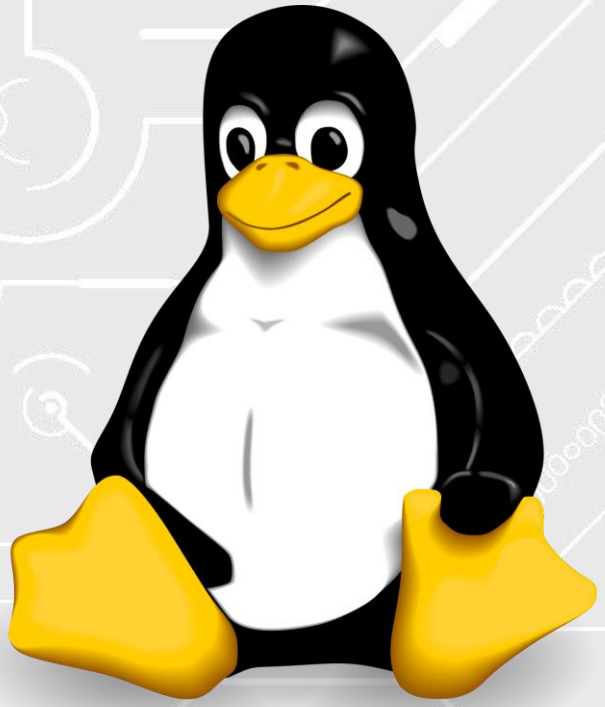
Linux työasemien hallinta Intunella



Ville Valkila

Enrollment

- https://learn.microsoft.com/en-us/intune/intune-service/user-help/microsoft-intune-app-linux
- Asennetaan intune-portal app
- Asennuskomennot vaihtelevat distron mukaan, saatavilla MS dokumentaatiosta
- Sign-in ja enrollment seuraamalla ohjeita
- Enrollmentin jälkeen tarkistaa compliance-tilanteen ja ajaa määritetyt skriptit
- Intune-portal appin ei tarvitse olla päällä hallinnointia varten

Viralliset vaatimukset

- https://learn.microsoft.com/en-us/intune/intune-service/user-help/enroll-device-linux#system-requirements
- Käyttöjärjestelmä
  - Ubuntu (22.04 LTS, 24.04 LTS)
  - RedHat Enterprise Linux (8, 9)
- Fyysinen laite tai VM, ei WSL2
- GNOME työpöytäympäristö
- Microsoft Edge
- Microsoft Intune app

Käyttöjärjestelmä

Virallinen tuki

Käytännössä testattu

Ubuntuun pohjautuvat distrot

Työpöytäympäristö

Virallinen tuki

Käytännössä testattu

Huom! Työpöytäympäristöä vaihdettaessa vaatii hyvin mahdollisesti uudelleen enrollauksen.
Intune käyttää oletuksena **GNOME Keyring** appia tallentamaan kirjautumistiedot:

- OAuth tokenit Entra ID:sta
- Device registration secretit
- Mahdollisesti Intune MDM sertifikaatti

Jos uudella DE:llä ei pääsyä esim `gnome-keyring-daemon` serviceen, pitää enrollaus tehdä uudestaan.
Osaa käyttää muidenkin ympäristöjen salaisuusmanagereja

Microsoft Edge

Virallinen tuki

Käytännössä testattu

Pääasiallinen tarkoitus vaatimukselle on **Conditional Access** pääsyjen toimivuus.

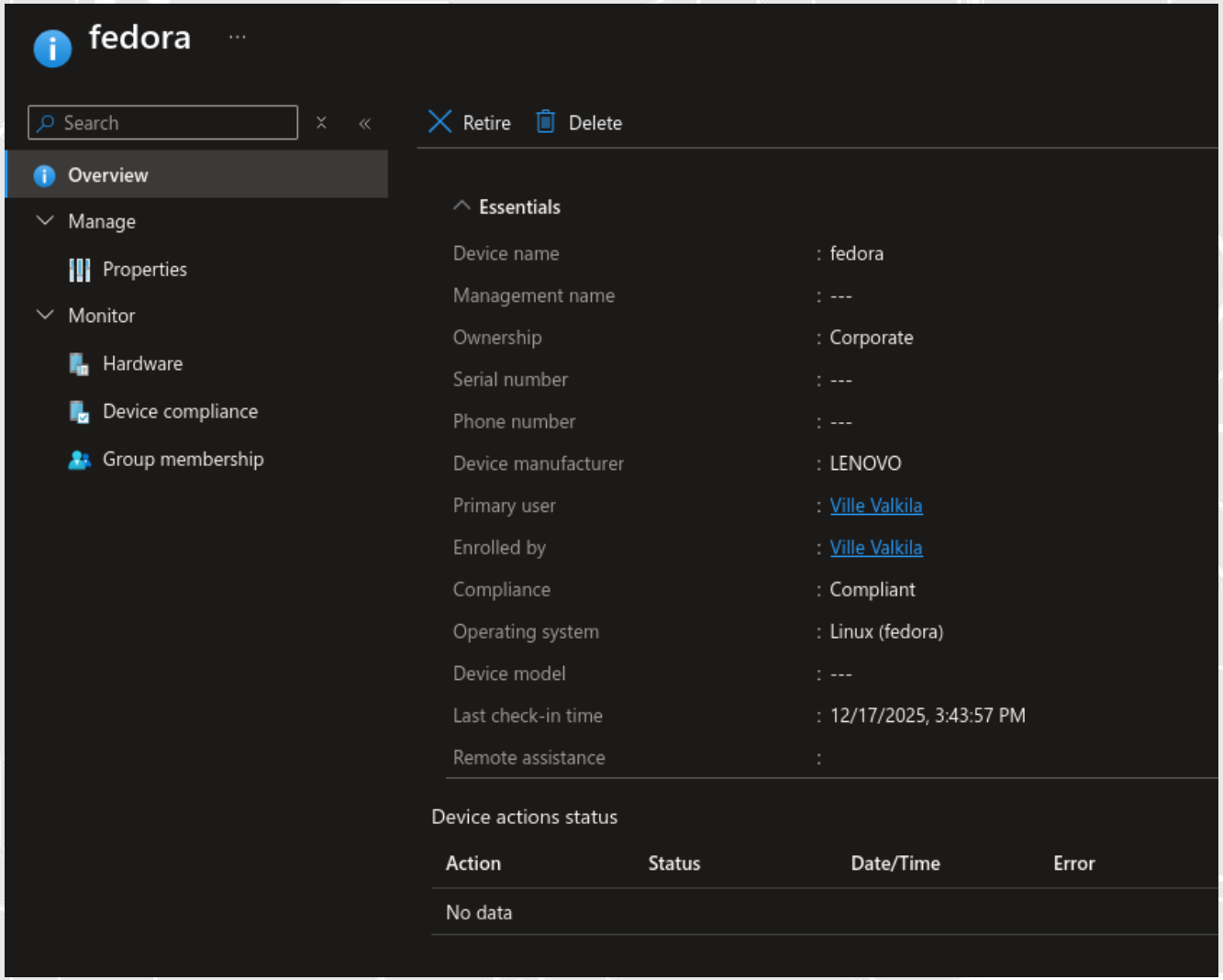
Kirjautuessa haetaan microsoft-identity-broker servicestä JWT-token joka syötetään x-ms-RefreshTokenCredential headeriin.

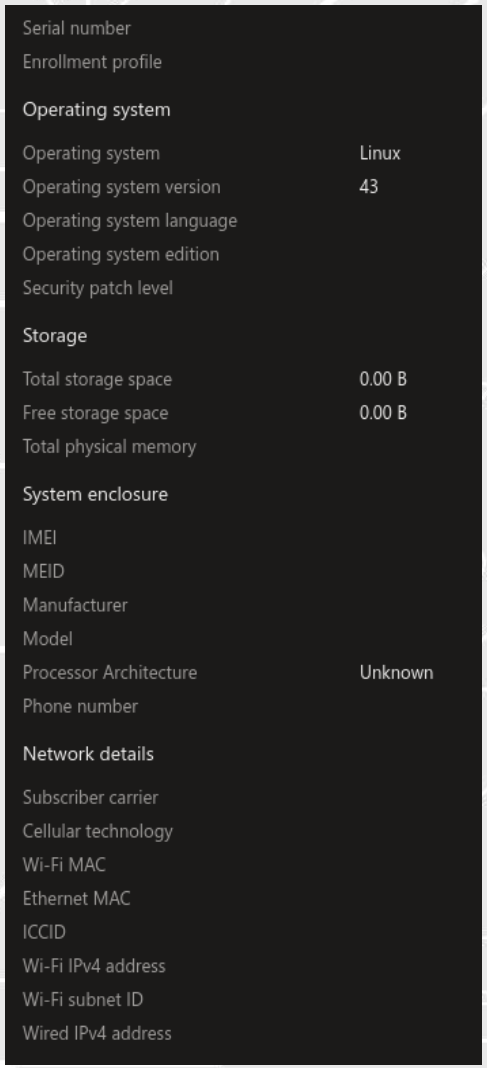
Edge tekee tämän automaattisesti kun selaimeen on kirjauduttu samalla käyttäjällä jolla Intune enrollment tehty.

Muihin selaimiin olemassa Siemensin kehittämä lisäosa joka tekee saman: https://github.com/siemens/linux-entra-sso

Suositus: Pidä Edge asennettuna vaikka käyttäisit muita selaimia

Näkyvyys laitteen tietoihin





Compliance

Natiivi

- Device Encryption
- Password Policy
- Distro ja versio

Custom

Mahdollista tehdä custom Compliance Policyja Bash skripteillä.

Kaksiosaisia:

- **Discovery script**: ajettava skripti, jonka output tulee olla JSON-parsetettava string
- **Rules file:** JSON-objekti johon skriptin outputtia verrataan ja jonka perusteella päätetään policyn tila

Mahdolisuuksia:

- Päivitysten tarkistus
- Microsoft Defender for Endpoint statuksen tarkistus

Skriptit

Laitteille voidaan ajaa omia Bash-skriptejä Intunen kautta.

Mahdollisuuksia:

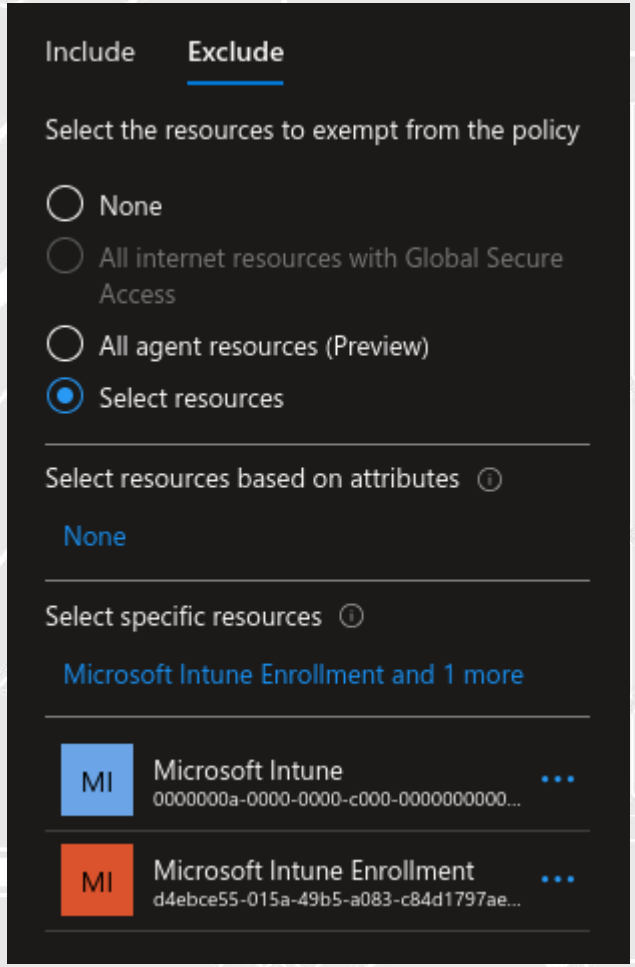
- Microsoft Defender for Endpoint
  - Asennus
  - Onboarding
- VPN asennus

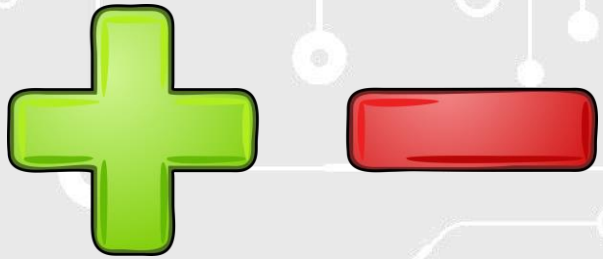
Rajoituksia:

- Maksimi ajoaika: 5 minuuttia
- Maksimi skriptin koko: 1 MB
- Maksimi output: 1 MB

Conditional Access

- Conditional Access policyn kautta voidaan rajoittaa pääsyä non-compliant Linux laitteilta.
- Include: All resources
- Exclude:
  - Microsoft Intune 0000000a-0000-0000-c000-000000000000
  - Microsoft Intune Enrollment d4ebce55-015a-49b5-a083-c84d1797ae8c
- Compliancen hallinta intune-portal appin kautta.
- Compliancen tarkistus microsoft-identity-broker servicen ja selaimen kautta





Plussat

- Näkyvyyttä ja hallintaa Linux työasemille samoilla työkaluilla mitkä jo käytössä
- Toiminnallisuudet ja toimintavarmuus kehittyneet nopeasti
- Custom complianceilla saadaan näkyvyys melkein mihin vain halutaan

Miinukset

- Linuxin avoin ekoympäristö tekee hallinnasta vaikeaa ilman rajoituksia
- Intunen vajavaiset toiminnallisuudet Linuxille suhteessa muihin alustoihin
- Skriptien aikarajoitukset rajoittavat hallintaa
- Jotkut toiminnallisuudet eivät toimi kuten virallisesti ohjeistettu

Bonus

Lisähallintaa Ansiblen avulla

Intune-skriptien aikaraja tekee tiettyjen sovellusten asentamisesta ja päivittämisestä käytännössä mahdotonta pelkkien skriptien avulla.

Intunen avulla voitaisiin kuitenkin asentaa Ansible ja määrittää ajoitetut taskit joiden avulla saadaan git-repositoriosta haettua ajantasaiset konfiguraatiot.

Mahdollistaa:

- Ajoitetut päivitykset
- Sovelluspaketit rooleittain
- Uudelleenkäynnistys tarvittaessa