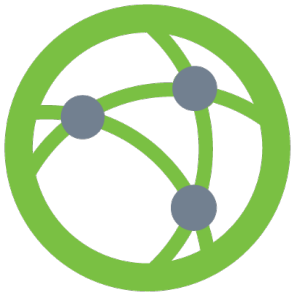


Malwarebytes
ENDPOINT
SECURITY

Endpoint Security
Evaluation Guide

Version 1.9

20 November 2018

Malwarebytes

Laying the Groundwork

Thank you for evaluating *Malwarebytes Endpoint Security* as your endpoint protection product. We have created this Evaluation Guide to help you get started. To keep this guide brief, we make several references to other documentation that provides in-depth technical information, and we encourage you to have those documents available. The following guides are referenced.

- *Management Console Administrator Guide*
- *Endpoint Security Best Practices Guide*
- *Managing Malwarebytes in Large Networks Best Practices Guide*

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

- ***Malwarebytes Anti-Malware*** – Our award-winning anti-malware client is the only client which detects and neutralizes zero-day malware that most anti-virus products cannot even detect. Our real-time protection keeps you safe against zero-day malware through a combination of malware signatures and heuristic analysis.
- ***Malwarebytes Anti-Exploit*** – This innovative technology analyzes, detects and neutralizes vulnerability exploits based on behavior. No signatures are necessary, as *Malwarebytes Anti-Exploit* uses proactive techniques to evaluate *how* threats are introduced to the endpoint rather than focusing on *what* is introduced.
- ***Malwarebytes Anti-Ransomware –*** This Windows-based client guards against ransomware – the newest and most dangerous threat being faced today. This client continuously monitors the endpoint for ransomware behaviors, and blocks ransomware attacks before they can cause damage. This proprietary signature-less technology is capable of detecting unknown and future ransomware variants.
- ***Malwarebytes Management Console*** – This is the control center for *Malwarebytes Endpoint Security*.

PLEASE NOTE: The following unmanaged clients are licensed for use only by businesses who have purchased *Malwarebytes Endpoint Security*. These clients cannot be centrally managed by *Malwarebytes Management Console*.

- ***Malwarebytes Anti-Rootkit –*** This Windows-based client detects and neutralizes malicious software designed to invisibly take control of your computer, and mask its presence from many protection products.
- ***Malwarebytes for Android*** – Our popular Android-based client is available for you to detect and eliminate ransomware, malware, adware, spyware, and PUPs from mobile Android devices.
- ***Malwarebytes for Mac*** – This client offers real-time protection and malware removal similar to *Malwarebytes Anti-Malware* for your Mac endpoints.
- ***Malwarebytes Breach Remediation–*** This client is designed to quickly detect and remove malware and adware from endpoints. Small in size, it can be easily deployed via command line (CLI) mode, or from a GUI for Mac OS X.
- ***Malwarebytes Forensic Timeliner*** – This Windows-Based client is used to retrospectively discover and display indicators of prior malware infection, notably the malware's source and the malware's effects on the endpoint.

Before You Begin

This guide uses a systematic approach to installation and configuration of *Malwarebytes Endpoint Security*. Other documentation is referenced in this guide, and it is recommended that this documentation is available when needed.

System Requirements

Each component of *Malwarebytes Endpoint Security* has system requirements which must be met. Please refer to the ***Management Console Administrator Guide***, *System Requirements* section (pages 3-6) for complete information on hardware and software requirements, as well as specific configuration to facilitate endpoint installation and operation.

Large User Count?

If your company has a large number (in the thousands) of users, you may encounter issues that would not be faced at smaller sites. Please read the ***Managing Malwarebytes in Large Networks Best Practices Guide*** to determine if any guidance provided there is of value to you during your evaluation.

Making the Right Database Choice

Microsoft SQL Express database software is installed as part of *Malwarebytes Management Console* installation, *unless* you elect to utilize an existing Microsoft SQL Server/SQL Express database instance. Malwarebytes does not recommend using SQL Express for more than 200 endpoints. Please refer to page 3 of the ***Endpoint Security Best Practices Guide*** for more information pertaining to database selection criteria.

External Access Requirements

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

https://data.service.malwarebytes.org	Port 443	outbound
https://data-cdn.mbamupdates.com	Port 443	outbound
https://*.mwbsys.com	Port 443	outbound

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

Installing Management Server and Primary Console

Installing the Management Server and Primary Console are simple. For the most part, this task is no different than installation of any other program. A few steps in this process require some extra information. They are shown here.

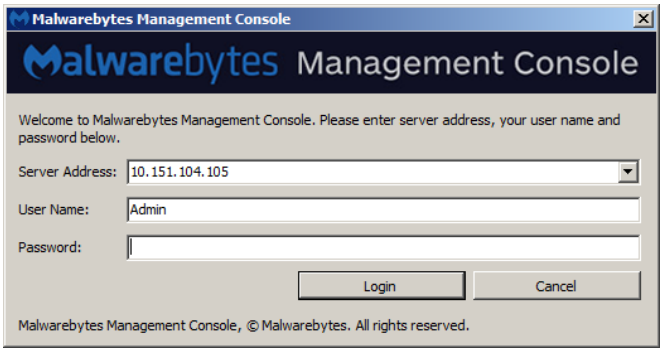
- Click the setup icon on your desktop to start installation of *Malwarebytes Management Console*.
- If not auto-populated for you, enter the Management Server Address (IP or FQDN), Client Communication Port and Server Administration Port. Port addresses may be changed if they conflict with existing port usage.

  HINT: *Using FQDN maintains server-endpoint communication capability should the server's IP address change.*

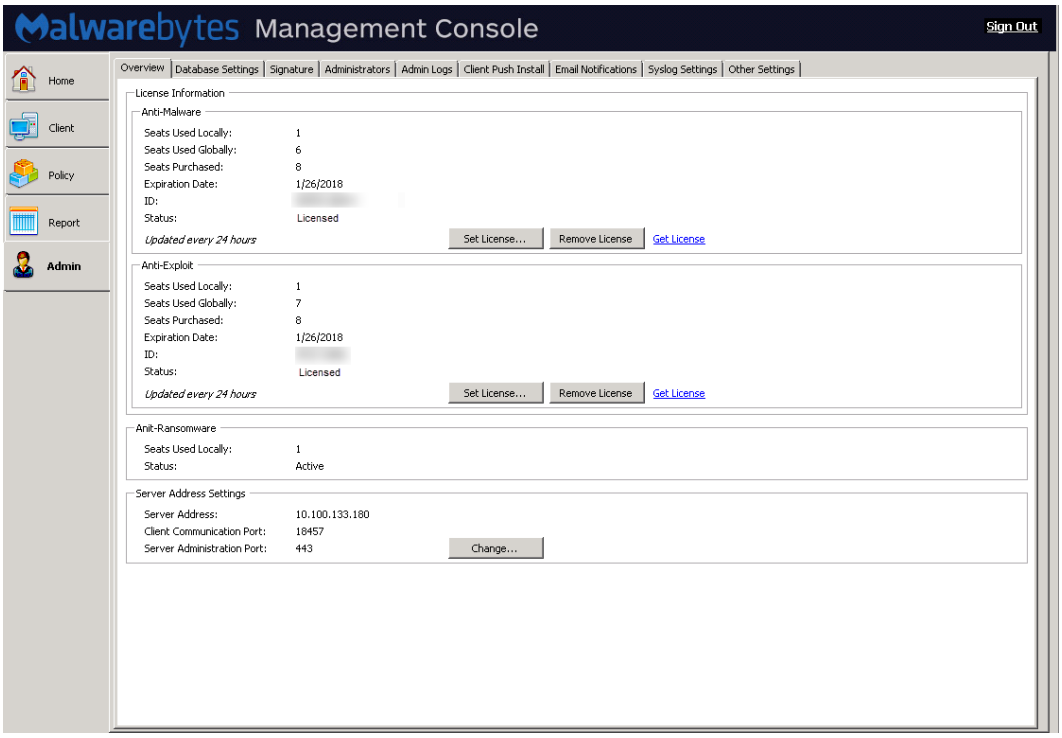
- Choose whether to use the embedded SQL Server Express database or an existing SQL Server database. If you use an existing database, you must specify the server, instance, and SQL Administrator username and password.

Continue through the remaining installation steps to complete the process. If you elected to launch the Management Console, the login window opens (as shown here). The server address is displayed, along with the default **Admin** user name.

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



Following installation and login, you must enter your evaluation license information to begin your evaluation. Click on the Admin panel (the bottom button on the left side). It will appear similar to what is shown below.



License information is shown for both *Malwarebytes Anti-Malware* and *Malwarebytes Anti-Exploit*. Click Set License to enter your evaluation key(s). After these keys have been verified, you will see the Status for each client change from Unlicensed to Evaluation.

Preparations for Your First Endpoint Install

When *Malwarebytes Management Console* is installed on the server, an icon will automatically be created on the desktop. This allows you to launch the program, and takes you directly to the login screen (shown above). In addition, you may access the login screen from the Windows Start Menu, using the **Malwarebytes Management Server ► Malwarebytes Management Console** link.

Defining the Basics

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

The **Domain Query Account** must be defined **if** you are using *Malwarebytes Management Console* in an Active Directory domain. Visibility of endpoints and authorization to perform tasks is based on security policies controlled by Active Directory. *Malwarebytes Management Console* works in conjunction with Active Directory, but cannot override policies governed by Active Directory. Go into the **Admin** panel (left side) and look for the **Domain Query Account** setting on the **Other Settings** tab. Click the **Change…** button and enter the specification that will be used in your environment.

A single **Administrator** account is activated during installation of *Malwarebytes Management Console* (username: **admin**, no password). Upon your first login to *Malwarebytes Management Console*, you are required to change your password. It is strongly recommended that you create additional administrator accounts, and leave **admin** as an emergency administrator account.

You can add new administrators and users under the **Admin ► Administrators** tab. The **Add new administrator…**, option works in a domain or non-domain environment, while the **Import domain user…** option only works in a domain environment. Please refer to the ***Management Console Administrator Guide***, *Administrators Tab* (pages 50-54) for complete information on users and their permissions.

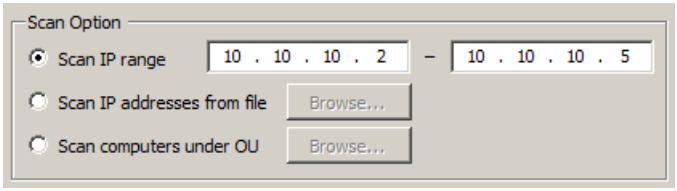
Policies determine behavior of *Malwarebytes Endpoint Security* clients on each endpoint that they are deployed to. Before deploying policies to any endpoint, it is critical that you read and understand the Policy Module chapter of the ***Management Console Administrator Guide*** (pages 23-36). The security of your endpoints depends on it!

Client Groups allow you to divide your endpoints into smaller segments based on the function they perform, or who uses them. Combined with policies, they help to maintain high network throughput when communication between server and clients is taking place. If you are using *Malwarebytes Management Console* in a domain-based environment, you can create groups based on your OU structure in Active Directory. While you can mimic AD's OU structure, you cannot override it. This is discussed in detail in the Client Module chapter of the ***Management Console Administrator Guide***, (pages 17-23).

Discovery of Network Endpoints

One more step is necessary before you can install a client on an endpoint. Discovery of networked endpoints allows you to know where Malwarebytes clients should be installed. This is done from the **Admin ►Client Push Install** tab. There are three different ways in which you can perform network discovery.

- **Scan IP range:** Allows you to discover by IP address. Beginning and ending addresses must have the first two octets in common. Along with computers, it will also return servers, printers, and other networked devices. A screenshot is shown here:



- **Scan IP addresses from file:** Allows you to enter IP addresses (one per line) in a file. This is helpful when including endpoints in IP blocks different from your primary addresses, as is common in VPN or VLAN implementations.
- **Scan computers under OU:** Allows you to get discovery criteria from Active Directory, by selecting an OU.

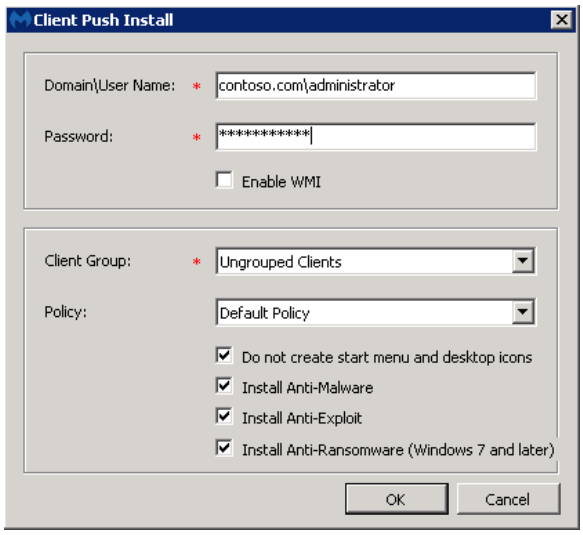
After selecting the range of endpoints to discover, you can these choose how they should be discovered. There are several methods available, and reasons for each to be used. This is documented in detail in the *Management Console Administrator Guide*, *Scanning the Network* section (pages 55-58).

Installing Your First Client

All pre-installation steps are now complete, so it's time to install a client. Please note the context (right-click) menu which appears on the discovery results screenshot on the previous page. The first two items on this menu are processes that we will now perform. This is documented in detail in the ***Management Console Administrator Guide*** *Simulate Client Install* and *Client Push Install* sections (page 59-60).

The ***Simulate Client Install*** option tests the ability of *Malwarebytes Endpoint Security* to communicate with an endpoint prior to client installation. Because this process adds, deletes and executes files on the endpoint, authentication is required on the client. If permissions issues prevent a successful simulation, 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.

The ***Client Push Install*** option allows client software to be installed on an endpoint.



Administrator-level authentication on the endpoint is required. If permissions issues prevent installation, the **Enable WMI** checkbox can be checked. You may install a client as a member of **Ungrouped Clients**, or as a member of a specific **Client Group**. You must select a **Policy** before installation can occur. You may also choose whether the client is visible to the user via entries on the Windows start menu and desktop icon.

That's all there is to it! A lot of work has gone into *Malwarebytes Endpoint Security*, so that the task of providing a secure, malware-free environment takes less work on your part. Thank you for evaluating Malwarebytes!