



INCIDENT
RESPONSE



ENDPOINT
PROTECTION

Malwarebytes Administrator Guide

11 January 2018

Notices

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

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

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

Copyright © 2018 Malwarebytes. All rights reserved.

Third Party Project Usage

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

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

Sample Code in Documentation

Sample code which may be 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, our protection capabilities are most effective 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

Laying the Groundwork.....	1
Introduction	1
What's New in Malwarebytes	1
New Features.....	1
Improvements.....	1
Known Issues.....	1
Before You Begin.....	2
Basic Environment – Console	2
Basic Environment – Endpoints.....	2
External Access Requirements.....	2
Antivirus and Firewall Exclusions	3
Getting Started.....	3
Screen Layout.....	4
My Account.....	4
Adding a New User.....	5
Discovery and Deployment Tool.....	6
Program Modes.....	6
Login.....	6
Discovery.....	6
Who to Discover	6
How We Discover	7
Scan	7
Endpoints.....	8
Preparing for Deployment.....	9
Deployment with Malwarebytes Methods	10
Deployment with Windows Methods (WMI)	10
Tasks.....	10
Special Installation Notes.....	11
Assembling the Pieces.....	12
Understanding Malwarebytes Agents.....	12
Endpoints	12
Add	14
Delete.....	15
Move	15
Actions (On-Demand Scans).....	15
Search	16
Policies	16
General Settings	16
Asset Management.....	16
Groups	16

Table of Contents (continued)

Adding Endpoints to Group.....	17
Exclusions.....	17
What's Next?	17
Malwarebytes Incident Response.....	18
Policies	18
General Settings and Asset Management.....	18
Scan Options	18
Impact of Scans on System	18
Reboot Options.....	19
Schedules.....	19
Scan Type	20
Scan Targets	20
Scan Schedule.....	20
Malwarebytes Endpoint Protection	21
Policies	21
General Settings and Asset Management.....	21
Real-Time Protection.....	21
Real-Time Protection Notifications.....	25
Scan Options.....	26
Protection Updates	26
Startup Options	26
Impact of Scans on System	26
Reboot Options.....	27
Windows Action Center.....	27
Schedules.....	28
Scan Type	28
Scan Targets	29
Scan Schedule.....	29
System Status.....	30
Dashboard	30
Detections.....	31
Quarantine.....	31
Reports	32
Events.....	32
Tasks.....	32
Discovery and Deployment Command Line Reference	33

Laying the Groundwork

The *Malwarebytes* platform is comprised of several components that enhance the security of your network, your endpoints, and your users. The purpose of this guide is to help you use the *Malwarebytes* platform. Please note that this guide is specifically for a Malwarebytes managed solution. Standalone product users should consult administrator guides for those products.

Introduction

The *Malwarebytes* platform consists of the following solutions which provide threat response against modern computing threats:

- ***Malwarebytes console*** – This web-based centralized management tool is responsible for discovery, deployment, management and administration of Malwarebytes agents on your company's endpoints. This console eliminates the need to dedicate web servers and database servers for management of your endpoint data integrity, and provides scalability for organizations of all sizes.
- ***Endpoint Agent***—This intermediary software component is in charge of direct communication between the Malwarebytes console and installed Malwarebytes products, and also in charge of installation of the endpoint product itself. It may also be called on to install third-party products.
- ***Endpoint Protection/Remediation products*** – These products are designed to protect and/or remediate malware and adware from Windows/Mac endpoints. They may be easily deployed by the Malwarebytes platform, Malwarebytes Discovery and Deployment Tool, Active Directory Group Policies, Microsoft SCCM, or a comparable tool of your choice.

What's New in Malwarebytes

This scheduled update to *Malwarebytes* contains many improvements and bug fixes. Following is a list of changes.

New Features

- Added new data fields (Process Name/MD5 hash) in the Detection Details dialog window.
- Added several new on-demand reports.
- Added Websites Blocked tile to console dashboard, showing website/IP blocks during previous 24 hours.

Improvements

- Updates for the *Malwarebytes Endpoint Protection* engine will be automatically metered by Malwarebytes to prevent overloading customer networks
- Updated the title bar of Endpoints detail page to display the selected endpoint's name
- Added deep link to view Scan Reports in the Event Details dialog window for Threat Found and Threat Cleaned event types
- Fixed: Under certain conditions for some customers, the endpoint agent service would fail to start in a timely manner leaving the endpoint agent in a stopped state
- Fixed: The *Malwarebytes Discovery & Deployment Tool* would display an error if the download server couldn't be reached
- Fixed: Tasks now show the correct quantity when filtered by Status
- Fixed: Using browser navigation from many pages required clicking the browser's back button twice to navigate back

Known Issues

- Customers migrating from legacy Malwarebytes products (including *Malwarebytes Anti-Malware*, *Malwarebytes Anti-Exploit*, and *Malwarebytes Endpoint Security*) will require two consecutive reboots to complete installation
- Running Sysprep with the *Malwarebytes Endpoint Protection* agent installed fails. The workaround is to stop the Endpoint Protection agent tray process before launching Sysprep
- Detections that have not been quarantined are not being counted in the Detection History tile on the Dashboard page—however the Number of Detections chart on the Dashboard page **is** counting them correctly

Before You Begin

Prior to installation of any endpoint agents, you should assure that endpoints meet minimum specifications. Network firewalls may also require attention, and requirements are listed here.

Basic Environment – Console

Following are system requirements for your Malwarebytes console.

- **Browser**
 - ◆ Google Chrome

Basic Environment – Endpoints

Following are hardware and operating system requirements for agent installation on endpoints. While most endpoints will exceed these specifications, this information is provided for special-purpose endpoints that still require protection.

- **Hardware (Windows)**
 - ◆ CPU: 1 GHz
 - ◆ RAM: 1 GB (client); 2 GB (server)
 - ◆ Disk space: 100 MB (program + logs)
 - ◆ Active Internet connection
 - **Operating Systems**
 - ◆ Windows Server 2016 †
 - ◆ Windows Server 2012/2012 R2 †
 - ◆ Windows Small Business Server 2011
 - ◆ Windows Server 2008 with SP2 †‡
 - ◆ Windows Server 2008 R2 with SP1 †‡
 - ◆ Windows Server 2003 (32-bit only)
 - ◆ .NET 4.5.2 or 4.6 installed on Windows systems
 - ◆ Windows 10
 - ◆ Windows 8.1
 - ◆ Windows 8
 - ◆ Windows 7
 - ◆ Windows Vista
 - ◆ Windows XP with SP3 (32-bit only)
 - ◆ Mac OS X 10.10 or later (Incident Response only)
- † Excludes Server Core installation option
‡ Microsoft patch KB4019276 must also be installed and enabled

Please note: Anti-Ransomware features are supported only on endpoints using Windows 7 client operating systems and newer.

External Access Requirements

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

https://cloud.malwarebytes.com	Port 443	outbound
https://data.service.malwarebytes.com	Port 443	outbound
https://telemetry.malwarebytes.com	Port 443	outbound
https://data-cdn.mbamupdates.com	Port 443	outbound
https://data-cdn-static.mbamupdates.com	Port 443	outbound
https://keystone.mwbsys.com	Port 443	outbound
https://meps.mwbsys.com	Port 443	outbound
https://keystone-akamai.mwbsys.com	Port 443	outbound
https://socket.cloud.malwarebytes.com	Port 443	outbound
https://sirius.mwbsys.com	Port 443	outbound
https://hubble.mb-cosmos.com	Port 443	outbound
https://blitz.mb-cosmos.com	Port 443	outbound
https://cdn.mwbsys.com	Port 443	outbound
https://ark.mwbsys.com	Port 443	outbound

Antivirus and Firewall Exclusions

Interactions between *Malwarebytes* protection products and other security software are possible. Some antivirus and firewall applications require that you define file and folder exclusions to prevent conflicts with the program, and we recommend that you exclude the following *Malwarebytes* folders and files.

- Windows Endpoints

```
%ProgramFiles%\Malwarebytes Endpoint Agent
%ProgramData%\Malwarebytes Endpoint Agent
%ProgramFiles%\Malwarebytes\Anti-malware\
%ProgramData%\Malwarebytes\MBAMService
%ProgramFiles%\Malwarebytes Endpoint Agent\Plugins\Incident Response\Logs
%SystemRoot%\system32\drivers\ESProtectionDriver.sys
%SystemRoot%\system32\drivers\farflt.sys
%SystemRoot%\system32\drivers\mbae.sys (mbae64.sys on an x64 system)
%SystemRoot%\system32\drivers\mbam.sys
%SystemRoot%\system32\drivers\MBAMChameleon.sys
%SystemRoot%\system32\drivers\MBAMSwissArmy.sys
%SystemRoot%\system32\drivers\mwac.sys
```

- Mac Endpoints

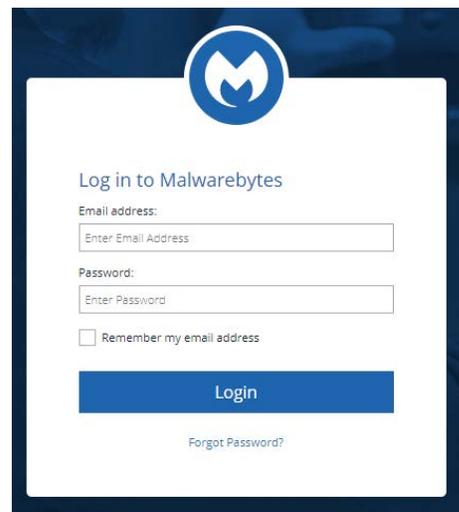
```
/Library/Application Support/Malwarebytes/Malwarebytes Endpoint Agent
/Library/Application Support/Malwarebytes/Malwarebytes Endpoint Agent/UserAgent.app
/Library/LaunchDaemons/com.malwarebytes.EndpointAgent.plist
```

Getting Started

Access to the *Malwarebytes* platform comes to the administrator in the form of an “invitation” email sent by Malwarebytes following purchase. Accepting that invitation created your account, using your email address as the login name. Enter your name, and create a password for your account. Your login name is your email address, and was registered to you when you accepted the invitation sent to you in email.

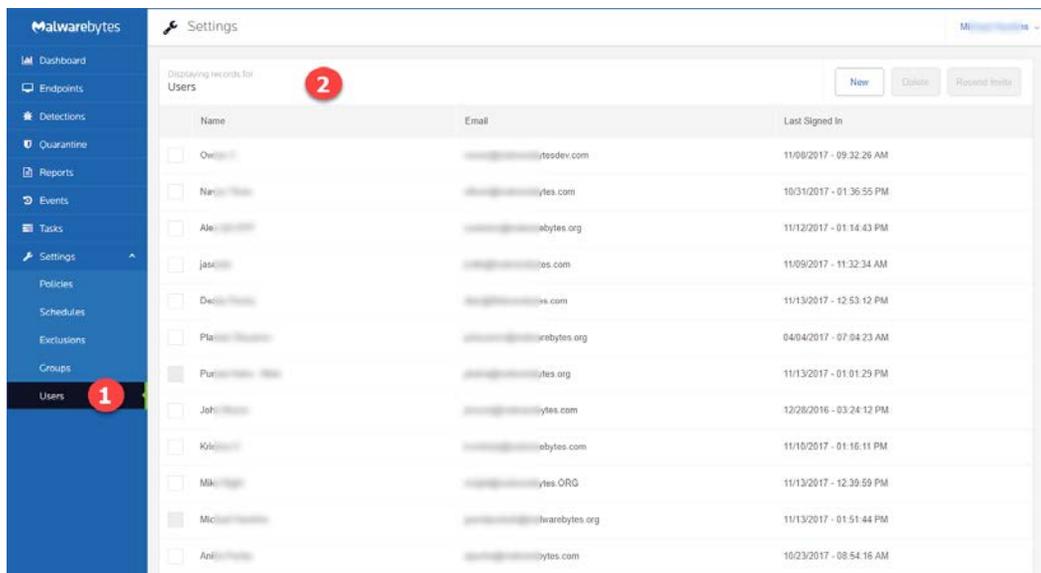
Confirm your password, accept the terms of the End User License Agreement (EULA) and click **Submit** to get started.

You may now login to the *Malwarebytes* platform (<https://cloud.malwarebytes.com>). You may wish to create a bookmark for this URL to simplify access.



Screen Layout

A typical view of the platform screen is shown below. Information shown here is associated partially with the console and partially with the *Incident Response* product. Depending on the product which you purchased. Your view may be different.



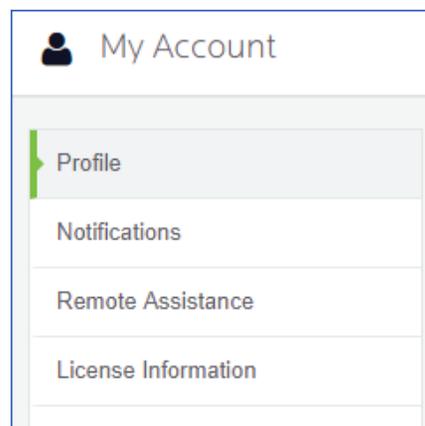
The *Options Menu* **1** is shown at the left side of the screen. Platform options and product options are both accessible on this menu. In this screenshot, *Settings* is selected. Specific settings corresponding to that option are shown indented underneath the Settings label. Selections shown here are all specific to the selected platform option (*Settings*), and may include selections related to both platform and product options. The majority of the screen is assigned to the selected option **2** itself.

My Account

Account settings can be found by use of a pulldown in the upper right corner of the browser screen. When **My Account** is selected, the My Account Options menu will be displayed, as shown here.

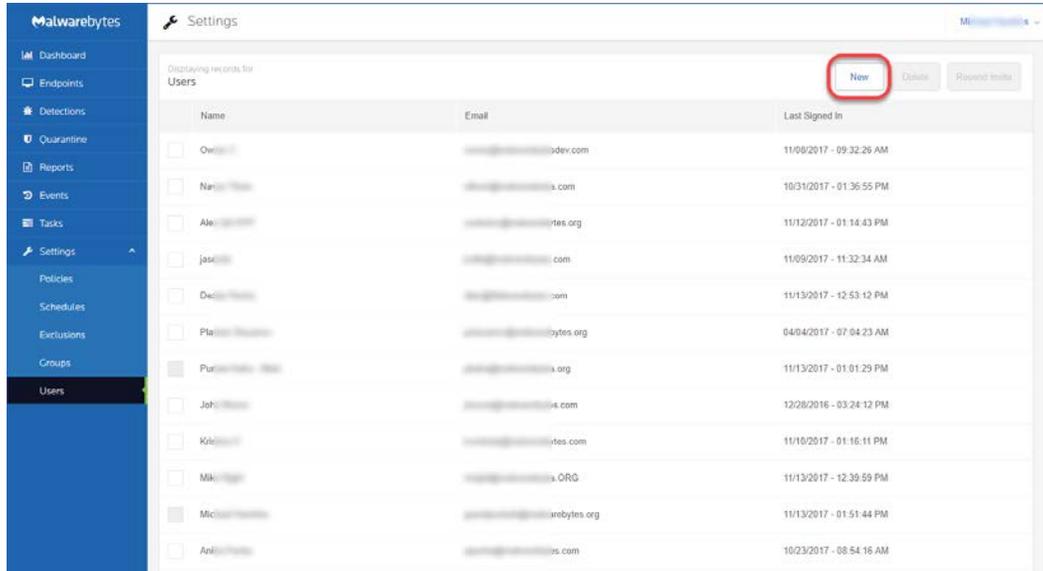
These options cover the following topics:

- **Profile:** Change your display name and password
- **Notifications:** Specify what type of events you wish to receive email notifications for.
- **Remote Assistance:** Enables a setting which allows Malwarebytes Customer Support to access your account (Customer Support will reset this once reason for access is resolved.).
- **License Information:** Provides information about your product license.



Adding a New User

Once the administrator has access to the *Malwarebytes* platform, he may extend invitations to others via email. That invitation is valid only for fourteen (14) days, but may be renewed. The process of accepting the invitation and creating an account are identical.



To add a new user, go to the **Settings** tab and select **Users**. A list of users will be displayed (to the right of the checkboxes which are the right border in this screenshot).

A **New** button (at the upper right of the screen) allows you to enter the email address for the prospective user.

If they do not respond within 14 days, select the user and press **Resend Invite**.

Discovery and Deployment Tool

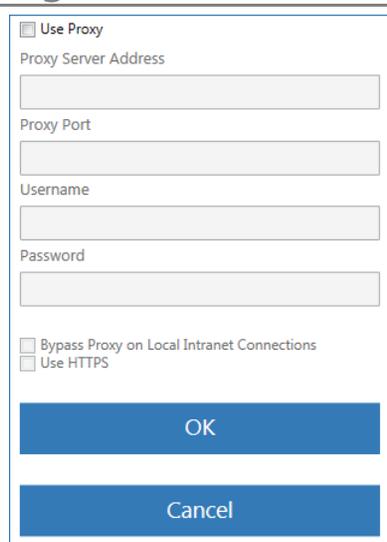
Malwarebytes has developed a utility program to assist you with the task of adding endpoints. The **Discovery and Deployment Tool** scans your network based on criteria which you specify, and identifies networked devices which may be suitable for agent deployment. It also identifies endpoints where Malwarebytes agents have already been installed. A wide range of criteria may be used to identify endpoints, and an equally wide range of analysis methods provide an accurate snapshot of information relevant to deployment. Once target endpoints have been identified, you may select them and begin the agent deployment process. The tool will access Malwarebytes servers to obtain the newest MSI installer package and then perform the deployment. Let's go inside!

Program Modes

The *Discovery and Deployment Tool* can perform its tasks in both GUI mode and command line mode. Please refer to the end of this guide for command line operation.

► **PLEASE NOTE:** This program must be executed from a local drive. Attempting to run it from a network drive will fail. ◀

Login



A login is required to gain access to the *Malwarebytes* platform. This is unique to your company and your identity. The default URL to access the *Malwarebytes* platform is <https://cloud.malwarebytes.com>. Your URL may differ (if you have been informed otherwise). Enter the URL, your email address and your password.

A **Proxy Settings** button is at the lower right corner of the login screen, needed when you require use of a proxy server to access the Internet. Click **Proxy Settings** to enter proxy specifications. No settings are enabled until Use Proxy is checked, and settings are ignored if Use Proxy is unchecked.

PLEASE NOTE: Proxy specifications used here will be propagated to endpoints deployed by this tool.

Discovery

Before an agent can be deployed to an endpoint, target endpoints must be identified.

Who to Discover

We provide three methods to discover endpoints and validate our results. Only one method is required.

- **Method 1** – Query Active Directory for a list of machines in your domain.
- **Method 2** – A Network Scan allows you to provide search criteria for endpoints in your network. You can specify several different criteria, and all will be tested. Criteria includes:
 - IPv4 address
 - IPv4 address range, with minimum and maximum values specified (e.g. 10.10.10.34-10.10.10.106)
 - IPv4 address block, in CIDR format (e.g. 10.10.1.1/16)
 - IPv4 address block, with mask (e.g. 10.1.1.1/255.255.255.0)
 - Hostname
 - FQDN
 - IPv6 address
- **Method 3** – A text file containing a list of endpoints (one entry per line), using criteria as listed for method 2.

How We Discover

For each endpoint we have identified as part of our target group, we determine if they are available for agent installation. Please note that the majority of the tests listed here require ports to be accessible through the firewall. Here's how we do it.

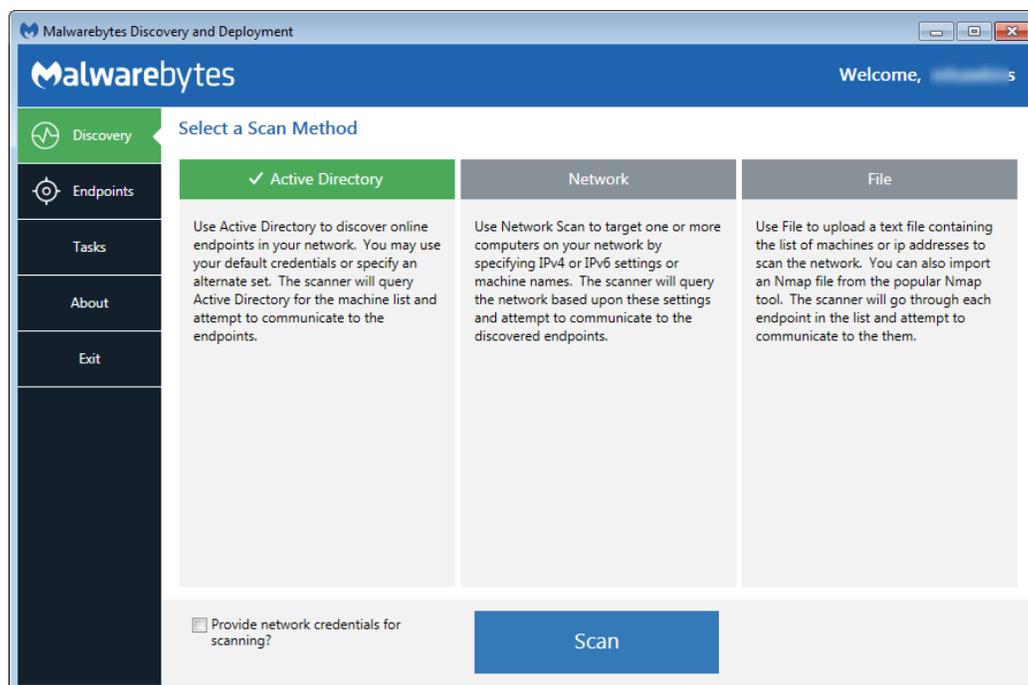
- **Ping** – This is a simple ICMP command which requests the target endpoint to respond. Endpoint configuration or network topology may block pings, so alternative means would be needed to reach those endpoints.
- **DNS** – The IP address or hostname specified in discovery criteria will be searched in the A record of the DNS server used by the host. The Time to Live (TTL) indicates an endpoint which is online or has been online recently.
- **UDP Datagram** – The program uses UDP to send a small datagram to the endpoint, and receive a response.
- **TCP/IP Probe** – Using the endpoint's IP address, attempts to communicate with several ports associated with critical services (NETBIOS, HTTP, SSH, Telnet, DNS, etc.). While some ports may not respond, it is likely that a machine which is online will respond to some degree. A response to any attempt is considered a success.
- **Nmap** – A powerful multi-purpose open source tool used for network discovery and security auditing. Much information about an endpoint can be found using this tool.

The following tests determine if an agent has been deployed to the endpoint, from the perspective of the endpoint as well as the *Malwarebytes* server.

- **Remote Registry Detector** – Determines whether this service is available to perform agent installation.
- **WMI Detector** – Determines whether Windows Management Instrumentation (WMI) is accessible for agent installation.
- **Service Controller Detector** – This allows the program to get a list of services running on the endpoint.
- **Agent Status Check** – Using endpoint identity information, the program will query the *Malwarebytes* server with that identity information, looking for evidence of a previous agent deployment

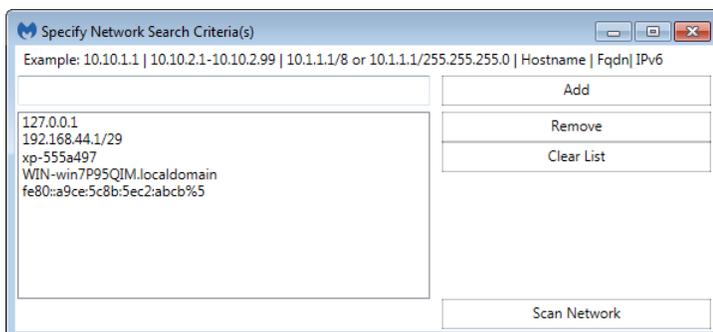
Scan

After specifications have been provided by the user, the *Discovery and Deployment Tool* will go through the list of endpoints which fit criteria, and using the discovery techniques listed above, determine which endpoints are online and which have an endpoint agent already installed. All that is required of the user is a simple press of the **Scan** button. If network credentials are required to scan the network, you may enter them here. The Scan screen looks like this:



Endpoints

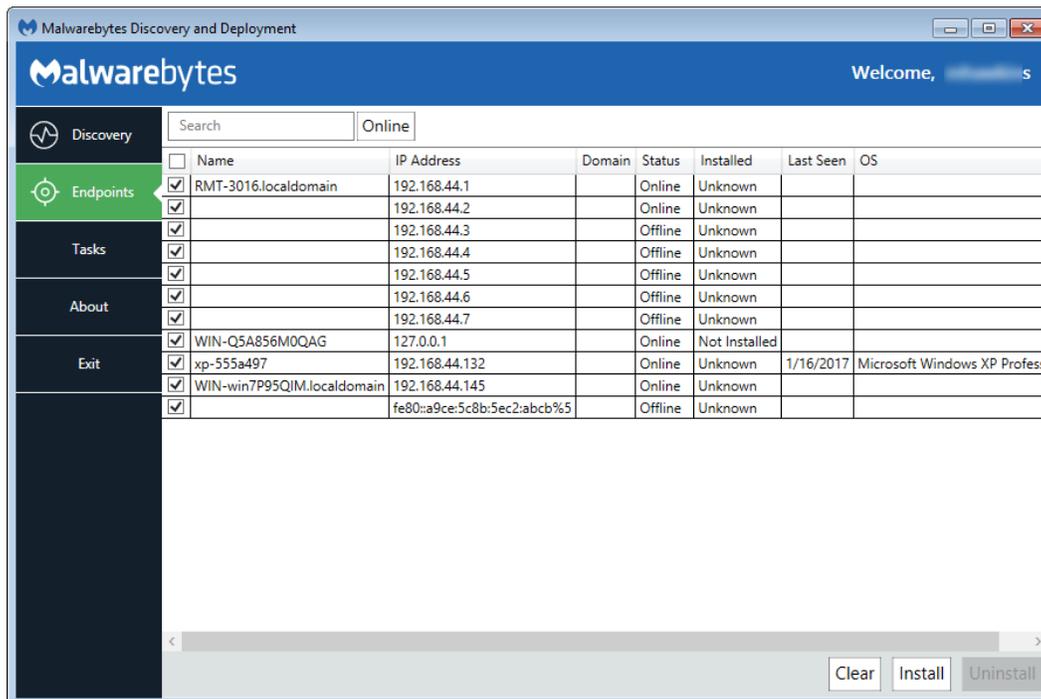
Once a scan has been initiated, this screen will show the results of that scan. Let's use a [Network Scan](#) as an example to demonstrate the process.



Here, five endpoint criteria were listed for the desired scan. You may add to this list in the box at the upper left, then clicking the **Add** button. Highlight an entry in the large box and click **Remove** to delete it, and press **Clear List** to remove all criteria.

When satisfied, press **Scan Network** to begin the scan.

As the discovery scan executes, the main program screen will show each endpoint specified and/or within the IP address range specified by the user. Please refer to the following screenshot.

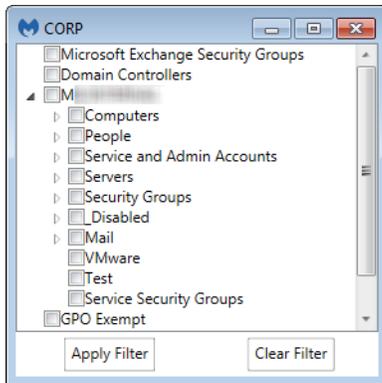


You may click on any field to sort on that field. Click again to reverse the order.

The [Search](#) box allows you to search for any endpoint (or group of endpoints) that match criteria which you specify. Please note that the search string will look for matches in both the [Name](#) and [IP Address](#) fields.

The pulldown next to the Search box allows filtering of discovery results, so that only endpoints which match the specified discovery status will be displayed. Allowable status includes *All*, *Online*, *Offline*, *Probing*, and *Queued for Probing*. Please note that while scanning is extremely fast, probing takes much more time. Probing is responsible for detection of endpoint status, agent installation status and operating system. The tool will probe as many endpoints as possible based on the resources required, and upon completion, will probe the next endpoint in the queue.

A second filter which can be applied in a domain environment is the [AD Filter](#). Clicking the [AD Filter](#) buttons superimposes the filter window (shown below) over the program interface.



This tree is a hierarchical view of your Active Directory layout, broken down by Organizational Unit (OU). A typical OU structure is shown here. We do not presume how your OU structure is defined, therefore all OU's are shown here.

If you filter based on the Computers OU, any child OU's are also selected by default. You can drill down and deselect any entries which are not to be included in the filter specifications.

Once you have completed OU selection, click **Apply Filter** to effect a change on your Endpoints screen. The AD Filter button on the Endpoints screen will turn black while a filter is used.

The Results filter and the AD Filter can be used at the same time.

Status is the status of each endpoint. **Installed** indicates whether a Malwarebytes agent has been installed. If **Status** is *online* and **Installed** is *unknown*, that may indicate an endpoint which can be reached but software detection cannot be performed. It is also possible that missing or incorrect credentials were specified by the user. Ports 135, 137, and 445 are required for software probing.

Finally, the Refresh button restarts the discovery process. There are no results saved from the previous discovery process. The Cancel button terminates the discovery process. In a large network environment, this may take a few moments.

Let's briefly shift gears and discuss an **Active Directory Scan**. Everything that has been said so far also applies to an AD scan, though there are a few differences. The program will query Active Directory for a list of endpoints in the domain, then display results of that query. The endpoint **Name** will show the full FQDN for the machine, and **Domain** will be populated by the Active Directory domain name. By clicking the **AD Filters** button, you can specify which Organizational Units (OUs) to focus on.

Please note: This method cannot discover Mac endpoints if they are not registered and/or managed by Active Directory. A secondary method may be required.

Preparing for Deployment

Now that we can see the state of our endpoints, we can use *remote deployment* to install agents on these endpoints. Select all (or specific) machines and click the **Install** button to begin deployment.

Please note: Domain administrators can override User Account Control (UAC) settings on domain endpoints. If an endpoint is a member of a **workgroup**, additional steps are required. Please read the following article for further information:

<https://support.microsoft.com/en-us/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows-vista>

Here are a few tips which will give you the best results.

- Administrator credentials are required to perform remote deployment. A domain account will suffice if the target endpoint is part of the domain and the domain account used is part of the local administrators group. Credentials should be in the form <IP>\username or <hostname>\username.
- Files will be copied to the Admin share on the destination Windows endpoint(s).
- Access on port 137 must be enabled on the destination Windows endpoint(s).
- Remote access should be enabled on the destination Mac endpoint(s).
- The installer will not attempt to overwrite a previously existing program version on the endpoint. You are permitted to uninstall the program on that endpoint.
- Endpoints whose **Status** is *Offline* or whose **Installed** state is *Unknown* may still be able to have software deployed via a push install. Status will be reported whether deployment is successful or not.

Finally, the *Discovery and Deployment Tool* must connect with Malwarebytes infrastructure servers to download the most current MSI install package and the account token which will be used as a unique identifier when software package updates are available.

The next two sections describe technical information related to deployment, but user interactions are limited to selecting the machine and clicking the **Install** button. This is simply to let you know what we're doing and how we're doing it!

Deployment with Malwarebytes Methods

We use a Windows construct called *Named Pipes* to communicate with Windows endpoints. Local admin credentials are used, and ports 137 and 445 need to be accessible. Three files (**EAInstall.bat**, **EAUninstall.bat** and **MBExec.exe**) are transferred to the endpoint to either **ADMIN\$** or **IPC\$**, based on availability. One of the two must be available for this method to succeed.

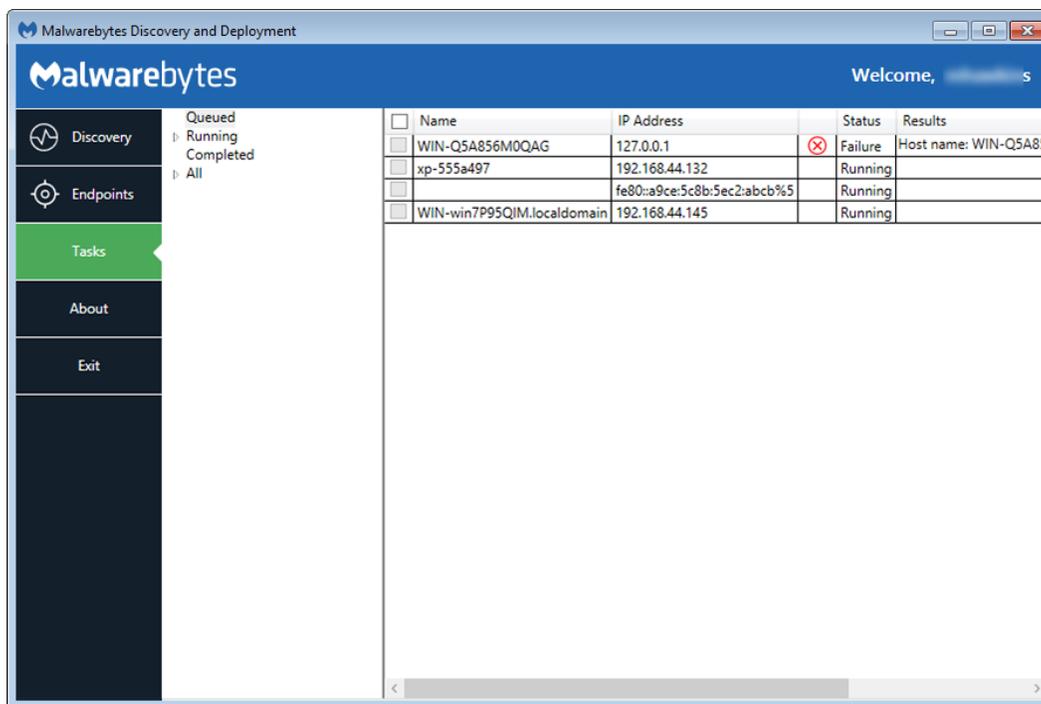
Deployment with Windows Methods (WMI)

Windows Management Instrumentation (WMI) is another method we use. It is typically used when our primary method is unsuccessful. WMI Deployment uses the **ADMIN\$** share. This share is used as a temporary home for files that we retrieve for updating and installing on the endpoint. You may need to enable Remote Management of the endpoint to successfully access the **ADMIN\$** share. Endpoint port 135 must be available through the firewall. Local admin credentials are required.

Please note: You should not use the *Discovery and Deployment Tool* to deploy agents to endpoints outside of your local network. This includes endpoints which connect to the network using a VPN connection. Ports opened for the deployment process would remain open after deployment is complete, creating a security risk on that endpoint.

Tasks

Once we have selected endpoints to install a Malwarebytes agent on, we can use the **Tasks** tab to look at status and progress of the agent deployment. A screenshot is shown here to illustrate this tab in use.



This tab is divided into two sections. The left section is a quick status of install/uninstall activity that has occurred or is currently in process. The view shown here indicates there are results in the *Running* and *All* categories, but neither are expanded to show results. You will also notice no indicator next to *Completed*. It looks like an error but it's not. Once remaining scans complete, status will be updated appropriately.

Queued
Running
11:01 AM-Install-255 0%
Completed
11:00 AM-Install-4 100%
11:01 AM-Install-4 100%
All
11:00 AM-Install-4 100%
11:01 AM-Install-4 100%
11:01 AM-Install-255 0%

Looking at this *Status* example, you can see that an install began at 11:00am and met with mixed results (exclamation mark denotes at least one failure). Another 4-point endpoint install began at 11:01am. The red X inside the circle indicates that all four installations failed.

Finally, a third installation began at 11:01am. This installation was for 255 machines, and completion status is shown at 0%. Completion status would increment to 100% with final status showing a green checkmark (complete success), exclamation mark (one or more failures), or red X inside a circle (complete failure).

The screenshot below shows installation results for these same four endpoints. *Status* is shown with both words and symbols, and *Results* shows relevant information as well as a link to view logs. Only an excerpt of the screen is shown here because the screen required expansion to show *Results* detail, and that action would have caused display of the full screen to become illegible here.

<input type="checkbox"/>	Name	IP Address	Status	Results
<input type="checkbox"/>	WIN-Q5A856M0QAG	127.0.0.1	Failure	Host name: WIN-Q5A856M0QAG; IP Address(es): IP Add... View log
<input type="checkbox"/>	xp-555a497	192.168.44.132	Success	Starting install for Host name: xp-555a497; IP Add... View log
<input type="checkbox"/>		fe80::a9ce:5c8b:5ec2:abcb%5	Failure	System.IO.IOException: The network path was not fo... View log
<input type="checkbox"/>	WIN-win7P95QIM.localdomain	192.168.44.145	Success	Starting install for Host name: WIN-win7P95QIM.loc... View log

Please note that when several endpoints are selected for installation, you may also see *Status* shown as Queued. Resources are required for each installation, and when requirements exceed availability, installation will be Queued until resources are available.

Special Installation Notes

There are a few special installation conditions which may cause issues. By mentioning them here, we hope to provide a smoother experience for all.

- Installation of standalone *Malwarebytes Anti-Malware* (v1.80) application is not prevented by the Malwarebytes agent. This would result in a defective installation. Please be careful!
- If you currently use the standalone *Malwarebytes Anti-Malware* (v1.75) application and wish to install a managed *Malwarebytes* agent, please uninstall the standalone application first.
- If you are a subscriber to *Malwarebytes Endpoint Protection* and have a Malwarebytes consumer version installed as well (*Malwarebytes Anti-Malware 2.x* or *Malwarebytes 3.x*), they will be uninstalled when *Malwarebytes Endpoint Protection* is enabled. Subscribers of Malwarebytes Incident Response are not affected.
- Installation of the *Malwarebytes* v3.x standalone consumer version over an existing managed Malwarebytes application will have negative performance results. Should you desire to use the standalone consumer app, you should delete and uninstall the managed endpoint application.
- Malwarebytes agents will fail to initialize properly if *Malwarebytes Anti-Malware* consumer version 2.x is installed on the endpoint. If this is the case, please assure that the consumer product has been removed first.

Assembling the Pieces

So far, we have created users and added endpoints. We may wish to add more endpoints at a later time. We also need to configure the environment so that a stable protection platform is in place. Let's begin!

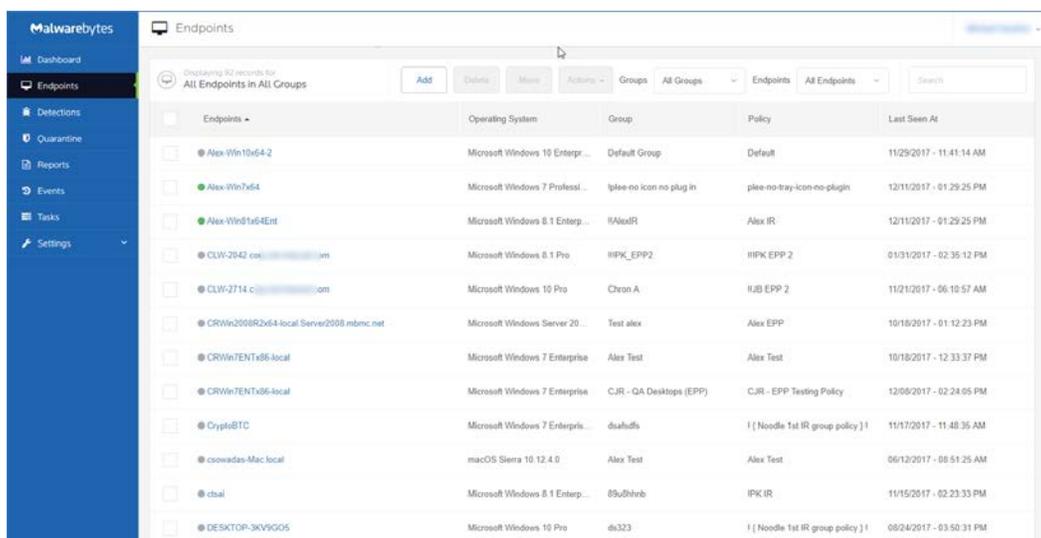
Understanding Malwarebytes Agents

Malwarebytes protection is delivered to you as an installable agent. Each agent serves a different purpose, and must be configured to provide proper functionality. Available agents include:

- **Incident Response** provides scheduled scanning of your endpoint based on specifications which you provide, as well as on-demand scanning of areas where a majority of malware is hidden. If a threat is detected, it is quarantined for later remediation. Asset management is also included in this product.
- **Endpoint Protection** provides all of the functionality that Incident Response offers, along with real-time protection against several types of threats (malware, exploits, ransomware, and malicious web controls). *Endpoint Protection* is an effective anti-virus replacement, and you may also choose whether it appears in Windows Action Center (Vista and later).

Endpoints

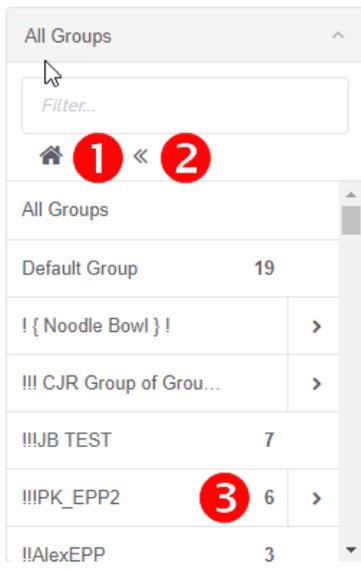
In the *Discovery and Deployment Tool* section of this guide (Chapter 2), we demonstrated how to add endpoints en masse. All endpoints added were assigned to the Default Group and associated with the Default Policy. You can also add individual endpoints at any time. On the [Platform Menu](#), click Endpoints. A display will appear that is similar to the screenshot shown here.



Endpoints	Operating System	Group	Policy	Last Seen At
Alex-Win10e4-2	Microsoft Windows 10 Enterpr...	Default Group	Default	11/29/2017 - 11:41:14 AM
Alex-Win7x64	Microsoft Windows 7 Profess...	Idle-no icon no plug in	Idle-no-tray-icon-no-plug-in	12/11/2017 - 01:29:25 PM
Alex-Win5ta54Ent	Microsoft Windows 8.1 Enterp...	IAlexIR	Alex IR	12/11/2017 - 01:29:25 PM
CLW-2042-coe...	Microsoft Windows 8.1 Pro	IRPK_EPP2	IRPK EPP 2	01/31/2017 - 02:35:12 PM
CLW-2714-c...	Microsoft Windows 10 Pro	Chron A	IRB EPP 2	11/21/2017 - 06:10:57 AM
CRWn2008R2x64-local-Server2008-mbmc.net	Microsoft Windows Server 20...	Test alex	Alex EPP	10/18/2017 - 01:12:23 PM
CRWn7ENTx65-local	Microsoft Windows 7 Enterprise	Alex Test	Alex Test	10/18/2017 - 12:33:37 PM
CRWn7ENTx65-local	Microsoft Windows 7 Enterprise	CJR - QA Desktops (EPP)	CJR - EPP Testing Policy	12/08/2017 - 02:24:05 PM
CryptaBTC	Microsoft Windows 7 Enterprise	duahds	[(Noodle 1st IR group policy)]	11/17/2017 - 11:48:35 AM
csovadas-Mac-local	macOS Sierra 10.12.4.0	Alex Test	Alex Test	06/12/2017 - 08:51:25 AM
ctbal	Microsoft Windows 8.1 Enterp...	89u8hhnb	IRPK IR	11/15/2017 - 02:23:33 PM
DESKTOP-3KV9G05	Microsoft Windows 10 Pro	ds323	[(Noodle 1st IR group policy)]	08/24/2017 - 03:50:31 PM

In this screenshot, several groups have been added. You may show all endpoints, those that are online only, offline only, or offline for more than seven (7) days. Endpoints which have been offline for 180 days or more will not be displayed in the console. If an affected endpoint returns to online status, it will again be shown on the display. You may show endpoints in all groups, or in a specified group.

Please refer to the following screenshot for information on how the Groups pulldown menu operates.



An excerpt of the All Groups pulldown is shown here. The Default Group and 5 other groups are visible. Three of these five groups are nested groups, shown by the right arrow. Group !!!PK_EPP2 – shown by 3 – is an example. Click on the arrow to view subgroups. At any point, child groups may be subdivided even further.

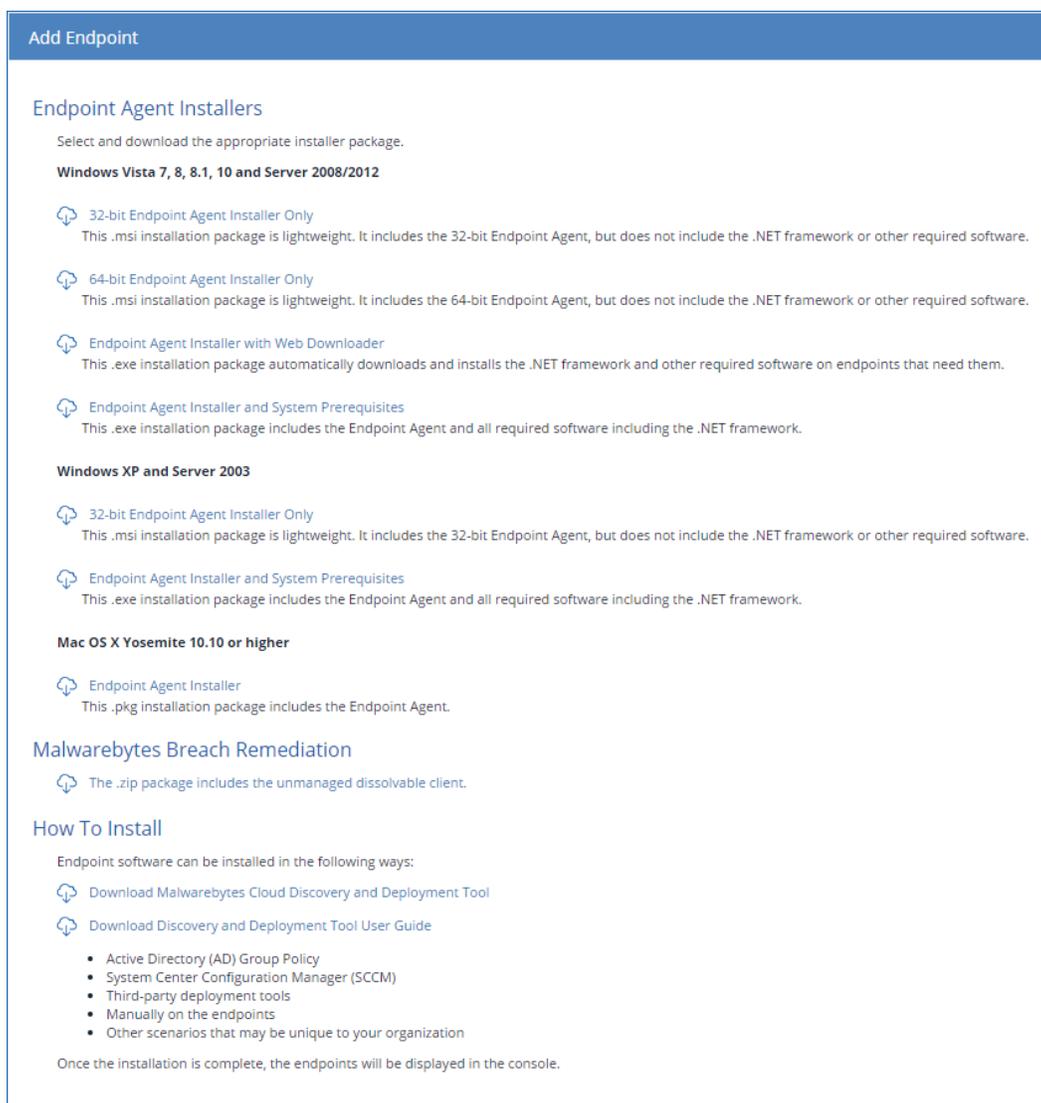
The Home button – shown by 1 – returns visibility to the All Groups level, regardless of your depth in the group tree.

The Back button – shown by 2 – returns visibility one level from your current position in the group tree.

The selector bar (above the list of endpoints) shows the five options available to the user. Beginning on the following page, they are:

Add

When this option is selected, a new screen opens with several options. Here, you may choose the most appropriate agent installer for your needs, the standalone *Breach Remediation* product, or the *Discovery and Deployment Tool*. By providing installers in this manner, we enable you to use the installation method which you prefer in your organization. Please note that any endpoints added in this manner are assigned to the Default Group and associated with the Default Policy. A screenshot of the Add Endpoint screen is shown here.



If you elect to silently install the *Malwarebytes* agent on a Windows endpoint, that can be performed using one of the following commands shown below. **Please note** that the MSI command is shown on multiple lines due to the length of the command.

```
EXE: Setup.Full.MBEndpointAgent.exe /quiet
MSI: msiexec /quiet /i Setup.MBEndpointAgent.msi
      NEBULA_PROXY_SERVER=http://<IP>
      NEBULA_PROXY_PORT=<port>
```

Four variables may be used in conjunction with this command. All are self-explanatory. They are:

```
NEBULA_PROXY_SERVER
NEBULA_PROXY_PORT
NEBULA_PROXY_USER
NEBULA_PROXY_PWD
```

If the proxy username or password contains embedded spaces, the username/password should be enclosed in double quotes.

You will notice a reference in this screenshot to *Malwarebytes Breach Remediation*, our highly-effective remediation program for Windows and Mac endpoints. There may be instances when its usage is more appropriate for your needs. You can also download this application here. Documentation is included in the ZIP file.

- System Administrators typically build machine images to use for rapid deployment. The SysAdmin may wish to load the Malwarebytes agent to the image. Because each Malwarebytes endpoint has a unique identity, this method can result in multiple endpoints sharing the same identity. Microsoft offers a system utility named Sysprep that can strip off the identity of the Malwarebytes agent so that it will become uniquely identified once the deployed image is put into service on a new endpoint. Sysprep is built into all modern Windows operating systems. Full instructions for Sysprep usage can be found on Microsoft's Technet blog, at:

<https://goo.gl/SwUQKs>

Please note: This shortened URL was used because Microsoft's Technet URL is extremely long.

Delete

This option removes endpoints from console control, and uninstalls Malwarebytes software from the endpoint itself. This includes applications (*Incident Response* and *Endpoint Protection*) as well as the agent which controls communications between the console and applications. To delete one or more endpoints, select those endpoints and click **Delete**. All deletions in a single group should be performed at the same time before acting on a different group, unless you are performing deletions from the **All Groups** list. Finally, groups whose entire endpoint population have been removed from console management will remain intact.

Please note: When deleting endpoints which are offline, they will be removed from console control immediately, but uninstallation of agents cannot occur until the endpoint returns to online status. If the endpoint comes back online within 90 days of the delete request, uninstallation will occur at that time. If the endpoint comes back online more than 90 days after the delete request was issued, the endpoint will again be shown as an active device in the console.

Move

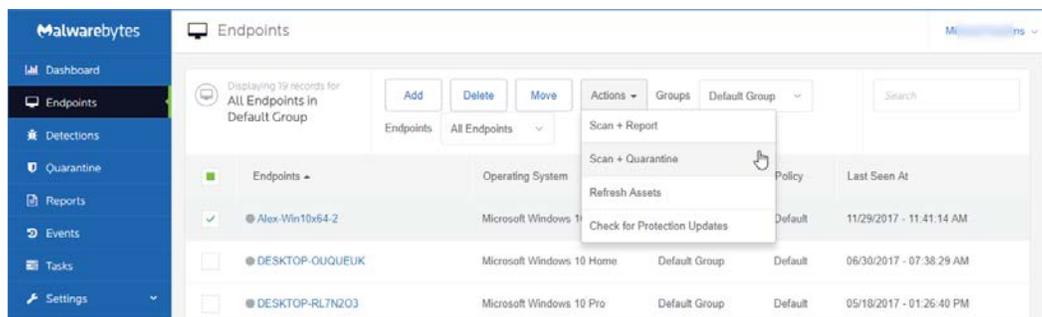
By selecting one or more endpoints, you can move them from one group to another. The value of this will become apparent after we discuss the relationship between endpoints, policies and groups.

Actions (On-Demand Scans)

Incident Response and *Endpoint Protection* both share a few endpoint-oriented actions. After selecting one or more endpoints, you may run one of the following on-demand scans:

- **Scan + Report** – Check for protection updates, run a threat scan and report the results. This scan method does not remove any threats which were detected during the scan.
- **Scan + Quarantine** – Check for protection updates, run a threat scan, quarantine any threats which were detected, and report scan results.
- **Refresh Assets** – Update hardware/software assets for the endpoint. Unless the administrator has created scheduled scans for this purpose, this may be the only method by which assets are checked.
- **Check for Protection Updates** – Perform an immediate check for protection updates. While scans also perform this task, this assures that real-time protection uses the most recent updates.

To show how this works, an excerpt from the *Endpoints* screen is shown below. One endpoint has been selected. This enabled the buttons in the gray bar (Delete, Move, Actions). From the **Actions** submenu, we have chosen to use the **Scan + Quarantine** option.



This results in execution of a scan on the selected endpoint. The amount of time required is dependent on the number of files to be scanned on the endpoint. If default policies are used, a Threat Scan will be executed. If malware is detected, it will be quarantined automatically, and a reboot may be required to assure no malware residue remains. There are several policy-related variables which may change this behavior, and they will be discussed later in this guide.

Search

It may be easier for you to search for a computer than to scroll through a list. Start typing the hostname of the endpoint, and the list of endpoints will be continually updated until you locate the endpoint you were searching for.

Policies

A policy defines the behavior a Malwarebytes product uses when running a scheduled scan. Each policy is used by a specific product, *Incident Response* or *Endpoint Protection*. It cannot serve both. A policy can be paired with multiple groups, providing flexibility for the administrator, although it is important to note that the policy can only have only one set of specifications.

Initially there is a single policy, called the Default Policy. It may not be deleted. If any other policy is not associated with a group, it may be deleted, or it may be renamed by selecting it and overwriting its existing Policy Name. Scheduled scans and Real-Time Protection both draw heavily on policy specifications, so policies will be discussed in detail in product sections (later in this guide). You may create several policies which are similar in nature. It is your best interest to use an easily discernable naming convention.

You can find this in **Settings ► Policies**.

Two groups of settings are not specific to either *Incident Response* or *Endpoint Protection*, and are itemized here:

General Settings

This screen is very limited in scope. It allows you to change the name of the policy being reviewed and allows modification of program-wide Endpoint Interface Options.

- **Show Malwarebytes icon in notification area** – Allows the endpoint user to see a Malwarebytes icon in the taskbar. Some administrators opt for visibility, while others do not. It's your choice. Hovering over the icon also displays a very brief program status message.
- **Allow users to run a Threat Scan** – Allow endpoint users to run threat scans. No other scan types are available to the end user, and all threats detected during the scan will be quarantined automatically. Endpoint users may cancel scans which they have initiated, but have no control over scheduled scans or on-demand scans initiated by the administrator. User-initiated scans will appear as "On demand" scans on the Console Events screen.
- **Display real-time protection notifications** – Shows real-time notifications in the corner of your screen. These are only available to users of *Endpoint Protection*.

Asset Management

You may also execute an asset management scan. This evaluates basic environmental settings of the endpoint being scanned, and reports changes which have occurred on any of the five available specifications. While there are options for both Windows and Mac endpoints, they contain identical settings, allowing you to track different assets for different platforms.

Groups

A group is defined as a collection of endpoints. Initially there is a single group, called the Default Group. It may not be deleted. You may add a new group at any time. When adding a new group, you may choose to create it as a subset of an existing group. You can rename a group by first selecting the group, then overwriting its existing Group Name. Here, you will associate a group with a policy. This defines protection characteristics for endpoints that are members of that group. You may create several groups which are similar in nature. It is your best interest to use an easily discernable naming convention.

You can find this in **Settings ► Groups**.

You may also delete a group if no endpoints are associated with that group. If a group has subgroups associated with it, deleting the top-level group will also delete the subgroups.

Adding Endpoints to Groups

The last piece of the puzzle is to specify members of the newly-added group. The group has been tied to a policy, and the endpoint will now be tied to the same policy for as long as it is a member of that group. Referring back to the screenshot in *Endpoints* (page 12), select one or more endpoints and click the **Move** button, which appears directly above the list of endpoints. A pulldown menu will appear which displays the names of available groups. Select the desired group to make the endpoint a member of that group.

Until you have performed the above action, newly added endpoints are associated with the Default Group.

Exclusions

You may find that exclusions are needed to provide satisfactory performance in your environment. They are often unnecessary. They may be needed if antivirus and anti-malware products interfere with each other's performance. They may also be needed if an application or data file which you trust is being flagged as a false positive—being seen as a threat when you know that it is not. Creating exclusions for these items helps to provide the best performance.

You may exclude files, folders, file extensions and registry keys. Wildcards (as used in Microsoft Windows) are accepted, anywhere in the text string that defines the exclusion. If you would like to exclude a group of registry values using a wildcard character, you may do so using the format `<PATH><KEY> | <VALUE>*`. For example:

```
HKU\*\*\SOFTWARE\*\MICROSOFT\*\WINDOWS\*\CURRENTVERSION\*\POLICIES\*\EXPLORER | NORUN*
```

You may exclude single characters in a string by using the question mark (?) in place of that character. You may exclude numbers by using the pound sign (#) in the appropriate character positions. **Please note** that these two wildcard characters represent single character exclusions only.

You can find this in **Settings ► Exclusions**.

What's Next

All prerequisites have been defined, and the stage is now set for us to dig in to your new Malwarebytes product. Along with a full description of console usage, this guide contains information for both *Incident Response* and *Endpoint Protection*. Let's begin with *Incident Response*.

Malwarebytes Incident Response

Malwarebytes Incident Response is available to all paid users of the *Malwarebytes* platform. It has four primary functions. These are:

- To execute on-demand scans of endpoints in your environment
- To execute scheduled scans of endpoints in your environment
- To remediate threats discovered during execution of the scan
- Provide scan and remediation results to the platform Dashboard.

We will focus here on scheduled scans and remediation, and leave results for the [Status](#) and [Results](#) section, later in this guide. Let's begin.

Policies

As mentioned previously, protection behavior is determined by the policy which is applied to the group of endpoints that are to be scanned. Go to **Settings ► Policies**, and select the [Default Policy](#), unless you have already created a policy. The Option Menu will show [General](#) settings, [Asset Management](#), [Incident Response](#) and [Endpoint Protection](#). Select [Incident Response](#) to view settings for this policy. Please note that Windows and Mac endpoints are handled separately due to differences between the two systems. The first setting enables you to turn *Incident Response* on or off. There is no harm in turning *Incident Response* off. You simply cannot use the product in the policy until it is turned on.

If you are an *Endpoint Protection* subscriber, you must remember the following:

- Turning on *Endpoint Protection* will automatically turn *Incident Response* off.
- Turning off *Endpoint Protection* followed by turning *Incident Response* on may require a reboot of affected endpoints.

General Settings and Asset Management

These two groups of settings are not specific to Incident Response, and were discussed previously on page 16 of this guide.

Scan Options

There are a number of settings here which may be defined. These are a function of the scan method selected, as well as the endpoint family being scanned. They are as follows:

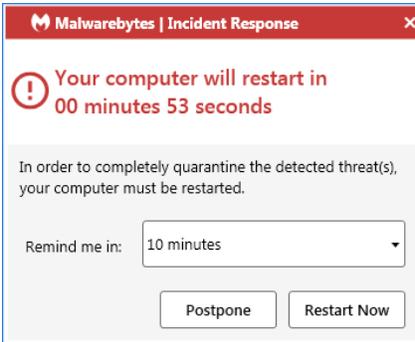
- **Scan Rootkits:** This setting applies only to Threat scans. This is always on for Macs, and may be turned on or off for Windows endpoints. The default setting is off.
- **Scan within Archives:** This also applies only to Threat scans. It may be turned on or off on Windows endpoints (the default is on), and is not currently supported for Macs.
- **Potentially Unwanted Programs (PUPs):** This applies to Threat and Hyper Scans, and specifies whether PUPs will be treated as malware, or ignored.
- **Potentially Unwanted Modifications (PUMs):** This applies to Threat and Hyper Scans, and specifies whether PUMs will be treated as malware, or ignored. This is not applicable to Mac endpoints,

Impact of Scans on System

Most users schedule scans to occur during times when their computer is typically idle. Execution of a manual scan may be performed as a matter of convenience, or while other tasks are being executed. The performance of lower-powered computers may be affected by execution of the Malwarebytes scan. This setting allows the user to determine the priority of the scan to be performed. Lower scan priority will require more time to execute while impacting other operations to a lesser degree. High priority allows the scan to be executed at the maximum speed which the computer allows, but may affect other tasks. **This option applies only to Windows endpoints.**

Reboot Options

Remediation does not end with quarantine of the visible threat. Malware may leave behind remnants which can be activated later, as well as copies of itself in memory. For this reason, a reboot is sometimes required to complete removal. When needed, you can choose whether the endpoint is restarted, and when. Not restarting the endpoint may leave the user in jeopardy.



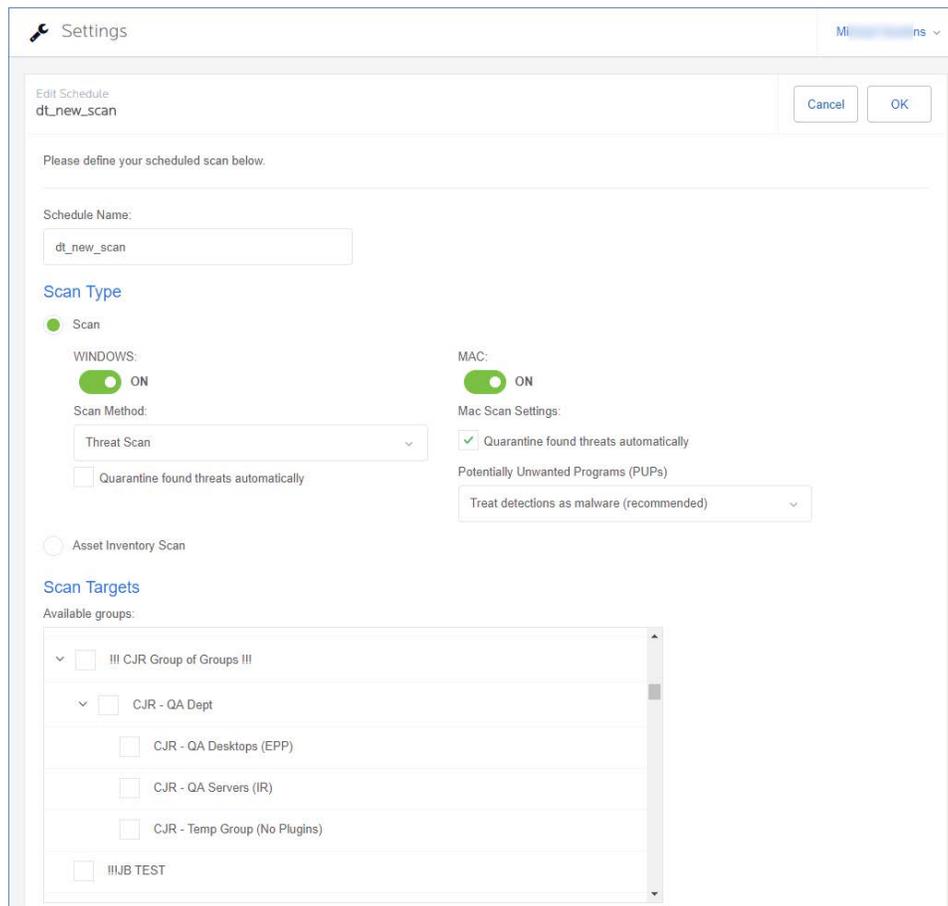
When you elect to allow a reboot, you may set a delay before this reboot occurs, as well as a user-definable text message which is displayed. Users are notified of the pending reboot. You may also allow endpoint users to postpone the reboot by 10, 20 or 60 minutes. They will receive a final notice one minute before the reboot occurs. If the postponement is greater than 10 minutes, they will also receive a warning at the 10-minute point. They can make that postponement indefinitely. All postponements generate an [Audit](#) event that appears on the [Events](#) screen.

The screen shown here is from a Windows endpoint. The Mac version is slightly different, while all functionality remains the same. Closing the dialog by clicking X in the upper right corner behaves in the same manner as the **Postpone** button.

In addition to remediation-related reboots, you may choose whether reboots are triggered by installations, uninstallation and updates. The setting which you choose applies to all of these processes.

Schedules

This ties the pieces together so that threat remediation can occur on a schedule you define, and according to your specifications. The best way to understand this process is to do it. Go to **Settings** ► **Schedules**, and click **New** to create a new scan schedule. You will see a screen which looks like this. Begin by giving the new scan a name. You may create several scans over time to serve your needs, so choose a name that will stand out when the number of scans mounts.



Scan Type

You may choose a [Scan](#) or an [Asset Inventory Scan](#), but not both at the same time. When running a Scan, there are individual settings for Windows endpoints and for Mac endpoints. You may include both in the same scan. While a Mac is limited to a Threat Scan, there are three types of scans available to a Windows endpoint.

The [Threat Scan](#) detects a large majority of threats that your computer may be faced with. Areas and methods tested include:

- **Memory Objects:** Memory which has been allocated by operating system processes, drivers, and other applications.
- **Startup Objects:** Executable files and/or modifications which will be initiated at computer startup.
- **Registry Objects:** Configuration changes which may have been made to the Windows registry.
- **File System Objects:** Files stored on your computer's local disk drives which may contain malicious programs or code snippets.
- **Heuristic Analysis:** Analysis methods which we employ in the previously-mentioned objects – as well as in other areas – which are instrumental in detection of and protection against threats, as well as the ability to assure that the threats cannot reassemble themselves.

The [Threat Scan](#) is the scan method which we recommend for daily scans. While it will not scan every file on your computer, it will scan the locations which most commonly are the launch point for a malware attack.

The [Hyper Scan](#) is limited to detection of immediate threats. Areas and methods tested include:

- **Memory Objects:** Memory which has been allocated by operating system processes, drivers, and other applications.
- **Startup Objects:** Executable files and/or modifications which will be initiated at computer startup.

While a [Hyper Scan](#) will clean any threats which have been detected, we strongly recommend that a [Threat Scan](#) be performed if a Hyper Scan has detected threats.

You may also choose to run a [Custom Scan](#). This allows you to scan according to specifications which you define at the time of the scan. These settings will override scan settings defined elsewhere. When performing a [Custom Scan](#), the following settings are available to you.

- **Quarantine found threats automatically:** This setting allows you to quarantine immediately on detection, or be prompted for each presumed threat detected during a scan.
- **Scan memory objects:** Memory which has been allocated by operating system processes, drivers, and other applications. It is important to note that threats detected during scans are still considered threats if they have an active component in memory. As an extra measure of safety, memory objects should be scanned.
- **Scan startup and registry settings:** Executable files and/or modifications which are initiated at computer startup, as well as registry-based configuration changes that can alter startup behavior.
- **Scan within archives:** If checked, archive files (ZIP, 7Z, RAR, CAB and MSI) will be scanned up to four levels deep. Encrypted (password-protected) archives cannot be tested. If left unchecked, archive files will be ignored.
- **Rootkits:** These are files stored on your computer's local disk drives which are invisible to the operating system. These files may also influence system behavior.

You can also choose whether Potentially Unwanted Programs (PUPs) and Potentially Unwanted Modifications (PUMs) will be considered as malware or simply ignored. You can choose each separately. Finally, you can specify a [Scan Path](#), which defines the top level of a folder tree to be scanned.

Scan Targets

This is where you choose the group of endpoints that will be scanned. Earlier, we created the policy that defines the behavior of the group, then we added endpoints as members of the group. Here is where it all comes together. Add or Remove groups from the list of groups to be scanned, and finally set the [Scan Schedule](#).

Scan Schedule

The last piece of the puzzle is to schedule the scan. You may not select a day that is in the past, and if you select today as a starting day for the schedule, you may not schedule it at a time that has already passed.

That's all there is to it! Later in this guide, we will look at System Status as a function of *Incident Response* activities.

Malwarebytes Endpoint Protection

This product offers Real-Time Protection, providing full proactive and reactive protection for your Windows endpoints. It is not currently available for Mac endpoints. These features include:

- Malicious web sites
- Exploits of application vulnerabilities
- Drive-by attacks
- Ransomware

We will focus here on all aspects of *Endpoint Protection* except results, leaving that for the [Status](#) and [Results](#) section (coming next).

Policies

As mentioned previously, protection behavior is determined by the policy which is applied to the group of endpoints that are to be scanned. Go to **Settings ► Policies**, and select the [Default Policy](#), unless you have already created a policy. The Option Menu will show [General](#) settings, [Asset Management](#), [Incident Response](#) and [Endpoint Protection](#). Select [Endpoint Protection](#) to view settings for this policy. At the present time, this product is available only for Windows endpoints.

The first setting enables you to turn *Endpoint Protection* on or off. **Please note** that turning this feature set off leaves you unprotected with regard to real-time threats. You should also be aware of the following:

- Turning on *Endpoint Protection* automatically turns *Incident Response* off.
- Turning off *Endpoint Protection* followed by turning *Incident Response* on may require a reboot of affected endpoints.

General Settings and Asset Management

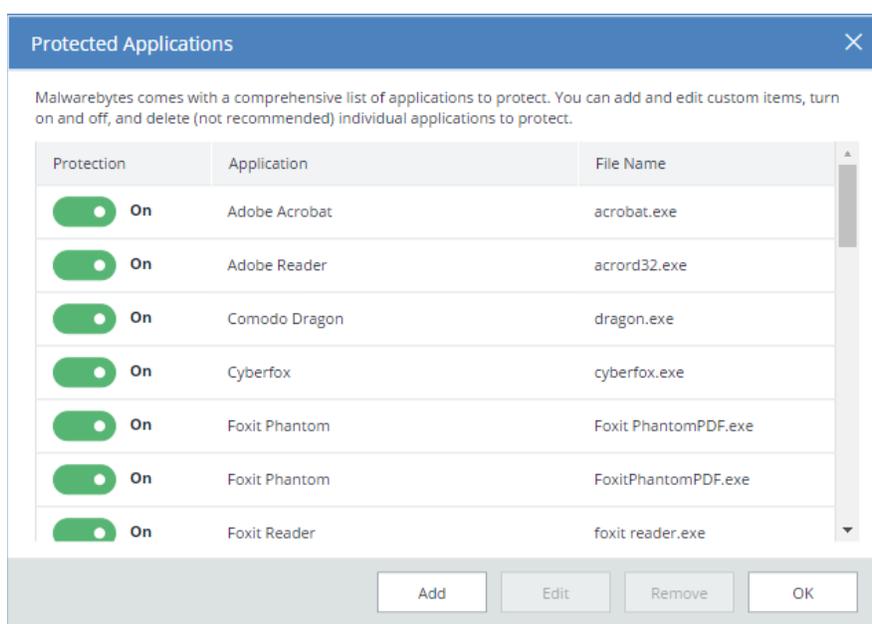
These two groups of settings are not specific to Incident Response, and were discussed previously on page 16 of this guide.

Real-Time Protection

The following is a description of the types of real-time protection offered by *Malwarebytes Endpoint Protection*.

Web Protection protects users by blocking access to/from Internet addresses which are known or suspected of engaging in malicious activity. This feature does not treat different protocols differently. It does not distinguish between your favorite game being served on one port and a potential malware source being served on another. Should you choose to disable this feature, you could inadvertently compromise your computer's safety.

Exploit Protection uses multiple protection layers to guard against attempted exploits of vulnerabilities in legitimate applications. When applications are launched by the user, exploit protection is also launched as a shield. This protection will often detect and neutralize attacks that go undetected by other security applications. It is on by default.



Many popular applications have been pre-configured for shielding. A screenshot is shown above. To change the status of any application, either use the Protection slider, or double click either the Application or File Name. You may add protection for other applications, and edit specifications for any defined shield. The Edit screen is shown here.

The Application Name can be the same as the Application File, or a more easily recognizable name. The Application File is the executable file you wish to protect. Select a Program Type which most closely resembles the purpose of the application. If you are unsure, select **Other**.

The same screen is used to edit existing entries.

Advanced Settings allows configuration or fine-tuning of some exploit mitigations included in *Malwarebytes Endpoint Protection*. Please note that not all exploit mitigations can be modified here. *Malwarebytes Endpoint Protection* has pre-defined defaults which strike the best possible balance between performance and protection. Those exploit mitigations 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 (e.g. false positives).

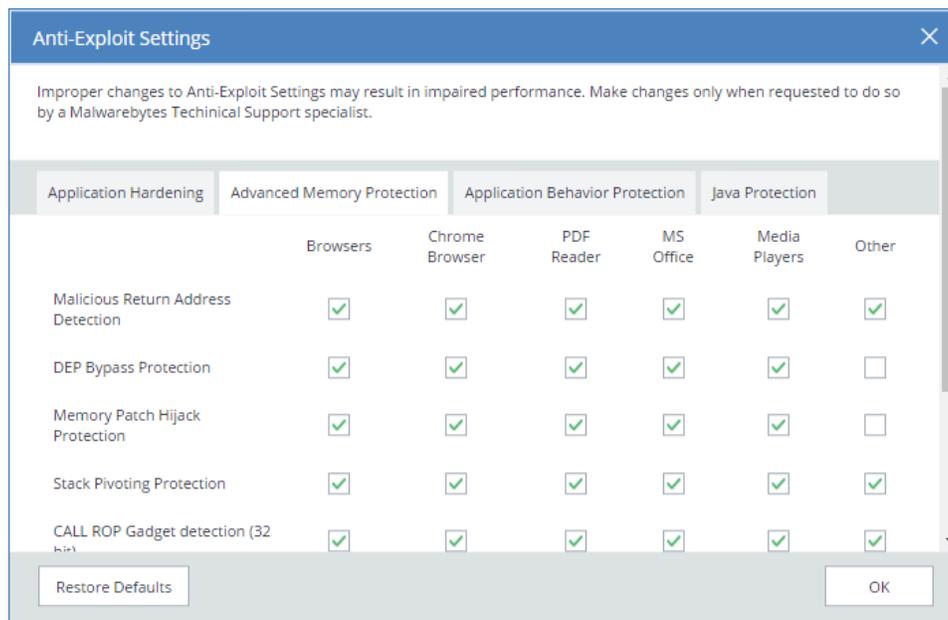
WARNING: Improper changes to these settings may result in improper performance and protection. Make changes only when required to do so by a Malwarebytes Customer Success specialist.

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.

	Browsers	Chrome Browser	PDF Reader	MS Office	Media Players	Other
DEP Enforcement	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Anti-HeapSpraying Enforcement	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Dynamic Anti-HeapSpraying Enforcement	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
BottomUp ASLR Enforcement	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Disable Internet Explorer VB Scripting	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

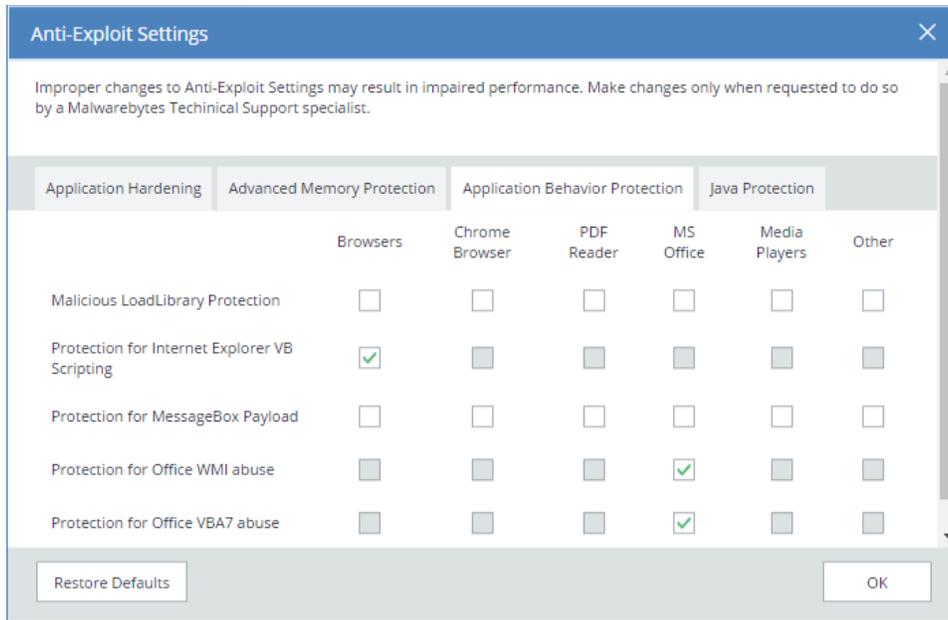
- **DEP Enforcement** is tasked with activation of permanent Data Execution Prevention (DEP) in those applications that do not do this by default.
- **Anti-HeapSpraying Enforcement** is designed to reserve certain memory ranges, to prevent them from being abused by Heap-Spraying attack techniques.
- **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.



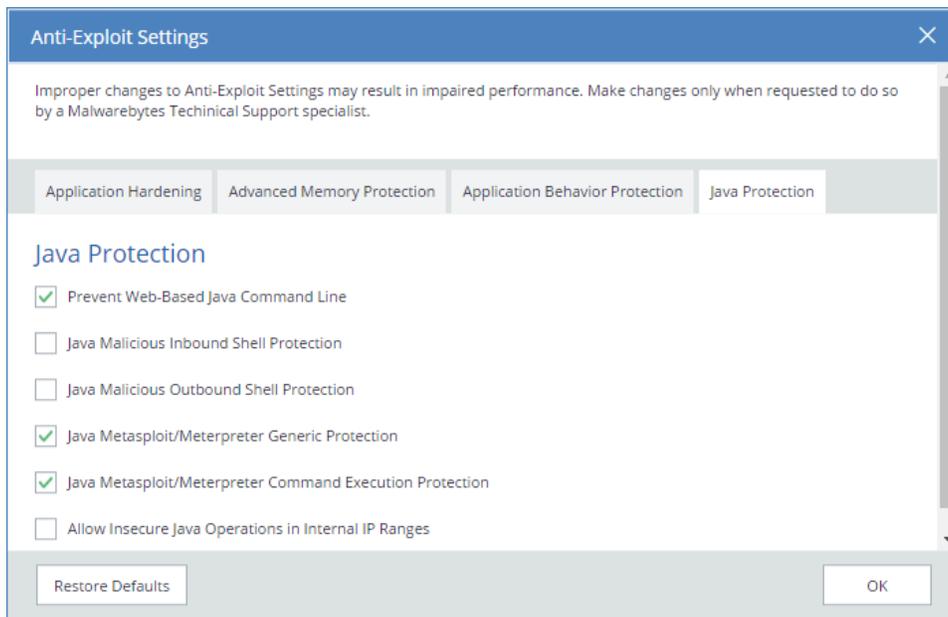
- **Malicious Return Address Detection** – also called “Caller” mitigation – detects if the code is executed outside of any loaded module.
- **DEP Bypass Protection** is tasked with detecting attempts to turn off Data Execution Prevention (DEP).
- **Memory Patch Hijack Protection** is designed to detect 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.



- **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.



- **Prevent Web-Based Java Command Line** protects against web-based Java programs issuing system commands.

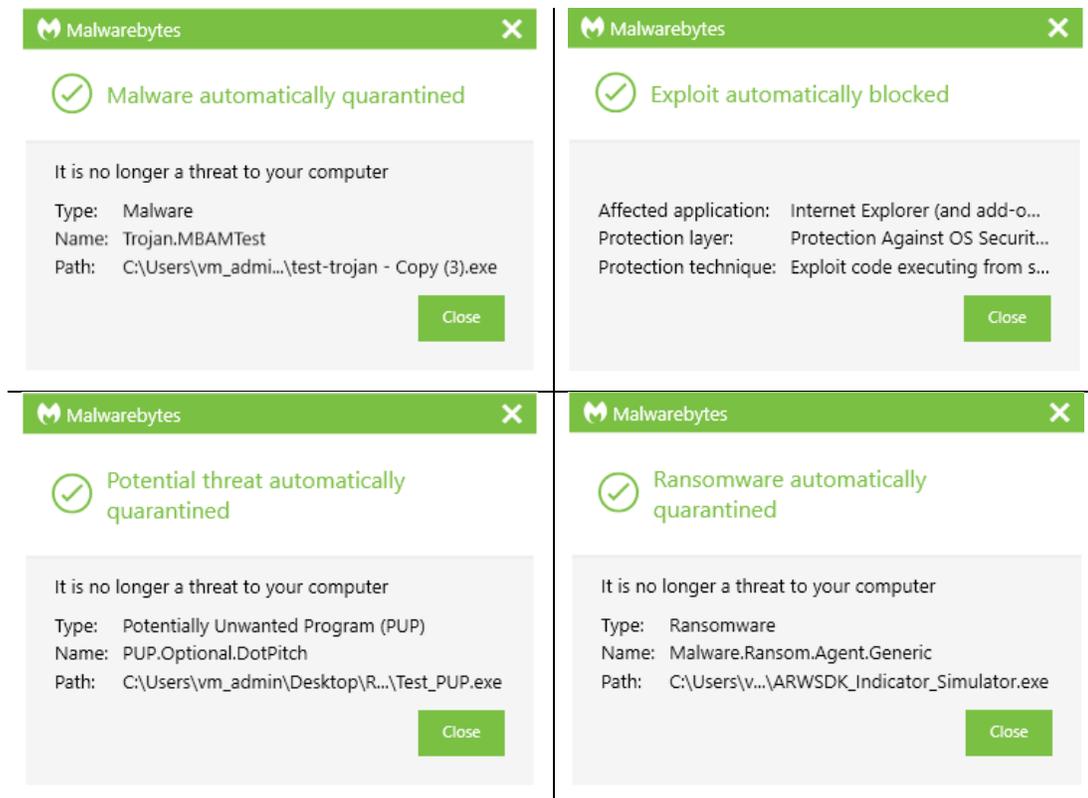
- **Java Malicious Inbound Shell Protection** guards against remote shell exploits whose payloads rely on inbound sockets.
- **Java Malicious Outbound Shell Protection** guards against remote shell exploits whose payloads rely on outbound sockets.
- **Java Metasploit/Meterpreter Generic Protection** 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.

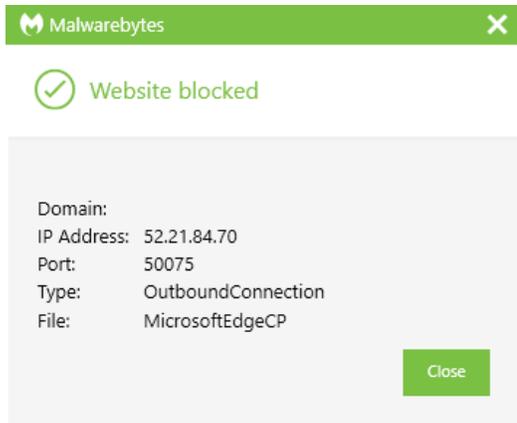
Malware Protection may be turned on or off as needed. It is on by default. This feature protects against infected code/files that try to execute on your computer. These files may have been downloaded, imported from a USB drive, or received as an email attachment. While we do not recommend disabling this protection mechanism, there may be times when it needs to be done to troubleshoot compatibility issues that arise with anti-virus updates or computer startup problems. If either situation does occur, start your computer in Safe Mode, disable Malware Protection, isolate and correct the issue, then turn Malware Protection back on.

Ransomware Protection provides protection against ransomware. This protection is not available for users of Windows XP or Windows Vista. While all other protection features may provide some degree of protection against ransomware, well-crafted ransomware may go undetected until it attempts to initiate its attack. As many computer users have found, there is little or no remedy available after the fact. We strongly recommend that ransomware protection be turned on at all times. It is on by default.

Real-Time Protection Notifications

As a function of real-time protection, *Endpoint Protection* has the capability to provide notifications on the endpoint in real-time when threats have been detected. This is dependent on notification settings you made in **Settings ► General**.





If real-time protection notifications are enabled in the policy, they will remain on-screen until closed by the user.

Scan Options

There are a number of settings here which may be defined. These are a function of the scan method selected, as well as the endpoint family being scanned. They are as follows:

- **Scan Rootkits:** This setting applies only to Threat scans. It may be turned on or off. The default setting is off.
- **Scan within Archives:** This also applies only to Threat scans. It may be turned on or off. The default setting is on.
- **Potentially Unwanted Programs (PUPs):** This applies to Threat and Hyper Scans, and specifies whether PUPs will be treated as malware, or ignored.
- **Potentially Unwanted Modifications (PUMs):** This applies to Threat and Hyper Scans, and specifies whether PUMs will be treated as malware, or ignored. This is not applicable to Mac endpoints,

Protection Updates

This setting determines how often Malwarebytes will poll our infrastructure servers for updates (both protection updates and program updates). The default check-in is set for one hour.

Startup Options

These settings define Real-Time Protection behavior when *Malwarebytes Endpoint Protection* starts. Let's look at each in detail.

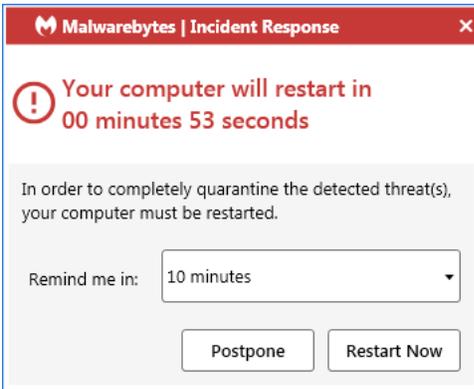
- **Delay Real-Time Protection when *Malwarebytes* starts:** There may be times when the combination of *Malwarebytes Endpoint Protection* and its Real-Time Protection services conflicts with services required by other applications. When this is the case, turn this setting on. You may also adjust the delay timing. You will need to experiment with the specific delay setting necessary to compensate for any conflicts that are noted. When required, this must be done on a case-by-case basis. The delay setting is adjustable from 15-180 seconds, in increments of 15 seconds.
- **Enable Self-Protection Module:** This setting controls whether *Malwarebytes Endpoint Protection* creates a *safe zone* to prevent malicious manipulation of the program and its components. Checking this box introduces a one-time delay as the self-protection module is enabled. While not a negative, the delay may be considered undesirable by some users. When unchecked, the "early start" option which follows is disabled.
- **Enable Self-Protection Module Early Start:** When self-protection is enabled, you may choose to enable or disable this option. When enabled, the self-protection module will become enabled earlier in the computer's boot process – essentially changing the order of services and drivers associated with your computer's startup. This setting is disabled unless Enable Self-Protection Module is turned on.

Impact of Scans on System

Most users schedule scans to occur during times when their computer is typically idle. Execution of a manual scan may be performed as a matter of convenience, or while other tasks are being executed. The performance of lower-powered computers may be affected by execution of the Malwarebytes scan. This setting allows the user to determine the priority of the scan to be performed. Lower scan priority will require more time to execute while impacting other operations to a lesser degree. High priority allows the scan to be executed at the maximum speed which the computer allows, but may affect other tasks.

Reboot Options

Threat remediation does not end with quarantine of the visible threat. Malware may leave behind remnants which may later be activated, as well as copies of itself in the endpoint's memory. For this reason, certain types of malware require a reboot to complete the removal task. When *Incident Response* determines that a restart is required to remove a threat, you can choose whether the endpoint is restarted, and when. Not restarting the endpoint may leave the user in jeopardy.



When you elect to allow a reboot, you may set a delay before this reboot occurs, as well as a user-definable text message which is displayed. Users are notified of the pending reboot. You may also allow endpoint users to postpone the reboot by 10, 20 or 60 minutes. They will receive a final notice one minute before the reboot occurs. If the postponement is greater than 10 minutes, they will also receive a warning at the 10-minute point. They can make that postponement indefinitely. All postponements generate an [Audit](#) event that appears on the [Events](#) screen.

Closing the dialog by clicking X in the upper right corner behaves in the same manner as the **Postpone** button.

In addition to remediation-related reboots, you may choose whether reboots are triggered by installations, uninstallation and updates. The setting which you choose applies to all of these processes.

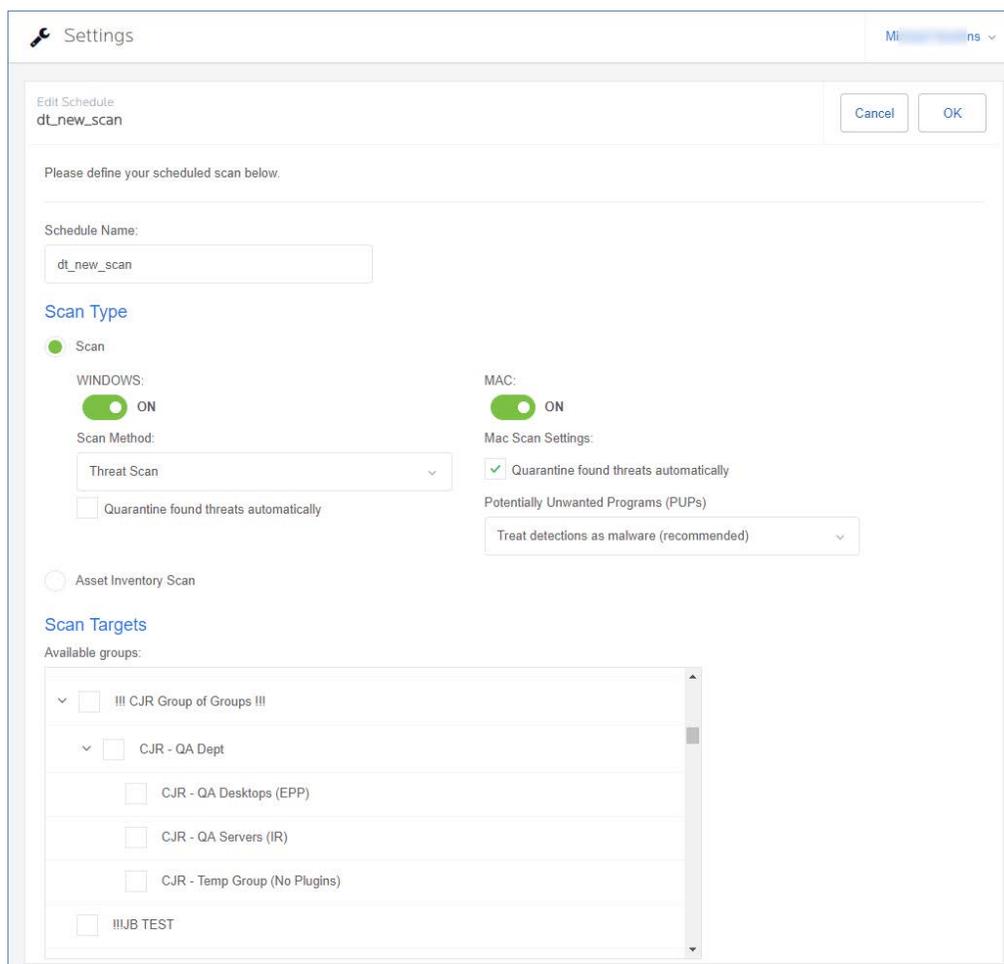
Windows Action Center

You may have noticed an icon in your system tray with a red X superimposed over a white flag. That is a status indicator for the Windows Action Center, which tells you when your computer has a security issue that needs your attention. *Malwarebytes Endpoint Protection* can now be registered as the security solution on your computer. There are three settings available, which will be abbreviated here for easier reading. Brief descriptions for the meaning of each setting are also provided.

- **Let Malwarebytes choose whether to register:** *Malwarebytes* will determine whether it should be registered in Action Center. The program will not register when Microsoft Security Essentials is in use on a Windows 7 or older operating system. It will also not register when Windows Defender is used on a Windows 8 or newer OS.
- **Never register Malwarebytes:** *Malwarebytes* program status will never appear in Action Center.
- **Always register Malwarebytes:** *Malwarebytes* program status will always appear in Action Center.

Schedules

This ties all of the pieces together so that *Endpoint Protection* can remediate threats on your endpoints on a schedule you define, and according to specifications you provide. The best way to understand this process is to do it. Go to **Settings ► Schedules**, and click New to create a new scan schedule. You will see a screen which looks like this. One of our test scans is used for illustration purposes. **Please note** that while Mac endpoints are not currently supported with real-time protection, you can still run scans on Mac Endpoints, either by themselves or combined with Windows endpoints.



Begin by giving the new scan a name. You may create several scans over time to serve your needs, so choose a name that will stand out when the number of scans mounts.

Scan Type

You may choose a Scan or an Asset Inventory Scan, but not both at the same time. When running a Scan, there are individual settings for Windows endpoints and for Mac endpoints. You may include both in the same scan. While a Mac is limited to a Threat Scan, there are three types of scans available to a Windows endpoint.

The **Threat Scan** detects a large majority of threats that your computer may be faced with. Areas and methods tested include:

- **Memory Objects:** Memory which has been allocated by operating system processes, drivers, and other applications.
- **Startup Objects:** Executable files and/or modifications which will be initiated at computer startup.
- **Registry Objects:** Configuration changes which may have been made to the Windows registry.
- **File System Objects:** Files stored on your local disk drives which may contain malicious programs or code snippets.
- **Heuristic Analysis:** Methods we employ which are instrumental in threat detection and protection, as well as the ability to assure that the threats cannot reassemble themselves.

The **Threat Scan** is the scan method which we recommend for daily scans. While it will not scan every file on your computer, it will scan the locations which most commonly are the launch point for a malware attack. The **Hyper Scan** is limited to detection of immediate threats. Areas and methods tested include:

- **Memory Objects:** Memory which has been allocated by operating system processes, drivers, and other applications.
- **Startup Objects:** Executable files and/or modifications which will be initiated at computer startup.

While a **Hyper Scan** will clean any threats which have been detected, we strongly recommend that a **Threat Scan** be performed if a Hyper Scan has detected threats.

You may also choose to run a **Custom Scan**. This allows you to scan according to specifications which you define at the time of the scan. These settings will override scan settings defined elsewhere. When performing a **Custom Scan**, the following settings are available to you.

- **Quarantine found threats automatically:** This setting allows you to quarantine immediately on detection, or be prompted for each presumed threat detected during a scan.
- **Scan memory objects:** Memory which has been allocated by operating system processes, drivers, and other applications. It is important to note that threats detected during scans are still considered threats if they have an active component in memory. As an extra measure of safety, memory objects should be scanned.
- **Scan startup and registry settings:** Executable files and/or modifications which are initiated at computer startup, as well as registry-based configuration changes that can alter startup behavior.
- **Scan within archives:** If checked, archive files (ZIP, 7Z, RAR, CAB and MSI) will be scanned up to four levels deep. Encrypted (password-protected) archives cannot be tested. If left unchecked, archive files will be ignored.
- **Rootkits:** These are files stored on your computer's local disk drives which are invisible to the operating system. These files may also influence system behavior.

You can also choose whether Potentially Unwanted Programs (PUPs) and Potentially Unwanted Modifications (PUMs) will be considered as malware or simply ignored. You can choose each separately. Finally, you can specify a **Scan Path**, which defines the top level of a folder tree to be scanned.

Scan Targets

This is where you choose the group of endpoints that will be scanned. Earlier, we created the policy that defines the behavior of the group, then we added endpoints as members of the group. Here is where it all comes together. Add or Remove groups from the list of groups to be scanned, and finally set the **Scan Schedule**.

Scan Schedule

The last piece of the puzzle is to schedule the scan. You may not select a day that is in the past, and if you select today as a starting day for the schedule, you may not schedule it at a time that has already passed.

That's all there is to it! Now it's time to look at **System Status**.

System Status

Malwarebytes products are now ready to protect your endpoints. You have set up scan schedules. You have configured protection layers of Real-Time Protection. It is time to discuss how Malwarebytes keeps you informed with regard to malware-related activities on your endpoints. Tabs and topics to be discussed here include:

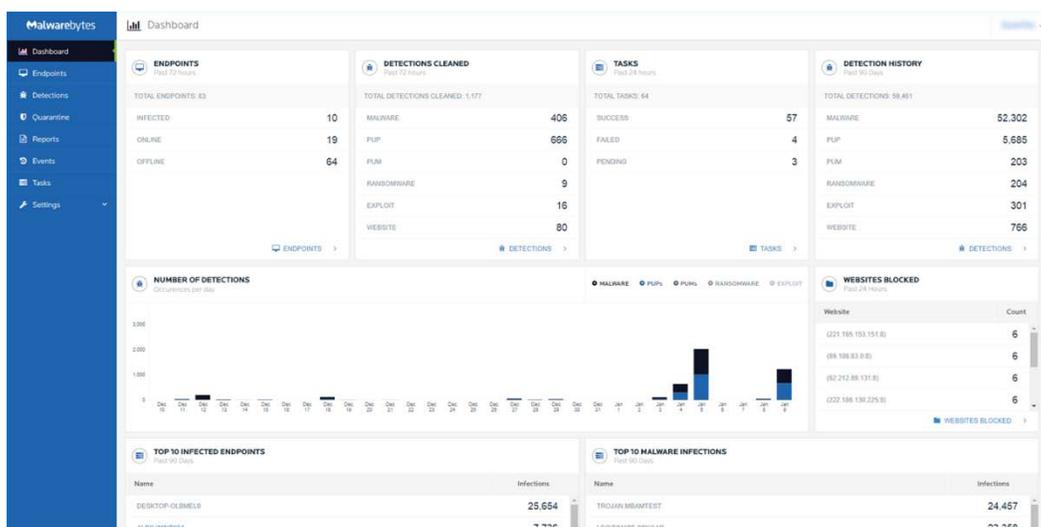
- Dashboard
- Threats
- Quarantine
- Real-Time Protection
- Events
- Tasks

Dashboard

When you first open the Malwarebytes console, the first screen that you will see is the Dashboard. It is designed to provide a high-level view of malware-related activities on your network. Data shown is a cross-section of information which is displayed in detail on the other Malwarebytes console status screens. The Dashboard view includes:

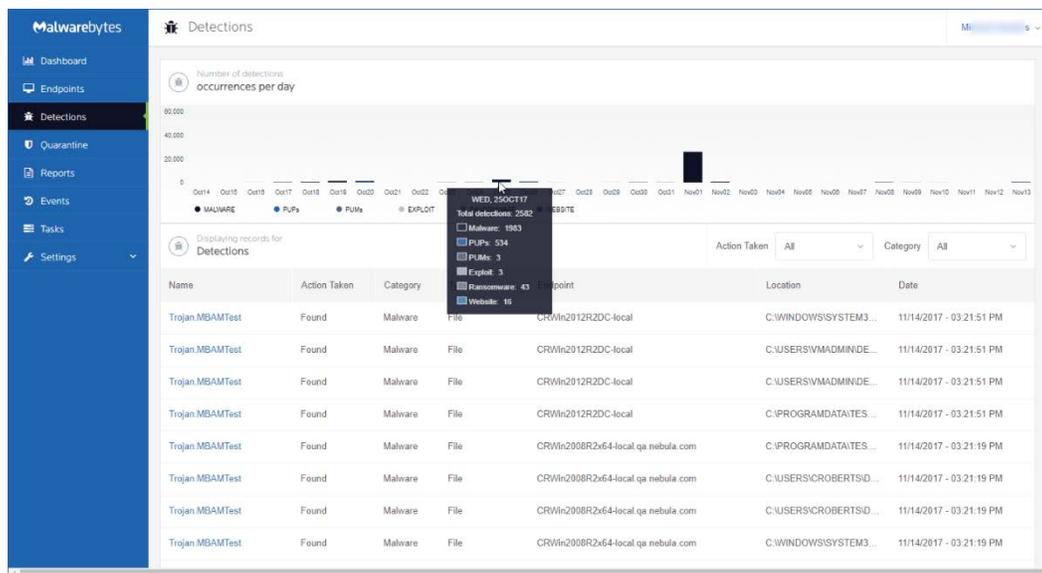
- Number of endpoints online, offline, and infected (both online and offline) over the most recent 72 hours
- Threats cleaned during the past 72 hours, broken down by Malware, PUP and PUM
- Tasks issued by the Malwarebytes console over the past 24 hours, broken down by status (success, failure or pending)
- Threats detected during the past 90 days, broken down by Malware, PUP and PUM
- A bar graph showing Malware, PUPs and PUMs by day, over the past 30 days
- List of Top 10 malicious/suspicious websites blocked in the last 24 hours
- List of Top 10 most highly-infected endpoints over the past 90 days
- List of Top 10 malware infections detected over the past 90 days
- List of Top 10 PUPs over the past 90 days
- List of Top 10 PUMs over the past 90 days

Information shown on the Dashboard is current as of the time you access the Dashboard. A screenshot of the Dashboard is shown below.



Detections

This tab provides a detailed itemization of every threat detected during a scan in the past thirty days. A bar graph indicates the level of threat activity on each day in that period. Hovering over any date in which threats were detected will show a breakdown of the count of the basic types of threats that were detected on that day. One specific date is shown in this screenshot for illustrative purposes.



You may also click on any specific detection to view more details about the detection. The main body of the screen is used to show threat data. Please note the two pulldown menus at the right center region of the screen. They are used to select what data is shown on the remainder of the screen.

<p>Action Taken</p> <ul style="list-style-type: none"> All Blocked Found Quarantined Deleted Restored Cleaned Offline 	<p><u>Action Taken</u> defines the current status of threats which have been detected. One description you may find curious is <i>Cleaned Offline</i>. That describes threats which were deleted from Quarantine manually, rather than under program control.</p> <p><u>Category</u> is the type of threat which was detected.</p> <p>Selecting subsets allows you to “remove the noise” and focus on the information you are most concerned with.</p>	<p>Category</p> <ul style="list-style-type: none"> All Malware PUP PUM Exploit Ransomware Website
--	--	--

Quarantine

A quarantined threat is one that has been detected, neutralized, and placed into a special container so that it cannot cause any damage to your computer. This tab allows you to view those threats. You may filter your view by choosing a specific threat category. This is a consolidated view, meaning that all quarantined threats on all managed endpoints are shown. In actuality, quarantined threats are stored on the endpoints themselves in an encrypted format. Two entries exist for each threat, the threat itself and proprietary information about the threat. Their location on each endpoint is:

`C:\ProgramData\Malwarebytes\MBAMService\Quarantine`

After selecting one or more quarantined threats, you may restore or delete them by selecting the threat(s) and then selecting the appropriate action. While you may restore or delete across multiple endpoints at the same time, you cannot restore *and* delete at the same time. Please note that false positives are possible in rare circumstances. Also, you may have items in Quarantine which are known, trusted files. You should not automatically assume that the contents of Quarantine are malicious, nor should you assume that they are safe.

Reports

You may now generate some basic **Detection Summaries** covering the previous day, week or month. These reports are provided in a Comma Separated Values (CSV) file format. Once a report has been requested, the request will be placed into a queue for processing. When the report is complete, an email will be sent to the email address associated with your account so that you can download the report. Please note that all times shown in reports uses Coordinated Universal Time (UTC).

Events

This tab displays a record of threats, remediation and other activities for installed endpoints. At the top of the screen is a bar graph showing system activities over the past thirty days. Immediately following is a pulldown menu which allows you to select the Severity of information being reported here. You may choose to display all activities, or narrow the view by selecting one of these settings. There are several event types which can be shown. A representative sample for each severity is as follows:

- **Severe** – Threat has been found
- **Warning** – Threat has been cleaned
- **Info** – Completion of a scan
- **Audit** – Endpoint registered

Use of the pulldown menu is strongly recommended. A large number of items can be reported here over time.

Tasks

This tab is a record of all on-demand activities (asset management scans, malware scans, restore, delete) that have been requested on endpoints. The top of the tab shows the number of activities in each status type, summarized over the past thirty days. Information pertaining to the activity request (who, where, when) is logged, as is status of the activity. To focus on a single status, click the bar underneath the 30-day total for that status.

Please note: Tasks have a finite lifespan. Any tasks which have not been acted upon by the affected endpoint within 90 days of the task's issuance will be removed from the task queue.

Discovery and Deployment Tool Command Line Reference

The *Discovery and Deployment tool* can be used via its GUI interface as well as a command line mode. All commands take the form:

```
EndpointAgentDeploymentTool -<switch1> <value1> [-<switchn> <valuen>]
```

Use of the tool is best illustrated by an example, which follows. This is all one line, but is broken up here for easier reading.

```
EndpointAgentDeploymentTool  
-Action=install  
-User=owner@malwarebytes.com  
-Pwd=MyNebulaPassword  
-targetUser=Corp\targetUserName  
-targetPwd=MyPassword  
-Results=c:\files\installresult.txt  
-computers=Computer1;Computer2;10.1.1.2;
```

Here, a silent installation was performed on three endpoints, two identified by name and one by IP address. The results of the installation process was saved to a file for later inspection. When using the command line mode, the following arguments may be used. They are listed here in alphabetical order.

-action

Deployment action that the program will perform on the endpoint. Valid values are **install** and **uninstall**.

-computers

List of computers used in discovery. While discrete computer names or IP addresses may be specified here, IP address ranges may also be used. Entries should be separated by semicolons (;).

-file

Location of a file which contains endpoint identity information used in discovery. Please refer to page 3 ("*Who to Discover*") for a list of specifications which this information can take.

-nebulauri

URL of the *Malwarebytes* server. Default value is <https://cloud.malwarebytes.com>.

-proxybypass

Specifies whether the proxy can be bypassed on communications on the local network. Valid answers are **yes/no**, **true/false**, or **1/0**. Only valid if **-proxyuse** is set to **{yes|true|1}**, and is ignored if **-proxyuse** is **{no|false|0}**.

-proxypassword

Password associated with **-proxyuser** for Internet access through a proxy. Only valid if **-proxyuse** is set to **{yes|true|1}**, and is ignored if **-proxyuse** is **{no|false|0}**.

-proxyport

If **-proxyuse** is set to **{yes|true|1}**, this is the port number associated with proxy server access to the Internet. It is ignored if **-proxyuse** is **{no|false|0}**.

-proxysl

Specifies whether SSL encryption should be used for Internet access through a proxy. Valid answers are **yes/no**, **true/false**, or **1/0**. Only valid if **-proxyuse** is set to **{yes|true|1}**, and is ignored if **-proxyuse** is **{no|false|0}**.

-proxyurl

If **-proxyuse** is set to **{yes|true|1}**, this is the FQDN or IP address of the proxy server to be used for Internet access. It is ignored if **-proxyuse** is **{no|false|0}**.

-proxyuse

Specifies whether a proxy server is required for connection to the *Malwarebytes* server. Valid answers are **yes/no**, **true/false**, or **1/0**.

-proxyuser

Username to be used for Internet access through a proxy. Only valid if **-proxyuse** is set to **{yes|true|1}**, and is ignored if **-proxyuse** is **{no|false|0}**.

-pwd

Password associated with *<user>*.

-results

A valid file path/name where results of the specified action should be stored. This allows install/uninstall activities to be performed in a silent manner.

-targetpwd

Password associated with *<targetuser>*.

-targetuser

Username that will be used for agent deployment on endpoints.

-user

User name for login to the *Malwarebytes* server.

-wmionly

If present, only WMI methods will be used for endpoint discovery.