Malwarebytes
ENDPOINT SECURITY

Management Console Administrator Guide

Version 1.9

20 November 2018

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.

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)

Table of Contents (continued)

Table of Contents (continued)

Introduction

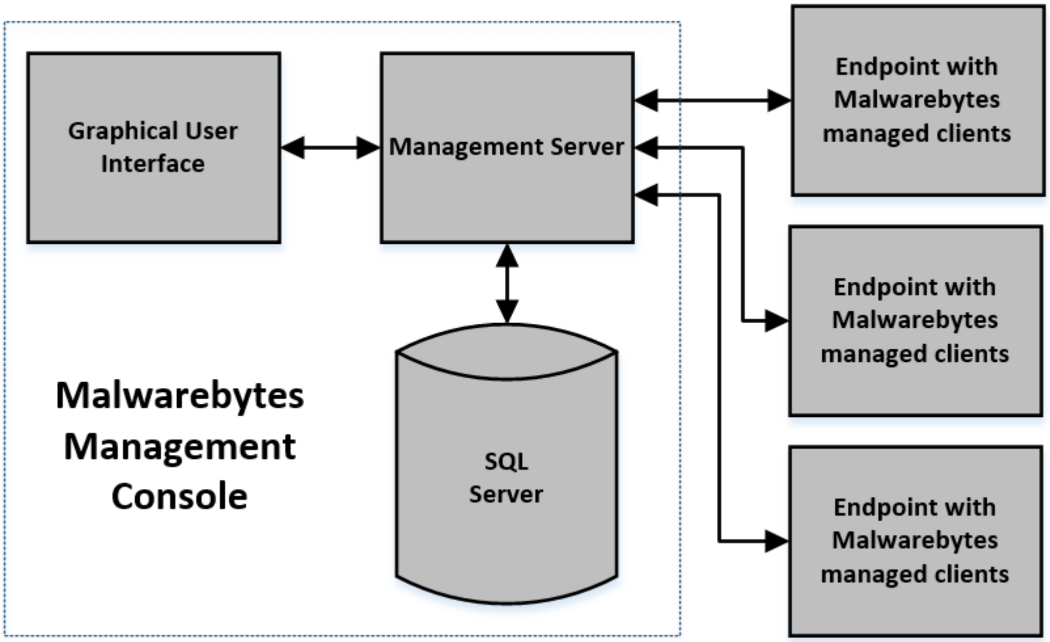
This guide was produced to assist system administrators with installation, maintenance and operation of *Malwarebytes Management Console*, and to provide a comprehensive reference to the product and to the protection clients which are integrated into *Malwarebytes Management Console*. Let's begin by discussing the components in play.

Malwarebytes Management Console

Malwarebytes Management Console enables IT administrators to deploy, control and manage Malwarebytes clients on every Windows-based endpoint in their organization. The Malwarebytes clients are full-featured versions, not stripped down versions. A sampling of features available in *Malwarebytes Management Console* is as follows:

- Full integration with *Malwarebytes Anti-Malware* managed client
- Full integration with *Malwarebytes Anti-Exploit* managed client
- Full integration with *Malwarebytes Anti-Ransomware* managed client
- Integration with Microsoft Active Directory management of users, groups, organizational units and endpoints, as well as adherence to security policies governed by Active Directory
- Ability to deploy managed clients to endpoints within *Malwarebytes Management Console*, or by creation of installation packages to be deployed using third-party utilities
- Ability to create endpoint groups for simplification of installation and management
- Ability to manage endpoints based on policies which define behavior for managed clients associated with those policies
- Scheduling of all scans and updates on endpoints, based on policies
- Ability to alert administrators of events via email notifications and syslog alerts
- Retention of data pertaining to endpoints, policies and threats in centralized SQL database
- Ability to distribute signature updates to endpoints from *Malwarebytes Management Console* or from alternate sources

All of these features – and more – are fully integrated into the product, so that every feature you have come to expect from Malwarebytes in a unmanaged version is available also in *Malwarebytes Management Console*, without sacrifice!


Graphical User Interface
Management Server
SQL Server
Malwarebytes Management Console
Endpoint with Malwarebytes managed clients
Endpoint with Malwarebytes managed clients
Endpoint with Malwarebytes managed clients

Malwarebytes Anti-Malware

Malwarebytes Anti-Malware is driven by a signature database which is updated 8-15 times daily, and supplemented by heuristic analysis to detect patterns that do not yet exist in the signature database. The focus is on recent, current and emerging threats. Only a small number of threats affecting computer users today are based on older threat vectors, as most (if not all) anti-virus and anti-malware software products are well equipped to deal with the older threats.

Policies developed by IT administrators and administered by *Malwarebytes Management Console* govern a majority of program functionality. Malware scans and signature updates are controlled by policies. Startup methods and sequences are controlled by policies. Real-time protection and quarantining of detected threats and exploits are also controlled by policies. The endpoint user may have additional capabilities determined by the IT administrator, and allowed through policies. While the *Malwarebytes Anti-Malware* managed client is designed for networked endpoints accessible to *Malwarebytes Managed Console*, it may also be used on endpoints which use Virtual Private Network (VPN) connectivity – with certain restrictions.

Malwarebytes Anti-Exploit

Malwarebytes Anti-Exploit takes a different approach to computer security. It does not use signatures of any known threats. Instead, it inspects incoming data streams, analyzes behavior, and determines whether it needs to respond to a suspected exploit attempt. Malware often attempts to bypass operating system protection mechanisms so that it can execute in an unrestricted fashion. Malware often uses memory manipulation methods so that it can function undetected. Malware often uses vulnerabilities in commonly-used applications to implant a threat, or uses the application as a means of transferring the threat from one location to another. In all cases, there is a common thread – the method being used signals the danger. *Malwarebytes Anti-Exploit* shields applications and processes from attack, while neutralizing and isolating the attacker. Even a zero-day threat is ineffective when protected by this technology.

Malwarebytes Anti-Ransomware

Malwarebytes Anti-Ransomware is similar to *Malwarebytes Anti-Exploit* in that it uses no signatures to detect threats. This client software will monitor processes on your endpoints and watch for abnormal behavior that is indicative of a ransomware attack. We monitor for several types of suspicious activity on each process – if a particular process continues to exhibit suspicious behavior, it will be terminated by *Malwarebytes Anti-Ransomware* to protect your endpoint. Since signatures are not required for the client to operate, zero-day or even zero-hour threats are detected. Clients can take advantage of this signatureless protection along with *Malwarebytes Anti-Exploit* to help protect clients that may not have access to *Malwarebytes Management Console* at all times.

What's New in Malwarebytes Management Console

With this version, *Malwarebytes Management Console* has been updated to provide the following new features.

New Features

- Added the option to manage Malwarebytes Anti-Ransomware endpoint agent, including:
    - Install and uninstall Anti-Ransomware from the Management Console
    - Visualize ransomware detections in logs, email alerts, and syslog
    - Add and remove Anti-Ransomware Exclusions
    - Restore Anti-Ransomware quarantine items
- Added unmanaged Malwarebytes Breach Remediation, Mac Real-Time Protection, and Android clients

Improvements

- Changed Sccomm logs for Adhelper to debug mode only

Fixes

- Fixed: Sccomm service does not start on some clients running Windows 10
- Fixed: Issue creating temporary file when updating Policies in the Management Console
- Fixed: Issue with server memory spike in certain cases during login after upgrading Management Console
- Fixed: Issue with Client tab and Home dashboard showing different number of online clients

System Requirements

Following are system requirements for components which make up *Malwarebytes Endpoint Security*. These do not include any other functionality that the endpoint is responsible for. The *Endpoint Security Best Practices Guide* should be consulted prior to equipment procurement as well as prior to *Malwarebytes Management Console* installation.

Management Server / Primary Console

Malwarebytes Management Console provides all system functionality via its Management Server. It provides all necessary Windows services, and communicates directly with the Primary Console and the managed endpoint. It runs strictly in the background.

Equipment Specifications

The following specifications are provided as minimum requirements which must be met to provide Management Server functionality.

- **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 Server 2008/2008 R2 (excludes Server Core installation option)
  - Windows Small Business Server 2011
- **Supported Microsoft SQL Servers**
  - Database embedded: Microsoft SQL Server 2008, 2012, 2014, 2016 Express (10 GB maximum size limitation)
  - Database supported: Microsoft SQL Server 2008/2008 R2, Microsoft SQL Server 2012/2012 R2, Microsoft SQL Server 2014/2014 R2

Secondary Console

All interaction with the Management Server is effected through the Primary and/or Secondary Console. The Management Server then interacts with the endpoints (managed clients). Specifications listed below are for a Secondary Console. The Primary Console is typically installed on the same computer as the Management Server.

Equipment Specifications

The following specifications must be met in order to provide Console functionality.

- **Hardware**
  - CPU: Core Duo 1.6 GHz
  - RAM: 1 GB
  - 1024x768 screen resolution
- **Software**
  - .NET Framework 3.5 or higher
  - 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 Server 2008/2008 R2 (excludes Server Core installation option)
  - Windows Small Business Server 2011
  - Windows 10
  - Windows 8.1
  - Windows 8
  - Windows 7
  - Windows Vista
  - Windows XP Pro with SP3

Managed Clients

The managed client provides security functionality on the endpoint. Commands are received from the Management Server after being issued by the user, and after processing which may be required. Status is returned to the Management Server, which processes results and provides visible notification to the user.

Equipment Specifications

The following specifications are provided as minimum requirements which must be met to provide Managed Client functionality.

- **Hardware**
  - CPU: 1 GHz
  - RAM: 1 GB
  - Disk space: 200 MB (program + logs)
  - 1024x768 screen resolution
  - Active Internet connection
- **Software**
  - .NET Framework 3.5 or higher
  - Windows Installer 4.0
- **Supported Operating Systems**
  - Windows Server 2016 (excludes Server Core installation option)
  - Windows Server 2012/2012 R2 (excludes Server Core installation option)
  - Windows Server 2008/2008 R2 (excludes Server Core installation option)
  - Windows Server 2003 (32-bit only)
  - Windows Small Business Server 2011
  - Windows 10
  - Windows 8.1
  - Windows 8
  - Windows 7
  - Windows Vista
  - Windows XP Pro with SP3 (32-bit only)

Pre-Requisites for Installation of Managed Clients

Endpoint configuration changes must be implemented to facilitate installation of a Malwarebytes managed client to those endpoints. Similar methods are required for the various operating systems, and they are grouped accordingly.

- **Windows Server endpoint preparation (all supported versions)**
  - 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.
  - Close the Control Panel screen.

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://hubble.mb-cosmos.com	Port 443	outbound
https://*.mwbsys.com	Port 443	outbound
https://telemetry.malwarebytes.com	Port 443	outbound

Please note: These URLs may not be configured to respond to pings.

System Checks

The following sections describe system checks that *Malwarebytes Management Console* makes during installation.

System Requirement Checks for Servers

If any of the following software has not already been installed, it will be automatically downloaded and installed:

- Internet Information Services (IIS) 7.5 Web Server
- .NET framework 4.0 (x86 and x64)
- Windows Installer 4.5
- SQL Server 2008 R2 Express

If system memory is less than 2 GB, the system administrator receives a warning and must explicitly choose to continue installation.

If free disk space is less than 10 GB but above 2 GB, the system administrator receives a warning, and must explicitly choose to continue installation.

If free disk space is less than 2 GB, the system administrator receives an error and installation aborts.

Address/Port Validity Checks for Servers

If the user-specified server address does not match the current server address (IP, server name, DNS name, FQDN), the system administrator receives the warning, "The server address is invalid."

If the input port is invalid or is occupied by other application, the system administrator receives the warning, "*The server port is invalid or occupied by other application*."

The server address is the most significant communication setting. Once the server address has been specified, subsequent changes may cause communication errors until configuration changes have been made . To prevent these errors, select an unchangeable property as the server address, such as a fully-qualified domain name (FQDN).

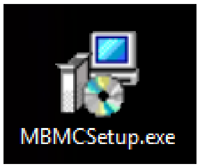
Program Installation

If you are a new user, you will only be concerned with the following section. This covers installation of *Malwarebytes Management Console*. Customers who are upgrading to this version will also want to read the section titled *Upgrading Malwarebytes Management Console* beginning on page 13. Information in that section is pertinent only for users when upgrading.

New Installation of Malwarebytes Management Console

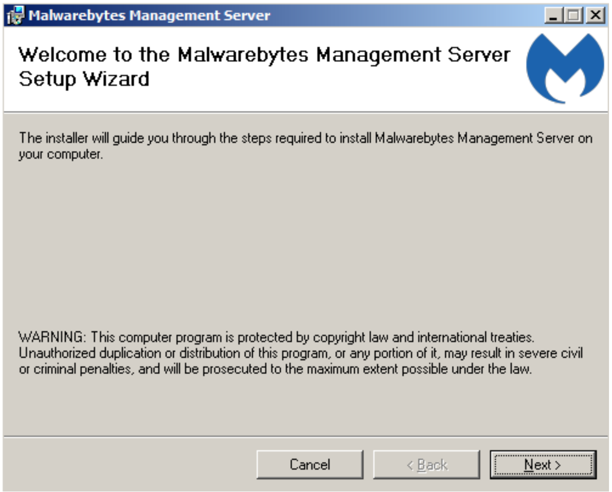
Malwarebytes Management Console is provided to customers in the *Malwarebytes Endpoint Security* ZIP archive. Please refer to page 2 of the *Endpoint Security Quick Start Guide* for an introduction to the layout of the ZIP file. After extracting the *Malwarebytes Management Console* installer from the ZIP file, please use the following instructions to install the product.

1. Click the setup icon to start program installation.



2. The Setup Wizard opens.

   Click *Next*.

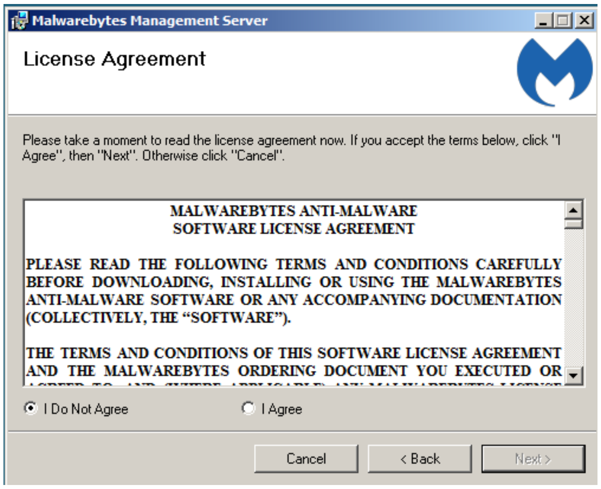


Welcome to the Malwarebytes Management Server Setup Wizard

The installer will guide you through the steps required to install Malwarebytes Management Server on your computer.

WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

3. Read the License Agreement and select the "I Agree" radio button. Click *Next*.



License Agreement

Please take a moment to read the license agreement now. If you accept the terms below, click "I Agree", then "Next". Otherwise click "Cancel".

MALWAREBYTES ANTI-MALWARE
SOFTWARE LICENSE AGREEMENT

PLEASE READ THE FOLLOWING TERMS AND CONDITIONS CAREFULLY BEFORE DOWNLOADING, INSTALLING OR USING THE MALWAREBYTES ANTI-MALWARE SOFTWARE OR ANY ACCOMPANYING DOCUMENTATION (COLLECTIVELY, THE "SOFTWARE").

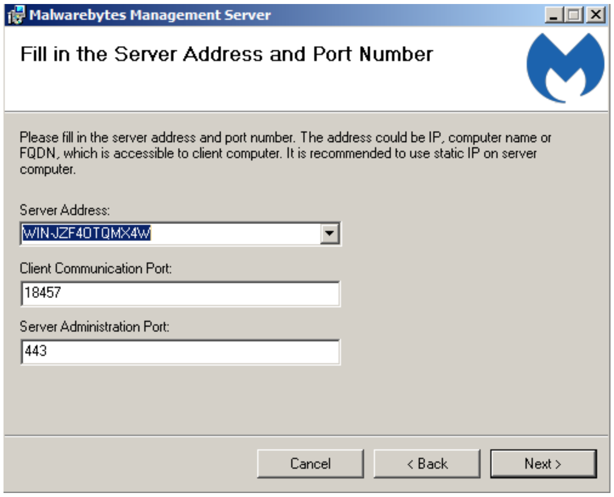
THE TERMS AND CONDITIONS OF THIS SOFTWARE LICENSE AGREEMENT AND THE MALWAREBYTES ORDERING DOCUMENT YOU EXECUTED OR

● I Do Not Agree ○ I Agree

4. Enter the Management Server address, Client Communication Port and Server Administration Port if they are not auto-populated for you. Your server address will be different from the one shown here. Port addresses may be changed if they conflict with existing needs.

   Click *Next*.

   WARNING: These settings control client/server communication. Changes made after client deployment may result in communication issues with that client.



Fill in the Server Address and Port Number

Please fill in the server address and port number. The address could be IP, computer name or FQDN, which is accessible to client computer. It is recommended to use static IP on server computer.

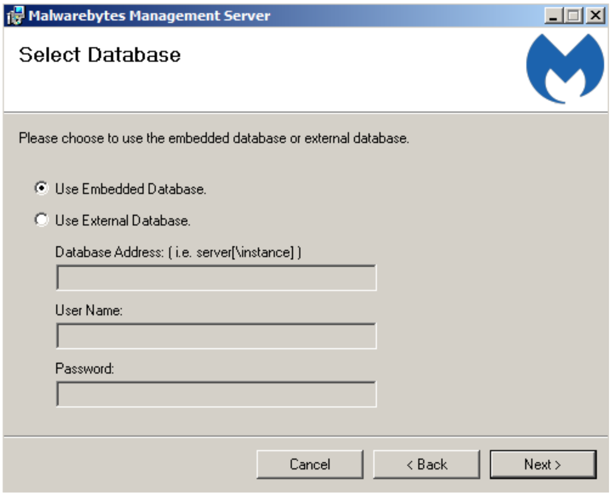
Server Address: WIN-JZF4OTQMX4W

Client Communication Port: 18457

Server Administration Port: 443

5. Choose whether to use the embedded SQL Server Express database or an existing database (SQL Server or SQL Express). If you use an existing database, you must specify the server and instance as well as the SQL Administrator username and password.

   Click *Next*.



Select Database

Please choose to use the embedded database or external database.

● Use Embedded Database.

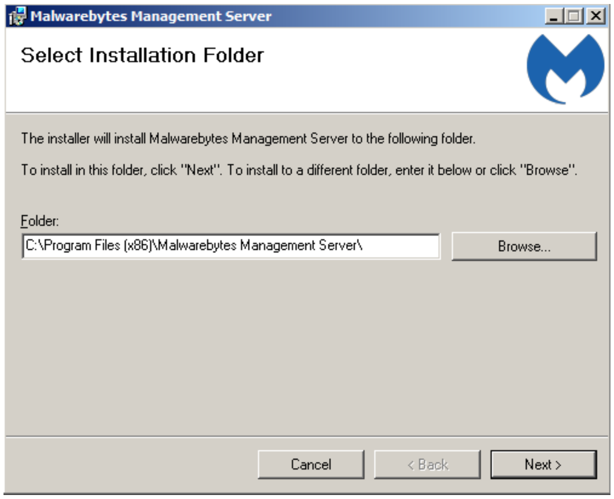
○ Use External Database.

Database Address: (i.e. server[\instance])

User Name:

Password:

6. Accept the default destination folder or browse and select another folder. Click *Next*.



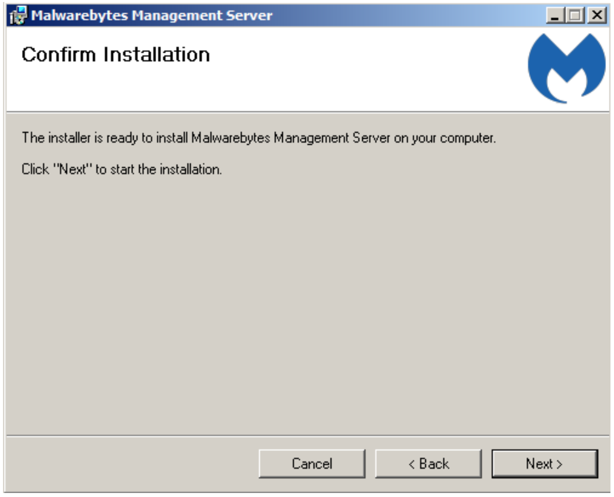
Select Installation Folder

The installer will install Malwarebytes Management Server to the following folder.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder: C:\Program Files (x86)\Malwarebytes Management Server\

7. Click *Next* to confirm installation.

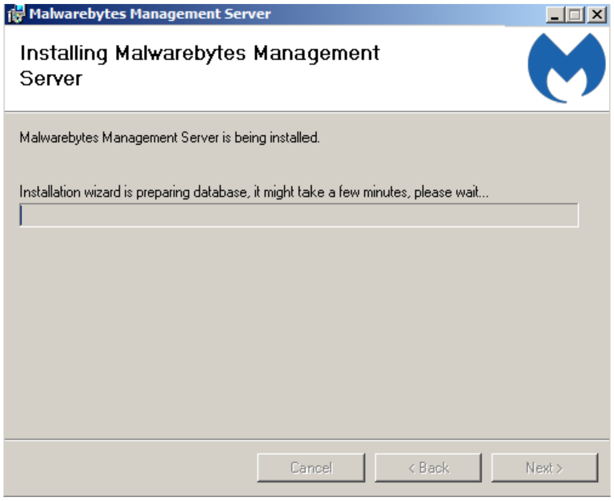


Confirm Installation

The installer is ready to install Malwarebytes Management Server on your computer.

Click "Next" to start the installation.

8. The installation progress window displays the installation as it takes place.



Installing Malwarebytes Management Server

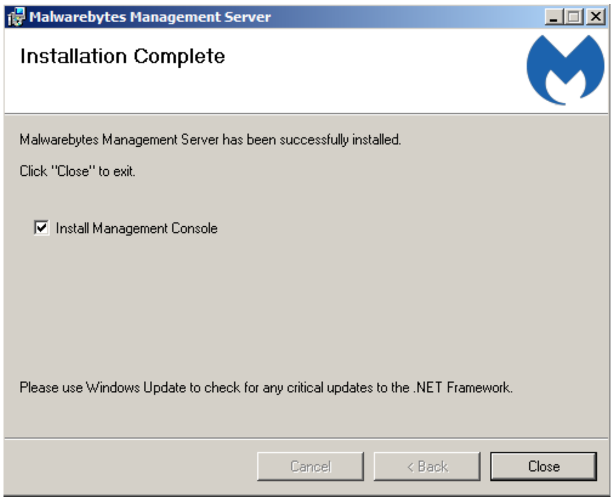
Malwarebytes Management Server is being installed.

Installation wizard is preparing database, it might take a few minutes, please wait...

9. This window opens following installation.

Leave the mark in the check box to Launch the *Management Server Console* installer.

Click *Close*.



Installation Complete

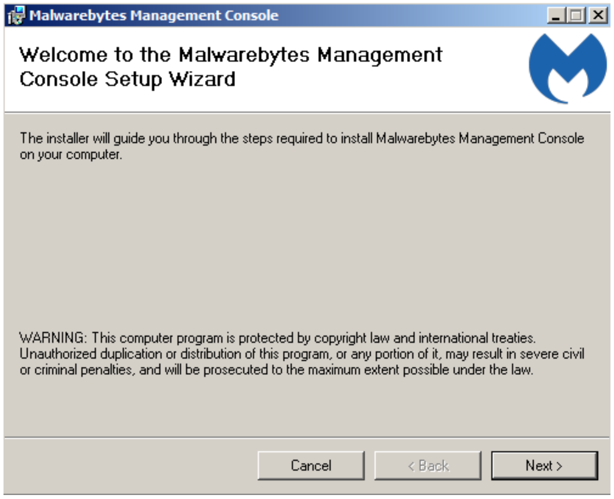
Malwarebytes Management Server has been successfully installed.

Click "Close" to exit.

☑ Install Management Console

Please use Windows Update to check for any critical updates to the .NET Framework.

10. Click Next to begin installation of the *Management Server Console*.



Malwarebytes Management Console

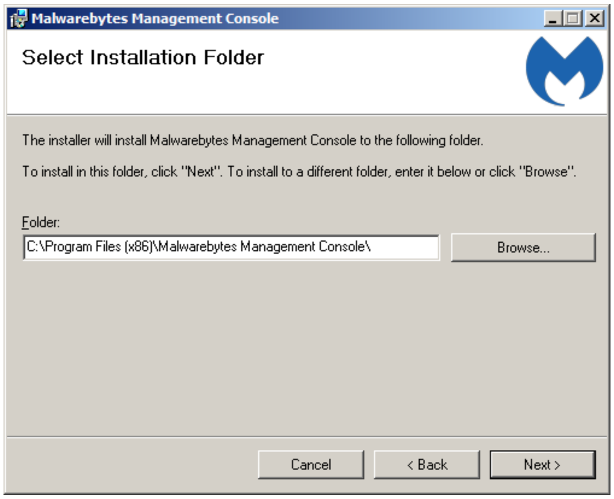
Welcome to the Malwarebytes Management Console Setup Wizard

The installer will guide you through the steps required to install Malwarebytes Management Console on your computer.

WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

11. Accept the default installation folder or browse and select another folder. Click *Next*.

.



Malwarebytes Management Console

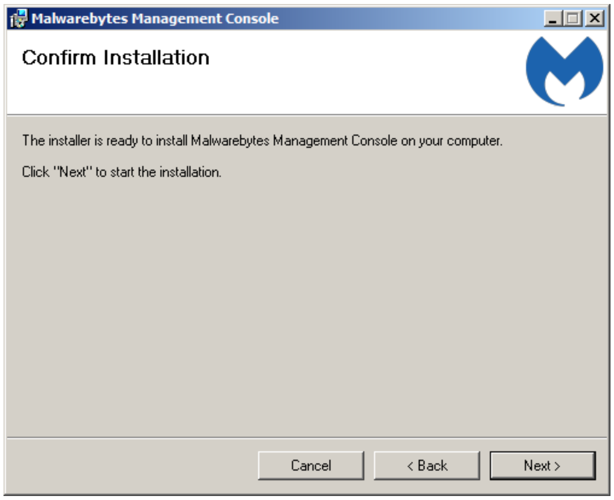
Select Installation Folder

The installer will install Malwarebytes Management Console to the following folder.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder:
C:\Program Files (x86)\Malwarebytes Management Console\

12. Click *Next* to confirm installation.



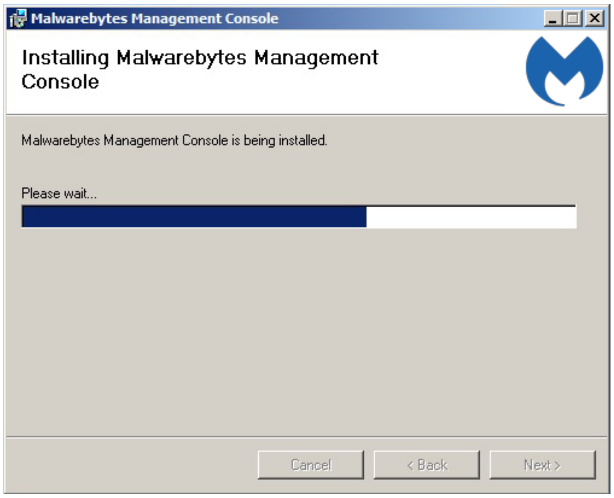
Malwarebytes Management Console

Confirm Installation

The installer is ready to install Malwarebytes Management Console on your computer.

Click "Next" to start the installation.

13. The installation progress window displays the installation as it takes place.



Installing Malwarebytes Management Console

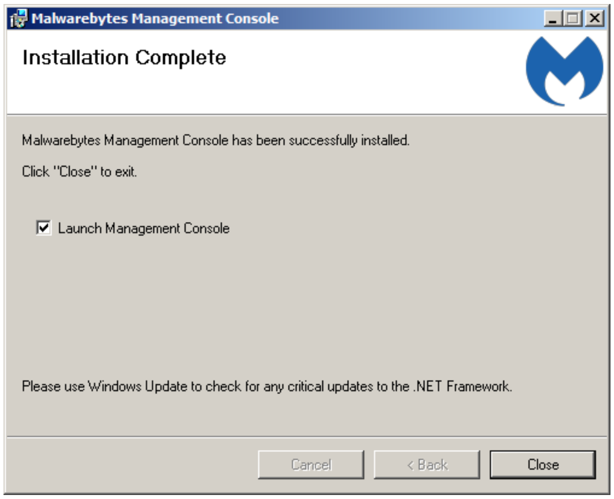
Malwarebytes Management Console is being installed.

Please wait...

14. The Installation Complete window opens when the installation finishes.

    Leave the mark in the check box to accept the default to *Launch Management Console*.

    Click *Close*.



Installation Complete

Malwarebytes Management Console has been successfully installed.

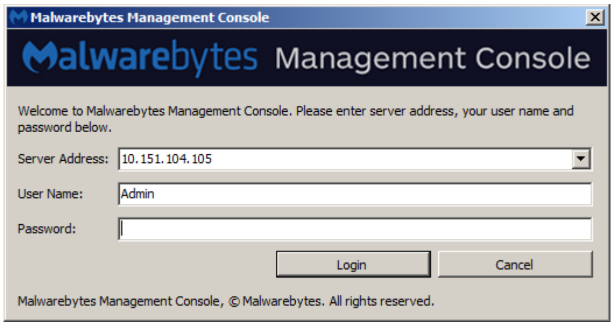
Click "Close" to exit.

☑ Launch Management Console

Please use Windows Update to check for any critical updates to the .NET Framework.

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

    The initial password is blank. You must create a new password before you can continue. Enter your new password and click *Login*.


Malwarebytes Management Console
Malwarebytes Management Console
Login
Cancel

Welcome to Malwarebytes Management Console. Please enter server address, your user name and password below.

Server Address: 10.151.104.105

User Name: Admin

Password:

Malwarebytes Management Console, © Malwarebytes. All rights reserved.

Upgrading Malwarebytes Management Console

When *Malwarebytes Management Console* is updated to a new version, existing clients are **not** updated as part of that process. If the new version contains new (or changed) client features which you consider to be important for those endpoints, you must install a new client over the top of the existing client. Please refer to page 22 to find out how to determine where new clients must be installed, and page 55 for information 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.

Introduction to Management Console

Malwarebytes Management Console is divided into four program modules, each accessible by buttons on the left edge of the user interface. Each module provides specific program functionality, and in many cases, functionality provided by one module serves as a foundation for the functionality of one or more other modules. Detailed functionality of each module will be described after the program layout has been outlined below. These modules are presented in the order which they appear in the user interface.

Home

Upon entry to the user interface, the Home page is displayed. While not a program module, the Home screen provides basic system status information pertaining to managed clients and threats detected by each client.

Client module

The Client module allows the *Malwarebytes Management Console* Administrator a dashboard view of all managed clients which have been installed on the corporate network, as well as detected endpoints which do not have managed clients installed. Limited information is available for endpoints without managed clients installed. Detailed status information is available for all managed clients, as well as access to system logs. Many operational functions are available from this screen. Clients may also be organized into a group, which allows functionality to be administered and controlled more easily.

Policy module

The Policy module enables the *Malwarebytes Management Console* Administrator to define rules and operational parameters that can be assigned to clients and client groups. In addition, this module allows installation packages to be built and deployed for endpoints that cannot be installed by standard means.

Report module

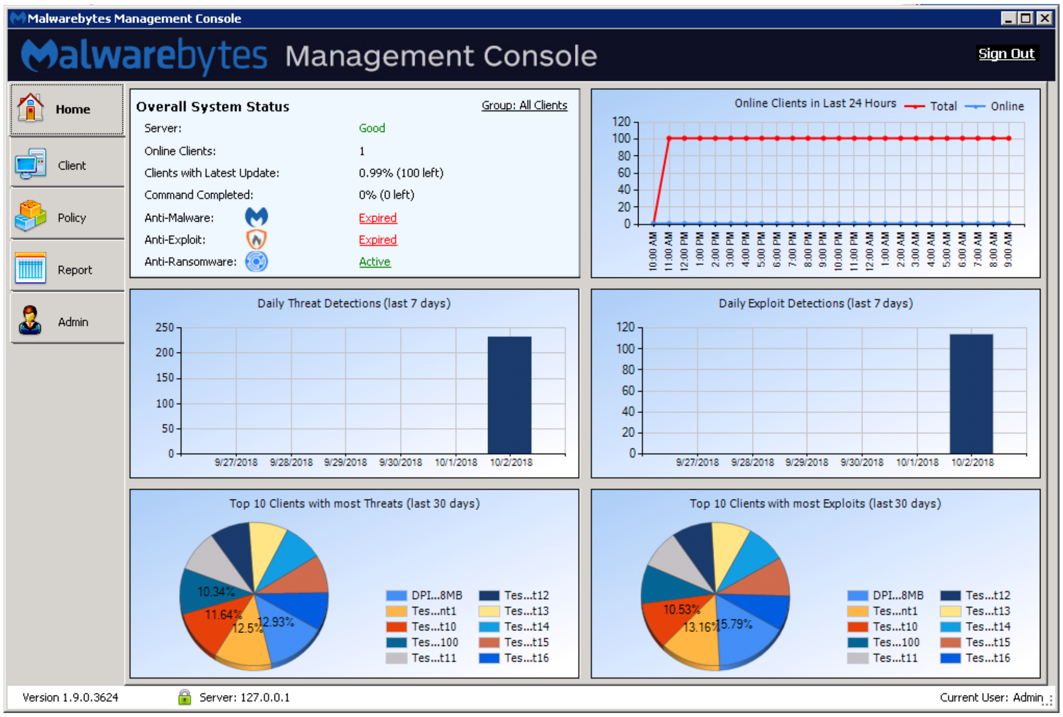
The Report module provides a comprehensive set of reports that provide detailed status on all aspects of *Malwarebytes Management Console* operation.

Admin module

The Admin module allows the *Malwarebytes Management Console* Administrator to control overall system functionality and how this functionality is interwoven with endpoint-specific and policy-specific functionality. In addition, this module provides the capability to define and oversee *Malwarebytes Management Console* users/administrators, and the specific types of program access granted to them.

Home Page Reports

When you launch *Malwarebytes Management Console*, the initial screen presented is the *Home* Page, which contains six high-level reports that provide basic status of your protected endpoints.



Overall System Status — Group: All Clients

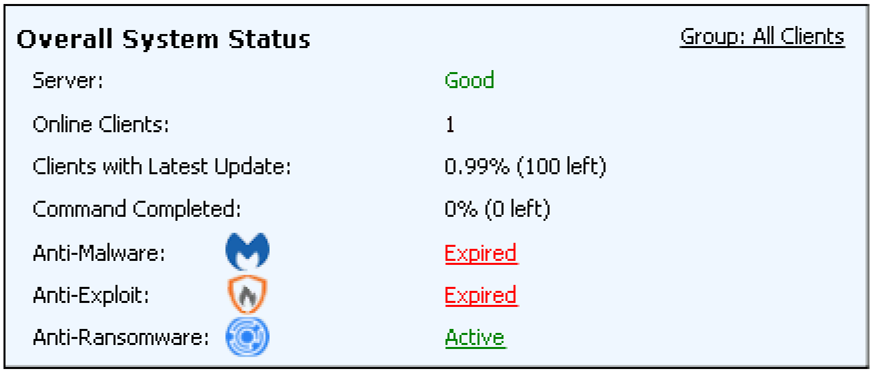
Server:	Good
Online Clients:	1
Clients with Latest Update:	0.99% (100 left)
Command Completed:	0% (0 left)
Anti-Malware:	Expired
Anti-Exploit:	Expired
Anti-Ransomware:	Active

Version 1.9.0.3624 Server: 127.0.0.1 Current User: Admin

Clicking on any of the graphical reports allows them to be superimposed over the *Home* Page in a larger format. Most reports are also available as individual reports (in the Reports module), accompanied by supporting data. Following is a list of the reports shown on this page, as well as a basic description of each.

Overall System Status

This report shows the condition of your server (good, normal, under stress), number of online endpoints, endpoints with latest update, number of commands completed, and the status of both Anti-Malware protection and Anti-Exploit protection.

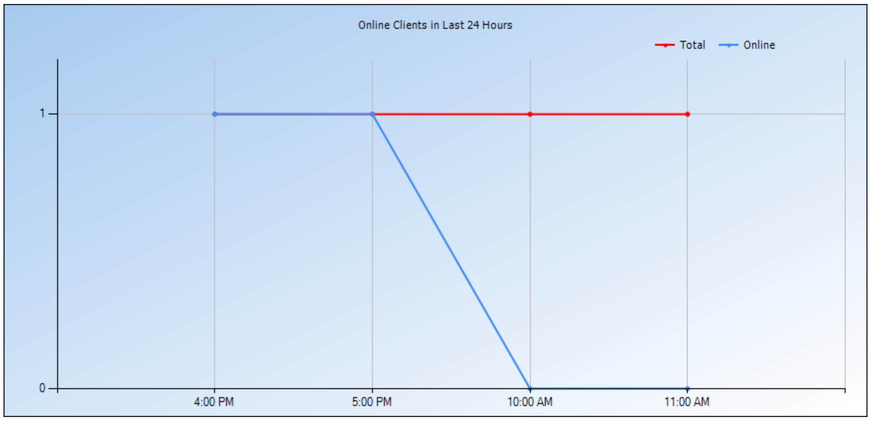


Overall System Status — Group: All Clients

Server:	Good
Online Clients:	1
Clients with Latest Update:	0.99% (100 left)
Command Completed:	0% (0 left)
Anti-Malware:	Expired
Anti-Exploit:	Expired
Anti-Ransomware:	Active

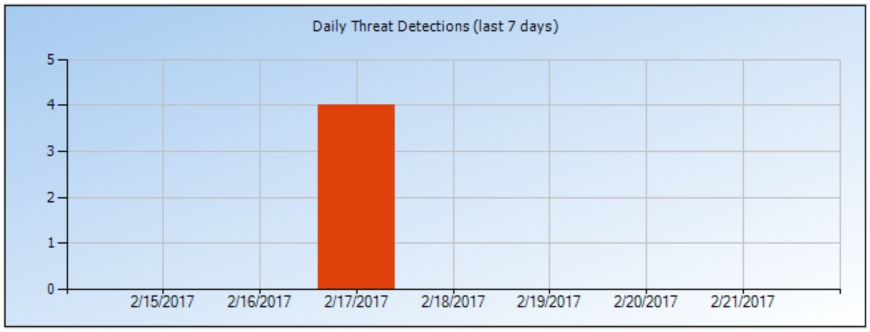
Online Clients in Last 24 Hours

This graph which shows the number of total endpoints registered within the last 24-hour period, as well as the number detected as being on-line.



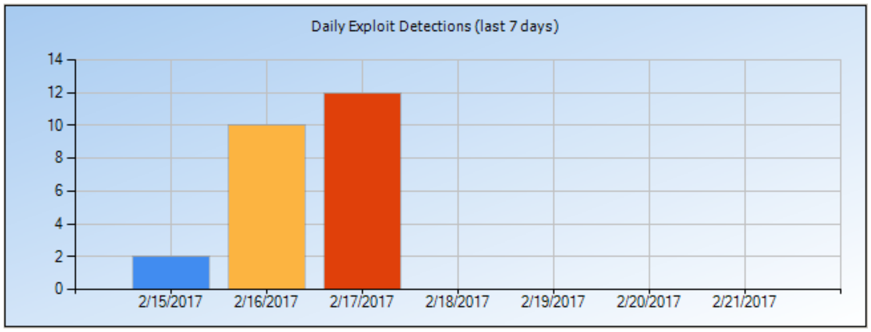
Daily Threat Detections (last 7/30 days)

This report shows how many threats were detected by the *Anti-Malware* managed client on each day. It can show up to seven days. Values along the vertical axis are the number of threats. Values along the horizontal axis are the dates when the threats occurred. Clicking on this report increases the days covered from 7 to 30.



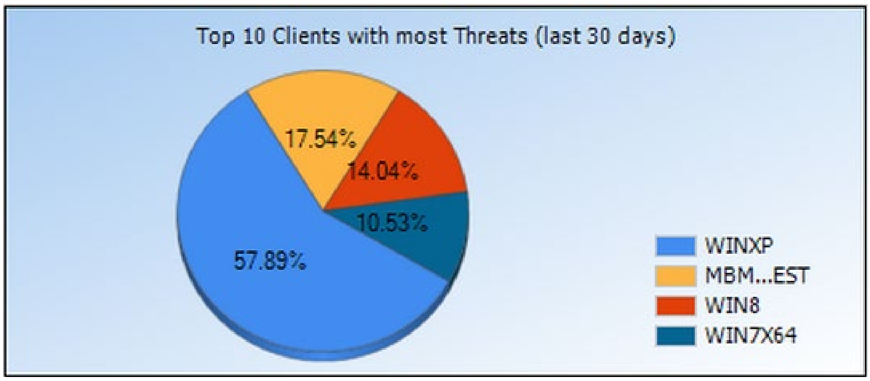
Daily Exploit Detections (last 7/30 days)

This report shows how many exploits were detected by the *Anti-Exploit* managed client on each day. It can show up to seven days. Values along the vertical axis are the number of exploits. Values along the horizontal axis are the dates when the exploits occurred. Clicking on this report increases the days covered from 7 to 30.



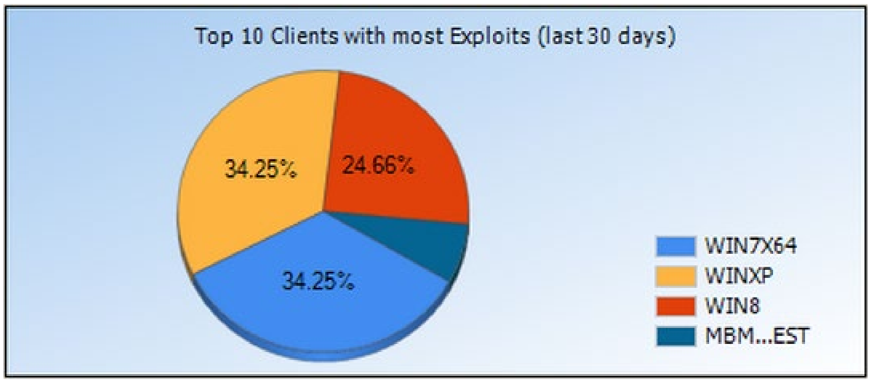
Top 10 Clients with Most Threats (last 30 days)

This report shows the top 10 endpoints with the most malware threats in the last 30 calendar days, as determined by the *Anti-Malware* managed client.



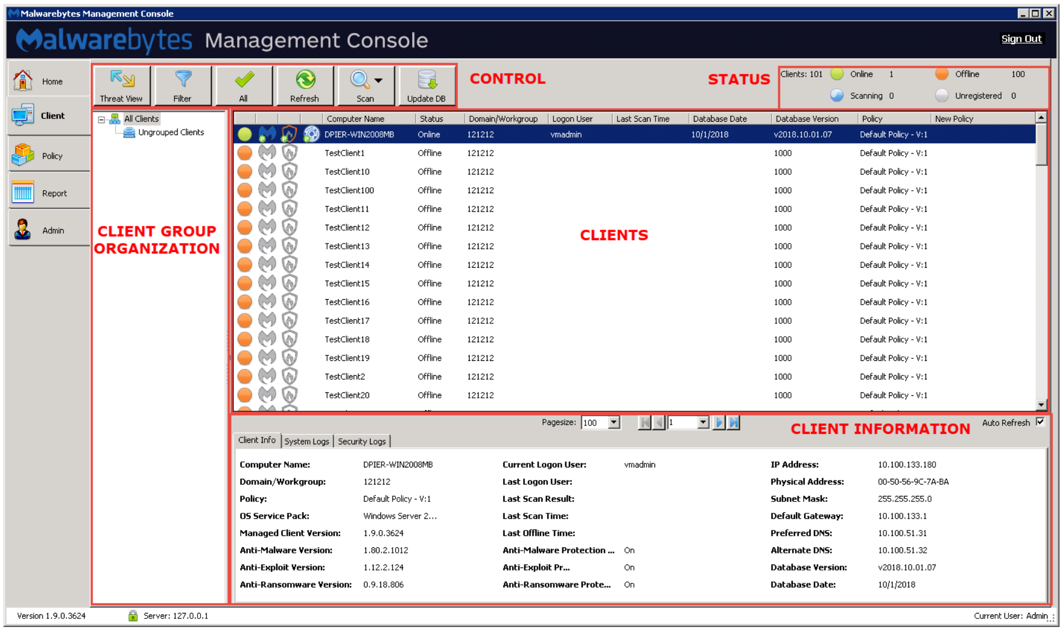
Top 10 Clients with Most Exploits (last 30 days)

This report shows the top 10 endpoints with the most exploit attempts in the last 30 calendar days, as determined by the *Anti-Exploit* managed client.



Client Module

The Client module enables you to monitor the status of all endpoints managed by *Malwarebytes Management Console*. The screenshot below shows the Client module, in *Client View* mode. The various main sections of the page are shown highlighted in red. A detailed description of all features follows.



Clients: 101 ● Online 1 ● Offline 100 ● Scanning 0 ○ Unregistered 0

Computer Name	Status	Domain/Workgroup	Logon User	Last Scan Time	Database Date	Database Version	Policy	New Policy
DPIER-WIN2008MB	Online	121212	vmadmin		10/1/2018	v2018.10.01.07	Default Policy - V:1	
TestClient1	Offline	121212				1000	Default Policy - V:1	
TestClient10	Offline	121212				1000	Default Policy - V:1	
TestClient100	Offline	121212				1000	Default Policy - V:1	
TestClient11	Offline	121212				1000	Default Policy - V:1	
TestClient12	Offline	121212				1000	Default Policy - V:1	
TestClient13	Offline	121212				1000	Default Policy - V:1	
TestClient14	Offline	121212				1000	Default Policy - V:1	
TestClient15	Offline	121212				1000	Default Policy - V:1	
TestClient16	Offline	121212				1000	Default Policy - V:1	
TestClient17	Offline	121212				1000	Default Policy - V:1	
TestClient18	Offline	121212				1000	Default Policy - V:1	
TestClient19	Offline	121212				1000	Default Policy - V:1	
TestClient2	Offline	121212				1000	Default Policy - V:1	
TestClient20	Offline	121212				1000	Default Policy - V:1	

Computer Name:	DPIER-WIN2008MB	**Current Logon User:**	vmadmin	**IP Address:**	10.100.133.180
Domain/Workgroup:	121212	**Last Logon User:**		**Physical Address:**	00-50-56-9C-7A-BA
Policy:	Default Policy - V:1	**Last Scan Result:**		**Subnet Mask:**	255.255.255.0
OS Service Pack:	Windows Server 2...	**Last Scan Time:**		**Default Gateway:**	10.100.133.1
Managed Client Version:	1.9.0.3624	**Last Offline Time:**		**Preferred DNS:**	10.100.51.31
Anti-Malware Version:	1.80.2.1012	**Anti-Malware Protection ...**	On	**Alternate DNS:**	10.100.51.32
Anti-Exploit Version:	1.12.2.124	**Anti-Exploit Pr...**	On	**Database Version:**	v2018.10.01.07
Anti-Ransomware Version:	0.9.18.806	**Anti-Ransomware Prote...**	On	**Database Date:**	10/1/2018

Control buttons

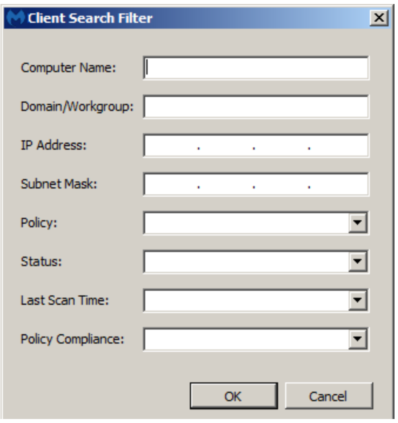
Functionality of the Control buttons is divided between Client module display characteristics and endpoint operations.

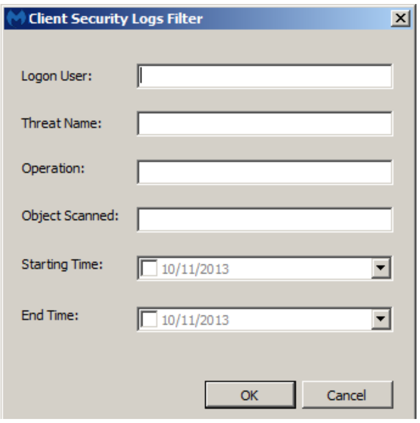
Threat View

Threat View specifically relates to detected threats, where found, and when. Threat view is very straightforward and easily understood on first glance. As a result, discussion of this module will focus on the Client View.

Filter/All

The Filter button allows you to filter information relating to endpoints (client view) or threats (threat view) so only that which is relevant is being displayed. Screenshots of the view-specific filter selection panels are shown below.





Starting Time: □ 10/11/2013

End Time: □ 10/11/2013

Most options need no explanation. The options listed below are explained so that you may utilize them more effectively.

- **Policy (client view) –** Policy created by *Malwarebytes Management Console* Administrator and deployed to endpoints
- **Status (client view) –** Status of the endpoint (offline, online and idle, scanning, unregistered)
- **Policy Compliance (client view) –** Whether the policy being used by the endpoint is current or out-of-date
- **Operation (threat view) –** End result of operations upon a detected threat (success, none, <blank>, quarantine, delete on reboot, or detail pertaining to blocked websites)
- **Object Scanned (threat view) –** Specific object (file, memory, registry key) where a threat was detected

To cancel the filtered view, click the *All* control button.

Refresh

Refresh simply keeps the screen updated. The *Auto Refresh* button (to the right of the Control buttons) will continuously update information, although it may prove to be disruptive when information of interest is not on the first page of the display.

Scan

Scan allows a scan to be performed on a selected endpoint (in the Clients panel). There are three types of scans which may be performed. These are:

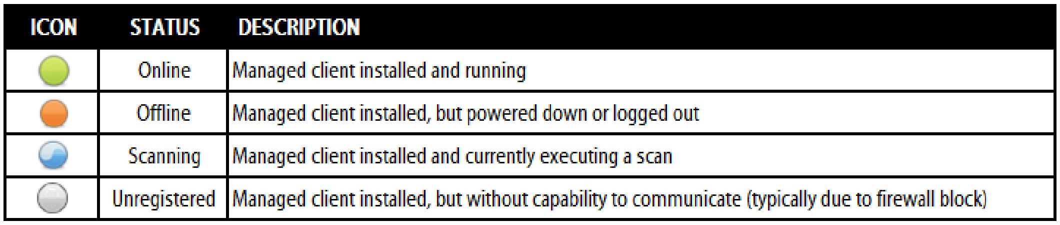
- **Quick Scan –** A scan of all system locations where malware is known to install itself. We recommend this method.
- **Full Scan –** Checks all files on selected drives as well as all areas scanned during a Quick Scan.
- **Flash Scan –** Scans system memory and startup locations for active infections.

Update DB

This option forces an immediate signature database update on the endpoint, using current signatures residing on the *Malwarebytes Management Console* server. If the selected endpoint is offline, a notification message is displayed to inform you that a database update will occur once the endpoint returns to online status.

Status indicators

Status of all endpoints is shown in the upper right corner of the Client module. Defined status settings are:



ICON	STATUS	DESCRIPTION
🟢	Online	Managed client installed and running
🟠	Offline	Managed client installed, but powered down or logged out
🔵	Scanning	Managed client installed and currently executing a scan
⚪	Unregistered	Managed client installed, but without capability to communicate (typically due to firewall block)

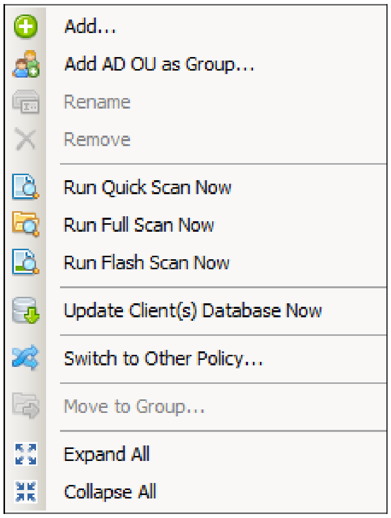
Client Group Organization panel

This panel allows addition of Client Groups, as well as certain operations based on specified Client Groups. The concept of Client Groups is a simple one. This allows endpoints to be organized into groups that either represent the way they are used, or the people/departments which use them. Groups allow the *Malwarebytes Management Console* Administrator to execute scans and updates in a coordinated manner. Combined with use of policies (to be discussed in the Policy Module section of this manual, beginning on page 24), server load and throughput can be maintained at high levels throughout the network while communication between *Malwarebytes Management Console* and endpoints takes place.

The presentation of this panel is similar in nature to Windows Explorer. Initially, the only group that exists is called *Ungrouped Clients*. You may add groups to suit your specific needs, and you may nest groups as deeply as you wish to create a granular structure, mimicking a Windows file system (as an example).

Right-Click Context Menu

All operations available in the *Client Group Organization* panel are performed using the right-click context menu, as shown below.



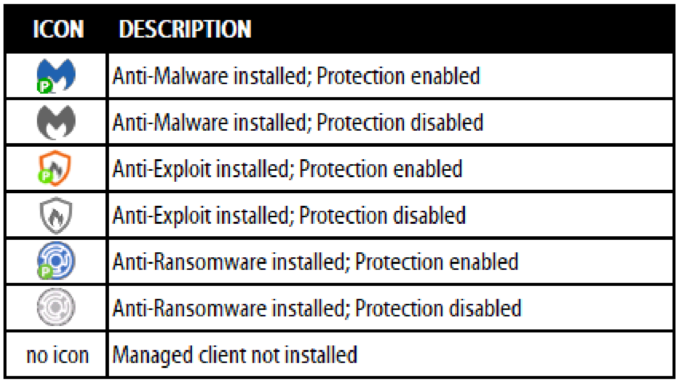
Following is a description of the operations which are available on this menu:

- **Add** – Add a new Client Group. The Group name must be unique as it pertains to the hierarchy in the group structure. To clarify, you could create a *Sales* group under *North America* as well as a *Sales* group under *Europe*, but you could not create two groups named *Sales* under *North America*.
- **Add AD OU as Group** – Add an Active Directory Organizational Unit as a Client Group. If your company utilizes Active Directory, you are already familiar with this concept as it is the basis of Group Policy Updates. This provides an extension to your existing methodology.
- **Rename** – Rename a Client Group. Names must maintain uniqueness within the same hierarchical level of the tree. Groups which have been added as Active Directory OUs may not be renamed.
- **Remove** – Remove a Client Group. If a Client Group is removed and there are endpoints which are members of that group, they will be moved to Ungrouped Clients.
- **Run Quick|Full|Flash Scan Now** – Run a scan of the type selected on all members of a selected Client Group. The various scan types are described in the Control discussion earlier in this section.
- **Update Client(s) Database Now** – Update signature databases on all members of a selected Client Group. Please note that while you could perform this operation on All Clients (the highest level of the tree), you may experience network performance issues due to the number of endpoints receiving updates concurrently.
- **Switch to Other Policy…** – Change all members of a selected Client Group to a new protection policy.
- **Move to Group…** – Move a selected Client Group to a new location in the tree, as a child directory of another group selected from a pulldown menu.
- **Expand All** – Expands the tree structure, using the selected Client Group as the top level of the tree.
- **Collapse All** – Collapses the tree structure, using the selected Client Group as the top level of the tree.

Clients panel

This panel provides high-level information for all endpoints in the network. For the most part, this panel is self-explanatory. Three items do merit additional comments.

- The status of Malwarebytes managed clients is shown just to the left of each endpoint. The following table indicates the possible states of the status icons.



ICON	DESCRIPTION
	Anti-Malware installed; Protection enabled
	Anti-Malware installed; Protection disabled
	Anti-Exploit installed; Protection enabled
	Anti-Exploit installed; Protection disabled
	Anti-Ransomware installed; Protection enabled
	Anti-Ransomware installed; Protection disabled
no icon	Managed client not installed

- *New Policy* only contains information on an interim basis. When the policy associated with an endpoint is changed, *Policy* is the "before" state and *New Policy* is the "after" state until the next time that the endpoint communicates with the server (defined on the *Communication* tab for the policy in the *Policy* module). Once the endpoint communicates with the server, *Policy* will show the "after" state and *New Policy* will be cleared.

- The status line containing endpoint information may at times be highlighted in alternate colors. If this line is highlighted in **red**, this indicates that a threat was detected. Even if the threat is removed, the red highlight remains until the next scheduled scan, or until a manual scan is performed on the endpoint. This is done specifically to draw attention to the event. **Yellow** highlighting indicates the endpoint is using an outdated policy or outdated signatures. If the situation clears, the yellow highlight will return to normal. If highlighting remains yellow, that likely indicates a communication problem between the endpoint and server which prevents the endpoint from getting current information.

Customizing Columns on the Client Tab

Information shown here is easily customized. By right-clicking on any column name, you can customize the columns which appear. Following are the various information fields which may be displayed. Fields shown in **bold print** are displayed by default.

● **Domain/Workgroup**	● IP Address
● **Logon User**	● Physical Address
● **Last Scan Time**	● Subnet Mask
● **Database Date**	● Default Gateway
● **Database Version**	● Preferred DNS
● **Policy**	● Alternate DNS
● **New Policy**	● Managed Client Version
● **Status**	● Anti-Exploit Version
● Last Logon User	● Anti-Malware Version
● Last Scan Result	● Anti-Malware Protection Module
● Last Offline Time	● Anti-Exploit Protection Module
● OS Service Pack	

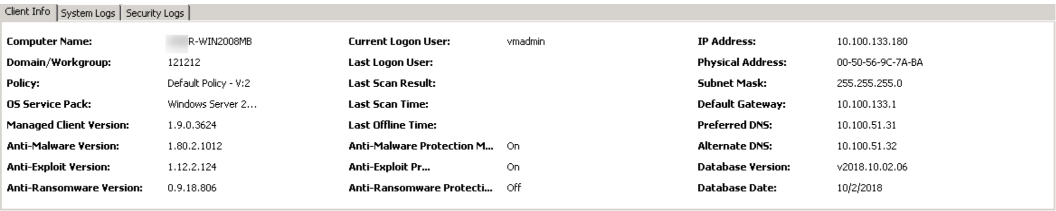
Checked fields may be hidden by clicking *Hide*. Unchecked fields may be displayed by clicking *Show*. Clicking the checkmark to change the state of the checkbox also has the same effect. You may also clear all client logs from the right-click menu.

Client Information panel

This panel provides detailed information pertaining to an endpoint which has been selected in the Clients panel. This panel is present only when an endpoint has been selected. Information displayed is broken down into three categories. Each is shown below, with supplemental screenshots to illustrate their purpose.

Client Info

Although detailed, this can be considered as summary information for the endpoint, its network connection, basic usage information, and certain Malwarebytes installation parameters. All information shown is read-only.



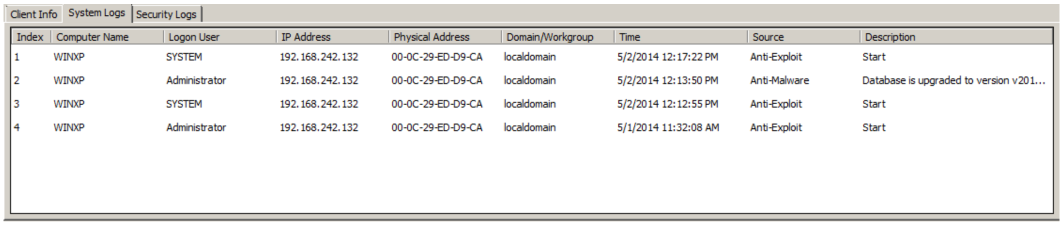
Computer Name:	[redacted]R-WIN2008MB	**Current Logon User:**	vmadmin	**IP Address:**	10.100.133.180
Domain/Workgroup:	121212	**Last Logon User:**		**Physical Address:**	00-50-56-9C-7A-BA
Policy:	Default Policy - V:2	**Last Scan Result:**		**Subnet Mask:**	255.255.255.0
OS Service Pack:	Windows Server 2...	**Last Scan Time:**		**Default Gateway:**	10.100.133.1
Managed Client Version:	1.9.0.3624	**Last Offline Time:**		**Preferred DNS:**	10.100.51.31
Anti-Malware Version:	1.80.2.1012	**Anti-Malware Protection M...**	On	**Alternate DNS:**	10.100.51.32
Anti-Exploit Version:	1.12.2.124	**Anti-Exploit Pr...**	On	**Database Version:**	v2018.10.02.06
Anti-Ransomware Version:	0.9.18.806	**Anti-Ransomware Protecti...**	Off	**Database Date:**	10/2/2018

Please note the entry for Managed Client Version on te left side. This indicates the version of *Malwarebytes Enterprise Edition* or *Malwarebytes Management Console* in use when the current client was installed. For users upgrading from a previous version, this also indicates functional limitations that are present in clients until a new push install is performed to upgrade the client.

As an example, clients with a Managed Client Version 1.8.x.*xxxx* have a newer version of *Malwarebytes Anti-Exploit* than clients with a version of 1.7.x.*xxxx*. This is insignificant for customers who are not using *Malwarebytes Anti-Exploit* on their clients, but important to those who are.

System Logs

This panel provides status for the endpoint. Scans and abbreviated scan results are available here, as are dates, times and results of signature database updates. If an endpoint is highlighted in yellow (in the Clients panel) – indicating an update issue – you can gain further information regarding that issue here.

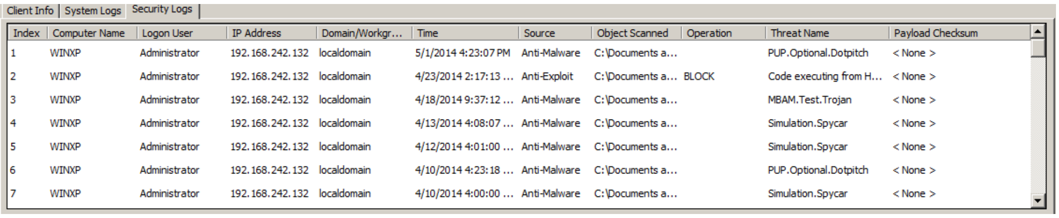


Index	Computer Name	Logon User	IP Address	Physical Address	Domain/Workgroup	Time	Source	Description
1	WINXP	SYSTEM	192.168.242.132	00-0C-29-ED-D9-CA	localdomain	5/2/2014 12:17:22 PM	Anti-Exploit	Start
2	WINXP	Administrator	192.168.242.132	00-0C-29-ED-D9-CA	localdomain	5/2/2014 12:13:50 PM	Anti-Malware	Database is upgraded to version v201...
3	WINXP	SYSTEM	192.168.242.132	00-0C-29-ED-D9-CA	localdomain	5/2/2014 12:12:55 PM	Anti-Exploit	Start
4	WINXP	Administrator	192.168.242.132	00-0C-29-ED-D9-CA	localdomain	5/1/2014 11:32:08 AM	Anti-Exploit	Start

You may use the scrollbar on the right side of this panel to scroll through all available status information. Initially, status information is available going back to installation of the managed client. If logs have been subsequently purged, information occurring before that date will no longer be available.

Security Logs

This panel provides information about specific threats and exploits which have been detected on the selected endpoint, as well as the resolution of those threats and exploits. As mentioned previously, threats are processed by the *Anti-Malware* managed client, and exploits are processed by the *Anti-Exploit* managed client.



Index	Computer Name	Logon User	IP Address	Domain/Workgr...	Time	Source	Object Scanned	Operation	Threat Name	Payload Checksum
1	WINXP	Administrator	192.168.242.132	localdomain	5/1/2014 4:23:07 PM	Anti-Malware	C:\Documents a...		PUP.Optional.Dotpitch	< None >
2	WINXP	Administrator	192.168.242.132	localdomain	4/23/2014 2:17:13 ...	Anti-Exploit	C:\Documents a...	BLOCK	Code executing from H...	< None >
3	WINXP	Administrator	192.168.242.132	localdomain	4/18/2014 9:37:12 ...	Anti-Malware	C:\Documents a...		MBAM.Test.Trojan	< None >
4	WINXP	Administrator	192.168.242.132	localdomain	4/13/2014 4:08:07 ...	Anti-Malware	C:\Documents a...		Simulation.Spycar	< None >
5	WINXP	Administrator	192.168.242.132	localdomain	4/12/2014 4:01:00 ...	Anti-Malware	C:\Documents a...		Simulation.Spycar	< None >
6	WINXP	Administrator	192.168.242.132	localdomain	4/10/2014 4:23:18 ...	Anti-Malware	C:\Documents a...		PUP.Optional.Dotpitch	< None >
7	WINXP	Administrator	192.168.242.132	localdomain	4/10/2014 4:00:00 ...	Anti-Malware	C:\Documents a...		Simulation.Spycar	< None >

You may use the scrollbar on the right side of this panel to scroll through all threats/exploits. Initially, status information is available going back to installation of the managed client. If logs have been subsequently purged, information occurring before that date will no longer be available.

Exporting Data

Information contained throughout various areas of the *Client* module can be exported to a CSV file. This is helpful in scenarios where custom reporting is necessary, or when information needs to be provided to personnel who do not access the console.

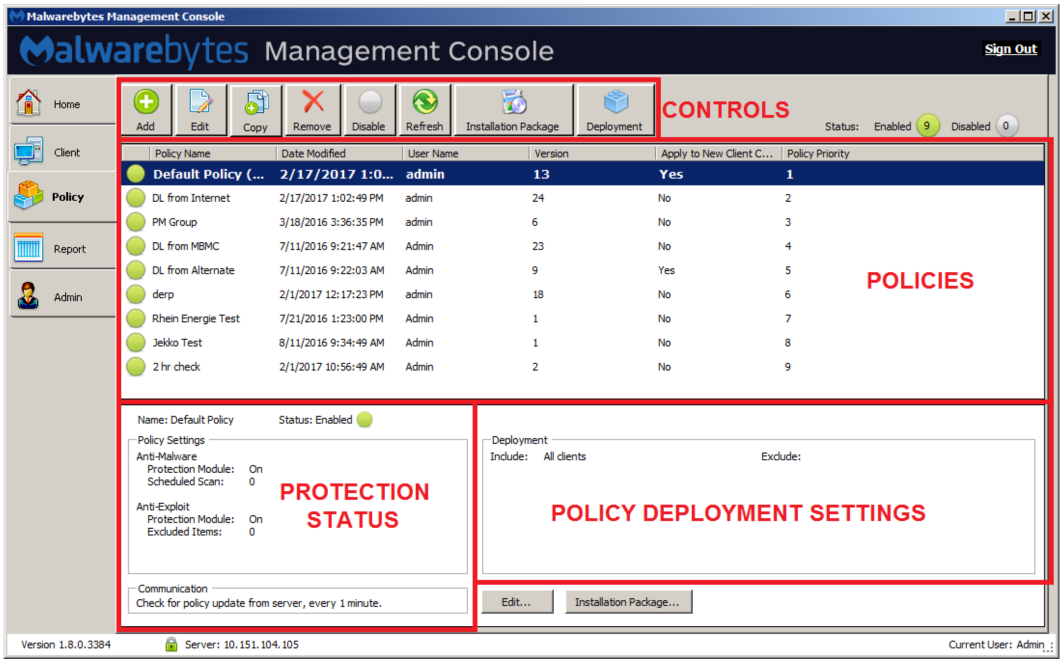
Data can be exported from the following areas via a right-click context menu, and selecting the appropriate action:

- Client View grid (Export Client View…)
- Threat View grid (Export Threat View…)
- System Logs tab (Export System Logs…)
- Security Logs tab (Export Security Logs…)

Data is exported based on the current view and visible columns. For example, if 100 rows are visible per page, but you want to export data for all pages, you will need to change the *Pagesize* to *all* before exporting.

Policy Module

The Policy Module allows the *Malwarebytes Management Console* Administrator to define one or more policies which describe specifically how *Anti-Malware*, *Anti-Exploit,* and *Anti-Ransomware* managed clients protect endpoints. Once defined, installation packages may be created which allow pre-configured managed clients to be packaged for deployment using alternative means. In this section, we will discuss each of the features and components which provide this functionality. The following is a screenshot of the Policy Module screen, marked (in red) to show the major sections of the screen.



Policy Name	Date Modified	User Name	Version	Apply to New Client C...	Policy Priority
Default Policy (...	2/17/2017 1:0...	admin	13	Yes	1
DL from Internet	2/17/2017 1:02:49 PM	admin	24	No	2
PM Group	3/18/2016 3:36:35 PM	admin	6	No	3
DL from MBMC	7/11/2016 9:21:47 AM	Admin	23	No	4
DL from Alternate	7/11/2016 9:22:03 AM	Admin	9	Yes	5
derp	2/1/2017 12:17:23 PM	admin	18	No	6
Rhein Energie Test	7/21/2016 1:23:00 PM	Admin	1	No	7
Jekko Test	8/11/2016 9:34:49 AM	Admin	1	No	8
2 hr check	2/1/2017 10:56:49 AM	Admin	2	No	9

Name: Default Policy Status: Enabled

Policy Settings

Anti-Malware
Protection Module: On
Scheduled Scan: 0

Anti-Exploit
Protection Module: On
Excluded Items: 0

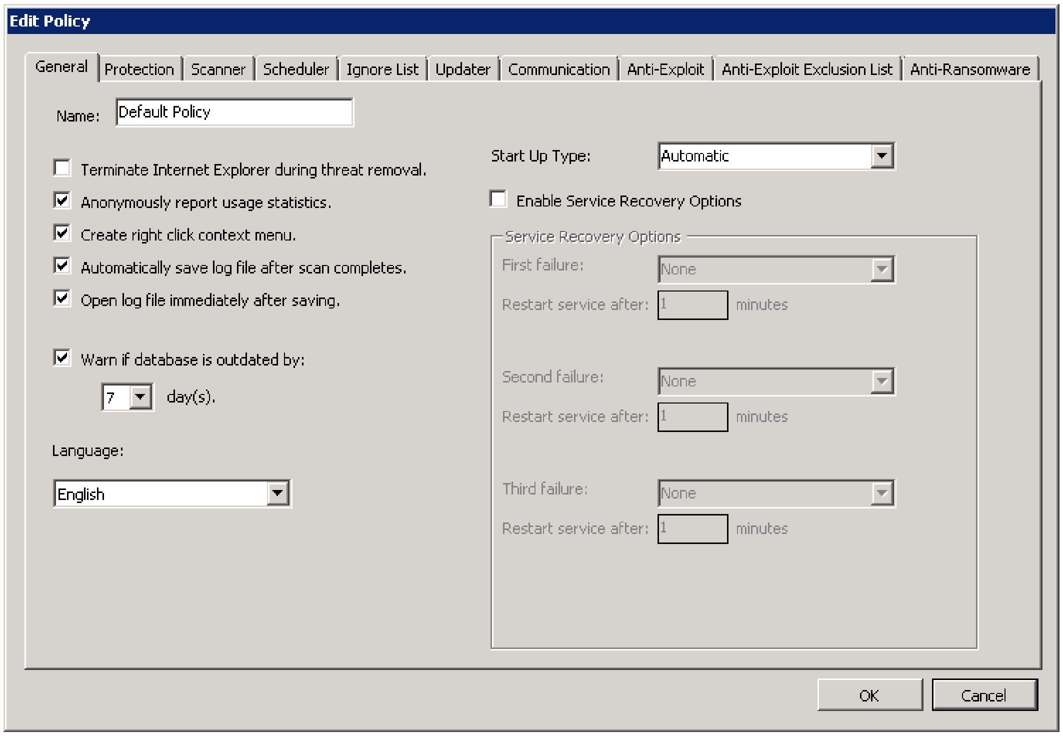
Communication
Check for policy update from server, every 1 minute.

Deployment
Include: All clients Exclude:

The Controls section operates primarily on selected policies, but also provides some generic functionality. The Policies section displays all policies which have been defined. Protection Status shows settings for the selected policy – in this case, the Default Policy. Policy Deployment Settings show which endpoints that the selected policy is defined for. We will begin discussion of policies by adding a new policy.

Add New Policy

Clicking the *Add* button in the Controls section launches the *New Policy* dialog box. This dialog box contains several tabs which allow a policy to be created which is very specific to your needs. **Please note** that the same configuration panels are used when adding a new policy or when editing an existing policy. The title bar is updated to display New Policy or Edit Policy depending on the mode selected.



Name: Default Policy

□ Terminate Internet Explorer during threat removal.

☑ Anonymously report usage statistics.

☑ Create right click context menu.

☑ Automatically save log file after scan completes.

☑ Open log file immediately after saving.

☑ Warn if database is outdated by:

7 day(s).

Language:

English

Start Up Type: Automatic

□ Enable Service Recovery Options

Service Recovery Options

First failure: None

Restart service after: 1 minutes

Second failure: None

Restart service after: 1 minutes

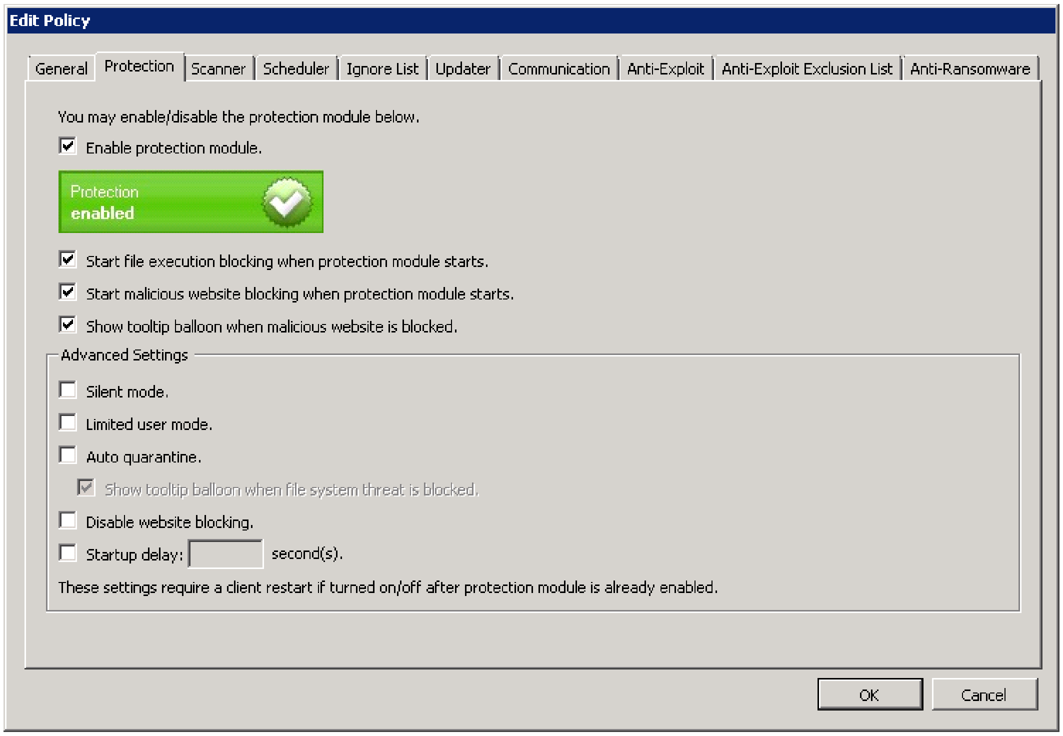
Third failure: None

Restart service after: 1 minutes

General Settings

The General Settings tab is used to name the policy, and to define basic policy behavior. Most of the settings here are self-explanatory, but a few are worth mentioning.

- The name specified for the policy must be unique.
- It may be necessary to terminate Internet Explorer during removal of certain threats. If this is the case, this checkbox may be checked and a scan executed after the policy has propagated out to the endpoint. Terminating Internet Explorer is obviously disruptive to the user, so this should only be done when necessary.
- The client is programmed to communicate information about threats detected to Malwarebytes corporate servers, to assist us in providing effective anti-malware solutions. At no time is information pertaining to your machines, your networks or your environment transmitted. You may uncheck the *Anonymously report usage statistics* checkbox if you wish, with no loss of functionality.
- You may check the *Create Right Click Context Menu* checkbox so that the endpoint user protected by the client can scan an individual file from within Windows Explorer by right-clicking the mouse. The context menu is available to the user whether or not this checkbox is checked, only the presence/absence of Malwarebytes protection as a menu choice is affected.
- Most settings here are related to behavior of the *Anti-Malware* managed client. The language setting is also associated with the *Anti-Exploit* managed client.
- The settings to the right, under **Start Up Type**, control the behavior of the endpoint client communicator service. You can change how the service starts, and how the service recovers in the case where it fails.



You may enable/disable the protection module below.

☑ Enable protection module.

☑ Start file execution blocking when protection module starts.

☑ Start malicious website blocking when protection module starts.

☑ Show tooltip balloon when malicious website is blocked.

Advanced Settings

□ Silent mode.

□ Limited user mode.

□ Auto quarantine.

☑ Show tooltip balloon when file system threat is blocked.

□ Disable website blocking.

□ Startup delay: ____ second(s).

These settings require a client restart if turned on/off after protection module is already enabled.

Protection Settings

The Protection Settings tab pertains to the *Anti-Malware* managed client. It is used to enable/disable real-time protection on the endpoint, and to define behavior of the Protection module. By default, the Protection module is enabled. If it is disabled, the green box with the embedded checkmark is replaced by a red box with an embedded 'X'. Settings are as shown in the above screenshot. Information about each of the Protection settings is as follows:

- While a majority of users choose to use file execution blocking, situations may arise which require that file execution blocking be disabled. These situations are rare, and are usually determined as a result of troubleshooting with or without support of Malwarebytes Business Support. A majority of these cases can be handled through usage of the Ignore List, which will be discussed later in this section.

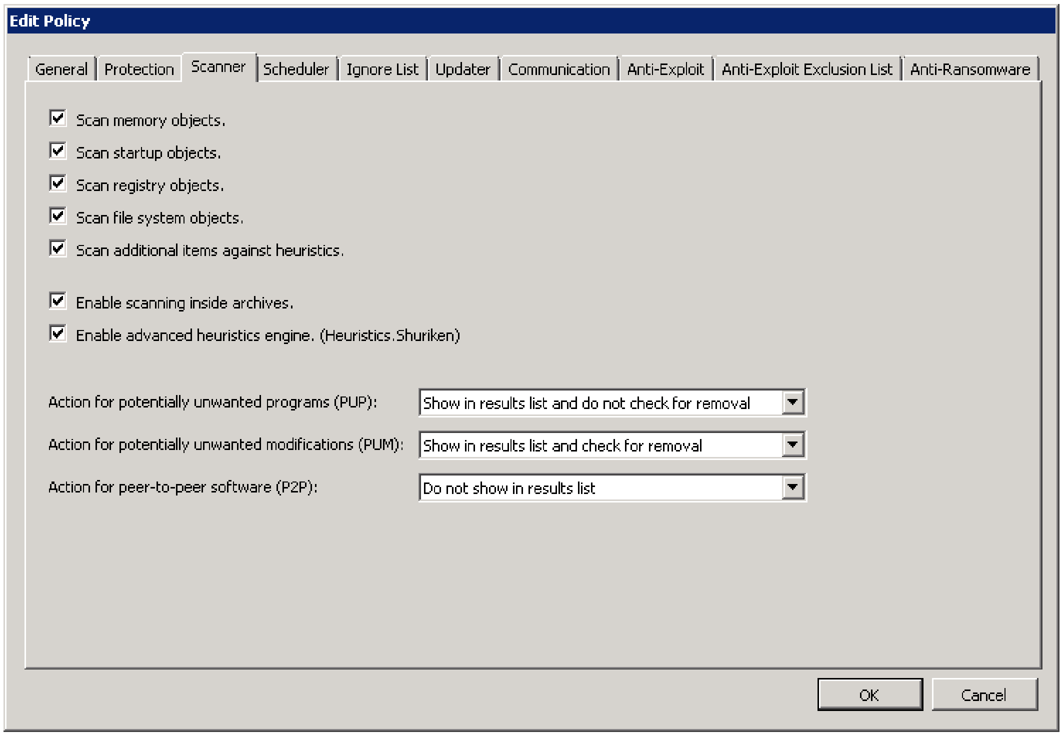
- As with file execution blocking, most users prefer to use malicious website blocking. In rare cases, a user may want or need to visit websites of this type. In this case, malicious website blocking may be disabled or blocking of specific websites may be disabled through use of the Ignore List, to be discussed later.

- Advanced Settings allow the *Malwarebytes Management Console* Administrator to configure the managed client to run with less of a user interface than normal, by selecting *Silent* mode or *Limited user* mode. In *Silent* mode, the only indication that the managed client is present on their machine is the right-click context menu, *if* that has been enabled on the General Settings tab. In *Limited user* mode, the managed client is visible as an icon in the system tray, but only with options to start a scan or to check for updates. The right-click context menu is available there as well, if enabled via General Settings.

- *Auto Quarantine* allows files detected as threats to be automatically moved to Quarantine, assuring they cannot be executed or modified. If this option is unchecked, detection of files classified as threats result in notifications being presented to the user while the file remains unaffected.

> **WARNING:** If legitimate files are detected as threats and Auto Quarantine is turned on, functionality related to these files would be adversely affected. Legitimate files detected in this manner should be added to the Ignore List.

- *Startup Delay* allows the Protection Module to delay activation by the number of seconds specified. In certain circumstances, endpoints using the Protection Module experience performance issues, usually related to slow startup. This is most common with Windows XP-based endpoints, though it may occur with other OS versions as well, depending on specific programs that are executed or initiated at startup. If this occurs in your environment, contact Malwarebytes Business Support for troubleshooting assistance.



☑ Scan memory objects.
☑ Scan startup objects.
☑ Scan registry objects.
☑ Scan file system objects.
☑ Scan additional items against heuristics.

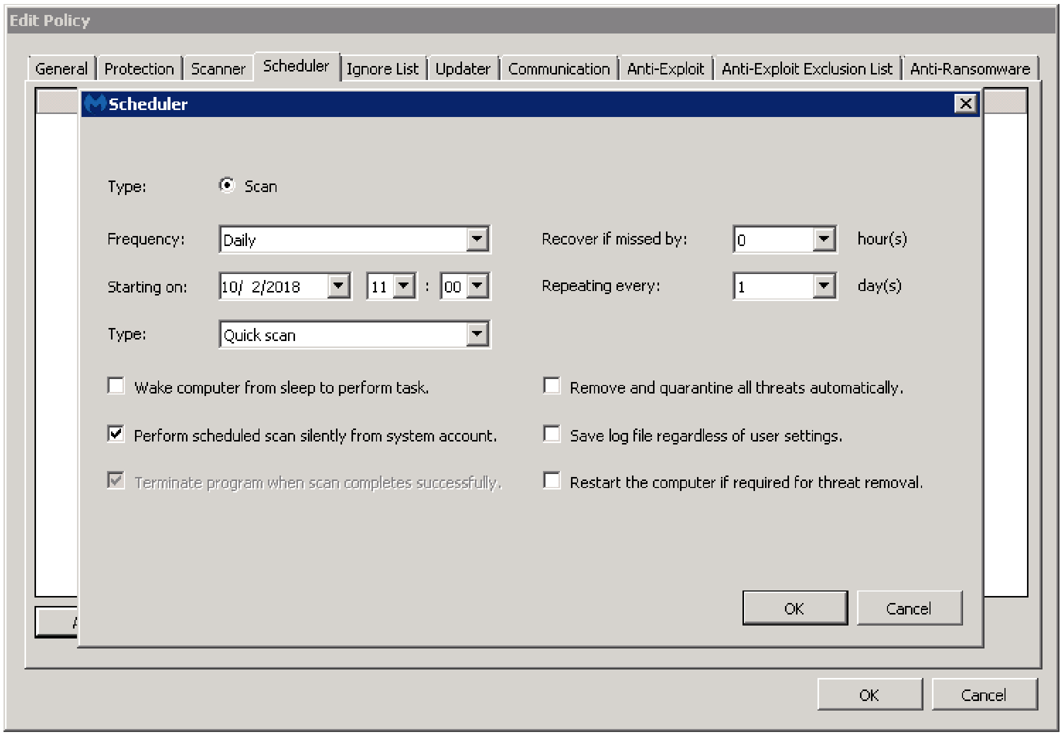
☑ Enable scanning inside archives.
☑ Enable advanced heuristics engine. (Heuristics.Shuriken)

Action for potentially unwanted programs (PUP): Show in results list and do not check for removal
Action for potentially unwanted modifications (PUM): Show in results list and check for removal
Action for peer-to-peer software (P2P): Do not show in results list

Scanner Settings

This tab specifies behavior of the *Anti-Malware* managed client during scanning (as compared to real-time protection offered by the Protection Module). Objects that may be selected are straight forward. The remaining settings are addressed as follows:

- There is no provision for scanning files or objects which are encrypted or password-protected.
- A Potentially Unwanted Program (PUP) is defined based on the following criteria:
  - Does a user intentionally install the program?
  - If the user notices the program and sees that it can be removed, do they intentionally remove it?
  - Do users typically refer to the program as malware, virus, or other non-benign label?
- A Potentially Unwanted Modification (PUM) typically takes the form of a registry edit or Active Directory Group Policy edit. By default, Malwarebytes will remove the PUM. You may override the default action via settings, or place a specific legitimate edit into the Ignore List.
- Peer-to-Peer (P2P) software is not shown in scan results by default. It is becoming more accepted as a means of updating commercial software, and is sometimes being used by corporate customers for software distribution within the enterprise. You may override the default setting based on your own requirements.



Type: ● Scan

Frequency: Daily

Starting on: 10/ 2/2018 11 : 00

Type: Quick scan

Recover if missed by: 0 hour(s)

Repeating every: 1 day(s)

□ Wake computer from sleep to perform task.

☑ Perform scheduled scan silently from system account.

☑ Terminate program when scan completes successfully.

□ Remove and quarantine all threats automatically.

□ Save log file regardless of user settings.

□ Restart the computer if required for threat removal.

Scheduler Settings

The Scheduler Settings tab allows addition, modifications and deletions of scans executed by the *Anti-Malware* managed client, under control of the policy. Added information to further describe Scheduler options are as follows:

- *Wake computer from sleep to perform task* allows an endpoint to be awakened from sleep mode if it is equipped with Wake-on-LAN hardware capability. Without this capability, the scan is based on the recovery setting specified here.
- *Perform scheduled scan silently from system account* when checked means that scans occur in the background, with no user interaction required. When unchecked, the scan is executed in the foreground by the logged-in user account.
- *Terminate program when scan completes successfully* checkbox determines whether the managed client user interface remains present on the user's screen if no threats were detected during a scan. This checkbox is relevant only if scans are executed by the logged-in user rather than the system account.
- *Restart the computer if required for threat removal* is not set by default. Checking this box would compromise the integrity of work being performed on that endpoint if a restart occurs. A log entry is created if a restart is required.

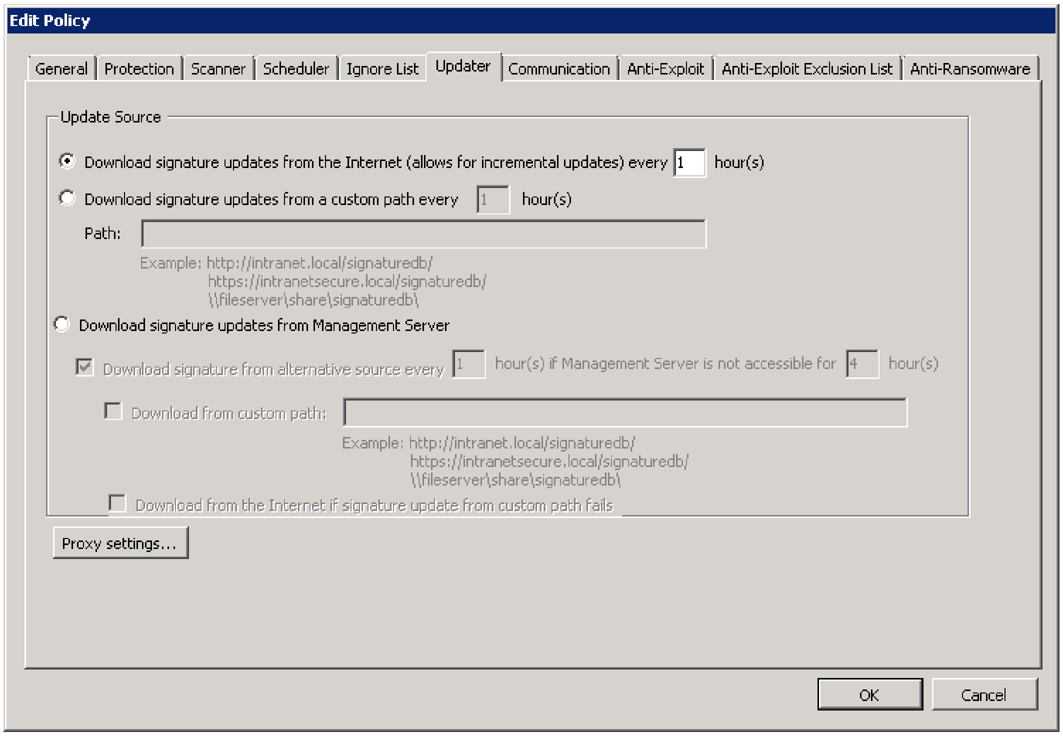
Once a new scan has been defined, you may highlight the scan in the New Policy window to edit or delete the scan. You may also add additional scans to be governed by the policy.

Ignore List

The Ignore List provides capability for the *Malwarebytes Management Console* Administrator to specify IP addresses, files, directories, and registry keys to be excluded from scanning by the *Anti-Malware* managed client. The primary purpose of this feature is to assure that legitimate files, directories and registry keys are not misinterpreted as threats during scans, and that IP addresses which may house files of this type do not trigger web blocking in the Protection Module. While threat signatures are highly accurate, it is impossible to guarantee that a string of data in a legitimate file will never be misinterpreted as a false positive. The following information will assist you with certain types of Ignore List entries:

- The specification `C:\Users\RNixon` refers to a file named `RNixon` in the `C:\Users` directory.
- The specification `C:\Users\RNixon\` refers to the `C:\Users\RNixon` directory and all files within that directory.
- The specification `C:\Users\RNixon\*` refers to the `C:\Users\RNixon` directory, all files within that directory, and any embedded subdirectories.

- `HKEY_USERS \*\Software\Policies\Microsoft\Internet Explorer\Control Panel|HomePage` ignores the value "`Home Page`" for this specific registry key for all users. Both private and public IP addresses may be specified.
- There is currently no provision for specification of hostnames or fully-qualified domain names. IP addresses that are dynamically-assigned will present issues with regard to the Ignore List.



Update Source

● Download signature updates from the Internet (allows for incremental updates) every 1 hour(s)

○ Download signature updates from a custom path every 1 hour(s)

Path:

Example: http://intranet.local/signaturedb/
https://intranetsecure.local/signaturedb/
\\fileserver\share\signaturedb\

○ Download signature updates from Management Server

☑ Download signature from alternative source every 1 hour(s) if Management Server is not accessible for 4 hour(s)

☐ Download from custom path:

Example: http://intranet.local/signaturedb/
https://intranetsecure.local/signaturedb/
\\fileserver\share\signaturedb\

☐ Download from the Internet if signature update from custom path fails

Updater Settings

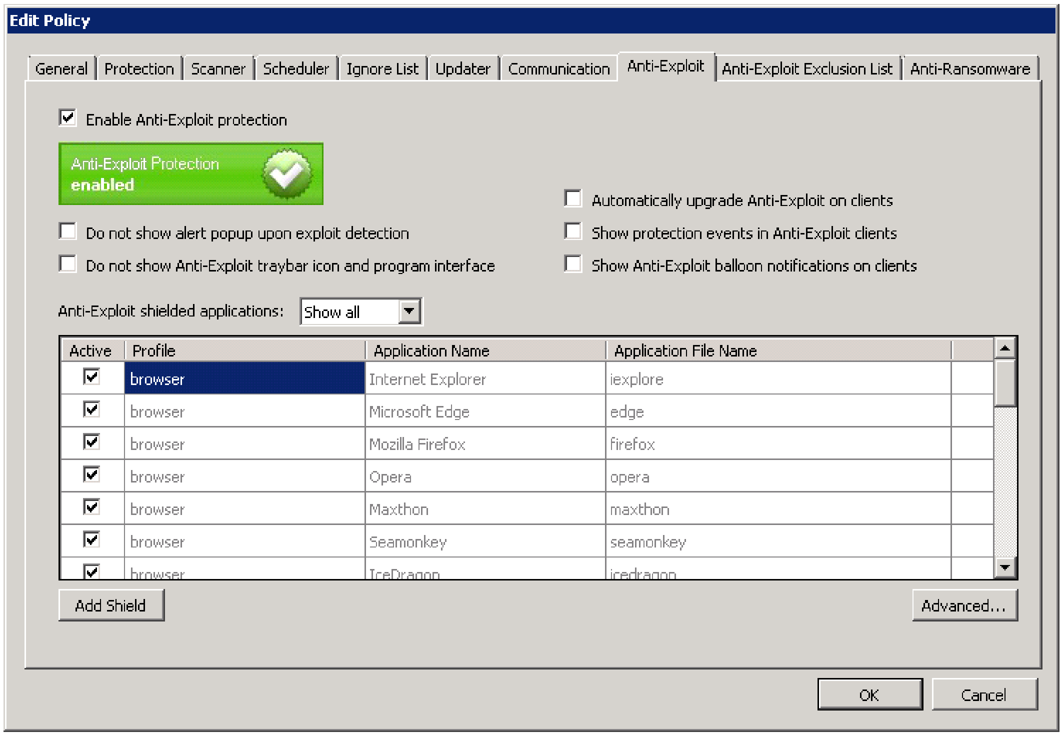
The Updater Settings tab controls how and when the *Anti-Malware* managed client receives signature updates which protect against the most current threats. The managed client normally receives incremental updates (roughly 3 kilobytes, *1/3000th the size of a full database update*) directly from the Malwarebytes Internet update server. By assuring that only new definitions are downloaded, network bandwidth is significantly reduced. If more than fifty (50) incremental updates are required to make databases current, a full update will instead be used. If a proxy is required, settings may be specified on this tab.

The second method is to receive updates from an alternate distribution source. If you choose an alternate source, you must specify an internet URL, IP address or a Windows UNC file specification where the signature update can be found.

The third method is to receive updates directly from the Management Server. When this method is used, incremental updates are not available – only full database updates (approximately 9-12 megabytes). The size of the full update is magnified by the number of endpoints covered by this policy which must receive the update in this manner. Network utilization may be affected during this update. If you choose to get signature updates from the Management Server and the server is not available or inaccessible, you may specify either a custom path or a direct Internet update be used as a failover. If the failover is employed, incremental updates are available.

Communication

The Communication tab allows the interval between policy/signature updates to be specified, as well as login information for a proxy server (if required for Internet access). The default setting is continuously variable, from 5 seconds (50 or fewer online endpoints) to 100 hours (200,000 or more online endpoints). You may override the default settings with a user-specified value, though the default interval is designed to strike a good balance between network performance and your protection needs. If you wish to see the table which defines the intervals, please refer to the *Managing Malwarebytes in Large Networks Best Practices Guide* for further information.



☑ Enable Anti-Exploit protection

☐ Automatically upgrade Anti-Exploit on clients

☐ Do not show alert popup upon exploit detection

☐ Show protection events in Anti-Exploit clients

☐ Do not show Anti-Exploit traybar icon and program interface

☐ Show Anti-Exploit balloon notifications on clients

Anti-Exploit shielded applications: Show all

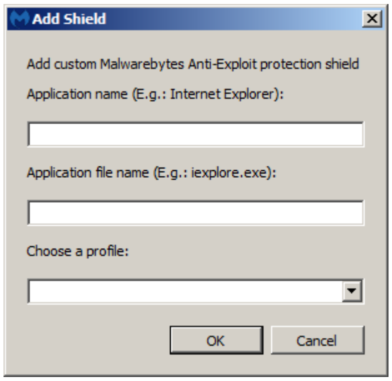
Active	Profile	Application Name	Application File Name
☑	browser	Internet Explorer	iexplore
☑	browser	Microsoft Edge	edge
☑	browser	Mozilla Firefox	firefox
☑	browser	Opera	opera
☑	browser	Maxthon	maxthon
☑	browser	Seamonkey	seamonkey
☑	browser	IceDragon	icedragon

Anti-Exploit

As shown in the above screenshot, this tab allows basic configuration of the *Anti-Exploit* managed client. Configuration capabilities of this client are limited, as its purpose dictates its operating characteristics. Settings which may be modified are:

- **Enable Anti-Exploit protection** determines whether Anti-Exploit protection is enabled. When enabled, the graphic immediately below this checkbox is green, with a text message indicating that it is enabled, and a checkmark provided as a quick visual indicator. When disabled, the graphic switches to red, with an accompanying text message, and a large "x" as a visual indicator. This setting also determines whether *Anti-Exploit shielded applications* can be modified.
- **Do not show alert popup upon exploit detection** determines whether user notifications are displayed when attempted exploits are detected. Notifications will be displayed only when this box is unchecked.
- **Do not show Anti-Exploit traybar icon and program interface** determines whether the *Anti-Exploit* managed client is working invisibly as a background task. The endpoint user may launch the *Anti-Exploit* managed client and/or see its icon in the system tray when this box is unchecked. Otherwise, the client is under complete control of the *Malwarebytes Management Console* administrator.
- **Automatically upgrade Anti-Exploit on clients** provides the capability to automatically upgrade the Anti-Exploit program on the client when an update becomes available. While this setting is specific to a policy, a system administrator would generally choose whether to enable or disable this setting for all policies in use.
- **Show protection events in Anti-Exploit clients** determines whether a shielded application will generate an entry in program logs when the application is started.
- **Show Anti-Exploit balloon notifications on clients** determines whether a shielded application will generate a visual taskbar notification to the user when the application is started.
- **Anti-Exploit shielded applications** is a list of software applications – grouped by type – which may be selected or deselected for shielding. For each application, you may choose whether to shield it or not. It is also important to note that the applications and the grouping of the applications has been chosen because all group members share common attack vectors. This provides optimum shielding capability.

Using the pulldown directly above the grid, you can choose to show all shields, custom shields, or only built-in shields. A checkmark immediately preceding an application indicates that the application is being shielded by *Malwarebytes Anti-Exploit*. The list of applications shielded by default is limited. You have the ability to add custom shields for other programs. To add a new custom shield, click the *Add Shield* button at the bottom left of the window.



Add Shield

Add custom Malwarebytes Anti-Exploit protection shield

Application name (E.g.: Internet Explorer):

Application file name (E.g.: iexplore.exe):

Choose a profile:

The window shown here launches when the *Add Shield* button is clicked. It allows you to create a new custom shield, by supplying the following information:

- **Application name** – The application name (as you would like it to appear).
- **Application file name** – The name and extension of the application (as it is stored on your endpoint). If an incorrect file name is specified, a shield will be created that accomplishes nothing.
- **Profile** – One of several application classes (browser, mediaplayer, office, other, pdfreader) that will be applied. Each of these has different behavior, so be as accurate as possible in order to provide the best protection.

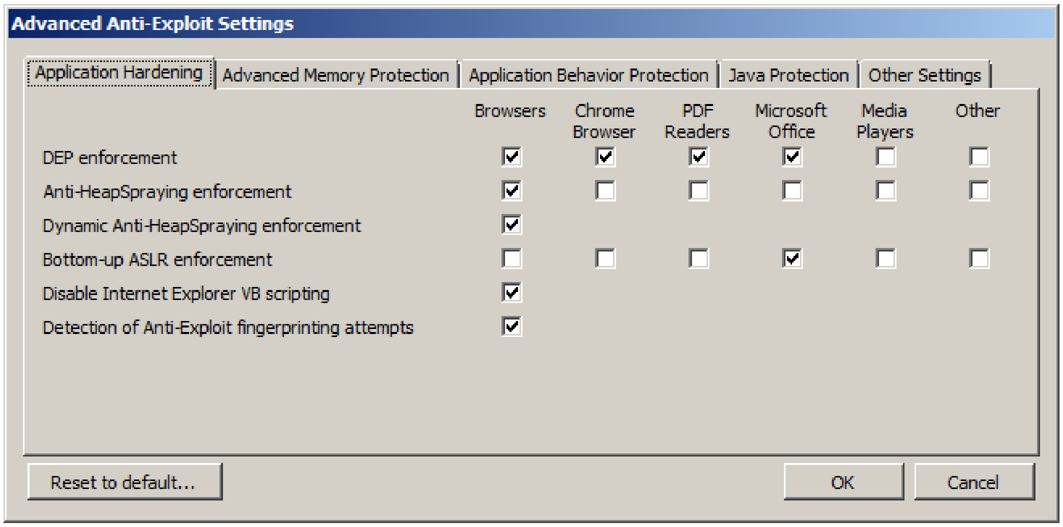
For more information on addition of custom shields via the command line , please refer to the *Malwarebytes Anti-Exploit Unmanaged Client Administrators Guide*.

Advanced Settings allows configuration or fine-tuning of some exploit mitigations included in *Malwarebytes Anti-Exploit*. Please note that not all exploit mitigations included in *Malwarebytes Anti-Exploit* can be modified here. *Malwarebytes Anti-Exploit* has pre-defined defaults which strike the best possible balance between performance and protection. Those exploit mitigations that are available for configuration have been deemed to be relevant to be tuned by users in scenarios where certain non-standard or heavily customized computing environments result in unexpected behavior by *Malwarebytes Anti-Exploit* (e.g. false positives).

Please note that while Chrome Browser options exist, *Malwarebytes Anti-Exploit* no longer protects these browsers. This is due to a change to Google Chrome in update 69 which prevents applications like *Malwarebytes Anti-Exploit* from interacting with the browser.

WARNING: Improper changes to these settings may result in improper performance and protection offered by *Malwarebytes Anti-Exploit*. Make changes only when required to do so by a Malwarebytes Customer Success specialist.

Settings on the **Application Hardening** tab refer to exploit mitigation techniques whose objective is to make protected applications more resilient against vulnerability exploit attacks, even if those applications have not been patched to the latest available fixes by their respective vendors. A screenshot shows the organization of the tab.



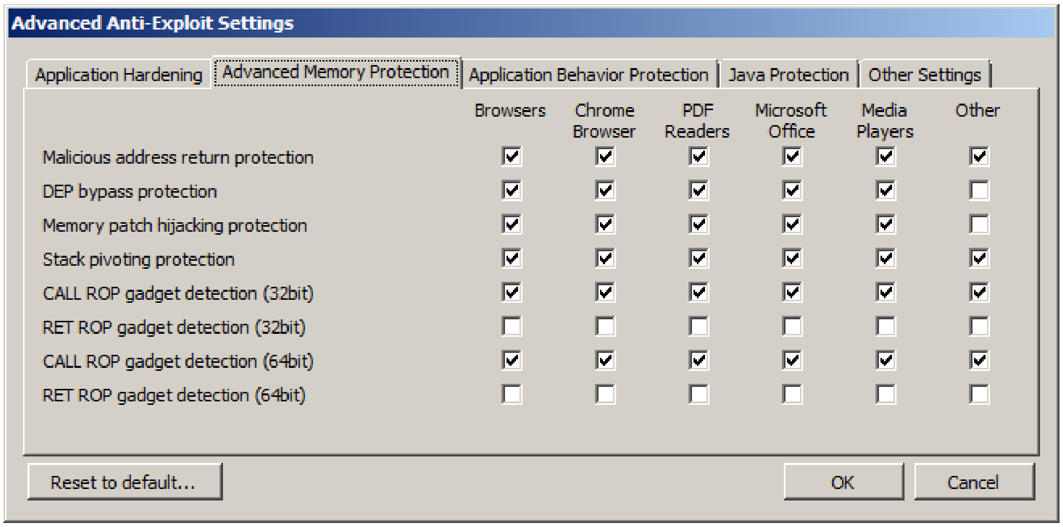
Advanced Anti-Exploit Settings

	Browsers	Chrome Browser	PDF Readers	Microsoft Office	Media Players	Other
DEP enforcement	☑	☑	☑	☑	□	□
Anti-HeapSpraying enforcement	☑	□	□	□	□	□
Dynamic Anti-HeapSpraying enforcement	☑					
Bottom-up ASLR enforcement	□	□	□	☑	□	□
Disable Internet Explorer VB scripting	☑					
Detection of Anti-Exploit fingerprinting attempts	☑					

- **DEP Enforcement** is tasked with activation of permanent Data Execution Prevention (DEP) in those applications that do not do this by default.
- **Anti-HeapSpraying Enforcement** is designed to reserve certain memory ranges, to prevent them from being abused by Heap-Spraying attack techniques.
- **Dynamic Anti-HeapSpraying Enforcement** analyzes the memory heap of a protected process in order to find evidence of malicious shellcode on the heap using heap spraying techniques.
- **Bottom-Up ASLR Enforcement** is tasked with addition of randomization to the memory heap when the process starts.

- **Disable Internet Explorer VB Scripting** is tasked with preventing the deprecated Visual Basic scripting engine from loading. The scripting engine is frequently abused by exploits. This setting applies only to the browser family.
- **Detection of Anti-Exploit fingerprinting attempts** is a technique which detects attempts by popular exploit kits (e.g. Angler) of fingerprinting the victim machine to determine if it should be attacked by its exploit arsenal.

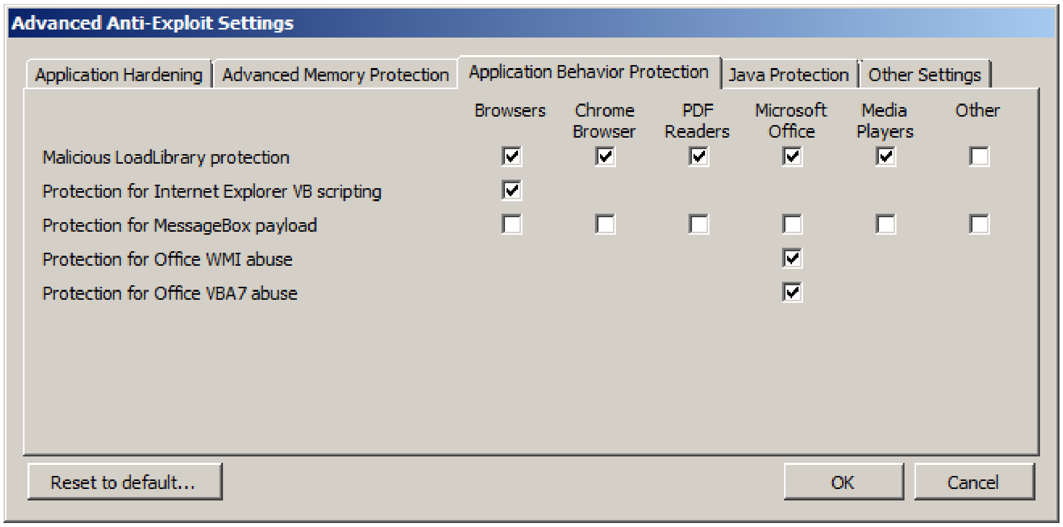
Advanced Memory Protection refers to exploit mitigation techniques whose objective is to prevent exploit shellcode from executing its payload code in memory.


Advanced Anti-Exploit Settings
Application Hardening
Advanced Memory Protection
Application Behavior Protection
Java Protection
Other Settings
Reset to default...
OK
Cancel

	Browsers	Chrome Browser	PDF Readers	Microsoft Office	Media Players	Other
Malicious address return protection	☑	☑	☑	☑	☑	☑
DEP bypass protection	☑	☑	☑	☑	☑	□
Memory patch hijacking protection	☑	☑	☑	☑	☑	□
Stack pivoting protection	☑	☑	☑	☑	☑	☑
CALL ROP gadget detection (32bit)	☑	☑	☑	☑	☑	☑
RET ROP gadget detection (32bit)	□	□	□	□	□	□
CALL ROP gadget detection (64bit)	☑	☑	☑	☑	☑	☑
RET ROP gadget detection (64bit)	□	□	□	□	□	□

- **Malicious Return Address detection** – also called "Caller" mitigation – detects if the code is executed outside of any loaded module.
- **DEP Bypass Protection** is tasked with detecting attempts to turn off Data Execution Prevention (DEP).
- **Memory Patch Hijacking Protection** is designed to detect and prevent against attempts to use WriteProcessMemory to bypass Data Execution Prevention (DEP).
- **Stack Pivoting Protection** is used to detect and prevent exploit code from creating and utilizing a fake memory stack.
- **ROP Gadget detection** is tasked with detection and prevention of Return Oriented Programming (ROP) gadgets when a Windows API is called. Provisions are made for individualized protection of CALL and RETurn instructions.

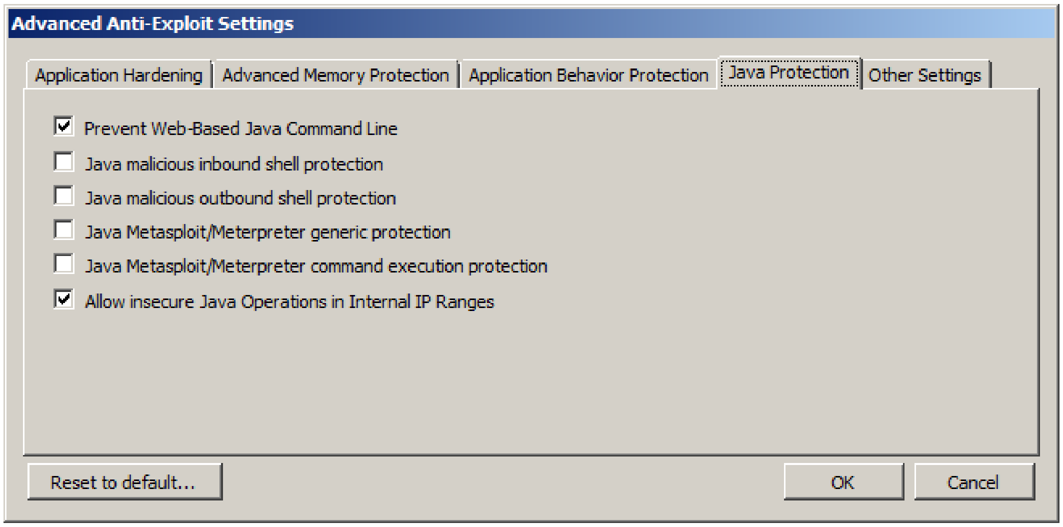
Application Behavior Protection settings provide mitigation techniques designed to prevent the exploit payload from executing and infecting the system. This represents the last line of defense if memory corruption exploit mitigations from previous layers are bypassed. This layer is also tasked with detecting exploits that do not rely on memory corruption (e.g. Java sandbox escapes, application design abuse exploits, etc.) and blocking their malicious actions.


Advanced Anti-Exploit Settings
Application Hardening
Advanced Memory Protection
Application Behavior Protection
Java Protection
Other Settings
Reset to default...
OK
Cancel

	Browsers	Chrome Browser	PDF Readers	Microsoft Office	Media Players	Other
Malicious LoadLibrary protection	☑	☑	☑	☑	☑	□
Protection for Internet Explorer VB scripting	☑					
Protection for MessageBox payload	□	□	□	□	□	□
Protection for Office WMI abuse				☑		
Protection for Office VBA7 abuse				☑		

- **Malicious LoadLibrary protection** prevents delivery of a payload library from a UNC network path.
- **Protection for Internet Explorer VB scripting** is designed to detect and prevent exploits related to an application design vulnerability known as CVE-2014-6332. For further information on this exploit, please refer to https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6332.
- **Protection for MessageBox payload** prevents exploits from delivering a messagebox as its payload. It is turned off by default as these payloads are normally only used in proof of concepts and do not cause any harm.
- **Protection for Office WMI abuse** protects against macro exploits in Microsoft Office using Windows Management Instrumentation (WMI).
- **Protection for Office VBA7** abuse protects against macro exploits in Microsoft Office using Visual Basic for Applications.

Java Protection refers to mitigation techniques which are unique to exploits commonly used in Java programs.

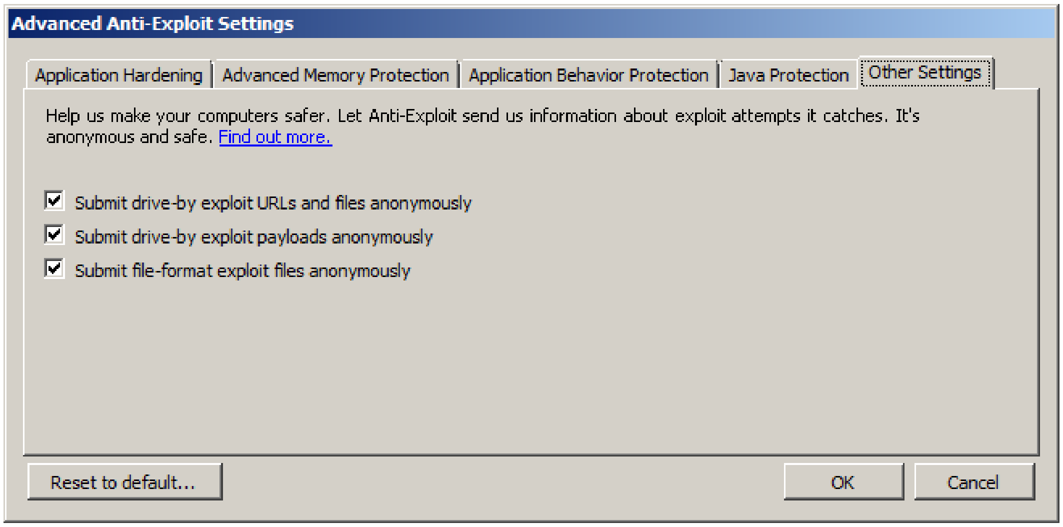

Advanced Anti-Exploit Settings
Application Hardening
Advanced Memory Protection
Application Behavior Protection
Java Protection
Other Settings

☑ Prevent Web-Based Java Command Line
□ Java malicious inbound shell protection
□ Java malicious outbound shell protection
□ Java Metasploit/Meterpreter generic protection
□ Java Metasploit/Meterpreter command execution protection
☑ Allow insecure Java Operations in Internal IP Ranges

Reset to default...
OK
Cancel

- **Prevent Web-Based Java Command Line** protects against web-based Java programs issuing system commands.
- **Java malicious inbound shell protection** guards against remote shell exploits whose payloads rely on inbound sockets.
- **Java malicious outbound shell protection** guards against remote shell exploits whose payloads rely on outbound sockets.
- **Java Metasploit/Meterpreter generic protection** is designed to generically detect and prevent attempts to use the Metasploit Java/Meterpreter payload.
- **Java Metasploit/Meterpreter command execution protection** is tasked with detecting and blocking commands in an established Java/Meterpreter session.
- **Allow Insecure Java Operations in Internal IP Ranges** is primarily used to allow insecure internal tools and applications used within a corporate network without compromising on protection from external Java threats.

The **Other Settings** tab contains settings which allow you to provide meaningful data to us about exploits you encounter. This is strictly voluntary, and provides information about exploits only…no confidential data will be sent to Malwarebytes. Discovering more about threats discovered in the wild gives us an opportunity to serve you better.


Advanced Anti-Exploit Settings

Help us make your computers safer. Let Anti-Exploit send us information about exploit attempts it catches. It's anonymous and safe. Find out more.

☑ Submit drive-by exploit URLs and files anonymously

☑ Submit drive-by exploit payloads anonymously

☑ Submit file-format exploit files anonymously

Anti-Exploit Exclusion List

This tab allows files to be excluded from anti-exploit testing. Actual filenames are optional, because they offer no measure of uniqueness. Many malware attacks have occurred because malware was hidden inside a file whose name was trusted. The *Anti-Exploit* managed client uses an MD5 signature to identify a file, because any change to the file results in a change of its MD5 signature. There are a number of MD5 programs available as free internet downloads, and all should generate identical MD5 signatures if hashing algorithms are properly encoded. You may exclude as many files as you wish by entering their MD5 signatures here, one entry per line. If you wish to include the name of the file, enter it after the file's signature, separating the MD5 and file name with a semi-colon.

Anti-Ransomware

This tab controls the behavior of *Malwarebytes Anti-Ransomware*. You can change whether the program is enabled or disabled using the checkbox at the top. If there are items you want to whitelist in the program, you can enter the file paths in the text box. Each exclusion must be entered as a separate line item. You can exclude either an individual file, or an entire folder. No additional configuration is needed for *Anti-Ransomware* to begin working.

Edit

The Edit control allows modification of a policy selected in the Policies panel. All screens described previously for *Add New Policy* are also used here. Upon completion of the policy edit, the policy's version number will increment. There is no provision for deleting interim policies. If the *Malwarebytes Management Console* Server maintains a communication path with endpoints affected by the modified policy, the policy will be pushed out to the endpoints. The Clients module should be monitored following a policy change to assure that the policy change has been effected on all endpoints. If a policy change does not occur on the endpoint, it will be highlighted in yellow. A second *Edit* button at the bottom of the Policies panel has identical functionality.

Copy

Malwarebytes administrators often create policies that provide uniform protection across all endpoints, then adjust these basic policies for small subsets of users. For this purpose, the **Copy** control allows for a new policy to be created from an existing policy. All settings from the selected policy will be applied to the new policy. When using this control, you will be prompted to name your new policy. The new policy will be appended with the word "Copy" as a reminder, and can be edited as necessary.

Remove

This control allows a policy to be removed. Any endpoints governed by the policy being removed will automatically be switched to the highest-priority policy with matching deployment include/exclude specifications. Subsequent policy assignment changes to affected endpoints must be performed manually by the *Malwarebytes Management Console* Administrator.

WARNING: If a large number of clients are reassigned as a result of a policy being removed, higher network traffic may result if a large number of clients are getting database updates simultaneously.

Disable

This control allows a policy to be disabled. By disabling a policy, you may not assign it to clients. A policy currently assigned to one or more clients may be disabled, following acknowledgement of a warning that the policy is in use. Any clients associated with the policy being disabled will be reassigned to the highest priority policy which is enabled.

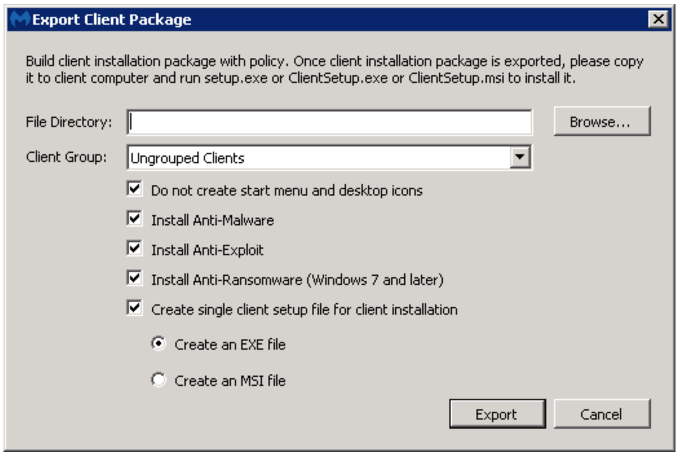
WARNING: If a large number of clients are reassigned as a result of a policy being removed, higher network traffic may result if a large number of clients are getting database updates simultaneously.

Refresh

This control simply redisplays the Policies panel using current policy information.

Installation Package

This option provides the capability of creating an client installer that can be used exclusive of *Malwarebytes Management Console*'s Client Push Install process. This is advantageous if your organization uses third-party installation software, Active Directory Group Policy updates, or has external employees which connect to your network via VPN. Clicking the *Installation Package* button launches the Export Client Package window, as shown below.



Build client installation package with policy. Once client installation package is exported, please copy it to client computer and run setup.exe or ClientSetup.exe or ClientSetup.msi to install it.

File Directory:

Client Group: Ungrouped Clients

☑ Do not create start menu and desktop icons

☑ Install Anti-Malware

☑ Install Anti-Exploit

☑ Install Anti-Ransomware (Windows 7 and later)

☑ Create single client setup file for client installation

● Create an EXE file

○ Create an MSI file

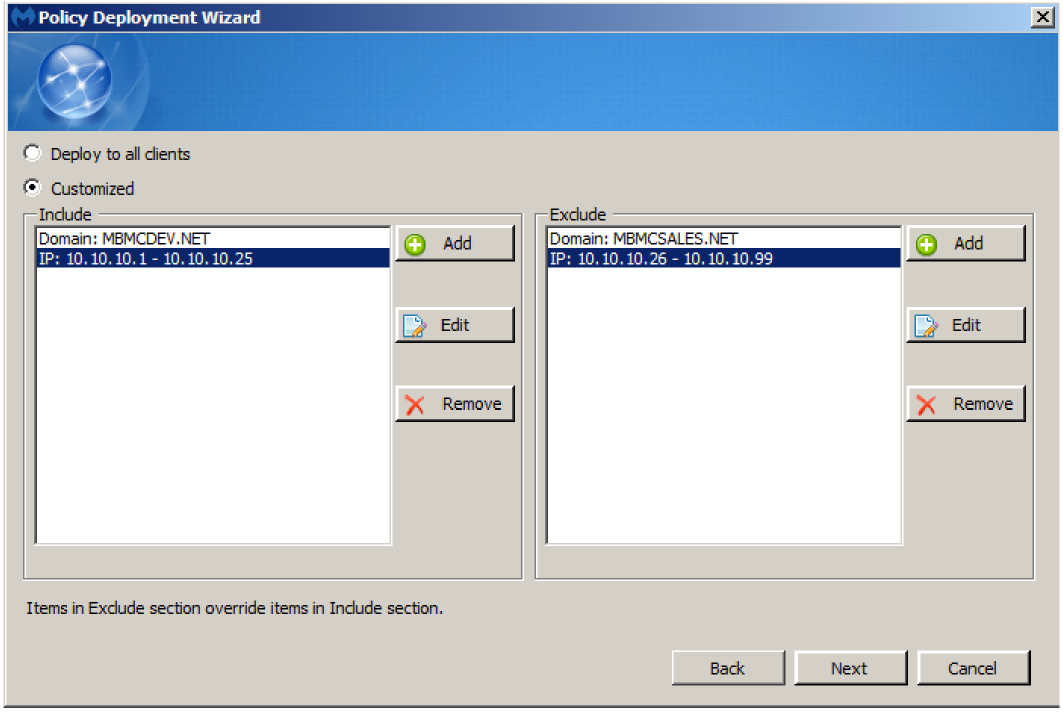
Choose a directory in which the client package will be installed. You can use the standard Windows Explorer dialog to browse to the location of your choice. You must select a client group which the client will be part of once installed. You may choose whether the managed client will be visible to the user by checking or unchecking the setting regarding start menu and desktop icons.

You can elect to install any combination of the *Malwarebytes Anti-Malware* managed client, the *Malwarebytes Anti-Exploit* managed client, or the *Malwarebytes Anti-Ransomware* managed client. If neither client is installed, communication capability between the server and the endpoint is defined and initialized.

You may also create a single managed client setup file, as either a stand-alone executable (EXE) file or a Windows Installer (MSI) file. An EXE file is ideal if sending the client via email, placing it on a shared network drive, or by transport on a USB stick. The MSI file is ideal when using third-party installers or AD Group Policy updates. The single file method is recommended. Once all settings have been specified, click *Export* and the file will be created in the specified directory.

Deployment

The Deployment Wizard is a series of four screens invoked by clicking the *Deployment* control at the top of the screen. The purpose of this is to make a new or modified policy effective on one or more endpoints. The second screen of the wizard allows the policy to be deployed to all endpoints, or to a customized subset using a combination of inclusion and exclusion. A screenshot of this screen is shown below.



Policy Deployment Wizard

○ Deploy to all clients

● Customized

Include

Domain: MBMCDEV.NET
IP: 10.10.10.1 - 10.10.10.25

Exclude

Domain: MBMCSALES.NET
IP: 10.10.10.26 - 10.10.10.99

Items in Exclude section override items in Include section.

Clicking the *Add* button in either the Include or Exclude areas of this screen will allow selection of five different parameters which can be used. Parameters available are:

- IP Range
- Client Group
- Domain
- Host Name
- Subnet

Once deployment parameters have been selected, you must confirm your settings, and finally click *Deploy Now* to deploy the policy to selected endpoints.

The screenshot shown above merits a brief discussion to explain why include and exclude specifications are used in the manner employed here. Specifications for domain and IP Range have both been used here, and they have been used for both include and exclude categories. When deploying *Malwarebytes Management Console* to your endpoints, you may wish to use policies which provide drastically different behavior for different endpoint groups. In this example, the 10.10.10.x subnet is shared by endpoints on at least two different domains. Because the subnet parameter was not chosen, it is possible that more endpoints in this subnet (10.10.10.100 and above) are managed by different policies. This specific policy will be deployed to endpoints who satisfy the Include specs *and* also satisfy the Exclude specs. Other new endpoints will be subjected to criteria testing as well. Also, if a policy is deleted for any reason, endpoints will be reassigned to other policies based on (1) Include/Exclude specs, and (2) Highest policy priority. That implies that an endpoint could be reassigned to a policy with low priority if it is the first one which meets Include/Exclude specs that the endpoint satisfies.

Policies panel

The Policies panel shows basic information about all policies which have been defined. All information fields displayed here have already been discussed in this section with one exception – policy priorities. This determines which policies are assigned to new clients as well as clients whose assigned policy has been removed or disabled. Policy priorities are determined by using the *Move Up* or *Move Down* buttons on the right-click context menu.

When performing a client push install via the Admin module, a policy is specifically assigned to the client. When changing a policy for a client via the Client module, a policy is specifically assigned there as well. If a policy is removed or disabled, clients who were associated with the now-absent policy are reassigned, and that is where policy priorities come into play. Based on the include/exclude specifications for enabled policies, those clients will be reassigned to the highest priority policy that applies to them. If multiple policies exist which satisfy include and exclude specifications, care should be taken to choose the correct policy for your needs.

Protection Status panel

This panel shows scanner settings that have been configured for the policy selected in the Policies panel. All information shown here is read-only.

Policy Deployment panel

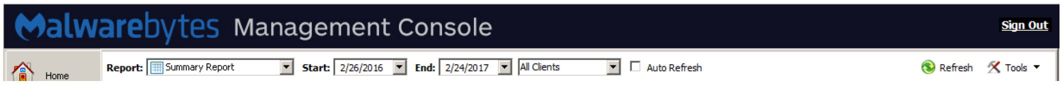
This panel shows deployment settings that have been configured for the policy selected in the Policies panel. All information shown here is read-only.

Report Module

The Report Module provides a series of reports designed to show how *Malwarebytes Management Console* is protecting endpoints in your environment, breaking down information in a number of formats. All reports can be viewed using the graphical interface. Additionally, they can be printed using the standard Windows print dialog.

Report Selector

At the top of the Report Module interface is the report selector. This allows the user to select a specific report to be viewed, the time frame which the report represents, and also provides print capability. The selector is shown here.



Report: Summary Report
Start: 2/26/2016
End: 2/24/2017
All Clients
☐ Auto Refresh

Reports that are available here via a pulldown menu are:

- Summary Report
- Top Risk Report
- Threat Trend Report
- Client Scan Report
- Client Signature Report
- Policy Deployment Report
- Server System Report

After selecting a report, you may specify a time frame for the report. Start and end dates may be entered directly, or you may use the pulldown feature to display a small calendar from which dates can be selected. An *Auto Refresh* button allows report data to be refreshed in real-time. If you are analyzing information which you can see only by scrolling down, you may wish to uncheck the *Auto Refresh* feature, as each refresh will return you to the top of the data display. You may also refresh on-demand, and use the *Tools* pulldown to print.

Reports

The remainder of this section will describe each of these reports, their purpose, and how they may also be used for troubleshooting of certain issues which may not be easily detected.

Summary Report

The Summary Report is a high-level dashboard view of *Malwarebytes Management Console* system operation. It contains six brief summaries, all based on specified time frames. The data shown in this report does not include *Anti-Ransomware* events. The summaries provided are:

- **Overall System Status –** A brief table which sums all of the information shown in the other five summaries, as well as the relative load on the *Malwarebytes Management Console* server.

- **Online Clients in Last 24 Hours –** A graphical representation of the number of clients monitored in the most recent 24-hour period, as well as the number of clients known to *Malwarebytes Management Console*. The two quantities may easily differ from one another for a variety of legitimate reasons.

- **Daily Threat Detections –** A bar graph showing the daily number of threats detected over the specified time frame by the *Anti-Malware* managed client.

- **Daily Exploit Detections –** A bar graph showing the daily number of exploits detected over the specified time frame by the *Anti-Exploit* managed client.

- **Top 10 Clients with most Threats –** A pie chart showing a maximum of ten (10) clients with the highest number of threats detected by the *Anti-Malware* managed client during the requested time frame. Each is shown with a unique color for ease of reading.

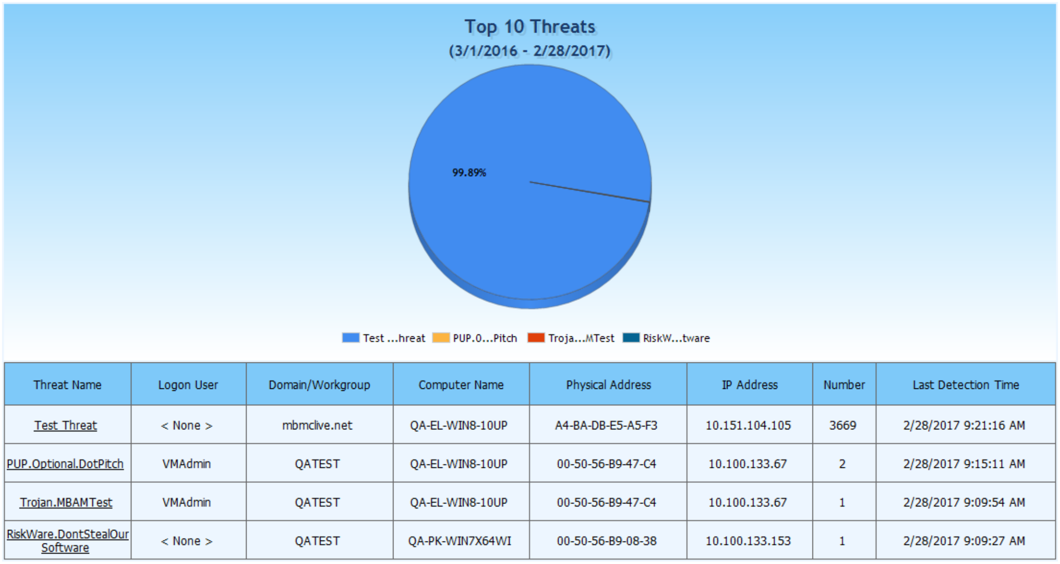
- **Top 10 Clients with most Exploits –** A pie chart showing a maximum of ten (10) clients with the highest number of exploits detected by the *Anti-Exploit* managed client during the requested time frame. Each is shown with a unique color for ease of reading.

All summaries which appear here are supplemented by more detailed reports that provide additional detail. The primary purpose here is simply to provide the high-level view of several topics, all at the same time.

Top Risk Report

This report provides several "top ten" pie charts with corresponding tables that provide further information. These are:

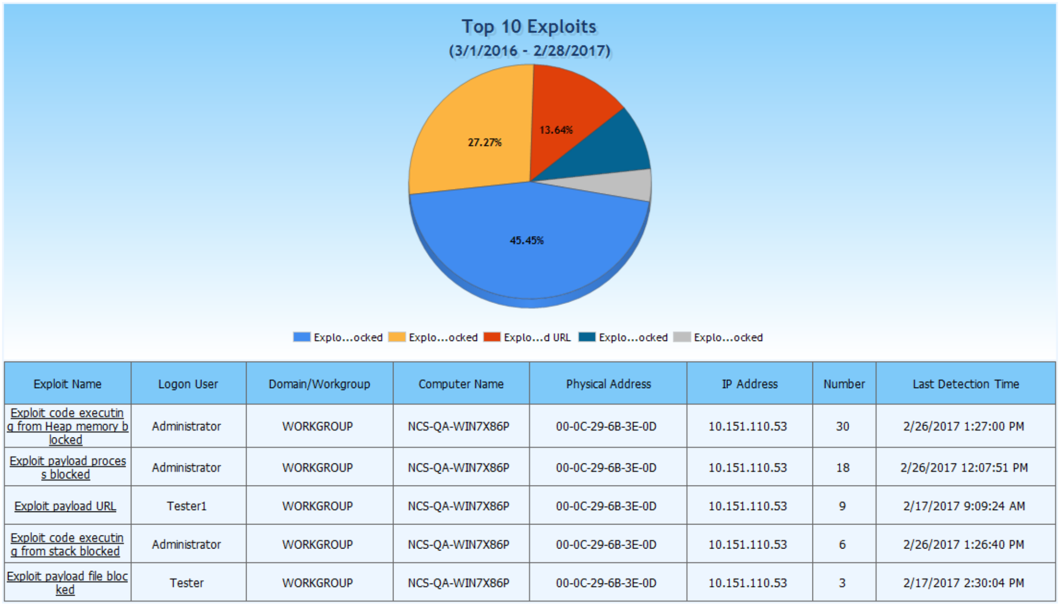
Top 10 Threats – Pie chart focused on specific threats detected by the *Anti-Malware* managed client, with information provided about users, endpoints and number of detections.



Top 10 Threats
(3/1/2016 - 2/28/2017)
99.89%
■ Test ...hreat ■ PUP.O...Pitch ■ Troja...MTest ■ RiskW...tware

Threat Name	Logon User	Domain/Workgroup	Computer Name	Physical Address	IP Address	Number	Last Detection Time
Test Threat	< None >	mbmclive.net	QA-EL-WIN8-10UP	A4-BA-DB-E5-A5-F3	10.151.104.105	3669	2/28/2017 9:21:16 AM
PUP.Optional.DotPitch	VMAdmin	QATEST	QA-EL-WIN8-10UP	00-50-56-B9-47-C4	10.100.133.67	2	2/28/2017 9:15:11 AM
Trojan.MBAMTest	VMAdmin	QATEST	QA-EL-WIN8-10UP	00-50-56-B9-47-C4	10.100.133.67	1	2/28/2017 9:09:54 AM
RiskWare.DontStealOurSoftware	< None >	QATEST	QA-PK-WIN7X64WI	00-50-56-B9-08-38	10.100.133.153	1	2/28/2017 9:09:27 AM

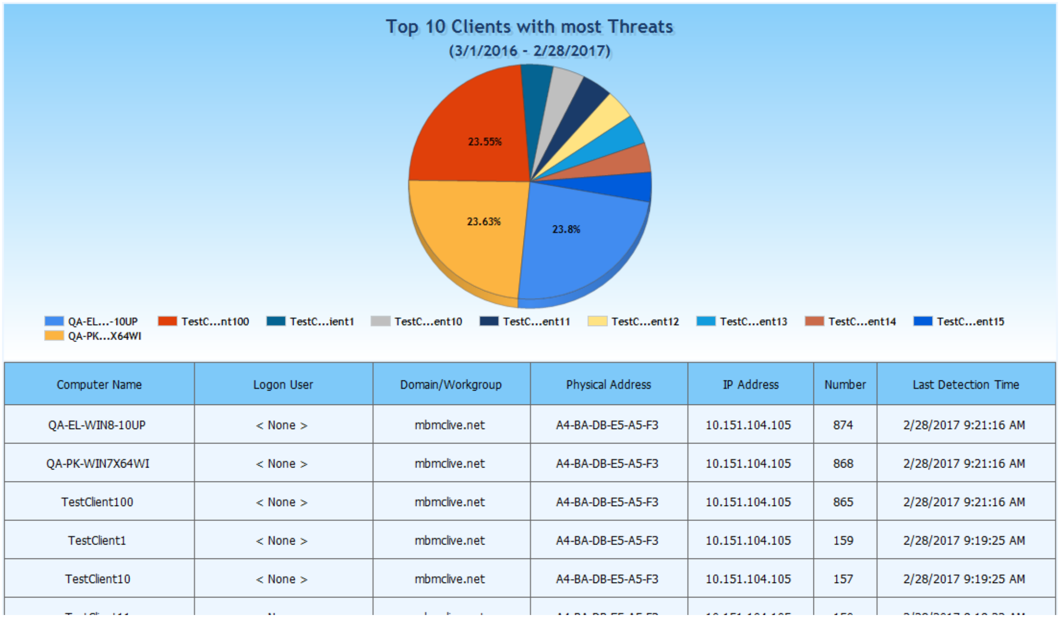
Top 10 Exploits – Pie chart focused on specific threats detected by the *Anti-Exploit* managed client, with information provided about users, endpoints and number of detections.



Top 10 Exploits
(3/1/2016 - 2/28/2017)
27.27%
13.64%
45.45%
■ Explo...ocked ■ Explo...ocked ■ Explo...d URL ■ Explo...ocked ■ Explo...ocked

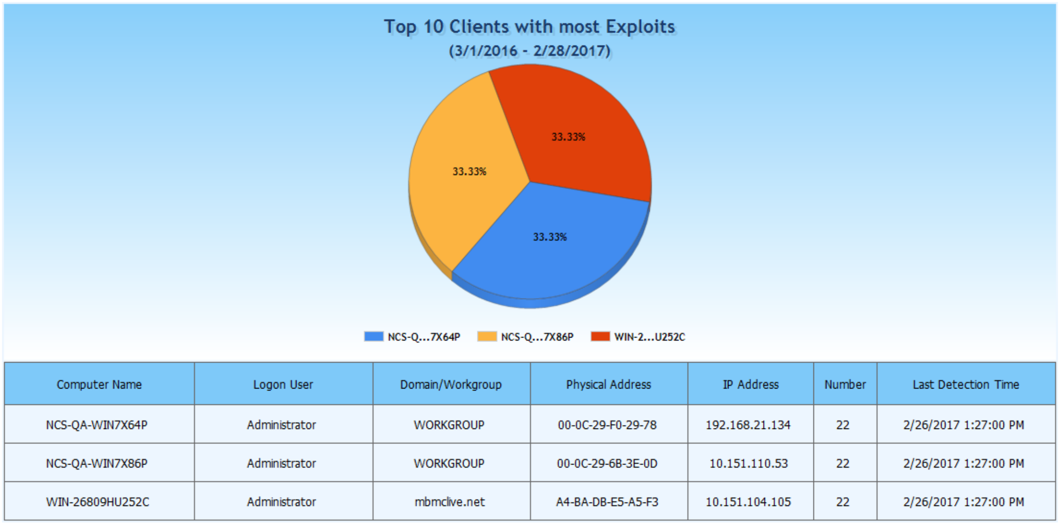
Exploit Name	Logon User	Domain/Workgroup	Computer Name	Physical Address	IP Address	Number	Last Detection Time
Exploit code executing from Heap memory blocked	Administrator	WORKGROUP	NCS-QA-WIN7X86P	00-0C-29-6B-3E-0D	10.151.110.53	30	2/26/2017 1:27:00 PM
Exploit payload process blocked	Administrator	WORKGROUP	NCS-QA-WIN7X86P	00-0C-29-6B-3E-0D	10.151.110.53	18	2/26/2017 12:07:51 PM
Exploit payload URL	Tester1	WORKGROUP	NCS-QA-WIN7X86P	00-0C-29-6B-3E-0D	10.151.110.53	9	2/17/2017 9:09:24 AM
Exploit code executing from stack blocked	Administrator	WORKGROUP	NCS-QA-WIN7X86P	00-0C-29-6B-3E-0D	10.151.110.53	6	2/26/2017 1:26:40 PM
Exploit payload file blocked	Tester	WORKGROUP	NCS-QA-WIN7X86P	00-0C-29-6B-3E-0D	10.151.110.53	3	2/17/2017 2:30:04 PM

Top 10 Clients with most Threats – Pie chart focused on the number of threats (as determined by the *Anti-Malware* managed client) encountered by each endpoint. There is no reference to specific threats involved.



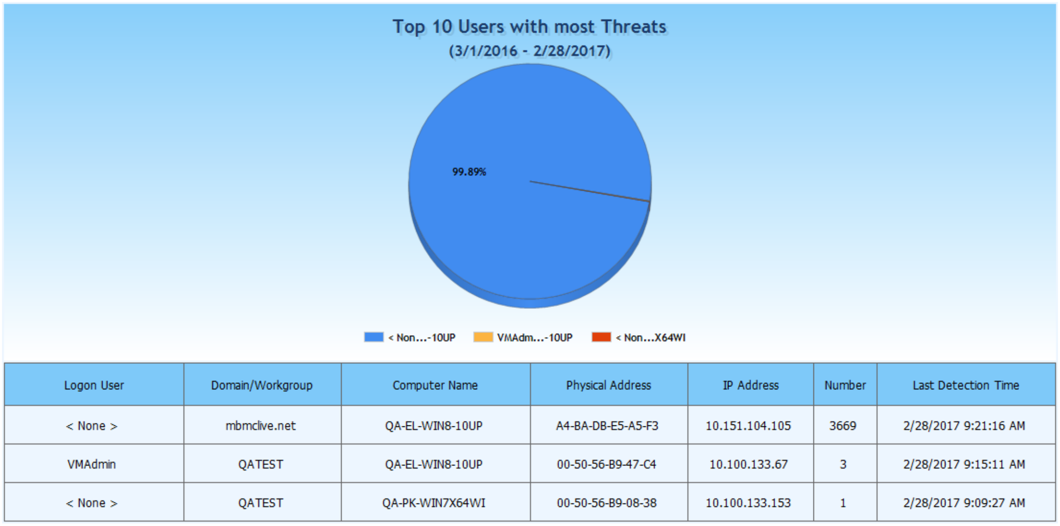
Computer Name	Logon User	Domain/Workgroup	Physical Address	IP Address	Number	Last Detection Time
QA-EL-WIN8-10UP	< None >	mbmclive.net	A4-BA-DB-E5-A5-F3	10.151.104.105	874	2/28/2017 9:21:16 AM
QA-PK-WIN7X64WI	< None >	mbmclive.net	A4-BA-DB-E5-A5-F3	10.151.104.105	868	2/28/2017 9:21:16 AM
TestClient100	< None >	mbmclive.net	A4-BA-DB-E5-A5-F3	10.151.104.105	865	2/28/2017 9:21:16 AM
TestClient1	< None >	mbmclive.net	A4-BA-DB-E5-A5-F3	10.151.104.105	159	2/28/2017 9:19:25 AM
TestClient10	< None >	mbmclive.net	A4-BA-DB-E5-A5-F3	10.151.104.105	157	2/28/2017 9:19:25 AM

Top 10 Clients with most Exploits – Pie chart focused on the number of exploits (as determined by the *Anti-Exploit* managed client) encountered by each endpoint. There is no reference to specific exploits involved.



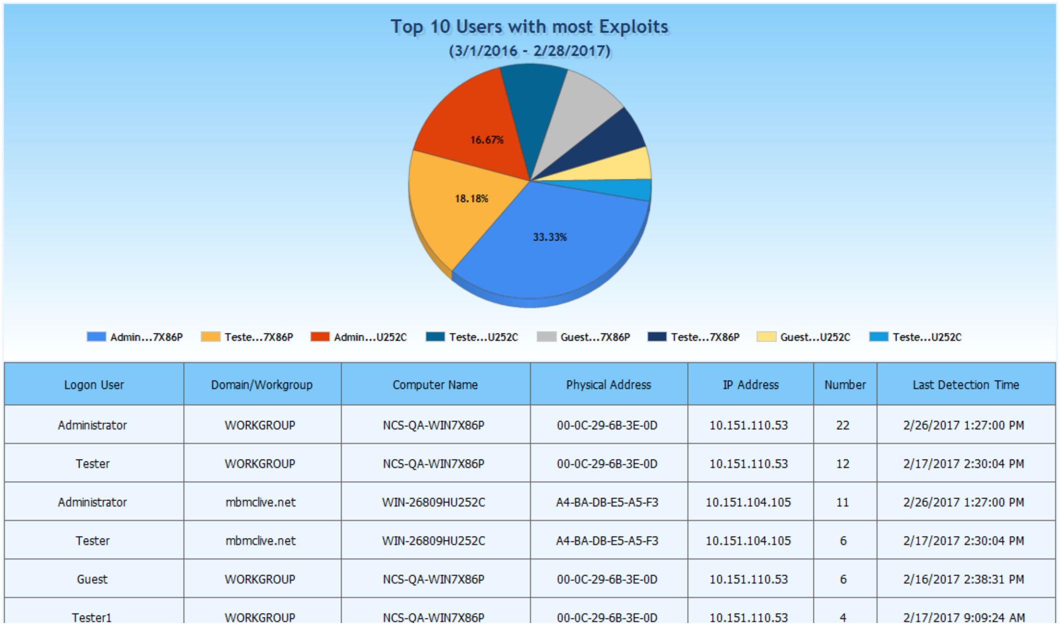
Computer Name	Logon User	Domain/Workgroup	Physical Address	IP Address	Number	Last Detection Time
NCS-QA-WIN7X64P	Administrator	WORKGROUP	00-0C-29-F0-29-78	192.168.21.134	22	2/26/2017 1:27:00 PM
NCS-QA-WIN7X86P	Administrator	WORKGROUP	00-0C-29-6B-3E-0D	10.151.110.53	22	2/26/2017 1:27:00 PM
WIN-26809HU252C	Administrator	mbmclive.net	A4-BA-DB-E5-A5-F3	10.151.104.105	22	2/26/2017 1:27:00 PM

Top 10 Users with most Threats – Pie chart focused on the number of threats encountered by each user, as determined by the *Anti-Malware* managed client. There is no reference to the specific threats involved.



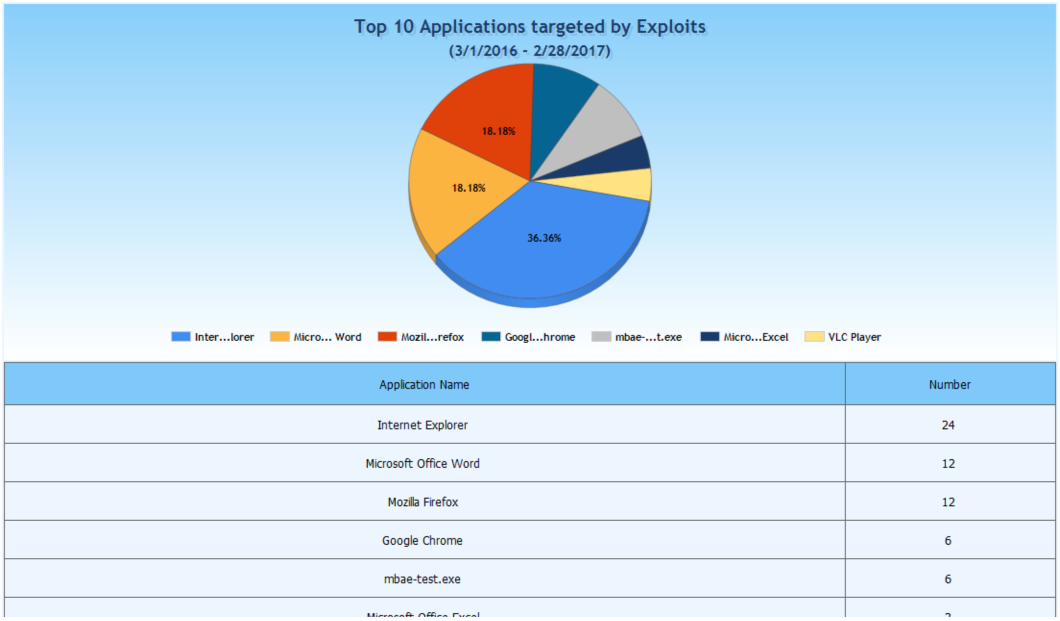
Logon User	Domain/Workgroup	Computer Name	Physical Address	IP Address	Number	Last Detection Time
< None >	mbmclive.net	QA-EL-WIN8-10UP	A4-BA-DB-E5-A5-F3	10.151.104.105	3669	2/28/2017 9:21:16 AM
VMAdmin	QATEST	QA-EL-WIN8-10UP	00-50-56-B9-47-C4	10.100.133.67	3	2/28/2017 9:15:11 AM
< None >	QATEST	QA-PK-WIN7X64WI	00-50-56-B9-08-38	10.100.133.153	1	2/28/2017 9:09:27 AM

Top 10 Users with most Exploits – Pie chart focused on the number of exploits encountered by each user, as determined by the *Anti-Exploit* managed client. There is no reference to specific exploits involved.



Logon User	Domain/Workgroup	Computer Name	Physical Address	IP Address	Number	Last Detection Time
Administrator	WORKGROUP	NCS-QA-WIN7X86P	00-0C-29-6B-3E-0D	10.151.110.53	22	2/26/2017 1:27:00 PM
Tester	WORKGROUP	NCS-QA-WIN7X86P	00-0C-29-6B-3E-0D	10.151.110.53	12	2/17/2017 2:30:04 PM
Administrator	mbmclive.net	WIN-26809HU252C	A4-BA-DB-E5-A5-F3	10.151.104.105	11	2/26/2017 1:27:00 PM
Tester	mbmclive.net	WIN-26809HU252C	A4-BA-DB-E5-A5-F3	10.151.104.105	6	2/17/2017 2:30:04 PM
Guest	WORKGROUP	NCS-QA-WIN7X86P	00-0C-29-6B-3E-0D	10.151.110.53	6	2/16/2017 2:38:31 PM
Tester1	WORKGROUP	NCS-QA-WIN7X86P	00-0C-29-6B-3E-0D	10.151.110.53	4	2/17/2017 9:09:24 AM

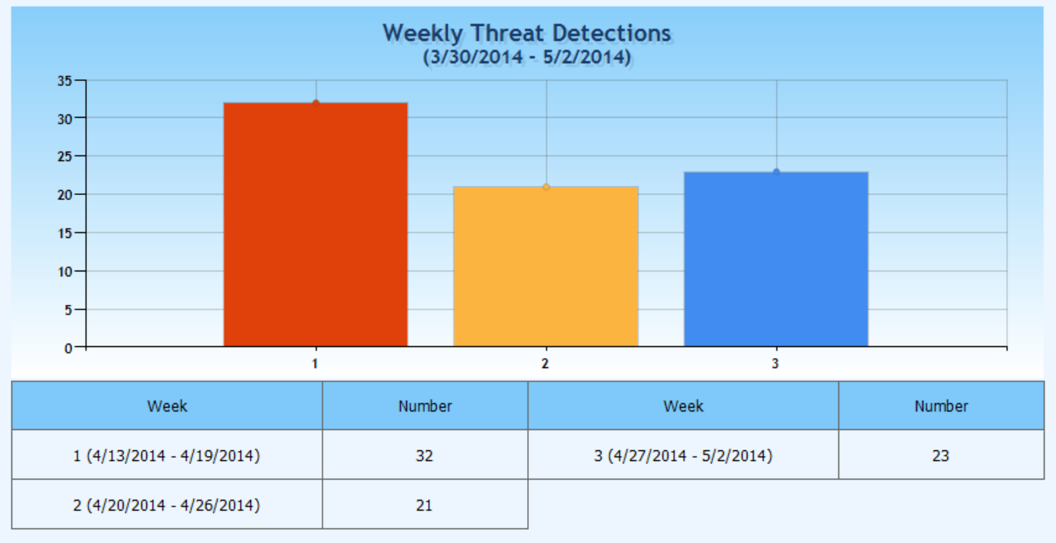
Top 10 Applications targeted by Exploits – Pie chart focused on the number of exploits encountered by each user, as determined by the *Anti-Exploit* managed client. There is no reference to specific exploits involved.



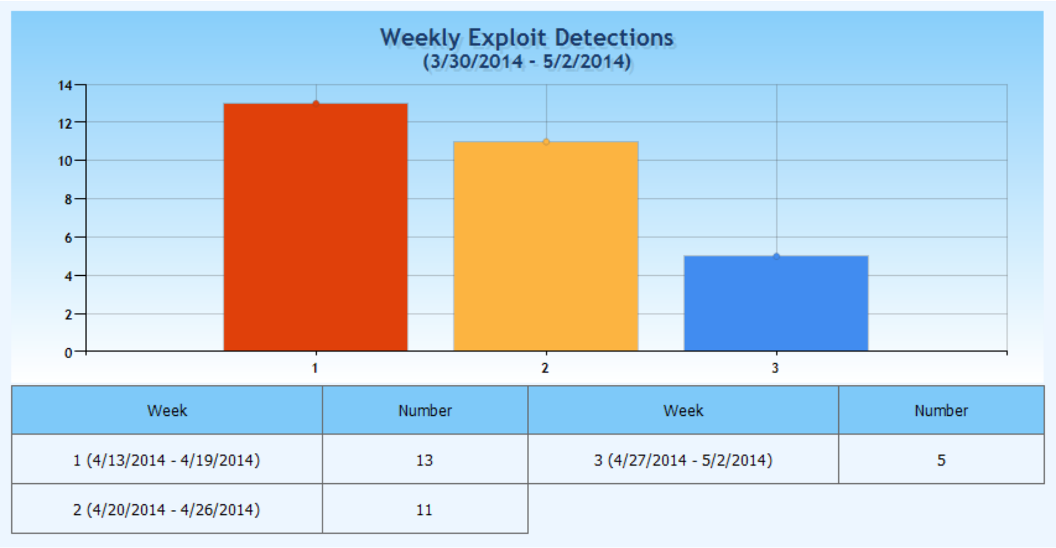
Application Name	Number
Internet Explorer	24
Microsoft Office Word	12
Mozilla Firefox	12
Google Chrome	6
mbae-test.exe	6
Microsoft Office Excel	[illegible]

Threat Trend Report

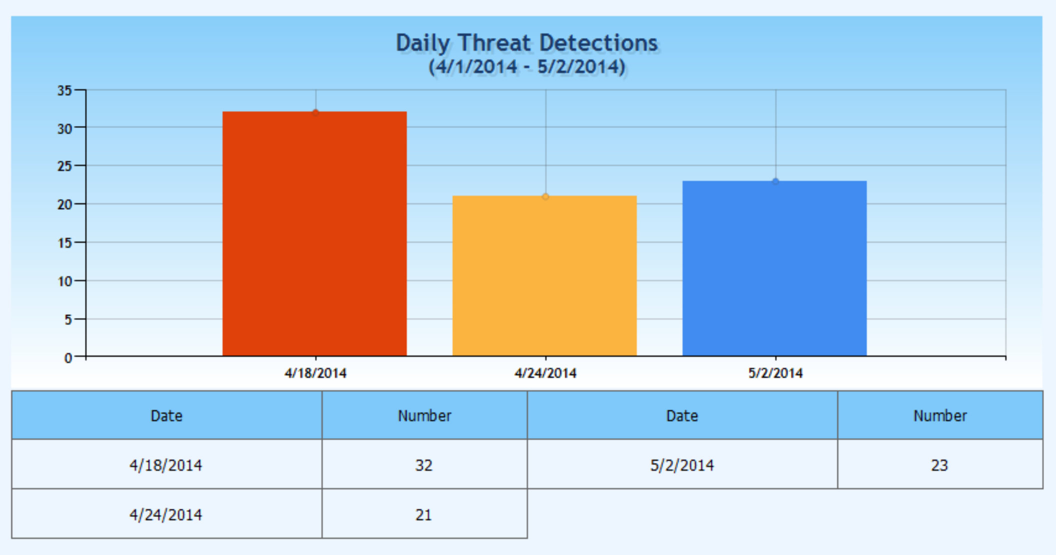
This report provides vertical bar graphs to show both threat detections and exploit detections for each week and each day of the specified time frame. There is no detail provided as to the number of threats/exploits, or to endpoints or usernames involved. Statistics pertaining to threats are based on detections by the *Anti-Malware* managed client. Statistics pertaining to exploits are based on detections by the *Anti-Exploit* managed client.



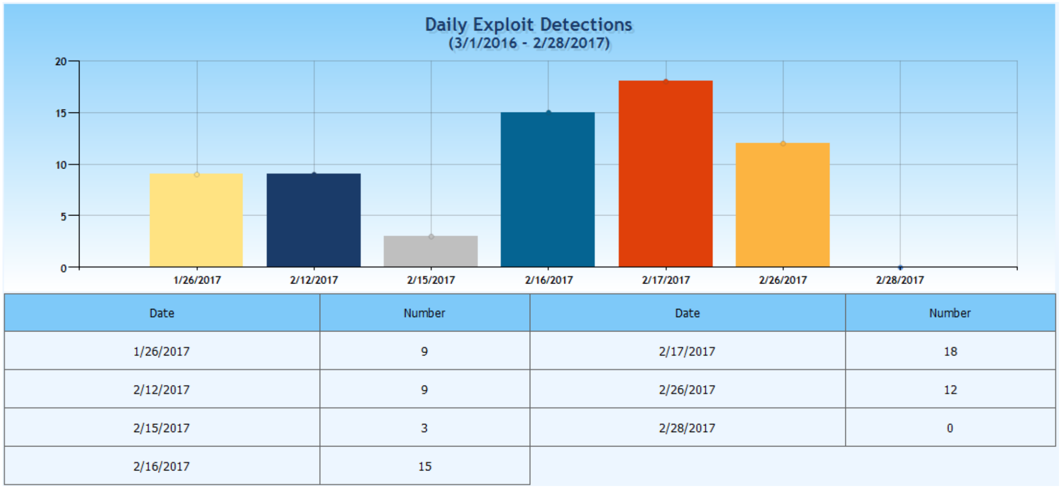
Week	Number	Week	Number
1 (4/13/2014 - 4/19/2014)	32	3 (4/27/2014 - 5/2/2014)	23
2 (4/20/2014 - 4/26/2014)	21		



Week	Number	Week	Number
1 (4/13/2014 - 4/19/2014)	13	3 (4/27/2014 - 5/2/2014)	5
2 (4/20/2014 - 4/26/2014)	11		



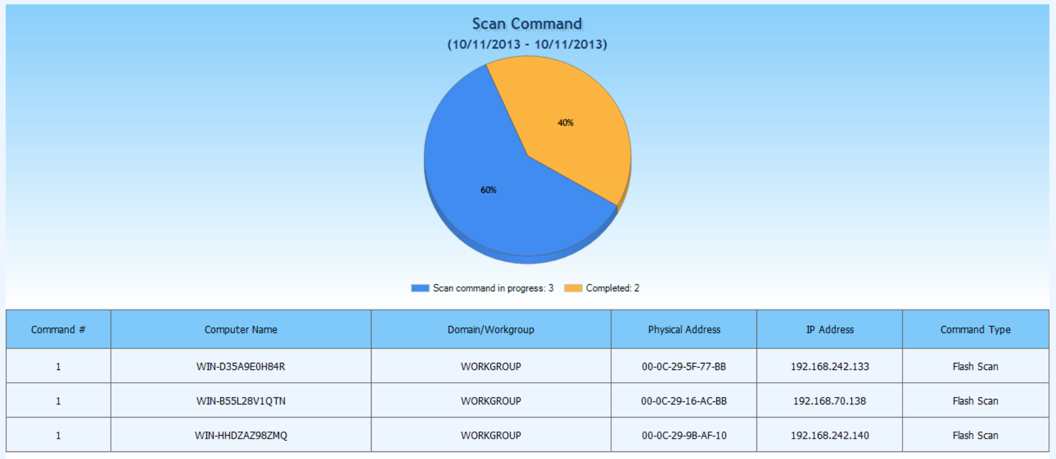
Date	Number	Date	Number
4/18/2014	32	5/2/2014	23
4/24/2014	21		



Date	Number	Date	Number
1/26/2017	9	2/17/2017	18
2/12/2017	9	2/26/2017	12
2/15/2017	3	2/28/2017	0
2/16/2017	15		

Client Scan Report

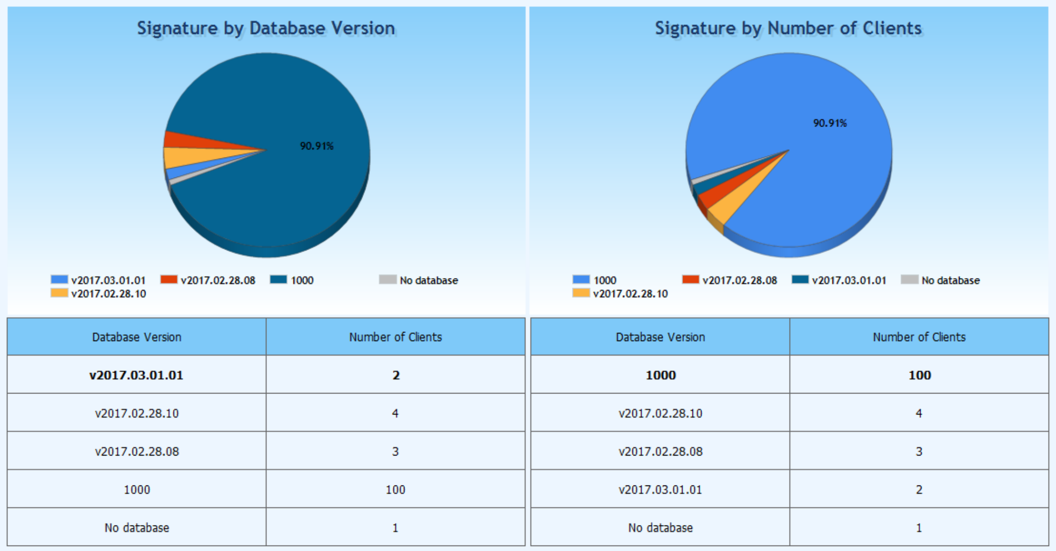
This report shows the ratio between completed scans and in-process scans over a specified time frame for all *Anti-Malware* managed clients. The number of in-process scans should be at or near zero, as these should reflect only those initiated but not yet completed. In-process scans that do not fit these criteria indicate problems on an endpoint which prevent scan completion.



Command #	Computer Name	Domain/Workgroup	Physical Address	IP Address	Command Type
1	WIN-D35A9E0H84R	WORKGROUP	00-0C-29-5F-77-BB	192.168.242.133	Flash Scan
1	WIN-B55L28V1QTN	WORKGROUP	00-0C-29-16-AC-BB	192.168.70.138	Flash Scan
1	WIN-HHDZAZ98ZMQ	WORKGROUP	00-0C-29-9B-AF-10	192.168.242.140	Flash Scan

Client Signature Report

This report shows two pie charts, the first representing the count of *Anti-Malware* managed clients sorted by Signature Database version, and the second sorted by the number of clients (in descending order) based on the Signature Database version used. Information presented on the two is essentially the same. Only the sort order is different. Information shown is current as of the time that the report is generated. There is no relation to selected start and end dates.



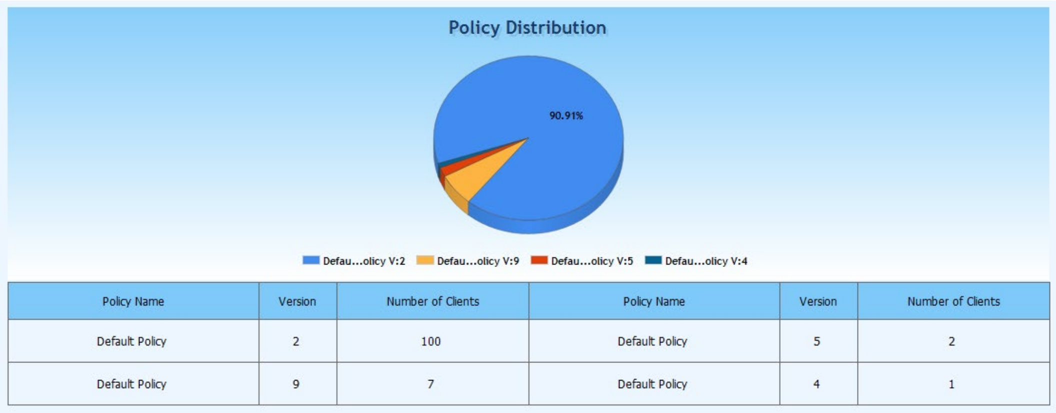
Database Version	Number of Clients
v2017.03.01.01	**2**
v2017.02.28.10	4
v2017.02.28.08	3
1000	100
No database	1

Database Version	Number of Clients
1000	**100**
v2017.02.28.10	4
v2017.02.28.08	3
v2017.03.01.01	2
No database	1

Policy Deployment Report

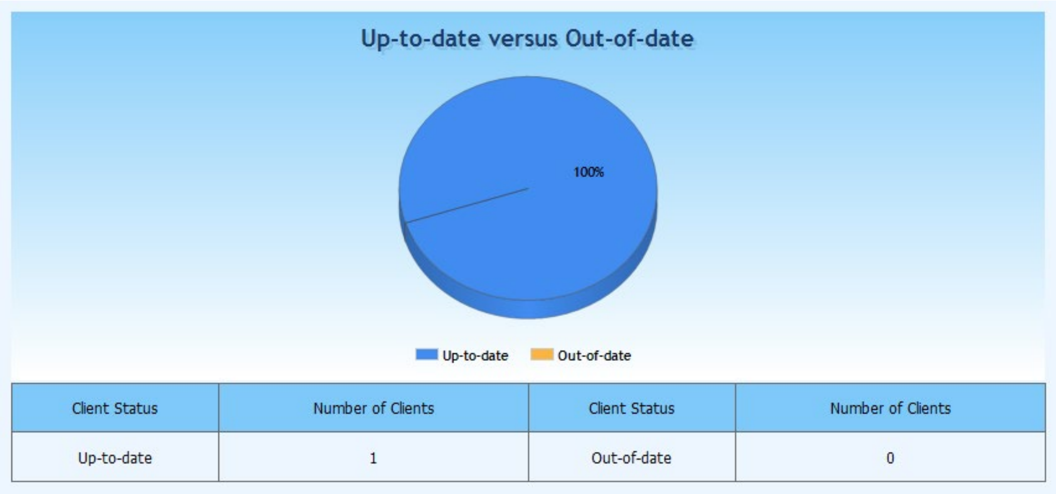
This report is a group of five subreports which focus specifically on policies used by managed clients. Please note that information shown is current…there is no relation to selected time frames. These subreports are:

Policy Distribution – This report shows a graphical representation of endpoints utilizing different policies/policy versions. *Malwarebytes Management Console* initially assigns a default policy which can be customized by the administrator, and also allows creation of new policies tailored more closely to specific needs of individual endpoints, departments, or users. If the *Up-to-date versus Out-of-date* report indicates endpoints using obsolete policies, this report will tell you which policies are affected, allowing the situation to be corrected.



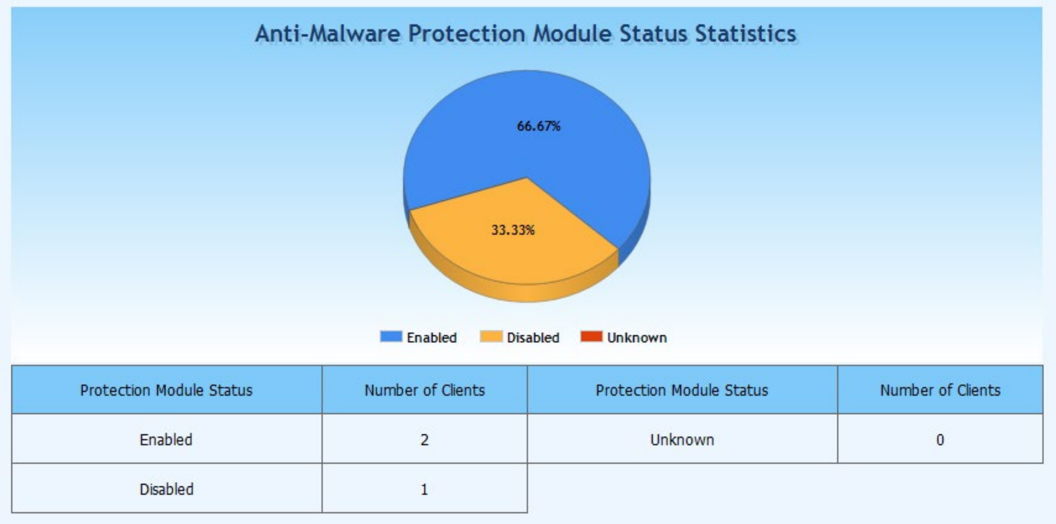
Policy Name	Version	Number of Clients	Policy Name	Version	Number of Clients
Default Policy	2	100	Default Policy	5	2
Default Policy	9	7	Default Policy	4	1

Up-to-date versus Out-of-date – This report shows the ratio between endpoints with up-to-date policies compared to out-of-date policies. This implies endpoints which have not updated to policies which have been updated. This indicates a communication issue between these endpoints and Server, and is clarified further by the *Policy Distribution* report.



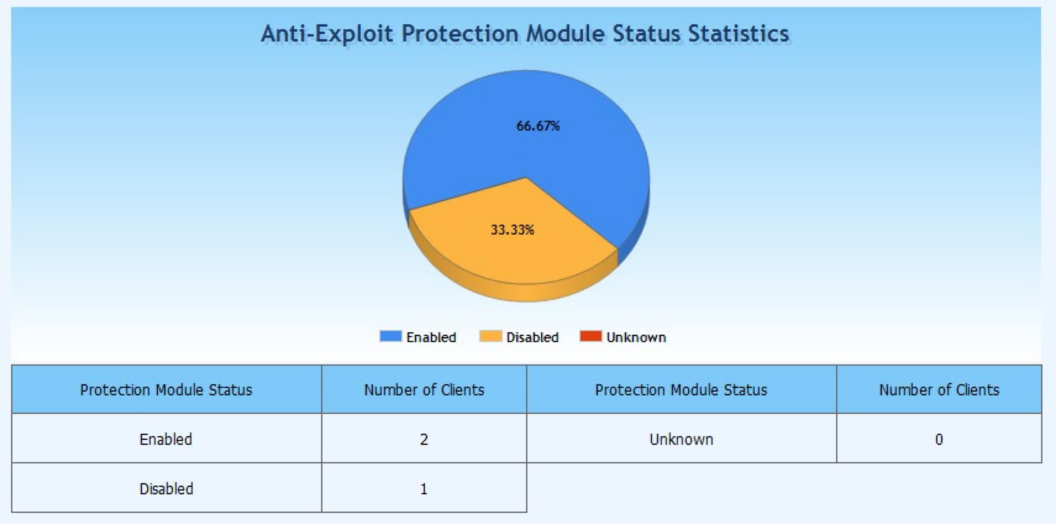
Client Status	Number of Clients	Client Status	Number of Clients
Up-to-date	1	Out-of-date	0

Anti-Malware Protection Module Status Statistics – This report shows the ratio between *Anti-Malware* managed clients taking advantage of real-time protection (Protection Module enabled) compared to remediation mode (scheduled scans only).



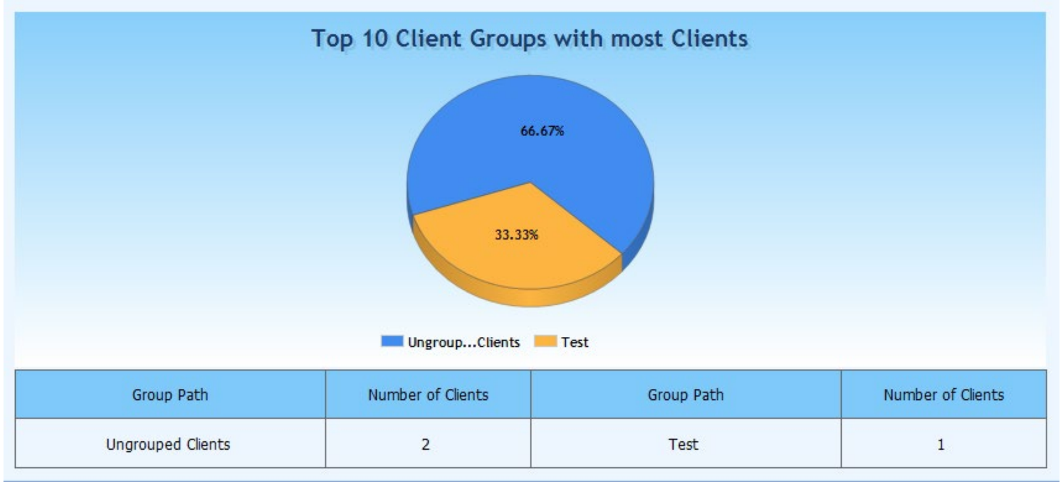
Protection Module Status	Number of Clients	Protection Module Status	Number of Clients
Enabled	2	Unknown	0
Disabled	1		

Anti-Exploit Protection Module Status Statistics – This report shows the ratio between *Anti-Exploit* managed clients taking advantage of real-time protection (Protection Module enabled) compared to endpoints with no Anti-Exploit client installed.



Protection Module Status	Number of Clients	Protection Module Status	Number of Clients
Enabled	2	Unknown	0
Disabled	1		

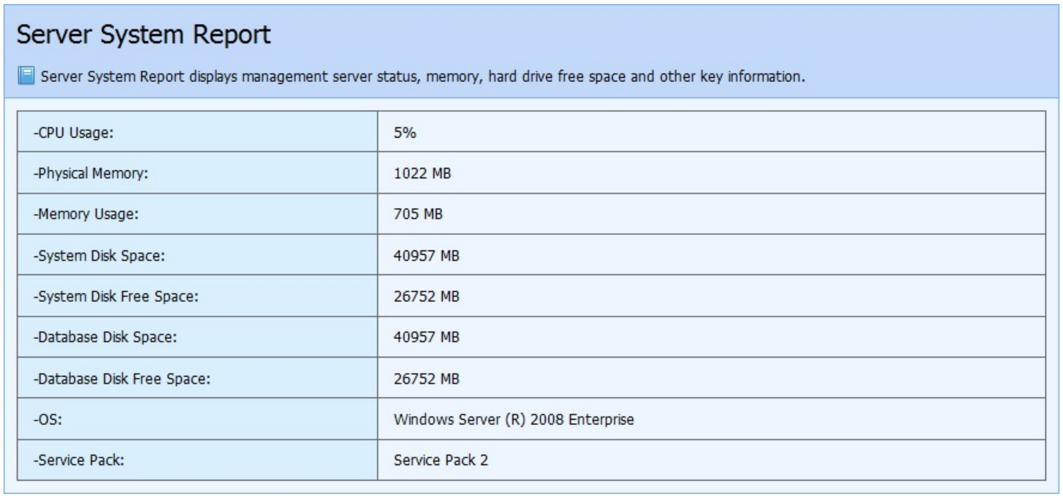
Top 10 Client Groups with most Clients – This report shows the distribution of endpoints by client groups in a pie chart format, with specific number of clients in each group shown in a corresponding table. This report is limited to the ten most populous client groups. Endpoints listed as Ungrouped Clients are also shown. Because network throughput can be negatively impacted by signature updates, scans and reporting of scan results, it is ideal to utilize Client Groups to equally distribute this load as widely as possible to minimize traffic spikes. This report is extremely valuable in that regard.



Group Path	Number of Clients	Group Path	Number of Clients
Ungrouped Clients	2	Test	1

Server System Report

This report shows various statistics pertaining to the *Malwarebytes Management Console* Server in a table form. While a majority of the information presented here is static in nature, the administrator should pay attention to the amount of system disk free space and database disk free space. Both of these values are critical to system operation.



Server System Report

Server System Report displays management server status, memory, hard drive free space and other key information.

-CPU Usage:	5%
-Physical Memory:	1022 MB
-Memory Usage:	705 MB
-System Disk Space:	40957 MB
-System Disk Free Space:	26752 MB
-Database Disk Space:	40957 MB
-Database Disk Free Space:	26752 MB
-OS:	Windows Server (R) 2008 Enterprise
-Service Pack:	Service Pack 2

- *System Disk Space* is a finite number, and on this report is limited to drive C (the primary disk drive).
- *System Disk Free Space* also refers specifically to drive C. *Malwarebytes Management Console* will have an effect on this value by creation of server logs, client logs being processed and logs which are created as a result of infrastructure operations. Additionally, if SQL Server is used in place of SQL Server Express, increases in Database Disk allocation will cut into System Disk Free Space as well. While no large changes are expected here, this should be monitored on a periodic basis.

- *Database Disk Space* represents the amount of disk space that has been allocated for database usage. If SQL Server Express is used, this number should not exceed 10000 MB (megabytes). If SQL Server is used, this value will often exceed 10000 MB, and may increase over time if the SQL Database Administrator determines that higher disk allocation is required.
- *Database Disk Free Space* is a critical parameter, and represents the difference between Database Disk Space and the amount of disk that is currently being used. If this value drops to near zero or begins to decrease at a more rapid pace than has been noted during monitoring, increased disk allocation (SQL Server), database maintenance (both SQL Server and SQL Server Express) or database migration (SQL Server Express) may be required. This parameter should be monitored on a regular basis.

Please note that all of these values are determined to be accurate only when the *Malwarebytes Management Console* Server is installed on a physical server. If installed on a VMware virtual machine, known accuracy issues exist.

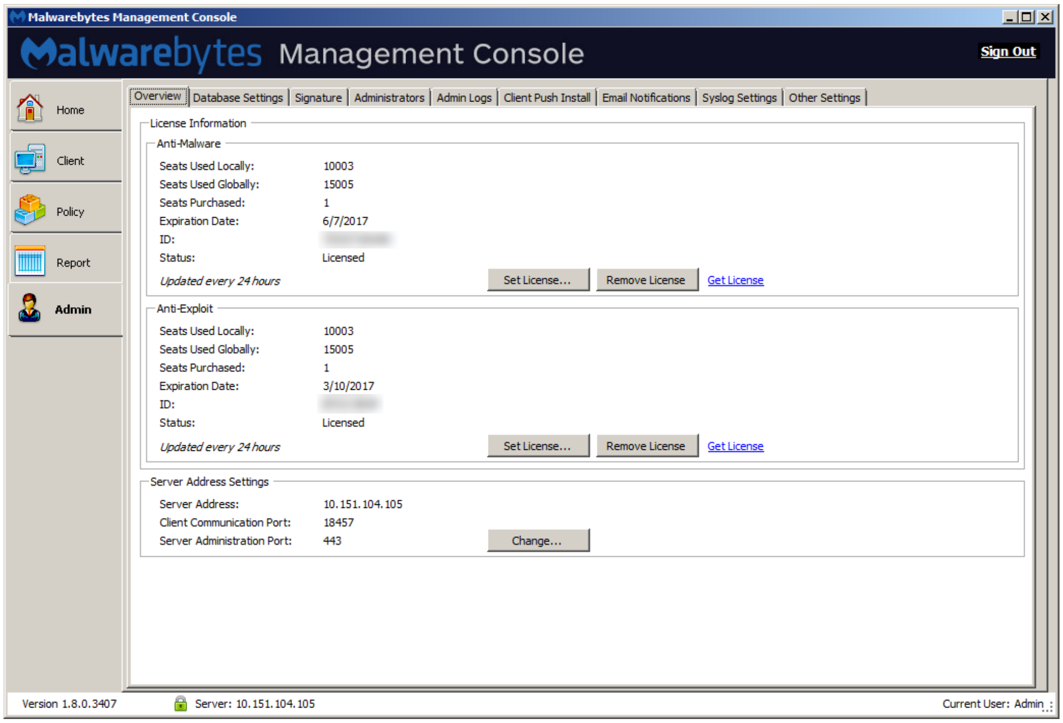
Admin Module

The Admin (Administration) module is used to perform server administration tasks. The Admin page features the following tabs:

- Overview – Server license/identity settings
- Database Settings – SQL database and cleanup settings
- Signature – Update settings
- Administrators – Defines administrators/users and their permissions
- Admin Logs – Access to server operation logs
- Client Push Install – Endpoint discovery, install simulation and client installation
- Email Notifications – Settings pertaining to email notifications
- Syslog Settings – Defining specifications for logging of client security events
- Other Settings – General server settings, including proxy and Active Directory connectivity

Overview tab

The Overview tab displays information pertaining to your *Malwarebytes Management Console* client license(s) and server communication settings. All settings are modifiable by the *Malwarebytes Management Console* Administrator. A screenshot is shown below.



License Information

Anti-Malware

Seats Used Locally: 10003
Seats Used Globally: 15005
Seats Purchased: 1
Expiration Date: 6/7/2017
ID: [redacted]
Status: Licensed
Updated every 24 hours

Anti-Exploit

Seats Used Locally: 10003
Seats Used Globally: 15005
Seats Purchased: 1
Expiration Date: 3/10/2017
ID: [redacted]
Status: Licensed
Updated every 24 hours

Server Address Settings

Server Address: 10.151.104.105
Client Communication Port: 18457
Server Administration Port: 443

Version 1.8.0.3407 Server: 10.151.104.105 Current User: Admin

Information for each setting is presented below.

License Information

This panel provides information pertaining to your client license(s), as well as the capability to contact Malwarebytes Sales regarding licensing and licensing questions, and to enter new product license(s) which you have obtained for your *Malwarebytes Management Console* installation.

Referring to the above screenshot, you will notice that *Malwarebytes Anti-Malware* has been installed. In this instance, *Malwarebytes Anti-Exploit* has also been installed. Both client license status are shown as Licensed. In addition, each has a *Get License* button. Clicking this button connects you to the Malwarebytes website so that you may purchase additional seats. If your status is Unlicensed, clicking the *Get License* link allows you to purchase licenses.

In addition to indicating the number of seats purchased for a given license, **Seats Used Locally** and **Seats Used Globally** are also displayed. These represent the number of seats used from the local management server as well as the number of seats used on all management servers which are associated with the same license key (if applicable).

Please note that license information is automatically updated every twenty-four (24) hours.

Server Address Settings

The Server Address Settings panel shows current settings for the *Malwarebytes Management Console* Server Address, Client Communication Port number, and Server Communication Port Number. Initially, the Server Address is based on the endpoint's IP address. You may also use a fully-qualified domain name (FQDN) instead of an IP address.

> **WARNING:** The *Server Address* is used for all communications between the *Malwarebytes Management Console* and managed clients deployed on endpoints. Use of a static IP address is highly recommended. If this is not possible, a fully-qualified domain name should be used instead. If the IP address is changed after any client software has been deployed, communication failures between client and server will occur.
>
> You may use the Force Managed Clients to use new address checkbox to push the server address out to clients, however offline clients may require further attention. If this is the case, please refer to the *Malwarebytes Endpoint Security Best Practices Guide*.

Port numbers shown are default ports used by *Malwarebytes Management Console*. The *Server Administration Port* uses the standard port number assigned for SSL communications. If the server used for *Malwarebytes Management Console* is also home to other web-based services/applications, you should change this port number to prevent conflicts.

Database Settings

The SQL Database Setting panel specifies the data storage mechanism used by *Malwarebytes Management Console*. It also allows a new external database/instance to be specified in place of the existing database, regardless of whether the existing database is SQL Server Express or an external SQL Server. If an external SQL Server database is specified, the following information must be supplied.

- **Database Address –** IP address/FQDN of the server on which SQL Server is installed (if different than the server on which *Malwarebytes Management Console* is installed), and the pre-existing instance name, in the format:

  ```
  IP-or-FQDN\instance
  ```

- **SA User Name** – Pre-existing username of the SQL Administrator (or another database user with permissions set to the same level as the SQL Administrator).

- **SA Password –** Password assigned to the database user.

The new database/instance must already exist prior to this change, and security permissions must be set appropriately for the SQL Administrator username that is also specified as part of this change.

> **WARNING:** If a change is to be made to the SQL Database setting after *Malwarebytes Management Console* has been put into operation, the customer must take responsibility to migrate all data from the old instance to the new instance prior to implementation of the database change. Depending on the volume of data to be migrated, the amount of time required to perform this task should be considered.

Cleanup Settings

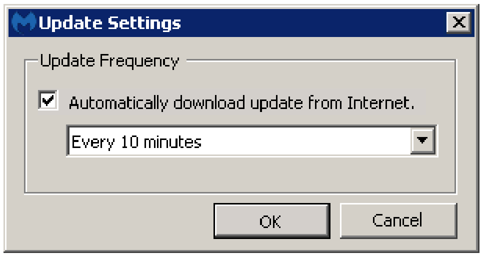
This option allows the Management Console Administrator to define how long threat information is retained, and as a result, the valid lifespan of reporting data. You may choose to retain data indefinitely, or you may choose one of several different cutoff dates. It is strongly recommended that the *Malwarebytes Management Console* Administrator be extremely familiar with disk usage as a function of available space in the SQL environment. This is typically more of an issue if SQL Server Express is used as the *Malwarebytes Management Console* system database, but should not be taken for granted.

Signature tab

This tab displays current database update settings, with provision to modify the time interval between updates. The version number of the threat database increments with each update. The version number shown uses a specific naming convention. Using an example will help to illustrate that. If the version shown is *v2017.02.24.09*, that indicates the ninth update issued on February 24, 2017. The calendar used is referenced to Greenwich Mean Time (GMT), so North American users may see version numbers which appear to be one day in the future if they look at this tab in the evening.

If you wish to load available signature updates prior to the next scheduled update time, you may do so by clicking the *Update Now* button. Clicking the *Change…* button associated with Update Frequency will display the *Update Settings* dialog as shown below.

Threat signatures are updated on a regular basis. One of several time intervals may be selected using the pulldown menu shown. If a direct connection to the internet is not available and a proxy server is used, you will need to configure proxy server settings, located in the *Other Settings* tab.



Update Settings

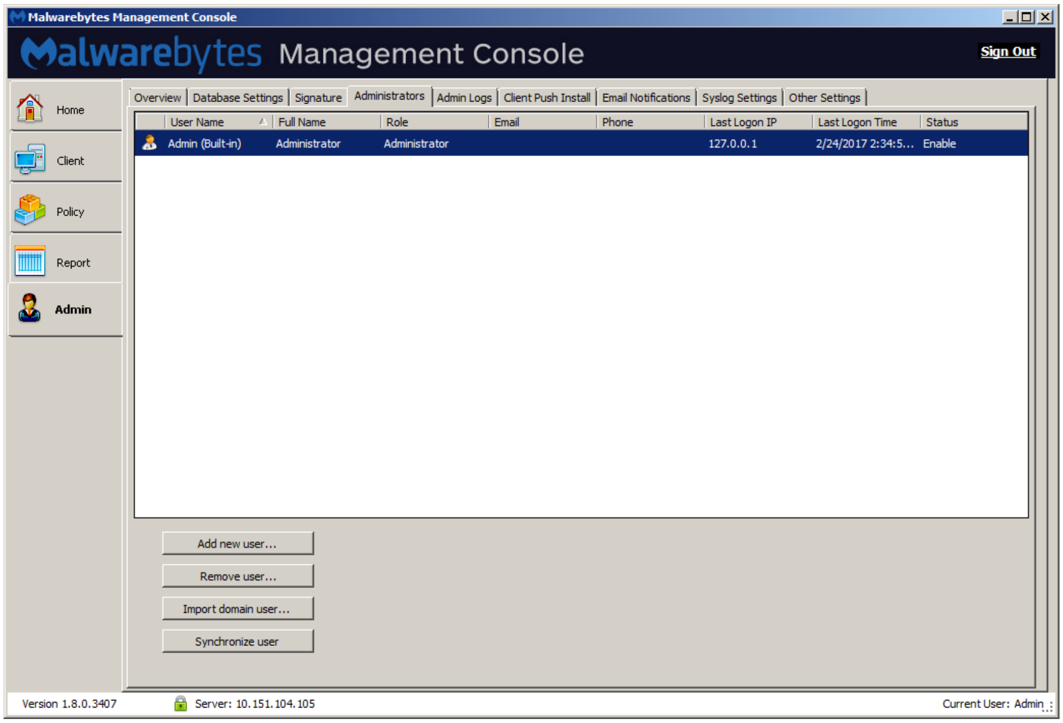
Update Frequency

☑ Automatically download update from Internet.

Every 10 minutes

Administrators Tab

The Administrators tab contains a list of system users/administrators authorized to use *Malwarebytes Management Console*. Within this discussion, the term *user* applies to both *Malwarebytes Management Console* users and administrators. For each user, the list contains name and contact information, their role, the IP address from which the user last logged on, and the date and time of that logon. The *Administrators* tab is shown here.



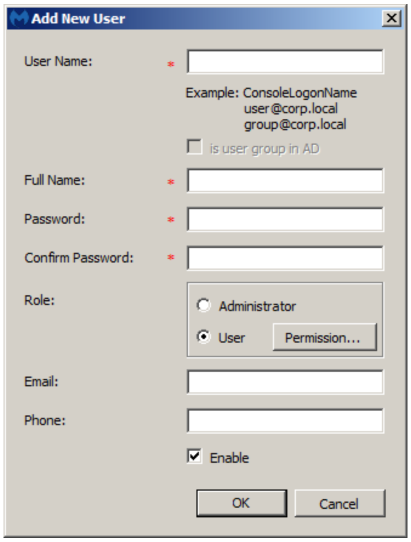
Malwarebytes Management Console

User Name	Full Name	Role	Email	Phone	Last Logon IP	Last Logon Time	Status
Admin (Built-in)	Administrator	Administrator			127.0.0.1	2/24/2017 2:34:5…	Enable

Version 1.8.0.3407 Server: 10.151.104.105 Current User: Admin

At the bottom left of the screen are four options which allow addition, deletion and modification of user information.

Add New User



Add New User

User Name: *

Example: ConsoleLogonName
user@corp.local
group@corp.local

□ is user group in AD

Full Name: *

Password: *

Confirm Password: *

Role: ○ Administrator
● User Permission...

Email:

Phone:

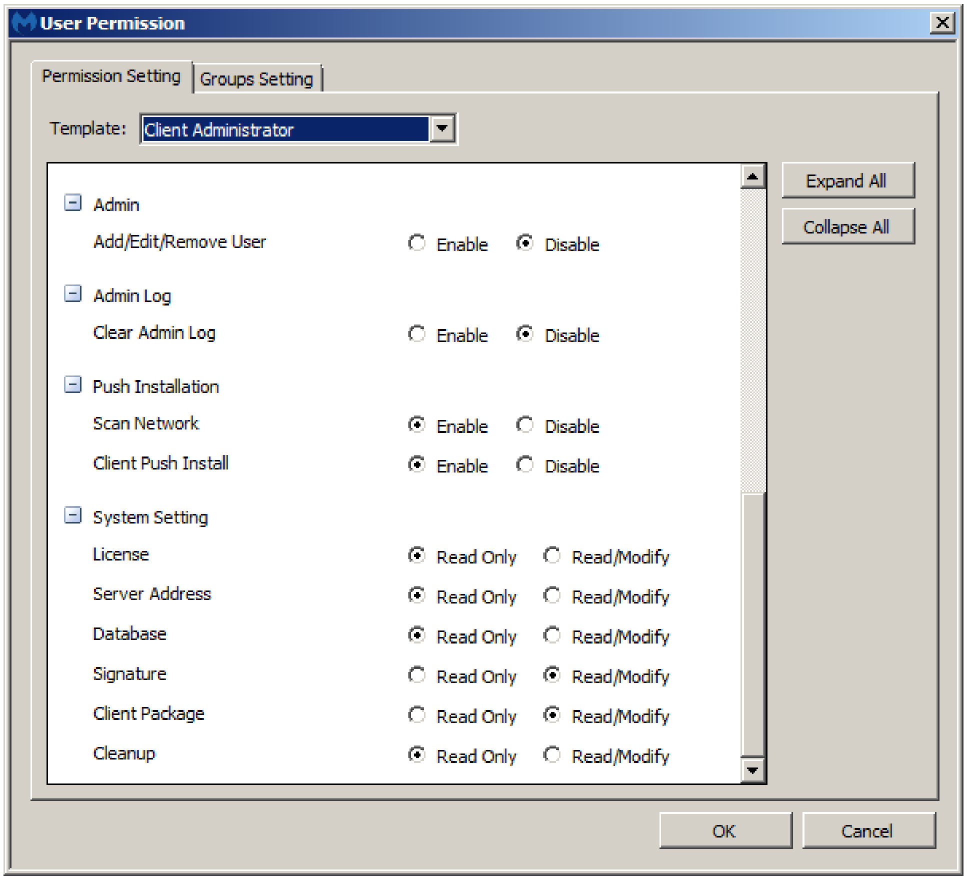
☑ Enable

Clicking the *Add new user…* button allows the addition of one or more new *Malwarebytes Management Console* users via the *Add New User* window, which pops up at the center of the screen. That window is shown here.

Panel behavior is dependent on whether users are input directly via this panel, or imported from Active Directory. This determination is made by checking construction of the User Name as it is being typed. If User Name contains a backslash (\) or at sign (@), data entry access to most other fields is immediately disabled, the assumption being that data will instead originate from Active Directory.

When *Malwarebytes Management Console* is integrated with Active Directory, you also have the ability to import AD groups. If the user name fits the criteria for an Active Directory domain, the *is user group in AD* checkbox becomes available for selection. There is no password associated with it. For that reason, a group cannot logon to *Malwarebytes Management Console* as a user. The value in adding an AD group here is that every member of the AD group becomes a valid user because of their AD group membership.

You may also assign a *Role* to the new user. If *Role* is defined as Administrator, the new user has full control of *Malwarebytes Management Console*. If *Role* is set to User, the *Permissions* button allows granular authority to be specified with the User Permission panel. A screenshot of a portion of that panel is shown below.

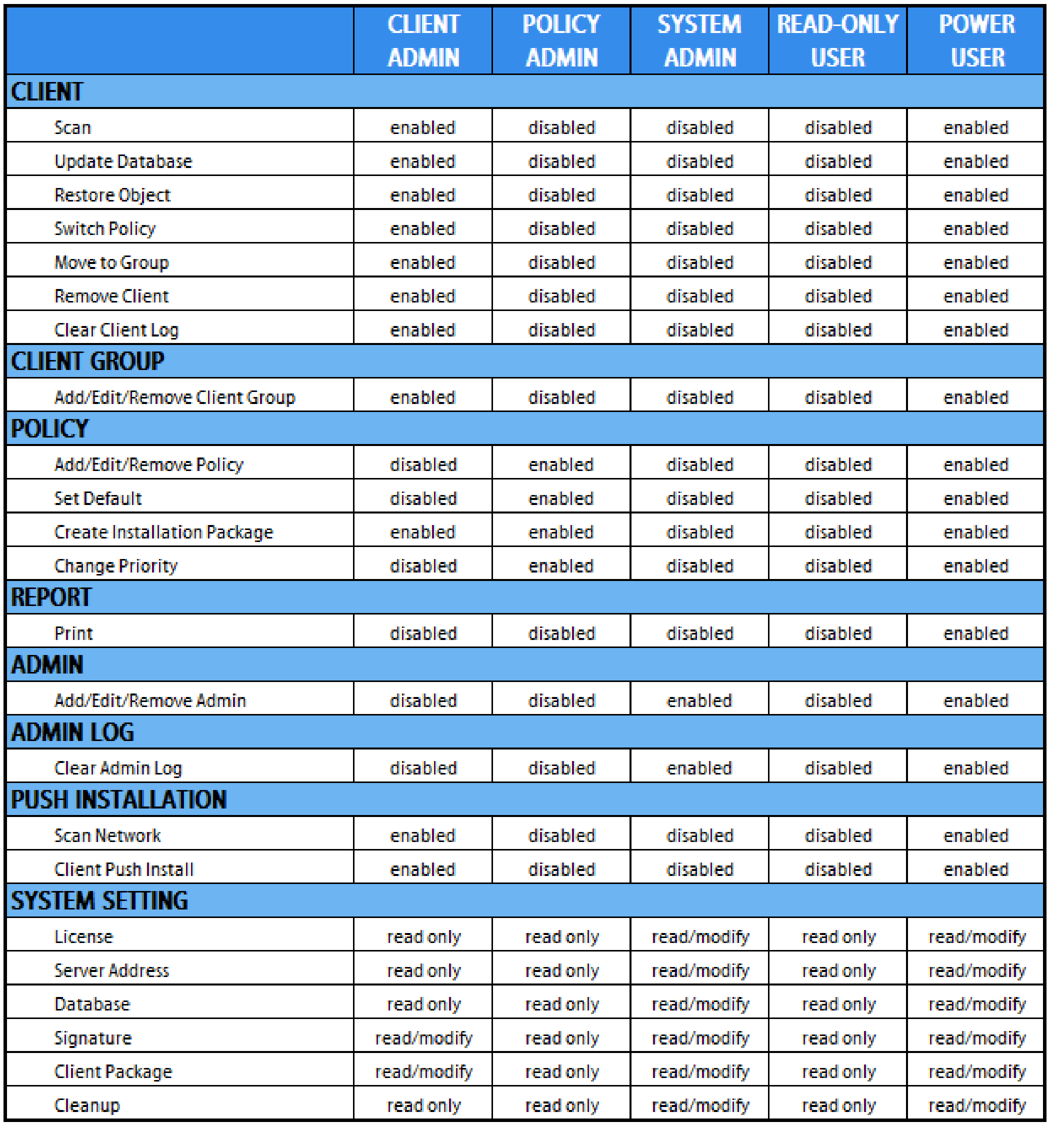


User Permission

Template: Client Administrator

⊟ Admin		
Add/Edit/Remove User	○ Enable	● Disable
⊟ Admin Log		
Clear Admin Log	○ Enable	● Disable
⊟ Push Installation		
Scan Network	● Enable	○ Disable
Client Push Install	● Enable	○ Disable
⊟ System Setting		
License	● Read Only	○ Read/Modify
Server Address	● Read Only	○ Read/Modify
Database	● Read Only	○ Read/Modify
Signature	○ Read Only	● Read/Modify
Client Package	○ Read Only	● Read/Modify
Cleanup	● Read Only	○ Read/Modify

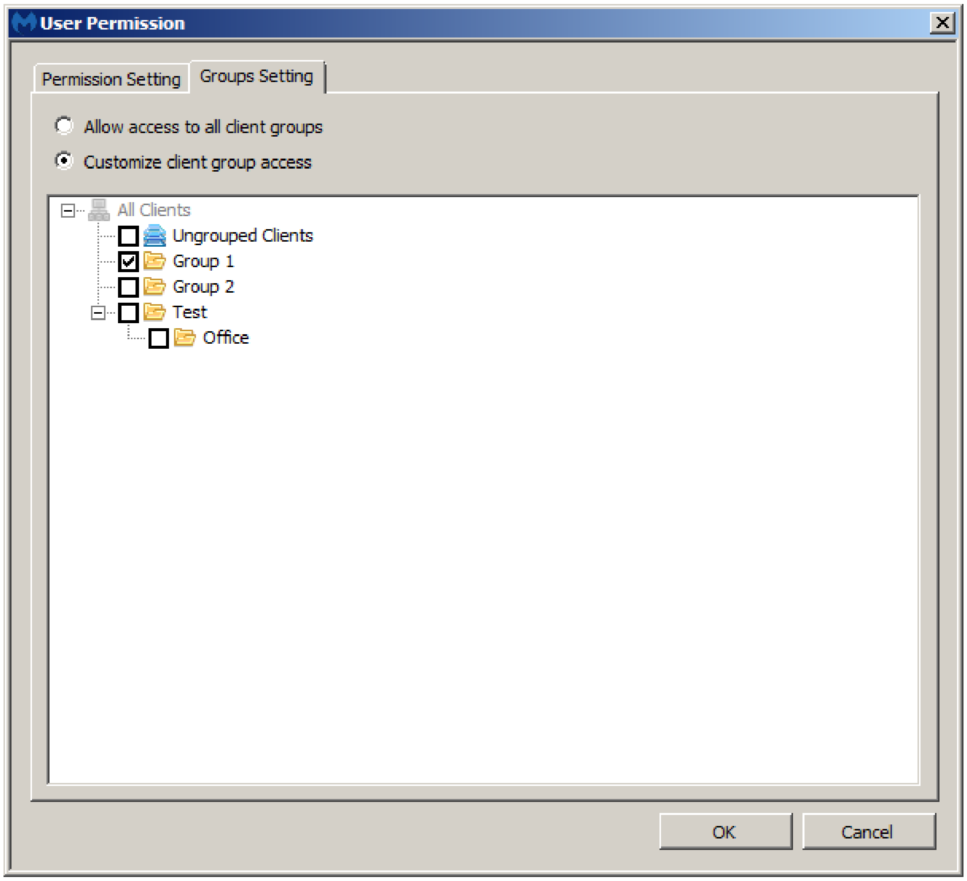
Five primary roles have been defined, which may be selected using the Template pulldown at the upper left corner. Once selected, you may choose specific permissions that you wish to be assigned to that role. In the screenshot above, only Client-based roles are shown to illustrate capabilities. A full list of default permissions assigned to each role is shown in the following table.



	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

In addition to the permissions which you have granted to the user, you may specify where the user may exert this authority. This is done on the *Groups Setting* tab. A *group* is a collection of endpoints that have been organized based on something which they have in common. This may be where they are located, who uses them, or the type of roles which they are used for. That is up to the administrator. Please see page 19 of this guide for more information pertaining to groups and how they may be used.

You may grant a user authority over all groups, or only over specified groups. A screenshot of the *Groups Setting* tab is shown here.



○ Allow access to all client groups
● Customize client group access

- All Clients
  - □ Ungrouped Clients
  - ☑ Group 1
  - □ Group 2
  - □ Test
    - □ Office

When you select *Customize client group access*, you may select the checkbox for each defined group to grant authority over the group. There are a few rules which apply here:

- If *Customize client group access* has been specified and all groups have been selected, that does not equate to *Allow access to all client groups*. If a new group is added later, the user will not have any authority over that group unless authority has been specifically granted for the newly-added group.
- Inheritance applies to group selection. Using the example shown above, selecting the Test group also selects the Office subgroup, because it is a child of Test. Selecting the Office group does not grant authority over the Test group.

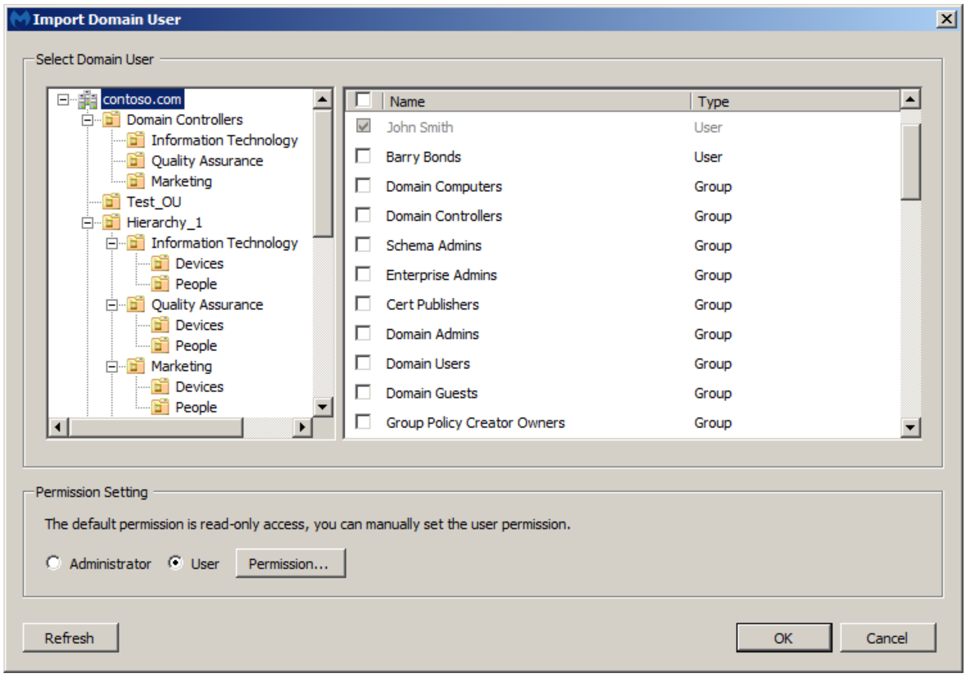
Remove User

This option removes the highlighted (selected) *Malwarebytes Management Console* user account, regardless of whether it was created locally or through Active Directory. All login credentials and permissions will be removed, and the account will no longer be active in the Administrators list. If the specified *Malwarebytes Management Console* user was created through Active Directory, the account will remain there until removed through Active Directory, but will no longer have login access to *Malwarebytes Management Console*.

Import Domain User

You may also create *Malwarebytes Management Console* users through the *Import Domain User* option. Clicking this button launches the Import Domain User panel, as shown below.

PLEASE NOTE: If you have not specified a Domain Query Account prior to execution of this command, you will be prompted for a user name and password associated with that account.



□	Name	Type
☑	John Smith	User
□	Barry Bonds	User
□	Domain Computers	Group
□	Domain Controllers	Group
□	Schema Admins	Group
□	Enterprise Admins	Group
□	Cert Publishers	Group
□	Domain Admins	Group
□	Domain Users	Group
□	Domain Guests	Group
□	Group Policy Creator Owners	Group

The default permission is read-only access, you can manually set the user permission.

○ Administrator ● User

The left side of the screen shows the Organizational Unit (OU) structure of the Active Directory installation. When the domain is selected (as shown here), the only AD users that can be imported are ones who are not members of an organizational unit. Selecting an individual OU permits only those users who are a member of that OU to be imported. Permission settings for the selected users may be defined in the same manner as described in the *Add New User* option which was outlined earlier. In the above screenshot, one AD user is grayed out, and his name is preceded by a checkmark in the checkbox. This indicates that he has already been added to the list of *Malwarebytes Management Console* Administrators.

You may also import Active Directory groups in a similar manner. As the above screenshot shows, both users and groups are available for import into *Malwarebytes Management Console*. Creation, organization, and membership of groups are performed in Active Directory, and all group settings are inherited by *Malwarebytes Management Console* when the group is imported. It is also possible for an Administrator to add a group of users with pre-set permissions, as well as import individuals that belong to that group as individual Administrators with different permissions than the group was assigned. This allows Active Directory administrators to update or change permissions for particular users through the *Malwarebytes Management Console* alone for Malwarebytes-specific permissions.

Synchronize User

This option issues queries to the domain's Active Directory Server for all Administrator users and groups, and updates *Malwarebytes Management Console* with data returned from the query. Domain User/Admin changes made in Active Directory must be reflected in *Malwarebytes Management Console* to remain synchronized with Active Directory. **Please note** that this option and the *Sync Now* button on the *Other Settings* tab of the Admin module perform different tasks. Here, synchronization is specific to AD users and groups. The *Sync Now* button is specific to endpoints and networked devices which are governed by Active Directory.

Admin Logs Tab

The Admin Logs tab contains a running log of user logins, logouts, actions taken by users, and the results of those actions. All information shown here is read-only. The following information is presented in the log:

- Event Date and Time
- User Name
- Console IP address
- Category (event type)
- Event ID
- Event Description
- *Malwarebytes Management Console* Server Name

You may sort on any of these items by clicking on the item. Clicking the item a second time reverses the sort order. Right-clicking anywhere in the active area of the log displays a context menu which enables the user to refresh the display, save the log as a text file, filter based on any of the categories shown, reset the filter, or clear all logs. Please note that this context menu does not act on individual log entries, but on the log as a whole.

Client Push Install Tab

This tab enables the *Malwarebytes Management Console* Administrator to remotely install managed client software on endpoints. There are pre-requisites that must be met before this is possible, to assure that the managed client can communicate with the *Malwarebytes Management Console*. These are listed in *System Requirements: Managed Clients*, on page 6.

Pre-Requisites – Creation of Policies (optional)

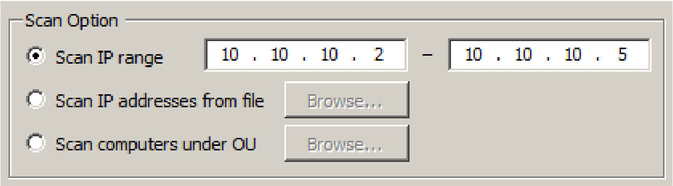
Another item which must be considered before client software can be pushed out to endpoints is the definition of policies. In a nutshell, a policy determines client behavior. Depending on an endpoint's function, location, and vulnerability level, many operational parameters may be tuned to afford the best protection. In lieu of a set of pre-defined policies, a single default policy may be used. This subject is described in detail in the **Policy Module** section of this guide, beginning on page 24.

Pre-Requisites – Creation of Client Groups (optional)

The final item which must be considered is creation of client groups. Assigning managed clients to client groups helps to maintain higher network throughput by coordinating use of network resources during heavier communication between *Malwarebytes Management Console* and its clients. This subject is described in detail in the **Client Module** section of this guide, beginning on page 18.

Scanning the Network – Scan Selection Options

The first step in deployment of client software is to identify endpoints. This is done by scanning the network. A preliminary required step is to choose *what* to scan. This is shown in the screenshot below.



Scan Option

● Scan IP range 10 . 10 . 10 . 2 – 10 . 10 . 10 . 5

○ Scan IP addresses from file

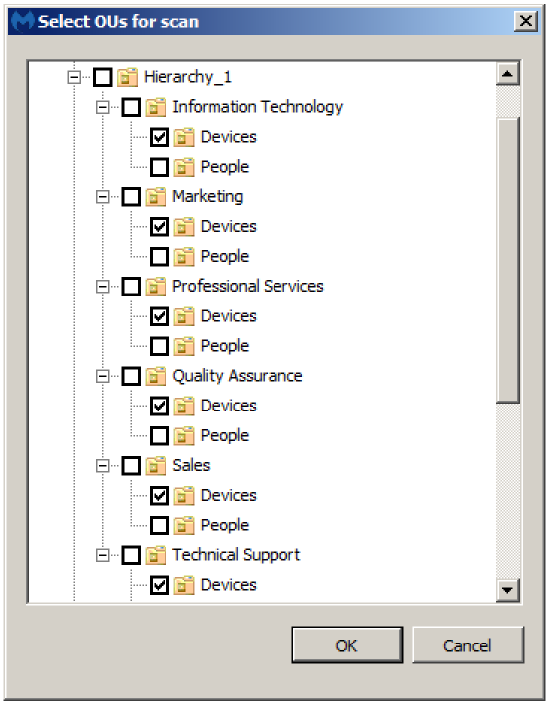
○ Scan computers under OU

- *Scan IP range* allows you to select a contiguous block of IP addresses. All networked devices within that address range are selected, without regard to device type. Computers, servers, printers, and all other networked devices whose address is within the specified range will be scanned.

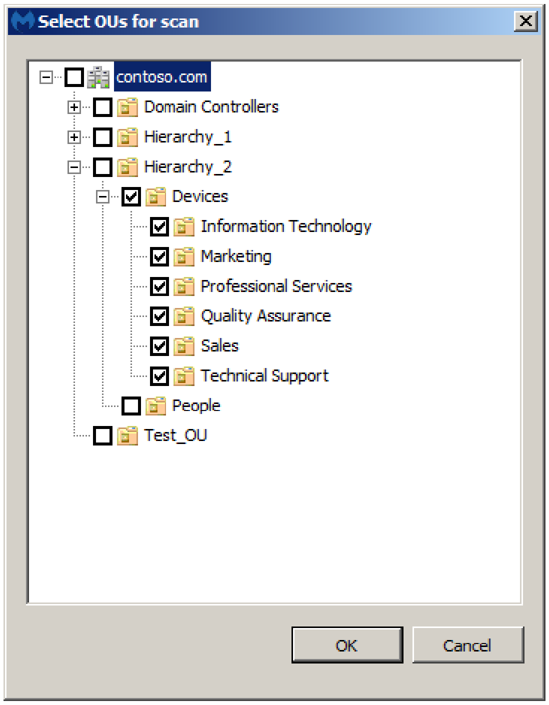
  PLEASE NOTE that a maximum of 65536 IP addresses can be scanned. Using the address shown above as an example, the maximum range is from 10.10.0.1 to 10.10.255.255. When using contiguous address ranges, the first two octets must remain fixed, while the full range of addresses in the last two octets is available.

- *Scan IP addresses from file* provides the capability to use a text file which contains a list of IP addresses, host names, and fully-qualified domain names (FQDNs) – one entry per line. This method is valuable if your LAN contains a small isolated subnet or if you utilize VPN connections for remote users/facilities.

- *Scan computers under OU* provides the capability to build your list of endpoints directly from the Organizational Unit structure contained in Active Directory, as shown in the screenshot below.


Select OUs for scan

- □ Hierarchy_1
  - □ Information Technology
    - ☑ Devices
    - □ People
  - □ Marketing
    - ☑ Devices
    - □ People
  - □ Professional Services
    - ☑ Devices
    - □ People
  - □ Quality Assurance
    - ☑ Devices
    - □ People
  - □ Sales
    - ☑ Devices
    - □ People
  - □ Technical Support
    - ☑ Devices


Select OUs for scan

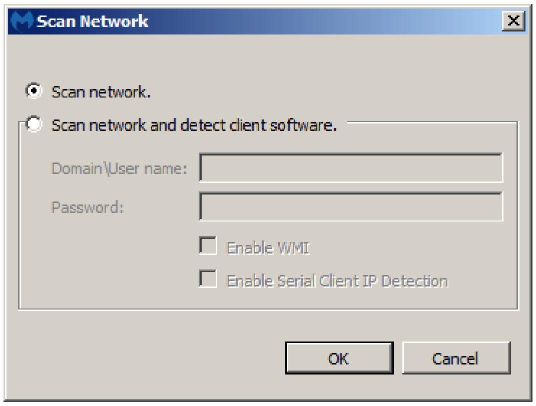
- □ contoso.com
  - □ Domain Controllers
  - □ Hierarchy_1
  - □ Hierarchy_2
    - ☑ Devices
      - ☑ Information Technology
      - ☑ Marketing
      - ☑ Professional Services
      - ☑ Quality Assurance
      - ☑ Sales
      - ☑ Technical Support
    - □ People
  - □ Test_OU

This screenshot shows two examples of how Organizational Units may be selected for scanning. Either of these models may represent your AD structure, but most Active Directory administrators agree that no single model is ideal for every company. The example on the left shows a hierarchy where each OU is individually selected. Each department has two OUs associated with it – Devices and People. Only the Devices OU is relevant for the purpose of scanning.

The example on the right shows a hierarchy where each departmental OU is part of a higher-level Devices OU. Here, selecting Devices will automatically select every departmental OU below it in the hierarchy. If any of those OUs were to be omitted, it by itself could be unchecked. Again, your AD layout will determine how you select OUs for scanning.

Scanning the Network – Scan Execution Options

Once endpoints/IP addresses have been selected for scanning, the actual scanning may take place. *Malwarebytes Management Console* provides a number of ways to scan your network. Clicking the *Scan…* button launches the Scan Network window in the center of the screen, as shown below.


Scan Network

● Scan network.

○ Scan network and detect client software.

Domain\User name:

Password:

□ Enable WMI

□ Enable Serial Client IP Detection

This window allows selection of the specific type of scan to be used. There are two primary scan options, the second option allowing for further specification of methods. Detailed descriptions of these methods are detailed here, to increase understanding of the process, as well as to assist with troubleshooting should any problems arise.

Option 1A: Scan IP range/Scan Network – *Malwarebytes Management Console* uses Address Resolution Protocol (ARP) to query each IP address in the specified address range. Detected endpoints respond with their IP address and MAC address. *Malwarebytes Management Console* then uses UDP to request identity information from these endpoints' NetBIOS Name Service. Detected endpoints respond with their hostname (in reverse-text order).

Option 1B: Scan IP range/Scan network and Detect Client Software – This method begins with the steps outlined in Option 1A. When complete, *Malwarebytes Management Console* uses SMB over TCP to transfer files to the remote endpoint. A remote service is then created and executed, which detects existing managed client software on the endpoint (if present). Detection status is returned to *Malwarebytes Management Console*, followed by termination of the remote service, deletion of the test files, and termination of the connection between server and endpoint. Authentication on the endpoint is required. If the user name specified does not have sufficient permissions, Windows Management Instrumentation (WMI) must be employed.

Option 2A: Scan IP addresses from file/Scan Network – This method behaves in the same manner as Option 1A, the only difference being that host names and/or fully-qualified domain names are converted to IP addresses via usage of NetBIOS Name Service before detection attempts take place.

Option 2B: Scan IP addresses from file/Scan network and Detect Client Software – This method is similar to Option 1B, the exception being that host names and/or fully-qualified domain names are converted to IP addresses via usage of NetBIOS Name Service before detection attempts take place.

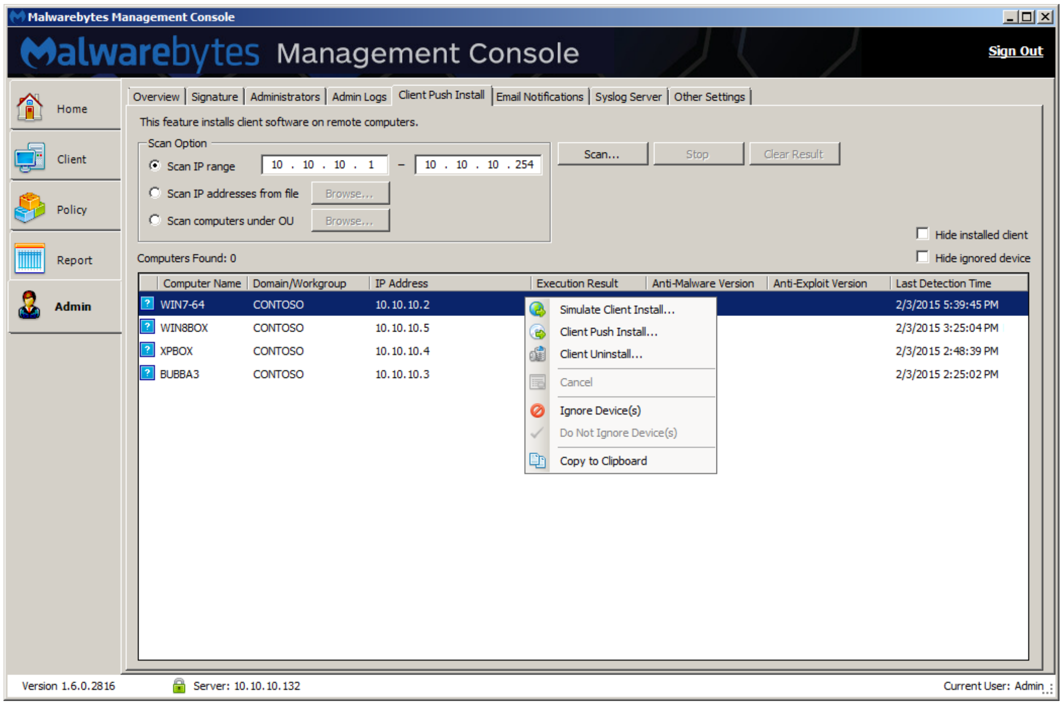
Option 3A: Scan endpoints under OU/Scan Network - *Malwarebytes Management Console* issues a LDAP query to Active Directory, requesting a list of all endpoints based in the selected Organizational Unit (OU). Using that list, *Malwarebytes Management Console* populates an internal database table with identifying information for each endpoint, then using the endpoint name returned from Active Directory, query the domain name server for the IP address. Finally, the MAC address will be obtained utilizing steps outlined in Option 1A (above)

> **WARNING:** Active Directory enforces a policy which specifies a maximum of five thousand (5000) results can be returned via an LDAP query. This policy may be changed by the AD administrator, but LDAP queries issued by *Malwarebytes Management Console* are subject to this policy. If the maximum number of results is returned as a result of this query, *Malwarebytes Management Console* cannot issue successive queries to access the remainder of the endpoints. In this case, lower level OUs should be utilized (when possible) to return all results.

> **WARNING:** The list of endpoints returned as a result of an LDAP query may contain both client and server-class computers if they are members of the same OU. A *Malwarebytes Anti-Malware* managed client should not be installed on a server, while it is acceptable to install a *Malwarebytes Anti-Exploit* client on a server. If you are not using *Malwarebytes Anti-Exploit*, you may ignore servers as part of any subsequent client installation and/or monitoring.

Option 3B: Scan computers under OU/Scan network and Detect Client Software - This method begins with the steps outlined in Option 3A. When complete, *Malwarebytes Management Console* uses SMB over TCP to transfer files to the endpoint. A remote service is then created and executed which detects managed client software on the endpoint (if present). Detection status is returned to *Malwarebytes Management Console*, followed by termination of the remote service, deletion of the test files, and termination of the server-client connection. Authentication on the remote endpoint is required. If the user name specified does not have sufficient permissions, Windows Management Instrumentation (WMI) must be employed. **Please note** that the warnings specified for Option 3A also apply here.

The following screenshot shows the results of a scan using the *Scan IP Range* method. In this case, there are four endpoints within the IP address range specified (10.10.10.2-10.10.10.254, *Malwarebytes Management Console* being 10.10.10.1).



This feature installs client software on remote computers.

Scan Option

● Scan IP range 10 . 10 . 10 . 1 – 10 . 10 . 10 . 254

○ Scan IP addresses from file

○ Scan computers under OU

□ Hide installed client

□ Hide ignored device

Computers Found: 0

Computer Name	Domain/Workgroup	IP Address	Execution Result	Anti-Malware Version	Anti-Exploit Version	Last Detection Time
? WIN7-64	CONTOSO	10.10.10.2				2/3/2015 5:39:45 PM
? WIN8BOX	CONTOSO	10.10.10.5				2/3/2015 3:25:04 PM
? XPBOX	CONTOSO	10.10.10.4				2/3/2015 2:48:39 PM
? BUBBA3	CONTOSO	10.10.10.3				2/3/2015 2:25:02 PM

Version 1.6.0.2816 Server: 10.10.10.132 Current User: Admin

If the scan showed results which contained endpoints where managed clients had previously been installed, you may hide those endpoints by checking the *Hide installed client* checkbox. The scan may also show devices which are not eligible for installation of managed clients (servers, printers, fax machines, etc.). These devices can be hidden by checking the *Hide ignored device* checkbox.

The *Admin Logs* tab will show the full results of the scan, including all of the IP addresses specified regardless of whether a networked device is associated with that address. Text that appears for addresses of this type is:

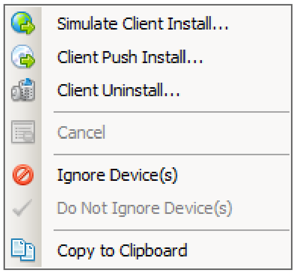
> *Scan failed. A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond*

Malwarebytes Management Console considers lack of response as a failure. *Malwarebytes Management Console* cannot determine whether a lack of response is due to no device present or due to a networking failure.

ICON	CLIENT STATUS
🟩	Client installed and operational
🟨	Client registration failure
?	Status unknown to server
?	Ignored device
▨	Passed simulation
☒	Error condition

Please note the icons shown to the left of each endpoint name. There are four unique icons used to indicate the status of each endpoint identified during the scan. This screenshot shows each status icon.

This is the first time that these endpoints have been scanned, specifically for the purpose of identifying targets for managed client installation. As a result, their status (as a client) is unknown.



Referring to the *Scan Results* screenshot, one endpoint is highlighted for the purpose of showing the context menu. The menu is shown here

Five different operations can be performed on selected clients using this context menu. Each of these operations is explained below.

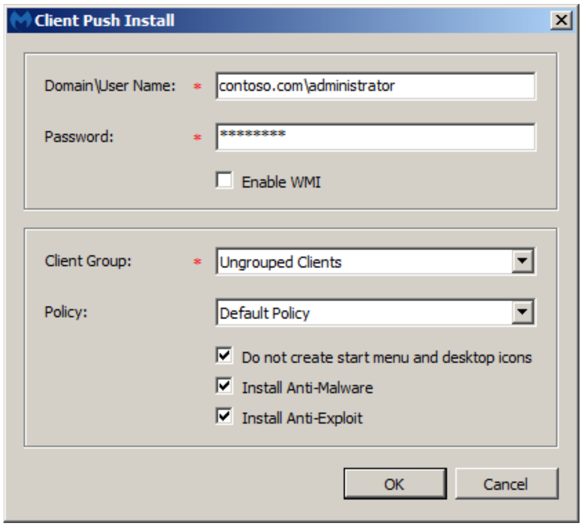
Simulate Client Install

This option tests the ability of *Malwarebytes Management Console* to open communication ports between itself and an endpoint on which a managed client is to be installed on. Once ports have been opened, the server will push several files to the endpoint, create a service on the endpoint, use that service to execute certain files, gather pass/fail status, return that status to the server, terminate the remote service, and finally delete files that were sent to the endpoint. If all of these tests pass, the simulation is considered to be a success. Please note that this is only a simulation, and does not actually perform a client push install.

Because this process adds, deletes and executes files that are located on another endpoint, authentication is required. The domain user name and password for an administrative user on the endpoint is required. In addition, there may be times in which 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.



Domain\User Name: * contoso.com\administrator

Password: * *********

☐ Enable WMI

Client Group: * Ungrouped Clients

Policy: Default Policy

☑ Do not create start menu and desktop icons

☑ Install Anti-Malware

☑ Install Anti-Exploit

A **Domain\User Name** and its associated **Password** are required for this process. These credentials must provide administrative access to the endpoint on which the managed client is to be installed. 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 elect to install managed client software on this endpoint as a member of **Ungrouped Clients**, or as a member of a specific **Client Group**. A complete discussion of this topic is in the *Client Module* section of this guide (page 18). In addition, a **Policy** must be selected before installation can occur. This determines behavior of the managed client during operation. A complete discussion of this topic is in the *Policy Module* section of this guide (page 24).

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 the *Malwarebytes Anti-Malware* client, the *Malwarebytes Anti-Exploit* client, either client or neither. If neither client is installed, communication capability between the server and the endpoint is defined and initialized.

Client Uninstall

This option uninstalls a managed client from a selected endpoint. This option should be used as a preferred method of uninstalling software because it removed the managed client and updates client status on the *Malwarebytes Management Console* Server.

Ignore Device(s)

A network scan will detect every networked device on a network. While you may wish to see every networked device appear on scan results, it is of little value to see printers, servers, or other networked devices where a managed client cannot be installed. Selecting and ignoring these devices will change their status icon. You may also check the *Hide ignored device* checkbox at the upper right corner of the display to hide them.

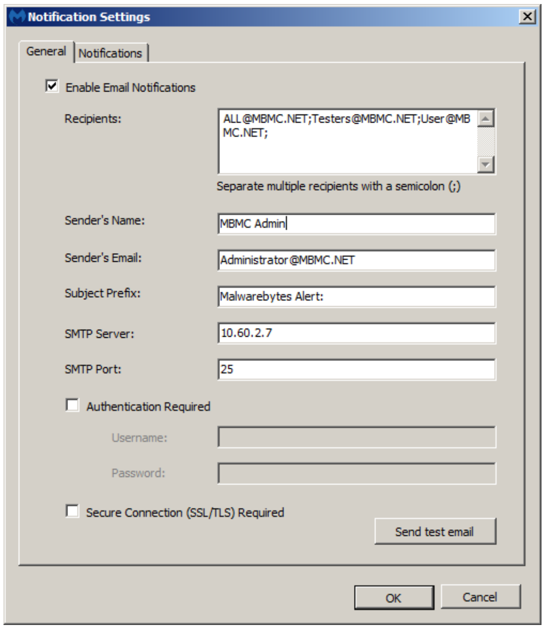
Copy to Clipboard

This option copies scan results (in text format) to your clipboard, so that you may paste it into Notepad. If you have changed the sort order of the displayed results, the copied results will reflect the information as displayed.

Email Notifications tab

This tab allows the administrator to define the conditions which will cause *Malwarebytes Management Console* to send out email notifications. Click the *Change…* button to define settings specific to your environment. That results in launch of the *Notification Settings* window, as shown below.

General tab



Notification Settings

General | Notifications

☑ Enable Email Notifications

Recipients: ALL@MBMC.NET;Testers@MBMC.NET;User@MBMC.NET;

Separate multiple recipients with a semicolon (;)

Sender's Name: MBMC Admin

Sender's Email: Administrator@MBMC.NET

Subject Prefix: Malwarebytes Alert:

SMTP Server: 10.60.2.7

SMTP Port: 25

☐ Authentication Required

Username:

Password:

☐ Secure Connection (SSL/TLS) Required

Here, you can specify detail about notifications to be sent, which includes:

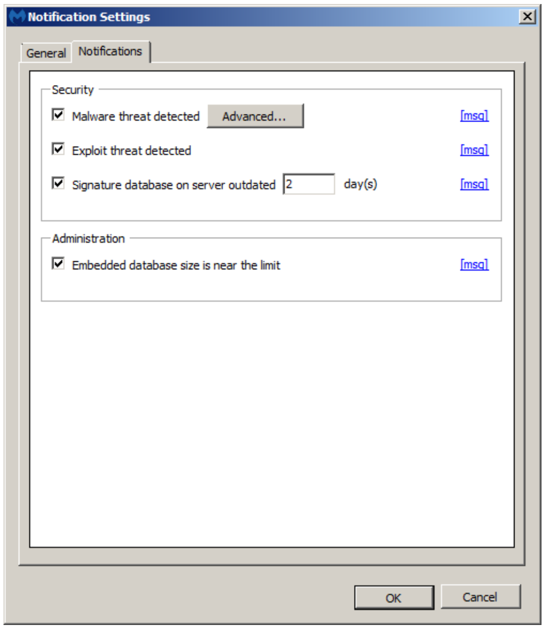
- Email addresses of notification recipient(s). Multiple recipients must be separated by a semicolon (;), and the recipient list must be terminated with a semicolon (;).
- Email sender, sender's email address and subject prefix of the notification.
- IP address (or Fully Qualified Domain Name) and port number of the mail server to be used.
- Whether authentication is to be used, and if so, a username and password that must be used for authentication.
- Whether SSL/TLS security is to be employed.

PLEASE NOTE:

- If you are unsure about server name/IP or port numbers to be used, please consult with your system administrator.
- All email addresses to be used may be subject to validation by your email server. Use the *Send test email* button to verify successful operation.

We can now turn to the notification message itself, which is handled in this window as well – on the *Notifications* tab. The following screenshots illustrate how individual messages are created.

Notifications tab



Security

☑ Malware threat detected Advanced... [msg]

☑ Exploit threat detected [msg]

☑ Signature database on server outdated 2 day(s) [msg]

Administration

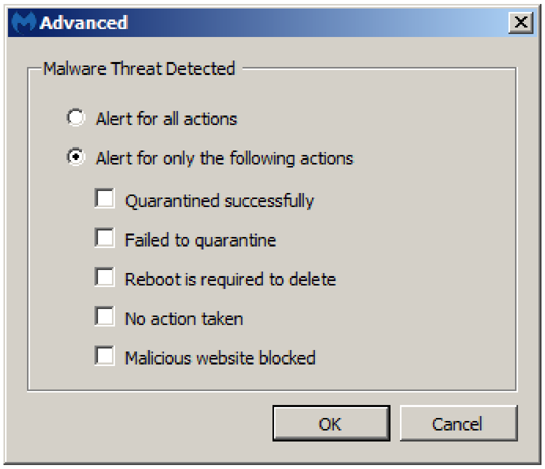
☑ Embedded database size is near the limit [msg]

This screen allows the administrator to select any or all of the four classes of notifications which may be sent. In the order shown, these are:

- Threat detected by Malwarebytes Anti-Malware
- Threat detected by Malwarebytes Anti-Exploit
- Issue preventing threat signature updates from being downloaded
- Management Server database size is nearing 70% of maximum allocation. Please note that this message class applies only when Microsoft SQL Express is used as the system database.

There are several subclasses available for anti-malware notifications, described in the following screenshot.

Also, note the **[msg]** links shown to the right of each notification class. They are described below.



Malware Threat Detected

○ Alert for all actions

● Alert for only the following actions

□ Quarantined successfully

□ Failed to quarantine

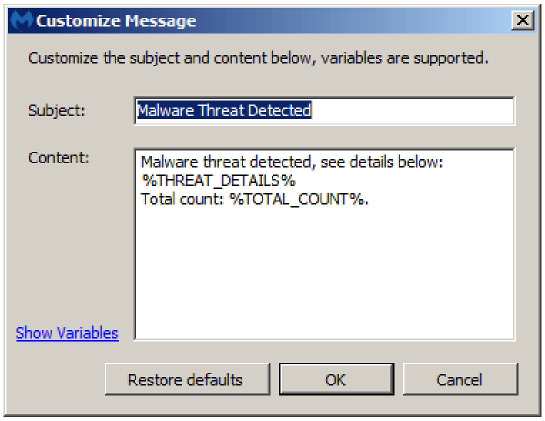
□ Reboot is required to delete

□ No action taken

□ Malicious website blocked

By clicking the *Advanced…* button, you can choose whether notifications will occur for all anti-malware threats, or only for certain criteria.

Please note that the added trigger criteria is available only for notifications related to detection of malware threats.



Customize the subject and content below, variables are supported.

Subject: Malware Threat Detected

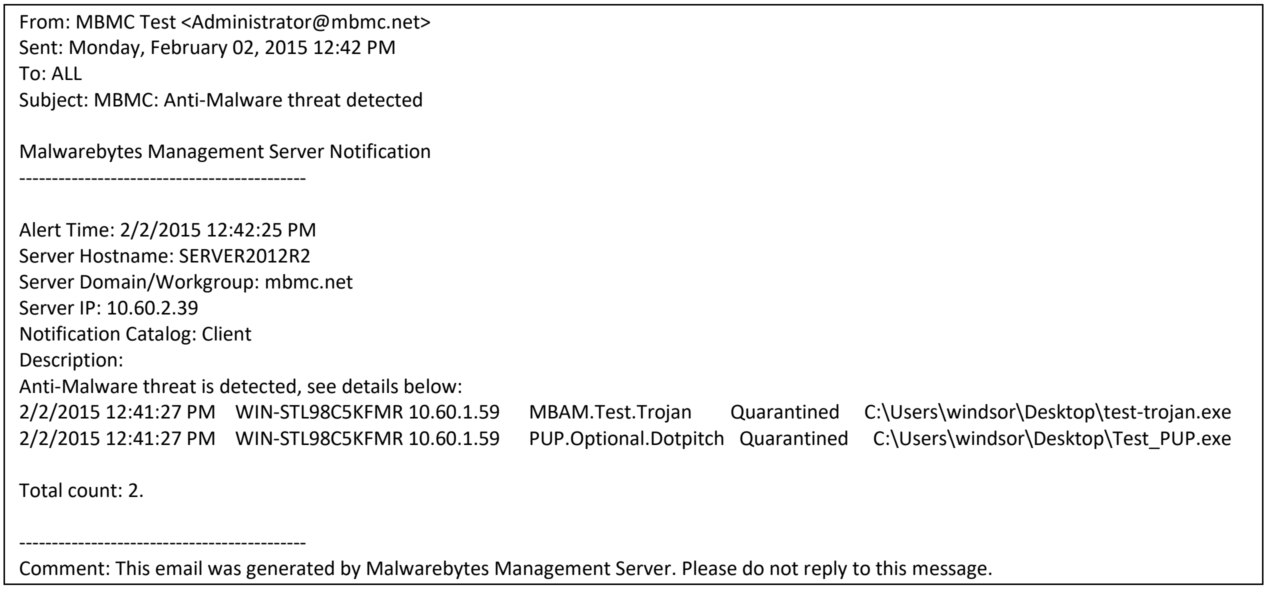
Content:

```
Malware threat detected, see details below:
%THREAT_DETAILS%
Total count: %TOTAL_COUNT%.
```

On this screen, you can define the notification subject and the message content. The subject is tacked onto the end of the subject prefix (defined on the first notification screen).

Each threat-based notification may reference multiple endpoints, and may be based on a single event, or on events which have occurred during a time interval. Please see *Additional Notification Settings* on the following page for more detail on this topic.

The following is a sample email notification sent as a result of product testing. While the specifics included on the message are unique to the testing environment, the overall structure of the message is consistent with what you can expect in your environment.



From: MBMC Test <Administrator@mbmc.net>
Sent: Monday, February 02, 2015 12:42 PM
To: ALL
Subject: MBMC: Anti-Malware threat detected

Malwarebytes Management Server Notification

Alert Time: 2/2/2015 12:42:25 PM
Server Hostname: SERVER2012R2
Server Domain/Workgroup: mbmc.net
Server IP: 10.60.2.39
Notification Catalog: Client
Description:
Anti-Malware threat is detected, see details below:

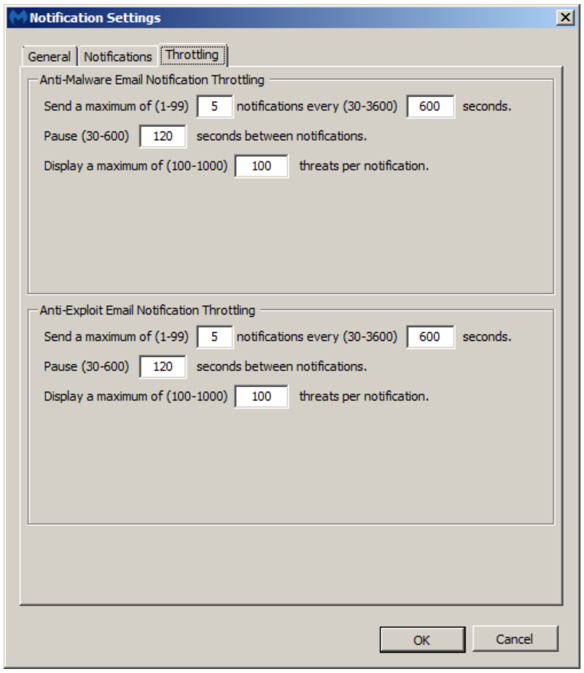
```
2/2/2015 12:41:27 PM   WIN-STL98C5KFMR 10.60.1.59   MBAM.Test.Trojan      Quarantined   C:\Users\windsor\Desktop\test-trojan.exe
2/2/2015 12:41:27 PM   WIN-STL98C5KFMR 10.60.1.59   PUP.Optional.Dotpitch  Quarantined   C:\Users\windsor\Desktop\Test_PUP.exe
```

Total count: 2.

Comment: This email was generated by Malwarebytes Management Server. Please do not reply to this message.

Throttling tab

Keeping you informed with regard to threats is very important to us, but and we want to make sure that meaningful notifications are delivered to you in a timely manner. We have provided throttling settings on this tab, which help to stabilize communications on overloaded email systems, or in the case of a severe malware attack. Please refer to the screenshot below.



Anti-Malware Email Notification Throttling

Send a maximum of (1-99) 5 notifications every (30-3600) 600 seconds.
Pause (30-600) 120 seconds between notifications.
Display a maximum of (100-1000) 100 threats per notification.

Anti-Exploit Email Notification Throttling

Send a maximum of (1-99) 5 notifications every (30-3600) 600 seconds.
Pause (30-600) 120 seconds between notifications.
Display a maximum of (100-1000) 100 threats per notification.

Notifications may be sent for individual threat detections or by time interval. You may fine-tune these settings. Malware notification settings are identical to exploit settings, and each are handled separately.

You can specify the number of notifications sent for all endpoints combined during a specific time period, the interval between notifications, and the maximum number of threats that will appear in each notification.

The interval is to prevent your email system from being overloaded. If the number of threats exceeds the maximum number specified, the notification will include a cross-section of the oldest and newest threats that appear in the notification.

Minimum, maximum and default values are shown in the screenshot.

Additional Notification Settings

There are two additional notifications whose configuration is not exposed to the user in the console interface. These pertain to database notifications.

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

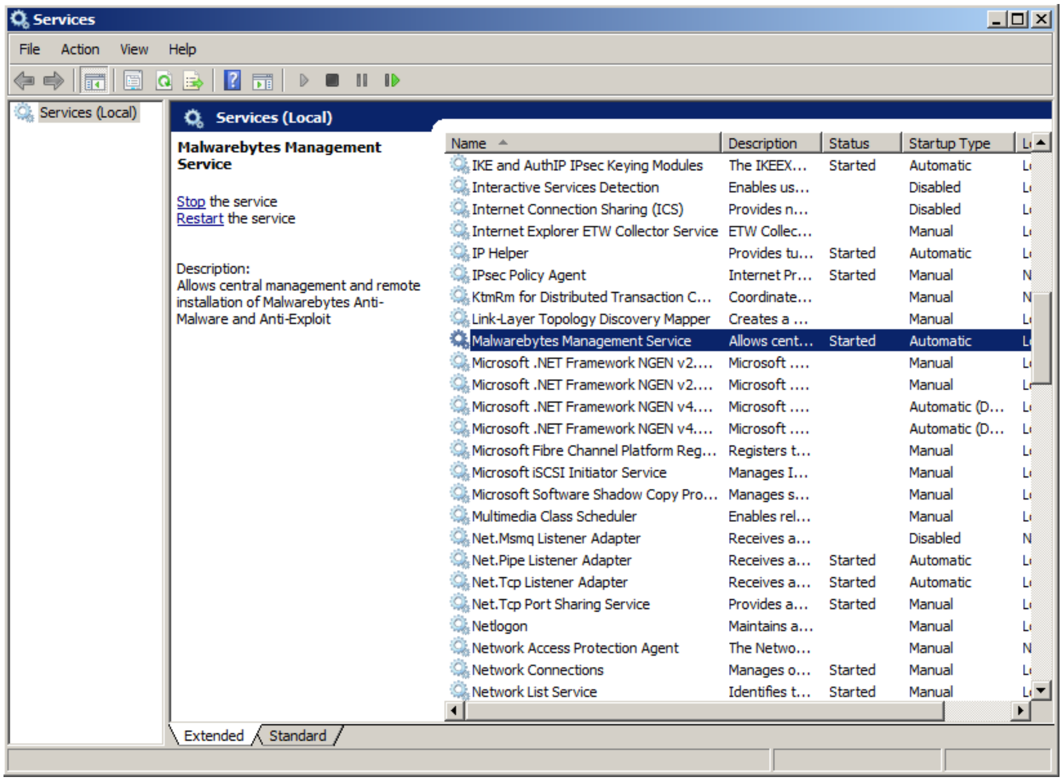
These settings can be found in file:

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

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

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

AlertMaxDatabaseLimit indicates the maximum storage allocation available in the SQL Express database instance (in bytes). You may choose a limit which is less than the maximum if you choose. **AlertMaxDatabaseThreshold** indicates the percentage of storage used as compared to maximum storage allocation. The default value is 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.



Malwarebytes Management Service

Stop the service
Restart the service

Description:
Allows central management and remote installation of Malwarebytes Anti-Malware and Anti-Exploit

Name	Description	Status	Startup Type	L
IKE and AuthIP IPsec Keying Modules	The IKEEX...	Started	Automatic	L
Interactive Services Detection	Enables us...		Disabled	L
Internet Connection Sharing (ICS)	Provides n...		Disabled	L
Internet Explorer ETW Collector Service	ETW Collec...		Manual	L
IP Helper	Provides tu...	Started	Automatic	L
IPsec Policy Agent	Internet Pr...	Started	Manual	N
KtmRm for Distributed Transaction C...	Coordinate...		Manual	N
Link-Layer Topology Discovery Mapper	Creates a ...		Manual	L
Malwarebytes Management Service	Allows cent...	Started	Automatic	L
Microsoft .NET Framework NGEN v2....	Microsoft		Manual	L
Microsoft .NET Framework NGEN v2....	Microsoft		Manual	L
Microsoft .NET Framework NGEN v4....	Microsoft		Automatic (D...	L
Microsoft .NET Framework NGEN v4....	Microsoft		Automatic (D...	L
Microsoft Fibre Channel Platform Reg...	Registers t...		Manual	L
Microsoft iSCSI Initiator Service	Manages I...		Manual	L
Microsoft Software Shadow Copy Pro...	Manages s...		Manual	L
Multimedia Class Scheduler	Enables rel...		Manual	L
Net.Msmq Listener Adapter	Receives a...		Disabled	N
Net.Pipe Listener Adapter	Receives a...	Started	Automatic	L
Net.Tcp Listener Adapter	Receives a...	Started	Automatic	L
Net.Tcp Port Sharing Service	Provides a...	Started	Manual	L
Netlogon	Maintains a...		Manual	L
Network Access Protection Agent	The Netwo...		Manual	N
Network Connections	Manages o...	Started	Manual	L
Network List Service	Identifies t...	Started	Manual	L

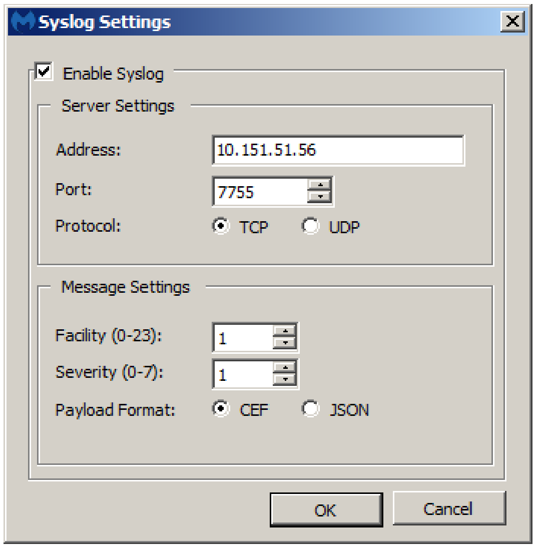
Displayable areas have been resized here to improve readability. Find the service named **Malwarebytes Management Service**, right-click to access the context menu and Restart the service. Once this has been completed, close the Services screen and launch *Malwarebytes Management Console*. This causes 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.

Syslog Settings

Malwarebytes Management Console includes the ability to send security events generated by *Malwarebytes Anti-Malware* and *Malwarebytes Anti-Exploit* managed clients to a syslog server. This allows your security administrator to view Malwarebytes protection activities as part of a site-wide security philosophy.

By default, logging to an external Syslog server is disabled. Click the *Change* button to launch the dialog box shown here.



Syslog Settings

☑ Enable Syslog

Server Settings

Address: 10.151.51.56

Port: 7755

Protocol: ● TCP ○ UDP

Message Settings

Facility (0-23): 1

Severity (0-7): 1

Payload Format: ● CEF ○ JSON

Enable logging by selecting the checkbox at the upper left corner. You must specify the IP (or FQDN) and port number of the Syslog server which you wish to connect to, as well as the preferred communication protocol. You may specify any *Facility* number (in the range 0-23) and any *Severity* (in the range 0-7) for events which originate from Malwarebytes managed clients.

<u>**Please note**</u> that no validation of these specifications is performed. It is the responsibility of the customer to assure that a proper communication channel exists based on data provided.

Log data is sent to the Syslog server in CEF or JSON formats. Each entry contains the date, time, Facility, Severity, Host (hostname for the server on which *Malwarebytes Management Console* is installed, application ("*Malwarebytes-Endpoint-Security*") and log data. Sample log entries are shown below, in both formats. For each, two versions are presented. The first version is the raw log entry as it would appear in system logs. The second version is presented solely to aid in the reader's understanding of the format.

CEF Raw Log Entry

```
04-08-2016 08:11:01 User.Alert 127.0.0.1 1 2016-04-08T08:11:01.10-07:00 PC-WIN123 Malwarebytes-
Endpoint-Security 824 - - ï»¿CEF:0|Malwarebytes|MBMC|1.7.0.3208 MBAM:1.80.2.1012 DB:913030101
MBAE:1.08.2.1189|DETECTION|Exploit ROP attack blocked|5|deviceExternalId=d6961b91-6098-48c4-a64e-
ff75c9e5550e dvchost=PC-WIN123 deviceDnsDomain=WORKGROUP deviceMacAddress=00-0C-29-7C-15-AB
dvc=192.168.10.50 rt=Apr 08 2016 08:10:57 -07:00 cn1=1 cn1Label=ObjectTypeScanned cs6=
cs6Label=ObjectScanned cat=DETECTION cn2=1 cn2Label=Action act=BLOCK outcome=success suser=jdoe
cs5=data cs5Label=Data msg=Attacked application: C:\\Users\\jdoe\\Desktop\\iexplore.exe; Parent
process name: explorer.exe; Layer: Protection Against OS Security Bypass; API ID: 453; Address:
0x76F5FE07; Module: ; AddressType: ; StackTop: 0x002F0000; StackBottom: 0x002ED000; StackPointer:
; Extra:  fname=Internet Explorer filePath=C:\\Users\\jdoe\\Desktop\\iexplore.exe
sourceServiceName=MBAE cs1= cs1Label=Payload cs2= cs2Label=PayloadChecksum cs3=
cs3Label=PayloadUrl cs4= cs4Label=PayloadProc
```

CEF Log Entry (simplified for understanding)

Please note that liberties have been taken here to improve readability of the log entry.

```
HEADER:
Syslog Prefix          : 04-08-2016 08:11:01 User.Alert 127.0.0.1 1 2016-04-08T08:11:01.10-07:00
                         PC-WIN123 Malwarebytes-Endpoint-Security 824 - - ï»¿CEF:0|
Device Vendor          : Malwarebytes|
Device Product         : MBMC|
Device Version         : 1.7.0.3208 MBAM:1.80.2.1012 DB:913030101 MBAE:1.08.2.1189|
Device Event Class ID  : DETECTION|
Name                   : Exploit ROP attack blocked
Severity               : 5

EXTENSION:
deviceExternalId       = d6961b91-6098-48c4-a64e-ff75c9e5550e
dvchost                = PC-WIN123
deviceDnsDomain        = WORKGROUP
deviceMacAddress       = 00-0C-29-7C-15-AB
dvc                    = 192.168.10.50
rt                     = Apr 08 2016 08:10:57 -07:00
cn1                    = 1
cn1Label               = ObjectTypeScanned
cs6                    =
cs6Label               = ObjectScanned
cat                    = DETECTION
```

```
cn2                    = 1
cn2Label               = Action
act                    = BLOCK
outcome                = success
suser                  = jdoe
cs5                    = data
cs5Label               = Data
msg                    = Attacked application: C:\\Users\\jdoe\\Desktop\\iexplore.exe;
                         Parent process name: explorer.exe;
                         Layer: Protection Against OS Security Bypass;
                         API ID: 453;
                         Address: 0x76F5FE07;
                         Module: ;
                         AddressType: ;
                         StackTop: 0x002F0000; StackBottom: 0x002ED000;
                         StackPointer: ;
                         Extra:
fname                  = Internet Explorer
filePath               = C:\\Users\\jdoe\\Desktop\\iexplore.exe
sourceServiceName      = MBAE
cs1                    =
cs1Label               = Payload
cs2                    =
cs2Label               = PayloadChecksum
cs3                    =
cs3Label               = PayloadUrl
cs4                    =
cs4Label               = PayloadProc
```

JSON Raw Log Entry

```
04-08-2016 08:10:41 User.Alert 127.0.0.1 1 2016-04-08T08:10:41.16-07:00 PC-WIN123 Malwarebytes-
Endpoint-Security 824 - - ï»¿{"security_log":{"client_id":"d6961b91-6098-48c4-a64e-ff75c9e5550e",
"host_name":"PC-WIN123","domain":"WORKGROUP","mac_address":"00-0C-29-7C-15-AB","ip_address":
"192.168.10.50","time":"2016-04-08T08:10:34-07:00","threat_level":"Moderate","object_type":
"FileSystem","object":"C:\\Users\\jdoe\\Desktop\\test-trojan.exe","threat_name":
"MBAM.Test.Trojan","action":"Quarantine","operation":"QUARANTINE","resolved":true,"logon_user":"j
doe","data":"data","description":"No description","source":"MBAM","payload":null,"payload_url":
null,"payload_process":null,"application_path":null,"application":null}}
```

JSON Log Entry (simplified for understanding)

Please note that liberties have been taken here to improve readability of the log entry.

```
JSON Log Header        : 04-08-2016 08:10:41 User.Alert 127.0.0.1 1 2016-04-08T08:10:41.16-07:00
                         PC-WIN123 Malwarebytes-Endpoint-Security 824 - - ï»¿
Log Data Header        : {"security_log":{
"client_id"            : :"d6961b91-6098-48c4-a64e-ff75c9e5550e",
"host_name"            : :"PC-WIN123",
"domain"               : :"WORKGROUP",
"mac_address"          : :"00-0C-29-7C-15-AB",
"ip_address"           : :"192.168.10.50",
"time"                 : :"2016-04-08T08:10:34-07:00",
"threat_level"         : :"Moderate",
"object_type"          : :"FileSystem",
"object"               : :"C:\\Users\\jdoe\\Desktop\\test-trojan.exe",
"threat_name"          : :"MBAM.Test.Trojan",
"action"               : :"Quarantine",
"operation"            : :"QUARANTINE",
"resolved"             : :true,
"logon_user"           : :"jdoe",
"data"                 : :"data",
"description"          : :"No description",
"source"               : :"MBAM",
"payload"              : :null,
"payload_url"          : :null,
"payload_process"      : :null,
"application_path"     : :null,
"application"          : :null
Log Data Footer        : }}
```

The following information will assist you in understanding construction of a log entry.

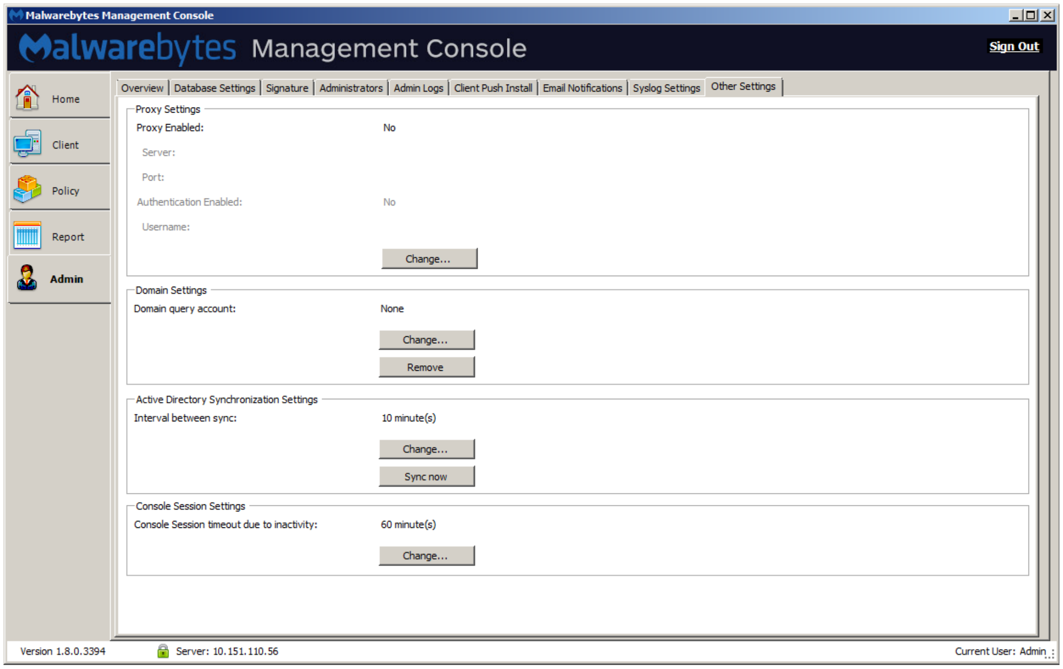
- `threat_level` values are 0 (minor), 1 (moderate) and (2) critical.
- `object_type` values are (0) memory, (1) registry, (2) filesystem and (3) extraobject.
- `action` values are (0) allow, (1) deny and (2) quarantine.
- `resolved` values are (1) true and (0) false.
- Log components "`data`" through "`application`" are reserved for *Malwarebytes Anti-Exploit* managed client events. They are left null for security events generated by the *Malwarebytes Anti-Malware* managed client.

For further information on Syslog in the corporate environment, please refer to internet standard RFC5424, at the following URL:

https://tools.ietf.org/html/rfc5424

Other Settings Tab

This tab provides capability to modify system settings related to Active Directory configuration and proxy settings. Please refer to the screenshot, followed by descriptions of the settings on this tab.



Proxy Settings

Proxy Enabled: No

Server:

Port:

Authentication Enabled: No

Username:

Domain Settings

Domain query account: None

Active Directory Synchronization Settings

Interval between sync: 10 minute(s)

Console Session Settings

Console Session timeout due to inactivity: 60 minute(s)

Version 1.8.0.3394 Server: 10.151.110.56 Current User: Admin

Proxy Settings

If your site security settings are restrictive, direct client connectivity to the Internet may require specification of either a proxy server or modified firewall settings. You can **Change** *Proxy Settings* to specify a proxy server and port number. If the proxy server requires authentication, a username and password may also be specified as part of this choice.

Domain Settings

This option allows the account used to query Active Directory to be changed or removed. If the account is removed, the ability to maintain synchronization between *Malwarebytes Management Console* and Active Directory is eliminated.

Active Directory Synchronization Setting

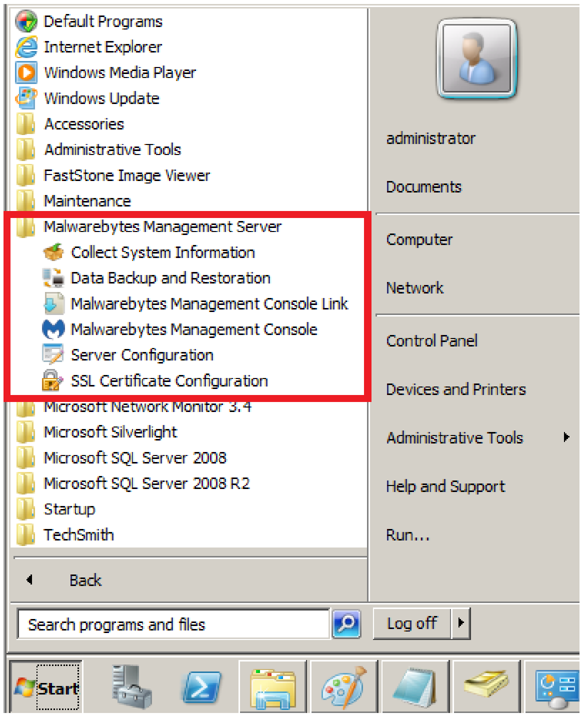
Malwarebytes Management Console attempts to synchronize with Active Directory on regular intervals, to assure that all endpoints controlled by Active Directory are visible to *Malwarebytes Management Console*. The default interval is ten minutes. This option allows adjustment of that interval. There is also a *Sync Now* button, so that outstanding changes may be immediately reflected in *Malwarebytes Management Console* rather than waiting for the next scheduled synchronization.

Console Session Settings

After a period of console inactivity, the user will automatically be logged out. This setting allows the timeout to be adjusted in one-minute increments from 15-480 minutes.

Windows Start Menu Options

A number of additional program options are available from the Windows Start Menu. By launching the menu and clicking All Programs, the Malwarebytes options are available as shown below.



None are considered essential for daily operation of *Malwarebytes Management Console*, though all will prove valuable for configuration, support, and troubleshooting. A description of each option is presented here.

Collect System Information

When troubleshooting a problem with *Malwarebytes Management Console*, you may be directed by Malwarebytes Technical Support to gather logs and send them in for analysis. That is done through this link. When clicked, a small program creates a folder on the desktop of the server which is the home of *Malwarebytes Management Console*. Inside that folder is an archive (ZIP) file which you should send to Malwarebytes Customer Success. The archive contains:

- **ServerSystemInfo.txt –** Basic configuration information regarding your *Malwarebytes Management Console* installation.
- **Console.txt –** Most current log information pertaining to communications between server and user interface (console).
- **Console.*yyyy*^{4}*mm*^{4}*dd*^{4}*nnnnnn*.txt –** Older console logs, with the date contained in the file name. *nnnnnn* is a sequence number; higher values of *n* represent earlier same-day data. A maximum of ten 5120 KB are retained.
- **management-service.txt –** Most current log information pertaining to communications between server and endpoints.
- **management-service.*yyyy-mm-dd.nnnnnn*.txt –** Older server logs, with the date contained in the file name, followed by a 6-digit sequence number. Higher values of *n* represent earlier same-day data. A maximum of ten 5120 KB are retained.

Data Backup and Restoration

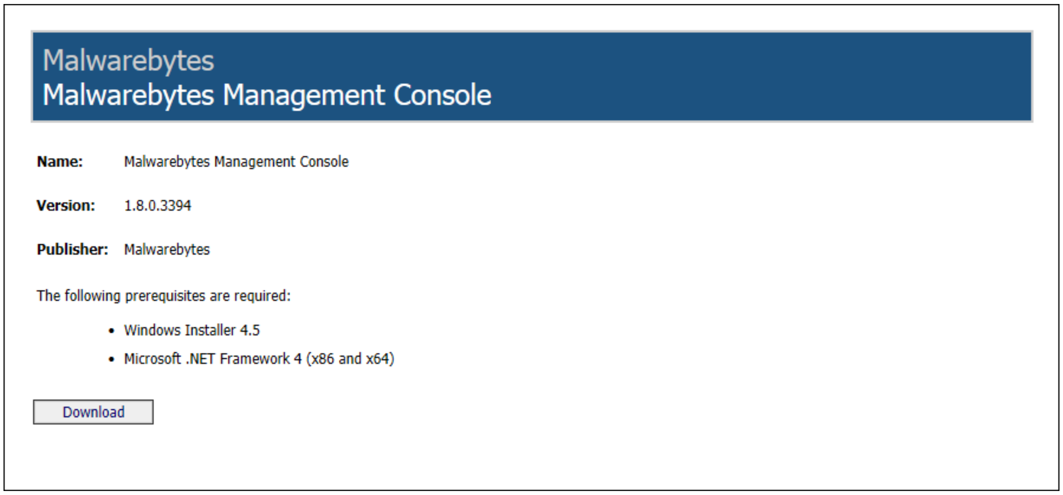
This option allows a security backup of vital *Malwarebytes Management Console* data, as well as program and configuration files used to create endpoint installation packages. Once data has been backed up, it is available to restore system databases should the need arise. When executing this option, you must select a valid folder for either backup or restore operations. The folder must already exist. There is no provision to add a new folder at time of execution.

Please note that this option may not be used if you are using a full Microsoft SQL Server database product. This is only available for *Malwarebytes Management Console* users who have chosen to store system data in a SQL Express database.

Malwarebytes Management Console Link

Many users expressed interest in accessing the program from a remote location. A server is often located in a server room, while the administrator may prefer to manage the system from their desk. For this reason, we provide the capability to download a secondary (auxiliary) console which can be used from any location that has access to the *Malwarebytes Management Console* server.

The screenshot below shows the screen that is displayed in your default browser once the option is selected.



Malwarebytes
Malwarebytes Management Console

Name: Malwarebytes Management Console

Version: 1.8.0.3394

Publisher: Malwarebytes

The following prerequisites are required:

- Windows Installer 4.5
- Microsoft .NET Framework 4 (x86 and x64)

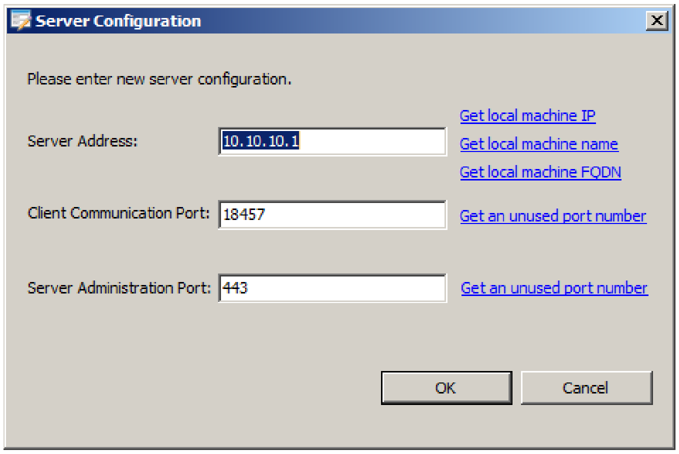
The installer will be downloaded to your standard download location. The filename is **mbmc-console-setup.exe**.

Malwarebytes Management Console

This is an alternate link to access *Malwarebytes Management Console*. It behaves in the same manner as the desktop icon to access the program.

Server Configuration

This option is a wizard to assist you if configuration changes are required. This option launches the dialog box shown here:



Server Configuration

Please enter new server configuration.

Server Address: 10.10.10.1

Client Communication Port: 18457

Server Administration Port: 443

You may enter information into any of the text boxes shown, but it is truly designed to provide that information for you. Clicking any of the first three links (*Get local machine IP/name/FQDN*), will load corresponding settings into the Server Address text box.

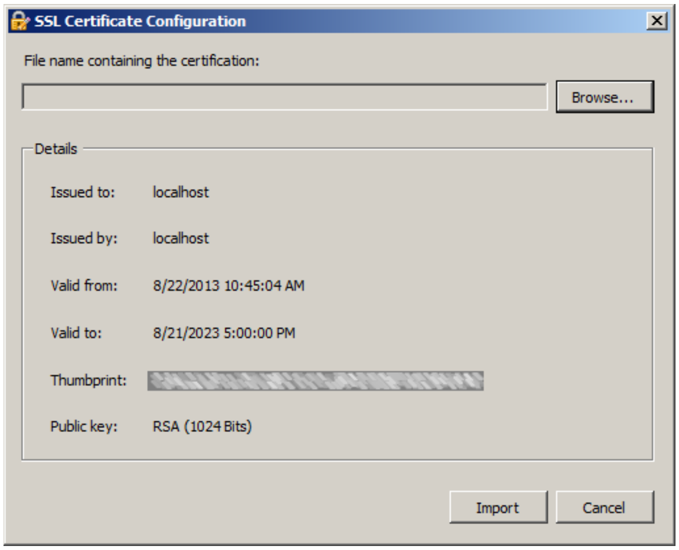
Clicking either port number link will populate the corresponding text box with an unused port number, based on ports currently in use. **Please note** that this wizard cannot evaluate your system for applications which assign ports on demand. In almost all cases, this wizard will provide an acceptable port number, though there is a very slight chance that a conflict may exist.

SSL Certificate Configuration

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.

Verifying Presence of a Certificate

Launching the SSL Certificate Configuration option displays the certificate panel as shown below.



SSL Certificate Configuration

File name containing the certification:

Details

Issued to: localhost

Issued by: localhost

Valid from: 8/22/2013 10:45:04 AM

Valid to: 8/21/2023 5:00:00 PM

Thumbprint: [redacted]

Public key: RSA (1024 Bits)

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

You may find an occasion where your self-signed certificate is not recognized by *Malwarebytes Management Console*. In this situation, you must export the certificate so that it can then be installed. 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) is selected as the default file format. 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 folder where the certificate is to be stored. Click *Next*.
- You will be presented with the certificate specifications. Click *Done* to complete the process.

When complete, your new certificate may be used 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.

Glossary

It is expected that technical documentation will contain technical terms. It is not uncommon that documentation from different sources will attach different meanings to the same word, causing confusion on the reader's part. We have developed this brief glossary so that the definition of terms used in this guide are clear to the reader.

client

A software package which may be installed on an endpoint under direct or indirect control of a centralized software application, and managed by that same centralized application. As it pertains to this guide, *Malwarebytes Management Console* serves as the centralized software application. *Anti-Malware* and *Anti-Exploit* are managed clients under control of *Malwarebytes Management Console*.

device

Initially, this is defined as a networked entity which responds to a network scan by *Malwarebytes Management Console*. Once a scan has been performed and the entity can be categorized, it is an entity which will be ignored because (a) it is not a computer, (b) It does not run on a Microsoft Windows operating system, or (c) It does not run on a supported version of Windows.

endpoint

A computer running on a supported version of the Microsoft Windows operating system which is an installable destination of a Malwarebytes managed client. For an *Anti-Exploit* managed client, this term applies to all computers running a supported version of Windows. For an *Anti-Malware* managed client, this specifically excludes server-class computers.

exploit

Use of a program or method to take advantage of a vulnerability in a legitimate software program. An exploit is typically designed to allow the attacker to gain access to resources, data or control of the computer on which the vulnerability was found. While many may not see a difference between an exploit and a threat, an exploit is focused on illicit manipulation of a vulnerability. Within the context of *Malwarebytes Management Console*, this term is associated with the *Anti-Exploit* managed client.

heuristics

A method of inspecting data which is used in conjunction with, or in lieu of signatures. Many malware samples are represented by known signatures which identify them as threats, and also categorize them as specific types of threats. The same cannot be said for zero-day threats. These are too new for signatures to have been generated, added to signature databases, and subsequently distributed to users of the anti-malware program. Heuristics inspect data for embedded commands, specific characteristics and references to areas of potential vulnerability. In addition, data which has the ability to transform cannot be readily identified by signatures, though their characteristics will allow them to be more easily detected through heuristics.

malware

Software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. 'Malware' is a general term used to refer to a variety of forms of hostile or intrusive software.

Source: Wikipedia (http://en.wikipedia.org/wiki/Malware)

policy

A set of rules which defines behavior for one or more managed clients. These rules define characteristics of real-time protection, anti-malware scans, anti-exploit shields, communications, signature updates, scheduling, and treatment of detected threats/exploits. Multiple policies may be used at the same time, though only one policy may apply to any single client.

signature

After a malware threat has been analyzed, characteristics of the threat can be condensed into data which can represent the threat itself. Signatures can only be created once a threat has been analyzed, and are of no value in prevention of zero-day attacks. Also, a signature cannot reliably be used in to detect a polymorphic virus, as the signature of this type of virus changes to allow it to avoid detection.

SQL Server Express

This is a version of Microsoft SQL Server which provides a majority of the functions of SQL Server, but is limited in terms of maximum usable resources and maximum storage capability. SQL Server Express can only use a single physical CPU on the server, is limited to a maximum of one (1) gigabyte of memory, and can store a maximum of ten (10) gigabytes of data per database. *Malwarebytes Management Console* is shipped with SQL Server Express, and you may choose whether to use this software, or existing SQL Server software. *Malwarebytes Management Console* can utilize only one database, so installations using SQL Server Express are bound by this limitation.

threat

Use of a program to gain access to resources, data or control of a computer which the program should not have access to. A threat may be delivered by an exploit, or it may be delivered by a web site or email. It is typically in the form of a file or registry modification, though it may also exist as a memory-resident code snippet. A threat may target a specific vulnerability, but in most cases takes advantages of user behavior to gain access to the target computer. Within the context of *Malwarebytes Management Console*, this term is associated with the *Anti-Malware* managed client.

vulnerability

A weakness or flaw in a software program which allows programs or methods to take advantage of that weakness or flaw, thus allowing access to system resources or data which were not intended by the developer of the program.