Malwarebytes
ENDPOINT SECURITY

Endpoint Security
Quick Start Guide

Version 1.8

21 March 2017

Malwarebytes

Notices

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

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

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

Copyright © 2017 Malwarebytes. All rights reserved.

Third Party Project Usage

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

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

Sample Code in Documentation

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

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

CWB10-1080a

Table of Contents

Laying the Groundwork 1
- Introduction 1
- Deployment & Management Options 1
- How to Choose the Correct Option for my Company 2
- Functionality Comparison 3
- System Documentation 3

Before You Begin 4
- System Requirements 4
  - Endpoint Clients (managed/unmanaged solution) 4
  - Servers and Primary Console (managed solution) 4
  - Secondary Console (managed solution) 5
- Making the Right Database Choice 5
- Preparing Endpoints for Managed Client Installation 7
- External Access Requirements 8
- Installing Management Server and Primary Console 8
- Installing a Secondary Console 10
- SSL Certificate Configuration (optional) 11
  - Verifying Presence of a Certificate 11
  - Exporting an Existing Certificate 11
  - Installing a Certificate 12

Preparations for Your First Install 13
- Defining the Basics 13
  - Domain Query Account (domain installation only) 13
  - Administrators / Users 13
  - Policies 16
  - Client Groups 17
- Discovery of Networked Computers 18
- Licenses for Purchases and Trials 19
- Installing Your First Client 20
  - Simulate Client Install 20
  - Client Push Install 20

Laying the Groundwork

Thank you for choosing Malwarebytes to protect your company from zero-day threats. *Malwarebytes Endpoint Security* is comprised of several clients designed to enhance the security of your network, your computers, and your users. We have created this Quick Start Guide to assist you in determining which specific clients you should install, and where.

Many administrators will be installing unmanaged versions of our protection clients, and do not need a central management console. Those users only need to read pages 1-7 of this guide. The remainder of the guide is designed to assist administrators of the managed version to perform installation, configuration and preparation steps so they can quickly take advantage of the protection *Malwarebytes Endpoint Security* provides.

Introduction

Malwarebytes Endpoint Security consists of the following solutions which provide protection against modern computing threats:

- ***Malwarebytes Anti-Malware for Business*** – Our award-winning Windows-based anti-malware client which detects and neutralizes zero-hour malware that most anti-virus products cannot even detect. Our real-time protection is designed to keep you safe against zero-hour malware through a combination of malware signatures and heuristic analysis. *Malwarebytes Anti-Malware* is available for managed and unmanaged environments.
- ***Malwarebytes Anti-Exploit for Business*** – This innovative technology analyzes, detects and neutralizes Windows-based vulnerability exploits based on their behavior. This signature-less technology uses 100% proactive techniques that evaluate *how* threats are introduced to the endpoint rather than *what* is introduced, eliminating the strategy which malware uses to bypass traditional endpoint security solutions. *Malwarebytes Anti-Exploit* is available for managed and unmanaged environments.
- ***Malwarebytes Management Console*** – This Windows-based centralized management tool combines the power of our award-winning Anti-Malware technology and our innovative patent-pending Anti-Exploit technology into a managed solution that provides the best protection against zero-hour malware and zero-hour exploits. Policy management and centralized reporting are also key features of *Malwarebytes Management Console*.

PLEASE NOTE: The following clients are licensed for use only by businesses who have purchased *Malwarebytes Endpoint Security*.

- ***Malwarebytes Anti-Ransomware –*** This Windows-based client guards against ransomware – the newest and most dangerous threat being faced today. This client continuously monitors the endpoint for ransomware behaviors, and blocks ransomware attacks before they can cause damage. This proprietary signature-less technology is capable of detecting unknown and future ransomware variants. This client cannot be centrally managed by *Malwarebytes Management Console*.
- ***Malwarebytes Anti-Rootkit –*** This Windows-based client detects and neutralizes malicious software designed to invisibly take control of your computer, and mask its presence from many protection products. This client cannot be centrally managed by *Malwarebytes Management Console*.
- ***Mac Remediation client –*** This client is designed to quickly detect and remove malware and adware from Mac OS X endpoints. Small in size, it can be easily deployed in your choice of GUI or command line (CLI) mode. This client cannot be centrally managed by *Malwarebytes Management Console*.

Deployment & Management Options

Most *Malwarebytes Endpoint Security* clients can be deployed in either Unmanaged mode or Managed mode. The ZIP archive which you received from Malwarebytes contains two sub-directories, which correspond to:

- ***Unmanaged:*** This deployment method consists of an EXE and MSI package which can be deployed manually across the network or via third-party network management agents. In addition, client protection can be managed via command line (*mbamapi.exe* or *mbae-cli.exe*) remotely, via network management agents, or by Active Directory GPO. Logging and reporting can be aggregated by unifying logs from endpoints and/or by submitting events to a Syslog server or SIEM.
- ***Managed:*** This method relies on the *Malwarebytes Management Console* to centrally deploy, manage and report on both Anti-Malware and Anti-Exploit managed clients. This method requires use of a Windows 2008/2012/2016 server as well as a SQL/SQL Express 2008/2012/2014/2016 database on the backend.

IMPORTANT NOTE:

NOTE 1: When deploying *Malwarebytes Endpoint Security* into environments of 10,000 or more endpoints, please refer to the ***Managing Malwarebytes in Large Networks Best Practices Guide*** for information which will assist you in your deployment efforts.
NOTE 2: The Endpoint Security ZIP archive contains additional programs which may be of value to you. MBAR.exe is our anti-rootkit client, and MBARW-Setup.exe is the installer for our new anti-ransomware client. They are mentioned here to prevent confusion later.

The screenshot shown here represents the structure of the *Malwarebytes Endpoint Security* ZIP archive which is delivered to the customer upon purchase. Technical documentation is contained in a subfolder under each folder.

How to Choose the Correct Option for my Company

All *Malwarebytes Endpoint Security* clients can be deployed and controlled either in Unmanaged mode or Managed mode. The overriding question is which mode (or combination thereof) is best for your company. Here are some scenarios and suggestions:

Who Should Use an Unmanaged Solution

- Small Office or Home Office environment with 2-10 computers. May have a file server, but may not be centrally managed in a domain.

  ► *Small offices operating standalone computers in a very small network (or no network).*

- Centralized network with existing comprehensive third-party network management solution and does not wish to introduce a second endpoint management system.

  ► *Large enterprises operating under control of scalable network management solution*

- Remote users without a central network

  ► *Retail businesses/franchises*

Who Should Use a Managed Solution

- Dedicated centralized solution to deploy, configure and report on all Malwarebytes endpoints

  ► *Small to medium size organizations with a single headquarters location*

- Centralized network without a reliable, high bandwidth or permanent dedicated connection or VPN tunnel to smaller remote office networks.

  ► *Organizations with headquarters location and regional offices*

- Centralized network, plus smaller satellite networks for remote offices which connect to the centralized network via a permanent dedicated connection or virtual private networking (VPN).

  ► *Organizations with headquarters location and regional offices*

Who Should Use a Hybrid Solution

- Centralized network plus remote users, or users that do not connect to the centralized network on a regular basis.

  ► *Schools/universities supporting facilities (classrooms/libraries/labs), staff and students*

Functionality Comparison

The following table addresses capabilities of clients, both managed and unmanaged.

UNMANAGED CLIENTS	Anti-Malware	Anti-Exploit	Anti-Ransomware	Anti-Rootkit	Mac Remediation
Discovery of endpoints on domain					
via Active Directory	■	■	■	■	■
via IP Scan	■	■	■	■	■
Automated Client Installation Methods					
Active Directory GPO	●	●	●	●	■
Third-Party Installers	●	●	●	●	●
Managed and Configured via Command Line	●	●	●	●	●
Deployment to Remote Endpoints	●	●	●	●	●
Customization of Client Behavior					
Remote (command line)	●	●	●	●	●
Remote (policies)	■	■	■	■	■
Local (user interface)	●	●	■	■	■
Scheduled Scans/Updates	●	■	■	■	■
Historical Data Retention					
Text files on endpoints	●	●	●	●	●
SQL data on server	■	■	■	■	■
Threat/Threat Trend Reporting (Syslog)	■	●	■	■	■

MANAGED CLIENTS	Anti-Malware	Anti-Exploit
Discovery of endpoints on domain		
via Active Directory	●	●
via IP Scan	●	●
Automated Client Installation Methods		
Malwarebytes Management Console	●	●
Active Directory GPO	●	●
Third-Party Installers	●	●
Managed and Configured via Command Line	■	■
Deployment to Remote Endpoints	■	■
Customization of Client Behavior		
Remote (command line)	■	■
Remote (policies)	●	●
Local (user interface)	■	■
Scheduled Scans/Updates	●	■
Historical Data Retention		
Text files on endpoints	●	●
SQL data on server	●	●
Threat/Threat Trend Reporting		
Malwarebytes Management Console	●	●
Syslog Integration	●	●

KEY to SYMBOLS	
●	Supported feature
■	Unsupported feature

System Documentation

In creating this guide, every attempt was made to include information that would provide a single reference source for the task at hand. That would also have turned this guide into a much larger document. As a result, there are references to other system documentation within this guide. The following is a list of all documentation which supports *Malwarebytes Endpoint Security*.

- Endpoint Security Quick Start Guide *(all modes)*
- Management Console Administrator Guide *(managed mode)*
- Endpoint Security Best Practices Guide *(managed mode)*
- Managing Malwarebytes in Large Networks Best Practices Guide *(managed mode)*
- Anti-Malware Unmanaged Client Administrator Guide *(unmanaged mode)*
- Anti-Exploit Unmanaged Client Administrator Guide *(unmanaged mode)*
- Anti-Ransomware Administrator Guide *(unmanaged mode)*
- Mac Remediation Client Administrator Guide *(unmanaged mode)*

Before You Begin

By taking a systematic approach to installation and configuration of *Malwarebytes Endpoint Security*, it is simple to come up to speed so that you receive the level of security which you expect. This section includes minimum system requirements for all components of *Malwarebytes Endpoint Security*, for both managed and unmanaged solutions.

System Requirements

Each component of *Malwarebytes Endpoint Security* has system requirements which must be met for installation and operation. Requirements for an unmanaged solution are simple, while a managed solution introduces complexity. For each, please consult the appropriate guide for full system requirements.

Endpoint Clients (managed/unmanaged solution)

Endpoint clients provide security functionality on the endpoint computer. In a managed solution, they receive commands from the Management Server (issued by the administrator from a primary/secondary console). Status is returned to the Management Server, which processes results and provides visible notification to the administrator. In an unmanaged solution, the endpoint client is autonomous – it executes only commands which have been issued locally.

- **Hardware (Windows)**
  - CPU: 1 GHz
  - RAM: 1 GB (client); 2 GB (server)
  - Disk space: 100 MB (program + logs)
  - 800x600 screen resolution
- **Software (Windows)**
  - .NET Framework 3.5
  - Windows Installer 4.0
- **Operating Systems (Windows)**
  - Windows Server 2016 (excludes Server Core installation option)
  - Windows Server 2012/2012 R2 (excludes Server Core installation option)
  - Windows Small Business Server 2011
  - Windows Server 2008/2008 R2 (excludes Server Core installation option)
  - Windows Server 2003 (32-bit only)
  - Windows 10
  - Windows 8.1
  - Windows 8
  - Windows 7
  - Windows Vista
  - Windows XP with SP3 (32-bit only, not supported for anti-ransomware client)
- **Hardware (Mac)**
  - Equivalent to OS X 10.9 minimum (validated by Apple at time of upgrade)
- **Software (Mac)**
  - no additional requirements
- **Operating Systems (Mac)**
  - OS X 10.9 or better

If you are utilizing an unmanaged solution, you do not need to continue reading the remainder of this guide.

Servers and Primary Console (managed solution)

Malwarebytes Management Console provides all system functionality via its Management Server. It provides all necessary Windows services, and communicates directly with both primary and optional secondary console(s), as well as managed endpoints. It runs strictly in the background. The Management Server and Database Server may both be installed on the same physical machine, or they may be installed separately. Both are required, but the implementation decision is the responsibility of the customer based on expected load and capabilities of the server(s) in question. Please note that the Management Server and Primary Console may only be used on Windows-based machines.

- **Hardware**
  - CPU: 1 GHz minimal, dual core 1.6 GHz recommended
  - RAM: 1 GB minimal, 2 GB recommended
  - Disk space: 2 GB minimal, 10 GB recommended
  - 1024x768 screen resolution
- **Software**
  - Windows Installer 4.5
  - .NET Framework 4
- **Supported Operating Systems**
  - Windows Server 2016 (excludes Server Core installation option)
  - Windows Server 2012/2012 R2 (excludes Server Core installation option)
  - Windows Small Business Server 2011
  - Windows Server 2008/2008 R2 (excludes Server Core installation option)
- **Supported Microsoft SQL Servers**
  - Database embedded: Microsoft SQL Server 2008, 2012, 2014, 2016 Express (10 GB maximum database size limitation)
  - Databases supported: Microsoft SQL Server 2008/2008 R2, 2012, 2014, 2016

Secondary Console (managed solution)

The primary and secondary console(s) provide all interaction with the Management Server, and direct interactions with managed endpoints. The primary console resides on the same computer as the management server. Specifications listed here are for a secondary console, which may also be a managed endpoint (if it is not a server-class machine). Please note that the Management Server and Primary Console may only be used on Windows-based machines.

- **Hardware**
  - CPU: Core Duo 1.6 GHz
  - RAM: 1 GB RAM
  - 1024x768 screen resolution
- **Software**
  - .NET Framework 4.0
  - Windows Installer 4.5
- **Supported Operating Systems**
  - Windows Server 2016 (excludes Server Core installation option)
  - Windows Server 2012/2012 R2 (excludes Server Core installation option)
  - Windows Small Business Server 2011
  - Windows Server 2008/2008 R2 (excludes Server Core installation option)
  - Windows Server 2003 (32-bit only)
  - Windows 10
  - Windows 8.1
  - Windows 8
  - Windows 7
  - Windows Vista
  - Windows XP Pro with SP3 (32-bit only)

Making the Right Database Choice

Microsoft SQL Express database server is installed by default as part of *Malwarebytes Management Console* installation unless you elect to utilize an existing Microsoft SQL Server/SQL Express database instance. If you do not use an existing Microsoft SQL Server installation, you must consider the number of endpoints to be protected and the level of risk which your endpoints encounter. SQL Express is limited in terms of data retention, and Malwarebytes does not recommend using this database solution for more than 200 endpoints.

Please refer to page 3 of the *Endpoint Security Best Practices Guide* for more complete information pertaining to database selection criteria.

Preparing Endpoints for Managed Client Installation

A few changes to endpoint configuration must be implemented to facilitate installation of a Malwarebytes managed client to those endpoints. Different preparation methods are required for each operating system, so they are grouped here by operating system.

- **Windows Server 2003/2008/2008 R2/SBS 2011/2012/2012 R2/2016 endpoint preparation**
  - From the Windows Start Menu, launch Control Panel
  - Launch Network and Sharing Center by double-clicking on its icon
  - Select Change advanced sharing settings from the menu on the left side of the screen
  - Click the arrow to the right of All Networks or Domain. (dependent on network environment)
  - Turn on Network discovery, File sharing and Printer sharing.
  - Click the Save changes button
  - Close the Control Panel screen.
  - Launch Server Manager by clicking its Icon
  - Select Administrative Tools
  - Select Add Feature
  - Select .Net 3.5 – Continue through the installation
  - **WORKGROUP ONLY:** Enable the built-in administrator account by opening a command prompt as administrator, and typing the following command:

    ```
    net user administrator /active:yes
    ```

- **Windows 7/8/8.1/10 endpoint preparation**
  - From the Windows Start Menu, launch Control Panel
  - Launch Network and Sharing Center by double-clicking on its icon
  - Select Change advanced sharing settings from the menu on the left side of the screen
  - Click the arrow to the right of All Networks or Domain (dependent on network environment).
  - Turn on Network discovery, File sharing and Printer sharing.
  - Click the Save changes button
  - Close the Control Panel screen.
  - **WORKGROUP ONLY:** Enable the built-in administrator account by opening a command prompt as administrator, and typing the following command:

    ```
    net user administrator /active:yes
    ```

- **Windows Vista endpoint preparation**
  - From the Windows Start Menu, launch Control Panel
  - Launch Network and Sharing Center by double-clicking on its icon
  - In the section titled *Sharing and Discovery*, turn on Network discovery, File sharing and Printer sharing.
  - Close the Control Panel screen.
  - **WORKGROUP ONLY:** Enable the built-in administrator account by opening a command prompt as administrator, and typing the following command:

    ```
    net user administrator /active:yes
    ```

- **Windows XP endpoint preparation**
  - From the Windows Start Menu, launch Control Panel.
  - Launch Windows Firewall by double-clicking on its icon.
  - Click the *Exceptions* tab.
  - Check the checkboxes for *File and Printer Sharing*.
  - Click *OK* to close the Windows Firewall screen.
  - Launch *Administrative Tools* by double-clicking on its icon.
  - Launch *Local Security Policy* by double-clicking on its icon. The Local Security Settings screen will open.
  - Click on *Local Policies* in the left panel. The main panel will refresh to show relevant settings.
  - Scroll down to *Network access: Sharing and security model for local accounts*. Double click on this setting.
  - Change the value to *Classic – local users authenticate as themselves*.
  - Click *OK* to make the change effective.
  - Close the Local Security Settings window.
  - Close the Administrative Tools window.

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

Installing Management Server and Primary Console

Malwarebytes Management Console is provided to customers in the *Malwarebytes Endpoint Security* ZIP archive. Please refer to pages 1-2 for an introduction to the layout of the ZIP file. After extracting the *Malwarebytes Management Console* installer from the ZIP file, you may begin installation. The steps shown below are the only ones that may not be self-explanatory.

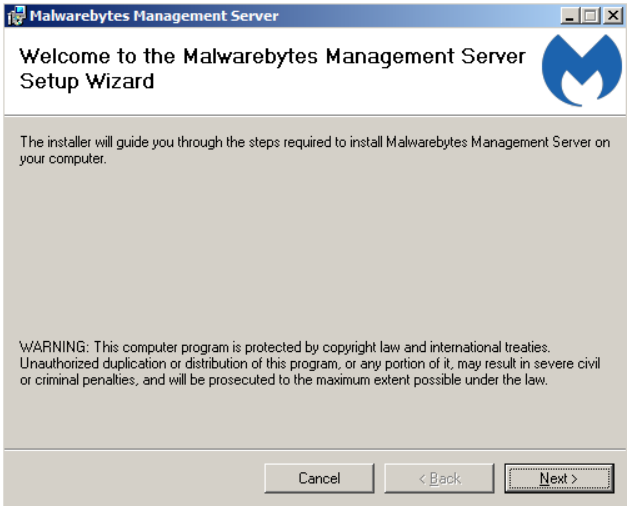
Click the setup icon on your desktop to start installation of *Malwarebytes Management Console*.

Server Address and Port Number: If they are not auto-populated for you, please enter the Management Server Address (IP or FQDN), Client Communication Port and Server Administration Port.

WARNING: These settings determine how clients will communicate with the server, and changes made after a client has been deployed may cause communication issues with that client.

Your server address will be different from the one shown here. Port addresses may be changed if they conflict with existing needs.

Click *Next*.

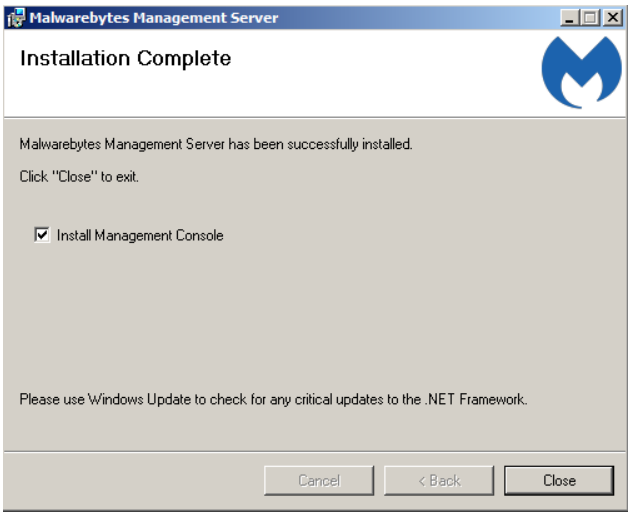


Select Database: Choose whether to use the embedded SQL Server Express database or an existing SQL Server database. If you choose to use an existing database, you must specify the server and instance as well as the SQL Administrator username and password.

Click *Next*.

Installation Complete (server): Don't be fooled! You're not done quite yet. The Management Server has been installed, but now it's time to install the Primary Console.

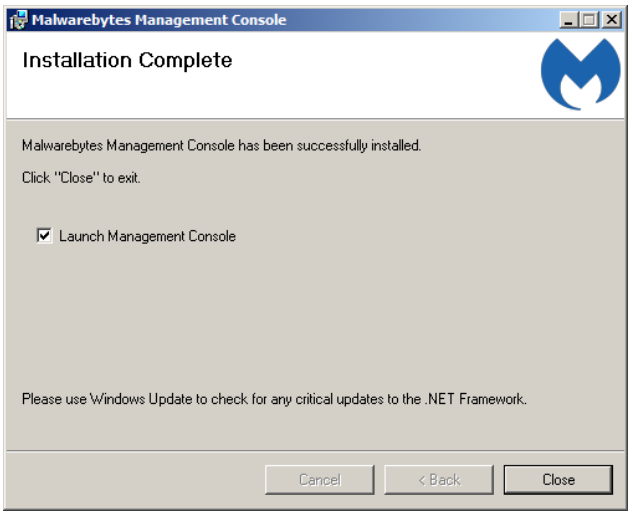
Click *Close*.



Installation Complete (console): This time you are done!

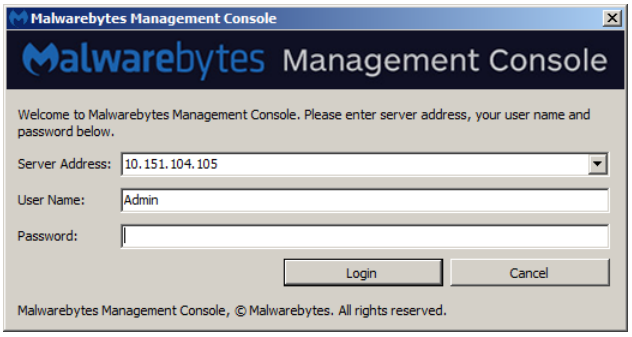
Leave the mark in the check box to accept the default to *Launch Management Console*, or uncheck the box to simply leave the installation program.

Click *Close*.



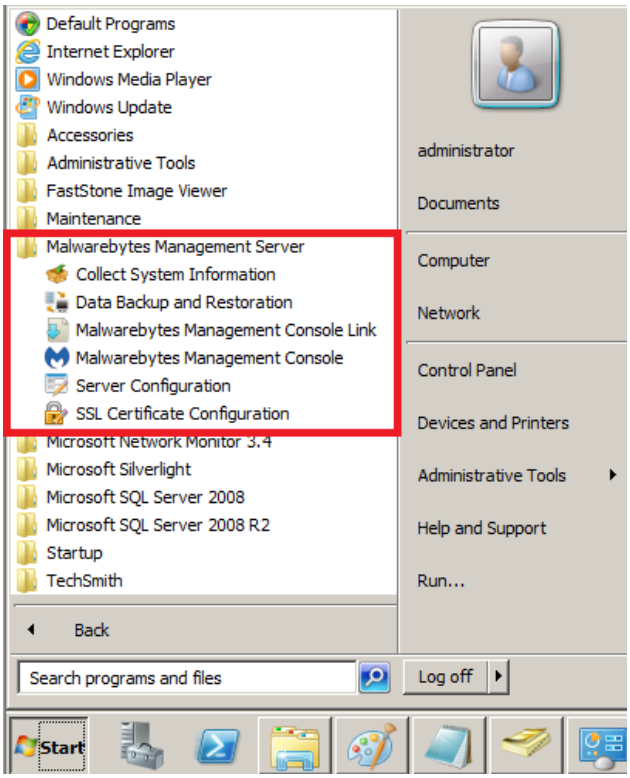
If you elected to launch the Management Console, the login window opens. The server address is displayed, along with the default **Admin** user name.

There is no initial password, so click *Login*. You will then be prompted for a new password before you are allowed to continue.

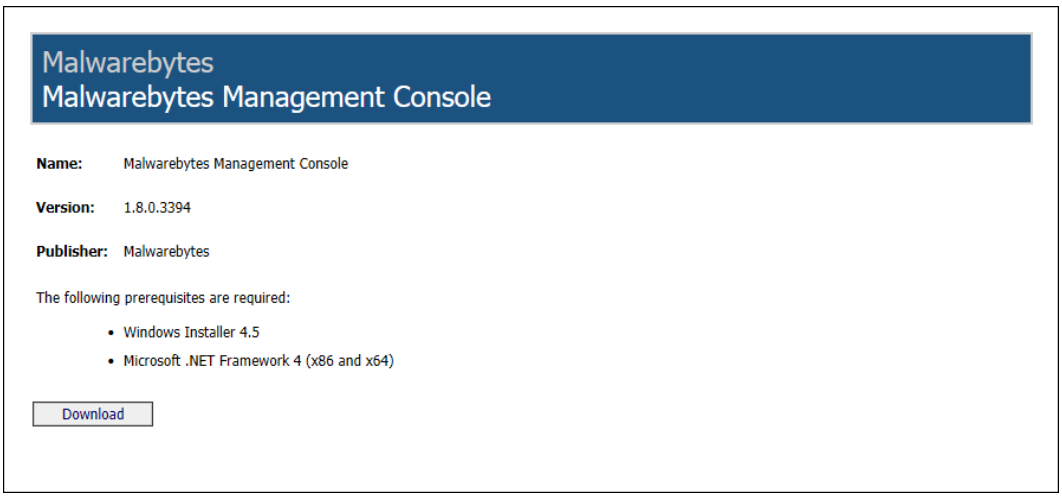


Installing a Secondary Console

If you have other things to do besides taking care of your company's servers, you probably would like to do as much as you can from your own desk. A Secondary Console allows you to manage *Malwarebytes Management Console* from more comfortable surroundings. Shown below is the Windows Start Menu, and links related to the *Malwarebytes Management Console* are shown bordered in red.



Selecting the **Malwarebytes Management Console Link** will launch a browser (or a new browser tab), which shows the following:



Click the **Download** button to download the installer for the Secondary Console to your standard download location. The file will be named mbmc-console-setup.exe. Copy that file to a thumb drive and execute it on the computer which you would like to use for your Secondary Console, and you will then be able to manage *Malwarebytes Management Console* remotely. **Please note** that the Secondary Console is optional. It is not required for normal operation.

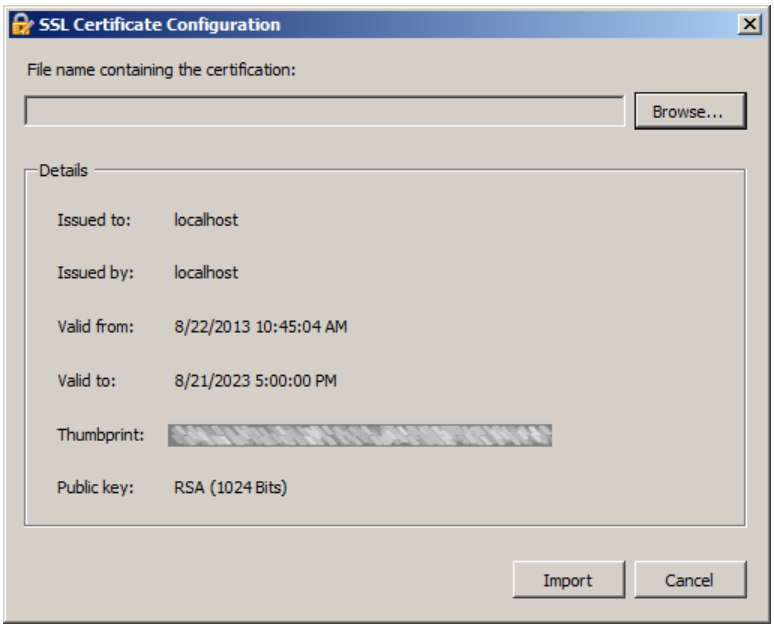
SSL Certificate Configuration (optional)

Malwarebytes Management Console installs with a valid certificate, though many corporate customers wish to utilize their own certificates. A certificate verifies authenticity of devices, and is a necessity when using SSL communications. The following information may provide some assistance if certificate-oriented steps are required.

Please note that you only need to perform these tasks if you are using certificates in your organization, and wish to have *Malwarebytes Management Console* be consistent with your certificate usage.

Verifying Presence of a Certificate

From the Windows Start menu, launch the SSL Certificate Configuration to display the certificate panel as shown below.



The Details section of this panel indicates that a certificate is present on this server. It is the generic certificate installed as part of a *Malwarebytes Management Console* installation.

Exporting an Existing Certificate

If your server's self-signed certificate is not recognized by *Malwarebytes Management Console*, you must export the certificate so that it can then be reinstalled. Do so by performing the following steps:

- Launch Microsoft Management Console (mmc.exe).
- If Certificates is not an option within mmc, choose *File* ► *Add/Remove Snap-Ins* ► *Certificates* ► *Add,* and specify that certificates will be managed for the Computer account. Press *Finish*, select Local Computer on the next screen, and *Finish* again. Finally, press *OK*. The Certificates manager is now loaded into MMC.
- Expand Certificates (Local Computer), then expand Personal. Available certificates will be displayed in the center panel.
- Select *All Tasks* ► *Export* to launch the Certificate Export Wizard.
- Click *Next* to access the Export Private Key screen.
- Select the radio button next to Yes, export the private key.
- Click *Next* to access the Export File Format screen.
- Personal Information Exchange (PFX) file format is selected by default. Click *Next* to progress to the Password screen.
- Enter the password twice and click Next to progress to the File to Export screen.
- Enter a filename for the certificate. You may also choose a directory in which it should be stored. Click *Next* when done.
- You will be presented with the certificate specifications. Click *Done* to complete the process.

Once these steps have been performed, you have a certificate which you may use for *Malwarebytes Management Console*.

Installing a Certificate

It is a simple process to import a certificate (self-signed or commercial), as long as the certificate is in the form of a PFX (Personal Information Exchange) file. Steps are as follows:

- Launch *SSL Certificate Configuration* from the Malwarebytes Management Server entry on the Windows Start Menu. The SSL Certificate Configuration screen (as shown earlier in this section) will be displayed.
- Click the *Browse* button to navigate to the directory where the new certificate is stored.
- Select the certificate and click *Open*.
- The certificate filename will be displayed at the top of the window. Click *Import* to import the new certificate.

Preparations for Your First Install

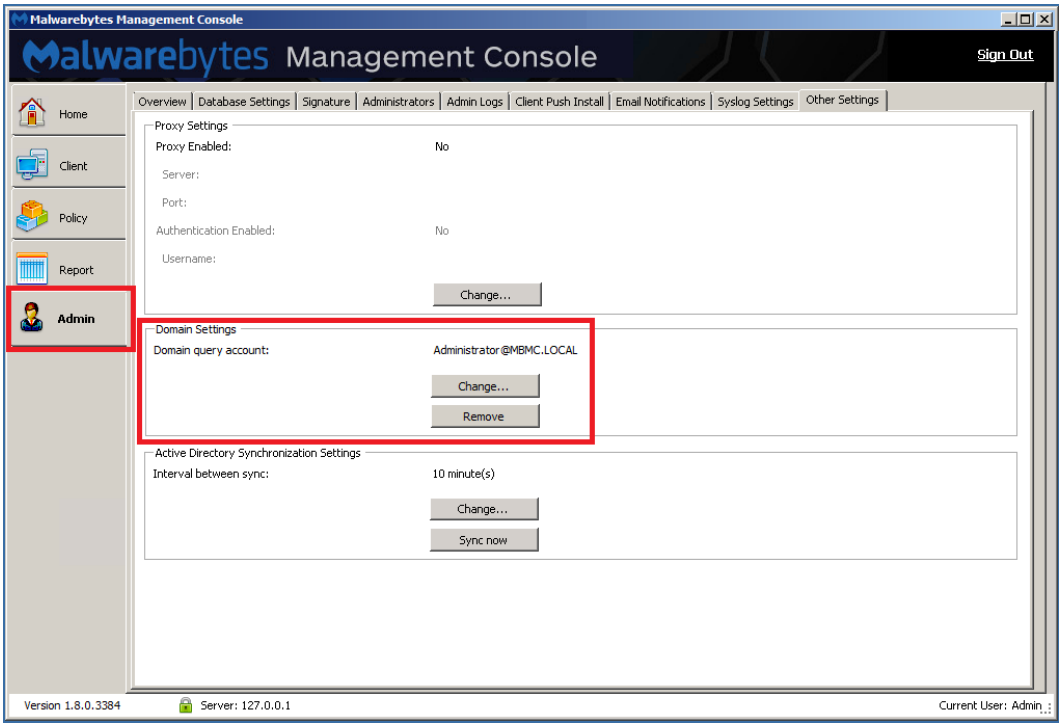
When *Malwarebytes Management Console* is installed on your server, an icon will automatically be created on your desktop. This allows you to launch the program, and takes you directly to the login screen (shown on page 10). In addition, you may access the login screen from the Windows Start Menu, using the **Malwarebytes Management Server ►Malwarebytes Management Console** link. This method is also shown on page 10. Be careful…two very similar looking links are present on the menu, but they perform drastically different functions.

Defining the Basics

A number of preliminary settings need to be configured before you can do full-scale deployments to your endpoints. We'll take care of the basics here to get you started. You will likely revisit this section as you become more familiar. These settings will be used on an everyday basis. These are listed below.

Domain Query Account (domain installation only)

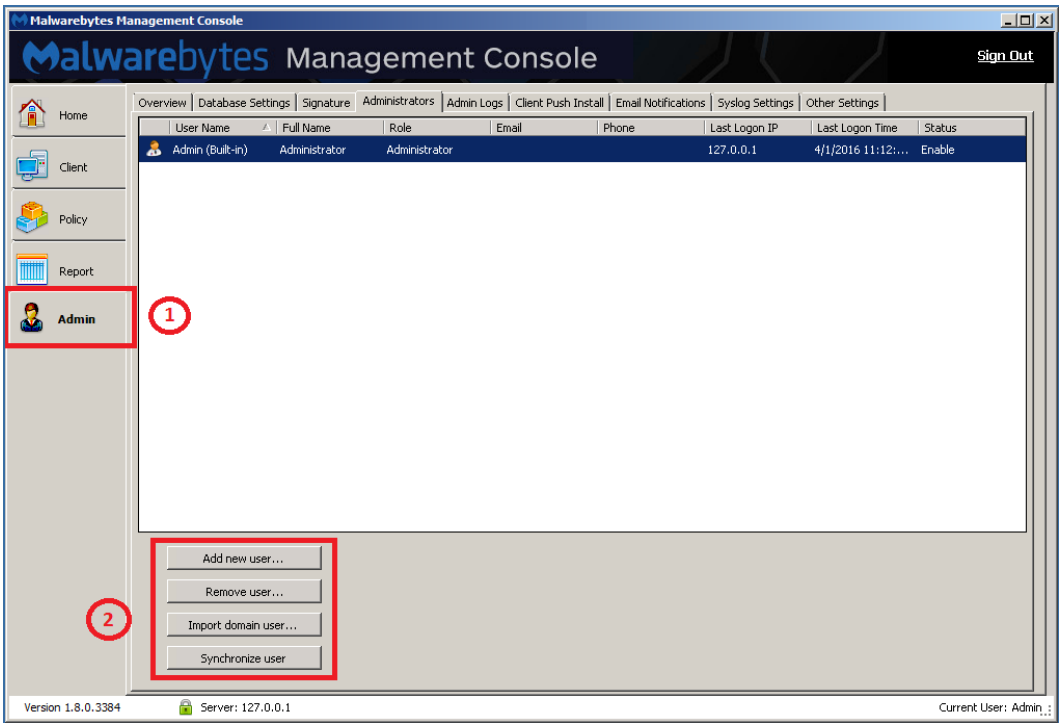
If you are using *Malwarebytes Management Console* in an Active Directory domain, you must define this system specification. All visibility to networked computers, and authorization to perform tasks is based on security policies which are controlled by Active Directory. *Malwarebytes Management Console* works in conjunction with Active Directory, but cannot override any policies which are governed by Active Directory. Go into the **Admin** panel (left side) and look for the **Domain Query Account** setting on the **Other Settings** tab, as shown here. Click the **Change…** button and enter the specification that will be used in your environment.



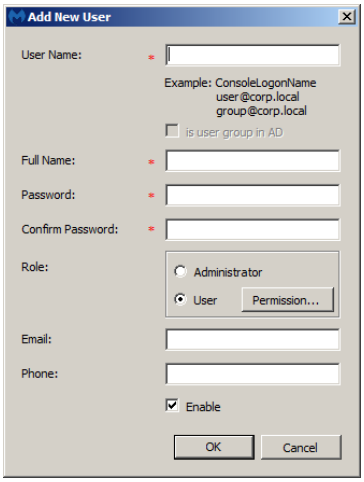
Administrators / Users

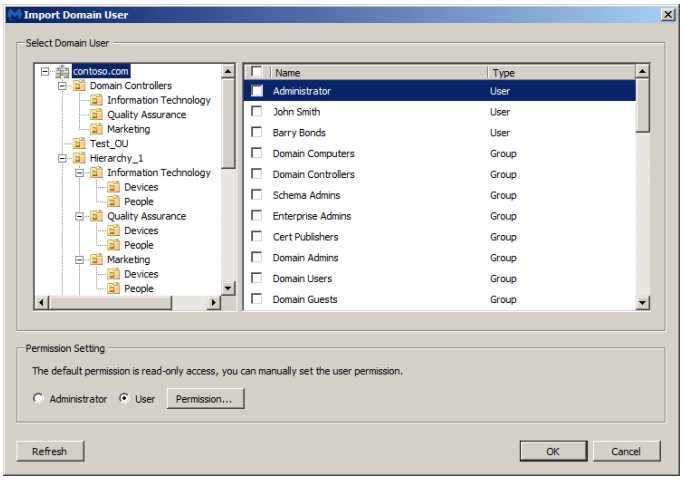
Malwarebytes Management Console is initially set up with one administrator account (username: **admin**, no password). Upon your first login to *Malwarebytes Management Console*, you are required to change your password. It is strongly recommended that you create additional administrator accounts, and leave **admin** as an emergency backup administrator account.

If you are using *Malwarebytes Management Console* in a domain-based environment, you can add new administrators and users using two different methods (**Add new user…**, and **Import domain user…**). Both are accessible from the **Admin** panel, on the **Administrators** tab, as shown below.



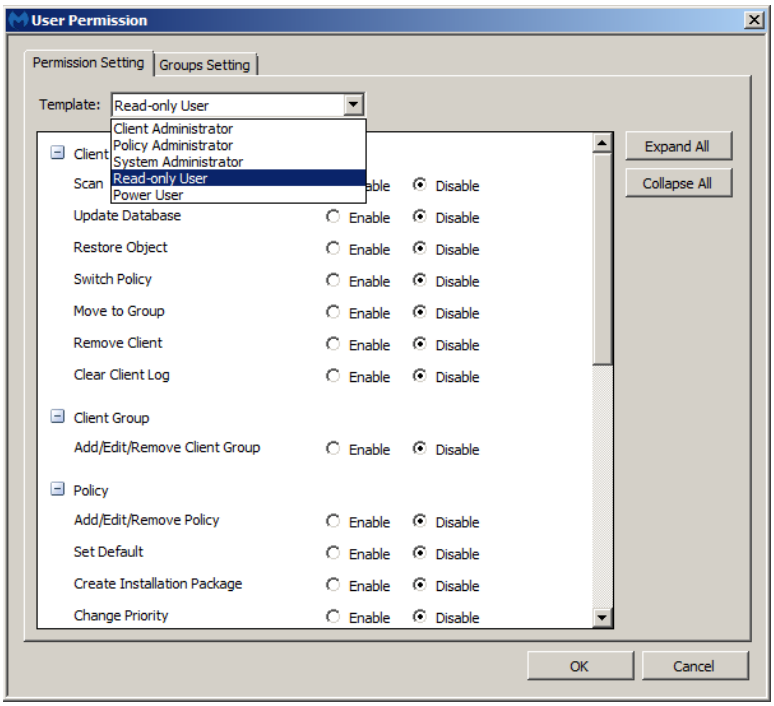
In an environment that does **not** include Active Directory, the **Add new user…** option allows you to add new administrators/users. The screenshots below show the windows that are opened as a results of clicking either the **Add new user…** button or the **Import domain user…** button.





While the **Add New User** window allows you to add a single user in a domain or non-domain based environment, the **Import Domain User** windows allows you to add one user, multiple users, or OUs at once. The **Import Domain User** window **only** works in a domain-based environment. In both windows, please note the Permission… button. That allows you to set specific permissions for users with regard to *Malwarebytes Management Console* operations, or to choose from a template-based set of permissions for different user classes.

The following screenshot shows the various templates available and illustrates some of the permissions. It is followed by a table which shows permissions in detail.

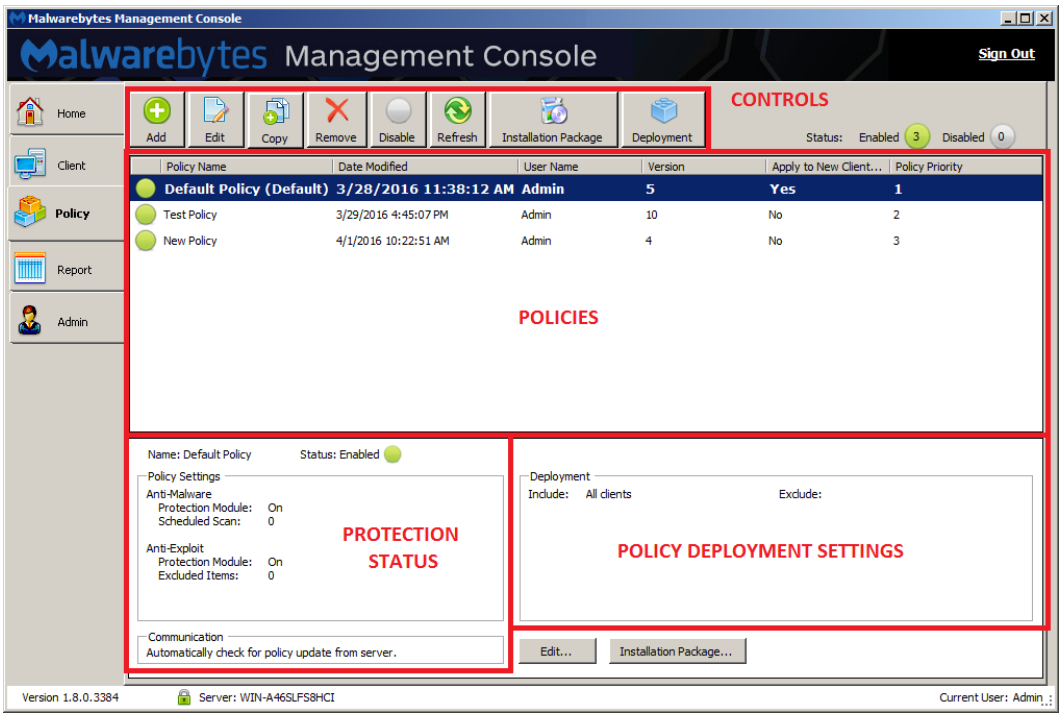


	CLIENT ADMIN	POLICY ADMIN	SYSTEM ADMIN	READ-ONLY USER	POWER USER
CLIENT					
Scan	enabled	disabled	disabled	disabled	enabled
Update Database	enabled	disabled	disabled	disabled	enabled
Restore Object	enabled	disabled	disabled	disabled	enabled
Switch Policy	enabled	disabled	disabled	disabled	enabled
Move to Group	enabled	disabled	disabled	disabled	enabled
Remove Client	enabled	disabled	disabled	disabled	enabled
Clear Client Log	enabled	disabled	disabled	disabled	enabled
CLIENT GROUP					
Add/Edit/Remove Client Group	enabled	disabled	disabled	disabled	enabled
POLICY					
Add/Edit/Remove Policy	disabled	enabled	disabled	disabled	enabled
Set Default	disabled	enabled	disabled	disabled	enabled
Create Installation Package	enabled	enabled	disabled	disabled	enabled
Change Priority	disabled	enabled	disabled	disabled	enabled
REPORT					
Print	disabled	disabled	disabled	disabled	enabled
ADMIN					
Add/Edit/Remove Admin	disabled	disabled	enabled	disabled	enabled
ADMIN LOG					
Clear Admin Log	disabled	disabled	enabled	disabled	enabled
PUSH INSTALLATION					
Scan Network	enabled	disabled	disabled	disabled	enabled
Client Push Install	enabled	disabled	disabled	disabled	enabled
SYSTEM SETTING					
License	read only	read only	read/modify	read only	read/modify
Server Address	read only	read only	read/modify	read only	read/modify
Database	read only	read only	read/modify	read only	read/modify
Signature	read/modify	read only	read/modify	read only	read/modify
Client Package	read/modify	read only	read/modify	read only	read/modify
Cleanup	read only	read only	read/modify	read only	read/modify

Malwarebytes Management Console provides the ability to allow user functionality while controlling accessibility according to *your* requirements.

Policies

Policies are critical when it comes to endpoint security. They determine behavior of *Malwarebytes Anti-Malware* and *Malwarebytes Anti-Exploit* clients on each endpoint that they are deployed to. The screenshot below illustrates *Malwarebytes Management Console's* **Policy** module, with overlays to divide the functional areas of the screen.



IMPORTANT: Before deploying policies to any endpoint, it is critical that you read and understand the Policies chapter (pages 25-36) of the *Management Console Administrator Guide*.

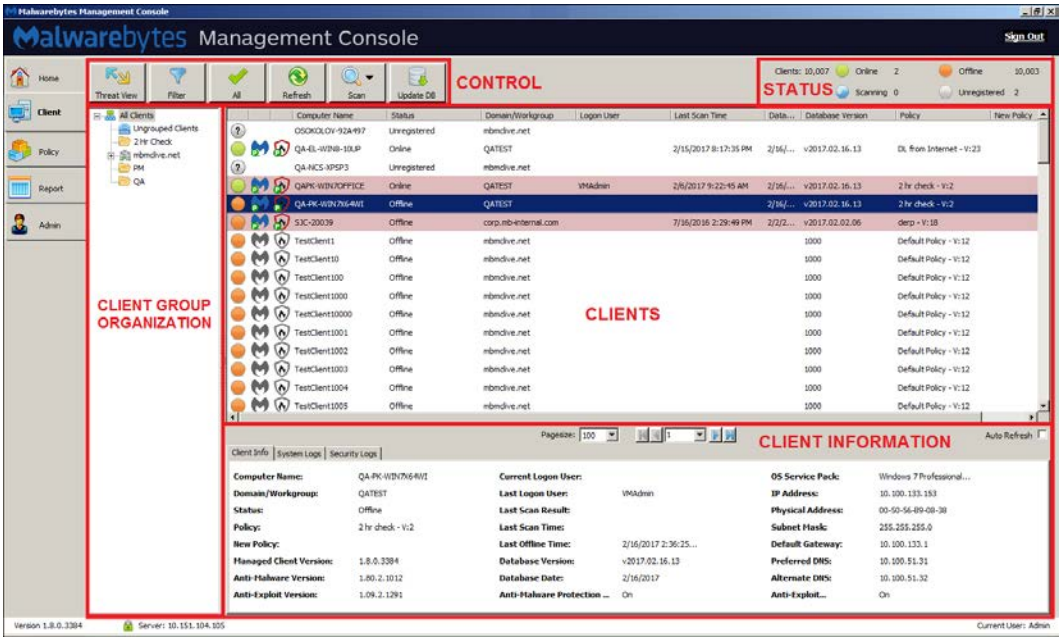
There are too many aspects of this program module to include in a Quick Start Guide. When you read this section of the Administrator Guide, the following will help you focus on the various aspects of adding new policies or editing existing policies.

- **General Settings:** General settings controlling basic settings for *Malwarebytes Anti-Malware* clients
- **Protection:** Determines which real-time protection components of *Malwarebytes Anti-Malware* will be enabled, as well as visibility of client to the endpoint user.
- **Scanner:** Specifies behavior of *Malwarebytes Anti-Malware* during malware scans. Threat remediation settings related to scans are located on the **Scheduler** tab.
- **Scheduler:** Allows the administrator to control when a malware scan will be executed, as well as the type of scan to be executed, and recovery mechanisms if the scan cannot be executed. Threat remediation settings are located here, rather than on the **Scanner** tab.
- **Ignore List:** Allows files, folders, registry keys and IP addresses to be excluded from malware scanning. **Please note** that entries made here should be made based on trust rather than convenience. If you do not trust the item you are excluding, you risk damage to your endpoint.
- **Updater:** Determines how your *Malwarebytes Anti-Malware* client will receive threat signature updates, and if an alternate method is used, when the updates will occur. This works in conjunction with settings found on the **Communication** tab. Because these updates are the foundation of your anti-malware protection, you want to assure a reliable update method.
- **Communication:** Controls when the endpoint checks in with *Malwarebytes Management Console*. This is an essential process for receiving policy updates, as well as receiving threat signature updates (when getting signature updates through standard methods).
- **Anti-Exploit:** Controls whether *Malwarebytes Anti-Exploit* is enabled, the client's visibility to the user, and which shields are to be used. Custom shields may be added here to supplement pre-defined shields.

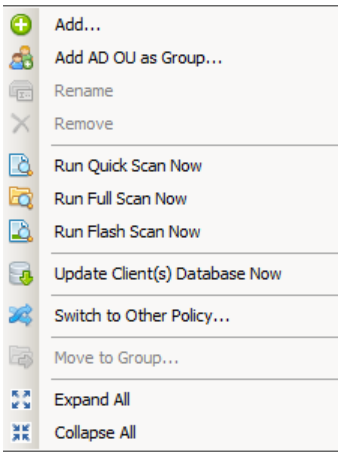
- **Anti-Exploit Exclusion List:** Allows files to be excluded from exploit testing by the *Malwarebytes Anti-Exploit* client. Each file to be excluded is specified by its MD5 signature, which is a highly unique method of identifying a file and its contents.

Client Groups

Client Groups allow you to divide your networked computers into smaller segments based on what function they perform, or who uses them. Combined with policies, they help to maintain high network throughput when communication between server and clients is taking place. If you are using *Malwarebytes Management Console* in a domain-based environment, you can create groups based on your OU structure in Active Directory. While you can mimic AD's OU structure, you cannot override it. The screenshot below shows the **Client** panel and the screen layout.



Client Groups appear in a vertical format on the left side of the screen. A context menu is available for Client Groups that provides certain functionality. That menu, and a brief description of selected commands is shown here:

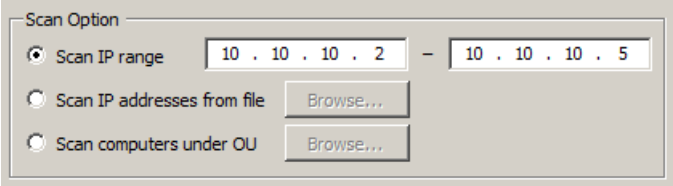


- **Add:** Add a new client group
- **Add AD OU as Group…:** Import an AD OU as a group. AD naming is used.
- **Rename:** Rename a non-AD group
- **Remove:** Remove a group. All computers will revert to Ungrouped Clients group.

All endpoint-related commands are functional only after groups have been defined and discovery has taken place.

Discovery of Network Computers

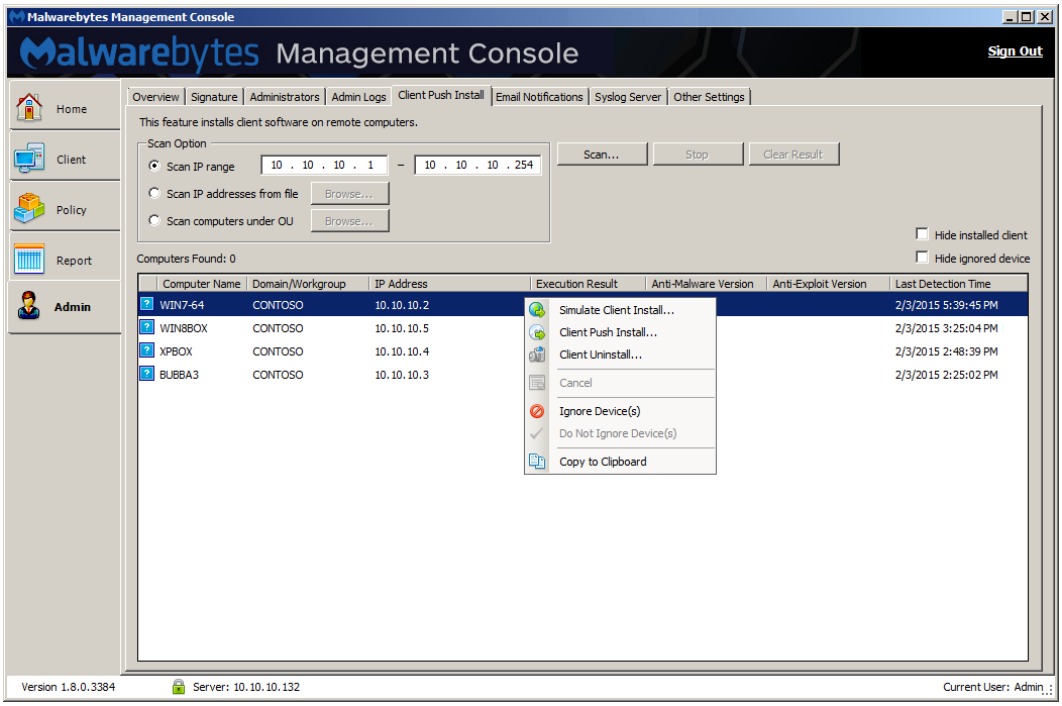
There is one more preliminary step before we can install a client on an endpoint. Discovery of networked computers allows us to know where Malwarebytes clients should be installed. This is done from the **Admin ► Client Push Install** tab. A screenshot is shown below.



There are three different ways in which you can perform network discovery.

- **Scan IP range:** Allows you to discover by IP address. Beginning and ending addresses must have the first two octets in common. Along with computers, it will also return servers, printers, and other networked devices.
- **Scan IP addresses from file:** Allows you to enter IP addresses (one per line) in a file. This is helpful when including computers in IP blocks different from your primary addresses, as is common in VPN or VLAN implementations.
- **Scan computers under OU:** Allows you to get discovery criteria from Active Directory, by selecting an OU.

After selecting the range of computers to discover, you can these choose how they should be discovered. There are several methods available, and reasons for each to be used. It is best to again refer you to the *Management Console Administrator Guide*, pages 55-59.



In the screenshot shown above, a discovery was performed on the IP range 10.10.10.2 – 10.10.10.254, which contained four computers. They are shown here, each with an icon to the left of the computer name. The icon shown (as well as other icons which may appear are shown here.

ICON	CLIENT STATUS
	Client installed and operational
	Client registration failure
	Status unknown to server
	Ignored device
	Passed simulation
	Error condition

During an initial discovery, you would expect only to see the "Status unknown to server" icon. The first two icons would appear only as a result of a client installation.

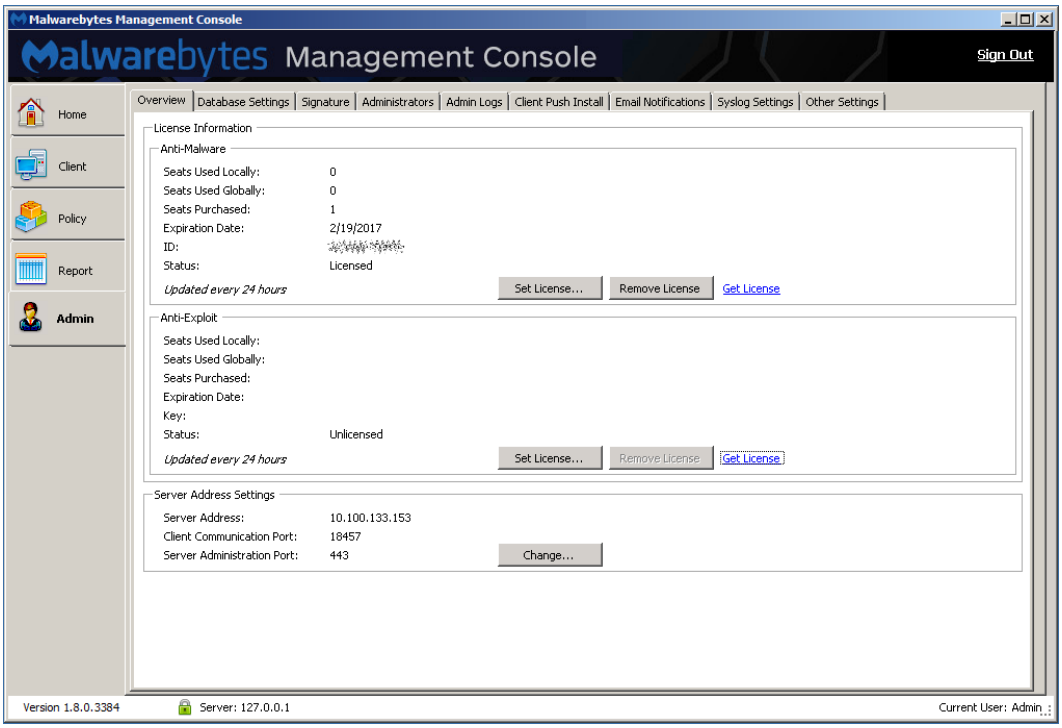
After performing discovery, you may choose to ignore certain devices because they are not suitable for client installations. The "Ignored device" icon would then appear.

In all cases, the "Error condition" icon warrants attention.

Licenses for Purchases and Trials

Malwarebytes Management Console will block the ability to deploy any Malwarebytes protection products to an endpoint unless a valid license has been entered. *Malwarebytes Anti-Malware* and *Malwarebytes Anti-Exploit* each have their own license. License keys will be issued by Malwarebytes (or by a reseller, if you purchased through a reseller). These license keys are used for purchases and for evaluations.

The following screenshot shows the Overview tab of the Admin panel. This screen allows you to enter the license key for each of our protection clients. Clicking the **Set License** button for the appropriate client allows you to enter the key. Again referring to the screenshot, a valid license has been provided for Malwarebytes Anti-Malware and its status is shown as *Licensed*. The key itself has been obfuscated. No license key has been provided for Malwarebytes Anti-Exploit, so it is shown as *Unlicensed*. Applying a license from a product purchase would change its status to *Licensed*, while a trial key would change the status to *Evaluation*.



If you are evaluating one or both managed clients and do not elect to purchase during (or at the end of) your trial, the trial will terminate and you owe nothing. You may evaluate either or both managed clients using this method, although you can only evaluate each one once.

Installing Your First Client

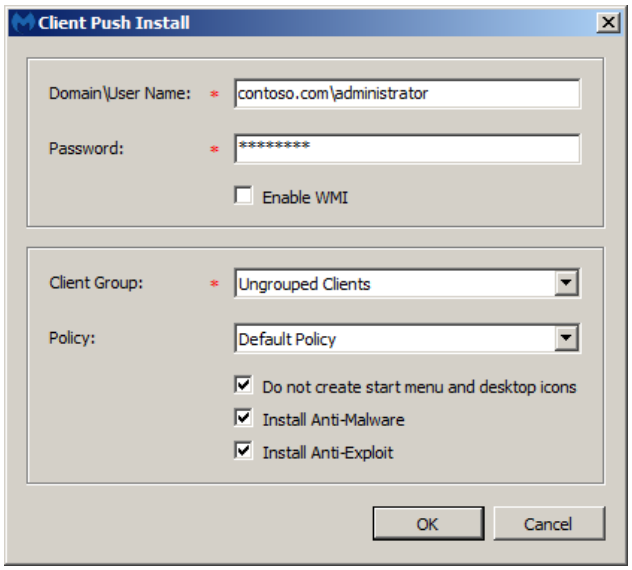
You have done your pre-requisites on all computers. You have set up your server. If you have Active Directory, you have set up your domain query account. You have begun to define policies. You may have set up client groups, and finally you have done a discovery on all or part of your computer network. It's time to install a client. Please note the context (right-click) menu which appears on the discovery results screenshot on the previous page. The first two items on this menu are processes that we will now perform.

Simulate Client Install

This option tests the ability of *Malwarebytes Management Console* to communicate with an endpoint on which a managed client is to be installed, to perform steps which simulate a client installation, and to verify results of these steps. Because this process adds, deletes and executes files that are located on the endpoint, authentication is required on the client. This consists of the user name and password for an administrative user on the endpoint. There may be instances when permissions for the administrative user do not provide the level of permissions required for an installation/simulation to occur. In this case, Windows Management Instrumentation (WMI) is utilized to perform the simulation. The WMI service must be running on the endpoint, and the simulation must be performed by an admin user whose permissions allow use of the WMI service.

Client Push Install

This option allows managed client software to be installed on an endpoint in the corporate network. A screenshot of the Client Push Install panel is shown below.



Administrator-level authentication on the endpoint is required. If there are any permissions issues where the admin user may not be able to accomplish installation tasks, the **Enable WMI** checkbox can be checked.

You may install managed client software on this endpoint as a member of **Ungrouped Clients**, or as a member of a specific **Client Group**. In addition, a **Policy** must be selected before installation can occur.

You may also choose whether the managed client is visible to the endpoint user via entries on the Windows start menu and desktop icon. If this option is selected, both will be created during installation. If unselected, neither will be created. There is no provision for creating only one of the two visible indicators of Malwarebytes presence on the endpoint. Finally, you can elect to install *Malwarebytes Anti-Malware*, *Malwarebytes Anti-Exploit*, or both clients.

That's all there is to it! A lot of work has went into *Malwarebytes Endpoint Security*, so that the task of providing a secure, malware-free environment takes less work on your part. Congratulations on taking the next step in computer security!