Microsoft®
Desktop Optimization Pack
for Software Assurance

Microsoft BitLocker Administration and Monitoring Evaluation Guide

Technical White Paper

Published: August 2011

By Anthony Smith and Jeff Gilbert

CONTENTS

Situation

MBAM can help any organization better provision, monitor, and support BitLocker.

Solution

At all stages, MBAM can help protect recovery data by encrypting network communication and the database, limiting access to recovery data, and supporting single-use recovery keys. MBAM also provide reports which help you how compliant your organization is with your defined BitLocker encryption policies

To learn more about how MBAM and MDOP for Software Assurance can help you better provision, monitor, and support BitLocker, see http://go.microsoft.com/fwlink/?LinkId=160297.

Benefits

Provisioning

- Configure and enforce BitLocker policies centrally by using Group Policy.
- Provision BitLocker during or after Windows 7 deployment.
- Manage a list of models that are exempt from encryption.

Monitoring

- Review the compliance status of the entire business
- Quickly see the compliance status of a single PC or a specific user's PCs
- Audit access to recovery data and changes to the Hardware Compatibility List.

Supporting

- Standard user accounts can perform basic operations without calling the help desk.
- MBAM provides tools that the help desk can use to help users recover locked drives and manage their Trusted Platform Module (TPM) microchips that are built into computers.

Products & Technologies

- Microsoft BitLocker Administration and Monitoring
- Microsoft Windows Group Policy
- Windows Server 2008 or Windows Server 2008 R2
- Microsoft SQL Server

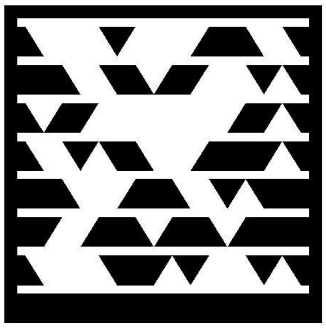
EXECUTIVE SUMMARY

Microsoft BitLocker Administration and Monitoring (MBAM) provides an administrative interface to manage BitLocker drive encryption. MBAM allows you to select BitLocker encryption policy options appropriate to your enterprise, monitor client compliance with those policies, report on the encryption status of the enterprise as well as individual computers, and recover lost encryption keys.

This white paper provides a technical overview of Microsoft BitLocker Administration and Monitoring (MBAM), part of the Microsoft Desktop Optimization Pack (MDOP). It offers an architectural overview of the infrastructure, describes how you provision BitLocker by using MBAM, and introduces the key features that can help you monitor compliance and reduce support costs. The intended audience for this white paper is MBAM administrators and technical personnel. This paper assumes that readers are already familiar with BitLocker and Group Policy administration. Each enterprise environment has unique circumstances; therefore, each organization should adapt the information described in this paper to meet its specific needs.

Note: *For security reasons, the sample names of forests, domains, internal resources, organizations, and internally developed security file names used in this paper do not represent real resource names used within Microsoft and are for illustration purposes only.*

Microsoft Tag 2D barcode symbols, like the one shown here, appear throughout this guide and let you connect to supplemental material online using a mobile phone.



For example, you can use a tag reader application installed on your mobile phone to scan this Microsoft Tag (or go to http://go.microsoft.com/fwlink/?LinkId=224780) to connect to the download page for this white paper.

Note: *To get the Tag Reader, visit http://gettag.mobi on your mobile phone browser. Or, visit http://tag.microsoft.com/consumer/index.aspx to send a text message to your phone with a link to the application.*

Microsoft Tag is also available for free in most mobile application stores; just search for 'Tag Reader' to get started.

INTRODUCTION

"We can use MBAM to get greater value from BitLocker. We can ensure that BitLocker is enabled and that we are compliant with corporate encryption mandates without taxing our employees or IT staff."

Bob Johnson
Director of IT
BT in the United States and Canada

Microsoft BitLocker Administration and Management (MBAM) can be used to provision BitLocker Drive Encryption throughout the enterprise. BitLocker Drive Encryption is a Windows 7 Enterprise and Ultimate feature that can help secure corporate and end user data on desktop and laptop PCs. It provides full-volume drive encryption for operating-system, fixed, and removable drives to help prevent offline attacks (e.g., mounting a drive to a second PC to gain access to its data). BitLocker also protects the operating-system startup files from tampering.

> **Note:** *You can learn more about BitLocker in the Springboard Series (http://www.microsoft.com/springboard/) on TechNet.*

This white paper will refer often to a scenario involving Contoso, Ltd. when describing the MBAM infrastructure; and its provisioning, monitoring, and support features. In this scenario, Contoso is rolling out Windows 7 Enterprise with BitLocker. Contoso investigated provisioning BitLocker by using System Center Configuration Manager 2007 and the Microsoft Deployment Toolkit (MDT) 2010; however, the tools available did not meet their requirements:

- Contoso needed a way to provision BitLocker using the Trusted Platform Module (TPM) plus a PIN to standard user accounts. Although existing tools can provision BitLocker with a PIN, they provision the same PIN to all PCs, and standard user accounts cannot change their PINs.
- Contoso required compliance reporting, which BitLocker alone does not provide. Additionally, Contoso needed a way to quickly identify risk in the event of a lost or stolen PC.
- Contoso wanted to better protect and secure recovery data. The company did not want to store recovery data in Active Directory, and it wanted to limit access to authorized users only. Last, Contoso wanted recovery keys to expire after a single use to ensure that they could not be misused.
- Contoso needed a way to streamline BitLocker support by quickly restoring users to work if they were locked out of their drives. It also wanted to enable users to perform basic operations, such as changing their PINs, without calling support.

In a time when Microsoft strongly recommends deploying standard user accounts rather than administrator accounts, having an enterprise solution for provisioning BitLocker before and after rolling out Windows 7 Enterprise is essential. That solution is MBAM, and Contoso chose to use it for the following reasons:

- Simplified Provisioning and Deployment. MBAM enables Contoso to provision BitLocker during or after a Windows 7 Enterprise deployment even when deploying standard user accounts. When Contoso provisions BitLocker as part of a rollout, MBAM will prompt users to change their PINs. If Contoso provisions BitLocker after deployment, MBAM will guide the user through the encryption process and prompt for PINs.
- Improved Compliance and Reporting. MBAM helps Contoso monitor compliance with BitLocker policy by providing enterprise and computer compliance reports. At a glance, Contoso can determine the compliance level of the entire organization or quickly check whether a specific PC is or a specific user's PCs are compliant. For example, if users

lose their PCs, Contoso can quickly determine the organization's risk by looking up their PCs in MBAM.

- Reduced Support Costs. MBAM helps reduce support costs for Contoso in two ways. First, it helps users perform basic operations without calling the help desk. For example, they can reset their PIN or encrypt a drive. Second, when users are locked out of their drives, the help desk can quickly look up the drives' recovery keys in MBAM. The security of recovery keys is very important, so MBAM protects recovery data at every step.

MBAM COMPONENTS

The best way to understand how MBAM works is to first understand its components, and then understand how those components work together. The following sections describe each of the components that comprise MBAM.

Administration and Monitoring Server

This server hosts the Management Console and service endpoints. Install this component on a server running Windows Server 2008 or Windows Server 2008 R2. This server requires the Web Server role with the role services and additional Windows features that Table 1 describes:

Table 1. Required Role Services and Windows Server Features

Category	Features
Web Server Role Services	
Common HTTP features	Static content Default document
Application development	ASP .NET .Net extensibility ISAPI extensions ISAPI filters
Security	Windows Authentication Request Filtering
Server Role Services	
.NET Framework 3.5.1 features	.NET Framework 3.5.1 WCF activation HTTP activation
Windows process activation service	Process model .NET environment Configuration APIs

MBAM administrators log on to the Management Console from a management workstation to view reports, audit activity, manage hardware compatibility, and access recovery data. The Administration and Monitoring Server connects to the following databases and services:

- Compliance and Audit Database. This Microsoft SQL Server database stores compliance data for PCs running the MBAM client. Additionally, it stores audit data for changes to the Hardware Compatibility list feature that you can use to exclude PCs from encryption by make and model, and drive recovery activity. Install this component on a server running Windows Server 2008 or Windows Server 2008 R2. It requires Microsoft SQL Server 2008 R2 Standard, Enterprise, Datacenter, or Developer edition with the SQL Server Database Engine Services feature running.
- Recovery and Hardware Database. This SQL Server database stores recovery data that the MBAM client gathers when encrypting drives. Additionally, it stores the Hardware

Compatibility list. Install this database component on a server running Windows Server 2008 or Windows Server 2008 R2. It requires Microsoft SQL Server 2008 R2 Enterprise, Datacenter, or Developer edition with the SQL Server Database Engine Services feature running.

- Compliance and Audit Reports. MBAM uses Microsoft SQL Server Reporting Services (SSRS) to provide MBAM reports. Install this component on a server running Windows Server 2008 or Windows Server 2008 R2. It requires Microsoft SQL Server 2008 R2 Standard, Enterprise, Datacenter, or Developer edition with the SSRS feature running. MBAM users can access MBAM reports directly from this server by using SSRS or through the Administration and Monitoring Server.

Policy Templates

The Group Policy administrative templates define the Group Policy settings that MBAM supports. You can install the template on each management workstation, or you can copy it to your Group Policy Central Store (http://support.microsoft.com/kb/929841).

Management Workstations

Management workstations are PCs from which MBAM users (e.g., help desk) log on to the MBAM Management Console (a web page hosted on the Administration and Monitoring Server) by using their web browser. Additionally, you can install the MBAM policy template and add the Group Policy Management Console (GPMC) feature from the Remote Server Administration Tools (RSAT) (http://go.microsoft.com/fwlink/?LinkId=225009) to management workstations that MBAM administrators will use to configure Group Policy.

MBAM Clients

The MBAM client software is used to enforce MBAM policies on users computers. It performs operations on behalf of users, so they can encrypt their drives and change their PINs with standard user accounts. The client also gathers recovery data for encrypted drives and reports compliance data to MBAM.

MBAM Deployment and Configuration

The MBAM Administrator's Guide on the web on the MDOP documentation home page (http://onlinehelp.microsoft.com/mdop) describes the system requirements, prerequisites, and installation of each component. The following sections describe how the components work together to provide a holistic solution for managing BitLocker Drive Encryption.

Choosing a Server Topology

You can install all of the MBAM components on a single computer. However, Microsoft doesn't recommend a single-computer topology for anything but testing purposes. Instead, it is recommended that you deploy a three-computer (Figure 1) or five-computer (Figure 2) topology on physical or virtual servers for MBAM. Contoso has about 1,500 desktop and laptop PCs, and it chose to deploy the three-computer topology that Figure 1 shows.

Three Computer Topology

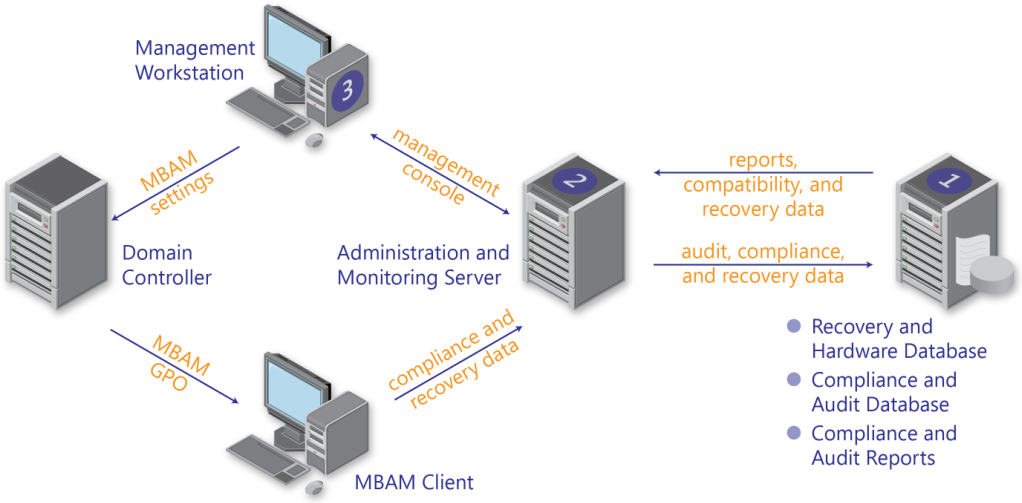


Figure 1. Three Computer Topology

The three-computer topology that Figure 1 illustrates has the following computers:

1. **Database and Report Server.** This server contains all of the MBAM databases and provides MBAM reports. Clients do not connect directly to these databases; instead, clients return data to the Administration and Monitoring Server, which stores the data in the database. MBAM users can open reports directly from SSRS on this server, or they can open reports from the Administration and Monitoring Server. MBAM encrypts the Recovery and Hardware Database by using transparent data encryption (TDE) in SQL Server.

2. **Administration and Monitoring Server.** MBAM clients report their compliance status to the Administration and Monitoring Server, which stores the information in the Compliance and Audit Database. Additionally, when the MBAM client encrypts a drive, it returns the recovery data to the Administration and Monitoring Server so that it can store the recovery data in the Recovery and Hardware Database. The Administration and

Monitoring Server generates audit information that it stores in the Compliance and Audit Database. MBAM users can access reports through this server.

3. **Management Workstation.** The management workstation is the computer from which MBAM users connect to the Management Console on the Administration and Monitoring Server. They can also configure GPOs containing MBAM policies by using the policy template from the management workstation.

Five Computer Topology

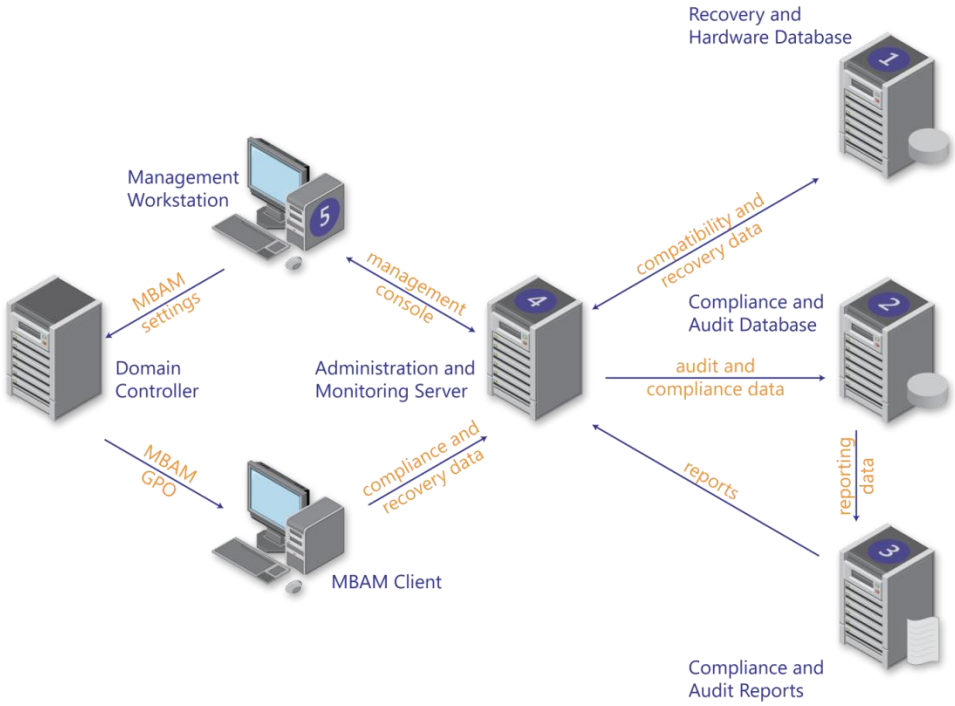


Figure 2. Five Computer Topology

The five-computer topology that Figure 2 illustrates includes the following computers:

1. **Recovery and Hardware Database.** This server contains the Recovery and Hardware Database, which MBAM encrypts by using Transparent Data Encryption (TDE) in SQL Server. The MBAM client does not connect directly to this database; instead, the client returns recovery data to the Administration and Monitoring Server, which writes it to the database.

2. **Compliance and Audit Database.** This server contains the Compliance and Audit Database. The MBAM client does not connect directly to this database; rather, it reports compliance data to the Administration and Monitoring Server, which stores it in the database. Additionally, the Administration and Monitoring Server generates audit information, which it stores here.

3. **Compliance and Audit Reports.** This server hosts SSRS and generates MBAM reports. MBAM users can open reports directly from SSRS on this server, or they can open reports from the Administration and Monitoring Server.

4. **Administration and Monitoring Server.** MBAM clients report their compliance status to the Administration and Monitoring Server, which stores the information in the Compliance and Audit Database. Additionally, when the MBAM client encrypts a drive, it returns the recovery data to the Administration and Monitoring Server so that it can store the recovery data in the Recovery and Hardware Database. The Administration and Monitoring Server generates audit information that it stores in the Compliance and Audit Database. MBAM users can access reports through this server.
5. **Management Workstation.** The management workstation is the computer from which MBAM users connect to the Management Console on the Administration and Monitoring Server. They also configure GPOs containing MBAM policies by using the policy template.

Use a tag reader application installed on your mobile phone to scan this Microsoft Tag (or go to http://go.microsoft.com/fwlink/?LinkId=224777) to view an overview video about MBAM deployment and architecture:

Configuring MBAM Administrator Roles

Similar to Advanced Group Policy Management (AGPM) (http://go.microsoft.com/fwlink/?LinkId=225010) in MDOP, MBAM supports role-based delegation. Table 2 describes the roles that MBAM supports. MBAM defines each role as a local security group on the server indicated in the table. For example, MBAM creates a local security group called MBAM Helpdesk Users on the Administration and Monitoring Server. To delegate each role, you add users or groups to each role's local security group.

Table 2. MBAM Roles

Role	Local security group host server	Features
MBAM System Administrators	Administration and Monitoring Server	All MBAM features
MBAM Hardware Users	Administration and Monitoring Server	Hardware Compatibility
MBAM Helpdesk Users	Administration and Monitoring Server	Help desk features
MBAM Report Users	Administration and Monitoring Server Compliance and Audit Reports Server Compliance and Audit Database Server	Compliance and audit reports
MBAM Advanced Helpdesk Users	Administration and Monitoring Server	Increased access to help desk features

Microsoft recommends that you manage each role by creating security groups in Active Directory and adding those groups to the corresponding local security group. In Figure 3, you see the local security group named MBAM Helpdesk Users. Contoso has created a domain security group by the same name, and has added that to the local security group. Contoso can now manage MBAM roles in Active Directory.

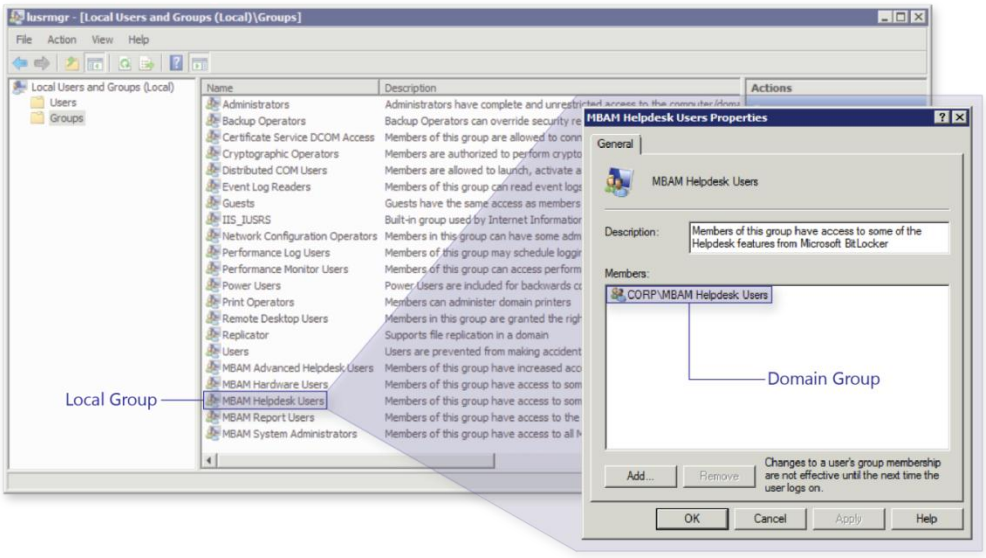


Figure 3. MBAM Local Security Groups

Securing Recovery Data

One of the key MBAM features is security. MBAM helps protects confidential data on laptop and desktop PCs by protecting the recovery data required to unlock drives:

- MBAM can store recovery data in an encrypted database—not in plain text.
- MBAM limits access to recovery data to authorized users only (defined by MBAM roles).
- MBAM supports single-use recovery keys. The MBAM client generates a new recovery key after unlocking a drive. Single-use recovery keys can help prevent their misuse.
- MBAM can encrypt network communication between the management console and the Administration and Monitoring Server; and between the Administration and Monitoring Server and the databases.

Encrypting network communication and recovery data in the database requires using SQL Server 2008 R2 Enterprise, Datacenter, or Developer edition. You enable encryption during MBAM installation.

Use a tag reader application installed on your mobile phone to scan this Microsoft Tag (or go to http://go.microsoft.com/fwlink/?LinkId=224778) to view a video about deploying the MBAM agent with System Center Configuration Manager 2007:

Deploying the MBAM Client to Existing Computers

The client is the centerpiece of MBAM. It enforces MBAM policies on PCs, and it reports compliance status to the Administration and Monitoring Server. You deploy the MBAM client to each PC running Windows 7 Enterprise or Windows 7 Ultimate on which you want to manage BitLocker.

The MBAM client is installed using a standard Windows Installer (.msi) file that you can deploy using any electronic software distribution (ESD) or operating-system deployment technology. Technologies that are available from Microsoft include (see http://www.microsoft.com/deployment):

- **System Center Configuration Manager 2007.** By using Configuration Manager, you can advertise the client to existing PCs, and you can install it during operating system deployment.
- **System Center Essentials 2010.** You can use Essentials to advertise the client to existing PCs.

Note: *Configuration Manager and Essentials allow you to target advertisements. For example, you can target the MBAM client to specific departments or types of PCs. Microsoft recommends that you install the MBAM client on all PCs on which you want to manage BitLocker, rather than targeting an advertisement. Installing the client on all PCs provides a more complete picture of enterprise compliance with MBAM policy. You can exempt users and PCs from encryption, as the section titled "Managing User and PC Exemptions" describes, and see their exempted status in the Management Console.*

- **Group Policy Software Installation.** You can deploy the MBAM client by using Group Policy Software Installation. For more information, see Editing Software Settings (http://go.microsoft.com/fwlink/?LinkId=225011).

Use a tag reader application installed on your mobile phone to scan this Microsoft Tag (or go to http://go.microsoft.com/fwlink/?LinkId=224776) to view a video about deploying the MBAM agent with Group Policy:

You can also use MDT 2010 to install the MBAM client during operating-system deployment. For example, you can use MDT 2010 to upgrade a PC that is already sitting on a user's desk to Windows 7 and install the MBAM client. It will prompt the user to encrypt the operating-system drive if required.

Contoso is using MDT 2010 to deploy the 64-bit version of Windows 7 Enterprise to PCs running an earlier Windows version and wants to deploy the MBAM client at the same time. Therefore, the company chose to deploy the MBAM client with the operating system.

Contoso first added the MBAM client to the deployment share as an application that installs silently. The installation command was simply **msiexec.exe /i MBAMClient-64bit.msi /q**. Then, Contoso added the application to its Windows 7 task sequence, as Figure 4 shows.

Use a tag reader application installed on your mobile phone to scan this Microsoft Tag (or go to http://go.microsoft.com/fwlink/?LinkId=224779) to view a video about deploying the MBAM agent with the Microsoft Deployment Toolkit:

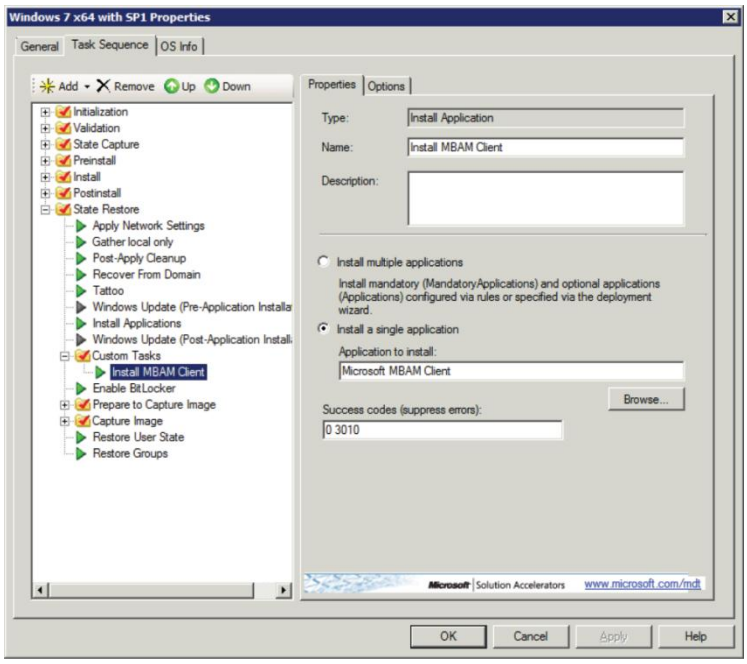


Figure 4. MBAM Deployment in an MDT 2010 Task Sequence

Deploying the MBAM Client With New Operating Systems

In addition to deploying the MBAM client to PCs that are already on users' desks by using ESD and operating-system deployment technology, you can install an operating-system image and the MBAM client on new PCs and encrypt their operating-system drives before delivering them to users (i.e., bench deployment). The benefit is that you know each PC is compliant before delivery because this process does not rely on the user to encrypt the drive.

This process is completed in two phases. First, an administrator encrypts the operating-system drive with the TPM protector prior to delivering the PC to the user. After the user logs on to the PC, the MBAM client prompts the user to provide a PIN.

You can use this two-phased deployment method not only for bench deployments but also when reimaging PCs that you have already delivered. This is useful when you want to ensure encryption of the operating-system drive without relying on the user to start the process. For more information about the steps required to encrypt PCs before delivering them to users, see the MBAM Administrator's Guide on the web on the MDOP documentation home page (http://onlinehelp.microsoft.com/mdop).

Configuring the MBAM Client

You configure the MBAM client by using Group Policy. After adding the GPMC feature from RSAT and installing the MBAM Policy Template component on a management workstation, you can create and configure a GPO containing MBAM policy settings. Of course, you must have permission to create and edit GPOs in the domain.

> **Note:** *AGPM is a terrific complement to MBAM. AGPM supports role-based delegation. Therefore, you can delegate permission to edit GPOs for MBAM to MBAM administrators without giving them permission to edit other GPOs in the domain. In fact, you can delegate roles in AGPM to the same security groups that you created for MBAM. For more information about AGPM, see Enhancing Group Policy (http://go.microsoft.com/fwlink/?LinkId=225012). If you are managing Group Policy by using AGPM, then you must also install and configure the AGPM client on each management workstation.*

You can use security and WMI filtering to target GPOs containing MBAM policy settings. For example, you can exclude specific security groups or types of PCs from the GPO. By using security and WMI filtering, you can deploy multiple MBAM configurations. If you do use security or WMI filtering to target MBAM policy settings, take care that you maintain 100 percent coverage of the PCs running the MBAM client; MBAM clients not configured by Group Policy will not report their status to the Administration and Monitoring Server, leaving you with an incomplete picture of enterprise compliance.

Configuring Group Policy Settings

Within the Group Policy Management Editor (GPME), the MBAM policy settings are in:

- Computer Configuration\Policies\Administrative Templates\Windows Components\MDOP MBAM (BitLocker Management)
- User Configuration\Policies\Administrative Templates\Windows Components\MDOP MBAM (BitLocker Management)

The majority of MBAM policy settings are in the Computer Configuration folder, whereas the User Configuration folder contains a setting to exempt users from encryption. For more information about exemptions, see the section titled “Managing User and PC Exemptions.”

Table 3 describes the policy settings in the MBAM policy template. Contoso required a basic MBAM implementation that configured the MBAM service endpoints, required encryption of the operating-system drive, allowed users to request exemption, enabled hardware compatibility checking, and gathered recovery data for fixed and removable drives. In Table 3, the policy settings that Microsoft recommends for a basic configuration like this are set in bold.

Table 3. MBAM Policy Settings

Location	Policy Settings
Global Settings	Choose drive encryption method and cipher strength Prevent memory overwrite on restart Validate smart card certificate usage rule compliance Provide the unique identifier for your organization
Client Management	**Configure MBAM services** **Allow hardware compatibility checking** **Configure user exemption policy**
Fixed Drive	**Fixed data drive encryption settings** Deny write access to fixed drives not protected by BitLocker Allow access to BitLocker-protected fixed data drive from earlier versions of Windows Configure use of password for fixed data drives Choose how BitLocker-protected fixed drives can be recovered
Operating System Drive	**Operating system drive encryption settings** Configure TPM platform validation profile Choose how BitLocker-protected operating system drives can be recovered
Removable Drive	**Control use of BitLocker on removable drives** Deny write access to removable drives not protected by BitLocker Allow access to BitLocker-protected removable data drive from earlier versions of Windows Configure use of password for removable data drives Choose how BitLocker-protected removable drives can be recovered

Figure 5 shows the Operating System Drive Encryption Settings policy locations and properties in the Group Policy Management Editor.

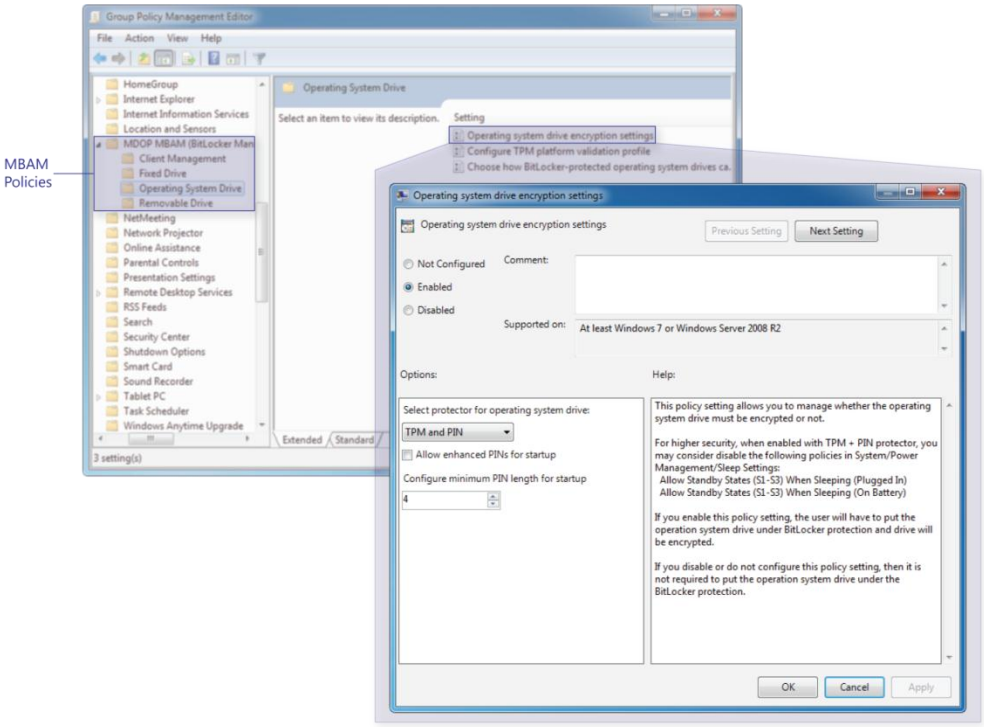


Figure 5. MBAM Group Policy Settings

Using Administrative Templates

When you install the MBAM Policy Template component on a management workstation, MBAM Setup installs two policy template files to the **PolicyDefinitions** subfolder of %SYSTEMROOT%:

- **BitLockerManagement.admx**. Defines policy settings in the Computer Configuration folder.
- **BitLockerUserManagement.admx**. Defines policy settings in the User Configuration folder.

Additionally, MBAM Setup copies matching language files to the appropriate language subfolder in the PolicyDefinitions folder. For example, it copies language files for a U.S. English installation to the folder en-US under PolicyDefinitions.

Users who log on to a management workstation, and have authority to edit Group Policy, can edit MBAM policy settings. However, other administrators using computers on which you have not installed the MBAM policy template will not see the MBAM policy settings.

To make these settings available to all Group Policy administrators without requiring them to install the MBAM Policy Template component, copy the policy template files to the Group Policy Central Store. Using a Central Store has the added benefit of ensuring that all Group Policy administrators are editing GPOs by using the same set of policy templates.

If you do not yet have a Group Policy Central Store, see Group Policy Central Store (http://support.microsoft.com/kb/929841). To add the MBAM policy templates to the Central Store, you simply copy the two .admx files to it. You must also copy the two .adml files from each language folder to the corresponding language folder in the central store. Figure 6 shows an example. In this case, Contoso has copied the policy template (.admx) files to the

PolicyDefinitions folder on SYSVOL. The company also copied the language (.adml) files to the subfolder named en-US. As a result, all of the Group Policy administrators can edit MBAM policy settings without installing the MBAM Policy Template component on their management workstations.

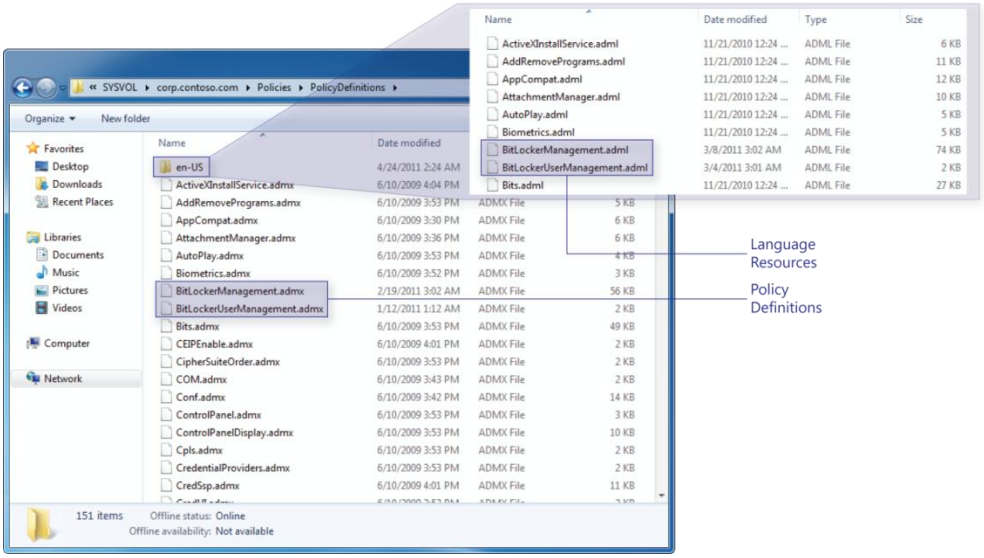


Figure 6. MBAM Policy Templates in the Central Store

Interacting with the MBAM Client

Contoso has almost finished deploying MBAM throughout the organization. It deployed a three-computer topology and the MBAM client to its PCs during a Windows 7 rollout by using MDT 2010. It also configured the MBAM client by using Group Policy. While Contoso intends to provision BitLocker before delivering new PCs to users (see the section titled “Deploying the MBAM Client Before Delivery”), the company must monitor and support users with existing PCs.

This section illustrates one of the primary ways that MBAM helps reduce BitLocker support costs. Users do not have to be administrators to encrypt drives. Even with standard user accounts, they can encrypt fixed and removable drives. They can even perform basic tasks, such as resetting their BitLocker PINs.

When MBAM policy requires encryption of a PC’s operating-system drive, it prompts users to begin the process, as Figure 7 shows. They have three choices:

- Click **Request Exemption** to request exemption from encryption. MBAM will provide the user a link for sending an email, opening a web page, or displaying a custom message to request an exemption. See the section titled “Managing User and PC Exemptions” for more information.
- Click **Postpone** to postpone encryption. You can use Group Policy to configure the maximum period of time that users can continue postponing encryption.
- Click **Start** to begin the encryption process immediately. The MBAM client first takes ownership of the TPM and reboots the PC, if necessary, and then prompts the user for a PIN. The user can continue working as encryption progresses.

Figure 7. MBAM Client User Interface

Once encryption is complete, users can still use the MBAM client to perform basic operations. For example, they can encrypt removable drives or manage their PINs. Figure 8 shows how the MBAM client user interface is represented in Windows Explorer. Users simply right-click a drive in Windows Explorer and click **BitLocker Encryption Options**.

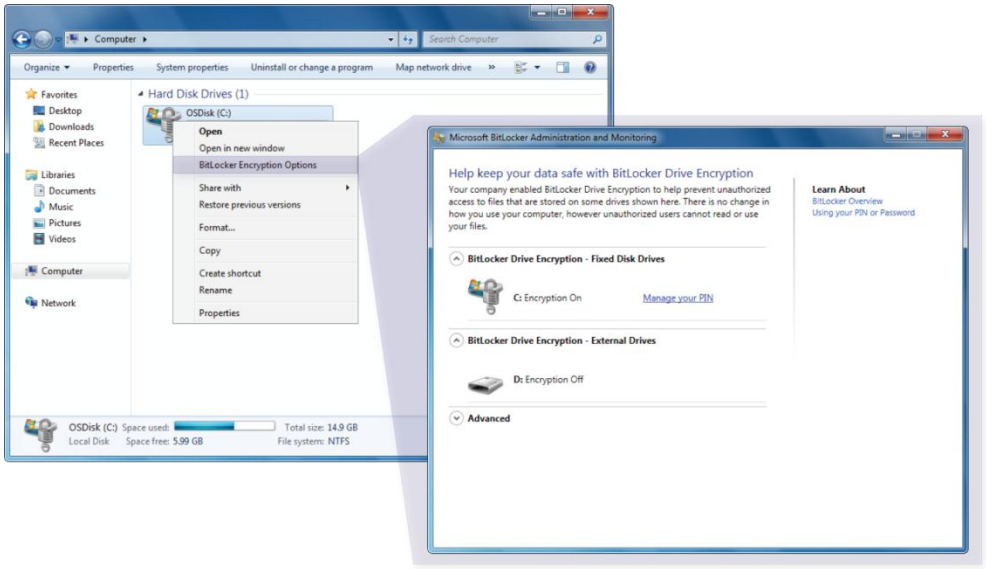


Figure 8. MBAM Integration with Windows Explorer

Managing User and PC Exemptions

If you enable the Configure User Exemption Policy setting, as Contoso did, users can request exemption from BitLocker policy. When they click Request Exemption, as described in the section titled “Interacting with the MBAM Client,” MBAM helps the user request an exemption from BitLocker encryption by using the method configured in the GPO that contains MBAM policy settings.

After reviewing the request, administrators can respond in one of three ways:

- **Deny the exemption.** You do not have to do anything to deny the exemption. The MBAM client will continue prompting the user to encrypt the operating-system drive.
- **Grant the exemption to the PC.** Exempting the PC prevents the MBAM client from encrypting the PC’s operating-system drive, regardless of which users log on to it. You grant a PC exemption by using security filtering to prevent the GPO that contains MBAM policy settings from applying to it. Create a security group in Active Directory that will contain the names of computer accounts that are exempt from encryption. Then, add that security group to the GPO’s access control list (ACL) and set the Apply Group Policy permission to Deny.
- **Grant the exemption to the user.** Exempting the user prevents the MBAM client from encrypting the operating-system drive on any PC that the user logs on to. You exempt a user by creating a GPO with the Allow The User To Be Exempted From BitLocker Encryption policy setting enabled. Then, create a security group in Active Directory that will contain the names of user accounts that are exempt from encryption, and configure the GPO’s security filtering so that it applies only to that security group.

Note: *The MBAM client will not decrypt a drive that is already encrypted by using BitLocker. Therefore, if you exempt a user from encryption, and the user logs on to a PC with an encrypted operating-system drive, the MBAM client will not decrypt the drive.*

Managing Hardware Compatibility

MBAM allows you to exclude PCs from BitLocker policy based on their make and model by using the Hardware Compatibility management feature. If you know that all of the PCs in your organization are compatible with BitLocker (see BitLocker Drive Encryption Overview, http://go.microsoft.com/fwlink/?LinkId=225013), you can deploy MBAM without using the Hardware Compatibility management feature.

To turn on the Hardware Compatibility management feature, you must enable the Allow Hardware Compatibility Checking policy in the GPO that contains MBAM policy settings. When MBAM finds a new PC model, MBAM sets its hardware compatibility status to Unknown. The MBAM client will exempt PCs with an Unknown hardware compatibility status from encryption. To manage each model’s hardware compatibility status, you use the Management Console.

Thus far in the Contoso Windows 7 deployment, MBAM has recorded only three PC models. The administrator logged on to the Management Console to manage the Hardware Compatibility list. As Figure 9 shows, the administrator set the status of one model to Compatible and two others to Incompatible:

- Compatible. Setting a model to Compatible indicates that it supports BitLocker encryption. The MBAM client will enforce MBAM policies on this model of PC.

- Incompatible. Setting a model to Incompatible indicates that it is not compatible with BitLocker or the organization does not support encryption on this model. The MBAM client will not enforce MBAM policies on this model of PC. Additionally, compliance reports will indicate that PCs of this model are hardware exempt.

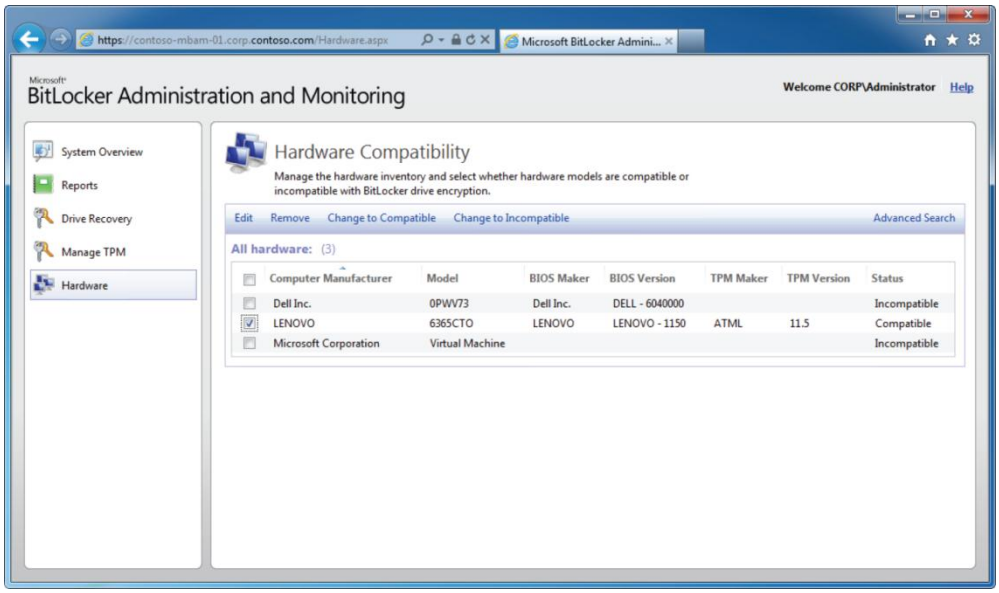


Figure 9. MBAM Hardware Compatibility

The MBAM client checks the Hardware Compatibility list periodically. You should also check the Hardware Compatibility list periodically to review any additional PC models that the MBAM client discovers and set their hardware compatibility status from Unknown to Compatible or Incompatible.

Displaying MBAM Reports

With MBAM fully deployed and the organization's PCs provisioned with BitLocker, Contoso can now move to an operating phase in which it monitors compliance and supports users. MBAM provides a variety of reports that can help Contoso:

- Understand the compliance of the entire organization
- Understand the compliance of a single PC or users' PCs
- Audit access to recovery data
- Audit changes to the Hardware Compatibility list

Note: *You can also create custom reports for MBAM by using the tools built into SSRS.*

Enterprise Compliance Report

MBAM considers a PC compliant when the status of encryption on the PC matches the requirements of the MBAM policy settings deployed to it—or the PC is hardware exempt. Otherwise, the PC is considered non-compliant.

MBAM provides the Enterprise Compliance Report to indicate which PCs are compliant and which are not. The top portion of the report provides an overview of the organization's compliance status, showing the number of compliant, non-compliant, and hardware-exempt

PCs as a pie chart. You can filter the report based on compliance and error status. You can also search, print, and export it.

Figure 10 shows a report that Contoso generated to see an overview of the entire organization's compliance status. About half of the organization's PCs are compliant with its BitLocker policies. Another quarter are non-compliant, and yet another quarter are hardware exempt. The bottom portion of the report shows the compliance status, user information, and status details for each PC. Notice that the PC named CONTOSO-PC-05 is non-compliant with BitLocker policy and that the user has postponed encryption.

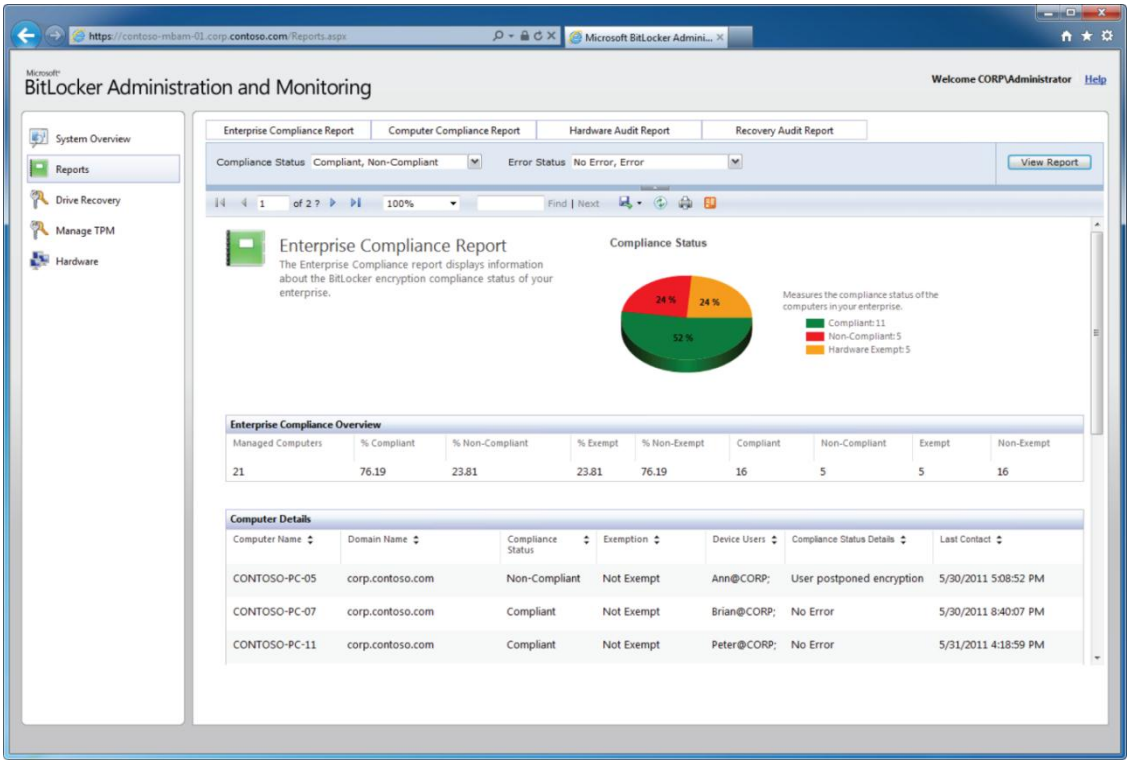


Figure 10. Enterprise Compliance Report

Computer Compliance Report

The Computer Compliance Report is similar to the Enterprise Compliance Report except that it focuses on a single computer or a single user's PCs. It also provides more detail, such as information about each drive, computer make and model, and so on. You provide the name of a PC or user, and click **View Report** to generate it. The top portion of the report provides a summary, which is mostly useful when searching for users who have multiple PCs, and the bottom portion displays details for each PC.

Not long after Contoso began deploying Windows 7 with the MBAM client, a user lost her PC while traveling. The PC contained confidential data, and Contoso was alarmed. However, administrators were able to generate the Computer Compliance Report that you see in Figure 11. It clearly shows that the lost PC was compliant with the organization's BitLocker policy because it was encrypted with BitLocker using the TPM plus a PIN. In just minutes, Contoso was able to quickly discover the risk of losing the PC.

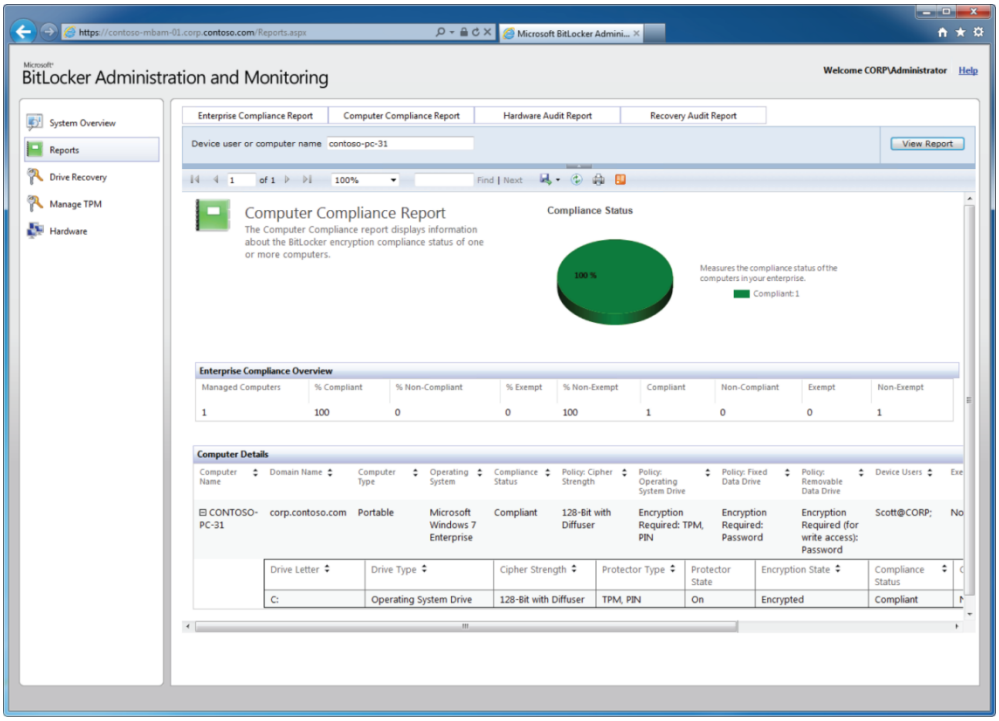


Figure 11. Computer Compliance Report

Recovery Audit Report

MBAM logs access to recovery data in the Compliance and Audit Database, and you can see it in the Recovery Audit Report. Figure 12 shows an example of the report that Contoso generated. You can filter the Recovery Audit Report in a variety of ways. You can display a specific help desk user, end user, result, key type, and date range.

Consider reviewing this report periodically to understand who is accessing recovery data and why. Additionally, if you suspect that MBAM users are misusing recovery data, you can audit their activity by searching specifically for their user accounts.

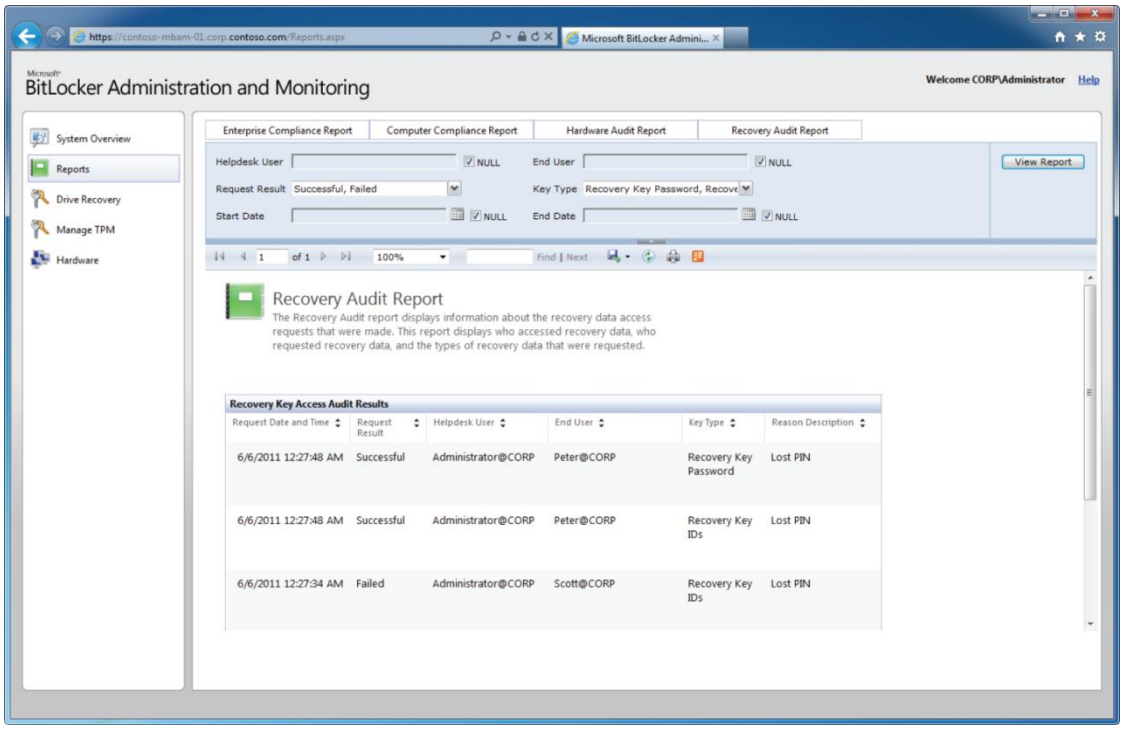


Figure 12. Recovery Audit Report

Hardware Audit Report

As with recovery data, MBAM logs changes to the Hardware Compatibility list in the Compliance and Audit Database. You view the audit information by using the Hardware Audit Report. Figure 13 shows a Hardware Audit Report that Contoso generated. In this report, you see that the administrator added two new PC models. As with other reports, you can filter the Hardware Audit Report based on the MBAM user, type of change, and a date range.

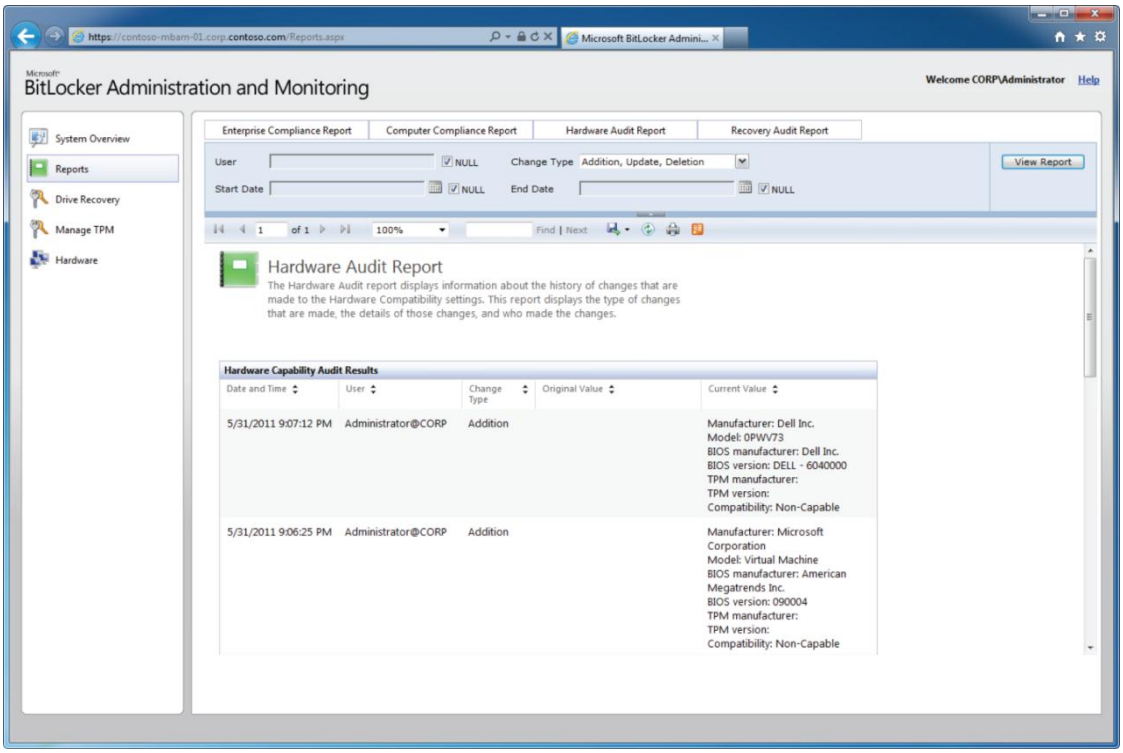


Figure 13. Hardware Audit Report

Supporting BitLocker Users

MBAM streamlines BitLocker support and reduces support costs by reducing the time required to help users recover locked drives. You use the Drive Recovery page in the Management Console to look up a drive's recovery key based on its recovery key ID as well as the user's ID and domain. The best way to describe this capability is by using Contoso as an example:

1. Peter is traveling, and he forgot his BitLocker PIN. When he starts his PC, he sees the BitLocker Recovery Console instead of the glowing Windows flag that he is used to seeing. So, he calls the help desk.
2. The help desk asks Peter for the first eight digits of the recovery key ID, which Peter sees on the BitLocker Recovery Console, and types it in to the Drive Recovery page on the Management Console. The help desk also types Peter's domain and user ID and chooses a reason for unlocking the drive. In this case, Peter simply forgot his PIN.
3. The Drive Recovery page displays the drive recovery key, as Figure 14 shows, and the help desk instructs Peter on how to unlock the drive by using the recovery key. After unlocking the drive, Peter gets quickly back to work.

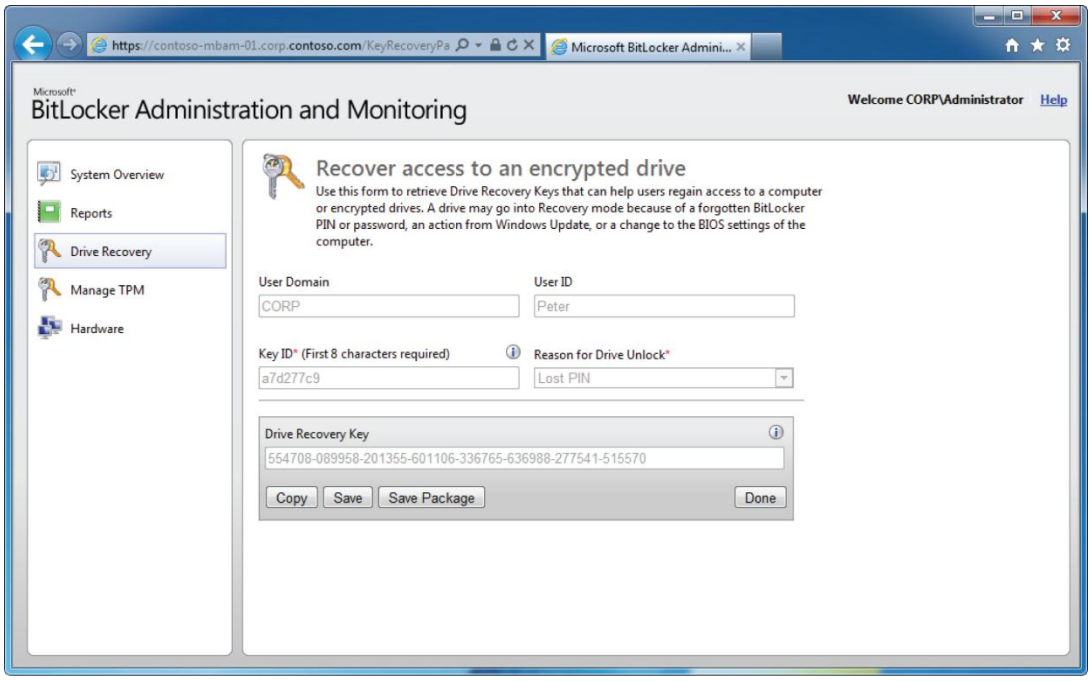


Figure 14. Drive Recovery in MBAM

> **Note:** *Members of the MBAM Advanced Helpdesk Users group do not have to provide a user ID or domain when looking up a recovery key. For example, if an IT pro finds a laptop PC in the closet, a member of the MBAM Advanced Helpdesk Users group can look up its recovery key by using MBAM.*

Importantly, after unlocking the drive by using the recovery key, the MBAM client generates a new recovery key for the drive and reports it to the Administration and Monitoring Server. Single-use keys help prevent their misuse. For example, users cannot record and keep their recovery keys for future use, which decreases the risk of an unauthorized user gaining access to the drive by using the key. For other ways that MBAM helps secure recovery keys, see the section titled “Securing Recovery Data.”

In addition to drive recovery, MBAM provides tools to help users manage their TPM. The Manage TPM page of the Management Console, which Figure 15 shows, can generate a TPM Owner Password File for each PC that the MBAM client encrypts. Users can use this file to unlock or manage their PC's TPM.

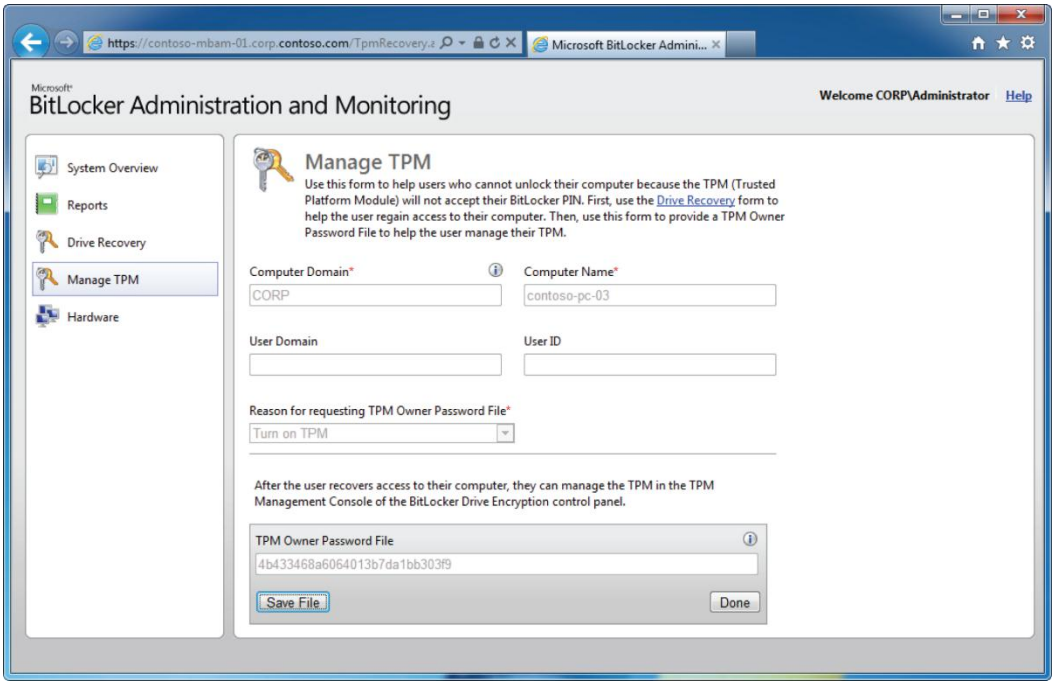


Figure 15. TPM Management in MBAM

EVALUATE MBAM

MBAM can help any organization better provision, monitor, and support BitLocker. MBAM is part of MDOP, an add-on license available to Software Assurance customers. Begin your evaluation today:

- Download and evaluate MBAM as part of MDOP. MDOP is available to Volume Licensing customers, Microsoft Developer Network (MSDN, http://msdn.microsoft.com/) subscribers, and Microsoft TechNet (http://technet.microsoft.com/) subscribers.
- See Microsoft Desktop Optimization Pack on Microsoft.com. To learn how MBAM and MDOP for Software Assurance can help you better provision, monitor, and support BitLocker, see http://go.microsoft.com/fwlink/?LinkId=160297.
- See Microsoft Desktop Optimization Pack on TechNet. For technical information about MBAM and MDOP for Software Assurance, see the MDOP TechCenter page (http://www.microsoft.com/technet/mdop) on TechNet.
- See the MBAM product documentation. For the official product documentation for MBAM, see the MBAM Administrator's Guide on the web on the MDOP documentation home page (http://onlinehelp.microsoft.com/mdop).

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