntöjen pohjalta. Hallintakäytännöt sekä niiden sisältämät asetukset ovat siis tuotantokelpoisia.

Seuraavaksi aloitetaan hallintakäytäntötehtävän käyttöönotto Vetonaula Demo -ympäristöön:

1. Valitaan Tenants-sivulta kohteena oleva asiakasympäristö, tässä tapauksessa Vetonaula Demo -ympäristö, jolloin avautuu Tenant Details -sivu.

2. Tenant Details -sivulta valitaan Deployment Plan -välisivu, jossa näkyvät hallintakäytäntölinjaukseen kohdistetut tehtävät sekä tehtävien tila (kts Kuva 15.).

Kuva 15. Deployment plan

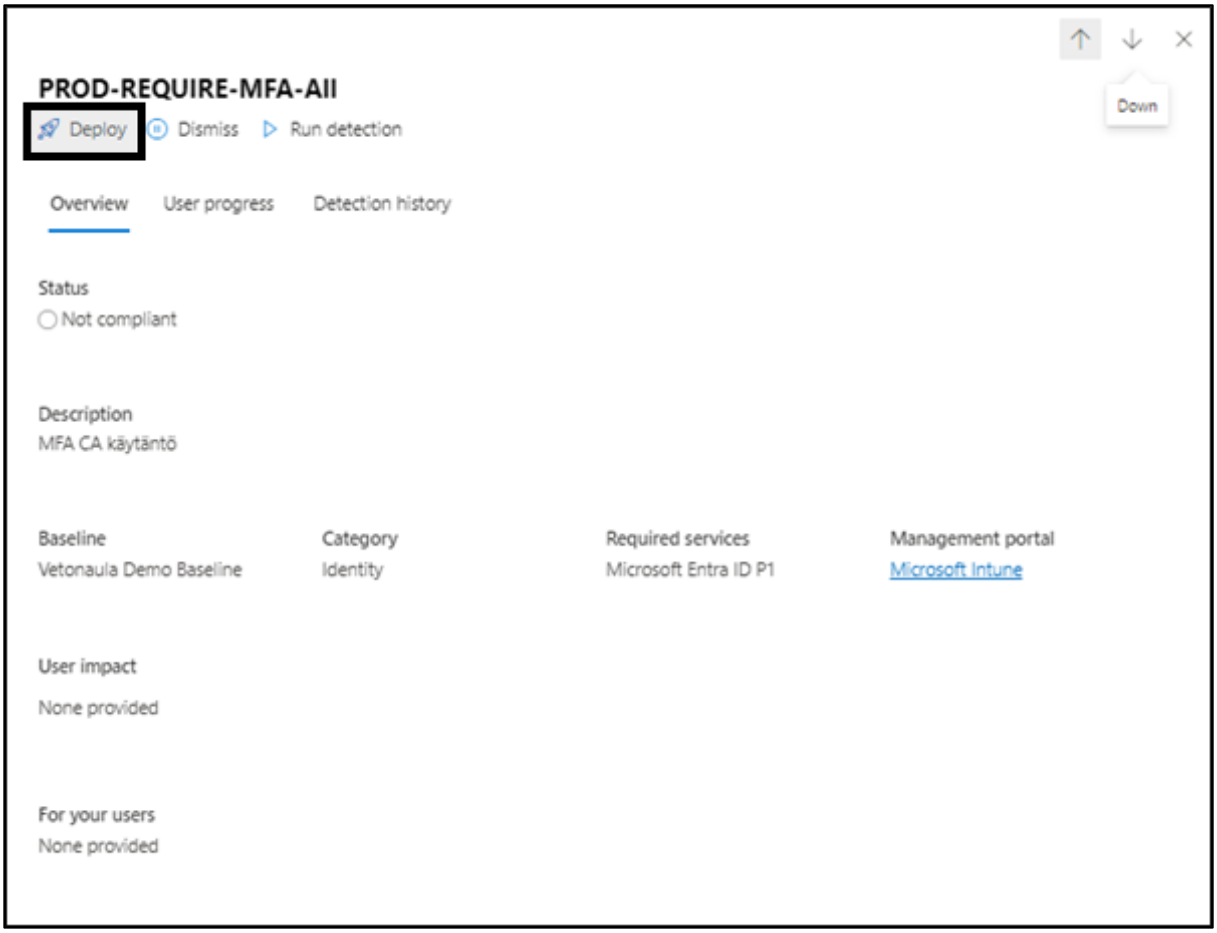


Hallintakäytäntötehtävän valinta:

3. Valitaan käyttöönotettava hallintakäytäntötehtävä ja painetaan "Deploy" tehtävän käyttöönottoa varten.

Tässä esimerkissä valitaan ehdollisen pääsynhallintakäytäntö, jonka loimme aikaisemmin. (kts. Kuva 16.).

Kuva 16. Hallintakäytäntötehtävän käyttöönoton aloitus

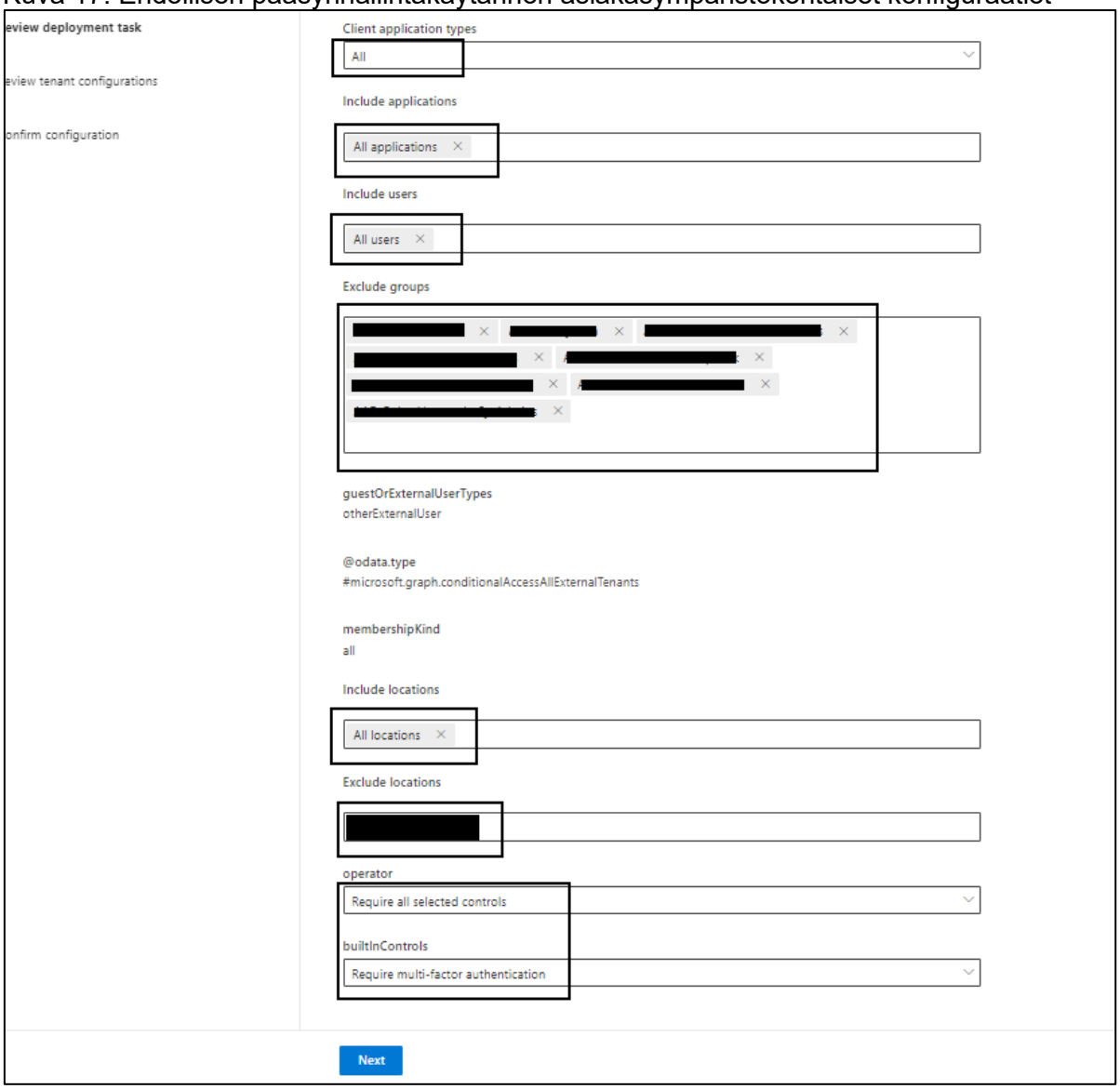


Hallintakäytäntötehtävän käyttöönoton aloituksen jälkeen avautuu tehtävän käyttöönoton ensimmäinen Review Deployment Task -vaihe, jossa muokataan hallintakäytäntötehtävän asiakasympäristökohtaiset konfiguraatioasetusten arvot:

4. Tämän tehtävän sisältämän ehdollisen pääsynhallintakäytännön kohdalla, esimerkiksi valitaan kohdistusryhmät, käytäntöön sisällytetyt sovellukset sekä käytäntöön sisällytetyt sijainnit. Tässä esimerkissä käytännöstä epäkohdistetaan Vetonaula Oy:n käyttämiä oikeusryhmiä, sekä valikoituja IP-osoiteavaruuksia.

Tässä vaiheessa Microsoft 365 Lighthouse hakee ainoastaan kyseisen asiakasympäristön käyttöoikeusryhmät, joten ne voidaan määrittää oikeiksi. Työssä tehdyt määritykset nähdään kuvassa 17.

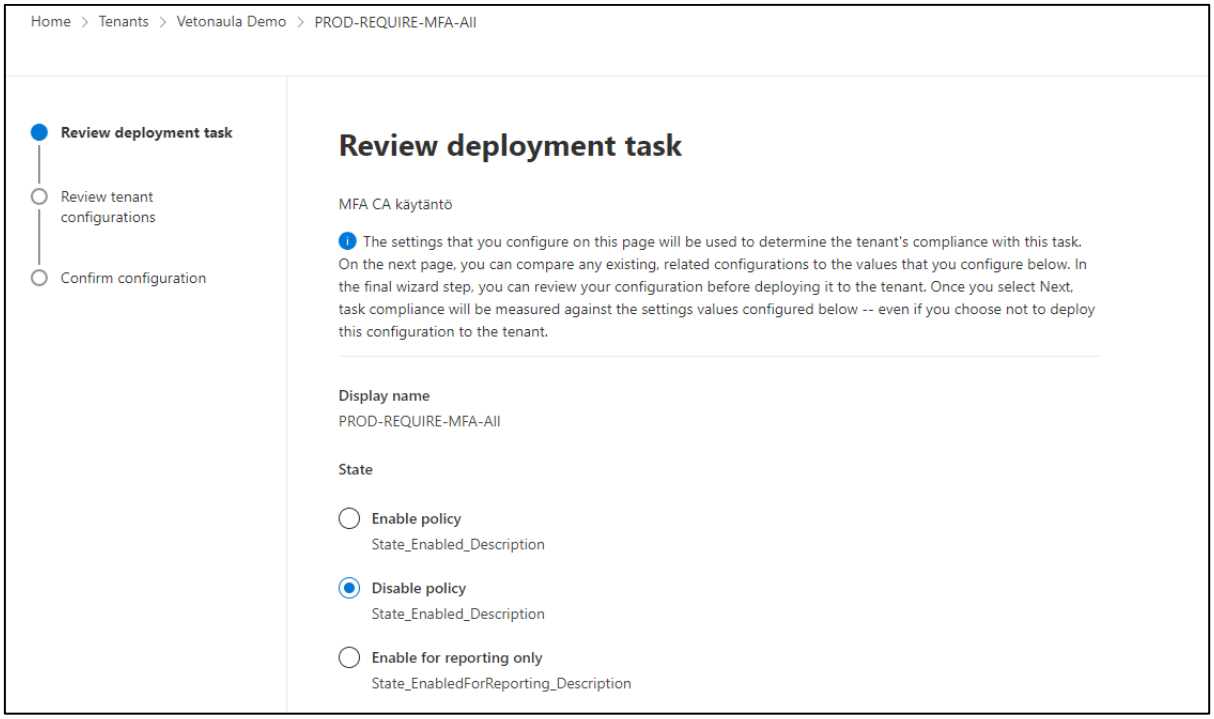
Kuva 17. Ehdollisen pääsynhallintakäytännön asiakasympäristökohtaiset konfiguraatiot



Review deployment task -vaiheessa valitaan, otetaanko hallintakäytäntö käyttöön Enabled, Disabled vai Report Only -tilassa. Tämä valinta on riippuvainen hallintakäytännön tyypistä, sillä kaikissa hallintakäytännöissä ei ole samankaltaista valinta mahdollisuutta.

5. Tässä esimerkissä yhdenmukaisuuskäytäntö käyttöönotetaan Disabled -tilassa.

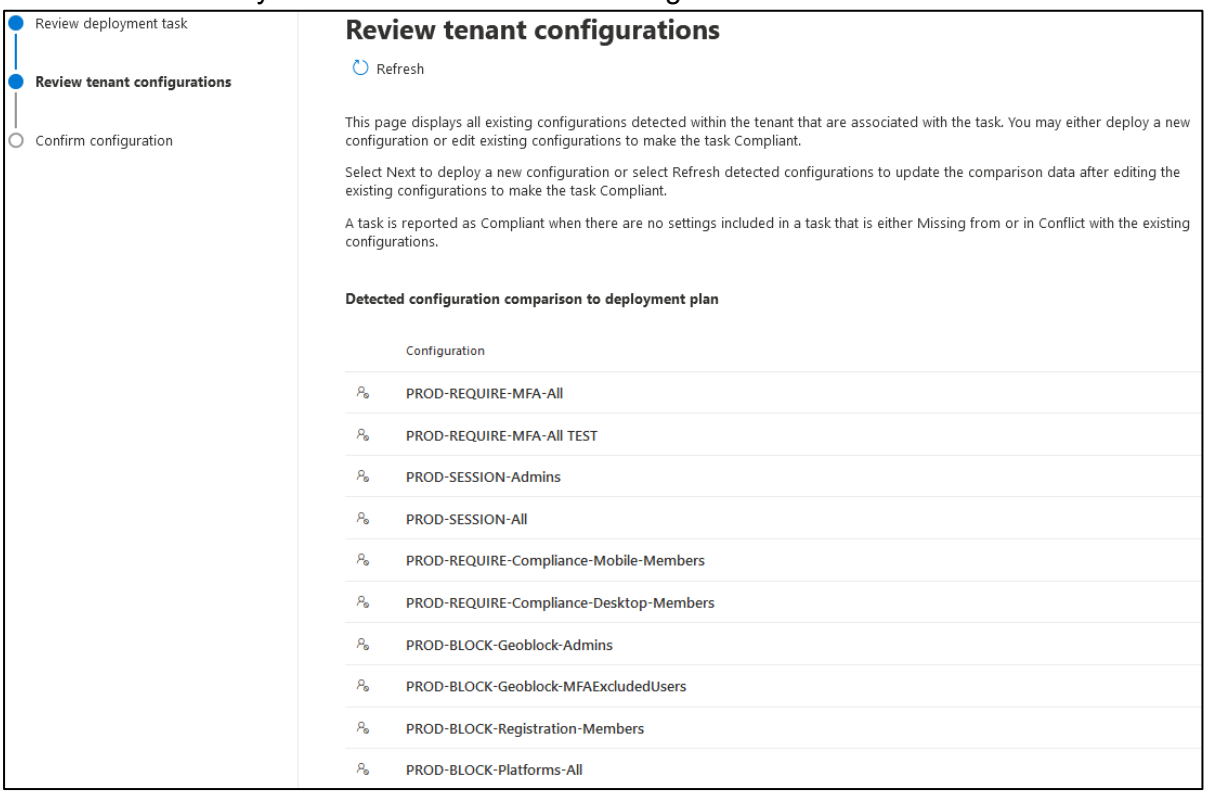
Kuva 18. Hallintakäytäntötehtävän käyttöönotto -tila



Käyttöönottoprosessin seuraavassa Review tenant configurations -vaiheessa tarkastetaan mahdolliset päällekkäiset tai ristiriitaiset konfiguraatiot.

Kuvassa 19 näytetty Review tenant configurations -vaihe tarjoaa yleiskuvan kaikista asiakasympäristön hallintakäytännöistä ja niiden konfiguraatioasetuksista, jotka saattavat olla ristiriidassa käyttöönotettavan tehtävän kanssa. Tämän vaiheen tarkoituksena on välttää päällekkäisyyksiä ja ristiriitaisia konfiguraatioasetusten arvoja samassa asiakasympäristössä.

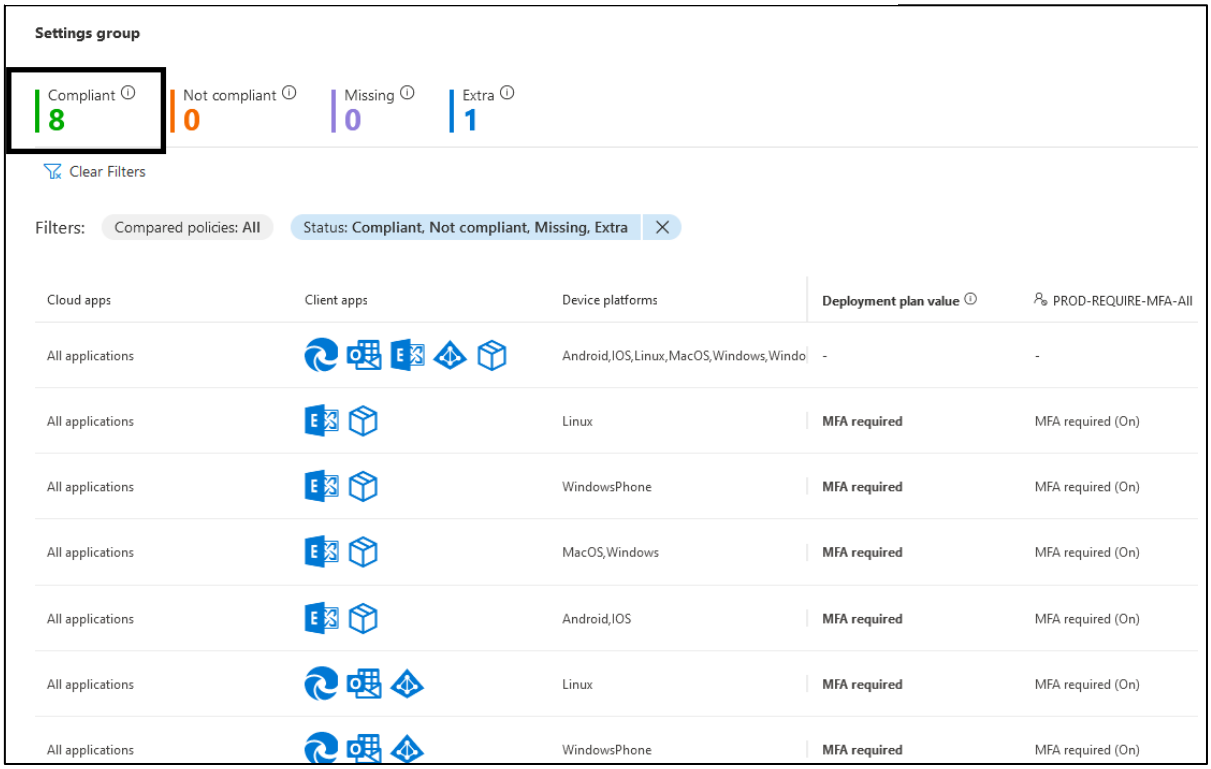
Kuva 19. Hallintakäytäntötehtävän ristiriitaiset konfiguraatiot



Mikäli käyttöönotettavan hallintakäytännön konfiguraatioasetusten arvoissa havaitaan ristiriitoja tai päällekkäisyyksiä samassa ympäristössä jo olevien hallintakäytäntöjen arvojen kanssa, ne ovat listattuna Review tenant configurations -vaiheessa, jossa arvoja voidaan verrata. Tässä vaiheessa voidaan esimerkiksi havaita, että samankaltaiset hallintakäytäntöasetukset ovat jo käyttöönotettuina kohteena olevaan asiakasympäristöön.

Kuvassa 20 nähdään, että tässä tapauksessa esimerkiksi kahdeksan hallintakäytännön asetusta ovat jo yhteensopivia (compliant).

Kuva 20. Hallintakäytäntötehtävän ristiriitaiset & päällekkäiset arvot



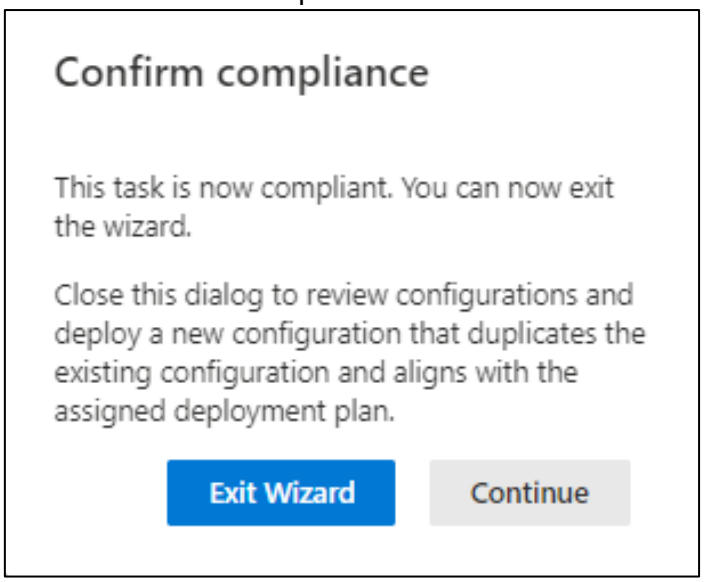
Mikäli asiakasympäristöstä löytyy ristiriitaisia tai päällekkäisiä konfiguraatioasetuksien arvoja, voidaan edetä kahdella eri tavalla:

1. Review tenant configurations -vaihe voidaan ohittaa, jolloin hallintakäytäntö määritettyineen asetuksineen käyttöönotetaan asiakasympäristöön. Ristiriitaiset tai päällekkäiset arvot saattavat kuitenkin aiheuttaa ongelmia ja ne pitää huolellisesti tarkastaa.

2. Mikäli jo asiakasympäristössä olemassa olevien hallintakäytäntöjen avulla voidaan toteuttaa käyttöönotettavan hallintakäytäntötehtävän haluttu tarkoitus, voidaan se todeta tässä, ja siirtyä asiakasympäristön Microsoft Intune -palvelun hallintaan muuttamaan samankaltaisten hallintakäytäntöjen asetuksia niin, että tehtävän haluttu tarkoitus toteutuu.
   Tämän jälkeen palataan Microsoft 365 Lighthouse -portaalin tehtävän käyttöönottonäkymään ja päivitetään näkymä, jolloin palvelu merkitsee tämän tehtävän tilan yhteensopivaksi, mikäli tehtävässä määritetyt hallintakäytännön konfiguraatioasetukset, ja niiden arvot ovat yhteensopivia (Kuva 21.).

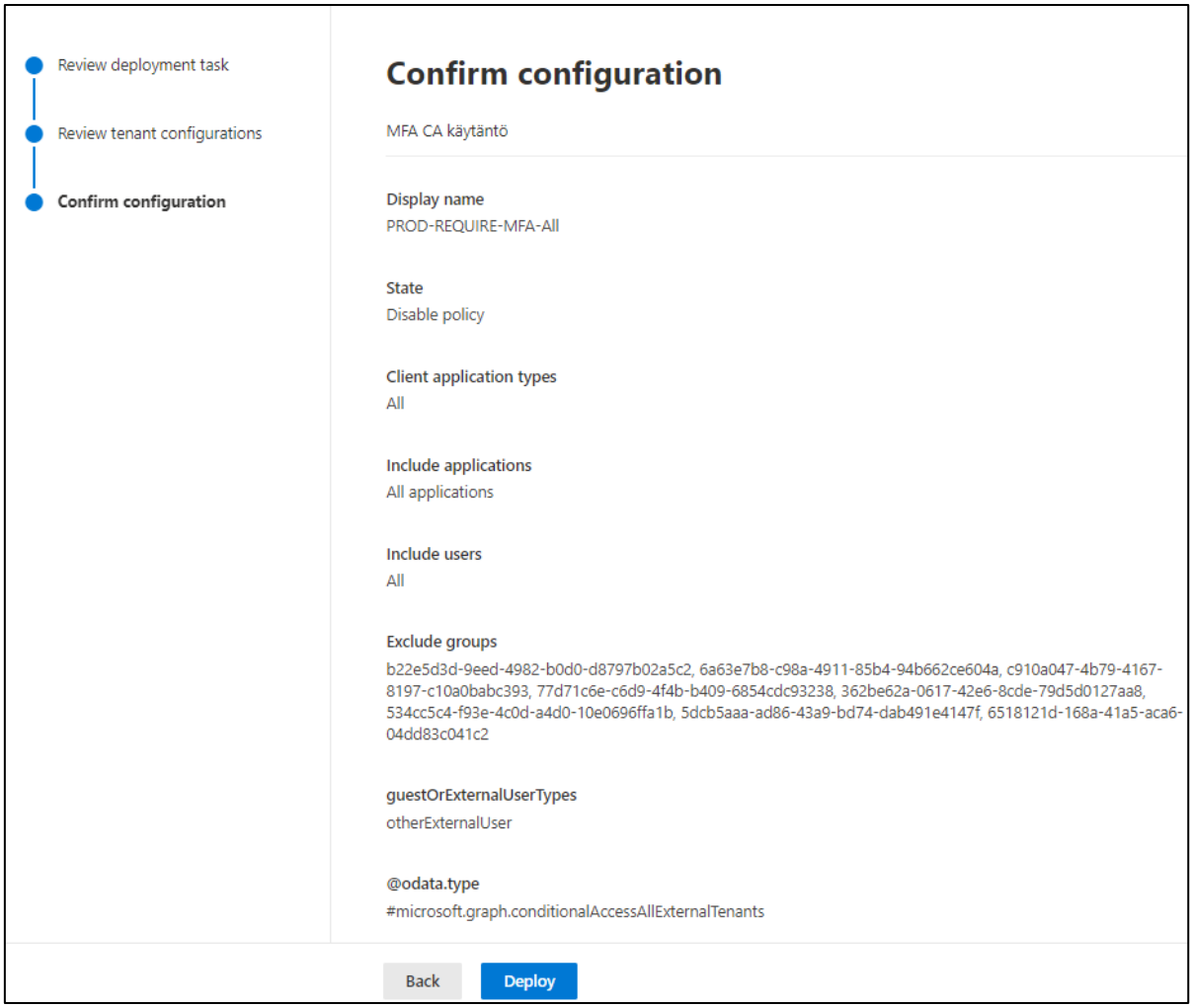
Menetelmässä 2. ei asiakasympäristöön käyttöönoteta uutta hallintakäytäntöä, mutta Microsoft 365 Lighthouse -portaalin puolella hallintakäytäntötehtävän tila muuttuu yhteensopivaksi.

Kuva 21. Confirm compliance



Mikäli hallintakäytäntötehtävän käyttöönotossa ei havaita ristiriitaisia tai päällekkäisiä konfiguraatioasetus arvoja, siirtyy prosessi suoraan viimeiseen “Confirm configuration” -vaiheeseen. Viimeisessä prosessin vaiheessa tehtävän asetukset sekä kohdistukset voidaan vielä kerran tarkistaa, ja tämän jälkeen suorittaa hallintakäytäntötehtävän käyttöönotto.

Kuva 22. Hallintakäytäntö tehtävän käyttöönoton viimeistely



Seuraavassa alaluvussa esitetään, kuinka hallintakäytäntötehtävien käyttöönoton jälkeen voidaan seurata tehtävien sisältämien hallintakäytäntöjen tilaa asiakasympäristössä ja nähdään kuinka kohteena oleva asiakasympäristö on ottanut hallintakäytännöt vastaan.

3.4 Hallintakäytäntötehtävien tilan seuranta asiakasympäristössä

Hallintakäytäntötehtävän tilaa voidaan seurata Deployment plan -sivulta sen käyttöönoton jälkeen. (Kuva 23).

Tehtävän tila voi olla yksi seuraavista (Microsoft, 2023-d):

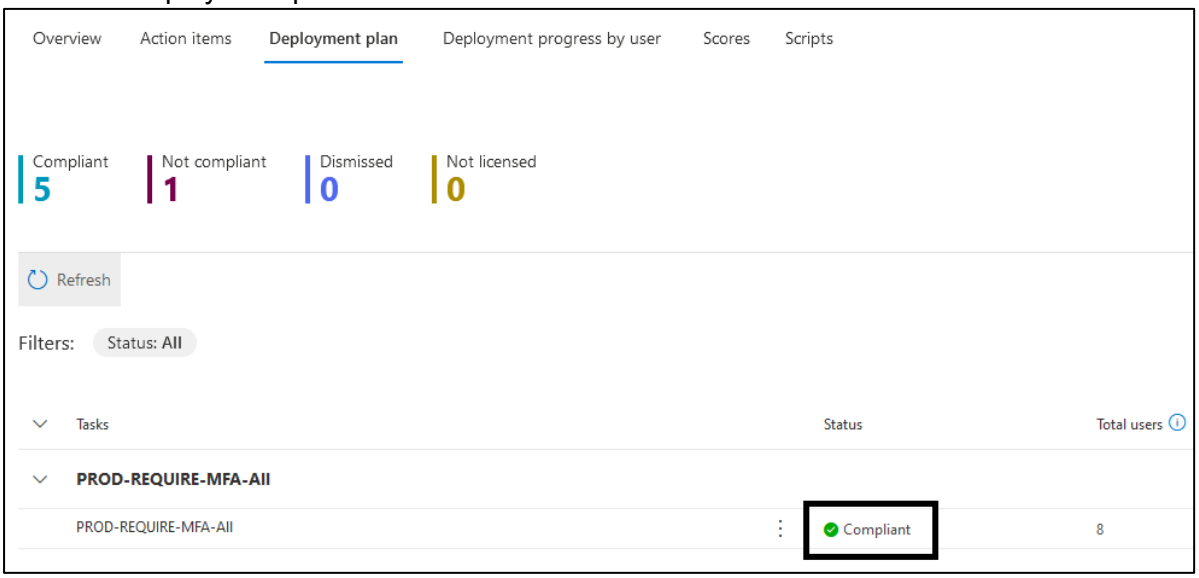
- Yhteensopiva (Compliant): Kaikki tehtävän asetukset ovat yhteensopivia. Mikään asetus ei ole ristiriidassa, tai puutu kaikista ympäristössä olemassa olevista hallintakäytännöistä. Riittää, että tehtävän konfiguraatioasetukset ovat jossain olemassa olevassa hallintakäytännössä yhteensopivia. Kaikki käyttäjät ovat joko yhteensopivia tehtävän konfiguraatioasetuksien arvoihin verrattaessa, tai poissuljettu (excluded) tehtävästä.

- Yhteensopimaton (Not compliant): Yksi tai useampi tehtävän konfigraatioasetus ei ole yhteensopiva asiakasympäristön hallintakäytäntöjen asetuksiin verrattaessa. Yksi tai useampi asetus puuttuu kaikista olemassa olevista hallintakäytännöistä.

- Ei lisensoitu (Not licensed): Asiakasympäristö ei ole lisensoitu tehtävään liittyvien konfiguraatioiden käyttöönottoon. Esimerkiksi ehdolliseen pääsynhallintakäytäntöön perustuva tehtävä voisi olla “ei lisensoitu”, jos kohteena oleva asiakasympäristö ei omista Entra ID -palvelun tilausta.

- Hylätty (Dismissed): Tehtävä on hylätty. Microsoft 365 Lighthouse -portaali lopettaa konfiguraatioiden havaitsemisen ja raportoimisen tehtäville, jotka on hylätty.

Kuva 23. Deployment plan



Kun valitaan tietty tehtävä Deployment Plan -sivulta, voidaan tarkastella myös käyttäjien tilaa (Kuva 24. s40). Käyttäjien tilan seuranta auttaa IT-kumppania varmistamaan, että kaikki käyttäjät ovat oikealla tavalla kohdennettuja valittuna olevaan hallintakäytäntötehtävään ja heillä on tarvittavat lisenssit. Tila myös kertoo, jos käyttäjä ei ole yhteensopiva hallintakäytänötehtävän konfiguraatioasetuksiin verrattaessa.

Käyttäjän tila voi olla yksi seuraavista (Microsoft, 2023-d):

- Yhteensopiva (Compliant): Käyttäjä on kohdennettu tehtävään ja hänelle on myönnetty kaikki tehtävän edellyttämät lisenssit. Käyttäjä on yhteensopiva tai toisinsanottuna yhdenmukainen kaikkien tehtävän sisältämien konfiguraatioasetusten kanssa.

- Yhteensopimaton (Not compliant): Käyttäjä on kohdennettu tehtävään, mutta käyttäjä ei ole yhteensopiva yhden tai useamman tehtävään sisältyvän konfiguraatioasetuksen kanssa.

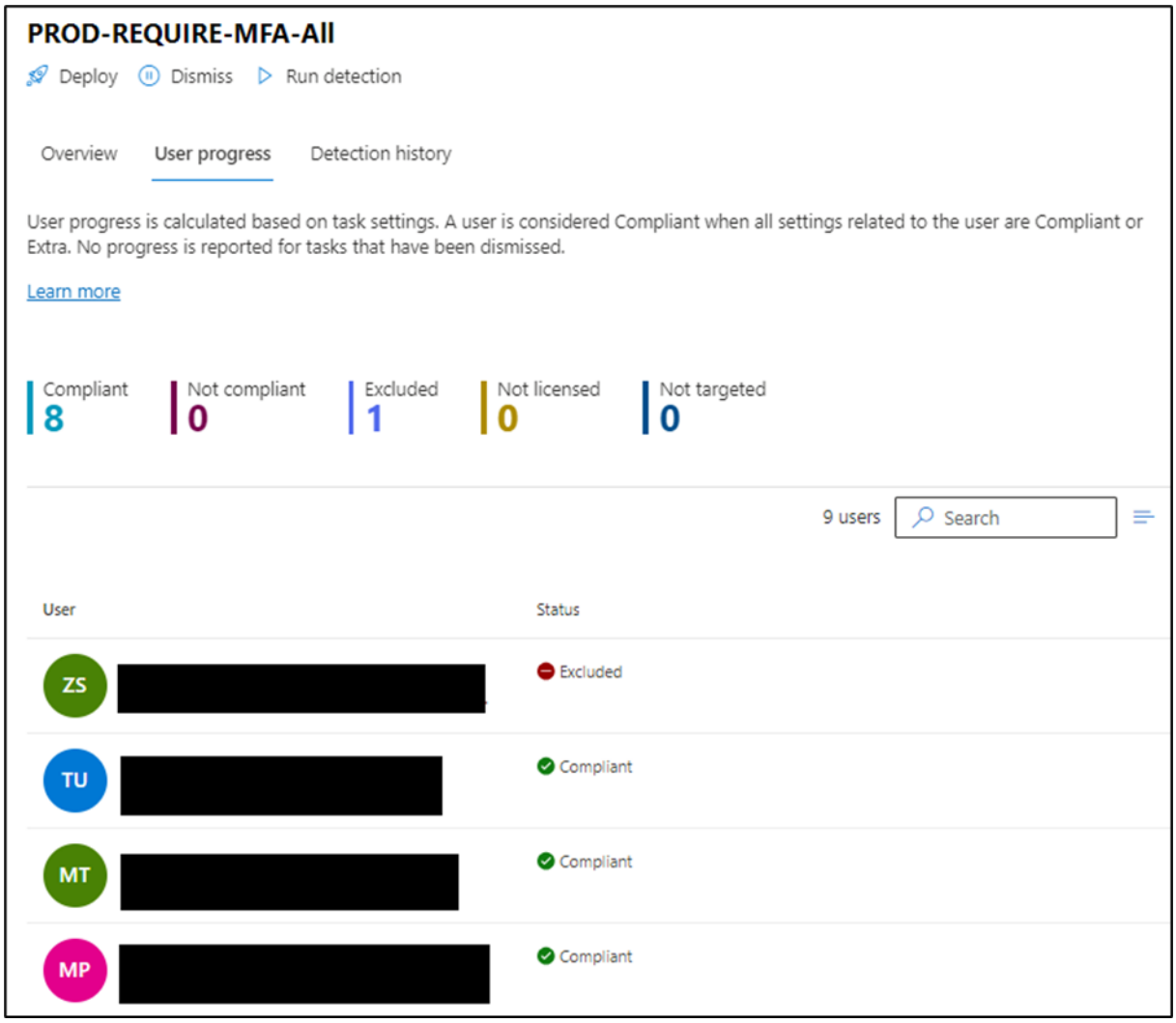
- Poissuljettu (Excluded): Käyttäjä on suljettu/epäkohdistettu pois tehtävästä. Kun käyttäjä on poissuljettu tehtävästä, tilan havaitseminen ja raportointi päivitetään vastaavasti, mutta poissuljettu käyttäjä ei vaikuta tehtävän yhdensopivuustilaan.

- Ei lisensoitu (Not licensed): Käyttäjällä ei ole lisenssiä tehtävään liittyvien palveluiden käyttöönottoon. Käyttäjä tulee poissulkea tehtävästä, jottei tehtävän tila muutu yhteensopimattomaksi.

- Ei kohdennettu (Not targeted): Käyttäjä ei ole tehtävän kohderyhmässä. Esimerkiksi, jos käyttäjä ei ole ylläpitäjä, hänen tilakseen raportoidaan “Not targeted” tehtävälle, joka on kohdennettu vain ylläpitäjille. Tämä ei vaikuta tehtävän yhteensopivuuteen.

Valitsemalla Deployment plan -sivulta tietyn hallintakäytäntötehtävän, aukeaa näkymä, josta voidaan käyttäjien tilan tarkastelun lisäksi hakea uusimmat tilatiedot painamalla “Run detection”, sekä katsella tilatietojen historiaa välilehdeltä “Detection history”.

Kuva 24. Tehtävien käyttäjien käyttöönottotila



4 Tulokset ja johtopäätökset

Tässä luvussa arvioidaan Microsoft 365 Lighthouse -palvelun toimivuutta ja soveltuvuutta Vetonaula Oy:n kaltaisille IT-palveluntarjoajille. Toiminnallisessa osuudessa kirjataan ylös selvinneitä ongelmia sekä arvioidaan Microsoft 365 Lightouse -palvelun dokumentaatiota.

4.1 Dokumentaatio

Microsoftin dokumentaatio Microsoft 365 Lighthouse -palvelusta ei ole kovin kattava, ja useissa tapauksissa se on myös virheellinen. Esimerkiksi monissa Microsoft 365 Lighthouse -ominaisuuksien vaatimuksissa viitataan "Lighthouse Admin" -käyttöoikeusrooliin, joka ei kuitenkaan vastaa mitään GDAP- tai RBAC-roolia. Dokumentaation artikkeleiden päiväykset ovat useimmiten vuodelta 2023, mikä saattaa viitata siihen, että palvelua tai sen dokumentaatiota ei päivitetä kovin aktiivisesti, vaikka se on vielä suhteellisen uusi.

Käyttäjältä vaaditaan oma-aloitteisuutta ja ongelmanratkaisukykyä tiettyjen toiminnallisuuksien käyttämiseen, koska toiminnallisuuksien vaatimuksia ei ole aina dokumentaatiossa listattu. Ongelmatilanteissa ei myöskään välttämättä saa kunnollista virheilmoitusta, tai virheilmoitusta ollenkaan. Työssä kohdattuja ongelmia kuvataan tarkemmin alaluvuissa 4.3 ja 4.4.

4.2 Microsoft 365 Lighthouse -käyttöoikeudet

Moni hallintakäytäntölinjauksien ja -tehtävien toiminnollisuuksista on Global Administrator -GDAP-roolin takana. Tämä rooli on vaadittu joko IT-kumppanin, tai hallittavien asiakkaiden Microsoft 365 -ympäristöön, riippuen suoritetusta työtehtävästä. Tätä Microsoft ei ole dokumentoinut, vaan dokumentaatiossa viitataan rooliin ”Lighthouse Admin”, joka ei todellisuudessa vastaa mitään GDAP- tai RBAC-roolia.

Global Administrator -GDAP-rooli antaa Microsoft 365 -ympäristöön täydet oikeudet, jonka jakaminen IT-kumppanin teknikoille saattaa olla ongelmallista pienissäkin IT-palvelutaloissa. Tämän roolin käyttämistä koitetaan yleisesti karttaa, tietoturvariskien minimoimiseksi. Ihannetapauksessa IT-teknikoilla olisi käyttöoikeudet pelkästään heille osoitettuihin työtehtäviin.

Microsoft 365 Lighthouse RBAC-käyttöoikeusrooleja on vain yksi, mikä vähentää käyttöoikeushallinnan joustavuutta. Useampien RBAC-roolien avulla IT-palveluntarjoaja pystyisi helpommin rajaamaan oikeuksia käyttäjien tehtävien vaatimusten mukaisesti, niiden avulla pystyisi myös mahdollisesti luopumaan Global Administrator -GDAP-roolin käyttämisestä.

4.3 Hallintakäytäntölinjauksen ja hallintakäytäntötehtävien luonti

Hallintakäytäntölinjauksen luonti on yksinkertaista, mutta Microsoftin dokumentaatio linjauksen luontiin vaadituista käyttöoikeuksista ei ole selkeä. Microsoft mainitsee dokumentaatiossaan, että käyttäjän tulee olla "Microsoft 365 Lighthouse admin", mutta kuten aikaisemmin todettu, tämä tieto on virheellinen.

Hallintakäytäntötehtävän luominen kopioimalla hallintakäytäntö IT-kumppanin hallitsemista asiakasympäristöistä on kattava ominaisuus, jolla pystytään Microsoft 365 Lighthouse -palvelun kautta kokoamaan IT-palveluntarjoajien usein käyttämiä hallintakäytäntöjä saman linjauksen alle. Kopioiminen toimii nopeasti ja luotettavasti, lukuun ottamatta asiakasympäristökohtaisia asetuksia. Hallintakäytäntötehtävään kopioidut asiakasympäristökohtaiset hallintakäytäntöjen konfiguraatioasetukset aiheuttavat ongelmia hallintakäytäntötehtävässä. Tämä huomattiin esimerkiksi, kun kopioitiin Vetonaulan käyttämä yhdenmukaisuuskäytäntö, jossa käytäntöön oli määritetty Microsoft Intune -laitehallintapalvelussa sijaitsevien sähköpostimallipohjien käyttäminen. Yhdenmukaisuuskäytäntö käyttää apunaan näitä mallipohjia tietyissä tilanteissa lähettääkseen käyttäjille tilannetietoja laitteen yhteensopivuuden tilasta ja tarvittavista toimenpiteistä.

Kun tämä kyseinen yhdenmukaisuuskäytäntö kopioitiin hallintakäytäntötehtävään ja sitä yritettiin käyttöönottaa Vetonaula Demo -asiakasympäristöön, Microsoft 365 Lighthouse -portaali antoi yleispätevän virhekoodin, eikä tehtävän käyttöönotto valmistunut. Tämä yhdenmukaisuuskäytäntö piti kopioida ilman sähköpostimalleja hyödyntäviä konfiguraatioasetuksia, jotta tehtävän käyttöönotto onnistui. Vastaavissa ongelmatilanteissa olisi hyödyllistä, jos palvelu valmistaisi yksityiskohtaisen virheilmoituksen, josta ongelman juurisyy olisi tunnistettavissa. Tämän lisäksi Microsoftin dokumentaatiossa voisi olla lueteltuna yksityiskohtaisemmat tiedot sisäänrakennetuista hallintakäytäntötehtävien rajoituksista.

Tällä hetkellä IT-palveluntarjoajan tulee käydä hallintakäytäntöjen konfiguraatioasetukset tarkasti läpi ja yksitellen testata niiden käyttöönottoa, mikäli käyttöönotto ei onnistu, tulee arvioida mikä hallintakäytännön konfiguraatioasetuksista mahdollisesti estää sen käyttöönoton.

Toinen hallintakäytäntöjen kopioinnissa vastaan tullut ongelma oli, että asiakasympäristöistä joihin Microsoft 365 Lighthouse -käyttäjällä ei ole Global Administrator -GDAP-roolia, ei kopiointia pysty suorittamaan valmiiksi. Tällöin ei tule virheilmoitusta, vaan Microsoft 365 Lighthouse -portaali jää kopioimaan hallintakäytäntöä loputtomiin.

Hallintakäytäntölinjauksia voidaan luoda useampia, joten on mahdollista jakaa IT-palveluntarjoajan asiakkuuksia eri hallintakäytäntöryhmiin, mikäli IT-palveluntarjoajalla on tämän kaltaisia tarpeita.

4.4 Hallintakäytäntötehtävien käyttöönotto asiakasympäristöön

Ilman Global Administrator -GDAP-roolia hallintakäytäntötehtävien käyttöönotto ei valmistu, mutta siitä ei myöskään tule virheilmoitusta.

Mikäli hallintakäytäntötehtävien käyttöönotto epäonnistuu, tai käyttöönotto ei ikinä valmistu, saattaa ongelmat johtua joko puuttuvista käyttöoikeuksista tai hallintakäytäntötehtävän sisäisistä konfigurointiasetusten ongelmista, kuten luvussa 4.3 puhutuista asiakasympäristökohtaisista sähköpostimallipohjista.

4.5 Johtopäätökset ja suositukset

Microsoft 365 Lighthouse -palvelun hallintakäytäntölinjaukset toimivat hyvänä mallipohjana, johon IT-palveluntarjoaja voi koota usein käyttämänsä hallintakäytännöt. Etenkin uusien asiakkuuksien Microsoft 365 -ympäristöjen käyttöönotossa, Microsoft 365 Lighthouse voisi nopeuttaa ja selkeyttää hallintakäytäntöjen käyttöönottoa, sekä vähentää manuaalisen työn aiheuttamia inhimillisiä virheitä. Hallintakäytäntölinjauksia voidaan myös luoda useampia, mikäli IT-palveluntarjoaja haluaa jakaa asiakkaitaan erilaisiin hallintakäytäntöryhmiin.

Hallintakäytäntölinjauksien kokoamisessa pitää huomioida Microsoft 365 Lighthouse -palvelun tämänhetkiset rajoitteet. Linjauksien hallintakäytäntötehtävät tulee testata tarkasti IT-palveluntarjoajan käyttötarkoitusten mukaisesti. Jokaisella IT-palveluntarjoajalla on omankaltaisensa hallintakäytäntöjen hierarkia, jonka tuominen Microsoft 365 Lighthouse hallintakäytäntölinjauksiin saattaa vaatia nykyisten hallintakäytäntöjen konfiguraatioasetusten mukauttamista, sekä yksilöllistä testaamista.

Palvelun käyttöönotto vaatii IT-palveluntarjoajalta sisäistä arviointia ja sovittamista omaan tuotantoonsa, mutta pidemmällä tähtäimellä Microsoft 365 Lighthouse säästää resursseja uusien asiakkuuksien Microsoft 365 -ympäristön käyttöönotossa, etenkin jos nykyisenä ratkaisuna luodaan hallintakäytännöt manuaalisesti. Microsoftin jatkaessa palvelun kehittämistä, nykyistenkin asiakkuuksien hallintakäytäntöjen hallinnan siirtäminen Microsoft 365 Lighthouse -portaaliin, voi olla keskitetyn asiakkuuksien hallinnan näkökulmasta kannattavaa.

Lähteet

Microsoft (2023.12.6-a). *Create a baseline in Microsoft 365 Lighthouse*. https://learn.microsoft.com/en-us/microsoft-365/lighthouse/m365-lighthouse-create-a-baseline?view=o365-worldwide

Microsoft (2024.5.21-a). *Microsoft Intune securely manages identities, manages apps, and manages devices*. https://learn.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune

Microsoft (2023,4.12-b). *Get started with your Microsoft Intune deployment*. https://learn.microsoft.com/en-us/mem/intune/fundamentals/get-started-with-intune

Microsoft (2024.1.18-c). *Overview of permissions in Microsoft 365 Lighthouse*. https://learn.microsoft.com/en-us/microsoft-365/lighthouse/m365-lighthouse-overview-of-permissions?view=o365-worldwide

Microsoft (2023.7.17-c). *Overview of Microsoft 365 Lighthouse*. https://learn.microsoft.com/en-us/microsoft-365/lighthouse/m365-lighthouse-overview?view=o365-worldwide

Microsoft (2024.2.16-d). *Overview of using Microsoft 365 Lighthouse baselines to deploy standard tenant configurations*. https://learn.microsoft.com/en-us/microsoft-365/lighthouse/m365-lighthouse-deploy-standard-tenant-configurations-overview?view=o365-worldwide

Microsoft (2023.6.21-d). *Understand deployment statuses in Microsoft 365 Lighthouse*. https://learn.microsoft.com/en-us/microsoft-365/lighthouse/m365-lighthouse-understand-deployment-statuses?view=o365-worldwide

Microsoft (2024.1.17-d). *Requirements for Microsoft 365 Lighthouse*. https://learn.microsoft.com/en-gb/microsoft-365/lighthouse/m365-lighthouse-requirements?view=o365-worldwide

Microsoft (2023.6.6-f). *Understanding deployment insights in Microsoft 365 Lighthouse*. https://learn.microsoft.com/en-us/microsoft-365/lighthouse/m365-lighthouse-deployment-insights-overview?view=o365-worldwide