Joonas Gumberg

Intunen käyttöönotto

Metropolia Ammattikorkeakoulu
Insinööri (AMK)
Tieto- ja viestintätekniikan tutkinto-ohjelma
Insinöörityö
21.7.2023

Tiivistelmä

Tekijä:	Joonas Gumberg
Otsikko:	Intunen käyttöönotto
Sivumäärä:	21 sivua + 13 liitettä
Aika:	21.7.2023

Tutkinto:	Insinööri (AMK)
Tutkinto-ohjelma:	Tieto- ja viestintätekniikka
Ammatillinen pääaine:	Monimuoto/Verkkototeutus
Ohjaajat:	Yliopettaja Janne Salonen

Tänä päivänä yhä useampi organisaatio siirtyy pilvipohjaisiin ratkaisuihin. Tämä trendi johtuu monista syistä, kuten skaalautuvuudesta, joustavuudesta, kustannustehokkuudesta ja uusien työkalujen ja teknologioiden jatkuvasta kehityksestä. Pilvipalvelut eivät enää ole vain isojen yritysten etuoikeus, vaan ne ovat myös pienempien yritysten ja organisaatioiden ulottuvilla. Jatkuvasti kasvavat ja kehittyvät työkalut tarjoavat uusia mahdollisuuksia, joita kaikkien organisaatioiden tulisi hyödyntää.

Yksi näistä työkaluista on Microsoft Intune, joka on osa Microsoftin laajempaa Enterprise Mobility + Security -palvelukokonaisuutta. Intune on pilvipohjainen palvelu, jonka avulla organisaatiot voivat hallita mobiililaitteitaan ja -sovelluksiaan, mukaan lukien tietoturvaominaisuudet.

Avainsanat: Intune, Azure, Autopilot

Abstract

Author:	Joonas Gumberg
Title:	Intune Deployment
Number of Pages:	21 pages + 13 appendices
Date:	21 July 2023
Degree:	Bachelor of Engineering
Degree Programme:	Information and Communication Technology
Professional Major:	Online Studies
Supervisors:	Principal Lecturer Janne Salonen

Today, an increasing number of organizations are moving towards cloud based solutions. This trend is due to various reasons such as scalability, flexibility, cost-effectiveness, and the continuous development of new tools and technologies. Cloud services are no longer just a privilege for large companies but are also within the reach of smaller businesses and organizations. Continuously growing and developing tools offer new opportunities that all organizations should take advantage of.

One of these tools is Microsoft Intune, which is part of Microsoft's broader Enterprise Mobility + Security service package. Intune is a cloud-based service that allows organizations to manage their mobile devices and applications, including security features.

Keywords: Intune, Azure, Autopilot

Sisällys

Lyhenteet ja Keskeiset käsitteet

AD: Windows palvelimella oleva Active Directory.

AAD: Pilvessä toimiva Azure Active Directory.

APP: Lyhennetty sanasta “Application”, eli suomeksi Applikaatio.

Autopilot: Autopilot on pilvipohjainen palvelu, joka on suunniteltu helpottamaan Windows-pohjaisten laitteiden (kuten pöytäkoneiden ja kannettavien tietokoneiden) käyttöönottoa.

Azure: Microsoftin pilvipalvelu ympäristö joka toimii verkossa.

B2B: Business to Business.

B2C: Business to Consumer.

BYOD: Lyhenne sanoista ”Bring Your Own Device”. Oman laitteen käyttäminen organisaation ympäristössä.

EMS: Microsoftin Enterprise Mobility + Security (EMS) -ratkaisu.

Intune: Microsoftin päätelaitehallinta työkalu.

MAM: ”Mobile Applicationa Management”, eli Mobiili applikaatiohallinta.

MDM: ”Mobile Device Management”, eli Mobiililaitehallinta.

MFA: ”Multi-Factor Authentication”, eli Monivaiheinen todennus.

SSO: ”Single Sign-On”, eli Yksi kirjautuminen.

VPN: ”Virtual Private Network”, eli Virtuaalinen yksityinen verkko.

1 Johdanto

Työn aihe löytyi, kun kävin keskustelun esimiehen kanssa opinnäytetyön aiheesta. Ehdotuksena tuli intunen käyttöönotto ja sitä lähdin työstämään.

Tänä päivänä yhä useampi organisaatio siirtyy pilvipohjaisiin ratkaisuihin. Tämä trendi johtuu monista syistä, kuten skaalautuvuudesta, joustavuudesta, kustannustehokkuudesta ja uusien työkalujen ja teknologioiden jatkuvasta kehityksestä. Pilvipalvelut eivät enää ole vain isojen yritysten etuoikeus, vaan ne ovat myös pienempien yritysten ja organisaatioiden ulottuvilla. Jatkuvasti kasvavat ja kehittyvät työkalut tarjoavat uusia mahdollisuuksia, joita kaikkien organisaatioiden tulisi hyödyntää. (Business Insider 2021)

Yksi näistä työkaluista on Microsoft Intune, joka on osa Microsoftin laajempaa Enterprise Mobility + Security -palvelukokonaisuutta. Intune on pilvipohjainen palvelu, jonka avulla organisaatiot voivat hallita mobiililaitteitaan ja sovelluksiaan, mukaan lukien tietoturvaominaisuudet.

Intune mahdollistaa monenlaisten laitteiden hallinnan, mukaan lukien älypuhelimet, tabletit ja tietokoneet. Tämä on erityisen tärkeää etätyössä, joka on yhä yleisempää. Etätyöskentelyn myötä työntekijät käyttävät monenlaisia laitteita usein myös organisaation ulkopuolella, jolloin laitteiden turvallisuus ja hallinta muuttuvat entistä tärkeämmiksi.

Intunen avulla organisaatiot voivat määrittää laite- ja sovelluskäytäntöjä, jotka auttavat hallitsemaan ja suojaamaan yrityksen tietoja. Esimerkiksi, organisaatio voi rajoittaa, mitkä sovellukset voivat käyttää yrityksen tietoja, tai vaatia laitteiden salausta ja salasanoja. Intune myös auttaa ylläpitämään laitteiden päivitykset, joka on tärkeä osa tietoturvaa.

Yrityksen tietoturvan lisäksi Intune myös parantaa työntekijöiden tuottavuutta. Intune voi esimerkiksi asentaa automaattisesti tarvittavat sovellukset uusiin laitteisiin, mikä tekee uusien laitteiden käyttöönotosta helppoa ja nopeaa.

Työntekijät voivat myös käyttää omia laitteitaan (BYOD, Bring Your Own Device), koska Intune pystyy erottamaan yrityksen tiedot ja henkilökohtaiset tiedot. (Microsoft 2016. Enterprise Mobility with App Management, Office 365, and Threat Mitigation: Beyond BYOD.)

Kun organisaatiot siirtyvät yhä enemmän pilvipohjaisiin ratkaisuihin, työkalujen, kuten Intunen, osaaminen tulee yhä tärkeämmäksi. Tietotekniikan ammattilaisten lisäksi myös esimiehet ja työntekijät hyötyvät ymmärtämisestä, miten nämä työkalut toimivat ja miten niitä voidaan hyödyntää parhaalla mahdollisella tavalla. Koulutus ja jatkuva oppiminen ovat avainasemassa tässä muutoksessa. (Accenture. Cloud Computing.)

Työntilaajana toimii Lounea Yritysratkaisut Oy. Lounea on suomen neljänneksi suurin operaattori. Lounea tarjoaa Suomen nopeimman laajakaista yhteyden käyttäjille tällä hetkellä. (Ookla® Speedtest® analysoi: Lounea Valokuitu on Suomen nopein netti) Lounea tarjoaa myös yritysasiakkaille IT- tuki ja hallinta palveluita. (Lounea Oy)

2 Tavoite

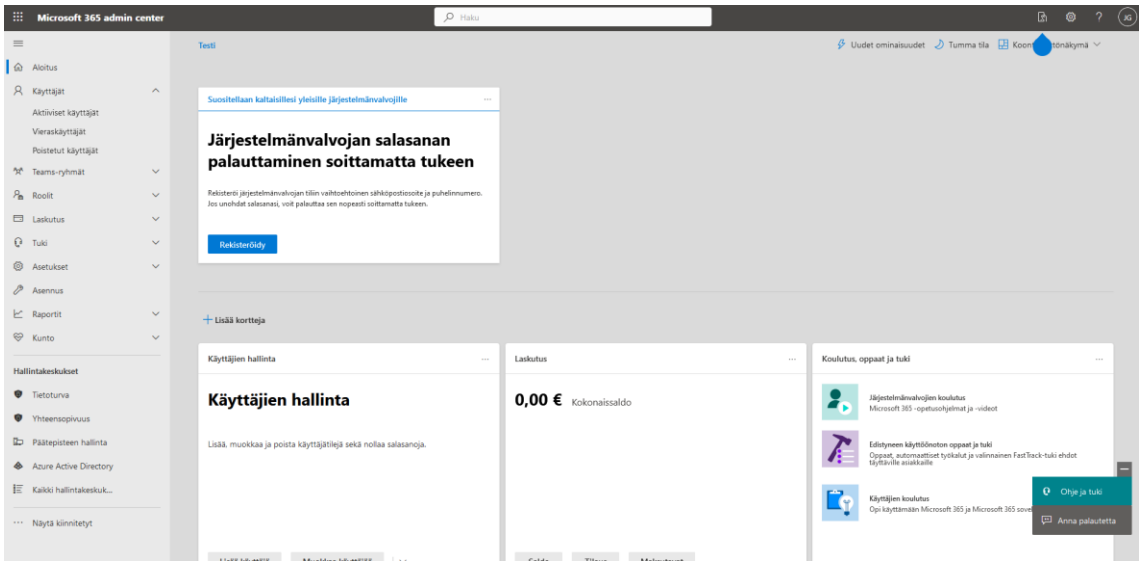
Tämä työ keskittyy Microsoft Intunen käyttöönoton yleisiin vaiheisiin ja sen keskeisiin toimintoihin Azure-palvelun yhteydessä. Vaikka tavoitteena on tarjota mahdollisimman selkeä ja kattava kuvaus Intunen käyttöönotosta, on tärkeää ymmärtää, ettemme voi syventyä liian yksityiskohtaisiin asetuksiin tai sovelluksiin. Tämä johtuu siitä, että jokaisella organisaatiolla on omat erityiset politiikkansa ja käytäntönsä sovellusten ja yritystoimintojen suhteen, ja nämä vaikuttavat siihen, miten Intunea käytetään käytännössä.

Esimerkiksi, organisaation turvallisuusvaatimukset, tietosuoja-asetukset, BYOD (Bring Your Own Device) -politiikat ja eri sovellusten käyttötarpeet voivat vaikuttaa siihen, miten Intunea konfiguroidaan ja käytetään. Jotkut organisaatiot saattavat vaatia tiukempia turvallisuusasetuksia, kun taas toiset saattavat painottaa käyttäjäystävällisyyttä ja joustavuutta.

Siksi on suositeltavaa, että organisaation IT-henkilöstö tai Intunea hallinnoiva taho tutustuu tähän työhön ja soveltaa sitä organisaation erityistarpeisiin ja -vaatimuksiin. Tässä työssä tarjottava ohjeistus on suunniteltu toimimaan lähtökohtana ja opastamaan Intunen käyttöönoton yleisissä vaiheissa, mutta se ei korvaa organisaation omien politiikkojen ja vaatimusten ymmärtämistä ja huomioimista.

3 Keskeiset Teknologiat

3.1 Azure



Kuva 1. Microsoft Azure Admin Center: Etusivu

Microsoft Azure on pilvipalvelualusta, joka tarjoaa monipuolisia työkaluja ja palveluita organisaatioiden käyttöön. Azure mahdollistaa organisaatioille erilaisten sovellusten ja palveluiden kehittämisen, käyttöönoton ja hallinnoinnin pilvessä. Se tarjoaa infrastruktuurin, alustan ja ohjelmiston palveluita, jotka auttavat organisaatioita skaalautumaan, tehostamaan toimintaansa ja kehittämään innovatiivisia ratkaisuja.

Azuren avulla organisaatiot voivat luoda ja hallinnoida virtuaalisia koneita, tallennustiloja, verkkoinfrastruktuureja ja tietokantoja pilvessä. Se tarjoaa myös palveluita, kuten tekoälyä, analytiikkaa, lohkoketjua, Internet of Things (IoT) -ratkaisuja ja paljon muuta. Näiden palveluiden avulla organisaatiot voivat kehittää älykkäitä sovelluksia, analysoida ja hyödyntää dataa, automatisoida prosesseja ja luoda uusia liiketoimintamahdollisuuksia.

Azuren etuihin kuuluu sen laaja skaalautuvuus, joka mahdollistaa organisaatioiden joustavan resurssien hallinnan. Organisaatiot voivat skaalata palveluitaan tarpeen mukaan ylös tai alas, mikä tekee siitä kustannustehokkaan ratkaisun. Azuren globaali saatavuus takaa myös korkean käytettävyyden ja suorituskyvyn organisaatioille eri puolilla maailmaa. (Azure. Scaling up vs. scaling out.)

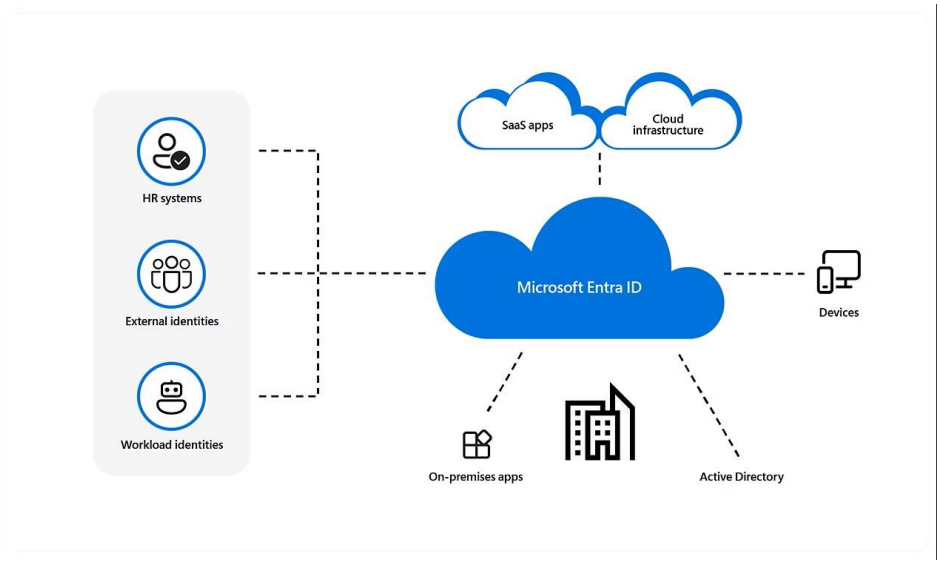
Azuren käyttöönotto on myös helppoa ja joustavaa. Organisaatiot voivat valita haluamansa palvelut ja skaalautua tarpeen mukaan. Azuren integroitavuus muiden Microsoftin tuotteiden ja palveluiden kanssa tekee siitä houkuttelevan vaihtoehdon organisaatioille, jotka jo käyttävät muita Microsoftin ratkaisuja.

Kuva 2. Microsoft Azure Security.

Sovellusten hallinta organisaatiosi laitteissa on keskeinen osa turvallista ja tuottavaa yritysinfrastruktuuria. Voit käyttää Microsoft Intunea hallitaksesi niitä

sovelluksia, joita yrityksesi työvoima käyttää. Sovellusten hallinnalla autat hallitsemaan, mitä sovelluksia yrityksesi käyttää sekä sovellusten asetuksia ja suojausta.

3.1.1 Azure Active Directory



Kuva 3. Microsoft Entra ID diagrammi.

Azure Active Directory (Azure AD tai AAD), joka toimii nykyään nimellä Microsoft Entra ID (Microsoft 2023. Azure Active Directory), on Microsoftin pilvipohjainen identiteetin- ja käyttöoikeuksienhallintapalvelu. Sen avulla organisaatiot voivat tarjota käyttäjilleen turvallisen ja helpon pääsyn niin yrityksen sisäisiin kuin ulkoisiinkin sovelluksiin. Azure AD tukee sekä sisäisten että ulkoisten käyttäjien tunnistusta ja valtuutusta, mukaan lukien käyttäjät, jotka tulevat muista organisaatioista tai ovat itsenäisiä kuluttajia.

Azure AD tarjoaa monia ominaisuuksia, kuten:

Yksi kirjautuminen (Single Sign-On, SSO)**:** SSO:n avulla käyttäjät voivat kirjautua sisään kerran ja saada pääsyn useisiin sovelluksiin ilman, että heidän tarvitsee muistaa useita käyttäjätunnuksia ja salasanoja.

Monivaiheinen todennus (Multi-Factor Authentication, MFA): MFA tarjoaa lisäkerroksen turvallisuutta vaatimalla käyttäjiltä useampia todentamismenetelmiä.

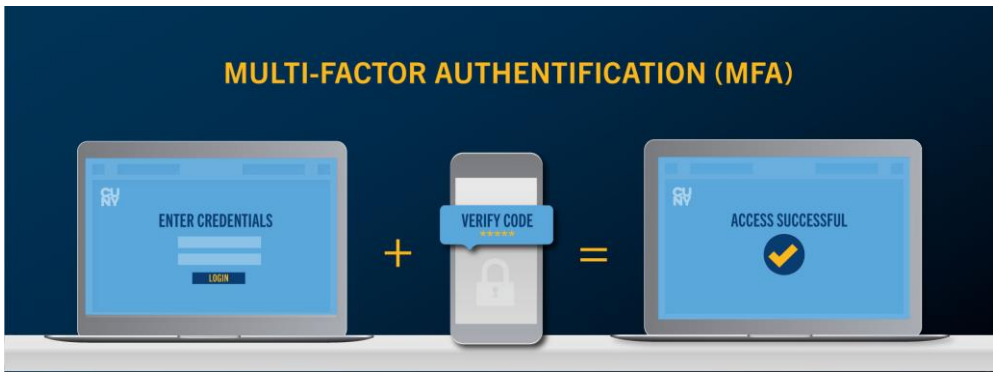
Ehdollinen pääsy (Conditional Access)**:** Tämän avulla voidaan määrittää käyttöehtoja, jotka on täytettävä ennen kuin käyttäjä voi saada pääsyn resursseihin.

Identiteettien suojelu (Identity Protection): Azure AD käyttää kehittynyttä koneoppimista, heuristiikkaa ja tunnistetietoja havaitakseen epätavalliset ja epäilyttävät käyttäjätunnistuksen yritykset ja toteuttaa tarvittavat toimenpiteet.

B2B- ja B2C-tunnistus: Azure AD tukee sekä Business-to-Business (B2B) että Business-to-Consumer (B2C) skenaarioita. B2B-ratkaisussa organisaatiot voivat jakaa sovelluksensa ja palvelunsa kumppaniorganisaatioiden kanssa, kun taas B2C-ratkaisussa organisaatiot voivat tarjota turvallisen ja skaalautuvan tunnistuksen kuluttajille.

Azure AD on myös laajasti integroitu muihin Microsoftin palveluihin, kuten Office 365, Azure, Dynamics 365, sekä kolmansien osapuolten sovelluksiin. Tämä mahdollistaa laajan käyttäjien ja resurssien hallinnan yhdestä paikasta. (Montra. Benefits of Microsoft 365 and Azure)

3.1.2 Monivaiheinen Todennus



Kuva 4. Monivaiheinen todennus esimerkki.

Monivaiheinen todennus, tai Multi-Factor Authentication (MFA), on tärkeä osa Microsoftin palvelujen turvallisuutta. Se lisää tietoturvan tasoa vaatimalla käyttäjiltä useampia todentamismenetelmiä. Tämä tarkoittaa, että käyttäjien on todistettava henkilöllisyytensä useammalla kuin yhdellä tavalla ennen kuin he voivat kirjautua sisään tai saada pääsyn resursseihin. (Microsoft 2023. Multifactor authentication in Azure AD.)

Microsoftin MFA:ssa käytetään yleensä kahta tai useampaa seuraavista todentamismenetelmistä:

Tieto: Jotain, mitä vain käyttäjä tietää, kuten salasana.

Hallussapito: Jotain, mitä vain käyttäjä omistaa, kuten puhelin, johon lähetetään vahvistuskoodi.

Olemus: Jotain, mitä vain käyttäjä on, kuten sormenjälki tai kasvontunnistus.

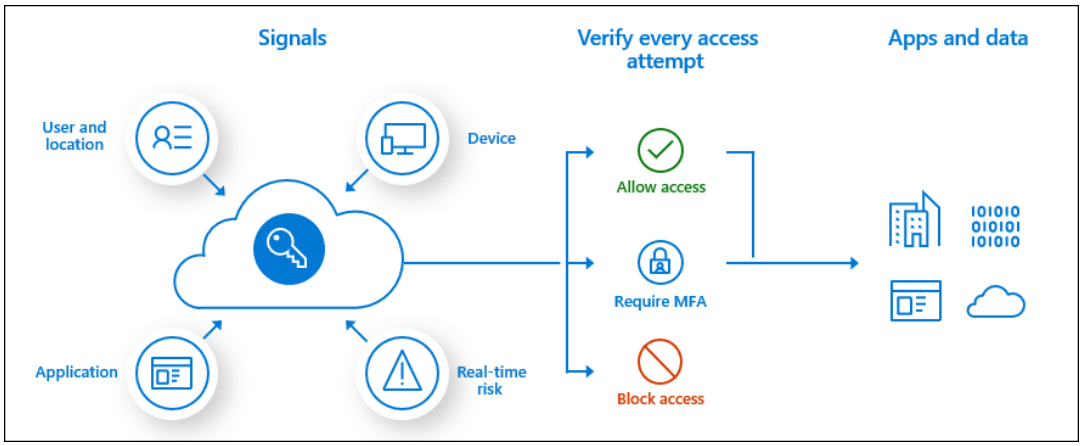
Microsoft tarjoaa monia eri tapoja toteuttaa MFA. Yksi yleisimmistä tavoista on Microsoft Authenticator -sovelluksen käyttö, joka on saatavilla sekä Androidille että iOS:lle. Kun käyttäjä yrittää kirjautua sisään, hän saa ilmoituksen Authenticator-sovellukseen. Käyttäjän on vahvistettava yritys sovelluksessa ennen kuin kirjautuminen hyväksytään.

Vaihtoehtoisesti voidaan käyttää tekstiviesti- tai puhelinsoitto -vahvistusta. Tekstiviestivahvistuksessa käyttäjä saa vahvistuskoodin tekstiviestinä puhelimeensa. Puhelinsoitto -vahvistuksessa käyttäjä saa puhelun, ja kirjautuminen hyväksytään kun käyttäjä vastaa puheluun ja painaa näppäintä.

MFA:n käyttöönotto Microsoftin palveluissa tapahtuu Azure Active Directoryn (Azure AD) kautta. Azure AD:n turvallisuusosiossa voidaan määrittää, ketkä käyttäjät tai ryhmät tarvitsevat MFA:n, ja minkälaisissa olosuhteissa MFA vaaditaan (esimerkiksi kaikissa olosuhteissa, tai vain silloin kun käyttäjä yrittää kirjautua sisään tuntemattomasta sijainnista).

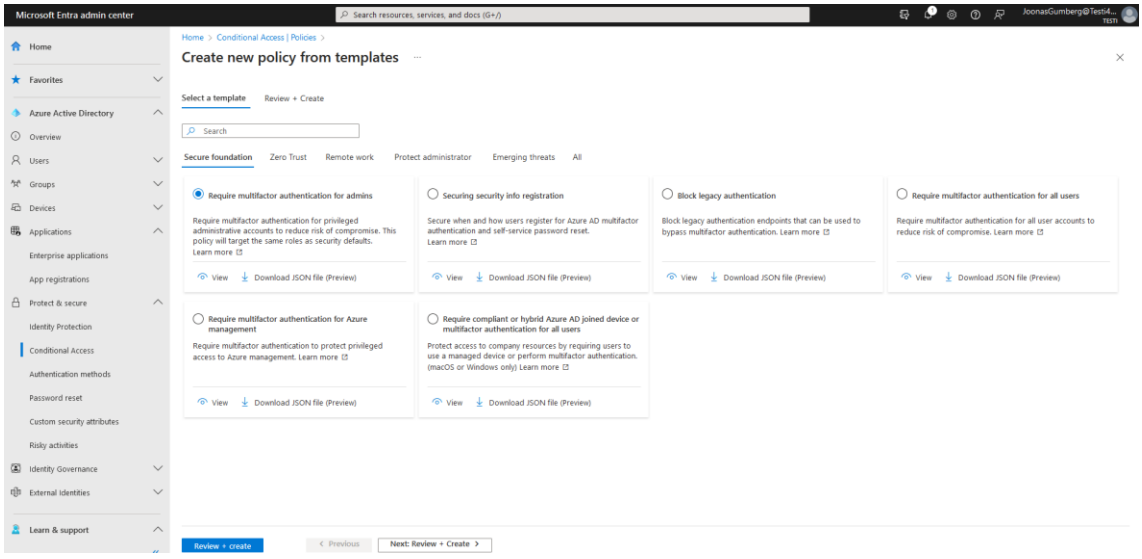
On tärkeää huomata, että vaikka MFA lisää turvallisuutta merkittävästi, se ei yksinään ole riittävä suojautuminen kaikilta tietoturvauhkilta. MFA:n käyttö on osa

laajempaa tietoturvastrategiaa, johon kuuluu myös esimerkiksi käyttäjien koulutuminen, järjestelmien päivittäminen, ja tietoturvaloukkauksien varalta varautuminen. (Cuny, The University of New York. Microsoft Multi-factor Authentication)



Kuva 5. Havainollistava kuva MFA:sta.

3.1.3 Politiikat



Kuva 6. Politiikat, eli käytäntö asetukset.

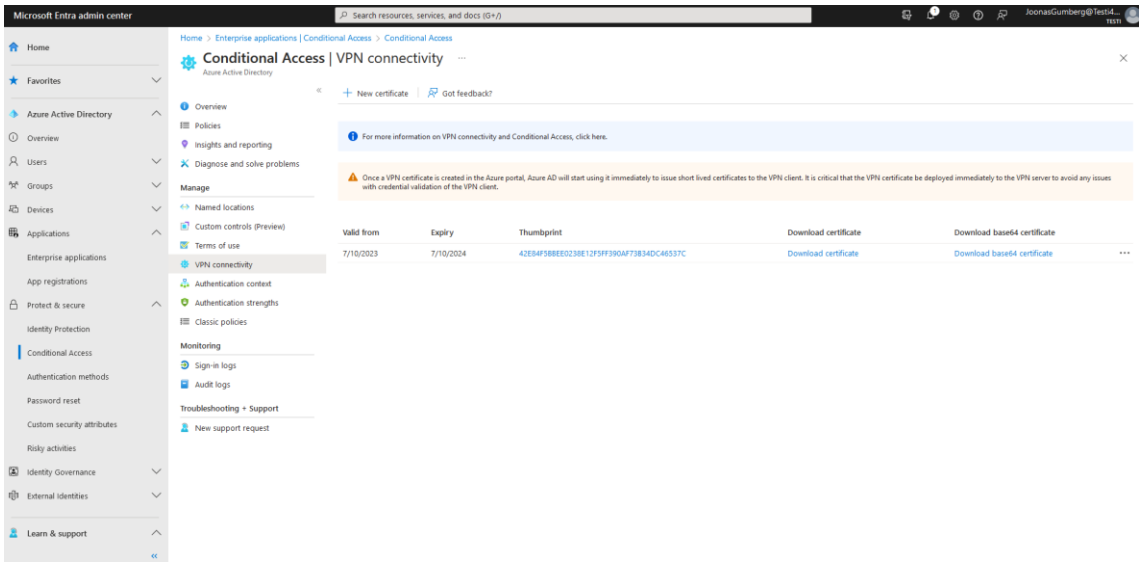
Yksi Intunen tarjoama tapa mobiilisovellusten turvaamiseen on käyttää politiikkoja. Sovelluksen suojelu -politiikat (APP) ovat sääntöjä, jotka varmistavat organisaation tietojen pysymisen turvassa tai hallinnassa hallinnoidussa

sovelluksessa. Politiikka voi olla sääntö, joka otetaan käyttöön, kun käyttäjä yrittää käyttää tai siirtää "yritys" -tietoja, tai joukko toimia, jotka ovat kiellettyjä tai seurattuja, kun käyttäjä on sovelluksen sisällä. Hallinnoitu sovellus on sovellus, johon sovellussuojapolitiikat on sovellettu ja sitä voidaan hallita Intunella.

Mobiilisovelluksen hallinta (MAM) sovelluksen suojelun politiikat mahdollistavat organisaation tietojen hallinnan ja suojaamisen sovelluksessa. Monia sovelluksia, kuten Microsoftin Office -sovelluksia, voidaan hallita Intunen MAM:n avulla.

Organisaatiot voivat käyttää sovellussuojapolitiikkoja sekä MDM:n kanssa että ilman sitä samaan aikaan. Esimerkiksi harkitse tilannetta, jossa työntekijä käyttää sekä yrityksen myöntämää tablettia että omaa henkilökohtaista puhelintaan. Yrityksen myöntämä tabletti on rekisteröity MDM:ään ja suojattu sovellussuojapolitiikoilla, kun taas henkilökohtainen puhelin on suojattu vain sovellussuojapolitiikoilla.

3.1.4 VPN



Kuva 7. VPN sertifikaatti hankittuna.

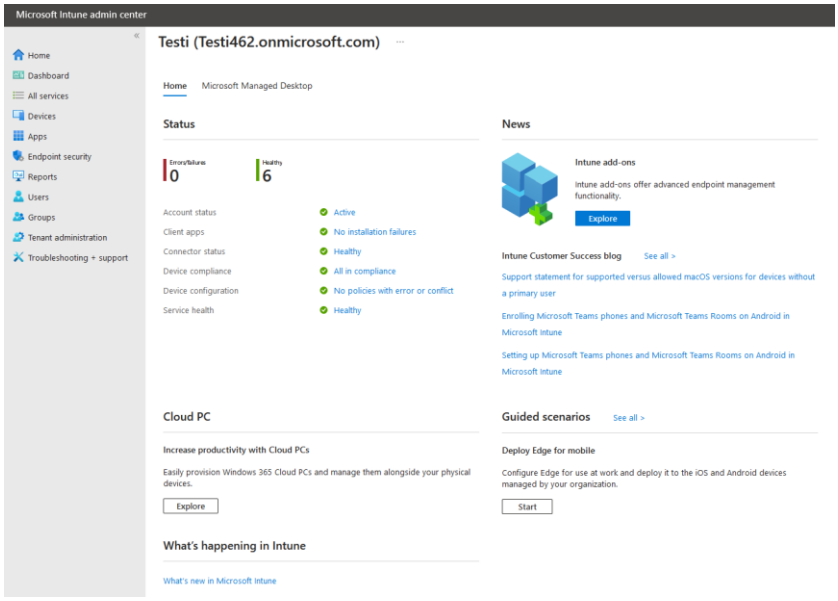
Virtuaaliset yksityisverkot (VPN) ovat tärkeä teknologia, jotka mahdollistavat turvallisen pääsyn etäresursseihin. Ne luovat salatun yhteyden käyttäjän laitteen ja tiettyjen resurssien, kuten yrityksen sisäverkon, välille. Tämä mahdollistaa turvallisen datan liikkumisen yleisissä verkoissa, kuten kotona, hotelleissa, kahviloissa ja muissa julkisissa paikoissa. (Cisco)

Microsoft Intune tarjoaa ratkaisuja laitteidenhallintaan ja sovellusten käyttöönottoon. Intunessa voit määrittää VPN-asiakassovelluksia Android Enterprise -laitteille käyttämällä sovelluksen määrityspolitiikkaa. Tämä tarkoittaa, että voit päättää, millaisia VPN-yhteyksiä laitteet voivat muodostaa ja mitä palvelimia ne voivat käyttää.

Määrityspolitiikan jälkeen voit asettaa tämän politiikan yhdessä VPN-määritysten kanssa organisaation laitteille. Tämä tarkoittaa, että voit hallita, miten ja milloin laitteet käyttävät VPN-yhteyksiä.

Intunessa voit myös luoda sovelluskohtaisia VPN-politiikkoja. Tätä ominaisuutta kutsutaan sovelluskohtaiseksi VPN:ksi, ja se tarkoittaa, että tietty sovellus voi muodostaa yhteyden VPN:ään silloin, kun se on aktiivinen ja käyttää resursseja jaan VPN:n kautta. Kun sovellus ei ole aktiivinen, VPN-yhteyttä ei käytetä. Tämä voi parantaa tietoturvaa ja vähentää tarpeetonta liikennettä VPN:ää pitkin.

3.2 Intune



Kuva 8. Intune Admin Center hallinta etusivu.

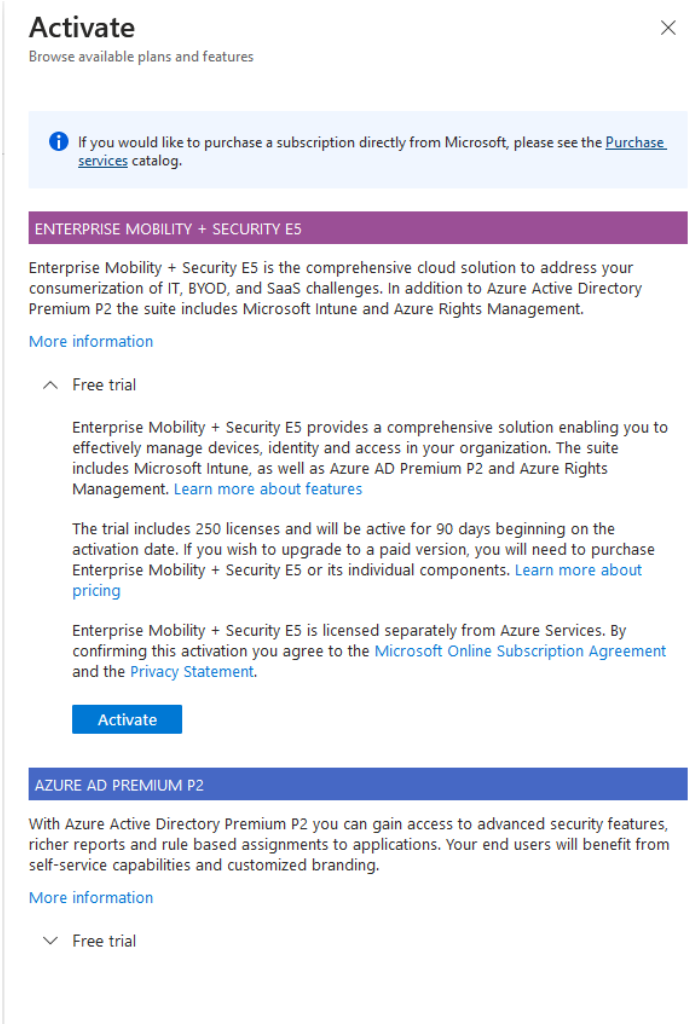
Microsoft Intune on osa Microsoftin laajempaa Enterprise Mobility + Security (EMS) -ratkaisua, joka on suunniteltu auttamaan organisaatioita hallitsemaan ja turvaamaan päätelaitteita ja sovelluksia. Intune toimii pilvipohjaisesti, mikä tarkoittaa, että sen hallinta ja toiminnallisuudet ovat saatavilla missä tahansa maailmassa, kunhan käyttäjällä on internet-yhteys. (Microsoft EMS)

Intune mahdollistaa useiden eri päätelaitteiden, kuten kannettavien tietokoneiden, pöytätietokoneiden, älypuhelimien ja tablettien, hallinnan. Se tukee useita käyttöjärjestelmiä, mukaan lukien Windows, macOS, iOS ja Android, mikä tekee siitä joustavan valinnan useimmille organisaatioille.

Yksi Intunen keskeisistä ominaisuuksista on niin sanottu Mobile Device Management (MDM), joka tarkoittaa mobiililaitteiden hallintaa. Sen avulla IT-osastot voivat määrittää ja valvoa turvallisuus- ja yksityisyysasetuksia, hallita sovelluksia ja päivityksiä, sekä suorittaa etädiagnostiikkaa ja -korjausta. Tämä vähentää merkittävästi IT-osastojen kuormitusta ja antaa niille mahdollisuuden keskittyä strategisempiin tehtäviin.

Lisäksi Intune sisältää Mobile Application Management (MAM) -ominaisuuksia, jotka mahdollistavat yrityssovellusten hallinnan ilman, että laitteen kokonaishallinta olisi välttämätöntä. Tämä on hyödyllistä esimerkiksi (BYOD) -käytännöissä, joissa työntekijät käyttävät omia laitteitaan työtehtävissä.

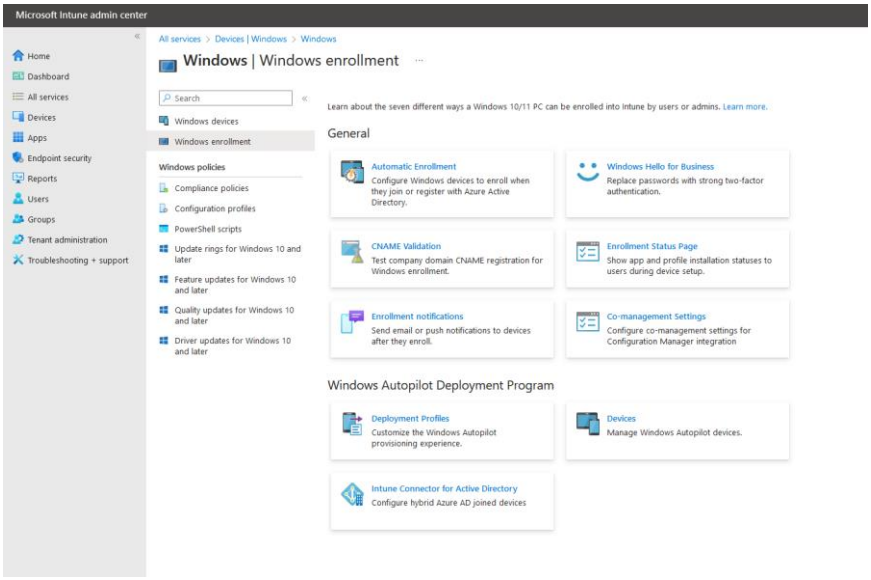
Intune on suunnattu kaikenkokoisille organisaatioille, sillä sen avulla voidaan hallita laajamittaisesti tuhansia laitteita samanaikaisesti. Palvelun joustavuus, monipuolisuus ja integroitavuus muiden Microsoftin pilvipalveluiden, kuten Azure Active Directoryn ja Office 365:n kanssa, tekevät siitä tehokkaan työkalun nykyaikaisen työpaikan hallintaan.



Kuva 9. Intunen aktivointi lisenssi.

Toimiakseen tarvitset Enterprise Mobility + Security lisenssin.

3.2.1 Autopilot



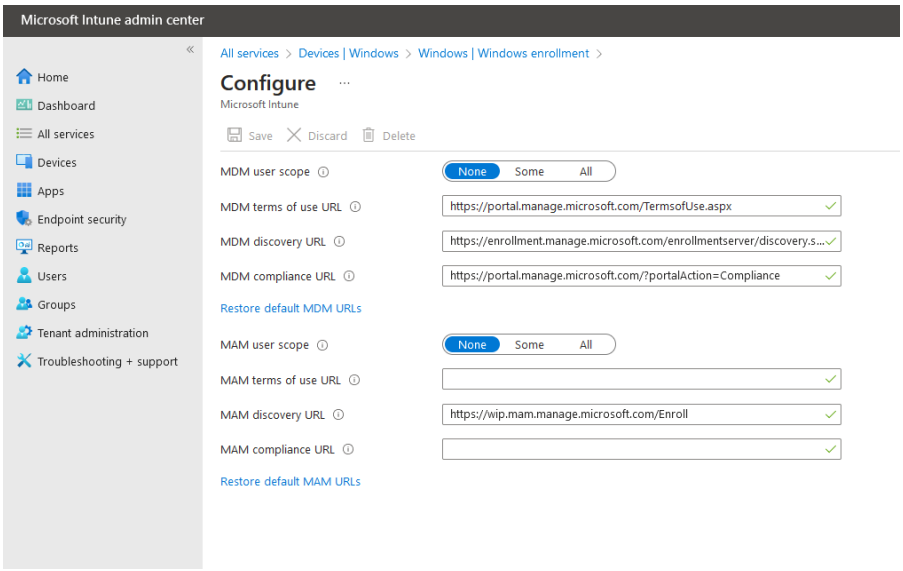
Kuva 10. Autopilot käyttöönotto.

Microsoft Intune Autopilot on pilvipohjainen palvelu, joka on suunniteltu helpottamaan Windows-pohjaisten laitteiden (kuten pöytäkoneiden ja kannettavien tietokoneiden) käyttöönottoa. Autopilotin avulla IT-osastot voivat automatisoida monia perinteisiä käyttöönottoon liittyviä tehtäviä, minkä ansiosta heille vapautuu enemmän aikaa muihin tehtäviin. (Wego)

Kun Autopilot on käytössä ja käyttäjä kirjautuu laitteeseen, laite liitetään automaattisesti Intunen hallintaan. Tämä tarkoittaa, että laitteen asetuksia, sovelluksia ja muita ominaisuuksia voidaan hallita etäyhteyden kautta, mikä voi merkittävästi helpottaa laitteen ylläpitoa ja turvallisuutta.

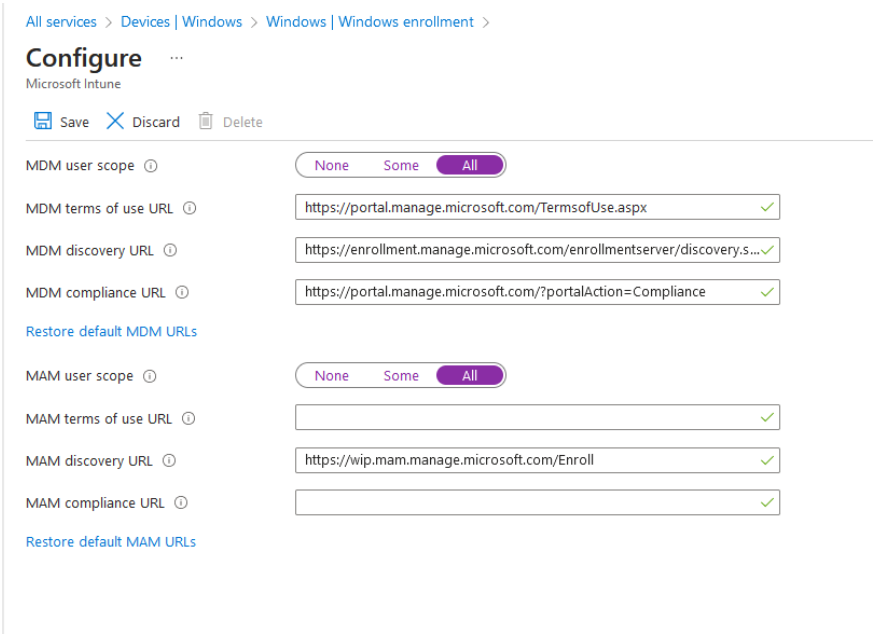
Autopilotin käyttöönotto aloitetaan menemällä Microsoft Intune -hallintakeskukseen. Siellä tulee ensin siirtyä "Devices" (Laitteet) -osioon ja etsiä sieltä "Windows". (Kuva 7). Tämän jälkeen valitaan "Windows Enrollment" (Windows-rekisteröinti), joka avaa useita erilaisia vaihtoehtoja. Tässä vaiheessa valitaan "Automatic Enrollment" (Automaattinen rekisteröinti), mikä käynnistää Autopilotin käyttöönoton.

Kun Autopilot on otettu käyttöön, IT-osasto voi määrittää useita erilaisia politiikkoja ja asetuksia, jotka koskevat laitteen käyttöönottoa ja hallintaa. Tämä voi sisältää esimerkiksi käyttäjäprofiilit, asennettavat sovellukset, päivitykset, turva-asetukset ja paljon muuta. Kaikki nämä asetukset voidaan määrittää keskitetysti ja niitä voidaan soveltaa automaattisesti kaikkiin organisaation laitteisiin, mikä tekee laitteiden hallinnasta paljon helpompaa ja tehokkaampaa.



Kuva 11. Autopilot MDM & MAM asetukset.

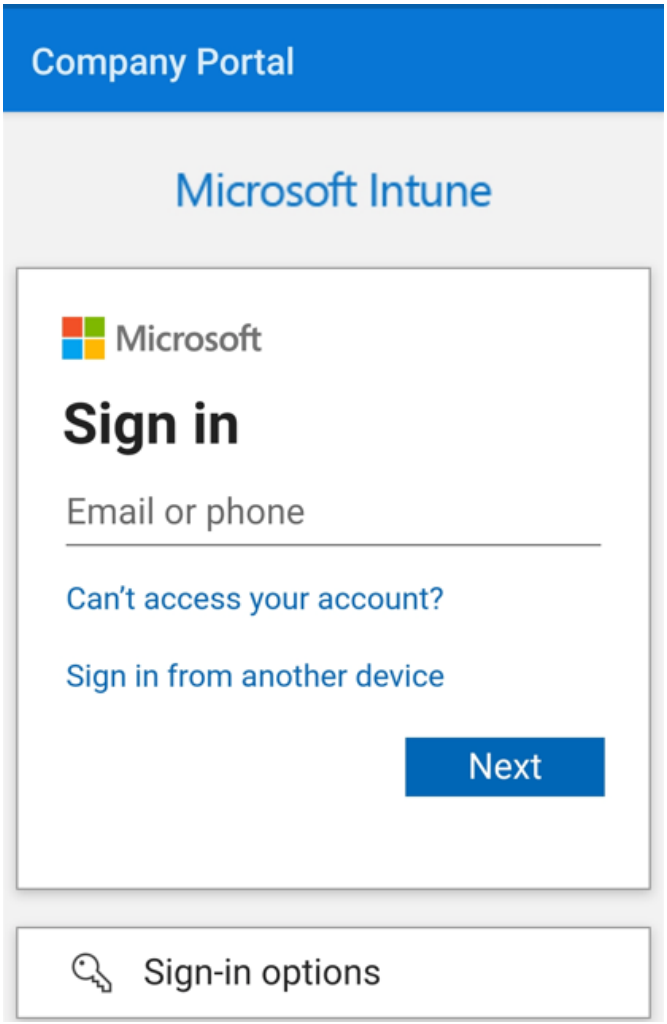
Ensimmäisenä kun ollaan ottamassa käyttöön autopilottia, niin otetaan MDM (Mobile Device Management) ja MAM (Mobile Application Management) käyttöön.



Kuva 12. MDM asetukset otettu käyttöön.

Tässä ohjeessa on otettu kaikki ehdotetut asetukset käyttöön autopilotissa. (Kuva 9)

3.2.2 Yritysportaali



Kuva 13. Yritysportaalin sovellukseen kirjautuminen.

Microsoft Intunen yritysportaali on erittäin tehokas työkalu, joka auttaa organisaatiota hallitsemaan työntekijöidensä laitteita ja sovelluksia, parantamaan tietoturvaa ja lisäämään tuottavuutta. Yritysportaali toimii sekä web-selaimessa, (Microsoft 2023. Using the Intune Company Portal website.) että mobiilisovelluksena, joten se on helposti saavutettavissa missä tahansa ja millä tahansa laitteella. (Microsoft 2023. Get the Intune Company Portal app.)

Yritysportaali tarjoaa monia käyttäjäystävällisiä ominaisuuksia, jotka tekevät laitteen ja sovellusten hallinnasta helppoa sekä IT-henkilöstölle että työntekijöille.

Yritysportaali mahdollistaa sovellusten asentamisen, päivittämisen ja hallinnan etänä. IT-henkilöstö voi jakaa sovelluksia työntekijöille yritysportaalin kautta, ja työntekijät voivat ladata ne suoraan laitteilleen. Tämä vähentää IT-tuen tarvetta ja tekee sovellusten käyttöönotosta nopeaa ja helppoa. (Techtarget. Compare capabilities of Office 365 MDM vs. Intune 2023.)

Yritysportaalissa työntekijät voivat rekisteröidä omat laitteensa (Lynnschools. How to Enroll the Device Using Intune Company Portal.) (BYOD, Bring Your Own Device) tai yrityksen laitteet. IT-henkilöstö voi sitten hallita laitteita etänä, määrittää turvallisuuskäytäntöjä, seurata laitteiden tilaa ja suorittaa tarvittaessa etätoimenpiteitä, kuten laitteen lukitseminen tai pyyhkiminen.

Intunen yritysportaali tukee useita turvallisuusominaisuuksia, kuten laitteiden salausta, salasanasuojauksia ja sovellusten tietosuojakäytäntöjä. Yritysportaali myös varmistaa, että yrityksen tiedot pysyvät erillään henkilökohtaisista tiedoista laitteissa, mikä on erittäin tärkeää BYOD-strategioissa. (Microsoft 2023. App protection policies overview 2023.)

Yritysportaali tarjoaa myös itsepalveluominaisuuksia, jotka lisäävät työntekijöiden tuottavuutta ja vähentävät IT-tuen tarvetta. Esimerkiksi, työntekijät voivat resetoida salasanoja, etsiä kadonneita laitteita, asentaa yrityksen hyväksymiä sovelluksia ja päivittää laiteasetuksia. (Medium. Microsoft Intune: Windows Company Portal App 2018.)

Intunen yritysportaalin käyttöönotto ja käyttö vaatii suunnittelua, määrittämistä ja ylläpitoa. On tärkeää, että IT-henkilöstö on koulutettu ja osaa hyödyntää Intunen yritysportaalin ominaisuuksia parhaalla mahdollisella tavalla.

4 Pohdinta

4.1 Pohdinta

Tässä opinnäytetyössä saavutetut tulokset ovat antaneet pintaraapaisun Intunen käyttöönotto prosessiin. On havaittu, että organisaatioiden suurimmat haasteet liittyvät usein tekniseen osaamiseen, resurssienhallintaan ja organisaatiokulttuuriin. Kuten teoriaosuudessa mainittiin, käyttöönoton sujuvuus riippuu merkittävästi näistä tekijöistä.

Organisaation kyky suunnitella ja toteuttaa Intunen käyttöönotto vaikuttaa merkittävästi prosessin tehokkuuteen. Se korostaa myös sitä, että asianmukainen koulutus ja tuki ovat avainasemassa henkilöstön omaksumisessa ja uuden teknologian käytön tehokkuudessa.

4.2 Johtopäätökset

Tämän opinnäytetyön perusteella on selvää, että Intunen käyttöönotto prosessi on monimutkainen hanke, joka vaatii huolellista suunnittelua, resurssien hallintaa ja laajaa teknistä tietämystä. Kuitenkin, kun nämä haasteet tunnistetaan ja niihin puututaan ajoissa, prosessi voi olla suhteellisen sujuva ja johtaa merkittäviin hyötyihin organisaatiolle.

Jatkossa suosittelen, että organisaatiot investoivat asianmukaiseen koulutukseen ja tukivälineisiin ennen Intunen käyttöönottoa. Tämä voisi sisältää esimerkiksi työpajoja, verkkokoulutusta tai konsultointia. Lisäksi organisaation johtoryhmän sitoutuminen on välttämätöntä prosessin onnistumisen kannalta.

Lopuksi tämän opinnäytetyön tulosten perusteella ehdotan, että jatkotutkimuksia tehtäisiin erityisesti Intunen vaikutuksista organisaatiokulttuuriin. Tämä opinnäytetyö on osoittanut, että tämä tekijä on olennainen, mutta se on vielä suhteellisen tutkimaton alue. Lisätietojen saaminen tästä näkökulmasta voisi antaa

arvokkaita oivalluksia siitä, kuinka teknologian käyttöönottoa voidaan parantaa ja tehostaa entisestään.

Lähteet

Accenture. Cloud Computing. Viitattu 17.7.2023. https://www.accenture.com/cz-en/cloud/insights/cloud-computing-index

Azure. Scaling up vs. scaling out. Viitattu 17.7.2023. https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/scaling-out-vs-scaling-up/#overview

Business Insider 2021. Why companies are flocking to the cloud more than ever. Viitattu 17.7.2023. https://www.businessinsider.com/cloud-technology-trend-software-enterprise-2021-2?r=US&IR=T

Cisco, What Is a Virtual Private Network (VPN). Viitattu 17.7.2023. https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html

Lounea Oy, Lounea Oy:n nettisivut. Viitattu 11.7.2023. https://lounea.fi/lounea/tietoa-louneasta

Lynnschools. How to Enroll the Device Using InTune Company Portal. Viitattu 17.7.2023. https://www.lynnschools.org/reopening_safely/documents/lps_ipad_enroll_using_intune_company_portal_en.pdf

Medium. Microsoft Intune: Windows Company Portal App 2018. Viitattu 17.7.2023. https://scottduf.medium.com/microsoft-intune-windows-company-portal-app-yes-you-should-be-deploying-it-a56c2ff5305b

Microsoft EMS, What is Microsoft EMS. Viitattu 15.7.2023. https://www.encore-business.com/blog/what-is-microsoft-ems/

Microsoft 2016. Enterprise Mobility with App Management, Office 365, and Threat Mitigation: Beyond BYOD. Viitattu 15.7.2023. https://books.google.fi/books?hl=fi&lr=&id=gi1fCwAAQBAJ&oi=fnd&pg=PT14

Microsoft 2023. Using the Intune Company Portal website. Viitattu 17.7.2023. https://learn.microsoft.com/fi-fi/mem/intune/user-help/using-the-intune-company-portal-website

Microsoft 2023. Get the Intune Company Portal app. Viitattu 17.7.2023. https://learn.microsoft.com/fi-fi/mem/intune/user-help/sign-in-to-the-company-portal

Microsoft 2023. App protection policies overview 2023. Viitattu 17.7.2023. https://learn.microsoft.com/en-us/mem/intune/apps/app-protection-policy

Microsoft 2023. Azure Active Directory is becoming Microsoft Entra ID. Viitattu 20.7.2023. https://www.microsoft.com/en-us/security/business/identity-access/azure-active-directory?rtc=1

Microsoft 2023. Multifactor authentication in Azure AD. Viitattu 21.7.2023. https://www.microsoft.com/en-us/security/business/identity-access/azure-active-directory-mfa-multi-factor-authentication

Montra. Benefits of Microsoft 365 and Azure Active Directory for Identity Management 2022. Viitattu 20.7.2023. https://montra.io/benefits-of-microsoft-365-and-azure-active-directory-for-identity-management/

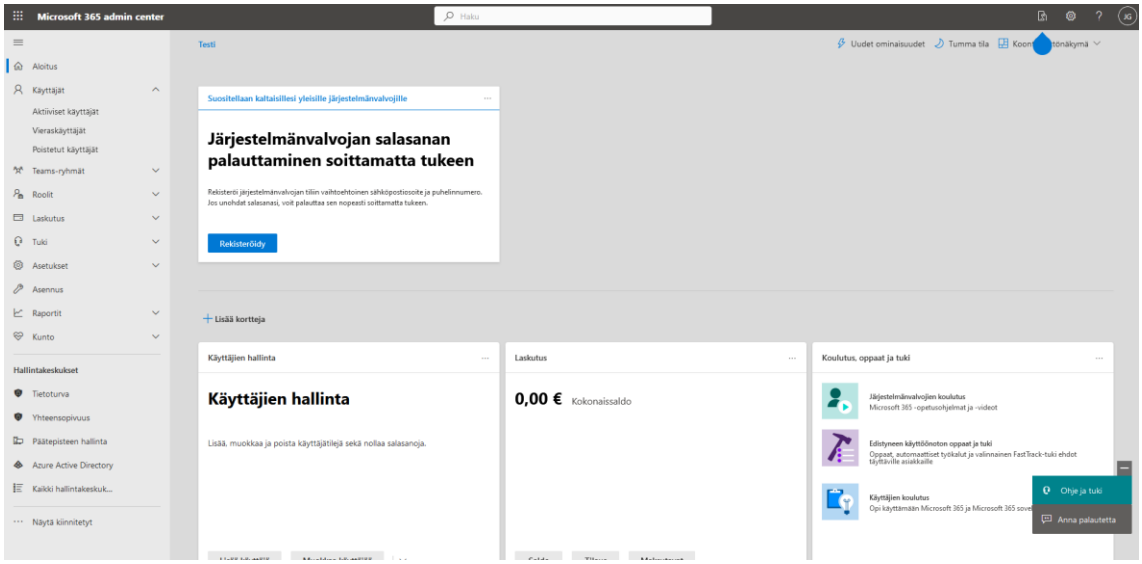
Ookla® Speedtest® analysoi: Lounea Valokuitu on Suomen nopein netti 2023. Viitattu 11.7.2023. https://lounea.fi/ooklar-speedtestr-analysoi-lounea-valokuitu-suomen-nopein-netti

Techtarget. Compare capabilities of Office 365 MDM vs. Intune 2023. Viitattu 17.7.2023. https://www.techtarget.com/searchenterprisedesktop/tip/Compare-capabilities-of-Office-365-MDM-vs-Intune

Wego, Windows Autopilot. Viitattu 17.7.2023. https://wegogroup.fi/palvelut/microsoft-autopilot-ja-intune/

Liitteet

Liite 1

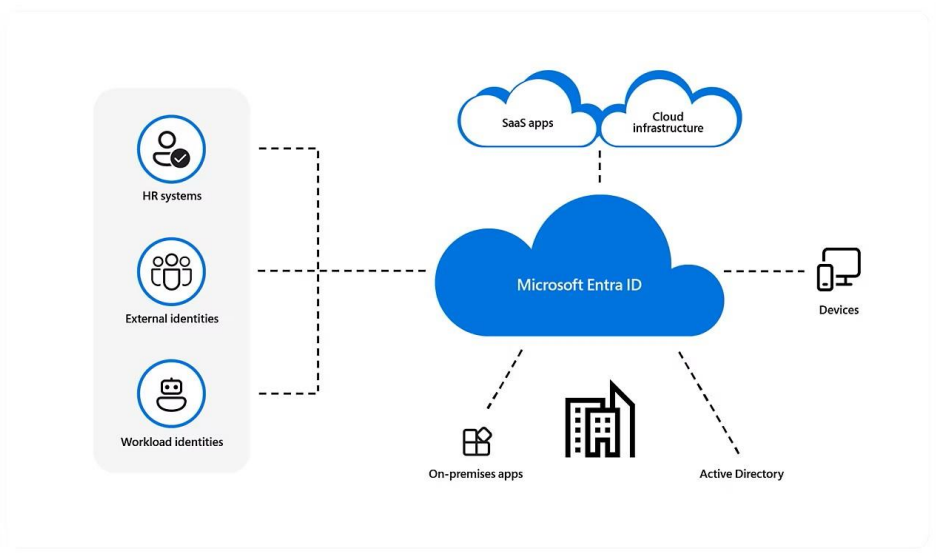


Microsoft Azure Admin Center: Etusivu

Liite 2

Microsoft Azure Security.

Liite 3

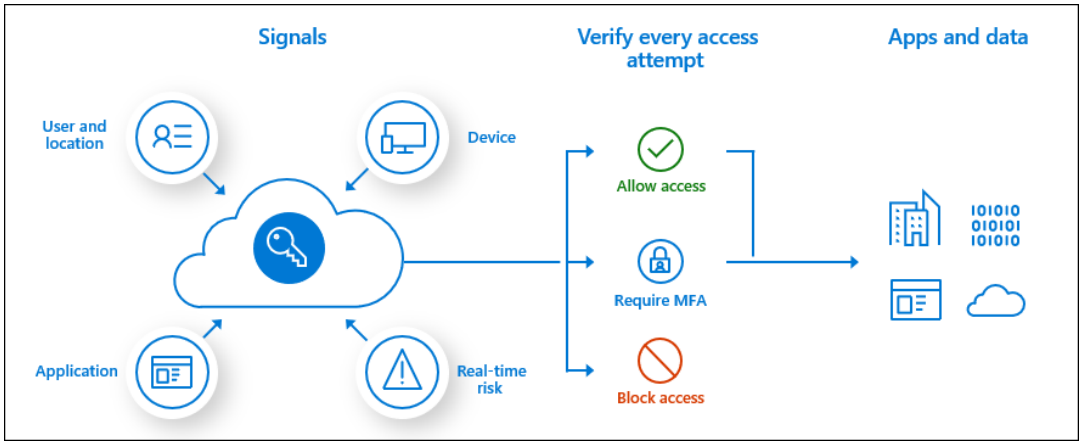


Microsoft Entra ID diagrammi.

Liite 4

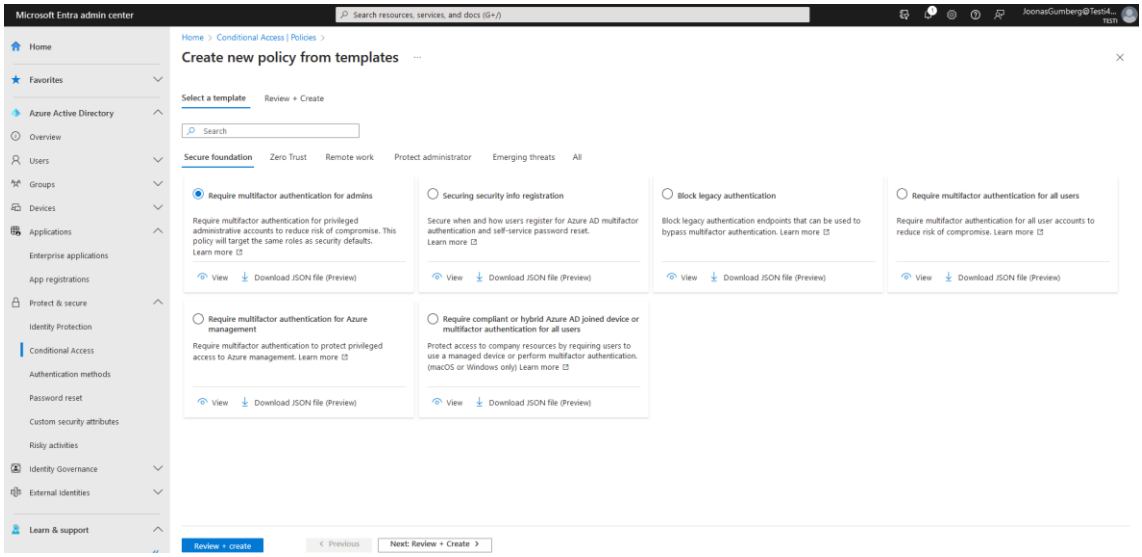
Monivaiheinen todennus esimerkki.

Liite 5



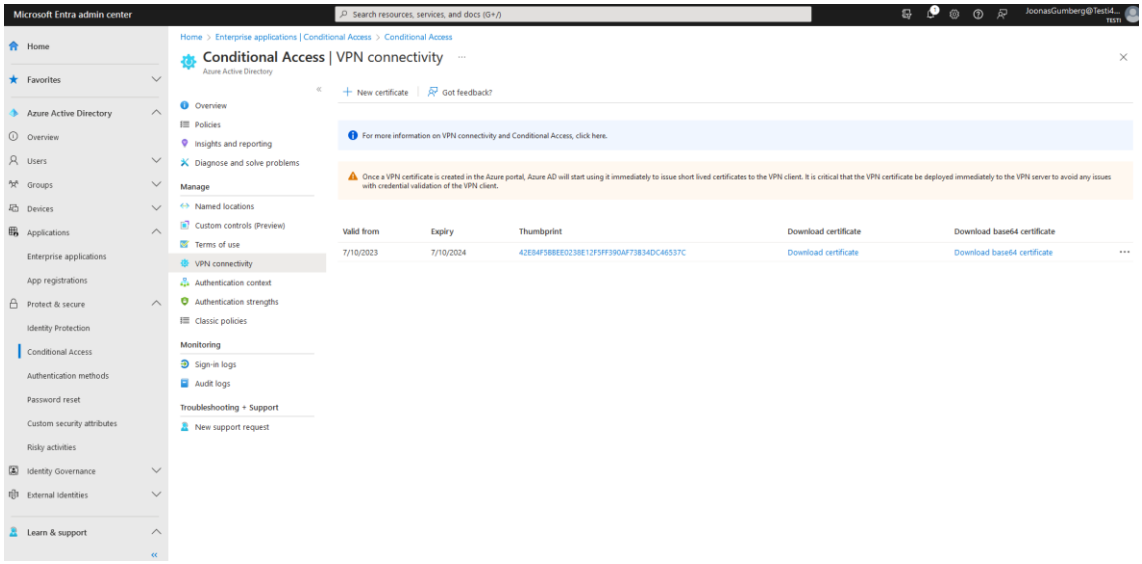
Havainollistava kuva MFA:sta.

Liite 6



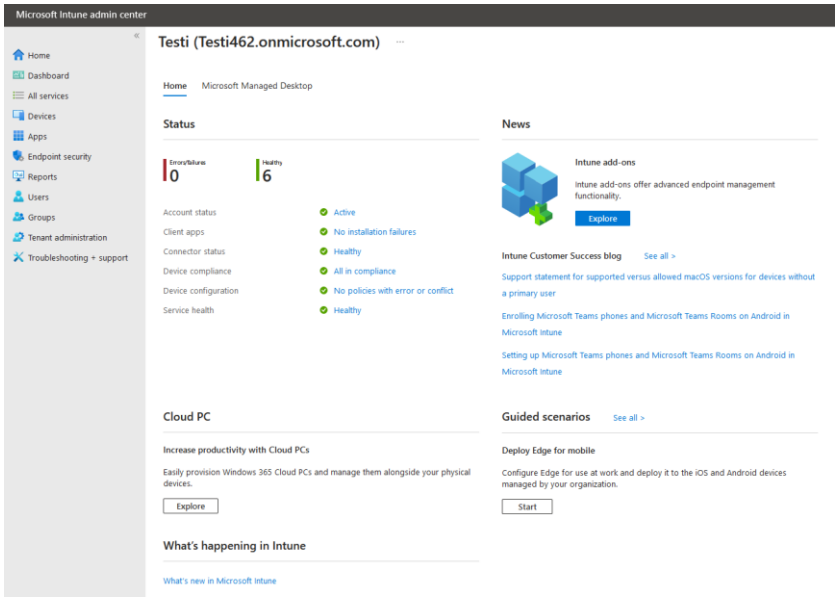
Politiikat, eli käytäntö asetukset.

Liite 7



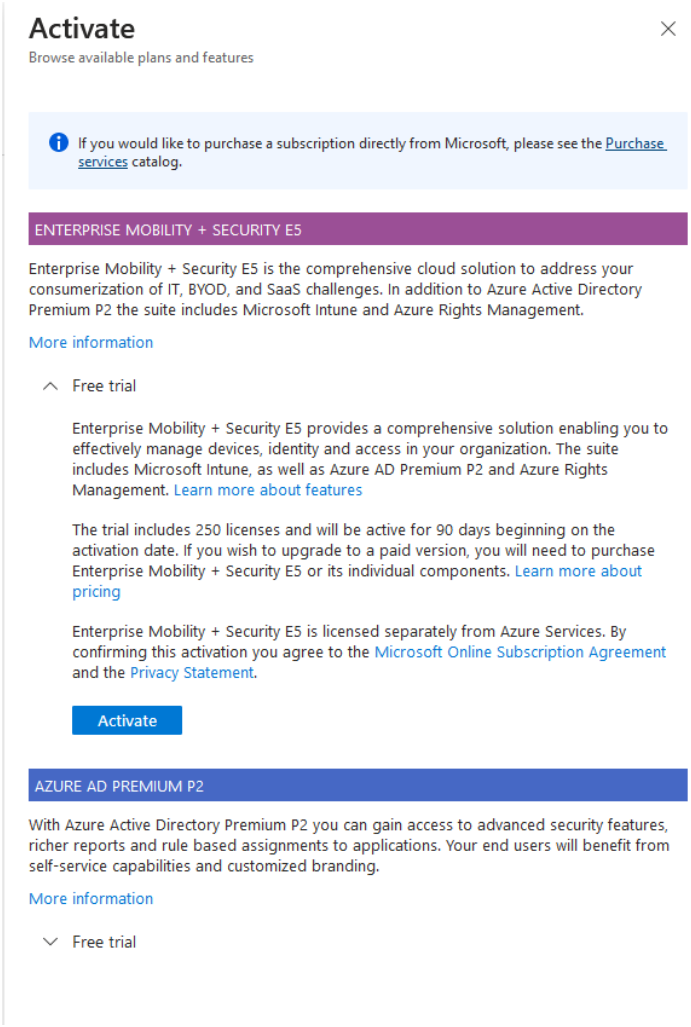
VPN sertifikaatti hankittuna.

Liite 8



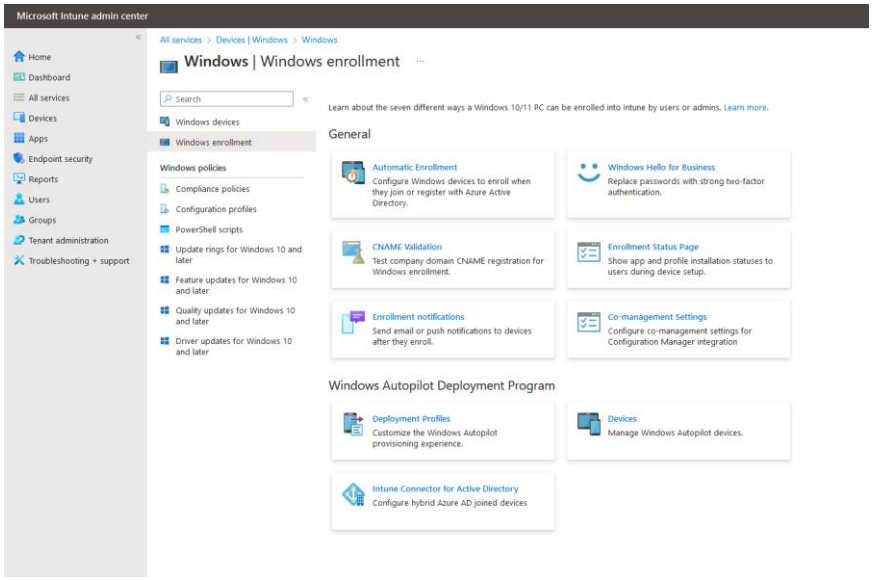
Intune Admin Center hallinta etusivu.

Liite 9



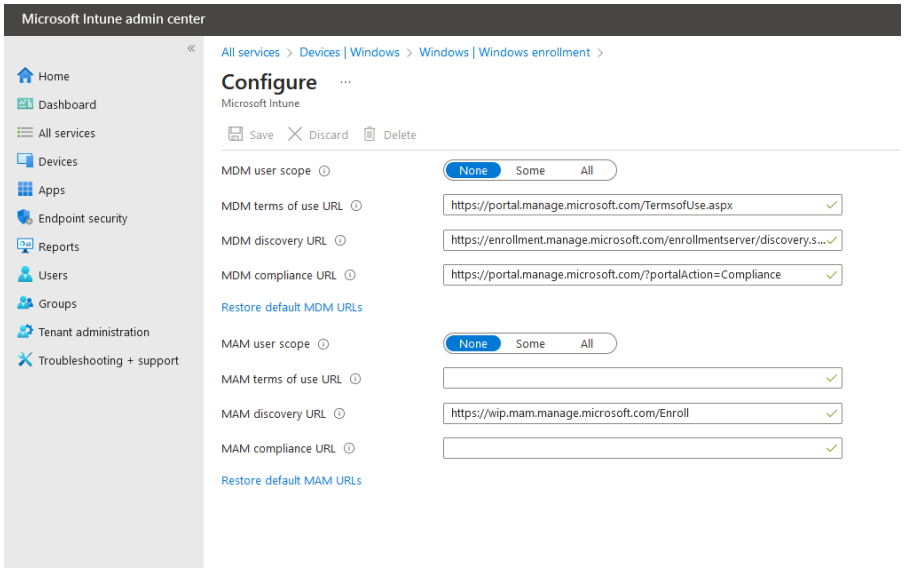
Intunen aktivointi lisenssi.

Liite 10



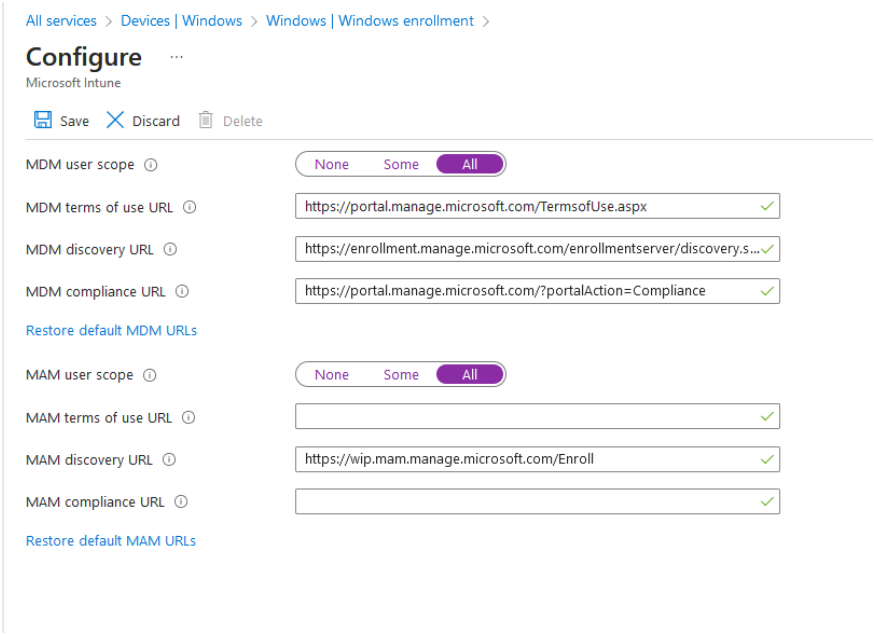
Autopilot käyttöönotto.

Liite 11



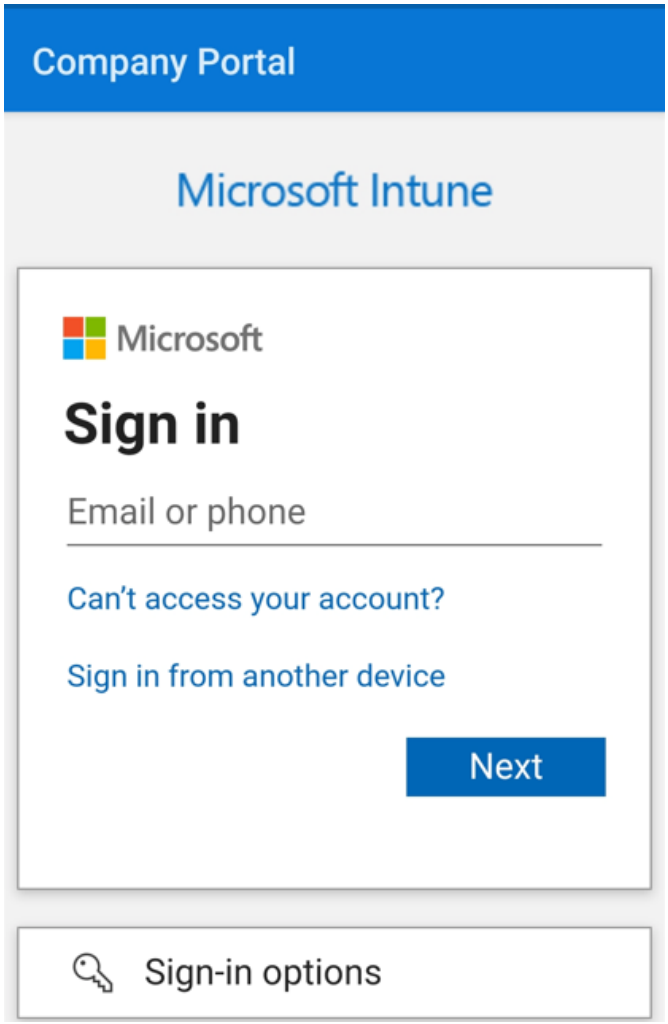
Autopilot MDM & MAM asetukset.

Liite 12



MDM asetukset otettu käyttöön.

Liite 13



Yritysportaalin sovellukseen kirjautuminen.