

Malwarebytes Enterprise Edition

Best Practices Guide

Version 1.3

21 March 2014



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 and Malwarebytes Enterprise Edition are trademarks of Malwarebytes Corporation. Windows, Internet Information Server, IIS, Active Directory, SQL Server and SQL Express are registered trademarks of Microsoft Corporation. All other trademarks or registered trademarks listed belong to their respective owners.

Copyright © 2014 Malwarebytes Corporation. All rights reserved.

Introduction

The purpose of this document is to assist IT personnel and/or staff responsible for installation and maintenance of Malwarebytes Enterprise Edition 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 *Malwarebytes Enterprise Edition System Administration 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.

Pre-Installation

MEE Client Ports: Ports 135, 137 and 445 must be accessible for installation of Malwarebytes Enterprise Edition client software on all endpoints. All ports are typically unassigned because they are used by Windows system processes, but they may be inaccessible due to firewall restrictions. If this is the case, endpoint firewall rules will need to be relaxed to satisfy this requirement. File sharing and NetBIOS must also be enabled on the endpoint.

MEE Server Ports: Malwarebytes Enterprise Edition server uses ports 443 and 18457 for operational communications. These ports must be available. If either of these ports are already in use at your site, you may specify alternate ports during product installation.

Remote Client Accessibility: Virtual Private Network (VPN) access is required for server-driven installation (push installs) of Malwarebytes Enterprise Edition on client computers not based on the corporate LAN. In addition, VPN connectivity is required for remote clients to register the client following installation as well as to report operational statistics to the server.

Client Preparation: If a standalone version of Malwarebytes Anti-Malware software has been installed on a client computer, it must be uninstalled prior to installation of a Malwarebytes Enterprise Edition client. Failure to do so will cause unexpected results in reporting.

Malwarebytes Server: The internet identity (IP address or Fully-Qualified Domain Name [FQDN]) of the Malwarebytes Enterprise Edition server is defined to the Malwarebytes client during client installation. There is no built-in method to change the identity at a later time. For this reason, it is strongly recommended that Malwarebytes Enterprise Edition 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, you must contact Malwarebytes Technical Support for instructions on re-establishing contact between client and server.

SQL Express: The embedded SQL Express database package bundled with Malwarebytes Enterprise Edition should only be used at sites with 200 or fewer client computers. 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.

SQL Express: If SQL Express 2005/2012 is running on the same server that Malwarebytes 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.

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

SQL Express/SQL Server: The SQL Administrator username associated with MEE 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 Enterprise Edition, 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: Microsoft has defined Active Directory response to LDAP queries so that no more than 1000 entries may be returned. If more than 1000 computers belong to an OU structure, this may impact your ability to scan and/or install Malwarebytes clients to the full number of computers 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 specifically configured by the Active Directory Administrator, and is not recommended by Microsoft.

Installation

Malwarebytes Server: Microsoft Internet Information Server (IIS) version 7.5 is required for operation of Malwarebytes Enterprise Edition, and is installed during the installation process.

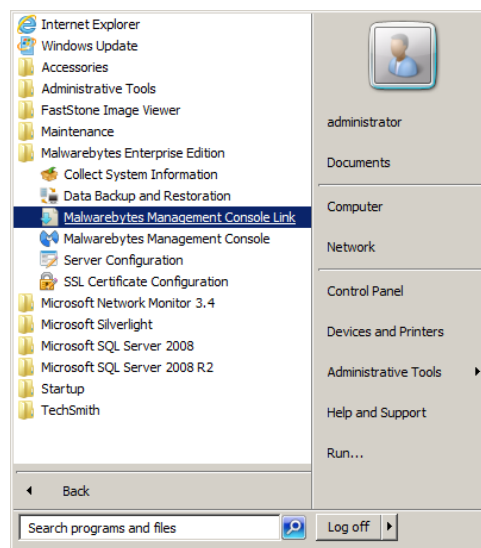
Malwarebytes Server: Microsoft SQL Express 2008 database server is installed as part of the Malwarebytes Enterprise Edition installation process. If customer elects to use a full SQL Server implementation, SQL Express may be uninstalled following Malwarebytes installation. There is no provision during installation to bypass installation of SQL Express.

Malwarebytes Client: Existing security software may attempt to block installation of Malwarebytes client software on a workstation. This usually occurs with a new release of the existing security software, though may occur at any time depending on signatures used by existing software. If this does occur, you should 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-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-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.

Management Console (secondary): The Malwarebytes Enterprise Edition Management Console (user interface) is installed as a secondary process during the Malwarebytes Server installation process. You may wish to install a second Management Console on another computer. If this is the case, you can download the Management Console installer from the Windows start menu (as shown below):



The Management Console installer does not include a Malwarebytes Enterprise Edition server installer.

Malwarebytes Client: Malwarebytes client software should not be installed on computers where a Malwarebytes Enterprise Edition server is installed.

Malwarebytes Client (with WMI): Depending on permissions settings on a target computer, you may encounter the following error message during a push install.

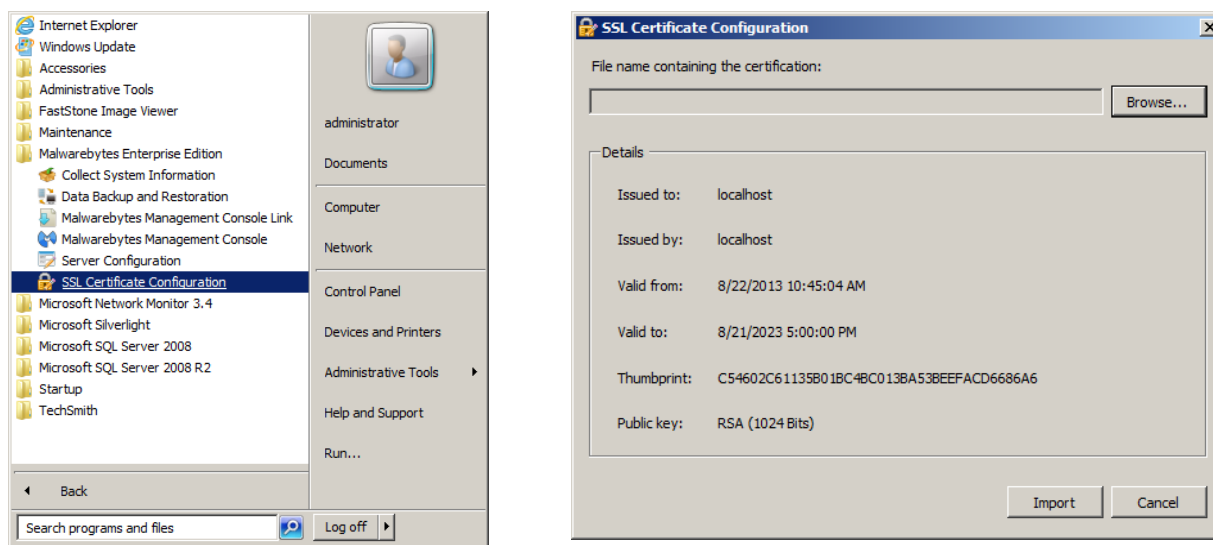
RPC server is unavailable. Please allow WMI through Windows Firewall.

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

```
netsh firewall set service RemoteAdmin enable
```

Installation should be able to continue as planned.

Customer SSL Certificate Usage: Malwarebytes Enterprise Edition uses a generic SSL certificate that is associated with the IIS Express server installed as part of the Malwarebytes installation process. If you have purchased a SSL certificate for use on this server, you can associate that certificate with Malwarebytes Enterprise Edition 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 Enterprise Server 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.

Malwarebytes Server Policy Module

Protection Settings: *Auto Quarantine* should be turned off for computers 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 computer/user in question.

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

Communication Settings: 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.

Communication Settings: In order to do database updates while maintaining high network availability, you may wish to consider optimizing update intervals – the repetition rate at which a client will poll for a new database update. Our experience is that many people choose *round numbers* to use in their policies. This helps, but only marginally. Multiples of round numbers end up resynchronizing at regular intervals, commonly leaving the customer with the same problem he was trying to avoid. The answer to this is using prime numbers for update intervals, because prime numbers are not multiples of any other smaller number. Let's use an example to demonstrate this...

A customer is using three policies, each with different update intervals.

- Policy #1 checks for updates every 5 minutes.
- Policy #2 checks every 7 minutes.
- Policy #3 checks every 11 minutes.

Assuming no delays:

- Policies 1 and 2 will coincide every 35 (5 x 7) minutes.
- Policies 1 and 3 will coincide every 55 (5 x 11) minutes.
- Policies 2 and 3 will coincide every 77 (7 x 11) minutes.
- All three policies will coincide every 385 (5 x 7 x 11) minutes.

More policies spread the time that all occur at the same time even further, as does using larger prime numbers. The key to making this work is assuring that only prime numbers are used for update intervals.

Updater Settings: If a Malwarebytes client loses connection to the server for any reason, it is still protecting the computer 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 download signature updates from the internet if you cannot reach your Malwarebytes Enterprise Edition server. As long as you have not experienced a loss of connectivity to the public internet, this assures that your client is always protecting you with the most current information available.

Updater Settings: Remote Malwarebytes clients must be configured to receive database updates over the internet unless they are able to connect to the Malwarebytes Enterprise Edition server via a VPN connection.

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.

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

Malwarebytes Server Client Module

Remote Clients: Remote clients must connect to the server at least once following installation of the Malwarebytes client software to enable the policy which has been assigned to the client. This is typically not a problem with a local client, but may be an issue with remote laptops and/or VPN-based clients who have received installation packages using means other than the Malwarebytes Enterprise Edition console.

Remote Clients: Remote clients who do not check in with the Malwarebytes Enterprise Edition server once every thirty days will lose their status as an active client from the server's perspective. This does not mean that the client 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 with the Malwarebytes server may generate unusually high network traffic as it transmits operating logs to the Malwarebytes server. Once all logs have been uploaded, the network traffic level generated by this client will return to normal.

Status Review: Client status should be reviewed weekly to assure that clients are up-to-date with database updates.

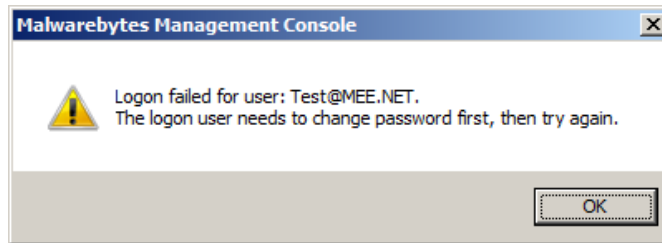
Client Communications: A client may be shown with a downlevel database and/or policy after an upgrade to either. If this is the case, the cause may be because the client has not checked in with the server since the database update and/or policy update. They will continue to operate with older information 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.

Malwarebytes Server Admin Module

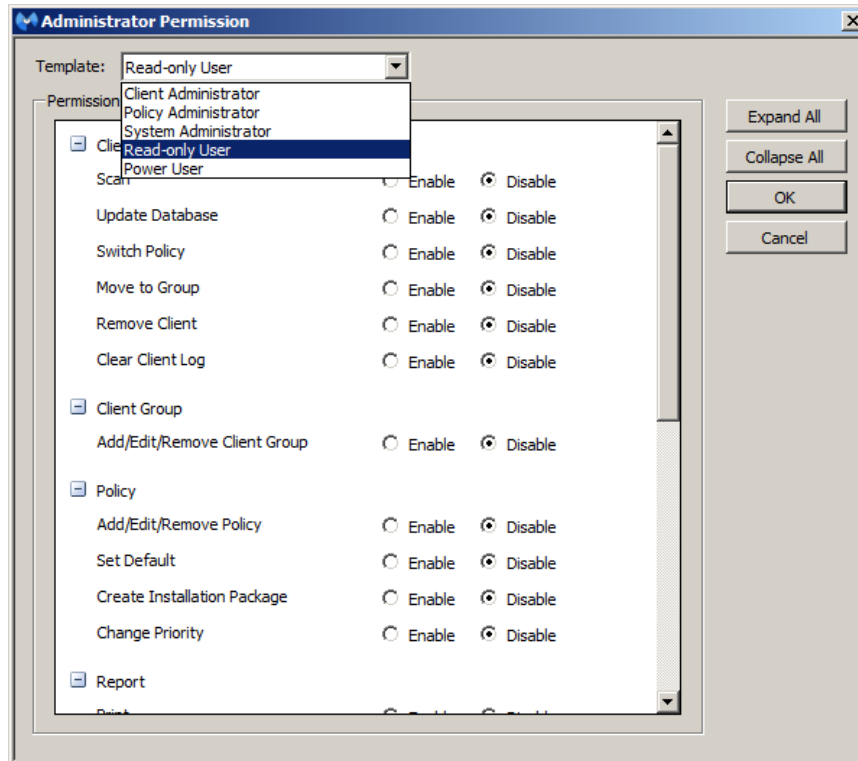
Domain Query Account (Other Settings): If you will be using Malwarebytes Enterprise Edition in an environment where operations are based on membership in Active Directory Organizational Units (OUs), you must define a domain query account that has access to computers listed in those OUs. This account is defined here. The account will typically be at the top of the tree, allowing access to all computers below it. If trust relationships exist within Active Directory, the domain query account may have access to computers 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.

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 Enterprise Edition. They may be added as a Malwarebytes user, but they will be denied login privileges until the password change has taken effect.



Client Push Install: If you are attempting to scan computers under your top level Organizational Unit (OU), Active Directory security policies limit the response to the necessary LDAPQuery to 1000 computers. You cannot issue subsequent queries to retrieve remaining computers. The Active Directory administrator may change this policy (at his discretion), but it is not a recommended practice.

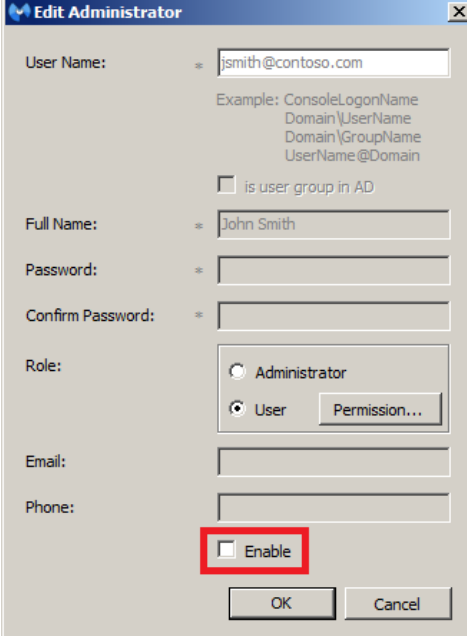
Add New Administrators: All Administrator usernames should be defined as read-only until you have had an opportunity to review to proposed permission levels that should be defined for each user.



An example of how to quickly set this permission level is shown above.

Add New Administrators: Additional Malwarebytes Administrators should be defined so that the master Administrator username is used only for emergency purposes. You may also add new Administrators through use of the **Import AD User** option.

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



The image shows a screenshot of the "Edit Administrator" dialog box. The dialog box has a title bar with a close button. It contains several fields and options:

- User Name:** A text box containing "jsmith@contoso.com". Below it, an example shows "ConsoleLogonName", "Domain\UserName", "Domain\GroupName", and "UserName@Domain".
- is user group in AD:** A checkbox that is currently unchecked.
- Full Name:** A text box containing "John Smith".
- Password:** A text box.
- Confirm Password:** A text box.
- Role:** A group box containing two radio buttons: "Administrator" (unchecked) and "User" (checked). A "Permission..." button is next to the "User" radio button.
- Email:** A text box.
- Phone:** A text box.
- Enable:** A checkbox that is currently unchecked and is highlighted with a red box.
- Buttons:** "OK" and "Cancel" buttons at the bottom.

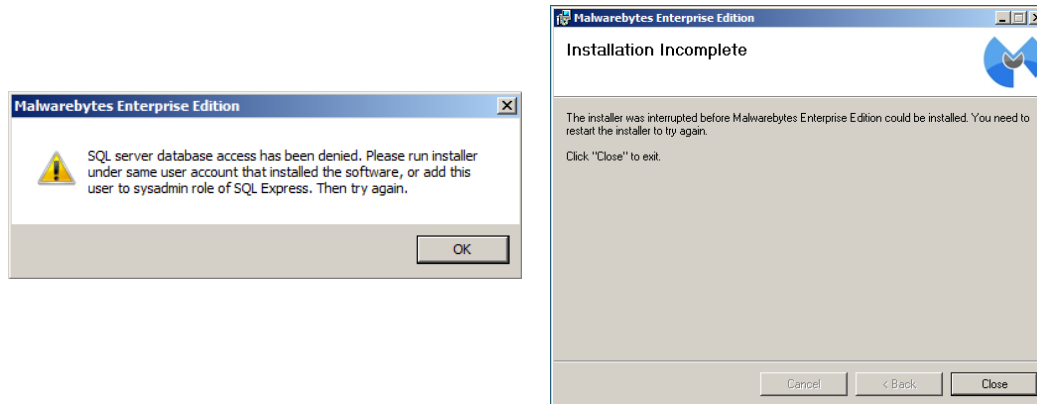
Security Review: Administrator rights should be audited on a regular basis.

Maintenance

Malwarebytes Server: If the Malwarebytes Server 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 client software to protect endpoints, but does stop their ability to report results and be managed by the Malwarebytes server, and depending on update settings, may stop their ability to receive database updates.

Upgrades

Malwarebytes Server: If an upgraded version of Malwarebytes Enterprise Edition 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/addselftoqlsysadmin/>

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.

SQL Server/SQL Express: An upgrade to a new version of Malwarebytes Enterprise Edition will include 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.