How do I configure Active Directory to store Bitlocker recovery information?

Service: Windows Infrastructure for Departments

You can configure BitLocker Drive Encryption to back up recovery information for BitLocker-protected drives and the Trusted Platform Module (TPM) to Active Directory Domain Services (AD DS). Recovery information includes the recovery password for each BitLocker-protected drive, the TPM owner password, and the information required to identify which computers and drives the recovery information applies to.

The first step, adding the BitLocker Recovery Password Viewer to the domain controllers, has already been completed for you. All that you'll need to do is to email consult@uic.edu and let us know which organizational unit (OU) contains the computers that you'll be encrypting and which group of users you'd like to have access to the stored bitlocker keys so that we can delegate the authority to non-domain administrators to view the recovery keys of the computer objects in that OU. After that's done, you'll need to set the proper group policy settings to configure the computers to back up the recovery information.

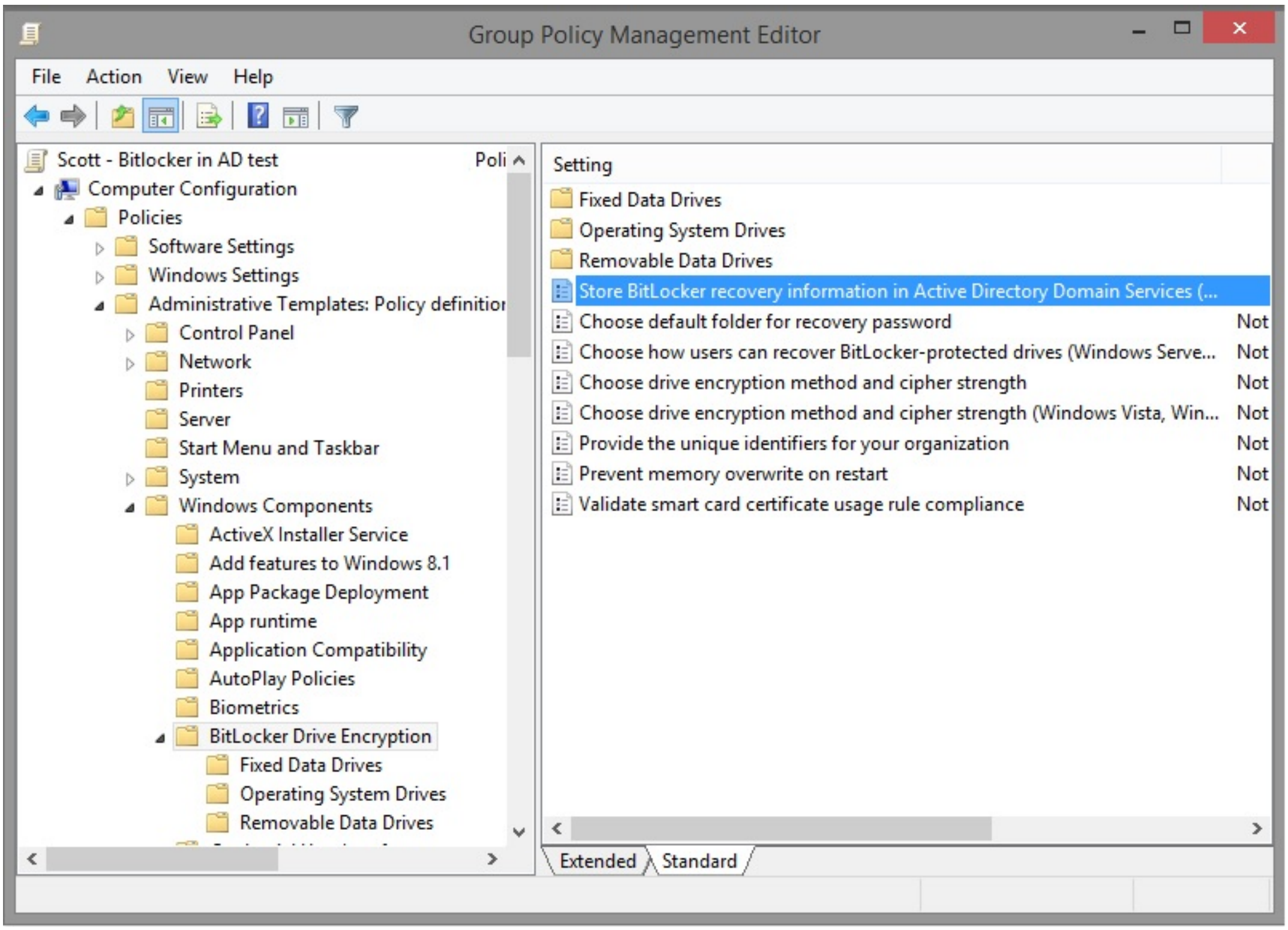
GPO Settings:

1. Open "Group Policy Management".

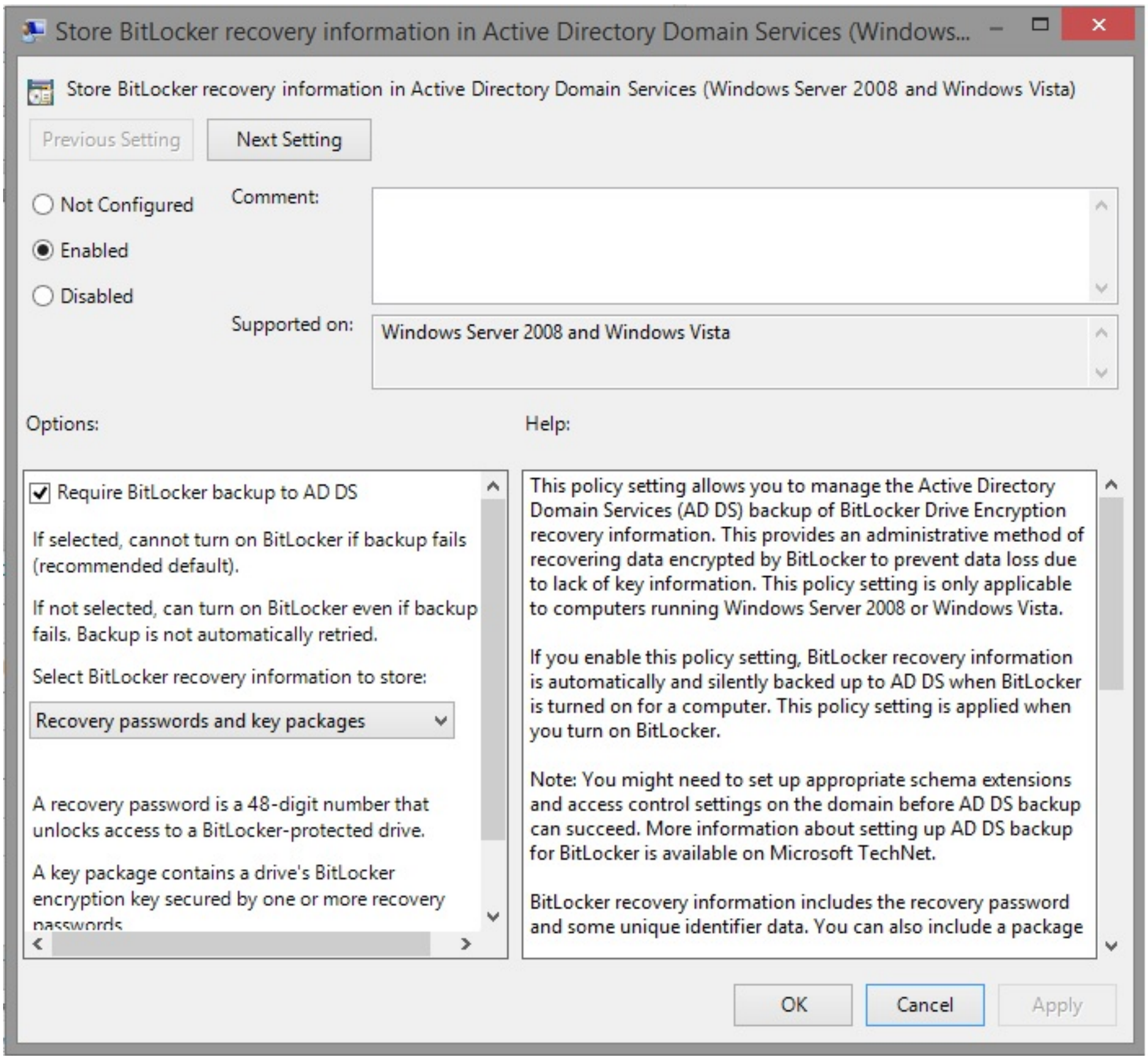
2. Navigate the the GPO that's linked to the OU that you want to contain your settings for Bitlocker.

3. Right click on the GPO and select "Edit"

4. Navigate to Computer Configuration->Policies->Administrative Templates->Windows Components->Bitlocker Drive Encryption.

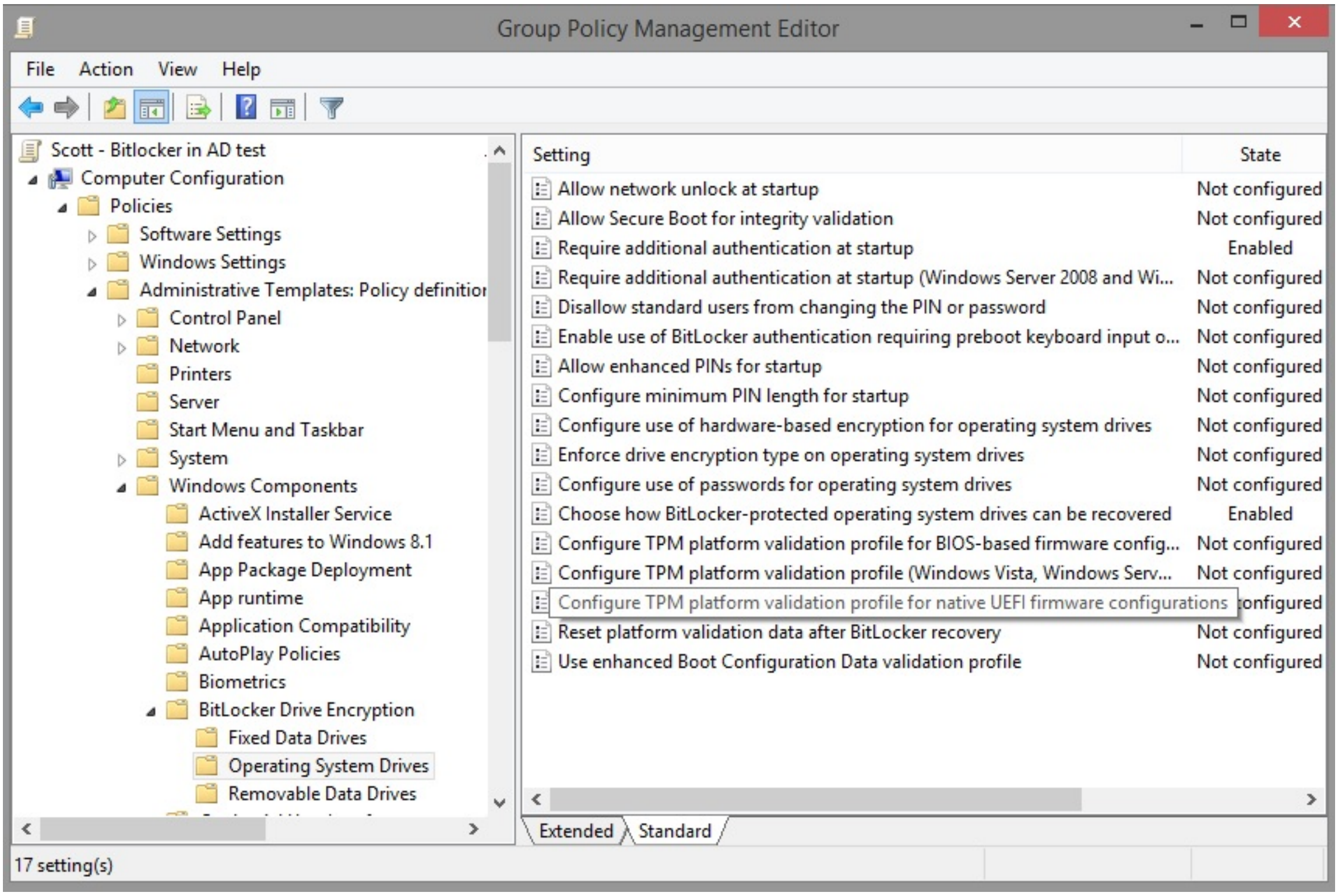


5. Double Click on "Store Bitlocker Recovery information in Active Directory Domain Services" and configure it as follows:

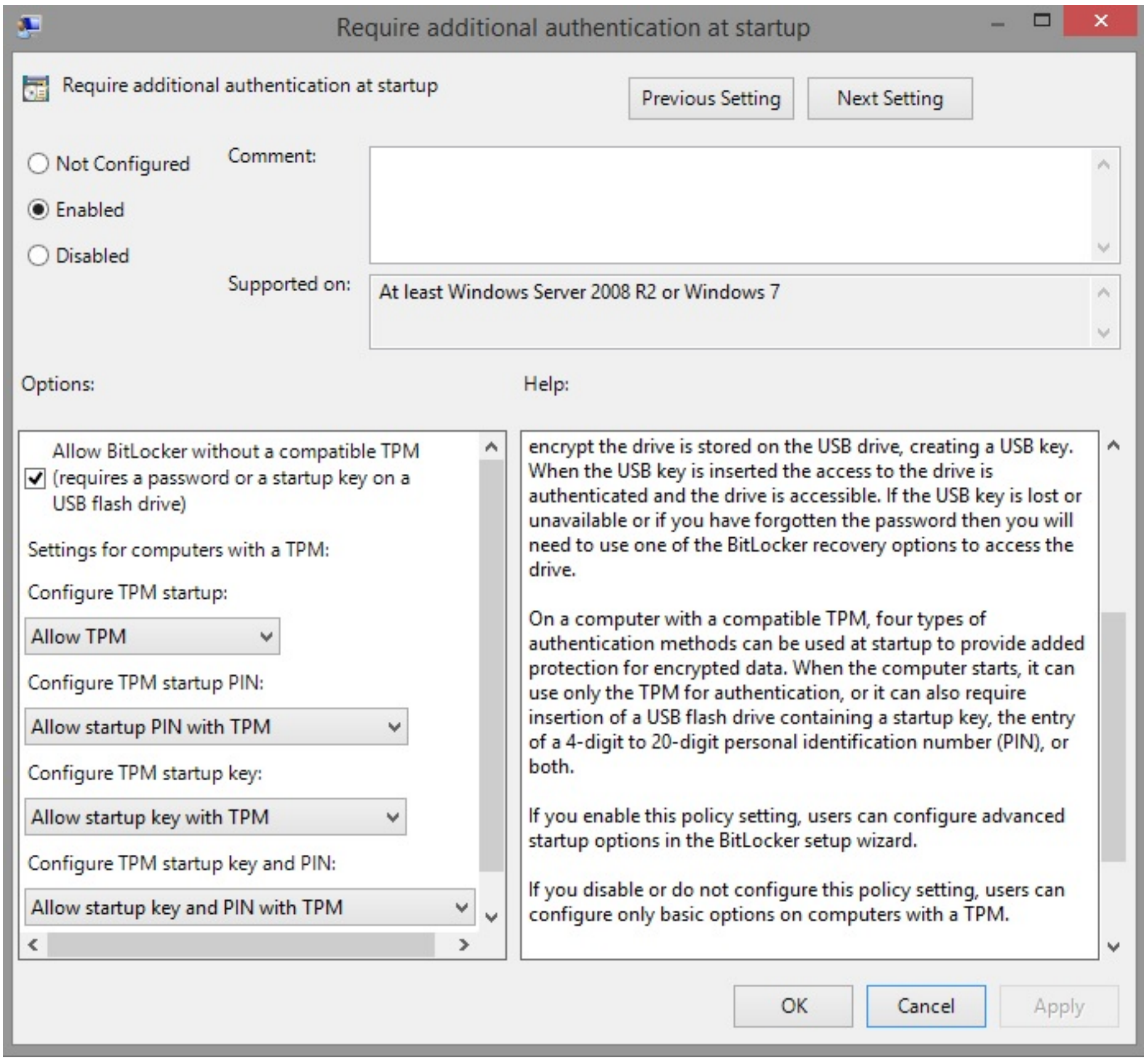


6. Click "OK".

7. Under Computer Configuration->Policies->Administrative Templates->Windows Components->Bitlocker Drive Encryption, click on the appropriate folder for your configuration. In this example, I'm configuring bitlocker to encrypt the OS drive.



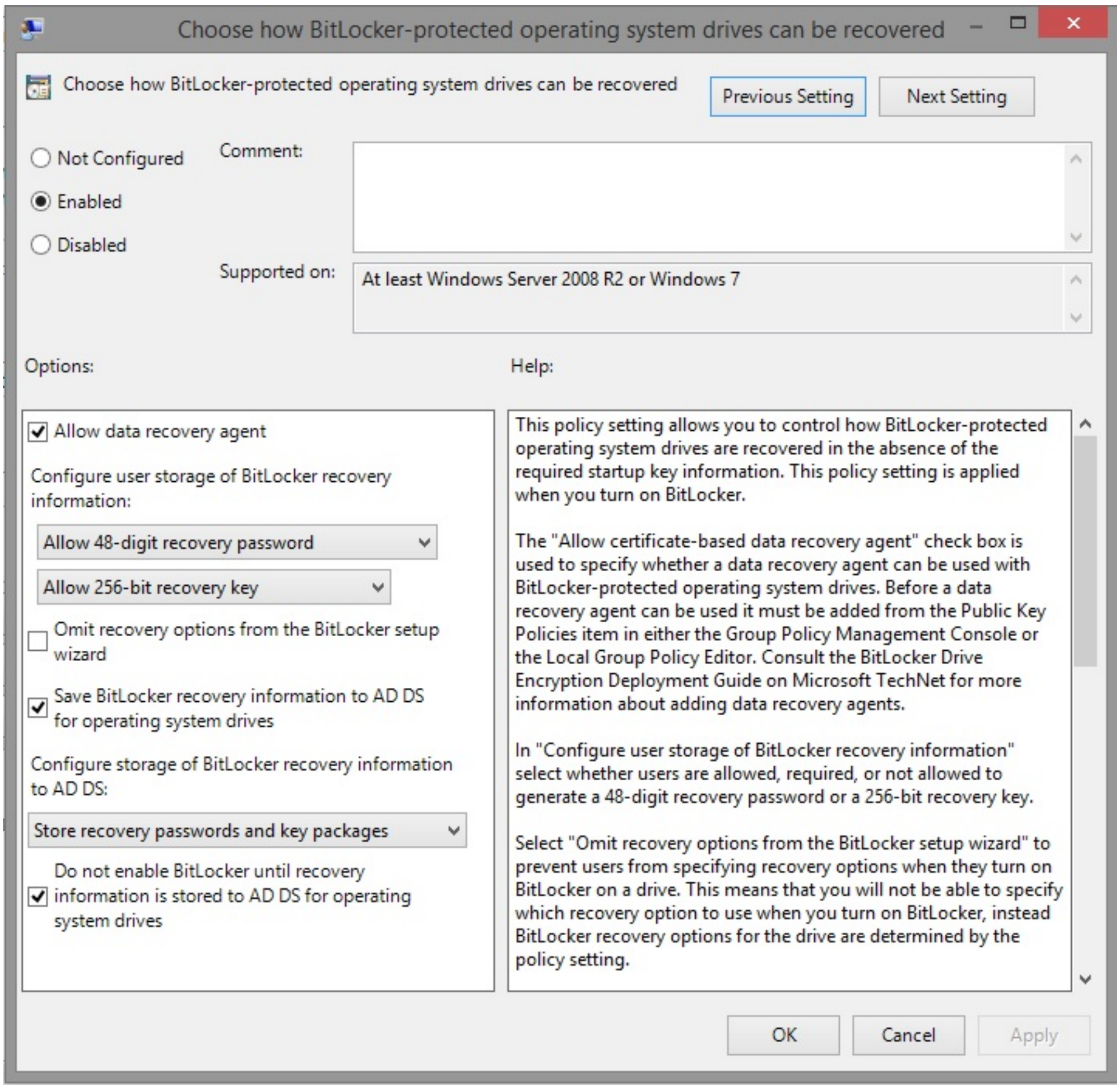
8. Double click on "Require additional authentication at startup" and configure your settings as follows:



NOTE: "Allow Bitlocker without a compatible TPM" need only be checked if at least one of the computers that you're encrypting do not have a trusted platform module.

9. Click "OK".

10. Double click on "Choose how Bitlocker-protected operating system drives can be recovered" and configure it as follows:



11. Click "OK".

12. Navigate to Computer Configuration->Policies->Administrative Templates->System->Trusted Platform Module and set "Turn on TPM backup to Active Directory Domain Services" to "Enabled".

13. Click "OK".

NOTE: Only machines that have downloaded the updated group policies and were encrypted after the group policy has been applied to the machine will have their recovery information stored in Active Directory. To ensure that the newly configured group policy settings are applied, please reboot the machine prior to encrypting and/or run "gpudate /force" from a command line on that machine. If a machine has already been encrypted, you can force it to store its information in Active directory by opening up powershell and typing manage-bde -protectors -get c: to get its bitlocker information and then typing manage-bde -protectors -adbackup c: -id '{<numerical password ID>}'

Need help?

Windows Infrastructure for Departments

Email	consult@uic.edu
Phone	312-413-0003

Last updated: July 15, 2015

Browse by tag

access accessibility Acheivements Acrobatiq active directory active learning adaptive release adda adding adding users addressbook administrator adsm android announcements anonymous answers antivirus argo assesments assessments assignment assignments audio-visual availability backup backup adsm Backups bitlocker blackberry blackboard blackboard collaborate blackboard im blackboard upgrade blank page blogs bluestem browser calendar cengage learning certificates chalk title management chat check course links classroom classroom capture classrooms clicker collaboration column columns communication compatibility computer lab computer replacement program computers conferencing connect contacts content content area content editor content package copy course availability course content course copy course link course messages courses tab course tab course tabs Crashplan database date management digital signage directory discussion board download echo360 edit mode eduroam email emergency sms encryption enter equipment error errors esri eudora event examsoft exchange Exchange Office365 iOS Exchange Office365 Outlook Exchange Online exchange outlook exemplary course template export grades fact file name file size file types flickr ftp glossary gmail Google Apps googleapps google groups grade center grading period grading schemas groups i-card i>clicker IAM IM instant messaging instant messenger instructor ipad iphone itunes ldap lecture capture linux listserv mac mailbox mailserv manage grades mashups massmail mbam media migrate migration mobile modules multimedia netid network non-accc Office365 Office365 Exchange Office365 Exchange Outlook Office365 Onedrive originality report outlook password passwords pgp phone phonebook pine printing qualtrics removing users res-net reservation resphone rt safeassign security SharePoint shibboleth software spss ssh stata statistical software storage student preview survey systat telecom template tests thunderbird tools troublshooting u-print uicalendar uicast unix video streaming virtual server voicemail voip vpn webdisk webhost webmail web publishing wifi wiki windows wireless

More