Manually Backup BitLocker Recovery Key to AD

How do I manually backup my BitLocker recovery key to AD if I encrypted BEFORE joining the computer to the WIN domain?

⚠️ You require local admin rights to run manage-bde commands.

STEP 1: Get the ID for the numerical password protector of the volume, in the example below we are using the C: drive. Run the command from an elevated command prompt.

On Windows 10 the key needs to be in quotation marks "key"

```
manage-bde -protectors -get c:
```

Example:

Bitlocker Drive Encryption: Configuration Tool version 6.1.7600
Copyright (C) Microsoft Corporation. All rights reserved.
All Key Protectors
  External Key:
    ID:{F12ADB2E-22D5-4420-980C-851407E9EB30}
    External Key File Name:
      F12ADB2E-22D5-4420-980C-851407E9EB30.BEK
  Numerical Password:
    ID:{DFB478E6-8B3F-4DCA-9576-C1905B49C71E}
    Password:
      224631-534171-438834-445973-130867-430507-680922-709896
    TPM And PIN:
      ID:{EBAFC4D6-D044-4AFB-84E3-26E435067AA5}

In the above result, you would find an ID and Password for Numerical Password protector.

STEP 2: Use the numerical password protector’s ID from STEP 1 to backup recovery information to AD

In the below command, replace the GUID after the -id with the ID of Numerical Password protector.

```
manage-bde -protectors -adbackup c: -id {DFB478E6-8B3F-4DCA-9576-C1905B49C71E}
```

Bitlocker Drive Encryption: Configuration Tool version 6.1.7600
Copyright (C) Microsoft Corporation. All rights reserved.
Recovery information was successfully backed up to Active Directory.

You should now be able to view the recovery information for the volume in the active directory.