

Linux työasemien hallinta Intunella



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



GNOME™

Käytännössä testattu



GNOME™



SWAY

Huom! Työpöytämääristöä 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** päisyjen toimivuus.

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

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

Muihin selaiimiin 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

fedora ...

Search X < Retire Delete

Overview

Manage Properties

Monitor Hardware Device compliance Group membership

Essentials

Device name	:	fedora
Management name	:	---
Ownership	:	Corporate
Serial number	:	---
Phone number	:	---
Device manufacturer	:	LENOVO
Primary user	:	Ville Valkila
Enrolled by	:	Ville Valkila
Compliance	:	Compliant
Operating system	:	Linux (fedora)
Device model	:	---
Last check-in time	:	12/17/2025, 3:43:57 PM
Remote assistance	:	

Device actions status

Action	Status	Date/Time	Error
No data			

Serial number
Enrollment profile
Operating system
Operating system
Operating system version
Operating system language
Operating system edition
Security patch level

Storage
Total storage space 0.00 B
Free storage space 0.00 B
Total physical memory

System enclosure
IMEI
MEID
Manufacturer
Model
Processor Architecture Unknown
Phone number

Network details
Subscriber carrier
Cellular technology
Wi-Fi MAC
Ethernet MAC
ICCID
Wi-Fi IPv4 address
Wi-Fi subnet ID
Wired IPv4 address

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

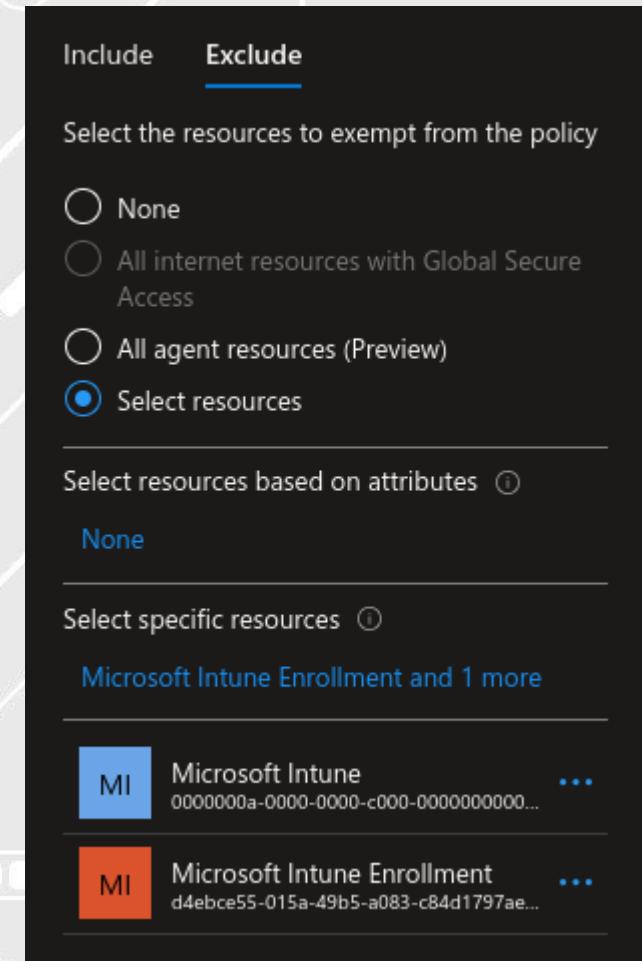
Rajoituksia:

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



Conditional Access

- Conditional Access poliisin kautta voidaan rajoittaa pääsyä non-compliant Linux laitteiltia.
- 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

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

Bonus

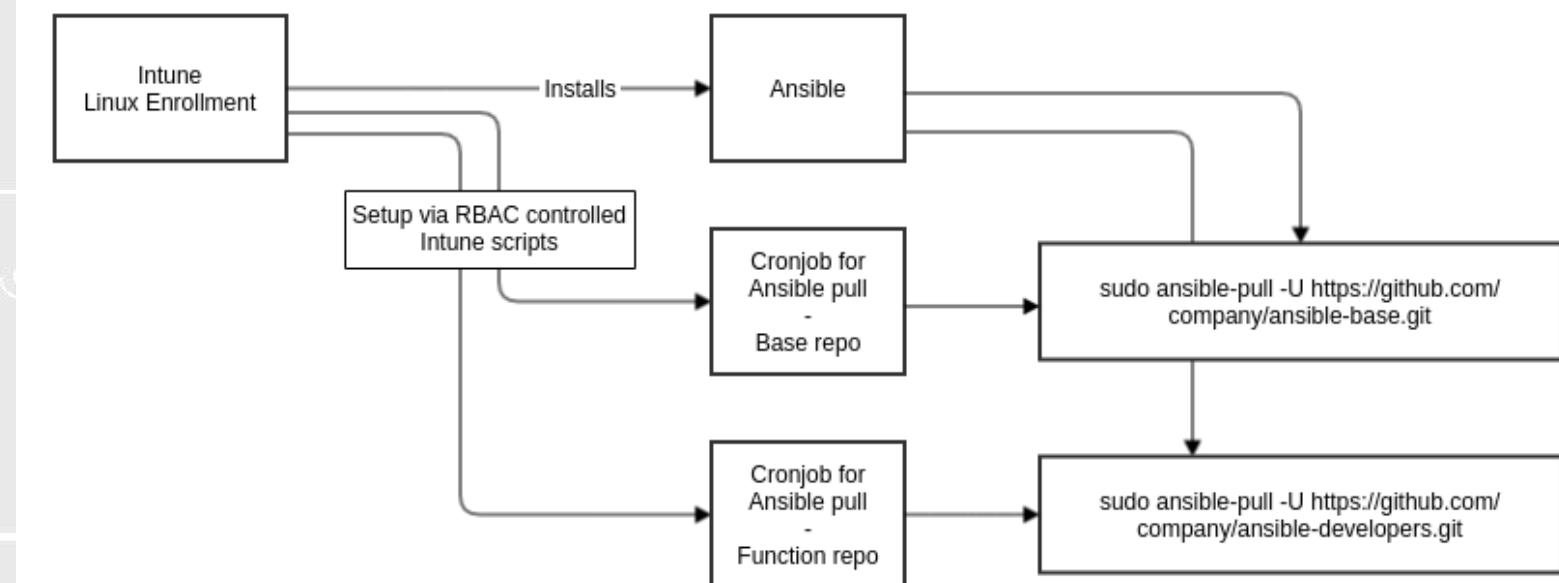
Lisähallintaa Ansiblen avulla

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



A N S I B L E