

Malwarebytes
**ENDPOINT
SECURITY**

**Managing Malwarebytes in Large Networks
Best Practices Guide**

Version 1.8
21 March 2017

Notices

Malwarebytes products and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. You may copy and use this document for your internal reference purposes only.

This document is provided "as-is." The information contained in this document is subject to change without notice and is not warranted to be error-free. If you find any errors, we would appreciate your comments; please report them to us in writing.

The Malwarebytes logo is a trademark of Malwarebytes. Windows is a registered trademark of Microsoft Corporation. All other trademarks or registered trademarks listed belong to their respective owners.

Copyright © 2017 Malwarebytes. All rights reserved.

Third Party Project Usage

Malwarebytes software is made possible thanks in part to many open source and third party projects. A requirement of many of these projects is that credit is given where credit is due. Information about each third party/open source project used in Malwarebytes software – as well as licenses for each – are available on the following page.

<https://www.malwarebytes.com/support/thirdpartynotices/>

Sample Code in Documentation

The sample code described herein is provided on an "as is" basis, without warranty of any kind, to the fullest extent permitted by law. Malwarebytes does not warrant or guarantee the individual success developers may have in implementing the sample code on their development platforms. You are solely responsible for testing and maintaining all scripts.

Malwarebytes does not warrant, guarantee or make any representations regarding the use, results of use, accuracy, timeliness or completeness of any data or information relating to the sample code. Malwarebytes disclaims all warranties, express or implied, and in particular, disclaims all warranties of merchantability, fitness for a particular purpose, and warranties related to the code, or any service or software related there to.

Table of Contents

Introduction	1
Server Architecture	2
Servers – Physical vs. Virtual	2
Server Hardware Requirements	2
Management Server	2
SQL Database Server	2
Server Connectivity	2
Active Directory OU Query Limitations	2
Server Installation	3
Management Server Identity	3
SQL Server vs. SQL Express	3
Policy Configuration	4
Planning Your Endpoint Configurations	4
Reducing Database Update Bandwidth	4
Endpoint Check-In Intervals	4
Emergency Maintenance	5
Management Server	5
SQL Server	5
Endpoint Log Cleanup	5
Endpoint Deployment	6
Endpoint Installations	6
Servers as Endpoints	6
Remote Clients Using Chained VPN Servers	6
Remote/Roaming Clients	6

Introduction

The purpose of this guide is to provide critical information pertaining to installation, operation and maintenance of *Malwarebytes Endpoint Security* in large corporate environments.

Systems operating in these environments face challenges which are unique and certain specifications must be tuned or altered to provide better system performance under the higher load encountered on a regular basis.

Companies using *Malwarebytes Management Console* in large environments may wish to consider using one Management Server for every 5,000 endpoints to maximize system performance. The Malwarebytes Licensing Agreement allows customers to install an unlimited number of Management Servers at no additional cost. Even when multiple Management Servers are used, tuning (as explained in this guide) is recommended to achieve the best results.

This guide is one of seven guides which make up the documentation set for *Malwarebytes Endpoint Security*. The full set is comprised of:

- *Endpoint Security Quick Start Guide*
- *Managing Malwarebytes in Large Networks Best Practices Guide*
- *Management Console Administrator Guide*
- *Endpoint Security Best Practices Guide*
- *Anti-Malware Unmanaged Client Administrator Guide*
- *Anti-Exploit for Unmanaged Client Administrator Guide*
- *Anti-Ransomware Administrator Guide*

We encourage you to become familiar with each of the guides. Each has been written to provide the reader with as much information as is possible with only as much content overlap as is necessary to provide continuity.

Server Architecture

This section details some basic information about integration of *Malwarebytes Endpoint Security* into your environment. We will build upon this as required to get you started on the right foot.

During installation, *Malwarebytes Endpoint Security* installs two components:

- **Management Server:** This is the central component of *Malwarebytes Endpoint Security*, and controls all communication with endpoints, the SQL Server data repository, user console, Active Directory, and optionally, the Malwarebytes update servers.
- **SQL Server:** This is the repository for all information about your endpoints, users, and security status. By default, Malwarebytes attempts to use a SQL Express database for storage. SQL Express is not suitable for large system environments. You should instead utilize a dedicated SQL Server.

Servers – Physical vs. Virtual

In an enterprise environment, Malwarebytes recommends that dedicated physical machines be utilized for servers associated with *Malwarebytes Endpoint Security*. Both the Management Server and SQL Server data repository may be heavily used, and dedicated physical machines help to assure minimum latency and maximum performance.

Server Hardware Requirements

As with many aspects of a large environment, *Malwarebytes Endpoint Security* also requires ample computing power to service its users and its endpoints. This is divided into two primary areas, as follows:

Management Server

The Management Server is responsible for all communications with all endpoints, as well as communication with the SQL data repository. Based on practical usage, you should utilize a dedicated server for the Management Server. In this role, the following hardware specification ranges are recommended depending on the number of endpoints to be serviced.

- **CPU:** 2 to 4 cores
- **RAM Memory:** 6 to 8 GB
- **Disk Space:** 500 GB, more space allows larger accumulation of log files

SQL Database Server

A dedicated SQL database server should be specified for use by *Malwarebytes Endpoint Security*. The SQL database server stores all security and system data associated with *Malwarebytes Endpoint Security*, and may sometimes be placed under a heavy load. By default, the Management Server deletes data older than ninety (90) days. In this case, 50-75 GB of disk allocated for use by SQL Server would serve your needs. *Malwarebytes Endpoint Security* does not archive data to external storage as part of its functionality, however security events can also be forwarded to a syslog server. If you wish to retain data longer than 90 days, you should gauge your own disk usage and change the default settings to fit your needs. Your corporate backup solution may be able to provide continuity for any data which exceeds the storage maximum that may be automatically deleted by the program.

Server Connectivity

Large environments will cause significantly more communication between the Management Server and the SQL Server data repository than will occur in smaller environments. To help alleviate bottlenecks, it is strongly recommended that both servers be in the same physical location, and should be served by gigabit (or better) networking.

Active Directory OU Query Limitations

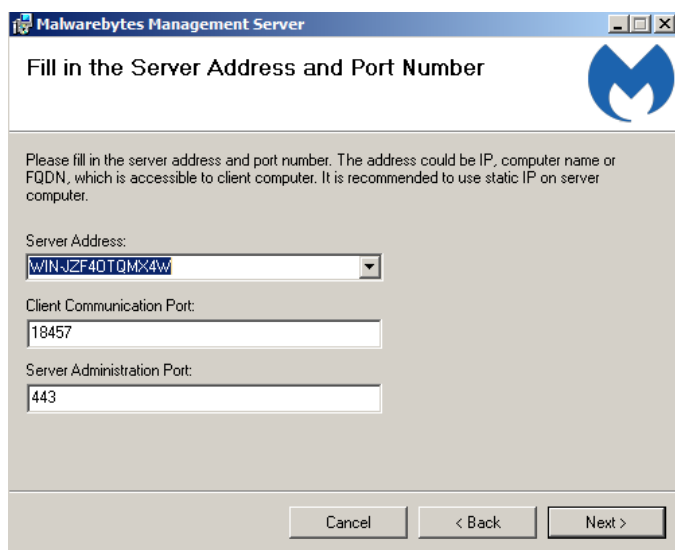
Microsoft has defined Active Directory response to LDAP queries so that no more than 5000 entries may be returned. If more than 5000 endpoints belong to a single Organizational Unit (OU), this may impact your ability to scan and/or install managed clients to the full number of endpoints based on the top-level OU. The Malwarebytes Administrator must take this limitation into account.

Server Installation

This section of the guide is limited in scope, as many installation requirements are covered in depth in the *Endpoint Security Best Practices Guide*. Only those items critical for large system deployment are covered here.

Management Server Identity

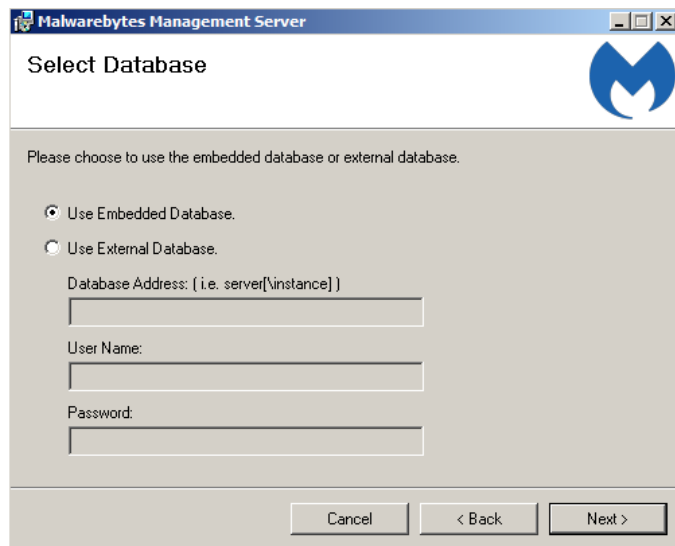
When a *Malwarebytes Anti-Malware* or *Malwarebytes Anti-Exploit* client is installed on an endpoint, the Internet identity (IP address, host name or Fully-Qualified Domain Name [FQDN]) of the Management Server is specified in configuration files. It is strongly recommended that the Management Server be installed on an endpoint which uses a Fully-Qualified Domain Name (FQDN). A host name or static IP address is also acceptable, providing that it remains constant. If you cannot use these specifications and must move your management server, please refer to page 49 of the *Management Console Administrator Guide* for information pertaining to online clients, and page 15 of the *Endpoint Security Best Practices Guide* for offline clients. The screenshot below depicts the Management Server installation step where this information is entered.



The screenshot shows a window titled "Malwarebytes Management Server" with a blue header and a logo. The main title is "Fill in the Server Address and Port Number". Below the title is a paragraph of instructions: "Please fill in the server address and port number. The address could be IP, computer name or FQDN, which is accessible to client computer. It is recommended to use static IP on server computer." There are three input fields: "Server Address" with a dropdown menu showing "WIN-JZF40TOMX4W", "Client Communication Port" with the value "18457", and "Server Administration Port" with the value "443". At the bottom are three buttons: "Cancel", "< Back", and "Next >".

If this cannot be done, use of a static IP address is also acceptable. If a static IP address is used and requires modification at a future date, you must contact Malwarebytes Technical Support for instructions on re-establishing contact between client and server.

SQL Server vs. SQL Express



The screenshot shows a window titled "Malwarebytes Management Server" with a blue header and a logo. The main title is "Select Database". Below the title is a paragraph of instructions: "Please choose to use the embedded database or external database." There are two radio buttons: "Use Embedded Database." (which is selected) and "Use External Database.". Below the radio buttons are three input fields: "Database Address: [i.e. server[instance]]", "User Name:", and "Password:". At the bottom are three buttons: "Cancel", "< Back", and "Next >".

When *Malwarebytes Endpoint Security* is installed, the default SQL data repository is Microsoft SQL 2008 Express. This is **not** suitable for a large system deployment **under any circumstances**. As mentioned previously, you should use a dedicated SQL server for *Malwarebytes Endpoint Security*. You may use Microsoft SQL Server 2008, SQL Server 2012 or SQL Server 2014, but please steer clear of SQL Express.

Policy Configuration

When it comes to *Malwarebytes Endpoint Security*, a significant amount of your network communications is directly related to endpoint policies, and the behavior dictated by those policies. The following guidance will help you to cut down on communication requirements.

Planning Your Endpoint Configurations

Every managed endpoint utilizes a policy to define its behavior, and that policy is set up and distributed by the Management Server. Every time a policy is updated and/or saved, it is distributed to endpoints governed by that policy. That results in network traffic. For this reason, we recommend that you read about policies, become familiar with the various policy screens, and if possible, define a cluster of endpoints which can serve as a testbed for policy experimentation. By doing this, you can make every policy change count and still maintain the highest network throughput possible.

Reducing Database Update Bandwidth

Definition updates provide the most updated protection for *Malwarebytes Endpoint Security* to use on your endpoints. There are two policy-driven methods of providing updated definitions to your endpoints. The default method is to receive incremental updates (roughly 3 kilobytes, *1/3000th the size of a full database update*) directly from the Internet update server. By assuring that only new definitions are downloaded, network bandwidth is significantly reduced. The second method is to receive updates from the Management Server, but that mode is limited to full database updates. The size of the full database update (approximately 9-12 megabytes) is magnified by the number of endpoints which must receive the update.

Endpoint Check-In Intervals

Policies dictate when endpoints check in with the Management Server for policy updates, definition updates, and commands issued via the Management Server. The default setting is continuously variable, from 5 seconds (50 or fewer online endpoints) to 100 hours (200,000 or more online endpoints). You may override the default settings with a user-specified value, though the default interval is designed to strike a good balance between network performance and your protection needs. Default check-in times are variable based upon the number of endpoints, but these defaults are designed with small and medium networks in mind. The following settings are recommended minimum check-in intervals for larger and distributed network environments.

Endpoints Served	Default Interval	Endpoints Served	Default Interval
1 — 50	5 seconds	30,001 — 40,000	12 hours
51 — 100	1 minute	40,001 — 50,000	18 hours
101 — 500	5 minutes	50,001 — 60,000	24 hours
501 — 2,500	10 minutes	60,001 — 75,000	30 hours
2,501 — 5,000	20 minutes	75,001 — 90,000	36 hours
5,001 — 7,500	30 minutes	90,001 — 125,000	48 hours
7,501 — 10,000	1 hour	125,001 — 150,000	60 hours
10,001 — 15,000	2 hours	150,001 — 175,000	72 hours
15,001 — 20,000	4 hours	175,001 — 200,000	88 hours
20,001 — 25,000	6 hours	200,001 — or more	100 hours
25,001 — 30,000	8 hours		

Emergency Maintenance

The purpose of this section is to highlight maintenance requirements which are brought on by unusual circumstances, and are exacerbated by the number of endpoints being serviced.

Management Server

During normal *Malwarebytes Endpoint Security* operations, there are numerous ongoing communications between the Management Server, protected endpoints, and the SQL Server data repository. Typical communications include policy distribution to endpoints, endpoint check-ins for policy and definition updates and endpoint event reporting, and SQL database updates. When more requests are made than can be serviced, the connection is dropped and an error is logged. In large installations, the sheer volume of errors which may be logged can compromise available disk space on the Management Server. Those log files can be found in the following folder:

```
c:\Windows\System32\LogFiles\HTTPERR
```

It is critical that the system administrator be aware of this Windows behavior and monitor this directory for rapidly accumulating log files, so that available disk space is not compromised. This data should be managed at your discretion.

SQL Database Server

A large-scale *Malwarebytes Endpoint Security* deployment will always result in significant disk space usage on your SQL Server database instance. We strongly recommend that system administrators periodically observe actual disk usage and record their findings for later comparison. By monitoring your actual usage – particularly the *TBL_ClientSecurityLog* table which keeps records of all detections on the endpoints – you can stay aware of conditions which may require intervention.

Endpoint Log Cleanup

The Management Server has the ability to purge information from its system database, and to purge client files which have been transmitted from endpoints to the server. However there is no built-in capability to remove XML log files which build up on the endpoint itself. If an endpoint is starting to run low on disk space, the following batch file can be executed on the endpoint to purge files older than `<days>` days.

```
forfiles -p "C:\ProgramData\Malwarebytes\Malwarebytes' Anti-Malware\Logs" -s -m *.*  
/D -<days> /C "cmd /c del @PATH"
```

Substitute `echo` for `del` to see results for yourself prior to deleting any files.

PLEASE NOTE: The path listed here is specific to *Malwarebytes Anti-Malware for Business*, versions 1.75 and 1.80. These are the only releases licensed for use in a business environment.

XML log files may accumulate on the endpoint if you encounter connectivity issues between the Management Server and managed clients, and may be compounded during a malware outbreak or false positive scenario. On a heavily-used endpoint, purging logs may prevent an outage caused by lack of disk space.

Endpoint Deployment

When it comes to deployment of *Malwarebytes Endpoint Security* onto an endpoint, there are few restrictions. This section details those restrictions, where you must create special settings, and where you must avoid installation.

Endpoint Installations

In large environments, we do not recommend push installation of *Malwarebytes Anti-Malware* or *Malwarebytes Anti-Exploit* clients directly from the Management Server. Installations are performed serially, which is generally more acceptable in smaller environments. Several excellent deployment methods exist which will serve your installation needs, including SCCM, Active Directory GPO, or other third-party management frameworks.

Servers as Endpoints

Experience has shown that installation of a *Malwarebytes Anti-Malware* client onto an endpoint running certain server software carries special conditions. We **strongly** recommend against deployment of *Malwarebytes Anti-Malware* client software onto virtual endpoints built on Terminal Services, RDP or Citrix client software. In addition, Malicious Website Blocking must be disabled if *Malwarebytes Anti-Malware* is being installed on an Exchange server.

OPERATING SYSTEM	Anti-Malware	Anti-Exploit	Anti-Ransomware	Anti-Rootkit	Windows Remediation	Management Server
Windows Server 2016 ^a	● ^{def}	●	■	◇	●	●
Windows Server 2012/2012 R2 ^a	● ^{def}	●	■	◇	●	●
Windows Small Business Server 2011	● ^{def}	●	■	◇	●	●
Windows Server 2008/2008 R2 ^a	● ^{def}	●	■	◇	●	●
Windows Server 2003/2003 R2 ^b	◇	●	■	◇	●	●
Windows 10	●	●	●	●	●	◇
Windows 8.1	●	●	●	●	●	◇
Windows 8.1	●	●	●	●	●	◇
Windows 7	●	●	●	●	●	◇
Windows Vista	●	●	■	●	●	◇
Windows XP ^{b,c}	●	●	■	●	●	◇

NOTES:
a - excludes Server Core installation option
b - 32-bit operating system only
c - Service Pack 3 required
d - Turn off Malicious Website Protection for Exchange Servers
e - Exclude Exchange Information Store from real-time protection
f - Exclude SQL database file(s) when SQL Server is installed

KEY to SYMBOLS
● Supported feature
■ Unsupported feature
◇ Untested

WINDOWS VIRTUAL ENVIRONMENT	Anti-Malware	Anti-Exploit	Anti-Ransomware	Anti-Rootkit	Breach Remediation	Management Server
Microsoft Terminal Services (TS)	■	◇	◇	◇	◇	◇
Microsoft Remote Desktop Services (RDS)	■	◇	◇	◇	◇	◇
Microsoft Hyper-V	●	●	●	●	●	●
Citrix XenDesktop	■	◇	◇	■	◇	◇
Citrix XenApp	■	◇	◇	■	◇	◇
VMware View	●	●	●	●	●	●
VMware Vshield	●	●	●	●	●	●
VMware Workstation	●	●	●	●	●	●

Remote Clients Using Chained VPN Servers

We have noticed that when multiple clients utilize a VPN server at a remote facility to connect to a VPN server at headquarters (i.e. VPN Server to VPN Server connection), there is confusion caused by multiple hostnames (endpoints) being associated with a single IP address and/or MAC address. The identity of the remote endpoint is masked because the IP/MAC of the *remote* VPN server which provides connectivity to headquarters is instead shown. In this case, we recommend that you follow the guidance shown in the

following section to properly identify and maintain the remote endpoint. This has no negative impact on protection of the remote endpoint, and allows the Management Server to maintain an accurate record of the remote endpoint's security status.

Remote/Roaming Clients

Large corporate customers typically support users connecting to the corporate network from both internal and external connections. If the user is not directly connected to the internal network, methods must be provided which guarantee that the user can receive database updates, policy updates, and can report the security status of their endpoint back to the Management Server.

One way to achieve this is through the use of VPNs. As long as roaming clients are connected to the internal network through the VPN, they will be able to communicate with the Management Server as intended.

Another method is illustrated in the following graphic. This method does not require VPN connectivity. In this scenario, the Management Server uses *mbmc.contoso.com* as its hostname, which is sent to each endpoint when *Malwarebytes Endpoint Security* is installed. Entries exist for this hostname in both internal and external DNS servers, though the IP address mapped to this server is different depending on which DNS server you are using. When the endpoint needs to contact the Management Server, a DNS lookup yields the public IP address for the corporate firewall. The firewall grants access to incoming requests on port 18457, and utilizes NAT (Network Address Translation) to route the connection request to the designated port on the Management Server.

