

Endpoint Security 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 for viewing here:

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
Pre-Installation	.2
External Access Requirements	2
Management Server Accessibility	2
Management Server Identity	. 2
Management Server Ports	. 2
Endpoint Accessibility	2
Managed Client Ports (Endpoint)	. 2
Remote Endpoint Accessibility	. 2
Removal of Unmanaged Malwarebytes Clients	.3
SQL Database Engine	3
SQL Express Size Limitations	. 3
Database Instance	. 3
SQL Express Instance Name	. 3
Database Authentication	. 3
Active Directory OU Query Limitations	.3
Installation	.4
Management Server	4
Internet Information Server (IIS) 7.5 Web Server	.4
SQL Express 2008	.4
Customer-Owned SSL Certificates	.4
Secondary User Interface	.5
Managed Client	5
Anti-Virus Programs and Exclusions	. 5
Managed Client Installation with WMI	. 6
Operation – Policy Module	.7
Auto Quarantine	7
Communication Settings	7
Remote Endpoints	.7
Use Groups to Maintain High Network Throughput	.7
Updater Settings	7
Database Updates – Full vs. Incremental	.7
Remote Endpoints	. 7
Planning for a Lack of Connectivity	. 8
Scan Scheduling	.8
Security Review	.8
Operation – Client Module	.9
Remote Endpoints	.9

## Table of Contents (continued)

Registration of Remote Endpoints	9
Periodic Check-In	9
Erratic/Unresponsive Status	9
Down-level Status	9
Weekly Status Review	9
Operation – Admin Module	10
Email Notifications – Threats	10
Email Notifications – Database Usage	10
Domain Query Account	11
Network Discovery in Large OU's	11
User/Administrator Guidelines	12
The Master Administrator is for Emergencies Only	12
New Users Should Start with Read-Only Status	12
Users and Windows Logon Status	12
Disable Inactive Users	
Periodic User Audit	
Maintenance	
Upgrades	
Moving Your Management Server	15
Install User vs. Upgrade User	16
Guarding Against Failures During Upgrades	16
Client Upgrades as part of Program Upgrades	16

# Introduction

The purpose of this document is to assist IT personnel and/or staff responsible for installation and maintenance of *Malwarebytes Management Console* in creating an operating environment that serves Malwarebytes needs while not causing disruption to your existing environment.

Information presented here is based on pre-installation planning as well as certain operational needs which are beyond the scope of the *Management Console Administrator Guide*. All recommendations are grouped by primary topic, and each is prefaced by a more focused topic. Nothing presented here is intended to replace troubleshooting procedures and techniques required to isolate and correct technical issues which may be encountered during normal operation.

*Malwarebytes Management Console* consists of three components, each providing a different function. Within the context of this guide, these components will be referred to as:

- Management Server: The web server, database server (embedded or external), and back-end product infrastructure
- Primary User Interface: The user interface which is installed on the same computer which hosts the Management Server
- Secondary User Interface: An auxiliary user interface which may be installed on one or more endpoints in your environment which are not serving as a host for the Management Server.

# **Pre-Installation**

This section of the guide provides information on topics that should be considered prior to installation of *Malwarebytes Management Console, Malwarebytes Anti-Malware* endpoint client and *Malwarebytes Anti-Exploit* endpoint client.

# **External Access Requirements**

If your company's Internet access is controlled by a firewall or other access-limiting device, you must grant access for *Malwarebytes Management Console* to reach Malwarebytes services. These are:

https://data.service.malwarebytes.org	port 443	outbound
https://data-cdn.mbamupdates.com	port 443	outbound
https://keystone.mwbsys.com	port 443	outbound

## **Management Server Accessibility**

The ability to install, manage and view status of Malwarebytes-protected endpoints is completely reliant on connectivity between Management Server, Management Console(s) and all endpoints. The following guidelines should be followed to achieve that goal.

### **Management Server Identity**

The Internet identity (IP address or Fully-Qualified Domain Name [FQDN]) of the management server is specified to *Malwarebytes Anti-Malware* and *Malwarebytes Anti-Exploit* managed clients when they are installed. Methods to change the identity at a later time may face limitations in the case of offline clients. It is strongly recommended that the management server be installed on a computer which uses a Fully-Qualified Domain Name (FQDN). 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, please refer to *Moving Your Management Server* (page 15).

#### **Management Server Ports**

Ports <u>443</u> and <u>18457</u> are required for communications between the Management Server and its Primary and Secondary Interfaces. In addition, port <u>18457</u> is required for communication with the managed client. These ports may be changed if you determine that these ports are unavailable in your environment. If either port is changed, unrestricted access is still required. If your company imposes firewall restrictions at the network level which affects internal traffic, restrictions must be relaxed for these two ports.

### **Endpoint Accessibility**

Endpoints which are to be protected and managed by *Malwarebytes Management Console* require certain settings to be modified. While some of these may be achieved by modification of Windows Firewall settings on the endpoint itself, others may be impacted by network security policies. Guidance is provided in the following instructions.

### Managed Client Ports (Endpoint)

Ports <u>135</u>, <u>137</u> and <u>445</u> must be accessible on all endpoints that will be home to a Malwarebytes managed client. These ports are used for automated installation of the managed client. These ports are typically available because they are used for Windows system processes, but access may be limited due to firewall restrictions at the network level. In addition, file sharing and NetBIOS must also be enabled on the endpoint. Please refer to page 6 of the *Management Console Administrator Guide* for instructions on how to enable these capabilities on each supported endpoint operating system. If these endpoint ports cannot be made available to the management server, all managed client installations must be performed manually.

#### **Remote Endpoint Accessibility**

Virtual Private Network (VPN) access is required for automated installation of managed clients on endpoints not based on the corporate LAN. In addition, VPN connectivity is required for remote endpoints to register their managed clients following installation as well as to report operational statistics to the server. Remote endpoints must also comply with the same port accessibility requirements as local endpoints.

# **Removal of Unmanaged Malwarebytes Clients**

If an unmanaged version of either *Malwarebytes Anti-Malware* or *Malwarebytes Anti-Exploit* has previously been installed on an endpoint, it must be uninstalled prior to installation of a managed client. Failure to do so may cause unexpected results in reporting.

# SQL Database Engine

*Malwarebytes Management Console* can utilize your existing Microsoft SQL database (SQL Server 2008/2012/2014/2016 or SQL Express 2008/2012/2014/2016), or a SQL Express 2008 database which is optionally installed as part of the management server installation process. In all cases, there are certain guidelines which should be followed.

### SQL Express Size Limitations

The embedded SQL Express database package bundled with *Malwarebytes Management Console* should only be used at sites with 200 or fewer endpoints. SQL Express has a maximum disk storage limitation of ten (10) gigabytes. Over an extended period of time, there is a possibility that you may reach this limit, particularly if your users encounter a large amount of malware. It is difficult to predict how much malware you may expect to encounter, or how long that SQL Express could serve your needs without danger of reaching its maximum allocation. It is always best to be cautious, and to plan for maximum reliability.

Management Console has capabilities to send notifications if database usage crosses a user-defined threshold. Please refer to *Additional Notification Settings* (page 62) of the *Management Console Administrator Guide* for further information.

#### **Database Instance**

A dedicated database instance should be utilized as a data repository for *Malwarebytes Management Console*. This applies to both SQL Server and SQL Express. This provides safeguards in case of data migration, data backups, and disaster recovery.

#### SQL Express Instance Name

If SQL Express 2005/2012/2014/2016 is running on the same server that *Malwarebytes Management Console* is to be installed on, it will already be using the SQLEXPRESS instance name (unless the default has been overridden at installation time). If this is the case, the SQL Express 2008 installed as part of the Malwarebytes installation must be configured to use a different instance name.

### **Database Authentication**

The SQL Administrator username associated with *Malwarebytes Management Console* operations must have full SQL security privileges. Many companies specifically forbid usage of the Microsoft-standard "SA" username, for good reason. Providing that an alternate username with the appropriate privileges is defined prior to installation of *Malwarebytes Management Console*, the Malwarebytes installer will allow this name to be associated with the database instance that will be used. We recommend that you grant *sysadmin* and *dbowner* privileges (at a minimum) to the username associated with Malwarebytes.

# 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 an OU structure, 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. Microsoft does allow a larger number of entries, but this must be configured by the Active Directory Administrator, and is specifically <u>not</u> recommended by Microsoft.

# Installation

Once your environment has been prepared for installation of *Malwarebytes Management Console*, you may proceed with the installation. Installation of the Management Server and Management Console components are relatively straight-forward, while some complexity is added for installation of managed clients on individual endpoints.

<u>Please note</u> that the <u>Server Core installation option</u> is specifically excluded from the list of supported operating systems for all program components (server, console, endpoint). This is due to the limited feature set available in this servers utilizing this option.

### **Management Server**

Installation of Management Server components is a simple process, but there is no room for error when installing (or connecting with an existing) database server. Please become familiar with requirements before performing the installation.

### Internet Information Server (IIS) 7.5 Web Server

Microsoft Internet Information Server (IIS) version 7.5 is required for operation of *Malwarebytes Management Console*, and is installed during the installation process. Many customers are also using other versions of IIS along with IIS 7.5 that is installed here. There have not been any reported conflicts.

#### SQL Express 2008

Microsoft SQL Express 2008 database server is installed as part of the *Malwarebytes Management Console* installation process <u>if</u> <u>needed</u>. If you wish to use an existing SQL Server or SQL Express implementation, you may bypass installation of SQL Express. To keep database installation simple, please refer to the previous page for information pertaining to instance names and user authentication.

### **Customer-Owned SSL Certificates**

Malwarebytes Management Console uses a generic SSL certificate that is associated with the IIS Express server installed during the installation process. If you have purchased a SSL certificate for use on this server, you can associate that certificate with Malwarebytes Management Console as well.

€	Default Programs		6	SSL Certificate	Configuration		x
Ć	Internet Explorer						
0	Windows Media Player			File name containin	g the certification:		
ē	Windows Update					Deserver	
	Accessories	administrator		J		browse	
	Administrative Tools	auministrator					
	FastStone Image Viewer	Documents		-Details			
	Maintenance	Jocamento					
J	Malwarebytes Management Server	Computer		Issued to:	localhost		
	🥌 Collect System Information	computer					
	📑 Data Backup and Restoration	Network		Issued by:	localhost		
	Malwarebytes Management Console Link						
	💓 Malwarebytes Management Console	Control Panel		Valid from:	8/22/2013 10:45:04 AM		
	Server Configuration						
	SSL Certificate Configuration	Devices and Printers		Valid to:	8/21/2023 5:00:00 PM		
J	Microsoft Network Monitor 3.4						
J	Microsoft Silverlight	Administrative Tools		Thumboriot:	C54602C61135B01BC4BC013B453BEEEACD668646		
J	Microsoft SQL Server 2008			manoprinti			
	Microsoft SQL Server 2008 R2	Help and Support		Dublic kow	DCA (1024 Pite)		
	Startup			Fublic Key.	KSA (102+bits)		
J	TechSmith	Run					
	D-di						
1	Dack				Import	Cancel	
5	earch programs and files	Log off					
1			_				_

The above screenshot (left panel) shows the Windows Start Menu link for **SSL Certificate Configuration**. Selecting this link will launch the dialog window shown in the right panel. Clicking **Browse...** allows you to navigate to the disk location where the certificate file is stored. You can then **Import** the file, and *Malwarebytes Management Console* will then be linked with your server's SSL certificate. <u>Please note</u> that the certificate must contain both a public and private key, and that it must have a .PFX file extension.

# Secondary User Interface

The primary user interface installs as a secondary process during *Malwarebytes Management Console* installation. You may wish to install a secondary user interface on another endpoint, allowing you to manage your Malwarebytes clients from a convenient location. You can download its installer from the Windows start menu (as shown below):



Once downloaded, the installer can be moved to the destination endpoint via USB drive, email attachment or storage on a shared network drive. Please note that this installer is for a secondary interface <u>only</u>. It does <u>not</u> include a server installer.

### Managed Client

The majority of requirements associated with installation of a managed client pertain to ports which must be accessible to the Management Server, as well as services which must be running on the endpoint. A few specifications remain, all of which must be handed at the time of installation.

### **Anti-Virus Programs and Exclusions**

**Malwarebytes Client:** Existing security software may attempt to block installation of Malwarebytes managed clients on an endpoint. This usually occurs with a new release of existing security software, though it may occur at any time depending on signatures used by existing software. If this does occur, add exclusions in that software so that it does not scan directories used by Malwarebytes software for installation and/or operation. While the need to add file exclusions is uncommon, the possibility does exist. Directories to be excluded are as follows:

- 64-bit Windows operating system:
  - C:\Program Files(x86)\Malwarebytes Anti-Exploit
  - C:\Program Files(x86)\Malwarebytes' Anti-Malware
  - C:\Program Files(x86)\Malwarebytes' Managed Client
  - C:\ProgramData\Malwarebytes
  - C:\ProgramData\sccomm
  - C:\Users\<*username*>\AppData\Roaming\Malwarebytes
- 32-bit Windows operating system:
  - C:\Program Files\Malwarebytes Anti-Exploit
  - C:\Program Files\Malwarebytes' Anti-Malware
  - C:\Program Files\Malwarebytes' Managed Client
  - C:\ProgramData\Malwarebytes
  - C:\ProgramData\sccomm
  - C:\Users\<username>\AppData\Roaming\Malwarebytes

The specific method of adding file exclusions varies from one product to another. Please consult user guides and/or on-line help for the software involved for assistance.

### Managed Client Installation with WMI

Depending on permissions settings on a target endpoint, you may encounter the following error message during a push install.

RPC server is unavailable. Please allow WMI through Windows Firewall.

If this occurs, open a command line window on the endpoint (as an administrator) and enter the following command:

#### netsh firewall set service RemoteAdmin enable

Installation should be able to continue as planned.

# **Operation – Policy Module**

Behavior of the *Malwarebytes Anti-Malware* and *Malwarebytes Anti-Exploit* managed clients on the endpoint itself are controlled by the Policy module. While all requirements can be easily defined on the tabs which make up this module, our experience with users in the field has led us to offer some additional guidelines here. These guidelines are designed to help maintain your network efficiency while also accomplishing program tasks. Settings mentioned here are unique to each customer's environment.

## Auto Quarantine

Auto Quarantine should be turned off for endpoints and users which are not considered high-risk. This will require knowledge of user habits as well as review of security software history associated with the endpoint/user in question.

# **Communication Settings**

Possibly the biggest issue that the Malwarebytes Administrator will face is determining the optimum settings for communication between the Management Server and managed clients. This is the key to efficient policy updates, database updates and continuing awareness of endpoint status.

#### **Remote Endpoints**

A remote endpoint must connect to the server at least once following installation of a Malwarebytes managed client, to enable the policy which has been assigned to the endpoint. This is typically not a problem with a local endpoint, but may be an issue with remote laptops and/or VPN-based clients who have received installation packages using means other than the *Malwarebytes Management Console*.

<u>Please note</u> that a remote endpoint that does not have connectivity to the Management Server is still being protected by its managed client. Because it is not connected to the Management Server, it is unable to inform the server of its current status. It also is collecting status logs locally until it is able to make connection with the Management Server and transfer those logs to the server. Depending on the amount of free disk space on the remote endpoint, this may create a maintenance issue.

### Use Groups to Maintain High Network Throughput

While it is important that Malwarebytes clients are equipped with the most current rules database, the database update process may cause some sites to experience network throughput issues. This can be minimized or eliminated through use of client groups, assignment of policies to client groups, and staggering of updates as part of the policy definitions assigned to clients and client groups. Experimentation may be required to achieve the desired results.

### **Updater Settings**

A key to Malwarebytes effectiveness in neutralizing threats is our ability to detect and remove zero-day infections. In large part, that is due to database updates which are available to all Malwarebytes subscribers. Your company must still assure that you can receive these updates when they are available. Let's look at a few non-standard conditions.

### Database Updates - Full vs. Incremental

Database updates provided by the server to the Anti-Malware client are full database updates (in the neighborhood of 12 megabytes). The **only** method by which a client receives incremental updates (roughly 3-8 kilobytes in size) is to download updates directly from the internet, which is the default setting for new installations. If a client requires more than fifty (50) incremental updates to become current, a full database update will be used instead. This requires less time and resources than processing and integration of the incremental updates.

### **Remote Endpoints**

Remote Malwarebytes clients must be configured to receive database updates over the Internet unless they are able to connect to the *Malwarebytes Management Console* via a VPN connection.

### Planning for a Lack of Connectivity

If a managed client loses connection to *Malwarebytes Management Console* for any reason, it is still protecting the endpoint which it is installed on. It cannot report detected threats or provide scan results while there is no server connection, and depending on *Updater Settings* in the policy assigned to the client, it may also be unable to update its rules database, which is essential to the protection that Malwarebytes provides. You may elect to have the endpoint download signature updates from the Internet if it is unable to reach your *Malwarebytes Management Console*. You may also use an alternate source (which you must specify and identify). As long as you have not experienced a loss of Internet connectivity, you are assured that your client is always protected with the most current information available.

### Scan Scheduling

All policies assigned to clients should assure that a detailed scan is performed at least once weekly.

### **Security Review**

Policies should be audited on a regular basis to assure that they continue to meet your security needs as well as the operational needs of your users.

# **Operation – Client Module**

The Client module allows the Malwarebytes Administrator to view the status of all managed endpoints, or only those endpoints which are part of a selected group. By selecting an individual client, more detailed status information is available in the bottom portion of the screen. If you do not take advantage of email notifications, this screen provides the first indication of a threat condition. The following guidelines assist you in making sure that this screen provides the most current information possible.

### **Remote Endpoints**

Remote endpoints pose special challenges when it comes to operation of a managed protection client. As has been documented previously, policies must accommodate the fact that the remote endpoint is not part of an environment which is connected at all times. This difference is also exhibited in the Client module.

### **Registration of Remote Endpoints**

Remote endpoints must connect to the server at least once following installation of Malwarebytes managed client software to enable the policy which has been assigned to the managed client. This is typically not a problem with endpoints based locally, but may be an issue with remote laptops and/or VPN-based endpoints who have received installation packages using means other than the *Malwarebytes Management Console*.

### Periodic Check-In

Remote clients who do not check in with the *Malwarebytes Management Console* once every thirty days will lose their status as an active client from the server's perspective. This does not mean that the endpoint is unprotected...the Malwarebytes client continues to function in its normal operating mode. The primary change is that the disconnected remote client's statistics and general health are unknown to the server. <u>Please note</u> that a remote client which usually operates without a persistent connection to the Malwarebytes server may generate unusually high network traffic when it is able to transmit operating logs to the Malwarebytes server. Once all logs have been uploaded, the network traffic level generated by this client will return to normal.

Please refer to *Remote/Roaming Clients* (page 7) of *Managing Malwarebytes in Large Networks Best Practices Guide* for suggestions and guidance on remote endpoint management.

### **Erratic/Unresponsive Status**

It is common for endpoints to exhibit erratic or unresponsive status if a managed client was installed over the top of a unmanaged client. Unmanaged clients should be uninstalled prior to installation of a managed client.

### **Down-level Status**

A client may be shown with a down-level database and/or policy after an upgrade to either. If this is the case, the cause may be because the client has not checked in with the server since the database update and/or policy update. They will continue to operate with older information until their scheduled check-in time.

<u>Please note</u> that multiple settings which pertain to clients are adjustable within the Policy Module, and not within the Client Module. Please refer to that section for further details. Certain information for clients is found there because settings are part of policies which are pushed out to clients.

## Weekly Status Review

Client status should be reviewed (at least) weekly to assure that clients are up-to-date with database updates.

# **Operation – Admin Module**

The Admin module controls information related to operation of Malwarebytes Management Console as a whole. Changes made here do not directly affect any managed client, though they will affect the ability of staff to manage clients.

# **Email Notifications – Throttling**

You may wish to use email notifications as a method of alerting IT and Security staff to threats detected on endpoints in your network. These threats may be your first indication of a more serious malware outbreak. They have now been incorporated into the user interface (*Admin*  $\blacktriangleright$  *Email Notifications*). You have control notifications about Malware and Exploits separately. An explanation of the Throttling tab will help you to use this to the best advantage. Let's look at the settings by example.

- Send a maximum of <a> notifications every <b> seconds.
- Pause <c> seconds between notifications.
- Display a maximum of <d> threats per notification.

Putting these parameters into perspective.....

<a></a>	<b></b>	<c></c>	<d></d>	EXPLANATION
5	600	120	100	Default Values. Keep tabs on general trends while you are learning
5	000	120	100	what your optimal settings should be.
-	000	190	10	Periodic Status. Keep tabs on general trends, sending an update every
5	900	180	10	five minutes.
500	1	0		Immediate Status!? Scheme is not practical because your email server
500	1	0	1	is overwhelmed by the volume of traffic you are sending it.
10	20		10	Malware Outbreak! Report on up too 100 threats each two seconds.
10	20	0 1 10		Quickly gather information and determine the best course of action.

It may take some time to find the right balance for your environment, but these examples should be able to help you move down that path.

### Email Notifications – Database Usage

Two database settings are not present in the Management Console user interface. They pertain to utilization of the system database. AlertMaxDatabaseLimit indicates the maximum storage allocation available in the SQL Express database instance (in bytes). AlertMaxDatabaseThreshold indicates the percentage of storage used as compared to maximum storage allocation. The default value is 70%.

The ability to manage endpoints with *Malwarebytes Management Console* ceases if maximum database allocation is reached, so it is critical to maintain free space in the system database. This feature is provided to assist users who do not have a database administrator (DBA) on staff, and is not meant to replace that staff role.

If you have upgraded from *Malwarebytes Enterprise Edition* (version 1.3 or earlier), these settings can be found in file:

C:\Program Files (x86)\Malwarebytes Enterprise Edition\SC.Server.WindowsService.exe.Config

If you installed Malwarebytes Management Console for the first time on version 1.4 or later, look for file:

C:\Program Files (x86)\Malwarebytes Management Server\SC.Server.WindowsService.exe.Config

In this XML configuration file, settings pertaining to notifications are at the bottom of the **<appSettings>** section. They are shown here:

<add key="AlertMaxDatabaseLimit" value="10737418240" />
<add key="AlertMaxDatabaseThreshold" value="70" />

After changes have been made to this configuration file, save the file and close it. While changes have been made, you must perform two final steps to make these changes go into effect. This should only be done during a quiet period or a maintenance period. First, exit *Malwarebytes Management Console*. Finally, use the <u>Windows Start Menu</u> to run **services.msc**. The Windows Services screen will be displayed as shown below.

File       Action       View       Help         Image: Services (Local)       Image: Services (Local)       Image: Services (Local)         Image: Max and the service Service Stop the service Service Service Service Service Service Service Detection Status       Started       Automatic       Local System         Description:       Automatic Service Service Service Service Service Service Detection Status       Started       Manual       Local System         Description:       Automatic Service Concellon Status       Started       Automatic Local System         Description:       Automatic Service Concellon Status       Started       Automatic Local System         Malware and Anti-Exploit       Grade Service Service Service Service Service Service Service Service Service Concellon Status       Started       Automatic Local System         Malware and Anti-Exploit       Grade Service Service Service Service Concellon Status       Started       Automatic Local System         Malware Service Malware Service Service Service Concellon Status       Started       Automatic Local System       Started         Malware Service Malware Service Service Concellon Status       Started       Automatic Local System       Started         Malware Service Service Service Concellon Service Concellon Service Concellon Service Concellon Service Started       Automatic Local System       Started       Automatic Local System         Mi	🖏 Services						_ 0	×
Image: Services (Local)         Mahwarebytes Management Service         Status       Startup Type       Log On As         Busice The service       Interactive Services Detection       Enables us         Description:       Altomatic Concellon Sharing (ICS)       Provides       Started         Altomatic network Service       Interactive Service Status       Provides       Started       Automatic       Local System         Allows central management and remote instalation of Maiwarebytes Anti- Melware and Anti-Exploit       Matwarebytes Maise       Cord Amaine       Started       Automatic       Local System         Allows central management and remote instalation of Maiwarebytes Maise       Maiwarebytes Maise       Cord Amaine       Started       Automatic       Local System         Allows central management and remote instalation of Maiwarebytes Maise       Maiwarebytes Maise       Maiwarebytes Maise	File Action View Help							
Services (Local)         Malwarebytes Management Service       Name       Description       Status       Startup Type       Log On As       A         Stop the service Restart the service       Stop the service Restart the service       Interactive Services Detection       Startup Type       Log On As       A         Description: Allows central management and remote installation of Malwarebytes Anti- Malware and Anti-Exploit       Interactive Services Detection       Finalles ne       Started       Automatic       Local System         Will Marker and Anti-Exploit       Interactive Service Colicy Agent       Interactive Service Marker       Automatic       Local System         Malware and Anti-Exploit       Projoles a       Started       Automatic       Local System         Malware for Management Service       Markerbytes Management Service       Started       Automatic       Local System         Malware and Anti-Exploit       Markerbytes Management Service       Allows central       Started       Automatic       Local System         Markerbytes Management Service       Markerbytes Management Service       Started       Automatic       Local System         Markerbytes Management Service       Markerbytes Management Service       Automatic       Local System         Markerbytes Management Service       Marosoft.NET Framework NGEN v2       Marcosoft.		à 🛃 🚺 📷 🕨 🔲 II IV 👘						
Name         Description         Status         Startup Type         Log On As           Service         Stop the service         The INEEX         Started         Automatic         Local System           Description:         Interactive Services Detection         Enables us         Manual         Local System           Description:         Interactive Services Detection         Enables us         Manual         Local System           Allows central management and remote installation of Malwarebytes Anti-Malwarebytes Anti-Malware and Anti-Exploit         Internet Connectors Sharing (ICS)         Provides a         Started         Automatic         Local System           Malware and Anti-Exploit         IP Bec Policy Agent         Internet Connectors Concernation         Started         Automatic         Local System           Malware bytes Anti-Malware bytes Anti-Malware bytes Anti-Malware bytes Management Service         On domain         Started         Automatic         Local System           Malware bytes Management Service         Started         Automatic         Local System         Local System           Malware bytes Management Service         Started         Automatic         Local System         Local System           Malware bytes Management Service         Started         Automatic         Local System         Local System	Services (Local)	🔕 Services (Local)						
Service       I/E and Auth/P IPsec Keying Modules       The IKEX       Started       Automatic       Local System         Stop the service       Interactive Services Detection       Enables u       Manual       Local System         Description:       Interactive Services Detection       Enables u       Started       Automatic       Local System         Allows central management and remote installation of Mulwarebytes Anti-Malware and Anti-Exploit       IP Helper       Provides a       Started       Automatic       Local System         Malware and Anti-Exploit       IP Helper       Provides a       Started       Automatic       Local System         Malware and Anti-Exploit       IP Helper       Provides a       Started       Automatic       Local System         Malware and Anti-Exploit       Interactive Services Management Service       Allows central management and remote installation of Mulwarebytes Management Service       Started       Automatic       Local System         Malwarebytes Management Service       Malwarebytes Management Service       Started       Automatic       Local System         Malwarebytes Management Service       Started       Automatic       Local System       Local System         Malwarebytes Management Service       Started       Automatic       Local System         Malwarebytes Manag		Malwarebytes Management	Name 🔺	Description	Status	Startup Type	Log On As	
Stop the service Restart the service       G. Interactive Services Detection       Enables us       Manual       Local System         Description: Allows central management and remote installation of Malwarebytes Anti- Malware and Anti-Exploit       Interactive Services Parti- G. Interactive Service Detection       Theraret Messaging       Enables us       Manual       Local System         Malware and Anti-Exploit       Interactive Service Detection       For domain       Started       Automatic       Local System         Malware and Anti-Exploit       Interactive Service Detection       On domain       Started       Automatic       Local System         Malware and Anti-Exploit       Interactive Service       On domain       Started       Automatic       Local System         Melwarebytes       Malwarebytes Management Service       Allows cent       Started       Automatic       Local System         Metasploit Worker       Started       Automatic       Local System       Markatic       Local System         Microsoft .NET Framework NGEN v2       Microsoft       Microsoft       Microsoft       Disabled       Local System         Microsoft Software Shadow Copy P.       Microsoft       Microsoft       Microsoft       Microsoft       Local System         Microsoft Software Shadow Copy P.       Manual       Local System       Micro		Service	🔍 IKE and AuthIP IPsec Keying Modules	The IKEEX	Started	Automatic	Local System	
Stop the service       Finternet Connection Sharing (ICS)       Provides n       Disabled       Local System         Description:       Allows central management and remote installation of Malwarebytes Anti- Malware and Anti-Exploit       Internet Connection Sharing (ICS)       Provides n       Started       Automatic       Local System         Malware and Anti-Exploit       Internet Started       Automatic       Local System       Automatic       Local System         Malware and Anti-Exploit       Internet Provides n       Started       Automatic       Local System         Malwarebytes Management Service       Condmain       Started       Automatic       Local System         Malwarebytes Management Service       Malwarebytes Management Service       Started       Automatic       Local System         Malwarebytes Management Service       Malwarebytes Management Service       Started       Automatic       Local System         Malwarebytes Management Network       Malwarebytes Management Network NGEN v2       Maretagolit Pro Service       Started       Automatic       Local System         Metasploit Worker       Started       Automatic       Local System       Matwarebytes Management NGEN v2       Microsoft       Disabled       Local System         Microsoft .NET Framework NGEN v2       Microsoft       Disabled <t< th=""><th></th><th></th><th>Interactive Services Detection</th><th>Enables us</th><th></th><th>Manual</th><th>Local System</th><th></th></t<>			Interactive Services Detection	Enables us		Manual	Local System	
Description:       Automatic       Local System         Allows central management and remote installation of Mawarebytes Anti- Malware and Anti-Exploit       IP Helper       Provides a       Started       Automatic       Local System         Malware and Anti-Exploit       IP Eace Policy Agent       Interrine Transaction       Coordinate       Started       Automatic       Network Service         Malware and Anti-Exploit       KmR for Distributed Transaction       Coordinate       Started       Automatic       Local System         Malware and Anti-Exploit       Malwarebytes Anti- Malwarebytes Management Service       Allows cent       Started       Automatic       Local System         Malwarebytes Management Service       Started       Automatic       Local System         Metasploit Pro Service       Started       Automatic       Local System         Metasploit Worker       Started       Automatic       Local System         Microsoft .NET Framework NGEN v4       Microsoft       Disabled       Local System		Stop the service	🔍 Internet Connection Sharing (ICS)	Provides n		Disabled	Local System	
Description: Alows central management and remote installation of Malwarebytes Anti- Malware and Anti-Exploit Malware and Anti-Exploit Malware and Anti-Exploit Malware and Anti-Exploit Malwarebytes Anti- Malware and Anti-Exploit Started Automatic Local System Metasploit Pro Service Metasploit Pro Service Metasploit Pro Service Metasploit Pro Service Metasploit Pro Service Metasploit Prostributed Transacton Coordinate Started Automatic Local System Manual Local System Manual Local System Mature Local System Mature Local System Metasploit Pro Service Metasploit Pro Service Metasploit Prostributed Transactor Started Automatic Local System Mature Local System Metasploit Pro Service Metasploit Pro Service Metasploit Prostributed Transactor Microsoft Microsoft .NET Framework NGEN v2 Microsoft Manual Local System Microsoft Manual Local System Microsoft Manual Local System Microsoft Manual Local System Microsoft Scil Initiator Service Microsoft Manual Local System Microsoft Manual Local System Microsoft Scil Initiator Service Microsoft Manual Local System Microsoft Scil Litiator Service Microsoft Manual Local System Manual Local System Manual Local System Manual Local System Manual Local System Manual Local System Microsoft Scil Litiator Service Microsoft Scil Litiator Servi			🔍 Intersite Messaging	Enables me	Started	Automatic	Local System	
Description: Allows central management and remote installation of Malwarebytes Anti- Malware and Anti-Exploit			🔍 IP Helper	Provides a	Started	Automatic	Local System	
Alons Certical Brain agent and Hender installation of Malwarebytes Anti- Malware and Anti-Exploit Automatic Automatic Council Automatic Automatic Council Automatic Council Automatic Council Automatic Council System Automatic Automatic Council Council Automatic Automatic Council System Automatic Council Council Automatic Council System Automatic Council System Metasploit Pro Service Metasploit Pro Service Metasploit Pro Service Metasploit Pro Service Metasploit Pro Service Metasploit PostgreSQL Microsoft .NET Framework NGEN V2 Microsoft Disabled Local System Microsoft .NET Framework NGEN V2 Microsoft Microsoft Microsoft Microsoft Manual Local System Microsoft SCSI Initiator Service Microsoft ScSI Initiator Service Manual Local System Manual Loca		Description:	🔍 IPsec Policy Agent	Internet Pr	Started	Automatic	Network Service	_
Malware and Anti-Exploit <ul> <li>KtmRm for Distributed Transaction Coordinate Started Linkt.ayer Topology Discovery Map Creates a Manual Local Service</li> <li>Malware and Anti-Exploit</li> <li>Metasploit Pro Service</li> <li>Started</li> <li>Automatic Local System</li> <li>Metasploit ProstresQL</li> <li>Started</li> <li>Automatic Local System</li> <li>Metasploit ProstresQL</li> <li>Started</li> <li>Automatic Local System</li> <li>Microsoft .NET Framework NGEN v2</li> <li>Microsoft</li> <li>Disabled</li> <li>Local System</li> <li>Microsoft .NET Framework NGEN v4</li> <li>Microsoft</li> <li>Microsoft .NET Framework NGEN v4</li> <li>Microsoft</li> <li>Microsoft</li></ul>		installation of Malwarebytes Anti-	Kerberos Key Distribution Center	On domain	Started	Automatic	Local System	
Link-Layer Topology Discovery Map       Creates a       Manual       Local System         Matasploit Pro Service       Allows cent       Started       Automatic       Local System         Metasploit Thin Service       Started       Automatic       Local System         Metasploit Thin Service       Started       Automatic       Local System         Metasploit Worker       Started       Automatic       Local System         Microsoft NET Framework NGEN V2       Microsoft       Disabled       Local System         Microsoft NET Framework NGEN V2       Microsoft       Disabled       Local System         Microsoft NET Framework NGEN V4       Microsoft       Disabled       Local System         Microsoft NET Framework NGEN V4       Microsoft       Automatic (D       Local System         Microsoft NET Framework NGEN V4       Microsoft       Automatic (D       Local System         Microsoft NET Framework NGEN V4       Microsoft       Automatic (D       Local System         Microsoft Rice Channel Platform R       Registers t       Manual       Local System         Microsoft Software Shadow Copy P       Manages s       Manual       Local System         Microsoft Software Shadow Copy P       Manages s       Manual<		Malware and Anti-Exploit	KtmRm for Distributed Transaction	Coordinate	Started	Automatic (D	Network Service	
Image: Started Automatic       Local System         Image: Started Automatic       Automatic         Image: Started Automatic       Local System         Image: Started Au			🔍 Link-Layer Topology Discovery Map	Creates a		Manual	Local Service	
Started       Automatic       Local System         Metasploit Thin Service       Started       Automatic       Local System         Metasploit Worker       Started       Automatic       Local System         Metasploit Worker       Started       Automatic       Local System         Microsoft NET Framework NGEN V2       Started       Automatic       Local System         Microsoft NET Framework NGEN V2       Microsoft       Disabled       Local System         Microsoft NET Framework NGEN V4       Microsoft       Automatic       Local System         Microsoft NET Framework NGEN V4       Microsoft       Automatic       Local System         Microsoft NET Framework NGEN V4       Microsoft       Automatic       Local System         Microsoft SCSI Initiator Service       Manual       Local System       Microsoft SiCSI Initiator Service         Microsoft SiCSI Initiator Service       Manual       Local System       Microsoft SiCSI Initiator Service       Manual       Local System         Microsoft SiCSI Initiator Service       Manual       Local System       Microsoft Service       Manual       Local System         Microsoft SiCSI Initiator Service       Manual       Local System       Microsoft Service       Manual       Local System         Microsoft Sic			🔍 Malwarebytes Management Service	Allows cent	Started	Automatic	Local System	
Metasploit Thin Service       Started       Automatic       Local System         Metasploit Worker       Started       Automatic       Local System         Metasploit Worker       Started       Automatic       Local System         Microsoft INET Framework NGEN V2       Microsoft       Disabled       Local System         Microsoft .NET Framework NGEN V2       Microsoft       Disabled       Local System         Microsoft .NET Framework NGEN V4       Microsoft       Automatic (D       Local System         Microsoft .NET Framework NGEN V4       Microsoft       Automatic (D       Local System         Microsoft .NET Framework NGEN V4       Microsoft       Automatic (D       Local System         Microsoft Ribre Channel Platform R       Registers t       Manual       Local System         Microsoft SicSI Initiator Service       Manual       Local System       Microsoft Software Shadow Copy P       Manual       Local System         Microsoft Software Shadow Copy P       Manual       Local System       Microsoft System       Microsoft Software Shadow Copy P       Manual       Local System         Multimedia Class Scheduler       Enables rel       Manual       Local System       Multimedia Class Scheduler       Enables rel       Disabled       Net.Wo			Metasploit Pro Service		Started	Automatic	Local System	
Image: Started Automatic Local System Started Automatic Local System Microsoft .NET Framework NGEN v2       Started Automatic Local System Disabled Local System Disabled Local System Of Microsoft .NET Framework NGEN v2         Image: Microsoft .NET Framework NGEN v2       Microsoft .NET Framework NGEN v2       Disabled Local System Disabled Local System Of Microsoft .NET Framework NGEN v4         Image: Microsoft .NET Framework NGEN v4       Microsoft .NET Framework NGEN v4       Microsoft .NET Coll System Of Microsoft         Image: Microsoft .NET Framework NGEN v4       Microsoft       Automatic (D Local System Of Microsoft Fibre Channel Platform R         Image: Microsoft Fibre Channel Platform R       Registers t       Manual Local System Of Microsoft SicSI Initiator Service Manages I         Image: Microsoft SicSI Initiator Service Manages S       Manual Local System Of Microsoft SicSI Initiator Service Manages S       Manual Local System Of Microsoft SicSI Initiator Service Or Manages S         Image: Microsoft Net Prep Listener Adapter       Receives a       Disabled Local Service Of Net.Trp Listener Adapter Receives a       Disabled Local Service Insabled Local			Metasploit Thin Service		Started	Automatic	Local System	
Started       Automatic       Local System         Microsoft .NET Framework NGEN v2       Microsoft       Disabled       Local System         Microsoft .NET Framework NGEN v2       Microsoft       Disabled       Local System         Microsoft .NET Framework NGEN v4       Microsoft       Disabled       Local System         Microsoft .NET Framework NGEN v4       Microsoft       Automatic (D       Local System         Microsoft .NET Framework NGEN v4       Microsoft       Automatic (D       Local System         Microsoft .NET Framework NGEN v4       Microsoft       Automatic (D       Local System         Microsoft fileCS1 Initiator Service       Manual       Local System       Microsoft Soft Ware Shadow Copy P       Manual       Local System         Microsoft Software Shadow Copy P       Manual       Local System       Microsoft Service       Manual       Local System         Microsoft Pipe Listener Adapter       Receives a       Disabled       Network Service       Net.Pipe Listener Adapter       Receives a       Disabled       Local Service         Net.Trp Listener Adapter       Receives a       Disabled       Local Service       V         Net.Trp Listener Adapter       Receives a       Disabled       Local Service       V <th></th> <th></th> <th>🔍 Metasploit Worker</th> <th></th> <th>Started</th> <th>Automatic</th> <th>Local System</th> <th></th>			🔍 Metasploit Worker		Started	Automatic	Local System	
Microsoft .NET Framework NGEN v2 Microsoft Disabled Local System     Microsoft .NET Framework NGEN v4 Microsoft Disabled Local System     Microsoft .NET Framework NGEN v4 Microsoft Automatic (D Local System     Microsoft .NET framework NGEN v4 Microsoft Automatic (D Local System     Microsoft .NET framework NGEN v4 Microsoft Manual Local System     Microsoft Size Channel Platform R Registers t Manual Local System     Microsoft Size Channel Platform R Registers t Manual Local System     Microsoft Size Channel Platform R Registers t Manual Local System     Microsoft Size Channel Platform R Registers t Manual Local System     Microsoft Size Channel Platform R Registers t Manual Local System     Microsoft Size Channel Platform R Registers t Manual Local System     Microsoft Size Channel Platform R Registers t Manual Local System     Microsoft Size Channel Platform R Registers t Manual Local System     Microsoft Size Channel Local System     Microsoft Size Channel Receives a Disabled Network Service     Net.Pipe Listener Adapter Receives a Disabled Local Service			metasploitPostgreSQL		Started	Automatic	Local System	
Microsoft .NET Framework NGEN v2       Microsoft       Disabled       Local System         Microsoft .NET Framework NGEN v4       Microsoft       Automatic (D       Local System         Microsoft .NET Framework NGEN v4       Microsoft       Automatic (D       Local System         Microsoft .NET Framework NGEN v4       Microsoft       Automatic (D       Local System         Microsoft Fibre Channel Platform R       Registers t       Manual       Local System         Microsoft SiCSI Initiator Service       Manages I       Manual       Local System         Microsoft Software Shadow Copy P       Manual       Local System         Multimedia Class Scheduler       Enables rel       Manual       Local System         Multimedia Class Scheduler       Enables rel       Manual       Local Service         Net.Msng Listener Adapter       Receives a       Disabled       Local Service         Net.Tcp Listener Adapter       Receives a			Microsoft .NET Framework NGEN v2	Microsoft		Disabled	Local System	
Microsoft .NET Framework NGEN v4 Microsoft Automatic (D Local System     Microsoft .NET Framework NGEN v4 Microsoft Automatic (D Local System     Microsoft Fibre Channel Platform R Registers t Manual Local System     Microsoft SiCSI Initiator Service Manages I Manual Local System     Microsoft Software Shadow Copy P Manages S Manual Local System     Microsoft Software Shadow Copy P Manages S Manual Local System     Microsoft Software Shadow Copy P Manages S Manual Local System     Mutimedia Class Scheduler Enables rel Manual Local System     Net.Msmq Listener Adapter Receives a Disabled Network Service     Net.Pipe Listener Adapter Receives a Disabled Local Service     Net.Tcp Listener Adapter Receives a Disabled Local Service     Net.Tcp Listener Adapter Receives a Disabled Local Service     Net.Pipe Listener Adapter Receives a Disabled Local Service     Net.Tcp Listener Adapter Receives a Disabled Local Service			Microsoft .NET Framework NGEN v2	Microsoft		Disabled	Local System	
Microsoft .NET Framework NGEN v4 Microsoft Automatic (D Local System     Microsoft Fibre Channel Platform R Registers t Manual Local System     Microsoft ISCSI Initiator Service Manages Manual Local System     Microsoft Software Shadow Copy P Manages Manual Local System     Microsoft Software Shadow Copy P Manages Manual Local System     Multimedia Class Scheduler Enables rel Manual Local System     Multimedia Class Scheduler Enables rel Manual Local System     More Multimedia Class Scheduler Enables rel Manual Local System     More Multimedia Class Scheduler Receives a Disabled Network Service     Net.Pipe Listener Adapter Receives a Disabled Local Service     Net.Pipe Listener Adapter Receives a Disabled Local Service     Net.Tcp Listener Adapter Receives a Disabled Local Service     Net.Tcp Listener Adapter Receives a Disabled Local Service     Net.Tcp Listener Adapter Receives a Disabled Local Service			Microsoft .NET Framework NGEN v4	Microsoft		Automatic (D	Local System	
Microsoft Fibre Channel Platform R Registers t Manual Local Service     Microsoft SCSI Initiator Service Manages I Manual Local System     Microsoft SCSI Initiator Service Manages S Manual Local System     Microsoft Software Shadow Copy P Manages S Manual Local System     Microsoft Software Shadow Copy P Manages S Manual Local System     Multimedia Class Scheduler Enables rel Manual Local System     Multimedia Class Scheduler Enables rel Manual Local System     Moltimedia Class Scheduler Receives a Disabled Network Service     Met.Pipe Listener Adapter Receives a Disabled Local Service     Net.Tcp Listener Adapter Receives a Disabled Local Service			Microsoft .NET Framework NGEN v4	Microsoft		Automatic (D	Local System	
Microsoft iSCSI Initiator Service Manages I Manual Local System     Microsoft iSCSI Initiator Service Manages S Manual Local System     Multimedia Class Scheduler Enables rel Manual Local System     Multimedia Class Scheduler Receives a Disabled Network Service     Net.Pipe Listener Adapter Receives a Disabled Local Service     Net.Tcp Listener Adapter Receives a Disabled Local Service			Microsoft Fibre Channel Platform R	Registers t		Manual	Local Service	
Microsoft Software Shadow Copy P Manages s Manual Local System     Multimedia Class Scheduler Enables rel Manual Local System     Multimedia Class Scheduler Receives a Disabled Network Service     Net.Msmq Listener Adapter Receives a Disabled Local Service     Net.Tcp Listener Adapter Receives a Disabled Local Service			Microsoft iSCSI Initiator Service	Manages I		Manual	Local System	
Multimedia Class Scheduler Enables rel Manual Local System     Net.Nsmq Listener Adapter Receives a Disabled Network Service     Net.Pipe Listener Adapter Receives a Disabled Local Service     Net.Tcp Listener Adapter Receives a Disabled Local Service     Net.Tcp Listener Adapter Receives a Disabled Local Service     Net.Tcp Listener Adapter Receives a Disabled Local Service			Microsoft Software Shadow Copy P	Manages s		Manual	Local System	
Avet.Msmq Listener Adapter     Receives a Disabled Network Service     Net.Pipe Listener Adapter     Receives a Disabled Local Service     Net.Tcp Listener Adapter     Receives a Disabled Local Service      Extended     Standard			🔅 Multimedia Class Scheduler	Enables rel		Manual	Local System	
Average And Average Avera			Net.Msmq Listener Adapter	Receives a		Disabled	Network Service	
Ketended / Standard /  Extended / Standard /		1	Net.Pipe Listener Adapter	Receives a		Disabled	Local Service	
Extended Standard /		1	🔍 Net.Tcp Listener Adapter	Receives a		Disabled	Local Service	-
		Extended Standard						-

Displayable areas have been resized here to improve readability. Find the service named **Malwarebytes Management Service**, rightclick to access the context menu and <u>Restart</u> the service. Once this has been completed, close the Services screen and launch *Malwarebytes Management Console*. This causes the configuration changes to take effect.

**WARNING:** This configuration file contains many system settings. It is not designed or intended for usage by customers. Endpoint protection may be impacted by direct modifications to this file. With the exception of the two settings shown in this section, please continue to make all system configuration changes through the Malwarebytes Management Console user interface.

# **Domain Query Account**

If you will be using *Malwarebytes Management Console* in an environment where operations are based on membership in Active Directory Organizational Units (OUs), you must define a domain query account that has access to endpoints listed in those OUs. This account is defined here. The account will typically be at the top of the tree, allowing access to all endpoints below it. If trust relationships exist within Active Directory, the domain query account may have access to endpoints outside of the immediate hierarchy. Before this account is defined, research should be undertaken to know exactly what resources the account ID does have access to.

## Network Discovery in Large OU's

If you are attempting to perform endpoint discovery under your top level Organizational Unit (OU), Active Directory security policies limit the response to the necessary LDAPQuery to 5000 endpoints. You cannot issue subsequent queries to retrieve remaining endpoints (those that were not returned in the initial query). The Active Directory administrator may change this policy (at his discretion), but it is not a recommended practice.

# **User/Administrator Guidelines**

*Malwarebytes Management Console* limits access to authorized users, and each authorized user is granted specific permissions by a *master* administrator. The following guidelines should be followed if possible.

### The Master Administrator is for Emergencies Only

The master administrator username should be used only for emergency purposes, and to initialize the process of creating users. Employees come and go, and you do not want to compromise your ability to manage your system by being unable to access it for any reason. You may also add new Administrators through use of the **Import AD User** option.

#### New Users Should Start with Read-Only Status

All usernames should be defined as read-only until you have had an opportunity to review proposed permission levels that should be defined for each user. You may also limit permissions through use of the **Groups Setting** tab.

Jser Permission				2
Permission Setting Groups Setting				
Template: Read-only User	•			
Client Administrator Policy Administrator System Administrator			E	kpand All
Scan Read-only User Power User	able	<li>O Disable</li>	Co	ollapse All
Update Database	C Enable	Oisable		
Restore Object	C Enable	O Disable		
Switch Policy	C Enable	O Disable		
Move to Group	C Enable	O Disable		
Remove Client	C Enable	O Disable		
Clear Client Log	C Enable	<li>Oisable</li>		
Client Group				
Add/Edit/Remove Client Group	C Enable	<li>Oisable</li>		
Policy				
Add/Edit/Remove Policy	C Enable	O Disable		
Set Default	C Enable	O Disable		
Create Installation Package	C Enable	<li>Disable</li>		
Change Priority	C Enable	O Disable	•	
			ОК	Cancel

#### **Users and Windows Logon Status**

If a Windows user's security settings specify "User must change password at next logon," they must change their password <u>before</u> they can login to *Malwarebytes Management Console*. They may be added as a Malwarebytes user, but they will be denied login privileges until the password change has taken effect.



### **Disable Inactive Users**

To avoid possible security risks, Users and Administrators who are on vacation/leave should be disabled for the duration of their absence.

🙌 Edit User	×
User Name:	* jsmith@contoso.com
	Example: ConsoleLogonName Domain\UserName Domain\GroupName UserName@Domain
	is user group in AD
Full Name:	* John Smith
Password:	*
Confirm Password:	*
Role:	C Administrator
	• User Permission
Email:	
Phone:	
	Enable
	OK Cancel

### Periodic User Audit

User rights should be audited on a regular basis, both in terms of permissions and as well as employment status.

# Maintenance

If the server on which *Malwarebytes Management Console* is installed runs out of disk space, all management and reporting operations will immediately cease. This could occur due to disk space as a whole, but will more likely be due to SQL Express reaching maximum disk allocation (ten gigabytes). Both characteristics should be monitored to prevent this from occurring. If disk usage trends indicate increasing disk usage, preparations should be made to allocate more disk, delete data based on aging, or migration from SQL Express to SQL Server. Should this occur before preventive measures can be taken, you should contact Malwarebytes Technical Support immediately. Please note that this does not affect the ability of your Malwarebytes managed clients to protect endpoints, but does stop their ability to report results and be managed by the *Malwarebytes Management Console*, and depending on update settings, may stop their ability to receive database updates.

# Upgrades

Upgrades sometimes present technical challenges. Whether those challenges are due to system limitations or program limitations, it is best to provide guidance that assist you in making the upgrade process as smooth as possible.

## Moving Your Management Server

When a managed client is installed on an endpoint, configuration files that are part of that installation identify the Management Server, using either its IP address or Fully Qualified Domain Name (FQDN). From that point on, that is how the client reports status, polls for policy changes, and receives database updates. If you move the Management Server from one server to another <u>and</u> the server's address or FQDN changes, the client is temporarily unaware of that change unless you checked the <u>Force Management Console Administrator Guide</u>, page 49) when changing the address of the Management Server.

Clients that are offline will remain unaware of the address change. In that situation, the following file on the affected endpoint must be modified to reflect the new address of the Management Server. That address is on line 10 of the file. The file is shown here in its entirety to assist you.

```
Endpoint file: C:\Program Files (x86)\Malwarebytes Managed Client\SCComm.exe.config
```

```
1
      <?xml version="1.0" encoding="utf-8"?>
 2
      <configuration>
 3
         <configSections>
            <section name="microsoft.web.services3"</pre>
 4
               type="Microsoft.Web.Services3.Configuration.WebServicesConfiguration,
               Microsoft.Web.Services3, Version=3.0.0.0, Culture=neutral,
                PublicKeyToken=31bf3856ad364e35" />
 5
         </configSections>
 6
         <runtime>
 7
            <generatePublisherEvidence enabled="false" />
 8
         </runtime>
 9
         <appSettings>
10
            <add key="remoteHost" value="https://WINSERVER2008R2:18457/SCClientService/" />
11
         </appSettings>
12
        <!-- WSE 3.0 settings -->
13
         <microsoft.web.services3>
14
            <diagnostics>
               <trace enabled="false" input="InputTrace.xml" output="OutputTrace.xml" />
15
               <detailedErrors enabled="false" />
16
            </diagnostics>
17
18
            <security>
19
               <timeToleranceInSeconds value="432000" />
20
               <defaultTtlInSeconds value="432000" />
21
            </security>
 22
         </microsoft.web.services3>
23
         <startup>
24
            <supportedRuntime version="v2.0.50727" />
25
         </startup>
26
      </configuration>
```

After changes have been made to this configuration file, save the file and close it. While changes have been made, you must perform one last step to make the change effective for that endpoint. Use the <u>Windows Start Menu</u> to run **services.msc**. The Windows Services screen will be displayed as a result. Find the service named **MEE Client Service**, right-click to access the context menu and <u>Restart</u> the service. Once this has been completed, close the Services screen. The endpoint will now be able to contact the Management Server.

If the old server is decommissioned and its IP address is reused, this should not be an issue. If the FQDN is reassigned to a new server **and** your DNS is updated to point to the new server, this also would not cause an issue.

# Install User vs. Upgrade User

If an upgraded version of *Malwarebytes Management Console* becomes available, it is critical that the Windows user who performed the installation also perform the upgrade, due to an issue with SQL Server/SQL Express database permissions. Please refer to the screenshots shown below.



The screenshot on the left is displayed if a different username is used during the upgrade, as compared to the original installation. After clicking **OK**, the screenshot on the right is displayed to inform you that the upgrade was halted due to the SQL permissions issue.

If a non-generic Windows username was used for the original installation, using the same name may not be possible if the user is no longer active. As an alternate approach, please refer to the Microsoft knowledge base article referenced here:

#### http://archive.msdn.microsoft.com/addselftosqlsysadmin/

This article explains the issue in detail, and links to a script which may be employed to circumvent the problem so that the upgrade may be performed as planned.

## **Guarding Against Failures During Upgrades**

An upgrade to a new version of *Malwarebytes Management Console* often includes modifications to database table structures and/or data necessary to make the transition from the old version to the new. A failure can occur during the upgrade, and depending on the nature of the failure (and when it occurs), the failure could leave the integrity of your data vulnerable. It is critical to backup your database instance to a separate location prior to performing the upgrade. If a failure does occur, you can restore your tables from this location, and assess the condition of your system and determine the next appropriate step.

## **Client Upgrades as part of Program Upgrades**

When *Malwarebytes Management Console* is upgraded from one version to another, this may include version upgrades of one or more managed clients. If a client (*Malwarebytes Anti-Malware* or *Malwarebytes Anti-Exploit*) is upgraded, the version of the client installed on an endpoint does not automatically get upgraded. Any client installations which occur <u>after</u> the upgrade will use the new client version, while previously installed clients retain the old version. If the new version contains new (or changed) features which you consider to be important for deployment on affected endpoints, you must install the new client over the top of the existing client. Page 22 of the *Management Console Administrator Guide* shows you how to easily determine which endpoints may be targets for new clients, and page 59 provides details on the client installation process.

**PLEASE NOTE:** When a managed *Malwarebytes Anti-Malware* client is upgraded to a new version, <u>the endpoint must be rebooted</u> to complete installation of the new program version.