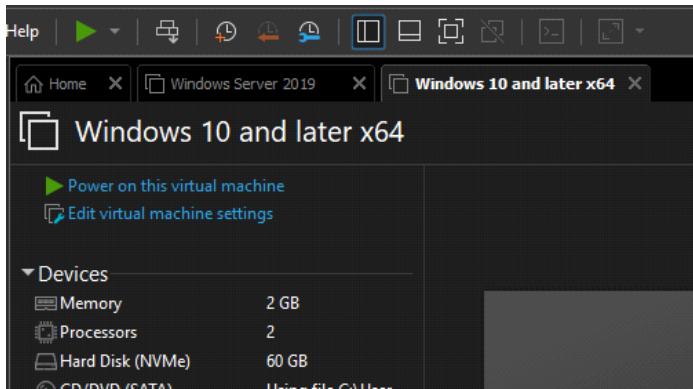


7.2.3. Bitlocker - 4

Monday, December 8, 2025 14:32

Tämä sivu jatkuu "7.2.1. Bitlocker 2:sta"

Koskien VM2 ja versus tosi elämässä



VM2:ssa, joka kerta käynnistäässä tulee toistuvasti sitä **bluescreen**, että syötä kyseinen Bitlocker salasana.

- Koska puuttuu TPM (trusted platform module)
- BitLocker ei voi **luottaa laitteeseen automaattisesti**, joten se vaatii **manuaalisen salasanan** ennen kuin Windows voi edes alkaa latautua.
- Tämä on **turvamekanismi**, kun TPM puuttuu – BitLocker ei halua avata levyä ilman varmennusta.

Tosi elämässä (oikea työasema Windows 10/11 + TPM)

- TPM tallentaa salausavaimen turvallisesti.
- Käynnistyksessä BitLocker **avaa levyt automaattisesti TPM:n avulla**.
- Käyttäjä näkee vain **normaalin kirjautumisruudun** (Ctrl+Alt+Del → salasana).
- BitLocker toimii taustalla, eikä käyttäjä edes huomaa sitä.

Miten saat VM2 toimimaan kuten oikea työasema?

Jos haluat, että VM2 ei kysy salasanaa joka bootissa, sinulla on kaksi vaihtoehtoa:

1. Lisää virtuaalinen TPM VMware Workstationiin

- Edellyttää UEFI + Secure Boot -asetuksia VM:ssä.
- BitLocker voi käyttää TPM:ää → levy avautuu automaattisesti.
- Käyttäjä näkee vain kirjautumisruudun.

2. Käytä USB-startup keytä

- BitLocker avaa levyn automaattisesti, jos USB-avain on kiinni.
- Ei yhtä kätevää kuin TPM, mutta poistaa salasanen tarpeen.

Yhteenveto

Ympäristö	BitLocker-käyttäytyminen
VM ilman TPM	Kysyy salasanaa joka bootissa
Oikea työasema TPM:llä	Avautuu automaattisesti, ei salasanaa
VM TPM:llä (virtuaalinen)	Sama kuin oikea työasema
USB-startup key	Avautuu automaattisesti, jos USB kiinni

Tosi elämässä Windows 10/11 -työasemassa, jossa on TPM-siru, konfigurointi menee hieman eri tavalla – mutta peruslogiikka on sama kuin mitä harjoittelun.

Tosi elämässä BitLocker-konfigurointi (TPM käytössä)

1. Ota BitLocker käyttöön
 - Control Panel → BitLocker Drive Encryption → Turn on BitLocker
 - Tai suoraan Settings → Device encryption (jos OEM on esiasentanut sen).
2. TPM hoitaa avaimen tallennuksen
 - BitLocker tallentaa avaimen TPM:ään automaattisesti.
 - Käyttäjältä ei kysytä salasanaa bootissa, ellei GPO vaadi PIN:iä.
 - Käynnistyksen yhteydessä levy avautuu taustalla → käyttäjä näkee vain kirjautumisruudun.
3. Recovery key tallennus

- Käyttäjälle tarjotaan vaihtoehdot: Save to file, Save to USB, Print.
- Yritysympäristössä GPO varmistaa, että recovery key tallentuu automaattisesti AD:hen tai Azure AD:hen.
- Tämä on sama kuin labissa – AD tallentaa useita avaimia, jos konfigurointi toistetaan.

4. Salaus käynnistyy

- Oletuksena *Used Space Only Encryption* → nopeampi.
- Salaus valmistuu taustalla, käyttäjä voi jatkaa töitä.

5. Normaali käyttö

- Käyttäjä ei näe BitLockeria arjessa.
- Bootissa levy avautuu TPM:n avulla → kirjautuminen Windowsiin toimii kuten aina.
- Recovery key tarvitaan vain poikkeustilanteessa (esim. TPM reset, BIOS-muutos, levy siirretään toiseen koneeseen).

Vertailu lab vs. oikea työasema

Ympäristö	Boot-käytätyminen	Recovery key tallennus
VM ilman TPM	Kysyy salasanaa joka bootissa	USB/file/AD, useita avaimia syntyy
Oikea työasema TPM:llä	Avautuu automaattisesti, ei salasanaa	Tallentuu AD/Azure AD automaattisesti
Yritysverkko (Network Unlock)	Avautuu automaattisesti sisäverkossa	Recovery key silti tallennetaan AD:hen

perusvaiheet ovat täsmälleen samat kuin mitä olet tehnyt labissa (BitLocker päälle, recovery key talteen, AD-tallennus). Ainoa iso ero on se, että TPM poistaa sen sinisen salasanaruudun bootissa ja tekee käytöstä "normaalina" työaseman kokemuksen.

#####

Tosi elämän konfigurointi tapa

miten tosi elämässä Windows Serverin kautta yrityksessä konfiguroidaan BitLocker GPO-asetukset, jotta työasemat saadaan salattua ja recovery key tallennettua AD:hen. Tämä menee hyvin lähelle sitä, mitä labrassa tehty, mutta oikeassa ympäristössä se tehdään keskitetysti ja hallitusti.

Tosi elämän BitLocker-konfigurointi Windows Serverissä (Domain-ympäristö)

1. GPO:n luonti

- Avaa **Group Policy Management Console (GPMC)** Windows Serverissä.
- Luo uusi GPO (esim. *BitLocker Policy*) ja linkitä se siihen OU:hun, jossa työasemat sijaitsevat.

2. BitLocker Drive Encryption -asetukset

Polku: Computer Configuration → Policies → Administrative Templates → Windows Components → BitLocker Drive Encryption
Tärkeimmät asetukset:

- Choose how BitLocker-protected operating system drives can be recovered
 - Allow data recovery agent
 - Allow 48-digit recovery password
 - Allow 256-bit recovery key
 - Save BitLocker recovery information to AD DS for operating system drives
 - Store recovery passwords and key packages
- Require additional authentication at startup
 - Enable, ja valitse *Allow BitLocker without a compatible TPM* jos haluat sallia salauksen myös koneille ilman TPM:ää (lab-tilanne).
 - Tosi elämässä TPM on yleensä käytössä, jolloin tämä ei ole pakollinen.
- Choose drive encryption method and cipher strength
 - XTS-AES 128 tai XTS-AES 256 (yrityksissä usein 256).
- Configure use of passwords for operating system drives
 - Voit sallia PIN/password, mutta TPM + PIN on yleisin käytäntö.

3. Recovery key tallennus AD:hen

- Kun GPO on asetettu, jokainen domainiin liittynyt työasema tallentaa automaattisesti recovery keyn AD DS:ään, kun BitLocker otetaan käyttöön.
- Admin voi hakea avaimen Active Directory Users and Computers → Computer Object → BitLocker Recovery -välilehti.

4. Käyttöönotto työasemilla

- Kun käyttäjä tai admin ottaa BitLockerin käyttöön työasemalla, se noudattaa GPO-asetuksia.
- Recovery key tallentuu automaattisesti AD:hen.
- TPM avaa levyn automaattisesti bootissa → käyttäjä näkee vain kirjautumisruudun.

Ero labin ja tosi elämän välillä

Lab (VM ilman TPM)	Tosi elämä (työasema TPM:llä)
Salasana joka bootissa	TPM avaa levyn automaattisesti

Recovery key tallennus USB/Desktop Recovery key tallennus AD/Azure AD automaattisesti

GPO: Allow BitLocker without TPM GPO: TPM käytössä, PIN optio

Käyttäjä näkee BitLocker-ruudun Käyttäjä näkee vain Windows login

Tosi elämässä Windows Serverin GPO-asetuksilla määritetään BitLocker-politiikka, ja recovery keyt tallennetaan AD:hen. Käyttäjät eivät näe BitLockeria arjessa, koska TPM hoitaa avauksen automaattisesti.

Kun **tosi elämässä** yritys ottaa BitLockerin käyttöön Windows Serverin kautta GPO:lla ja työasemissa on **TPM-siru**, käyttäjän kokemus on se "normaali":

- **Käynnistykseen ei näy BitLocker-salasana-ruutua** (sininen ruutu), vaan levy avautuu automaattisesti TPM:n avulla.
- Käyttäjä näkee vain Windowsin kirjautumisruudun ja syöttää tavallisen AD-salasanansa.
- BitLocker toimii taustalla, eikä käyttäjä huomaa sitä arjessa.

🔍 Voiko tulla virheitä tai poikkeuksia?

Kyllä, muutamia tilanteita voi aiheuttaa virheilmoituksia tai vianmääritystä:

- **TPM ei ole alustettu tai otettu käyttöön BIOS/UEFI:ssä** → BitLocker ei voi käyttää TPM:ää, jolloin se palaa salasanakyselyyn.
- **GPO-konfigurointi puuttuellinen** → esim. jos "Save recovery information to AD DS" ei ole oikein asetettu, recovery key ei tallennu AD:hen.
- **BIOS/UEFI-muutokset** (firmware-päivitys, Secure Boot pois päältä) → BitLocker voi tulkita tämän riskiksi ja pyytää recovery keytä bootissa.
- **Levy siirretään toiseen koneeseen** → BitLocker havaitsee ympäristön muuttuneen ja vaatii recovery keyn.
- **Virheellinen avainhallinta** → jos avaimia ei ole tallennettu AD:hen tai Azure AD:hen, admin ei saa levyä auki ongelmatilanteessa.
- **Käyttäjäkohtaiset PIN-säännöt** → jos GPO vaatii TPM+PIN, käyttäjältä kysytään PIN bootissa (mutta ei sitä 48-numeroista recovery keytä).

✓ Yhteenveto

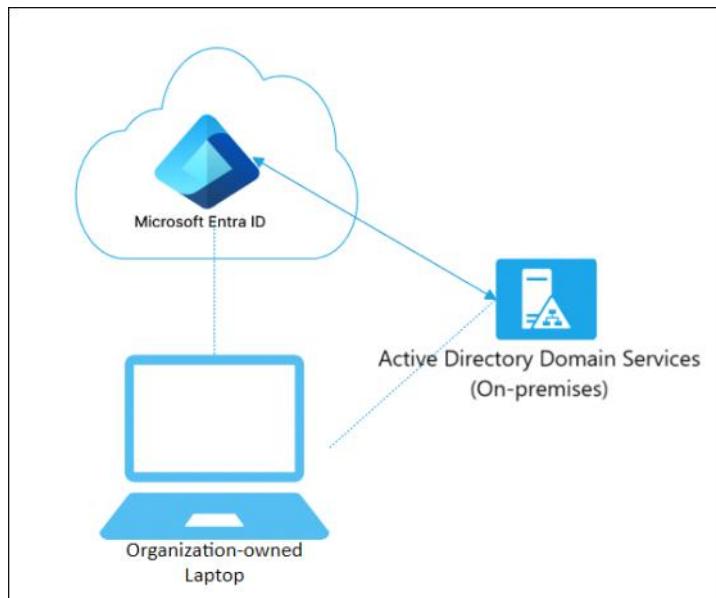
- **Normaalissa yritysympäristössä (TPM käytössä)**: ei tule joka kerta BitLocker-salasanaa → levy avautuu automaattisesti.
- **Virheitä voi tulla vain poikkeustilanteissa**: TPM ei käytössä, BIOS/UEFI muuttuu, levy siirretään, GPO väärin asetettu.
- **Recovery keyn tallennus AD:hen** on kriittinen, jotta admin voi aina avata levyn ongelmatilanteessa.

Tosi elämässä BitLocker ei häiritse käyttäjää joka bootissa, mutta poikkeustilanteissa se voi pyytää recovery keytä. Tämä on osa sen suojauslogiikkaa, ei virhe.

#####

Windows server + Entra (Hybridimalli)

Hybridimallissa (Entra ID + on-prem AD) BitLocker-konfiguraatio voi aiheuttaa ristiriitoja, jos samanaikaisesti käytetään sekä GPO:ta että Intune-politiikkoja. Intune-lisenssin puuttuminen ei sinänsä riko ympäristöä, mutta se rajaa hallintaa ja voi johtaa sekaannukseen, jos odotetaan MDM-hallintaa. Defender ja Intune eivät itsessään aiheuta teknistä konfliktia, mutta päälekkäiset asetukset eri hallintakanavista voivat johtaa epäselvyyksiin



🔑 Keskeiset huomiot hybridimallissa

- **BitLocker-politiikat voivat tulla useasta lähteestä:**
 - Group Policy (on-prem AD)
 - Intune (MDM)
 - Paikalliset asetukset → Jos samalle asetukselle on eri arvot, syntyy konflikti, eikä Intune voi aina ohittaa GPO:ta.

- **Intune-lisenssin vaikutus:**
 - Ilman Intune-lisenssiä et voi keskitetysti hallita BitLocker-asetuksia pilvestä.
 - Laite voi silti olla hybrid-joinattu (AD + Entra ID), mutta hallinta jää GPO:n varaan.
 - Tämä ei riko ympäristöä, mutta voi hämmättää, jos odotetaan Intunen raportointia tai avainten tallennusta AAD:hen.
- **Recovery key -tallennus:**
 - Hybridissä avaimet voidaan tallentaa joko AD DS:ään tai Entra ID:hen.
 - Jos molemmat polut ovat käytössä, varmista että prosessi on selkeä, ettei avaimet katoa tai tallennu väärään paikkaan.

Mahdolliset sekaannukset hiekkalaatikossa

- **Defender vs. Intune:**
 - Defenderin asetuksia voi hallita GPO:lla, Intunella tai Defender Security Centerillä.
 - Jos eri hallintakanavat asettavat ristiriitaisia sääntöjä (esim. AV exclusions, ASR rules), syntyy epäselvyyksiä.
- **Intune + GPO päällekkäisyys:**
 - Microsoft suosittelee valitsemaan ensisijaisen hallintakanavan (MDM tai GPO) ja minimoimaan päällekkäisyydet.
- **VMWorkstation sandbox:**
 - Testiympäristössä hybrid-join voi toimia, mutta Intune ei välttämättä hallitse virtuaalikonetta oikein, jos TPM ei ole käytettävissä.
 - Tämä voi estää BitLocker-politiikan täyden toteutumisen.

Suositeltu lähestymistapa

1. **Päätää hallintakanava:** Käytätkö BitLockerille GPO:ta vai Intunea? Älä sekoita molempia.
2. **Selkeytä recovery key -polku:** Valitse AD DS tai Entra ID, dokumentoi prosessi.
3. **Testaa sandboxissa erikseen:**
 - Ensin GPO-only skenaario
 - Sitten Intune-only skenaario
 - Lopuksi hybrid, jotta näet missä kohtaa konfliktit syntyvät.
4. **Defenderin hallinta:** Pidä asetukset yhdessä hallintakanavassa (Intune tai GPO), vältä päällekkäisyyksiä.

Hybridimalli ei itsessään ole ongelma, mutta **päällekkäiset politiikat eri hallintakanavista** (Intune, GPO, Defender) voivat aiheuttaa ristiriitoja. Sandboxissa tämä näkyy erityisesti TPM/BitLocker-politiikoissa ja avainten tallennuksessa.

GPO vs. Intune (MDM) politiikat

- **Group Policy (GPO):**
 - Windows Serverin kautta asetetut GPO:t ovat perinteisiä, ja ne soveltuват erityisesti on-prem AD -ympäristöön.
 - Ne kirjoittavat asetuksia suoraan rekisteriin ja voivat olla hyvin "pakottavia".
- **Intune / MDM policyt:**
 - Intune hallitsee asetuksia MDM-kanavan kautta.
 - MDM-politiikat eivät aina voi ohittaa GPO:ta, jos sama asetus on jo määritetty GPO:lla.
- **Konfliktitilanne:**
 - Jos samaa asetusta hallitaan sekä GPO:lla että Intunella, GPO yleensä voittaa, koska se kirjoittaa suoraan rekisteriin.
 - Tämä voi johtaa siihen, että Intunen raportointi näyttää politiikan epäonnistuneena tai "not applicable".
 - Käytännössä syntyy sekaannusta, jos ei ole selkeästi päättetty, kumpi hallintakanava on ensisijainen.

Esimerkki BitLockerista

- **GPO:** Voit määrittää BitLocker-politiikat (esim. avainten tallennus AD DS:ään).
- **Intune:** Voit määrittää BitLocker-politiikat (esim. avainten tallennus Entra ID:hen).
- Jos molemmat ovat käytössä, laite voi yrittää noudattaa molempia → tuloksena ristiriita tai epäonnistunut konfiguraatio.

Microsoftin suositus

- **Valitse yksi hallintakanava per asetus:**
 - Jos käytät Intunea, vältä päällekkäisiä GPO-asetuksia.
 - Jos käytät GPO:ta, älä otta samaa asetusta käyttöön Intunessa.
- **Hybrid join ei itsessään ole ongelma, mutta hallintakanavien päällekkäisyys voi aiheuttaa sekaannusta.**

Windows Serverin GPO-asetukset voivat sekoittua Intunen MDM-politiikkoihin, jos molemmat hallitsevat samoa asetuksia. Paras käytäntö on päättää selkeästi, kumpi hallintakanava hallitsee mitäkin, ja dokumentoida se.