Microsoft BitLocker Administration and Monitoring

Microsoft BitLocker Administration and Monitoring Administrator's Guide

Published: August 1, 2011

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.

The most current MBAM documentation can be found online at the MDOP documentation home page at http://onlinehelp.microsoft.com/mdop.

The MBAM release notes can be found online at http://go.microsoft.com/fwlink/?LinkId=218347.

Applies To

Microsoft BitLocker Administration and Monitoring (MBAM)

Feedback

Send suggestions and comments about this document to mdopdocs@microsoft.com

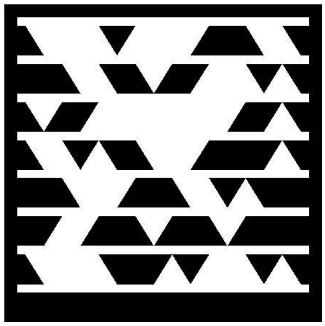
Revision History

Release Date	Changes
August 1, 2011	Original release of this guide.

Getting Started With MBAM

Microsoft BitLocker Administration and Monitoring (MBAM) provides a simplified administrative interface to BitLocker drive encryption. MBAM lets you select BitLocker encryption policy options appropriate to your enterprise so that you can monitor client compliance with those policies and report on the encryption status of the enterprise in addition to individual computers. Also, you can access recovery key information when a user forgets their PIN or password, or when their BIOS or boot record changes.

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



For example, you can use a tag reader application installed on your mobile phone to scan this Microsoft Tag (or go to http://go.microsoft.com/fwlink/?LinkId=225356) to download this guide.

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

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

In This Section

About Microsoft BitLocker Administration and Monitoring

Provides overview information about this release of MBAM.

High-Level Architecture for MBAM

Provides information about the components that make-up the MBAM BitLocker management solution.

MBAM Keyboard Shortcuts

Provides information about the keyboard shortcuts that can be used with MBAM.

See Also

Planning for MBAM

Deploying MBAM

Operations for MBAM

Troubleshooting MBAM

About Microsoft BitLocker Administration and Monitoring

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

Note
BitLocker is not covered in detail in this guide. For an overview of BitLocker see BitLocker Drive Encryption Overview (http://go.microsoft.com/fwlink/?LinkId=225013).

This Microsoft BitLocker Administration and Monitoring help 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 technical personnel.

Release notes for MBAM are available online at http://go.microsoft.com/fwlink/?LinkId=218347.

Additional MBAM evaluation information is available by downloading the MBAM Evaluation Guide (http://go.microsoft.com/fwlink/?LinkId=224780).

See Also

Getting Started With MBAM

Release Notes for MBAM

High-Level Architecture for MBAM

Microsoft BitLocker Administration and Monitoring (MBAM) is a client/server data encryption solution that includes the components described in the following section.

Architecture Overview

Administration and Monitoring Server: Hosts the Management Console and monitoring web services. The Management Console is used to determine enterprise compliance status and audit activity, manage hardware capability, and access recovery data (for example, BitLocker recovery keys).

Compliance and Audit Database: Stores compliance data for Microsoft BitLocker Administration and Monitoring client computers. This data is used primarily for reports hosted by SQL Server Reporting Services (SSRS).

Recovery and Hardware Database: Stores recovery data and hardware information that is collected from Microsoft BitLocker Administration and Monitoring client computers.

Compliance and Audit Reports: Uses SQL Server Reporting Services (SSRS) to provide Microsoft BitLocker Administration and Monitoring reports. These reports can be accessed from the Management Console or directly from the SSRS server.

Policy Template: The Group Policy template that specifies the Microsoft BitLocker Administration and Monitoring implementation settings for BitLocker drive encryption.

The **Microsoft BitLocker Administration and Monitoring client agent** 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 computer
- Collects compliance data for the computer and passes the data to the reporting system

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

See Also

Getting Started With MBAM

MBAM Keyboard Shortcuts

The keyboard shortcuts that are described in this Help topic refer to the U.S. keyboard layout. Keys on other layouts might not correspond exactly to the keys on a U.S. keyboard.

Finding and Using Keyboard Shortcuts

For keyboard shortcuts in which you press two or more keys at the same time, the keys to press are separated by a plus sign (+) in Microsoft BitLocker Administration and Monitoring (MBAM) Help. For keyboard shortcuts in which you press one key immediately followed by another key, the keys to press are separated by a comma (,).

Search This Article

1. Press CTRL+F.
   The Search dialog box opens, with the cursor ready for you to type.
2. Type the search text in the box.
3. Press ENTER.

Print This Article

To print this topic, press CTRL+P.

Keyboard Shortcuts for MBAM Setup

The following table describes the keyboard shortcuts available to use during MBAM setup.

To do this	Press
Close setup	ALT+C
Next button	ALT+N
Back button	ALT+B
Browse button	ALT+B
Install button	ALT+I
Check prerequisites again	ALT+C
Review documentation	ALT+R

To do this	Press
Select Machine Account button	ALT+S
Instance of SQL Server	ALT+I
Release Notes	ALT+R
Read documentation	ALT+R
Deployment Guide	ALT+D
Browse CD	ALT+B
MDOP Online	ALT+M
SQL Server reporting services instance	ALT+S
Details	ALT+D

Keyboard Shortcuts for MBAM Console

The following table describes the keyboard shortcuts available to use on the Microsoft BitLocker Administration and Monitoring console website.

To do this	Press
Copy	CTRL+Y
Save Recovery Password	CTRL+M
Save Recovery Package	CTRL+G
Save	CTRL+M

For additional keyboard shortcuts, refer to your browser's help to determine the keyboard shortcuts available for use.

See Also

Getting Started With MBAM

Planning for MBAM

Planning the server infrastructure, client deployment strategies, and hardware management are all necessary for a successful MBAM deployment. Additionally, a Group Policy template must be configured for your enterprise before you can deploy MBAM or monitor BitLocker drive encryption.

Use the information in this section to help plan the Microsoft BitLocker Administration and Monitoring (MBAM) deployment that best meets your business requirements.

In This Section

MBAM Supported Configurations

Describes the system requirements and configurations necessary to support MBAM deployment and operations.

Planning and Configuring Group Policy for MBAM

Provides guidance about how to plan and configure Group Policy for MBAM.

Planning the Server Infrastructure for MBAM

Provides guidance on how to configure your server infrastructure for MBAM.

Planning for MBAM Administrator Roles

Provides information on the different types of administrative user roles in MBAM.

Planning for MBAM Client Deployment

Provides guidance on deploying the MBAM client to your organization's computers.

Planning Hardware Management for MBAM

Provides guidance on determining the need for Hardware Management in your organization.

Planning for Single Use Recovery Keys

Describes how to configure and use the Single Use Recovery Key feature of MBAM.

See Also

BitLocker Administration and Monitoring Home

Getting Started With MBAM

Deploying MBAM

Operations for MBAM

Troubleshooting MBAM

MBAM Supported Configurations

This topic specifies the supported configurations for Microsoft BitLocker Administration and Monitoring (MBAM) server and client computers.

Note

Microsoft provides support for the current service pack, and in some cases, the earlier service pack. To find the support timelines for your product, see the Lifecycle Supported Service Packs (http://go.microsoft.com/fwlink/?LinkId=31975). For more information about Microsoft Support Lifecycle Policy, see Microsoft Support Lifecycle Support Policy FAQ (http://go.microsoft.com/fwlink/?LinkId=31976).

Operating System Requirements for MBAM Server Computers

The following operating systems support the server roles required for Microsoft BitLocker Administration and Monitoring.

Operating system	Editions	Service pack	System architecture
Windows Server 2008	Standard, Enterprise, Data Center, or Web Server	SP2 only	x86 and x64
Windows Server 2008 R2	Standard, Enterprise, Data Center, or Web Server		64-bit

Warning

It is not recommended to install the services, reports, or databases on a domain controller.

This section contains configuration information that is specific to this release.

Installation Prerequisites for BitLocker Administration and Monitoring Servers

Each of the Microsoft BitLocker Administration and Monitoring server features has specific prerequisites that must be met before the MBAM features can be successfully installed. MBAM Setup checks that all prerequisites are met before installation starts.

Prerequisites for Administration and Monitoring Server

The following is a list of the prerequisites for the Microsoft BitLocker Administration and Monitoring server:

- **Windows Server Web Server Role**
- **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**
  - .NET Framework 3.5.1 features
    - .NET Framework 3.5.1
    - WCF Activation
      - HTTP Activation
      - Non-HTTP Activation
  - Windows Process Activation Service
    - Process Model
    - .NET Environment
    - Configuration APIs

Prerequisites for the Compliance and Audit Reports Server

The Compliance and Audit Reports Server prerequisites include the SQL Server Reporting Services (SSRS) feature of Microsoft SQL Server 2008 R2, Enterprise, Datacenter, or the Developer edition.

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

Prerequisites for the Recovery and Hardware Database Server

The Recovery and Hardware Database Prerequisites include the following:

- Microsoft SQL Server 2008 R2, Enterprise, Datacenter, or Developer edition
- SQL Server must have Database Engine Services installed and running during MBAM server installation.

Prerequisites for the Compliance Status Database Server

The Compliance Status Database Prerequisites include the following:

- Microsoft SQL Server 2008 R2, Standard, Enterprise, Datacenter, or Developer edition
- SQL Server must have Database Engine Services installed and running during MBAM server installation.

Operating System Requirements for MBAM Client Computers

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

You can install the Microsoft BitLocker Administration and Monitoring client on any computer that meets the following requirements.

Operating system	Edition	Service pack	System architecture
Windows 7	Enterprise Edition	None, SP1	x86 or x64
Windows 7	Ultimate Edition	None, SP1	x86 or x64

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

Warning

Ensure that the keyboard, mouse, and video are directly connected and not managed through a keyboard, video, mouse (KVM) switch. A KVM switch can interfere with the ability of the computer to detect the physical presence of hardware.

There are no special RAM requirements that are specific to Microsoft BitLocker Administration and Monitoring.

See Also

Planning for MBAM

Planning and Configuring Group Policy for MBAM

Before Microsoft BitLocker Administration and Monitoring (MBAM) can manage clients in the enterprise, you must define Group Policy for the encryption requirements of your environment.

Important
Microsoft BitLocker Administration and Monitoring will not work with policies for stand-alone BitLocker drive encryption. Group Policy must be defined for Microsoft BitLocker Administration and Monitoring, or BitLocker encryption and enforcement will fail.

Group Policy Requirements

Microsoft BitLocker Administration and Monitoring requires Group Policy to be set for MBAM features. This section describes the policies to use for setting up BitLocker Drive Encryption.

To set Group Policy for BitLocker Administration and Monitoring

1. Make sure that MBAM Group Policy feature is installed on the computer that is managing Group Policy settings for BitLocker.
2. Using the Group Policy Management Console (GPMC), the Advanced Group Policy Management (AGPM), or the Local Group Policy Editor on the computer that is managing Group Policy for BitLocker t, browse to **Computer configuration**, select **Policies**, select **Administrative Templates**, click **Windows Components**, and then select **MDOP MBAM (BitLocker Management)**.
3. Select the policy setting to edit. The Group Policy settings for BitLocker Administration and Monitoring include the following:
   - Client Management
   - Operating System Drive
   - Fixed Drive
   - Removable Drive
4. Edit your policy settings. Recommended policy settings for basic MBAM implementation include the following:

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**. Required to save operating system drive data to the MBAM Key Recovery server.
Removable Drive	Control Use of BitLocker on removable drives	Enabled. Required if MBAM will save removable drive data to the MBAM Key Recovery server. Check the **Allow users to apply BitLocker protection on removable data drives** option
Fixed Drive	Control Use of BitLocker on fixed drives	Enabled. 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**.

Global Policy Definitions

This section describes Global Policy definitions for BitLocker Administration and Monitoring.

Policy Name	Overview and Suggested Policy Setting
Prevent memory overwrite on restart	Configure this policy to improve restart performance without overwriting BitLocker

Policy Name	Overview and Suggested Policy Setting
	secrets in memory on restart. Suggested Configuration: **Not configured** When the policy is not configured, BitLocker secrets are removed from memory when the computer restarts.
Validate smart card certificate usage rule	Configure this policy to use smartcard certificate-based BitLocker protection. Suggested Configuration: **Not configured** When 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	Configure this policy to use a certificate-based data recovery agent or the BitLocker To Go reader. Suggested Configuration: **Not configured** When policy is not configured, the **Identification** field is not used. 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 aligned with this Group Policy setting.
Choose drive encryption method and cipher strength	Configure this policy to use a specific encryption method and cipher strength. Suggested Configuration: **Not configured** When policy is not configured, BitLocker will use the default encryption method of AES 128-bit with Diffuser or the encryption method specified by the setup script.

Client Management Policy Definitions

This section describes MBAM Client Management Policy definitions.

Policy Name	Overview and Suggested Policy Settings
Configure MBAM Services	This policy setting lets you configure key recovery service to back up BitLocker recovery information. It also lets you configure status reporting service for collecting compliance status reports. The policy provides an administrative method of recovering data encrypted by BitLocker to prevent data loss because of 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 disable this policy setting, the Key recovery information will not be saved; status report and key recovery activity will not be reported to server. Suggested Configuration: **Enabled** When **Select BitLocker recovery information to store** is set to **Recovery Password and key package**, the recovery password and key package will be automatically and silently backed up to configured key recovery server location. This policy setting manages how frequently the client checks the BitLocker protection policies and status on the client computer. This policy also manages how frequently the client compliance status is saved to the server. The client will check the BitLocker protection policies and status on the client computer, and also back up the client recovery key at the configured frequency. Set these frequencies based on the requirement set by your company on how frequently to check the compliance status of the computer, and how frequently to back up the client recovery key.
Allow hardware compatibility checking	This policy setting lets you check hardware compatibility before you enable BitLocker

Policy Name	Overview and Suggested Policy Settings
	protection on drives of a computer. When enabling this policy, the administrator has to make sure that Microsoft BitLocker Administering and Monitoring service is installed with the “Hardware Capability” feature. When enabling this policy, you can set the “Configure Key Recovery service”. If you enable this policy setting, once every 24 hours the model of the computer is validated against the hardware compatibility list before the policy enables BitLocker protection on drives of a computer. If you either disable or do not configure this policy setting, the computer model is not validated against the hardware compatibility list. Suggested Configuration: **Enabled** Enable this if your enterprise has older computer hardware or computers that do not support TPM. If this is the case, enable hardware compatibility checking to make sure that MBAM is only applied 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**.
Configure user exemption policy	This policy lets your organization exempt a user from BitLocker protection. The policy also lets you configuring a URL, email address, or telephone number for instruction on how to request exemption from BitLocker protection. If you enable this policy setting and provide a URL, mailing address, or telephone number, the user will able to apply for exemption and see a dialog for instruction on how to apply exemption form the BitLocker protection. If you disable or do not configure this policy setting, the user will not see a message for instructions on how to apply for an exemption

Policy Name	Overview and Suggested Policy Settings
	from BitLocker protection. The request exemption form will not be available to the user. Suggested Configuration: **Not Configured**

Operating System Drive Policy Definitions

This section describes MBAM Operating System Drive Policy Definitions.

Policy Name	Overview and Suggested Policy Setting
Operating system drive encryption settings	This policy setting determines whether 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 TPM PIN for operating system protection. • Configure enhanced startup PINs to permit characters such as uppercase and lowercase letters, symbols, numbers, and spaces. If you enable this policy setting, the user is required then to secure the operating system drive by using BitLocker. If you do not configure or if you disable the setting, the user is not required to secure the operating system drive by using BitLocker. If you disable this policy, the MBAM agent will decrypt the operating system volume if it is encrypted. Suggested configuration: **Enabled** When it is enabled, this policy setting requires the user 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

Policy Name	Overview and Suggested Policy Setting
	minimum PIN length to 8. 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)
Choose how BitLocker-protected operating system drives can be recovered	Configure this policy to enable the BitLocker data recovery agent or to save BitLocker recovery information to Active Directory Domain Services (AD DS). Suggested Configuration: **Not configured** When this policy is not configured, the data recovery agent is allowed, recovery information is not backed up to AD DS. MBAM operation does not require recovery information to be backed up to AD DS.
Configure TPM platform validation profile	This policy setting lets you configure how the Trusted Platform Module (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 has already been turned on with TPM protection. Suggested Configuration: **Not configured** When this policy is not configured, the TPM uses the default platform validation profile or the platform validation profile specified by the setup script.

Fixed Drive Policy Definitions

This section describes MBAM Fixed Drive Policy definitions.

Policy Name	Overview and Suggested Policy Setting
Fixed data drive encryption settings	This policy setting let you manage whether

Policy Name	Overview and Suggested Policy Setting
	fixed drives must be encrypted or not. When enabling this policy, you must not disable the “Configure use of password for fixed data drives” policy. If the **Enable auto-unlock fixed data drive** option is checked, the operating system volume must be encrypted If you enable this policy setting, the user will have to put all fixed drives under BitLocker protection and the drives will be encrypted. If you do not configure this policy or you disable this policy, then it is not required to put fixed drives under BitLocker protection. If you disable this policy, the MBAM agent will decrypt any encrypted fixed drives. Suggested Configuration: **Enabled**, and check the **Enable auto-unlock fixed data drive** option if the operating system volume is required to be encrypted. If encrypting the operating system volume is not required, clear the **Enable auto-unlock fixed data drive** checkbox.
Deny write access to fixed drives not protected by BitLocker	This policy setting determines whether BitLocker protection is required for fixed drives to be writable on a computer. This policy setting is applied when you turn on BitLocker. Suggested Configuration: **Not configured** When the policy is not configured, all fixed data drives on the computer will be mounted with read and write access.
Allow access to BitLocker-protected fixed drives from earlier versions of Windows	Enable this policy to let fixed drives with the FAT file system be unlocked and viewed on Windows Server 2008 computers. Suggested configuration: **Not configured** When the policy is not configured, fixed drives formatted with the FAT file system can be unlocked on computers that are running Windows Server 2008, Windows Vista,

Policy Name	Overview and Suggested Policy Setting
	Windows XP with SP3, or Windows XP with SP2, and their content can be viewed. These operating systems have read-only access to BitLocker-protected drives.
Configure use of password for fixed drives	Enable this policy to configure password protection on fixed drives. Suggested configuration: **Not configured** When the policy is not configured, passwords will be supported with the default settings that do not include password complexity requirements and require only 8 characters. For higher security, enable this policy and check **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	Configure this policy to enable the BitLocker data recovery agent or to save BitLocker recovery information to Active Directory Domain Services (AD DS). Suggested Configuration: **Not configured** When 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 recovery information to be backed up to AD DS.

Removable Drive Policy Definitions

This section describes MBAM Removable Drive Policy definitions.

Policy Name	Overview and Suggested Policy Setting
Control use of BitLocker on removable drives	This policy controls the use of BitLocker on removable data drives. Check the **Allow users to apply BitLocker protection on removable data drives** option to let the user run the BitLocker setup wizard on a removable data drive. Choose **Allow users to suspend and decrypt**

Policy Name	Overview and Suggested Policy Setting
	BitLocker on removable data drives to permit the user to remove BitLocker drive encryption from the drive or suspend the encryption while maintenance is performed. Suggested configuration: **Enabled** When this policy is enabled and the **Allow users to apply BitLocker protection on removable data drives** option is checked, the MBAM agent saves the recovery information about removable drives to the MBAM key recovery server and lets a user recover the drive if the password is lost.
Deny write access to removable drives not protected by BitLocker	Enable this policy to only allow write access to BitLocker protected drives. Suggested Configuration: **Not configured** When this policy is enabled, all removable data drives on the computer require encryption before write access is allowed.
Allow access to BitLocker-protected removable drives from earlier versions of Windows	Enable this policy to allow fixed drives with the FAT file system to be unlocked and viewed on Windows Server 2008 computers. Suggested Configuration: **Not configured** When this policy is not configured, removable data drives formatted with the FAT file system can be unlocked on computers that are running Windows Server 2008, Windows Vista, Windows XP with SP3, or Windows XP with SP2, and their content can be viewed. These operating systems have read-only access to BitLocker-protected drives.
Configure use of password for removable data drives	Enable this policy to configure password protection on removable data drives. Suggested configuration: **Not configured** When this policy is not configured, passwords are supported with the default settings that do not include password complexity requirements and require only 8 characters. For increased security, you may enable this

Policy Name	Overview and Suggested Policy Setting
	policy and check **Require password for removable data drive**, select **Require password complexity**, and set the preferred **minimum password length**.
Choose how BitLocker-protected removable drives can be recovered	Configure this policy to enable the BitLocker data recovery agent or to save BitLocker recovery information to Active Directory Domain Services (AD DS). Suggested Configuration: **Not configured** When 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 recovery information to be backed up to AD DS.

Windows Policies

Microsoft BitLocker Administration and Monitoring offers a customized BitLocker control panel application that, when it is configured, replaces the default BitLocker control panel application in Windows. The updated BitLocker Encryption Options control panel application allows users to manage their PIN and passwords and unlock drives. The updated control panel application also hides the interface that lets administrators decrypt a drive or to suspend or resume BitLocker encryption.

Important
The customized MBAM control panel application is not deployed automatically. You must follow these steps to configure and deploy the MBAM control panel application:

Hide BitLocker in Control Panel

1. 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, browse to **User configuration**, click **Policies**, select **Administrative Templates**, and then click **Control Panel**.
2. Double-click **Hide specified Control Panel items** in the details pane, and then select **Enabled**.
3. Click **Show**, and then type Microsoft.BitLockerDriveEncryption. This policy hides the BitLocker Drive Encryption application in Control Panel and replaces it with the updated BitLocker Encryption Options tool in the Windows control panel.

See Also

Planning for MBAM

Planning the Server Infrastructure for MBAM

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

Planning for MBAM Server Deployment

The following Microsoft BitLocker Administration and Monitoring features represent the server infrastructure features for an MBAM server deployment:

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

These features can be installed on a single server or distributed across multiple servers.

In addition to the server related Microsoft BitLocker Administration and Monitoring features, the server setup application includes a MBAM Group Policy template feature. This feature can be installed on any client able to run the Group Policy Management Console (GPMC) or Advanced Group Policy Management (AGPM).

Microsoft BitLocker Administration and Monitoring server components can be installed in different configurations, by using from one to five servers. Generally, we recommend that you use a three- or five-server configuration for production environments, though two or four servers can be used also.

- **Single computer configuration**

  All Microsoft BitLocker Administration and Monitoring features are installed on a single server. This configuration is supported, but only recommended for testing.

- **Three-computer configuration**

  Server features are installed in the following configuration

  - Recovery and Hardware Database, Compliance Status Database, and Compliance and Audit Reports features are installed on a server.
  - Administration and Monitoring Server feature is installed on a server.
  - Group Policy template is installed on a server or client computer.

- **Five-computer configuration**

  Each server feature is installed on dedicated computers:

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

- Group Policy Template is installed on a server or client computer

Note

A three or five computer configuration is recommended for production environments.

Order of Deployment of BitLocker Administration and Monitoring Server Features

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

Note

Keep track of the names of the servers each feature is installed on. This information will be used throughout the installation process.

Each Microsoft BitLocker Administration and Monitoring feature has specific prerequisites. For a full list of server component prerequisites, see MBAM Supported Configurations.

See Also

Planning for MBAM

Deploying MBAM on a Single Server

Deploying MBAM on Distributed Servers

Planning for High Availability for MBAM

The information in this topic can be used to configure a highly available Microsoft BitLocker Administration and Monitoring (MBAM) installation.

High Availability Scenarios for MBAM

Microsoft BitLocker Administration and Monitoring (MBAM) was designed to be fault-tolerant and not impact the users in the event a server is not available. For example, if the MBAM Agent cannot connect to the MBAM Web Server, the user will not be prompted for action.

When planning for your Microsoft BitLocker Administration and Monitoring (MBAM) install, consider the following scenarios which can affect availability of the MBAM service:

- Encrypting a drive – if a Recovery Password cannot be escrowed, the encryption will not start on a client computer
- Upload Compliance Status – if the server hosting the compliance status report service is not available, the compliance data will grow stale
- Help Desk and Key Recovery console - if the Help Desk console is not available, users will be unable to get to their Recovery Keys
- Get Compliance Reports – reports will not be available if the server hosting the Compliance Reports feature is not available

The main scenario to consider around High Availability is BitLocker Key Recovery Help Desk availability. If help desk cannot provide a Recovery Key, a user that is locked out cannot access their computer. For this reason, it is worth considering using redundant web servers and databases to ensure High Availability.

General guidance on high availability for SQL Server can be found here:
http://go.microsoft.com/fwlink/?LinkId=221504

General guidance on availability and scalability for Web Servers can be found here:
http://go.microsoft.com/fwlink/?LinkId=221503

See Also

Planning for MBAM

Planning for MBAM Administrator Roles

Microsoft BitLocker Administration and Monitoring (MBAM) administrator roles are managed by local groups that are created by Microsoft BitLocker Administration and Monitoring Setup when you install the BitLocker Administration and Monitoring Server, the Compliance and Audit Reports, and Compliance Status Database features.

The membership of Microsoft BitLocker Administration and Monitoring roles can best be managed by creating security groups in Active Directory, adding the appropriate administrator accounts to those groups, and then adding those security groups to the BitLocker Administration and Monitoring local groups. For more information, see How to Manage MBAM Administrator Roles.

Planning for Administrator Roles

List of available Administrator Roles in MBAM:

MBAM System Administrators

Administrators in this role have access to all Microsoft BitLocker Administration and Monitoring 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 Microsoft BitLocker Administration and Monitoring. 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 Microsoft BitLocker Administration and Monitoring. 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 from Microsoft BitLocker Administration and Monitoring. The local group for this role is installed on the Administration and Monitoring Server, Compliance and Audit Reports Server, and Compliance Status Database Server.

MBAM Advanced Helpdesk Users

Administrators in this role have increased access to the Helpdesk features from Microsoft BitLocker Administration and Monitoring. 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 reports an administrative user must be a member of the **MBAM Report Users** security group on the Administration and Monitoring Server. Compliance Status database server, and the server hosting the Compliance and Reports feature. As a best practice, create a security group in Active Directory with rights on these local **MBAM Report Users** security group on both the Administration and Monitoring Server and the server hosting the Compliance and Reports feature.

See Also

Planning for MBAM

Planning for MBAM Client Deployment

With Microsoft BitLocker Administration and Monitoring (MBAM), you can encrypt a computer in your organization either before the end-user receives the computer or afterwards using group policy.

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

Note

To review the MBAM client system requirements, see MBAM Supported Configurations.

Computer Encryption before Distribution to the User

In organizations where computers are received and configured centrally, you can encrypt each computer before any user data is written to the new computer. The benefit of this process is that every computer is compliant. 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 Trusted Platform Modules (TPM) to encrypt computers, adding this protector type is completed when the administrator encrypts 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 encrypts the system volume with the TPM protector, and then the user selects a PIN the first time the user logs on. If your organization decides to only use the PIN protector, the administrator does not have to encrypt the volume first. When the user logs on, Microsoft BitLocker Administration and Monitoring prompts the user to provide a PIN or a PIN and password to be used on later computer restarts.

Note

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

Computer Encryption after Distribution to the User

By configuring and distributing Group Policy and the Microsoft BitLocker Administration and Monitoring client agent software by using either Active Directory Domain Services or an enterprise software distribution system, users who have Windows computers are prompted to encrypt their computer. This lets Microsoft BitLocker Administration and Monitoring collect the data including the PIN and password, and then begin the encryption process.

Note
In this approach, the user is prompted to activate and initialize the TPM chip if it has not been previously activated.

See Also

Planning for MBAM

Deploying the MBAM Client

Planning Hardware Management for MBAM

The Microsoft BitLocker Administration and Monitoring (MBAM) Hardware Compatibility feature can be used to ensure that only the computer hardware that you specify as supporting BitLocker will be encrypted. When this feature is turned on, Microsoft BitLocker Administration and Monitoring will only encrypt computers that are marked as compatible.

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

The Hardware Compatibility feature is best used when your organization has older computer hardware or computers that do not support Trusted Platform Module (TPM) chips. If this is the case, you can use the Hardware Compatibility feature to ensure that BitLocker encryption is only applied 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.

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, Trusted Platform Module (TPM) maker, and TPM version and then passes this 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. This list is automatically updated by the MBAM client agents deployed in the enterprise with all new computer makes and models added with a state of **Unknown**. An administrator can then use the MBAM Administration console website to change list entires to specify a particular computer make and model as **Compatible** or **Incompatible**.
4. Before the MBAM client agent begins encrypting, 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 re-check the hardware compatibility status of the computer one time per day.
   - If the hardware is marked as incompatible, the agent will log an event and pass a ‘hardware exempted’ state as part of compliance reporting. The agent will check every 7 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 re-check the hardware compatibility status of the computer one time per day.

Warning

If the MBAM client agent attempts to encrypt a computer that does not support BitLocker drive encryption, there is a possibility that the computer will be corrupted. Because of this, you should ensure that the hardware compatibility feature is correctly configured when your organization has older hardware that does not support BitLocker.

See Also

Planning for MBAM

Planning for Single Use Recovery Keys

With the Microsoft BitLocker Administration and Monitoring (MBAM) Recovery Password feature, you can unlock a BitLocker-encrypted device without the main protector type, for example, a Trusted Platform Module (TPM) and a PIN, or only a PIN. As useful as this is, the limitation of this feature is that the user can reuse the computer without any control from the MBAM administrators. If a user gets the recovery password and saves it or leaves a copy on their desk, a malicious user can reuse the recovery password on the computer to bypass the BitLocker protection.

The Single Use Recovery Key feature of MBAM works to mitigate this risk in the following ways:

1. When a BitLocker-protected drive enters recovery mode, the user requires a recovery key to unlock the drive. Normally, this recovery key could be used again to unlock the drive. To prevent this, configure Microsoft BitLocker Administration and Monitoring to use single-use recovery keys that expire upon use. See Planning and Configuring Group Policy for MBAM for steps on how to configure single-use recovery keys.
2. The single use of a recovery password is automatically applied to operating system drives and fixed drives. For a removable drives, it is applied when the drive is removed, and then re-inserted and unlocked on a computer that has group policy settings activated to manage removable drives.

See Also

Planning for MBAM

Deploying MBAM

Before deploying Microsoft BitLocker Administration and Monitoring (MBAM), you should complete the necessary planning tasks by following the topics listed in the Planning for MBAM section of this guide. This will help you to fully understand what MBAM is and how you can use MBAM to meet your organization's needs.

After completing all necessary planning, use the information in this section to help you deploy MBAM in your environment.

Note
MBAM requires that you use the same values for all features, so ensure that you keep track of all values that you use as you install each feature.

Deploying MBAM

Deploying MBAM Group Policies

Describes the Group Policies used by MBAM and how to configure them.

Deploying MBAM on a Single Server

Describes how to install MBAM and its various server components in a single server configuration.

Deploying MBAM on Distributed Servers

Describes how to install MBAM and its various server components in a multi-server configuration.

Deploying the MBAM Client

Describes how to install the MBAM client and manage its service.

See Also

BitLocker Administration and Monitoring Home

Getting Started With MBAM

Planning for MBAM

Operations for MBAM

Troubleshooting MBAM

Deploying MBAM Group Policies

To successfully deploy Microsoft BitLocker Administration and Monitoring (MBAM), you first have to determine the Group Policies that you will use in your implementation of MBAM. See Planning and Configuring Group Policy for MBAM for more information on the different policies that are available. As soon as you have determined the policies that you are going to use, you then must create one or more Group Policy objects (GPO) that include the policy settings for MBAM.

Deploying MBAM Group Policy Settings

After you create the necessary GPOs, use the following steps to deploy the MBAM group policy settings to your organization's client computers.

To edit MBAM client GPO settings

1. On a computer that has Group Policy settings for BitLocker installed, make sure Microsoft BitLocker Administration and Monitoring services are enabled.
2. Using the Group Policy Management Console (GPMC.msc), the Advanced Group Policy Management (AGPM), or the Local Group Policy Editor (GPEDIT.msc) on the BitLocker Group Policies computer, select **Computer configuration**, choose **Policies**, click **Administrative Templates**, select **Windows Components**, and then click **MDOP MBAM (BitLocker Management)**.
3. Next, edit the setting for the Microsoft BitLocker Administration and Monitoring policy. For each policy in the table that follows, select **Policy Group**, click the **Policy**, and then configure the **Setting**. The following table lists Group Policy settings that are required to enable Microsoft BitLocker Administration and Monitoring services on client computers:

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**. Required to save operating system drive data to the MBAM Key Recovery server.
Removable Drive	Control Use of BitLocker on removable drives	Enabled. Required if MBAM will save removable drive data to the MBAM Key Recovery server.
Fixed Drive	Control Use of BitLocker on fixed drives	Enabled. 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 and Configuring Group Policy for MBAM for Group Policy configuration details for all MBAM policies.

Hide Windows BitLocker Control Panel

Microsoft BitLocker Administration and Monitoring offers a customized MBAM control panel that can replace the default Windows BitLocker control panel when it is configured. The updated BitLocker Encryption Options control panel lets users manage their PIN and passwords and unlock drives. The control panel also hides the interface that lets administrators decrypt a drive or to suspend or resume BitLocker encryption.

To hide BitLocker Control Panel in Windows

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. Next, click **Policies**, select **Administrative Templates**, and then click **Control Panel**.

2. Double-click **Hide specified Control Panel items** in the details pane, and then select **Enabled**.
3. Click **Show**, and then type Microsoft.BitLockerDriveEncryption. This policy hides the default Windows BitLocker Management tool from the Windows control panel and lets the user open the updated BitLocker Encryption Options tool from the Windows control panel.

See Also

Planning and Configuring Group Policy for MBAM

Deploying MBAM

Deploying 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, see MBAM 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 Planning the Server Infrastructure for MBAM before beginning MBAM deployment.

Note

In order to obtain the setup log files, you have to install Microsoft BitLocker Administration and Monitoring by using the msiexec package and the /L <location> option. Log files are created in the location specified.

Additional setup log files are created in the installing user's %temp% folder.

Deploying the MBAM Server

The following steps describe how to install general Microsoft BitLocker Administration and Monitoring features.

Note

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

Starting the MBAM Server Install

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

   For more information about how to plan the Microsoft BitLocker Administration and

Monitoring server infrastructure, see Planning the Server Infrastructure for MBAM. For prerequisites of each MBAM server feature, see MBAM Supported Configurations.

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

Deploying the MBAM Server Features

1. In the **Configure the Recovery and Hardware database** window, specify the instance of SQL Server and name of the database that will store the recovery and hardware data. You must also specify both where the database files will be located and where the log information will be located.
2. Click **Next** to continue.
3. In the **Configure the Compliance and Audit database** window, specify the instance of SQL Server and name of the database that will store the compliance and audit data. You must also specify where the database files will be located and where the log information will be located.
4. Click **Next** to continue.
5. In the **Configure the Compliance and Audit Database** 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 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 is specified 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**. This does not turn on Automatic Updates in Windows.

10. As soon as the Setup wizard has collected the necessary feature information, the Microsoft BitLocker Administration and Monitoring installation is ready to start. Click **Back** to move back through the wizard if you have to review or change your installation settings. Click **Install** to being the installation. Click **Cancel** to exit Setup. Setup installs the Microsoft BitLocker Administration and Monitoring features and notifies you that the installation is completed.
11. Click **Finish** to exit the wizard.
12. Now that the Microsoft BitLocker Administration and Monitoring server components have now been installed, users have to be added to the Microsoft BitLocker Administration and Monitoring roles. For more information, see How to Manage MBAM Administrator Roles.

Post Installation Configuration

1. After setup is finished, you must add users Roles before users have access to features in the MBAM management console. On the Administration and Monitoring Server, add users to the following local groups to give them access to the features in the management console.
   - **MBAM Hardware Users** =

     Members of this local group will have access to the Hardware feature in the management console.
   - **MBAM Helpdesk Users**

     Members of this local group will have access to the Drive Recovery and Manage TPM features in the management console. All fields in Drive Recovery and Manage TPM are required fields for a Helpdesk User.
   - **MBAM Advanced Helpdesk Users**

     Members of this local group will have advanced access to the Drive Recovery and Manage TPM features in the management console. For Advanced Helpdesk Users, only the “Key ID” field is required in Drive Recovery. In Manage TPM, only the “Computer Domain” and “Computer Name” fields are required.
2. On the Administration and Monitoring, Compliance Status Database, Compliance and Audit Reports Server and add users to the following local group to enable them access the Reports feature in the management console.
   - **MBAM Report Users:** Members of this local group will have access to the Reports features in the management console.

     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, Compliance Status Database, Compliance and Audit Reports Server features are installed.

     The recommended way to do this is to create a domain security group and add that domain group to each local MBAM Report Users group. As soon as you do

this, manage the group memberships by way of the domain group.

Validating the MBAM Server Feature Installations

As soon as the Microsoft BitLocker Administration and Monitoring installation is complete, we recommend that you validate the installation has successfully set up all the necessary features for BitLocker. Use the following procedure to confirm that the Microsoft BitLocker Administration and Monitoring service is functional.

To validate an MBAM installation

1. On each server where a Microsoft BitLocker Administration and Monitoring feature is deployed, open the Control Panel. Select **Programs**, and then select **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 feature 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 Status Database feature 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 feature is 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. The actual URL can be found by using the Reporting Services Configuration Manager tool and selecting the instances specified during setup.

   Confirm that a reports 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 <*machinename*>, 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 browse to the following locations in the MBAM website to verify 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

   This list assumes the services are installed on the default port 80 without network encryption. If the services were 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.

See Also

Deploying MBAM

Deploying MBAM on Distributed Servers

The procedures in this topic describe the full installation of the Microsoft BitLocker Administration and Monitoring (MBAM) features on a multiple servers. Each server feature has certain prerequisites. To verify that you have met the prerequisites, see MBAM 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 Planning the Server Infrastructure for MBAM before beginning MBAM deployment.

Note

In order to obtain the setup log files, you have to install Microsoft BitLocker Administration and Monitoring by using the msiexec package and the /L <location> option. Log files are created in the location specified.

Additional setup log files are created in the installing user's %temp% folder.

Deploying the MBAM Server

The following steps describe how to install general Microsoft BitLocker Administration and Monitoring features.

Note

Make sure that you use the 32-bit setup on 32-bit servers and the 64-bit setup on 6-bit servers.

To deploy MBAM server features

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

   For more information about how to plan the MBAM server infrastructure, see Planning the

Server Infrastructure for MBAM. For prerequisites of each MBAM server feature, see MBAM Supported Configurations.

The installation wizard checks the prerequisites for your installation and displays 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 installation pages for the selected features. The following sections describe installation procedures for each feature.

   Note
   The following instructions assume that each feature will be installed on a separate server. If you are installing multiple features on a single server, some steps may be altered or eliminated.

To install the Recovery and Hardware Database feature

a. 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 Certificate Authority-provisioned certificate that is used for encryption.
b. Click **Next** to continue.
c. To configure access to the Recovery and Hardware Database, specify the names of the computers that will be running the Administration and Monitoring Server feature. Once the Administration and Monitoring Server feature is deployed, it connects to the database 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 both where the database will be located and where the log information will be located.
f. Click **Next** to continue with the Microsoft BitLocker Administration and Monitoring Setup wizard.

To install the Compliance Status Database feature

a. MBAM can encrypt the communication between the Compliance Status database and the Administration and Monitoring servers. If you choose the option to encrypt communication, you are asked to select the Certificate 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. To configure access to the Compliance Status Database, specify the

computer names of the machines that will be running the Administration and Monitoring Server and Compliance and Audit Reports features. Once the Administration and Monitoring and Compliance and Audit Reports Server features are deployed they will connect to the databases 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 Microsoft BitLocker Administration and Monitoring Setup wizard.

To install the Compliance and Audit Reports feature

a. Specify the remote SQL Server instance (for example: <*ServerName*>) where the Compliance Status Database was installed.

b. Next, specify where the name of the Compliance Status Database. By default, the database name is “MBAM Compliance Status,” although this may be altered when you install the Compliance Status Database feature.

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 for accessing the compliance database.

e. Click **Next** to continue with the Microsoft BitLocker Administration and Monitoring Setup wizard.

To install the Administration and Monitoring Server feature

a. 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 Certificate 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 Status Database was installed.

d. Next, specify the name of the Compliance Status Database. By default, the database name is “MBAM Compliance Status,” however this may be altered when installing the Compliance Status Database feature.

e. Click **Next** to continue.

f. Specify the remote SQL Server instance (for example: <*ServerName*>) where the Recovery and Hardware Database was installed.

g. Next, specify the name of the Recovery and Hardware Database. By default,

the database name is **MBAM Recovery and Hardware**; however, this may be altered when installing 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 can be found at:

http://<*NameofMBAMReportsServer*>/ReportServer

Note
If SQL Server Reporting Services was configured as a named instance the URL resemble 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 is specified must be an unused port number on the Administration and Monitoring server unless a unique host header name is specified.

l. Click **Next** to continue with the Microsoft BitLocker Administration and Monitoring Setup wizard.

5. Specify whether to use Microsoft Updates to help keep your computer secure, and then click **Next**.
6. As soon as the selected Microsoft BitLocker Administration and Monitoring feature information is complete, the Microsoft BitLocker Administration and Monitoring installation by using the Setup wizard is ready to start. Click **Back** to move through the wizard if you have to review or change your installation settings. Click **Install** to being the installation. Click **Cancel** to exit the Wizard. Setup installs the Microsoft BitLocker Administration and Monitoring features that you have selected and notifies you that the installation is finished.
7. Click **Finish** to exit the wizard.
8. Although the Microsoft BitLocker Administration and Monitoring server components have now been installed, users have to be added to the Microsoft BitLocker Administration and Monitoring roles. For more information, see How to Manage MBAM Administrator Roles.

Post Installation Configuration

1. After the Setup is finished, you must add users Roles before users have access to features in the MBAM management console. On the Administration and Monitoring Server, add users to the following local groups to give them access to the features in the management console.

- **MBAM Hardware Users**

  Members of this local group will have access to the Hardware feature in the management console.
- **MBAM Helpdesk Users**

  Members of this local group will have access to the Drive Recovery and Manage TPM features in the management console. All fields in Drive Recovery and Manage TPM are required fields for a Helpdesk User.
- **MBAM Advanced Helpdesk Users**

  Members of this local group will have advanced access to the Drive Recovery and Manage TPM features in the management console. For Advanced Helpdesk Users, only the “Key ID” field is required in Drive Recovery. In Manage TPM, only the “Computer Domain” and “Computer Name” fields are required.

2. On the Administration and Monitoring, Compliance Status Database, and Compliance and Audit Reports Server, add users to the following local group to give them access to the Reports feature in the management console.
   - **MBAM Report Users:**

     Members of this local group will have access to the Reports features in the management console.

   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, Compliance Status Database, Compliance and Audit Reports Server feature are installed.

Validating the MBAM Server Feature Installations

As soon as the Microsoft BitLocker Administration and Monitoring installation is complete, we recommend that you validate that the installation has successfully set up all the necessary features for MBAM. Use the following procedure to confirm that the Microsoft BitLocker Administration and Monitoring service is functional.

To validate an MBAM installation

1. On each server where a Microsoft BitLocker Administration and Monitoring feature is deployed, open the Control Panel. Select **Programs**, and then select **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 feature 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 Status Database feature 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 feature is 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. The actual URL can be found by using the Reporting Services Configuration Manager tool and selecting the instances specified during setup.

   Confirm that a reports 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 <*machinename*>, select **Sites**, and select **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 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
   This list assumes the services are installed on the default port 80 without network encryption. If the services were 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.

See Also

Deploying MBAM

Deploying the MBAM Client

The Microsoft BitLocker Administration and Monitoring (MBAM) client enables administrators to enforce and monitor BitLocker drive encryption on computers within 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.

To deploy the MBAM client to desktop or laptop computers

1. Locate the Microsoft BitLocker Administration and Monitoring client installation files: MBAMClient-64bit.msi and MBAMClient-32bit.msi, which are provided with the MBAM software.
2. Use Active Directory Domain Services or an enterprise software deployment tool like Microsoft System Center Configuration Manager 2007 to deploy the Windows Installer package to target computers.

   Note
   It is not recommend to use Group Policy to deploy the Windows Installer package.
3. Configure the distribution settings or Group Policy to run the client software file. After it is installed, the client reads the Group Policy settings that are received from a domain controller.

To encrypt a computer as part of Windows deployment

Encrypting client computers with BitLocker during the initial imaging stage of a Windows deployment can lower the administrative overhead necessary for implementing MBAM in an organization. It also ensures that every computer that is deployed already has BitLocker running and is configured correctly.

1. If your organization is planning 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 BIOS of the computer. Refer to the manufacturer documentation for more details about how to configure the TPM chip.
2. Install the Microsoft BitLocker Administration and Monitoring client agent.

3. Join the computer to a domain (recommended).
   - If the computer is not joined to the 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. Run the command prompt as an administrator, stop the MBAM service, and then set the service to **manual** or **on demand**, and then start by typing the following commands:

   net stop maltaagent

   sc config maltaagent start= demand
5. Set the registry settings for the MBAM agent to ignore Group Policy and run the TPM for "operating system only encryption" by running Regedit, and then importing 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 = Uploads Recovery Key Only
	1 = Uploads Recovery Key and Key Recovery Package (default)
KeyRecoveryServiceEndPoint	Set this value to the URL for the Key Recovery web server, for example, http://<computer name>/MBAMRecoveryAndHardwareService/CoreService.svc.

   Note

   MBAM policy or registry values can be set here to override 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 maltaagent

8. The system should restart. On restart, the BIOS prompts you to accept a TPM change. Accept this change.
9. During the Windows client operating system imaging process, when you are ready to start encryption, restart the MBAM agent service, and set start to **automatic** by running a command prompt as an administrator and typing the following commands:

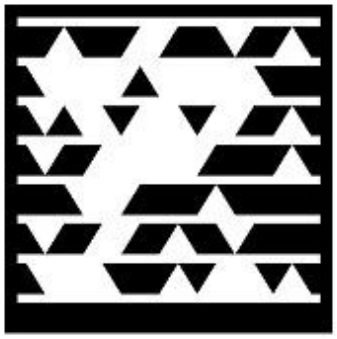
   sc config maltaagent start= auto

   net start maltaagent
10. Remove the bypass registry values by running Regedit and going to the "HKLM\SOFTWARE\Microsoft" registry entry. To delete the **MBAM** node, right-click the node to select **Delete**.

See Also

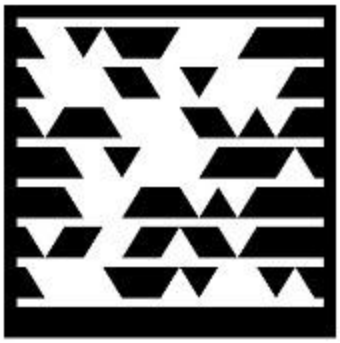
Deploying MBAM

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



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

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



Operations for MBAM

After completing all necessary planning and then deploying MBAM, you can configure and use it to manage enterprise BitLocker encryption.

The information in this section describes post-installation configuration, management, and day-to-day operations tasks.

Note

By default, BitLocker uses the IIS logs for its websites and services. These are located under $systemdrive$\inetpub\logs\w3svc

Web service and website trace logs are created under the folder specified for installing the websites and services.

How to Use MBAM Reports

Describes MBAM reporting and what information the reports contain, as well as how to generate reports on enterprise compliance, individual computers, key recovery activity, and hardware compatibility.

How to Determine BitLocker Encryption State of Lost Computers

Describes how to determine whether volumes on a computer are encrypted if there is a loss or theft of a computer.

How to Recover an Encrypted Drive

Describes how to access the BitLocker centralized key recovery data system that can provide a recovery password for data recovery on locked, corrupted, or moved drives.

How to Reset a TPM Lockout

Describes how to unlock a computer if there is a TPM lockout.

How to Manage Hardware Compatibility

Describes how to manage BitLocker compatibility for computer models in an enterprise organization.

How to Manage User and Computer Exemptions

Describes how an organization can set up computer or user exemption from MBAM protection.

How to Manage MBAM Administrator Roles

Describes how to give administrative users access to one or more MBAM features.

How to Use the Client Control Panel

Describes the MBAM BitLocker Encryption Options control panel.

How to Move MBAM Features to Another Server

Describes the steps that you should take to move one or more Microsoft BitLocker Administration and Monitoring (MBAM) features to a different computer.

How to Administer MBAM Using PowerShell

Describes how to administer MBAM using PowerShell.

See Also

BitLocker Administration and Monitoring Home

Getting Started With MBAM

Planning for MBAM

Deploying MBAM

Troubleshooting MBAM

How to Use MBAM Reports

Microsoft BitLocker Administration and Monitoring (MBAM) generates different reports to monitor BitLocker usage and compliance. The procedures that follow describe the steps that are needed to generate reports on enterprise compliance, individual computers, key recovery activity, and hardware compatibility. In addition, this topic also includes detailed information to help understand MBAM reports.

Note
To run the reports, you must be a member of the **Report Users Role** on the servers where the "Administration and Monitoring Server," "Compliance and Audit Reports," and "Compliance Status Database" features are installed.

To open the MBAM Management Console

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

   Note
   If the management console was installed on a port other than 80, you have to specify the port in the URL (for example: *http://<computername>:<port>*. If you specified a Host Name for the management console during the installation, the URL would be *http://<hostname>*.

2. In the left side pane, click **Reports** and then select the report you want to run from the top menu bar.

   Note
   For more information about what is presented in MBAM reports, see the **Understanding MBAM Reports** section at the end of this topic.

The following sections describe the MBAM Compliance and Auditing reports.

To generate an Enterprise Compliance Report

1. From the Management Console, select the Reports node from the left side navigation pane, select **Enterprise Compliance Report**, and select the filters that you want to use. The available filters for the Enterprise Compliance Report are the following.
   - **Compliance Status**. Use this filter to specify the compliance status types (for example, Compliant, or Noncompliant) of the report
   - **Error State**. Use this filter to specify the Error State types (for example, No Error, or Error) of the report
2. Click **View Report** to display the selected report.

   Results can be saved in different formats, such as HTML, Microsoft Word, and Microsoft

Excel.

Note

The Enterprise Compliance report is generated by a SQL job that runs every 6 hours. Therefore, the first time you attempt to view the report you may find that some data is missing.

3. Select a computer name to view information about the computer in the Computer Compliance Report.
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 Management Console, select the Report node from the left hand 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 different formats, such as HTML, Microsoft Word, and Microsoft Excel.
3. Select a computer name to display the more information about the computer in the Computer Compliance Report.
4. Select the plus sign (+) next to the computer name to view information about the volumes on the computer.

To generate the Recovery Key Audit Report

1. From the Management Console, select the Report node in the left hand 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**. This filter enables the user to specify the user name of the requestor. The requestor is the person in helpdesk who accessed the key on behalf of a user.
   - **Requestee**.This filter enables the user to specify the user name of the requestee. The requestee is the person who called helpdesk to obtain a recovery key.
   - **Request Result**.This filter enables the user to specify the request result types (for example: Success or Failed) that they want to base the report on. For example, the user may want to view failed key access attempts.
   - **Key Type**. This filter enables the user to specify the Key Type (for example: Recovery Key Password or TPM Password Hash) that they want to base the report on.
   - **Start Date**. This filter is used to define the Start Date part of the date range that they user want to report on.
   - **End Date**. This filter is used to define the End Date part of the date range that they user want to report on.
2. Click **View Report** to view the report.

Results can be saved in different formats, such as HTML, Microsoft Word, and Microsoft Excel.

To generate the Hardware Compatibility Audit Report

1. From the Management Console, select the **Report** node from the left navigation pane, and select the **Hardware Audit Report**. Select the appropriate filters for your Hardware Audit report. The available filters for Hardware Audits include the following:
   - **User (Domain\User)**. This filter enables the user to specify the name of the user who made a change.
   - **Change Type**. This filter enables the user to specify the type of changes they are looking for.
   - **Start Date**. This filter is used to define the Start Date part of the date range that they user want to report on.
   - **End Date**. This filter is used to define the End Date part of the date range that they user want to report on.
2. Click **View Report** to view the report.

   Results can be saved in different formats, such as HTML, Microsoft Word, and Microsoft Excel.

Understanding Reports

To access the Reports feature of Microsoft BitLocker Administration and Monitoring, open a web browser and open the MBAM management console. Select **Reports** in the left menu bar and then select from the top menu bar the kind of report that you want to generate.

Enterprise Compliance Report Use this report type to collect information on overall BitLocker compliance in your organization. You can use different filters to narrow your search results to Compliance state and Error status. This report runs every 6 hours.

Enterprise Compliance Report Fields

Column Name	Description
Computer Name	This is the user-specified DNS name that is being managed by MBAM
Domain Name	This is the fully qualified domain name where the client computer resides and is managed by MBAM
Compliance Status	An indication of two states; Noncompliant and Compliant according to the policy specified for the computer (see table Enterprise Compliance Report Compliance States for more information about how to interpret compliance states)

Column Name	Description
Exemption	Describes the state of the computer hardware for the identification of the hardware type, and whether the computer is 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 (the hardware was identified and is not exempt from policy)
Device Users	Lists known users on the computer that is being managed by MBAM
Compliance Status Details	Lists the error and status messages of the compliance state of the computer in accordance to the policy specified
Last Contact	Indicates the 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	Expand the Computer Compliance Report details by clicking on Computer Name, 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 may be in process, or there is an error on the computer. If there is no error, then the likely cause is that the

Compliance Status	Exemption	Description	User Action
			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; the state of the computer can be confirmed by viewing the Computer Compliance Report.
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 compliant	No action needed; the state of the computer is exempt by policy from
Compliant	Hardware Unknown	Indicates that the hardware type was identified by MBAM. However, it is unknown by MBAM whether it is exempt or not exempt (meaning an administrator has not set the compatible status), therefore reverts by default to Compliant status.	This is the initial state of a newly deployed MBAM client. It is usually but not always a transient state. Even if the administrator has marked the Hardware (See Hardware function) as Compatible, there is a delay or wait-time (configurable by was of MBAM policy) between the user request to make compatible and the time the client computer reports back in. Notice the time of Last Contact, and check in again after

Compliance Status	Exemption	Description	User Action
			the specified interval to determine if the state has changed. If the state has not changed on the new report interval, there may be an error for this computer or hardware type.

Computer Compliance Report Use this report type to collect information that is specific to a computer or user.

This report can be viewed by clicking the computer name in the Enterprise Compliance Report, or by typing in the computer name in the Computer Compliance Report. The Computer Compliance Report provides detailed encryption information about each drive (Operating System and Fixed data drives) on a computer, and also an indication of the policy that is applied to each drive type on the computer. To view the details of each drive, expand the Computer Name entry

Note

Removable Data Volume encryption status will not be shown in the report.

Compliance Report Fields

Column Name	Description
Computer Name	This is the user specified DNS computer name that is being managed by MBAM
Domain Name	This is the fully qualified domain name where the client computer resides and is managed by MBAM
Computer Type	Indicates the kind of computer. Valid types are non-Portable and Portable.
Operating System	Specifies the Operating System type found on the MBAM managed client computer.
Compliance Status	Indicates the overall Compliance Status of the computer managed by MBAM. Valid states are Compliant and Noncompliant. Notice that the compliance status per drive (see table that follows) may indicate different compliance states. This field however represents that compliance state in accordance to the policy

Column Name	Description
	specified.
Policy Cypher Strength	Indicates the Cipher Strength selected by the Administrator during MBAM policy specification. (for example, 128-bit with Diffuser)
Policy Operating System Drive	Indicates if encryption is required for the O/S and the appropriate protector type.
Policy-Fixed Data Drive	Indicates if encryption is required for the Fixed Drive.
Policy Removable Data Drive	Indicates if encryption is required for the Removable Drive.
Device Users	Lists a known users on the computer that is being managed by MBAM
Exemption	Describes the state of the computer hardware for the identification of the hardware type, and 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 (the hardware was identified and is not exempt from policy).
Manufacturer	Specifies the computer manufacturer name as it appears in the computer BIOS
Model	Specifies the computer manufacturer model name as it appears in the computer BIOS
Compliance Status Details	Lists the error and status messages of the compliance state of the computer in accordance to the policy specified
Last Contact	Indicates the date and time when the computer last contacted the server to report compliance status. This time is configurable (see MBAM policy settings)

Compliance Report Drive Fields

Column Name	Description
Drive Letter	Indicates the computer drive letter that was assigned to the particular drive by the user.
Drive Type	Indicates the kind of drive. Valid values are Operating System Drive and Fixed Data Drive. These are physical drives not logical volumes.
Cypher Strength	Indicates the Cipher Strength selected by the Administrator during MBAM policy specification.
Protector Type	Indicates the type of protector selected via policy used to encrypt an OS or Fixed volume. The valid protector types on an O/S are TPM or TPM+PIN and for a Fixed Data Volume is Password.
Protector State	Indicates that the computer being managed by MBAM has enabled the protector type specified in the policy. The valid states are ON or OFF.
Encryption State	Indicates the encryption state of the drive. Valid states are Encrypted, Not Encrypted, and Encrypting.
Compliance Status	An indication of two states; Noncompliant and Compliant in accordance with the policy specified for the drive.
Compliance Status Details	Lists the error and status messages of the compliance state of the computer in accordance to the policy specified

Hardware Audit Report Use this report to audit changes to the Hardware Compatibility status of specific computer makes and models. You can use different filters to narrow your search results, for example, the user who made the change and what kind of change occurred. Each state change is tracked by user and date & time. The Hardware Type is automatically populated by the MBAM agent running on the client computer, this report tracks user changes to the information collected directly from the MBAM managed computer. The typical type of administrative change is changing from Compatible to incompatible; however the administrator can also update any field.

Hardware Audit Report fields

Column Name	Description
Date and Time	Indicates the date and time that a change was

Column Name	Description
	made to the Hardware Type. There is at least one entry for every unique hardware type that was reported by MBAM.
User	Indicates the Administrative user that has made the change for the particular entry.
Change Type	Indicates the type of change that was made by the administrative user to the hardware type information. Valid values are Addition (new entry), Update (of an existing entry), or Deletion (of an existing entry).
Original Value	Indicates the value of the hardware type specification before a change was made.
Current Value	Indicates the value of the hardware type specification after a change was made.

Recovery Audit Report Use this report type to audit users who have requested access to recovery keys. The report offers several filters based on the desired filtering criteria. The user can filter on a specific type of user, either a helpdesk user or an end-user, whether the request failed or was successful, the specific type of key requested, and a date range that the retrieval occurred. This will let the administrator produce contextual reports based on need.

Recovery Audit Report fields

Column Name	Description
Request Date and Time	Indicates the date and time that a key retrieval request was made by an end user or help desk user.
Request Status	Indicates that the request was either Successful (the key was retrieved), or Failed (the key was not retrieved).
Helpdesk User	Indicates the Help Desk user that has initiated the request for key retrieval. Note if the helpdesk user retrieves the key on behalf on an end-user, the End User field will be blank.
User	Indicates the end-user that has initiated the request for key retrieval.
Key Type	Indicates the type of key that was requested by either the help desk user or the end user. The

Column Name	Description
	three types of keys MBAM collects are; Recovery Key Password (used to recovery a computer in recovery mode)' Recovery Key ID (used to recover a computer in recovery mode on behalf of another user), and TPM Password Hash (used to recover a computer with a locked TPM).
Reason Description	Indicates the reason why the specified Key Type was requested by the Helpdesk user or the end user. The reasons are specified in the Drive Recovery and Manage TPM features of the Administrative web site. The valid entries are; 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 • Turn on TPM • Turn off TPM • Change TPM password • Clear TPM

Note
Report results can be saved to a file by clicking the **Export** button on the reports menu bar. For more information about how to run MBAM reports, see How to Manage Hardware Compatibility.

See Also

Operations for MBAM

How to Determine BitLocker Encryption State of Lost Computers

Microsoft BitLocker Administration and Monitoring (MBAM) includes the ability to track the last known encryption status of computers that were lost or stolen. The following procedure explains how to determine whether the volumes on a computer are encrypted if there is a loss or theft.

To determine the BitLocker Encryption State of lost computers

1. Open a web browser and navigate to the BitLocker Administration and Monitoring management console.

   Note
   Note: The default address for the BitLocker Administration and Monitoring management console is http://<*computername*>. Using the fully qualified server name will yield faster browsing results.
2. Selects the **Report** node from the navigation pane and 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, thus verification of deployed policies is recommended when you are trying to determine the BitLocker encryption state of a device.

See Also

Operations for MBAM

How to Recover an Encrypted Drive

The Encrypted Drive Recovery features of Microsoft BitLocker Administration and Monitoring (MBAM) ensure the capture and storage of data and availability of tools required to access a BitLocker-protected volume when BitLocker goes into recovery mode, is moved, or becomes corrupted. Use the following procedures to recover a BitLocker-protected drive.

To Recover a Locked Drive

The Encrypted Drive Recovery features of Microsoft BitLocker Administration and Monitoring ensure the capture and storage of data and availability of tools required to access a BitLocker-protected volume when BitLocker goes 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 changes to the BIOS or startup files of a computer.

Use this procedure to access the centralized key recovery data system that can provide a recovery password, as long as a recovery password ID and associated user identifier are supplied.

1. Open a web browser and navigate to the Microsoft BitLocker Administration and Monitoring website.
2. In the navigation pane, click **Drive Recovery**. This opens the “Recover access to an encrypted drive” webpage.
3. Enter the Window Logon domain and user name of the user to view recovery information and the first eight digits of the recovery key ID to receive a list of possible matching recovery keys or 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. Microsoft BitLocker Administration and Monitoring 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 critical information necessary to attempt to recover the drive.
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 message. 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.

To Recover a Moved Drive

When you move an operating system drive that is encrypted by usingMicrosoft BitLocker Administration and Monitoring, the drive will not accept the PIN used in previous computer because of the change to the Trusted Platform Module (TPM) chip. You will need a way to obtain the recovery key ID to retrieve the recovery password in order to use the moved drive. Use the following procedure to recover a drive that has moved.

1. Start the computer that contains the moved drive in Windows recovery environment (WinRE) mode, or start the computer by using Microsoft Diagnostic and Recovery Tool 6.5 (MS DaRT).
2. As soon as the computer has been started with WinRE or MS 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 may click **I forget the PIN** during the startup process and enter the recovery mode. This also displays the recovery key ID.
3. Use the recovery key ID to retrieve the recovery password and unlock the drive from the MBAM console website.
4. If the moved drive was configured to use a TPM chip on the original computer, you must take additional steps after unlocking the drive and completing the start process. In WinRE mode, open a command prompt and use the 'manage-bde' tool to decrypt the drive, this is the only way to remove the TPM plus PIN protector without the original TPM chip.
5. As soon as this is completed, start the system normally. The MBAM agent will now enforce the policy to encrypt the drive with the new computer's TPM plus PIN.

To Recover a Corrupted Drive

To recover a corrupted drive protected by BitLocker, a Microsoft BitLocker Administration and Monitoring help desk user will need to create a recovery key package file. This package file can then be copied to the computer that contains the corrupted drive, and then used to recover the drive. Use the following procedure for the steps needed to do this.

1. To create the recovery key package necessary to recover a corrupted drive, start a web browser and open the MBAM console webpage.

2. Select **Drive Recovery** from the left-side navigation pane. Enter the user's domain name, user name, 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**. Rightclick 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
   Replace <fixed drive> with an available hard disk drive 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 hard disk drive.

See Also

Operations for MBAM

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 needed to manage the Trusted Platform Module (TPM). This topic covers how to access the centralized Key Recovery data system in the MBAM Management Console, which can provide a TPM owner password file when a computer ID and associated user identifier are supplied.

A TPM lockout can occur if a user enters the 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.

To reset a TPM lockout

1. Open a web browser and navigate to the MBAM Management website.
2. In the left-side navigation pane, select **Manage TPM**. This will display the **Manage TPM** page.
3. Enter the fully qualified domain name for the computer and the computer name and enter the user's Windows logon domain and user name of the user to retrieve the TPM owner password file. Select one of the predefined options in the **Reason for requesting TPM owner password file** drop-down menu. Click **Submit**.
4. Microsoft BitLocker Administration and Monitoring 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. After the TPM owner password is retrieved, the owner password will be displayed. The password can be saved to a .tpm file by clicking 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.

See Also

Operations for MBAM

How to Manage Hardware Compatibility

Microsoft BitLocker Administration and Monitoring (MBAM) can collect information on both make and model of client computers if you deploy the “Allow Hardware Compatibility Checking” Group Policy. If this policy is configured, then as soon as the MBAM client is deployed on a client computer, the MBAM agent will report the make and model information for the computer to the MBAM server.

Note

The MBAM Hardware Compatibility feature is not enabled by default. It can be enabled by selecting the Hardware Compatibility sub feature under the Administration and Monitoring Server feature during setup. For more information about how to set up and configure Hardware Compatibility, see Planning Hardware Management for MBAM.

How 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-side pane, click **Advanced Search** and filter to display a list of all computer models that have a **Capability** status of **Unknown**. This returns a list of computer models matching the search criteria. 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.
5. Administrators should monitor regularly the hardware compatibility list to review new models discovered by the Microsoft BitLocker Administration and Monitoring agent, and then update their compatibility setting to **Compatible** or **Incompatible** as appropriate.

See Also

Operations for MBAM

How to Manage User and Computer Exemptions

Microsoft BitLocker Administration and Monitoring (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. Your organization can also manage BitLocker protection by exempting users, if there are users who do not need or want their drives encrypted.

To exempt users from BitLocker protection, an organization will have to create an infrastructure to support exempted users, such as giving the user a contact telephone number, webpage, or mailing address to request exemption. Also, an 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. However, 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 computer	BitLocker protection is not enforced on computer
User exempt	BitLocker protection is not enforced on computer	BitLocker protection is not enforced on computer

Managing User Exemptions

To exempt a user from BitLocker encryption

1. In some cases, an organization may decide to control BitLocker exemption on a user-by-user basis. In this case, the user to be exempted must be added to a security group in Active Directory in order to bypass any computer-based BitLocker protection rules.
2. Create a Group Policy object by using the MBAM Planning and Configuring Group Policy for MBAM and associate it with the Active Directory group that you created in the previous step.
3. As soon as a security group for BitLocker-exempted users is created, add to this group the names of the users who are requesting exemption. As soon as the users log 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 when using 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. If you have deployed the User Exemption Policy template, a user can request exemption from BitLocker protection through the MBAM client.
2. As soon as the user logs on to a computer that was marked as **Compatible** in the MBAM Hardware Compatibility list, they receive a notification that their computer is going to be encrypted. They 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. If the user selects **Request Exemption**, they will receive a notification telling them to contact your organizations BitLocker administration group. Depending on how the “Configure User Exemption Policy” is configured, the user will be provided with one or more of the following contact methods:
   - Phone Number
   - Webpage URL
   - Mailing Address

   As soon as the exemption request is received, the MBAM Administrator can take decide if it is appropriate to add the user to the BitLocker Exemption Active Directory group.

   Note
   As soon as the postpone time limit set in the User Exemption Policy has expired, the user will not see options to request exemption to the encryption policy. At this point, the user must contact the MBAM administrator directly to receive exemption from BitLocker Protection.

See Also

Operations for MBAM

How to Manage MBAM Administrator Roles

After Microsoft BitLocker Administration and Monitoring (MBAM) setup is complete for all server components, administrative users will have to be granted access to one or more features. As a best practice, administrators who will manage or use MBAM features should be assigned to Active Directory groups.

How to Modify MBAM Administrator Role Memberships

1. Assign administrative users to groups in Active Directory Domain Services.
2. Add security groups to the roles for MBAM on the Microsoft BitLocker Administration and Monitoring server for the respective features.
   - **MBAM System Administrators** have access to all Microsoft BitLocker Administration and Monitoring features in the MBAM Management Console
   - **MBAM Hardware Users** have access to the Hardware Compatibility features in the MBAM Management Console
   - **MBAM Helpdesk Users** have access to the Manage TPM and Drive Recovery options in the MBAM Management Console, 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 Management Console
   - **MBAM Advanced Helpdesk Uses** have access to the Manage TPM and Drive Recovery options in the MBAM Management Console but 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 the Server Infrastructure for MBAM.

See Also

Operations for MBAM

How to Use the Client Control Panel

Microsoft BitLocker Administration and Monitoring (MBAM) has a customized MBAM control panel under **System and Security** called BitLocker Encryption Options that replaces the default Windows BitLocker control panel. The MBAM control panel can be used to unlock encrypted fixed and removable drives, and also manage your PIN or password.

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**. As soon as **Control Panel** opens, select **System and Security**. You can also right-click a drive in Windows Explorer and select **BitLocker Encryption Options** to open Control Panel
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, in addition to an option to manage your PIN or passwords.
3. The list of hard disk drives on the computer can be used to verify encryption status, unlock a drive, or request an exemption for BitLocker protection if the User and Computer Exemption policies have been deployed.
4. The BitLocker Encryption Options control panel also allows for non-administrator users to manage their PIN or passwords. By selecting **Manage PIN**, the user is prompted to enter both a current PIN and a new PIN (in addition to confirming the new PIN). Selecting **Update PIN** will reset the PIN to the new one selected by the user.
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.

See Also

Operations for MBAM

How to Move MBAM Features to Another Server

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 moving more than one Microsoft BitLocker Administration and Monitoring feature you should move them in the following order:

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

Moving the Recovery and Hardware Database Feature

If you choose to move the MBAM Recovery and Hardware Database Feature from one computer to another (that is, move feature from Server A to Server B) you should use the following procedure. The process includes the following steps:

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

Stop 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 Stop the MBAM web site which is named “Microsoft BitLocker Administration and Monitoring”.
2. To automate this procedure execute a command line similar to the following using Windows PowerShell:

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

Note

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

Run MBAM setup on Server B

1. Run MBAM setup on Server B and just select the Recovery and Hardware Database feature for installation.
2. To automate this procedure execute a command line similar to the following 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$ - Input the server name and instance where the Recovery and Hardware Database will be moved to.
- $DOMAIN$\$SERVERNAME$ - Input the domain and server names of each MBAM Application and Monitoring Server that will contact the Recovery and Hardware Database. If there are multiple use a semi-colon to separate them each one in the list (e.g.: $DOMAIN\SERVERNAME$;$DOMAIN\$SERVERNAME$$). Each server name must be followed by a “$” as shown in the example. (e.g.: MyDomain\MyServerName1$; MyDomain\MyServerName2$)

Backup the Database on Server A

1. To backup the Recovery and Hardware Database on Server A use SQL Server Management Studio and the Task named Back Up…. By default the database name will be “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 model.

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

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

3. Next execute the SQL File using a command line similar to the following using the SQL Server PowerShell:

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

Note

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

- $SERVERNAME$\$SQLINSTANCENAME$ - Input the server name and instance where the Recovery and Hardware Database will be backed up from.

Move the Database and Certificate from Server A to B

1. Move the following file from Server A to Server B using Windows Explorer
   - MBAM Recovery and Hardware Database Data.bak
2. To move the Certificate for the encrypted database you will need to use the automation steps listed below. To automate this procedure execute command lines similar to the following using Windows PowerShell:

```
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 following value in the example above with those that match your environment:

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

Restore the Database on Server B

1. Restore the Recovery and Hardware Database on Server B by using SQL Server Management Studio and the Task named Restore Database
2. Once the task has been executed, select the database backup file by selecting the From Device option and then use the Add command to select 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 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 log files.

```
RESTORE DATABASE [MBAM Recovery and Hardware]
```

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

Note

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

- $PASSWORD$ - Input a password that you was used to encrypt the Private Key file.

5. Next, execute the SQL File using a command line similar to the following using the SQL Server PowerShell:

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

Note

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

- $SERVERNAME$\$SQLINSTANCENAME$ - Input the server name and instance where the Recovery and Hardware Database will be restored to.

Configure 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 running the MBAM Administration and Monitoring feature to the Local Group named “MBAM Recovery and Hardware DB Access”.
2. To automate this procedure, execute a command line similar to the following using Windows PowerShell on Server B.

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

Note

Replace the following values in the example above with the applicable values for your environment:

- $DOMAIN$\$SERVERNAME$$ - Input the domain and machine name of the MBAM Administration and Monitoring Server. The server name must be followed by a “$” as shown in the example. (e.g.: MyDomain\MyServerName1$)

This command-line must be run for each Administration and Monitoring Server that will be accessing the database within your environment.

Update database connection data on MBAM Administration and Monitoring servers

1. On each of the servers running 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 within the Microsoft BitLocker Administration and Monitoring website:

- MBAMAdministrationService
- MBAMRecoveryAndHardwareService

2. Select each Application and use the **Configuration Editor** feature which can be found under the **Management** section of the **Feature View**.
3. From here, select the **configurationStrings** option from the Section list control.
4. Next select the row named **(Collection)** and open the **Collection Editor** by selecting the button on the right hand side of the row.
5. Within the **Collection Editor**, select the row named **KeyRecoveryConnectionString** when updating the configuration for the 'MBAMAdministrationService' application or the row named **Microsoft.Mbam.RecoveryAndHardwareDataStore.**ConnectionString when updating the configuration for the 'MBAMRecoveryAndHardwareService'.
6. Update the **Data Source=** value for the **configurationStrings** property such to list the server name and instance (for example, $SERVERNAME$\$SQLINSTANCENAME$) where the Recovery and Hardware Database was moved to.
7. To automate the procedure above, execute a command line similar to the following 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 following value in the example above with those that match your environment:

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

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 which is named "Microsoft BitLocker Administration and Monitoring".
2. To automate this procedure execute a command line similar to the following using Windows PowerShell:

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

Moving the Compliance Status Database Feature

If you choose to move the MBAM Compliance Status Database Feature from one computer to another (i.e.: move feature from Server A to Server B) you should use the following procedure. The process includes the following steps:

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

Stop 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 Stop the MBAM web site named "Microsoft BitLocker Administration and Monitoring".
2. To automate this procedure, execute a command line similar to the following using Windows PowerShell:

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

Note

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

Run MBAM setup on Server B

1. Run MBAM setup on Server B and just select the Compliance Status Database feature for installation.
2. To automate this procedure, execute a command line similar to the following 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

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

- $SERVERNAME$\$SQLINSTANCENAME$ - Input the server name and instance

where the Compliance Status Database will be moved to.

- $DOMAIN$\$SERVERNAME$ - Input the domain and server names of each MBAM Application and Monitoring Server that will contact the Compliance Status Database. If there are multiple, use a semi-colon to separate them each one in the list (such as, $DOMAIN\SERVERNAME$;$DOMAIN\$SERVERNAME$$). Each server name must be followed by a "$" as shown in the example. (such as, MyDomain\MyServerName1$; MyDomain\MyServerName2$)
- $DOMAIN$\$USERNAME$ - Input the domain and user name that will be used by the Compliance and Audit reports feature to connect to the Compliance Status Database.

Backup the 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 will be "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. Next execute the SQL File using a command line similar to the following using the SQL Server PowerShell:

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

Note

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

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

Move the Database from Server A to B

1. Move the following files from Server A to Server B using Windows Explorer
   - MBAM Compliance Status Database Data.bak
2. To automate this procedure, execute command lines similar to the following using Windows PowerShell:

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

Note

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

- $SERVERNAME$ - Input the server name where the files will be copied to.
- $DESTINATIONSHARE$ - Input the name of share and path where the files will be copied 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 has been executed, select the database backup file by selecting the From Device option and then use the Add command to select the MBAM Compliance Status Database Data.bak file. Select 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. Next, execute the SQL File using a command line similar to the following using the SQL Server PowerShell:

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

Note

Replace the following value in the example above with those that match your

environment:

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

Configure 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 running the MBAM Administration and Monitoring feature to the Local Group named “MBAM Compliance Status DB Access”.
2. To automate this procedure, execute command lines similar to the following 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 following value in the example above with the applicable values for your environment:

- $DOMAIN$\$SERVERNAME$$ - Input the domain and machine name of the MBAM Administration and Monitoring Server. The server name must be followed by a “$” as shown in the example. (e.g.: MyDomain\MyServerName1$)
- $DOMAIN$\$REPORTSUSERNAME$ - Input the user account name that was used to configure the data source for the Compliance and Audit reports

The command-line for adding the servers to the MBAM Compliance Auditing DB Access local group must be run for each Administration and Monitoring Server that will be accessing the database within your environment.

Update database connection data on MBAM Administration and Monitoring servers

1. On each of the servers running 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 within the Microsoft BitLocker Administration and Monitoring website:
   - MBAMAdministrationService
   - MBAMComplianceStatusService
2. Select each Application and use the **Configuration Editor** feature which can be found under the **Management** section of the **Feature View**.
3. Select the **configurationStrings** option from the Section list control.
4. Next select the row named **(Collection)** and open the Collection Editor by selecting the button on the right-hand side of the row.
5. Within the Collection Editor select the row named **ComplianceStatusConnectionString** when updating the configuration for the MBAMAdministrationService application or the row named

Microsoft.Windows.Mdop.BitLockerManagement.StatusReportDataStore.ConnectionString when updating the configuration for the MBAMComplianceStatusService.

6. Update the **Data Source=** value for the **configurationStrings** property to list the server name and instance (such as, $SERVERNAME$\$SQLINSTANCENAME) where the Recovery and Hardware Database was moved to.
7. To automate this procedure, execute a command line similar to the following using Windows PowerShell 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$;Initial Catalog=MBAM Compliance
Status;Integrated Security=SSPI;"
PS C:\> Set-WebConfigurationProperty
'/connectionStrings/add[@name="Microsoft.Windows.Mdop.BitLockerManagement.StatusRe
portDataStore.ConnectionString"]' -PSPath "IIS:\sites\Microsoft Bitlocker
Administration and Monitoring\MBAMComplianceStatusService" -Name
"connectionString" -Value "Data Source=$SERVERNAME$\$SQLINSTANCENAME;Initial
Catalog=MBAM Compliance Status;Integrated Security=SSPI;"
```

Note

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

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

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 execute a command line similar to the following using Windows PowerShell:

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

Moving the Compliance and Audit Reports Feature

If you choose to move the MBAM Compliance and Audit Reports feature from one computer to another (i.e.: 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 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

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, execute a command line similar to the following 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 following values in the example above with those that match your environment:

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

Configure 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, execute a command line similar to the following using Windows PowerShell on Server B.

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

Note

Replace the following value in the example above with the applicable values for your environment:

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

The command-line for adding the users to the MBAM Report Users local group must be run for each user that will be accessing the reports within your environment.

Stop 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 Stop the MBAM web site named

“Microsoft BitLocker Administration and Monitoring”.

2. To automate this procedure, execute a command line similar to the following using Windows PowerShell:

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

Update database connection data on MBAM Administration and Monitoring servers

1. On each of the servers running 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. Next, 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 hand side of the row.
5. Within 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 to add or update the name of the instance to the URL (e.g.: http://$SERVERNAME$/ReportServer_$SQLSRSINSTANCENAME$/Pages....)
7. To automate this procedure, execute a command line similar to the following using Windows PowerShell 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 following value in the example above with those that match your environment:

- $SERVERNAME$ - Input the server name where the Compliance and Audit Reports were installed to.
- $SRSINSTANCENAME$ - Input the name of the SQL Reporting Services instance where the Compliance and Audit Reports were installed 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, execute a command line similar to the following using

Windows PowerShell:

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

Note

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

Moving the Administration and Monitoring Feature

If you choose to move the MBAM Administration and Monitoring Reports Feature from one computer to another (i.e.: 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

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, execute a command line similar to the following 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 following values in the example above 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$ - Input the domain and user name that will be used by the Compliance and Audit reports feature to connect to the Compliance Status Database.
- $ REPORTSSERVERURL$ - Input 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 formatted “http://$SERVERNAME$/ReportServer_$SQLINSTANCENAME$”.

Configure 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 running 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, execute a command line similar to the following 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 execute a command line similar to the following using Windows PowerShell.

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

Note

Replace the following value in the example above with the applicable values for your environment:

- $DOMAIN$\$SERVERNAME$$ - Input the domain and machine name of the MBAM Administration and Monitoring Server. The server name must be followed by a “$” as shown in the example. (e.g.: MyDomain\MyServerName1$)
- $DOMAIN$\$REPORTSUSERNAME$ - Input the user account name that was used to configure the data source for the Compliance and Audit reports

The command-lines listed for adding servers machine accounts to the MBAM local groups must be run for each Administration and Monitoring Server that will be accessing the databases within your environment.

See Also

Operations for MBAM

Troubleshooting MBAM

Troubleshooting content is not included in the help content for Microsoft BitLocker Administration and Monitoring (MBAM). Instead, troubleshooting information for Microsoft BitLocker Administration and Monitoring can be found on the TechNet Wiki (http://go.microsoft.com/fwlink/?LinkId=224905).

How to Find Troubleshooting Information

Use the guidance that follows to find troubleshooting and additional information for Microsoft BitLocker Administration and Monitoring.

Search the MDOP Documentation

To find help for Microsoft BitLocker Administration and Monitoring, first perform a scoped search in the Microsoft Desktop Optimization Pack (MDOP) Online Help product documentation. If your issue is not addressed in the Online Help documentation, search for Microsoft BitLocker Administration and Monitoring troubleshooting information in the TechNet Wiki. The TechNet Wiki portal offers guidance contributed by Microsoft teams and community-generated troubleshooting information.

To search the MDOP OnlineHelp documentation

1. In a web browser, locate the MDOP OnlineHelp home page (http://go.microsoft.com/fwlink/?LinkId=224906).
2. In the **Search MDOP Help** search box on the MDOP Online Help home page, enter the search terms or briefly describe your issue.
3. Review the search results for your issue.

To search the TechNet Wiki

1. In a web browser, locate the TechNet Wiki home page (http://go.microsoft.com/fwlink/?LinkId=224905).
2. In the **Search TechNet Wiki** search box located on the TechNet Wiki home page, enter the search terms or briefly describe your issue. Be sure to include the word “MBAM” to help scope your search.
3. Review the search results for your issue.

How to Create a Troubleshooting Article

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

To create a TechNet Wiki troubleshooting or best practices article

1. In a web browser, locate the TechNet Wiki home page (http://go.microsoft.com/fwlink/?LinkId=224905).
2. Log on with your Windows Live ID.
3. Review the Wiki: Getting Started (http://go.microsoft.com/fwlink/?LinkId=224937) information to learn about the TechNet Wiki and its articles.
4. Select **Post an article >>** at the end of the **Getting Started** section.
5. On the Wiki article **Add Page** page on the tool bar, click **Insert Template**, select the troubleshooting article template (**Troubleshooting.html**), and then click **Insert**.
6. Give the article a descriptive title and then overwrite the template information to create your troubleshooting article.
7. After reviewing your article, create the following tags to help others find your article:
   a. **Troubleshooting**
   b. **MBAM**
8. Click **Save** to publish the article to the TechNet Wiki.

See Also

BitLocker Administration and Monitoring Home

Getting Started With MBAM

Planning for MBAM

Deploying MBAM

Operations for MBAM