CapaBitLocker

August 2022

Author

Dan Svendsen

Technical Program Manager

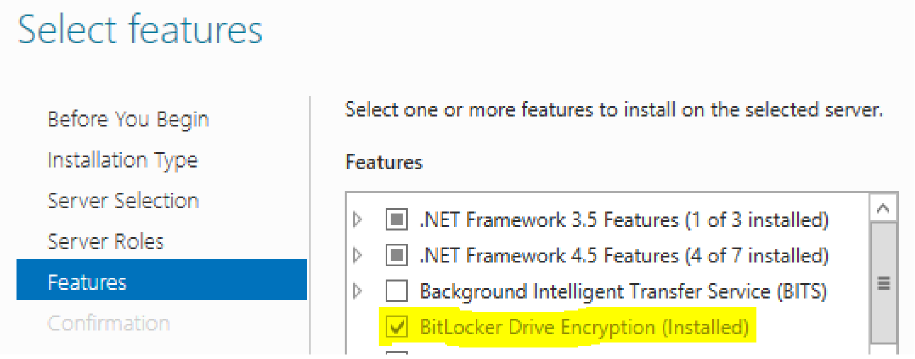
CapaSystems A/S

Introduction

If you already use BitLocker in your environment, you can skip steps 1 and 2 from this guide.

1) Feature Installation

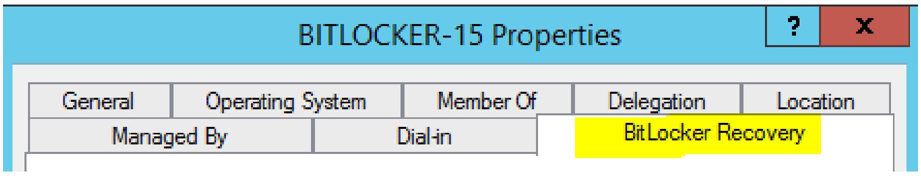
Install the *BitLocker Drive Encryption* feature on all Domain Controllers.



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

- ▣ .NET Framework 3.5 Features (1 of 3 installed)
- ▣ .NET Framework 4.5 Features (4 of 7 installed)
- □ Background Intelligent Transfer Service (BITS)
- ☑ BitLocker Drive Encryption (Installed)

If the feature is installed correctly, you should be able to see the *BitLocker Recovery* tab on computer objects in your Active Directory.



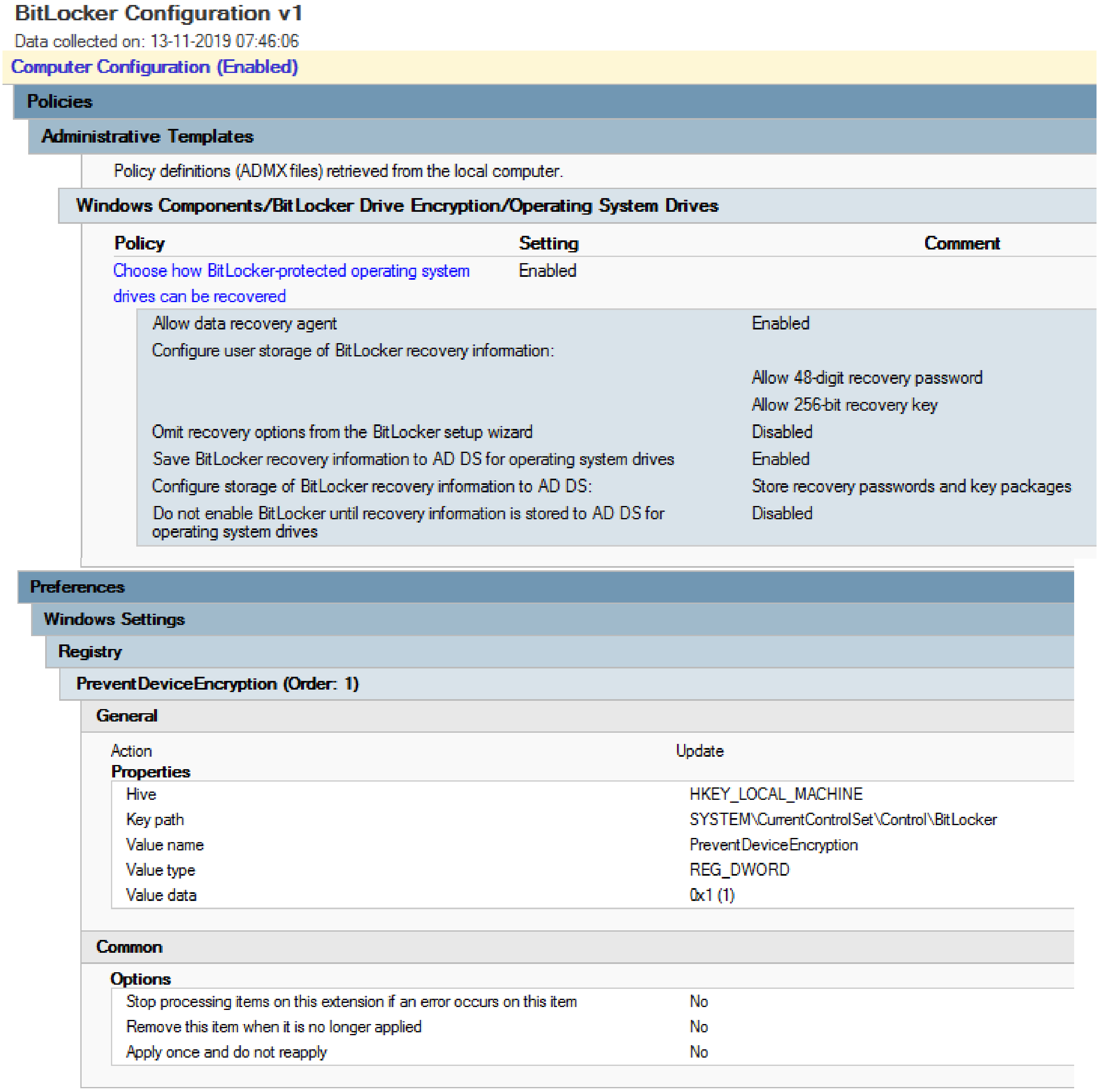
Installing the BitLocker Drive Encryption feature often requires a restart.

If you want to access the *BitLocker Recovery* tab from servers that are not Domain Controllers, you must also install the *BitLocker Drive Encryption* feature on that server.

2) Group Policy Object

You must create a Group Policy Object, that allows the BitLocker recovery information to be saved in Active Directory.

The Group Policy Object must look like the one below. Please do not add additional settings or change the settings below at this point.



BitLocker Configuration v1

Data collected on: 13-11-2019 07:46:06

Computer Configuration (Enabled)

Policies

Administrative Templates

Policy definitions (ADMX files) retrieved from the local computer.

Windows Components/BitLocker Drive Encryption/Operating System Drives

Policy	Setting	Comment
Choose how BitLocker-protected operating system drives can be recovered	Enabled	

Allow data recovery agent	Enabled
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	Disabled
Save BitLocker recovery information to AD DS for operating system drives	Enabled
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	Disabled

Preferences

Windows Settings

Registry

PreventDeviceEncryption (Order: 1)

General

Action	Update

Properties

Hive	HKEY_LOCAL_MACHINE
Key path	SYSTEM\CurrentControlSet\Control\BitLocker
Value name	PreventDeviceEncryption
Value type	REG_DWORD
Value data	0x1 (1)

Common

Options

Stop processing items on this extension if an error occurs on this item	No
Remove this item when it is no longer applied	No
Apply once and do not reapply	No

3) Service account

By default, computer objects do not have permission to look up msFVE information in Active Directory.

Hence, we need to create a service account, with permissions to look up the necessary msFVE information.

We recommend that you name the service account something recognizable, ie. *CapaBitLocker*

The service account must be created as a member of the predefined security group Domain Users.

Next, you must delegate control to allow the new service account to look up msFVE information.

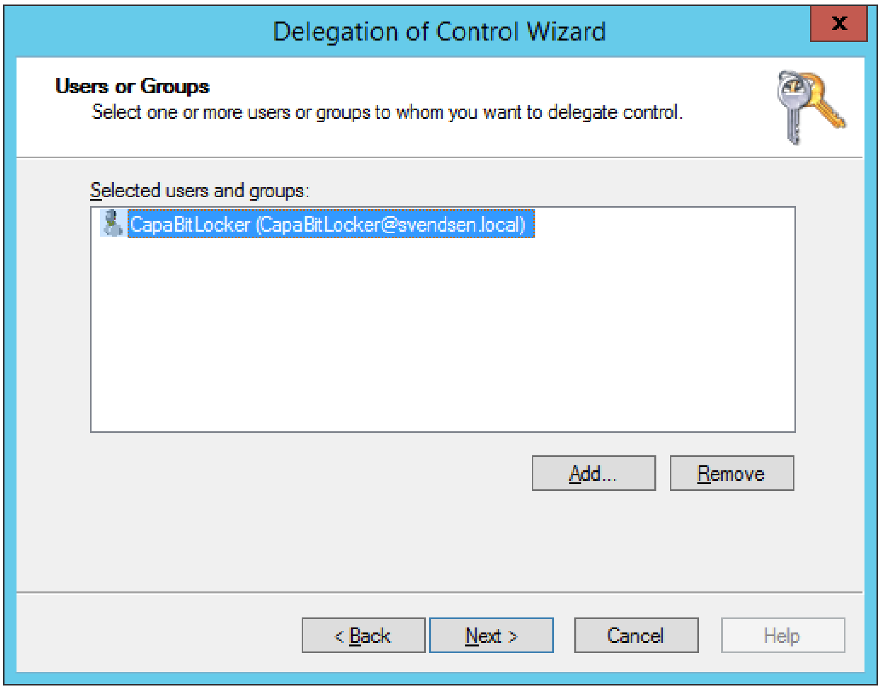
3.1) Delegate Control

Use the following procedure to enable access to BitLocker recovery information on the domain level to a service account named *CapaBitLocker* in Active Directory.

In **Active Directory Users and Computers**, right-click the domain name and select *Delegate Control…*

In the first dialog of the Delegation of Control Wizard, click *Next*

In the **Users or Groups** dialog, add the *CapaBitLocker* user for delegation to the list and click *Next*



Delegation of Control Wizard

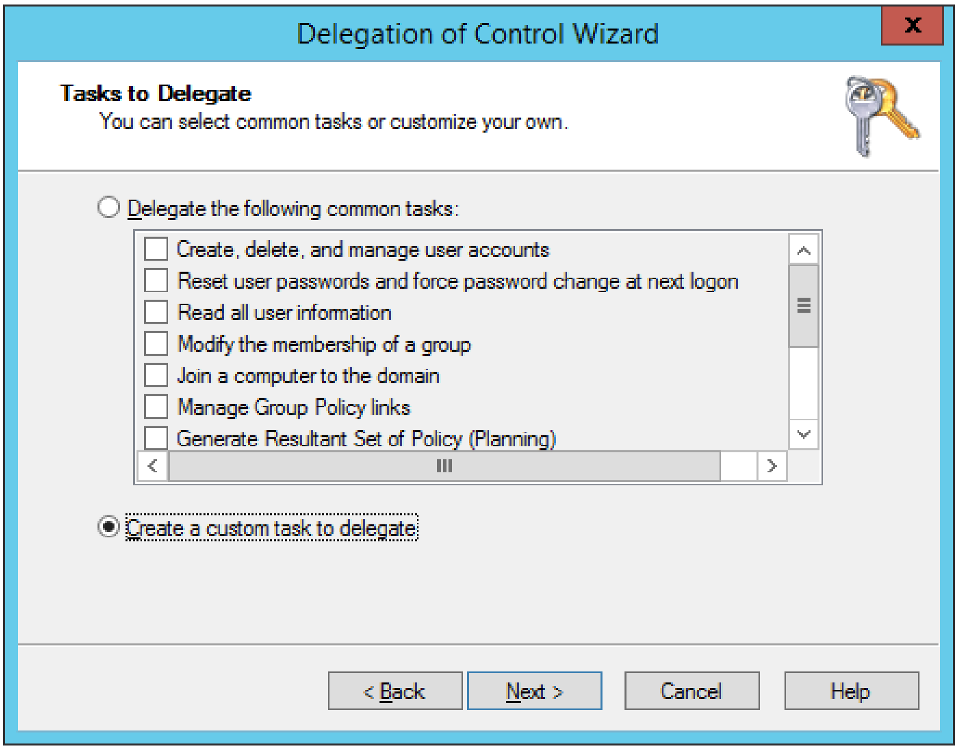
Users or Groups

Select one or more users or groups to whom you want to delegate control.

Selected users and groups:

CapaBitLocker (CapaBitLocker@svendsen.local)

In the **Tasks to Delegate** dialog, select Create a custom task to delegate and click *Next*



Delegation of Control Wizard

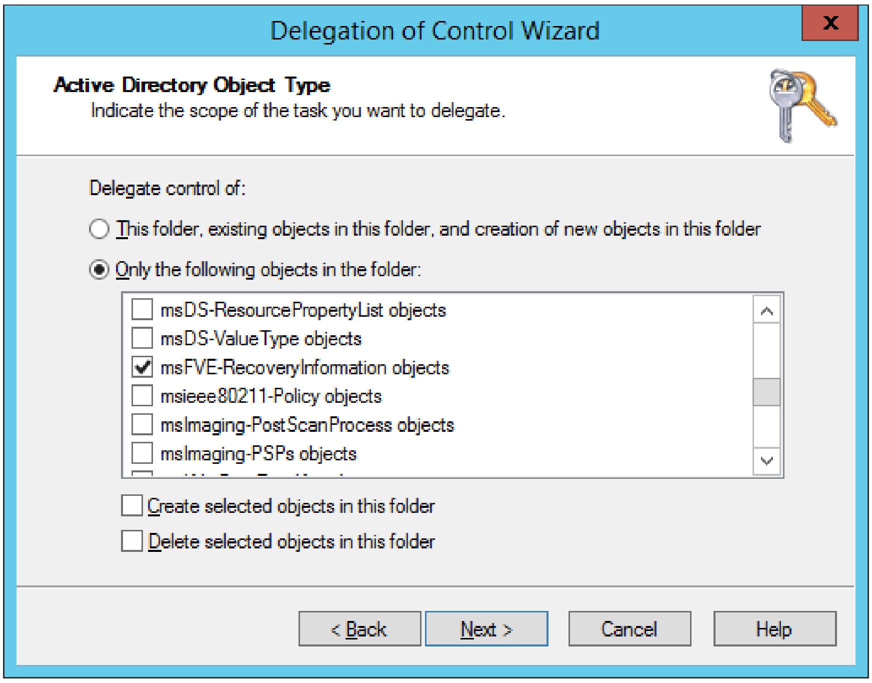
Tasks to Delegate
You can select common tasks or customize your own.

○ Delegate the following common tasks:
- □ Create, delete, and manage user accounts
- □ Reset user passwords and force password change at next logon
- □ Read all user information
- □ Modify the membership of a group
- □ Join a computer to the domain
- □ Manage Group Policy links
- □ Generate Resultant Set of Policy (Planning)

● Create a custom task to delegate

In the **Active Directory Object Type** dialog, select *Only the following objects in the folder:*

In the list select *msFVE-RecoveryInformation objects* and click *Next*



Delegation of Control Wizard

Active Directory Object Type
Indicate the scope of the task you want to delegate.

Delegate control of:

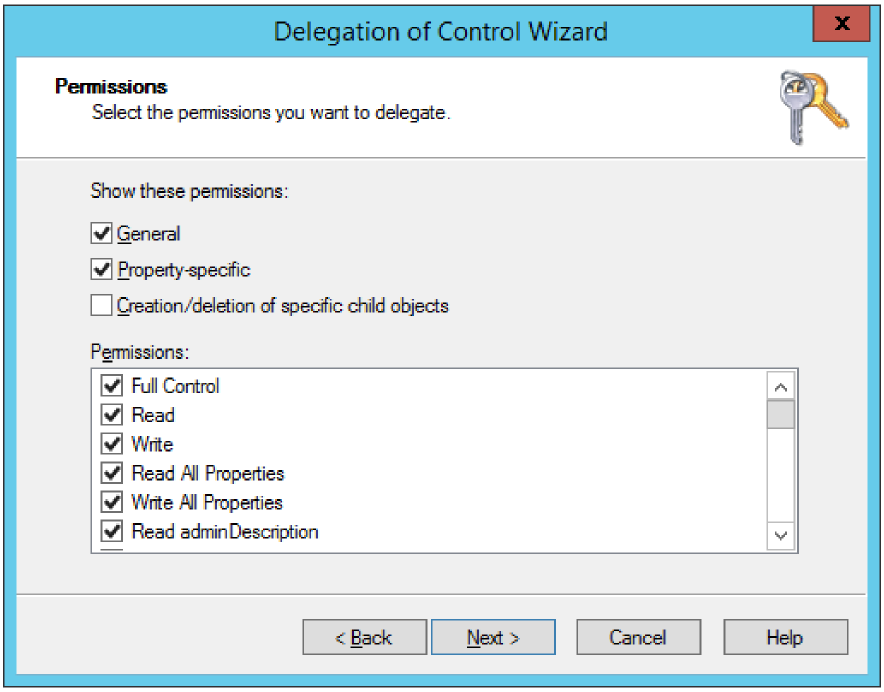
○ This folder, existing objects in this folder, and creation of new objects in this folder

● Only the following objects in the folder:
- □ msDS-ResourcePropertyList objects
- □ msDS-ValueType objects
- ☑ msFVE-RecoveryInformation objects
- □ msieee80211-Policy objects
- □ msImaging-PostScanProcess objects
- □ msImaging-PSPs objects

□ Create selected objects in this folder

□ Delete selected objects in this folder

In the **Permissions** dialog, select *Full Control* under Permissions and click *Next*



Delegation of Control Wizard

Permissions
Select the permissions you want to delegate.

Show these permissions:

☑ General
☑ Property-specific
□ Creation/deletion of specific child objects

Permissions:

☑ Full Control
☑ Read
☑ Write
☑ Read All Properties
☑ Write All Properties
☑ Read adminDescription

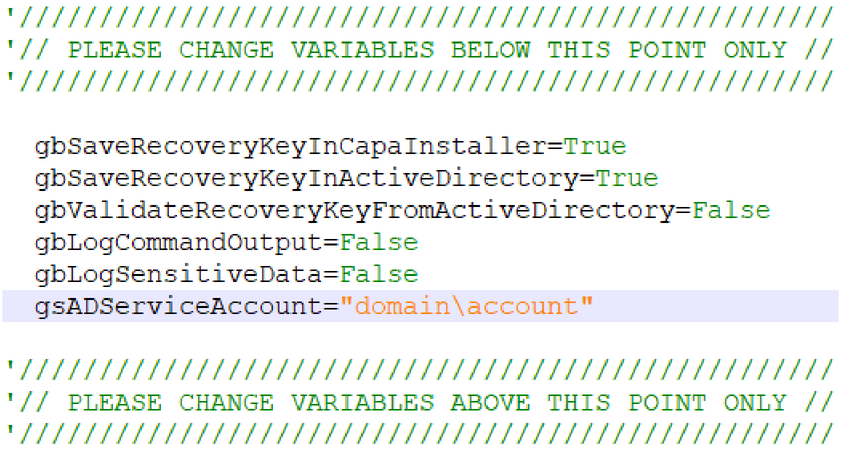
Click *Finish*

The service account *CapaBitLocker* is now granted permission to access BitLocker recovery information in Active Directory.

4) Script update

You can use the global variables below to control how the package script behaves.

With the default settings, all active BitLocker recovery keys are saved in Active Directory and CapaInstaller.



```
'///////////////////////////////////////////////////
'// PLEASE CHANGE VARIABLES BELOW THIS POINT ONLY //
'///////////////////////////////////////////////////

  gbSaveRecoveryKeyInCapaInstaller=True
  gbSaveRecoveryKeyInActiveDirectory=True
  gbValidateRecoveryKeyFromActiveDirectory=False
  gbLogCommandOutput=False
  gbLogSensitiveData=False
  gsADServiceAccount="domain\account"

'///////////////////////////////////////////////////
'// PLEASE CHANGE VARIABLES ABOVE THIS POINT ONLY //
'///////////////////////////////////////////////////
```

4.1) Common

The settings listed below can be used to control how the package script behaves.

gbSaveRecoveryKeyInCapaInstaller

True = Save the BitLocker recovery keys from the workstation in CapaInstaller

False = Don't save the BitLocker recovery keys from the workstation in CapaInstaller

gbSaveRecoveryKeyInActiveDirectory

True = Save the BitLocker recovery keys from the workstation in Active Directory

False = Don't save the BitLocker recovery keys from the workstation in Active Directory

gbValidateRecoveryKeyFromActiveDirectory

True = Validate that the BitLocker recovery keys are saved correctly in Active Directory

False = Don't validate that the BitLocker recovery keys are saved correctly in Active Directory

You must update the script with the settings described in **step 4.2** if you enable this setting

gbLogCommandOut

True = Log the output from the commands used by the package script

False = Don't log output from the command used by the package script

If you enable this setting, sensitive data will be visible in the package log and the option should primarily be used for troubleshooting

gbLogSensistiveData

True = Make sensitive data visible in the package log

False = Mask sensitive data in the package log

If you enable this setting, sensitive data will be visible in the package log and the option should primarily be used for troubleshooting

4.2) Active Directory

If *gbValidateRecoveryKeyFromActiveDirectory* is enabled you must update the settings below to match your environment.

gsAdServiceAccount

The service account is used to retrieve and validate msFVE recovery information from Active Directory.

The service account name must be specified in clear text.

The service account password must be encrypted using our password encryption tool and then saved in the package kit folder. You can read more about using our password encryption tool **here**

💡 Remember to rebuild the CapaInstaller.kit file after having updated the registry file with the encrypted password.