Administrator's Guide for Microsoft BitLocker Administration and Monitoring 1.0

MDOP Information Experience Team

Guide

Microsoft

Administrator's Guide for Microsoft BitLocker Administration and Monitoring 1.0

MDOP Information Experience Team

Summary: Microsoft BitLocker Administration and Monitoring (MBAM) builds on BitLocker in Windows 7 and offers you an enterprise solution for BitLocker provisioning, monitoring and key recovery. MBAM will help you simplify BitLocker provisioning and deployment independent or as part of your Windows 7 migration, improving compliance and reporting of BitLocker, and reducing support costs. This document assumes that you generally already understand BitLocker and group policies, and that you want a tool to more easily manage those security features.

This guide provides background information about MBAM and describes how to install and use the product. The intended audience for the guide is MBAM administrators and IT personnel.

Category: Guide
Applies to: MBAM 1.0
Source: TechNet Library (http://go.microsoft.com/fwlink/?LinkId=217222)
E-book publication date: February 2013

Microsoft

Contents

Getting Started with MBAM 1.0

Microsoft BitLocker Administration and Monitoring (MBAM) requires thorough planning before you deploy it or use its features. Because this product can affect every computer in your organization, you might disrupt your entire network if you do not plan your deployment carefully. However, if you plan your deployment carefully and manage it so that it meets your business needs, MBAM can help reduce your administrative overhead and total cost of ownership.

If you are new to this product, we recommend that you read the documentation thoroughly. Before you deploy it to a production environment, we also recommend that you validate your deployment plan in a test network environment. You might also consider taking a class about relevant technologies. For more information about Microsoft training opportunities, see the Microsoft Training Overview at http://go.microsoft.com/fwlink/p/?LinkId=80347.

Note
You can find a downloadable version of this documentation and the MBAM Evaluation Guide at http://go.microsoft.com/fwlink/p/?LinkId=225356.

This section of the MBAM Administrator's Guide includes high-level information about MBAM to provide you with a basic understanding of the product before you begin the deployment planning. Additional MBAM documentation can be found on the MBAM Documentation Resources Download page at http://go.microsoft.com/fwlink/p/?LinkId=258391.

Getting started with MBAM 1.0

- About MBAM 1.0

  Provides a high-level overview of MBAM and how it can be used in your organization.
- Evaluating MBAM 1.0

  Provides information about how you can best evaluate MBAM for use in your organization.
- High Level Architecture for MBAM 1.0

  Provides a description of the MBAM features and how they work together.
- Accessibility for MBAM 1.0

  Provides information about features and services that make this product and its corresponding documentation more accessible for people with disabilities.

About MBAM 1.0

Microsoft BitLocker Administration and Monitoring (MBAM) provides a simplified administrative interface to BitLocker drive encryption and offers enhanced protection against data theft or data exposure for computers that are lost or stolen. BitLocker encrypts all data that is stored on the

Windows operating system volume and configured data volumes, which includes the Windows operating system, hibernation and paging files, applications, and the data that is used by applications.

With Microsoft BitLocker Administration and Monitoring, you can select the BitLocker encryption policy options that are appropriate for your enterprise so that you can monitor the client compliance with those policies and then report the encryption status of both the enterprise and individual computers. In addition, you can access recovery key information when users forget their PIN or password or when their BIOS or boot record changes.

Note

BitLocker is not covered in detail in this guide. For an overview of BitLocker, see BitLocker Drive Encryption Overview.

The following groups might be interested in using MBAM to manage BitLocker:

- Administrators, IT security professionals, and compliance officers who are tasked with ensuring that confidential data is not disclosed without authorization
- Administrators who are responsible for securing computers in remote or branch offices
- Administrators who are responsible for servers or Windows client computers that are mobile
- Administrators who are responsible for decommissioning servers that contain confidential data

MBAM 1.0 Release Notes

For more information and for latest updates, see Release Notes for MBAM 1.0.

Evaluating MBAM 1.0

Before you deploy Microsoft BitLocker Administration and Monitoring (MBAM) into a production environment, you should evaluate it in a lab environment. You can use the information in this topic to set up MBAM in a single server lab environment for evaluation purposes only.

While the actual deployment steps are very similar to the scenario that is described in How to Install and Configure MBAM on a Single Server, this topic contains additional information to enable you to set up an MBAM evaluation environment in the least amount of time.

Set up the Lab Environment

Even when you set up a non-production instance of MBAM to evaluate in a lab environment, you should still verify that you have met the deployment prerequisites and the hardware and software requirements. For more information, see MBAM 1.0 Deployment Prerequisites and MBAM 1.0 Supported Configurations. You should also review Preparing your Environment for MBAM 1.0 before you begin the MBAM evaluation deployment.

Plan for an MBAM Evaluation Deployment

	Task	References	Notes
☐	Review the Getting Started information about MBAM to gain a basic understanding of the product before you begin your deployment planning.	Getting Started with MBAM 1.0	
☐	Prepare your computing environment for the MBAM installation. To do so, you must enable the Transparent Data Encryption (TDE) on the SQL Server instances that will host MBAM databases. To enable TDE in your lab environment, you can create a .sql file to run against the master database that is hosted on the instance of the SQL Server that MBAM will use. **Note** You can use the following example to create a .sql file for your lab environment to quickly enable TDE on the SQL Server instance that will host the MBAM databases. These SQL Server commands will enable TDE by using a locally signed SQL Server certificate. Make sure to back up the TDE certificate and its associated encryption key to the example local backup path of *C:\Backup*\. The TDE certificate and key are required when recover the database or move the certificate and key to another server that has TDE encryption in place.	MBAM 1.0 Deployment Prerequisites Database Encryption in SQL Server 2008 Enterprise Edition	

	Task	References	Notes
	USE master; GO CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'P@55w0rd'; GO CREATE CERTIFICATE tdeCert WITH SUBJECT = 'TDE Certificate'; GO BACKUP CERTIFICATE tdeCert TO FILE = 'C:\Backup\TDECertificate.cer' WITH PRIVATE KEY (FILE = 'C:\Backup\TDECertificateKey.pvk', ENCRYPTION BY PASSWORD = 'P@55w0rd'); GO		
☐	Plan for and configure MBAM Group Policy requirements.	Planning for MBAM 1.0 Group Policy Requirements	
☐	Plan for and create the necessary Active Directory Domain Services security groups and plan for MBAM local security group membership requirements.	Planning for MBAM 1.0 Administrator Roles	
☐	Plan for MBAM Server feature deployment.	Planning for MBAM 1.0 Server Deployment	
☐	Plan for MBAM Client deployment.	Planning for MBAM 1.0 Client Deployment	

Perform an MBAM Evaluation Deployment

After you complete the necessary planning and software prerequisite installations to prepare your computing environment for an MBAM installation, you can begin the MBAM evaluation deployment.

☐	Review the MBAM supported configurations information to make sure that the selected client and server computers are supported for the MBAM feature installation.	MBAM 1.0 Supported Configurations	
☐	Run MBAM Setup to deploy MBAM Server features on a single server for evaluation purposes.	How to Install and Configure MBAM on a Single Server	
☐	Add the Active Directory Domain Services security groups that you created during the planning phase to the appropriate local MBAM Server feature local groups on the new MBAM server.	Planning for MBAM 1.0 Administrator Roles and How to Manage MBAM Administrator Roles	
☐	Create and deploy the required MBAM Group Policy Objects.	Deploying MBAM 1.0 Group Policy Objects	
☐	Deploy the MBAM Client software.	Deploying the MBAM 1.0 Client	

Configure Lab Computers for MBAM Evaluation

You can change the frequency settings on the MBAM Client status reporting by using Registry Editor. However, these modifications should be used for testing purposes only.

Warning

This topic describes how to change the Windows registry by using Registry Editor. If you change the Windows registry incorrectly, you can cause serious problems that might require you to reinstall Windows. You should make a backup copy of the registry files (System.dat and User.dat) before you change the registry. Microsoft cannot guarantee that the problems that might occur when you change the registry can be resolved. Change the registry at your own risk.

Modify the Frequency Settings on MBAM Client Status Reporting

The MBAM Client wakeup and status reporting frequencies have a minimum value of 90 minutes when they are set to use Group Policy. You can change these frequencies on MBAM client computers by editing the Windows registry to lower values, which will help speed up the testing. To modify the frequency settings on MBAM Client status reporting, use a registry editor to navigate to **HKLM\Software\Policies\FVE\MDOPBitLockerManagement**, change the values for **ClientWakeupFrequency** and **StatusReportingFrequency** to **1** as the minimum client

supported value, and then restart BitLocker Management Client Service. When you make this change, the MBAM Client will report every minute. You can set values this low only when you do so manually in the registry.

Modify the Startup Delay on MBAM Client Service

In addition to the MBAM Client wakeup and status reporting frequencies, there is a random delay of up to 90 minutes when the MBAM Client agent service starts on client computers. If you do not want the random delay, create a **DWORD** value of **NoStartupDelay** under **HKLM\Software\Microsoft\MBAM**, set its value to **1**, and then restart BitLocker Management Client Service.

High Level Architecture for MBAM 1.0

Microsoft BitLocker Administration and Monitoring (MBAM) is a client/server data encryption solution that can help you simplify BitLocker provisioning and deployment, improve BitLocker compliance and reporting, and reduce support costs. MBAM includes the features that are described in this topic.

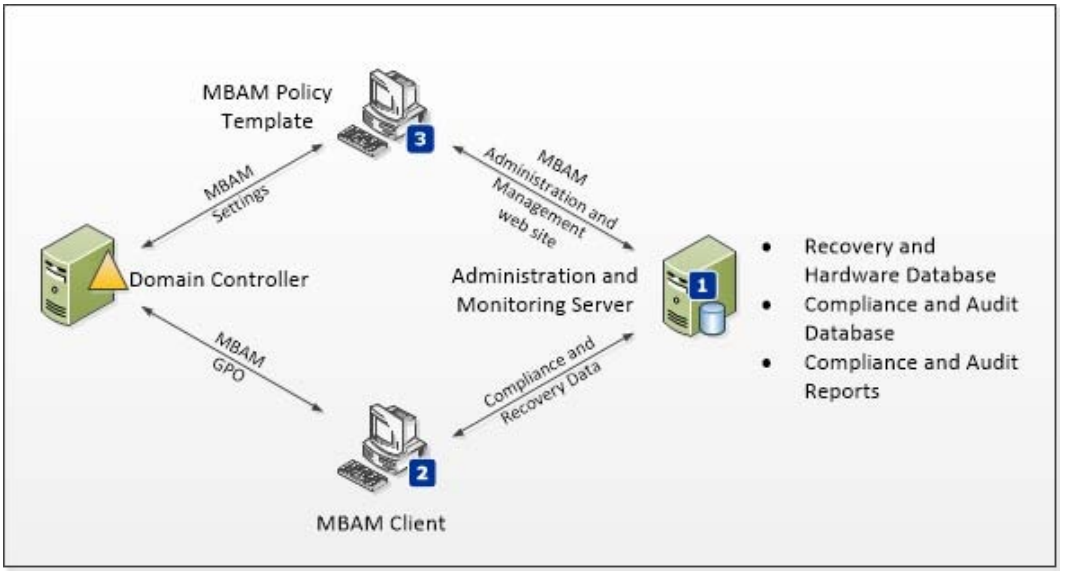
Additionally, there is a video that provides an overview of the MBAM architecture and MBAM Setup. For more information, see MBAM Deployment and Architecture Overview.

Architecture Overview

The following diagram displays the MBAM architecture. The single-server MBAM deployment topology is shown to introduce the MBAM features. However, this MBAM deployment topology is recommended only for lab environments.

Note

At least a three-computer MBAM deployment topology is recommended for a production deployment. For more information about MBAM deployment topologies, see Deploying the MBAM 1.0 Server Infrastructure.



1. **Administration and Monitoring Server**. The MBAM Administration and Monitoring Server is installed on a Windows server and hosts the MBAM Administration and Management website and the monitoring web services. The MBAM Administration and Management website is used to determine enterprise compliance status, to audit activity, to manage hardware capability, and to access recovery data, such as the BitLocker recovery keys. The Administration and Monitoring Server connects to the following databases and services:
   - Recovery and Hardware Database. The Recovery and Hardware database is installed on a Windows-based server and supported SQL Server instance. This database stores recovery data and hardware information that is collected from MBAM client computers.
   - Compliance and Audit Database. The Compliance and Audit Database is installed on a Windows server and supported SQL Server instance. This database stores compliance data for MBAM client computers. This data is used primarily for reports that are hosted by SQL Server Reporting Services (SSRS).
   - Compliance and Audit Reports. The Compliance and Audit Reports are installed on a Windows-based server and supported SQL Server instance that has the SSRS feature installed. These reports provide Microsoft BitLocker Administration and Monitoring reports. These reports can be accessed from the MBAM Administration and Management website or directly from the SSRS Server.
2. **MBAM Client**. The Microsoft BitLocker Administration and Monitoring Client performs the following tasks:
   - Uses Group Policy to enforce the BitLocker encryption of client computers in the enterprise.
   - Collects the recovery key for the three BitLocker data drive types: operating system drives, fixed data drives, and removable data (USB) drives.
   - Collects recovery information and hardware information about the client computers.
   - Collects compliance data for the computer and passes the data to the reporting system.

3. **Policy Template**. The MBAM Group Policy template is installed on a supported Windows-based server or client computer. This template is used to specify the MBAM implementation settings for BitLocker drive encryption.

Accessibility for MBAM 1.0

Microsoft is committed to making its products and services easier for everyone to use. This section provides information about features and services that make this product and its corresponding documentation more accessible for people with disabilities.

Access Any Command with a Few Keystrokes

Access keys let you quickly use a command by pressing a few keys. You can get to most commands by using two keystrokes. To use an access key:

1. Press ALT.

   The keyboard shortcuts are displayed over each feature that is available in the current view.
2. Press the letter shown in the keyboard shortcut over the feature that you want to use.

Note

To cancel the action that you are taking and hide the keyboard shortcuts, press ALT.

Documentation in Alternative Formats

If you have difficulty reading or handling printed materials, you can obtain the documentation for many Microsoft products in more accessible formats. You can view an index of accessible product documentation on the Microsoft Accessibility website. In addition, you can obtain additional Microsoft publications from Learning Ally (formerly Recording for the Blind & Dyslexic, Inc.). Learning Ally distributes these documents to registered, eligible members of their distribution service.

For information about the availability of Microsoft product documentation and books from Microsoft Press, contact:

Learning Ally (formerly Recording for the Blind & Dyslexic, Inc.) 20 Roszel Road Princeton, NJ 08540	
Telephone number from within the United States:	(800) 221-4792
Telephone number from outside the United States and Canada:	(609) 452-0606

Fax:	(609) 987-8116
http://www.learningally.org/	Web addresses can change, so you might be unable to connect to the website or sites mentioned here.

Customer Service for People with Hearing Impairments

If you are deaf or hard-of-hearing, complete access to Microsoft product and customer services is available through a text telephone (TTY/TDD) service:

- For customer service, contact Microsoft Sales Information Center at (800) 892-5234 between 6:30 AM and 5:30 PM Pacific Time, Monday through Friday, excluding holidays.
- For technical assistance in the United States, contact Microsoft Product Support Services at (800) 892-5234 between 6:00 AM and 6:00 PM Pacific Time, Monday through Friday, excluding holidays. In Canada, dial (905) 568-9641 between 8:00 AM and 8:00 PM Eastern Time, Monday through Friday, excluding holidays.

Microsoft Support Services are subject to the prices, terms, and conditions in place at the time the service is used.

For More Information

For more information about how accessible technology for computers helps to improve the lives of people with disabilities, see the Microsoft Accessibility website.

Planning for MBAM 1.0

The goal of deployment planning is to successfully and efficiently deploy Microsoft BitLocker Administration and Monitoring (MBAM) so that it does not disrupt your users or the network.

There are a number of different deployment configurations and prerequisites that you should consider before you try to deploy the MBAM. This section includes information that can help you gather the information that you need to formulate a deployment plan that best meets your business requirements. It can assist you in preparing your network and computing environment, and it provides the information necessary for you to properly plan to deploy MBAM features.

Planning information

- Preparing your Environment for MBAM 1.0

  This section describes the computing environment requirements and installation prerequisites that you should plan for before you begin the MBAM Setup.
- Planning to Deploy MBAM 1.0

This section describes the minimum hardware and software requirements necessary for the MBAM Client and Server feature installation. It also provides information about the MBAM deployment topology that you can use, and other MBAM Server and Client planning considerations.

- MBAM 1.0 Planning Checklist

  This section provides a planning checklist that you can use throughout the MBAM deployment.

Preparing your Environment for MBAM 1.0

Before you begin the Microsoft BitLocker Administration and Monitoring (MBAM) Setup, make sure that you have met the necessary prerequisites to install the product. If you know the prerequisites in advance, you can efficiently deploy the product and enable its features, which can support the business objectives of your organization more effectively.

Review MBAM 1.0 deployment prerequisites

The MBAM Client and each of the MBAM Server features have specific prerequisites that must be met before they can be successfully installed.

To ensure successful installation of MBAM Clients and MBAM Server features, you should plan to ensure that computers specified for MBAM Client or MBAM Server feature installation are properly prepared for MBAM Setup.

Note

MBAM Setup verifies if all prerequisites are met before installation starts. If they are not met, Setup will fail.

MBAM 1.0 Deployment Prerequisites

Plan for MBAM 1.0 Group Policy requirements

Before MBAM can manage clients in the enterprise, you must define the Group Policy for the encryption requirements of your environment.

Important

MBAM will not work with policies for stand-alone BitLocker drive encryption. Group Policy must be defined for MBAM; otherwise, the BitLocker encryption and enforcement will fail.

Planning for MBAM 1.0 Group Policy Requirements

Plan for MBAM 1.0 administrator roles

MBAM administrator roles are managed by local groups that are created by MBAM Setup when you install the following: BitLocker Administration and Monitoring Server, the Compliance and Audit Reports feature, and the Compliance and Audit Status Database.

The membership of MBAM roles can be managed more effectively if you create security groups in Active Directory Domain Services, add the appropriate administrator accounts to those groups, and then add those security groups to the MBAM local groups. For more information, see How to Manage MBAM Administrator Roles.

Planning for MBAM 1.0 Administrator Roles

MBAM 1.0 Deployment Prerequisites

Before you begin the Microsoft BitLocker Administration and Monitoring (MBAM) Setup, make sure that you meet the necessary prerequisites to install the product. This section contains information to help you successfully prepare your computing environment before you deploy the MBAM Clients and Server features.

Installation prerequisites for MBAM Server features

Each of the MBAM server features has specific prerequisites that must be met before they can be successfully installed. MBAM Setup verifies if all prerequisites are met before the installation starts.

Installation prerequisites for Administration and Monitoring Server

The following table contains the installation prerequisites for the MBAM Administration and Monitoring Server:

Prerequisite	Details
Windows ServerWeb Server Role	This role must be added to a server operating system supported for the MBAM Administration and Monitoring Server feature.
Web Server (IIS) Management Tools	**IIS Management Scripts and Tools**
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
Windows Server Features	**Microsoft .NET Framework 3.5.1 features:**

Prerequisite	Details

	• .NET Framework 3.5.1
	• WCF Activation
	  • HTTP Activation
	  • Non-HTTP Activation
	Windows Process Activation Service
	• Process Model
	• .NET Environment
	• Configuration APIs

Note
For a list of supported operating systems, see MBAM 1.0 Supported Configurations.

Installation prerequisites for the Compliance and Audit Reports

The Compliance and Audit Reports must be installed on a supported version of SQL Server. Installation prerequisites for this feature include SQL Server Reporting Services (SSRS).

SSRS must be installed and running during MBAM server installation. SSRS should also be configured in “native” mode, not in the “unconfigured” or “SharePoint” mode.

Note
For a list of supported operating systems and SQL Server versions, see MBAM 1.0 Supported Configurations.

Installation prerequisites for the Recovery and Hardware Database

The Recovery and Hardware Database must be installed on a supported version of SQL Server.

SQL Server must have Database Engine Services installed and running during the MBAM server installation. The Transparent Data Encryption (TDE) feature must be enabled.

Note
For a list of supported operating systems and SQL Server versions, see MBAM 1.0 Supported Configurations.

The TDE SQL Server feature performs real-time input/output (I/O) encryption and decryption of the data and log files. TDE protects data that is "at rest,” which include the data and the log files. It provides the ability to comply with many laws, regulations, and guidelines that are established in various industries.

Note
Because TDE performs real-time decryption of database information, the recovery key information will be visible if the account under which you are logged in has permissions to the database when you view the recovery key information SQL tables.

Installation prerequisites for the Compliance and Audit Database

The Compliance and Audit Database must be installed on a supported version of SQL Server.

SQL Server must have Database Engine Services installed and running during MBAM server installation.

Note

For a list of supported operating systems and SQL Server versions, see MBAM 1.0 Supported Configurations.

Installation prerequisites for MBAM Clients

The necessary prerequisites that you must meet before you begin the MBAM Client installation are the following:

- Trusted Platform Module (TPM) v1.2 capability
- The TPM chip must be turned on in the BIOS and it must be resettable from the operating system. For more information, see the BIOS documentation.

Warning

Ensure that the keyboard, mouse, and video are directly connected to the computer, instead of to a keyboard, video, mouse (KVM) switch. A KVM switch can interfere with the ability of the computer to detect the physical presence of hardware.

Planning for MBAM 1.0 Group Policy Requirements

Microsoft BitLocker Administration and Monitoring (MBAM) Client management requires custom Group Policy settings to be applied. This topic describes the available policy options for Group Policy Object (GPO) when you use MBAM to manage BitLocker Drive Encryption in the enterprise.

Important

MBAM does not use the default GPO settings for Windows BitLocker drive encryption. If the default settings are enabled, they can cause conflicting behavior. To enable MBAM to manage BitLocker, you must define the GPO policy settings after you install the MBAM Group Policy Template.

After you install the MBAM Group Policy template, you can view and modify the available custom MBAM GPO policy settings that enable MBAM to manage the enterprise BitLocker encryption. The MBAM Group Policy template must be installed on a computer that is capable of running the Group Policy Management Console (GPMC) or the Advanced Group Policy Management (AGPM) MDOP technology. Next, to edit the applicable GPO, open the GPMC or AGPM, and then navigate to the following GPO node: **Computer Configuration\Administrative Templates\Windows Components\MDOP MBAM (BitLocker Management)**.

The MDOP MBAM (BitLocker Management) GPO node contains four global policy settings and four child GPO setting nodes, respectively. The four GPO global policy settings are: Client Management, Fixed Drive, Operating System Drive, and Removable Drive. The following sections

provide policy definitions and suggested policy settings to help you plan for the MBAM GPO policy setting requirements.

Note
For more information about configuring the minimum suggested GPO settings to enable MBAM to manage BitLocker encryption, see How to Edit MBAM 1.0 GPO Settings.

Global policy definitions

This section describes the MBAM Global policy definitions, which can be found at the following GPO node: **Computer Configuration\Administrative Templates\Windows Components\MDOP MBAM (BitLocker Management)**.

Policy Name	Overview and Suggested Policy Setting
Choose drive encryption method and cipher strength	Suggested Configuration: **Not Configured** Configure this policy to use a specific encryption method and cipher strength. When this policy is not configured, BitLocker uses the default encryption method of AES 128-bit with Diffuser or the encryption method specified by the setup script.
Prevent memory overwrite on restart	Suggested Configuration: **Not Configured** Configure this policy to improve restart performance without overwriting BitLocker secrets in memory on restart. When this policy is not configured, BitLocker secrets are removed from memory when the computer restarts.
Validate smart card certificate usage rule	Suggested Configuration: **Not Configured** Configure this policy to use smartcard certificate-based BitLocker protection. When this policy is not configured, a default object identifier 1.3.6.1.4.1.311.67.1.1 is used to specify a certificate.
Provide the unique identifiers for your organization	Suggested Configuration: **Not Configured** Configure this policy to use a certificate-based data recovery agent or the BitLocker To Go reader. When this policy is not configured, the **Identification** field is not used.

Policy Name	Overview and Suggested Policy Setting
	If your company requires higher security measurements, you may want to configure the **Identification** field to make sure that all USB devices have this field set and that they are aligned with this Group Policy setting.

Client Management policy definitions

This section describes the Client Management policy definitions for MBAM, found at the following GPO node: **Computer Configuration\Administrative Templates\Windows Components\MDOP MBAM (BitLocker Management) \ Client Management**.

Policy Name	Overview and Suggested Policy Settings
Configure MBAM Services	Suggested Configuration: **Enabled** • **MBAM Recovery and Hardware service endpoint**. This is the first policy setting that you must configure to enable the MBAM Client BitLocker encryption management. For this setting, enter the endpoint location similar to the following example: **http:**//<*MBAM Administration and Monitoring Server Name*>**:**<*port the web service is bound to*>**/MBAMRecoveryAndHardwareService/CoreService.svc**. • **Select BitLocker recovery information to store**. This policy setting lets you configure the key recovery service to back up the BitLocker recovery information. It also lets you configure the status reporting service for collecting compliance and audit reports. The policy provides an administrative method of recovering data encrypted by BitLocker to help prevent data loss due to the lack of key information. Status report and key recovery activity will automatically and silently be sent to the configured report server location. If you do not configure or if you disable this policy setting, the key recovery information will not be saved, and status report and key recovery activity will not be reported to server. When this setting is set to **Recovery Password and key package**, the recovery password and key package will be automatically and silently backed up to the configured key recovery server location. • **Enter the client checking status frequency in minutes**. This policy setting manages how frequently the client checks

Policy Name	Overview and Suggested Policy Settings
	the BitLocker protection policies and the status on the client computer. This policy also manages how frequently the client compliance status is saved to the server. The client checks the BitLocker protection policies and status on the client computer, and it also backs up the client recovery key at the configured frequency. Set this frequency based on the requirement established by your company on how frequently to check the compliance status of the computer, and how frequently to back up the client recovery key. • **MBAM Status reporting service endpoint**. This is the second policy setting that you must configure to enable MBAM Client BitLocker encryption management. For this setting, enter the endpoint location by using the following example: **http:**//<*MBAM Administration and Monitoring Server Name*>**:**<*port the web service is bound to*>**/MBAMComplianceStatusService/StatusReportingService. svc**.
Allow hardware compatibility checking	Suggested Configuration: **Enabled** This policy setting lets you manage the verification of hardware compatibility before you enable BitLocker protection on drives of MBAM client computers. You should enable this policy option if your enterprise has older computer hardware or computers that do not support Trusted Platform Module (TPM). If either of these criteria is true, enable the hardware compatibility verification to make sure that MBAM is applied only to computer models that support BitLocker. If all computers in your organization support BitLocker, you do not have to deploy the Hardware Compatibility, and you can set this policy to **Not Configured**. If you enable this policy setting, the model of the computer is validated against the hardware compatibility list once every 24 hours, before the policy enables BitLocker protection on a computer drive. **Note** Before enabling this policy setting, make sure that you have configured the **MBAM Recovery and Hardware service endpoint** setting in the **Configure MBAM Services** policy options. If you either disable or do not configure this policy setting, the

Policy Name	Overview and Suggested Policy Settings
	computer model is not validated against the hardware compatibility list.
Configure user exemption policy	Suggested Configuration: **Not Configured** This policy setting lets you configure a web site address, email address, or phone number that will instruct a user to request an exemption from BitLocker encryption. If you enable this policy setting and provide a web site address, email address, or phone number, users will see a dialog with instructions on how to apply for an exemption from BitLocker protection. For more information about how to enable BitLocker encryption exemptions for users, see How to Manage User BitLocker Encryption Exemptions. If you either disable or do not configure this policy setting, the instructions about how to apply for an exemption request will not be presented to users. **Note** User exemption is managed per user, not per computer. If multiple users log on to the same computer and one user is not exempt, the computer will be encrypted.

Fixed Drive policy definitions

This section describes the Fixed Drive policy definitions for MBAM, which can be found at the following GPO node: **Computer Configuration\Administrative Templates\Windows Components\MDOP MBAM (BitLocker Management)** \ **Fixed Drive**.

Policy Name	Overview and Suggested Policy Setting
Fixed data drive encryption settings	Suggested Configuration: **Enabled**, and select the **Enable auto-unlock fixed data drive** check box if the operating system volume is required to be encrypted. This policy setting lets you manage whether or not to encrypt the fixed drives. When you enable this policy, do not disable the **Configure use of password for fixed data drives** policy. If the **Enable auto-unlock fixed data drive** check box is selected, the operating system

Policy Name	Overview and Suggested Policy Setting
	volume must be encrypted. If you enable this policy setting, users are required to put all fixed drives under BitLocker protection, which will encrypt the drives. If you do not configure this policy or if you disable this policy, users are not required to put fixed drives under BitLocker protection. If you disable this policy, the MBAM agent decrypts any encrypted fixed drives. If encrypting the operating system volume is not required, clear the **Enable auto-unlock fixed data drive** check box.
Deny “write” permission to fixed drives that are not protected by BitLocker	Suggested Configuration: **Not Configured** This policy setting determines if BitLocker protection is required for fixed drives on a computer so that they are writable. This policy setting is applied when you turn on BitLocker. When the policy is not configured, all fixed drives on the computer are mounted with read/write permissions.
Allow access to BitLocker-protected fixed drives from earlier versions of Windows	Suggested configuration: **Not Configured** Enable this policy to unlock and view the fixed drives that are formatted with the file allocation table (FAT) file system on computers that are running Windows Server 2008, Windows Vista, Windows XP with SP3, or Windows XP with SP2. These operating systems have read-only permissions to BitLocker-protected drives. When the policy is disabled, fixed drives formatted with the FAT file system cannot be unlocked and their content cannot be viewed on computers that are running Windows Server 2008, Windows Vista, Windows XP with SP3, or Windows XP with SP2.
Configure use of password for fixed drives	Suggested configuration: **Not Configured** Enable this policy to configure password protection on fixed drives.

Policy Name	Overview and Suggested Policy Setting
	When the policy is not configured, passwords will be supported with the default settings, which do not include password complexity requirements and require only eight characters. For higher security, enable this policy and select **Require password for fixed data drive**, select **Require password complexity**, and set the desired **minimum password length**.
Choose how BitLocker-protected fixed drives can be recovered	Suggested Configuration: **Not Configured** Configure this policy to enable the BitLocker data recovery agent or to save BitLocker recovery information to Active Directory Domain Services (AD DS). When this policy is not configured, the BitLocker data recovery agent is allowed, and recovery information is not backed up to AD DS. MBAM does not require the recovery information to be backed up to AD DS.

Operating System Drive policy definitions

This section describes the Operating System Drive policy definitions for MBAM, found at the following GPO node: **Computer Configuration\Administrative Templates\Windows Components\MDOP MBAM (BitLocker Management) \ Operating System Drive**.

Policy Name	Overview and Suggested Policy Setting
Operating system drive encryption settings	Suggested configuration: **Enabled** This policy setting determines if the operating system drive will be encrypted. Configure this policy to do the following: • Enforce BitLocker protection for the operating system drive. • Configure PIN usage to use a Trusted Platform Module (TPM) PIN for operating system protection. • Configure enhanced startup PINs to permit characters such as uppercase and lowercase letters, symbols, numbers, and spaces.

Policy Name	Overview and Suggested Policy Setting
	If you enable this policy setting, users are required to secure the operating system drive by using BitLocker. If you do not configure or if you disable the setting, users are not required to secure the operating system drive by using BitLocker. If you disable this policy, the MBAM agent decrypts the operating system volume if it is encrypted. When it is enabled, this policy setting requires users to secure the operating system by using BitLocker protection, and the drive is encrypted. Based on your encryption requirements, you may select the method of protection for the operating system drive. For higher security requirements, use TPM + PIN, allow enhanced PINs, and set the minimum PIN length to eight characters. When this policy is enabled with the TPM + PIN protector, you can consider disabling the following policies under **System** / **Power Management** / **Sleep Settings**: • Allow Standby States (S1-S3) When Sleeping (Plugged In) • Allow Standby States (S1-S3) When Sleeping (On Battery)
Configure TPM platform validation profile	Suggested Configuration: **Not Configured** This policy setting lets you configure how the TPM security hardware on a computer secures the BitLocker encryption key. This policy setting does not apply if the computer does not have a compatible TPM or if BitLocker already has TPM protection enabled. When this policy is not configured, the TPM uses the default platform validation profile or the platform validation profile specified by the setup script.
Choose how to recover BitLocker-protected operating system drives	Suggested Configuration: **Not Configured** Configure this policy to enable the BitLocker

Policy Name	Overview and Suggested Policy Setting
	data recovery agent or to save BitLocker recovery information to Active Directory Domain Services (AD DS). When this policy is not configured, the data recovery agent is allowed, and the recovery information is not backed up to AD DS. MBAM operation does not require the recovery information to be backed up to AD DS.

Removable Drive policy definitions

This section describes the Removable Drive Policy definitions for MBAM, found at the following GPO node: **Computer Configuration\Administrative Templates\Windows Components\MDOP MBAM (BitLocker Management)** \ **Removable Drive**.

Policy Name	Overview and Suggested Policy Setting
Control the use of BitLocker on removable drives	Suggested configuration: **Enabled** This policy controls the use of BitLocker on removable data drives. Enable the **Allow users to apply BitLocker protection on removable data drives** option, to allow users to run the BitLocker setup wizard on a removable data drive. Enable the **Allow users to suspend and decrypt BitLocker on removable data drives** option to allow users to remove BitLocker drive encryption from the drive or to suspend the encryption while maintenance is performed. When this policy is enabled and the **Allow users to apply BitLocker protection on removable data drives** option is selected, the MBAM Client saves the recovery information about removable drives to the MBAM key recovery server, and it allows users to recover the drive if the password is lost.
Deny the “write” permissions to removable drives that are not protected by BitLocker	Suggested Configuration: **Not Configured** Enable this policy to allow write-only permissions to BitLocker protected drives.

Policy Name	Overview and Suggested Policy Setting
	When this policy is enabled, all removable data drives on the computer require encryption before write permissions are allowed.
Allow access to BitLocker-protected removable drives from earlier versions of Windows	Suggested Configuration: **Not Configured** Enable this policy to unlock and view the fixed drives that are formatted with the (FAT) file system on computers that are running Windows Server 2008, Windows Vista, Windows XP with SP3, or Windows XP with SP2. These operating systems have read-only permissions to BitLocker-protected drives. When the policy is disabled, removable drives formatted with the FAT file system cannot be unlocked and their content cannot be viewed on computers that are running Windows Server 2008, Windows Vista, Windows XP with SP3, or Windows XP with SP2.
Configure the use of password for removable data drives	Suggested configuration: **Not Configured** Enable this policy to configure password protection on removable data drives. When this policy is not configured, passwords are supported with the default settings, which do not include password complexity requirements and require only eight characters. For increased security, you can enable this policy and select **Require password for removable data drive**, select **Require password complexity**, and then set the preferred **minimum password length**.
Choose how BitLocker-protected removable drives can be recovered	Suggested Configuration: **Not Configured** You can configure this policy to enable the BitLocker data recovery agent or to save BitLocker recovery information to Active Directory Domain Services (AD DS). When the policy is set to **Not Configured**, the data recovery agent is allowed and recovery information is not backed up to AD DS. MBAM operation does not require the recovery

Policy Name	Overview and Suggested Policy Setting
	information to be backed up to AD DS.

Planning for MBAM 1.0 Administrator Roles

This topic includes and describes the administrator roles that are available in Microsoft BitLocker Administration and Monitoring (MBAM), as well as the server locations where the local groups are created.

MBAM Administrator roles

MBAM System Administrators

Administrators in this role have access to all MBAM features. The local group for this role is installed on the Administration and Monitoring Server.

MBAM Hardware Users

Administrators in this role have access to the Hardware Capability features from MBAM. The local group for this role is installed on the Administration and Monitoring Server.

MBAM Helpdesk Users

Administrators in this role have access to the Helpdesk features from MBAM. The local group for this role is installed on the Administration and Monitoring Server.

MBAM Report Users

Administrators in this role have access to the Compliance and Audit Reports feature from MBAM. The local group for this role is installed on the Administration and Monitoring Server, Compliance and Audit Database, and on the server that hosts the Compliance and Audit Reports.

MBAM Advanced Helpdesk Users

Administrators in this role have increased access to the Helpdesk features from MBAM. The local group for this role is installed on the Administration and Monitoring Server. If a user is a member of both MBAM Helpdesk Users and MBAM Advanced Helpdesk Users, the MBAM Advanced Helpdesk Users permissions will overwrite the MBAM Helpdesk User permissions.

Important

To view the reports, an administrative user must be a member of the **MBAM Report Users** security group on the Administration and Monitoring Server, Compliance and Audit Database, and on the server that hosts the Compliance and Reports feature. As a best practice, create a security group in Active Directory with rights on the local **MBAM Report Users** security group on both the Administration and Monitoring Server and on the server that hosts the Compliance and Reports.

Planning to Deploy MBAM 1.0

You should consider a number of different deployment configurations and prerequisites before you create your Microsoft BitLocker Administration and Monitoring (MBAM) 1.0 deployment plan. This section includes information that can help you gather the information that you must have to formulate a deployment plan that best meets your business requirements.

Review the MBAM 1.0 supported configurations

After you prepare your computing environment for the MBAM Client and Server feature installation, make sure that you review the Supported Configurations information for MBAM to confirm that the computers on which you install MBAM meet the minimum hardware and operating system requirements. For more information about MBAM deployment prerequisites, see MBAM 1.0 Deployment Prerequisites.

MBAM 1.0 Supported Configurations

Plan for MBAM 1.0 Server and Client deployment

The MBAM server infrastructure depends on a set of server features that can be installed on one or more server computers, based on the requirements of the enterprise. These features can be installed on a single server or distributed across multiple servers.

The MBAM Client enables administrators to enforce and monitor the BitLocker drive encryption on computers in the enterprise. The BitLocker client can be integrated into an organization by deploying the client through tools like Active Directory Domain Services or by directly encrypting the client computers as part of the initial imaging process.

With MBAM, you can encrypt a computer in your organization either before the end user receives the computer or afterwards, by using Group Policy. You can use one or both methods in your organization. If you choose to use both methods, you can improve compliance, reporting, and key recovery support.

Planning for MBAM 1.0 Server Deployment

Planning for MBAM 1.0 Client Deployment

MBAM 1.0 Supported Configurations

This topic specifies the necessary requirements to install and run Microsoft BitLocker Administration and Monitoring (MBAM) in your environment.

MBAM server system Requirements

Server operating system requirements

The following table lists the operating systems that are supported for the Microsoft BitLocker Administration and Monitoring Server installation.

Note
Microsoft provides support for the current service pack and, in some cases, the immediately preceding service pack. To find the support timelines for your product, see the Lifecycle Supported Service Packs. For additional information about Microsoft Support Lifecycle Policy, see Microsoft Support Lifecycle Support Policy FAQ.

Operating System	Edition	Service Pack	System Architecture
Windows Server 2008	Standard, Enterprise, Datacenter, or Web Server	SP2 only	32-bit or 64-bit
Windows Server 2008 R2	Standard, Enterprise, Datacenter, or Web Server		64-bit

Warning
There is no support for installing MBAM services, reports, or databases on a domain controller computer.

Server random access memory (RAM) requirements

There are no RAM requirements that are specific to MBAM Server installation.

SQL Server Database requirements

The following table lists the SQL Server versions that are supported for the MBAM Server feature installation.

MBAM Server Feature	SQL Server Version	Edition	Service Pack	System Architecture
Compliance and Audit Reports	Microsoft SQL Server 2008	R2, Standard, Enterprise, Datacenter, or Developer Edition	SP2	32-bit or 64-bit
Recovery and Hardware Database	Microsoft SQL Server 2008	R2, Enterprise, Datacenter, or Developer Edition **Important** SQL Server Standard Editions are not supported for MBAM Recovery and Hardware Database Server feature installation.	SP2	32-bit or 64-bit
Compliance and Audit Database	Microsoft SQL Server 2008	R2, Standard, Enterprise, Datacenter, or Developer Edition	SP2	32-bit or 64-bit

MBAM Client system requirements

Client operating system requirements

The following table lists the operating systems that are supported for MBAM Client installation.

Note
Microsoft provides support for the current service pack and, in some cases, the immediately preceding service pack. To find the support timelines for your product, see the Lifecycle Supported Service Packs. For additional information about Microsoft Support Lifecycle Policy, see Microsoft Support Lifecycle Support Policy FAQ.

Operating System	Edition	Service Pack	System Architecture
Windows 7	Enterprise Edition	None, SP1	32-bit or 64-bit
Windows 7	Ultimate Edition	None, SP1	32-bit or 64-bit

Client RAM requirements

There are no RAM requirements that are specific to the MBAM Client installation.

Planning for MBAM 1.0 Server Deployment

The Microsoft BitLocker Administration and Monitoring (MBAM) server infrastructure depends on a set of server features that can be installed on one or more server computers, based on the requirements of your enterprise.

Planning for MBAM Server deployment

The following MBAM features represent the server infrastructure for an MBAM server deployment:

- Recovery and Hardware Database
- Compliance and Audit Database
- Compliance and Audit Reports
- Administration and Monitoring Server

MBAM server databases and features can be installed in different configurations, depending on your scalability needs. All MBAM Server features can be installed on a single server or distributed across multiple servers. Generally, we recommend that you use a three-server or five-server configuration for production environments, although configurations of two or four servers can also be used, depending on your computing needs.

Note

For more information about performance scalability of MBAM and recommended deployment topologies, see the MBAM Scalability and High-Availability Guide white paper at http://go.microsoft.com/fwlink/p/?LinkId=258314.

Each MBAM feature has specific prerequisites. For a full list of server feature prerequisites and hardware and software requirements, see MBAM 1.0 Deployment Prerequisites and MBAM 1.0 Supported Configurations.

In addition to the server-related MBAM features, the server Setup application includes an MBAM Group Policy template. This template can be installed on any computer that is able to run the Group Policy Management Console (GPMC) or Advanced Group Policy Management (AGPM).

Order of deployment of MBAM Server Features

When you deploy the MBAM Server features, install the features in the following order:

1. Recovery and Hardware Database
2. Compliance and Audit Database
3. Compliance Audit and Reports
4. Administration and Monitoring Server
5. Policy Template

Note

Keep track of the names of the computers on which you install each feature. You will use this information throughout the installation process. You can print and use a deployment checklist to assist you in the installation process. For more information about the MBAM deployment checklist, see MBAM 1.0 Deployment Checklist.

Planning for MBAM 1.0 Client Deployment

Depending on when you deploy the Microsoft BitLocker Administration and Monitoring (MBAM) Client, you can enable BitLocker encryption on a computer in your organization either before the end user receives the computer or afterwards. To enable BitLocker encryption after the end user receives the computer, configure Group Policy. To enable BitLocker encryption before the end user receives the computer, deploy the MBAM Client software by using an enterprise software deployment system.

You can use one or both methods in your organization. If you use both methods, you can improve compliance, reporting, and key recovery support.

Note

To review the MBAM Client system requirements, see MBAM 1.0 Supported Configurations.

Deploying the MBAM Client to enable BitLocker encryption after computer distribution to end users

After you configure the Group Policy, you can use an enterprise software deployment system product, such as Microsoft System Center Configuration Manager 2012 or Active Directory Domain Services, to deploy the MBAM Client installation Windows Installer files to the target computers. The two MBAM Client installation Windows Installer files are MBAMClient-64bit.msi and MBAMClient-32bit.msi, which are provided with the MBAM software. For more information about how to deploy MBAM Group Policy Objects, see Deploying MBAM 1.0 Group Policy Objects.

When you deploy the MBAM Client, after you distribute the computers to end users, the end users are prompted to encrypt their computers. This lets MBAM collect the data, to include the PIN and password, and then begin the encryption process.

Note

In this approach, users are prompted to activate and initialize the Trusted Platform Module (TPM) chip, if it has not been previously activated.

Using the MBAM Client to enable BitLocker encryption before computer distribution to end users

In organizations where computers are received and configured centrally, you can install the MBAM Client to manage BitLocker encryption on each computer before any user data is written on it. The benefit of this process is that every computer will then be compliant with the BitLocker encryption. This method does not rely on user action because the administrator has already encrypted the computer. A key assumption for this scenario is that the policy of the organization installs a corporate Windows image before the computer is delivered to the user.

If your organization wants to use (TPM) to encrypt computers, the administrator must encrypt the operating system volume of the computer with TPM protector. If your organization wants to use the TPM chip and a PIN protector, the administrator must encrypt the system volume with the TPM protector, and then the users select a PIN the first time they log on. If your organization decides to use only the PIN protector, the administrator does not have to encrypt the volume first. When users log on their computers, MBAM prompts them to provide a PIN or a PIN and a password that they will use when they restart their computer later.

Note

The TPM protector option requires for the administrator to accept the BIOS prompt to activate and initialize the TPM before delivering the computer to the user.

MBAM 1.0 Planning Checklist

You can use this checklist to plan and prepare your computing environment for Microsoft BitLocker Administration and Monitoring (MBAM) deployment.

Note

This checklist outlines the recommended steps and a high-level list of items to consider when you plan for an MBAM deployment. We recommend that you copy this checklist into a spreadsheet program and customize it for your use.

	Task	References	Notes
☐	Review the “getting started” information about MBAM to gain a basic understanding of the product before you begin the deployment planning.	Getting Started with MBAM 1.0	
☐	Plan for MBAM 1.0 Deployment	MBAM 1.0 Deployment	

	Task	References	Notes
	Prerequisites and prepare your computing environment.	Prerequisites	
☐	Plan for and configure MBAM Group Policy requirements.	Planning for MBAM 1.0 Group Policy Requirements	
☐	Plan for and create necessary Active Directory Domain Services security groups and plan for MBAM local security group membership requirements.	Planning for MBAM 1.0 Administrator Roles	
☐	Review the MBAM 1.0 Supported Configurations documentation to ensure hardware that meets MBAM installation system requirements is available.	MBAM 1.0 Supported Configurations	
☐	Plan for MBAM Server feature deployment.	Planning for MBAM 1.0 Server Deployment	
☐	Plan for MBAM Client deployment.	Planning for MBAM 1.0 Client Deployment	
☐	Validate your deployment plan in a lab environment.	Evaluating MBAM 1.0	

Deploying MBAM 1.0

Microsoft BitLocker Administration and Monitoring (MBAM) supports a number of different deployment configurations. This section of the Administrator's Guide for Microsoft BitLocker Administration and Monitoring includes information that you should consider about the deployment of MBAM and step-by-step procedures to help you successfully perform the tasks that you must complete at different stages of your deployment.

Deployment information

- Deploying the MBAM 1.0 Server Infrastructure

  This section describes the different topology options for MBAM deployment and how to use MBAM Setup to deploy MBAM Server features.

- Deploying MBAM 1.0 Group Policy Objects

  This section describes how to create and deploy the MBAM Group Policy Objects that are required to manage MBAM Clients and BitLocker encryption policies throughout the enterprise.
- Deploying the MBAM 1.0 Client

  This section describes how to use the MBAM Client Windows Installer files to deploy the MBAM Client software.
- Deploying the MBAM 1.0 Language Release Update

  This section describes how to deploy the MBAM language release update to provide support for additional non-English language user interfaces.
- MBAM 1.0 Deployment Checklist

  This section provides a deployment checklist that can help you deploy MBAM Server and MBAM Client.

Deploying the MBAM 1.0 Server Infrastructure

You can install Microsoft BitLocker Administration and Monitoring (MBAM) Server features in different configurations by using one to five servers. Generally, you should use a configuration of three to five servers for production environments, depending on your scalability needs. For more information about performance scalability of MBAM and recommended deployment topologies, see the MBAM Scalability and High-Availability Guide White Paper.

Deploy all MBAM 1.0 on a single server

In this configuration, all MBAM features are installed on a single server. This deployment topology for MBAM server infrastructure will support up to 21,000 MBAM client computers.

Important
This configuration is supported, but we recommend it for testing only.

The procedures in this section describe the full installation of the MBAM features on a single server.

How to Install and Configure MBAM on a Single Server

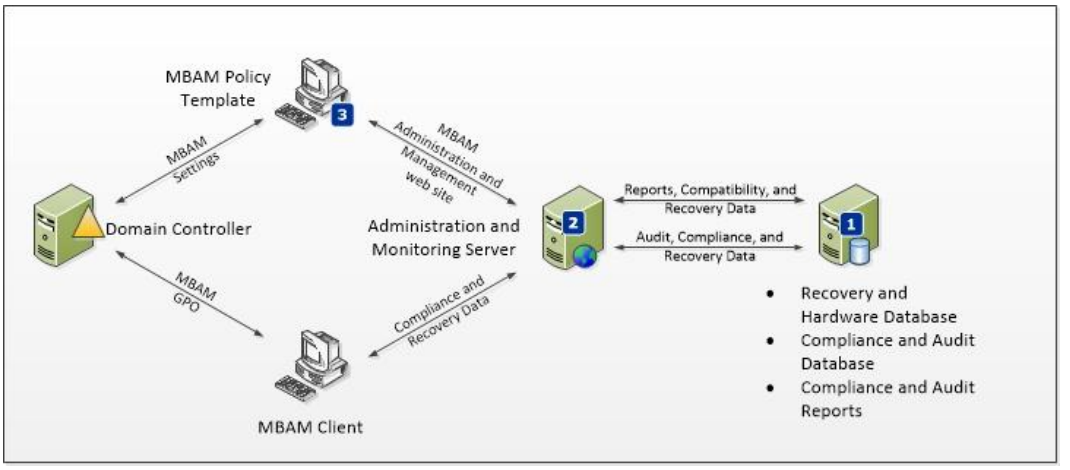
Deploy MBAM 1.0 on distributed servers

MBAM features can be installed in different configurations, depending on your scalability needs. For more information about how to plan for MBAM server feature deployment, see Planning for MBAM 1.0 Server Deployment.

The procedures in this section describe the full installation of the MBAM features on distributed servers.

Three-computer configuration

The following diagram displays the three-computer deployment topology for MBAM. We recommend this topology for production environments that support up to 55,000 MBAM Clients.

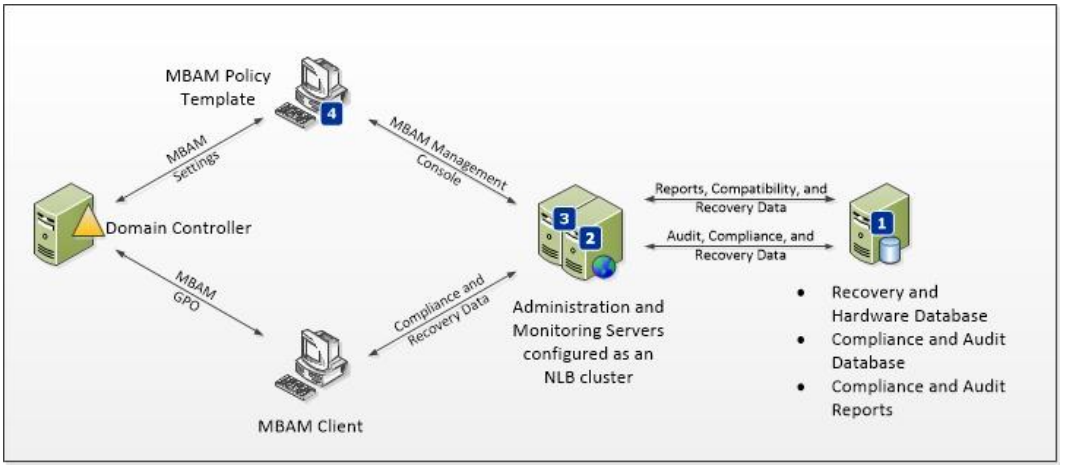


In this configuration, MBAM features are installed in the following configuration:

1. Recovery and Hardware Database, Compliance and Audit Database, and Compliance and Audit Reports are installed on a server.
2. Administration and Monitoring Server feature is installed on a server.
3. MBAM Group Policy template is installed on a computer that is capable of modifying Group Policy Objects (GPO).

Four-computer configuration

The following diagram displays the four-computer deployment topology for MBAM. We recommended this topology for production environments that support up to 110,000 MBAM Clients.

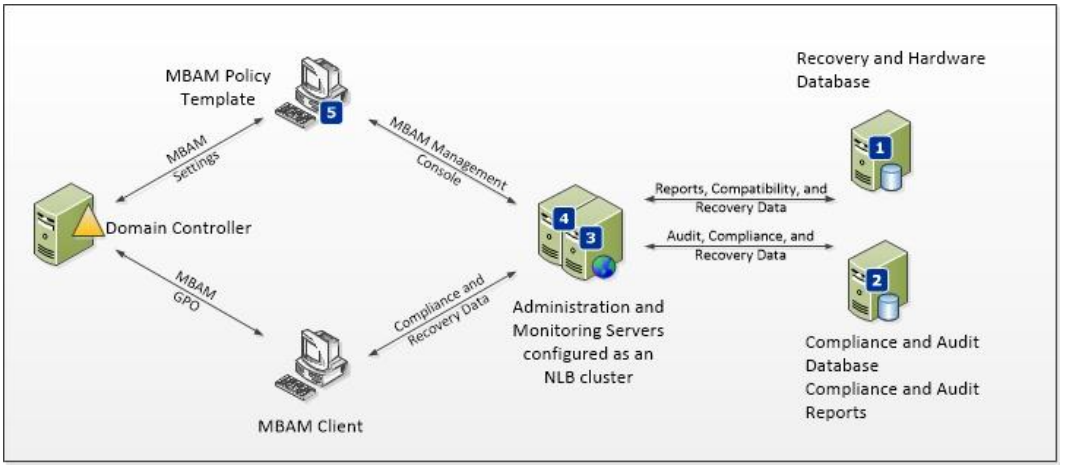


In this configuration, MBAM features are installed in the following configuration:

1. Recovery and Hardware Database, Compliance and Audit Database, and Compliance and Audit Reports are installed on a server.
2. Administration and Monitoring Server feature is installed on a server that is configured in a Network Load Balancing (NLB) Server Cluster.
3. MBAM Group Policy template is installed on a computer that is capable of modifying the Group Policy Objects.

Five-computer configuration

The following diagram displays the five-computer deployment topology for MBAM. We recommend this topology for production environments that support up to 135,000 MBAM Clients.



In this configuration, MBAM features are installed in the following configuration:

1. Recovery and Hardware Database is installed on a server.
2. The Compliance and Audit Database and Compliance and Audit Reports are installed on a server.
3. Administration and Monitoring Server feature is installed on a server that is configured in a Network Load Balancing (NLB) Server Cluster.
4. MBAM Group Policy template is installed on a computer that is capable of modifying Group Policy Objects.

How to Install and Configure MBAM on Distributed Servers

How to Configure Network Load Balancing for MBAM

How to Install and Configure MBAM on a Single Server

The procedures in this topic describe the full installation of the Microsoft BitLocker Administration and Monitoring (MBAM) features on a single server.

Each server feature has certain prerequisites. To verify that you have met the prerequisites and the hardware and software requirements, see MBAM 1.0 Deployment Prerequisites and MBAM 1.0 Supported Configurations. In addition, some features also have information that must be provided during the installation process to successfully deploy the feature. You should also review Preparing your Environment for MBAM 1.0 before you begin the MBAM deployment.

Note

To obtain the setup log files, you must install MBAM by using the **msiexec** package and the **/l** <location> option. Log files are created in the location that you specify.

Additional setup log files are created in the %temp% folder of the user who is installing MBAM.

To install MBAM Server features on a single server

The following steps describe how to install general MBAM features.

Note

Make sure that you use the 32-bit setup on 32-bit servers and the 64-bit setup on 64-bit servers.

To start MBAM Server features installation

1. Start the MBAM installation wizard. Click **Install** at the Welcome page.
2. Read and accept the Microsoft Software License Terms, and then click **Next** to continue the installation.
3. By default, all MBAM features are selected for installation. Features that will be installed on the same computer must be installed together at the same time. Clear the features that you want to install elsewhere. You must install the MBAM features in the following order:
   - Recovery and Hardware Database
   - Compliance and Audit Database
   - Compliance Audit and Reports
   - Administration and Monitoring Server
   - MBAM Group Policy Template

   Note

   The installation wizard checks the prerequisites for your installation and displays the prerequisites that are missing. If all the prerequisites are met, the installation continues. If a missing prerequisite is detected, you must resolve the missing

prerequisites, and then click **Check prerequisites again**. After all prerequisites are met, the installation resumes.

4. You are prompted to configure the network communication security. MBAM can encrypt the communication between the Recovery and Hardware Database, the Administration and Monitoring Server, and the clients. If you decide to encrypt the communication, you are asked to select the authority-provisioned certificate that will be used for encryption.
5. Click **Next** to continue.
6. The MBAM Setup wizard will display the installation pages for the selected features.

To deploy MBAM Server features

1. In the **Configure the Recovery and Hardware database** window, specify the instance of SQL Server and the name of the database that will store the recovery and hardware data. You must also specify both the database files location and the log information location.
2. Click **Next** to continue.
3. In the **Configure the Compliance and Audit database** window, specify the instance of the SQL Server and the name of the database that will store the compliance and audit data. Then, specify the database files location and the log information location.
4. Click **Next** to continue.
5. In the **Compliance and Audit Reports** window, specify the report service instance that will be used and provide a domain user account for accessing the database. This should be a user account that is provisioned specifically for this use. The user account should be able to access all data available to the MBAM Reports Users group.
6. Click **Next** to continue.
7. In the **Configure the Administration and Monitoring Server** window, enter the **Port Binding**, the **Host Name** (optional), and the **Installation Path** for the MBAM Administration and Monitoring server.

   Warning
   The port number that you specify must be an unused port number on the Administration and Monitoring server, unless a unique host header name is specified.
8. Click **Next** to continue.
9. Specify whether to use Microsoft Updates to help keep your computer secure, and then click **Next**. The Microsoft Updates option does not turn on the Automatic Updates in Windows.
10. When the Setup wizard has collected the necessary feature information, the MBAM installation is ready to start. Click **Back** to move back through the wizard if you want to review or change your installation settings. Click **Install** to begin the installation. Click **Cancel** to exit Setup. Setup installs the MBAM features and notifies you that the installation is completed.
11. Click **Finish** to exit the wizard.

12. After you install MBAM server features, you must add users to the MBAM roles. For more information, see Planning for MBAM 1.0 Administrator Roles.

To perform post installation configuration

1. After Setup is finished, you must add user roles so that you can give users access to features in the MBAM administration website. On the Administration and Monitoring Server, add users to the following local groups:
   - **MBAM Hardware Users**: Members of this local group can access the Hardware feature in the MBAM administration website.
   - **MBAM Helpdesk Users**: Members of this local group can access the Drive Recovery and Manage TPM features in the MBAM administration website. All fields in Drive Recovery and Manage TPM are required fields for a Helpdesk User.
   - **MBAM Advanced Helpdesk Users**: Members of this local group have advanced access to the Drive Recovery and Manage TPM features in the MBAM administration website. For Advanced Helpdesk Users, only the Key ID field is required in Drive Recovery. For Manage TPM users, only the Computer Domain field and Computer Name field are required.
2. On the Administration and Monitoring Server, Compliance and Audit Database, and on the computer that hosts the Compliance and Audit Reports, add users to the following local group to enable them to access the Reports feature in the MBAM administration website:
   - **MBAM Report Users**: Members of this local group can access the Reports features in the MBAM administration website.

Note

Identical user membership or group membership of the **MBAM Report Users** local group must be maintained on all computers where the Administration and Monitoring Server features, Compliance and Audit Database, and Compliance and Audit Reports are installed.

To maintain identical memberships on all computers, you should create a domain security group and add that domain group to each local MBAM Report Users group. When you do this, you can manage the group memberships by using the domain group.

Validating the MBAM Server feature installation

When the MBAM installation is complete, validate that the installation has successfully set up all the necessary MBAM features that are required for BitLocker management. Use the following procedure to confirm that the MBAM service is functional:

To validate MBAM Server feature installation

1. On each server where an MBAM feature is deployed, open **Control Panel**. Click **Programs**, and then click **Programs and Features**. Verify that **Microsoft BitLocker Administration and Monitoring** appears in the **Programs and Features** list.

   Note
   To validate the installation, you must use a Domain Account that has local computer administrative credentials on each server.

2. On the server where the Recovery and Hardware Database is installed, open SQL Server Management Studio and verify that the **MBAM Recovery and Hardware** database is installed.
3. On the server where the Compliance and Audit Database is installed, open SQL Server Management Studio and verify that the **MBAM Compliance and Audit Database** is installed.
4. On the server where the Compliance and Audit Reports are installed, open a web browser with administrative privileges and browse to the “Home” of the SQL Server Reporting Services site.

   The default Home location of a SQL Server Reporting Services site instance is at http://<*NameofMBAMReportsServer*>/Reports. To find the actual URL, use the Reporting Services Configuration Manager tool and select the instances specified during setup.

   Confirm that a folder named **Malta Compliance Reports** is listed and that it contains five reports and one data source.

   Note
   If SQL Server Reporting Services was configured as a named instance, the URL should resemble the following:http://<*NameofMBAMReportsServer*>/Reports_<*SRSInstanceName*>

5. On the server where the Administration and Monitoring feature is installed, run **Server Manager** and browse to **Roles**, select **Web Server (IIS)**, and click **Internet Information Services (IIS) Manager**
6. In **Connections**, browse to <*computername*>, select **Sites**, and select **Microsoft BitLocker Administration and Monitoring**. Verify that **MBAMAdministrationService**, **MBAMComplianceStatusService**, and **MBAMRecoveryAndHardwareService** are listed.
7. On the server where the Administration and Monitoring feature is installed, open a web browser with administrative privileges, and then browse to the following locations in the MBAM website to verify that they load successfully:
   - *http://<computername>/default.aspx* and confirm each of the links for navigation and reports
   - *http://<computername>/MBAMAdministrationService/AdministrationService.svc*
   - *http://<computername>/MBAMComplianceStatusService/StatusReportingService.svc*
   - *http://<computername>/MBAMRecoveryAndHardwareService/CoreService.svc*

Note

Typically, the services are installed on the default port 80 without network encryption. If the services are installed on a different port, change the URLs to include the appropriate port. For example, http://<*computername*>:<*port*>/default.aspx or http://<*hostheadername*>/default.aspx.

If the services are installed with network encryption, change http:// to https://.

How to Install and Configure MBAM on Distributed Servers

The procedures in this topic describe the full installation of the Microsoft BitLocker Administration and Monitoring (MBAM) features on distributed servers.

Each server feature has certain prerequisites. To verify that you have met the prerequisites and hardware and software requirements, see MBAM 1.0 Deployment Prerequisites and MBAM 1.0 Supported Configurations. In addition, some features require that you provide certain information during the installation process to successfully deploy the feature. You should also review **Planning the Server Infrastructure for MBAM** before you begin the MBAM deployment.

Note

To obtain the setup log files, you have to install MBAM by using the **msiexec** package and the **/l <location>** option. Log files are created in the location that you specify.

Additional setup log files are created in the %temp% folder of the user that runs the MBAM installation.

Deploy the MBAM Server features

The following steps describe how to install the general MBAM features.

Note

Make sure that you use the 32-bit setup on 32-bit servers and the 64-bit setup on 64-bit servers.

To Deploy MBAM Server features

1. Start the MBAM installation wizard, and click **Install** at the Welcome page.
2. Read and accept the Microsoft Software License Terms, and then click **Next** to continue the installation.
3. By default, all MBAM features are selected for installation. Clear the features that you want to install elsewhere. Features that you want to install on the same computer must be installed all at the same time. MBAM features must be installed in the following order:
   - Recovery and Hardware Database

- Compliance and Audit Database
- Compliance Audit and Reports
- Administration and Monitoring Server
- MBAM Group Policy Template

Note

The installation wizard checks the prerequisites for your installation and displays the prerequisites that are missing. If all the prerequisites are met, the installation continues. If a missing prerequisite is detected, you have to resolve the missing prerequisites, and then click **Check prerequisites again**. If all prerequisites are met this time, the installation will resume.

4. The MBAM Setup wizard will display the installation pages for the selected features. The following sections describe the installation procedures for each feature.

Note

Typically, each feature is installed on a separate server. If you want to install multiple features on a single server, you may change or eliminate some of the following steps.

To install the Recovery and Hardware Database

a. Choose an option for MBAM communication encryption. MBAM can encrypt the communication between the Recovery and Hardware Database and the Administration and Monitoring servers. If you choose the option to encrypt communication, you are asked to select the authority-provisioned certificate that is used for encryption.
b. Click **Next** to continue.
c. Specify the names of the computers that will be running the Administration and Monitoring Server feature, to configure access to the Recovery and Hardware Database.. Once the Administration and Monitoring Server feature is deployed, it connects to the database by using its domain account.
d. Click **Next** to continue.
e. Specify the **Database Configuration** for the SQL Server instance that stores the recovery and hardware data. You must also specify where the database will be located and where the log information will be located.
f. Click **Next** to continue with the MBAM Setup wizard.

To install the Compliance and Audit Database

a. Choose an option for the MBAM communication encryption. MBAM can encrypt the communication between the Compliance and Audit Database and the Administration and Monitoring servers. If you choose the option to encrypt communication, you are asked to select the authority-provisioned certificate that will be used for encryption.

b. Click **Next** to continue.

c. Specify the user account that will be used to access the database for reports.

d. Click **Next** to continue.

e. Specify the computer names of the computers that you want to run the Administration and Monitoring Server and the Compliance and Audit Reports, to configure the access to the Compliance and Audit Database.. After the Administration and Monitoring and the Compliance and Audit Reports Server are deployed, they will connect to the databases by using their domain accounts.

f. Specify the **Database Configuration** for the SQL Server instance that will store the compliance and audit data. You must also specify where the database will be located and where the log information will be located.

g. Click **Next** to continue with the MBAM Setup wizard.

To install the Compliance and Audit Reports

a. Specify the remote SQL Server instance. For example, <*ServerName*>,where the Compliance and Audit Database are installed.

b. Specify the name of the Compliance and Audit Database. By default, the database name is “MBAM Compliance Status”, but you can change the name when you install the Compliance and Audit Database.

c. Click **Next** to continue.

d. Select the SQL Server Reporting Services instance where the Compliance and Audit Reports will be installed. Provide the username and password used to access the compliance database.

e. Click **Next** to continue with the MBAM Setup wizard.

To install the Administration and Monitoring Server feature

a. Choose an option for the MBAM communication encryption. MBAM can encrypt the communication between the Recovery and Hardware Database and the Administration and Monitoring servers. If you choose the option to encrypt communication, you are asked to select the authority-provisioned certificate that is used for encryption.

b. Click **Next** to continue.

c. Specify the remote SQL Server instance, For example, <*ServerName*>, where the Compliance and Audit Database are installed.

d. Specify the name of the Compliance and Audit Database. By default, the database name is MBAM Compliance Status, but, you can change the name when you install the Compliance and Audit Database.

e. Click **Next** to continue.

f. Specify the remote SQL Server instance. For example, <*ServerName*>,where the Recovery and Hardware Database are installed.

g. Specify the name of the Recovery and Hardware Database. By default, the database name is **MBAM Recovery and Hardware**, but you can change the name when you install the Recovery and Hardware Database feature.

h. Click **Next** to continue.

i. Specify the URL for the "Home" of the SQL Server Reporting Services (SRS) site. The default Home location of a SQL Server Reporting Services site instance is at:

http://<*NameofMBAMReportsServer*>/ReportServer

Note
If you configured the SQL Server Reporting Services as a named instance, the URL resembles the following:http://<*NameofMBAMReportsServer*>/ReportServer_<*SRSInstanceName*>

j. Click **Next** to continue.

k. Enter the **Port Number**, the **Host Name** (optional), and the **Installation Path** for the MBAM Administration and Monitoring server

Warning
The port number that you specify must be an unused port number on the Administration and Monitoring server, unless you specify a unique host header name.

l. Click **Next** to continue with the MBAM Setup wizard.

5. Specify whether to use Microsoft Updates to help keep your computer secure, and then click **Next**.
6. When the selected MBAM feature information is complete, you are ready to start the MBAM installation by using the Setup wizard. Click **Back** to move through the wizard if you have to review or change your installation settings. Click **Install** to begin the installation. Click **Cancel** to exit the Wizard. Setup installs the MBAM features that you selected and notifies you that the installation is finished.
7. Click **Finish** to exit the wizard.
8. Add users to appropriate MBAM roles, after the MBAM server features are installed.. For more information, see Planning for MBAM 1.0 Administrator Roles.

Post-installation configuration

1. After MBAM Setup is finished, you must add user Roles before users can access to features in the MBAM administration website. On the Administration and Monitoring Server, add users to the following local groups.

   - **MBAM Hardware Users**: Members of this local group can access the Hardware feature in the MBAM administration website.
   - **MBAM Helpdesk Users**: Members of this local group can access the Drive Recovery and Manage Trusted Platform Modules (TPM) features in the MBAM administration

website. All fields in Drive Recovery and Manage TPM are required fields for a Helpdesk User.

- **MBAM Advanced Helpdesk Users**: Members of this local group have advanced access to the Drive Recovery and Manage TPM features in the MBAM administration website. For Advanced Helpdesk Users, only the Key ID field is required in Drive Recovery. In Manage TPM, only the Computer Domain field and Computer Name field are required.

2. On the Administration and Monitoring Server, Compliance and Audit Database, and on the server that hosts the Compliance and Audit Reports, add users to the following local group to give them access to the Reports feature in the MBAM administration website.
   - **MBAM Report Users**: Members of this local group can access the Reports in the MBAM administration website.

   Note
   Identical user or group membership of the **MBAM Report Users** local group must be maintained on all computers where the MBAM Administration and Monitoring Server features, Compliance and Audit Database, and the Compliance and Audit Reports are installed.

Validate the MBAM Server feature installation

When the MBAM Server feature installation is complete, you should validate that the installation has successfully set up all the necessary features for MBAM. Use the following procedure to confirm that the MBAM service is functional.

To validate an MBAM installation

1. On each server, where an MBAM feature is deployed, open **Control Panel**, click **Programs**, and then click **Programs and Features**. Verify that **Microsoft BitLocker Administration and Monitoring** appears in the **Programs and Features** list.

   Note
   To validate the MBAM installation, you must use a Domain Account that has local computer administrative credentials on each server.
2. On the server where the Recovery and Hardware Database is installed, open SQL Server Management Studio and verify that the **MBAM Recovery and Hardware** database is installed.
3. On the server where the Compliance and Audit Database is installed, open SQL Server Management Studio and verify that the **MBAM Compliance Status** database is installed.
4. On the server where the Compliance and Audit Reports are installed, open a web browser with administrative privileges and browse to the “Home” of the SQL Server Reporting Services site.

   The default Home location of a SQL Server Reporting Services site instance can be found at http://<*NameofMBAMReportsServer*>/Reports.aspx. To find the actual URL, use

the Reporting Services Configuration Manager tool and select the instances specified during setup.

Confirm that a folder named **Malta Compliance Reports** is listed and that it contains five reports and one data source.

Note
If SQL Server Reporting Services was configured as a named instance, the URL should resemble the following:http://*<NameofMBAMReportsServer>*/Reports_*<SRSInstanceName>*

5. On the server where the Administration and Monitoring feature is installed, run **Server Manager** and browse to **Roles**, select **Web Server (IIS)**, and then click **Internet Information Services (IIS) Manager**. In **Connections** browse to *<computername>*, click **Sites**, and click **Microsoft BitLocker Administration and Monitoring**. Verify that **MBAMAdministrationService**, **MBAMComplianceStatusService**, and **MBAMRecoveryAndHardwareService** are listed.
6. On the server where the Administration and Monitoring feature is installed, open a web browser with administrative privileges and browse to the following locations in the MBAM web site, to verify that they load successfully:
   - *http://<computername>/default.aspx* and confirm each of the links for navigation and reports
   - *http://<computername>/MBAMAdministrationService/AdministrationService.svc*
   - *http://<computername>/MBAMComplianceStatusService/StatusReportingService.svc*
   - *http://<computername>/MBAMRecoveryAndHardwareService/CoreService.svc*

   Note
   Typically, services are installed on the default port 80 without network encryption. If the services are installed on a different port, change the URLs to include the appropriate port. For example, http://*<computername>:<port>*/default.aspx or http://*<hostheadername>*/default.aspx

   If the services were installed with network encryption, change http:// to https://.

   Verify that each web page loads successfully.

How to Configure Network Load Balancing for MBAM

To verify that you have met the prerequisites and hardware and software requirements to install the Administration and Monitoring Server feature, see MBAM 1.0 Deployment Prerequisites and MBAM 1.0 Supported Configurations.

Note
To obtain the setup log files, you must install Microsoft BitLocker Administration and Monitoring (MBAM) by using the **msiexec** package and the **/l** <location> option. The Log files are created in the location that you specify.

Additional setup log files are created in the %temp% folder of the user who installs MBAM.

The Network Load Balancing (NLB) clusters for the Administration and Monitoring Server feature provides scalability in MBAM and it should support more than 55,000 MBAM client computers.

Note

Windows Server Network Load Balancing distributes client requests across a set of servers that are configured into a single server cluster. When Network Load Balancing is installed on each of the servers (hosts) in a cluster, the cluster presents a virtual IP address or fully qualified domain name (FQDN) to client requests. The initial client requests go to all the hosts in the cluster, but only one host accepts and handles the request.

All computers that will be part of a NLB cluster have the following requirements:

- All computers in the NLB cluster must be in the same domain.
- Each computer in the NLB cluster must use a static IP address.
- Each computer in the NLB cluster must have Network Load Balancing enabled.
- The NLB cluster requires a static IP address, and a host record must be manually created in the domain name system (DNS).

Configuring Network Load Balancing for MBAM Administration and Monitoring Servers

The following steps describe how to configure an NLB cluster virtual name and IP address for two MBAM Administration and Monitoring servers, and how to configure MBAM Clients to use the NLB Cluster.

Before you begin the procedures described in this topic, you must have the MBAM Administration and Monitoring Server feature successfully installed by using the same IIS port binding on two separate server computers that meet the prerequisites for both MBAM Server feature installation and NLB Cluster configuration.

Note

This topic describes the basic process of using Network Load Balancing Manager to create an NLB Cluster. The exact steps to configure a Windows Server as part of an NLB cluster depend on the Windows Server version in use.. For more information about how to create NLBs on Windows Server 2008, see Creating Network Load Balancing Clusters in the Windows Server 2008 TechNet library.

To configure an NLB Cluster Virtual Name and IP address for two MBAM Administration and Monitoring Servers

1. Click **Start**, click **All Programs**, click **Administrative Tools**, and then click **Network Load Balancing Manager**.

Note

If the NLB Manager is not present, you can install it as a Windows Server feature. You must install this feature on both MBAM Administration and Monitoring servers if you want to configure it into the NLB cluster.

2. On the menu bar, click **Cluster**, and then click **New** to open the **Cluster Parameters** dialog box.
3. In the **Cluster Parameters** dialog box, enter the information for the NLB cluster IP configuration:
   - **IP address:** NLB cluster IP address registered in DNS
   - **Subnet mask:** NLB cluster IP address subnet mask registered in DNS
   - **Full Internet name:** FQDN of NLB cluster name registered in DNS
4. Ensure that **Unicast** is selected in **Cluster operation mode**, and then click **Next**.
5. On the **Cluster IP Addresses** page, click **Next**.
6. On the **Port Rules** page, click **Edit** to define the ports that the NLB cluster will respond to and configure the ports that are used for client-to-site system communication as they are defined for the site, or click **Next** to enable the NLB cluster IP address to respond to all TCP/IP ports.

   Note

   Ensure that **Affinity** is set to **Single**.
7. On the **Connect** page, enter an MBAM Administration and Monitoring server instance host name that will be part of the NLB cluster in **Host**, and then click **Connect**.
8. In **Interfaces available for configuring a new cluster**, select the networking interface that will be configured to respond to NLB cluster communication, and then click **Next**.
9. On the **Host Parameters** page, review the information displayed to ensure that the **Dedicated IP configuration** settings display the dedicated host IP configuration for the correct NLB cluster host, check that the Initial host state **Default state:** is **Started**, and then click **Finish**.

   Note

   The **Host Parameters** page also displays the NLB cluster host priority, which is 1 through 32. As new hosts are added to the NLB cluster, the host priority must differ from the previously added hosts. The priority is automatically incremented when you use the Network Load Balancing Manager.
10. Click **<NLB cluster name>** and ensure that the NLB host interface **Status** displays **Converged** before you continue. This step might require that you refresh the NLB cluster display as the host TCP/IP configuration that is being modified by the NLB Manager.
11. To add additional hosts to the NLB cluster, right-click **<NLB cluster name>**, click **Add Host to Cluster,** and then repeat steps 7 through 10 for each site system that will be part of the NLB cluster.
12. On a computer that has MBAM Group Policy template installed, modify the MBAM Group Policy settings to configure the MBAM services endpoints to use the NLB Cluster name and the appropriate IIS port binding to access the MBAM Administration and Monitoring

Server features that are installed on the NLB Cluster computers. For more information about how to edit MBAM GPO settings, see How to Edit MBAM 1.0 GPO Settings. If the MBAM Administration and Monitoring servers are new to your environment, ensure that the required local security group memberships have been properly configured. For more information about security group requirements, see Planning for MBAM 1.0 Administrator Roles.

13. When the NLB Cluster configuration is complete, we recommend that you validate that the MBAM Administration and Monitoring NLB Cluster is functional. To do this, open a web browser on a computer other than the servers that are configured in the NLB, and ensure that you can access the MBAM Administration and Monitoring web site by using the NLB FQDN.

Deploying MBAM 1.0 Group Policy Objects

To successfully deploy Microsoft BitLocker Administration and Monitoring (MBAM), you must first determine the Group Policies that you will use in your implementation of MBAM. For more information about the various available policies, see Planning for MBAM 1.0 Group Policy Requirements. When you have determined the policies that you are going to use, you must use the MBAM 1.0 Group Policy template to create and deploy one or more Group Policy objects (GPO) that include the MBAM policy settings.

Install the MBAM 1.0 Group Policy template

In addition to providing server-related features of MBAM, the server setup application includes an MBAM Group Policy template. You can install this template on any computer that is able to run the Group Policy Management Console (GPMC) or Advanced Group Policy Management (AGPM).

How to Install the MBAM 1.0 Group Policy Template

Deploy MBAM 1.0 Group Policy settings

After you create the necessary GPOs, you must deploy the MBAM Group Policy settings to your organization’s client computers.

How to Edit MBAM 1.0 GPO Settings

Display the MBAM Control Panel in Windows

Because MBAM offers a customized MBAM control panel that can replace the default Windows BitLocker control panel, you can also choose to hide the default BitLocker Control Panel from end users by using Group Policy.

How to Hide Default BitLocker Encryption in The Windows Control Panel

How to Install the MBAM 1.0 Group Policy Template

In addition to the server-related features of Microsoft BitLocker Administration and Monitoring (MBAM), the server setup application includes an MBAM Group Policy template. You can install this template on any computer that is capable of running the Group Policy Management Console (GPMC) or Advanced Group Policy Management (AGPM).

The following steps describe how to install the MBAM Group Policy template.

Note
Make sure that you use the 32-bit setup on 32-bit servers and the 64-bit setup on 64-bit servers.

To install the MBAM Group Policy template

1. Start the MBAM installation wizard; then, click **Install** on the Welcome page.
2. Read and accept the Microsoft Software License Terms, and then click **Next** to continue the installation.
3. By default, all MBAM features are selected for installation. Clear all feature options except for **Policy Template**, and then click **Next** to continue the installation.

   Note
   The installation wizard checks the prerequisites for your installation and displays the prerequisites that are missing. If all the prerequisites are met, the installation continues. If a missing prerequisite is detected, you must resolve the missing prerequisite and then click **Check prerequisites again**. Once all prerequisites are met, the installation will resume.
4. After the MBAM Setup wizard displays installation pages for the selected features, click **Finish** to close MBAM Setup.

How to Edit MBAM 1.0 GPO Settings

To successfully deploy Microsoft BitLocker Administration and Monitoring (MBAM), you must first determine the Group Policies that you will use in your implementation of Microsoft BitLocker Administration and Monitoring. For more information about the various available policies, see Planning for MBAM 1.0 Group Policy Requirements. After you have determined the policies that you are going to use, you then must modify one or more Group Policy Objects (GPO) that include the MBAM policy settings.

The following steps describe how to configure the basic, recommended Group Policy object (GPO) settings to enable MBAM to manage BitLocker encryption for your organization's client computers.

To edit the MBAM Client GPO settings

1. On a computer that has MBAM Group Policy template installed, make sure that MBAM services are enabled.
2. Use the Group Policy Management Console (GPMC.msc) or the Advanced Group Policy Management (AGPM) MDOP product for these actions: Select **Computer configuration**, choose **Policies**, click **Administrative Templates**, select **Windows Components**, and then click **MDOP MBAM (BitLocker Management)**.
3. Edit the Group Policy Object settings that are required to enable MBAM Client services on client computers. For each policy in the table that follows, select **Policy Group**, click the **Policy**, and then configure the **Setting**.

Policy Group	Policy	Setting
Client Management	Configure MBAM Services	Enabled. Set **MBAM Recovery and Hardware service endpoint** and **Select BitLocker recovery information to store**. Set **MBAM compliance service endpoint** and **Enter status report frequency in (minutes)**.
	Allow hardware compatibility checking	Disabled. This policy is enabled by default, but is not needed for a basic MBAM implementation.
Operating System Drive	Operating system drive encryption settings	Enabled. Set **Select protector for operating system drive**. This is required to save operating system drive data to the MBAM Key Recovery server.
Removable Drive	Control Use of BitLocker on removable drives	Enabled. This is required if MBAM will save removable drive data to the MBAM Key Recovery server.
Fixed Drive	Control Use of BitLocker on fixed drives	Enabled. This is required if MBAM will save fixed drive data to the MBAM Key

		Recovery server. Set **Choose how BitLocker-protected drives can be recovered** and **Allow data recovery agent**.

Important
Depending on the policies that your organization decides to deploy, you may have to configure additional policies. See Planning for MBAM 1.0 Group Policy Requirements for Group Policy configuration details for all of the available MBAM GPO policy options.

How to Hide Default BitLocker Encryption in The Windows Control Panel

Microsoft BitLocker Administration and Monitoring (MBAM) offers a customized control panel for MBAM client computers that is named called BitLocker Encryption Options. This customized control panel can replace the default Windows BitLocker control panel that is named BitLocker Drive Encryption. The BitLocker Encryption Options control panel, located under System and Security in the Windows control panel, enables users to manage their PIN and passwords, unlock drives, and hides the interface that allows administrators to decrypt a drive or to suspend or resume BitLocker encryption.

To hide default BitLocker Encryption in the Windows Control Panel

1. Browse to **User configuration** by using the Group Policy Management Console (GPMC), the Advanced Group Policy Management (AGPM), or the Local Group Policy Editor on the BitLocker Group Policies computer.
2. Click **Policies**, select **Administrative Templates**, and then click **Control Panel**.
3. In the **Details** pane, double-click **Hide specified Control Panel items**, and then select **Enabled**.
4. Click **Show**, **click Add…**, and then type Microsoft.BitLockerDriveEncryption. This policy hides the default Windows BitLocker Management tool from the Windows Control Panel and allows the user to open the updated MBAM BitLocker Encryption Options tool from the Windows Control Panel.

Deploying the MBAM 1.0 Client

The Microsoft BitLocker Administration and Monitoring (MBAM) Client enables administrators to enforce and monitor BitLocker drive encryption on computers in the enterprise. The BitLocker client can be integrated into an organization by deploying the client through tools like Active Directory Domain Services or by directly encrypting the client computers as part of the initial imaging process.

Depending on when you deploy the MBAM Client, you can enable BitLocker encryption on a computer in your organization either before or after the end user receives the computer. To control this timing, you configure Group Policy and deploy the MBAM Client software by using an enterprise software deployment system.

You can use either or both of these methods in your organization. If you use both methods, you can improve compliance, reporting, and key recovery support.

Deploy the MBAM Client to desktop or laptop computers

After you have configured Group Policy, you can deploy the MBAM Client installation Windows Installer files to target computers. You can do this by use of an enterprise software deployment system product like Microsoft System Center 2012 Configuration Manager or Active Directory Domain Services. The two available MBAM Client installation Windows Installer files are MBAMClient-64bit.msi and MBAMClient-32bit.msi. These files are provided with the MBAM software. For more information about how to deploy MBAM Group Policy Objects, see Deploying MBAM 1.0 Group Policy Objects.

How to Deploy the MBAM Client to Desktop or Laptop Computers

Deploy the MBAM Client as part of a Windows deployment

In some organizations, new computers are received and configured centrally. This situation enables administrators to install the MBAM Client to manage BitLocker encryption on each computer before any user data is written to the computer. This approach helps to ensure that computers are properly encrypted because the administrator performs the action without reliance on end-user action. A key assumption for this scenario is that the policy of the organization installs a corporate Windows image before the computer is delivered to the user.

How to Deploy the MBAM Client as Part of a Windows Deployment

How to Deploy the MBAM Client to Desktop or Laptop Computers

The Microsoft BitLocker Administration and Monitoring (MBAM) Client enables administrators to enforce and monitor BitLocker drive encryption on computers in the enterprise. The MBAM Client can be integrated into an organization by deploying the client through tools, such as Active Directory Domain Services or an enterprise software deployment tool such as Microsoft System Center 2012 Configuration Manager.

Note

To review the MBAM Client system requirements, see MBAM 1.0 Supported Configurations.

To deploy the MBAM Client to desktop or laptop computers

1. Locate the MBAM Client installation files that are provided with the MBAM software.

2. Deploy the Windows Installer package to target computers by using Active Directory Domain Services or an enterprise software deployment tool, such as Microsoft System Center 2012 Configuration Manager.

   Note
   You should not use Group Policy to deploy the Windows Installer package.

3. Configure the distribution settings or Group Policy to run the MBAM Client installation file. After successful installation, the MBAM Client applies the Group Policy settings that are received from a domain controller to begin BitLocker encryption and management functions. For more information about MBAM Group Policy settings, see Planning for MBAM 1.0 Group Policy Requirements.

   Important
   The MBAM Client will not start BitLocker encryption actions if a remote desktop protocol connection is active. All remote console connections must be closed before BitLocker encryption will begin.

How to Deploy the MBAM Client as Part of a Windows Deployment

The Microsoft BitLocker Administration and Monitoring (MBAM) Client enables administrators to enforce and monitor BitLocker drive encryption on computers in the enterprise. The BitLocker Client can be integrated into an organization by enabling BitLocker management and encryption on client computers during the computer imaging and Windows deployment process.

Note
To review the MBAM Client system requirements, see MBAM 1.0 Supported Configurations.

Encryption of client computers with BitLocker during the initial imaging stage of a Windows deployment can lower the administrative overhead for MBAM implementation. This approach also ensures that every computer that is deployed already has BitLocker running and is configured correctly.

Warning
This topic describes how to change the Windows registry by using Registry Editor. If you change the Windows registry incorrectly, you can cause serious problems that might require you to reinstall Windows. You should make a backup copy of the registry files (System.dat and User.dat) before you change the registry. Microsoft cannot guarantee that the problems that might occur when you change the registry can be resolved. Change the registry at your own risk.

To encrypt a computer as part of Windows deployment

1. If your organization plans to use the Trusted Platform Module (TPM) protector or the TPM + PIN protector options in BitLocker, you must activate the TPM chip before the initial

deployment of MBAM. When you activate the TPM chip, you avoid a reboot later in the process, and you ensure that the TPM chips are correctly configured according to the requirements of your organization. You must activate the TPM chip manually in the computer's BIOS. Refer to the manufacturer documentation for more details about how to configure the TPM chip.

2. Install the MBAM client agent.
3. We recommend that you join the computer to a domain...
   - If the computer is not joined to a domain, the recovery password is not stored in the MBAM Key Recovery service. By default, MBAM does not allow encryption to occur unless the recovery key can be stored.
   - If a computer starts in recovery mode before the recovery key is stored on the MBAM server, the computer has to be reimaged. No recovery method is available.
4. Open a command prompt as an administrator, stop the MBAM service, and then set the service to **manual** or **on demand**. Then, run the following commands:

   net stop mbamagent

   sc config mbamagent start= demand
5. Set the registry settings for the MBAM agent to ignore Group Policy and run the TPM for **operating system only encryption** To do this, run **regedit**, and then import the registry key template from C:\Program Files\Microsoft\MDOP MBAM\MBAMDeploymentKeyTemplate.reg.
6. In regedit, go to HKLM\SOFTWARE\Microsoft\MBAM and configure the settings that are listed in the following table.

Registry entry	Configuration settings
DeploymentTime	0 = OFF
	1 = Use deployment time policy settings (default)
UseKeyRecoveryService	0 = Do not use key escrow (The next two registry entries are not required in this case.)
	1 = Use key escrow in Key Recovery system (default) Recommended: The computer must be able to communicate with the Key Recovery service. Verify that the computer can communicate with the service before you proceed.
KeyRecoveryOptions	0 = Upload Recovery Key Only
	1 = Upload Recovery Key and Key Recovery Package (default)
KeyRecoveryServiceEndPoint	Set this value to the URL for the Key Recovery web server. Example: http://<computer

	name>/MBAMRecoveryAndHardwareService/CoreService.svc.

Note
MBAM policy or registry values can be set here to override the previously set values.

7. The MBAM agent restarts the system during MBAM client deployment. When you are ready for this reboot, run the following command at a command prompt as an administrator:

   net start mbamagent

8. When the computers restarts and the BIOS prompts you to accept a TPM change, accept the change.
9. During the Windows client operating system imaging process, when you are ready to start encryption, restart the MBAM agent service. Then, to set start to **automatic**, open a command prompt as an administrator and run the following commands:

   sc config mbamagent start= auto

   net start mbamagent

10. Remove the bypass registry values. To do this, run regedit, browse to the HKLM\SOFTWARE\Microsoft registry entry, right-click the **MBAM** node, and then click **Delete**.

Deploying the MBAM 1.0 Language Release Update

Microsoft BitLocker Administration and Monitoring (MBAM) 1.0 Language Release is an update to MBAM and includes the support of new languages. The new languages are:

- English (en-us)
- French (fr)
- Italian (it)
- German (de)
- Spanish (es)
- Korean (ko)
- Japanese (ja)
- Brazilian Portuguese (pt-br)
- Russian (ru)
- Chinese Traditional (zh-tw)
- Chinese Simplified (zh-cn)

The MBAM 1.0 language update will change the version number from MBAM 1.0.1237.1 to MBAM 1.0.2001.

You do not need to reinstall all of the MBAM features in order to add these additional languages. This topic defines the steps required to add the newly supported languages.

Deploy the MBAM international release to MBAM Server features

To begin, you must update the following MBAM server features:

- Compliance and Audit Report
- Administration and Monitoring Server
- Policy Templates

Then, you must run **MbamSetup.exe** to upgrade the MBAM features that run on the same server at the same time.

How to Install the MBAM Language Update on a Single Server

How to Install the MBAM Language Update on Distributed Servers

Install the MBAM language update for Group Policies

The MBAM Group Policy templates can be installed on each management workstation or they can be copied to the Group Policy central store, in order to make the templates available to all Group Policy administrators. The policy templates cannot be directly installed on a domain controller. If you do not use a Group Policy central store, then you must copy the policies manually to each domain controller that manages MBAM Group Policy.

To add the MBAM language policies templates, copy the Group Policy language files from %SystemRoot%\PolicyDefinitions on the computer where the “Policy Templates” role was installed to the same location on the workstation computer. Here are some examples of Group Policy files:

- BitLockerManagement.admx
- BitLockerUserManagement.admx
- en-us\BitLockerManagement.adml
- en-us\BitLockerUserManagement.adml
- fr-fr\ BitLockerManagement.adml
- fr-fr\ BitLockerUserManagement.adml
- (and similarly for each supported language)

Known issues in the MBAM international release

This topic contains known issues for Microsoft BitLocker Administration and Monitoring International Release.

Known Issues in the MBAM International Release

How to Install the MBAM Language Update on a Single Server

Microsoft BitLocker Administration and Monitoring (MBAM) includes four server roles that can be run on one or more computers. However, only two MBAM Server features require the update to support installation of the MBAM 1.0 language release and the MBAM Policy Template. To update all three of the required MBAM features to be installed on one computer, perform the steps described in this topic.

To install the MBAM language update on a single server

1. Open the Internet Information Services (IIS) Management Console, go to **Sites**, and then shut down the Microsoft BitLocker Administration and Monitoring website.
2. Edit the bindings for the MBAM website, and then temporarily modify the bindings of the site. For example, change the port from 443 to 9443.
3. Locate and run the MBAM setup wizard (MBAMsetup.exe) and select the following three features:
   a. Compliance and Audit Reports
   b. Administration and Monitoring Server
   c. Group Policy Templates

   Important
   The MBAM server features must be updated in the following order: Compliance and Audit Reports first, then Administration and Monitoring Server. The Group Policy templates can be updated at any time without concern for sequence.
4. After you upgrade the server database, open the IIS Management Console and review the bindings of the Microsoft BitLocker Administration and Monitoring website.
5. Delete one of the bindings and ensure that the remaining binding has the correct host name, certificate, and port number for the MBAM enterprise configuration.
6. Restart the MBAM website.
7. Test the MBAM website functionality:
   - Open the MBAM web interface and ensure you can fetch a recovery key for a client.
   - Enforce encryption of a new or manually decrypted client computer.

     Note
     The MBAM client opens only if it can communicate with the Recovery and Hardware database.

How to Install the MBAM Language Update on Distributed Servers

Microsoft BitLocker Administration and Monitoring (MBAM) includes four server roles that can be run on one or more computers. However, only two MBAM Server features require the update to support the installation of the MBAM 1.0 language release and the MBAM Policy Template. In

configurations with the MBAM Server features installed on multiple computers, only the following server features need to be updated:

- The MBAM Compliance and Audit Reports
- The MBAM Administration and Monitoring Server

Important
The MBAM server features must be updated in this order: Compliance and Audit Reports first, and then the Administration and Monitoring Server. The MBAM Group Policy templates can be updated at any time without concern for sequence.

To install the MBAM Language Update on the MBAM Compliance and Audit Report Server feature

1. On the computer running the MBAM Compliance and Audit Report feature, locate and run the MBAM Language Update setup wizard (MBAMsetup.exe).
2. Complete the wizard for the Compliance and Audit Reports and then close the wizard.

To install the MBAM Language Update on the MBAM Administration and Monitoring Server feature

1. On the computer that is running the MBAM Administration and Monitoring feature, open the Internet Information Services (IIS) management console, go to **Sites**, and then shut down the Microsoft BitLocker Administration and Monitoring website.
2. Choose to edit the bindings for the MBAM website, and then modify the bindings of the site. For example, change the port from 443 to 9443.
3. Locate and run the MBAM Language Update setup wizard (MBAMsetup.exe). Complete the wizard for the Administration and Monitoring Server feature and then close the wizard.
4. After you upgrade the server database, open IIS Management Console and review the bindings of the Microsoft BitLocker Administration and Monitoring website.
5. Delete the old binding and ensure that the remaining binding has the correct host name, certificate, and port number for the MBAM enterprise configuration.
6. Restart the MBAM web site.
7. Test the MBAM web site functionality:
   - Open the MBAM web interface and ensure that you can obtain a recovery key for a client.
   - Enforce encryption of a new or manually decrypted client computer.

Note
The MBAM client opens only if it can communicate with the Recovery and Hardware database.

Known Issues in the MBAM International Release

This section contains known issues for Microsoft BitLocker Administration and Monitoring (MBAM) International Release.

Known Issues in the MBAM International Release

The Installation Process Does Not Specify Update

Upon updating the Microsoft BitLocker Administration and Monitoring server or servers, the Setup program does not state that an update is being installed.

Workaround: None.

Certificates Used for the Administration and Monitoring Server Role

If you are using a certificate for authentication between MBAM servers, after updating the MBAM Administration and Monitoring server you must ensure that the certificate is valid and not revoked or expired.

Workaround: None.

MBAM Svclog File Filling Disk Space

If you have followed Knowledge Base article 2668170, http://support.microsoft.com/kb/2668170, you might have to repeat the KB steps after you install this update.

Workaround: None.

MBAM 1.0 Deployment Checklist

This checklist is designed to facilitate your deployment of Microsoft BitLocker Administration and Monitoring (MBAM).

Note
This checklist outlines the recommended steps and provides a high-level list of items to consider when you deploy the MBAM features. We recommend that you copy this checklist into a spreadsheet program and customize it for your specific needs.

	Task	References	Notes
☐	Complete the planning phase to prepare the computing environment for MBAM deployment.	MBAM 1.0 Planning Checklist	
☐	Review the information on MBAM supported configurations to make sure that your selected client and server computers are supported for MBAM feature installation.	MBAM 1.0 Supported Configurations	

	Task	References	Notes
☐	Run MBAM Setup to deploy MBAM Server features in the following order: 1. Recovery and Hardware Database 2. Compliance Status Database 3. Compliance Audit and Reports 4. Administration and Monitoring Server 5. MBAM Group Policy Template **Note** Keep track of the names of the servers each feature is installed on. You will use this information throughout the installation process.	Deploying the MBAM 1.0 Server Infrastructure	
☐	Add Active Directory Domain Services security groups created during the planning phase to the appropriate local MBAM Server feature administrators groups on the appropriate servers.	Planning for MBAM 1.0 Administrator Roles and How to Manage MBAM Administrator Roles	
☐	Create and deploy the required MBAM Group Policy Objects.	Deploying MBAM 1.0 Group Policy Objects	
☐	Deploy the MBAM Client software.	Deploying the MBAM 1.0 Client	

Operations for MBAM 1.0

This section of the Administrator's Guide for Microsoft BitLocker Administration and Monitoring (MBAM) includes information about the various types of Microsoft BitLocker Administration and Monitoring administration and operating tasks that are typically performed by an administrator. This section also includes step-by-step procedures to help you successfully perform those tasks.

Operations information

- Administering MBAM 1.0 Features

  After you complete all necessary MBAM planning and deploying, you can configure and use MBAM features to manage enterprise BitLocker encryption. The information in this section describes post-installation day-to-day MBAM feature operations and maintenance tasks.

- Monitoring and Reporting BitLocker Compliance with MBAM 1.0

  This section describes how to generate and understand the various MBAM reports to help you monitor the BitLocker usage and compliance activities throughout your enterprise environment.

- Performing BitLocker Management with MBAM

  This section describes post-installation day-to-day BitLocker encryption management tasks that are accomplished by using MBAM.

- Maintaining MBAM 1.0

  This section describes how to configure MBAM to run in a highly available manner. It also describes how to use MBAM to manage enterprise BitLocker encryption operations. The information in this section describes high availability options for MBAM, as well as how to move MBAM Server features if necessary.

- Security and Privacy for MBAM 1.0

  This section provides an overview of MBAM security considerations and explains many of the data collection and use practices of MBAM.

- Administering MBAM 1.0 by Using PowerShell

  This section describes the set of Windows PowerShell cmdlets that are available for administrators to perform various MBAM server tasks from the command prompt rather than from the MBAM administration website.

Administering MBAM 1.0 Features

After you complete all necessary Microsoft BitLocker Administration and Monitoring (MBAM) planning and deployment, you can configure and use MBAM to manage enterprise BitLocker encryption. The information in this section describes post-installation day-to-day MBAM feature operations tasks.

Manage MBAM Administrator Roles

After MBAM Setup is complete for all server features, administrative users must be granted access to these server features. As a best practice, administrators who will manage or use MBAM server features, should be assigned to Active Directory security groups and then those groups should be added to the appropriate MBAM administrative local group.

How to Manage MBAM Administrator Roles

Manage Hardware Compatibility

The MBAM Hardware Compatibility feature can help you to ensure that only the computer hardware that you specify as supporting BitLocker will be encrypted. When this feature is turned on, bit_admmontla will encrypt only computers that are marked as Compatible.

Important
When this feature is turned off, all computers where the MBAM policy is deployed will be encrypted.

MBAM can collect information on both the make and model of client computers if you deploy the “Allow Hardware Compatibility Checking” Group Policy. If you configure this policy, the MBAM agent reports the computer make and model information to the MBAM Server when the MBAM Client is deployed on a client computer.

How to Manage Hardware Compatibility

How to Manage User BitLocker Encryption Exemptions

Manage BitLocker encryption exemptions

MBAM can grant two forms of exemption from BitLocker encryption: computer exemption and user exemption. Computer exemption is typically used when a company has computers that do not have to be encrypted, such as computers that are used in development or testing, or older computers that do not support BitLocker. In some cases, local law may also require that certain computers are not encrypted. You may also choose to exempt users who do not need or want their drives encrypted.

How to Manage Computer BitLocker Encryption Exemptions

Manage MBAM Client BitLocker Encryption Options by using the Control Panel

If enabled through a Group Policy Objects (GPO), a custom MBAM control panel that is named BitLocker Encryption Options will be available under **System and Security**. This customized control panel replaces the default Windows BitLocker control panel. The MBAM control panel enables you to unlock encrypted drives (fixed and removable), and also helps you manage your PIN or password.

How to Manage MBAM Client BitLocker Encryption Options by Using the Control Panel

How to Manage MBAM Administrator Roles

After Microsoft BitLocker Administration and Monitoring (MBAM) Setup is complete for all server features, administrative users must be granted access to these server features. As a best practice, administrators who will manage or use MBAM server features, should be assigned to

Active Directory security groups and then those groups should be added to the appropriate MBAM administrative local group.

To manage MBAM Administrator Role memberships

1. Assign administrative users to security groups in Active Directory Domain Services.
2. Add Active Directory Domain Services security groups to the roles for MBAM administrative local groups on the Microsoft BitLocker Administration and Monitoring server for the respective features. The user roles are as follows:
   - **MBAM System Administrators** have access to all Microsoft BitLocker Administration and Monitoring features in the MBAM administration website.
   - **MBAM Hardware Users** have access to the Hardware Compatibility features in the MBAM administration website.
   - **MBAM Helpdesk Users** have access to the Manage TPM and Drive Recovery options in the MBAM administration website, but must fill in all fields when they use either option.
   - **MBAM Report Users** have access to the Compliance and Audit reports in the MBAM administration website.
   - **MBAM Advanced Helpdesk Uses** have access to the Manage TPM and Drive Recovery options in the MBAM administration website. These users are not required to fill in all fields when they use either option.

   For more information about roles for Microsoft BitLocker Administration and Monitoring, see Planning for MBAM 1.0 Administrator Roles.

How to Manage Hardware Compatibility

Microsoft BitLocker Administration and Monitoring (MBAM) can collect information about the manufacturer and model of client computers after you deploy the Allow Hardware Compatibility Checking Group Policy. If you configure this policy, the MBAM agent reports the computer make and model information to the MBAM Server when the MBAM Client is deployed on a client computer.

The Hardware Compatibility feature is helpful when your organization has older computer hardware or computers that do not support Trusted Platform Module (TPM) chips. In these cases, you can use the Hardware Compatibility feature to ensure that BitLocker encryption is applied only to computer models that support it. If all computers in your organization will support BitLocker, you do not have to use the Hardware Compatibility feature.

Note

By default, MBAM Hardware Compatibility feature is not enabled. To enable it, select the **Hardware Compatibility** feature under the **Administration and Monitoring Server** feature during setup. For more information about how to set up and configure Hardware Compatibility, see Deploying the MBAM 1.0 Server Infrastructure.

The Hardware Compatibility feature works in the following way.

1. The MBAM client agent discovers basic computer information such as manufacturer, model, BIOS maker, BIOS version, TPM maker, and TPM version, and then passes this information to the MBAM server.
2. The MBAM server generates a list of client computer makes and models to enable you to differentiate between those that can or cannot support BitLocker
3. The MBAM client agents that are deployed in the enterprise automatically update this list with all new computer makes and models that are discovered with a state of **Unknown**. An administrator can then use the MBAM administration website to change list entries to specify a particular computer make and model as **Compatible** or **Incompatible**.
4. Before the MBAM client agent begins encrypting a drive, the agent first verifies the BitLocker encryption compatibility of the hardware it is running on.
    - If the hardware is marked as compatible, the BitLocker encryption process starts. MBAM will also recheck the hardware compatibility status of the computer one time per day.
    - If the hardware is marked as incompatible, the agent logs an event and passes a “hardware exempted” state as part of compliance reporting. The agent checks every seven days to see whether the state has changed to “compatible.”
    - If the hardware is marked as unknown, the BitLocker encryption process will not begin. The MBAM client agent will recheck the hardware compatibility status of the computer one time per day.

Warning

If the MBAM client agent tries to encrypt a computer that does not support BitLocker drive encryption, there is a possibility that the computer will become corrupted. Ensure that the hardware compatibility feature is correctly configured when your organization has older hardware that does not support BitLocker.

To manage hardware compatibility

1. Open a web browser and navigate to the Microsoft BitLocker Administration and Monitoring website. Select **Hardware** in the left menu bar.
2. On the right pane, click **Advanced Search**, and then filter to display a list of all computer models that have a **Capability** status of **Unknown**. A list of computer models matching the search criteria is displayed. Administrators can add, edit, or remove new computer types from this page.
3. Review each unknown hardware configuration to determine whether the configuration should be set to **Compatible** or **Incompatible**.
4. Select one or more rows, and then click either **Set Compatible** or **Set Incompatible** to set the BitLocker compatibility, as appropriate, for the selected computer models. If set to **Compatible**, BitLocker tries to enforce drive encryption policy on computers that match the supported model. If set to **Incompatible**, BitLocker will not enforce drive encryption policy on those computers.

Note
After you set a computer model as compatible, it can take more than twenty-four hours for the MBAM Client to begin BitLocker encryption on the computers matching that hardware model.

5. Administrators should regularly monitor the hardware compatibility list to review new models that are discovered by the MBAM agent, and then update their compatibility setting to **Compatible** or **Incompatible** as appropriate.

How to Manage Computer BitLocker Encryption Exemptions

Microsoft BitLocker Administration and Monitoring (MBAM) can be used to exempt certain computers from BitLocker protection. For example, an organization may decide to control BitLocker exemption on a computer-by-computer basis.

To exempt a computer from BitLocker encryption, you must add the computer to a security group in Active Directory Domain Services in order to bypass any computer-based BitLocker protection rules.

Note
If the computer is already BitLocker-protected, the computer exemption policy has no effect.

To exempt a computer from BitLocker encryption

1. Add the computer account that you want to be exempted to a security group in Active Directory Domain Services. This allows you to bypass any computer-based BitLocker protection rules.
2. Create a Group Policy Object by using the MBAM Group Policy template, then associate the Group Policy Object with the Active Directory group that you created in the previous step. For more information about creating the necessary Group Policy Objects, see Deploying MBAM 1.0 Group Policy Objects.
3. When an exempted computer starts, the MBAM client checks the Computer Exemption Policy setting and suspends protection based on whether the computer is part of the BitLocker exemption security group.

How to Manage User BitLocker Encryption Exemptions

Microsoft BitLocker Administration and Monitoring (MBAM) can be used to manage BitLocker protection by exempting users who do not need or want their drives encrypted.

To exempt users from BitLocker protection, an organization must first create an infrastructure to support such exemptions. The supporting infrastructure might include a contact telephone number, webpage, or mailing address to request exemption. Also, any exempt user will have to be added to a security group for Group Policy created specifically for exempted users. When members of this security group log on to a computer, the user Group Policy shows that the user is

exempted from BitLocker protection. The user policy overwrites the computer policy, and the computer will remain exempt from BitLocker encryption.

Note

If the computer is already BitLocker-protected, the user exemption policy has no effect.

The following table shows how BitLocker protection is applied based on how exemptions are set.

User Status	Computer Not Exempt	Computer Exempt
User not exempt	BitLocker protection is enforced on the computer.	BitLocker protection is not enforced on the computer.
User exempt	BitLocker protection is not enforced on the computer.	BitLocker protection is not enforced on the computer.

To exempt a user from BitLocker Encryption

1. Create an Active Directory Domain Services security group that will be used to manage user exemptions from BitLocker encryption.
2. Create a Group Policy Object setting by using the MBAM Group Policy template. Associate the Group Policy Object with the Active Directory group that you created in the previous step. For more information about the necessary policy settings to enable users to request exemption from BitLocker encryption, see the Configure User Exemption Policy section in Planning for MBAM 1.0 Group Policy Requirements.
3. After creating a security group for BitLocker-exempted users, add to this group the names of the users who are requesting exemption. When a user logs on to a computer controlled by BitLocker, the MBAM client will check the User Exemption Policy setting and will suspend protection based on whether the user is part of the BitLocker exemption security group.

   Note

   Shared computer scenarios require special consideration regarding user exemption. If a non-exempt user logs on to a computer shared with an exempt user, the computer may be encrypted.

To enable users to request exemption from BitLocker Encryption

1. After you have configured user-exemption policies by usingwith the MBAM Policy template, a user can request exemption from BitLocker protection through the MBAM client.
2. When a user logs on to a computer that is marked as **Compatible** in the MBAM Hardware Compatibility list, the system presents the user with a notification that the computer is going to be encrypted. The user can select **Request Exemption** and postpone the encryption by selecting **Later**, or select **Start** to accept the BitLocker encryption.

Note
Selecting **Request Exemption** will postpone the BitLocker protection until the maximum time set in the User Exemption Policy.

3. When a user selects **Request Exemption**, the user is notified to contact the organization's BitLocker administration group. Depending on how the Configure User Exemption Policy is configured, users are provided with one or more of the following contact methods:
   - Phone Number
   - Webpage URL
   - Mailing Address

   After submittal of the request, the MBAM Administrator can decide if it is appropriate to add the user to the BitLocker Exemption Active Directory group.

   Note
   Once the postpone time limit from the User Exemption Policy has expired, users will not see the option to request exemption to the encryption policy. At this point, users must contact the MBAM administrator directly in order to receive exemption from BitLocker Protection.

How to Manage MBAM Client BitLocker Encryption Options by Using the Control Panel

A Microsoft BitLocker Administration and Monitoring (MBAM) control panel application, called BitLocker Encryption Options, will be available under **System and Security** when the MBAM Client is installed. This customized MBAM control panel replaces the default Windows BitLocker control panel. The MBAM control panel enables you to unlock encrypted drives (fixed and removable), and also helps you manage your PIN or password. For more information about enabling the MBAM control panel, see How to Hide Default BitLocker Encryption in The Windows Control Panel.

Note
For the BitLocker client, the Admin and Operational log files are located in Event Viewer, under **Application and Services Logs** / **Microsoft** / **Windows** / **BitLockerManagement**.

To use the MBAM Client Control Panel

1. To open BitLocker Encryption Options, click **Start**, and then select **Control Panel**. When **Control Panel** opens, select **System and Security**.
2. Double-click **BitLocker Encryption Options** to open the customized MBAM control panel. You will see a list of all the hard disk drives on the computer and their encryption

status. You will also see an option to manage your PIN or passwords.

3. Use the list of hard disk drives on the computer to verify the encryption status, unlock a drive, or request an exemption for BitLocker protection if the User and Computer Exemption policies have been deployed.
4. Non-administrators can use the BitLocker Encryption Options control panel to manage PINs or passwords. A user can select **Manage PIN,** and then enter both a current PIN and a new PIN. Users can also confirm their new PIN. The **Update PIN** function will reset the PIN to the new one that the user selects.
5. To manage your password, select **Unlock drive** and enter your current password. As soon as the drive is unlocked, select **Reset Password** to change your current password.

Monitoring and Reporting BitLocker Compliance with MBAM 1.0

If you use Microsoft BitLocker Administration and Monitoring (MBAM), you can generate various reports to monitor BitLocker usage and compliance activities.

Understand MBAM reports

MBAM reports have many fields that you should be familiar with before you generate MBAM reports.

Understanding MBAM Reports

Generate MBAM Reports

If you use MBAM reporting, you can generate reports on enterprise compliance, individual computers, hardware compatibility, and key recovery activity.

How to Generate MBAM Reports

Understanding MBAM Reports

Microsoft BitLocker Administration and Monitoring (MBAM) generates various reports to monitor BitLocker usage and compliance. This topic describes the MBAM reports for enterprise compliance, individual computers, hardware compatibility, and key recovery activity.

Understanding Reports

To access the Reports feature of MBAM, open the MBAM administration website. Select **Reports** in the navigation pane. Then, in the main content pane, click the tab for your report type: **Enterprise Compliance Report**, **Computer Compliance Report**, **Hardware Audit Report**, or **Recovery Audit Report**.

Enterprise Compliance Report

An Enterprise Compliance Report provides information on overall BitLocker compliance in your organization. The available filters for this report allow you to narrow your search results according to Compliance state and Error status. This report runs every six hours.

Enterprise Compliance Report fields

Column Name	Description
Computer Name	The user-specified DNS name that is being managed by MBAM.
Domain Name	The fully qualified domain name where the client computer resides and is managed by MBAM.
Compliance Status	The state of compliance for the computer, according to the policy specified for the computer. The possible states are Noncompliant and Compliant. For more information, see Enterprise Compliance Report Compliance States in this topic.
Exemption	The state of the computer hardware for determining the identification of the hardware type and whether the computer is exempt from policy. There are three possible states: Hardware Unknown (the hardware type has not been identified by MBAM), Hardware Exempt (the hardware type was identified and was marked as exempt from MBAM policy), and Not Exempt (the hardware was identified and is not exempt from policy).
Device Users	Known users on the computer that is being managed by MBAM.
Compliance Status Details	Error and status messages about the compliance state of the computer in accordance to the specified policy.
Last Contact	Date and time when the computer last contacted the server to report compliance status. This time is configurable. See MBAM policy settings.

Enterprise Compliance Report Compliance states

Compliance Status	Exemption	Description	User Action
Noncompliant	Not Exempt	The computer is noncompliant according to the specified policy, and the hardware type has not been indicated as exempt from policy.	Click **Computer Name** to expand the Computer Compliance Report and determine whether the state of each drive complies with the specified policy. If the encryption state indicates that the computer is not encrypted, encryption might still be in process, or there might be an error on the computer. If there is no error, the likely cause is that the computer is still in the process of connecting or establishing the encryption status. Check back later to determine if the state changes.
Compliant	Not Exempt	The computer is compliant in accordance with the specified policy.	No Action needed. Optionally, you can view the Computer Compliance Report to confirm the state of the computer.
Compliant	Hardware Exempt	If the Hardware type is exempt. Regardless of how the policy is set or the individual status of each hard-drive, the overall state is considered to be	No action needed.

Compliance Status	Exemption	Description	User Action
		compliant.	
Compliant	Hardware Unknown	MBAM recognizes the hardware type, but MBAM does not know whether it is exempt or not exempt. This occurs if the administrator has not set the Compatible status for the hardware. Therefore, MBAM reverts to Compliant status by default.	This is the initial state of a newly deployed MBAM client. It is typically only a transient state. Even if the administrator has marked the Hardware as Compatible, there can be a significant delay or configurable wait time before the client computer reports back in. Make note of the time of Last Contact, and check in again after the specified interval to see if the state has changed. If the state has not changed, there may be an error for this computer or hardware type.

Computer Compliance Report

The Computer Compliance Report displays information that is specific to a computer or user.

The Computer Compliance Report provides detailed encryption information and applicable policies for each drive on a computer, including operating system drives and fixed data drives. To view this report type, click the computer name in the Enterprise Compliance Report or type the computer name in the Computer Compliance Report. To view the details of each drive, expand the Computer Name entry.

Note

This report does not provide encryption status for Removable Data Volumes.

Computer Compliance Report fields

Column Name	Description
Computer Name	The user-specified DNS computer name that is being managed by MBAM.
Domain Name	The fully qualified domain name where the client computer resides and is managed by MBAM.
Computer Type	The portability type of computer. Valid types are non-Portable and Portable.
Operating System	Operating System type installed on the MBAM managed client computer.
Compliance Status	The overall Compliance Status of the computer managed by MBAM. Valid states are Compliant and Noncompliant. While it is possible to have Compliant and Noncompliant drives in the same computer, this field indicates the overall computer compliance per specified policy.
Policy Cypher Strength	The Cipher Strength selected by the Administrator during MBAM policy specification. For example, 128-bit with Diffuser
Policy Operating System Drive	Indicates whether encryption is required for the O/S and the protector type as applicable.
Policy Fixed Data Drive	Indicates whether encryption is required for the Fixed Drive.
Policy Removable Data Drive	Indicates whether encryption is required for the Removable Drive.
Device Users	Provides the identity of known users on the computer.
Exemption	Indicates whether the computer hardware type is recognized by MBAM and, if known, whether the computer has been indicated as exempt from policy. There are three states: Hardware Unknown (the hardware type has not been identified by MBAM); Hardware Exempt (the hardware type was identified and was marked as exempt from MBAM policy); and Not Exempt

Column Name	Description
	(the hardware was identified and is not exempt from policy).
Manufacturer	The computer manufacturer name as it appears in the computer BIOS.
Model	The computer manufacturer model name as it appears in the computer BIOS.
Compliance Status Details	Error and status messages of the compliance state of the computer in accordance with the specified policy.
Last Contact	Date and time that the computer last contacted the server to report compliance status. T

Computer Compliance Report Drive fields

Column Name	Description
Drive Letter	Computer drive letter that was assigned to this particular drive by the user.
Drive Type	Type of drive. Valid values are Operating System Drive and Fixed Data Drive. These are physical drives rather than logical volumes.
Cypher Strength	Cipher Strength selected by the Administrator during MBAM policy specification.
Protector Type	Type of protector selected via policy used to encrypt an operating system or Fixed volume. The valid protector types on an operating system drive are TPM or TPM+PIN. The only valid protector type for a Fixed Data Volume is Password.
Protector State	This field indicates whether the computer has enabled the protector type specified in the policy. The valid states are ON or OFF.
Encryption State	This is the current encryption state of the drive. Valid states are Encrypted, Not Encrypted, and Encrypting.
Compliance Status	Indicates whether the drive is in accordance with the policy. States are Noncompliant and

Column Name	Description
	Compliant.
Compliance Status Details	Contains error and status messages regarding the compliance state of the computer.

Hardware Audit Report

This report can help you audit changes to the Hardware Compatibility status of specific computer makes and models. To help you narrow your search results, this report includes filtering on criteria such as type of change and time of occurrence. Each state change is tracked by user and date and time. The Hardware Type is automatically populated by the MBAM agent that runs on the client computer. This report tracks user changes to the information collected directly from the MBAM managed computer. A typical administrative change is changing from Compatible to incompatible. However, the administrator can also revise any field.

Hardware Audit Report fields

Column Name	Description
Date and Time	Date and time that a change was made to the Hardware Type. Note that every unique hardware type is assigned to at least one entry.
User	Administrative user that has made the change for the particular entry.
Change Type	Type of change that was made to the hardware type information. Valid values are Addition (new entry), Update (change existing entry), or Deletion (remove existing entry).
Original Value	Value of the hardware type specification before the change was made.
Current Value	Value of the hardware type specification after the change was made.

Recovery Audit Report

The Recovery Audit Report can help you audit users who have requested access to recovery keys. The filter criteria for this report includes type of user making the request, type of key requested, time of occurrence, success or fail, time of occurrence, and type of user requesting (help desk, end user). This report enables administrators to produce contextual reports based on need.

Recovery Audit Report Fields

Column Name	Description
Request Date and Time	The date and time that a key retrieval request was made by an end user or help desk user.
Request Status	Status of the request. Valid statuses are either Successful (the key was retrieved) or Failed (the key was not retrieved).
Helpdesk User	The help desk user who initiated the request for key retrieval. If the help desk user retrieves the key on behalf of an end user, the End User field will be blank.
User	The end user who initiated the request for key retrieval.
Key Type	The type of key that was requested. MBAM collects three key types: Recovery Key Password (to recovery a computer in recovery mode); Recovery Key ID (to recover a computer in recovery mode on behalf of another user); and Trusted Platform Module (TPM) Password Hash (to recover a computer with a locked TPM).
Reason Description	The reason that the specified Key Type was requested. The reasons are specified in the Drive Recovery and Manage TPM features of the Administrative web site. Valid entries include user-entered text or one of the following reason codes: • Operating System Boot Order changed • BIOS changed • Operating System files changed • Lost Startup key • Lost PIN • TPM Reset • Lost Passphrase • Lost Smartcard • Reset PIN lockout

Column Name	Description
	• Turn on TPM • Turn off TPM • Change TPM password • Clear TPM

Note
To save report results to a file, click the **Export** button on the reports menu bar.

How to Generate MBAM Reports

Microsoft BitLocker Administration and Monitoring (MBAM) generates various reports to monitor BitLocker encryption usage and compliance. This topic describes how to open the MBAM administration website and how to generate MBAM reports on enterprise compliance, individual computers, hardware compatibility, and key recovery activity. For more information about MBAM reports, see Understanding MBAM Reports.

Note
To run the reports, you must be a member of the **Report Users** role on the computers where you have installed the Administration and Monitoring Server features, Compliance and Audit Database, and Compliance and Audit Reports.

To open the MBAM Administration website

1. Open a web browser and navigate to the MBAM website. The default URL for the website is *http://<computername>* of the Microsoft BitLocker Administration and Monitoring server.

   Note
   If the MBAM administration website was installed on a port other than port 80, you must specify that port number in the URL. For example, *http://<computername>:<port>*. If you specified a Host Name for the MBAM administration website during the installation, the URL would be *http://<hostname>*.

2. In the navigation pane, click **Reports**. In the main pane, click the tab for your report type: **Enterprise Compliance Report**, **Computer Compliance Report**, **Hardware Audit Report**, or **Recovery Audit Report**.

Note

Historical MBAM Client data is retained in the compliance database. This retained data may be needed in case a computer is lost or stolen. When running enterprise reports, you should use appropriate start and end dates to scope the time frames for the reports from one to two weeks to increase the reporting data accuracy.

To generate an enterprise Compliance Report

1. On the MBAM administration website, click **Reports** in the navigation pane, then click the **Enterprise Compliance Report** tab and select the appropriate filters for your report. For the Enterprise Compliance Report, you can set the following filters.
   - **Compliance Status**. Use this filter to specify the compliance status types (for example, Compliant or Noncompliant) to include in the report.
   - **Error State**. Use this filter to specify the Error State types, such as No Error or Error, to include in the report.
2. Click **View Report** to display the specified report.

   The report results can be saved in any of several available file formats such as HTML, Microsoft Word, and Microsoft Excel.

   Note

   The Enterprise Compliance report is generated by a SQL job that runs every six hours. Therefore, the first time you try to view the report you may find that some data is missing.
3. To view information about a computer in the Computer Compliance Report, select the computer name.
4. Select the plus sign (+) next to the computer name to view information about the volumes on the computer.

To generate the Computer Compliance Report

1. In the MBAM administration website, select the **Report** node in the navigation pane, and then select the **Computer Compliance Report**. Use the Computer Compliance report to search for **user name** or **computer name**.
2. Click **View Report** to view the computer report.

   Results can be saved in any of several available file formats such as HTML, Microsoft Word, and Microsoft Excel.
3. To display more information about a computer in the Computer Compliance Report, select the computer name.

4. Select the plus sign (+) next to the computer name to view information about the volumes on the computer.

Note

An MBAM Client computer is considered compliant if the computer matches the requirements of the MBAM policy settings or the computer's hardware model is set to incompatible. Therefore, when you are viewing detailed information about the disk volumes associated with the computer, computers that are exempt from BitLocker encryption due to hardware compatibility can be displayed as compliant even though their drive volume encryption status is displayed as noncompliant.

To generate the Hardware Compatibility Audit Report

1. From the MBAM administration website, select the **Report** node from the navigation pane, and then select the **Hardware Audit Report**. Select the appropriate filters for your Hardware Audit report. The Hardware Audit report offers the following available filters:
   - **User (Domain\User)**. Specifies the name of the user who made a change.
   - **Change Type**. Specifies the type of changes you are looking for.
   - **Start Date**. Specifies the Start Date part of the date range that you want to report on.
   - **End Date**. Specifies the End Date part of the date range that you want to report on.
2. Click **View Report** to view the report.

   Results can be saved in several available file formats such as HTML, Microsoft Word, and Microsoft Excel.

To generate the Recovery Key Audit Report

1. From the MBAM administration website, select the **Report** node in the navigation pane, and then select the **Recovery Audit Report**. Select the filters for your Recovery Key Audit report. The available filters for Recovery Key audits are as follows:
   - **Requestor**. Specifies the user name of the requestor. The requestor is the person in the help desk who accessed the key on behalf of a user.
   - **Requestee**. Specifies the user name of the requestee. The requestee is the person who called the help desk to obtain a recovery key.
   - **Request Result** Specifies the request result types, such as: Success or Failed. For example, you may want to view failed key access attempts.
   - **Key Type**. Specifies the Key Type, such as: Recovery Key Password or TPM Password Hash.
   - **Start Date**. Specifies the Start Date part of the date range.
   - **End Date**. Specifies the End Date part of the date range.
2. Click **View Report** to display the report.

   Results can be saved in several available file formats such as HTML, Microsoft Word, and Microsoft Excel.

Performing BitLocker Management with MBAM

After you deploy Microsoft BitLocker Administration and Monitoring (MBAM), you can configure and use MBAM to manage enterprise BitLocker encryption. This section describes post-installation, day-to-day BitLocker encryption management tasks that can be accomplished by using MBAM.

Reset a TPM Lockout with MBAM

A Trusted Platform Module (TPM) microchip provides basic security-related functions. These functions are accomplished primarily by the use of encryption keys. The TPM is typically installed on the motherboard of a computer or laptop and communicates with the rest of the system by using a hardware bus. Computers that incorporate a TPM can create cryptographic keys that can be decrypted only by the TPM. A TPM lockout can occur if a user enters an incorrect PIN too many times. The number of times that a user can enter an incorrect PIN before the TPM locks varies from manufacturer to manufacturer. The Key Recovery data system on the MBAM administration website enables you to obtain a reset TPM owner password file.

How to Reset a TPM Lockout

Recover drives with MBAM

Make sure that you know how to attempt data recovery from encrypted drives in the event of hardware failure, changes in personnel, or other situations in which encryption keys are lost. The Encrypted Drive Recovery features of MBAM provide the capture and storage of data and availability of tools required to access a BitLocker-protected volume when the volume goes into recovery mode, is moved, or becomes corrupted.

How to Recover a Drive in Recovery Mode

How to Recover a Moved Drive

How to Recover a Corrupted Drive

Determine BitLocker Encryption State of lost computers by Using MBAM

When you use MBAM, you can determine the last known BitLocker encryption status of computers that were lost or stolen.

How to Determine the BitLocker Encryption State of a Lost Computers

How to Reset a TPM Lockout

The Encrypted Drive Recovery feature of Microsoft BitLocker Administration and Monitoring (MBAM) encompasses both the capture and storage of data and the availability for tools that are required to manage the Trusted Platform Module (TPM). This topic covers how to access the centralized Key Recovery data system in the bit_admmon_tlanextref administration website. The

Key Recovery data system can provide a TPM owner password file when the computer identity and the associated user identifier are supplied.

A TPM lockout can occur if a user enters an incorrect PIN too many times. The number of times that a user can enter an incorrect PIN before the TPM lockout is based on the computer manufacturer's specification.

To reset a TPM lockout

1. Open the MBAM administration website.
2. In the navigation pane, select **Manage TPM**. This opens the **Manage TPM** page.
3. Enter the fully qualified domain name (FQDN) for the computer and the computer name. Enter the user's Windows Logon domain and the user's user name. Select one of the predefined options in the **Reason for requesting TPM owner password file** drop-down menu. Click **Submit**.
4. MBAM will return one of the following:
   - An error message if no matching TPM owner password file is found
   - The TPM owner password file for the submitted computer

   Note
   If you are an Advanced Helpdesk User, the user domain and user ID fields are not required.
5. Upon retrieval, the owner password is displayed. To save this password to a .tpm file, click the **Save** button.
6. The user will run the TPM management console and select the **Reset TPM lockout** option and provide the TPM owner password file to reset the TPM lockout.

How to Recover a Drive in Recovery Mode

Microsoft BitLocker Administration and Monitoring (MBAM) includes Encrypted Drive Recovery features. These features ensure the capture and storage of data and availability of tools that are required to access a BitLocker-protected volume when BitLocker puts that volume into recovery mode. A BitLocker-protected volume goes into recovery mode when a PIN or password is lost or forgotten, or when the Trusted Module Platform (TPM) chip detects a change to the computer's BIOS or startup files.

Use this procedure to access the centralized Key Recovery data system that can provide a recovery password when a recovery password ID and associated user identifier are supplied.

Important
MBAM generates single-use recovery keys. Under this limitation, a recovery key can be used only once and then it is no longer valid. The single use of a recovery password is automatically applied to operating system drives and fixed drives. On removable drives,

the single use is applied when the drive is removed and then re-inserted and unlocked on a computer that has the group policy settings activated to manage removable drives.

To recover a drive in Recovery Mode

1. Open the MBAM website.
2. In the navigation pane, click **Drive Recovery**. The **Recover access to an encrypted drive** webpage opens.
3. Enter the user's Windows Logon domain and user name and the first eight digits of the recovery key ID, to receive a list of possible matching recovery keys. Alternatively, enter the entire recovery key ID to receive the exact recovery key. Select one of the predefined options in the **Reason for Drive Unlock** drop-down list, and then click **Submit**.

   Note
   If you are an MBAM Advanced Helpdesk User, the user domain and user ID entries are not required.
4. MBAM returns the following:
   a. An error message if no matching recovery password is found
   b. Multiple possible matches if the user has multiple matching recovery passwords
   c. The recovery password and recovery package for the submitted user

   Note
   If you are recovering a damaged drive, the recovery package option provides BitLocker with the critical information necessary to attempt the recovery.
5. After the recovery password and recovery package are retrieved, the recovery password is displayed. To copy the password, click **Copy Key**, and then paste the recovery password into an email or other text file for temporary storage. Or, to save the recovery password to a file, click **Save**.
6. When the user types the recovery password into the system or uses the recovery package, the drive is unlocked.

How to Recover a Moved Drive

When you move an operating system drive that has been previously encrypted by using Microsoft BitLocker Administration and Monitoring (MBAM), you must resolve certain issues. After a PIN is attached to the new computer, the drive will not accept the start-up PIN that was used in previous computer. The system considers the PIN to be invalid because of the change to the Trusted Platform Module (TPM) chip. You must obtain a recovery key ID to retrieve the recovery password in order to use the moved drive. To do this, use the following procedure.

To recover a moved drive

1. On the computer that contains the moved drive, start in Windows Recovery Environment (WinRE) mode, or start the computer by using the Microsoft Diagnostics and Recovery Toolset (DaRT).
2. Once the computer has been started with WinRE or DaRT, MBAM will treat the moved operating system drive as a data drive. MBAM will then display the drive's recovery password ID and ask for the recovery password.

   Note
   In some cases, you might be able to click **I forget the PIN** during the startup process to enter the recovery mode. This also displays the recovery key ID.
3. On the MBAM administration website, use the recovery key ID to retrieve the recovery password and unlock the drive.
4. If the moved drive was configured to use a TPM chip on the original computer, you must take additional steps after you unlock the drive and complete the start process. In WinRE mode, open a command prompt and use the **manage-bde** tool to decrypt the drive. The use of this tool is the only way to remove the TPM-plus-PIN protection without the original TPM chip.
5. After the removal is complete, start the system normally. The MBAM agent will proceed to enforce the policy to encrypt the drive with the new computer's TPM plus PIN.

How to Recover a Corrupted Drive

To recover a corrupted drive that has been protected by BitLocker, a Microsoft BitLocker Administration and Monitoring (MBAM) help desk user must create a recovery key package file. This package file can be copied to the computer that contains the corrupted drive and then used to recover the drive. To accomplish this, use the following procedure.

To Recover a Corrupted Drive

1. Open the MBAM administration website.
2. Select **Drive Recovery** from the navigation pane. Enter the user's domain name and user name, the reason for unlocking the drive, and the user's recovery password ID.

   Note
   If you are a member of the Help Desk Administrators role, you do not have to enter the user's domain name or user name.
3. Click **Submit**. The recovery key will be displayed.
4. Click **Save**, and then select **Recovery Key Package**. The recovery key package will be created on your computer.
5. Copy the recovery key package to the computer that has the corrupted drive.

6. Open an elevated command prompt. To do this, click **Start** and type `cmd` in the **Search programs and files** box. In the search results list, right-click **cmd.exe** and select **Run as Administrator**.
7. At the command prompt, type the following:

   ```
   repair-bde <fixed drive> <corrupted drive> -kp <location of keypackage> -rp
   <recovery password>
   ```

   Note
   For the <fixed drive> in the command, specify an available storage device that has free space equal to or larger than the data on the corrupted drive. Data on the corrupted drive is recovered and moved to the specified fixed drive.

How to Determine the BitLocker Encryption State of a Lost Computers

Microsoft BitLocker Administration and Monitoring (MBAM) enables you to determine the last known BitLocker encryption status of computers that are lost or stolen. Use the following procedure to determine whether the volumes have been encrypted on computers that are no longer in your possession.

Determine a Computer's Last Known BitLocker Encryption state

1. Open the MBAM website.

   Note
   The default address for the MBAM website is http://<*computername*>. Use the fully qualified server name for faster browsing results.
2. Select the **Report** node from the navigation pane, and then select the **Computer Compliance Report**.
3. Use the filter fields in the right-side pane to narrow the search results, and then click **Search**. Results will be shown below your search query.
4. Take the appropriate action as determined by your policy for lost devices.

   Note
   Device compliance is determined by the deployed BitLocker policies. You should verify these deployed policies when you are trying to determine the BitLocker encryption state of a device.

Maintaining MBAM 1.0

After you complete all the necessary planning and then deploy Microsoft BitLocker Administration and Monitoring (MBAM), you can configure MBAM to run in a highly available fashion while using it to manage enterprise BitLocker encryption operations. The information in this section describes high availability options for MBAM, as well as how to move MBAM Server features if necessary.

MBAM Management Pack

The Microsoft System Center Operations Manager Management Pack for MBAM is available for download from the Microsoft Download Center.

This management pack monitors the critical interactions in the server-side infrastructure, such as the connections between the web services and databases and the operational calls between websites and their supportive web service. It also uploads the requests between desktop clients and their respective receiving web service endpoints.

Microsoft BitLocker Administration And Monitoring Management Pack

Ensure high availability for MBAM 1.0

MBAM is designed to be fault-tolerant. If a server becomes unavailable, the users should not be negatively affected. The information in this section can be used to configure a highly available MBAM installation.

High Availability for MBAM 1.0

Move MBAM 1.0 features to another server

When you need to move an MBAM Server feature from one server computer to another, there is a specific order and required steps that you should follow to avoid loss of productivity or data. This section describes the steps that you should take to move one or more MBAM Server features to a different computer.

How to Move MBAM 1.0 Features to Another Computer

High Availability for MBAM 1.0

This topic describes how to configure a highly available installation of Microsoft BitLocker Administration and Monitoring (MBAM).

High Availability Scenarios for MBAM

Microsoft BitLocker Administration and Monitoring (MBAM) is designed to be fault-tolerant. If a server becomes unavailable, the users should not be negatively affected. For example, if the MBAM agent cannot connect to the MBAM web server, users should not be prompted for action.

When you plan your MBAM installation, consider the following concerns that can affect the availability of the MBAM service:

- Drive encryption and recovery password – If a recovery password cannot be escrowed, the encryption will not start on the client computer.
- Compliance status data upload – If the server that hosts the compliance status report service is not available, the compliance data will not remain current.
- Help Desk recovery key access - If the Help Desk cannot access MBAM database information, they will be unable to provide recovery keys to users.

- Availability of reports – Reports will not be available if the server that hosts the Compliance and Audit Reports is not available.

The main concern for MBAM high availability is BitLocker key recovery availability. If the help desk cannot provide recovery keys, users who are locked out cannot unlock their computers. To avoid this problem, consider implementing redundant web servers and databases to ensure high availability.

For more information about MBAM scalability and high availability, see the MBAM Scalability White Paper (http://go.microsoft.com/fwlink/p/?LinkId=229025).

For general guidance on high availability for Microsoft SQL Server, see High Availability (http://go.microsoft.com/fwlink/p/?LinkId=221504).

For general guidance on availability and scalability for web servers, see Availability and Scalability (http://go.microsoft.com/fwlink/p/?LinkId=221503).

How to Move MBAM 1.0 Features to Another Computer

This topic describes the steps that you should take to move one or more Microsoft BitLocker Administration and Monitoring (MBAM) features to a different computer. When you move more than one MBAM feature to another computer, you should move them in the following order:

1. Recovery and Hardware Database
2. Compliance and Audit Database
3. Compliance and Audit Reports
4. Administration and Monitoring

To move the Recovery and Hardware Database

You can use the following procedure to move the MBAM Recovery and Hardware Database from one computer to another (you can move this MBAM Server feature from Server A to Server B):

1. Stop all instances of the MBAM Administration and Monitoring web site.
2. Run the MBAM Setup on Server B.
3. Back up the MBAM Recovery and Hardware database on Server A.
4. MBAM Recovery and Hardware database from Server A to B
5. Restore the MBAM Recovery and Hardware database on Server B
6. Configure the access to the MBAM Recovery and Hardware database on Server B
7. Update the database connection data on MBAM Administration and Monitoring servers
8. Resume all instances of the MBAM Administration and Monitoring web site

To stop all instances of the MBAM Administration and Monitoring website

1. Use the Internet Information Services (IIS) Manager console to stop the MBAM website on each of the servers that run the MBAM Administration and Monitoring feature. The

MBAM website is named **Microsoft BitLocker Administration and Monitoring**.

2. To automate this procedure, you can use a command at the command prompt that is similar to the following, by using Windows PowerShell:

```
PS C:\> Stop-Website "Microsoft BitLocker Administration and Monitoring"
```

Note

To run this PowerShell command prompt, you must add the IIS Module for PowerShell to the current instance of PowerShell. In addition, you must update the PowerShell execution policy to enable the execution of scripts.

To run MBAM setup on Server B

1. Run the MBAM setup on Server B and select the Recovery and Hardware Database for installation.
2. To automate this procedure, you can use a command at the command prompt that is similar to the following, by using Windows PowerShell:

```
PS C:\> MbamSetup.exe /qn I_ACCEPT_ENDUSER_LICENSE_AGREEMENT=1
AddLocal=KeyDatabase ADMINANDMON_MACHINENAMES=$DOMAIN$\$SERVERNAME$$
RECOVERYANDHWDB_SQLINSTANCE=$SERVERNAME$\$SQLINSTANCENAME$
```

Note

Replace the following values in the example above with those that match your environment:

- $SERVERNAME$\$SQLINSTANCENAME$ - Enter the name of the server and instance to which the Recovery and Hardware database will be moved.
- $DOMAIN$\$SERVERNAME$ - Enter the domain and server names of each MBAM Application and Monitoring Server that will contact the Recovery and Hardware database. If there are multiple domain and server names, use a semicolon to separate each one of them in the list. For example, $DOMAIN\SERVERNAME$;$DOMAIN\$SERVERNAME$$. Additionally, each server name must be followed by a **$**. For example, MyDomain\MyServerName1$, MyDomain\MyServerName2$.

To back up the Database on Server A

1. To back up the Recovery and Hardware database on Server A, use SQL Server Management Studio and the Task named **Back Up…**. By default, the database name is **MBAM Recovery and Hardware Database**.
2. To automate this procedure, create a SQL file (.sql) that contains the following SQL script:

   Modify the MBAM Recovery and Hardware Database to use the full recovery mode.

```
USE master;
GO
```

```
ALTER DATABASE "MBAM Recovery and Hardware"
   SET RECOVERY FULL;
GO
```

Create MBAM Recovery and Hardware Database Data and MBAM Recovery logical backup devices.

```
USE master
GO
EXEC sp_addumpdevice 'disk', 'MBAM Recovery and Hardware Database Data Device',
'Z:\MBAM Recovery and Hardware Database Data.bak';
GO
```

Back up the full MBAM Recovery and Hardware database.

```
BACKUP DATABASE [MBAM Recovery and Hardware] TO [MBAM Recovery and Hardware
Database Data Device];
GO
BACKUP CERTIFICATE [MBAM Recovery Encryption Certificate]
TO FILE = 'Z:\SQLServerInstanceCertificateFile'
WITH PRIVATE KEY
(
    FILE = ' Z:\SQLServerInstanceCertificateFilePrivateKey',
    ENCRYPTION BY PASSWORD = '$PASSWORD$'
);
GO
```

Note

Replace the values from the preceding example with those that match your environment:

- $PASSWORD$ - Enter a password that you will use to encrypt the Private Key file.

3. Execute the SQL file by using SQL Server PowerShell and a command that is similar to the following:

```
PS C:\> Invoke-Sqlcmd -InputFile
'Z:\BackupMBAMRecoveryandHardwarDatabaseScript.sql' -ServerInstance
$SERVERNAME$\$SQLINSTANCENAME$
```

Note

Replace the value in the previous example with those that match your environment:

- $SERVERNAME$\$SQLINSTANCENAME$ - Enter the name of the server and the instance from which you back up the Recovery and Hardware database.

To move the Database and Certificate from Server A to B

1. Move the MBAM Recovery and Hardware database data.bak from Server A to Server B by using Windows Explorer.
2. To move the certificate for the encrypted database, you will need to use the following automation steps. To automate this procedure, you can use Windows PowerShell to enter a command that is similar to the following:

```
PS C:\> Copy-Item "Z:\MBAM Recovery and Hardware Database Data.bak"
\\$SERVERNAME$\$DESTINATIONSHARE$

PS C:\> Copy-Item "Z:\SQLServerInstanceCertificateFile"
\\$SERVERNAME$\$DESTINATIONSHARE$

PS C:\> Copy-Item "Z:\SQLServerInstanceCertificateFilePrivateKey"
\\$SERVERNAME$\$DESTINATIONSHARE$
```

Note

Replace the value from the preceding example with those that match your environment:

- $SERVERNAME$ - Enter the name of the server to which the files will be copied.
- $DESTINATIONSHARE$ - Enter the name of the share and path to which the files will be copied.

To restore the Database on Server B

1. Restore the Recovery and Hardware database on Server B by using the SQL Server Management Studio and the Task named **Restore Database**.
2. Once the task has been executed, choose the database backup file by selecting the **From Device** option, and then use the **Add** command to choose the MBAM Recovery and Hardware database **Data.bak** file.
3. Select **OK** to complete the restoration process.
4. To automate this procedure, create a SQL file (.sql) that contains the following SQL script:

```
-- Restore MBAM Recovery and Hardware Database.

USE master

GO
```

Drop the certificate created by MBAM Setup.

```
DROP CERTIFICATE [MBAM Recovery Encryption Certificate]

GO
```

Add certificate

```
CREATE CERTIFICATE [MBAM Recovery Encryption Certificate]

FROM FILE = 'Z: \SQLServerInstanceCertificateFile'

WITH PRIVATE KEY
```

```
(
    FILE = ' Z:\SQLServerInstanceCertificateFilePrivateKey',
    DECRYPTION BY PASSWORD = '$PASSWORD$'
);
GO
```

Restore the MBAM Recovery and Hardware database data and the log files.

```
RESTORE DATABASE [MBAM Recovery and Hardware]
   FROM DISK = 'Z:\MBAM Recovery and Hardware Database Data.bak'
   WITH REPLACE
```

Note

Replace the values from the preceding example with those that match your environment:

- $PASSWORD$ - Enter the password that you used to encrypt the Private Key file.

5. Use Windows PowerShell to enter a command line that is similar to the following:

```
PS C:\> Invoke-Sqlcmd -InputFile
'Z:\RestoreMBAMRecoveryandHardwarDatabaseScript.sql' -ServerInstance
$SERVERNAME$\$SQLINSTANCENAME$
```

Note

Replace the value from the receding example with those that match your environment:

- $SERVERNAME$\$SQLINSTANCENAME$ - Enter the name of the server and the instance to which the Recovery and Hardware Database will be restored.

Configure the access to the Database on Server B

1. On Server B, use the Local user and Groups snap-in from Server Manager, to add the computer accounts from each server that runs the MBAM Administration and Monitoring feature to the Local Group named **MBAM Recovery and Hardware DB Access**.
2. To automate this procedure, you can use Windows PowerShell on Server B to enter a command that is similar to the following:

```
PS C:\> net localgroup "MBAM Recovery and Hardware DB Access"
$DOMAIN$\$SERVERNAME$$  /add
```

Note

Replace the values from the preceding example with the applicable values for your environment:

- $DOMAIN$\$SERVERNAME$$ - Enter the domain name and machine name of the MBAM Administration and Monitoring Server. The server name must be followed by a **$**, for example, MyDomain\MyServerName1$.

You must run the command for each Administration and Monitoring Server that will be accessing the database in your environment.

To update the Database Connection data on MBAM Administration and Monitoring Servers

1. On each of the servers that run the MBAM Administration and Monitoring feature, use the Internet Information Services (IIS) Manager console to update the Connection String information for the following applications, which are hosted in the Microsoft BitLocker Administration and Monitoring website:
   - MBAM Administration Service
   - MBAM Recovery And Hardware Service
2. Select each application and use the **Configuration Editor** feature, which is located under the **Management** section of the **Feature View**.
3. Select the **configurationStrings** option from the Section list control.
4. Choose the row named **(Collection)**, and open the **Collection Editor** by selecting the button on the right side of the row.
5. In the **Collection Editor**, choose the row named **KeyRecoveryConnectionString** when you updated the configuration for the 'MBAMAdministrationService' application, or choose the row named **Microsoft.Mbam.RecoveryAndHardwareDataStore.**ConnectionString, when updating the configuration for the 'MBAMRecoveryAndHardwareService'.
6. Update the **Data Source=** value for the **configurationStrings** property to list the server name and the instance where the Recovery and Hardware Database was moved to. For example, $SERVERNAME$\$SQLINSTANCENAME$.
7. To automate this procedure, you can use a command that is similar to the following one, by using Windows PowerShell on each Administration and Monitoring Server:

```
PS C:\> Set-WebConfigurationProperty
'/connectionStrings/add[@name="KeyRecoveryConnectionString"]' -PSPath
"IIS:\sites\Microsoft BitLocker Administration and
Monitoring\MBAMAdministrationService" -Name "connectionString" -Value "Data
Source=$SERVERNAME$\$SQLINSTANCENAME$;Initial Catalog=MBAM Recovery and
Hardware;Integrated Security=SSPI;"

PS C:\> Set-WebConfigurationProperty
'/connectionStrings/add[@name="Microsoft.Mbam.RecoveryAndHardwareDataStore.Connect
ionString"]' -PSPath "IIS:\sites\Microsoft BitLocker Administration and
Monitoring\MBAMRecoveryAndHardwareService" -Name "connectionString" -Value "Data
Source=$SERVERNAME$\$SQLINSTANCENAME$;Initial Catalog=MBAM Recovery and
Hardware;Integrated Security=SSPI;"
```

Note

Replace the value from the preceding example with those that match your environment:

- $SERVERNAME$\$SQLINSTANCENAME$ - Enter the server name and instance where the Recovery and Hardware database is.

To resume all instances of the MBAM Administration and Monitoring website

1. On each of the servers that run the MBAM Administration and Monitoring feature, use the Internet Information Services (IIS) Manager console to Start the MBAM website, which is named **Microsoft BitLocker Administration and Monitoring**.
2. To automate this procedure, you can use a command that is similar to the following one, by using Windows PowerShell:

```
PS C:\> Start-Website "Microsoft BitLocker Administration and Monitoring"
```

To move the Compliance Status Database feature

If you choose to move the MBAM Compliance Status Database feature from one computer to another, such as from Server A to Server B, you should use the following procedure:

1. Stop all instances of the MBAM Administration and Monitoring website
2. Run MBAM setup on Server B
3. Backup the Database on Server A
4. Move the Database from Server A to B
5. Restore the Database on Server B
6. Configure Access to the Database on Server B
7. Update database connection data on MBAM Administration and Monitoring servers
8. Resume all instances of the MBAM Administration and Monitoring website

To stop all instances of the MBAM Administration and Monitoring website

1. On each of the servers that run the MBAM Administration and Monitoring feature, use the Internet Information Services (IIS) Manager console to Stop the MBAM website, which is named **Microsoft BitLocker Administration and Monitoring**.
2. To automate this procedure, you can use a command that is similar to the following one,by using Windows PowerShell:

```
PS C:\> Stop-Website "Microsoft BitLocker Administration and Monitoring"
```

Note

To execute this command, you must add the IIS Module for PowerShell to current instance of PowerShell. In addition, you must update the PowerShell execution policy to enable the execution of scripts.

To run MBAM Setup on Server B

1. Run MBAM Setup on Server B and select the Compliance Status Database feature for installation.

2. To automate this procedure, you can use a command that is similar to the following one, by using Windows PowerShell:

```
PS C:\> MbamSetup.exe /qn I_ACCEPT_ENDUSER_LICENSE_AGREEMENT=1 AddLocal=
ReportsDatabase ADMINANDMON_MACHINENAMES=$DOMAIN$\$SERVERNAME$
COMPLIDB_SQLINSTANCE=$SERVERNAME$\$SQLINSTANCENAME$
REPORTS_USERACCOUNT=$DOMAIN$\$USERNAME$
```

Note

Replace the values from the preceding example with those that match your environment:

- $SERVERNAME$\$SQLINSTANCENAME$ - Enter the server name and instance where the Compliance Status Database will be moved to.
- $DOMAIN$\$SERVERNAME$ - Enter the domain names and server names of each MBAM Application and Monitoring Server that will contact the Compliance Status Database. If there are multiple domain names and server names, use a semicolon to separate each one of them in the list. For example, $DOMAIN\SERVERNAME$;$DOMAIN\$SERVERNAME$$. Each server name must be followed by a **$** as shown in the example. For example, MyDomain\MyServerName1$, MyDomain\MyServerName2$.
- $DOMAIN$\$USERNAME$ - Enter the domain and user name that will be used by the Compliance and Audit reports feature to connect to the Compliance Status Database.

To back up the Compliance Database on Server A

1. To back up the Compliance Database on Server A, use SQL Server Management Studio and the Task named **Back Up…**. By default, the database name is **MBAM Compliance Status Database**.
2. To automate this procedure, create a SQL file (.sql) that contains the following-SQL script:

```
-- Modify the MBAM Compliance Status Database to use the full recovery model.
USE master;
GO
ALTER DATABASE "MBAM Compliance Status"
   SET RECOVERY FULL;
GO
-- Create MBAM Compliance Status Data logical backup devices.
USE master
GO
EXEC sp_addumpdevice 'disk', 'MBAM Compliance Status Database Data Device',
'Z: \MBAM Compliance Status Database Data.bak';
GO
```

-- Back up the full MBAM Recovery and Hardware database.

```
BACKUP DATABASE [MBAM Compliance Status] TO [MBAM Compliance Status Database Data Device];
GO
```

3. Run the SQL file with a command that is similar to the following one, by using the SQL Server PowerShell:

```
PS C:\> Invoke-Sqlcmd -InputFile "Z:\BackupMBAMComplianceStatusDatabaseScript.sql" -ServerInstance $SERVERNAME$\$SQLINSTANCENAME$
```

Note

Replace the value from the preceding example with those that match your environment:

- $SERVERNAME$\$SQLINSTANCENAME$ - Enter the server name and the instance from where the Compliance Status database will be backed up.

To move the Database from Server A to B

1. Move the following files from Server A to Server B, by using Windows Explorer:
   - MBAM Compliance Status Database Data.bak
2. To automate this procedure, you can use a command that is similar to the following using Windows PowerShell:

```
PS C:\> Copy-Item "Z:\MBAM Compliance Status Database Data.bak" \\$SERVERNAME$\$DESTINATIONSHARE$
```

Note

Replace the value from the preceding example with those that match your environment:

- $SERVERNAME$ - Enter the server name where the files will be copied to.
- $DESTINATIONSHARE$ - Enter the name of share and path where the files will be copied to.

To restore the Database on Server B

1. Restore the Compliance Status database on Server B by using SQL Server Management Studio and the Task named **Restore Database…**.
2. Once the task is executed, select the database backup file, by selecting the From Device option, and then use the Add command to choose the MBAM Compliance Status Database Data.bak file. Click OK to complete the restoration process.
3. To automate this procedure, create a SQL file (.sql) that contains the following-SQL script:

```
-- Create MBAM Compliance Status Database Data logical backup devices.
Use master
GO
```

-- Restore the MBAM Compliance Status database data files.

```
RESTORE DATABASE [MBAM Compliance Status Database]
   FROM DISK = 'C:\test\MBAM Compliance Status Database Data.bak'
   WITH REPLACE
```

4. Run the SQL File with a command that is similar to the following one, by using the SQL Server PowerShell:

```
PS C:\> Invoke-Sqlcmd -InputFile
"Z:\RestoreMBAMComplianceStatusDatabaseScript.sql" -ServerInstance
$SERVERNAME$\$SQLINSTANCENAME$
```

Note

Replace the value from the preceding example with those that match your environment:

- $SERVERNAME$\$SQLINSTANCENAME$ - Enter the server name and instance where the Compliance Status Database will be restored to.

To configure the Access to the Database on Server B

1. On Server B use the Local user and Groups snap-in from Server Manager to add the machine accounts from each server that runs the MBAM Administration and Monitoring feature to the Local Group named **MBAM Compliance Status DB Access**.
2. To automate this procedure, you can use a command that is similar to the following one, by using Windows PowerShell on Server B:

```
PS C:\> net localgroup "MBAM Compliance Auditing DB Access" $DOMAIN$\$SERVERNAME$$
/add
PS C:\> net localgroup "MBAM Compliance Auditing DB Access"
$DOMAIN$\$REPORTSUSERNAME$  /add
```

Note

Replace the value from the preceding example with the applicable values for your environment:

- $DOMAIN$\$SERVERNAME$$ - Enter the domain and machine name of the MBAM Administration and Monitoring Server. The server name must be followed by a **$**.For example, MyDomain\MyServerName1$.
- $DOMAIN$\$REPORTSUSERNAME$ - Enter the user account name that was used to configure the data source for the Compliance and Audit reports

For each Administration and Monitoring Server that will access the database of your environment, you must run the command that will add the servers to the MBAM Compliance Auditing DB Access local group.

To update the database connection data on MBAM Administration and Monitoring servers

1. On each of the servers that run the MBAM Administration and Monitoring feature, use the Internet Information Services (IIS) Manager console to update the Connection String information for the following Applications, which are hosted in the Microsoft BitLocker Administration and Monitoring website:
   - MBAMAdministrationService
   - MBAMComplianceStatusService
2. Select each application and use the **Configuration Editor** feature, which is located under the **Management** section of the **Feature View**.
3. Select the **configurationStrings** option from the Section list control.
4. Select the row named **(Collection)**, and open the Collection Editor by selecting the button on the right side of the row.
5. In the **Collection Editor**, select the row named **ComplianceStatusConnectionString**, when you update the configuration for the MBAMAdministrationService application, or the row named **Microsoft.Windows.Mdop.BitLockerManagement.StatusReportDataStore.ConnectionString**, when you update the configuration for the MBAMComplianceStatusService.
6. Update the **Data Source=** value for the **configurationStrings** property to list the server name and the instance name. For example, $SERVERNAME$\$SQLINSTANCENAME, to which the Recovery and Hardware Database was moved.
7. To automate this procedure, you can use Windows PowerShell to enter a command that is similar to the following one on each Administration and Monitoring Server:

```
PS C:\> Set-WebConfigurationProperty
'/connectionStrings/add[@name="ComplianceStatusConnectionString"]' -PSPath
"IIS:\sites\Microsoft BitLocker Administration and
Monitoring\MBAMAdministrationService" -Name "connectionString" -Value "Data
Source=$SERVERNAME$\$SQLINSTANCENAME$;Initial Catalog=MBAM Compliance
Status;Integrated Security=SSPI;"
PS C:\> Set-WebConfigurationProperty
'/connectionStrings/add[@name="Microsoft.Windows.Mdop.BitLockerManagement.StatusReportDataStore.ConnectionString"]' -PSPath "IIS:\sites\Microsoft BitLocker
Administration and Monitoring\MBAMComplianceStatusService" -Name
"connectionString" -Value "Data Source=$SERVERNAME$\$SQLINSTANCENAME;Initial
Catalog=MBAM Compliance Status;Integrated Security=SSPI;"
```

Note

Replace the value from the preceding example with those that match your environment:

- $SERVERNAME$\$SQLINSTANCENAME$ - Enter the server name and instance name where the Recovery and Hardware Database is located.

To resume all instances of the MBAM Administration and Monitoring website

1. On each of the servers running the MBAM Administration and Monitoring feature, use the Internet Information Services (IIS) Manager console to start the MBAM web site named **Microsoft BitLocker Administration and Monitoring**.
2. To automate this procedure, you can use Windows PowerShell to enter a command that is similar to the following:

   PS C:\> Start-Website "Microsoft BitLocker Administration and Monitoring"

To moving the Compliance and Audit Reports

If you choose to move the MBAM Compliance and Audit Reports from one computer to another (specifically, if you move feature from Server A to Server B), you should use the following procedure and steps:

1. Run MBAM setup on Server B
2. Configure Access to the Compliance and Audit Reports on Server B
3. Stop all instances of the MBAM Administration and Monitoring website
4. Update the reports connection data on MBAM Administration and Monitoring servers
5. Resume all instances of the MBAM Administration and Monitoring website

To run MBAM setup on Server B

1. Run MBAM setup on Server B and only select the Compliance and Audit feature for installation.
2. To automate this procedure, you can use a command that is similar to the following, by using Windows PowerShell:

```
PS C:\> MbamSetup.exe /qn I_ACCEPT_ENDUSER_LICENSE_AGREEMENT=1 AddLocal=Reports
COMPLIDB_SQLINSTANCE=$SERVERNAME$\$SQLINSTANCENAME$
REPORTS_USERACCOUNTPW=$PASSWORD$
```

Note

Replace the values from the preceding example with those that match your environment:

- $SERVERNAME$\$SQLINSTANCENAME$ - Enter the server name and instance where the Compliance Status Database is located.
- $DOMAIN$\$USERNAME$ - Enter the domain name and user name that will be used by the Compliance and Audit reports feature to connect to the Compliance Status Database.
- $PASSWORD$ - Enter the password of the user account that will be used to connect to the Compliance Status Database.

To configure the access to the Compliance and Audit Reports on Server B

1. On Server B, use the Local user and Groups snap-in from Server Manager to add the user accounts that will have access to the Compliance and Audit Reports. Add the user accounts to the local group named “MBAM Report Users”.
2. To automate this procedure, you can use a command that is similar to the following, by using Windows PowerShell on Server B.

```
PS C:\> net localgroup "MBAM Report Users" $DOMAIN$\$REPORTSUSERNAME$  /add
```

Note

Replace the following value from the preceding example with the applicable values for your environment:

- $DOMAIN$\$REPORTSUSERNAME$ - Enter the user account name that was used to configure the data source for the Compliance and Audit reports

The command to add the users to the MBAM Report Users local group must be run for each user that will be accessing the reports in your environment.

To stop all instances of the MBAM Administration and Monitoring website

1. On each of the servers that run the MBAM Administration and Monitoring Feature use the Internet Information Services (IIS) Manager console to Stop the MBAM website named **Microsoft BitLocker Administration and Monitoring**.
2. To automate this procedure, you can use a command that is similar to the following one, by using Windows PowerShell:

```
PS C:\> Stop-Website “Microsoft BitLocker Administration and Monitoring”
```

To update the Database Connection Data on MBAM Administration and Monitoring Servers

1. On each of the servers that run the MBAM Administration and Monitoring Feature, use the Internet Information Services (IIS) Manager console to update the Compliance Reports URL.
2. Select the **Microsoft BitLocker Administration and Monitoring** website and use the **Configuration Editor** feature which can be found under the **Management** section of the **Feature View**.
3. Select the **appSettings** option from the Section list control.
4. From here, select the row named **(Collection)**, and open the **Collection Editor** by selecting the button on the right side of the row.
5. In the **Collection Editor**, select the row named “Microsoft.Mbam.Reports.Url”.
6. Update the value for Microsoft.Mbam.Reports.Url to reflect the server name for Server B. If the Compliance and Audit reports feature was installed on a named SQL Reporting Services instance, make sure that you add or update the name of the instance to the URL. For example, http://$SERVERNAME$/ReportServer_$SQLSRSINSTANCENAME$/Pages....

7. To automate this procedure, you can use Windows PowerShell to enter a command that is similar to the following one on each Administration and Monitoring Server:

```
PS C:\> Set-WebConfigurationProperty
'/appSettings/add[@key="Microsoft.Mbam.Reports.Url"]' -PSPath
"IIS:\sites\Microsoft BitLocker Administration and Monitoring" -Name "Value" -
Value
"http://$SERVERNAME$/ReportServer_$SRSINSTANCENAME$/Pages/ReportViewer.aspx?/Malta
+Compliance+Reports/"
```

Note

Replace the value from the preceding example with those that match your environment:

- $SERVERNAME$ - Enter the name of the server to which the Compliance and Audit Reports were installed.
- $SRSINSTANCENAME$ - Enter the name of the SQL Reporting Services instance to which the Compliance and Audit Reports were installed.

To resume all instances of the MBAM Administration and Monitoring website

1. On each of the servers that run the MBAM Administration and Monitoring feature, use the Internet Information Services (IIS) Manager console to Start the MBAM web site named **Microsoft BitLocker Administration and Monitoring**.
2. To automate this procedure, you can use a command that is similar to the following one, by using Windows PowerShell:

```
PS C:\> Start-Website "Microsoft BitLocker Administration and Monitoring"
```

Note

To execute this command, the IIS Module for PowerShell must be added to the current instance of PowerShell. In addition, you must update the PowerShell execution policy to enable execution of scripts.

To move the Administration and Monitoring feature

If you choose to move the MBAM Administration and Monitoring Reports feature from one computer to another, (if you move feature from Server A to Server B), you should use the following procedure. The process includes the following steps:

1. Run MBAM setup on Server B
2. Configure Access to the Database on Server B

To run MBAM setup on Server B

1. Run MBAM setup on Server B and only select the Administration feature for installation.
2. To automate this procedure, you can use a command that is similar to the following one, by using Windows PowerShell:

```
PS C:\> MbamSetup.exe /qn I_ACCEPT_ENDUSER_LICENSE_AGREEMENT=1
AddLocal=AdministrationMonitoringServer,HardwareCompatibility
COMPLIDB_SQLINSTANCE=$SERVERNAME$\$SQLINSTANCENAME$
RECOVERYANDHWDB_SQLINSTANCE=$SERVERNAME$\$SQLINSTANCENAME$
SRS_REPORTSITEURL=$REPORTSSERVERURL$
```

Note

Replace the values from the preceding example with those that match your environment:

- $SERVERNAME$\$SQLINSTANCENAME$ - For the COMPLIDB_SQLINSTANCE parameter, input the server name and instance where the Compliance Status Database is located. For the RECOVERYANDHWDB_SQLINSTANCE parameter, input the server name and instance where the Recovery and Hardware Database is located.
- $DOMAIN$\$USERNAME$ - Enter the domain and user name that will be used by the Compliance and Audit reports feature to connect to the Compliance Status Database.
- $ REPORTSSERVERURL$ - Enter the URL for the Home location of the SQL Reporting Service website. If the reports were installed to a default SRS instance the URL format will formatted “http:// $SERVERNAME$/ReportServer”. If the reports were installed to a default SRS instance, the URL format will be formatted to “http://$SERVERNAME$/ReportServer_$SQLINSTANCENAME$”.

To configure the Access to the Databases

1. On server or servers where the Recovery and Hardware, and Compliance and Audit databases are deployed, use the Local user and Groups snap-in from Server Manager to add the machine accounts from each server that run the MBAM Administration and Monitoring feature to the Local Groups named “MBAM Recovery and Hardware DB Access” (Recovery and Hardware DB Server) and “MBAM Compliance Status DB Access” (Compliance and Audit DB Server).
2. To automate this procedure, you can use a command that is similar to the following one, by using Windows PowerShell on the server where the Compliance and Audit databases were deployed.

   ```
   PS C:\> net localgroup "MBAM Compliance Auditing DB Access" $DOMAIN$\$SERVERNAME$$
   /add

   PS C:\> net localgroup "MBAM Compliance Auditing DB Access"
   $DOMAIN$\$REPORTSUSERNAME$  /add
   ```

3. On the server where the Recovery and Hardware databases were deployed, run a command that is similar to the following one, by using Windows PowerShell.

   ```
   PS C:\> net localgroup "MBAM Recovery and Hardware DB Access"
   $DOMAIN$\$SERVERNAME$$  /add
   ```

Note

Replace the value from the preceding example with the applicable values for your environment:

- $DOMAIN$\$SERVERNAME$$ - Enter the domain and machine name of the MBAM Administration and Monitoring Server. The server name must be followed by a **$**. For example, MyDomain\MyServerName1$)
- $DOMAIN$\$REPORTSUSERNAME$ - Enter the user account name that was used to configure the data source for the Compliance and Audit reports.

The commands listed for adding the server computer accounts to the MBAM local groups must be run for each Administration and Monitoring Server that will be accessing the databases in your environment.

Security and Privacy for MBAM 1.0

The topics in this guide will help you plan for security and privacy considerations for Microsoft BitLocker Administration and Monitoring (MBAM).

Security considerations for MBAM 1.0

Before you deploy and use MBAM in your computing environment, you should consider potential security-related issues. The information in the Security Considerations topic provides a brief overview of Active Directory Domain Services user accounts and groups, log files, and other security-related considerations for MBAM.

Security Considerations for MBAM 1.0

Privacy for MBAM 1.0

This topic covers many of the data collection and use practices of MBAM.

Privacy Statement for MBAM 1.0

Security Considerations for MBAM 1.0

This topic contains a brief overview of the accounts and groups, log files, and other security-related considerations for Microsoft BitLocker Administration and Monitoring (MBAM). For more information, follow the links in this article.

General security considerations

Understand the security risks. The most serious risk to MBAM is that its functionality could be hijacked by an unauthorized user who could then reconfigure BitLocker encryption and gain BitLocker encryption key data on MBAM Clients. However, the loss of MBAM functionality for a short period of time due to a denial-of-service attack would not generally have a catastrophic impact.

Physically secure your computers. Security is incomplete without physical security. Anyone with physical access to an MBAM Server could potentially attack the entire client base. Any potential physical attacks must be considered high risk and mitigated appropriately. MBAM servers should be stored in a physically secure server room with controlled access. Secure these computers when administrators are not physically present by having the operating system lock the computer, or by using a secured screen saver.

Apply the most recent security updates to all computers. Stay informed about new updates for operating systems, Microsoft SQL Server, and MBAM by subscribing to the Security Notification service (http://go.microsoft.com/fwlink/p/?LinkId=28819).

Use strong passwords or pass phrases. Always use strong passwords with 15 or more characters for all MBAM and MBAM administrator accounts. Never use blank passwords. For more information about password concepts, see the "Account Passwords and Policies" white paper on TechNet (http://go.microsoft.com/fwlink/p/?LinkId=30009).

Accounts and Groups in MBAM

A best practice for user account management is to create domain global groups and add user accounts to them. Then, add the domain global accounts to the necessary MBAM local groups on the MBAM Servers.

Active Directory Domain Services Groups

No groups are created automatically during MBAM Setup. However, you should create the following Active Directory Domain Services global groups to manage MBAM operations.

Group Name	Details
MBAM Advanced Helpdesk Users	Create this group to manage members of the MBAM Advanced Helpdesk Users local group that was created during MBAM Setup.
MBAM Compliance Auditing DB Access	Create this group to manage members of the MBAM Compliance Auditing DB Access local group that was created during MBAM Setup.
MBAM Hardware Users	Create this group to manage members of the MBAM Hardware Users local group that was created during MBAM Setup.
MBAM Helpdesk Users	Create this group to manage members of the MBAM Helpdesk Users local group that was created during MBAM Setup.
MBAM Recovery and Hardware DB Access	Create this group to manage members of the MBAM Recovery and Hardware DB Access local group that was created during MBAM Setup.

Group Name	Details
MBAM Report Users	Create this group to manage members of the MBAM Report Users local group that was created during MBAM Setup.
MBAM System Administrators	Create this group to manage members of the MBAM System Administrators local group that was created during MBAM Setup.
BitLocker Encryption Exemptions	Create this group to manage user accounts that should be exempted from BitLocker encryption starting on computers that they log on to.

MBAM Server Local Groups

MBAM Setup creates local groups to support MBAM operations. You should add the Active Directory Domain Services Global Groups to the appropriate MBAM local groups to configure MBAM security and data access permissions.

Group Name	Details
MBAM Advanced Helpdesk Users	Members of this group have expanded access to the Helpdesk features of Microsoft BitLocker Administration and Monitoring.
MBAM Compliance Auditing DB Access	This group contains the machines that have access to the MBAM Compliance Auditing Database.
MBAM Hardware Users	Members of this group have access to some of the Hardware Capability features from Microsoft BitLocker Administration and Monitoring.
MBAM Helpdesk Users	Members of this group have access to some of the Helpdesk features from Microsoft BitLocker Administration and Monitoring.
MBAM Recovery and Hardware DB Access	This group contains the computers that have access to the MBAM Recovery and Hardware Database.
MBAM Report Users	Members of this group have access to the Compliance and Audit reports from Microsoft BitLocker Administration and Monitoring.
MBAM System Administrators	Members of this group have access to all the

Group Name	Details
	features of Microsoft BitLocker Administration and Monitoring.

SSRS Reports Access Account

The SQL Server Reporting Services (SSRS) Reports Service Account provides the security context to run the MBAM reports available through SSRS. This account is configured during MBAM Setup.

MBAM Log Files

During MBAM Setup, the following MBAM Setup log files are created in the %temp% folder of the user who installs the

MBAM Server Setup log files

MSI<five random characters>.log

Logs the actions taken during MBAM Setup and MBAM Server Feature installation.

InstallComplianceDatabase.log

Logs the actions taken to create the MBAM Compliance Status database setup.

InstallKeyComplianceDatabase.log

Logs the actions taken to create the MBAM Recovery and Hardware database.

AddHelpDeskDbAuditUsers.log

Logs the actions taken to create the SQL Server logins on the MBAM Compliance Status database and authorize helpdesk web service to the database for reports.

AddHelpDeskDbUsers.log

Logs the actions taken to authorize web services to database for key recovery and create logins to the MBAM Recovery and Hardware database.

AddKeyComplianceDbUsers.log

Logs the actions taken to authorize web services to MBAM Compliance Status database for compliance reporting.

AddRecoveryAndHardwareDbUsers.log

Logs the actions taken to authorize web services to MBAM Recovery and Hardware database for key recovery.

Note

In order to obtain additional MBAM Setup log files, you must install Microsoft BitLocker Administration and Monitoring by using the **msiexec** package and the **/l** <location> option. Log files are created in the location specified.

MBAM Client Setup log files

MSI<five random characters>.log

Logs the actions taken during MBAM Client installation.

MBAM Database TDE considerations

The Transparent Data Encryption (TDE) feature available in SQL Server 2008 is a required installation prerequisite for the database instances that will host MBAM database features.

With TDE, you can perform real-time, full database-level encryption. TDE is a well-suited choice for bulk encryption to meet regulatory compliance or corporate data security standards. TDE works at the file level, which is similar to two Windows features: the Encrypting File System (EFS) and BitLocker Drive Encryption, both of which also encrypt data on the hard drive. TDE does not replace cell-level encryption, EFS, or BitLocker.

When TDE is enabled on a database, all backups are encrypted. Thus, special care must be taken to ensure that the certificate that was used to protect the Database Encryption Key (DEK) is backed up and maintained with the database backup. Without a certificate, the data will be unreadable. Back up the certificate along with the database. Each certificate backup should have two files; both of these files should be archived .It is best to archive them separately from the database backup file for security.

For an example of how to enable TDE for MBAM database instances, see Evaluating MBAM 1.0.

For more information about TDE in SQL Server 2008, see Database Encryption in SQL Server 2008 Enterprise Edition.

Privacy Statement for MBAM 1.0

To see the MBAM 1.0 Privacy Statement, see http://go.microsoft.com/fwlink/?LinkId=272928 on TechNet.

Administering MBAM 1.0 by Using PowerShell

Microsoft BitLocker Administration and Monitoring (MBAM) provides the following listed set of Windows PowerShell cmdlets. Administrators can use these PowerShell cmdlets to perform various MBAM server tasks from the command prompt rather than from the MBAM administration website.

How to administer MBAM by using PowerShell

Use the PowerShell cmdlets described here to administer MBAM.

Name	Description
Add-MbamHardwareType	Adds a new hardware model to the MBAM hardware inventory. This cmdlet can also specify whether the hardware is supported or unsupported for BitLocker drive encryption.
Get-MbamBitLockerRecoveryKey	Requests an MBAM recovery key that will enable a user to unlock a computer or encrypted drive.
Get-MbamHardwareType	Gets a master hardware inventory that contains data that indicates whether hardware models are compatible or incompatible with BitLocker drive encryption.
Get-MbamTPMOwnerPassword	Provides a TPM owner password for a user to manage their TPM (Trusted Platform Module) access. Helps users when TPM has locked them out and will no longer accept their PIN.
Install-Mbam	Installs MBAM features that provide advanced group policy, encryption, key recovery, and compliance reporting tools.
Remove-MbamHardwareType	Removes the hardware models from the hardware inventory.
Set-MbamHardwareType	Allows management of a master hardware inventory to designate whether or not hardware models are capable or incapable to perform BitLocker encryption.
Uninstall-Mbam	Removes previously installed MBAM features that provide advanced policy, encryption, key

Name	Description
	recovery, and compliance reporting tools.

Troubleshooting MBAM 1.0

Troubleshooting content is not included in the Administrator's Guide for this product. Instead, you can find troubleshooting information for this product on the TechNet Wiki.

How to Find Troubleshooting Content

You can use the following information to find troubleshooting or additional technical content for this product.

Search the MDOP Documentation

The first step to find help content in the Administrator's Guide is to search the MDOP documentation on TechNet.

After you search the MDOP documentation, your next step would be to search the troubleshooting information for the product in the TechNet Wiki.

To search the MDOP product documentation

1. Use a web browser to navigate to the MDOP Information Experience TechNet home page.
2. Enter applicable search terms in the **Search TechNet with Bing** search box at the top of the MDOP Information Experience home page.
3. Review the search results for assistance.

To search the TechNet Wiki

1. Use a web browser to navigate to the TechNet Wiki home page.
2. Enter applicable search terms in the **Search TechNet Wiki** search box on the TechNet Wiki home page.
3. Review the search results for assistance.

How to Create a Troubleshooting Article

If you have a troubleshooting tip or a best practice to share that is not already included in the MDOP OnlineHelp or TechNet Wiki, you can create your own TechNet Wiki articles.

To create a TechNet Wiki troubleshooting or best practices article

1. Use a web browser to navigate to the TechNet Wiki home page.
2. Log in with your Windows Live ID.
3. Review the **Getting Started** section to learn the basics of the TechNet Wiki and its articles.
4. Select **Post an article >>** at the bottom of the **Getting Started** section.
5. On the Wiki article **Add Page** page, select **Insert Template** from the toolbar, select the troubleshooting article template (**Troubleshooting.html**), and then click **Insert**.
6. Be sure to give the article a descriptive title and then overwrite the template information as needed to create your troubleshooting or best practice article.
7. After you review your article, be sure to include a tag that is named **Troubleshooting** and another for the product name. This helps others to find your content.
8. Click **Save** to publish the article to the TechNet Wiki.