Contents

[Microsoft BitLocker Administration and Monitoring Planning, Deployment, and Operations Guide 5](#_Toc295118827)

[In This Section 5](#_Toc295118828)

[Related Sections 5](#_Toc295118829)

[Getting Started With MBAM 5](#_Toc295118830)

[In This Guide: 6](#_Toc295118831)

[See Also 6](#_Toc295118832)

[High-Level Architecture for MBAM 7](#_Toc295118833)

[Architecture Overview 7](#_Toc295118834)

[About Microsoft BitLocker Administration and Monitoring 8](#_Toc295118835)

[MBAM Supported Configurations 8](#_Toc295118836)

[Server Operating System Requirements 8](#_Toc295118837)

[Prerequisites for BitLocker Administration and Monitoring Server Components 9](#_Toc295118838)

[Prerequisites for Administration and Monitoring Server 9](#_Toc295118839)

[Prerequisites for the Compliance and Audit Reports Server 10](#_Toc295118840)

[Prerequisites for the Recovery and Hardware Database Server 10](#_Toc295118841)

[Prerequisites for the Compliance Status Database Server 10](#_Toc295118842)

[MBAM Client Operating System Requirements 10](#_Toc295118843)

[Release Notes for MBAM 11](#_Toc295118844)

[Section Heading 11](#_Toc295118845)

[Subsection Heading 11](#_Toc295118846)

[Privacy Statement 11](#_Toc295118847)

[Privacy Statement 11](#_Toc295118848)

[Planning for MBAM 13](#_Toc295118849)

[In This Section 13](#_Toc295118850)

[MBAM Supported Configurations 14](#_Toc295118851)

[Server Operating System Requirements 14](#_Toc295118852)

[Prerequisites for BitLocker Administration and Monitoring Server Components 14](#_Toc295118853)

[Prerequisites for Administration and Monitoring Server 14](#_Toc295118854)

[Prerequisites for the Compliance and Audit Reports Server 15](#_Toc295118855)

[Prerequisites for the Recovery and Hardware Database Server 15](#_Toc295118856)

[Prerequisites for the Compliance Status Database Server 16](#_Toc295118857)

[MBAM Client Operating System Requirements 16](#_Toc295118858)

[Planning and Configuring Group Policy for MBAM 16](#_Toc295118859)

[Group Policy Requirements 17](#_Toc295118860)

[Global Policy Definitions 18](#_Toc295118861)

[Data Recovery Policy Definitions 19](#_Toc295118862)

[Operating System Drive Policy Definitions 20](#_Toc295118863)

[Fixed Data Drive Policy Definitions 21](#_Toc295118864)

[Removable Data Drive Policy Definitions 23](#_Toc295118865)

[Report Policy Definitions 25](#_Toc295118866)

[Client Management Policy Definition 26](#_Toc295118867)

[User-Based Group Policy Definitions 28](#_Toc295118868)

[Windows Policies 29](#_Toc295118869)

[Planning Server Infrastructure for MBAM 29](#_Toc295118870)

[Planning the Server Deployment 30](#_Toc295118871)

[Planning for Administrator Roles 31](#_Toc295118872)

[Planning Client Deployment for MBAM 32](#_Toc295118873)

[Client System Requirements 32](#_Toc295118874)

[Computer Encryption before Distribution to the User 32](#_Toc295118875)

[Computer Encryption after Distribution to the User 33](#_Toc295118876)

[Planning Hardware Management for MBAM 33](#_Toc295118877)

[Deploying MBAM 34](#_Toc295118878)

[Deploying MBAM 34](#_Toc295118879)

[Deploying MBAM Group Policies 35](#_Toc295118880)

[Deploying MBAM Group Policy 35](#_Toc295118881)

[Deploying the Updated BitLocker Encryption Options Control Panel 36](#_Toc295118882)

[See Also 37](#_Toc295118883)

[Deploying MBAM on a Single Server 37](#_Toc295118884)

[Deploying the MBAM Server 37](#_Toc295118885)

[Validating the MBAM Server Feature Installations 39](#_Toc295118886)

[Deploying MBAM on Distributed Servers 41](#_Toc295118887)

[Deploying the MBAM Server 41](#_Toc295118888)

[Validating the MBAM Server Feature Installations 45](#_Toc295118889)

[Deploying the MBAM Client 46](#_Toc295118890)

[How to Encrypt a Computer as part of Windows Deployment 47](#_Toc295118891)

[Operations for MBAM 49](#_Toc295118892)

[In This Section 49](#_Toc295118893)

[How to Generate MBAM Reports 50](#_Toc295118894)

[Understanding MBAM Reports 52](#_Toc295118895)

[Reports 53](#_Toc295118896)

[How to Determine BitLocker Encryption State of Lost Computers 60](#_Toc295118897)

[How to Recover an Encrypted Drive 61](#_Toc295118898)

[How to Recover a Corrupted Drive 62](#_Toc295118899)

[How to Recover a Moved Drive 62](#_Toc295118900)

[Recovering a Moved Drive 63](#_Toc295118901)

[How to Utilize Single Use Recovery Keys 63](#_Toc295118902)

[How to Reset a TPM Lockout 64](#_Toc295118903)

[How to Manage Hardware Compatibility 65](#_Toc295118904)

[How to Manage User and Computer Exemptions 65](#_Toc295118905)

[Managing Hardware and User Exemptions 66](#_Toc295118906)

[How to Manage Roles for MBAM 68](#_Toc295118907)

[How to Use the Client Control Panel 68](#_Toc295118908)

[See Also 69](#_Toc295118909)

[Best Practices for MBAM 69](#_Toc295118910)

[In This Section 69](#_Toc295118911)

[See Also 70](#_Toc295118912)

[Technical Reference for MBAM 70](#_Toc295118913)

[In This Section 70](#_Toc295118914)

[See Also 70](#_Toc295118915)

[MBAM Installation Checklists 70](#_Toc295118916)

[BitLocker Administration and Monitoring Installation Checklist 71](#_Toc295118917)

[List of Log Files for MBAM 74](#_Toc295118918)

[Setup 74](#_Toc295118919)

[Application and Monitoring 74](#_Toc295118920)

[Client 74](#_Toc295118921)

[Moving MBAM Features to Another Server 74](#_Toc295118922)

[Moving the Recovery and Hardware Database Feature 75](#_Toc295118923)

[Moving the Compliance Status Database Feature 80](#_Toc295118924)

[Moving the Compliance and Audit Reports Feature 84](#_Toc295118925)

[Moving the Administration and Monitoring Feature 87](#_Toc295118926)

[MBAM Keyboard Shortcuts 88](#_Toc295118927)

[Finding and Using Keyboard Shortcuts 88](#_Toc295118928)

[Search This Article 89](#_Toc295118929)

[Print This Article 89](#_Toc295118930)

[Keyboard Shortcuts for MBAM Setup 89](#_Toc295118931)

[Keyboard Shortcuts for MBAM Console 90](#_Toc295118932)

# Microsoft BitLocker Administration and Monitoring Planning, Deployment, and Operations Guide



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 already understand Bitlocker and group policies in general, 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.

## In This Section

This guide provides information on the following topics:

Getting Started with MBAM

About MBAM

[Planning for MBAM](#z3c957c203f224ee3802ff422b490b940)

Deploying MBAM

[Operations for MBAM](#zb4cb64f22b6e4aaa80dcff32989f204c)

[Technical Reference for MBAM](#z49e9c2c7846a4c7da61405c104b2e091)

## Related Sections

For detailed information about Bitlocker, please see: [BitLocker Drive Encryption](http://technet.microsoft.com/en-us/library/cc731549(WS.10).aspx).

# 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.

## In This Guide:

[Planning for MBAM](#z3c957c203f224ee3802ff422b490b940)

|  |
| --- |
| Provides information about required planning of the BitLocker group policy, MBAM server infrastructure, and client management for MBAM deployment. |

[Deploying MBAM](#zd9fa7c5fac1e419b968abbaf5a5c828d)

|  |
| --- |
| Provides information about deploying MBAM group policy, installing the MBAM server features, and how to deploy the MBAM client. |

[Operations for MBAM](#zb4cb64f22b6e4aaa80dcff32989f204c)

|  |
| --- |
| Provides information about how to work with MBAM reports, manage client encryption states and TPM states, manage MBAM roles, and how to recover locked computers. You can also manage hardware compatibility, exemption and use the Control Panel program to specify options for MBAM. |

Troubleshooting MBAM

|  |
| --- |
| Provides information about how to resolve issues with MBAM and BitLocker drive encryption. |

[Best Practices for MBAM](#z2bf54b730e1446d2aca74173ae7f5f6f)

|  |
| --- |
| Provides information about best practices for MBAM. |

[Technical Reference for MBAM](#z49e9c2c7846a4c7da61405c104b2e091)

|  |
| --- |
| Provides information about MBAM including lists of log files, keyboard short cuts, and instructions how to move MBAM server features to a different server. |

## See Also

[Planning for MBAM](#z3c957c203f224ee3802ff422b490b940)

[Deploying MBAM](#zd9fa7c5fac1e419b968abbaf5a5c828d)

[Operations for MBAM](#zb4cb64f22b6e4aaa80dcff32989f204c)

Troubleshooting MBAM

[Best Practices for MBAM](#z2bf54b730e1446d2aca74173ae7f5f6f)

[Technical Reference for MBAM](#z49e9c2c7846a4c7da61405c104b2e091)

# High-Level Architecture for MBAM

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

 Administration and monitoring server

 Compliance and status database

 Recovery and hardware database

 Compliance and audit reports

 Policy template

 Microsoft BitLocker Administration and Monitoring client agent

## 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 for use by the reporting service.

Recovery and Hardware Database ˚˚Stores recovery data that is collected from Microsoft BitLocker Administration and Monitoring client computers

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

Policy Template ˚˚The Group Policy template that specifies the Microsoft BitLocker Administration and Monitoring implementation of BitLocker drive encryption.

TheMicrosoft BitLocker Administration and Monitoring client agent performs the following tasks:

 Uses Group Policy to enforce the BitLocker encryption of client computers in the enterprise

 Gathers the recovery key for the three BitLocker data drive types, operating system drives, fixed data drives, and removable data drives (that is, USB drives)

 Gathers compliance data for computer and passes the data to the reporting system

# About Microsoft BitLocker Administration and Monitoring

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

This Microsoft BitLocker Administration and Monitoring help guide provides background information about MBAM and describes how to install and use the product. An overview of MBAM architecture is provided in the “MBAM Architecture Notes.” The intended audience for the guide is MBAM administrators and technical personnel.

For an overview of BitLocker, reference the BitLocker Drive Encryption article (http://technet.microsoft.com/en-us/library/cc731549(WS.10).aspx) on TechNet.

# 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 prior service pack. To find the support timelines for your product, see the [Lifecycle Supported Service Packs](http://go.microsoft.com/fwlink/?LinkId=31975) (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) (http://go.microsoft.com/fwlink/?LinkId=31976).

## Server Operating System Requirements

The server roles required for Microsoft BitLocker Administration and Monitoring are supported on the following operating systems:

| **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 |

This section contains configuration information that is specific to the website requirements for this release.

## Prerequisites for BitLocker Administration and Monitoring Server Components

Each of the Microsoft BitLocker Administration and Monitoring feature servers has specific prerequisites that must be met before the MBAM features can be successfully installed. MBAM Setup will check 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 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 Prerequisites include the Reporting Services feature from Microsoft SQL Server R2 Enterprise, Datacenter, Developer edition.

Note



Note that SQL Reporting Service must be running during installation.

### Prerequisites for the Recovery and Hardware Database Server

The Recovery and Hardware Database Prerequisites: includes the following:

 Microsoft SQL Server R2 Enterprise, Datacenter or Developer edition.

 SQL Server must have Database Engine Services and Full-Text Search features installed.

Note



Be aware that prerequisite services must be running during installation.

Note



Enterprise, Datacenter, or Developer editions are required if you choose the “Use certificates to encrypt database and network communication” option when installing the Recovery and Hardware Database feature.

### Prerequisites for the Compliance Status Database Server

The Compliance Status Database Prerequisites include:

 Microsoft SQL Server R2 Standard, Enterprise, Datacenter, Developer edition

 SQL Server must have Database Engine Services and Full-Text Search features installed.

## MBAM Client Operating System Requirements

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. Look in the BIOS documentation for more information.

Warning



Make sure that the keyboard, mouse and video are directly connected and not managed through a keyboard, video, mouse (KVM) switch. A KVM switch may 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.

# Release Notes for MBAM

Section Intentionally Left Blank. Content will be added next week, post TR.

## Section Heading

Insert section body here.

### Subsection Heading

Insert subsection body here.

# Privacy Statement

## Privacy Statement

Microsoft BitLocker Administration and Monitoring (MBAM) Privacy Statement

Applies To: Microsoft BitLocker Administration and Monitoring (MBAM)

Last Updated: June 2011

At Microsoft, we're working hard to protect your privacy, while delivering products that bring you the performance, power and convenience you desire in your personal computing. This privacy statement explains many of the data collection and use practices of Microsoft BitLocker Administration and Monitoring (MBAM). This privacy statement focuses on features that communicate with the Internet and is not intended to be an exhaustive list. It does not apply to other online or offline Microsoft sites, products or services.

Collection and Use of Your Personal Information:

When we need information that personally identifies you or allows us to contact you, we will explicitly ask you for it. The personal information we collect from you will be used by Microsoft and its controlled subsidiaries and affiliates to provide the service(s) or carry out the transaction(s) you have requested or authorized, and may also be used to request additional information on feedback that you provide about the product or service that you are using; to provide critical updates and notifications regarding the software; to improve the product or service, for example bug and survey form inquiries, or to provide you with advance notice of events or to tell you about new product releases.

Except as described in this statement, personal information you provide will not be transferred to third parties without your consent. We occasionally hire other companies to provide limited services on our behalf, such as performing statistical analysis of our services. We will only provide those companies the personal information they need to deliver the service, and they are prohibited from using that information for any other purpose.

Information that is collected by or sent to Microsoft may be stored and processed in the United States or any other country in which Microsoft or its affiliates, subsidiaries or agents maintain facilities, and by using a Microsoft site or service, you consent to any such transfer of information outside of your country. Microsoft abides by the safe harbor framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of data from the European Union. Microsoft may disclose personal information about you if required to do so by law or in the good faith belief that such action is necessary to: (a) conform to the edicts of the law or comply with legal process served on Microsoft or the site; (b) protect and defend the rights or property of Microsoft (including enforcing our agreements), or (c) act in urgent circumstances to protect the personal safety of Microsoft employees, users of Microsoft products or services, or members of the public.

Collection and Use of Information About Your Computer:

Microsoft BitLocker Administration and Monitoring contains Internet-enabled features that can collect certain standard information from your computer ("standard computer information") along with information needed for a specific feature and send it to Microsoft. Standard computer information includes information such as your IP address, operating system version, a code that identifies the manufacturer of your computer, and your regional and language settings. This computer information is generally not personally identifiable.

Security of Your Information:

Microsoft is committed to protecting the security of your personal information. We use a variety of security technologies and procedures to help protect your personal information from unauthorized access, use, or disclosure. For example, we store the information you provide on computer servers with limited access that are located in controlled facilities.

Changes to the Privacy Statement:

We may occasionally update this privacy statement. When we do, we will revise the "last updated" date at the top of the privacy statement. We encourage you to periodically review this privacy statement to be informed of how Microsoft is protecting your information.

For More Information:

Microsoft welcomes your comments regarding this privacy statement. If you have questions about this statement or believe that we have not adhered to it, please contact us at:

Microsoft Privacy

Microsoft Corporation

One Microsoft Way

Redmond, Washington 98052 USA

# Planning for MBAM

Planning for the components of Microsoft BitLocker Administration and Monitoring (MBAM) allows you to encrypt client computers with BitLocker. Without a Group Policy template configured for your enterprise, as described in [Planning and Configuring Group Policy for MBAM](#z48a45d7492674f14b43c6c1f38f8ed39) you cannot successfully deploy and monitor BitLocker encryption. Planning the server infrastructure, client deployment strategies, and hardware management are also necessary for successful deployment. Be sure to keep track of all values you use to install each component and feature. MBAM requires you to use the same values for all components and features.

## In This Section

[MBAM Supported Configurations](#zd1ce21c430964a169b5efb10feadc2af)

|  |
| --- |
| Details the requirements and configurations necessary for MBAM |

[Planning and Configuring Group Policy for MBAM](#z48a45d7492674f14b43c6c1f38f8ed39)

|  |
| --- |
| Provides guidance on planning and configuring MBAM Group Policy |

[Planning Server Infrastructure for MBAM](#z962f2f48e80043f2ab25664a8a6298ee)

|  |
| --- |
| Provides guidance on how to configure your server infrastructure for MBAM |

[Planning Client Deployment for MBAM](#z5bcac939aa15441284661fa363640026)

|  |
| --- |
| Provides guidance on deploying the MBAM client to your organization’s computers |

[Planning Hardware Management for MBAM](#z187322413b1d45dba513c56a31d96015)

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

# 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 prior service pack. To find the support timelines for your product, see the [Lifecycle Supported Service Packs](http://go.microsoft.com/fwlink/?LinkId=31975) (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) (http://go.microsoft.com/fwlink/?LinkId=31976).

## Server Operating System Requirements

The server roles required for Microsoft BitLocker Administration and Monitoring are supported on the following operating systems:

| **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 |

This section contains configuration information that is specific to the website requirements for this release.

## Prerequisites for BitLocker Administration and Monitoring Server Components

Each of the Microsoft BitLocker Administration and Monitoring feature servers has specific prerequisites that must be met before the MBAM features can be successfully installed. MBAM Setup will check 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 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 Prerequisites include the Reporting Services feature from Microsoft SQL Server R2 Enterprise, Datacenter, Developer edition.

Note



Note that SQL Reporting Service must be running during installation.

### Prerequisites for the Recovery and Hardware Database Server

The Recovery and Hardware Database Prerequisites: includes the following:

 Microsoft SQL Server R2 Enterprise, Datacenter or Developer edition.

 SQL Server must have Database Engine Services and Full-Text Search features installed.

Note



Be aware that prerequisite services must be running during installation.

Note



Enterprise, Datacenter, or Developer editions are required if you choose the “Use certificates to encrypt database and network communication” option when installing the Recovery and Hardware Database feature.

### Prerequisites for the Compliance Status Database Server

The Compliance Status Database Prerequisites include:

 Microsoft SQL Server R2 Standard, Enterprise, Datacenter, Developer edition

 SQL Server must have Database Engine Services and Full-Text Search features installed.

## MBAM Client Operating System Requirements

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. Look in the BIOS documentation for more information.

Warning



Make sure that the keyboard, mouse and video are directly connected and not managed through a keyboard, video, mouse (KVM) switch. A KVM switch may 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.

# Planning and Configuring Group Policy for MBAM

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

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. A Group Policy template for MBAM is set on a BitLocker Group Policies computer.

## Group Policy Requirements

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

How to Set up Group Policies for BitLocker Administration and Monitoring



|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Make sure that MBAM services are enabled on the BitLocker Group Policies computer.  2. 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 Computer configuration, select Policies, select Administrative Templates, click Windows Components, and then select MDOP MBAM (BitLocker Management).  3. Select the Setting to edit. The settings for BitLocker Administration and Monitoring include the following:   Client Management   Data Recovery   Fixed Drive   Operating System Drive   Removable Drive   Reports  4. Edit the setting for your policy. Recommended policies for basic MBAM implementation include the following:   | **Policy Group** | **Policy** | **Setting** | | --- | --- | --- | | Data Recovery | Configure key recovery service | Enabled. Set Key recovery service endpoint and Key recovery information to backup | | Reports | Configure status reporting service | Enabled. Set Status reporting service endpoint and Enter frequency status in (minutes). | | Operating System Drive | Enforce operating system drive encryption | 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. | | Client Management | Allow hardware compatibility checking | Disabled. This policy is enabled by default, but is not needed for a basic MBAM implementation. | | Fixed Drive | Control Use of BitLocker on fixed drives | Enabled. Required if MBAM will save fixed drive data to the MBAM Key Recovery server. | |

## 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 | This policy setting is the same as the BitLocker policy.  Configure this policy to improve restart performance without overwriting BitLocker 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 | This policy setting is the same as the BitLocker policy.  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 identifier for your organization | This policy setting is the same as the BitLocker policy.  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. |
| Choose drive encryption method and cipher strength | This policy setting is the same as the BitLocker policy.  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. |



|  |
| --- |
| 1. |

### Data Recovery Policy Definitions

This section describes MBAM Data Recovery Policy Definitions

Important



The Configure key recovery service policy is critical to the functionality of MBAM. If this policy is not enabled, BitLocker will not encrypt drives on client computers.

| **Policy Name** | **Overview and Suggested Policy Setting** |
| --- | --- |
| Configure key recovery service | This policy setting lets you manage the key recovery service to back up BitLocker recovery information. The setting provides an administrative method of recovering data encrypted by BitLocker to prevent data loss because of the lack of key information.  Suggested Configuration: Enabled when Key recovery information to backup is set to Recovery Password and key package.  When this policy setting is enabled, the recovery password and key package will be automatically and silently backed up to configured key recovery server location. |

### 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 allow the use of characters including uppercase and lowercase letters, symbols, numbers, and spaces.  If you enable this policy setting, the user will have to secure the operating system drive using BitLocker.  If you do not configure or if you disable the setting, the user will not have to secure the operating system drive with BitLocker.    Suggested configuration: Enabled  When enabled, this policy setting requires that the user secures the operating system by using BitLocker protection and drive is encrypted.Based on your encryption requirements, you may select the method of protection for the operating system drive. For higher security requirements, use “TPM + PIN”, allow enhanced PINs, and set the minimum PIN length to 8. |
| Choose how BitLocker-protected operating system drives can be recovered | This policy setting is the same as the BitLocker policy.  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, and the recovery options, including the recovery password and recovery key, can be specified by the user. |
| Configure TPM platform validation profile | This policy setting is the same as the BitLocker policy.  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 Data Drive Policy Definitions

This section describes MBAM Fixed Data Drive Policy definitions.

| **Policy Name** | **Overview and Suggested Policy Setting** |
| --- | --- |
| Fixed data drive encryption settings | This policy setting let you manage whether the fixed data drive 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 OS volume must be encrypted  If you enable this policy setting, the user will have to put all fixed data drives under BitLocker protection and the drives will be encrypted.  If you disable this policy setting, then it is not required to put fixed data drive under BitLocker protection.  If you do not configure this policy setting, then it is not required to put fixed data drive under BitLocker protection.  Suggested Configuration: Enabled; and check the Enable auto-unlock fixed data drive option. |
| Deny write access to fixed drives not protected by BitLocker | This policy setting is the same as the BitLocker policy.  This policy setting determines whether BitLocker protection is required for fixed data 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 data drive from earlier versions of Windows | This policy setting is the same as the BitLocker policy.  Enable this policy to allow fixed data drives with the FAT file system to be unlocked and viewed on Windows Server 2008 computers.  Suggested configuration: Not configured  When the policy is not configured, fixed 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 fixed data drives | This policy setting is the same as the BitLocker policy.  Enable this policy to configure password protection on fixed data 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. |
| Choose how BitLocker-protected fixed drives can be recovered | This policy setting is the same as the BitLocker policy.  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, the recovery options, including the recovery password and recovery key, can be specified by the user, and recovery information is not backed up to AD DS |

### Removable Data Drive Policy Definitions

This section describes MBAM Removable Data Drive Policy definitions.

| **Policy Name** | **Overview and Suggested Policy Setting** |
| --- | --- |
| Control use of BitLocker on removable drives | This policy setting is the same as the BitLocker policy.  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 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 |
| Deny write access to removable drives not protected by BitLocker | This policy setting is the same as the BitLocker policy.  Enable this policy to only allow write access to BitLocker protected drives.  Suggested Configuration: Not configured  When this policy is not configured, all removable data drives on the computer will be mounted with read and writes access. |
| Allow access to BitLocker-protected removable data drive from earlier versions of Windows | This policy setting is the same as the BitLocker policy.  Enable this policy to allow for fixed data 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 | This policy setting is the same as the BitLocker policy  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. |
| Choose how BitLocker-protected removable drives can be recovered | This policy setting is the same as the BitLocker policy.  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 not configured, the data recovery agent is allowed, the recovery options can be specified by the user including the recovery password and recovery key, and recovery information is not backed up to AD DS. |
|  |

### Report Policy Definitions

This section describes the MBAM Report Policy definitions.

| **Policy Name** | **Overview and Suggested Policy Setting** |
| --- | --- |
| Configure status reporting service | This policy setting establishes a location for collecting compliance status reports and sets the time between the generating of reports.  If you enable this policy setting, status report and key recovery activity will be automatically and silently send to configured report server location.  If you do not configure or disable this policy setting, the status report and key recovery activity will not be saved.  Suggested Configuration: Enabled  When it is enabled, this policy provides an administrative method of generating a compliance report.  The default is set to every 720 minutes.  Set this frequency based on the requirement set by your company on how frequently to check the compliance status of the computer. |

### Client Management Policy Definition

This section describes MBAM Client Management Policy definitions.

| **Policy Name** | **Overview and Suggested Policy Setting** |
| --- | --- |
| Configure client checking frequency in minutes | 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 recovery key is backed up to the server.  If you enable this policy setting, the client will check the BitLocker protection policies and status on the client computer, as well as back up the client recovery key, at the configured frequency.  If you do not configure or disable this policy setting, the client checks the BitLocker protection policies and status on the client computer and backs up the client recovery key every 90 minutes.  Suggested Configuration: Enabled  The default is set to every 90 minutes.  Set this frequency based on the requirement set by your company on how frequently to check the compliance status of the computer and back up the client recovery key. |  |
| Allow hardware compatibility checking | This policy setting allows you to manage the checking of hardware compatibility before enabling BitLocker 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 must enable the “Configure Key Recovery service” policy and have it configured.  If you enable this policy setting, every 24 hours the model of the computer will be validated against the hardware compatibility list before it enables BitLocker protection on drives of a computer.  If you disable or do not configure this policy setting, the computer model will not be 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 it. 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 allows your organization to exempt a user from BitLocker protection. It also allows you to configuring a URL, email address, or telephone number that will instruct users 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 from BitLocker protection. The request exemption form will not be available to the user.  Suggested Configuration: Not Configured |  |

### User-Based Group Policy Definitions

This section describes user-based MBAM Group Policy definitions.

| **Policy Name** | **Overview and Suggested Policy Settings** |
| --- | --- |
| Allow the user to be exempted from BitLocker encryption | This policy lets MBAM to be configured to exempt a user from BitLocker encryption.  If you enable this policy setting, the specified user is exempted from BitLocker encryption.  If you disable this policy setting, the specified user is denied exemption from BitLocker encryption. Also, the exemption is not available to the user.  If you do not configure this policy setting, the user is not exempted from BitLocker encryption, and the exemption option is not available to the user.  Suggested Configuration: Not configured |

### Windows Policies

Microsoft BitLocker Administration and Monitoring offers a customized BitLocker control panel that replaces the default Windows BitLocker control panel when configured. The updated BitLocker Encryption Options control panel offers users additional functionality in managing their PIN and passwords, as well as easy access to Trusted Module Platform (TPM) management.

Note



The customized MBAM control panel is not deployed automatically. If you choose to use the the BitLocker Encryption Options control panel in your deployment of MBAM, you must use the following steps to configure and deploy it:

To Configure BitLocker Encryption Options



|  |
| --- |
| 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 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. |

# Planning 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 the Server Deployment

The following Microsoft BitLocker Administration and Monitoring features represent the sever 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 a variety of configurations, using from one to five servers. In general, we recommend using a three or five server configuration for production environments, though two and four servers can be used as well.

 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 purposes.

 Three-computer configuration   
Server features are installed in the following configuration

 Recovery and Hardware Database, Compliance and Audit Reports, 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 3 or 5 computer configuration is recommended for production environments.

Microsoft BitLocker Administration and Monitoring server components can be installed individually (for example, you can install the Recovery and Hardware Database feature, finish the install and then start the Setup Wizard again to install the next feature) but they must be installed in the following order:

Order of Deployment of BitLocker Administration and Monitoring Server Components



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

Each Microsoft BitLocker Administration and Monitoring feature has specific prerequisites. For a full list of server component prerequisites, see [MBAM Supported Configurations](#zd1ce21c430964a169b5efb10feadc2af).

## Planning for Administrator Roles

When planning for the BitLocker Administration and Monitoring infrastructure and policy, it is important to determine the roles and responsibilities of the Microsoft BitLocker Administration and Monitoring administrators across the enterprise. These 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 and then adding those security groups to the BitLocker Administration and Monitoring roles (that is, local groups).

 MBAM System Administrators 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 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 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 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 Uses 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.

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.



|  |
| --- |
| 1. |

# Planning Client Deployment for MBAM

There are two ways to encrypt a computer in your organization with Microsoft BitLocker Administration and Monitoring (MBAM):

 Encrypted by an administrator before the user receives the computer

 Encrypted by using Group Policy after the user receives the computer

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

## Client System Requirements

For a list of supported configurations for MBAM, see [MBAM Supported Configurations](#zd1ce21c430964a169b5efb10feadc2af).



|  |
| --- |
| 1. |

## 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 it means 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 it 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 encrypt the operating system volume of the computer with TPM protector. If your organization wants to use the TPM chip as well as a PIN protector, the administrator encrypts the system volume with the TPM protector and then user chooses a PIN the first time they log 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 in, 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



If you choose to use the TPM protector option, the administrator must accept the BIOS prompt to enable and initialize the TPM before delivering the computer to the user.



|  |
| --- |
| 1. |

## 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 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 must accept the BIOS prompt to enable and initialize the TPM chip if it is required by the policy of the organization.



|  |
| --- |
| 1. |

# Planning Hardware Management for MBAM

The Microsoft BitLocker Administration and Monitoring (MBAM) Hardware Compatibility feature allows your company to ensure only computer hardware that you specify as supporting BitLocker is encrypted. When this feature is on, Microsoft BitLocker Administration and Monitoring will only encrypt computers that are marked as Compatible. When this feature is turned off, all computers where the MBAM policy has been deployed will be encrypted.

The Hardware Compatibility feature works in the following way;

1. The MBAM agent collects essential computer information like 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 will create a list of make/models to allow you to clarify which can or cannot support BitLocker

3. The list is automatically populated by the MBAM agent, all new make/models are added with a state of Unknown. An administrator can modify that list to specify a make/model as Compatible or Incompatible.

4. Before the MBAM agent begins encrypting, it will verify that the hardware is marked as Compatible.

 If the hardware is marked as Compatible, BitLocker will start the encryption process.

 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 periodically check to see if the state has changed to Compatible.

This feature is best used when your organization has older computer hardware or computers that do not support TPM. If this is the case, deploy the Hardware Compatibility feature to make sure that Microsoft BitLocker Administration and Monitoring is only applied to computer models that support it. If all computers in your organization will support BitLocker, you do not have to deploy the Hardware Compatibility feature.

Note



The Hardware Compatibility feature is set to ‘on’ by default.  The agent is managed via a Group Policy object and when ‘on’ it will verify that the hardware is marked as Compatible before encrypting.  The server component can be optionally installed on the server. If installed, the hardware list will be created.



|  |
| --- |
| 1. |

# Deploying MBAM

Before continuing to the Deployment section of this help guide, make sure you have completed the planning phase of your Microsoft BitLocker Administration and Monitoring (MBAM) install, by following the topics in [Planning for MBAM](#z3c957c203f224ee3802ff422b490b940). This will help ensure that you have met all prerequisites for MBAM and considered which policies and features you want to use, and how. Once you have completed your planning stage, use the topics in this section to help you deploy MBAM to your environment.

## Deploying MBAM

[Deploying MBAM Group Policies](#zcf45ea35968f48ec96479bb0dae1056c)

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

[Deploying MBAM on a Single Server](#z9acd19e2b1424524a2ed94384c18f1eb)

|  |
| --- |
| Describes how to install MBAM and its various server components on a single server configuration |

[Deploying MBAM on Distributed Servers](#z1fc4917fae784ba999d8fc69b32abfe6)

|  |
| --- |
| Describes how to install MBAM and its various server components on a multi-server configuration |

[Deploying the MBAM Client](#z7caaae4fa798460f8b8409e5a4f03853)

|  |
| --- |
| Describes how to install the MBAM client and manage its service |

# Deploying MBAM Group Policies

## Deploying MBAM Group Policy

To successfully deploy Microsoft BitLocker Administration and Monitoring (MBAM), you first need to determine which policies you are going to use in your implementation of MBAM. See [Planning and Configuring Group Policy for MBAM](#z48a45d7492674f14b43c6c1f38f8ed39) for detailed information on the different policies available. Once you have determined the policies you are going to use, you will need to create one or more Group Policy objects (GPO) that include the policy settings for MBAM.

Once you have created the necessary GPOs, use the following steps to deploy the MBAM service to your organization’s client machines.

How to Deploy the MBAM Service to Client Machines



|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. On a computer with the BitLocker Group Policies installed, make sure Microsoft BitLocker Administration and Monitoring services are enabled.  2. 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, select Computer configuration, choose Policies, click Administrative Templates, select Windows Components, and then click MDOP MBAM (BitLocker Management).  3. Next, edit the setting for your 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** | | --- | --- | --- | | Data Recovery | Configure key recovery service | Enabled. Set Key recovery service endpoint and Key recovery information to backup | | Reports | Configure status reporting service | Enabled. Set Status reporting service endpoint and Enter frequency status in (minutes). | | Client Management | Configure client checking status frequency (minutes) | Enabled. Set Enter frequency in (minutes) | | Operating System Drive | Enforce operating system drive encryption | Enabled. Set Select protector for operating system drive. Required to save operating system drive data to the Microsoft BitLocker Administration and Monitoring Key Recovery server. |   iImportant  Depending on the policies that your organization chooses to deploy, you may need to configure additional policies. See [Planning and Configuring Group Policy for MBAM](#z48a45d7492674f14b43c6c1f38f8ed39) for Group Policy configuration details for all MBAM policies. |

### Deploying the Updated BitLocker Encryption Options Control Panel

Microsoft BitLocker Administration and Monitoring offers a customized BitLocker control panel that replaces the default Windows BitLocker control panel when configured. The updated BitLocker Encryption Options control panel offers users additional functionality in managing their PIN and passwords, as well as easy access to Trusted Module Platform (TPM) management.



|  |
| --- |
| 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 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](#z48a45d7492674f14b43c6c1f38f8ed39)

# Deploying MBAM on a Single Server

The procedure describing installation includes 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 necessary prerequisites, see [MBAM Supported Configurations](#zd1ce21c430964a169b5efb10feadc2af) In addition, some features also have information that must be provided during the install process to successfully deploy the feature.

## Deploying the MBAM Server

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

How to Deploy the MBAM Server Features



|  |
| --- |
| 1. Start the Microsoft BitLocker Administration and Monitoring installation wizard.  2. Read and accept the Microsoft Software License Terms, and click Next to continue the installation.  3. By default, all Microsoft BitLocker Administration and Monitoring features are selected for installation. 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 Server Infrastructure for MBAM](#z962f2f48e80043f2ab25664a8a6298ee). For prerequisites of each MBAM server feature, see [MBAM Supported Configurations](#zd1ce21c430964a169b5efb10feadc2af).  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 Microsoft BitLocker Administration and Monitoring Setup wizard will display installation pages for the selected features  5. You will be prompted to configure network communication security. MBAM can optionally encrypt the communication between the Recovery and Hardware Database, the Administration and Monitoring servers, and the clients. If you choose to encrypt, you will be asked to select the Certificate Authority provisioned certificate that will be used for encryption.  6. Click Next to continue.  7. In the Configure the Recovery and Hardware database window, specify the SQL Server instance and name of the database that will store the recovery and hardware data. You must also specify both where the database file will be located and where the log information will be located.  8. Click Next to continue.  9. In the Configure the Compliance and Audit database window, specify the SQL Server instance and name of the database that will store the compliance and audit data. You must also specify where the database file will be located and where the log information will be located.  10. Click Next to continue.  11. Specify report service instance that will be used and provide a user account for accessing the database.  12. Click Next to continue.  13. 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.  14. Click Next to continue.  15. Specify whether to use Microsoft Updates to help keep your computer secure, and then click Next.  16. Once the Setup wizard has collected the necessary feature information, the Microsoft BitLocker Administration and Monitoring installation is ready to start. Click Back to navigate back through the wizard if you need 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 finished.  17. Click Finish to exit the wizard.  18. 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 Roles for MBAM](#z0c83cce46b124a258d41f4b0fd0a32c3). |

Post Installation Configuration



|  |
| --- |
| 1. After setup completes, you must add users Roles before users will have access to features within the MBAM management console. On the Administration and Monitoring Server add users to the following local groups to enable them access 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.   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.  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 machines 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 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.

How 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 Home location of a SQL Server Reporting Services site instance can be found at:  http://<NameofMBAMReportsServer>/Reports  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 will look like 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. 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 within the MBAM web site to verify they load successfully:   http://<computername>:<port>/default.aspx and confirm each of the links for navigation and reports   http://<computername>:<port>/MBAMAdministrationService/AdministrationService.svc   http://computername/MBAMComplianceStatusService/StatusReportingService.svc   http://<computername>:<port>/MBAMRecoveryAndHardwareService/CoreService.svc  Note  This list assumes the services are installed on the default port 80. 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  Verify that each web page loads successfully. |

# Deploying MBAM on Distributed Servers

The procedure describing installation includes the full installation of the Microsoft BitLocker Administration and Monitoring (MBAM) service on multiple servers. Each server feature has certain prerequisites. Some features also have additional information that must be provided to successfully deploy the component for the enterprise.

## Deploying the MBAM Server

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

How to Deploy the MBAM Server Features



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. Start the Microsoft BitLocker Administration and Monitoring installation wizard.  2. Read and accept the Microsoft Software License Terms, and click Next to continue the installation.  3. By default, all Microsoft BitLocker Administration and Monitoring features are selected for installation. 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 Server Infrastructure for MBAM](#z962f2f48e80043f2ab25664a8a6298ee). For prerequisites of each MBAM server feature, see [MBAM Supported Configurations](#zd1ce21c430964a169b5efb10feadc2af).  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 Microsoft BitLocker Administration and Monitoring Setup wizard will display installation pages for the selected features. The following sections describe installation procedures for each feature.  Note  The following instructions are based on the assumption 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.  Recovery and Hardware Database Feature   |  | | --- | | a. MBAM can optionally encrypt the communication between the Recovery and Hardware Database and the Administration and Monitoring servers. If you choose to encrypt, you will be asked to select the Certificate Authority provisioned certificate that will be 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 will connect to the database using its Network Service 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. |   Compliance Status Database Feature   |  | | --- | | a. MBAM can optionally encrypt the communication between the Recovery and Hardware Database and the Administration and Monitoring servers. If you choose to encrypt, you will be asked to select the Certificate Authority provisioned certificate that will be used for encryption.  b. Click Next to continue.  c. 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 Network Service accounts.  d. 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.  e. Click Next to continue.  f. Specify the user account that will be used to access the database for reports.  g. Click Next to continue with the Microsoft BitLocker Administration and Monitoring Setup wizard. |   Compliance and Audit Reports Feature   |  | | --- | | a. Specify the remote SQL Server instance (for example: <ServerName\InstanceName>) 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” however this can be altered when installing 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. |   Administration and Monitoring Server Feature   |  | | --- | | a. MBAM can optionally encrypt the communication between the Recovery and Hardware Database and the Administration and Monitoring servers. If you choose to encrypt, you will be asked to select the Certificate Authority provisioned certificate that will be used for encryption.  b. Click Next to continue.  c. Specify the remote SQL Server instance (for example: <ServerName\InstanceName>) where the Compliance Status Database was installed.  d. Next specify where the name of the Compliance Status Database. By default the database name is “MBAM Compliance Status” however this can be altered when installing the Compliance Status Database feature.  e. Click Next to continue.  f. Specify the remote SQL Server instance (for example: <ServerName\InstanceName>) 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 can 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 Home location of a SQL Server Reporting Services site instance can be found at:  http://<NameofMBAMReportsServer>/Reports  Note  If SQL Server Reporting Services was configured as a named instance the URL will look like the following:http://<NameofMBAMReportsServer>/Reports\_<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. Once the selected Microsoft BitLocker Administration and Monitoring feature information is complete, the Microsoft BitLocker Administration and Monitoring installation using the Setup wizard is ready to start. Click Back to navigate back through the wizard if you need 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 Roles for MBAM](#z0c83cce46b124a258d41f4b0fd0a32c3). |

Post Installation Configuration



|  |
| --- |
| 1. After setup completes, you must add users Roles before users will have access to features within the MBAM management console. On the Administration and Monitoring Server add users to the following local groups to enable them access 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.   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.  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 machines 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 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.

How 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 Home location of a SQL Server Reporting Services site instance can be found at:  http://<NameofMBAMReportsServer>:<port>/Reports.aspx  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 will look like the following:http://<NameofMBAMReportsServer>:<port>/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. 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 within the MBAM web site to verify they load successfully:   http://<computername>:<port>/default.aspx and confirm each of the links for navigation and reports   http://<computername>:<port>/MBAMAdministrationService/AdministrationService.svc   http://computername/MBAMComplianceStatusService/StatusReportingService.svc   http://<computername>:<port>/MBAMRecoveryAndHardwareService/CoreService.svc  Note  This list assumes the services are installed on the default port 80. 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  Verify that each web page loads successfully. |

# Deploying the MBAM Client

The Microsoft BitLocker Administration and Monitoring (MBAM) client helps administrators 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 or by directly encrypting the client computers as part of the initial imaging process.

How 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) provided with the MBAM software.  2. Use Active Directory or an enterprise software deployment tool to push the MSI to the target computers.  3. Configure the distribution process or Group Policy to run the client software file. Once installed, the client will read the Group Policy pushed from the Domain Controller. |

## How 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 with the proper configuration.



|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. If your organization is going to be using the Trusted Platform Module (TPM) protector or TPM + PIN protector options in BitLocker, it is important to activate the TPM chip before the initial deployment of MBAM. This removes the need for a reboot later in the process and ensures that the TPM chips are properly configured per your organization’s requirements. Activating the TPM chip must be set manually in the BIOS of the computer. Refer to the manufacturer documentation for more details on how to configure the TPM chip.  a. Set TPM to ENABLED  b. Set TPM to ACTIVE  c. Set TPM to NOT OWNED  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, then the Recovery Password will not be stored in the MBAM Key Recovery Service. By default, MBAM will not allow encryption to occur unless the Recovery Key can be stored.   If a computer starts up in recovery mode before the Recovery Key is stored to the MBAM server, the computer will need to be reimaged. No recovery method is available.  4. Run the command prompt as administrator and stop the MBAM service and set to manual or on demand start by typing the following:  a. Net stop maltaagent  b. Sc config maltaagent start= demand  5. Set the registry settings to allow the MBAM agent to ignore Group Policy and execute 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. From regedit, go to “HKLM\SOFTWARE\Microsoft\MBAM” and configure the settings used the following table:   | **Registry Entry** | **Configuration Settings** | | --- | --- | | DeploymentTime | 0 = OFF | | 1 = Use deployment time policy settings (default) | | UseKeyRecoveryService | 0 = Do not escrow key ( the next two registry entries are not needed in this case) | | 1 = Escrow in Key Recovery system (default)  Recommended: the computer needs to be able to communicate with Key Recovery Service. Verify the computer can communicate with the service before proceeding. | | KeyRecoveryOptions | 0 = Uploads Recovery Key Only | | 1 = Uploads Recovery Key and Key Recovery Package (default) | | KeyRecoveryServiceEndPoint | Set this value to the URL for Key Recovery web server (for example, http://<machinename>/MBAMRecoveryAndHardwareService/CoreService.svc). |   nNote  MBAM policy or registry values can be set here to override previously set values.  7. The MBAM agent will reboot the system during MBAM client deployment. When you are ready for this reboot, run the following from a Command Prompt as administrator:  a. Net start MaltaAgent  8. The system should reboot. On restart the BIOS will prompt 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 administrator and typing the following:  a. sc config maltaagent start= auto  b. net start maltaagent  10. Remove the bypass registry values by running regedit and going to the “HKLM\SOFTWARE\Microsoft” registry entry. Delete the MBAM node by right-clicking it and selecting Delete. |

# Operations for MBAM

The operations and troubleshooting guide provides information about how to configure and use Microsoft BitLocker Administration and Monitoring (MBAM) for post-installation configuration, management, and day-to-day operations tasks.

## In This Section

[How to Generate MBAM Reports](#z1eb6da6323204cabb43acb6832270fcb)

|  |
| --- |
| Describes how to generate reports on enterprise compliance, individual computers, key recovery activity, and hardware compatibility. |

[Understanding MBAM Reports](#z1a53da827b58483e90ba572970500cc5)

|  |
| --- |
| Provides details on reporting in MBAM and what information the reports contain |

[How to Determine BitLocker Encryption State of Lost Computers](#z11218476bed74fb8babe4bf43dad405c)

|  |
| --- |
| Describes how to determine if the volumes on a computer are encrypted in case of loss or theft. |

[How to Recover an Encrypted Drive](#z9b4a2fb5e2604f05b3997a638d1d216c)

|  |
| --- |
| Describes how to access the BitLocker key recovery data system, which can provide a recovery password for data recovery |

[How to Recover a Corrupted Drive](#zad61a1f0ee824761a62a8b32a4b2cc1b)

|  |
| --- |
| Describes how to use the BitLocker key recovery data system to recover a damaged or corrupted drive |

[How to Recover a Moved Drive](#zde8790df6f2f4678b90d1d3a8cdc92fa)

|  |
| --- |
| Describes how to use the BitLocker key recovery data system to unlock a drive that has been moved to a new computer |

[How to Utilize Single Use Recovery Keys](#zd296ec32193b43349c98ad4d624cb2f6)

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

[How to Reset a TPM Lockout](#zff3f16b3da84484b8c84ade2b6a8723d)

|  |
| --- |
| Describes how to unlock a computer in case of a TPM lockout |

[How to Manage Hardware Compatibility](#z99f1f9f7967b47028528ce3bcf2f6cb4)

|  |
| --- |
| Describes how to manage BitLocker compatibility of computer models in an enterprise organization |

[How to Manage User and Computer Exemptions](#z9af95067d20743bfacf7a63e63a25370)

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

[How to Manage Roles for MBAM](#z0c83cce46b124a258d41f4b0fd0a32c3)

|  |
| --- |
| Describes how to grant administrative users access to one or more MBAM features |

[How to Use the Client Control Panel](#z174d5e774dc241b6a80f0eab62850f00)

|  |
| --- |
| Details the MBAM BitLocker Encryption Options control panel |

# How to Generate MBAM Reports

Microsoft BitLocker Administration and Monitoring (MBAM) lets you run a variety of reports to monitor BitLocker usage and compliance. The procedure that follows shows the steps needed to generate reports on enterprise compliance, individual computers, key recovery activity, and hardware compatibility.

Note



To run the reports, you must be a member of the Report Users Role on both 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 go to the Microsoft BitLocker Administration and Monitoring web site. The default URL for the administration web site is http://<machinename> of the Microsoft BitLocker Administration and Monitoring server.  2. In the left side pane, click Reports and then select the report you want to run from the top menu bar.  Note  For details on the information presented in MBAM reports, see [Understanding MBAM Reports](#z1a53da827b58483e90ba572970500cc5). |

The following sections describe the MBAM Compliance and Auditing reports.

Enterprise Compliance Report



|  |
| --- |
| 1. From the Management Console, select the Reports node from the left side navigation pane, select the “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 Non-Compliant) 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.  Note  The Enterprise Compliance report is generated by a SQL job that runs every 6 hours, so the first time you attempt to view the report, data may be missing.  3. Results can be saved in a variety of formats, including HTML, Microsoft Word, and Microsoft Excel.  4. Select a computer name to view information about the computer in the Computer Compliance Report.  5. Select the plus sign (+) beside the computer name to view information about the volumes on the computer. |

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.  3. Results can be saved in a variety of formats, including HTML, Microsoft Word, and Microsoft Excel.  4. Select a computer name to display the more information about the computer in the Computer Compliance Report.  5. Select the plus sign (+) beside the computer name to view information about the volumes on the computer. |

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 the following:   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 acquire 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 instance 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.  3. Results can be saved in a variety of formats, including HTML, Microsoft Word, and Microsoft Excel. |

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.  3. Results can be saved in a variety of formats, including HTML, Microsoft Word, and Microsoft Excel. |

# Understanding MBAM Reports

Microsoft BitLocker Administration and Monitoring (MBAM) collects information from Active Directory and client machines to let you run different reports to monitor BitLocker usage and compliance. Using the Reports section of the MBAM management console, you can generate reports on enterprise compliance, individual computers, key recovery activity, and hardware compatibility.

## Reports

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

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.

Table: Enterprise Compliance Report Fields

| **Column Name** | **Description** |
| --- | --- |
| Computer Name | This is the user specified DNS machine name that is being managed by MBAM |
| Domain Name | This is the fully qualified domain name where the client machine resides and is managed by MBAM |
| Compliance Status | An indication of two states; Non-Compliant and Compliant in accordance with the policy specified for the machine (see table Enterprise Compliance Report Compliance States for details regarding interpretation of states) |
| Exemption | Describes the state of the machine hardware with respect to the identification of the hardware type, and whether it 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 has been identified and has been marked as exempt from MBAM policy), and Not Exempt (the hardware has been identified and is not exempt from policy) |
| Device Users | Lists known users on the machine that is being managed by MBAM |
| Compliance Status Details | Lists the error and status messages of the compliance state of the machine in accordance to the policy specified |
| Last Contact | Indicates the date and time of the last time the machine contacted the server to report compliance status. This time is configurable (see MBAM policy settings) |

Table: Enterprise Compliance Report Compliance States:

| **Compliance Status** | **Exemption** | **Description** | **User Action** |
| --- | --- | --- | --- |
| Non-Compliant | Not Exempt | The machine is non-compliant 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 review that the state of each drive is in accordance with the specified policy. If the encryption state is not encrypted, it could mean the encryption is in process, or there is an error on the machine. If there is no error, then the likely cause is the machine is still in process and to check back again later to determine if the state changes |
| Compliant | Not Exempt | The machine is compliant in accordance with the specified policy | No Action, 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, the state of the computer with respect to encryption is exempt via policy |
| Compliant | Hardware Unknown | Indicates that the hardware type has been identified by MBAM but it is unknown by MBAM whether it is exempt or not exempt (meaning an administrator has not set the compatible status) so it defaults to a 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 via MBAM policy) between the user request to make compatible and the time the client machine reports back in. Note the time of the Last Contact, and check in again after 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 machine or hardware type. |

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

This report can be accessed by clicking on 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 as well as an indication of the policy applied to each of the drive types on the computer. To view the details of each drive, expand the Computer Name entry

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

Table: Compliance Report Fields

| **Column Name** | **Description** |
| --- | --- |
| Computer Name | This is the user specified DNS machine 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 type 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 Non-Compliant. Note that the compliance status per drive (see table below) may indicate different compliance states. This field however represents that compliance state in accordance to the policy 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 machine that is being managed by MBAM |
| Exemption | Describes the state of the machine hardware with respect to the identification of the hardware type, and whether it 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 has been identified and has been marked as exempt from MBAM policy), and Not Exempt (the hardware has been identified and is not exempt from policy). |
| Manufacturer | Specifies the computer manufacturer name as it appears in the machine BIOS |
| Model | Specifies the computer manufacturer model name as it appears in the machine BIOS |
| Compliance Status Details | Lists the error and status messages of the compliance state of the machine in accordance to the policy specified |
| Last Contact | Indicates the date and time of the last time the machine contacted the server to report compliance status. This time is configurable (see MBAM policy settings) |

Table: Compliance Report Drive Fields

| **Column Name** | **Description** |
| --- | --- |
| Drive Letter | Indicates the computer drive letter that has been assigned to the particular drive by the user. |
| Drive Type | Indicates the type 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; Non-Compliant 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 machine in accordance to the policy specified |

Hardware Audit Report   Use this report type 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, which user 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.

Table: Hardware Audit Report fields

| **Column Name** | **Description** |
| --- | --- |
| Date and Time | Indicates the date and time that a change was 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 allow the administrator to produce contextual reports based on need.

Table: 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 helpdesk user or the end user. The 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 modified  **** 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 additional details about how to run MBAM reports, see [How to Manage Hardware Compatibility](#z99f1f9f7967b47028528ce3bcf2f6cb4).

# 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.

How to Determine the BitLocker Encryption State of Lost Computers



|  |
| --- |
| 1. Open a web browser and open the BitLocker Administration and Monitoring management console.  Note  Note: The default address for the BitLocker Administration and Monitoring management console is http:// <machinename>.  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 regarding lost devices.  Note  Device compliance is determined by the deployed BitLocker policies, so verification of deployed policies is recommended when attempting to determine the BitLocker encryption state of the device. |

# 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. A BitLocker-protected volume will go into recovery mode in the case of a lost or forgotten PIN or password, or if the Trusted Module Platform (TPM) chip detects changes to the computer’s BIOS or startup files.

This document covers how 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.

How to Recover an Encrypted Drive



|  |
| --- |
| 1. Open a web browser and browse to the Microsoft BitLocker Administration and Monitoring website.  2. In the left navigation bar, select 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. Select one of the predefined options in the Reason for Drive Unlock drop-down menu. Click Submit.  Note  If you are an MBAM Advanced Helpdesk user, the user domain and user ID fields are not required.  4. Microsoft BitLocker Administration and Monitoring will return 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 will provide BitLocker with critical information necessary to attempt to recover the drive.  5. After the recovery password and recovery package is retrieved, the recovery password is displayed. The password can be copied by clicking Copy Key, and then you can paste the recovery password into an email message. Or, you can save the recovery password to a file by clicking Save.  6. As soon as the user inputs the recovery password into their system or uses the recovery package, the drive will be unlocked.  Note  If a single-use recovery key is used to recover a system, that recovery key cannot be used again. |

# How to Recover a Corrupted Drive

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

Recovering a Corrupted Drive



|  |
| --- |
| 1. To create the recovery key package necessary to recover a corrupted drive, open a web browser and go to the MBAM console web page.  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 need 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 containing the corrupted drive.  6. Open an elevated command prompt. To do this, click Start and type cmd in the Search programs and files box. Right click cmd.exe and select Run as Administrator.  7. At the command prompt, type the following:  repair-bde <fixed drive> <corrupted drive> -kp <location of keypackage> -rp <recovery password>  Note  Replace <fixed drive> with an available hard drive that has free space equal or larger than the data on the corrupted drive. Data on the corrupted drive will be recovered and moved to the specified hard drive. |

# How to Recover a Moved Drive

When you move a Microsoft BitLocker Administration and Monitoring (MBAM) encrypted operating system drive to another computer, the drive will not accept the PIN used in a previous computer because of the change to the Trusted Platform Module (TPM) chip. You will need a way to get 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 been moved.

## Recovering a Moved Drive



|  |
| --- |
| 1. Start the computer containing the moved drive in Windows recovery environment (WinRE) mode, or start the computer with Microsoft Diagnostic and Recovery Tool 6.5 (MS DaRT).  2. Once the computer has been started with WinRE or MS DaRT, it will treat the moved operating system drive as a data drive. It 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, which will also display the recovery key ID.  3. Use the recovery key ID to retrieve the recovery password and unlock the drive from the MBAM console web site.  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+PIN protector without the original TPM chip.  5. Once this is complete, start the system normally. The MBAM agent will now enforce the policy to encrypt the drive with the new computer’s TPM + PIN. |

# How to Utilize Single Use Recovery Keys

The Microsoft BitLocker Administration and Monitoring (MBAM) Recovery Password feature allows a BitLocker encrypted device to be unlocked without the main protector type that may be used, for example TPM+PIN or just PIN. As useful as this is, the limitation for this feature is it can be reused by the user with no control from the MBAM administrators. If a user gets the Recovery Password and saves it or leaves a copy on their desk, it could allow a malicious user to reuse the Recovery Password on the computer to bypass the BitLocker protection.

This topic details how you can use the Single Use Recovery Key feature of MBAM to mitigate this risk.

How to Utilize Single Use Recovery Keys



|  |
| --- |
| 1. When a BitLocker protected drive is put into Recovery Mode, the user will need a Recovery Key in order to unlock the drive. Normally, this Recovery Key could be used again in the future to unlock the drive. To prevent this Microsoft BitLocker Administration and Monitoring can be configured to utilize Single Use Recovery keys that expire upon use. ~~To do this, you must configure and deploy the following Group Policies:~~  ~~ Enable Single Use Recovery Password~~  ~~ Enable PIN change prompt after OS Recovered~~  ~~ Configure Key Expiration Period for Data Volumes.~~  ~~Note~~  ~~See [Planning and Configuring Group Policy for MBAM](#z48a45d7492674f14b43c6c1f38f8ed39) for details on the above policies.~~  ~~2. Once the appropriate Group Policies have been deployed, Microsoft BitLocker Administration and Monitoring administrators can provide users with a Recovery Key that will expire once it is used. For detailed steps on how to recover a BitLocker protected drive, see [How to Recover an Encrypted Drive](#z9b4a2fb5e2604f05b3997a638d1d216c).~~ |

# How to Reset a TPM Lockout

The Encrypted Drive Recovery feature of Microsoft BitLocker Administration and Monitoring (MBAM) ensures the capture and storage of data and availability of tools required to manage TPM. This topic covers how to access the centralized Key Recovery data system in the MBAM Management Console, which can provide a Trusted Platform Module (TPM) owner password file as long as a computer ID and associated user identifier are supplied.

A TPM lockout can happen ~~if the TPM chip detects changes to the computer’s BIOS or startup files, or if the hard drive has been moved to a different computer~~.

How to Reset a TPM Lockout



|  |
| --- |
| 1. Open a web browser and go to the MBAM Management website.  2. In the left-side navigation pane, select Manage TPM. This will bring up 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:  a. An error message if no matching TPM owner password file is found  b. The TPM owner password file for the submitted computer  Note  If you are an Advanced Helpdesk user then the user domain and user ID fields are not required  5. After the TPM owner password is retrieved, the owner password hash will be displayed. The password can be saved to a 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. |

# How to Manage Hardware Compatibility

Microsoft BitLocker Administration and Monitoring (MBAM) can collect information on model and make of client computers if you deploy the “Allow Hardware Compatibility Checking” Group Policy. If this policy is configured, once the MBAM client has been deployed on a client computer, the Microsoft BitLocker Administration and Monitoring agent will report the model information of the computer to the MBAM server. ~~The frequency that the client reports to the server can be managed within the “Allow Hardware Compatibility Checking” policy.~~

How to Manage Hardware Compatibility



|  |
| --- |
| 1. Open a web browser and browse to the Microsoft BitLocker Administration and Monitoring web site. Select Hardware in the left menu bar.  2. In the right side pane, click Advanced Search and filter to display a list of all computer models with a Capability status of Unknown. A list of computer models matching the search criteria is returned.  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 click either Set Compatible or Set Incompatible to set the BitLocker compatibility, as appropriate, for the selected computer models. If set to Compatible, BitLocker attempts 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 the hardware compatibility list on a regular basis 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. |

# How to Manage User and Computer Exemptions

Microsoft BitLocker Administration and Monitoring (MBAM) can grant two forms of exemption from BitLocker protection, computer exemption and user exemption. Computer exemption is normally used if your organization has older computer hardware that does not support BitLocker. Your organization can also manage BitLocker protection by exempting users, if local laws or business reasons require it. Because BitLocker policy is applied to the computer, we recommend that you control BitLocker protection by exempting computers.

To exempt users from BitLocker protection, an organization will need to create an infrastructure to support exempted users, such as providing the user with a phone 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 sign 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 protected. 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 ~~Hardware and~~ User Exemptions

How to Exempt a Computer from BitLocker Protection



|  |
| --- |
| 1. ~~Open a web browser and go to the MBAM Management Console. Select Hardware in the left side navigation pane. This will display the hardware compatibility list for your organization.~~  ~~Note~~  ~~You must be an MBAM administrator to view this page; otherwise you will receive an error page.~~  ~~2. Use the Search field to locate the computer you want to exempt from BitLocker protection. You can search by Computer Manufacturer, Model name, Bios Maker, Bios Version, TPM Maker, TPM Version, and Capability Status to help narrow down the search results.~~  ~~3. Once you’ve located the computer you want to exempt from BitLocker protection, click the arrow next to the status of the computer under the Status column and select Incompatible. The computer will now be exempted from BitLocker protection~~ |

How to Exempt a User from BitLocker Protection



|  |
| --- |
| 1. In some cases, an organization may choose to control BitLocker exemption on a 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 using the MBAM [Planning and Configuring Group Policy for MBAM](#z48a45d7492674f14b43c6c1f38f8ed39) and associate it with the Active Directory group created in the previous step.  3. Once a security group for BitLocker exempted users is created, add the user names of the users requesting exemption to this group. Once 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. |

How a User Requests Exemption from BitLocker Protection



|  |
| --- |
| 1. If you have deployed the User Exemption Policy template, a user can request exemption from BitLocker protection through the MBAM client.  2. Once the user logs on to a computer that has been marked as Compatible in the MBAM Hardware Compatibility list, they will receive a notification that their computer is going to be encrypted. They can select Request Exemption, postpone the encryption by selecting Later, or select Start to accept the BitLocker encryption.  Note  Selecting Request Exemption ~~or Later~~ 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 organization’s 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  Once the exemption request is received, the MBAM Administrator can decide if it is appropriate to add the user to the BitLocker Exemption Active Directory group.  Note  Once the postpone time limit set in the User Exemption Policy has expired, the user will not see options to request exemption to ~~or postpone~~ the encryption policy. At this point the user must contact the MBAM administrator directly to receive exemption from BitLocker Protection. |

# How to Manage Roles for MBAM

After Microsoft BitLocker Administration and Monitoring (MBAM) setup is completed 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 groups by using Active Directory.

How to Grant Access to MBAM Roles



|  |
| --- |
| 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 ~~some of~~ the Hardware Capability 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 using 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 using either option  For more information about roles for Microsoft BitLocker Administration and Monitoring, see [Planning Server Infrastructure for MBAM](#z962f2f48e80043f2ab25664a8a6298ee). |

# How to Use the Client Control Panel

Microsoft BitLocker Administration and Monitoring (MBAM) allows administrators to configure policy to hide the existing BitLocker control panel and install a customized MBAM control panel under System and Security called BitLocker Encryption Options. The MBAM control panel can be used to unlock encrypted fixed and removable drives, as well as manage your PIN or password.

Using the MBAM Client Control Panel



|  |
| --- |
| 1. To open BitLocker Encryption Options, click Start and then select Control Panel. Once the Control Panel opens, select System and Security.  2. Double-click BitLocker Encryption Options to open the customized MBAM control panel. You will see a list of all the hard drives on the computer and their encryption status, as well as an option to manage your PIN or passwords.  3. The list of hard 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](#z9af95067d20743bfacf7a63e63a25370) 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 will be prompted to enter their current PIN and their new PIN (as well as confirmation of 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 input your current password. Once the drive is unlocked, select Reset Password to change your current password. |

## See Also

How to Grant Hardware and User Exemptions

# Best Practices for MBAM

Section Intentionally Left Blank. Content will be added next week, post-TR.

This section should contain sub-topics listing security information that would be interesting to IT Pros.

For example: list of all accounts, groups, and security permissions required to complete tasks, security best practices and recommendations, port configurations required, data protection, auditing, account requirements for roles of Malta.

Best-practices guidelines for Malta administrators are also shared into this section from the planning, deployment, and operations sections.

## In This Section

The item being defined goes here.

|  |
| --- |
| Planning Security Best Practices |

The item being defined goes here.

|  |
| --- |
| Deployment Security Best Practices |

The item being defined goes here.

|  |
| --- |
| Operations Security Best Practices |

## See Also

[Microsoft BitLocker Administration and Monitoring Planning, Deployment, and Operations Guide](#z81de3502896e42d595a88a7670f93ead)

# Technical Reference for MBAM

This section should contain sub-topics listing technical reference information that would be interesting to administrators.

For example: all of the log file locations used by Microsoft BitLocker Administration and Monitoring (MBAM), additional deep technical information pulled from specs that customers might be interested in, programming reference, feature reference, and tools reference..

Technical reference topics are also shared into this section from the deployment and operations sections.

## In This Section

|  |
| --- |
| [List of Log Files for MBAM](#ze0abc9aaa4794619b552967039fae551) |

|  |
| --- |
| [Moving MBAM Features to Another Server](#z192d0a4de16242ee8a8f7f582634dd39) |

.

|  |
| --- |
| [MBAM Keyboard Shortcuts](#z5c479aa2b35043eeb6afed8e787b6449) |

## See Also

[Moving MBAM Features to Another Server](#z192d0a4de16242ee8a8f7f582634dd39)

# MBAM Installation Checklists

The following checklist provides a high-level list of items to consider and outlines the steps that you should take to deploy Microsoft BitLocker Administration and Monitoring (MBAM). .

## BitLocker Administration and Monitoring Installation Checklist

Note



It is not required to extend the Active Directory schema as BitLocker recovery data (known as keys) are in stored in the Recovery and Hardware database for Microsoft BitLocker Administration and Monitoring.

|  |  |
| --- | --- |
| Step | Reference |
| Define the system architecture for Microsoft BitLocker Administration and Monitoring that will support managing your environment. | Microsoft BitLocker Administration and Monitoring Deployment Guide: [Planning for MBAM](#z3c957c203f224ee3802ff422b490b940) |
| Provision the Windows Servers that will be used to host the following Microsoft BitLocker Administration and Monitoring features within your environment:  ****** MBAM Administration and Monitoring server  ****** MBAM Recovery and Hardware Database server  ****** MBAM Compliance Status Database server  ****** MBAM Compliance and Audit Reports server | Microsoft BitLocker Administration and Monitoring Deployment Guide: [MBAM Supported Configurations](#zd1ce21c430964a169b5efb10feadc2af) |
| Install the required Windows Server Roles, Role Services, and features to the Windows Servers that will be used to host the following Microsoft BitLocker Administration and Monitoring features within your environment  ****** MBAM Administration and Monitoring server | BitLocker Administration and Monitoring Deployment Guide: [MBAM Supported Configurations](#zd1ce21c430964a169b5efb10feadc2af) |
| Install any critical Windows updates on the following servers:  ****** MBAM Administration and Monitoring server  ****** MBAM Recovery and Hardware Database server  ****** MBAM Compliance Status Database server  ****** MBAM Compliance and Audit Reports server | http://go.microsoft.com/fwlink/?LinkId=105851 |
| Provision the SQL Server Database Engine and other SQL features to the Windows Servers that will be used to host the following Microsoft BitLocker Administration and Monitoring features within your environment  ****** MBAM Recovery and Hardware Database server  ****** MBAM Compliance Status Database server | BitLocker Administration and Monitoring Deployment Guide: [MBAM Supported Configurations](#zd1ce21c430964a169b5efb10feadc2af) |
| Provision the SQL Server Reporting Services to the Windows Servers that will be used to host the following BitLocker Administration and Monitoring features within your environment  ****** MBAM Compliance and Audit Reports server | BitLocker Administration and Monitoring Deployment Guide: [MBAM Supported Configurations](#zd1ce21c430964a169b5efb10feadc2af) |
| Configure the SQL Server Reporting Services instance on the MBAM Compliance and Audit Reports server such that it is operational and in a running state. | BitLocker Administration and Monitoring Deployment Guide: [MBAM Supported Configurations](#zd1ce21c430964a169b5efb10feadc2af) |
| Install any critical Microsoft SQL Server updates on the following servers:  ****** MBAM Recovery and Hardware Database server  ****** MBAM Compliance Status Database server  ****** MBAM Compliance and Audit Reports server | http://go.microsoft.com/fwlink/?LinkId=105851 |
| Decide if you will choose to encrypt communication between Microsoft BitLocker Administration and Monitoring features. If so initiate any processes necessary to ensure that an appropriate certificate has been provisioned to each server via your Public Key Infrastructure (PKI). In this case certificates should be provisioned to the following servers.  ****** MBAM Recovery and Hardware Database server  ****** MBAM Compliance Status Database server  ****** MBAM Compliance and Audit Reports server  Important  Certificates must be provisioned to each server in advance of installing BitLocker Administration and Monitoring features. | BitLocker Administration and Monitoring Deployment Guide: [Planning for MBAM](#z3c957c203f224ee3802ff422b490b940) |
| Run the Microsoft BitLocker Administration and Monitoring setup from the MDOP installation media, from a copy of the installation media located on a network shared folder, or other storage media.  Important  When installing Microsoft BitLocker Administration and Monitoring features across multiple servers,install the features in the following order:  ****** MBAM Administration and Monitoring server  ****** MBAM Recovery and Hardware Database server  ****** MBAM Compliance Status Database server  ****** MBAM Compliance and Audit Reports server  ****** MBAM Administration and Monitoring server | BitLocker Administration and Monitoring Deployment Guide: [Deploying MBAM](#zd9fa7c5fac1e419b968abbaf5a5c828d) |
| Verify that the Microsoft BitLocker Administration and Monitoring features were successfully deployed and are operational. | BitLocker Administration and Monitoring Deployment Guide: Post Installation Steps |
| Define and initiate a back-up policy for the MBAM Recovery & Hardware and Compliance Status databases. | BitLocker Administration and Monitoring Deployment Guide: Post Installation Steps |
| If you chose to encrypt the MBAM Recovery and Hardware Database feature create a backup the certificate that was used to encrypt the database. | BitLocker Administration and Monitoring Deployment Guide: Post Installation Steps |
| Add users to the Microsoft BitLocker Administration and Monitoring Local Groups on the following servers:  ****** MBAM Administration and Monitoring server  ****** MBAM Compliance and Audit Reports server | BitLocker Administration and Monitoring Deployment Guide: Post Installation Steps |
| Define the Microsoft BitLocker Administration and Monitoring policies and provision them to Active Directory. | BitLocker Administration and Monitoring Deployment Guide: Post Installation Steps |
| Deploy the Microsoft BitLocker Administration and Monitoring client to desktops on the network and any images that are used for provisioning new desktops. |  |

# List of Log Files for MBAM

The following article describes the locations for the log files used by Microsoft BitLocker Administration and Monitoring (MBAM) during setup and operation.

## Setup

In order to get setup log files, you must install Microsoft BitLocker Administration and Monitoring using msiexec package with the /L <location> option. Log files will be created in the location specified.

## Application and Monitoring

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

## Client

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

# Moving 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$$ RECOVERYANDHWDB\_SQLINSTANCE=$SERVERNAME$\$SQLINSTANCENAME$  Note  Replace the following values in the example above with those that match your environment:   $SERVERNAME$\$SQLINSTANCENAME$ - Input the server name and instance where the Recovery and Hardware Database will be moved to.   $DOMAIN$\$SERVERNAME$ - Input the domain and server names of each MBAM Application and Monitoring Server that will contact the Recovery and Hardware Database. If there are multiple, use a semi-colon to separate them in the list (e.g.: $DOMAIN\SERVERNAME$;$DOMAIN\$SERVERNAME$$). 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 masterGOEXEC 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];GOBACKUP 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 masterGO-- Drop certificate created by MBAM setup. DROP CERTIFICATE [MBAM Recovery Encryption Certificate]GO--Add certificateCREATE 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.ConnectionString"]' -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;GOALTER DATABASE "MBAM Compliance Status" SET RECOVERY FULL;GO-- Create MBAM Compliance Status Data logical backup devices. USE masterGOEXEC 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 masterGO-- 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$;Initial Catalog=MBAM Compliance Status;Integrated Security=SSPI;"  PS C:\> Set-WebConfigurationProperty '/connectionStrings/add[@name="Microsoft.Windows.Mdop.BitLockerManagement.StatusReportDataStore.ConnectionString"]' -PSPath "IIS:\sites\Microsoft Bitlocker Administration and Monitoring\MBAMComplianceStatusService" -Name "connectionString" -Value "Data Source=$SERVERNAME$\$SQLINSTANCENAME;Initial Catalog=MBAM Compliance Status;Integrated Security=SSPI;"  Note  Replace the 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 was 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. |

# 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 |
| 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 Microsoft BitLocker Administration and Monitoring console website does not use any MBAM specific keyboard shortcuts. Refer to your browser’s help to determine the keyboard shortcuts available for use.