Jesse Lainio

Microsoft 365 Business Premiumin käyttöönotto ja laitehallinta Microsoft Intunen avulla

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tieto- ja viestintätekniikan tutkinto-ohjelma

Insinöörityö

17.12.2024

Tiivistelmä

Tekijä:	Jesse Lainio
Otsikko:	Microsoft 365 Business Premiumin käyttöönotto ja laitehallinta Microsoft Intunen avulla
Sivumäärä:	15 sivua + 7 liitettä
Aika:	17.12.2024
Tutkinto:	Insinööri (AMK)
Tutkinto-ohjelma:	Tieto- ja viestintätekniikan tutkinto-ohjelma
Ammatillinen pääaine:	Monimuotototeutus
Ohjaaja:	Janne Salonen

Tämä insinöörityö käsittelee Microsoft 365 Business Premiumin käyttöönottoa ja laitehallintaa Microsoft Intunen avulla. Työssä kuvataan vaiheittain käyttöönottoprosessi, Intunen tarjoamat mobiili- ja työasemalaitteiden hallintamahdollisuudet sekä tietoturvan parantaminen Defender-tuotteiden ja Conditional Accessin avulla. Lisäksi esitellään Windows Autopilot, joka automatisoi laiteasennukset ja helpottaa käyttöönottoa. Tuloksena on selkeä toimintamalli, joka tehostaa organisaation IT-hallintaa ja parantaa tietoturvaa.

Avainsanat:	Microsoft 365 Business Premium, Intune, Defender, Windows Autopilot

---

Abstract

Author:	Jesse Lainio
Title:	Deployment of Microsoft 365 Business Premium and device management using Microsoft Intune
Number of Pages:	15 pages + 7 appendices
Date:	17 December 2024
Degree:	Bachelor of Engineering
Degree Programme:	Information and Communication Technology
Professional Major:	Blended Learning Implementation
Supervisor:	Janne Salonen

This thesis examines the deployment of Microsoft 365 Business Premium and device management using Microsoft Intune. It outlines the implementation process, Intune's capabilities for managing mobile and workstation devices, and enhancing security with Defender products and Conditional Access. Additionally, it introduces Windows Autopilot, which automates device installations and simplifies deployment. The result is a clear operational model that streamlines IT management and improves organizational security.

Keywords: Microsoft 365 Business Premium, Intune, Windows Autopilot

Sisällys

Lyhenteet

AD: Active Directory. mahdollistaa käyttäjien ryhmien ja laitteiden hallinnan keskitetysti sekä tukee verkon turvallisuutta ja skaalautuvuutta.

LAPS: Local Administrator Password Solution. Työkalu, joka hallinnoi paikallisten järjestelmänvalvojan salasanojen turvallista käyttöä ja vaihtamista.

MDM: Mobile Device Management. Mobiililaitteiden hallintaan tarkoitettu järjestelmä, joka mahdollistaa laiteasetusten ja tietoturvan hallinnan keskitetysti.

MAM: Mobile Application Management. Sovellusten hallintaan tarkoitettu järjestelmä, joka hallinnoi yrityksen sovelluksia ja niiden sisältämää dataa erillään henkilökohtaisista tiedoista.

EDR: Endpoint Detection and Response. Päätelaitteiden suojausratkaisu, joka havaitsee ja reagoi uhkiin reaaliaikaisesti.

OOBE: Out-of-Box Experience. Prosessi, jossa uusi päätelaite konfiguroidaan automaattisesti käyttäjän kirjautuessa ensimmäistä kertaa.

ASR: Attack Surface Reduction. Tietoturvakovennuksia, joilla estetään haittaohjelmien ja hyökkäysten mahdollisuuksia päätelaitteissa.

CIS: Center for Internet Security. Organisaatio, joka määrittää parhaita käytäntöjä ja standardeja tietoturvalle.

Tenant: Microsoft 365 -ympäristössä organisaation oma eristetty tila, jossa hallinnoidaan käyttäjiä, resursseja ja asetuksia.

Bitlocker: Microsoftin tietojen salaustekniikka, joka suojaa laitteen tiedot salauksella.

RAM: Random Access Memory. Tietokoneen lyhytaikainen muistivarasto, jossa dataa käsitellään väliaikaisesti.

MFA: Multi-Factor Authentication. Monivaiheinen tunnistautuminen, jossa käytetään vähintään kahta erillistä todennusmenetelmää.

CA: Conditional Access. Ehdollinen pääsykäytäntö, joka määrittää, millä ehdoilla käyttäjät voivat päästä organisaation resursseihin.

Defender: Microsoftin tietoturvapalvelu, joka suojaa laitteita haittaohjelmilta ja muilta uhkilta. Sisältää muun muassa Defender for Endpoint ja Defender for Office 365 -tuotteet.

Entra ID: Microsoftin identiteetinhallintapalvelu, joka mahdollistaa käyttäjien ja sovellusten hallinnan pilviympäristössä.

1 Johdanto

Tämä opinnäytetyö käsittelee Microsoft 365 Business Premiumin ja Microsoft Intunen käyttöönottoa keskisuuressa organisaatioympäristössä. Työn aihe nousi esiin työtehtävieni kautta, joissa olen osallistunut organisaation IT-ympäristön kehittämiseen ja modernisointiin. Tarve keskitetylle laitehallinnalle ja tietoturvan parantamiselle oli ilmeinen, ja Microsoft Intune osoittautui ratkaisuksi, joka vastaa näihin haasteisiin nykyaikaisella tavalla.

Microsoft 365 Business Premium tarjoaa laajan valikoiman työkaluja, kuten Microsoft Intunen, Defender-tuotteet ja Windows Autopilotin, joiden avulla yrityksen IT-infrastruktuuria voidaan hallita keskitetysti ja sujuvasti.

Työn toteutustapa perustuu workshopeihin, joissa määritetään organisaation tarpeisiin sopivat asetukset, sekä testikäyttöönottoon pilottiryhmällä. Pilottiryhmä mahdollistaa mahdollisten ongelmien havaitsemisen ja korjaamisen ennen laajamittaista käyttöönottoa, mikä helpottaa siirtymistä tuotantoympäristöön.

Työ tarjoaa kokonaisvaltaisen tarkastelun siitä, miten Microsoftin tarjoamat työkalut voidaan ottaa käyttöön ja optimoida organisaation tarpeiden mukaisesti. Työssä keskitytään erityisesti päätelaitteiden hallintaan, tietoturvakäytäntöjen toteuttamiseen ja käyttöönottoprosessien automatisointiin. Lopputuloksena syntyy selkeä toimintamalli, joka tukee yrityksen strategiaa ja vahvistaa tietoturvaa. Lisäksi työ tarjoaa dokumentoidun toimintasuunnitelman, jota voidaan soveltaa vastaavissa projekteissa tulevaisuudessa.

2 Tehokkuutta ja tietoturvaa Microsoft 365 -ratkaisuilla

Nykyajan organisaatioympäristöissä tietoturva ja tehokas IT-hallinta ovat kriittisiä tekijöitä menestyvän liiketoiminnan tukemisessa. Yritysten kohtaamat haasteet, kuten tietoturvauhkien lisääntyminen, etä- ja hybridityöskentelyn yleistyminen sekä digitaalisten työkalujen käyttöön liittyvä monimutkaisuus, vaativat moderneja ja joustavia ratkaisuja.

Microsoft 365 Business Premium tarjoaa keskitetyn alustan, joka yhdistää laitehallinnan, tietoturvan ja tuottavuustyökalut. Ratkaisu valittiin erityisesti siksi, että se vastaa keskisuuren organisaation tarpeisiin kustannustehokkaasti ja skaalautuvasti. Microsoft Intunen avulla organisaation laitteiden ja sovellusten hallinta voidaan toteuttaa keskitetysti, samalla kun Windows Autopilot automatisoi työasemien käyttöönoton, nopeuttaen laitteiden siirtymistä tuotantokäyttöön.

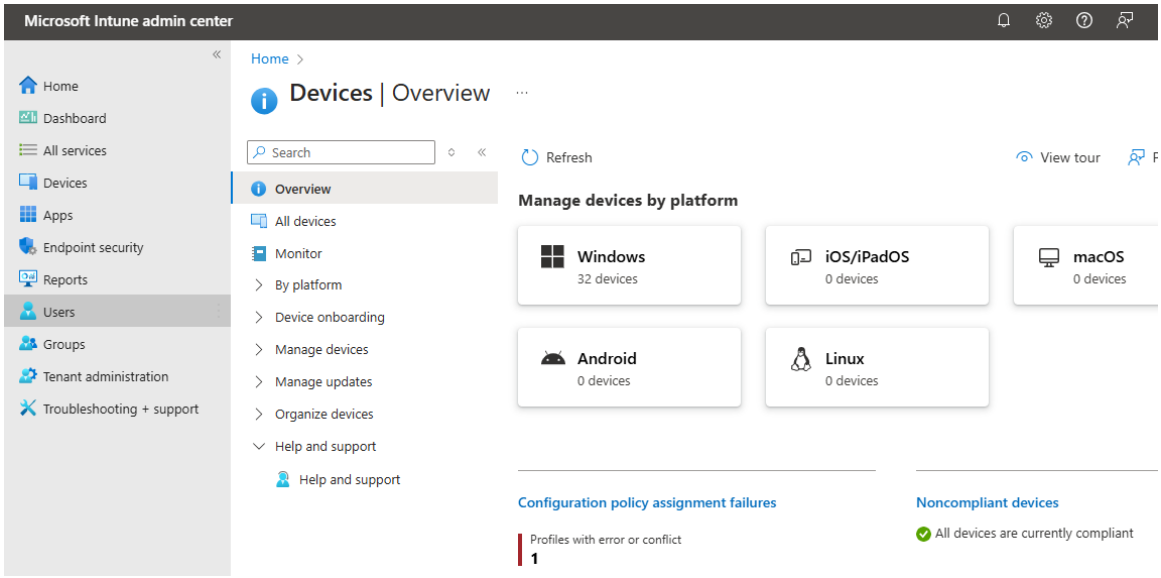
Tietoturvan merkitys korostuu entisestään nykypäivän digitalisoituneessa maailmassa. Keskitetyt tietoturvakäytännöt, kuten Microsoftin tarjoamat Defender-tuotteet ja Conditional Access -ratkaisut, mahdollistavat organisaation tietojen suojauksen sekä ennakoivan reagoinnin uhkiin.

2.1 Lähtötilanne ja organisaation tarpeet

Ennen Microsoft 365 Business Premiumin ja Intunen käyttöönottoa organisaation IT-ympäristö koostui hajautetuista ratkaisuista, jotka eivät täysin vastanneet nykyajan vaatimuksia. Tietoturvaan liittyvät prosessit olivat osittain manuaalisia, mikä lisäsi hallinnollista kuormitusta ja potentiaalisia riskejä. Lisäksi päätelaitteiden hallinta oli hajautettua, mikä teki ylläpidosta monimutkaista ja aikaa vievää.

Etätyöskentelyn yleistyminen toi mukanaan uusia haasteita, kuten tarvetta varmistaa laitteiden turvallinen käyttö organisaation ulkopuolella. Tämä korosti tarvetta yhtenäiselle ja keskitetylle ratkaisulle, joka mahdollistaa laitteiden ja sovellusten hallinnan, tietoturvan ylläpidon sekä työasemien tehokkaan käyttöönoton.

2.2 Käyttöönotettavat palvelut ja niiden tekniset ominaisuudet



Kuva 1. Microsoft Intune admin center

Käyttöönotossa organisaatio ottaa käyttöön keskeiset Microsoft 365 Business Premium -palvelut, jotka tarjoavat kattavat tekniset ratkaisut päätelaitteiden hallintaan, tietoturvaan ja käyttäjäautentikointiin.

Microsoft Intune on pilvipohjainen laitehallintapalvelu, joka tukee sekä MDM (Mobile Device Management)- että MAM (Mobile Application Management) -toimintoja. Intune mahdollistaa laitekonfiguraatioiden hallinnan, kuten Wi-Fi-asetusten, sertifikaattien ja salausmääritysten keskitetyn määrittämisen. Compliance Policy -käytäntöjen avulla voidaan määrittää, mitkä laitteet ovat organisaation tietoturvavaatimusten mukaisia, ja estää ei-yhteensopivien laitteiden pääsy resursseihin. Lisäksi Intune tukee Zero Trust -arkkitehtuuria, varmistaen, että vain tunnistetut ja turvalliset laitteet pääsevät organisaation resursseihin [1].

Osana Intunen laitehallinnan ratkaisuja otetaan käyttöön Local Administrator Password Solution (LAPS), joka parantaa tietoturvaa hallitsemalla paikallisten järjestelmänvalvojan salasanojen turvallisuutta. LAPS luo jokaiselle laitteelle uniikin järjestelmänvalvojan salasanan, joka tallennetaan keskitetysti Intune-palveluun. Salasanat vaihtuvat automaattisesti ennalta määritellyin aikavälein,

mikä estää niiden väärinkäytön ja vähentää riskiä paikallisten tunnusten kautta tapahtuviin tietoturvahyökkäyksiin.

2.3 Microsoft Defender

Defender for Business ja Defender for Office 365 tuovat kattavat tietoturvaominaisuudet organisaatioon. Defender for Business tarjoaa päätelaitteiden EDR (Endpoint Detection and Response) -ominaisuudet, jotka tunnistavat ja reagoivat nopeasti haittaohjelmiin, epäilyttäviin tiedostoihin ja käyttäytymismalleihin. Palvelu hyödyntää Microsoftin pilvipohjaista tietoturvainfrastruktuuria, koneoppimista ja jatkuvaa uhkatietojen päivitystä [2]. Defender for Office 365 sisältää muun muassa Safe Links- ja Safe Attachments -ominaisuudet, jotka suojaavat käyttäjiä haitallisilta verkkosivuilta ja liitteiltä sähköposteissa. Palvelu käyttää reaaliaikaista sandboxing-ympäristöä tiedostojen tarkistamiseen ennen avaamista sekä tarjoaa sähköpostin karanteeni- ja raportointityökaluja IT-osastolle [3].

2.4 Windows Autopilot

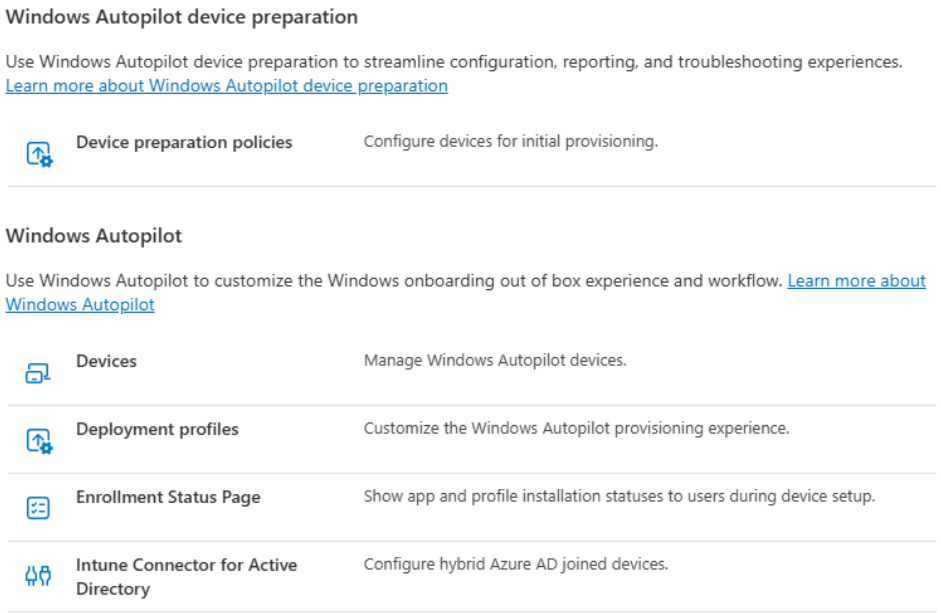
Windows Autopilot automatisoi työasemien käyttöönoton, minimoiden manuaalisen laitekonfiguroinnin. Se tukee Out-of-Box Experience (OOBE) -prosessia, jossa laite yhdistetään automaattisesti Intuneen käyttäjän ensimmäisellä kirjautumisella. Windows Autopilot mahdollistaa hybrid Azure AD -liitoksen, jolloin laite voidaan rekisteröidä sekä paikalliseen Active Directoryyn että Azure AD:hen. Lisäksi se sisältää White Glove -palvelun, jossa IT-osasto tai laitetoimittaja voi esikonfiguroida laitteen ennen käyttäjälle toimittamista [4].

2.5 Conditional Access ja MFA

Conditional Access ja monivaiheinen tunnistautuminen (MFA) lisäävät organisaation tietoturvaa tarjoamalla joustavat mutta turvalliset pääsyratkaisut. Conditional Access hyödyntää Azure AD:n reaaliaikaisia päätöksiä käyttäjän, laitteen ja sijainnin perusteella. Esimerkiksi pääsyä voidaan estää epäilyttävistä IP-osoitteista tai vaatia MFA-tunnistautumista. MFA lisää lisäturvaa pyytämällä

käyttäjältä toisen tunnistustavan, kuten puhelinsovelluksen (Microsoft Authenticator) ilmoituksen, tekstiviestin tai biometrisen tunnistuksen. Conditional Access tukee myös Granular Access Control -politiikkoja, joiden avulla voidaan luoda tarkkoja sääntöjä pääsyn hallintaan eri resursseissa ja sovelluksissa [5].

2.6 Automatisoinnin vaikutus



Kuva 2. Windows Autopilot konfiguraatiot

Ennen Windows Autopilotin käyttöönottoa uusien laitteiden käyttöönotto organisaatiossa oli täysin manuaalinen prosessi. IT-osaston vastuulla oli päivittää laitteen käyttöjärjestelmä, asentaa ajurit sekä kaikki tarvittavat ohjelmistot ja työkalut erillisistä asennuskansioista. Tämä vei huomattavan paljon aikaa ja altisti virheille, koska jokainen laite oli asennettava yksittäin ja ilman keskitettyä hallintaa.

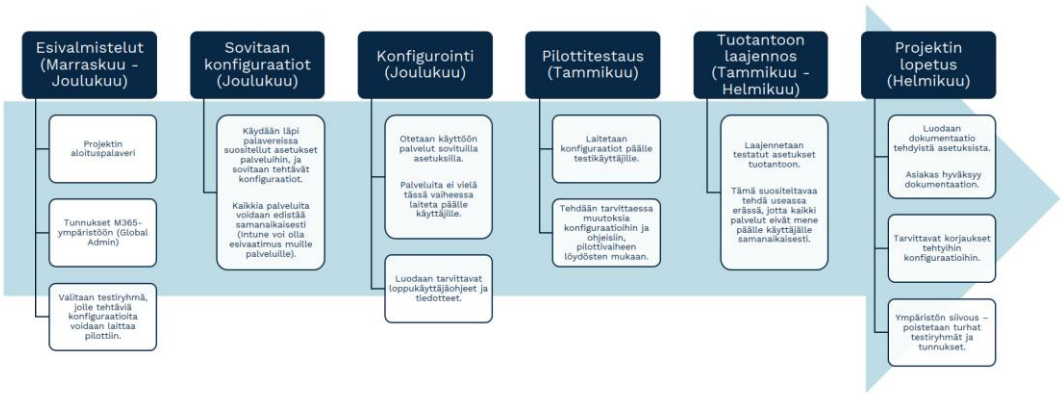
Windows Autopilot toi prosessiin kaivattua automatisointia. Autopilotin avulla laitteet voidaan määrittää ja ottaa käyttöön suoraan pilvipalvelusta, tämä

mahdollistaa kaikkien tarvittavien ohjelmistojen, asetusten ja tietoturvakäytäntöjen asentamisen automaattisesti, kun käyttäjä kirjautuu ensimmäistä kertaa laitteeseen.

3 Käyttöönoton prosessi

3.1 Esivalmistelut

Käyttöönotto alkoi huolellisilla esivalmisteluilla, joiden tavoitteena oli varmistaa sujuva siirtymä uusiin järjestelmiin ja minimoida häiriöt käyttäjätasolla. Ensimmäinen askel oli työntekijöiden informoiminen tulevista muutoksista jo varhaisessa vaiheessa. Syksyllä aloitettiin informointi toimihenkilöiden kuukausipalaverien ohella, jossa kerrottiin käyttöönoton aikataulu, siihen liittyvät muutokset ja järjestelmien tarjoamat hyödyt. Tämä auttoi vähentämään käyttöönoton aiheuttamaa epätietoisuutta ja loi pohjan positiiviselle vastaanotolle[6] [7].



Kuva 3. Projektin aikataulu

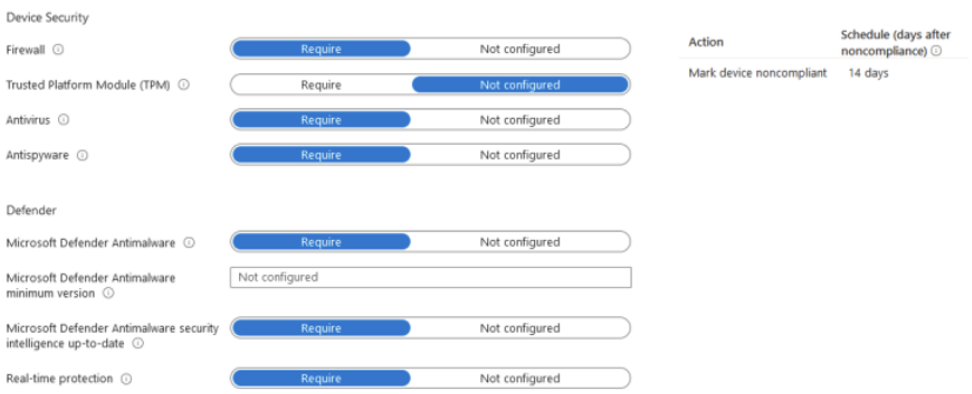
Seuraavaksi laadittiin tarkka aikataulu yhteistyössä projektikumppanin kanssa. Aikataulun tavoitteena oli jakaa tehtävät vaiheittain ja varmistaa, että kaikki tekniset ja hallinnolliset valmistelut olivat valmiina ennen pilottivaihetta. Tämä sisälsi tarvittavien tunnusten avaamisen Microsoft 365 -ympäristöön sekä testikäyttäjien ja -ryhmien luomisen. Testiryhmät koostuivat erilaisista

käyttäjäprofiileista, mukaan lukien tavalliset käyttäjät ja globaalit järjestelmänvalvojat. Tämä varmisti, että järjestelmien toimivuutta voitiin arvioida kattavasti erilaisissa käyttötilanteissa[6] [7].

Esivalmisteluihin kuului myös ensimmäiset työpajat, joissa tutkittiin mahdollisia käytettäviä konfiguraatiota ja asetuksia. Näissä työpajoissa käytiin läpi suositusten mukaiset parhaat käytännöt. Security Defaults -asetusten poistaminen käytöstä ja niiden korvaaminen tarkemmilla Conditional Access -käytännöillä. Laitteiden hallinnan asetukset, jotka estivät esimerkiksi laitteen rekisteröineen käyttäjän lisäämisen paikalliseksi järjestelmänvalvojaksi[6] [7] [8].

Lopuksi esivalmisteluvaiheessa varmistettiin, että tekniset resurssit ja dokumentointi olivat ajan tasalla.

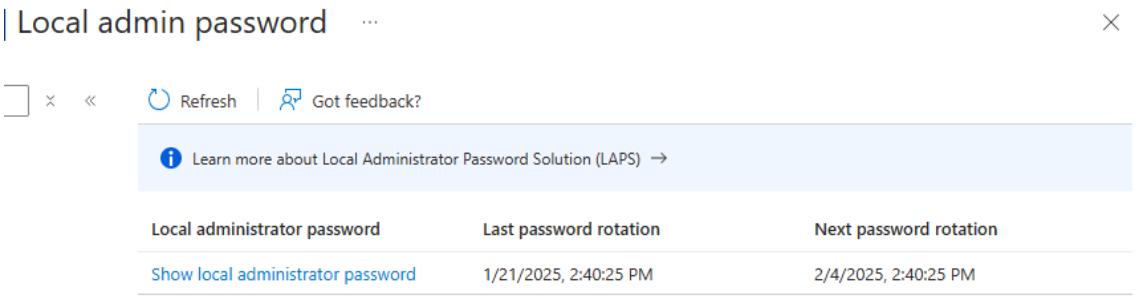
3.2 Konfiguraatiot



Kuva 4. Laitevaatimusten määrittäminen Microsoft Intunessa

Microsoft 365 -ympäristössä toteutettiin useita hallinnollisia muutoksia tietoturvan ja hallittavuuden parantamiseksi. Ensimmäiseksi määritettiin Break Glass -

tunnus, joka toimii varajärjestelmänvalvojana kriittisissä tilanteissa. Tämä tunnus mahdollistaa pääsyn ympäristöön myös tilanteessa, jossa MFA-asetukset eivät toimisi odotetusti [6] [7]. Security Defaults -asetukset poistettiin käytöstä ja korvattiin tarkemmilla Conditional Access -politiikoilla, jotka antavat yksityiskohtaisemman hallinnan pääsyoikeuksille. Lisäksi käyttäjien mahdollisuus rekisteröidä uusia Entra ID -sovelluksia ja luoda uusia tenantteja estettiin hallintaympäristön kontrollin varmistamiseksi [6] [7] [8].



Kuva 5. LAPS

Päätelaitteiden hallinnassa hyödynnettiin Intunen tarjoamia edistyneitä toimintoja. Local Administrator Password Solution (LAPS) otettiin käyttöön. Lisäksi otettiin käyttöön Windows Update for Business -toiminto, jonka avulla laitteiden päivitykset automatisoitiin kahdessa eri ryhmässä: pilottiryhmässä ja tuotannossa. Pilottiryhmä sai päivitykset ensimmäisenä, mikä mahdollisti ongelmien havaitsemisen ennen päivitysten laajempaa levittämistä, ja tuotantoryhmä sai päivitykset kahden viikon viiveellä [8] [9].

Tietoturvakovennusten osalta toteutettiin Attack Surface Reduction (ASR) -säännöt, näihin sääntöksiin sisältyi muun muassa autorun-ominaisuuksien estäminen, joka ehkäisi haittaohjelmien leviämistä, sekä Defenderin konfigurointi tarkistamaan irrotettavat tallennusmediat haitallisen sisällön varalta [10]. Samanaikaisesti toteutettiin CIS-standardien mukaisia kovennuksia, kuten Bitlocker-suojauksen varmistaminen ja hybrid sleep -ominaisuuden poistaminen

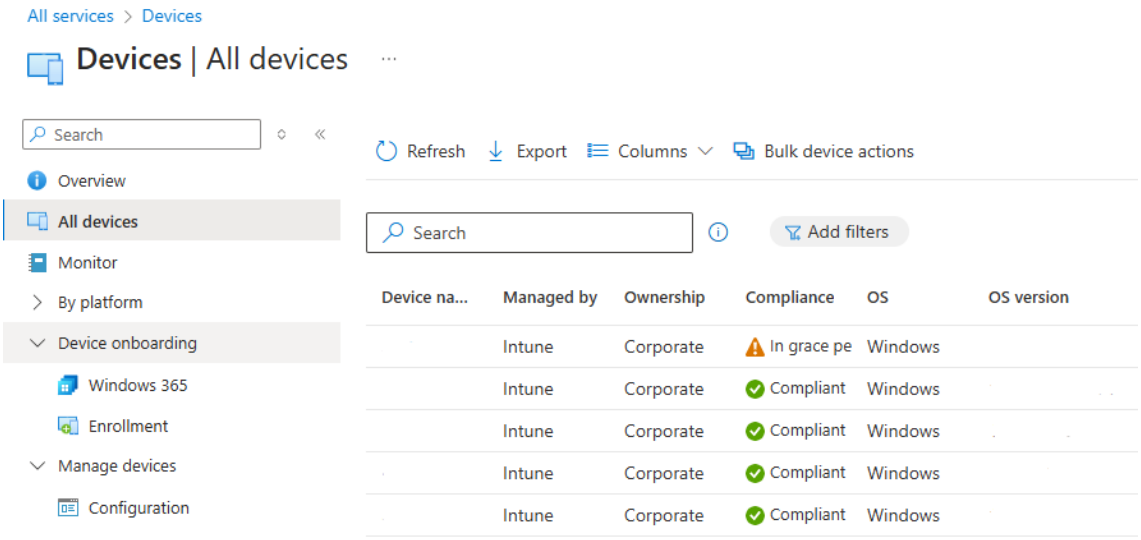
käytöstä. Hybrid sleep -tilan katsottiin olevan tietoturvariski, koska se voi tallentaa Bitlocker-avaimia RAM-muistiin, josta avaimet voidaan mahdollisesti varastaa [11].

Konfiguroinnit sisälsivät myös tärkeiden Microsoft 365 -sovellusten ja palveluiden hallinnan. Windows Outlook määritettiin kirjautumaan automaattisesti sisään ja luomaan käyttäjille oletusprofiilit. Windows OneDrive puolestaan konfiguroitiin siirtämään automaattisesti käyttäjien työpöydät, tiedostot ja kuvat pilveen, mikä helpotti käyttäjien tiedostojen hallintaa ja varmuuskopiointia. Lisäksi Defenderin ja muiden tietoturvapalveluiden laajennukset asennettiin Google Chrome -selaimeen parantamaan tietoturvaa ja käyttäjäkokemusta[8] [9].

Osana konfiguraatioita lisättiin myös Windows Health Monitoring -toiminto Intuneen. Tämä toiminto kerää ja lähettää tietoja laitteiden suorituskyvystä ja luotettavuudesta, kuten Windows Updaten onnistumisista, boottiajoista ja yleisestä kunnosta. Näitä tietoja hyödynnetään IT-tuen tehostamiseen ja päätelaitteiden optimointiin. Lisäksi Intune mahdollisti laitteiden, erityisesti mobiili- ja tablet-laitteiden, paikannuksen ja käyttäjätietojen hallinnan. Tämä tarkoitti, että IT-osasto pystyi näkemään laitteen sijainnin ja sen, kuka on kirjautunut laitteeseen. Näin voitiin tehokkaasti seurata, kenen hallussa laite on, mikä paransi huomattavasti hallittavuutta ja turvallisuutta [6] [7].

Lisäksi tehtiin useita muita tärkeitä asetuksia, kuten hybrid sleep -ominaisuuden poistaminen käytöstä Windows Power Settings -asetuksissa turvallisuussyistä. Virtapainike määritettiin sammuttamaan laite, ja Xbox-palvelut estettiin tarpeettomien resurssien kulutuksen sekä mahdollisten tietoturva-aukkojen välttämiseksi. Myös käyttäjien mahdollisuus käyttää sisäänrakennettua Remote Assistance -toimintoa estettiin, mikä vähensi etäkäyttötoimintojen väärinkäytöksen riskiä [6] [8].

3.3 Pilottivaihe



Kuva 6. Pilotin alku

Pilottivaiheessa valittiin viisi käyttäjää, joiden laitteet liitettiin Microsoft Intunen laitehallintaan. Tämä mahdollisti uusien määritysten ja tietoturvakäytäntöjen käyttöönoton hallitusti ja pienimuotoisesti. Pilottivaihe kesti noin viikon, jonka aikana käyttäjien kokemuksia ja mahdollisia haasteita seurattiin tiiviisti. Käyttäjien kanssa käytiin aktiivista keskustelua, jotta voitiin tunnistaa ongelmat ja ratkaista ne nopeasti.

Pilottivaiheen aikana havaittiin, että tiukemmat palomuurimääritykset aiheuttivat haasteita joidenkin ohjelmointiohjelmien käytössä. Tämä korostaa pilottivaiheen merkitystä, sen avulla ongelmat voidaan tunnistaa ja ratkaista ennen laajamittaista käyttöönottoa tehokkaasti. Kyseiset määritykset muokattiin toimiviksi ilman, että tietoturvasta tingittiin.

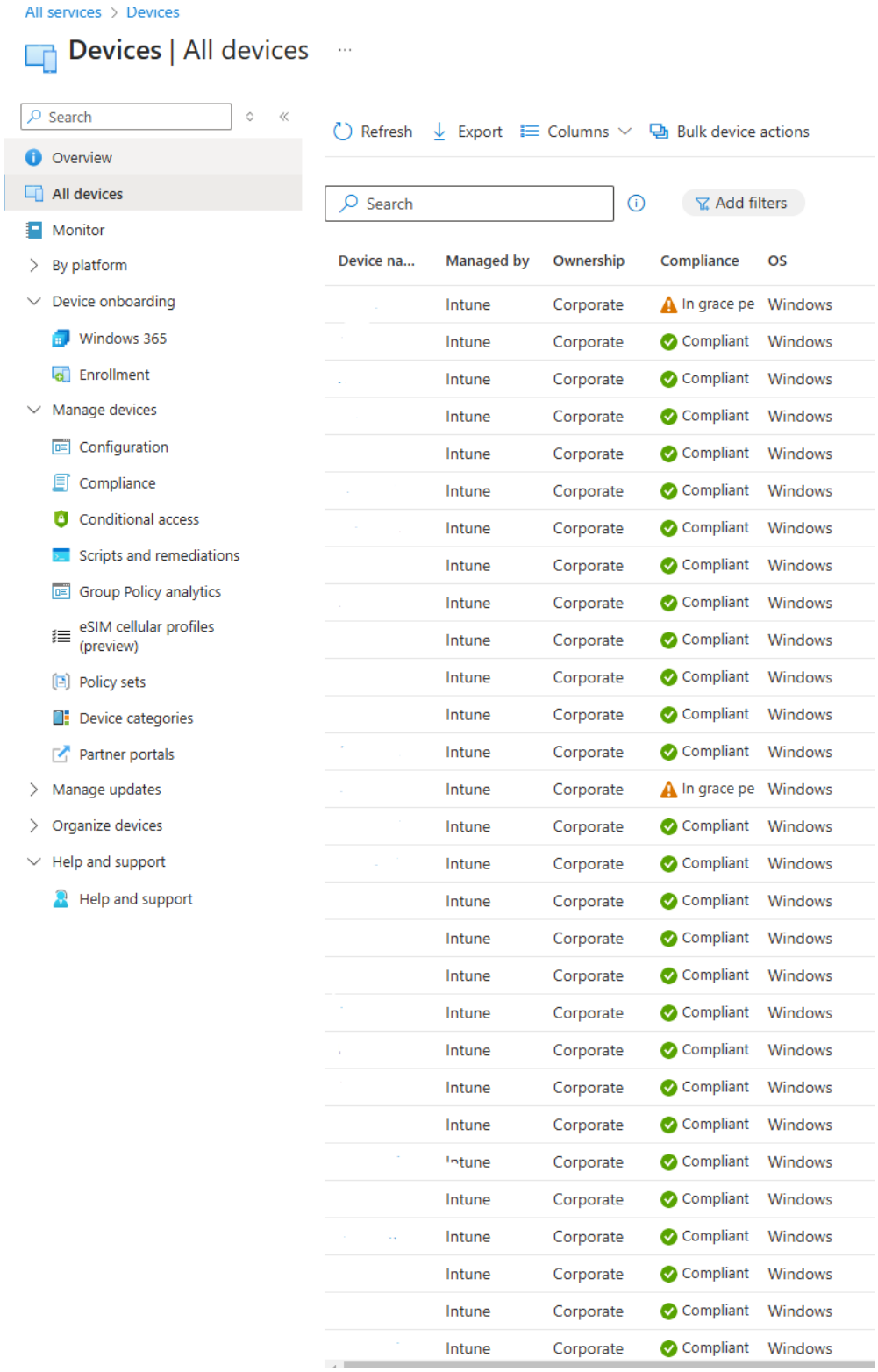
Samalla pilottivaiheen aikana yhteistyössä projektikumppanin kanssa pohdittiin keinoja, joilla siirtyminen Intuneen voitaisiin toteuttaa nopeasti ja tehokkaasti koko tuotantoympäristön osalta. Nykyisessä ympäristössä käytössä oli AD -> Entra-hybridilaitteita, joita ei voitu enää siirtää Group Policyn avulla keskitetysti. Tämän vuoksi kehitettiin ja testattiin erilaisia PowerShell-skriptejä. Skriptien

avulla voitiin automatisoida laitteiden siirtäminen Intuneen, määrittää laite-asetukset tehokkaasti ja varmistaa, että uudet määritykset toimivat odotetusti. Tämä ratkaisu säästi merkittävästi aikaa ja mahdollisti siirtymisen hallitusti.

Pilottivaihe toimi erittäin tärkeänä osana projektin kokonaisuutta, sillä sen aikana varmistettiin, että kaikki keskeiset järjestelmät ja käytännöt olivat valmiita täysimittaiseen käyttöönottoon.

3.4 Tuotantoon siirtyminen

Tuotantoon siirtyminen aloitettiin heti, kun pilottivaiheessa havaitut haasteet oli ratkaistu. Prosessi toteutettiin hallitusti ja asteittain. Siirtymisprosessissa pilottiryhmän kokoa kasvatettiin asteittain lisäämällä uusia käyttäjiä päivittäin. Tämä lähestymistapa varmistaa, että siirtyminen oli hallittu ja mahdolliset ongelmatilanteet voitiin ratkaista käytännössä heti. Strategia osoittautui tehokkaaksi, sillä se mahdollisti siirtymisen hallitusti ja käyttäjäystävällisesti ilman suuria katkoksia organisaation toiminnassa.



Kuva 7. Siirtymäprosessi

Siirtyminen toteutettiin kahdella tavalla. Ensimmäinen tapa oli kehitettyjen PowerShell-skriptien käyttö, joiden avulla laitteet voitiin siirtää Intunen hallintaan

automaattisesti. Skriptien avulla laiteasetukset voitiin määrittää ennen liittämistä Intuneen ja sen jälkeen laite rekisteröityi ajastetulla taustaprosessilla Intunen hallintaan, mikä nopeutti prosessia merkittävästi sekä käyttäjä pystyi jatkamaan työtä keskeytyksettä. Toinen tapa oli suorittaa siirtyminen käyttäjän laitteen kautta tilinhallinnan avulla. Tässä menetelmässä käyttäjä liitti itse laitteensa hallintapalveluun. Näiden kahden menetelmän yhdistelmä tarjosi joustavuutta ja mahdollisti siirtymisen myös käyttäjäkohtaisesti, mikä oli erityisen hyödyllistä poikkeavissa laitekokoonpanoissa.

4 Projektin päätös

4.1 Dokumentointi ja ympäristön siivous

Projektin päätösvaiheessa korostettiin huolellista dokumentointia ja ympäristön viimeistelyä. Itse tämä Insinöörityö on osa projektin tarkkaa dokumentointia ja tarjoaa selkeän kuvan projektin vaiheista, toteutetuista konfiguraatioista sekä käytetyistä menetelmistä. Kaikki käyttöönotossa tehdyt konfiguraatiot ja asetukset dokumentoitiin huolellisesti vielä yrityksen tietohallinnon arkistoon. Tähän kuului muun muassa Intuneen luodut policyt, käytetyt PowerShell-skriptit sekä toteutetut tietoturvakäytännöt. Ympäristön siivouksen tarve jäi vähäiseksi, sillä tapa, jolla projekti toteutettiin, vähensi siivottavan määrää merkittävästi. Pilottiryhmä muodostettiin alun perinkin oikeista käyttäjistä, ja käyttäjäryhmän kokoa kasvatettiin hallitusti projektin edetessä. Tämä lähestymistapa mahdollisti sen, että uusia käyttäjiä ja laitteita voitiin lisätä suoraan tuotantoon ilman ylimääräisiä testikäyttäjiä tai -ryhmiä. Näin varmistettiin, että ympäristön hallinta pysyi yksinkertaisena ja järjestelmässä oli vain aktiivisia ja tarpeellisia resursseja.

4.2 Arviointi ja jatkotoimenpiteet

Käyttöönoton arvioinnissa keskityttiin tarkastelemaan projektin tavoitteiden saavuttamista sekä käyttäjien ja järjestelmän toimintaa uudessa ympäristössä. Projektin käyttöönottovaihe on virallisesti päättynyt, mutta työ jatkuu edelleen, sillä ympäristön laajuus ja käyttäjäkunta kasvavat jatkuvasti. Tämä korostaa

jatkuvan kehittämisen ja ylläpidon merkitystä, jotta ympäristö pysyy toimivana ja tietoturvallisena. Jatkotoimenpiteinä on sovittu tiivis yhteistyö projektin kumppanin kanssa. Yhteistyön tavoitteena on varmistaa järjestelmän toimivuus ja tuki, kun uusia käyttäjiä ja laitteita lisätään ympäristöön. Lisäksi pyritään ylläpitämään sujuvaa kommunikaatiota, joka mahdollistaa nopean reagoinnin mahdollisiin muutostarpeisiin tai ongelmatilanteisiin.

Ympäristön kasvun ja kehityksen myötä organisaation IT-osasto jatkaa aktiivisesti laitteiden hallintaa, konfiguraatioiden päivittämistä ja uusien palveluiden käyttöönottoa tarpeen mukaan. Näin varmistetaan, että Microsoft 365 Business Premium -ympäristö tukee liiketoiminnan tavoitteita myös tulevaisuudessa.

Lähteet

Vancouver-järjestelmä (numeroviitejärjestelmä):

Lisää lähteet siinä järjestyksessä, kuin ne on mainittu tekstissä.

1 https://learn.microsoft.com/en-us/mem/intune/

2 https://learn.microsoft.com/en-us/microsoft-365/security/defender

3 https://learn.microsoft.com/en-us/microsoft-365/security/defender-office-365

4 https://learn.microsoft.com/en-us/mem/autopilot/

5 https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/

6 Yrityksen sisäinen dokumentti

7 Yrityksen sisäinen dokumentti

8 Yrityksen sisäinen dokumentti

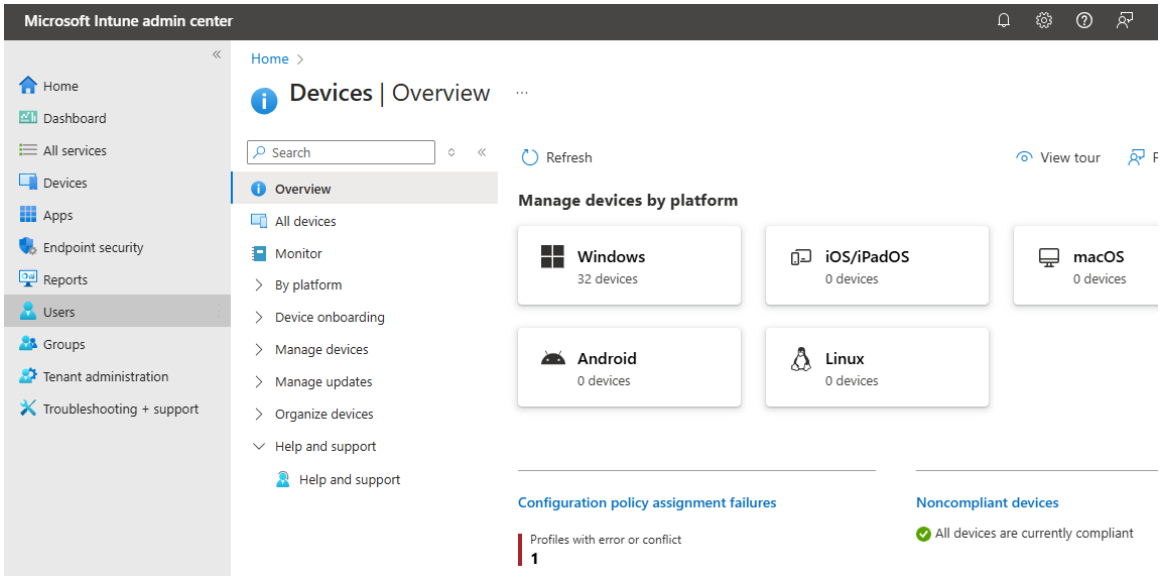
9 Yrityksen sisäinen dokumentti

10 https://learn.microsoft.com/en-us/microsoft-365/security/defender/attack-surface-reduction-rules

11 https://www.cisecurity.org/cis-benchmarks

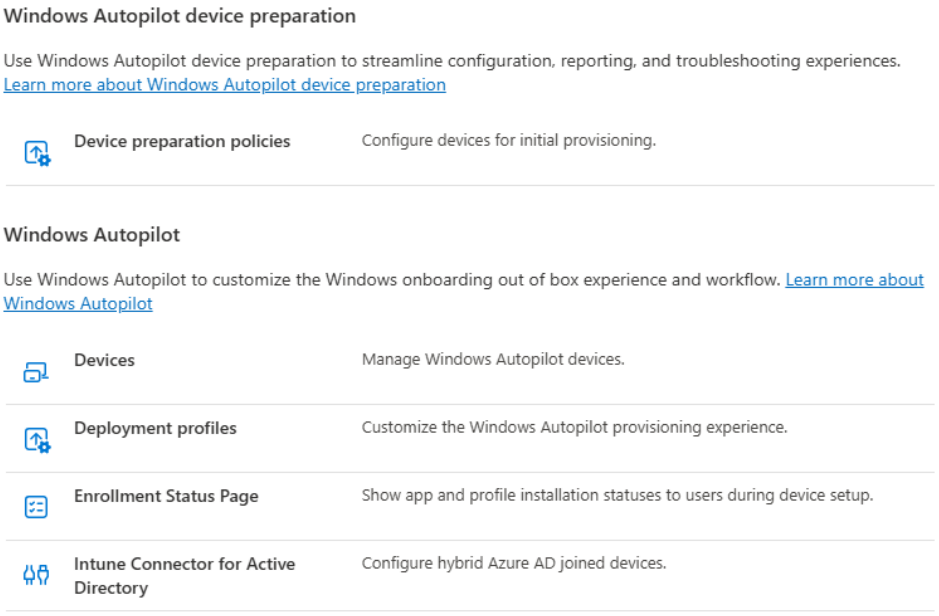
Liitteet

Liite 1



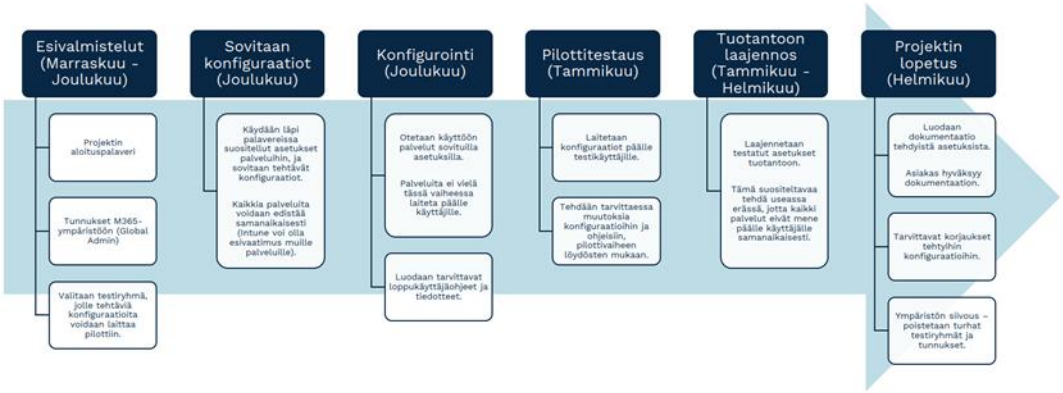
Microsoft Intune admin center

Liite 2



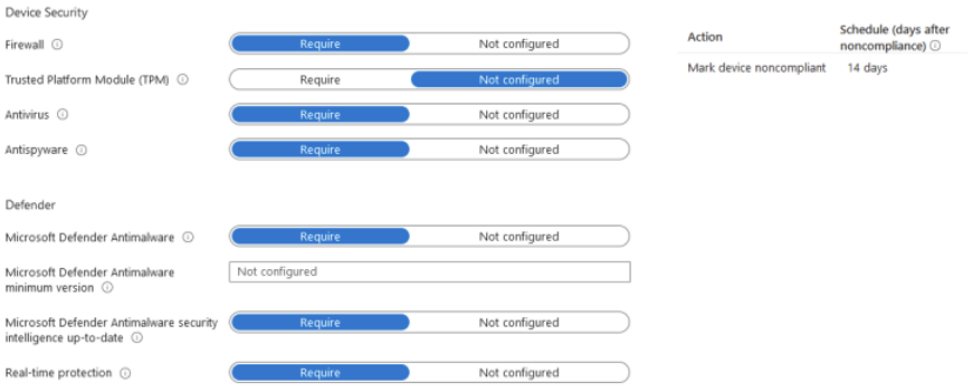
Windows Autopilot konfiguraatiot

Liite 3



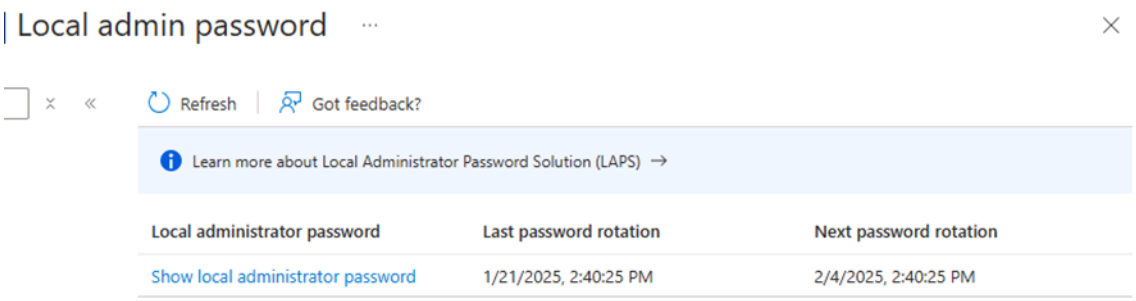
Projektin aikataulu

Liite 4



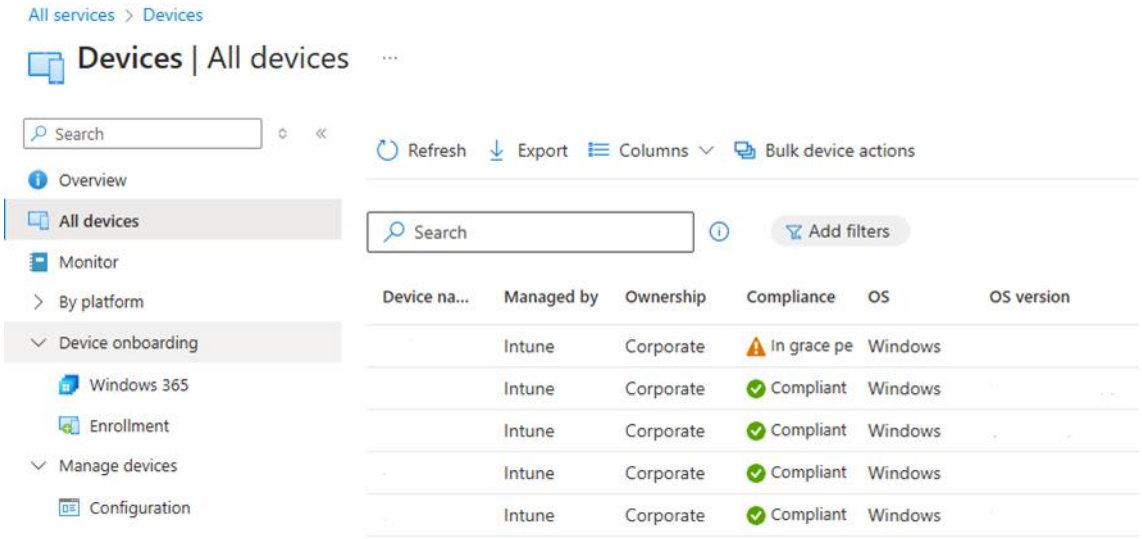
Laitevaatimusten määrittäminen Microsoft Intunessa

Liite 5



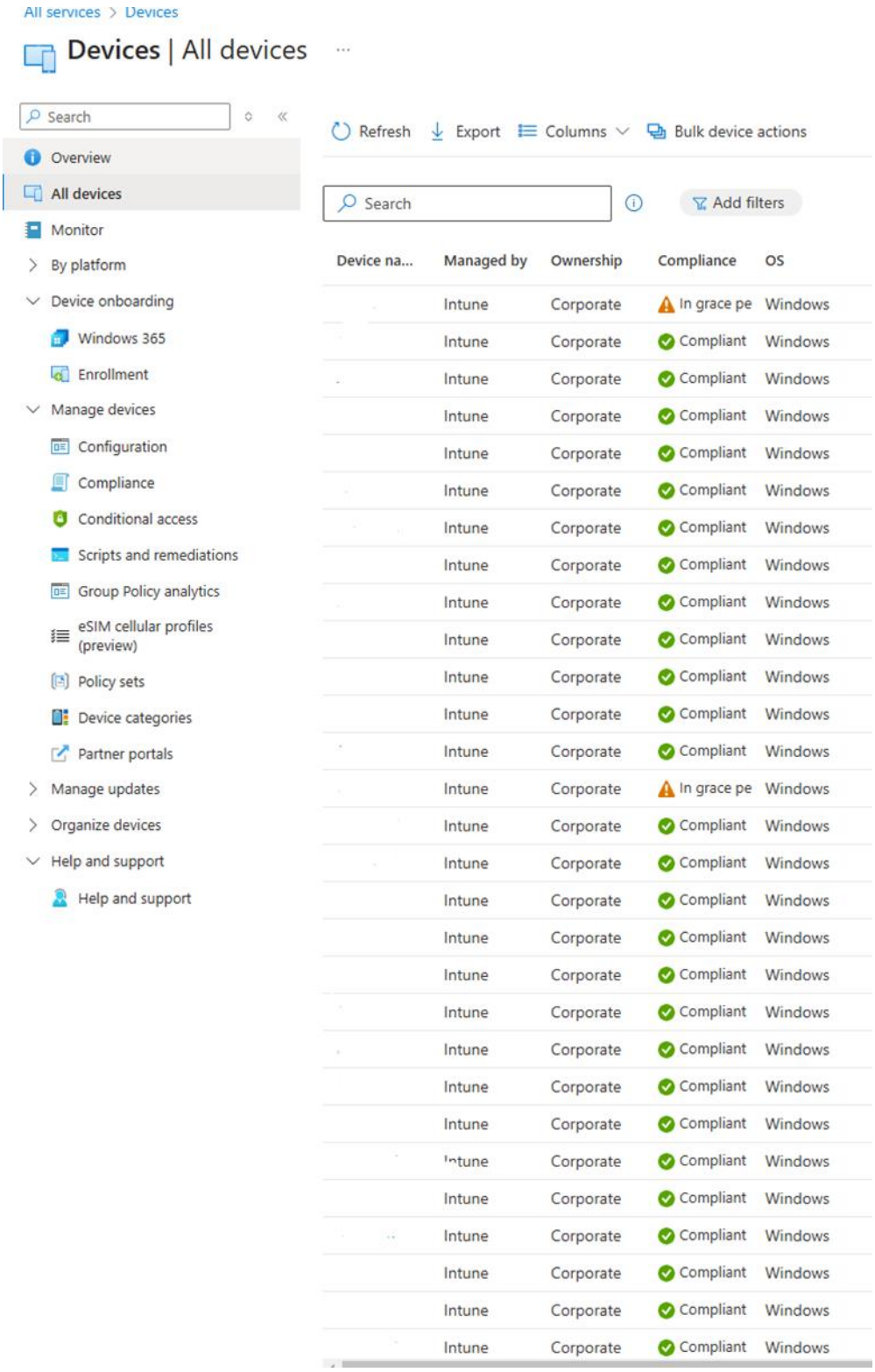
LAPS (Local Administrator Password Solution)

Liite 6



Pilotin alku

Liite 7



Siirtymäprosessi