Lab 16:

Windows BitLocker

Windows Server Security  
 2024-2025

© Daan Pareit, Henk Brouckxon

## Introduction

# Lab concept

In this lab, we’ll investigate BitLocker and how it can be used to protect data on Windows systems. We’ll also investigate how Active Directory Group Policy Objects can be used to impose BitLocker-related corporate data security policies on the Windows client systems in the domain.



# Learning goals

* Implementing BitLocker on a Windows client system
* Backing up BitLocker recovery keys (local / Active Directory)
* Implementing BitLocker policies for enterprise networks (Active Directory Group Policies)

# Practicalities and prerequisites

You’ll need:

* Your Windows VMs as configured during the previous labs
* Make sure your pfSense and Windows VMs (server and client) are running.

## Introduction - prerequisites for BitLocker and AD BitLocker management

### BitLocker hardware prerequisites

Even though it can be omitted, an important hardware prerequisite for BitLocker typically is the availability of a Trusted Platform Module (TPM) that will protect the encryption keys. Because a TPM is also one of the (more controversial) hardware prerequisites for Windows 11, you’ll notice your VM contains such a module.

Now let’s have a look at the properties of our VM’s TPM…

# Step 1 – Trusted platform module

* On your Windows 11 VM, use a PowerShell cmdlet to find out information about the Trusted Platform Module (TPM). What is its manufacturer name? Can you find the TPM specification version?

`Get-TPM` cmdlet.

A screenshot of a computer

Description automatically generated

Manufacturer name – VMW

TPM Specification version – I guess 2.101.0.1

* Start a GUI-based tool to find out more information about the TPM. What is its TPM specification version?

Specification version is 2.0

to launch it: Win+R > tpm.msc

A screenshot of a computer

Description automatically generated

# Step 2 – Add a floppy drive to the virtual machine

When the OS disk is encrypted, BitLocker will ask to save a recovery key to disk. For this, we’ll need another disk (the key file cannot be saved to an encrypted disk), for which we will use a floppy drive. (In real life you’d use something less old fashioned 😉 like a USB thumb drive or something else, but for your VM, this is the easiest way forward and the principles stay the same.)

* Shut down the Windows 11 VM and add a floppy drive in the VM settings (make a new image file called “floppy.flp”, and make sure that the floppy is connected at startup).

A screenshot of a computer

Description automatically generated

* Restart the VM, make sure you can access the floppy drive and format it (use the right-click menu in file explorer). What is the capacity of this disk? Yes, that’s what it was like in the nineties 😉

A screenshot of a computer

Description automatically generated

1.38 MB

### Prerequisites for AD BitLocker management

Active Directory allows us to centrally manage several rules and policies regarding BitLocker for the Windows client systems in a domain. This is done through so-called Group Policy Objects [1] . Therefore, we first need to install the relevant ‘Windows Optional Features’ for remote system administration on our Windows 11 client machine.

# Step 3 – Install RSAT tools for GPM and BitLocker

* Log into your Windows 11 VM with your domain administrator account ‘COMPANY-<firstname>\Administrator’ or ‘Donald’.
* If you’ve done the lab about WSUS already, you would need to have Windows Optional Features to be downloaded onto your WSUS server. This would require a rather large and slow download on your Windows Server VM. Therefore, as a more pragmatic method for this lab setup, temporarily unlink your Windows 11 VM from the WSUS server:
  + in Server Manager via the Group Policy Editor: right click the policy you’ve created with WSUS settings and uncheck 'link enabled'
  + in Server Manager via de WSUS tool: remove your Windows 11 desktop (you might need to set the view to 'any' to see the PC)
  + Reboot your Windows 11 VM and/or execute a 'gpupdate /force'
* Go to the ‘Windows optional features’ settings window (via Settings – System – Optional Features), and install the following features (if not yet installed already):
  + RSAT: Group Policy Management Tools Utilities
  + RSAT: BitLocker Drive Encryption Administration Utilities
* Log into the King server as domain admin ‘Donald’, and install the BitLocker tools on this server by running the following cmdlet:

Install-WindowsFeature BitLocker -IncludeAllSubFeature -IncludeManagementTools

And restart the server.

A screen shot of a computer screen

Description automatically generated

* Back on the Windows 11 VM, open Server Manager and start the “Active Directory Users and Computers” tool. A new ´BitLocker recovery´ tab should be available in the device properties of the Windows 11 machine.

A screenshot of a computer

Description automatically generated

## BitLocker OS Drive Encryption

# Step 4 – Group Policy for recovery key backup

As we´ll see later, Windows creates a recovery key that can be printed or saved to an external disk, and that can be used to unlock the drive when it is in recovery mode (when an event happens that locks the device). Devices that have joined an AD domain can also be configured to automatically back up their recovery keys to the AD server using a group policy. We´ll now do this for the devices in our domain.

* In Server Manager, start the “Group policy management editor” tool, and edit the ‘Default Domain Policy’ GPO (or create a new GPO linked to your OU ‘PCs’).

A screenshot of a computer

Description automatically generated

* In the GPO, go to Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption.
* **Question**: What policy should be enabled to ensure that the BitLocker recovery key for the OS disk is automatically backed up to the AD server for our Win11 client? (Hint: pay attention to what Windows version(s) a policy is supported on, to identify the correct one!)

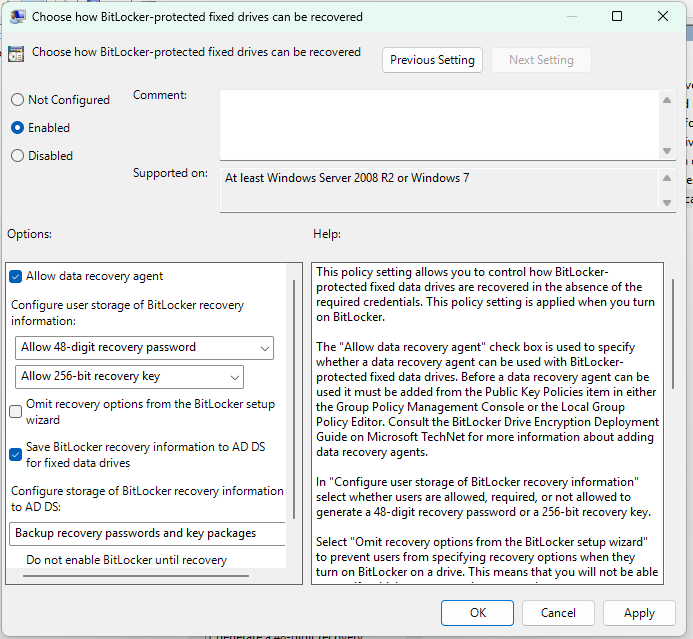
Choose how BitLocker-protected operating system drives can be recovered

This can be found inside Fixed Data Drives section.

A screenshot of a computer screen

Description automatically generated

* Enable this policy using default settings. Notice one of the checkboxes ensures that the intended behavior -saving recovery info into the AD DS- is enforced.



WRONG

The one I need is in Operating System Drives.

A screenshot of a computer

Description automatically generated

* Ensure that the policy is applied to the machine. What command should you use to immediately apply the policy? (Cfr earlier in this lab.)

gpupdate /force

# Step 5 – Apply BitLocker to the OS disk of the Windows 11 system

* On your Windows 11 machine, start file explorer and right-click the OS disk. Turn on BitLocker drive encryption and save the recovery key to the floppy disk.
* Wait until encryption is complete (if this takes a long time, you can already start on the next section, “BitLocker-on-the-go”) and **copy the contents of the recovery file (from the floppy disk) to your physical pc (not the VM)**. Make sure you can read this recovery file, since we may need this information later!

## BitLocker-on-the-go - Removable drive encryption

# Step 6 – Group policy for removable disks

Even though we can apply BitLocker to the operating system and internal data disks, this may not always suffice to protect sensitive data. For example, if the user chooses to make a backup of sensitive data to a USB disk, this disk can be lost or stolen, and in that way the data can be compromised. In high-security environments therefore, we can add the requirement that any USB/removable disk that is used on a computer should also be “BitLocked”.

* Question: What policy (in the group policy management editor) can be enabled to ensure that the user can only write to BitLocked USB disks?   
  **remark: Do NOT enable this policy! It would also make your floppy disk unreadable…**

A screenshot of a computer

Description automatically generated

`Deny write access to removable drives not protected by BitLocker`

## Recovering a lost BitLocker key

Unfortunately, Donald -the user of our Windows 11 machine- has recently lost the floppy disk which contains his BitLocker recovery key. He now asks us if there is a way to recover this key from the system.

# Step 7 – Local key recovery on the Windows 11 device

Since the device’s disk is not locked, Donald can retrieve the recovery key himself on the Windows 11 device. This can be done via the BitLocker GUI, but also through the command line:

* Question: What command should Donald type to recover his key using the manage-BDE command line utility?

**`manage-bde -protectors -get C:`**

* Verify that the obtained recovery key is indeed the same as the one you previously saved on your laptop host after completing the initial encryption.

Yes, it is the same! Just saying for the quiz that it is 48 characters long.

# Step 8 – Remote key recovery on the AD server

If Donald is unable to retrieve the recovery key himself (e.g. when the disk is in recovery mode and the device is locked), we can fortunately also retrieve the key from the AD server.

* Imagine our Win11 PC would be another client PC on which Donald has still access. In Server Manager, go to the ´Active Directory Users and Computers´ tool, and right-click your desktop device name. Select ´Properties´ and go to the ´BitLocker Recovery´ tab. Verify you find the recovery password indeed.
  + Remark: The AD server saves a full history of the BitLocker recovery keys for the machine. Therefore, if BitLocker was disabled and re-enabled previously, multiple recovery keys may be shown for the OS disk. Only the most recent of these keys is typically still active.

A screenshot of a computer

Description automatically generated

* On the AD server itself (without the desktop experience), you can also access the recovery keys via PowerShell cmdlets:

Get-ADObject -Filter {objectclass -eq 'msFVE-RecoveryInformation'} -SearchBase (Get-ADComputer -Filter 'Name -like "Desktop\*"').DistinguishedName -Properties msFVE-RecoveryPassword

A computer screen with white and blue text

Description automatically generated

## Recovering a locked BitLocker disk

There are several events which may trigger BitLocker to lock the OS disk (e.g. moving the disk to another machine or updating the machine firmware). We´ll now simulate what happens in this case, and how the system can be recovered using the recovery password/ floppy disk.

* **Make sure you’ve saved the BitLocker recovery key to your host PC, we’ll need this key to restore your windows 11 to a working state. Without the key, your VM may become unusable!**
* **More importantly, make sure none of the commands are executed on your laptop host, but always on your VM!**

# Step 9 – Disaster strikes – Recovering a BitLocker disk

* To simulate a locking event, run the following command from the command line on your Windows 11 VM (as administrator):

manage-bde -forcerecovery c:

What will this command do?

It looks like it deletes some recovery codes or identifiers, hence it makes the drive to go into recovery mode

* Restart the VM. Does it boot to the Windows login screen?

A screenshot of a computer error

Description automatically generated

It boots into recovery mode.

* Now follow the recovery process, using the recovery key you saved before.

# Step 10 – Back to normal

Because the manage-bde command deleted the BitLocker encryption key from the drive/TPM, it will cause the Windows 11 machine to show the BitLocker recovery screen on every restart. To solve this, we can use another manage-bde command to replace the TPM-based key. Once you are logged in again to the machine, run the following command in a command line terminal with elevated privileges:

manage-bde.exe -protectors -add c: -tpm

Done as well

Alternatively, it’s also possible to completely disable BitLocker and put the disk back in an unencrypted state.

I will disabled it because I am not comfortable with it.

## Resources

|  |  |
| --- | --- |
| [1] | C. Ledoux, T. Clauwaert en H. Brouckxon, Course notes for module "Windows labs", Howest. |
| [2] | Microsoft, „BitLocker Recovery guide,” [Online]. Available: https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-recovery-guide-plan. |
| [3] | Microsoft, „commands by server role,” [Online]. Available: https://docs.microsoft.com/nl-nl/windows-server/administration/windows-commands/commands-by-server-role. |
| [4] | Microsoft, „BitLocker,” [Online]. Available: https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview. |