Microsoft® Desktop Optimization Pack for Software Assurance

Using MBAM Data Encryption With MDT

TPM-Only Encryption of New Computers Using the Microsoft Deployment Toolkit (MDT) and Microsoft BitLocker Administration and Monitoring (MBAM)

Technical White Paper

Published: September 2011

Craig Ducharme, William Lees, and Nathan Barnett

Microsoft®

CONTENTS

Situation

Need to deploy Windows 7 and other applications to a new computer with TPM-only encryption using MDT.

Solution

Using MDT, the IT Pro can deploy Windows 7, Office 2010, and other applications, start the encryption process so as to hand the end user a completely encrypted computer and avoid the time-consuming process of encryption

Benefits

- Delivers a secure, compliant computer to the end user
- Simplify the encryption process for the end user
- Tracks compliance of the computer once joined to the domain
- Stores the Recovery Key in the remote database for future recovery by IT Pro

Products & Technologies

- Microsoft Deployment Tool Kit (MDT)
- Asset Inventory Service (AIS)
- Microsoft Desktop Administration and Monitoring (MBAM)

EXECUTIVE SUMMARY

The purpose of this whitepaper is to help customers deploy new computers in their enterprise in a TPM-only encrypted state. Upon receiving the new computer, the end user does not have to go through the TPM activation reboot and the process of encryption. Instead, the user is prompted for a PIN when the new computer joins the domain if a PIN is required by the deployed group policy.

This paper assumes that readers are familiar with BitLocker Drive Encryption, Group Policy, Microsoft Deployment Toolkit, and Windows Domain technologies. For more information about MBAM, see the product documentation at http://go.microsoft.com/fwlink/?LinkId=218349.

INTRODUCTION

BitLocker Drive Encryption (BDE) is a Windows security feature used by enterprise customers to secure their data on corporate assets - particularly portable devices. BitLocker Drive Encryption allows you to encrypt all of the data stored on the Windows operating system volume and configured data volumes (fixed and removable). It also ensures the integrity of early boot components by using a Trusted Platform Module (TPM).

Microsoft BitLocker Administration and Monitoring (MBAM) provides features to manage BitLocker encryption of computers in an enterprise. BitLocker creates recovery information at the time of encryption and MBAM stores that information in the recovery data store. It is desirable but not necessary to store this information at the time of TPM encryption but ultimately this information must be sent upon joining the corporate domain. Recovery information is required to recover BitLocker-protected drives in case an unlock method cannot be used, for example if the TPM cannot validate the boot components, if the personal identification number (PIN) is forgotten, or if the password volume passphrase is forgotten. In these instances, the user must provide a recovery key password to unlock the encrypted data on the drive.

Prior to enabling BitLocker on a computer with a TPM version 1.2, the user must initialize the TPM chip and ownership must be "taken." The initialization process generates a TPM owner password, set on the TPM chip. The user must supply the TPM owner password to change the state of the TPM, such as when enabling or disabling the TPM or resetting after a TPM lockout.

MBAM supports encryption of a computer's operating system hard drive in a fashion referred to as "TPM-only." TPM-only encryption encrypts all data on the drive but does not require user intervention unless the state of the hardware changes. This whitepaper provides guidelines to install the MBAM client via MDT (the Microsoft Deployment Tool for pre-user deployment), set TPM ownership, and finish with the computer in a first-user configuration with the computer in a "TPM-only" encryption state. For more information about configuring BitLocker encryption for MBAM, see "Planning and Configuring Group Policy for MBAM" (http://go.microsoft.com/fwlink/?LinkId=217225).

Another advantage of encryption of an asset prior to end-user receipt is that it protects corporate intellectual property (IP) pre-installed during the MDT phase.

There are three variants of the early-encryption pre-deployment scenarios:

1. Install the MBAM client, activate and own the TPM, encrypt the operating system drive, and save recovery information to the MBAM server prior to end-user receipt of the computer. This variant requires that the computer be domain joined before installing the MBAM client on the computer.
2. Install the MBAM client, activate and own the TPM, encrypt the operating system drive, and save recovery information to the MBAM server using a domain user account that the MBAM server can authenticate against, prior to end-user receipt of the computer. This variant does not require that the computer be domain joined during the first phase of the process and will synchronize the machine data in the MBAM database with the new user at domain joining of the machine.
3. Install the MBAM client, activate and own the TPM, and encrypt the operating system drive, but not save the recovery information before end-user receipt of the computer.

This variation does not require the computer to be domain joined and does not require the MBAM server infrastructure to be accessible. The operating system drive recovery information is saved later during end-user configuration. The TPM recovery information (TPM Hash), however, is never saved because the TPM recovery data becomes inaccessible after initialization. TPM-specific recovery information is rarely used and is unnecessary in most cases. In cases where the recovery information (TPM owner password) is needed, it can be used for gaining access to a machine that has gone into "anti-hammering" (protection against too many failed attempts) mode (although this condition will also clear by itself after a delta of time has elapsed). Another use of this information is to remotely manage the TPM state, which is not widely used at this time.

Note: When the MBAM client agent saves a recovery key to MBAM server, it associates the names of users who have logged-on to the computer, with that key for later recovery purposes. During MDT when the key is saved in cases 1 and 2 above, you may choose whether to have a "logon record" already at the computer or not. The benefit of having a logon record is if a recovery is required before end-user receipt, the username already attached to the key allows a "Tier 1" help desk operator to help a technician recover the computer. Without a "logon record" saved when the machine with the key, the key is associated with an empty list of "interested-party users". In this case, only a "Tier 2" help desk operator could assist a technician to recover the computer.

There are two ways to manage the encryption process delay after the pre-deployment process is complete:

A. The administrator leaves the computer running for a time that is dependent upon the computer and disk (determinable by experimentation) to ensure that encryption is complete. This ensures that the computer is protected during transit, and that the user will not detect system "slowdown" caused by encryption activity.

B. The operator can shut down the computer after the TPM initializes and encryption starts. Encryption resumes when the user starts the computer and completes the final configuration. Depending on the computer, final encryption may be invisible to the user.

1. TPM-ONLY ENCRYPTION PROCESS TO DEPLOY A NEW COMPUTER IN THE ENTERPRISE - DOMAIN JOINED

Encrypt Computer as part of Windows 7 Deployment
MBAM augments the tools your organization uses to deploy a Windows 7 image on new and existing computers. The following steps provide guidelines for the sequence of events necessary encrypt computers using MBAM. More detailed guidance is provided in later sections.

1. Enable the TPM chip. This requires a power down and restart of the computer. This is a manual process managed in the BIOS. Each manufacturer handles TPM setting differently. See product documentation for more details. Sample BIOS settings:

   Set TPM to ENABLED

   Set TPM to ACTIVE

   Set TPM to NOT OWNED

2. Domain-join the computer
3. Install the MBAM agent

4. Stop the MBAM service and set to manual or demand start.

Run cmd as as Administrator.

Type in the following:

```
Net stop mbamagent
```

```
“Sc config mbamagent start= demand”
```

(Note the space between the equal sign and the value.

5. Set the registry settings that allow the MBAM agent to ignore Group Policy and use TPM encryption on the operating system drive only.

   Run RegEdit

   Import the registry key template from “c:\Program Files\Microsoft\MDOP MBAM\MBAMDeploymentKeyTemplate.reg”

   Navigate in the registry to “HKLM\SOFTWARE\Microsoft\MBAM”

   DeploymentTime

   - 0 = OFF
   - **1 = BYPASS (DEFAULT)**

   UseKeyRecoveryService

   - 0 = don’t escrow key (next two aren’t needed in this case)
   - **1 = ESCROW IN KEY RECOVERY SYSTEM (RECOMMENDED – COMPUTER NEEDS TO BE ABLE TO COMMUNICATE WITH KEY RECOVERY SERVICE – VERIFY THIS BEFORE PROCEEDING).**

   KeyRecoveryOptions

   - =0 uploads Recovery Key Only
   - **=1 (DEFAULT) UPLOADS RECOVERY KEY AND KEY RECOVERY PACKAGE**

6. Set URL for Key Recovery WS

   KEYRECOVEYRSERVICEENDPOINT =

   http://<yourserverhere>/MBAMRecoveryAndHardwareService/CoreService.svc

   Note: Any of the MBAM policy/registry values can be placed here for override.

   Example of exported registry setting:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MBAM]
"NoStartupDelay"=dword:00000001
"DeploymentTime"=dword:00000001
"Installed"=dword:00000001
"KeyRecoveryOptions"=dword:00000001
```

"UseKeyRecoveryService"=dword:00000001

"KeyRecoveryServiceEndPoint"=
http://<yourserverhere>/MBAMRecoveryAndHardwareService/CoreService.svc

7. Towards the end of the Windows 7 imaging process, when you are ready to start encryption, restart the service and set to automatic start.

   Launch cmd as 'Run as administrator'

   Type in the following:

   sc config mbamagent start= auto

   net start mbamagent

8. Remove the by-pass registry values.

   Run RegEdit

   Navigate in the registry to "HKLM\SOFTWARE\Microsoft\MBAM"

   Do not delete the key "MBAM" itself.

   Remove all values except the value "Installed".

   Example of cleaned-up registry setting:

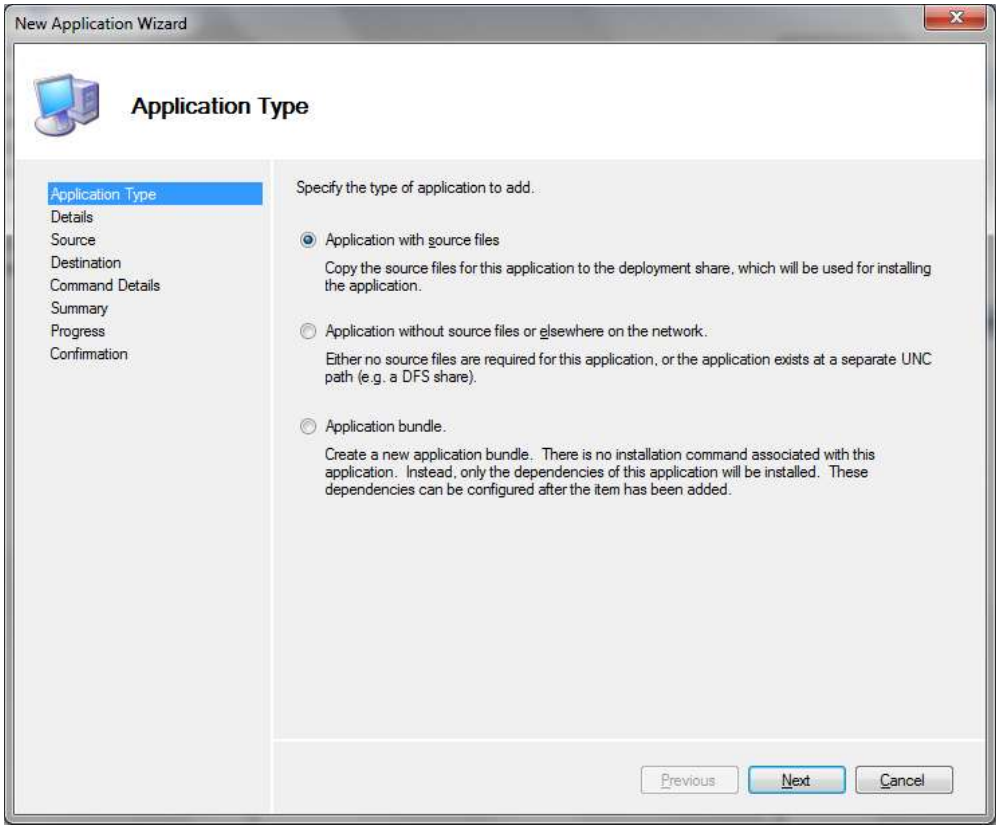
   [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MBAM]

   "Installed"=dword:00000001

2. MDT CUSTOM ACTIONS TO INITIATE TPM-ONLY ENCRYPTION PROCESS - USING DOMAIN USER LOGIN

When using MDT to deploy Windows 7 on new computers in an enterprise you must install the MBAM client, and start the TPM-only encryption process.

1. First, import the MBAM client .MSI file into the MDT Application Installer by right-clicking the Applications folder in the MDT Deployment Share tree structure and running the New Application Wizard.



Specify the type of application to add.

● Application with source files

Copy the source files for this application to the deployment share, which will be used for installing the application.

○ Application without source files or elsewhere on the network.

Either no source files are required for this application, or the application exists at a separate UNC path (e.g. a DFS share).

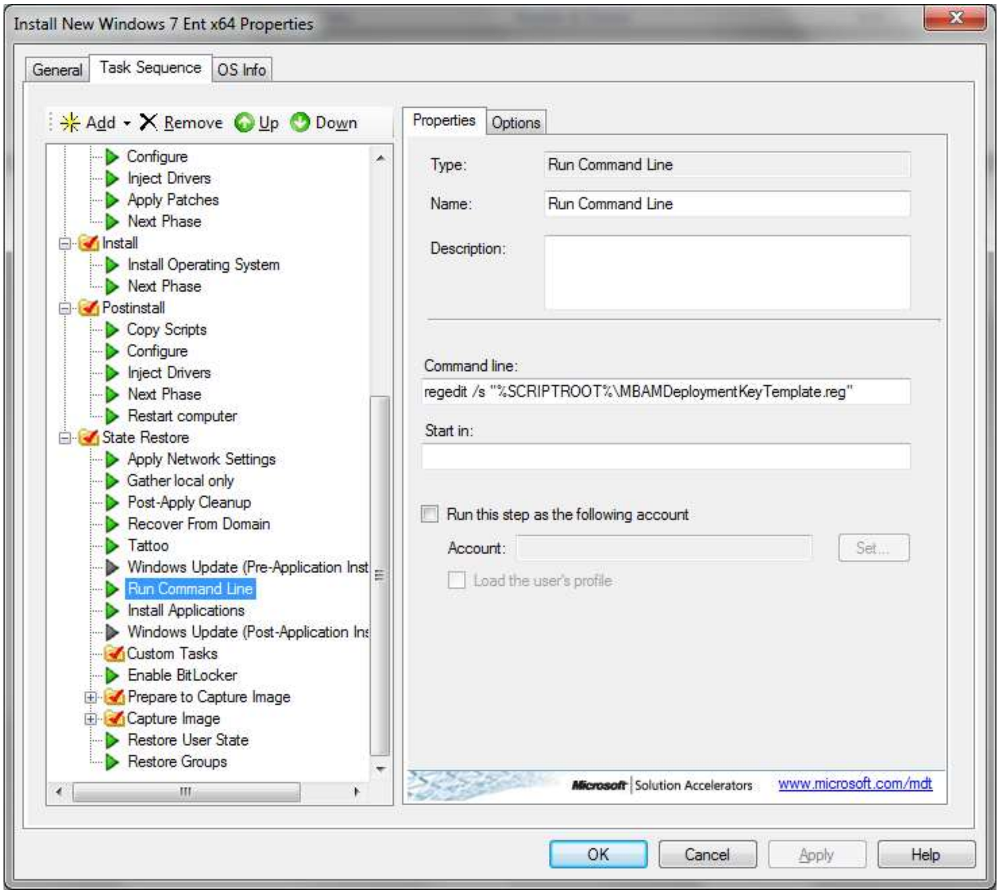
○ Application bundle.

Create a new application bundle. There is no installation command associated with this application. Instead, only the dependencies of this application will be installed. These dependencies can be configured after the item has been added.

2. A registry file is deposited in the client installation directory under "C:\Program Files\Microsoft\MDOP MBAM." Copy this file to the MDT Deployment Share in the Scripts Root Directory and then call it via the custom command as shown below.

   Example:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MBAM]
"KeyRecoveryOptions"=dword:00000001
"UseKeyRecoveryService"=dword:00000001
"KeyRecoveryServiceEndPoint"=
http://<yourserverhere>/MBAMRecoveryAndHardwareService/CoreService.svc
"DeploymentTime"=dword:00000001
```



Type: Run Command Line

Name: Run Command Line

Description:

Command line:

```
regedit /s "%SCRIPTROOT%\MBAMDeploymentKeyTemplate.reg"
```

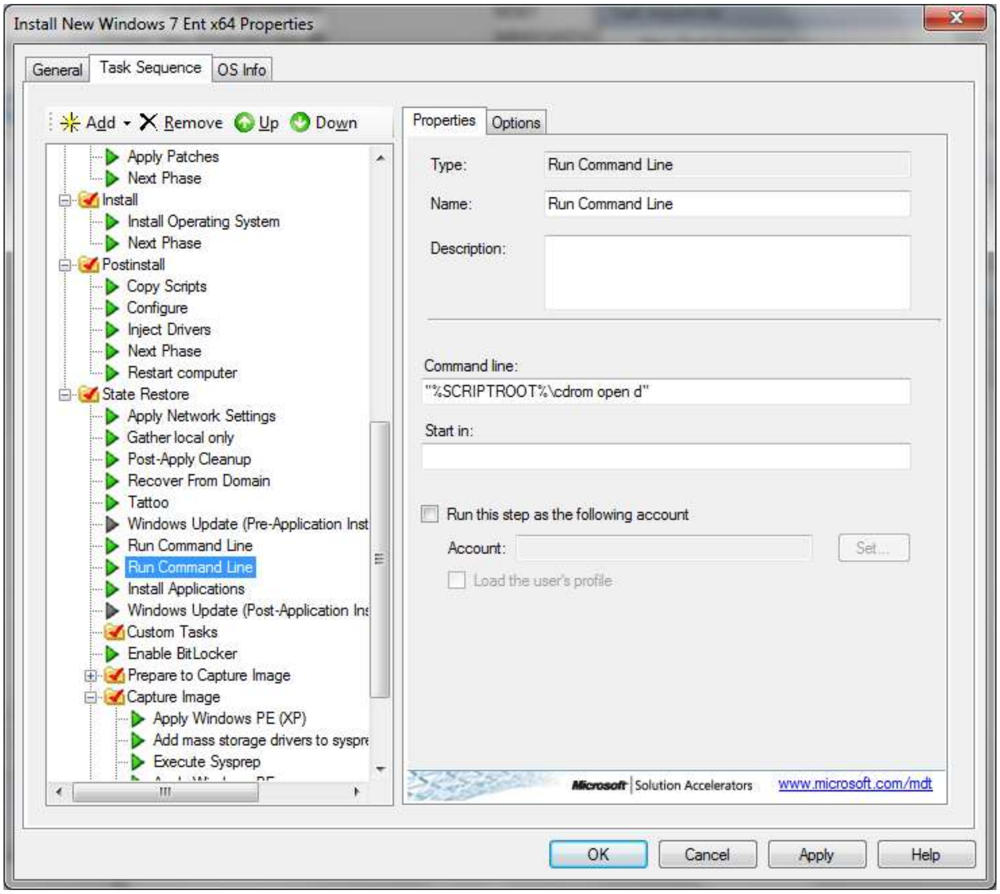
Start in:

□ Run this step as the following account

Account: Set...

□ Load the user's profile

Important: *Eject the CD-ROM before the MBAM Service starts. BitLocker cannot start the encryption process with a disk in the drive. In a custom run command below, a script ejects the CD or DVD.*



Type: Run Command Line

Name: Run Command Line

Description:

Command line: "%SCRIPTROOT%\cdrom open d"

Start in:

□ Run this step as the following account

Account: Set...

□ Load the user's profile

3. After the service has started BitLocker and the encryption process has begun, you must remove the registry keys imported earlier in the process. This can be done by running regedit on the registry file with a minus sign added to the keys that were imported.

   Example:

   Windows Registry Editor Version 5.00

   [-HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MBAM]

   "KeyRecoveryOptions"=dword:00000001

   "UseKeyRecoveryService"=dword:00000001

   "KeyRecoveryServiceEndPoint"= http://<yourserverhere>/MBAMRecoveryAndHardwareService/CoreService.svc

   "DeploymentTime"=dword:00000001

Note: A "KeyRecoveryServiceEndPoint" must be custom edited in the imported .reg file. As long as the user account used during the MDT login process exists with the correct permissions for both the MDT deployment share and is a Domain User known to MBAM, then the recovery package with the TPM owner password will be pushed to the MBAM Service and be stored in the Recovery Key Database associated to a Machine ID.

Note for Example 3: If an endpoint is not provided or the user account used at MDT login is not known to MBAM, such as a local administrator account, then the TPM-Only encryption process will start but the TPM recovery information will not be sent to the MBAM recovery database. When the computer is given to the end user and joins the enterprise domain, the computer will receive MBAM group policy. The MBAM client can be silently updated if necessary, and the user can be prompted to create a PIN. From the end user perspective, adding the PIN will take seconds instead of hours because the operating system drive is already encrypted.

FOR MORE INFORMATION

For more information about Microsoft products or services, call the Microsoft Sales Information Center at (800) 426-9400. In Canada, call the Microsoft Canada information Centre at (800) 563-9048. Outside the 50 United States and Canada, please contact your local Microsoft subsidiary. To access information through the World Wide Web, go to:

http://www.microsoft.com

http://www.microsoft.com/technet/itshowcase