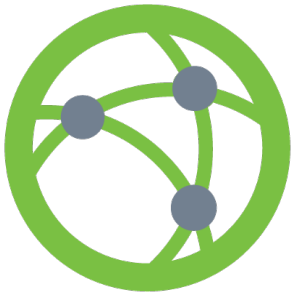


Malwarebytes
ENDPOINT
SECURITY

Endpoint Security
Best Practices Guide

Version 1.9

20 November 2018

Malwarebytes

Notices

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.

The Malwarebytes Protection Strategy

Malwarebytes' products incorporate several prevention features which utilize a layered defense strategy to protect you against malware threats which you face daily. Each layer is designed to disrupt the attack chain at a different stage. While all Malwarebytes products are highly effective in dealing with attacks that are becoming all too commonplace, we can only assure your protection when you take advantage of the full product suite, allowing each prevention layer to do the job they are best suited for.

It's your data. Protect it wisely!

Table of Contents

Table of Contents (continued)

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, *Malwarebytes Anti-Exploit* endpoint client, and the *Malwarebytes Anti-Ransomware* 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://*.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 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 **443** and **18457** are required for communications between the Management Server and its Primary and Secondary Interfaces. In addition, port **18457** 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 **135**, **137** and **445** 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 4 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 *Malwarebytes Anti-Malware*, *Malwarebytes Anti-Exploit,* or *Malwarebytes Anti-Ransomware* 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 60) 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 not 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 straightforward, while some complexity is added for installation of managed clients on individual endpoints.

Please note that the Server Core installation option 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

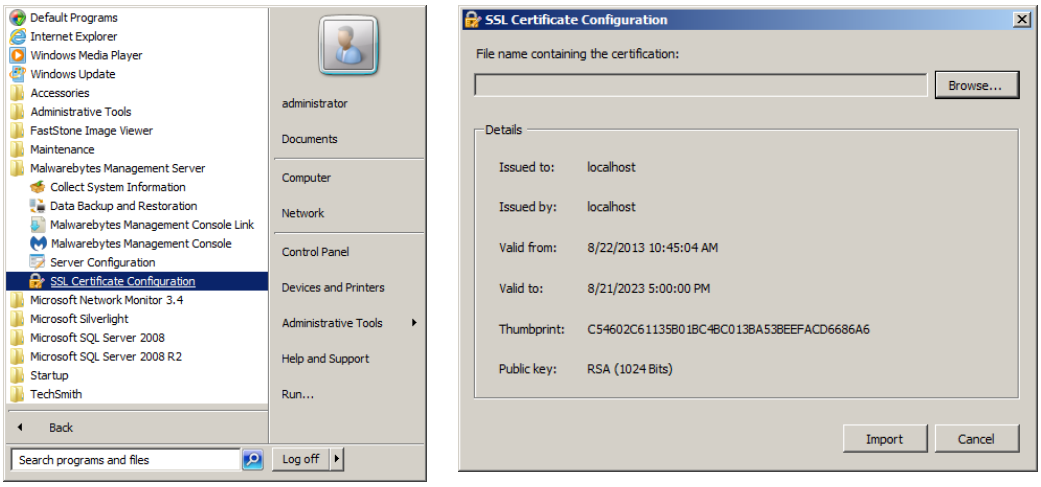
Microsoft Internet Information Server (IIS) version 7.5 is required for operation of *Malwarebytes Management Console*, and is installed during the installation process. Many customers are also using other versions of IIS along with IIS 7.5 that is installed here. There have not been any reported conflicts.

SQL Express 2008

Microsoft SQL Express 2008 database server is installed as part of the *Malwarebytes Management Console* installation process if needed. 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

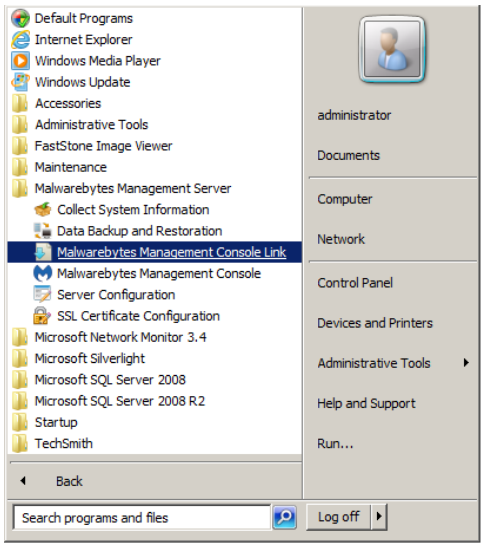
Malwarebytes Management Console uses a generic SSL certificate that is associated with the IIS Express server installed during the installation process. If you have purchased a SSL certificate for use on this server, you can associate that certificate with *Malwarebytes Management Console* as well.



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. **Please note** 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 only. It does not 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:

- All Client Operating Systems:
  - C:\Program Files\Malwarebytes
  - C:\ProgramData\Malwarebytes
  - C:\ProgramData\sccomm
  - C:\Users\<*username*>\AppData\Roaming\Malwarebytes
- 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
- 32-bit Windows operating system:
  - C:\Program Files\Malwarebytes Anti-Exploit
  - C:\Program Files\Malwarebytes' Anti-Malware
  - C:\Program Files\Malwarebytes' Managed Client

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*, *Malwarebytes Anti-Exploit,* and *Malwarebytes Anti-Ransomware* 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*.

Please note 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. **Please note** 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 6) 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.

Please note 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* ► *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>	<b>	<c>	<d>	EXPLANATION
5	600	120	100	Default Values. Keep tabs on general trends while you are learning what your optimal settings should be.
5	900	180	10	Periodic Status. Keep tabs on general trends, sending an update every five minutes.
500	1	0	1	Immediate Status!? Scheme is not practical because your email server is overwhelmed by the volume of traffic you are sending it.
10	20	1	10	Malware Outbreak! Report on up too 100 threats each two seconds. 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
```

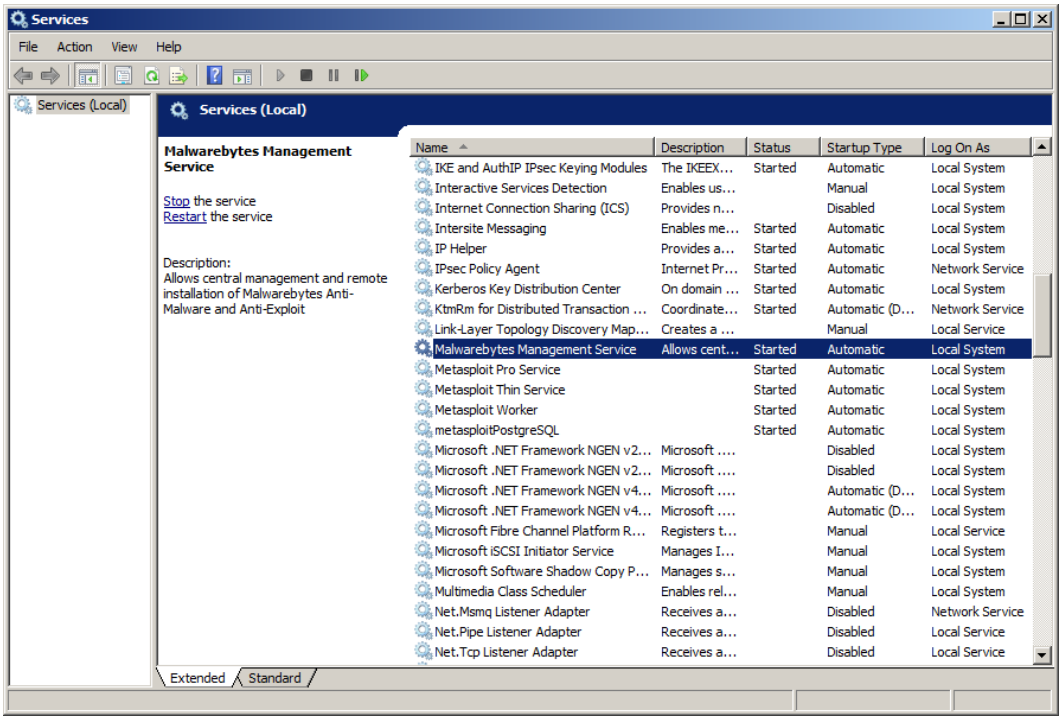
If you installed *Malwarebytes Management Console* for the first time on version 1.4 or later, look for file:

```
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 Windows Start Menu to run **services.msc**. The Windows Services screen will be displayed as shown below.



Displayable areas have been resized here to improve readability. Find the service named **Malwarebytes Management Service**, right-click to access the context menu and Restart 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

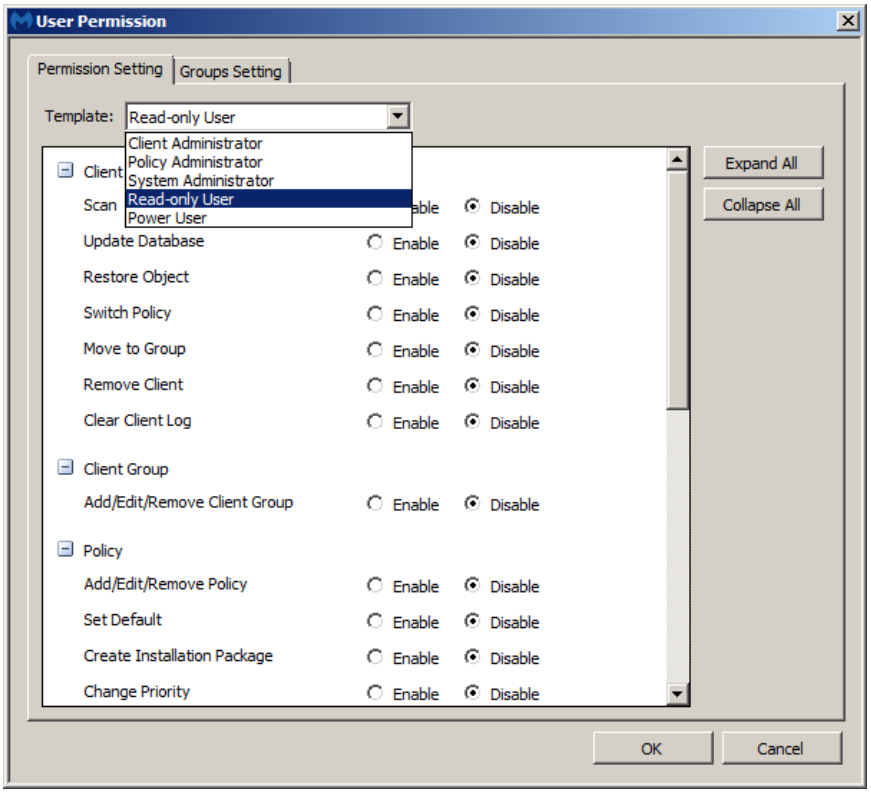
Malwarebytes Management Console limits access to authorized users, and each authorized user is granted specific permissions by a *master* administrator. The following guidelines should be followed if possible.

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.

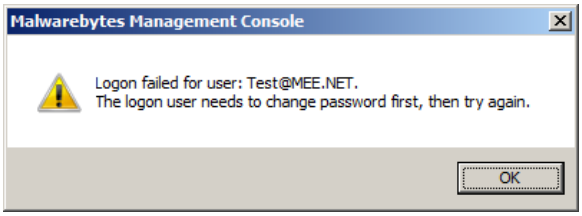
New Users Should Start with Read-Only Status

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.



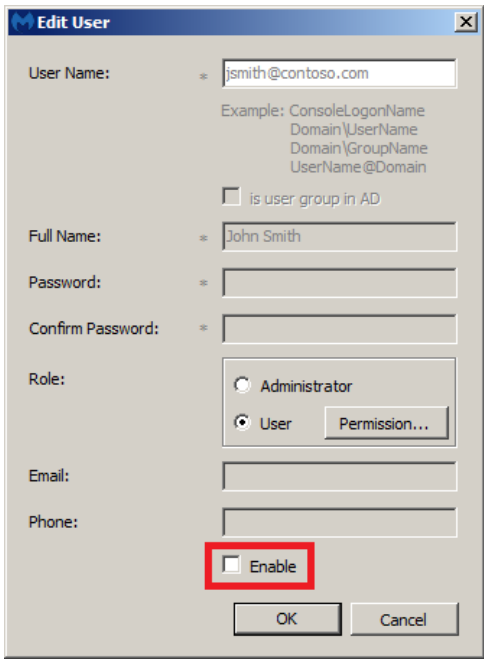
Users and Windows Logon Status

If a Windows user's security settings specify "*User must change password at next logon*," they must change their password before 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.



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 **and** the server's address or FQDN changes, the client is temporarily unaware of that change unless you checked the Force Managed Clients to use new address checkbox (see ***Management Console Administrator Guide***, 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

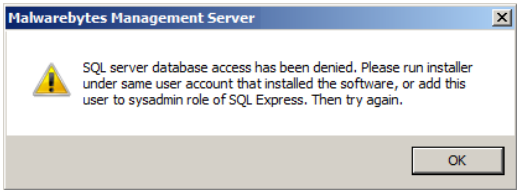
```
 1  <?xml version="1.0" encoding="utf-8"?>
 2  <configuration>
 3     <configSections>
 4        <section name="microsoft.web.services3"
              type="Microsoft.Web.Services3.Configuration.WebServicesConfiguration,
              Microsoft.Web.Services3, Version=3.0.0.0, Culture=neutral,
              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>
15           <trace enabled="false" input="InputTrace.xml" output="OutputTrace.xml" />
16           <detailedErrors enabled="false" />
17        </diagnostics>
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>
```

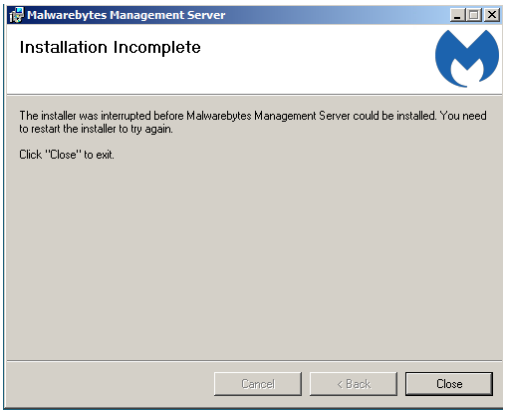
After changes have been made to this configuration file, save the file and close it. While changes have been made, you must perform one last step to make the change effective for that endpoint. Use the Windows Start Menu to run **services.msc**. The Windows Services screen will be displayed as a result. Find the service named **MEE Client Service**, right-click to access the context menu and Restart 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*, *Malwarebytes Anti-Exploit,* or *Malwarebytes Anti-Ransomware*) is upgraded, the version of the client installed on an endpoint does not automatically get upgraded. Any client installations which occur **after** 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 21 of the ***Management Console Administrator Guide*** shows you how to easily determine which endpoints may be targets for new clients, and page 55 provides details on the client installation process.

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