Joona Salven

Kannettavien tietokoneiden keskitetty hallinta laitehallintapalvelun avulla

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tieto- ja viestintätekniikan tutkinto-ohjelma

Insinöörityö

16.11.2022

Tiivistelmä

Tekijä:	Joona Salven
Otsikko:	Kannettavien tietokoneiden keskitetty hallinta laitehallinta-palvelun avulla
Sivumäärä:	46 sivua + 1 liite
Aika:	16.11.2022
Tutkinto:	Insinööri (AMK)
Tutkinto-ohjelma:	Tieto- ja viestintätekniikka
Ammatillinen pääaine:	Mediatekniikka
Ohjaajat:	Lehtori Toni Spännäri IT-turvapäällikkö Matti Saarelainen

---

Insinöörityön tavoitteena oli toimeksiantaneen yrityksen macOS-tietokoneiden keskitetty hallinta ja nollakosketusjakelu Microsoft Intune -palvelua apuna käyttäen. Microsoft Intune on pilvipohjainen päätelaitteiden hallintatyökalu, joka on osa Microsoft Endpoint Management -kokonaisuutta. Se tarjoaa organisaatioille yhtenäistetyn ja osittain automatisoidun laitteiden, sovellusten ja käyttäjätilien hallinnan, seuraamisen ja turvaamisen.

Työssä perehdyttiin yrityksen macOS-tietokoneiden hallinnan ja Apple Automated Device Enrollment -rekisteröinnin kannalta olennaisiin Apple Business Manager- ja Microsoft Endpoint Management -ympäristöihin ja tarvittaviin lisensseihin. Työ toteutettiin yrityksen IT-osaston vetäjän valvonnassa. Lisäksi selvitettiin laitekäyttäjäyhteyden vaikutuksia laitejakeluun erityisesti Google-identiteettiä käytettäessä Microsoft-tileille kirjauduttaessa.

Toteutuksessa rakennettiin ympäristöjen konfiguraatioita ja esimäärityksiä Automated Device Enrollment- ja Company Portal -rekisteröinnin mahdollistamiseksi. Laitteiden käyttöönoton automatisoimiseksi Intune-ympäristöön ja Azure Active Directory -ryhmiin määriteltiin jaettavat konfiguraatioprofiilit, sovellukset ja automaatioskriptit. Näiden määritysten jälkeen macOS-tietokoneiden automaattinen käyttöönotto Intune-hallinnan kautta oli mahdollista.

Lopputuloksena saatiin tuotantoon valmis Intune-hallintakokonaisuus, jossa macOS-laitteita voidaan hallita keskitetysti ja laitteiden käyttöönottoprosessi on automatisoitu saattamaan laitteet yrityksen määrittelemään oletuskäyttötilaan, jossa laitteilla on käytössä tietoturvan ja työnteon kannalta olennaiset ominaisuudet. Intune-palvelua on yrityksen tarpeiden perusteella mahdollista jatkokehittää esimerkiksi Windows-laitteiden hallintaan.

Avainsanat: Microsoft Intune, keskitetty laitehallinta, macOS

Abstract

Author:	Joona Salven
Title:	Centralized management of laptop computers using a device management service
Number of Pages:	46 pages + 1 appendix
Date:	16 November 2022
Degree:	Bachelor of Engineering
Degree Programme:	Information and Communications Technology
Professional Major:	Media Technology
Supervisors:	Toni Spännäri, Senior Lecturer Matti Saarelainen, IT Security Manager

---

The goal of this engineering thesis was the centralized management and zero-touch distribution of the commissioning company's macOS laptops using the Microsoft Intune service. Microsoft Intune is a cloud-based endpoint management tool that is part of Microsoft Endpoint Management. It offers organizations unified and partially automated management, tracking and securing of devices, applications, and user accounts.

The work was done with the company's IT team leader's supervision. It concentrated on Apple Business Manager and Microsoft Endpoint Manager environments as well as their necessary licenses, which all are essential for the management of macOS laptops and the usage of Apple Automated Device Enrollment. Also, the effects of using user affinity during device distribution were investigated, especially in the case of signing into a Microsoft account using Google as an identity provider.

The implementation uses configurations and presets to enable ADE and Company Portal enrollment. To automate the setup of devices - distributable configuration profiles, applications and automation scripts were defined into the Intune environment and Azure Active Directory -based groups. As a consequence, the automated enrollment of macOS laptops through Intune was possible.

The result of this study was a production-ready Intune management entity where macOS devices can be managed centrally and the device setup process is automated to bring the devices to the default use state defined by the company, where the devices have essential features for security and work. Based on the company's needs, it is possible to further develop the Intune service, for example, to manage Windows devices.

Keywords: Microsoft Intune, Mobile Device Management, macOS

Sisällys

Lyhenteet ja käsitteet

1 Johdanto 1

2 Laitteiden keskitetty hallinta 3

3 Työn tavoitteet 7

4 Yrityksen keskitetyn hallinnan ympäristöt 10

4.1 Apple-ympäristö 11
4.2 Microsoft-ympäristö 14
4.3 Google SSO -todennus ja M365 autoprovisioning -käyttäjäpääsy 17

5 Yrityksen keskitetyn hallinnan käyttöönotto 20

5.1 Apple Business Manager -laiterekisteröinti 21
5.2 Intune-ympäristön esimääritykset 22
5.3 Intune-rekisteröinnin määrittely 25
5.4 Konfiguraatioprofiilit 28
5.5 Sovellushallinta ja -jakelu 31
5.6 macOS-laitejakelu Intune-palvelimelta 37

6 Tulokset ja pohdinta 39

7 Yhteenveto 41

Lähteet 42

Liitteet

Liite 1: WithSecure-Bash-skripti

Lyhenteet ja käsitteet

AD: *Active Directory*. Microsoftin kehittämä hakemistopalvelu ja tietokanta käyttäjä-, laite- ja verkkoresursseille. Myöhemmin siitä on tullut yleispätevä termi hakemistopohjaisille palveluille.

ADE: *Automated Device Enrollment*. Apple-yrityksen tarjoama laitteiden automaattinen rekisteröintiprosessi macOS- ja iOS-laitteille, jolla laitteet määritellään yrityksen omistukseen.

BYOD: *Bring your own device*. Termi viittaa siihen, että henkilö saa käyttää henkilökohtaista laitettaan organisaatiossa sen sijaan, että häntä vaadittaisiin käyttämään esimerkiksi yrityksen tarjoamaa laitetta.

Enrollment: Jonkin asian ilmoittamista tai rekisteröimistä osaksi jotakin listaa tai ryhmää. Esimerkiksi kannettava tietokone voidaan ilmoittaa osaksi yrityksen laitehallintaa kolmannen osapuolen palvelussa.

Affiniteetti: Tämän työn kontekstissa affiniteetti tarkoittaa yhteyttä. Käyttäjäaffiniteetti tarkoittaa käyttäjän yhteyttä johonkin, esimerkiksi laitteeseen.

LOB: *Line-of-Business application*. Ohjelmistosovellukset, joita käytetään ryhmän, osaston, yrityksen tai toimialan ainutlaatuisten vaatimusten täyttämiseen.

MAM: *Intune Mobile Application Management*. MAM-termillä tarkoitetaan Intune-hallintaominaisuuksia, joiden avulla voidaan julkaista, viedä, määritellä, valvoa, suojata ja ylläpitää mobiilisovelluksia.

MDM: *Mobile Device Management*. Mobiililaitteiden, kuten älypuhelimien ja kannettavien tietokoneiden hallinta ja käyttöönotto.

MEM: *Microsoft Endpoint Management*. Pilvipohjainen kokonaisuus, joka on suunniteltu yritysten laitteiden jakeluun, hallintaan ja turvaamiseen. Se koostuu muun muassa Intune- ja Azure AD -palveluista, sekä MEM-portaalista.

MFA: *Multi Factor Authentication*. Monimenetelmäinen todentaminen on sähköinen todennusmenetelmä, jossa käyttäjälle myönnetään pääsy palveluun vasta sen jälkeen, kun hän on onnistuneesti todentanut henkilöllisyytensä vähintään kahdella tapaa, esimerkiksi salasanalla ja tekstiviestillä.

Token: Token on varmenne, joka ohjelmisto- ja laitteistotapauksessa edustaa oikeutta suorittaa jokin toimenpide.

1 Johdanto

Insinöörityön tarkoituksena oli automatisoida mahdollisimman monta työn tilaajayrityksen laitteen käyttöönoton vaihetta sekä mahdollistaa laitteiden etähallinta ja tilan seuranta yhdestä keskitetystä palvelusta. Automatisoimalla laitteen käyttöönotto vältyttäisiin monilta potentiaalisilta ongelma- ja virhetilanteilta, pienennettäisiin yrityksen IT-osaston työtaakkaa vähentämällä manuaalisia asennuksia sekä varmistuttaisiin siitä, että laitteiden käyttöönotto on tapahtunut IT-osaston asettamin ehdoin. Työssä selvitettiin palvelun sopivuutta yrityksen käyttötarkoituksiin sekä sen yleistä soveltuvuutta MacBook macOS -laiterekisteröintiin ja -hallintaan.

Insinöörityö toteutettiin yhteistyössä Nordhealth Oy:n IT-osaston kanssa, ja kyseessä oli toiminnallinen insinöörityö. Nordhealth on pohjoismainen kasvava terveysalan ohjelmistoyritys, joka työllistää yli 350 työntekijää ympäri maailman. Nordhealth on toiminut vuodesta 2001 lähtien ja on tällä hetkellä Pohjoismaiden johtava terveysalan ohjelmistopalveluiden tarjoaja. (1.)

Insinöörityön aihe syntyi aloitettuani työskentelyn Nordhealth Oy:ssä vuoden 2021 kesällä. Työnkuvaan kuului muun muassa työntekijöiden laitteiden tilaaminen ja valmistelu käyttäjille sekä tuen antaminen ongelmatilanteissa. Yrityksen kovan kasvun vuoksi aikaisemmin käsin tehtyyn laitehallintaan meni kasvavissa määrin enemmän aikaa ja muita resursseja, minkä vuoksi esimieheni ehdotti insinöörityön aiheeksi macOS-laitteiden nollakosketuskäyttöönoton ja hallinnan. Projektin myötä sain työni kannalta tarvittavaa kokemusta Mobile Device Management -palveluista ja -ympäristöistä ja sain laajennettua osaamistani macOS-käyttöjärjestelmästä ja sitä ympäröivistä teknologioista.

Projektin Mobile Device Management -palveluksi valikoitui Microsoft Intune -palvelu, sillä yrityksellä on entuudestaan käytössä muita Microsoft-palveluita ja se on yhteensopiva yrityksen muiden resurssien kanssa. Koska yrityksessä on käytössä paljon Microsoftin tuotteita, kuten Microsoft Office 365 -tuoteperhe ja Power BI, laitehallinnan yhdistäminen Microsoft-tilien yhteyteen yksinkertaistaisi

hallintaa organisaation IT-osaston kannalta. Iso vaikuttava tekijä päätöksessä oli macOS-laitteiden tuen viimeaikainen laajeneminen tarpeeksi kattavaksi ja monipuoliseksi. Tulevaisuutta ajatellen Intune olisi myös suuri etu yhtiön Windows-laitteiden Mobile Device Management -hallintaa ja jakelua varten, jota alettaisiin työstämään macOS-implementaation jälkeen.

2 Laitteiden keskitetty hallinta

Mobiililaitteiden suosio yritysmaailmassa aloitti kasvunsa 2000-luvun alussa laajentuneen saatavuuden myötä ja on jatkanut tasaista kasvuaan siitä asti. Mobiililaitteista on tullut integraalinen osa nykypäivän työnkuvaa, mutta ilman hallintaa niistä voi vastaavasti olla haittaa yrityksille ja sen käyttäjille. Standardisoidun hallinnan puute voi johtaa pahimmissa tapauksissa muun muassa turvallisuusriskeihin ja haavoittuvuuksiin esimerkiksi vanhentuneiden ja riskialttiiden ohjelmistojen sekä riittämättömän laitesalauksen vuoksi. Tästä huolimatta ensimmäiset kaupalliset mobiililaitteiden hallintajärjestelmät tulivat markkinoille vasta 2010-luvun tuntumassa. (2; 3.)

Mobile Device Management

Mobile Device Management, MDM, on laitteiden keskitetyn hallinnan muoto, joka viittaa mobiilipäätelaitteiden, kuten älypuhelimien, kannettavien tietokoneiden ja tablettien hallintaan. MDM on osa laajempaa kokonaisuutta nimeltä Enterprise Mobility Management, joka taas puolestaan tarkoittaa koko mobiililaitteiden elämänkaaren hallintaa työpaikalla. Pohjimmiltaan MDM on siis laitteiden valvomista, hallitsemista ja turvaamista ja näin ollen olennainen osa yrityksen tietoturvaa. MDM säännöstelee mobiililaitteita ja turvaa organisaation resursseja käyttämällä ohjelmistoa, konfiguraatioita ja käytänteitä. Hallinta suoritetaan usein kolmannen osapuolen ratkaisuilla, joissa palvelimen ajoon on kaksi yleistä vaihtoehtoa: paikallisesti tai pilvessä. Näistä edullisempi ja pienemmän kynnyksen vaihtoehto keskikokoisille yrityksille on käyttää pilvipalvelua jonkin palveluntarjoajan ympäristössä. (2; 3.)

Hallittava laite voi olla yrityksen käyttäjälle luovuttama työkäyttöön tarkoitettu laite tai käyttäjän omistama laite, joka on jälkikäteen yhdistetty palveluun. Käyttäjien omista laitteista käytetään nimitystä BYOD eli bring your own device. MDM mahdollistaa BYOD-laitteilla yrityksen ja käyttäjän persoonallisen datan ja tilien erittelyn roolipohjaisella pääsyllä, mikä on erityisen hyödyllistä esimerkiksi kouluissa. MDM:n avulla esimääritelty käyttäjälle rekisteröity laite voidaan

varustaa tietoturvan kannalta välttämättömillä konfiguraatioilla ja ohjelmistoilla, joita hallitsemalla parannetaan tietoturvaa entisestään esimerkiksi vaaratilanteissa, jolloin viimeisenä vaihtoehtona koko laite voidaan pyyhkiä tyhjäksi. (4.)

Ennen hallintaa tulee laitteet kuitenkin rekisteröidä MDM-palvelimelle (2; 3). Tähän käytetään myyjäkohtaisia rekisteröintipalveluita, kuten esimerkiksi tässä projektissa käytetty Apple Automated Device Enrollment (ADE). ADE-palvelu rekisteröi valtuutetulta jälleenmyyjältä hankitut laitteet automaattisesti suoraan yrityksen Apple Business -ympäristöön, josta niille voidaan määritellä MDM-palvelin (5, s. 1). Enrollment vuorostaan tarkoittaa laitteen ilmoittamista tai rekisteröimistä osaksi jotakin palvelua tai listaa. ADE-rekisteröinti on erityisen hyödyllinen yrityksille, sillä laitteen ei tarvitse missään välissä käydä yrityksen IT-osaston kautta esiasennettavana, vaan rekisteröity laite voi hakea tarvittavat resurssit suoraan verkon ylitse MDM-palvelimelta käyttöönoton yhteydessä (6). Vaihtoehtoisesti laiterekisteröinti Apple Business Manager (ABM) -palveluun voidaan suorittaa myös jälkikäteen yrityksen IT-osaston toimesta käyttämällä Apple Configurator -sovellusta, jos yhteensopiva laite on hankittu esimerkiksi jälleenmyyjältä, joka ei tarjoa ADE-palvelua. (7.)

Mobile Application Management (MAM) vuorostaan on hallintatoiminto, jolla voidaan julkaista, viedä, määritellä, valvoa, suojata ja ylläpitää mobiilisovelluksia yrityksen käyttäjiä varten. MAM siis mahdollistaa yrityksen järjestelmänvalvojille hienovaraisemman hallintamahdollisuuden sovellusten koko elinkaaren ajalta. Joissain tapauksissa voidaan jopa hallita muuttujia sovellustasolla ja esimerkiksi Intune mahdollistaa Microsoft Office -tuotteiden hallinnan. (8.)

Keskitetyn hallinnan tietoturva

Covid-19-pandemian jäljiltä on ympäri maailman siirrytty entuudestaan kiihtyvää vauhtia etätyöhön, ja monelle organisaatiolle sekä työntekijälle tämä saattaa olla pysyvä ratkaisu. Etätöiden yleistyessä on myös tietoturvariskien määrä ja muoto muuttunut merkittävästi (9). Nykyisessä etätyöympäristössä ei enää riitä, että yrityksen oma sisäinen tietoverkko on suojattu, sillä kasvavissa määrin

laitteita on sisäisen tietoverkon ulkopuolella käyttäjien etätoimistoissa ja esimerkiksi työmatkoilla. VPN-yhteyden käyttö kaiken datan tunneloimiseksi ei ole kestävä eikä tarpeeksi tietoturvallinen ratkaisu esimerkiksi kaistanleveysvaatimusten ja kannettavien tietokoneiden vuoksi, sillä ne ovat luonteeltaan jatkuvasti liikkeellä ja siksi iso riski esimerkiksi varkauden tai häviämisen myötä, jolloin laitteisiin on helpompi päästä fyysisesti käsiksi.

Suomen Kyberturvallisuuskeskus, joka on Liikenne- ja viestintäviraston alaisuudessa, listaa sivullaan työpaikan turvallisuuden kannalta oleelliset seikat: salasanat, tietoturvakäytännöt, tunnistautuminen, päivitykset, arkaluontoisen tiedon käsittely, häiriötilanteiden hallinta ja varmuuskopiot (10). Suurin osa näistä voidaan suojata keskitetyn laitehallinnan keinoin. Useimmat keskitetyn hallinnan pilvipalvelutarjoajat, kuten Microsoft Intune, tarjoavat laajan kirjon ratkaisuja yrityksen ja käyttäjien datan hallintaan ja turvaamiseen. Microsoft Intune on osa Microsoft Enterprise Mobility + Security -pakettia, jonka tärkein toiminto on juuri antaa organisaation järjestelmävalvojille työkalut laitehallintaan ja turvaamiseen. Keskeisimpänä tietoturvatoimintona Intune-hallinnassa on laitejakelurajoitusten käyttö hallintaa varten, laitteen vaatimustenmukaisuuskäytäntöjen noudattamisen valvominen, ehdollinen pääsy yrityksen dataan ja Mobile Application Management -toiminnon käyttö sitä tukevissa sovelluksissa. (11.)

MDM-laitejakelussa on mahdollista hyödyntää rajoituksia parempaa hallintaa varten. Laitteille voidaan siis asettaa vaatimuksia, jotka tulee täyttää, ennen kuin ne voidaan ilmoittaa MDM-palvelun hallintaan ja datan jakeluun. Tällä tavoin voidaan esimerkiksi rajoittaa ei-haluttujen laitteiden rekisteröiminen, kuten henkilökohtaiset kannettavat tietokoneet ja puhelimet tai liian vanhanaikaiset laitteet. Jakelun jälkeen voidaan hienosäädöksi lisätä laitteen vaatimustenmukaisuuskäytäntöjä, joihin kuuluvat esimerkiksi järjestelmä- ja sovellusversioiden minimivaatimukset. Näitä vaatimustenmukaisuuksia on usein mahdollista seurata MDM-portaalissa, joka helpottaa käyttäjien kanssa kommunikointia ja vaatimusten täyttämistä. Ehdollisella hallinnalla voidaan vieläkin tarkemmin rajoittaa pääsyjä laite tai- ja käyttäjäkohtaisesti. Microsoft Intunen vahva ehdollinen hallinta on mahdollista, sillä se keskustelee jatkuvasti Azure AD -tietokannan

kanssa, josta se saa tarpeellisia ominaisuustietoja muun muassa käyttäjästä ja laitteesta, ja niiden perusteella se voi rajoittaa pääsyä yrityksen tietoihin ja sovelluksiin. Tätä kautta on esimerkiksi mahdollista estää tiettyjen tietojen näkeminen yrityksen verkon ulkopuolella. Kaikki nämä ominaisuudet ovat monipuolisesti hallittavissa yrityksen järjestelmävalvojien toimesta, ja sääntöjä voidaan soveltaa käytännössä rajattomasti. Viimeisin hallinnan tietoturvakäytäntö on erillinen MAM-toiminto, joka on lisäulottuvuus MDM:n rinnalle. Sillä voidaan suojata yrityksen ja käyttäjän dataa sovellusten sisällä yrityksen omilla tai ulkoisilla laitteilla, eli se ei vaadi perinteistä MDM-laitehallintaa toimiakseen. Tämä perustuu sovellusten sisäisiin turvatoimiin, kuten tietojen salaukseen. (11.)

Valvonnan ja rajoitusten lisäksi tärkeä osa tietoturvallisuutta on käyttäjävirheiden minimointi. CompTIA:n hiljattain tekemässä tutkimuksessa ilmenee, että vain 30 % yrityksistä on huolissaan käyttäjävirheistä johtuvista ongelmista, huolimatta siitä, että 52 % tietoturvaloukkauksista tapahtuu inhimillisten virheiden vuoksi (12). On siis erittäin tärkeää pyrkiä minimoimaan näitä tapauksia, minkä vuoksi ratkaisuna ongelmaan saattaakin tietoturvakoulutuksen lisäksi olla käyttäjän roolin minimoiminen yhtälössä. Automatisoimalla mahdollisimman suuri osa laitejakeluvaiheesta sekä yritysdatapääsyn rajoittamisesta MDM-palvelua käyttäen voidaan varmistua siitä, että laitteet on otettu oikea oppisesti käyttöön ja niiden turvallisuusasetukset ja salaukset vastaavat IT-osaston asettamia vaatimuksia.

3 Työn tavoitteet

Insinöörityöprojektin tavoitteena on konfiguroida Nordhealth Oy:n Intune Mobile Device Management -palvelu, joka on osa Microsoft Endpoint Management -kokonaisuutta, käyttövalmiiksi macOS-laitteiden keskitettyä hallintaa ja jakelua varten. Tarkoituksena on viedä projekti tuotantoon asti, jolloin palveluun voidaan rekisteröidä yrityksen sekä uudet että entuudestaan käyttäjille jaetut macOS-laitteet. Palvelulla halutaan seurata laitteiden tilaa ja asettaa niille vaatimuksia sekä rajoitteita yrityksen tarpeiden ja tietoturvavaatimusten mukaisesti. Tarkoituksena on käyttää Intune-palvelua työn ja tietoturvan kannalta olennaisten sovellusten jakeluun sekä laitteiden asetusten ja käytäntöjen automaattiseen pakottamiseen määritellyille laitteille.

Itse projektin toteutuksen lisäksi keskeinen osa työtä on macOS- ja MDM-osaamisen kartoitus ja laajentaminen. Läheinen työskentely kannettavien macOS-tietokoneiden ja niihin liittyvien teknologioiden kanssa toivottavasti syventää tekijän omaa osaamista, joka on projektin alussa erittäin pintapuolinen. Laajempi osaaminen tulee olemaan hyödyllinen toteutuksen jälkeen, kun tekijä jatkaa käyttäjä- ja laitehallintaroolissa työskentelyä ja ylläpitoa.

Työn keskeisin tavoite on automatisoida erinäiset vaiheet macOS-laitteiden käyttöönotossa niin, että tukkuliikkeestä tilattaessa laite ensin ADE-rekisteröidään yritykselle, minkä jälkeen laite voidaan toimittaa suoraan käyttäjälle ilman, että yrityksen IT-osasto ensin rekisteröi ja asentaa laitteen. Näin vältytään potentiaalisilta käyttäjävirheiltä asennuksen aikana ja vähennetään IT-osaston työmäärää. Laitteen rekisteröinnissä käytetään Applen tarjoamaa Automatic Device Enrollment -prosessia, joka mahdollistaa laiterekisteröinnin yrityksen alle Apple Business Management -portaaliin. ABM-portaalista laitteet voidaan jatkotoimenpiteenä määrittää Intune MDM -palvelun piiriin. Kuitenkin tilanteissa, joissa laitteita ei voida rekisteröidä ABM-palveluun, voidaan hyödyntää Intune Company Portal -jakelua, jonka kautta laitteille voidaan ladata hallintaprofiilit ilman erillistä rekisteröintiä. Intunen kautta laitteet saavat niille siellä määritellyt

konfiguraatioprofiilit ja sovellukset automaattisesti käyttöönoton tai jälkirekisteröinnin yhteydessä, kunhan laite on ensin yhdistetty verkkoon.

Jakelua varten ollaan todennäköisesti ottamassa käyttöön käyttäjäaffiniteetti, jossa jokainen laite ja jakelu tapahtuisi Microsoft-tilikohtaisesti niin ADE- kuin Company Portal -jakelutapauksissa. Organisaatiolla on tällä hetkellä käytössä käyttäjähallintaa varten Google Workspace -ympäristö, johon on luotu Microsoft-tilien autoprovisioning-integraatio, joka mahdollistaa Google-tilien automaattisen pääsyn ja hallinnan Microsoft-ympäristössä käyttämällä Google SAML SSO -kirjautumista. Tässä on ollut tähän asti etuna se, että käyttäjällä ei tarvitse olla erillistä Microsoft-tiliä ja käyttäjä voi kirjautua Microsoft-ympäristöön Google tunnuksillaan. Ongelmaksi muodostuu kuitenkin se, että macOS ei tue Googlea identiteetin tarjoajana Microsoft-tilien kohdalla riittävän hyvin, jotta Intune-implementaatio käyttäjäaffiniteettia käyttäen olisi mahdollista. (13.) Työssä tutkitaan, onko ongelmaan vaihtoehtoisia ratkaisuja, ja tehdään päätös affiniteetin kanssa etenemisestä.

Työn kannalta oleellisimmat tavoitteet ovat ABM- ja Microsoft-palveluiden konfigurointi tuotantokelpoisiksi. Oikein konfiguroituna saadaan macOS-laitteet rekisteröityä yritykselle ABM-palveluun, josta ne saadaan määriteltyä Intune-palvelimelle valitsemalla MDM-palvelin ABM-portaalista. Intune-palvelussa laitteille määritellään yrityksen ja loppukäyttäjän tarpeiden perusteella mukautettuja ja esimallinnettuja konfiguraatioprofiileita, joilla asetetaan ja lukitaan laitteen asetuksia sekä käyttäytymistä yrityksen määrittelemien tarpeiden mukaisiksi.

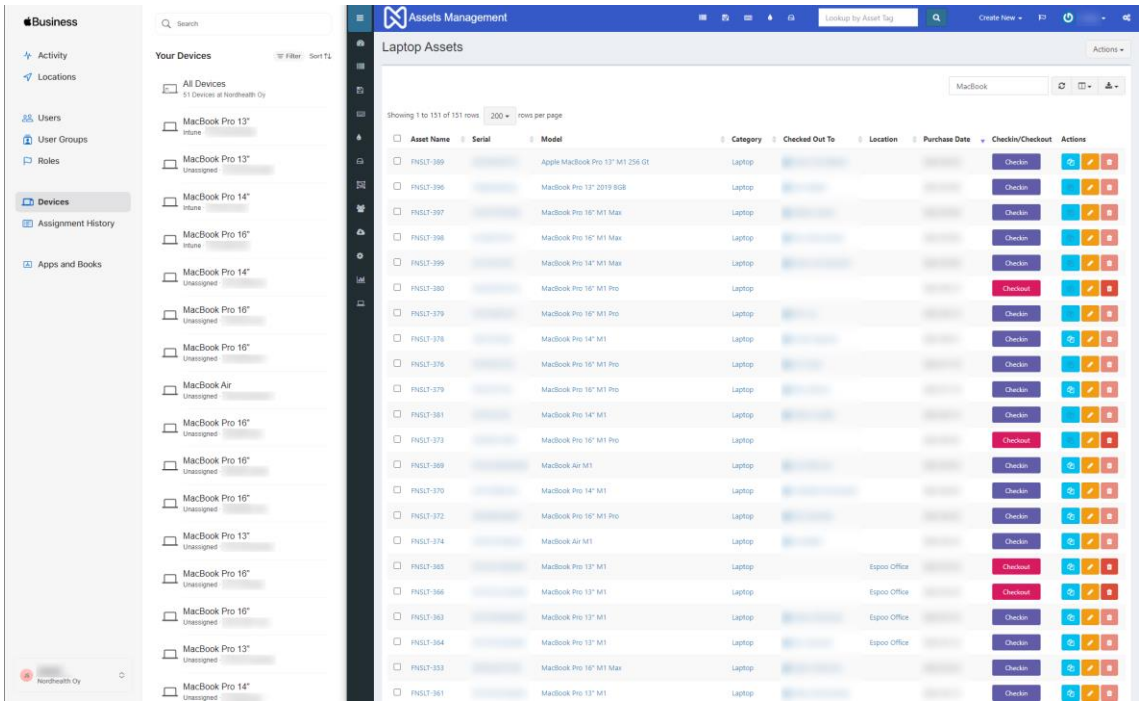
Tietoturvan osalta palvelussa pakotetaan päätelaitteille FileVault-levynsalaus ja paikallisen tilin salasanan minimivaatimukset. Palveluun luodaan eri laite- ja käyttäjäryhmiä, joilla voidaan hallita laitteille asetettuja profiileita ja pääsyä yrityksen resursseihin eritasoisten vaatimuksien perusteella. Käyttäjien ja laitteiden jakelu eri ryhmiin voidaan toteuttaa joko määritetysti tai dynaamisesti eri ehtoja käyttäen, kuten esimerkiksi maittain tai lisenssien perusteella. Intune-palveluun konfiguroidaan automaattinen sovellusten jakelu niin, että päätelaitteille saadaan jaettua käsinpaketoituja Line-Of-Business-sovelluksia ja esipaketoituja

Microsoft-sovelluksia. Pakotettuihin asennuksiin sisältyvät ainakin antivirus- ja Company Portal -sovellus. Automaattisen jakelun lisäksi loppukäyttäjille mahdollistetaan vaihtoehtoisten sovellusten asennus Intune Company Portal -sovelluksen kautta. Viimeiseksi Intune-palveluun konfiguroidaan shell-skriptien vienti päätelaitteille mukautettuja asetuksia ja sovelluksia varten, joita Intune ei tue luonnostaan.

Lopullisena tavoitteena implementaation jäljiltä on pystyä seuraamaan laitteita keskitetysti Microsoft Endpoint Management -portaalin kautta niin, että yrityksen IT-osastolla on tiedossa laitteille jaetut ja asennetut sovellukset, hallintaprofiilit, ryhmät ja tietoturvakäytänteet. Seuraamisen lisäksi halutaan myös pystyä hallitsemaan tiettyjä laitteiden toimintoja etänä, kuten lukitseminen ja tyhjennys. Intune-implementaation myötä voidaan olettaa, että IT-tiimin ja yrityksen työntekijöiden käyttämä aika laitteiden valmisteluun ja hallintaan vähenee ja työ helpottuu huomattavasti. Seurauksena aikaa ja resursseja jäisi enemmän muihin töihin.

4 Yrityksen keskitetyn hallinnan ympäristöt

Lähtökohtana projektille on tilanne, jossa yritykselle on valmiiksi perustettu molemmat, Apple Business Manager- ja Microsoft Endpoint Manager -ympäristöt. ABM on konfiguroitu siihen pisteeseen, että projektin työosuus voidaan suoraan aloittaa laiterekisteröinnillä. MEM-kokonaisuuden Intune-palvelu vaatii vielä muutaman oletuskonfiguraation, minkä jälkeen voidaan laitteita viedä ABM:stä Intune-ympäristöön. Yrityksellä on käsin ylläpidetyn laiterekisterin perusteella noin 120 kannettavaa macOS-tietokonetta aktiivisesti käytössä, joista noin 42 % on ADE-rekisteröity ABM-palveluun yrityksen alle (kuva 1). Rekisteröimättömille macOS-laitteille on tarkoitus selvittää paras mahdollinen keino ja kannattavuus laiterekisteröintiä ja jakelua varten. Rekisteröintiin vaikuttaa esimerkiksi laitteiden ikä ja varustelu sekä mahdollisuus päästä laitteeseen fyysisesti käsiksi Apple Configurator -sovelluksen käyttöä varten. Tilanteissa, joissa laitetta ei voida jälkeenpäin rekisteröidä Apple Business Manageriin, voidaan hyödyntää esimerkiksi Intune Company Portal -jakelua, jossa laitteelle ladattava sovellus hakee tarvittavat profiilit Intunesta.



Kuva 1. Yrityksen kannettavat MacBook-tietokoneet Apple Business Manager -portaalissa ja yrityksen sisäisessä laitehallinnassa.

IT-osastolla ei ole nykyisessä tilanteessa luotettavaa tapaa hallita laitteita ja niiden ohjelmistoa. Aikaisemmin IT-osastolle on riittänyt yhdistettynä kokonaisuutena erillinen laiterekisteri, F-Secure-tietoturvapaketti ja fyysinen pääsy laitteisiin toimistoympäristössä, mutta yrityksen kasvaessa ja etätöiden yleistyessä on laitteiden luotettavan etähallinnan ja seuraamisen tärkeys myös lisääntynyt huomattavasti, eivätkä edellä mainitut toimet ole enää riittävät.

Laitehallinnan puuttuessa on IT-osaston lähes mahdotonta seurata käyttäjien kannettavien tietokoneiden tilaa tietoturvan kannalta. F-Secure-tietoturvapaketilla on mahdollista seurata joitain laiteominaisuuksia, mutta se ei anna yhtä laajaa hallinta- ja seurantamahdollisuutta, kuin mitä keskitetty hallinta mahdollistaisi esimerkiksi Intune-palvelun kautta. Intune mahdollistaa myös F-Secure-tietoturvapaketin pakotetun jakelun laitteille, joille sitä ei välttämättä ole vielä asennettu.

Työn alkutilanteessa macOS-laitteiden käyttöönotto on täysin manuaalista tukkuliikkeiden ADE-rekisteröintiä lukuun ottamatta. Ensiasennuksen tekee joko IT-osasto tai käyttäjä itse seuraamalla IT-osaston kirjoittamia macOS-käyttöönotto-ohjeita, jotka löytyvät yrityksen sisäisestä verkosta. Laite nimetään käsin yrityksen laiterekisteristä saadun laitetunnisteen perusteella, minkä jälkeen laitteille asennetaan F-Secure-tietoturvapaketti, joka jaellaan käsin sähköpostitse. Viimeiseksi laitteelle otetaan käyttöön FileVault-levynsalaus, jonka palautusavain lähetetään IT-osastolle käyttäen sisäistä viestintää tai muistitikkua. Kun laite on saatu niin sanottuun oletustilaan, voi käyttäjä asentaa loput tarvitsemansa sovellukset ja ympäristöt. Kaikki edellä mainitut vaiheet oletustilaan asti on mahdollista automatisoida käyttäen keskitettyä Intune-hallintaa.

4.1 Apple-ympäristö

Projektin alussa henkilökohtainen tietämykseni macOS-käyttöjärjestelmästä ja siihen liitetyistä teknologioista oli erittäin pintapuolinen. Projektia lähdettiinkin lähestymään ihan ensiksi testikäyttöön tarkoitetuilla vuoden 2018 Intel x86- ja vuoden 2021 M1 ARM- kannettavilla tietokoneilla. Laitteet valikoitiin sillä

perusteella, että ne kattaisivat mahdollisimman laajan kirjon laiterekisteristä löytyvistä laitetyypeistä. Kannettavilla tietokoneilla voidaan siis testata ADE- ja Company Portal -rekisteröityjen laitteiden jakelutyyppejä sekä x86- ja ARM-pohjaisten laitteiden eroavaisuuksia tai vaatimuksia. Esimerkiksi ARM-pohjaiset laitteet saattavat vaatia Rosetta 2 -emulaatiota kääntämään x86-sovellusten koodin ARM-yhteensopivaksi. (14.)

Laitteisiin tutustumisen lisäksi oleellinen osa projektia oli myös tutustua Apple Business Manager -ympäristöön. ABM on Microsoft Endpoint Manageriin ja Intuneen verrattuna pienempi kokonaisuus, joten sen pääominaisuuksiin tutustuminen ei vienyt kovin kauan aikaa. Yleiskuvan palvelusta ja sen toiminnoista sain lukemalla läpi Applen dokumentaatiota (15), minkä jälkeen loput perehtymisestä tapahtui käytännön kokemuksen kautta ja Intune-ohjeita seuraamalla.

macOS-esiasennusvaiheet

Ennen kuin aloitettiin Intunen konfiguraatiota tai Apple Business Manager -laiterekisteröintiä, asennettiin kannettavat tietokoneet manuaalisesti IT-tiimin ohjeiden perusteella käyttäjälle valmiiseen tilaan. Tämä tehtiin siksi, että olisi konfigurointia varten tiedossa, mitä toimintoja laitteilta ja käyttäjiltä vaaditaan käyttövalmista tilaa varten. Prosessi aloitettiin kannettavien tietokoneiden nollauksella käyttämällä *Disk Utility* -toimintoa (16).

Kun kannettava tietokone otetaan ensimmäistä kertaa käyttöön joko suoraan jälleenmyyjältä tai nollauksen jälkeen, tulee käydä MacBookin Setup Assistant -vaiheet läpi ja määritellä asetukset ohjeiden mukaisesti. Henkilökohtaiset ja mieltymyksiin liittyvät asetukset ovat käyttäjälle vapaasti asetettavissa, mutta Migration Assistant- ja Apple ID -asetukset tulee ohittaa tietoturvasyistä, sillä laitteita ei haluta rekisteröidä kenenkään henkilökohtaiselle Apple ID -tilille tai viedä yhtiön dataa Applen pilvipalveluun. Laitteelle luodaan paikallinen järjestelmävalvojatili, jolle asetetaan vähintään 13 merkin uniikki salasana.

Esiasetusten jälkeen kannettavalle tietokoneelle konfiguroidaan käyttöjärjestelmäasetukset. Ensiksi määritellään laitteelle FNSLT-laiterekisterinumeron

muotoinen verkkonimi, joka perustuu laitteelle laiterekisterissä määriteltyyn *Asset Tag* -numeroon. Seuraavaksi laitteelle otetaan käyttöön palomuuri ja levynsalaus. FileVault-levynsalauksen kanssa tulee olla tarkkana, että sitä käyttöönotettaessa valitaan *Create a recovery key and do not use my iCloud account* -vaihtoehto. Näin palautusavain voidaan kirjata muistiin, jotta se saadaan IT-tiimille eteenpäin varmuuskopiointia varten. (17.)

Konfiguraatioiden jälkeen laitteelle asennetaan F-Secure-tietoturvapaketti, jonka asennuspaketti jaetaan käyttäjäkohtaisesti käyttäjän työsähköpostiin F-Securen portaalin kautta. Ohjelman asennus on yksinkertainen, joskin hieman aikaa vievä ja vaatii kannettavilla ARM-tietokoneilla Rosetta 2 -emulaatio-ohjelman yhteensopivuuden takaamiseksi. Asennuksen jälkeen ohjelmisto vaatii F-Secure-järjestelmälaajennuksen käyttöönoton. Laiteasennus viimeistellään hakemalla ja ajamalla uusin toimivaksi todettu macOS-järjestelmäpäivitys.

Apple Business Manager

Apple tarjoaa kriteerit täyttäville organisaatioille Apple Business Manager -palvelua, joka on web-pohjainen portaali IT-järjestelmänvalvojille. Sen kautta on mahdollista hallita organisaation Apple-laitteita, -sovelluksia ja -käyttäjätilejä. ABM:n tärkein toiminto tämän projektin kannalta on automatisoida ja yksinkertaistaa yritykselle ADE-rekisteröityjen laitteiden kirjaamista ennalta määritetylle kolmannen osapuolen MDM-palvelimelle, kuten Microsoft Intune. Laitehallinnan lisäksi ABM mahdollistaa hallittujen Apple ID -tunnusten luomisen yrityksen käyttäjille sekä sovellusten ja kirjojen ostamisen ja jakelun MDM-palvelun kautta. (18.)

Kun organisaatio hyväksytään Apple Business Manager -ohjelmaan, portaali on konfiguroitava Applen asettamien ohjeiden mukaisesti organisaation tietoihin pohjautuen (19). Esimääritysten jälkeen on mahdollista aloittaa laiterekisteröinti, joka voidaan toteuttaa kahdella tapaa laitteen tilan mukaan. Uutta laitetta tilattaessa voidaan Applen valtuuttamien jälleenmyyjien kohdalla hyödyntää ADE-rekisteröintiä, jossa jälleenmyyjälle ilmoitetaan organisaation uniikki Organization

ID. Tällä ID:llä rekisteröidään ostettu laite yrityksen ABM-palveluun ja omistukseen, eikä se vaadi organisaation järjestelmänvalvojalta muita toimenpiteitä. Vastaavasti taas laiterekisteröinti ABM-palveluun voidaan tehdä myös jälkikäteen hyödyntämällä Apple Configurator -sovellusta, joka vaatii laitteen nollaamisen sekä järjestelmävalvojan fyysisen pääsyn laitteeseen. Tämän jälkeen yhdistetään vähintään yksi kolmannen osapuolen MDM-ratkaisu ja asetetaan se rekisteröidylle laitteelle joko automaattisesti tai manuaalisesti. Kun MDM-palvelin on asetettu laitteelle, se viedään synkronoinnin yhteydessä kolmannen osapuolen MDM-palveluun, jossa sille voidaan asettaa hallinta käytänteitä. (20; 21.)

Laiterekisteröinnin jälkeen voidaan aloittaa laitteen jakelu, joka myös voidaan toteuttaa kahdella tapaa laitteen tilan mukaan. ADE-rekisteröityjen laitteiden kohdalla voidaan jakelu toteuttaa esiasennusvaiheesta eteenpäin, sillä macOS ottaa yhteyden MDM-palvelimeen esiasennusvaiheessa, jolloin se saa tarvitsemansa Enrollment-profiilin ja hallintaprofiilin. Mikäli laite on jo otettu käyttöön, voidaan laite yhdistää Intune-palvelimeen käyttäen terminaalia. Vastaavasti taas laitteet, joita ei ole ADE-rekisteröity, voidaan rekisteröidä Intune-palvelimelle käyttämällä Intune Company Portal -sovellusta. Se on ADE-palvelua huomattavasti manuaalisempi tapa, mutta vaihtoehtojen puitteissa pakollinen. Company Portal -rekisteröinti vaati laitteen käyttäjää hoitamaan rekisteröinnin, minkä vuoksi on tarpeellista tarjota kattava ohjeistus. Company Portal- ja ADE-rekisteröinnin jälkeen ovat laitteet käytännössä verrannolliset ja suurin osa Intune-toiminnoista laitteiden hallinnan osalta sujuvat samoja reittejä pitkin. (21.)

4.2 Microsoft-ympäristö

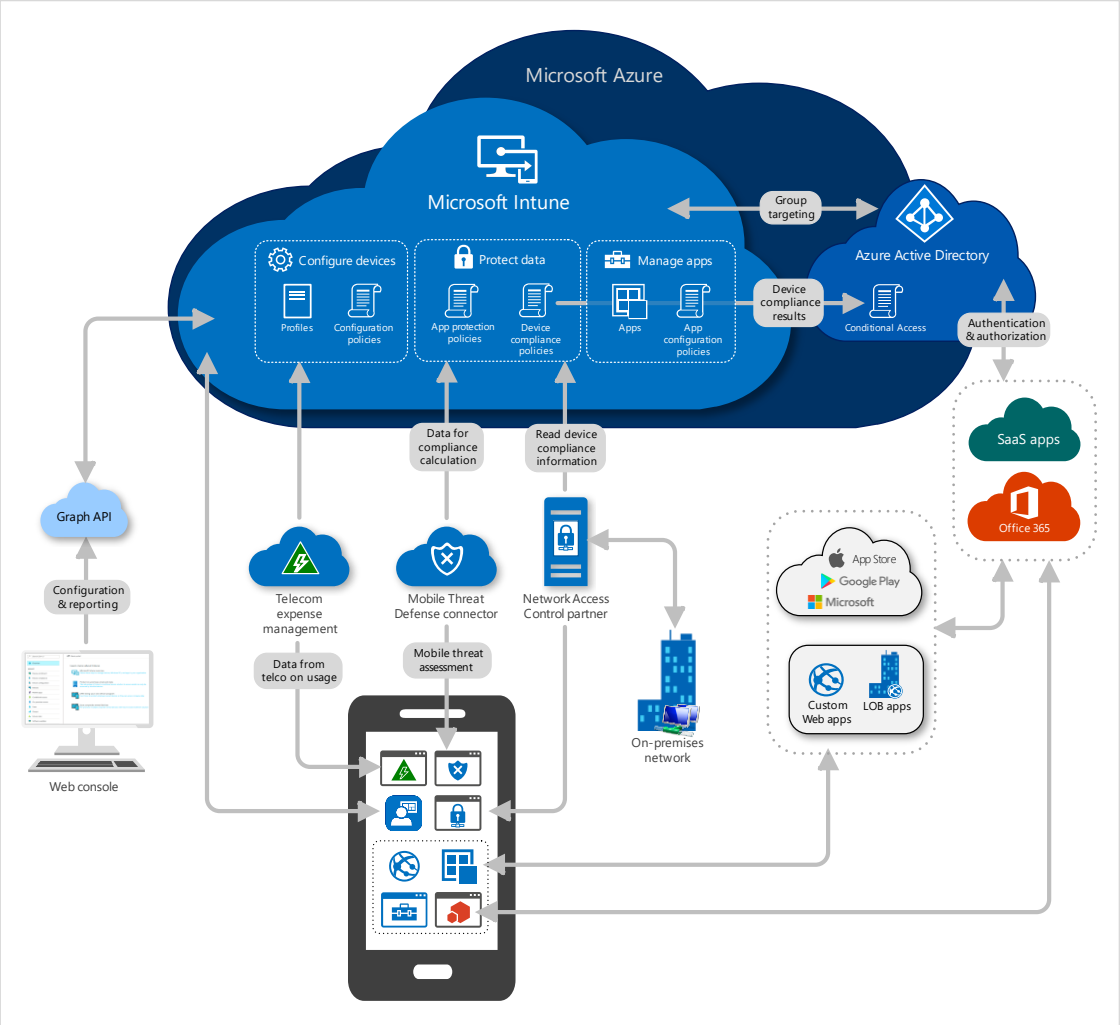
Microsoft Endpoint Managerin Intune-palvelu ja sen ympäristöt olivat itselleni projektin alussa käytännössä täysin tuntemattomia. Olen aikaisemmissa työpaikoissa ollut hieman tekemisissä Microsoft AD- ja Office 365 -palveluiden kanssa, mutta nämä ovat olleet vain pintaraapaisuja verrattuna Microsoft Endpoint Managerin ja Azure AD:n laajaan tarjontaan. Aloitukseksi perehdyin esimieheni kanssa hieman Intunen päätoimintoihin ja siihen, miten ne liittyvät projektiin, sekä taustalla pyörivään Azure AD -tietokantaan. Ympäristöjen

yleiskuvan selvenemisen jälkeen aloitin itseopiskelun aiheen parissa, jossa käytin hyödykseni Microsoftin virallista dokumentaatiota, joka on vapaasti luettavissa Learn Microsoft -sivustolla (22). Saadakseni tarpeellisen ymmärryksen aiheesta ja sen sisäisestä toiminnasta luin dokumentaatiota ja esimerkkiratkaisuja järjestyksessä. Kohdatessani asioita tai kokonaisuuksia, jotka eivät dokumentaation avulla selvinneet riittävästi, oli oman osaamisen ja projektin edistämisen kannalta erittäin tärkeätä, että pystyin kysymään asioista esimieheltäni ja muilta IT-osaston henkilöiltä.

Microsoft-lisenssit ovat oleellinen osa työtä, sillä lisenssit oikeuttavat pääsyn tiettyihin Microsoft-tuotteisiin, kuten Microsoft 365 ja Microsoft Intune. Lisenssejä on tarjolla monenlaisia, ja kukin oikeuttaa eriävissä määrin pääsyjä tiettyihin tuotteisiin ja toimintoihin, joten jokainen voi organisaation tai yrityksen koon perusteella valita itselleen sopivat lisenssit ja yhdistellä niitä käyttäjäkohtaisesti.

Tilaajayrityksessä Intune-käyttöönotto vaatii ensin tarpeet kattavan lisenssin hankkimisen järjestelmähaltijan tilille, minkä jälkeen lisenssejä voidaan tätä kautta lisätä niitä tarvitseville tileille. Intunen kohdalla IT-osaston kanssa päädyttiin Enterprise Mobility + Security E3 -lisenssiin, joka kattaa organisaation tarpeiden ja työn kannalta oleellisimmat toiminnot. Oleellisimpia toimintoja ovat käyttöoikeuksien ehdollinen hallinta, laitteiden ja mobiilisovellusten paikallinenhallinta, monimenetelmäinen todentaminen, tietoturvaraportointi ja Microsoft Advanced Threat Analytics. (23; 24.)

Azure Active Directory on Microsoftin kehittämä pilvipohjainen universaali tilien ja käyttöoikeuksien hallintapalvelu, jolla mahdollistetaan muun muassa pääsyjä yrityksen sisäisiin resursseihin. Työn kannalta tärkein toiminto Azure AD -puolella ovat AAD-ryhmät, joiden avulla voidaan Intune-palvelussa jakaa tai rajoittaa käyttäjä- ja laitekohtaisesti resursseja. Azure AD ei välttämättä ole niin oleellinen päivittäisessä käytössä, mutta se on kuitenkin aina taustalla käytössä, kun tehdään tili-, laite- ja ryhmäkohtaisia muutoksia (Kuva 2) (25). Yhdessä Intune-hallinnan kanssa ne muodostavat tehokkaan yhdistelmän yrityksen resurssienhallintaa varten.



Kuva 2. Microsoft Azure -palvelun arkkitehtuuri [26].

Osa Intunen ja Azure AD:n opiskelua dokumentaation lukemisen lisäksi on tietenkin itse ympäristöihin tutustuminen portaalien kautta ja asioiden testailu lukemisen ohella. Päätin aloittaa testaamisen, kun olin mielestäni sisäistänyt projektin kannalta oleelliset osa-alueet ja saanut selvän kuvan siitä, mitä Microsoftin kannalta vaaditaan projektin valmistumiseksi.

Microsoft Intune

Microsoft Intune on pilvipohjainen päätelaitteiden hallintatyökalu ja osa Microsoft Endpoint Management -kokonaisuutta. Sen päätarkoituksena on tarjota yritykselle yhtenäistetty ja osittain automatisoitu hallinta organisaation ja käyttäjien

BYOD-laitteiden, sovellusten ja käyttäjätilien hallintaan, monitorointiin ja turvaamiseen. Hallinta tapahtuu Microsoft Endpoint -verkkoportaalin kautta, jonne on kerätty laaja kirjo hallintatyökaluja Microsoftin muista hallintapaneeleista, kuten Azure AD ja Microsoft Admin Center. Tässä on etuna se, että suuri osa hallinnasta voidaan toteuttaa MEM-portaalin kautta, eikä välissä välttämättä tarvitse vaihtaa palvelua kuin tilanteissa, joissa tarvitaan tarkempaa säätöä esimerkiksi käyttäjätileille. Intune tukee myös laajasti kolmannen osapuolen laitteita ja sovelluksia, minkä vuoksi macOS-jakelu on ylipäänsä mahdollista. Näin yrityksen on mahdollista käyttää yhtä hallintakokonaisuutta Windows-, macOS-, Android- ja iOS-jakeluun ja hallintaan. (27.)

Portaalin kautta voidaan sinne viedyille laitteille ja käyttäjille asettaa muun muassa vaatimuksia, rajoituksia tai pääsyjä yrityksen resursseihin. Laitteet ja käyttäjät voidaan jakaa näiden tarpeiden mukaisesti joko manuaalisesti tai automaattisesti eri Azure AD -ryhmiin, joiden avulla voidaan helpommin hallita, mitä toimintoja tarjotaan tai pakotetaan kullekin ryhmälle. (27.) Ryhmät voidaan tämän jälkeen joko lisätä tai sulkea pois toimintokohtaisesti, eli esimerkiksi koko organisaatiolle voidaan yhden ryhmän avulla pakottaa laitteille paikallisesti levynsalaus ja sulkea pääsy yrityksen resursseihin, jos tätä ei ole otettu vielä käyttöön.

Kannettavien macOS-tietokoneiden kannalta oleellisimpia toimintoja Intune-palvelussa on sen tuki Apple Automated Device Enrollment -ohjelmalle, joka automatisoi ja yksinkertaistaa laiteasennusprosessia ja jakelua. ADE-rekisteröity laite hakee Applen ympäristöstä sille merkityn Intune MDM -palvelimen, josta se saa ladattua tarvittavat hallintaprofiilit, käytänteet, sovellukset ja skriptit.

4.3 Google SSO -todennus ja M365 autoprovisioning -käyttäjäpääsy

Projektia suunniteltaessa ja Intune-käyttöönoton vaiheita läpikäytäessä huomiota herätti käyttäjäaffiniteettikonsepti ja sen mahdolliset vaikutukset projektin toteuttamiseen. Käyttäjäaffiniteetti tarkoittaa Intune-yhteydessä sitä, että jaeltu laite rekisteröidään yhdelle käyttäjälle käyttöönottorekisteröinnin yhteydessä.

Tämä tarkoittaa, että Microsoft-ympäristössä on jokaiselle käyttäjälle oltava Microsoft-tili, jotta rekisteröitävät laitteet voidaan yhdistää tileihin. Tätä kautta mahdollistetaan esimerkiksi käyttäjäkohtaisesti rajattu pääsy yrityksen resursseihin ja sovelluksiin Company Portal -sovelluksen kautta. Ongelmia tulee kuitenkin laitteiden rekisteröintitilanteessa, kun laitteella pitäisi kirjautua sisään Microsoft-tilille ja käyttää monimenetelmäistä todentamista. Kuten työn tavoitteissa luvussa 3 jo mainittiin, organisaatiossa on käytössä Google Workspace Office suite, jonka ympärille yrityksen käyttäjätilit ja hallinta keskittyvät.

Yrityksen käyttäjien Microsoft 365 -tilit on yhdistetty Google Workspace -identiteettiin käyttämällä Google Single Sign On- ja M365 user autoprovision -konfiguraatiota. Käytännössä tämä tarkoittaa sitä, että Microsoft-tilit voidaan luoda autoprovision-toimintoa käyttäen Google-tileihin pohjautuvalla tiedolla automaattisesti ja Microsoft-kirjautumiseen voidaan hyödyntää Google SSO -todennusta, jolloin käyttäjien ei tarvitse muistaa erillistä salasanaa Microsoft-ympäristöön. (28.) Implementaatio on ollut erittäin hyödyllinen tähän asti, sillä käyttäjähallinta on saatu kohdennettua yhden ympäristön alle. Työn kannalta implementaatiossa on kuitenkin ongelma, sillä Intune Enrollment käyttäjäaffiniteettia hyödyntäen ei toimi, kun Microsoft-tilien kirjautumiseen käytetään Google SSO -todennusta. Laitetta käyttöönotettaessa tulee *Setup Assistant* -aikana kirjautua sisään käyttäen Microsoft-tunnuksia, mutta laite ei yksinkertaisesti huoli tunnuksia, kun käyttäjätilillä on käytössä Google SSO -todennus.

Ongelmatilanteessa päädyttiin IT-osaston kanssa siihen, että laiterekisteröinnissä käytetty käyttäjäaffiniteetti on työn kannalta niin olennainen ominaisuus, että SSO- ja autoprovision-konfiguraatiot täytyy purkaa. Purkamiseen liittyy käyttäjätilien luonteen vuoksi toinenkin ongelma, jossa Microsoft-tilit, jotka on luotu autoprovision-toimintoa käyttäen, eivät sisällä asetettua salasanaa. Tämä tarkoittaisi siis sitä, että tileille ei voi kirjautua sisään, ennen kuin niiden salasanat on nollattu. Tämä ei sinänsä ole ongelma, sillä järjestelmävalvojat voivat tilien salasanat nollata, mutta tilanteessa, jossa tilejä on satoja, tulisi tästä erittäin paljon manuaalista työtä. Microsoftilla on tähän kuitenkin ratkaisu, jonka nimi on Self Service Password Reset eli salasanan palautuksen itsepalvelu.

SSPR:n avulla yritykset, joilla on tarvittavat Azure AD -lisenssit, ja käyttäjät, joilla on tilillä käytössä monimenetelmäinen todentaminen, voivat omatoimisesti nollata salasanansa ilman yrityksen IT-osaston apua. Microsoft on kattavasti dokumentoinut SSPR-käyttöönoton Learn Microsoft -sivustollansa (29), joten sen käyttöönotto sujui suhteellisen mutkattomasti. Isompia ongelmia ei syntynyt, lukuun ottamatta Microsoftille tyypillisiä evästeisiin pohjautuvia kirjautumiskierteitä. SSPR-implementoinnin jälkeen voitiin Google domain federation poistaa käytöstä muuttamalla Microsoftin puolella Nordhealth-verkkotunnuksen todennus liitetystä muodosta hallituksi. Ennen muutosta on kuitenkin hyvä luoda varmuudeksi Microsoftin puolelle paikallinen järjestelmävalvojatili, joka ei vaadi Google SSO:ta kirjautumiseen ja jonka avulla voidaan hallita Microsoft-ympäristön asetuksia ongelmatilanteissa. Muutoksen ajon jälkeen on myös huomioitava, että Azure AD saattaa vaatia jopa tunnin aikaa muutoksen tekemiseen, ja tänä aikana kirjautuminen Microsoft-tileille ei välttämättä ole mahdollista. Muutoksesta on siis hyvä ilmoittaa etukäteen käyttäjille, jotta he voivat kirjautua Microsoft-palveluihin etukäteen.

5 Yrityksen keskitetyn hallinnan käyttöönotto

Intune MDM -palvelun hallinta macOS-laitteita varten on hyvin dokumentoitu Microsoftin virallisella Docs-sivustolla, jossa se tarjoaa monipuolisen ja kattavan oppaan MDM-käyttöönottoon ja laitteiden hallintaan Ohjeita seuraamalla ja soveltamalla saadaan Intune-implementaatio muovattua siihen tilaan, että macOS-laitteiden rekisteröinti palveluun on mahdollista ja niille saadaan jaettua yrityksen määrittelemät hallintaprofiilit, käytänteet, sovellukset ja pääsyt.

Ennen kuin laitteita voidaan kuitenkaan viedä Intune-hallinnan piiriin, jossa niille voidaan jakaa määrityksiä, tulee mahdollisuuksien mukaan laitteet rekisteröidä yrityksen hallittavaksi Apple Business Manageriin. Tämän lisäksi Microsoft on ohjesivullaan listannut Intune-palvelun laiterekisteröintiä varten seitsemän esimääritystä, jotka tulee käydä läpi ja konfiguroida, ennen kuin laitteiden vienti Intune- hallinnan piiriin on mahdollista. (30.) Listalta voidaan jättää pois laitteiden kelpoisuuden tarkistaminen, sillä yli kolme vuotta vanhoja laitteita ei tulla rekisteröimään yrityksen laitekannan iän perusteella. Tämän jälkeen jää kuusi vaihetta läpikäytäväksi:

- Intune MDM -valtuuksien asettaminen
- yrityksen verkkotunnuksen konfigurointi
- Apple MDM -push-sertifikaatti
- lisenssien määrittäminen Microsoft 365 -hallintakeskuksessa
- ryhmien luominen organisointia varten
- Company Portal -sovelluksen konfigurointi.

ABM-laiterekisteröinnin ja Intune-esimääritysten jälkeen voidaan aloittaa Intune Enrollment Setup -vaihe, joka mahdollistaa ABM-rekisteröityjen laitteiden Apple Automated Device Enrollment -viennin Intunen piiriin. Enrollment setup -vaiheessa Intuneen määritellään Apple ADE -token, hallittu Apple ID -tili ja oletus rekisteröintiprofiili, minkä jälkeen synkronoidaan laitteet ABM:n ja Intunen välillä.

5.1 Apple Business Manager -laiterekisteröinti

Apple Business Managerista on mahdollista viedä rekisteröidyt laitteet automaattisesti Intune-hallinnan piiriin. Laitteet, joita ei ole rekisteröity ABM-palveluun, voidaan vastaavasti viedä hallintaan käyttämällä Intune Company Portal -sovellusta, joka asennetaan paikallisesti vietävälle laitteelle. Lähtökohtana yrityksen vaatimusten kannalta on, että mahdollisuuksien mukaan laitteet on ensin rekisteröitävä ABM-palveluun. ABM-rekisteröidyt laitteet on virtuaalisesti paritettu yritykselle, eikä niitä voi muun tahon toimesta ottaa käyttöön tai uudelleen rekisteröidä, ennen kuin ne on vapautettu IT-osaston toimesta yrityksen hallinnasta. Rekisteröinti vaatii laitteen tilauksen yhteistyötukkuliikkeeltä tai fyysisen pääsyn rekisteröitävään laitteeseen, joka tukee Apple Configurator -sovelluksella rekisteröimistä.

Laiterekisteröinti Apple Configurator -sovelluksen avulla

Applen macOS- ja iOS-laitteet, joita ei ole ADE-rekisteröity tukkuliikkeen toimesta valmiiksi, voidaan manuaalisesti rekisteröidä yrityksen IT-osaston toimesta Apple Configurator -puhelinsovelluksen avulla. Vaatimuksena rekisteröinnille on, että laitteeseen on fyysinen pääsy ja siinä on joko Apple-silikoniin perustuva prosessori tai Apple T2 -tietoturvasiru ja minimissään macOS 12.0.1 -käyttöjärjestelmä ja laitteen tulee olla nollattu esiasennusvaiheeseen. iPhone-puhelimen, jolla rekisteröinti tehdään, tulee olla minimissään iOS 15 -käyttöjärjestelmäversiossa. Lopuksi hallitulla Apple ID -tilillä tulee olla vähintään Device Enrollment Manager -rooli ABM:ssä, joka oikeuttaa Apple-laitteiden osoittamisen. (31.)

Apple Configurator -sovellus voidaan asentaa sitä tukevalle iPhone-puhelimelle Apple App Store -kaupasta. Sovellukseen kirjaudutaan sisään käyttämällä ABM-portaaliin rekisteröityä hallittua Apple ID:tä. Laiterekisteröinti aloitetaan laitteen käyttöönoton Setup Assistant -vaiheen alettua, ja ruudulle ilmestyvä skannattava kuvio skannataan Apple Configurator -sovelluksen kameranäkymää käyttäen. Onnistuneen skannauksen jälkeen laitteen tiedot viedään

automaattisesti ABM-ympäristöön, jossa sille voidaan määritellä MDM-palvelin. (31.) Tässä kohtaa laite on ominaisuuksiensa osalta samassa tilassa kuin ADE-rekisteröity laite.

5.2 Intune-ympäristön esimääritykset

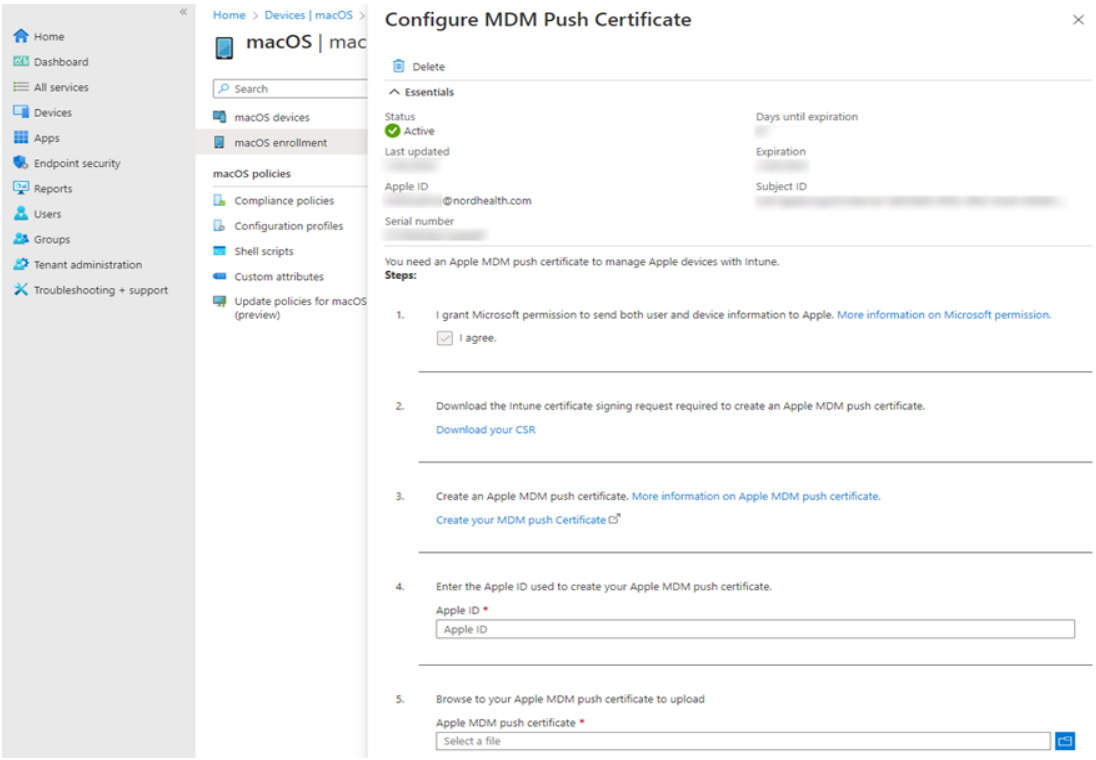
MDM-valtuuden asettaminen määrittelee, minkä palvelun kautta laitteita hallitaan. Tätä varten on ollut kolme vaihtoehtoista konfiguraatiota organisaatiotason MDM-valtuutukselle: Intune MDM Authority, Configuration Manager MDM Authority ja ei mikään. Nordhealth-yrityksen Intune-palvelun julkaisu on 1911-version jälkeinen versio, minkä vuoksi MDM-valtuudet on valmiiksi asetettu Intune-palvelulle eivätkä ne vaadi tässä vaiheessa työtä muutoksia. (32.)

Yrityksen oman verkkotunnuksen konfigurointi Microsoft 365 Admin -keskuksen kautta on Intune MDM:n toimivuuden kannalta periaatteessa vapaaehtoista, mutta saattaa helpottaa yrityksen toimintaa tulevaisuudessa. Vapaaehtoisen tästä vaiheesta tekee se, että Microsoft tarjoaa organisaatiolle rekisteröitymistilanteessa alustavan verkkotunnuksen, joka isännöidään Microsoft Azure Active Directory -palvelussa. Alustava verkkotunnus on muotoa *yrityksen-verkkotunnus*.onmicrosoft.com. (33.)

Omalla verkkotunnuksella voidaan esimerkiksi yksinkertaistaa kirjautumista Microsoft-ympäristöön käyttämällä yrityksen yleisessä käytössä olevaa verkkotunnusta. Verkkotunnuksella on esimerkiksi implikaatioita, jos macOS-laitteet rekisteröidään käyttäjäaffiniteetilla, jolloin laitteelle kirjaudutaan Microsoft-tunnuksella ja laite on yhdistetty tiettyyn tiliin (21). Nordhealthin tapauksessa laitteet tullaan rekisteröimään käyttäen käyttäjäaffiniteettiä, joten omasta verkkotunnuksesta on projektin kannalta etua. Yrityksellä on ollut Microsoft Azure- ja M365- ympäristöt käytössä jo entuudestaan, joten Nordhealth-verkkotunnukset on rekisteröity valmiiksi eivätkä ne vaadi tässä vaiheessa muutoksia.

Apple MDM -push-sertifikaatti on yrityksen Apple-mobiililaitteiden Intune-palveluun viennin kannalta pakollinen varmenne, jota ilman macOS-laitteita ei voida

rekisteröidä Intune-palveluun. Microsoft Intune -palvelu vaatii Applen allekirjoittaman varmenteen laiterekisteröintiä varten, ja varmenne tulee uusia vuosittain tai se vanhenee (34). Varmenne luodaan MEM-portaalin Apple enrollment -kategorian alta löytyvästä Configure MDM Push Certificate -näkymästä (kuva 3). Tästä näkymästä löytää myös tulevaisuuden kannalta tärkeää tietoa, kuten esimerkiksi varmenteen raukeamispäivämäärän ja Apple ID -tilin, jolla varmenne luotiin.



Kuva 3. Microsoft Endpoint Manager -portaalin MDM Push Certificate -näkymä.

Intune-palvelun allekirjoituspyyntö-CSR-tiedosto allekirjoitetaan kirjautumalla Apple Push Certificate -portaaliin käyttäen yrityksen Admin Apple ID -tunnusta. Kirjautumista varten suositellaan käyttämään erillistä yhtiökohtaista tiliä, jotta varmenteen uusiminen tulevaisuudessa ei ole kenenkään yksittäisen henkilön takana. Kun varmenne on allekirjoitettu, ladataan allekirjoitettu varmenne PEM-tiedostomuodossa Intune-palvelimelle ja ennen tallennusta merkitään moduuliin Apple ID, jolla varmenne luotiin. (34.)

Intune lisenssien määrittäminen Microsoft 365 -hallintakeskuksessa voidaan toteuttaa joko yksi kerrallaan manuaalisesti tai dynaamisia ryhmiä käyttämällä. Testausvaiheessa lisenssit lisätään yksittäisille käyttäjille käsin kulujen minimoimiseksi, ja työn lopuksi voidaan lisenssit lisätä kaikille MacBookia käyttäville tileille, kun laitejakelu on tuotannossa ja todettu toimivaksi. Itse Intune-palvelu sisältyy useampaan lisenssiin, joista on mainittu enemmän luvun 4.2 ohjaavan otsikon Microsoft-lisenssit yhteydessä. Tähän projektiin sopi parhaiten Enterprise Mobility + Security E3 -lisenssi, jossa on Nordhealthin käyttötarkoitukseen tarvittavan laajat turvallisuus- ja hallintamahdollisuudet. (35.) Näihin ominaisuuksiin sisältyvät muun muassa Microsoft Intune -palvelu, käyttöoikeuksien hallinta ja suojaus, MFA, ehdollinen käyttöoikeus, tietoturvaraportointi, mobiilisovellusten ja tietokoneiden hallinta sekä jatkuva tietojen suojaus.

Intune-ryhmien luominen pohjautuu Azure Active Directory -ryhmiin, joilla hallinnoidaan laitteita ja käyttäjiä. Tämä mahdollistaa yrityksen tarpeisiin mukautettujen ryhmien luomisen, joilla on mahdollista organisoida käyttäjiä ja laitteita esimerkiksi maantieteellisen sijainnin, yrityksen sisäisen osaston tai laitteiston perusteella. Projektin kannalta ryhmien tärkein toiminto on kuitenkin mahdollistaa sovellusten, asetusten ja käytänteiden jakelu oikeille päätelaitteille.

AAD-ryhmiä on Intunessa kahdenlaisia: *Assigned* ja *Dynamic*. Assigned-ryhmissä käyttäjät ja laitteet lisätään manuaalisesti staattiseen ryhmään, johon ei tule muutoksia ilman manuaalista muokkausta. Dynamic-ryhmissä taas käyttäjiä ja laitteita voidaan lisätä tai poistaa automaattisesti perustuen ryhmälle määriteltyihin sääntöihin. Esimerkiksi jos dynaamisen jäsenyyden säännöksi on asetettu, että laitteen käyttöjärjestelmän tulee olla macOS, lisätään ryhmään kaikki Azure AD -järjestelmään rekisteröidyt macOS-laitteet. (36.)

Projektin testaamisen ajaksi Intune-ympäristöön luotiin alustavasti kolme ryhmää: macOS – MDM, macOS – Deployment ja macOS – Users. *MDM*-ryhmää käytettiin sovellusten ja konfiguraatioiden jakeluun, jotka on tarkoitettu pohjaksi jokaiselle Intune-macOS-jakelun piiriin kuuluvalle käyttäjälle. *Deployment*-ryhmää käytettiin vuorostaan Intune Company Portalin kautta jaettavien

sovellusten testaamista varten. Viimeiseksi *Users*-ryhmää käytettiin pääsääntöisesti kaikkien macOS-käyttäjien tilien yleisen hallinnan ja ylläpidon referoimiseen ja se pohjautui organisaation IT-osaston ylläpitämään laiterekisteriin. Ryhmän kautta oli helppo selvittää, kenen kuuluu lisätä lisenssejä ja ryhmäpääsyjä, kun laiterekisteröinti käyttäjille aloitettiin.

5.3 Intune-rekisteröinnin määrittely

Apple Automated Device Enrollment vaatii vielä muutaman toimenpiteen, jotta laitteiden synkronointi palveluiden välillä saadaan automatisoitua ja profiilien jakelu toteutettua laitteille. Tätä varten tarvitsee lisätä Microsoft Endpoint Manager -portaaliin Applen toimittama ADE-token sekä ainakin yksi Apple enrollment -profiili, joka luodaan ADE-tokenin taakse ja joka määritetään synkronoiduille laitteille, ennen kuin niillä voidaan aloittaa rekisteröinti. (21.)

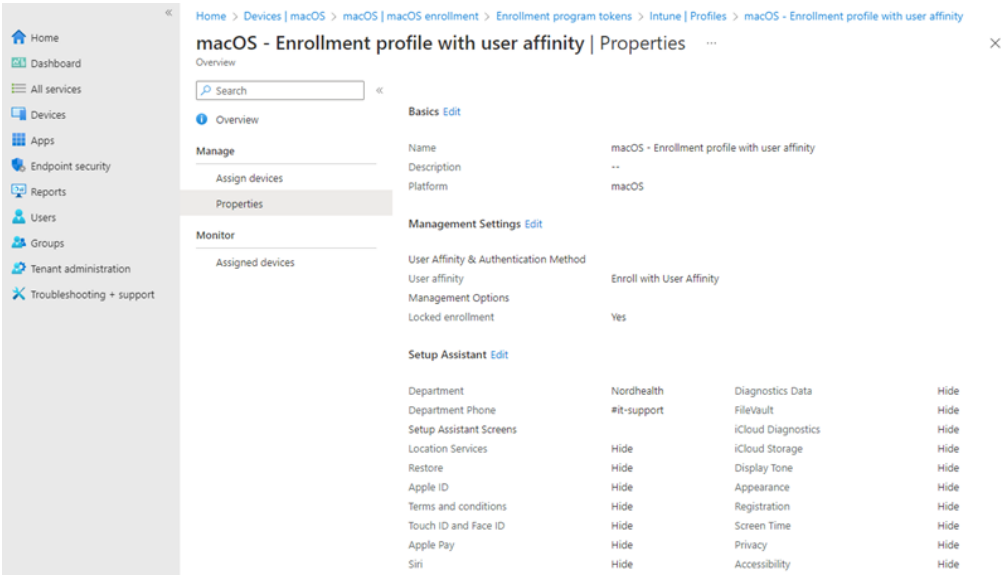
Enrollment Program Token

Apple ADE -token oikeuttaa yrityksen omistamien laitteiden synkronoinnin ABM- ja Intune-palveluiden välillä, ja se tulee uusia vuosittain, jotta palveluiden välinen synkronointi toimii kuten pitää. Määrittely aloitetaan MEM-portaalista ladattavalla Intune Public Key -varmenteella. Varmenneavain on muodoltaan PEM-tiedosto, jolla pyydetään luottamussuhdevarmenne Applen ympäristöstä.

PEM-tiedoston latauksen jälkeen siirrytään Apple Business Manager -portaaliin. On suositeltavaa, että ADE-token allekirjoitetaan yrityksen yhteisellä Apple-järjestelmähallitsijatilillä, jotta token-varmenteen uusiminen ei ole lukittu kenenkään työntekijän henkilökohtaisen tilin taakse. ABM-portaalissa lisätään Intune MDM -palvelin, ja se konfiguroidaan nimeämällä ja lisäämällä aikaisemmin Intune-puolelta ladattu PEM-tiedosto. PEM-tiedoston tallentamisen jälkeen ladataan Applen allekirjoittama versio tiedostosta yrityksen MEM-portaaliin ja lisätään muut tarvittavat yksilölliset tiedot. (21.)

Apple Enrollment -profiili

Enrollment-profiili asettaa laitteelle rekisteröinti- ja jakeluasetukset, ja siinä määritellään, käytetäänkö rekisteröinnissä käyttäjäaffiniteettia, onko se suljettu vai avoin sekä macOS Setup Assistant -vaiheessa käyttäjälle näytettävät vaiheet (kuva 4). Profiili luodaan MEM-portaalissa aikaisemmin luodun ADE-token-varmenteen taakse. Profiilille asetetaan kuvaava nimi ja profiilin tarkoitusta hyvin mukaileva kuvaus. Nimen kanssa kannattaa olla tarkkana, sillä sitä voi jatkossa käyttää dynaamisten ryhmien luomisen yhteydessä, jolloin profiili voidaan asettaa automaattisesti ryhmän jäsenille.



Kuva 4. Apple Enrollment -profiilin konfiguraatio.

Seuraavaksi profiilille määritellään käyttäjäaffiniteetti, eli onko laite käyttäjäkohtainen vai ei. Käyttäjäaffiniteetti rekisteröi laitteen käyttäjälle, kun laitteelle kirjaudutaan ensimmäisen kerran Microsoft-tunnuksilla käyttöönoton tai Company Portal -sovelluksen yhteydessä (37). Koska organisaatiossa jokaisella käyttäjällä on henkilökohtainen kannettava tietokone, otettiin rekisteröinnissä käyttäjäaffiniteetti käyttöön. Tällä valinnalla oli muutamia seuraamuksia, joita käsitellään työssä myöhemmin. Seuraavaksi valitaan jakelutyyppi, eli onko kyseessä lukittu vai avoin jakelu. Lukittu jakelu poistaa käytöstä macOS-laitteilta löytyvän asetuksen, jolla käyttäjät voivat itsenäisesti poistaa hallintaprofiileja. Tuotantoon

vietävässä rekisteröintiprofiilissa tämä asetus kannattaa olla lukittu, jotta käyttäjät eivät voi poistaa hallintaprofiileja laitteiltansa. Vastaavasti avoin jakelu on kuitenkin erittäin hyödyllinen esimerkiksi Intune-implementaation testausta varten, jolloin kannettavalta tietokoneelta voi tässä yhteydessä helposti poistaa turhia tai virheellisiä profiileja.

Enrollment-profiili viimeistellään käymällä läpi viimeinen konfiguraatio-osuus, jossa määritellään macOS Setup Assistant -vaiheet. Käytännössä tämä tarkoittaa sitä, mitkä asetukset piilotetaan tai näytetään käyttäjälle laitteen käyttöönoton yhteydessä ja samalla voidaan lisätä jakelun osastonimi sekä osastopuhelinnumero. Käyttöönoton yksinkertaistamiseksi ja tietoturva mielessä päätettiin IT-osaston toimesta, että Setup Assistant -vaiheesta piilotetaan kaikki Apple ID:hen ja pilveen liittyvät osiot sekä Applelle jaettavat sijainti- ja muut tiedot. Osa näistä tiedoista määritellään laitteille jaettavien hallintaprofiilien toimesta. (21.)

Laitteiden synkronointi

Apple Business Manager -lisäämisen ja Microsoft Endpoint Manager -määritysten jälkeen laitteille voidaan määritellä MDM-palvelin ABM-portaalissa, minkä jälkeen laitteet voidaan synkronoida ABM:n ja MEM:n välillä, jolloin laitteet tuodaan ABM-palvelusta Intunen puolelle. Kun Intune MDM -palvelin on valittu halutuille laitteille ABM-palvelussa, voidaan MEM-portaalissa navigoida projektia varten luodun Enrollment program -tokenin alle, josta on mahdollista synkronoida laitteet. Synkronointia tehtäessä kannattaa kuitenkin pitää mielessä, että Apple on asettanut tietyt rajoitukset laitesynkronointiin palveluiden välillä, jotta liikenne palveluiden välillä pysyy maltillisena.

- Koko laitelista voidaan synkronoida kerran viikossa ABM-palvelusta. Laitteet, jotka on poistettu Intune-palvelusta, mutta ei vapautettu ABM-palvelusta, vaativat täyden synkronoinnin, ennen kuin niitä voidaan synkronoida takaisin Intune-palveluun.
- Laitteet, jotka on vapautettu ABM-palvelussa, voivat viedä 45 päivää, ennen kuin ne poistuvat Intune-laitelistalta automaattisesti. Laitteita voi poistaa yksi kerrallaan manuaalisesti Intunen puolella.

- Synkronointi ajetaan automaattisesti joka 24. tunti, mutta järjestelmävalvoja voi aloittaa synkronoinnin manuaalisesti 15 minuutin välein. Tämä synkronointi päivittää olemassa olevat laitteet ja tuo uudet laitteet, jotka on merkitty Intune-palvelimelle ABM-palvelussa.

Laitteiden synkronoinnin jälkeen niille voidaan määritellä rekisteröintiprofiili MEM-portaalissa. Rekisteröintiprofiili asetetaan Enrollment program -tokenin takaa, josta valitaan aikaisemmin luotu rekisteröintiprofiili laitteen käyttötarkoituksen perusteella. Tässä kohtaa on myös mahdollista valita niin sanottu oletusprofiili kyseisen program tokenin ja palvelimen kautta tuleville laitteille. Tämä voi olla hyödyllinen toiminto, jos tiedetään, että kaikki tätä kautta Intune-hallinnan piiriin tuotavat laitteet käyttävät samaa profiilia. Laitteiden synkronoinnin ja rekisteröintiprofiilin määrittelyn jälkeen laitteiden rekisteröinti voidaan käytännössä aloittaa testaukseen tarkoitetuilla laitteilla. (21.) On suositeltavaa luoda tuotantoon vietävät konfiguraatioprofiilit, käytänteet ja sovellukset ennen, kuin rekisteröinti ja jakelu aloitetaan loppukäyttäjien laitteilla, jotta kaikki saadaan vietyä laitteille kerralla ja laitteet ovat heti käyttövalmiita käyttäjille.

5.4 Konfiguraatioprofiilit

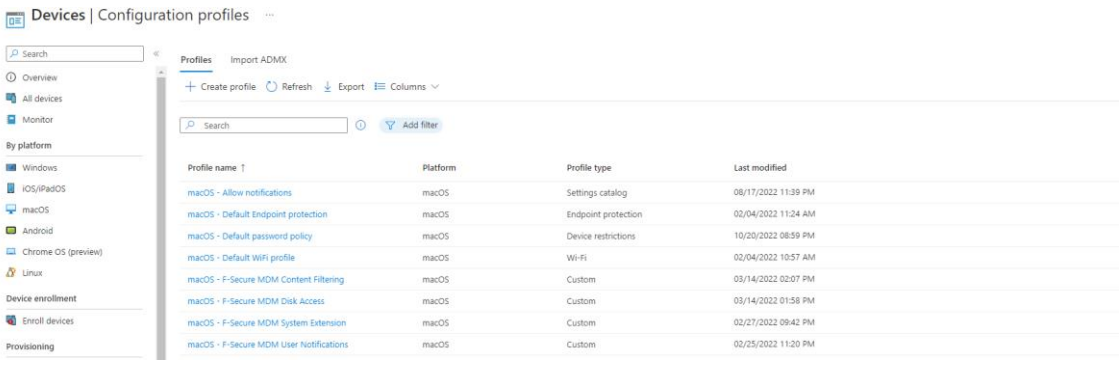
Microsoft Intune sisältää sisäänrakennettuja ja mukautettuja konfiguraatioprofiileita, jotka ovat käytännössä laiteasetuksia, joita voidaan jakaa laitteille yksilö- tai ryhmäkohtaisesti rekisteröinnin yhteydessä tai sen jälkeen. Näillä profiileilla on mahdollista muun muassa asettaa tietoturvapakotteita laitteelle, kuten salasanan minimipituus ja laitteen käyttöönoton osittainen automatisointi asetusten osalta. Mukautettujen profiilien kohdalla on kuitenkin tärkeä tiedostaa, että niitä ei kannata käyttää arkaluontoisen tiedon käsittelyyn, vaan tätä varten kannattaa käyttää sisäänrakennettuja profiileita, jotka on konfiguroitu tiettyä käyttötarkoitusta varten. (38.)

MacOS-laitteille jaettaessa konfiguraatioprofiilit ilmestyvät laitteen System Preferences -asetuksista löytyvän Profiles-valikon alle, jossa niistä voidaan tarkastella ja Apple Enrollment -profiilin asetusten mukaan mahdollisesti poistaa

käytöstä. Intune-rekisteröinnin jäljiltä laitteille jaetaan oletushallintaprofiili, jonka lisäksi tarkoitus on konfiguroida laitteille muutama Intunen valmis profiilipohja:

- *Endpoint Protection* -profiili sisältää FileVault-laitesalaus- ja palomuurikäytännöt. Profiili pakottaa toiminnot käyttöön, ja niitä voidaan konfiguroida Applen asettamien rajojen puitteissa.
- *Device Restrictions* -profiili sisältää muun muassa salasanakäytännön. Profiili pakottaa salasanan käyttöön paikallisella tilillä ja valvoo, että se täyttää profiilissa käytetyt salasanan minimivaatimukset.
- *Wi-Fi*-profiili voidaan konfiguroida yhdistämään automaattisesti yrityksen toimistojen Wi-Fi-verkkoihin. Konfigurointi tapahtuu mallintamalla asetukset toimiston verkkojen ominaisuuksiin perustuen.
- *Settings Catalog* -profiili sisältää laiteilmoituksien asetukset, joilla voidaan sallia esimerkiksi eri sovellusten työpöytäilmoitukset käyttäjille ilman, että heidän tarvitsee erikseen käydä sallimassa niitä.

Oletuskonfiguraatioiden lisäksi Intuneen lisätään muutama mukautettu WithSecure-antiviruskohtanen profiili. Mukautetut profiilit käyttävät hyödykseen XML- tai PLIST-kieltä salliakseen sovellukselle laajemman pääsyn paikallisen laitteen resursseihin, jotta asennus toimisi odotetusti. Konfiguraatioprofiileita voidaan lisätä MEM-portaalin *Devices*-kategorian alta löytyvästä *Configuration profiles* -näkymästä (kuva 5).



Kuva 5. Yrityksen käytössä olevat Intune-konfiguraatioprofiilit.

WithSecure-tapauksessa profiilit ovat mukautettuja profiileja, joita ei voi konfiguroida Intune GUI -näkymästä ollenkaan, sillä niille ei ole toimivaa pohjaa valmiina. Mukautetuissa profiileissa asetukset ja muutokset tulee konfiguroida itse käyttämällä XML- tai PLIST-merkintäkieltä tai vaihtoehtoisesti esimerkiksi

sovelluksen kehittäjältä saatavia konfiguraatioita. Valmis tiedosto viedään MEM-portaalissa luodun profiilin konfiguraatiokenttään. (38.) Tässä työssä käytettiin neljää mukautettua profiilia WithSecure Antivirus -sovelluksen toiminnan edesauttamiseksi. Kukin profiili muutti jonkin macOS-asetuksen, jotta sovelluksella olisi laajempi pääsy laitteen resursseihin. PLIST-tiedostot, jotka profiileihin ladattiin, perustuivat WithSecurelta saatuihin pohjiin (39).

FileVault-levynsalauksen ja paikallisen tilin salasanapakotusten ja -vaatimusten kohdalla on muutamia asioita, jotka kannattaa huomioida käyttöönoton ja konfiguroinnin yhteydessä. FileVaultin käyttöönotto ei ole täysin mutkatonta, sillä laitteille, joissa on jo ennalta käytössä FileVault-levynsalaus, ei voida salausavainta luoda uusiksi Intunen kautta. Tämä tarkoittaa sitä, että palautusavain ei siirry automaattisesti Intuneen. Organisaation tapauksessa tämä ei keskitettyä hallintaa lukuun ottamatta ollut suuri ongelma, sillä tapauksissa, joissa laitteella on FileVault käytössä, on palautusavain myös varmuuskopioitu talteen IT-osaston ylläpitämään ympäristöön.

Password-käytännössä profiilin salasanakonfiguraatiossa on useita eri monimutkaisuusasetuksia, joita voidaan hyödyntää vahvan salasanan pakottamiseksi laitteiden paikalliselle järjestelmähaltijatilille (40). Testivaiheessa kuitenkin huomattiin, että monimutkainen salasana ei ole järkevä ratkaisu, sillä se on työläs muistaa ja kirjoittaa. Salasanan kohdalla päädyttiin siihen, että kaikki muut vaatimukset poistettiin paitsi salasanan minimipituus, joka on tällä hetkellä 13 merkkiä. Salasanaprofiilia muokattaessa on hyvä pitää mielessä, että jokainen muutos salasana-asetuksiin pakottaa uuden paikallisen salasanan asettamisen enrolled-laitteilla, vaikka salasana täyttäisi entuudestaan profiilin minimivaatimukset. Toinen huomion aihe Intunen salasanakonfiguraatioissa on *Block simple passwords* -asetus, joka estää yksinkertaisten salasanojen käyttämisen. Asetus estää lukujonot ja toistuvat merkit, mutta se ei toimi kovin hyvin suomen kielen kanssa, sillä se estää sanojen käytön, joissa on kaksi peräkkäistä samaa kirjainta.

5.5 Sovellushallinta ja -jakelu

Sovellusten jakelu päätelaitteille on yksi projektin kriittisimmistä osuuksista ja perusedellytys projektin onnistumiselle. Intune MDM:n avulla sovelluksia voidaan jakaa käyttäjille käytännössä kahdella eri tavalla: pakotettu asennus ja vapaaehtoinen asennus Company Portal -sovelluksen kautta. Sovellusten jakelu voidaan määritellä eri käyttäjille ja ryhmille näiden tarpeiden tai pakotteiden perusteella (41). Esimerkiksi tietoturvaohjelmisto on luonteeltaan olennainen sovellus jokaiselle laitteelle, minkä vuoksi se voidaan määritellä sovelluksen jakeluasetuksissa pakolliseksi, kun taas Microsoft 365 -ohjelmistot eivät ole olennaisia ja voidaan lisätä Company Portal -jakeluun. Jakelun ja hallinnan lisäksi kaikkien Intunen kautta jaettujen sovelluksien tilaa voidaan seurata jälkikäteen sovelluksen yleiskatsaussivulta MEM-portaalissa

Intune MDM -palvelun avulla macOS-laitteille voidaan jakaa sovelluksia erityyppisinä riippuen yrityksen tarpeista (41), mutta tässä projektissa keskityttiin näistä kolmeen: Microsoft-sovellukset, Line-of-Business-sovellukset ja macOS shell -asennusskriptit. Näillä jakelutyypeillä saadaan jaettua yrityksen määrittelemät tarpeelliset sovellukset macOS-laitteille. Jakelua käyttäjille hallitaan pääasiassa AAD-ryhmiä käyttäen, ja jakelun tilaa voidaan seurata MEM-portaalista.

Microsoft-sovellukset ovat Microsoftin kuratoimia sovelluksia, joille on Endpoint-portaalissa oma sovellustyyppinsä, esimerkiksi Microsoft 365 Apps. Näiden sovellusten jakelu voidaan toteuttaa esimerkiksi Company Portal -sovelluksen kautta, eivätkä ne vaadi konfiguraatiota. Line-of-Business-sovellukset ovat vuorostaan joko yrityksen itsensä tekemiä mukautettuja ratkaisuja tai kolmannen osapuolen sovelluksia. Yritys toimittaa itse asennuspaketin joko Intunemac- tai pkg-pakettimuodossa Intune-palvelimelle. macOS shell -asennusskripti jaellaan päätelaitteelle Intune Agentin avulla, jossa skripti ajetaan paikallisesti. Shell-skriptit mahdollistavat sovellusasennukset ja laitemääritykset, jotka eivät ole teknisesti mahdollisia tai käytännöllisiä suoraan Intune-palvelun kautta. (42.)

Line-of-Business-sovellukset ja pkg-paketit

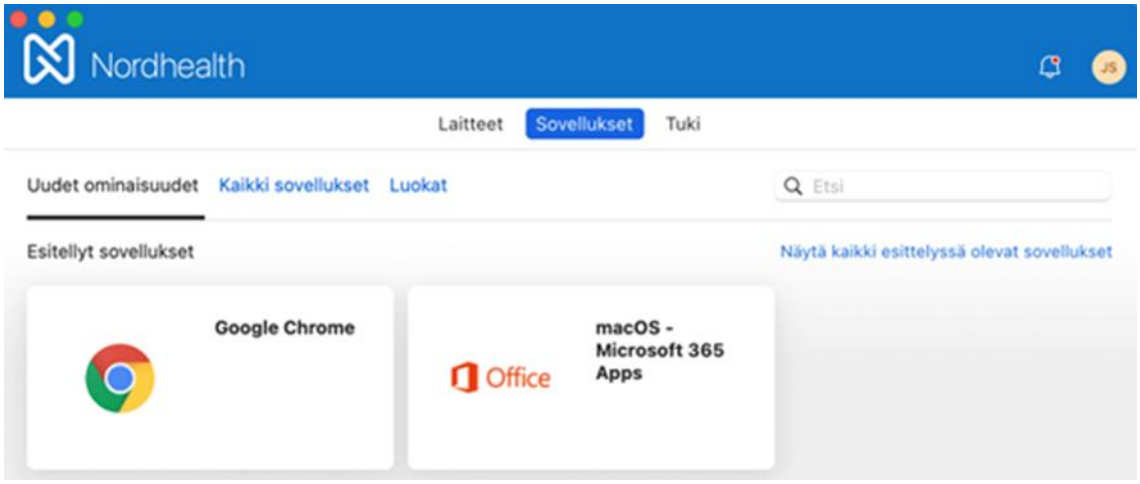
Line-of-Business eli LoB-sovellukset ovat sovelluksia, jotka lisätään Intune-hallintaan jaettaviksi asennuspaketteina. Lisättävät sovellukset ovat macOS-tapauksessa pkg-paketteja. Pkg on Applen käyttämä tiedostojen kompressointi- ja paketointiformaatti, joita käytetään pääasiassa sovellusten asennuksissa. Laitehallinnan osalta LoB-sovellusjakelu on hyödyllinen yksinkertaisten yhden sovelluksen pakettien jakelutilanteissa, jos halutaan jakaa pakotettuja asennuksia AAD-ryhmiin perustuen tai mahdollistaa vapaaehtoinen asennus Company Portal -sovelluksen kautta.

Työn kirjoittamisen aikana Intune MDM -palvelun Line-of-Business-sovellusten jakelussa tapahtui muutos, joka mahdollistaa pkg-pakettien suoran lisäämisen Intune-sovellusjakeluun. Ennen elokuuta 2022 jaettavat asennuspaketit täytyi uudelleen paketoida intunemac-muotoon käyttämällä Microsoftin IntuneAppUtil-työkalua (43). Intunemac-paketit olivat ongelmallisia tilanteissa, joissa paketit sisälsivät useampia sovelluksia. Microsoft suosittelikin jakamaan vain yksinkertaisia yhden sovelluksen paketteja LoB-toimintoa käyttäen. Ongelmaksi pakettien kohdalla muodostui, että Intune ei osannut yhdistää sovellusten App bundle ID -identiteettejä keskenään ja toisena ongelmana pienimmätkin muutokset pakettien sisäisiin tiedostoihin vaativat sovelluksien uudelleen paketoinnin, jolloin Apple vaatii paketille Developer ID -varmenteen.

Company Portal -sovelluksen jakelu ja konfiguraatio

Company Portal -sovellus voidaan lisätä Intune-jakeluun Line-of-Business-tyyppinä ja pakottaa asennus jokaiselle käyttäjälle käyttämällä aikaisemmin luotua AAD-jakeluryhmää *macOS – MDM*, jolloin sovellus asentuu jokaiselle laitteelle rekisteröinnin yhteydessä (44). Company Portal -sovellukseen voidaan lisätä käyttäjille jaettavia sovelluksia MEM-portaalin kautta hyödyntämällä AAD-ryhmiä (45). Konfiguroinnin jälkeen käyttäjät voivat kirjautua Company Portal -sovellukseen organisaatioon luoduilla henkilökohtaisilla Microsoft-tunnuksillansa,

minkä jälkeen he voivat asentaa heille AAD-ryhmillä jaettuja sovelluksia vapaaehtoisesti (kuva 6).



Kuva 6. Company Portal -sovelluksen Sovellukset-välilehti.

Company Portal -sovelluksella on myös mahdollista jakaa sovelluksia käyttäjille, joiden laitteita ei ole rekisteröity Intune-hallintaan. Sovellukset voivat olla yrityksen omia sovelluksia tai yleisiä sovelluksia, joiden asentamista halutaan helpottaa kokoamalla ne yhteen paikkaan. Toiminto on erityisen hyödyllinen tapauksissa, joissa halutaan jakaa tiettyjä sovelluksia esimerkiksi yrityksen ulkopuolisille konsulteille tai yhteistyökumppaneille. (45.)

macOS-Bash-skriptit ja Intune Agent

Apple macOS-Bash-skriptit ovat tiedostoja, joissa yhdistetään yksi tai useampi UNIX-komento yhdeksi kokonaisuudeksi, ja skriptiä kutsuttaessa komennot suoritetaan siinä määritellyssä järjestyksessä. Intunen macOS-rekisteröintitapauksessa Bash-skriptejä voidaan käyttää Intune-laitehallinnan toimintojen laajentamiseksi ja sellaisten sovellusten jakamiseen, joita ei voida asentaa muilla keinoilla tai joiden asennus vaatii muuta mukauttamista. Skriptien ajamisen hallituilla laitteilla mahdollistaa Intune Agent -sovellus, joka jaetaan laitteille, joille on MEM-portaalissa lisätty vähintään yksi skripti. (46.)

Intune Management Agent on tarpeellinen sovellus macOS-laitteilla, joilla halutaan suorittaa Intune-hallinnan kautta jaettuja skriptejä. Intune Agent mahdollistaa kehittyneemmän laitteenhallinnan toiminnoilla, joita macOS ei tue luonnostaan. Sovellus jaetaan laitteille niin sanottuna *silent installation* -tyyppinä, mikä tarkoittaa sitä, että sovellus asennetaan käyttöjärjestelmän kulisseissa, eikä sitä päällepäin näy loppukäyttäjälle. Agentin toiminta perustuu Intune-hallinnan kanssa käytyyn todentamiseen kahdeksan tunnin välein, ennen kuin Bash-skriptit jaetaan laitteelle, minkä jälkeen vastaanotettu skripti ajetaan paikallisella laitteella sille määriteltyjen konfiguraatioiden perusteella. (47.) Bash-skriptejä jaetaan käyttäjille MEM-portaalista käsin lisäämällä ne macOS- alaosaston alta löytyvästä *Scripts*-kategoriasta. Bash-skriptit jaetaan niitä tarvitseville käyttäjille AAD-ryhmiä käyttäen.

Yrityksen macOS-jakelussa Bash-skriptejä käytetään toistaiseksi kahteen tarkoitukseen, joista ensimmäinen on laitteiden verkkonimien muuttaminen muotoon FNSLT-*sarjanumero* (esimerkkikoodi 1) ja toinen on yrityksen WithSecure-virustorjuntasovelluksen jakelu (liite 1). Verkkonimen muuttaminen vaatii yksinkertaisen Bash-skriptin, joka koostuu vajaasta kymmenestä rivistä komentoja.

```
#!/usr/bin/env bash

# Get the Serial Number of the Machine
sn=$(system_profiler SPHardwareDataType | awk '/Serial/ {print $4}')

# Set the ComputerName, HostName and LocalHostName
scutil --set ComputerName "FNSLT-$sn"
scutil --set HostName "FNSLT-$sn"
scutil --set LocalHostName "FNSLT-$sn"
dscacheutil -flushcache
```

Esimerkkikoodi 1. macOS-Bash-skripti, joka muuttaa paikallisen laitteen verkkonimen kuvastamaan laitteen uniikkia sarjanumeroa. Intune Agent -sovellus ajaa Bash-skriptin kutsumalla sitä, kun skripti on jaettu laitteelle Intune-hallinnasta.

Verkkonimen muutos -Bash-skripti ajetaan laitteilla sen takia, että Intune-hallintaan saadaan päivitettyä uniikit laitenimet, joita voidaan tarvittaessa verrata IT-osaston ylläpitämään erilliseen laitehallintaan. Vastaavasti verkkonimen muutos

edesauttaa myös yrityksen WithSecure-antivirusseurantaa, jossa laitteita monitoroidaan verkkonimen perusteella.

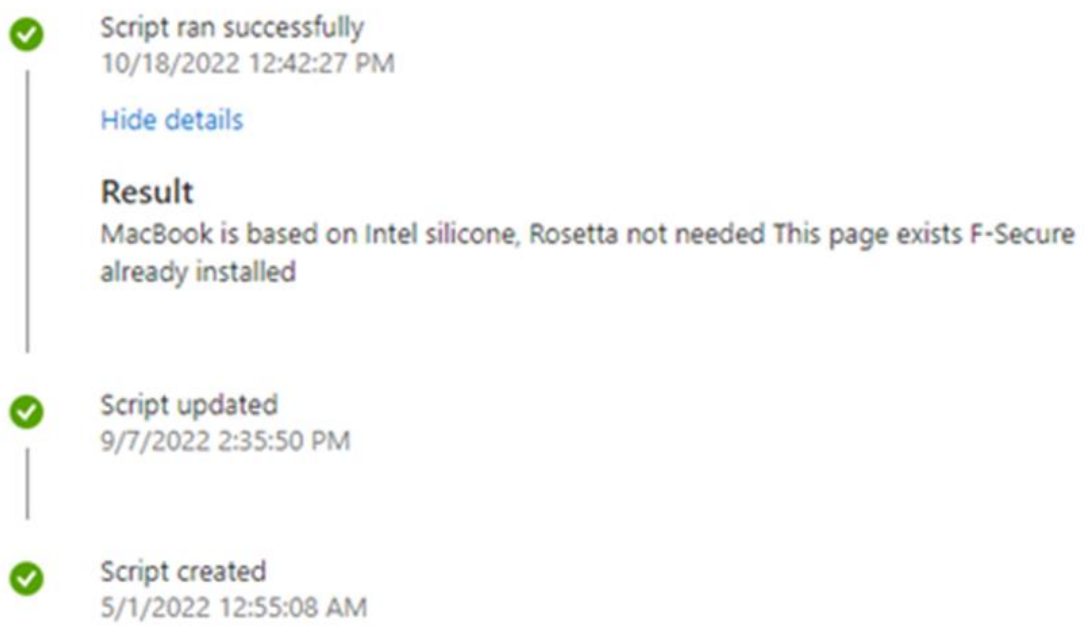
WithSecure-Bash-skripti on komentosarjakokonaisuus, jonka päätarkoitus on ladata, asentaa ja konfiguroida WithSecure-sovellus macOS-laitteille paikallisesti. WithSecure-sovelluksen LoB-asennusongelmien vuoksi päädyttiin lopputulokseen, että skriptiasennus on luotettavampi tapa sovelluksen jakeluun. Skriptissä hyödynnetään WithSecuren verkossa isännöimää mpkg-asennuspakettia, joka ladataan laitteelle paikallisesti asennusta varten. Liitteen 1 Bash-skriptissä käytetyt muuttujat on listattu tiedoston alkuun Bash-skripti-identifikaation *#!/bin/bash* jälkeen.

- sas-muuttuja viittaa WithSecuren isännöimän asennuspaketin lataukseen käytettyyn verkko-osoitteeseen, jota käytetään sivun olemassaolon varmistamiseen ja paketin lataamiseen laitteelle.
- mpkgfile-muuttuja viittaa ladattavalle sovellukselle tallennussijainnin, jota voidaan käyttää myöhemmin Bash-skriptissä myös asennuspaketin poistamiseen.
- profile_id-muuttuja viittaa WithSecure-virustorjunnan sisällä käytetyn macO -profiilin identifiointiin, jotta asennettu laite kirjataan halutun profiilin alle.
- activation_key-muuttuja viittaa yrityksen WithSecure-asennuksen aktivointiavaimeen, jota käytetään asennuksen jälkeen sovelluslisenssin aktivoimiseen.

Muuttujien perustamisen jälkeen lisätään komennot. Liitteen 1 Bash-skriptissä on käytetty *if else* -ehtoja, joiden avulla varmistetaan yhteensopivuuksia, joiden täytyttyä voidaan skriptin ajamista jatkaa. Vastaavasti tilanteissa, joissa ehdot eivät täyty, skriptin ajaminen keskeytetään exit-komennolla.

- Skripti aloitetaan tiedustelemalla laitteelta, perustuuko sen prosessori Intel x86- vai Apple M1-arkkitehtuuriin, jonka perusteella Intel-laitteille asennetaan Rosetta 2 -emulaatio-ohjelmisto x86-arkkitehtuurin sovellusten käyttöä varten.
- Seuraavaksi varmistetaan, onko WithSecure-sovelluspaketin URL tavoitettavissa.
- Jos URL on tavoitettavissa, laitteelta varmistetaan, onko siihen jo asennettu WithSecure-virustorjunta käyttöön.

- Jos sovellusta ei ole vielä asennettu laitteelle, se ladataan verkko-osoitteen takaa laitteelle, minkä jälkeen se asennetaan /Applications-kansioon.
- Sovellus aktivoidaan yrityksen profiili-ID:tä ja aktivointiavainta käyttäen ajamalla *WithSecure activator* -ohjelma annetuilla muuttujilla.
- Lopuksi skripti siivoaa ladatut paketit poistamalla ne laitteelta.



Kuva 7. Laitekohtaiset Bash-skriptin ajovaiheet.

Laitteille jaettujen skriptien tilaa voidaan seurata MEM-portaalista käsin navigoimalla halutun skriptin tietoihin, josta voidaan valita haluttu tila käyttäjän tai laitteen perusteella. Ajettujen skriptien kohdalla voidaan laitetilan takaa käydä tarkistamassa onnistuneiden ajojen jälkeen, mitkä vaiheet skriptissä on käyty läpi skriptin echo-komentoihin perustuen (kuva 7). Tämä on hyödyllinen toiminto skriptien ongelmatilanteissa, sillä tulostettujen echo-viestien perusteella nähdään, mitkä skriptin vaiheet on ajettu onnistuneesti ja missä kohtaa ajo on lopetettu.

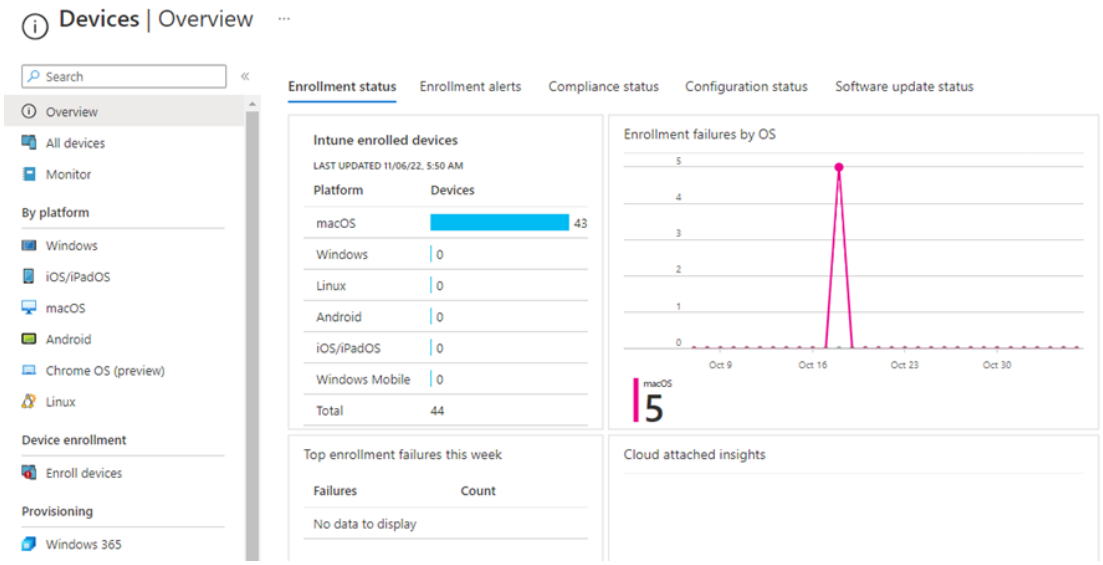
5.6 macOS-laitejakelu Intune-palvelimelta

Kannettavien macOS-tietokoneiden rekisteröinti laitehallinnan piiriin voidaan aloittaa, kun ABM- ja Intune-ympäristöt on määritelty ja Intunen puolelle on lisätty käyttöönoton kannalta olennaiset konfiguraatioprofiilit ja sovellukset. Jakelu voidaan toteuttaa automaattisesti ADE-jakelua käyttäen tai manuaalisesti Intune Company Portal -sovelluksen kautta.

ADE-rekisteröidyn laitteiden tapauksessa rekisteröity laite täytyy määritellä Intune-palvelimelle ABM-portaalissa, minkä jälkeen laite synkronoituu MEM-portaalin puolella ja laitteelle määritellään aikaisemmin luotu rekisteröintiprofiili. Käyttäjälle lisätään Enterprise Mobility + Security E3 -lisenssi ja hänet lisätään jakelua varten luotuun *macOS – MDM* AAD-ryhmään. Näiden käyttäjä- ja laitekohtaisten esivalmisteluiden jälkeen kannettava macOS-tietokone on valmis MDM-jakeluun. ADE-rekisteröityä kannettavaa tietokonetta ensi kertaa käyttöönotettaessa edetään *Setup Assistant* -vaiheita normaalisti, kunnes verkkoon liittymisen jälkeen käyttäjältä kysytään Nordhealth Oy:n alaisia Microsoft-tunnuksia. Kirjautumisen jälkeen laite ottaa yhteyttä MDM-palvelimelle ja asettaa laitteen käyttöönottoa varten rekisteröintiprofiilin mukaiset asetukset. Setup Assistant -vaiheen jälkeen laite siirtyy macOS-työpöydälle ja alkaa lataamaan sille AAD-ryhmillä asetettuja konfiguraatioprofiileita, sovelluksia ja skriptejä. Jos ADE-rekisteröity laite on jo otettu käyttöön, mutta sitä ei ole liitetty Intune MDM -jakelun piiriin, se voidaan liittää komentorivikomentoa käyttäen. (6.)

Company Portal -jakelu tapauksessa ADE-osuudessa mainittuja esivalmisteluita ei tarvitse tehdä. Käyttäjälle lisätään tarvittava Intune-lisenssi ja jakeluun tarkoitettu AAD-ryhmä, minkä jälkeen laite käyttöönotetaan tavalliseen tapaan. Setup Assistant -osuuden jälkeen se voidaan liittää Intune MDM -jakelun piiriin Company Portal -sovelluksen kautta. Käyttäjä seuraa IT-osaston kirjoittamaa ohjeistusta yrityksen sisäverkosta. Asennuksen jälkeen sovellukseen kirjaudutaan organisaation alaisilla Microsoft-tunnuksilla ja sovellus ohjeistaa käyttäjän asentamaan hallintaprofiilin. Hallintaprofiilin jälkeen laite on käytännössä katsoen samassa tilassa kuin ADE-rekisteröity laite Setup Assistantin jäljiltä.

Laitteiden liityttyä Intune MDM -jakelun piiriin ne ilmestyvät MEM-portaalin Devices-näkymään (kuva 8) ja niille alkaa automaattinen konfiguraatioprofiilien, käytänteiden ja sovellusten jakelu. Profiilien jakelun jälkeen laite pyytää käyttäjää ottamaan FileVault-laitesalauksen käyttöön ja syöttämään uuden salasanan minimivaatimusten mukaan. Laitteen verkkonimen muutos ja virustorjunnan asennus ajetaan automaattisesti taustalla Bash-skriptillä, ja Company Portal -sovellus ladataan tarvittaessa LoB-sovelluksena Intune-palvelusta. Jakelun jälkeen laite on käyttövalmis ja suojattu kokonaisuus, jota käyttäjä voi käyttää työntekoon.



Kuva 8. Devices-kategorian yleisnäkymä.

Jakelun aikana ja jälkeen laitetta voidaan seurata MEM-portaalin kautta *Devices*-kategorian alta. Sivulta on mahdollista seurata koko laitekantaa ja laitteiden rekisteröintitilaa eri alakategorioiden perusteella, joiden avulla voidaan keskittyä esimerkiksi pelkästään yhden tietyn konfiguraation jakelun tilaan. Yleisnäkymä on erityisen hyödyllinen nopeisiin tilannekatsauksiin, sillä se kerää olennaista dataa yhteen näkymään koko laitekannasta, jolloin suurien laitemäärien yhtäaikainen seuraaminen helpottuu. Näkymästä on mahdollista navigoida laitteiden tilan perusteella yksittäisten laitteiden näkymään, josta voidaan lähteä diagnosoimaan vikatilanteita virhekoodien ja -lokien perusteella.

6 Tulokset ja pohdinta

Microsoft Intune mahdollistaa nykyisessä muodossaan tehokkaan kannettavien macOS-tietokoneiden keskitetyn laitehallinnan eikä kärsi enää yhtä vakavasti muutaman vuoden takaisesta vajaasta tuesta. Projektin alussa ja aikana asetetut tavoitteet saavutettiin Intune-hallinnan tarjoamin keinoin, ja ongelmatilanteisiin löytyi aina ratkaisu tai vaihtoehtoinen lähestymistapa. Työn aikana luotujen konfiguraatioiden, määrittelyiden ja testien pohjalta Intune-palvelu saatiin tuotantovalmiiksi, ja se otettiin käyttöön työn tilanneen yrityksen toimesta.

Työn tuloksena oli tuotantovalmis palvelu ja prosessi, jossa yritykselle hankitut macOS-laitteet rekisteröidään ja viedään ABM- ja Intune-ympäristöihin. Laitteiden nollakosketusjakelutavoitteeseen päästiin, ja loppukäyttäjälle suoraan tukkuliikkeeltä tilattu laite saadaan automaattisesti käyttöönoton yhteydessä Intune-jakelun piiriin, josta sille jaetaan tarvittavat rajoitukset, pääsyt ja sovellukset. Vanhojen laitteiden kohdalla saatiin onnistuneesti otettua käyttöön myös Company Portal -sovellus, jonka kautta laitteet voidaan rekisteröidä hallinnan piiriin.

Microsoft Intunen ja Azure AD:n kanssa työskennellessä oli tiedostettava, että kyseessä ovat valtavat pilvipohjaiset kokonaisuudet. Palveluiden luonteen vuoksi pienetkin muutokset ympäristöön saattoivat viedä aikaa, ennen käytäntöön tulemista. Toimintojen testaaminen ja virhetilojen ratkominen vei yhä enemmän aikaa, kun pyydetyt muutokset synkronoituvat ympäristöjen välillä. Prosessia vaikeutti myös, ettei toimintotilaa välttämättä nähnyt jokaiselle toiminnolle. Microsoftilla on selvästi vielä kehitettävää ympäristöjen käyttöliittymissä.

Intune-palveluun konfiguroidut skripti-, sovellus- ja profiilijakelut onnistuvat jakelun piiriin kuuluville kannettaville tietokoneille valtaosan ajasta, mutta epäonnistuvat välillä yksittäisistä päätelaitekohtaisista syistä. Intune-palvelun tarjoama laaja laitekannan seurausmahdollisuus MEM-portaalin kautta on erittäin hyödyllinen kannan tilan yleiseen seuraamiseen, mutta taipuu myös yksittäisten laitteiden tarkkaan virhetilojen seurantaan. Testivaiheessa yksittäisten laitteiden

seuraaminen laitekohtaisesti oli helppoa, kun laitteen tilan tapahtumista ja muutoksista oltiin tietoisia etukäteen. Loppukäyttäjien laitteiden kohdalla tilanne on kuitenkin eri, kun laitteiden tilat ja muutokset ovat odottamattomia, minkä vuoksi yleisnäkymän seuraamisesta tuli kriittinen osa työtä jakelun testaamista.

Yrityksen IT-osaston työtaakan kannalta Intune-hallinnan implementaatio oli eduksi. Työn määrä jakelussa ja käyttöönotossa väheni huomattavasti, mikä pantiin merkille jo testilaitteiden kohdalla. Isoimmaksi eduksi Intune-hallinnassa muodostui laitteiden turvaamisen automatisointi, joka oli tähän asti ollut työläin ja epävarmin osuus IT-osaston laitehallinnassa. Laitteiden tietoturvatilan seuraaminen MEM-portaalissa sekä FileVault-levynsalauksen, paikallisen tilin salasanan ja tietoturvaohjelman asennuksen pakottaminen poisti epävarmuutta laitteiden tietoturvan osalta.

Microsoft Intune ja sen ympäröimät ympäristöt ovat erittäin laajoja kokonaisuuksia, minkä vuoksi projektin ja kirjoitustyön aikataulutus ja laajuus eivät pysyneet täysin alkuperäisissä arvioissa. Microsoftin tarjoamat ensimmäisen osapuolen dokumentaatiot ja ohjeistukset auttoivat kuitenkin työn etenemisen ja itseopiskelun osalta valtavasti, ja suuri osa työstä oli mahdollista tehdä itsenäisesti. Insinöörityö projektin ja kirjoittamisen aikana Microsoft Intune -palvelun ominaisuudet ja ohjeistukset päivittyivät useampaan kertaan. Intune on jatkuvassa kehityksessä, joten muutaman aihepiirin kohdalla dokumentaatiota täytyi lukea uudestaan ja implementaatiota muuttaa päivitysten mukaisiksi. Tämä vaikeuttaa myös yrityksen sisäisten dokumentaatioiden ja käyttäjäohjeistuksien kirjoittamista ja ylläpitoa, sillä niitä joutuu jatkuvasti päivittämään ajan tasalle.

Työn aikana kerrytetyn kokemuksen ja tietotaidon pohjalta todennäköisesti jatkan yrityksen Intune-hallinnan jatkokehityksessä ja ylläpidossa. Yrityksellä on aikeena Windows-laitteiden jakelun aloittaminen Intune-palvelun avulla, johon voidaan osittain hyödyntää macOS-laitteiden jakeluun käytettyjä konfiguraatioita ja tietämystä. Lisäksi tarkoituksena on myös laajentaa macOS-puolen implementaatiota nykyisestä, kunhan ensin on saatu koko yrityksen laitekanta vietyä Intune MDM -jakelun piiriin.

7 Yhteenveto

Insinöörityössä selvitettiin Intune-palvelun soveltuvuutta tilaajayrityksen kannettavien MacBook-tietokoneiden keskitettyyn hallintaan. Työn tavoitteena oli rakentaa hallintakokonaisuus, jolla automatisoidaan laitteiden monivaiheista käyttöönottoprosessia, turvaamista ja valvomista, jotta käyttäjävirheiden määrä ja IT-osaston työtaakka vähentyisivät ja laitteilla olisi käyttöönoton yhteydessä vakiotietoturvakäytänteet. Yrityksen aikaisemmassa hallinnassa laitteiden tila ja käyttöönottoprosessi olivat usein IT-osaston pääsyn ulkopuolella.

Selvitystyön perusteella rakennettu MacBook-tietokoneiden keskitetty hallinta, jakelu ja turvaaminen Intune-palvelun avulla onnistui odotetusti. Työn tuloksena oli kokonaisuus, jossa yritykselle Apple Automated Device Enrollment -ohjelmalla rekisteröity laite saadaan määriteltyä Apple Business -ympäristöstä Intune-laitehallinnan piiriin. Lisäksi voidaan rekisteröidä laitteita, joita ei ole ADE-rekisteröity, käyttämällä Intune Company Portal -sovellusta hallintaprofiilien jakeluun. Rekisteröidyt laitteet saavat verkon yli haettua niille Intune-palvelussa määritellyt Azure Active Directory -ryhmäkohtaiset sovellukset, asetukset, käytänteet ja resurssit.

Työssä perehdyttiin erityisesti sovellusten jakeluun eri paketointimuodoissa, shell-skriptikonfigurointiin ja määrityskäytäntöprofiileihin. Näillä varmistettiin, että laitteiden käyttöönotto tilanteessa käyttäjä saa mahdollisimman valmiin laiteasennuksen, jonka prosessi olisi yksinkertainen ja selkeä. Välttämällä käyttäjävirheitä, automatisoimalla prosesseja ja keskittämällä laitteiden hallinta ja seuraaminen yhteen ympäristöön saatiin vähennettyä IT-osaston työmäärää ja parannettua laiteturvallisuutta.

Jatkokehityksenä työlle voitaisiin laajentaa macOS-laitteiden hallinnasta myös Windows-laitteiden hallintaan ja jakeluun. Jatkokehityksessä voidaan osittain hyödyntää samoja konfiguraatioita ja perustettuja ympäristöjä. Näin saataisiin yrityksen koko laitekanta saman hallinnan piiriin.

Lähteet

1 Company. Verkkoaineisto. Nordhealth. <https://nordhealth.com/company/>. Luettu 20.5.2022.

2 Mixon, Erica. 2020. Mobile device management (MDM). Verkkoaineisto. TechTarget. <https://www.techtarget.com/searchmobilecomputing/definition/mobile-device-management>. Luettu 20.5.2022.

3 Keinänen, Katja. A Complete Guide to Mobile Device Management (MDM). Verkkoaineisto. Miradore. <https://www.miradore.com/blog/mdm-mobile-device-management/>. Luettu 20.5.2022.

4 Why mobile device management is important. Verkkoaineisto. IBM. <https://www.ibm.com/topics/mobile-device-management>. Luettu 27.5.2022.

5 Apple Deployment Programs Device Enrollment Program Guide. 2017. Verkkoaineisto. Apple. <https://www.apple.com/mx/business-docs/DEP_Guide.pdf>. Luettu 20.5.2022.

6 Automatically enroll macOS devices with the Apple Business Manager or Apple School Manager. 2022. Verkkoaineisto. Microsoft. <https://docs.microsoft.com/en-us/mem/intune/enrollment/device-enrollment-program-enroll-macos>. Luettu 20.5.2022.

7 Intro to Apple Configurator. Verkkoaineisto. Apple. <https://support.apple.com/guide/apple-configurator-mac/intro-to-apple-configurator-cadf1802aed/mac>. Luettu 20.5.2022.

8 What is Microsoft Intune app management? 2022. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/mem/intune/apps/app-management>. 31.10.2022. Luettu 3.11.2022.

9 Ohjeita turvalliseen etätyöhön. 2021. Verkkoaineisto. Huoltovarmuusorganisaatio. <https://www.huoltovarmuuskeskus.fi/files/7f58b0da92e4f19003e0c4a7337c71c8c37c5bef/ohjeita-turvalliseen-etatyohon.pdf>. Luettu 17.9.2022.

10 Näin pidät huolta tietoturvasta kotona ja työpaikalla. 2020. Verkkoaineisto. Kyberturvallisuuskeskus. <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-pidat-huolta-tietoturvasta-kotona-ja-tyopaikalla>. 21.7.2020. Luettu 17.9.2022.

11 Woude, Peter. 2020. Learn 5 Microsoft Intune security features for mobile admins. Verkkoaineisto. TechTarget. <https://www.tech-target.com/searchmobilecomputing/tip/Learn-5-Microsoft-Intune-security-features-for-mobile-admins>. 9.10.2020. Luettu 17.9.2022.

12 Trends in information security study. 2015. Verkkoaineisto. CompTIA. <https://connect.comptia.org/content/research/trends-in-information-security-study>. 3.2015. Luettu 17.9.2022.

13 Configure Microsoft Office 365 auto-provisioning. Verkkoaineisto. Google. <https://support.google.com/a/answer/7365072>. Luettu 31.10.2022.

14 If you need to install Rosetta on your Mac. 2022. Verkkoaineisto. Apple. <https://support.apple.com/en-us/HT211861>. 17.5.2022. Luettu 1.11.2022.

15 Apple Business Manager User Guide. 2022. Verkkoaineisto. Apple. <https://support.apple.com/guide/apple-business-manager/welcome/web>. Luettu 1.11.2022.

16 Use Disk Utility to erase an Intel-based Mac. 2022. Verkkoaineisto. Apple. <https://support.apple.com/en-us/HT208496>. 4.8.2022. Luettu 1.11.2022.

17 Use FileVault to encrypt your Mac startup disk. 2022. Verkkoaineisto. Apple. <https://support.apple.com/en-us/HT204837>. 24.10.2022. Luettu 1.11.2022.

18 Intro to Apple Business Manager. 2022. Verkkoaineisto. Apple. <https://support.apple.com/en-hk/guide/apple-business-manager/axmd344cdd9d/web>. 27.4.2022. Luettu 27.05.2022.

19 Edit preferences in Apple Business Manager. 2022. Verkkoaineisto. Apple. <https://support.apple.com/en-hk/guide/apple-business-manager/axmb43b66449/web>. 27.4.2022. Luettu 21.5.2022.

20 Device workflow in Apple Business Manager. 2022. Verkkoaineisto. Apple. <https://support.apple.com/en-hk/guide/apple-business-manager/axm6a88f692e/web>. 11.5.2022. Luettu 27.5.2022.

21 Automatically enroll macOS devices with the Apple Business Manager or Apple School Manager. 2022. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/mem/intune/enrollment/device-enrollment-program-enroll-macos>. 12.7.2022. Luettu 1.11.2022.

22 Azure Active Directory documentation. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/azure/active-directory/>. Luettu 26.10.2022.

23 Enterprise Mobility + Security pricing options. Verkkoaineisto. Microsoft. <https://www.microsoft.com/en-ww/microsoft-365/enterprise-mobility-security/compare-plans-and-pricing>. Luettu 26.10.2022.

24 Microsoft Intune licensing. 2022. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/mem/intune/fundamentals/licenses>. 20.9.2022. Luettu 26.10.2022.

25 What is Azure Active Directory? 2022. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis>. 15.9.2022. Luettu 26.10.2022.

26 Getting started with Microsoft Endpoint Manager. 2022. Verkkoaineisto. Microsoft. <https://techcommunity.microsoft.com/t5/intune-customer-success/getting-started-with-microsoft-endpoint-manager/ba-p/2497614>. 29.6.2021. Luettu 26.10.2022.

27 Eby, Doug. 2022. Microsoft Intune is an MDM and MAM provider for your devices. Verkkoaineisto. Microsoft. <https://docs.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune>. Luettu 24.5.2022.

28 Winegar, James. 2019. Setting up Single Sign-On (SSO) between G Suite and Office 365 with G Suite as identity provider (IdP). Verkkoaineisto. Medium. <https://medium.com/@james.winegar/how-to-single-sign-on-sso-between-g-suite-and-office-365-with-g-suite-as-identity-provider-idp-5bf5031835a0>. Luettu 1.11.2022.

29 Plan an Azure Active Directory self-service password reset deployment. 2022. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment>. 6.8.2022. Luettu 26.10.2022.

30 Newsad, Laura. 2022. Set up enrollment for macOS devices in In-tune. Verkkoaineisto. Microsoft Docs. <https://docs.microsoft.com/en-us/mem/intune/enrollment/macos-enroll>. Luettu 27.5.2022.

31 Apple Configurator User Guide. Verkkoaineisto. Apple. <https://support.apple.com/guide/apple-configurator/welcome/ios>. Luettu 20.10.2022.

32 Set the mobile device management authority. 2022. Verkkoaineisto. Microsoft. <https://docs.microsoft.com/en-us/mem/intune/fundamentals/mdm-authority-set>. 13.1.2022. Luettu 27.5.2022.

33 Configure a custom domain name. 2020. Verkkoaineisto. Microsoft. <https://docs.microsoft.com/en-us/mem/intune/fundamentals/custom-domain-name-configure>. 28.8.2020. Luettu 27.5.2022.

34 Get an Apple MDM push certificate. 2022. Verkkoaineisto. Microsoft. <https://docs.microsoft.com/en-us/mem/intune/enrollment/apple-mdm-push-certificate-get>. 3.11.2022. Luettu 6.11.2022.

35 Enterprise Mobility + Security. Verkkoaineisto. Microsoft. <https://www.microsoft.com/en-us/licensing/product-licensing/enterprise-mobility-security>. Luettu 20.10.2022.

36 Add groups to organize users and devices. 2022. Verkkoaineisto. Microsoft. <https://docs.microsoft.com/en-us/mem/intune/fundamentals/groups-add>. 7.4.2022. Luettu 20.10.2022.

37 Manage user and group identities in Microsoft Intune. 2022. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/mem/intune/fundamentals/manage-identities>. 12.10.2022. Luettu 20.10.2022.

38 Use custom settings for macOS devices in Microsoft Intune. 2022. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/mem/intune/configuration/custom-settings-macos>. 29.9.2022. Luettu 24.10.2022.

39 Using MDM profiles to set up the product. Verkkoaineisto. F-Secure. <https://help.f-secure.com/product.html#business/psb-portal/latest/en/task_4C1198AA5CE0499BA55A85BA8A1E288C-psb-portal-latest-en>. Luettu 24.10.2022.

40 macOS device settings to allow or restrict features using Intune. 2022. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/mem/intune/configuration/device-restrictions-macos>. 29.9.2022. Luettu 24.10.2022.

41 Add apps to Microsoft Intune. 2022. Verkkoaineisto. Microsoft. <https://docs.microsoft.com/en-us/mem/intune/apps/apps-add>. 29.10.2022. Luettu 27.5.2022.

42 Guide for Apple IT: Introduction to Mac Scripting. 2022. Verkkoaineisto. Kandji. <https://blog.kandji.io/guide-for-apple-it-introduction-to-mac-scripting>. 7.7.2022. Luettu 1.11.2022.

43 How to add macOS line-of-business (LOB) apps to Microsoft Intune. 2022. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/mem/intune/apps/lob-apps-macos>. 28.10.2022. Luettu 1.11.2022.

44 Add the macOS Company Portal app. 2022. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/mem/intune/apps/apps-company-portal-macos>. 30.3.2022. Luettu 1.11.2022.

45 Assign apps to groups with Microsoft Intune. 2022. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/mem/intune/apps/apps-deploy>. 26.10.2022. Luettu 1.11.2022.

46 Use shell scripts on macOS devices in Intune. 2022. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/mem/intune/apps/macos-shell-scripts>. 18.8.2022. Luettu 1.11.2022.

47 Microsoft Intune management agent for macOS. 2022. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/mem/intune/apps/lob-apps-macos-agent>. 27.1.2022. Luettu 01.11.2022.

WithSecure-Bash-skripti

WithSecure-tietoturvaohjelman asennuksen Bash-skripti

```
#!/bin/bash

sas="
mpkgfile="
profile_id="
activation_key="

#Check if MacBook is on Apple silicone and needs Rosetta 2
if [[ $(uname -p) == 'arm' ]]; then
    echo "MacBook is based on M1 silicone, Rosetta needed"
    if [ $(/usr/bin/pgrep oahd >/dev/null 2>&1;echo $?) -eq 0 ]; then
        echo "Rosetta already installed"
    else
        echo "Rosetta not installed. Installing..."
        sudo /usr/sbin/softwareupdate --install-rosetta --agree-to-license
        if [ $? -eq 0 ]; then
            echo "Rosetta installed and license agreed to succesfully"
        else
            echo "Rosetta installation or license agreement unsuccessful"
            exit 1
        fi
    fi
else
    echo "MacBook is based on Intel silicone, Rosetta not needed"
fi

#Check if installation URL exists
if curl --head --silent --fail $sas &> /dev/null; then
    echo "This page exists"
else
    echo "This page does not exist"
    exit 1
fi

#Check if F-Secure is installed
if [ -e /Applications/F-Secure/"F-Secure Mac Protection.app" ]; then
    echo "F-Secure already installed"
    exit 0
else
    echo "F-Secure not installed"
fi

#Download package
curl -L -f -o "$mpkgfile" "$sas"
if [ $? -eq 0 ]; then
    echo "F-Secure downloaded successfully"
else
    echo "F-Secure not downloaded"
    #Go to next step to see if package already exists
fi

#Install package
sudo installer -pkg "$mpkgfile" -target /Applications

#Activate application
sudo /Library/F-Secure/bin/activator --profile-id $profile_id --subscription-key $activation_key
if [ $? -eq 0 ]; then
    echo "F-Secure activated successfully"
else
    echo "F-Secure not activated"
    #Go to next step for clean up
fi

#Cleaning Up
sudo rm -rf $mpkgfile
if [ $? -eq 0 ]; then
    echo "Clean up done successfully"
else
    echo "Clean up not successful"
    exit 1
fi

exit 0
```