

7.2.1. Bitlocker - 2

Monday, December 8, 2025 14:32

Tässä sivustossa alkaa virallinen demo konffausta ja testataan toinen vm2 työasema, että testaan se bitlocker avain saanti. Huomoina tämä koskee myös vm1 windows serverin administrator käyttäjää itsensä.

#####
#####

Install ohjeita:

<https://www.scribd.com/document/792644888/Enabling-BitLocker-on-Windows-Server>

[https://mcsa15.biz/mcsa15/BitLocker%202012\(2\).pdf](https://mcsa15.biz/mcsa15/BitLocker%202012(2).pdf)

<https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/install-server>

<https://99rdp.com/enable-bitlocker-encryption-on-windows-server/>

HARJOITUKSEN DEMO OHJE VIDEO - alemman mukaan

[Windows Server 2022 - Configure and Enable BitLocker Drive Encryption on Windows Server 2022](#)



OMA ACTION - START HERE;

Alkuun suoritin ensimmäiset skannaukset, että tämä windows serveri toimii ja ei ole mitään virusta.

- Tämä komento hyvä esim. Tarkistaa troubleshootit ja häiriötä - kannattaa suorittaa esim. Ennen vm ohjelman suljemista ja/tai aloittaa konfiguroimaan/lataa uutta ominaisuutta työkalua windows serveriin.

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator>
PS C:\Users\Administrator> sfc /scannow

Beginning system scan. This process will take some time.

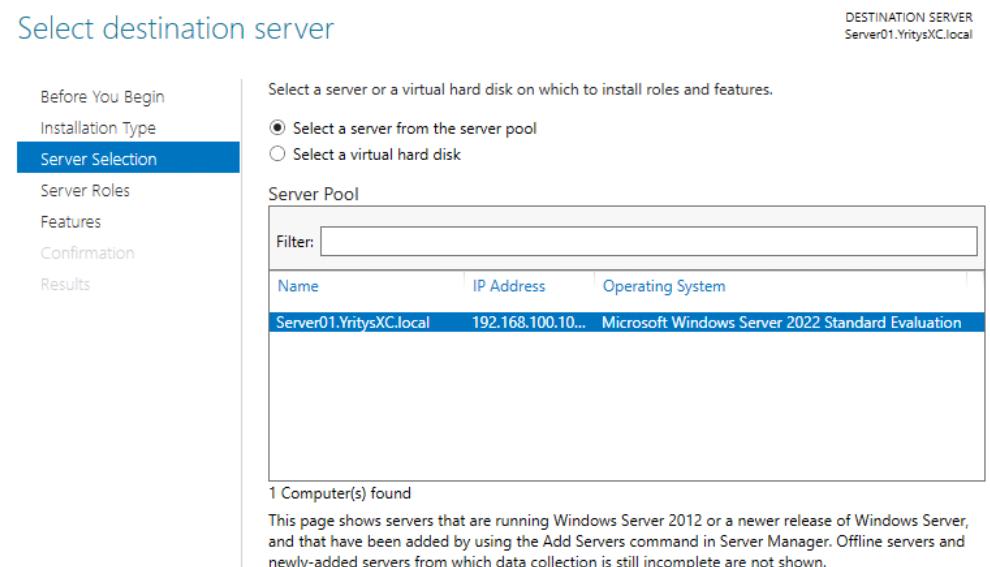
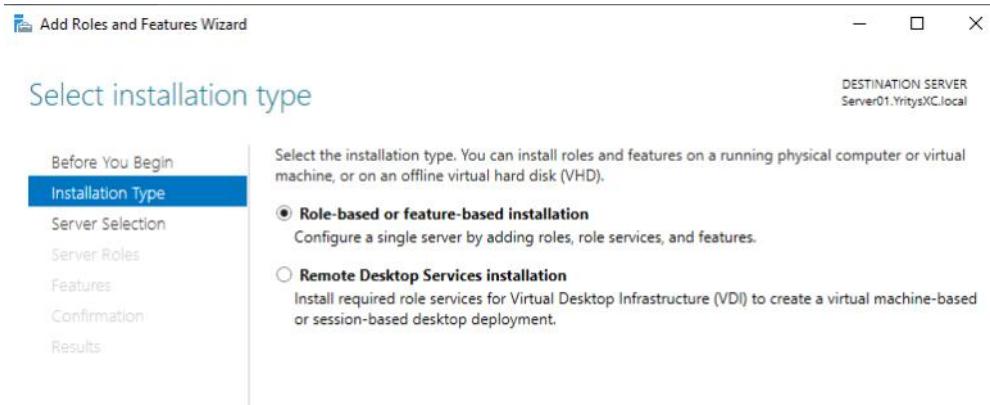
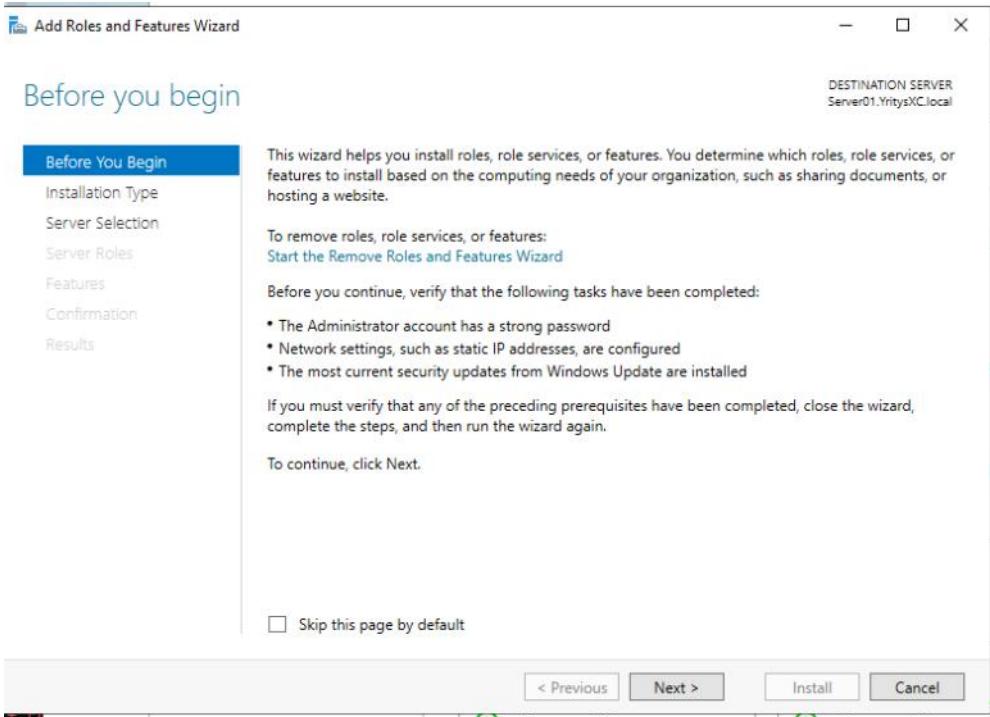
Beginning verification phase of system scan.
Verification 100% complete.

Windows Resource Protection did not find any integrity violations.
PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator> DISM /Online /Cleanup-Image /RestoreHealth

Deployment Image Servicing and Management tool
Version: 10.0.20348.2849

Image Version: 10.0.20348.4297

[=====100.0%=====] The restore operation completed successfully.
The operation completed successfully.
PS C:\Users\Administrator>
```



Select server roles

DESTINATION SERVER
Server01.YritysXC.local

- Before You Begin
- Installation Type
- Server Selection
- Server Roles**
- Features
- Confirmation
- Results

Select one or more roles to install on the selected server.

Roles	Description
<input checked="" type="checkbox"/> Active Directory Certificate Services (1 of 6 installed)	Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.
<input checked="" type="checkbox"/> Active Directory Domain Services (Installed)	
<input type="checkbox"/> Active Directory Federation Services	
<input type="checkbox"/> Active Directory Lightweight Directory Services	
<input type="checkbox"/> Active Directory Rights Management Services	
<input type="checkbox"/> Device Health Attestation	
<input checked="" type="checkbox"/> DHCP Server (Installed)	
<input checked="" type="checkbox"/> DNS Server (Installed)	
<input type="checkbox"/> Fax Server	
<input checked="" type="checkbox"/> File and Storage Services (3 of 12 installed)	
<input type="checkbox"/> Host Guardian Service	
<input type="checkbox"/> Hyper-V	
<input type="checkbox"/> Network Policy and Access Services	
<input type="checkbox"/> Print and Document Services	
<input type="checkbox"/> Remote Access	
<input type="checkbox"/> Remote Desktop Services	
<input type="checkbox"/> Volume Activation Services	
<input type="checkbox"/> Web Server (IIS)	
<input type="checkbox"/> Windows Deployment Services	

< Previous Next > Install Cancel

Huom tämä ensimmäinen tieto koskien Bitlockerista

BitLocker Drive Encryption on se varsinainen levyn salausomaisuus, jota tarvitset Windows Serverissä. BitLocker Network Unbck taas on lisäomaisuus, joka mahdollistaa automaattisen käynnistyksen ilman PIN-koodia, jos palvelin tai työasema käynnistyy yrityksen sisäverkossa. Jos olet vain ottamassa BitLockeria käyttöön palvelimelle, et välittämättä tarvitse Network Unlockia – se on tarkoitettu lähinnä domain-ypäristöihin, joissa halutaan helpottaa hallintaa.

BitLocker Drive Encryption

- **Tarkoitus:** Salaa koko levyn (yleensä käyttöjärjestelmän C:-asema ja/tai datalevyt).
- **Käyttö:** Suojaa dataa varkauden, katoamisen tai luvattoman käytön varalta.
- **Avainhallinta:** Voit käyttää TPM:ää, PIN-koodia, USB-avainta tai tallentaa palautusavaimen AD:hen.
- **Tarve:** Tämä on se ominaisuus, jota käytännössä tarvitset, kun haluat salata Windows Serverin levyn.

🌐 BitLocker Network Unlock

- **Tarkoitus:** Mahdollistaa automaattisen levyn avauksen, kun kone käynnistyy yrityksen sisäverkossa.
- **Miten toimii:** Kun palvelin tai työasema on kytketty langalliseen verkoon, käynnistyksen yhteydessä avain toimitetaan verkon yli (DHCP + WDS-palvelin tarvitaan).
- **Hyöty:** Poistaa tarpeen syöttää PIN-koodia jokaisessa bootissa, mikä helpottaa esim. palvelinten etähallintaa ja työasemien Wake-on-LAN -skenarioita.
- **Vaatii:** Erillisen infrastruktuurin (Windows Deployment Services + Network Unlock -palvelu). Ei toimi ilman domain-ypäristöä ja oikeaa verkkosetusta.

⚖️ Tarvitsetko Network Unlockin?

- **Jos käytät BitLockeria vain yksittäisellä Windows Serverillä:** Et tarvitse Network Unlockia. Riittää, että otat käyttöön BitLocker Drive Encryptionin ja hallitset avaimet (TPM, PIN, AD-tallennus).
- **Jos hallitset useita palvelimia/työasemia domainissa:** Network Unlock voi olla hyödyllinen, koska se vähentää PIN-koodien syöttämisen tarvetta ja helpottaa automaattisia uudelleenkäynnistyksiä.
- **Jos ei ole domainia tai WDS-palvelua:** Network Unlockista ei ole hyötyä, eikä sitä tarvitse asentaa.

⚠️ Riskit ja huomioitavaa

- **Ilman Network Unlockia:** Jokainen boottaus vaatii PIN-koodin tai avaimen, mikä voi olla hallinnollisesti raskasta mutta turvallisempaa.
- **Network Unlock käytössä:** Helpottaa hallintaa, mutta vaatii lisäinfrastruktuurin ja toimii vain sisäverkossa. Jos kone viedään verkon ulkopuolelle, PIN-koodi tai avain tarvitaan edelleen.
- **Suositus:** Aloita BitLocker Drive Encryptionilla. Network Unlockia kannattaa harkita vasta, jos hallitset laajaa domain-ypäristöä ja haluat automatisoida boot-prosessin.

Select features

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results

DESTINATION SERVER
Server01.YritysXC.local

Select one or more features to install on the selected server.

Features	Description
<input type="checkbox"/> .NET Framework 3.5 Features	.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.
<input checked="" type="checkbox"/> .NET Framework 4.8 Features (2 of 7 installed)	
<input checked="" type="checkbox"/> Azure Arc Setup (Installed)	
<input type="checkbox"/> Background Intelligent Transfer Service (BITS)	
<input type="checkbox"/> BitLocker Drive Encryption	
<input type="checkbox"/> BitLocker Network Unlock	
<input type="checkbox"/> BranchCache	
<input type="checkbox"/> Client for NFS	
<input type="checkbox"/> Containers	
<input type="checkbox"/> Data Center Bridging	
<input type="checkbox"/> Direct Play	

Select one or more features to install on the selected server.

Features	Description
<input type="checkbox"/> .NET Framework 3.5 Features	
<input checked="" type="checkbox"/> .NET Framework 4.8 Features (2 of 7 installed)	
<input checked="" type="checkbox"/> Azure Arc Setup (Installed)	
<input type="checkbox"/> Background Intelligent Transfer Service (BITS)	
<input checked="" type="checkbox"/> BitLocker Drive Encryption	BitLocker Drive Encryption helps to protect data on lost, stolen, or inappropriately decommissioned computers by encrypting the entire volume and checking the integrity of early boot components. Data is only decrypted if those components are successfully verified and the encrypted drive is located in the original computer. Integrity checking requires a compatible Trusted Platform Module (TPM).
<input type="checkbox"/> BitLocker Network Unlock	
<input type="checkbox"/> BranchCache	
<input type="checkbox"/> Client for NFS	
<input type="checkbox"/> Containers	
<input type="checkbox"/> Data Center Bridging	
<input type="checkbox"/> Direct Play	
<input checked="" type="checkbox"/> Enhanced Storage	
<input type="checkbox"/> Failover Clustering	

Confirm installation selections

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results

DESTINATION SERVER
Server01.YritysXC.local

To install the following roles, role services, or features on selected server, click Install.

Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

BitLocker Drive Encryption
Enhanced Storage
Remote Server Administration Tools
Feature Administration Tools
BitLocker Drive Encryption Administration Utilities
BitLocker Recovery Password
BitLocker Drive Encrypt

If a restart is required, this server restarts automatically, without additional notifications. Do you want to allow automatic restarts?

Yes No

Export configuration settings
Specify an alternate source path

< Previous Next >

Installation progress

DESTINATION SERVER
Server01.YritysXC.local

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results

View installation progress

Starting installation

BitLocker Drive Encryption
Enhanced Storage
Remote Server Administration Tools
 Feature Administration Tools
 BitLocker Drive Encryption Administration Utilities
 BitLocker Recovery Password Viewer
 BitLocker Drive Encryption Tools

Export configuration settings

< Previous Next > Install Cancel

Installation progress

DESTINATION SERVER
Server01.YritysXC.local

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results

View installation progress

Feature installation

Installation started on Server01.YritysXC.local

BitLocker Drive Encryption
Enhanced Storage
Remote Server Administration Tools
 Feature Administration Tools
 BitLocker Drive Encryption Administration Utilities
 BitLocker Recovery Password Viewer
 BitLocker Drive Encryption Tools

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

< Previous Next > Close Cancel

Latauksessa saattaa mennä vähä aikaan, mutta odotellaan ja avaa **AD Users and computers**

Installation progress

DESTINATION SERVER
Server01.YritysXC.local

Results

View installation progress

i Feature installation

Installation succeeded on Server01.YritysXC.local.

BitLocker Drive Encryption
Enhanced Storage
Remote Server Administration Tools
Feature Administration Tools
 BitLocker Drive Encryption Administration Utilities
 BitLocker Recovery Password Viewer
 BitLocker Drive Encryption Tools

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

[Export configuration settings](#)

[< Previous](#) [Next >](#) [Close](#) [Cancel](#)

AD Users and computers

- Tämä on aikaisempi kone (vm2) ja yleinen kone esim. Just EU alueella vaikkapa yksikkönä/alueena ja kaksois klikkauksena näkee ponnahdus ja ilmoituksena "Bitlocker recovery" polku.

Active Directory Users and Computers ja katsottu koneen (vm2) objekti, siellä näkyvä BitLocker Recovery -polku ja sen alla oleva BitLocker Recovery Passwords -ikkuna liittyy siihen, että BitLocker voi tallentaa palautusavaimet (recovery keys) Active Directoryyn.

Mitä BitLocker Recovery Passwords tarkoittaa?

- **Recovery Password = palautusavain** Kun BitLocker salaa levyn, se luo ns. palautusavaimen (48-numeroinen koodi). Tämä on varmuuskeino, jolla levy voidaan avata, jos TPM, PIN tai muu avausmenetelmä ei toimi.
- **Tallennus AD:hen** Jos Group Policy on määritetty niin, että BitLocker-tietoturva-avaimet tallennetaan Active Directoryyn, ne näkyvät koneen objektiin alla ADUC:ssa.
- **BitLocker Recovery Passwords -ikkuna** näyttää kaikki tallennetut palautusavaimet, jotka liittyvät kyseiseen koneeseen. Jokaisella avaimella on GUID-tunniste ja itse 48-numeroinen koodi.

Käyttötarkoitus

- **Adminin näkökulmasta:** Jos käyttäjä tai palvelin ei enää pääse käynnistymään normaalista (esim. TPM-ongelma, PIN unohtunut, laite siirretty toiseen ympäristöön), admin voi hakea palautusavaimen AD:stä ja antaa sen käyttäjälle.
- **Käyttäjän näkökulmasta:** Palautusavainta syötetään BitLocker-käynnistyksen yhteydessä, kun normaali avaus ei onnistuu.
- **Organisaation näkökulmasta:** Tämä on keskeinen osa hallittua BitLocker-ympäristöä, jotta data ei jää ikuisesti lukkoon, jos avausmekanismi epäonnistuu.

Tarvitsetko tämän?

- **Kyllä, ehdottomasti** jos käytät BitLockeria domain-ympäristössä. Recovery-avainten tallennus AD:hen on paras käytäntö, koska se varmistaa, että avaimet eivät katoa.
- **Jos testaat labressa:** Tämä on lähiinä varmistus. Voit halutessasi katsoa, että avaimet tallentuvat oikein, mutta et välttämättä tarvitse niitä pääivittäisessä käytössä – ne ovat häitävara.

BitLocker Recovery Passwords -ikkuna näyttää ne varmuusavaimet, joilla voit avata salatun levyn, jos normaali avaus ei onnistuu. Ne tallentuvat AD:hen juuri siksi, että admin voi palauttaa koneen käyttöön ongelmatilanteessa. Tämä (ylempi kuva) on ensimmäinen näkymä, josta ei olla konfiguroitu bitlockeriä vielä.

Seuraavaksi avaa tämä (alempi kuva)

- Kun **Active Directory Users and Computers** -konsolissa kaksoisklikkaat koneen objekti ja valitset **Find BitLocker Recovery Password**, avautuva ikkuna on **hakutykälu**, jolla voit etsiä ja palauttaa BitLocker-palautusavaimen AD:stä.

🔍 Find BitLocker Recovery Password -ikkunan tarkoitus

- Hakutoiminto:** Sen avulla voit etsiä BitLocker-palautusavaimia Active Directorysta.
- Hakukriteerit:** Voit hakea avaimia esimerkiksi:
 - Recovery Key ID** (GUID, joka näkyy BitLocker-käynnistyksen yhteydessä, kun kone pyytää avainta).
 - Computer name** (jos tiedät minkä koneen avainta etsit).
- Tulokset:** Kun hakuehto täsmää, ikkuna näyttää sen koneen tallennetut palautusavaimet (48-numeroinen koodi), joita voidaan käyttää levyn avaamiseen.

🛠️ Käyttötilanne

- Kun kone ei käynnisty normaalisti:** Käyttäjä näkee ruudulla viestin, jossa pyydetään BitLocker Recovery Keytä. Samalla näytetään **Key ID**.
- Admin hakee AD:stä:** Admin avaa ADUC:n, valitsee *Find BitLocker Recovery Password*, syöttää Key ID:n, ja saa esiin oikean 48-numeron palautusavaimen.
- Avain annetaan käyttäjälle:** Käyttäjä syöttää sen koneelle, jolloin levy avautuu ja käyttö jatkuu normaalista.

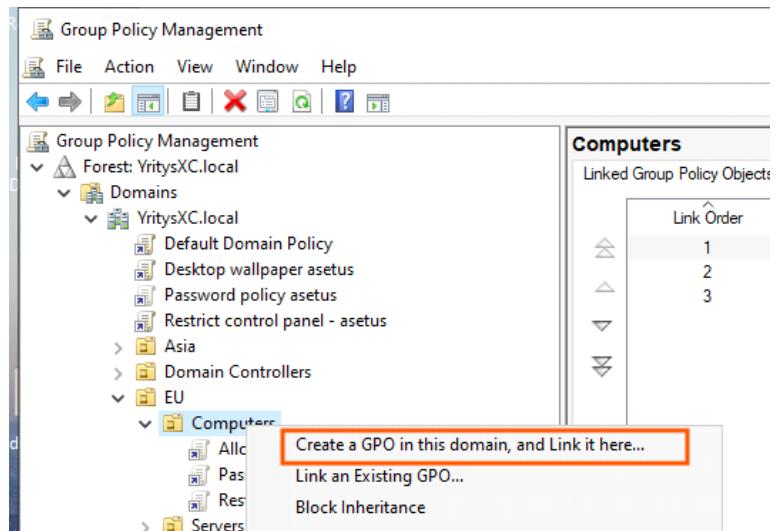
👑 Miksi tämä on tärkeää?

- Turvallisuus:** Recovery-avaimet varmistavat, ettei data jää ikuisesti lukkoon, jos TPM/PIN/USB-avaus epäonnistuu.
- Hallinta:** AD-tallennus ja hakutoiminto tekevät avainten hallinnasta keskitettyä ja auditointavaa.
- Best practice:** Organisaatioissa tämä on olennainen osa BitLocker-hallintaa – ilman tätä admin joutuisi etsimään avaimia manuaalisesti käyttäjiltä.

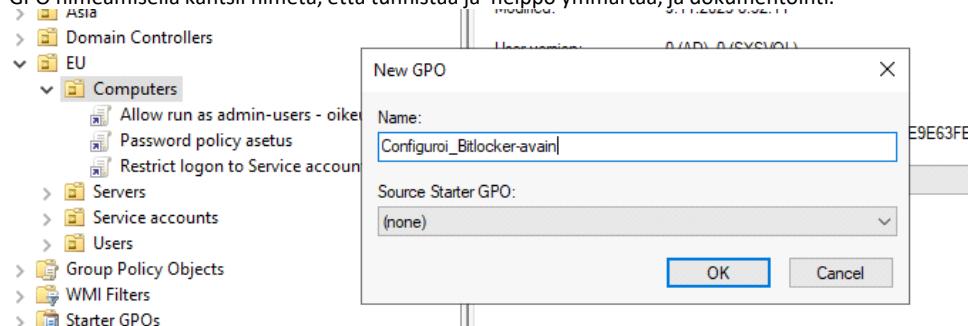
Find BitLocker Recovery Password -ikkuna on hakutykälu, jolla admin voi etsiä ja palauttaa BitLocker-palautusavaimen AD:stä esimerkiksi Key ID:n perusteella.

Seuraavaksi avataan GPO policy management

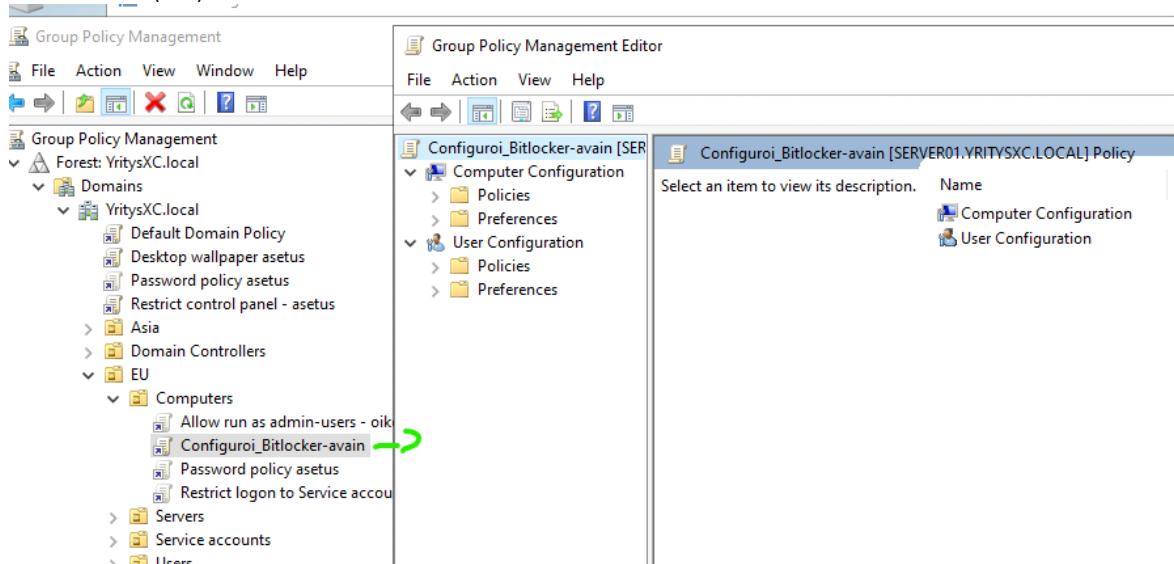
- Avataan se "ainoa" kone tässä harjotuksen polussa missä se sijaitseekaan (**EU/Computers**)
- Siinä luodaan uusi GPO sääntö
 - o **MUISTUTUS (SULJE TARVITTAESSA (DISABLE) MUITA GPO SÄÄNTÖJÄ JOS NIITÄ EI KÄYTETÄ)** ettei tule ristiriittoja ja useiden GPO pelisääntöjen kanssa.



GPO nimeämisen kautta on helppo tunnistaa ja dokumentoida.



Avaa siitä vaan (edit) hiiren kaksoisklikkauksesta



Seuraavaksi tällaiseen polkuun:

- Computer configuration >> policies >> administrative templates : policy definition >> windows components >> BitLocker drive encryption

Group Policy Management Editor

File Action View Help

Configruoi_Bitlocker-avain [SERVER01.YRITYSX.C.LOC]

Computer Configuration Policies Administrative Templates: Policy definition Control Panel Network Printers Server Start Menu and Taskbar System Windows Components ActiveX Installer Service Add features to Windows 10 App Package Deployment App Privacy App runtime Application Compatibility AutoPlay Policies Biometrics BitLocker Drive Encryption Fixed Data Drives Operating System Drives Removable Data Drives Camera

BitLocker Drive Encryption

Select an item to view its description.

Setting	State	Comment
Fixed Data Drives	Not configured	No
Operating System Drives	Not configured	No
Removable Data Drives	Not configured	No
Store BitLocker recovery information in Active Directory Do...	Not configured	No
Choose default folder for recovery password	Not configured	No
Choose how users can recover BitLocker-protected drives (...)	Not configured	No
Disable new DMA devices when this computer is locked	Not configured	No
Choose drive encryption method and cipher strength (Wind...	Not configured	No
Choose drive encryption method and cipher strength (Wind...	Not configured	No
Provide the unique identifiers for your organization	Not configured	No
Prevent memory overwrite on restart	Not configured	No
Validate smart card certificate usage rule compliance	Not configured	No

Valitaan tämä ensimmäinen

BitLocker Drive Encryption

Store BitLocker recovery information in Active Directory

Domain Services (Windows Server 2008 and Windows Vista)

Edit policy setting

Requirements: Windows Server 2008 and Windows Vista

Setting	State	Comment
Fixed Data Drives	Not configured	No
Operating System Drives	Not configured	No
Removable Data Drives	Not configured	No
Store BitLocker recovery information in Active Directory Do...	Not configured	No
Choose default folder for recovery password	Not configured	No
Choose how users can recover BitLocker-protected drives (...)	Not configured	No
Disable new DMA devices when this computer is locked	Not configured	No
Choose drive encryption method and cipher strength (Wind...	Not configured	No

Asettaan "enabled" ja toiv ruksi päälle ja valitaan "recovery passwords and key packages"

- Apply ja OK

Store BitLocker recovery information in Active Directory Domain Services (Windows Server 2008 ...)

Store BitLocker recovery information in Active Directory Domain Services (Windows Server 2008 and Windows Vista)

Previous Setting Next Setting

Comment: Enabled

Supported on: Windows Server 2008 and Windows Vista

Options:

Require BitLocker backup to AD DS

If selected, cannot turn on BitLocker if backup fails (recommended default).

If not selected, can turn on BitLocker even if backup fails. Backup is not automatically retried.

Select BitLocker recovery information to store:

Recovery passwords and key packages

A recovery password is a 48-digit number that unlocks access to a BitLocker-protected drive.

A key package contains a drive's BitLocker encryption key secured by one or more recovery passwords

This policy setting allows you to manage the Active Directory Domain Services (AD DS) backup of BitLocker Drive Encryption recovery information. This provides an administrative method of recovering data encrypted by BitLocker to prevent data loss due to lack of key information. This policy setting is only applicable to computers running Windows Server 2008 or Windows Vista.

If you enable this policy setting, BitLocker recovery information is automatically and silently backed up to AD DS when BitLocker is turned on for a computer. This policy setting is applied when you turn on BitLocker.

Note: You might need to set up appropriate schema extensions and access control settings on the domain before AD DS backup can succeed. More information about setting up AD DS backup for BitLocker is available on Microsoft TechNet.

BitLocker recovery information includes the recovery password and some unique identifier data. You can also include a package that contains a BitLocker-protected drive's encryption key. This

OK Cancel Apply

Se muuttui kuitenkin

BitLocker Drive Encryption		Setting	State	Comment
Store BitLocker recovery information in Active Directory	Setting			
Domain Services (Windows Server 2008 and Windows Vista)	<input type="checkbox"/> Fixed Data Drives <input type="checkbox"/> Operating System Drives <input type="checkbox"/> Removable Data Drives			
Edit policy setting	Store BitLocker recovery information in Active Directory Do...	Enabled	No	
Requirements:				
Windows Server 2008 and	<input type="checkbox"/> Choose default folder for recovery password <input type="checkbox"/> Choose how users can recover BitLocker-protected drives (...) <input type="checkbox"/> Disable new DMA devices when this computer is locked	Not configured Not configured Not configured	No No No	

Seuraavaksi mennään sama alikansioon (operating system drives)

Valitaan: "choose how bitlocker-protected operating system drives can be recovered"

The screenshot shows the Group Policy Management Editor. On the left, under 'Administrative Templates: Policy definitions', there is a tree view with various policy categories like Control Panel, Network, System, and Windows Components. Under Windows Components, 'BitLocker Drive Encryption' is expanded, and 'Operating System Drives' is selected. This selection is highlighted in grey. On the right, the details for this policy are shown in a table format.

Setting	State	Comment
<input type="checkbox"/> Allow network unlock at startup	Not configured	No
<input type="checkbox"/> Allow Secure Boot for integrity validation	Not configured	No
<input type="checkbox"/> Require additional authentication at startup	Not configured	No
<input type="checkbox"/> Require additional authentication at startup (Windows Serve...	Not configured	No
<input type="checkbox"/> Disallow standard users from changing the PIN or password	Not configured	No
<input type="checkbox"/> Allow devices compliant with InstantGo or HSTI to opt out ...	Not configured	No
<input type="checkbox"/> Enable use of BitLocker authentication requiring preboot ke...	Not configured	No
<input type="checkbox"/> Allow enhanced PINs for startup	Not configured	No
<input type="checkbox"/> Configure minimum PIN length for startup	Not configured	No
<input type="checkbox"/> Configure use of hardware-based encryption for operating s...	Not configured	No
<input type="checkbox"/> Enforce drive encryption type on operating system drives	Not configured	No
<input type="checkbox"/> Configure use of passwords for operating system drives	Not configured	No
<input checked="" type="checkbox"/> Choose how BitLocker-protected operating system drives ca...	Not configured	No
<input type="checkbox"/> Configure TPM platform validation profile for BIOS-based fir...	Not configured	No
<input type="checkbox"/> Configure TPM platform validation profile (Windows Vista, ...	Not configured	No
<input type="checkbox"/> Configure TPM platform validation profile for native UEFI fir...	Not configured	No
<input type="checkbox"/> Configure pre-boot recovery message and URL	Not configured	No
<input type="checkbox"/> Reset platform validation data after BitLocker recovery	Not configured	No
<input type="checkbox"/> Use enhanced Boot Configuration Data validation profile	Not configured	No

Valita "enabled" - niin sen jälkeen se automaattisesti täyttää oletus asetukset kuntoon, josta on:

- Allow data recovery agent (Päällä)
- Allow 48-digit recovery password
- Allow 256-bit recovery key
- Save bitlocker recovery information to AD DS for operting system drives
- Store recovery passwords and key packages

Sitten: apply ja OK

The screenshot shows the 'Choose how BitLocker-protected operating system drives can be recovered' dialog box. It has two tabs: 'Previous Setting' and 'Next Setting'. The 'Enabled' radio button is selected. The 'Supported on:' dropdown shows 'At least Windows Server 2008 R2 or Windows 7'. The 'Options:' section contains several checkboxes:

- Allow data recovery agent
- Configure user storage of BitLocker recovery information:
 - Allow 48-digit recovery password
 - Allow 256-bit recovery key
 - Omit recovery options from the BitLocker setup wizard
 - Save BitLocker recovery information to AD DS for operating system drives
- Configure storage of BitLocker recovery information to AD DS:
 - Store recovery passwords and key packages
 - Do not enable BitLocker until recovery information is stored to AD DS for operating system drives

 The 'Help:' section provides detailed descriptions for each option, explaining their purpose and how they interact with BitLocker.

Jostain syystä videon mukaan laittoi ton viimeisimmän ruksin päälle eli:

- "do not enable bitlocker until recovery information is stored to AD DS for operating system drives."
- Apply ja OK

Setting	Value	Status
Enforce drive encryption type on operating system drives	Not configured	No
Configure use of passwords for operating system drives	Not configured	No
Choose how BitLocker-protected operating system drives ca...	Enabled	No
Configure TPM platform validation profile for BIOS-based fir...	Not configured	No
Configure TPM platform validation profile (Windows Vista, ...)	Not configured	No

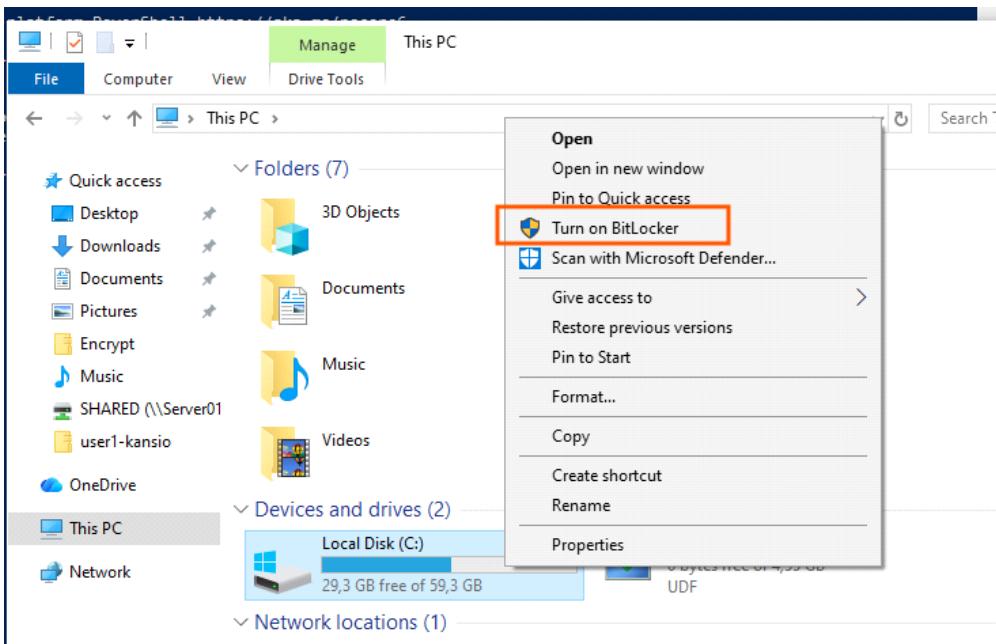
Seuraavaksi päivitä powershell kautta, että aktivoidaan tämä bitlocker käyntiin eli powershell \$gpupdate /force

Seuraavaksi avataan VM2 (toinen työasema)

Avaa ihan cmd/powershell - ja ihan normi päivitystä (\$upgadte force), että se saa DNS yhteydestä windows serveriltä päivityksensä

Seuraavaksi avataan ihan "this pc" eli oma kansio , ja hiiren klikkauksella nähdään voidaan seuraavaksi aktivoida bitlockeria.

- Välissä tuli kysyy jotakin admin tunnusta että sallitaan tehdä muutosta



Jaahas jotakin error

← BitLocker Drive Encryption (C:)

Starting BitLocker

- X This device can't use a Trusted Platform Module. Your administrator must set the "Allow BitLocker without a compatible TPM" option in the "Require additional authentication at startup" policy for OS volumes.

BitLocker ei voi käyttää TPM:ää (Trusted Platform Module), koska joko:

1. TPM ei ole käytettävissä (esim. virtuaalikoneessa),
2. TPM ei ole yhteensopiva,
3. TPM on pois päältä BIOS/UEFI:ssä,
4. Tai GPO-asetusta ei ole vielä otettu käyttöön oikein.

🔧 Mitä virheilmoitus tarkoittaa?

"This device can't use a Trusted Platform Module. Your administrator must set the 'Allow BitLocker without a compatible TPM' option..." Tämä tarkoittaa, että BitLocker yrittää käyttää TPM:ää, mutta ei löydä sitä. Jotta voit käyttää BitLockeria **ilman TPM:ää**, sinun täytyy sallia se ryhmäkäytännöissä (GPO).

☑ Korjausvaiheet: BitLocker ilman TPM:ää

1. Aava Group Policy Editor (gpedit.msc)

- Mene kohtaan: Computer Configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption > Operating System Drives

2. Etsi ja aktivoi:

- "Require additional authentication at startup"
- Aseta se Enabled
- Vailitse: "Allow BitLocker without a compatible TPM (requires a password or a startup key on a USB flash drive)"

3. Käynnistä kone uudelleen (tai suorita gpupdate /force)

4. Käynnistä BitLocker uudelleen

- Nyt BitLocker antaa sinun käyttää **USB-avainta tai salasanaa** käynnistyksen yhteydessä, vaikka TPM ei ole käytössä.

Oma toiminta - jatkuu - koskien ylempien ohjeen mukaan - START HERE

Group Policy Management Editor

File Action View Help

Configuroi_Bitlocker-avain [SERVER01.YRITYSXC.LOC]

Operating System Drives

Require additional authentication at startup

[Edit policy setting](#)

Requirements: At least Windows Server 2008 R2 or Windows 7

Description: This policy setting allows you to configure whether BitLocker requires additional authentication each time the computer starts and whether you are using BitLocker with or without a Trusted Platform Module (TPM). This policy setting is applied when you turn on BitLocker.

Note: Only one of the additional authentication options can be required at startup, otherwise a policy error occurs.

If you want to use BitLocker on a computer without a TPM, select the "Allow BitLocker without a compatible TPM" check box. In this mode either a password or a

Setting	State	Comment
Allow network unlock at startup	Not configured	No
Allow Secure Boot for integrity validation	Not configured	No
Require additional authentication at startup	Not configured	No
Require additional authentication at startup (Windows Serve...	Not configured	No
Disallow standard users from changing the PIN or password	Not configured	No
Allow devices compliant with InstantGo or HSTI to opt out o...	Not configured	No
Enable use of BitLocker authentication requiring preboot ke...	Not configured	No
Allow enhanced PINs for startup	Not configured	No
Configure minimum PIN length for startup	Not configured	No
Configure use of hardware-based encryption for operating s...	Not configured	No
Enforce drive encryption type on operating system drives	Not configured	No
Configure use of passwords for operating system drives	Not configured	No
Choose how BitLocker-protected operating system drives ca...	Enabled	No
Configure TPM platform validation profile for BIOS-based fir...	Not configured	No
Configure TPM platform validation profile (Windows Vista, ...	Not configured	No
Configure TPM platform validation profile for native UEFI fir...	Not configured	No
Configure pre-boot recovery message and URL	Not configured	No
Reset platform validation data after BitLocker recovery	Not configured	No
Use enhanced Boot Configuration Data validation profile	Not configured	No

Require additional authentication at startup

[Previous Setting](#) [Next Setting](#)

Enabled Comment:

Disabled Supported on: At least Windows Server 2008 R2 or Windows 7

Options:

Allow BitLocker without a compatible TPM (requires a password or a startup key on a USB flash drive)

Settings for computers with a TPM:

Configure TPM startup: Allow TPM

Configure TPM startup PIN: Allow startup PIN with TPM

Configure TPM startup key: Allow startup key with TPM

Configure TPM startup key and PIN: Allow startup key and PIN with TPM

Help:

This policy setting allows you to configure whether BitLocker requires additional authentication each time the computer starts and whether you are using BitLocker with or without a Trusted Platform Module (TPM). This policy setting is applied when you turn on BitLocker.

Note: Only one of the additional authentication options can be required at startup, otherwise a policy error occurs.

If you want to use BitLocker on a computer without a TPM, select the "Allow BitLocker without a compatible TPM" check box. In this mode either a password or a USB drive is required for startup. When using a startup key, the key information used to encrypt the drive is stored on the USB drive, creating a USB key. When the USB key is inserted the access to the drive is authenticated and the drive is accessible. If the USB key is lost or unavailable or if you have forgotten the password then you will need to use one of the BitLocker recovery options to access the drive.

On a computer with a compatible TPM, four types of authentication methods can be used at startup to provide added protection for encrypted data. When the computer starts, it can use only the TPM for authentication, or it can also require insertion of a USB flash drive containing a startup key, the entry of a 6-digit to 20-digit personal identification number (PIN), or both.

[OK](#) [Cancel](#) [Apply](#)

Tähän väliin vaan powershell komennolla päivitystä ja sama päätee vm2:ssa uudelleen käynnistystä, että powershell komennolla suorita päivitystä

Takaisin VM2:lle ja testataan, että toimii (KYLLÄ)

- Valitaan alempi vaihtoehto eli syötettää salasana jonka muistettaan esim. "Salasana123"

Choose how to unlock your drive at startup

 Some settings are managed by your system administrator.

To help keep your data more secure, you can have BitLocker prompt you to enter a password or insert a USB flash drive each time you start your PC.

→ Insert a USB flash drive

→ Enter a password

Kun BitLocker pyytää sinua **tallentamaan Recovery Keyn**, se tarjoaa kolme vaihtoehtoa. Kaikki tallentavat saman 48-numeroisen palautusavaimen, mutta eri muotoon ja eri paikkaan.

BitLocker Recovery Key -tallennusvaihtoehdot

Vaihtoehto	Kuvaus	Hyödyt	Riskit
Save to USB flash drive	Tallentaa palautusavaimen suoraan USB-driveiksi .txt-tiedostona	Helppo käyttää käynnistysessä, jos kone pyytää avainta	Jos USB hukkuu tai vioittuu, avain menetetään
Save to a file	Tallentaa .txt-tiedoston paikallisesti tai verkkoasemalle	Voit hallita sijaintia itse (esim. verkko, pilvi, AD)	Jos tiedosto ei ole suojattu, voi joutua väärin käsii
Print the recovery key	Tulostaa avaimen paperille	Fyysisen varmuuskopio, ei riippuvainen laitteista	Paperi voi kadota, joutua väärin käsii tai unohtua

- **Testilabroissa tai yksittäisissä koneissa:** → Save to a file tai USB flash drive riittää.
- **Organisaatioympäristössä:** → Recovery key kannattaa tallentaa Active Directoryyn automaattisesti GPO:n kautta, jolloin admin voi hakea sen tarvittaessa.
- **Lisävarmuus:** → Voit tallentaa useampaan paikkaan (esim. USB + tuloste), mutta varmista että ne ovat **turvallisesti säilytettyä**.

How do you want to back up your recovery key?

A recovery key can be used to access your files and folders if you're having problems unlocking your PC. It's a good idea to have more than one and keep each in a safe place other than your PC.

→ Save to a USB flash drive

→ Save to a file

→ Print the recovery key

Videon mukaan suoraan (NEXT) ettei valittu noista kolmesta vaihtoehdosta..

- BitLocker ei anna sinun jatkaa salauksen käyttöönnottoa.
- **Recovery key on pakollinen:** BitLocker vaatii aina, että palautusavain tallennetaan johonkin ennen kuin salaus alkaa.
- **Turvallisuussyyistä:** Jos käynnistys epäonnistuu (TPM-ongelma, PIN unohtuu, levy siirretään toiseen koneeseen), ilman recovery keytä et voisikaan avata levyä.
- **Estää datan menetyksen:** Microsoft on tehnyt tästä pakollisen, jotta kukaan ei vahingossa luki se itseään ulos pysyvästi.

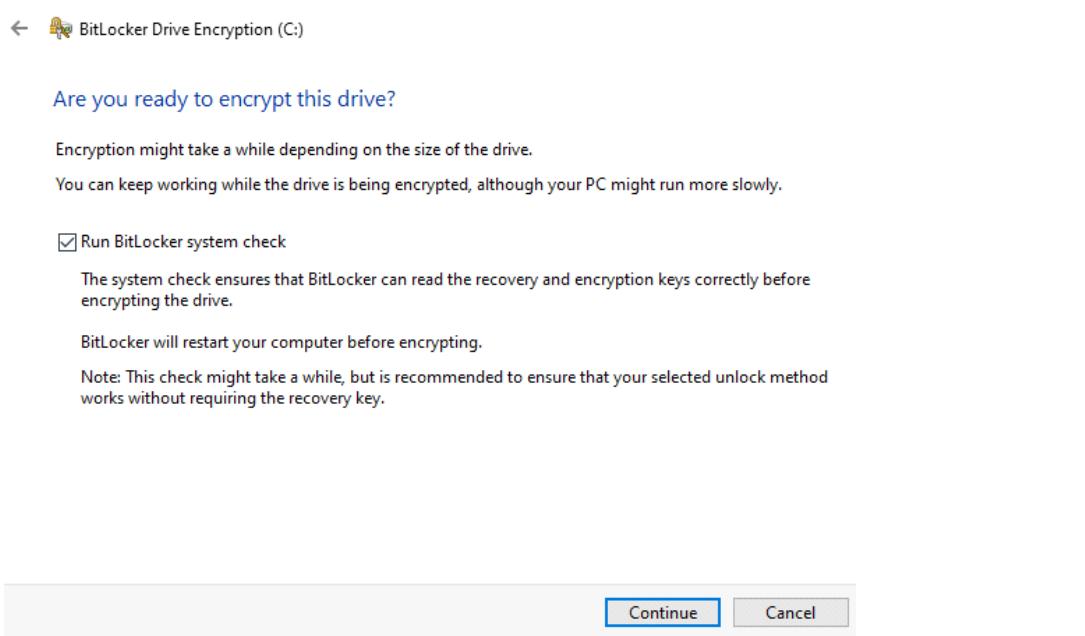
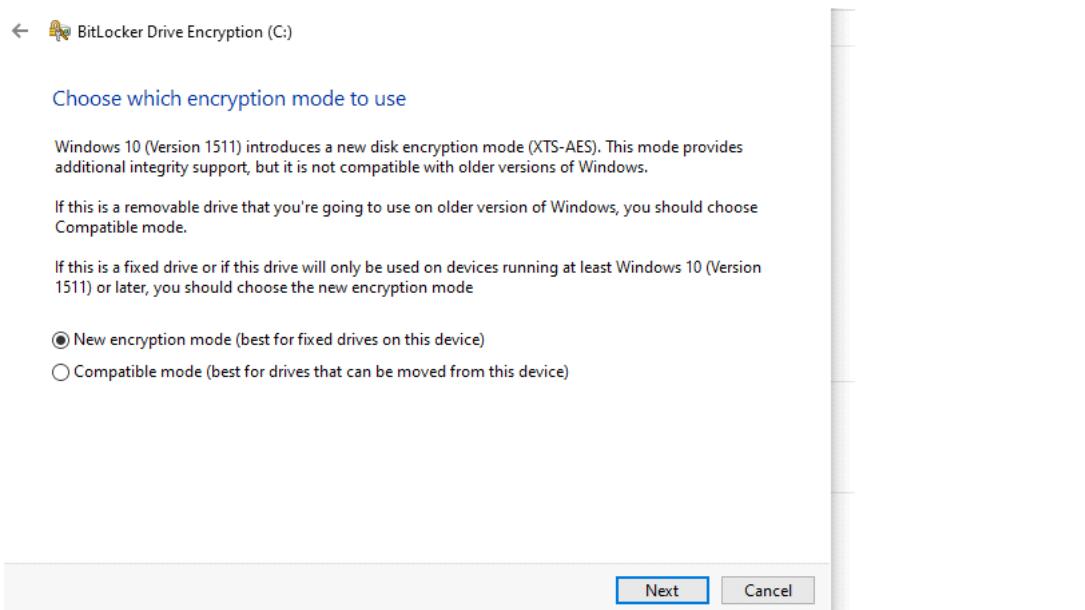
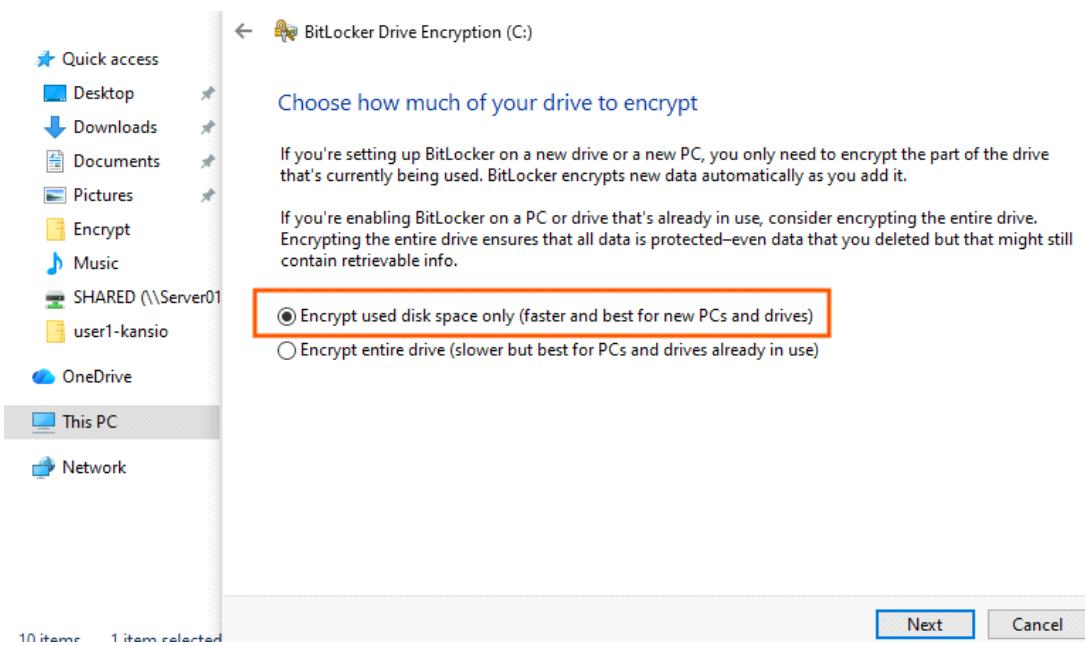
Käytännössä

- Jos et valitse mitään → BitLocker pysäyttää prosessin ja pyytää sinua tallentamaan avaimen.
- Vasta kun avain on tallennettu (USB, tiedosto, tuloste, tai AD/GPO), voit jatkaa ja aloittaa salauksen.

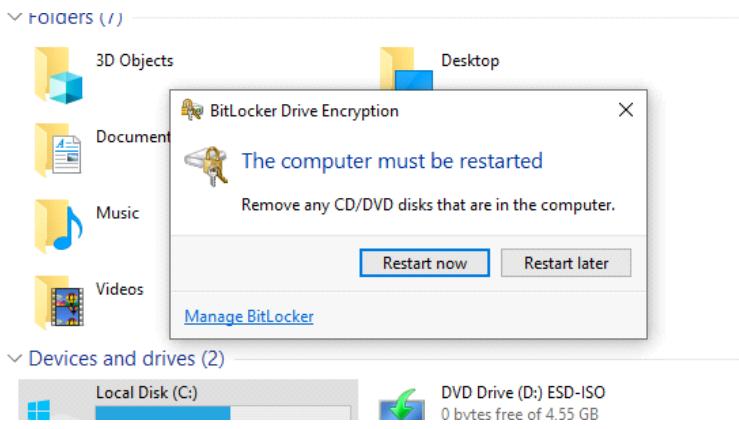
Vinkki

- Labratestissä riittää, että tallennat avaimen **tiedostoon** (esim. D:\ tai verkkoasema).
- Tuotantoymäristössä kannattaa käyttää **AD/GPO-tallennusta**, jolloin avaimet menevät automaattisesti domainiin.

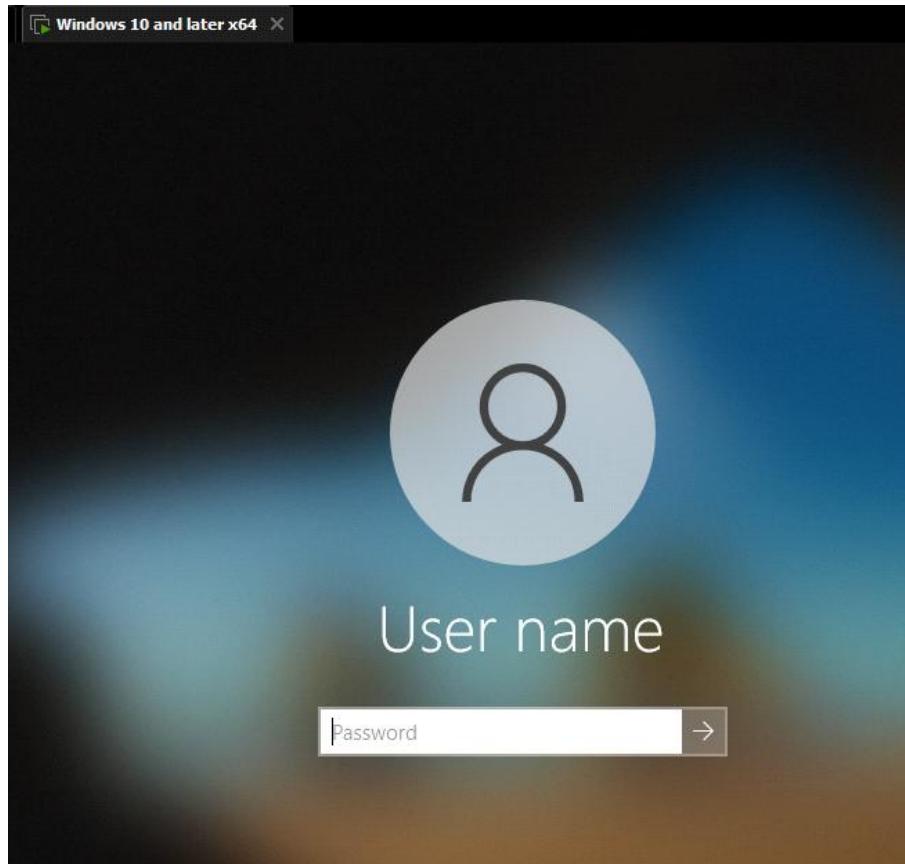
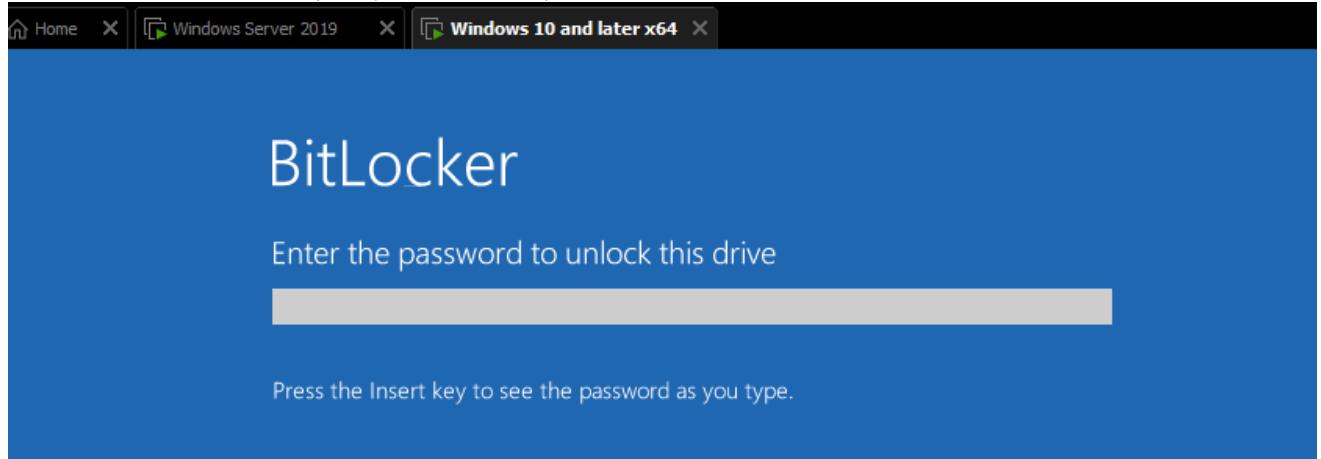
Oletuksena ensimmäinen vaihtoehto



Sitten se pyytää buuttauksen niin buuttamaan vaan.
Jostakin syystä ei anna buuttaa, että antoi vaan error ja suoraan käyttöliittymän kautta..



VM2 jouduin käynnistää käsin.. Ja apua
Onneksi antoi kaksi vaihtoehtoa, joko syötä avain tai escape (ESC)



Pieni vilkaisu VM1 windows serveristä

Vilkaisin VM1 windows serveristä, että huomattua ja päivitettyä että on tullut pienä muutosta ja vau

Active Directory Users and Computers

File Action View Help

Active Directory Users and Computers [1]

- Active Directory Users and Computers
- Saved Queries
- YritysXC.local
 - Asia
 - Builtin
 - Computers
 - Domain Controllers
 - EU
 - Computers
 - Servers
 - Service accounts
 - Users
 - ForeignSecurityPrincipals
 - Keys
 - LostAndFound
 - Managed Service Accounts
 - Program Data
 - System
 - Users
 - NTDS Quotas
 - TPM Devices

DESKTOP-S8U072N Properties

LAPS	Location	Managed By	Object	Security
General	Operating System	Member Of	Delegation	Password Replication
Dial-in		Attribute Editor		BitLocker Recovery

BitLocker Recovery Passwords:

Date Added	Password ID
2025-12-09 17:43	D

Details:

Recovery Password:
591734-
065527-

Computer: DESKTOP-... .YritysXC.local
Date: 2025-12-09 17:43:12 +0200
Password ID: D F

OK Cancel Apply Help

Nyt takaisin vm2:lle ja testataan uudestaan

This PC

File Computer View Drive Tools

This PC

Folders (7)

- Quick access
- Desktop
- Downloads
- Documents
- Pictures
- Encrypt
- Music
- SHARED (\Server01)
- user1-kansio
- OneDrive
- This PC
- Network

Devices and drives (2)

- Local Disk (C:)

Network locations (1)

Open

- Open in new window
- Pin to Quick access
- Turn on BitLocker**
- Scan with Microsoft Defender...
- Give access to
- Restore previous versions
- Pin to Start
- Format...
- Copy
- Create shortcut
- Rename
- Properties

Kokeillaan syötää salasana

← BitLocker Drive Encryption (C:)

Choose how to unlock your drive at startup

i Some settings are managed by your system administrator.

To help keep your data more secure, you can have BitLocker prompt you to enter a password or insert a USB flash drive each time you start your PC.

→ Insert a USB flash drive

→ Enter a password

Syötetty passu ja next

Se tulee kysyy mihin tallennetaan, mutta harjoituksen kannalta suoraan next

← BitLocker Drive Encryption (C:)

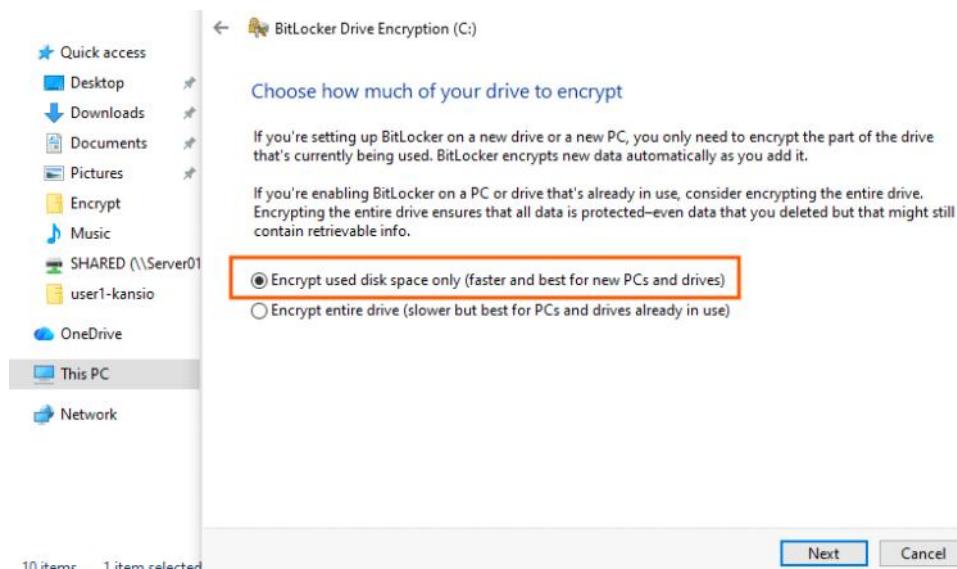
How do you want to back up your recovery key?

A recovery key can be used to access your files and folders if you're having problems unlocking your PC.
It's a good idea to have more than one and keep each in a safe place other than your PC.

→ Save to a USB flash drive

→ Save to a file

→ Print the recovery key



← BitLocker Drive Encryption (C:)

Choose which encryption mode to use

Windows 10 (Version 1511) introduces a new disk encryption mode (XTS-AES). This mode provides additional integrity support, but it is not compatible with older versions of Windows.

If this is a removable drive that you're going to use on older version of Windows, you should choose Compatible mode.

If this is a fixed drive or if this drive will only be used on devices running at least Windows 10 (Version 1511) or later, you should choose the new encryption mode

- New encryption mode (best for fixed drives on this device)
 Compatible mode (best for drives that can be moved from this device)

Next Cancel

Are you ready to encrypt this drive?

Encryption might take a while depending on the size of the drive.

You can keep working while the drive is being encrypted, although your PC might run more slowly.

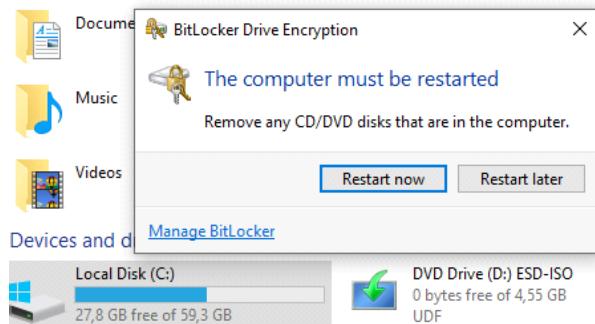
Run BitLocker system check

The system check ensures that BitLocker can read the recovery and encryption keys correctly before encrypting the drive.

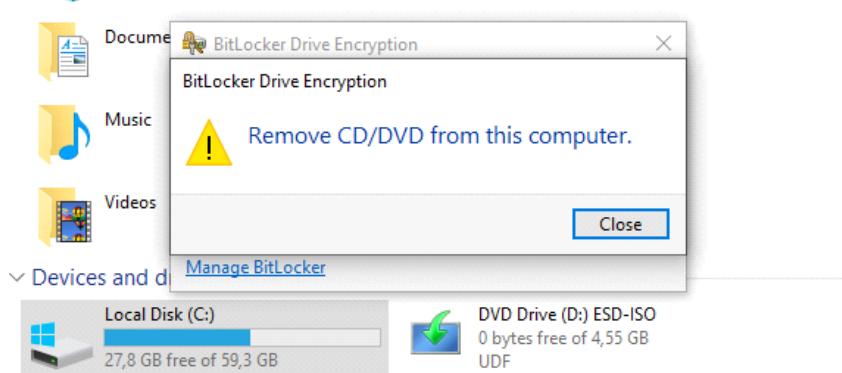
BitLocker will restart your computer before encrypting.

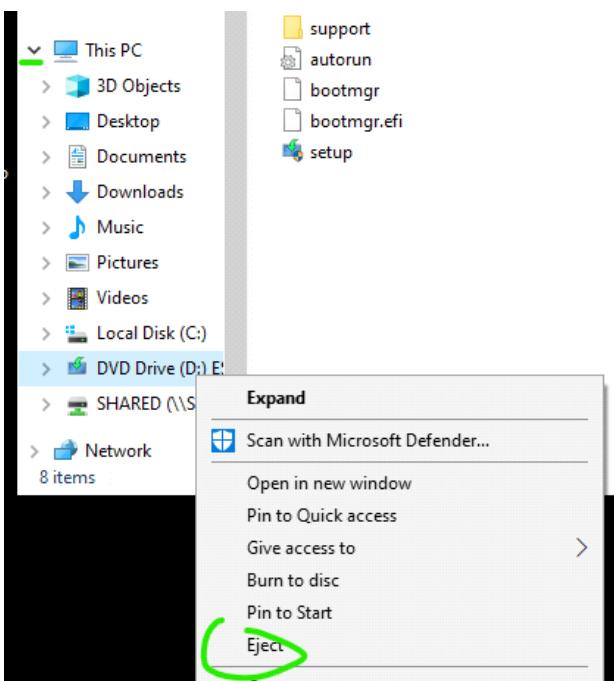
Note: This check might take a while, but is recommended to ensure that your selected unlock method works without requiring the recovery key.

Taas vaattii buuttausta, mutta se ei pitäisi toimia mutta ei buutatta vielä ettei tulla paniikkiin

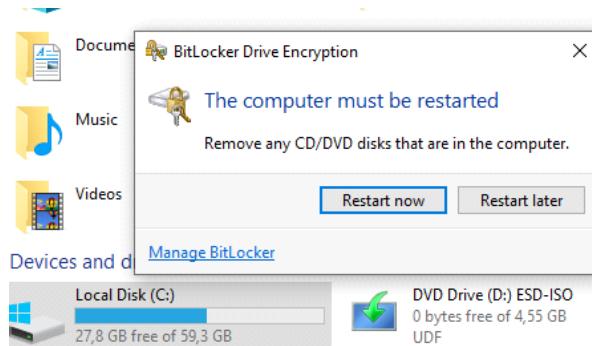


Jos yrittää buuttaa se kysyy näin.. Mennään kikka kolmonen



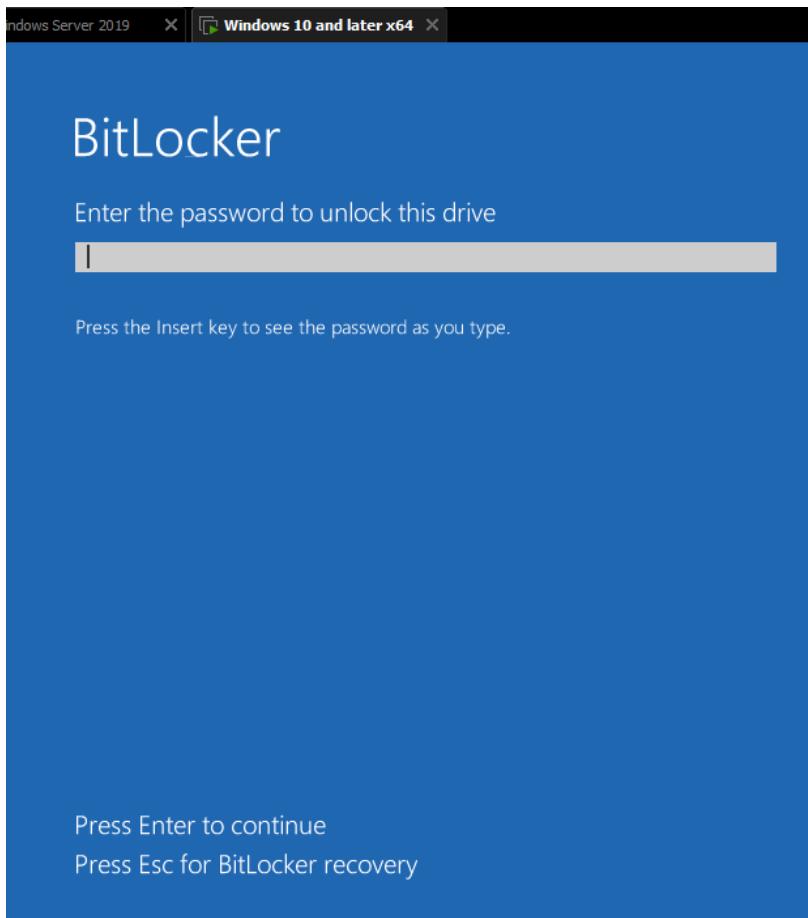


Nyt buuttataan eli normi klikkaa että uudelleen käynnistys



Tästä voi skippata eli esc

- Jos ei reagoi mitään se sulkee jotakin jännästi tämän vm ohjelmansa
- Tätä testastua se onkin se syöttämisen salasana



Hmm outoa



UUSI YRITYS

Kokeillaan jos tallennetaan tämä (save to file)

← BitLocker Drive Encryption (C:)

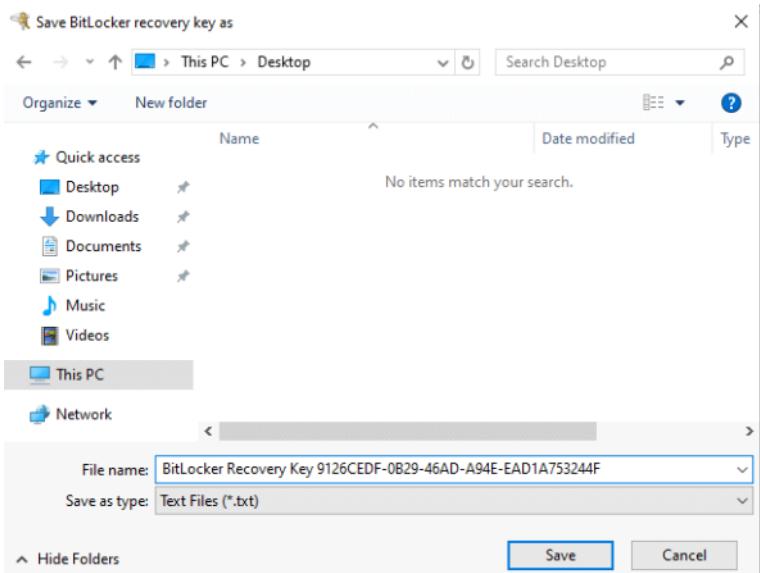
How do you want to back up your recovery key?

A recovery key can be used to access your files and folders if you're having problems unlocking your PC.
It's a good idea to have more than one and keep each in a safe place other than your PC.

→ Save to a USB flash drive

→ Save to a file

→ Print the recovery key



Tästä jotakin syystä ei tykkää tallentaa mihinkään (save file) metodilla - kokeilin ilman sitä tallennusta kuitenkin. Kirjoitin ton Bitlocker recovery key pitkän ID talteen