

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

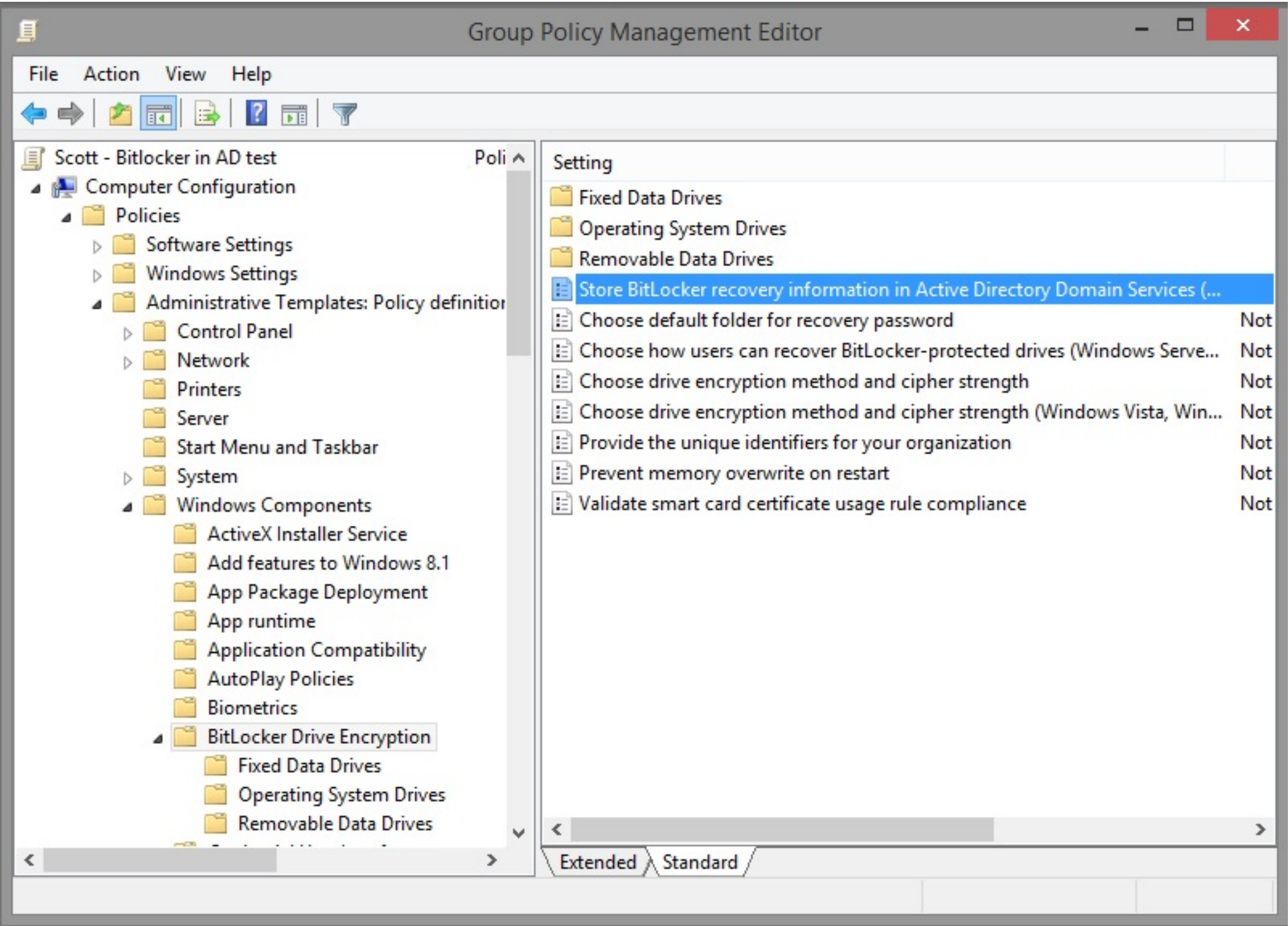
**Service:** [Windows Infrastructure for Departments](#)

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](mailto: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:

Store BitLocker recovery information in Active Directory Domain Services (Windows...

Store BitLocker recovery information in Active Directory Domain Services (Windows Server 2008 and Windows Vista)

Previous Setting

Next Setting

☐ Not Configured

☒ Enabled

☐ Disabled

Comment:

Supported on:

Windows Server 2008 and Windows Vista

Options:

☒ Require BitLocker backup to AD DS

If selected, cannot turn on BitLocker if backup fails (recommended default).

If not selected, can turn on BitLocker even if backup fails. Backup is not automatically retried.

Select BitLocker recovery information to store:

Recovery passwords and key packages

A recovery password is a 48-digit number that unlocks access to a BitLocker-protected drive.

A key package contains a drive's BitLocker encryption key secured by one or more recovery passwords

Help:

This policy setting allows you to manage the Active Directory Domain Services (AD DS) backup of BitLocker Drive Encryption recovery information. This provides an administrative method of recovering data encrypted by BitLocker to prevent data loss due to lack of key information. This policy setting is only applicable to computers running Windows Server 2008 or Windows Vista.

If you enable this policy setting, BitLocker recovery information is automatically and silently backed up to AD DS when BitLocker is turned on for a computer. This policy setting is applied when you turn on BitLocker.

Note: You might need to set up appropriate schema extensions and access control settings on the domain before AD DS backup can succeed. More information about setting up AD DS backup for BitLocker is available on Microsoft TechNet.

BitLocker recovery information includes the recovery password and some unique identifier data. You can also include a package

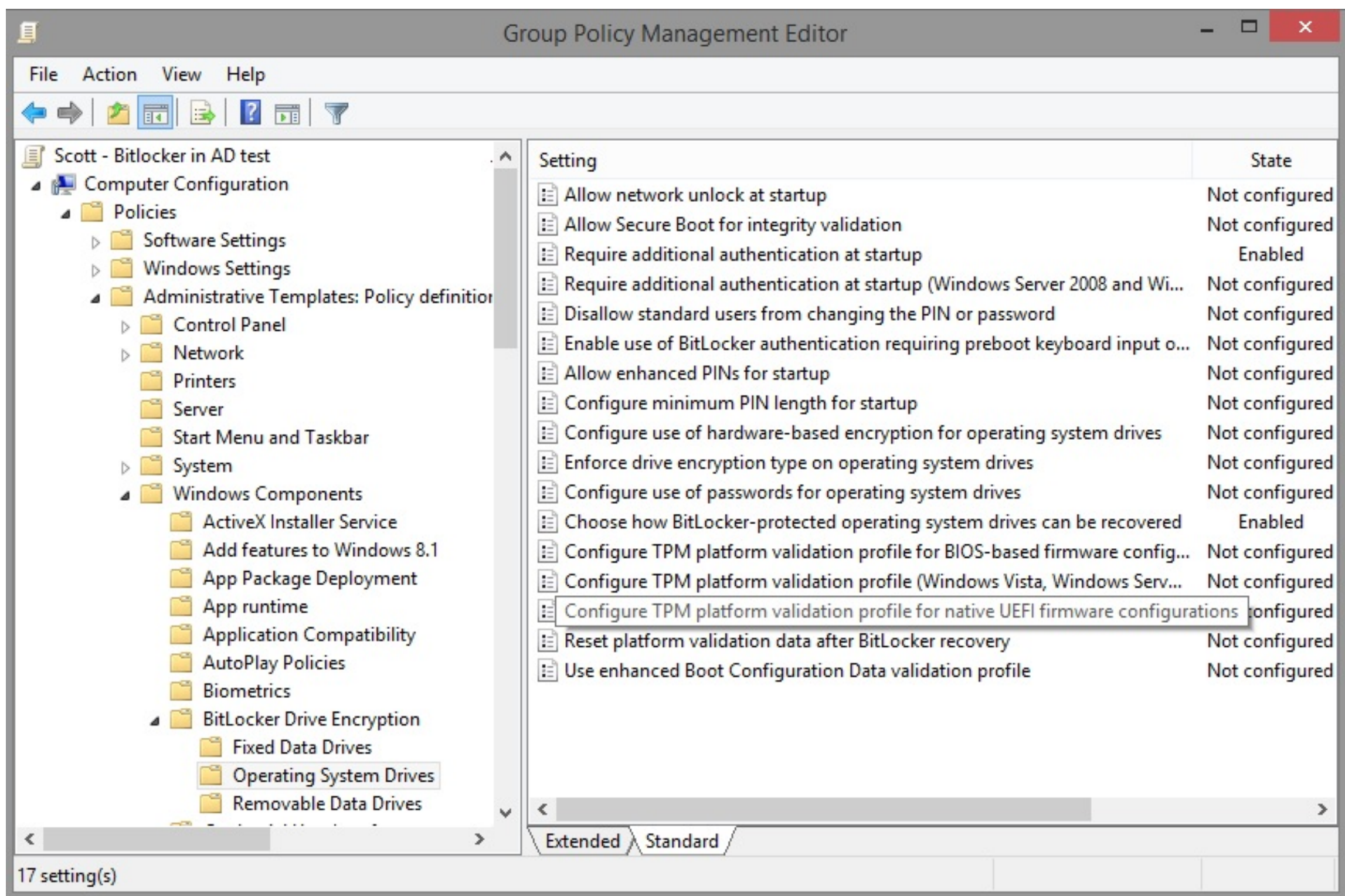
OK

Cancel

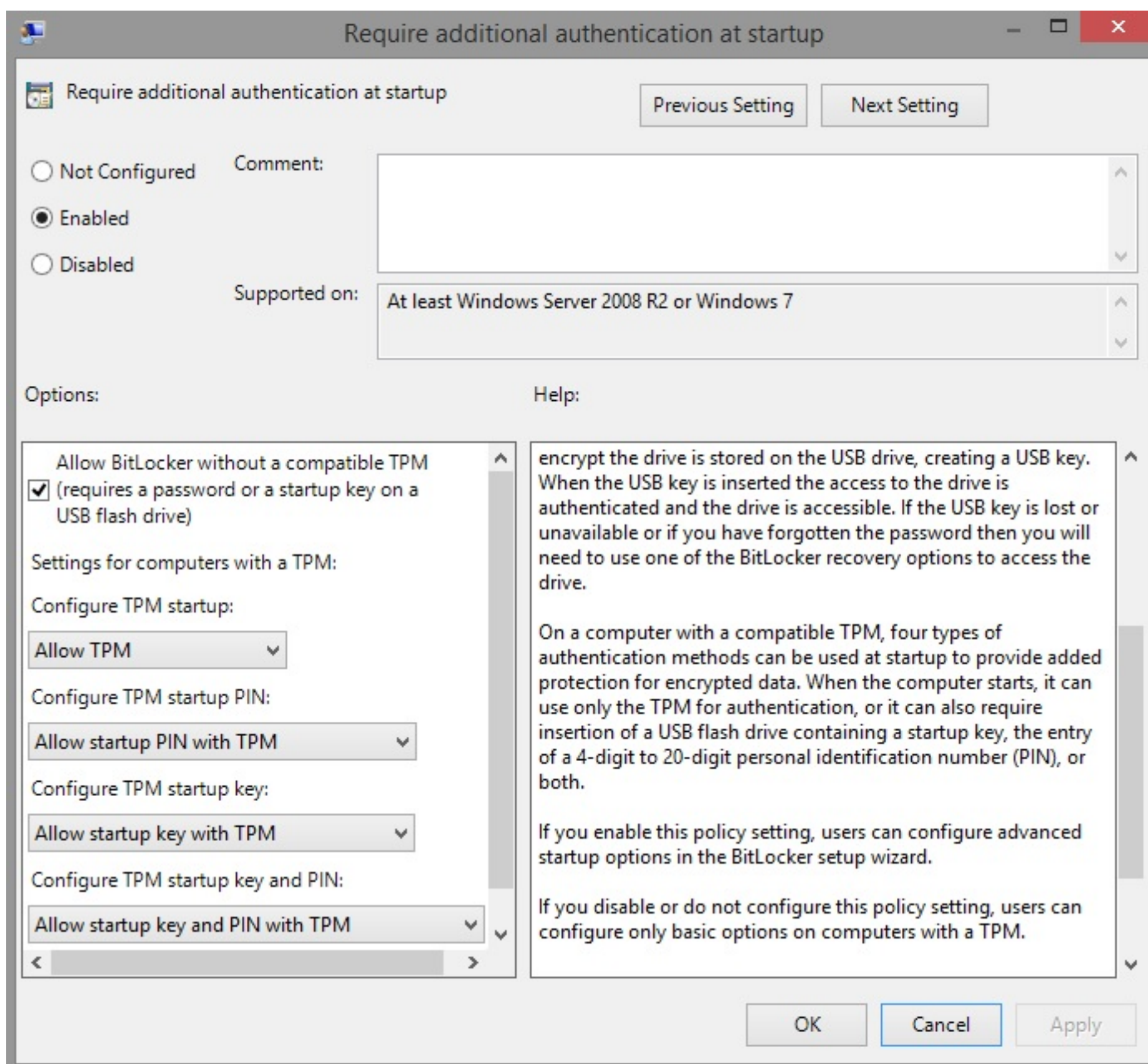
Apply

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:

Choose how BitLocker-protected operating system drives can be recovered

Choose how BitLocker-protected operating system drives can be recovered

Previous Setting

Next Setting

☐ Not Configured

☒ Enabled

☐ Disabled

Comment:

Supported on:

At least Windows Server 2008 R2 or Windows 7

Options:

☒ Allow data recovery agent

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

☒ Save BitLocker recovery information to AD DS for operating system drives

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

Help:

This policy setting allows you to control how BitLocker-protected operating system drives are recovered in the absence of the required startup key information. This policy setting is applied when you turn on BitLocker.

The "Allow certificate-based data recovery agent" check box is used to specify whether a data recovery agent can be used with BitLocker-protected operating system drives. Before a data recovery agent can be used it must be added from the Public Key Policies item in either the Group Policy Management Console or the Local Group Policy Editor. Consult the BitLocker Drive Encryption Deployment Guide on Microsoft TechNet for more information about adding data recovery agents.

In "Configure user storage of BitLocker recovery information" select whether users are allowed, required, or not allowed to generate a 48-digit recovery password or a 256-bit recovery key.

Select "Omit recovery options from the BitLocker setup wizard" to prevent users from specifying recovery options when they turn on BitLocker on a drive. This means that you will not be able to specify which recovery option to use when you turn on BitLocker, instead BitLocker recovery options for the drive are determined by the policy setting.

OK

Cancel

Apply

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 "gpupdate /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	<a href="mailto:consult@uic.edu">consult@uic.edu</a>
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-acc](#) [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](#) [troubleshooting](#) [u-print](#) [uicalendar](#) [uicast](#) [unix](#) [video](#) [streaming](#) [virtual server](#) [voicemail](#) [voip](#) [vpn](#) [webdisk](#) [webhost](#) [webmail](#) [web publishing](#) [wifi](#) [wiki](#) [windows](#) [wireless](#)

More