How to configure BitLocker (Part 2)

In Part 1 of this series, I showed you how to configure BitLocker and some complex issues to know before you start using this feature.

In this article, I will continue the discussion of BitLocker from an Active Directory perspective and consider configuring TPM and BitLocker with Group Policy and how to perform key recovery.

The problems still exist

We think we need to say BitLocker in an Active Directory environment is probably the most used scenario. By using BitLocker in an Active Directory environment, you can get all the security features from BitLocker combined with all security, availability and scalability issues with Active Directory. But before you start, consider some of the following issues that still exist:

1. Microsoft has not released their BitLocker Deployment Kit yet, so we will not be able to provide you with official links or copy the scripts used in the article.

2. On the other hand we have not yet seen the official BitLocker deployment to be released soon, but the scripts we are using are provided by Microsoft. However, you should note that the names and script numbers given in this article may change when the BitLocker Deployment Kit is officially released.

3. As soon as Microsoft releases the various scripts and articles that are included in this article, the article will be updated with the corresponding links to match its file name. We will let you know when the post is updated.

Conditions decided

Before you begin, let's take a look at some of the conditions that must be met to allow you to control BitLocker from Active Directory.

1. You need to expand the schema in Active Directory
2. If you want to control TPM recovery information from Active Directory, you need to change the permissions on the Computer class object in Active Directory.
3. BitLocker Active Directory schema extensions are only supported on domain controllers that are running Windows Server 2003 SP1 or later, Windows Server 2003 R2 and Windows Server 'Longhorn'
4. BitLocker is only supported to run on Windows Vista Enterprise, Windows Vista Ultimate and Windows 'Longhorn' Server

Note : While the author is writing this article, Service Pack 2 for Windows Server 2003 already has an RTM version. SP2 will not have BitLocker schema updates. You will be able to run the BitLocker schema extension script explained in this article after installing SP2 on the Windows Server 2003 setup.

Necessary scripts

This is when we started, looking at the required files to make BitLocker integrated with an Active Directory on Windows Server 2003. The following files are used for Active Directory Windows Server 2003 support for BitLocker.

1. BitLockerTPMSchemaExtension.ldf
2. Add-TPMSelfWriteACE.vbs

Use the files below to help you verify the BitLocker configuration in Active Directory. We will use one of those files in the following example of this article

1. List-ACEs.vbs
2. Get-BitLockerRecoveryInfo.vbs
3. Get-TPMOwnerInfo.vbs

Expand schema in Active Directory

After verifying prerequisites and verifying scripts, it's time to get ready for extending Active Directory to save TPM and BitLocker recovery information in Active Directory.

The way it works is: BitLocker recovery information is stored in Computer's child object in Active Directory, which means that the Computer object serves as a container for one or more BitLocker restore objects fit with a specific Computer object. The reason why we say that one or more BitLocker recovery objects is because it can have multiple recovery keys associated with a computer using BitLocker, for example if you have encrypted multiple publications on the same computer.