Malwarebytes | CLOUD

Cloud-based Management Platform
Quick Start Guide

Version 1.0

24 April 2017

Malwarebytes

Notices

Third Party Project Usage

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

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

Sample Code in Documentation

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.

Table of Contents

Laying the Groundwork

The *Malwarebytes* cloud platform is comprised of several components designed to enhance the security of your network, your endpoints, and your users. The purpose of this Quick Start Guide is to help you get started using the *Malwarebytes* cloud platform. Please note that this guide is designed specifically for a Malwarebytes managed solution. Users of standalone products should consult administrator guides for those products.

Introduction

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

- ***Malwarebytes cloud console*** – This web-based centralized management tool is responsible for discovery, deployment, management and administration of Malwarebytes agents on your company's endpoints. This console eliminates the need to dedicate web servers and database servers for management of your endpoint data integrity, and provides scalability for any size organization.
- ***Incident Response agent*** – This client is designed to quickly detect and remove both malware and adware from Windows-based endpoints. Small in size, it can be easily deployed by the Malwarebytes cloud platform, Malwarebytes Discovery and Deployment Tool, Active Directory Group Policies, Microsoft SCCM, or a comparable tool of your choice.

System Documentation

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

- Cloud Quick Start Guide
- Discovery and Deployment Tool User Guide

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.

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://telemetry.malwarebytes.com	Port 443	outbound
https://data-cdn.mbamupdates.com	Port 443	outbound
https://data-cdn-static.mbamupdates.com	Port 443	outbound
https://keystone.mwbsys.com	Port 443	outbound
https://keystone-akamai.mwbsys.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

Basic Environment

Following and 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)
  - 800x600 screen resolution
  - Active Internet connection
- Operating Systems (Windows)
  - Windows Server 2012/2012 R2†
  - Windows Small Business Server 2011
  - Windows Server 2008/2008 R2†
  - Windows Server 2003 (32-bit only)
  - Windows 10
  - Windows 8.1
  - Windows 8
  - Windows 7
  - Windows Vista
  - Windows XP with SP3 (32-bit only)

    † Excludes Server Core installation option

Additional Software

The Microsoft .net application framework is required for endpoint functionality. Windows XP/Server 2003 requires Version 4, while version 4.5 is used for all other supported versions of Windows. If not present, it is installed as part of the agent installation.

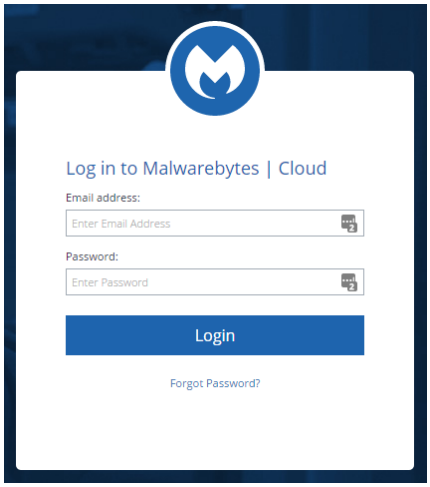
Creating an Account

Access to the *Malwarebytes* cloud platform comes to the administrator in the form of an "invitation" email sent by Malwarebytes following the purchase of a subscription. Accepting that invitation began the process of creating your account, using your email address as the login name. You must then provide your first and last names, then create and confirm your password. Finally, accept the terms of the End User License Agreement (EULA) and click **Submit**.

Enter your first and last 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 then login to the *Malwarebytes* cloud platform login screen (https://cloud.malwarebytes.com). You may wish to create a bookmark for this URL to simplify access.



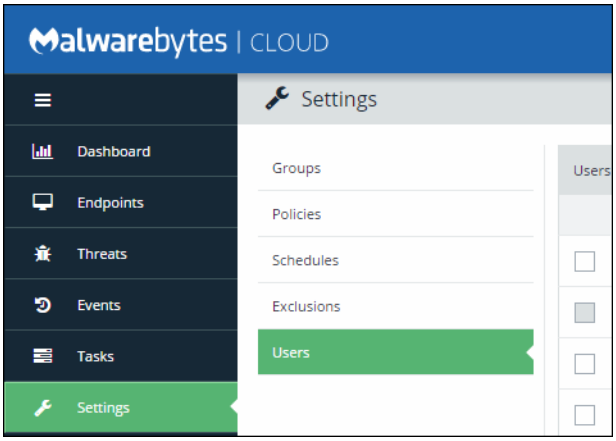
Adding a New User

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

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

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

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



Adding a New Endpoint

There are several methods of adding endpoints, one which has several variations. Let's start with the easy one!

Using the Discovery & Deployment Tool

The Discovery & Deployment Tool is designed to scan your network based on criteria which you specify, and identify networked devices which may be suitable for agent deployment. It will also identify 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 are used to provide an accurate snapshot of information relevant to deployment. Once target endpoints have been identified, you may select them and begin the deployment process. The tool will access Malwarebytes servers to obtain the newest MSI installer package and then perform the deployment.

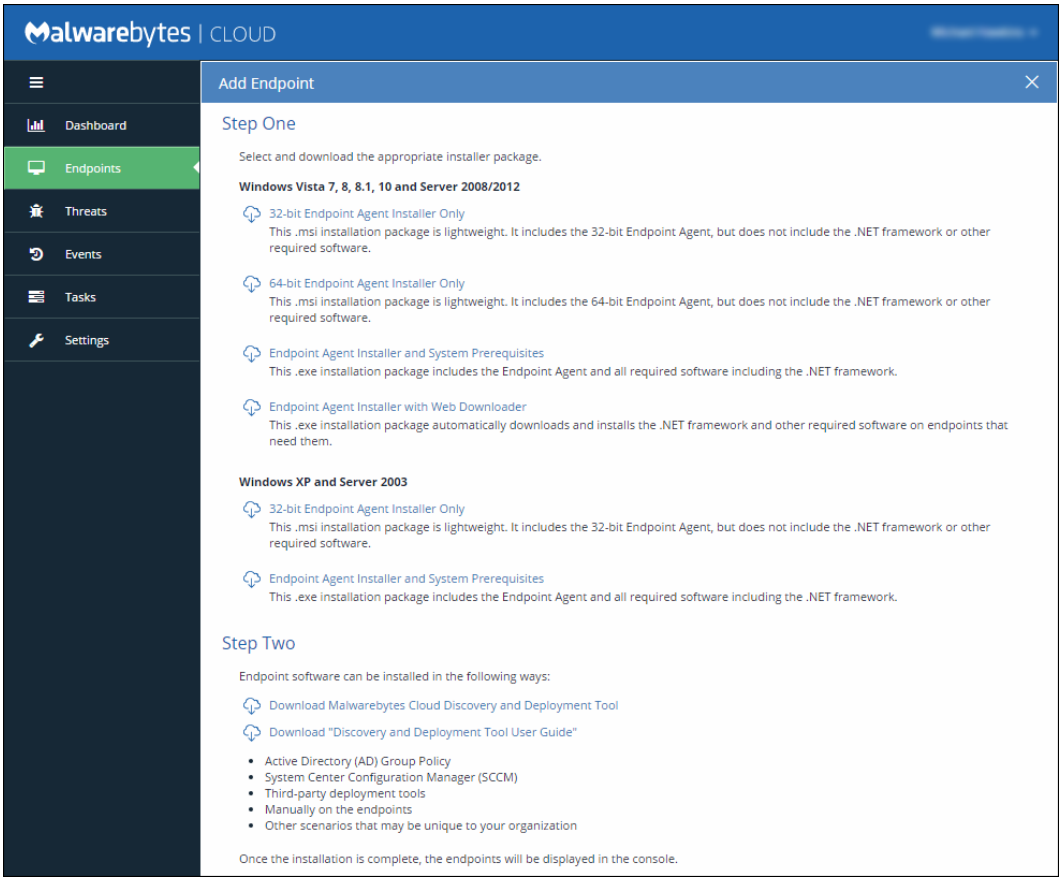
For complete information on this tool, please refer to the *Discovery and Deployment Tool User Guide*.

Do It Yourself Installers

Many companies have their own preference as to how software is deployed on their endpoints. These may include:

- Microsoft Active Directory (AD) Group Policy
- Microsoft System Center Configuration Manager (SCCM)
- Third-party deployment tools
- Manual installation
- Company-specific methods

We recognize the value of these methods, and have created installers which are designed for use by these methods. The following screenshot outlines various options. There are separate installers for Windows XP and Windows Server 2003, due to the older architecture present in the operating system kernels.



Creating New Policies

Once agents have been installed, you can begin creating the building blocks that will respond to attacks in your environment. The first block is **policies**. Policies are assigned to groups of endpoints, and define agent behavior on those computers. Every user-configurable setting for installed Malwarebytes agents (*Incident Response* and *Asset Management*) can be specified. You can (and should) create multiple policies, because your endpoints and your users are not "one size fits all." They have differing remediation needs, and the combination of groups and policies helps assure effective detection and remediation.

You can find these settings in **Settings ► Policies**.

► **HINT:** Before setting up policies and groups, take time to consider the needs of your users and their endpoints.

Creating New Groups

As mentioned in the last section, a **group** is a collection of endpoints. Each group is associated with a policy that defines the behavior of Malwarebytes agents on those endpoints. Only one policy can be assigned to a group, so it is up to the administrator to determine the best usage of both policies and groups. You may elect to group endpoints by department, facility, user type or degree of exposure to threats. It is completely up to you.

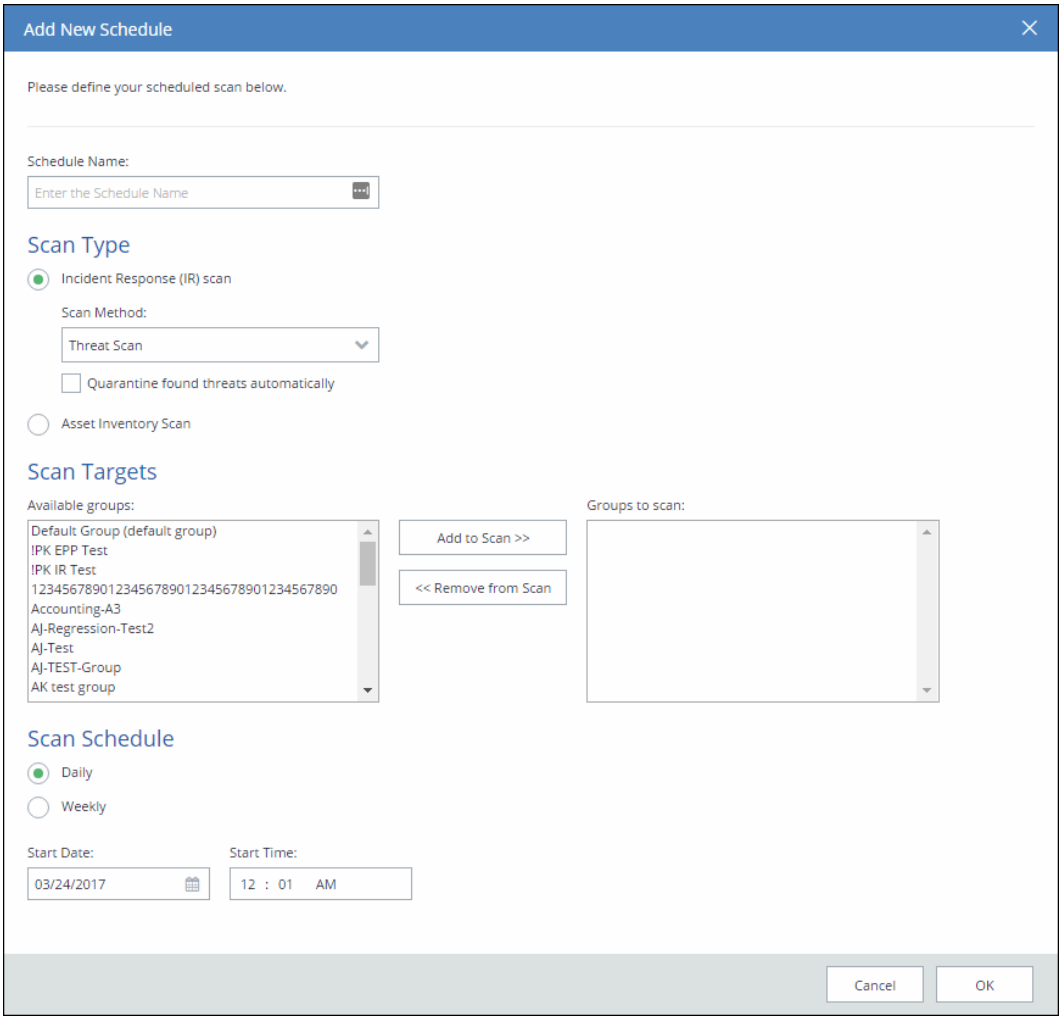
You can find this in **Settings ► Groups**.

Creating Schedules

The last building block for daily Malwarebytes cloud platform use is Schedules. You can choose the type of scan, which endpoints the scan is executed on, and when the scan should be executed. There are four types of scans available to you:

- **Incident Response Hyper Scan –** Scans only running operating system processes, drivers, applications and startup objects. This scan executes very quickly.
- **Incident Response Threat Scan –** Scans memory, disk, registry, running processes and startup objects in areas commonly used for delivering malware. Heuristic analysis is also included to identify zero-day threats. This is the most common Malwarebytes scan due to its effectiveness. This scan executes quickly.
- **Incident Response Custom Scan –** Scans the endpoint according to your specifications. This is the only scan method that will scan selected file paths, as well as scan for rootkits. This scan may take significant time to execute depending on scan specs.
- **Asset Inventory Scan –** Reports on endpoint hardware and software as specified in **Settings ► Policies ► Asset Management**.

Scan Targets allows you to specify groups that will be part of the scan, and **Scan Schedule** allows you to set up a Daily or Weekly scan, and specify the start date and time. You can find this in **Settings ►Schedules**. Because this is where everything comes together, a screenshot is in order.



Creating Exclusions

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

You may exclude files, folders, file extensions and registry keys. Wildcards (as used in Microsoft Windows) are accepted, anywhere in the text string that defines the exclusion.

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

Running a Scan

The previous three sections have defined the pre-requisites for recurring scans. Everything mentioned up to this point has been a pre-requisite for the ability to run a scan, both scheduled and on-demand. There are two other methods which you may use to run an on-demand scan. A few different scan types are available to you. They are:

- **Scan + Report:** A Threat Scan followed by a report of detected malware. No threats are removed by this scan method.
- **Scan + Quarantine:** Also a Threat Scan, but any threats detected during the scan are quarantined, preventing them from doing any damage to your endpoint.
- **Refresh Assets:** This performs an Asset Inventory Scan reflecting current status of the endpoint.

The first is to navigate to **Endpoints ► <selected Group>**, and select one or more endpoints using the checkbox preceding the endpoint name. Then, under **Actions**, select the desired scan type. The second method – also from that same screen – is to select an endpoint by clicking on the endpoint name. A number of information screens are available to you, allowing inspection of many aspects of the endpoint and its protection history, all on their own screen. Each of those screens contains a **Related Tasks** button at the bottom right, and all of the scan types mentioned above are available here.