BitLocker N-Central Setup

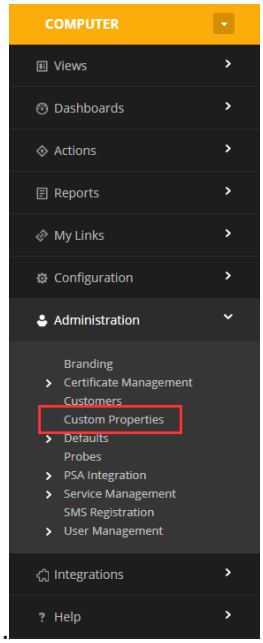
This document is to help you setup N-Central to work with the BitLocker Script/Automation Policy. In this document you will also see how to setup a client environment as well before being able to run the Automation Policy.

N-Central Setup

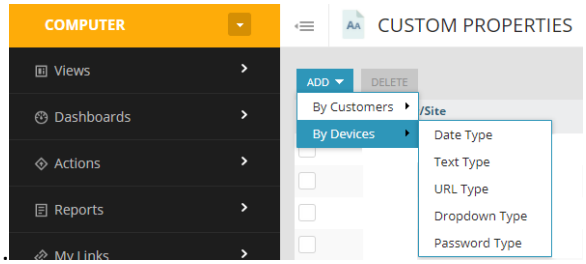
1. N-Central Custom Properties

1.1. Navigate to the top level in N-Central (Yellow Level).

1.2. Navigate to **Administration > Custom Properties**.

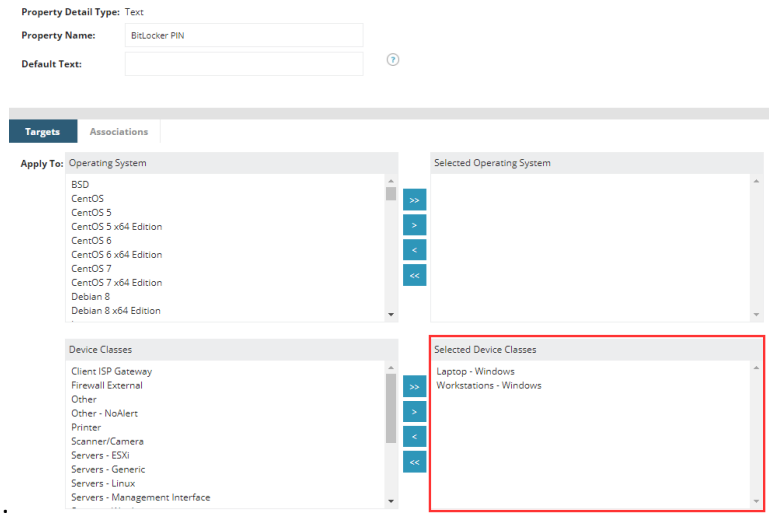
1.2.1. 

1.3. In Custom Properties, click **ADD > By Device > Text.**

1.3.1. 

1.3.2. Name this property **BitLocker PIN**. Then assign it to Windows Laptops & Workstations.

BitLocker N-Central Setup

1.3.3. 

1.4. In Custom Properties, click **ADD > By Device > Dropdown.**

1.4.1. Name this property **BitLocker Task**. Assign it to Windows Laptops & Workstations.

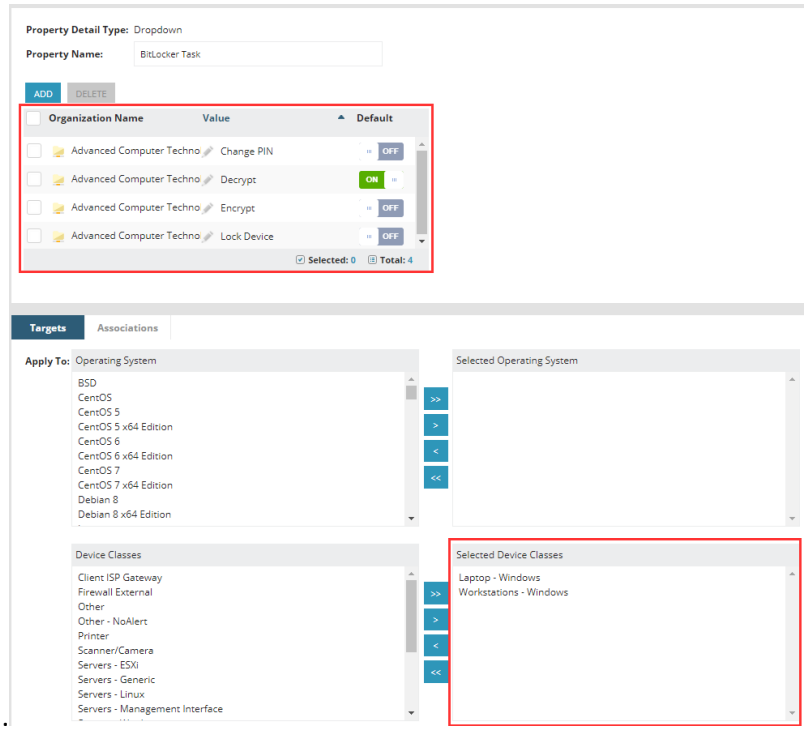
1.4.2. Add the following values to be included in the dropdown:

1.4.2.1. Change PIN

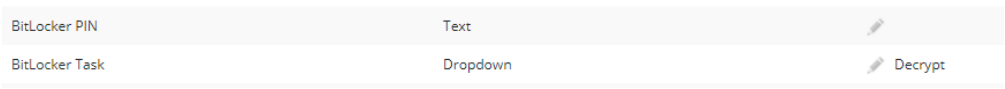
1.4.2.2. Decrypt (Default)

1.4.2.3. Encrypt

1.4.2.4. Lock Device

1.4.3. 

1.5. N-Central's Custom Properties are now all setup. You should now see the properties you created on a Windows device under **Settings > Custom Properties.**

1.5.1. 

BitLocker N-Central Setup

2. Setting BitLocker properties per device

2.1. To perform a BitLocker task on a device we will need to setup the custom properties so the N-Central Automation policy will know what to do.

2.2. Navigate to the device you want to perform a BitLocker task on. Click on the device to get to the device **Overview**. Next navigate to **Settings > Custom Properties**

2.3. The Custom Properties that you created before should show up. Enter the information you need and set the task to be run on this device.

2.4. **BitLocker PIN** = The Password that will be set on the device when prompted to decrypt machine.

2.5. **BitLocker Task** = What you want the script to do.

2.6. 

2.7. Once the properties are all set and saved, we can move on to creating and running the encryption task on the machine.

3. Creating BitLocker Encryption Task

3.1. The Automation Policy should already be in the N-Central repository. If not use the pre-compiled .AMP.

3.2. Navigate to the Customer/Site level you would like to push the BitLocker Task on.

3.3. Click ADD > Automation Policy.

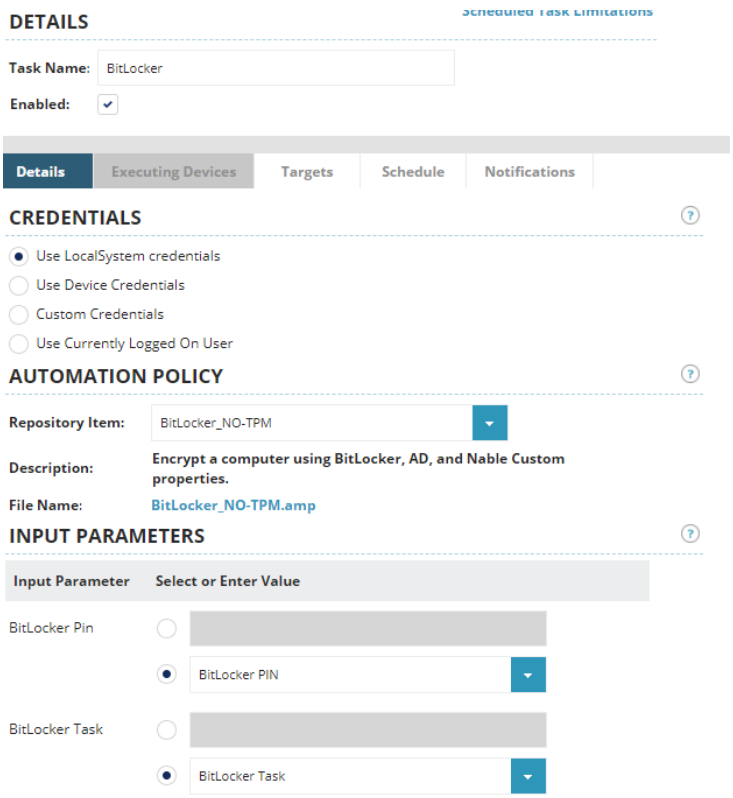
3.4. Name your task, and set the following settings as so.

3.4.1. Credentials = Use “Custom Credentials” and use the domain admin for the task.

3.4.2. Automation Policy = Select the BitLocker.amp that has been uploaded. (At this time it is named BitLocker_NO-TPM)

3.4.3. Input Parameters = Make sure to select the correct Custom Property for the correct input.

BitLocker N-Central Setup



3.4.4.

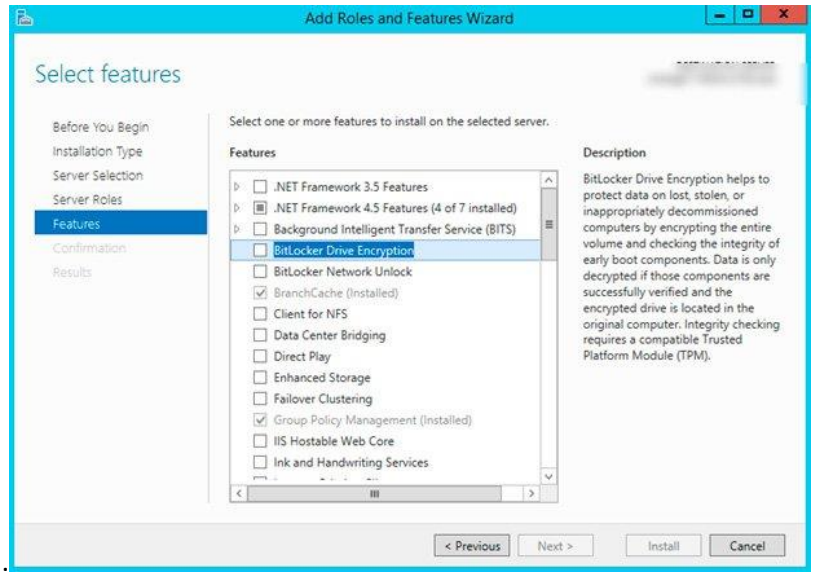
3.4.5. Like with all other N-Central tasks, make sure to finish setting the Targets, Schedule, and Notification tabs. Once all complete save and run the task. When the task runs it will pull the PIN and Task data from the N-Central custom properties fields and apply them to the device via the script.

Customer Setup

1. BitLocker Management Tools Install (Req. 2012 R2 +)

1.1. We will need to install BitLocker management tools on your AD server. On your domain controller you will need to open Server Manager. Navigate to **Add Roles & Features > Feature BitLocker Drive Encryption**.

BitLocker N-Central Setup

1.1.1. 

1.2. Your server might need to reboot. Once rebooted you should now have the management tools installed.

2. Group Policy Creation

2.1. Open Group Policy and create a new GPO. This GPO will need to be linked to the OU that your computers are in.

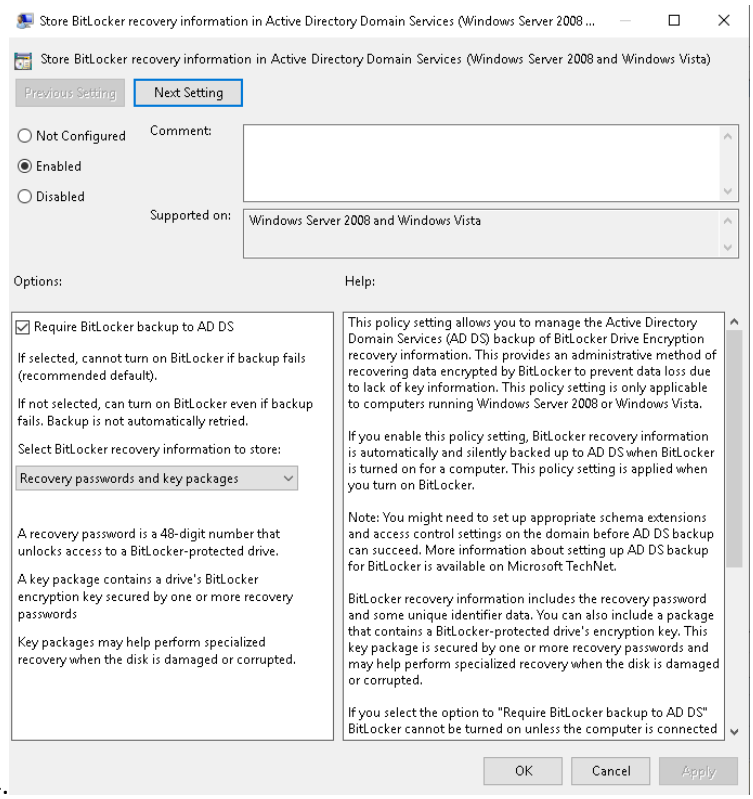
2.2. Setup the following policies:

2.2.1. Navigate to **Computer Configuration > Policies > Administrative Templates > Windows Components > BitLocker Drive Encryption**

2.2.2. Enable the ***Store BitLocker Recovery information in Active Directory Domain Services*** policy.

2.2.3. Select ***Require BitLocker back to AD DS*** & ***Recovery passwords and key packages***.

BitLocker N-Central Setup

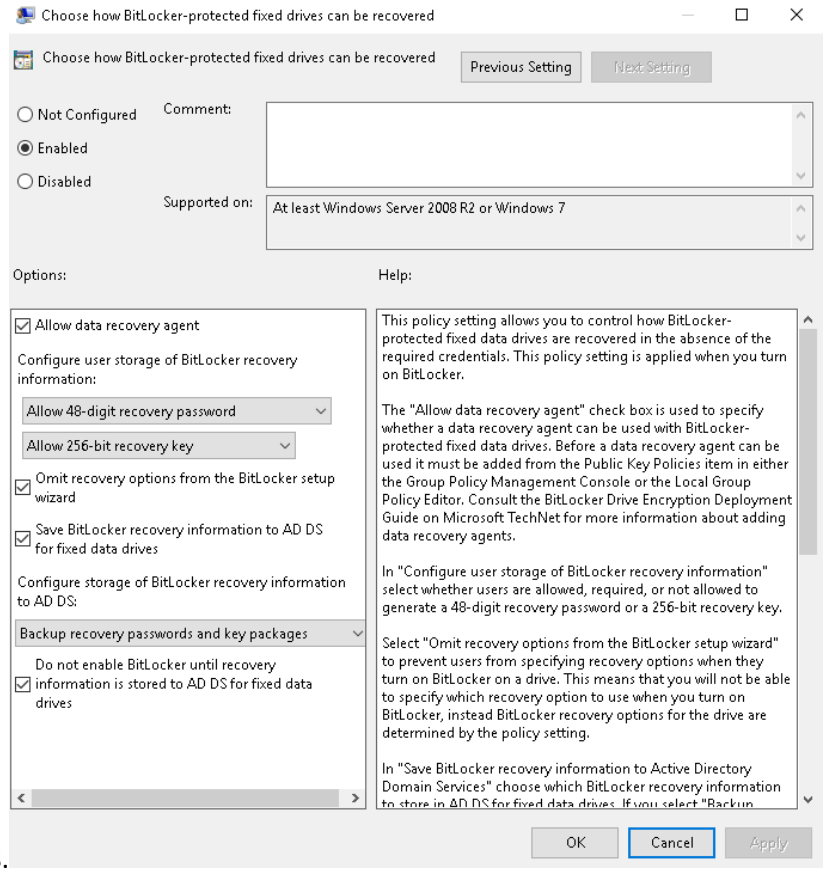
2.2.4. 

2.2.5. Navigate to **Computer Configuration > Policies > Administrative Templates > Windows Components > BitLocker Drive Encryption > Fixed Data Drives**

2.2.6. Enable the ***Choose how BitLocker-protected fixed drives can be recovered*** policy.

2.2.7. Select ***Allow data recovery agent, Allow 48-digit recovery password, Allow 256-bit recovery key, Omit recovery options from BitLocker setup wizard, Save BitLocker recovery information to AD DS for fixed data drives, Backup recovery passwords and key packages, Do not enable BitLocker until recovery information is stored o AD DS for fixed data drives.***

BitLocker N-Central Setup

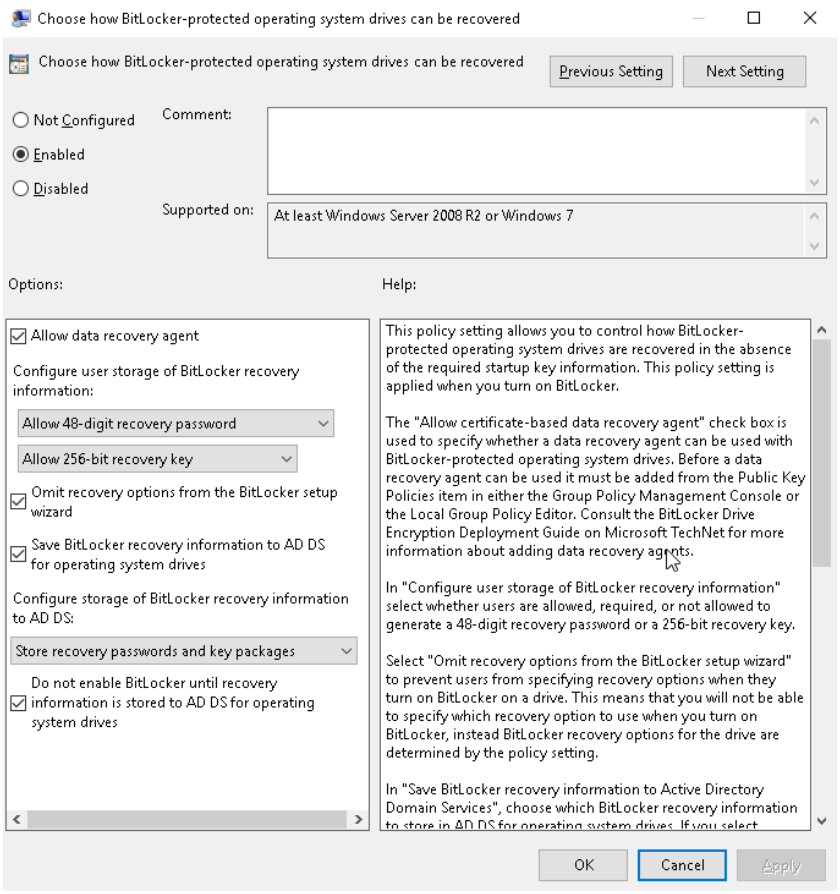
2.2.8. 

2.2.9. Navigate to **Computer Configuration > Policies > Administrative Templates > Windows Components > BitLocker Drive Encryption > Operating System Drives.**

2.2.10. Enable the ***Choose how BitLocker-protected operating system drives can be recovered*** policy.

2.2.11. Select ***Allow data recovery agent, Allow 48-digit recovery password, Allow 256-bit recovery key, Omit recovery options from BitLocker setup wizard, Save BitLocker recovery information to AD DS for fixed data drives, Backup recovery passwords and key packages, Do not enable BitLocker until recovery information is stored o AD DS for operating system drives.***

BitLocker N-Central Setup



2.2.12.

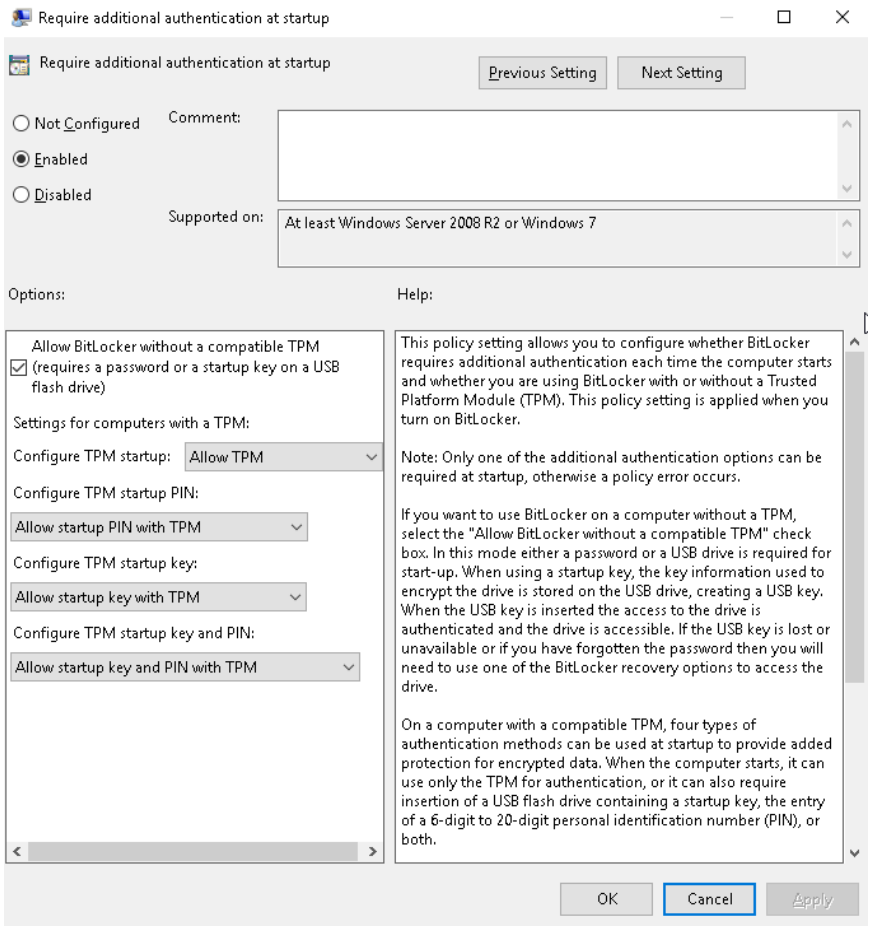
2.2.13. Navigate to **Computer Configuration > Policies > Administrative Templates > Windows Components > BitLocker Drive Encryption > Operating System Drives.**

2.2.14. Enable the ***Require additional authentication at startup***.

2.2.15. **Note** During this documentation, the script does not have good logic for TPM. We will need to set a password for all encryptions. This means we need to enable BitLocker for no TPM devices. Once the script has better logic, we will be able to see TPM and have better options of encryption with that method.

2.2.16. Select ***Allow BitLocker without a compatible TPM, Allow TPM, Allow startup PIN with TPM, Allow startup key with TPM, Allow startup key with TPM, Allow startup key and PIN with TPM.***

BitLocker N-Central Setup



2.2.17.

2.2.18. Close your GPO. Make sure to apply the GPO to the correct OU that has your workstations you want to encrypt.

3. BitLocker Recovery Keys

3.1. To find your BitLocker recovery keys you will need to open **Active Directory Users & Computers** (On your DC with BitLocker management tools installed)

3.2. Navigate to the computer you want to see the keys for. **Right Click > Properties**.

3.3. In the machine properties box, you will now see a tab called ***BitLocker Recovery***. Navigate to that tab to reveal all BitLocker Recovery Passwords ever added to AD.

BitLocker N-Central Setup

3.4.