Malwarebytes

Malwarebytes Cloud Console Administrator Guide
29 November 2018

Malwarebytes

Notices

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

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

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

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

Table of Contents (continued)

Table of Contents (continued)

What's New in Malwarebytes

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

New Features

- Redesigned the Global exclusions page to improve usability and include advanced capability to specify technologies the exclusion is applied to.
- Added ability to automatically exclude commonly detected Potentially Unwanted Modifications (PUMs) caused by Group Policy Objects.
- Added an endpoint interface option to create Start Menu and Desktop shortcuts for end-users
- [**Malwarebytes Endpoint Protection and Response only**]: Added an aggressive detection mode policy option for Suspicious Activity.

Improvements

- [**Malwarebytes Endpoint Protection and Response only**]: Suspicious Activity detections will now be included in Syslog messages
- Changed our unmonitored email address to do_not_reply@cloud.malwarebytes.com to reduce the chance of cloud console emails being flagged as spam
- Fixed: [**Malwarebytes Endpoint Protection and Response only**] – When a remediation action succeeds but rollback action fails, the Suspicious Activity status is stuck and displays "Pending Remediation"
- Fixed: The Deployment and Discovery tool would generate a 504 error when importing Active Directory groups that contained a large number of endpoints
- Fixed: Some temporary files were being left behind after installation or endpoint agent updates
- Fixed: Customers with a large number of endpoints were unable to sort by "Last Seen At" on the Manage Endpoints page
- Fixed: In some cases, when a reboot prompt is shown, the reboot timer resets with a 1-minute countdown

Known Issues

- Exclusions that have been entered with short file name paths such as "c:\progra~2\" are not being applied
- Modal windows are showing an unnecessary scroll bar
- All Malwarebytes scans will inspect archived files regardless of the policy setting
- When administrators reboot endpoints from the cloud console, if the initial reboot task has not completed, subsequent reboot commands are queued rather than replacing the initial reboot command (this would result in execution of multiple reboots)
- When administrator chooses "Restart Immediately" option in the Restart Options dialog, end users are still allowed to postpone the reboot even though the "Allow user to postpone" option is grayed out. Current workaround involves selecting the "Restart in ____ minutes" radio button, unchecking the "Allow user to postpone" checkbox, then select the "Restart Immediately" radio button and click the blue Restart button
- Clicking on the Remediate button causes the Remediation Required indicator to lose its badge on hover and on click behavior— nothing happens on click (should give you the option to view details) and nothing happens on hover (should show "Remediation Pending"). This issue is resolved by refreshing the browser
- Memory and storage objects in endpoint properties are not visible until the page is refreshed
- The Endpoint Agent can fail to initialize when using the GROUP ID parameter with an incorrect format
- [**Malwarebytes Endpoint Protection for Mac only**]: Scan History tab does not get information populated if Threat Scan does not detect any threats
- [**Malwarebytes Endpoint Protection for Mac only**]: Timestamps in Scan History tab for macOS endpoints are in GMT, and not the web browser's locale
- [**Malwarebytes Endpoint Protection for Mac only**]: Check for Protection Updates action does not update "Last Refreshed" on first run

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 in charge of discovery, deployment, management and administration of Malwarebytes agents on your company's endpoints. It 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 the endpoint. You may deploy the agent using the Malwarebytes platform, Malwarebytes Discovery and Deployment Tool, Active Directory Group Policies, Microsoft SCCM, or a comparable tool of your choice.
- *Endpoint Agent Plugins* – These modular components are installed on your endpoints via the *Endpoint Agent*, and configured using the *Malwarebytes* console. Plugins are deployed to your endpoints based on your policy settings. The specific subscription you have purchased from Malwarebytes determines which plugins you may use.

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, 2012, 2012 R2, SBS 2011, 2008 R2 SP1[‡§], 2008 SP2 [‡§], 2008[§]
  - **Windows Client:** 10, 8.1, 8, 7, Vista[§], XP SP3[§*]
  - **Macintosh:** macOS 10.10 or later

†	Excludes Server Core installation option
‡	Microsoft patch KB4019276 must also be installed and enabled
§	As of July 2018, development has halted for Endpoint Clients using this operating system
*	32-bit only
	.NET 4.5.2 or 4.6 must be installed and enabled on Windows systems

Please note:
- *Anti-Ransomware* features are supported only on endpoints using Windows 7 client operating systems and newer.
- *Endpoint Protection and Response* is supported only on endpoints using Windows 7 client operating systems and newer. Transport Layer Security (TLS) 1.1/1.2 must be enabled.
- *Endpoint Protection and Response* endpoints using Server 2008 R2, Server 2012 R2, and Server 2016 support Isolation only.

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://telemetry.malwarebytes.com	Port 443	outbound
https://detect-remediate.cloud.malwarebytes.com	Port 443	outbound
https://data-cdn-static.mbamupdates.com	Port 443	outbound
https://keystone.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
https://storage.gra3.cloud.ovh.net	Port 443	outbound
https://nebula-agent-installers-mb-prod.s3.amazonaws.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\flightrecorder.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
```
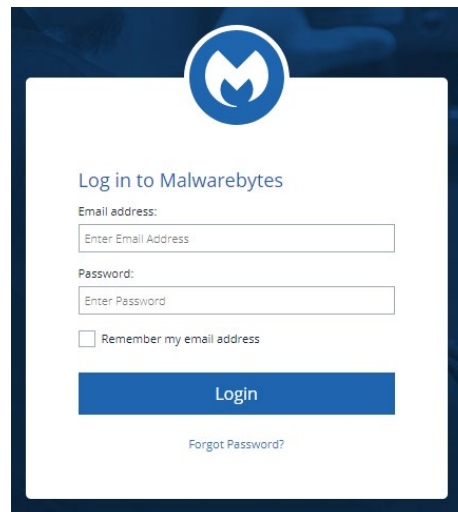
- Mac Endpoints

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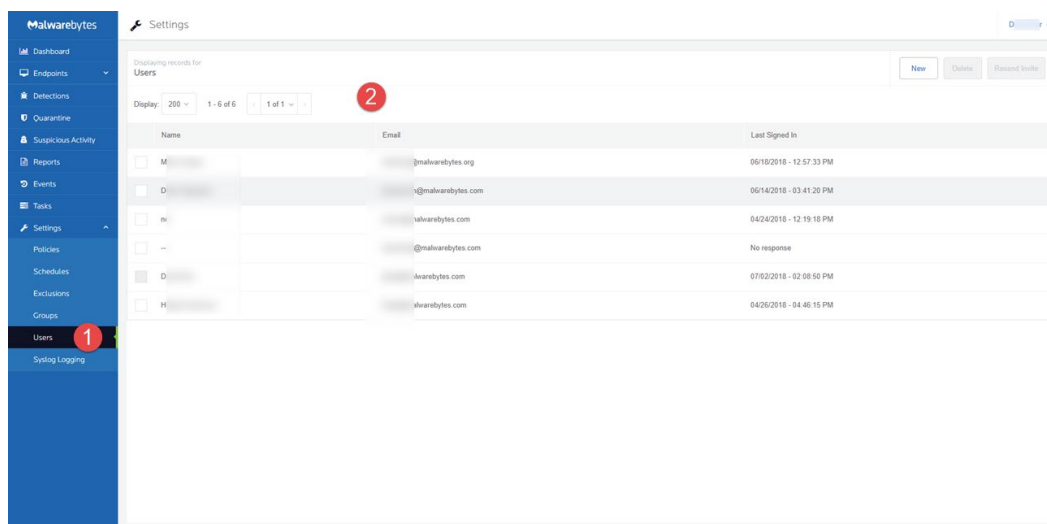
Confirm your password, accept the terms of the End User License Agreement (EULA) and click **Submit** to get started.

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. Depending on the product that you purchased, your view may be different.

The *Options Menu* ❶ 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 ❷ itself.

Profile

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

These options cover the following topics:

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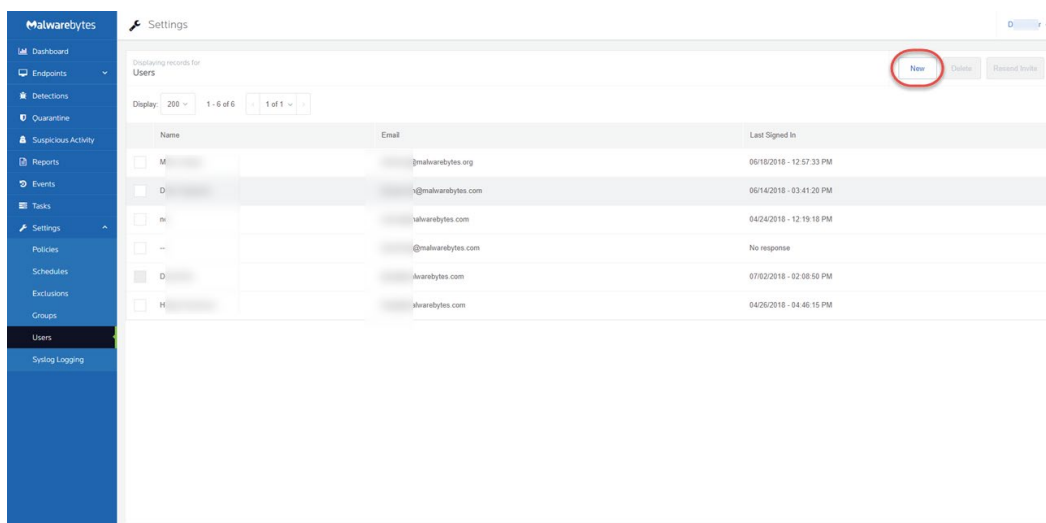- **Notifications:** Specify what type of events you wish to receive email notifications for.
- **Remote Assistance:** Enables a setting that allows Malwarebytes Customer Support to access your account (Customer Support will reset this once reason for access is resolved.).
- **License Information:**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

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 <u>Settings</u> tab and select <u>Users</u>. A list of users will be displayed (to the right of the checkboxes that are the left border in this screenshot).

A <u>New</u> button (at the upper right of the screen) allows you to create a new user account. Enter the email address for the prospective user. Next, select the <u>User Role</u>. The three roles are:

- **Super Admin –** The user will have unrestricted access to the *Malwarebytes* console.
- **Administrator –** The user will have full read/edit access to any groups they are assigned. They cannot edit global settings.
- **Read Only –** The user will have read access to any groups they are assigned. They can generate reports and receive notifications but cannot make any changes.

The bottom menu shows a list of Groups that are available in your *Malwarebytes* console. By default, new users have access to <u>All Groups</u>. If you want to restrict access to specific groups for a new user, scroll through the list and un-check the box to the left of any group to remove the user's access. Removing access to a group prevents a user from seeing any information from endpoints in those groups; they will not appear in the console, nor will they appear in reports that the user generates.

When you have configured the user's access, click **<u>Invite</u>** to send them an email to create an account.

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

The administrator's account is flagged as the account owner in the console; it cannot be deleted by any user. If you need to change the account owner, please contact us.
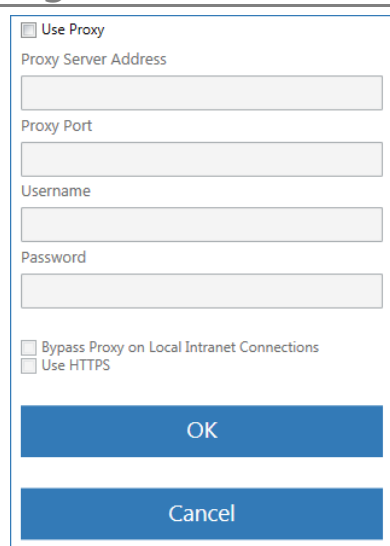
Discovery and Deployment Tool

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 that you specify, and identifies networked devices that 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 interactive mode and command line mode. Please refer to the end of this guide for command line operation. Parameters set in the command line mode do not carry over to the GUI mode.

> ► **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

For each endpoint that you wish to install, 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
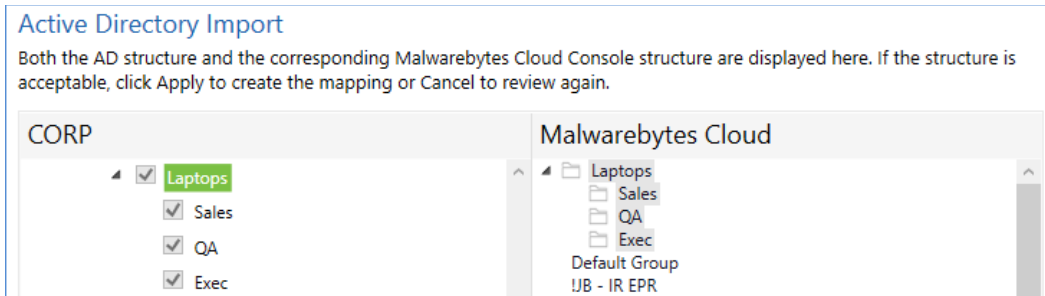
Active Directory Import

Most likely, you have already organized your endpoints in Active Directory to fit your needs. You can import the same Active Directory structure to *Malwarebytes*. This allows you to quickly install the Endpoint Agent and create groups in the *Malwarebytes* console to mimic your existing configuration. Click **Active Directory Import** to begin.

The tool will use the current logged in Windows account to query the Domain Controller. If you need to provide a different account, click **Change Active Directory Credentials** at the bottom right of the tool. You can search for specific Organizational Units (OUs) using the Search menu at the top right of the tool. The arrows next to the menu allow you to quickly browse the results. You can also use **F3** and **Shift+F3** to browse search results.

Select all OUs you wish to import to *Malwarebytes* using the checkboxes to the left of the OU name. When you have selected the OUs to import, click **Preview** to view a display showing how the selected OU(s) will appear in the console. These groups will appear with a folder icon in the Discovery Tool, as well as in the console once they are imported. An example appears below.

Active Directory Import
Both the AD structure and the corresponding Malwarebytes Cloud Console structure are displayed here. If the structure is acceptable, click Apply to create the mapping or Cancel to review again.
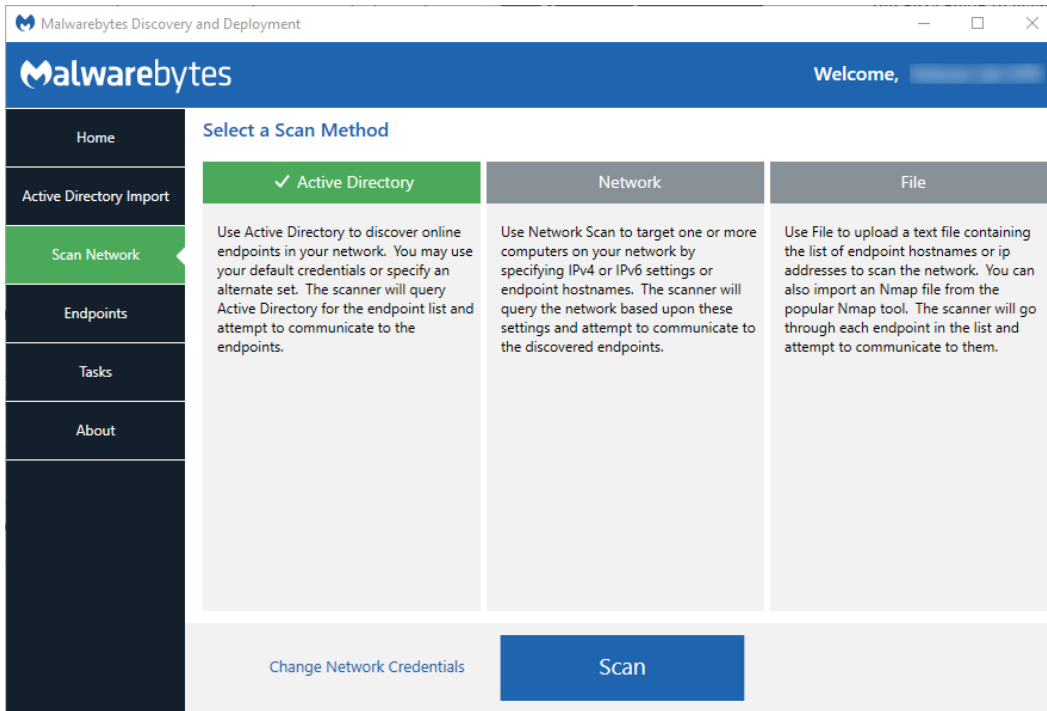
Click **Apply** to import the OU as a Group. You can now begin installing the endpoint agent on computers inside the selected OU, or select a subset of imported Active Directory OUs using the AD Filter (discussed in the next section).

Scan Network

If you do not have Active Directory, or wish to install the Endpoint Agent on specific Endpoints, click **Scan Network** from the Home menu. Before you can deploy the Endpoint Agent, you need to identify the target endpoints. We provide three methods to discover endpoints and validate our results. Only one method is required.
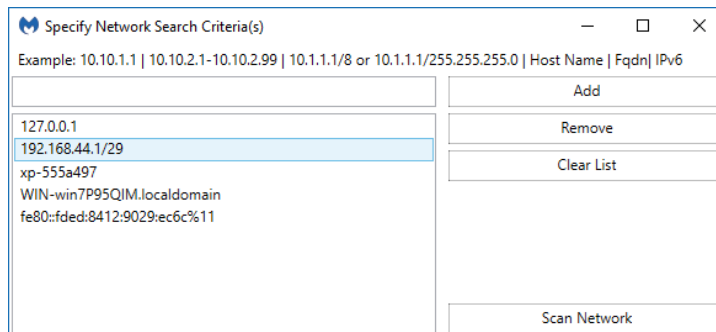
- **Method 1 –** Query Active Directory for a list of machines in your domain.
- **Method 2 –** A Network Scan allows you to provide search criteria for endpoints in your network. You can specify several different criteria, and all will be tested. Criteria includes:
    - IPv4 address
    - IPv4 address 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.

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 <u>Network Scan</u> 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.

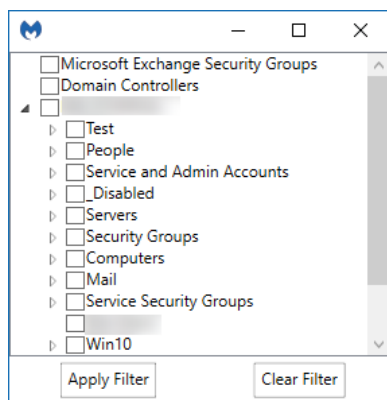The pulldown next to the Search box allows filtering of discovery results, so that only endpoints which match the specified discovery status will be displayed. Allowable status includes *All*, *Online*, *Offline*, *Probing*, and *Queued for Probing*. Please note that while scanning is extremely fast, 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 <u>Active Directory Scan</u>. 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 <u>Name</u> will show the full FQDN for the machine, and <u>Domain</u> will be populated by the Active Directory domain name. By clicking the <u>AD Filters</u> 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 <u>workgroup</u>, 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 <u>and</u> 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 (SSH) should be enabled on the destination Mac endpoint(s).
- The installer will not uninstall *Malwarebytes for Mac*, our home product. You should remove this from your Mac endpoint(s) ahead of installation.
- The installer will not attempt to overwrite previous endpoint agent installations. You must un-install the program prior to re-installing.
- The installer will download the latest Protection Updates prior to finishing.
- Endpoints whose <u>Status</u> is *Offline* or whose <u>Installed</u> 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.

Deploying Endpoint Agent for Windows Endpoints

The next two sections describe technical information related to deployment, but user interactions are limited to selecting the machine and clicking **Install**. 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 that 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.

Deploying Endpoint Agent for Mac Endpoints

Apple has made changes in macOS High Sierra (version 10.13.x) that affect the ability to deploy software using kernel extensions. Because *Malwarebytes* Real-Time Protection on Mac uses a kernel extension, there are some things to be aware of when deploying to endpoints running High Sierra. You will need to take these steps for every Mac you wish to use Real-Time Protection on. If you are only using scans (scheduled or on-demand), these instructions will not apply. If you decide later to make use of Real-Time Protection, then you will need to perform these steps.

Direct Deployment

If you are installing *Malwarebytes* by manually running the *Endpoint Agent* installer, you will see a prompt saying "System Extension Blocked" when installation finishes. After you receive the prompt, an <u>Allow</u> button will appear in the General tab of the Security & Privacy pane of System Preferences for half an hour. After half an hour, macOS will remove the button.

You must click this button in order to finish the installation and enable Real-time Protection. You may not click the button remotely via screen sharing or scripted actions– you **must** physically click the button from the endpoint to finish installation. If you do not click the button within half an hour, you may restart the endpoint to cause the button to reappear for another half an hour.

Remote Deployment for macOS 10.13 – 10.13.3

To prepare a Mac to install *Malwarebytes* remotely, you must meet two requirements.

- The endpoint must be enrolled in Apple's Device Enrollment Program (DEP)
- The endpoint must have a Mobile Device Manager (MDM) that was deployed through DEP

If the endpoint meets these requirements, the scenario described earlier for direct deployment will not occur. You will not receive the prompt, or need to click the button to allow the installation to finish.

Remote Deployment for macOS 10.13.4 and above

Apple added one additional requirement in macOS 10.13.4. In addition to the two requirements mentioned above, you must also deploy a kernel extension policy, `com.apple.syspolicy.kernel-extension-policy`, to the endpoint. The policy must be delivered via a user approved MDM server. We have provided an example of a policy file:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
  <dict>
    <key>AllowUserOverrides</key>
    <false/>
    <key>AllowedTeamIdentifiers</key>
    <array>
      <string>GVZRY6KDKR</string>
    </array>
    <key>AllowedKernelExtensions</key>
    <dict>
      <key>GVZRY6KDKR</key>
      <array>
        <string>com.malwarebytes.mbam.rtprotection</string>
      </array>
    </dict>
  </dict>
</plist>
```

Take note of the key value, `GVZRY6KDKR`. This key is specific to the Real-Time Protection kernel extension. You may also add additional keys for other applications you wish to install which require kernel extensions.

Alternative Method

If the endpoint you are deploying to is not enrolled in DEP, or is enrolled but do not have an MDM that was deployed via DEP, there is an alternative besides requiring someone to click **Allow**. Restart the endpoint in Recovery mode, and then open the Terminal in Recovery. In the terminal, enter the following command:

```
spctl kext-consent add GVZRY6KDKR
```

This will whitelist the *Malwarebytes* kernel extension on that machine. You can also utilize this technique with NetBoot, NetInstall, and NetRestore images.

Additional Information

We have covered a lot of information to prepare how to deploy Real-Time Protection to your Mac environment. If you would like additional information regarding these steps, please refer to Apple's website.

User Approved Kernel Extension Loading:
https://developer.apple.com/library/content/technotes/tn2459/_index.html
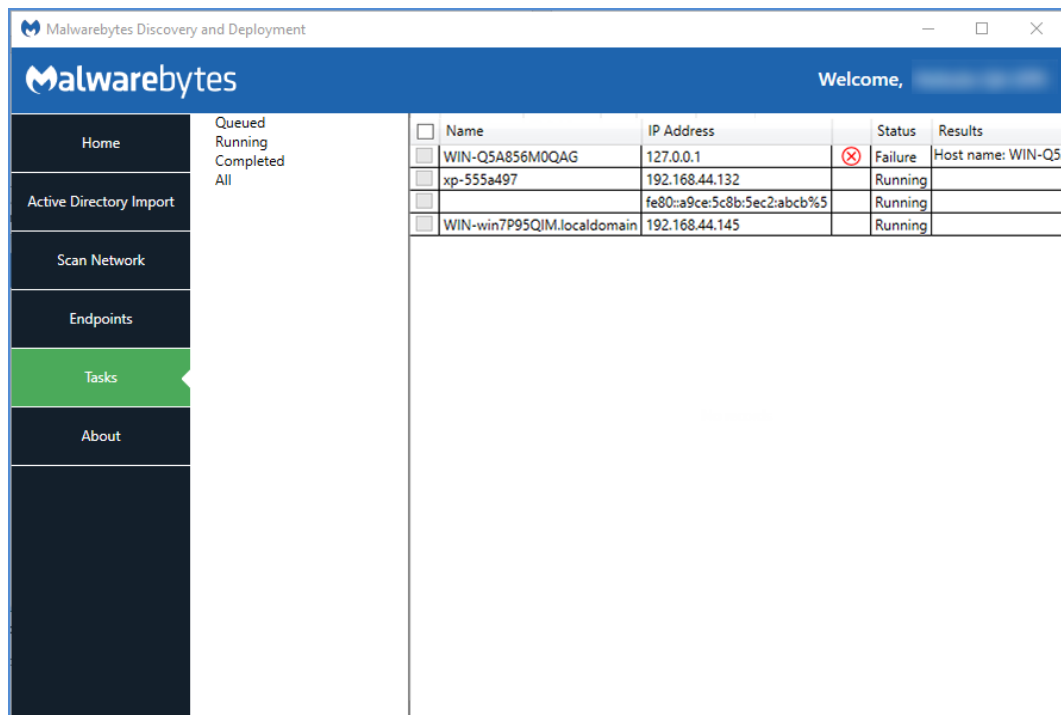
Kernel Extension Policy:
https://developer.apple.com/library/content/featuredarticles/iPhoneConfigurationProfileRef/Introduction/Introduction.html#//apple_ref/doc/uid/TP40010206-CH1-SW63

Create a NetBoot, NetInstall, or NetRestore image:
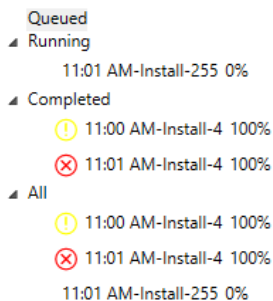https://support.apple.com/en-us/HT202770

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.

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.

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.
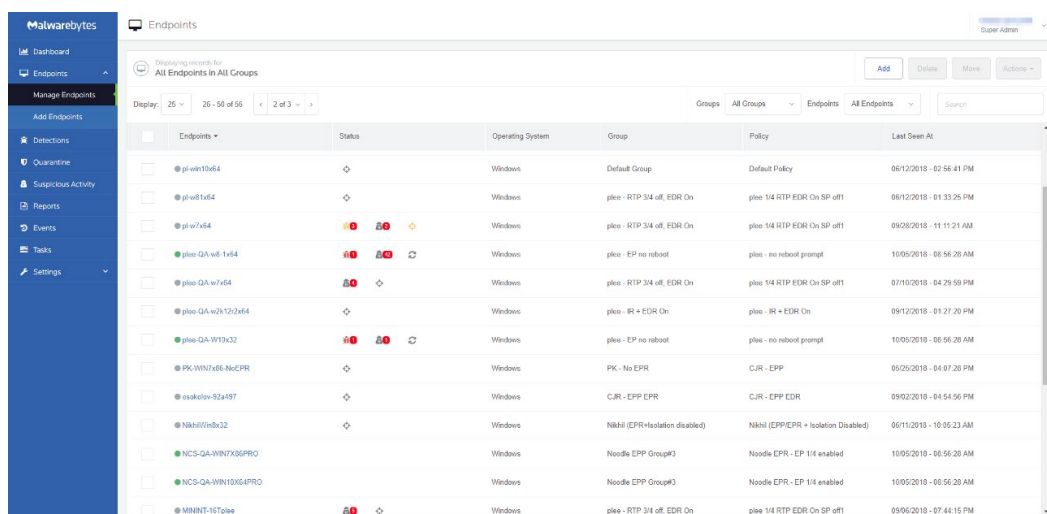
Special Installation Notes

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.
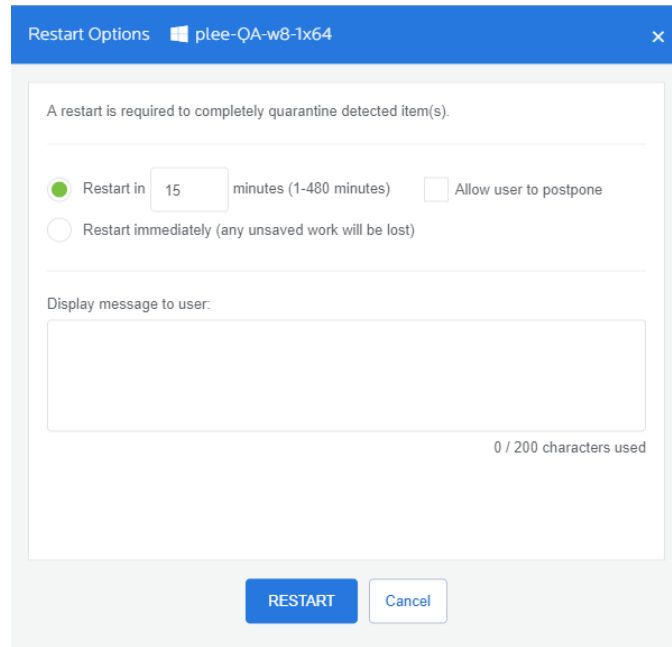
Endpoints

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**. The menu option will expand to show two options – Manage Endpoints and Add Endpoints. Click **Manage Endpoints**. A display will appear that is similar to the screenshot shown here.

In this screenshot, several groups have been added. The Status column shows icons to help quickly identify endpoints that need attention. The table below shows the different status icons that you may see while using the console, along with a brief description. In this example, some endpoints have unresolved suspicious activity, and some endpoints have been isolated. You may read more about these statuses in the Endpoint Protection and Response section of this guide.
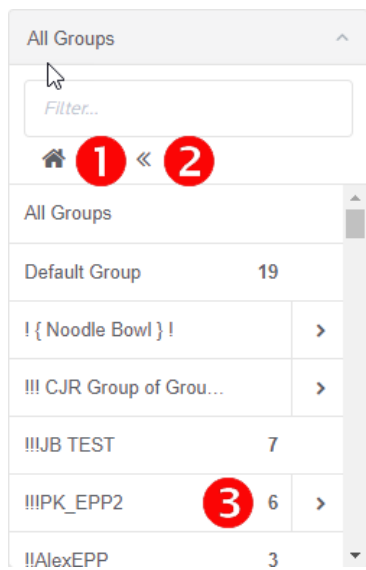
ICON	STATUS
	The endpoint has not run a *Malwarebytes* scan for a long period of time. A scan should be run to check for threats.
	A scan is pending on the endpoint.
	A scan is currently running on the endpoint.
	The endpoint has threats that were detected during a scan that need to be remediated.
	Remediation of threats is pending on the endpoint.
	The endpoint is actively undergoing remediation.
	The endpoint should be restarted to completely quarantine items found during a scan.
	A restart command was issued to the endpoint and is currently pending.
	The endpoint is restarting and the console is waiting for it to reconnect.
	Suspicious activity was detected on the endpoint. This is only available to *Endpoint Protection and Response* customers.
	The endpoint is currently isolated. This is only available to *Endpoint Protection and Response* customers.

You can click any icon to see additional details, or to take action on the endpoint. If a restart is required, you will see a prompt to enter additional parameters for the reboot. You can choose when the restart will occur, if the end user can postpone the reboot, and what message (if any) the end user will see.

The Manage Endpoints page allows you to show all endpoints, those that are online only, offline only, or offline for more than seven (7) days. 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 ❸ – is an example. Click on the arrow to view subgroups. At any point, child groups may be subdivided even further.

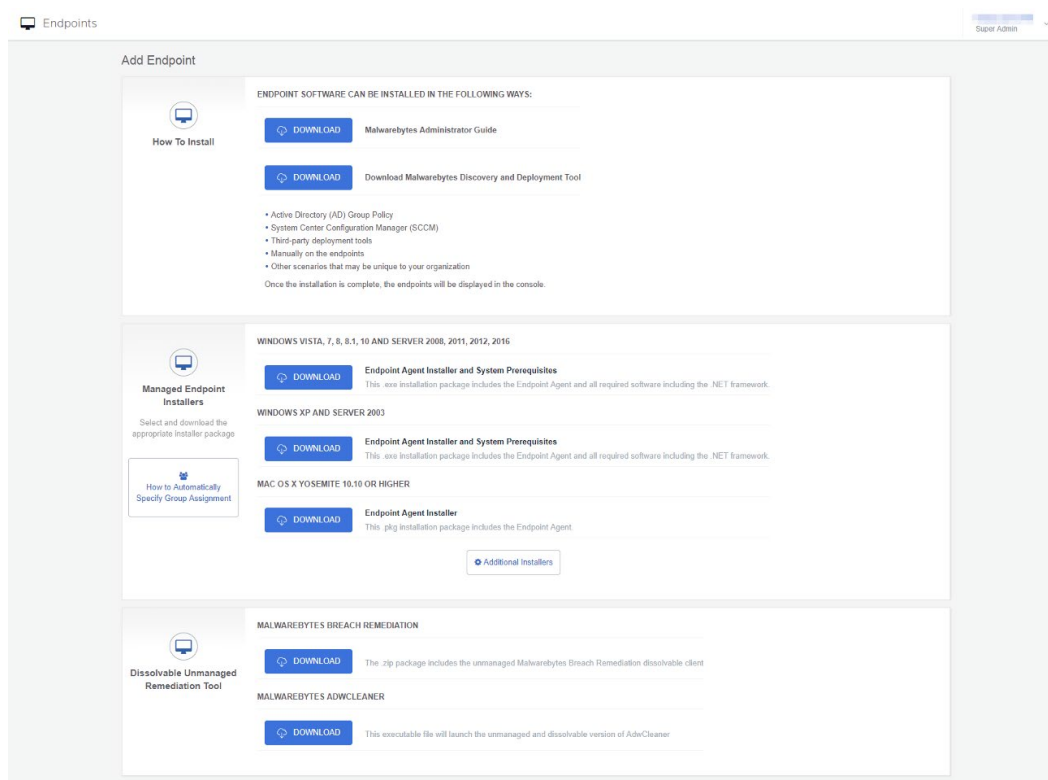The Home button – shown by ❶ – returns visibility to the All Groups level, regardless of your depth in the group tree.

The Back button – shown by ❷ – 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. They are:

Add

When this option is selected, a new screen opens with several options. You can also reach this screen by clicking **Add Endpoints** from the Platform Menu. Here, you may choose the most appropriate agent installer for your needs, the standalone *Breach Remediation* dissolvable client, or the *Discovery and Deployment Tool*. By providing installers in this manner, we enable you to use the installation method which you prefer. Please note that endpoints added in this manner are assigned to the Default Group and

associated with the Default Policy unless you specify a group. More information on that shortly. 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. <u>Please note</u> 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>`
           `GROUP=<group_ID>`

Five variables may be used in conjunction with this command. They are:

```
GROUP
NEBULA_PROXY_SERVER
NEBULA_PROXY_PORT
NEBULA_PROXY_USER
NEBULA_PROXY_PWD
```

If you would like to install endpoints via command line and have them join a specific Group, you must use the GROUP variable and provide the Group ID. To locate the Group ID, click the link titled **How to Automatically Specify Group Assignment** on the Add Endpoints page. A new window will open, showing you all of the groups available in your console. Next to each group is a string of characters, the Group ID. Click the button to the right to copy it to your clipboard. If the Group ID given in the command does not match any groups, the installer will add the endpoint to the Default Group and Default Policy.

The other four variables for the installer are for you to specify information for a proxy server. 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, dissolvable remediation program for Windows and Mac endpoints. There may be instances when its usage is more appropriate for your needs. You can download this application from this page by clicking **Download**. Documentation is included in the ZIP file.

We have also made our *Malwarebytes AdwCleaner* utility available to you on the same page. You can click **Download** to obtain the dissolvable executable. Documentation is available from the Malwarebytes website.

- 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 the endpoint applications as well as the agent which controls communications between the console and applications. To delete one or more endpoints, select those endpoints and click <u>Delete</u>. 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 <u>All Groups</u> 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.
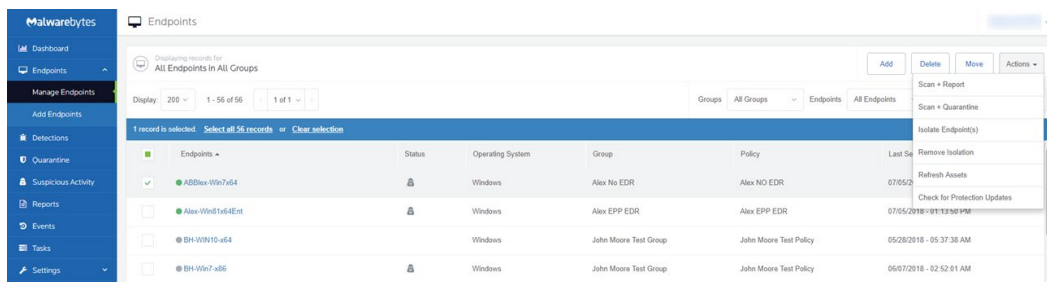
Move

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

After selecting one or more endpoints, you may perform one of the following actions:

- **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.
- **Isolate Endpoint(s) –** Isolate the endpoint(s) from your network environment to prevent an active threat from spreading. The Malwarebytes Console will continue to communicate with the endpoint. This action is described further in the *Endpoint Protection and Response* section of this guide.
- **Remove Isolation –** Restores access to the currently isolated endpoint(s). This action is described further in the *Endpoint Protection and Response* section of this guide.
- **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 <u>Actions</u> submenu, we have chosen to use the **Scan + Quarantine** option.
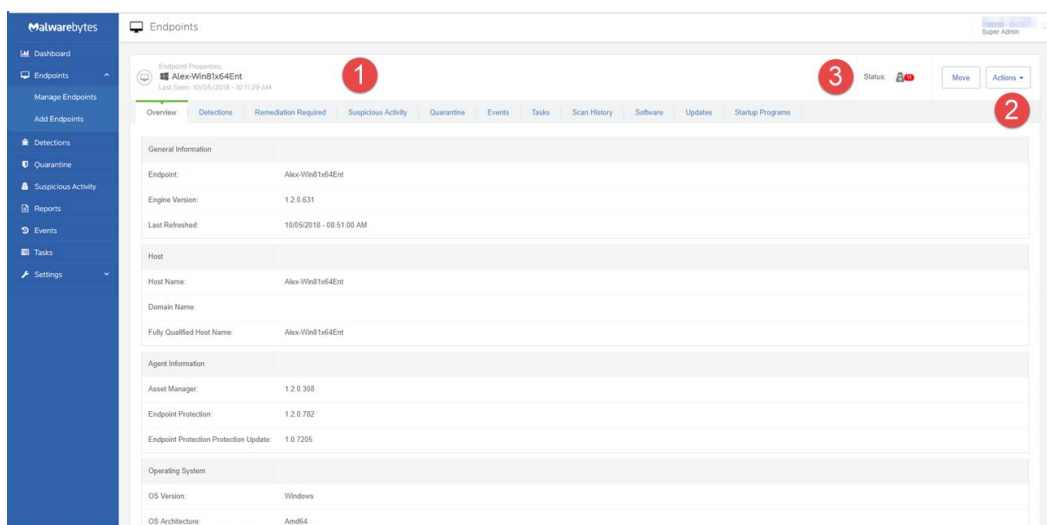
This results in execution of a scan on the selected endpoint. The amount of time required is dependent on the number of files to be scanned on the endpoint. If default policies are used, a Threat Scan will be executed. If malware is detected, it will be quarantined automatically, and a reboot may be 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.

Endpoint Details

Additional details for each endpoint can be viewed by clicking the name of an endpoint in the list. This will take you to a screen where you can view detailed information for the endpoint selected, shown below:

Details for the selected endpoint are shown in the center of the screen. You may click items shown in the list to see further information pertaining to the item. The tabs along the top of the screen can be used to view additional reports ❶. You can move the selected endpoint to a new group or run an on-demand scan from the upper right corner ❷. Available actions for you to take are shown as icons along the top ❸. You may return to the list of endpoints at any time using your browser's **Back** button.

Agent Information

This section of the endpoint details page contains valuable information about the version of Malwarebytes software on the selected endpoint. Depending on your policy settings, you will see the following items:

- **Engine Version:** The primary endpoint agent that is responsible for communicating between the endpoint and the cloud.
- **Asset Manager:** The endpoint plugin that collects the information for the Overview tab of Endpoint details.

- **Endpoint Protection:** The endpoint plugin that powers real-time protection from exploits, ransomware, and malware.
- **Endpoint Protection Protection Update:** The threat signatures and components that enable real-time protection. As a reminder, we employ both signature-based and signature-less technologies.
- **Endpoint Protection and Response:** The endpoint plugin that powers Suspicious Activity Monitoring and endpoint Rollback.

Groups

A group is a collection of endpoints. Initially there is a single group, called the Default Group. You cannot delete the Default Group. 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 19), 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.

Policies

A policy defines *Malwarebytes* behavior when running a scheduled scan, using Real-Time Protection, or monitoring Suspicious Activity. You can access policies by clicking **Settings ►Policies**. Initially there is a single policy, called the Default Policy. You cannot delete the Default Policy.

To create a new policy, click **New** in the upper right. A window will open. The top section of this window contains policy settings that apply to both Windows and Mac operating systems. The bottom half contains settings that are specific to the operating system selected at the time. We will begin by discussing the features shared by both operating systems.

Policy Information

Each policy must have a unique name. You can rename a policy at any time by editing the Policy Name field.

Endpoint Interface Options allow you to customize how your endpoint users see and interact with the *Malwarebytes* interface.
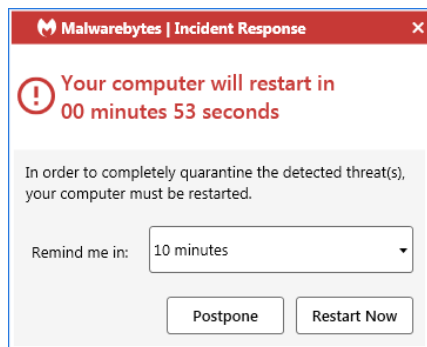
- **Show Malwarebytes icon in notification area** – Allows the endpoint user to see a Malwarebytes icon in the taskbar. Hovering over the icon also displays a very brief program status message.
- **User Threat Scan –** Allow endpoint users to run Threat Scans. No other scan types are available to the 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.
- **Threat Scan Shortcuts** – Creates Start Menu and desktop shortcuts for end-users on Windows endpoints. User Threat Scan must be enabled to enable this setting.
- **Show Malwarebytes option in context menus (Windows only)** – Allow endpoint users to scan individual files by right clicking them. Context menu scans share the same behavior as Threat Scans run by endpoint users.
- **Display real-time protection notifications** – Shows real-time notifications in the corner of your screen. These are only available if you have enabled Real-Time Protection.

Both Windows and Mac endpoints can use one policy. You can configure both General options and specific Settings for each Operating System independently.

General

These options are available to all endpoints. They will not change what threats *Malwarebytes* detects, but can improve your experience using the application.

Reboot Options control how *Malwarebytes* will handle requests to restart your endpoints. Remediation does not end with quarantine of the visible threat. Malware may leave behind remnants that can activate 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 restarts, 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 that displays to the endpoint user. Users will receive a notification 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, reboots may trigger due to installations, uninstallation and updates. Your choice for this setting applies to all of these processes.

Asset Management allows *Malwarebytes* to collect information regarding hardware and software from your endpoints. You can choose to collect all, some, or none of this data. This will not affect your use of *Malwarebytes*, but is available to you as a convenient way to help administrate your environment. Choosing to collect asset data from Windows endpoints does not influence data collected for Mac endpoints and vice versa.

Protection Updates 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. Endpoints will check for updates prior to running a scan as well.

Policy Settings

Here you can choose how to handle threats detected during scans to best suit your needs. You may also change specific behaviors for Real-Time Protection if you are a *Malwarebytes Endpoint Protection* subscriber. Some features are not available for Mac endpoints.

FEATURE	WINDOWS	MAC
Scheduled Scans	🟢	🟢
Manual Scans	🟢	🟢
Real-time Filesystem Protection	🟢	🟢
Malicious Website Blocking	🟢	🟥
Payload Analysis	🟢	🟥
Application Hardening	🟢	🟥
Application Behavior Protection	🟢	🟥
Exploit Mitigation	🟢	🟥
Anomaly Detection Machine Learning	🟢	🟥
Ransomware Mitigation	🟢	🟥
Suspicious Activity Monitoring	🟢	🟥
Endpoint Isolation	🟢	🟥
Rollback	🟢	🟥

KEY TO SYMBOLS	
🟢	Supported feature
🟥	Unsupported feature

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. These settings apply to Threat scans only:

- **Scan Rootkits:** Scans will search for rootkits. This may increase scan duration. The default setting is off.
- **Scan within Archives:** Scans will examine the contents of compressed folders. The default setting is on.
- **Anomalous File Detection:** Scans will utilize a signature-less detection method to check for file anomalies. The default setting is on.

These settings apply to Threat Scans, Hyper Scans, and Real-Time Protection events:

- **Potentially Unwanted Programs (PUPs):** Specifies whether PUPs will be treated as malware, or ignored.
- **Potentially Unwanted Modifications (PUMs):** Specifies whether PUMs will be treated as malware, or ignored. This is not applicable to Mac endpoints.

Scan Priority

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. Scans may impact the performance of lower-powered computers. This setting you to determine the priority of the scan on the system. Lower priority scans will require more time to execute while affecting 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.**

Endpoint Protection

The following is a description of the types of real-time protection offered by *Malwarebytes Endpoint Protection*. You should keep in mind that not all Real-Time Protection features are available for Mac, as described earlier on page 22. A *Malwarebytes Incident Response* subscription does not include these features. To use Real-Time Protection, you must enable it in a policy under the Policy Settings menu. When you enable a Real-Time Protection layer, the Endpoint Agent will install the Real-Time Protection Plugin for you. You do not need to redeploy or reinstall any software on your endpoints.

Policy Settings

You can choose to enable some or all of the protection layers in your policy. We advise using each layer to help protect your endpoints from threats at multiple points. However, your needs may vary and it is up to you to determine which layers are best for your environment. A description of each layer, along with any additional settings that apply to that layer, follows.
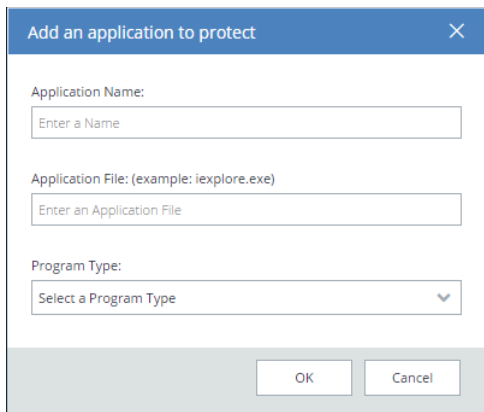
Web Protection

This layer 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

This layer 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 <u>on</u> by default.

Many popular applications have been pre-configured for shielding. A screenshot is shown above. You can change which applications are protected by clicking **Manage Protected Applications**. To change the status of any application, either use the <u>Protection</u> slider, or double click either the <u>Application</u> or <u>File Name</u>. You may add protection for other applications, and edit specifications for any defined shield. The Edit screen is shown here.
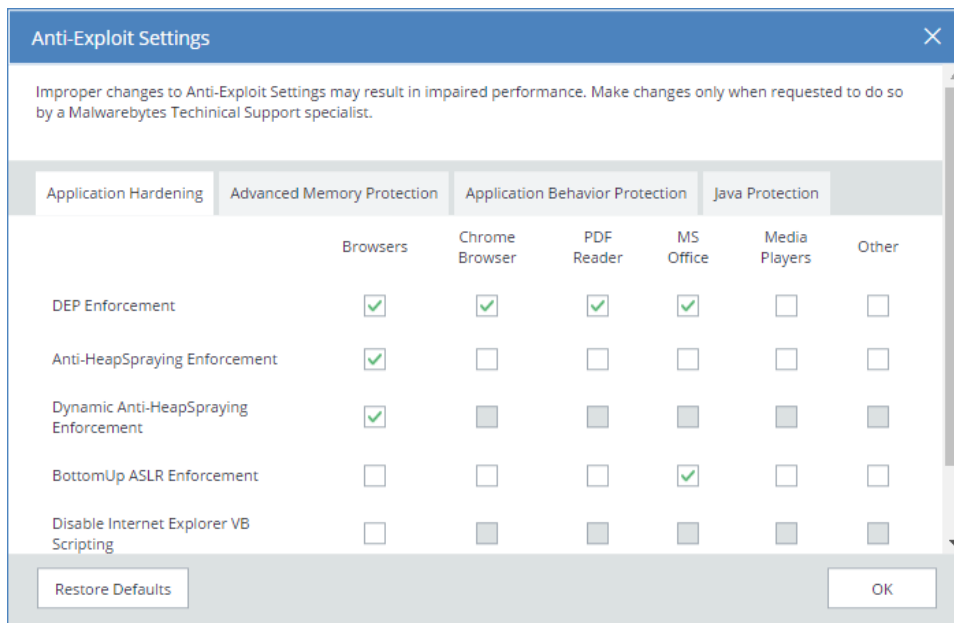
The Application Name can be the same as the Application File, or a more easily recognizable name. The Application File is the executable file you wish to protect. Select a Program Type which most closely resembles the purpose of the application. If you are unsure, select **Other**.

The same screen is used to edit existing entries.

Advanced Settings allows configuration or fine-tuning of some exploit mitigations. Please note that not all exploit mitigations can be modified here. The pre-defined defaults 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.
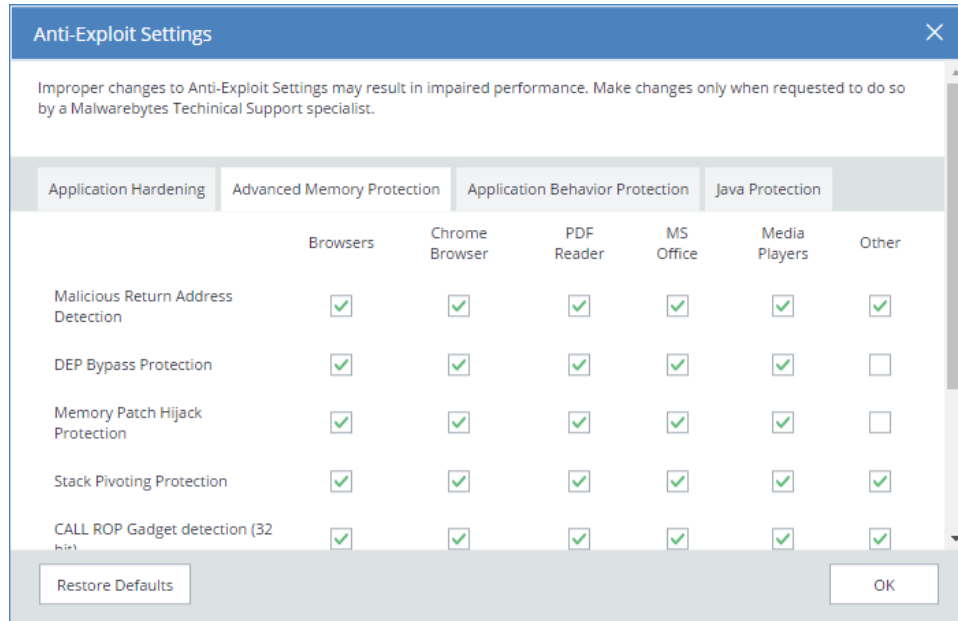
Settings on the **Application Hardening** tab refer to exploit mitigation techniques whose objective is to make protected applications more resilient against vulnerability exploit attacks, even if those applications have not been patched to the latest available fixes by their respective vendors. A screenshot shows the organization of the tab.

- **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.
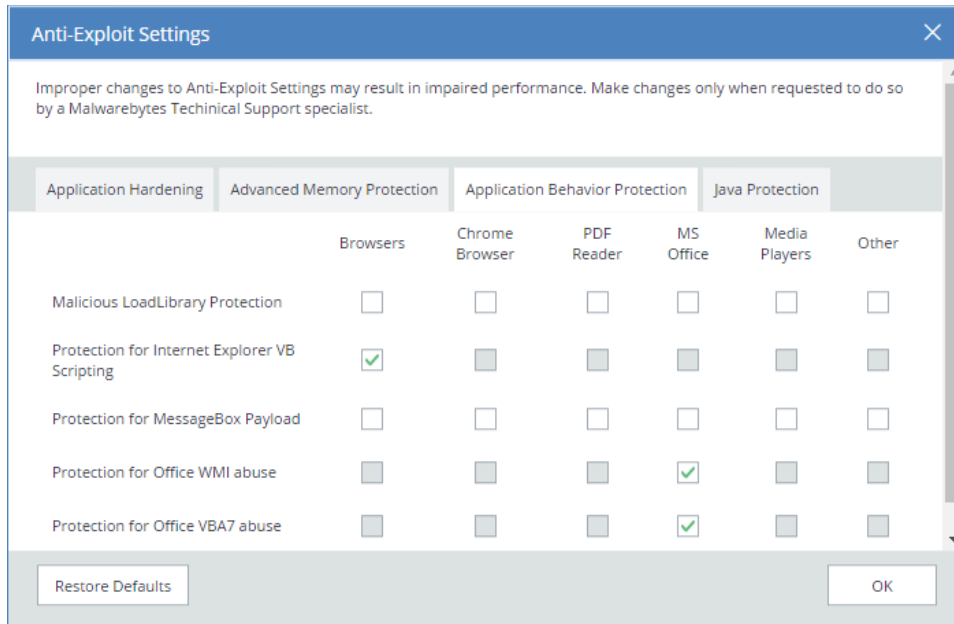
- **Disable Internet Explorer VB Scripting** is tasked with preventing the deprecated Visual Basic scripting engine from loading. The scripting engine is frequently abused by exploits. This setting applies only to the browser family.
- **Detection of Anti-Exploit fingerprinting attempts** is a technique 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

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. Malware Protection is <u>on</u> by default. 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. Malware Protection is always enabled on Macs with Real-Time Protection enabled.

Behavior Protection

This layer provides protection against both known and unknown ransomware threats. <u>This protection is not available for users of Windows XP or Windows Vista.</u> 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 <u>on</u> by default.

Startup Options

These settings define Real-Time Protection behavior when *Malwarebytes* starts.

- **Delay Real-Time Protection when *Malwarebytes* starts:** There may be times when Real-Time Protection services conflict with services required by other applications. When this is the case, turn this setting on. You may also adjust delay timing. You will need to experiment with the specific delay necessary to compensate for any conflicts that are noted. 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* 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 <u>Enable Self-Protection Module</u> is turned on.

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* can now be registered as the security solution on your computer. Windows Action Center integration is not supported for endpoints using a Server operating system. 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.

Suspicious Activity Monitoring

These features are available for subscribers to *Malwarebytes Endpoint Protection and Response.* We discuss them further on page 30.

Real-Time Protection Notifications

As a function of real-time protection, *Malwarebytes* 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 ► Policy Information**.

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

Endpoint Protection and Response

If you are a subscriber to *Malwarebytes Endpoint Protection and Response*, you can enable the <u>Suspicious Activity Monitoring</u> and <u>Endpoint Isolation</u> features and associated plugin. These features are only available for Windows endpoints running Windows 7 or higher. Suspicious Activity Monitoring is not available on Server operating systems, but you may enable Endpoint Isolation on servers using Server 2008 R2, Server 2012 R2, or Server 2016. If you enable this feature on your endpoints, *Malwarebytes* will monitor process, registry, file system, and network activity for behavior that could indicate a malware infection. The plugin logs the behavior and sends it to our servers to compare against an ever-growing list of malicious behaviors and patterns. If the activity on your endpoints matches a pattern that we have marked as suspicious, we will generate an alert in your *Malwarebytes* console. We label alerts for these items as <u>Suspicious Activity</u> to help you distinguish them from known malware detected by scans or real-time protection. These alerts are usually, but not always, indicative of a malware infection. To begin, you must enable Suspicious Activity Monitoring via your Policy.

Policy Settings

Suspicious Activity Monitoring is turned <u>off</u> by default. To use this feature, you must enable it in a Policy, as described on page 21. When you enable Suspicious Activity Monitoring, the Endpoint Agent will install the plugin for you. You do not need to redeploy or reinstall any software on your endpoints. If you turn this feature on, *Malwarebytes* will begin to analyze behavior from your endpoints to help detect potentially dangerous or anomalous files. You will have the option to roll back damage done by a threat, as well as to isolate endpoints from the rest of your network to help keep threats from spreading. Let's discuss these options now.

> **Please note.** To facilitate this analysis, Malwarebytes will leverage machine learning models as well as analysis from cloud systems. We recommend that you reserve 1.1Mbps (Megabits per second) of network traffic for every 100 endpoints you enable Suspicious Activity Monitoring on. This will help ensure optimal performance of the feature.
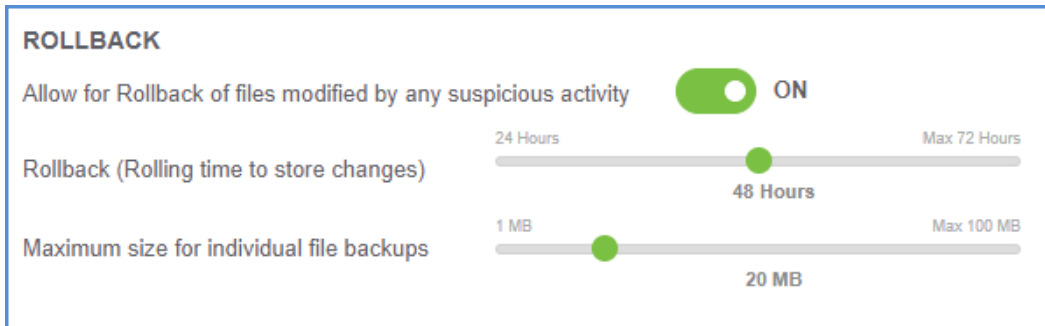
Aggressive Mode

Malwarebytes uses an advanced machine learning model to detect anomalous files via Suspicious Activity Monitoring. As files and processes run on your endpoints, any suspicious activity they perform is compared to a threshold. When a process performs enough suspicious activity to cross the threshold, *Malwarebytes* will take action. If you enable Aggressive Mode, *Malwarebytes* will adjust the model to lower the threshold for when a process is flagged as suspicious. Enabling this can help protect your systems against additional unknown threats, but you may see an increase in False Positives with this mode enabled. We advise that you only enable this setting for your most sensitive assets.

Rollback

This setting is available once you enable Suspicious Activity Monitoring. The Rollback feature is dependent on activity monitoring – you <u>must</u> enable monitoring to allow for Rollback. Once Rollback is enabled, *Malwarebytes* will create a local cache on the endpoint to store changes to files on the system. The application uses this cache to help revert changes caused by a threat. Endpoints typically use 200MB – 500MB for the cache, depending on usage and how you configure Rollback. Two options exist to customize Rollback in your environment. They are:

- **Rolling time to store changes –** This setting determines how long *Malwarebytes* will store information in the cache. Increasing this time will increase the size of the cache on your endpoints, as they will store any changes to the endpoint in the time window you specify. The default value is 48 hours.
- **Maximum size for individual file backups –** This setting controls which files are saved in cache based on size. The default setting is 20MB – meaning that any file larger than 20MB will not be saved in cache. Increasing the maximum file size will increase the size of the cache.

ROLLBACK

Allow for Rollback of files modified by any suspicious activity ⬤ ON

Rollback (Rolling time to store changes)
24 Hours   Max 72 Hours
48 Hours

Maximum size for individual file backups
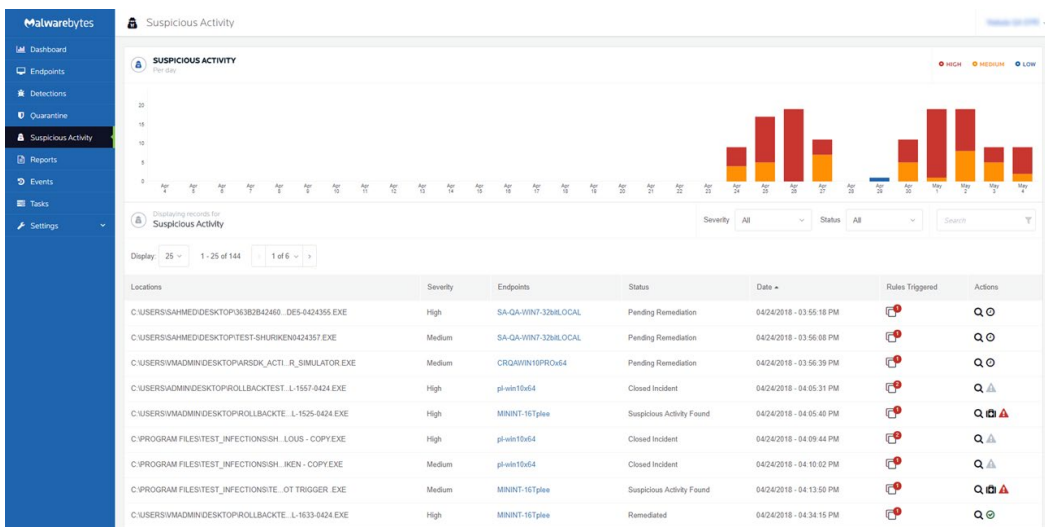1 MB   Max 100 MB
20 MB

By enabling Rollback, you allow *Malwarebytes* additional options to help recover damage caused by threats on your endpoints. In conjunction with our existing Malware Removal Engine, the Rollback Cache allows the Endpoint Agent to restore files that malware removed or encrypted.

Endpoint Isolation

You can enable Endpoint Isolation independently from <u>Suspicious Activity Monitoring</u> and <u>Rollback</u>. Once enabled, Endpoint Isolation allows you to temporarily prevent threats from spreading between network endpoints by restricting their communication or access. An isolated endpoint will always be able to communicate to the *Malwarebytes* server, and will always allow *Malwarebytes* processes to run. Details on how to perform isolation are in the following section of this guide.

Managing Suspicious Activity

Now that you have configured Suspicious Activity Monitoring, let's discuss how you can act on any activity that may appear. The central hub for you to access any Suspicious Activity can be found by clicking the <u>Suspicious Activity</u> tab from the left menu. Below is a screenshot of the Suspicious Activity menu.

The bar graph will display the number of activities detected, broken down by their severity. *Malwarebytes* automatically categorizes and assigns severity based on the nature of the behavior detected. The console will display the highest severity of any given process. If the endpoint plugin detects multiple behaviors from a process, you will need to open the activity details to see each of them. Each severity has an associated visual cue: low severity behaviors are blue, medium severity behaviors are yellow, and high severity behaviors are red. By default, the list of activities is sorted by Date. You can change the sort order by clicking the column headers. Not all columns are available for sorting.

Activity Details

When an endpoint detects suspicious activity, *Malwarebytes* will show the location of the originating process, the endpoint associated, the rules triggered, and the actions available. Clicking the endpoint name will bring you to the details page for that endpoint. Clicking the icon under *Rules Triggered* will bring you to a page with detailed information on the behaviors that the endpoint agent detected.

The page will show suspicious activities by their parent process ❶. Next to each parent process is a radio button – click this to see more information in the Process Graph, described on the following page. You can click the + to expand the parent process and show any child processes created ❷. Each child process will display the individual behaviors that *Malwarebytes* detected ❸. You can click any of these colored boxes to learn more about the behavior. If a process has a large number of behaviors associated with it, you will need to click the ellipses (•••) to the right of the screen ❹. If you click on any individual behavior, you will see a screen showing you more information. You can see what the endpoint detected and why it is suspicious. You also will see the specific context of the behavior from the endpoint.
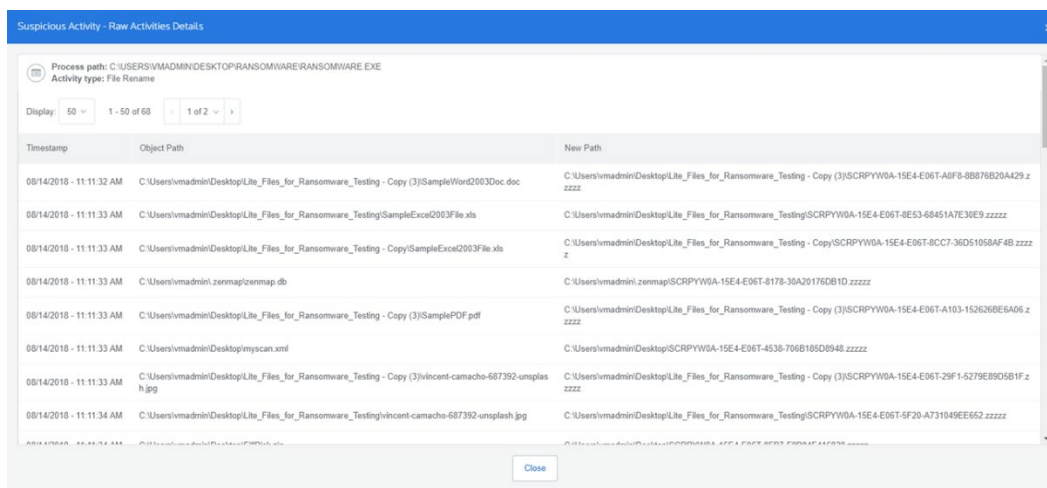
The context shown will depend on the suspicious behavior detected and the rule that behavior triggered. In the example shown, the process was detected because it launched a suspicious file. The context shows you the run command, as well as the file that was opened. Different rules will show different contextual information to help you understand the specific reason why *Malwarebytes* detected a process. If our Cloud Sandbox detected the process, you will see a list of all sandbox rules that the detection triggered.

Process Graph

When we detect suspicious behavior, it is often not clear what happened based off log data. The Process Graph helps provide additional context so you can understand what exactly a process did. This will help you better decide if the behavior is actually malicious, or just unusual. To begin, select the parent process of the activity you want to investigate further using the radio button to the left of the process name. The Process Graph will appear in the lower section of the screen.

The main display of the graph shows a visual representation of the process ❶. Child processes or injected processes will appear as new branches from the parent. Details on the parent process, including the process path, PID, and the total time the infection was left unresolved on the system, are shown above the graph ❷. If the graph has many processes, you can navigate with your mouse, or you can use the controls along the right side of the screen ❸. The controls allow you to zoom in/out, reposition the graph, or expand/collapse additional context. If you want to view additional details on a process, click the node to select it. Additional context and information will appear to the right ❹. This pane will show you additional details such as the command and switches used to launch the process. You can click the links under Activities ❺ to view specific file operation details.
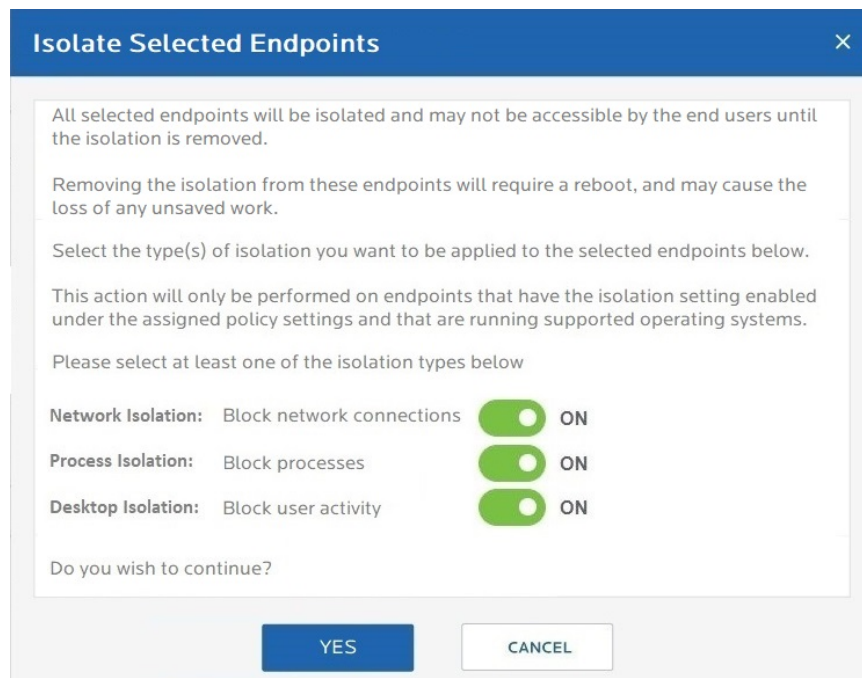

Endpoint Isolation

Before you can isolate an endpoint, *Malwarebytes* must run a Threat Scan on the system. This is necessary to install all of the plugins for the Endpoint Agent. We automatically run a Threat Scan on an endpoint when *Malwarebytes* is first installed, but you may decide to run a scan ahead of this. Once the scan finishes, you will be able to isolate the endpoint.

There are three different isolation modes – you can enable each mode separately, or you can combine them to create a more restrictive isolation. The three isolation types are:

- **Network Isolation:** Prevent the endpoint from communicating with other devices via your network.
- **Process Isolation:** Restrict which processes can run on the endpoint, and prevent processes from interacting.
- **Desktop Isolation:** Prevent end-users from accessing endpoint completely.

To isolate an endpoint, you must select the **Isolate Endpoint(s)** action from the Manage Endpoints page. For information on how to reach this menu, refer to page 18 in this guide. When you select the endpoint(s) to isolate, a prompt will appear asking you to confirm the level of isolation. You can specify the degree of isolation by toggling each layer individually. The default value is On for all three isolation methods.
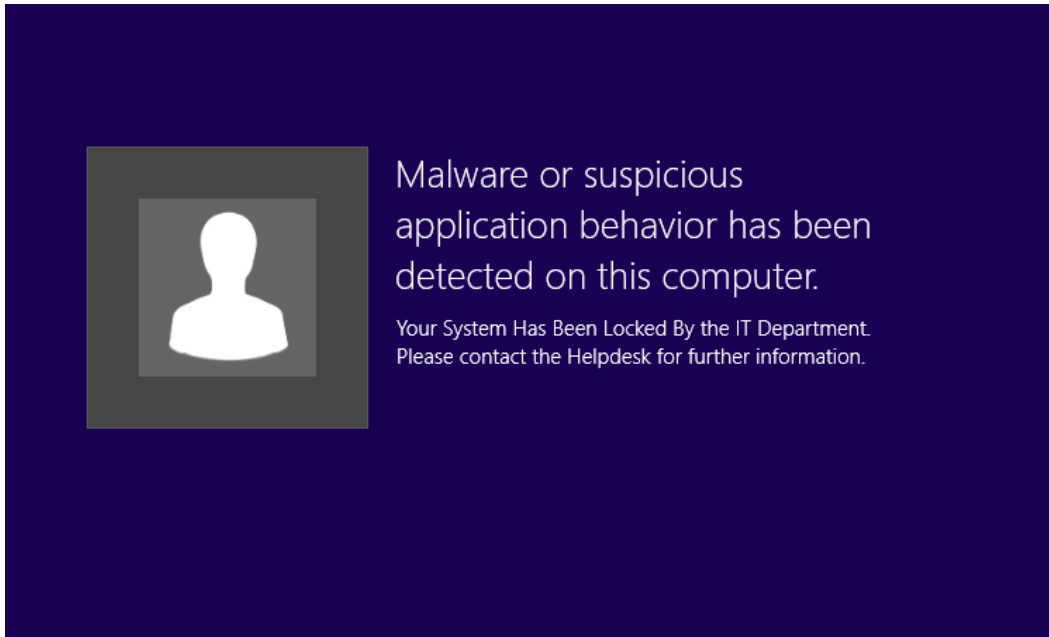

If you select multiple endpoints to isolate, and some of those endpoints are already isolated, then the isolation modes you apply will be cumulative. If for example you isolated an endpoint previously with Process Isolation, then later you attempt to isolate that endpoint (along with others) with Process Isolation and Network Isolation, the initial endpoint would have both isolation types active.

You cannot modify the isolation type of an individual endpoint. If you need to change the isolation type, you must either remove isolation entirely, or apply the isolation update as part of a group as described earlier. You can remove an endpoint from isolation using the **Remove Isolation** action from the Manage Endpoints page – this will require a reboot. You cannot remove individual isolation types from endpoints.

If you have enabled Process Isolation, only Privileged Processes are allowed to launch on the endpoint. Privileged Processes belong to one of the criteria below:

- Predefined (hardcoded) processes. Currently only two such processes are defined: CONSENT.exe, necessary to execute UAC elevated processes, and CSRSS.EXE which is a critical system process.
- Processes digitally signed by Malwarebytes. All such processes are allowed to run on isolated endpoints unrestricted.
- Processes spawned by other Privileged Processes. Any process with a Privileged parent process becomes Privileged itself. These processes can further create child processes which are privileged.

An example screenshot of what an end user will see on an endpoint with Desktop Isolation is shown on the following page.
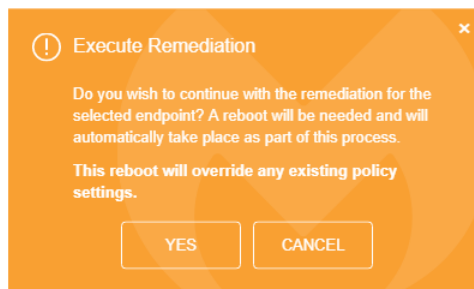
Rollback and Remediation

When you are ready to act on suspicious activity, you will see five potential icons for a threat. Let's discuss each of these.

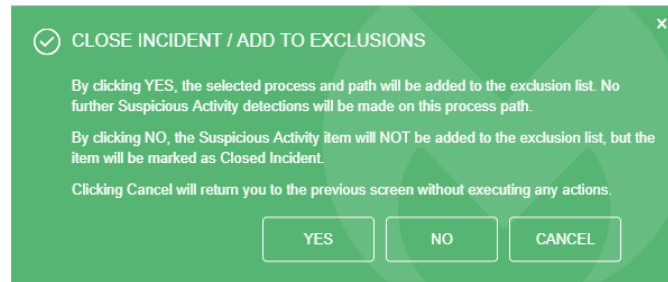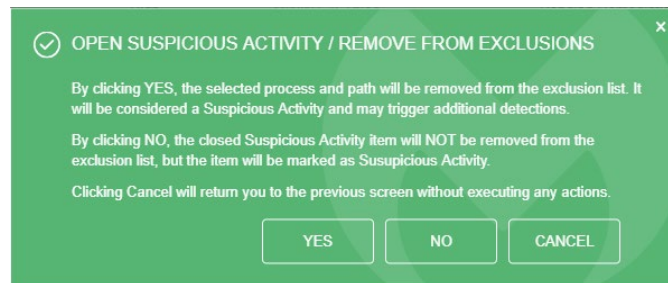|	
🔍	This icon will take you to the list of Rules Triggered as described earlier.

🧰	This icon initiates remediation on the endpoint. *Malwarebytes* will analyze suspicious activity, then combine our Malware Removal Engine and Rollback cache to remove remaining threats and restore files which the threat removed or encrypted. If you have not enabled the Rollback cache in your policy, you may not be able to restore all files. The endpoint will reboot automatically to finish remediation, which could result in the loss of any unsaved work. You can perform remediation on an isolated endpoint.
	
	In some situations, *Malwarebytes* may not be able to restore all files. If this occurs, you can manually attempt to restore files from the endpoint. Files will be stored in the folder:
	
	`%PROGRAMDATA%\Malwarebytes Endpoint Agent\Plugins\EDRPlugin`
	`    \Restored Files`
	
	Malwarebytes will create several folders inside this directory that are associated with the attempted rollback. These folders will contain subfolders with the username of the Windows account the files originated from, if the program was able to record it. There is no guarantee a particular file will be recoverable using this method.

	These icons appear after you send a remediation request to an endpoint. The first icon indicates that the endpoint has a scheduled remediation task which has not yet finished. The second icon appears once the remediation task finishes.
	This icon allows you to mark the suspicious activity as closed if you elect not to perform remediation. Most likely, you would use this in the case of a False Positive. As *Malwarebytes* analyzes behavior of a process, a non-malicious file may appear to be suspicious. This is not an indication that the file is harmful, but instead that it behaves in a suspicious manner. When you mark an activity as closed, you will see a prompt asking if you want to add the process to your Exclusions list. If you do this, *Malwarebytes* will not flag future behavior from this process. If you choose not to add the process as an exclusion, the single activity will be marked as closed, but you may see future events from the same process.
	This icon will only appear for an activity previously marked as closed. Clicking on the icon will allow you to re-open the activity, and remove the process from the Exclusions list. You can choose to re-open an activity but to leave it in the Exclusions list.

Settings

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

Policies

Policies define the behavior of the *Malwarebytes Endpoint Agent*. For information on configuring and using policies, refer to the **Policies** chapter, starting on page 21 of this guide.

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 that 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 <u>Scan</u> or an <u>Asset Inventory Scan</u>, 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.

Exclusions

You may find that exclusions are needed to provide satisfactory performance in your environment. They may be needed if antivirus and anti-malware products interfere with each other's performance. They may also be needed if a trusted application or data file is being flagged as a false pos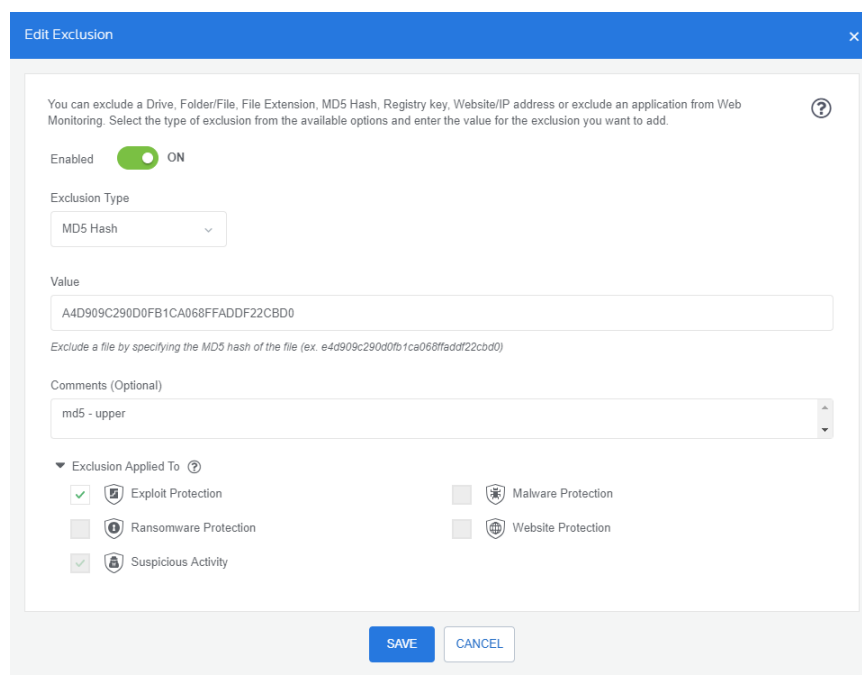itive–being seen as a threat when you know that it is not. Creating exclusions for these items helps to provide the best performance. You can access Exclusions by clicking **Settings ►Exclusions**. The screenshot below shows an example of the Exclusions page.

Each exclusion can be toggled on or off, should you need to temporarily allow a previously excluded item. In the upper right, a toggle is available to **Automatically exclude registry keys detected as PUMs due to common Group Policy Objects.** The list of which registry keys are excluded is available by hovering on the help icon. There are several types of exclusions you can add to *Malwarebytes*. These are listed below, along with examples. When you add an exclusion, we will automatically apply the exclusion to protection layers based on the type of exclusion you choose. If you want to customize what layers the exclusion is for, click **Exclusion Applied To** to expand the list. Note that not all exclusion types can be applied to all layers.

Some exclusions support wildcards. To exclude multiple entries with a common component in their name, use asterisk (*) and question mark (?) wildcards. The * matches any number of any character; the ? matches any single character.

Exclusion Type	Technology	Example(s)
File by Path	Malware Protection Ransomware Protection	C:\Windows\Foo\Bar.exe
Folder by Path	Malware Protection Ransomware Protection	C:\Windows\temp\
File/Folder with Wildcard†	Malware Protection Ransomware Protection	C:\Users*\Documents* C:\Users*\Desktop\test*.exe C:\temp\test?.exe C:\temp*.exe
File Extension	Malware Protection	doc pdf
MD5 Hash	Anti-Exploit	e4d909c290d0fb1ca068ffaddf22cbd0 9e107d9d372bb6826bd81d3542a419d6
Registry Key	Malware Protection	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Foobar
Registry Key with Wildcard††	Malware Protection	HKU*\Software\Microsoft\Windows\CurrentVersion\Policies\Associations|*
Web Monitoring	Website Protection	C:\Windows\Zoom\Zoom.exe
Website/IP Address	Website Protection	www.malwarebytes.com 234.213.143.154 2001:4860:4860::8888

† Ransomware Protection exclusions do not support wildcards.

†† 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>*.`

Groups

Groups are used to join several endpoints into one functional area, allowing you to apply manage them simultaneously with one Policy. For information on Groups, refer to page 19 of this guide.
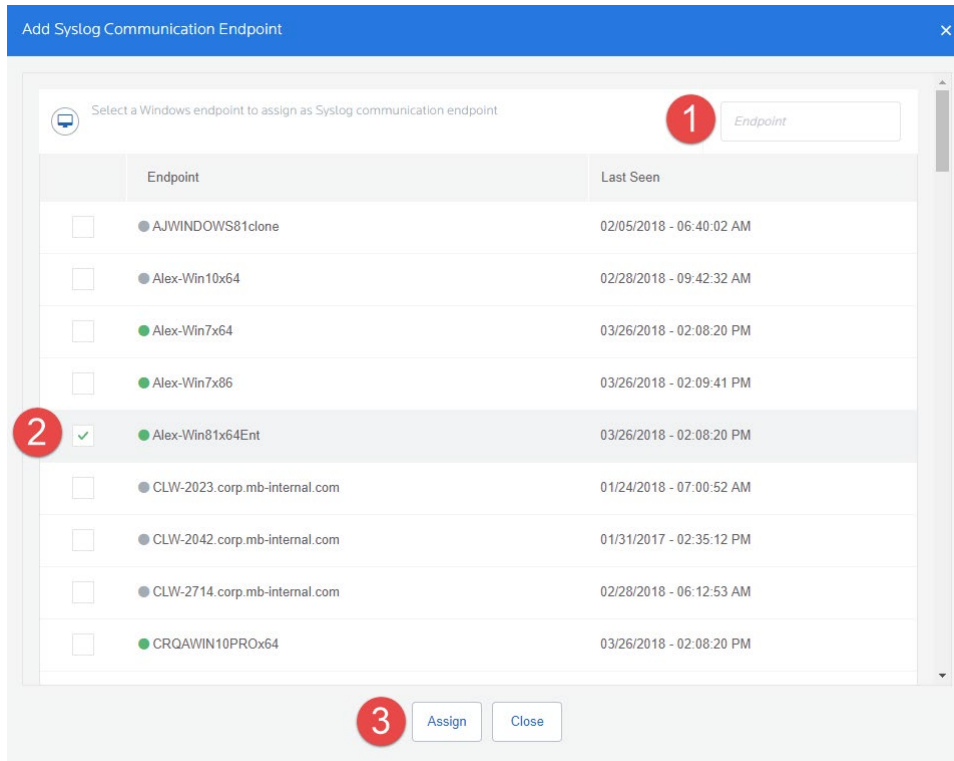
Users

For information on how to manage your existing users, or how to invite new users, refer to page 5 of this guide.

Syslog Logging

In addition to the reporting available in the application, you can export data from *Malwarebytes* to a Syslog server. To do so, you must promote an existing endpoint to act as an intermediary between the Malwarebytes server and your Syslog server. We refer to this endpoint as the Syslog Communication Endpoint. The first step in this process is to configure your Syslog server settings. Go to **Settings ► Syslog Logging** and click **Add** to begin. You will see a screen that looks like this. You will need to provide the information for your Syslog server. These settings will apply to your entire *Malwarebytes* account.

- **IP Address/Host:** The address of your Syslog server.
- **Port:** The port you have specified on your Syslog server.
- **Protocol:** You may choose to use either TCP or UDP protocol.
- **Severity:** This setting determines the Severity of *Malwarebytes* events in Syslog. All events sent to Syslog will use the same Severity.
- **Log Format:** This field is informational only. All logs are sent in CEF format.
- **Communication Interval (Minutes):** The value entered in this field determines how often the Communication Endpoint will gather Syslog data from the *Malwarebytes* server. If the endpoint is unable to contact Malwarebytes, we will buffer data from the last 24 hours. Data older than 24 hours ago will not be sent to Syslog.

Once you have entered the information for your Syslog server, click **Save.** You will now choose an endpoint to promote as the Communication Endpoint. You must choose a Windows endpoint that has the *Malwarebytes* agent installed. Mac endpoints are not available to promote as the Communication Endpoint. You may scroll to find the endpoint, or search for it by name in the upper right ❶. Select the endpoint you want to promote ❷, and then click **Assign** ❸. A confirmation window will appear. Click **Yes** to promote the endpoint and return to the settings page.

You have now configured your Syslog server and your Communication Endpoint. The endpoint will now begin to transfer data to Syslog automatically – there is no additional configuration needed on the endpoint. You can change the settings for your Syslog server by clicking **Syslog Settings**. If you need to use a different endpoint as the Communication Endpoint, you must first click **Remove** to demote the existing endpoint. Then, you can promote a new endpoint by clicking **Add**. You can temporarily demote the Communication Endpoint using the **On/Off** toggle on this page. This is a useful option when troubleshooting your Syslog settings.

Single Sign-On

If your organization uses a Single Sign-On (SSO) provider, you can connect it to *Malwarebytes* from this menu option. The first time you open this menu page, the feature is turned off. Click the **On/Off** toggle to begin. Now that you have enabled SSO, you will need to connect *Malwarebytes* to your provider.

Your SSO tool should be able to generate an XML file to integrate with new platforms. If you are unsure of how to do this, you should contact your SSO provider. Once you have the XML file from your SSO, you can drag it into the *Malwarebytes* console to begin upload. If you need to change which SSO tool *Malwarebytes* connects to in the future, you can upload a new XML file at any time.

Now that you have entered the metadata from your SSO into *Malwarebytes*, you will need to enter similar metadata from *Malwarebytes* into your SSO. Scroll further down the page to the section titled Malwarebytes Service Provider Details. Click the first item in the list, **Service Provider Metadata**. This hyperlink will download an XML file for you to upload to your SSO tool to complete the connection. The other items in this section provide information for you to manually enter into your SSO tool, if necessary. If your SSO does not require any manual entry, you can ignore these items.

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:
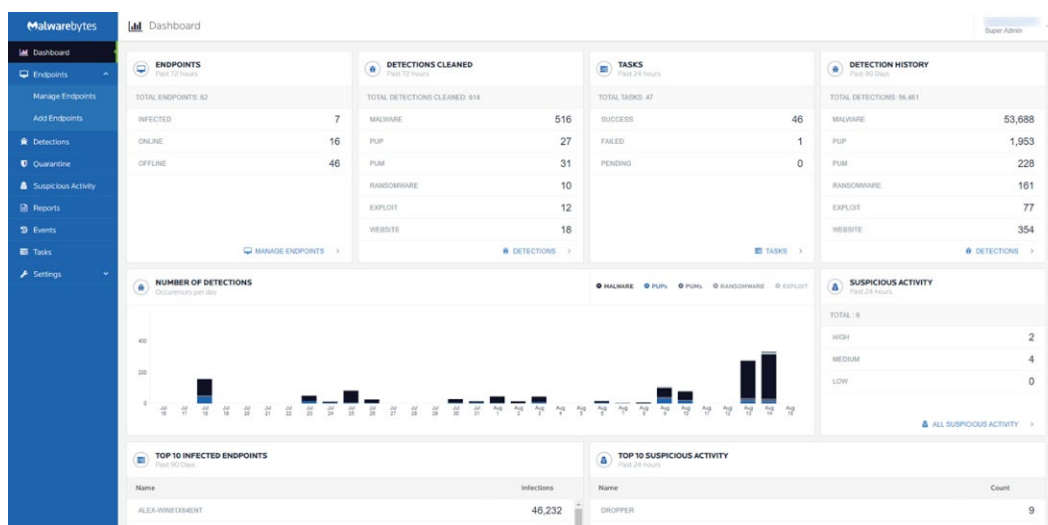
- Dashboard
- Threats
- Quarantine

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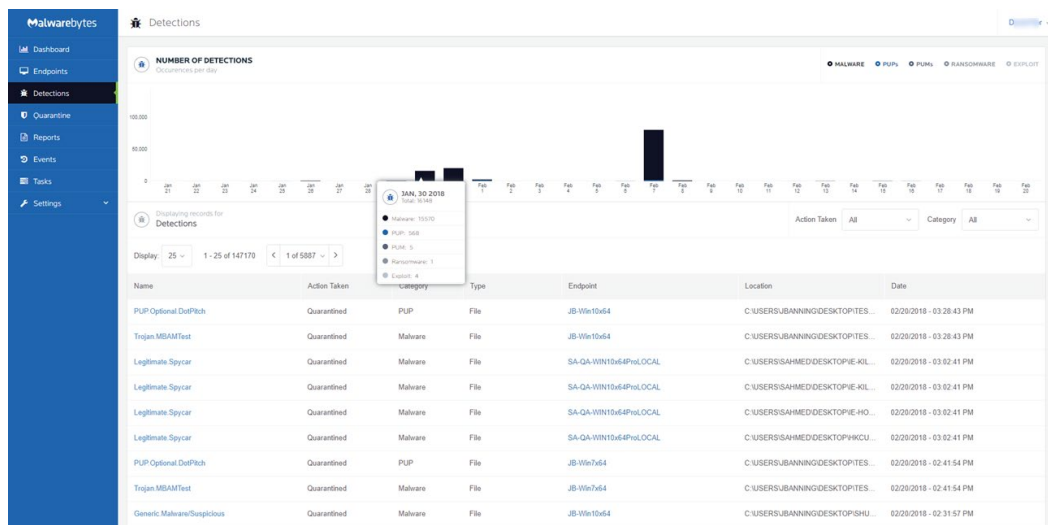
- Number of endpoints online, offline, and infected (both online and offline) over the most recent 72 hours
- Threats cleaned during the past 72 hours, broken down by Malware, PUP, PUM, Ransomware, Exploits, and Websites
- Tasks issued by the Malwarebytes console over the past 24 hours, broken down by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

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, divided into pages. You may navigate between pages, or change how many items are shown on each page, using the controls at the left center region of the screen. 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.

Action Taken defines the current status of detected threats. One description you may find curious is *Cleaned Offline*. That describes threats which were deleted from Quarantine manually, rather than under program control.

Category is the type of threat which was detected.

Selecting subsets allows you to "remove the noise" and focus on the information you are most concerned with.

Quarantine

A quarantined threat is one that *Malwarebytes* has 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 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 assume that the contents of Quarantine are malicious, nor should you assume that they are safe.

Mac endpoints using Real-Time Protection handle quarantine differently. Threats are not encrypted, and are moved to a different folder. They will be stored here:

```
/Library/Application Support/Malwarebytes/NCEP/Quarantine/
```

You may restore quarantined threats on Mac endpoints by moving the file from Quarantine to the original location. This action must be done on the endpoint, and is not available from the console.

Suspicious Activity

This tab displays a report of all Suspicious Activity detected on your endpoints. Suspicious Activity Monitoring is only available if you are a subscriber to M*alwarebytes Endpoint Protection and Response*. For more information on using this tab and feature, refer to the Endpoint Protection and Response chapter, starting on page 29 of this guide.

Reports

This tab allows you to generate reports that summarize details covering the previous day, week or month. Reports are available On-Demand or can be scheduled at regular intervals. The following report types are available:

- Detection Summary
- Quarantine Summary

- Endpoint Summary
- Asset Summary

- Events Summary
- Tasks Summary

These reports are provided in a Comma Separated Values (CSV) file format. Once an On-Demand 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. All scheduled reports are generated at the times specified below.

- **Daily Reports** – Every 24 hours at 05:00 UTC
- **Weekly Reports –** Every Saturday at 05:00 UTC
- **Monthly Reports** – The last day of every month at 05:00 UTC

Scheduled reports are delivered once they have finished generating. There may be a slight delay based on the size of the queue. 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.
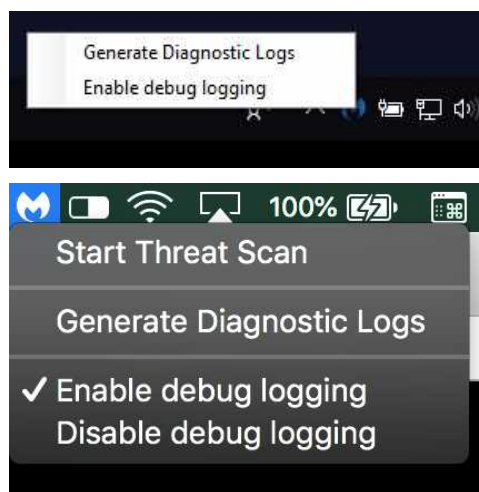
Appendices

The following sections are supplementary to the rest of this guide. You may not need the information within, but it is provided for your benefit. These appendices are shown to give additional examples to some functionality and tools provided with *Malwarebytes.*

Appendix 1: Enable Debug Logging

There may be times when working with our Customer Support team that you need to enable Debug Logging on your endpoints. Debug logging is a more detailed log level that helps when troubleshooting. You can enable Debug logging on both Windows and Mac endpoints. You can enable Debug Logging in two ways; from the tray icon for the Endpoint Agent, or from a Command Line.

To enable Debug Logging from a single endpoint, right-click the *Malwarebytes* icon in the tray/Mac Menu while holding the CTRL key. From the menu, click **Enable Debug Logging**. You can disable the logging by following these steps again.

If you need to enable Debug Logging without having to be physically present at each endpoint, you can do so with the following commands. These examples assume the default installation directory – you will need to modify the path if you have specified a different installation folder.

Windows

`MBCloudEA.exe -loglevel=debug`	Enable Debug Logging
`MBCloudEA.exe -loglevel=info`	Disable Debug Logging

Mac

`EndpointAgentDaemon -logging=debug`	Enable Debug Logging
`EndpointAgentDaemon -logging=info`	Disable Debug Logging

Appendix 2: Example Syslog Entry

An example of a Syslog entry generated by *Malwarebytes* is included here, ithe raw CEF format. Following the raw format, we have expanded the values for the Syslog prefixes, CEF Headers, and Extensions used.

```
2018-04-13T21:06:05Z MININT-16Tjdoe CEF:0|Malwarebytes|Malwarebytes Endpoint
Protection|Endpoint Protection 1.2.0.719|Detection|Website
blocked|1|deviceExternalId=e150291a2b2513b9fd67941ab1135afa41111111 dvchost=MININT-16Tjdoe
deviceDnsDomain=jdoeTest.local dvcmac=00:0C:29:33:C6:6A dvc=192.168.2.100 rt=Apr 13 2018
21:05:56 Z fileType=OutboundConnection cat=Website act=blocked msg=Website blocked\nProcess
name: C:\Users\vmadmin\Desktop\test.exe filePath=drivinfosproduits.info(81.171.14.67:49846)
cs1Label=Detection name cs1=Malicious Websites
```

Syslog Prefix:	Description	Example(s)
Timestamp	Time of recorded event	2018-04-13T21:06:05Z
Host	Affected endpoint	MININT-16Tjdoe

CEF Header:		
Version	Version of the CEF format	CEF:0
Device Vendor	This will always be Malwarebytes	Malwarebytes
Device Product	Plugin installed on endpoint at time of event	Malwarebytes Endpoint Protection Malwarebytes Incident Response Malwarebytes Endpoint Protection and Response
Device Version	Plugin name and version	Endpoint Protection 1.2.0.719
Device Event Class ID	Type of event reported	Detection
Name	Category of event and action taken	Website blocked
Severity	Severity set in Syslong settings	1

Extension:		
deviceExternalId	Unique identifier of device generating event	e150291a2b2513b9fd67941ab1135afa41111111
dvchost	Device hostname	MININT-16Tjdoe
deviceDnsDomain	Device's DNS domain name	jdoeTest.local
dvcmac	Device's MAC address	00:0C:29:33:C6:6A
dvc	Device's IPv4 address	192.168.2.100
rt	Date/Time when the event occurred	Apr 13 2018 21:05:56 Z
filetype	Type of file that caused event	OutboundConnection File Module Process Registry Value Exploit
Cat	Category of the Event	Malware PUP PUM Ransomware Exploit Website

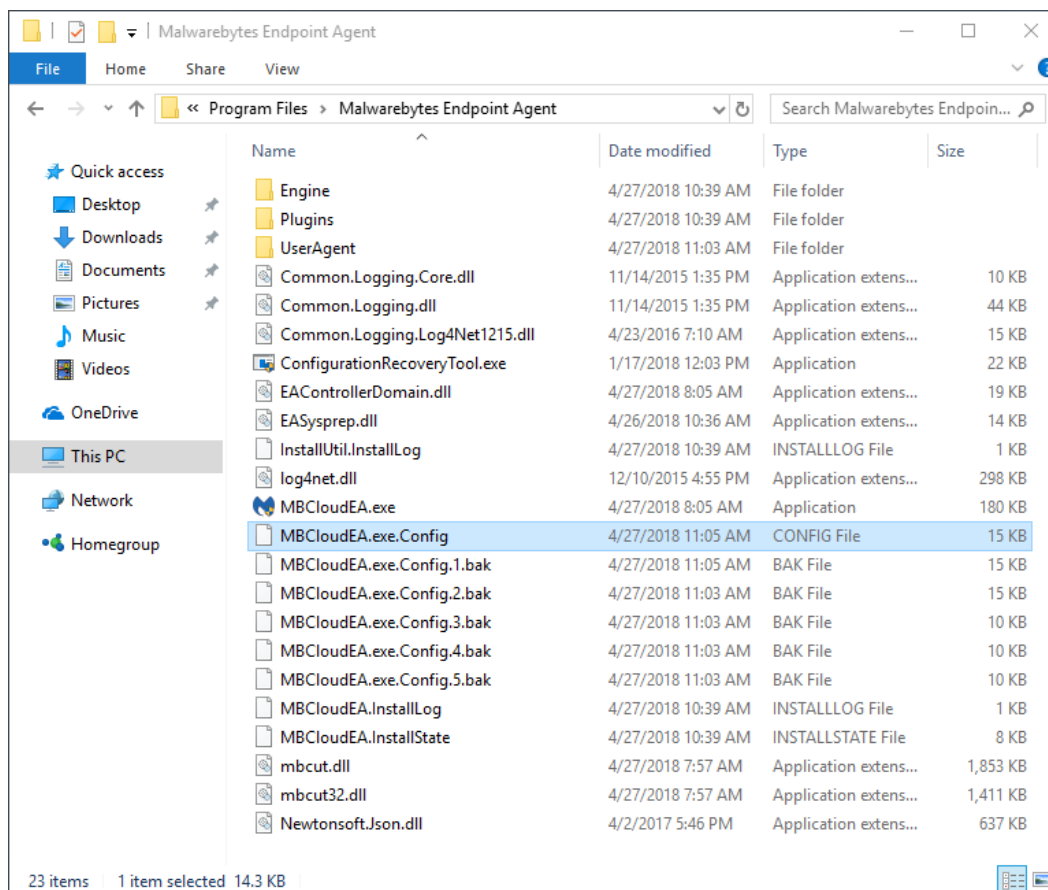| Extension: (continued)	Description	Example(s)
Act	Action Taken	blocked found quarantined deleted restored
Msg	Details of the system event	Website blocked\nProcess name: C:\Users\vmadmin\Desktop\test.exe
filePath	Path to the file, or blocked website domain	drivinfosproduits.info(81.171.14.67:49846) C:\users\vmadmin\Desktop\test.exe
cs1Label	The name label for the field cs1	Detection name
cs1	The detection name	Malicious Websites

Appendix 3: Configuration Recovery Tool

The *Malwarebytes* Endpoint Agent stores certain settings for operation in a configuration file, `MBCloudEA.exe.config`. This file is saved in the same directory as the Endpoint Agent executable. For the sake of this guide, we will use one installation directory example. Your installation directory may be different based on your environment. The directory we will use is:

`C:\Program Files\Malwarebytes Endpoint Agent\`

Occasionally the configuration file can become corrupted, for instance if a PC lost power while saving a setting to the file. The Endpoint Agent service is unable to start if this happens. To combat this, *Malwarebytes* will automatically create backups of the configuration file that you can restore using the Configuration Recovery Tool.

On initialization, the Endpoint agent creates up to five backups of the configuration file. The Configuration Recovery Tool will use one of these backups to restore a corrupted `MBCloudEA.exe.config` file. The newest file will have the lowest number. These files are stored in the same directory as the configuration file. An example is shown below.

The aptly named `ConfigurationRecoveryTool.exe` is located in the same directory as the configuration file and its backups. You will need to run the Recovery Tool from an elevated Administrator level command prompt. The tool will try to load the current configuration file – if it is successful, it will report that it does not need to replace the file. If the tool fails to load the configuration file, it will attempt to restore and load the most recent backup. If the backup fails to load, the recovery tool will repeat the process using the next oldest backup file. The recovery tool continues this process until it has either successfully restored a backup or has failed to restore all existing backups. If the tool is unable to restore from any of the backups, it will display a message to inform you that no valid backups were available. In this scenario, you will need to either restore the configuration manually or reinstall the endpoint.

Usage

To use the Configuration Recovery Tool, open an elevated command prompt and navigate to the Endpoint Agent installation directory. You must then run the tool with the following command:
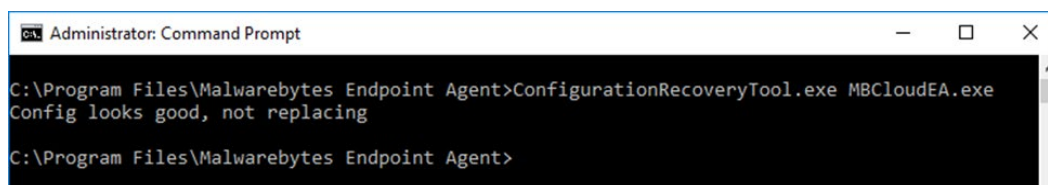
```
ConfigurationRecoveryTool.exe [path to exe] [Optional path to backup folder]
```

Two parameters are available to use with the Recovery Tool. If you do not enter any parameters, the tool will show examples of their usage. The parameters are:

- **[path to exe]** is the name of the executable that the configuration file you are restoring was created for. For the Malwarebytes Endpoint Agent, this will be **MBCloudEA.exe.**
- **[Optional Path to backup folder]** allows you to provide a specific directory containing backups. If you do not provide this parameter, the tool will attempt to recovery the configuration file using the backups in the current directory.
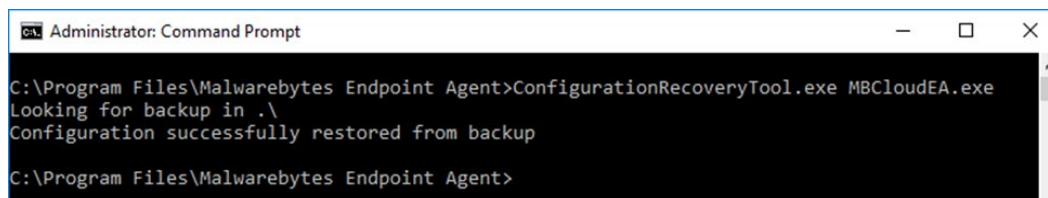
After the Recovery tool finishes running, there are three possible outcomes.

- **Configuration file loads successfully:** If the tool successfully loaded the configuration file with no corruption. No replacement occurred and the tool will automatically exit.
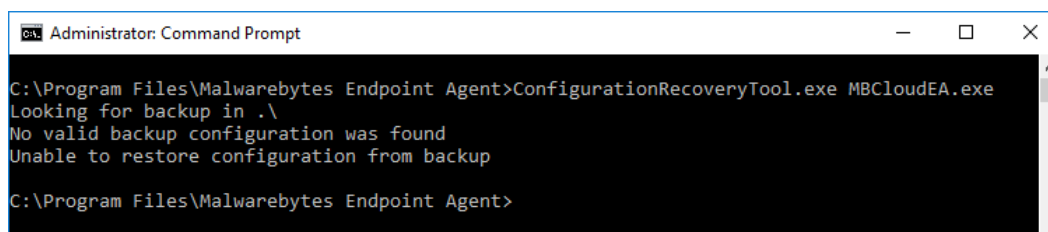

- **Configuration file is corrupt and there is a valid backup:** The configuration file was corrupted and the tool successfully replaced it with an existing backup.

- **Configuration file is corrupt and there is no valid backup:** The configuration file was corrupted and the tool was unable to restore an existing backup. You will need to either restore a backup from a different path, or reinstall the endpoint.

Appendix 4: 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 9 ("*Scan Network*") 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**}.

-proxyssl

> 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**. If no action is specified, the proxy settings are not applied.

-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.