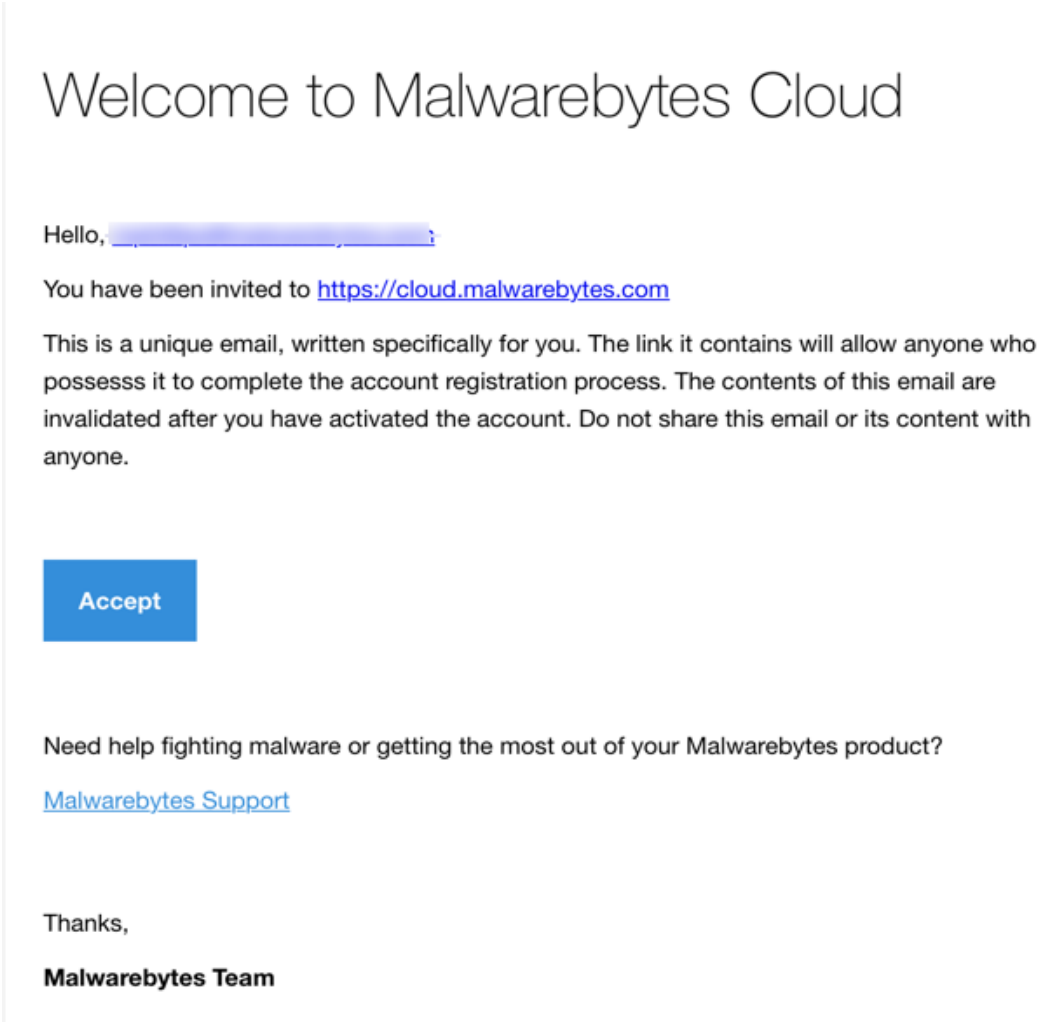
Malwarebytes Incident Response Quick Start Guide for LGFL

This is a quick start guide intended for users of Malwarebytes Incident Response offered by LGFL. This guide contains some useful first steps to get you up and running and successfully deploy your first few agents without much effort.

For a more comprehensive administration guide, please download it from here
https://www.malwarebytes.com/pdf/guides/MalwarebytesAdministratorGuide.pdf

Account Creation

To setup your account at cloud.malwarebytes.com look out for an email from no-reply@malwarebytes.com. You may need to check your clutter, SPAM or junk folders.



Welcome to Malwarebytes Cloud

Hello,

You have been invited to https://cloud.malwarebytes.com

This is a unique email, written specifically for you. The link it contains will allow anyone who possesss it to complete the account registration process. The contents of this email are invalidated after you have activated the account. Do not share this email or its content with anyone.

Accept

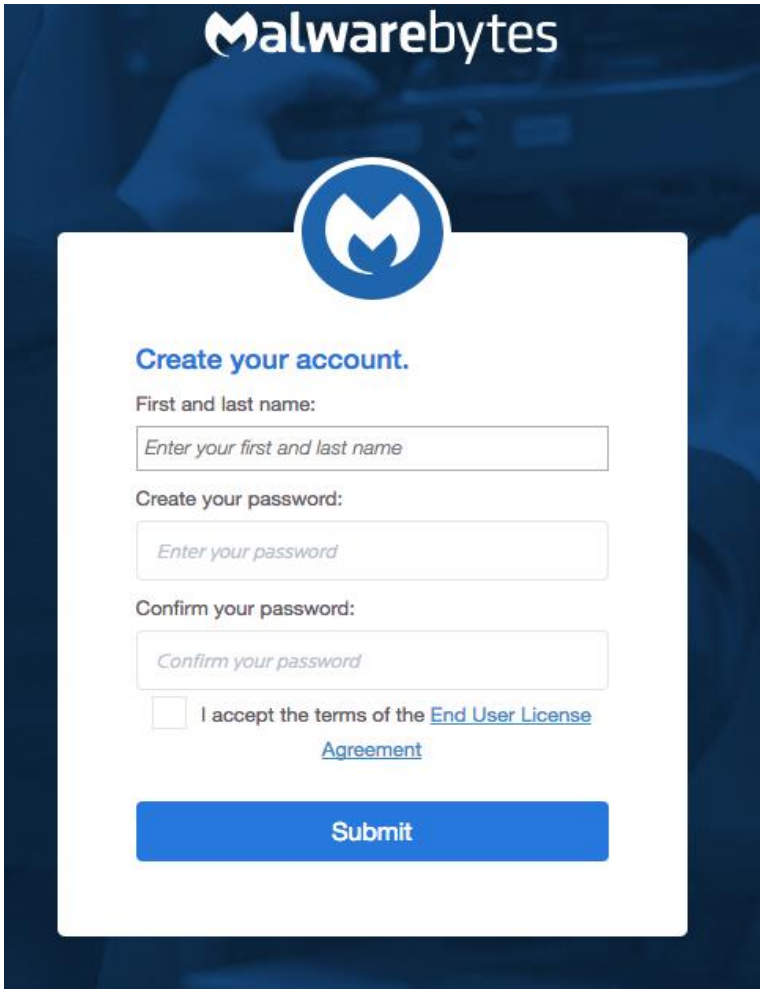
Need help fighting malware or getting the most out of your Malwarebytes product?

Malwarebytes Support

Thanks,

Malwarebytes Team

Click the “Accept” button and it will take you to the screen you see below



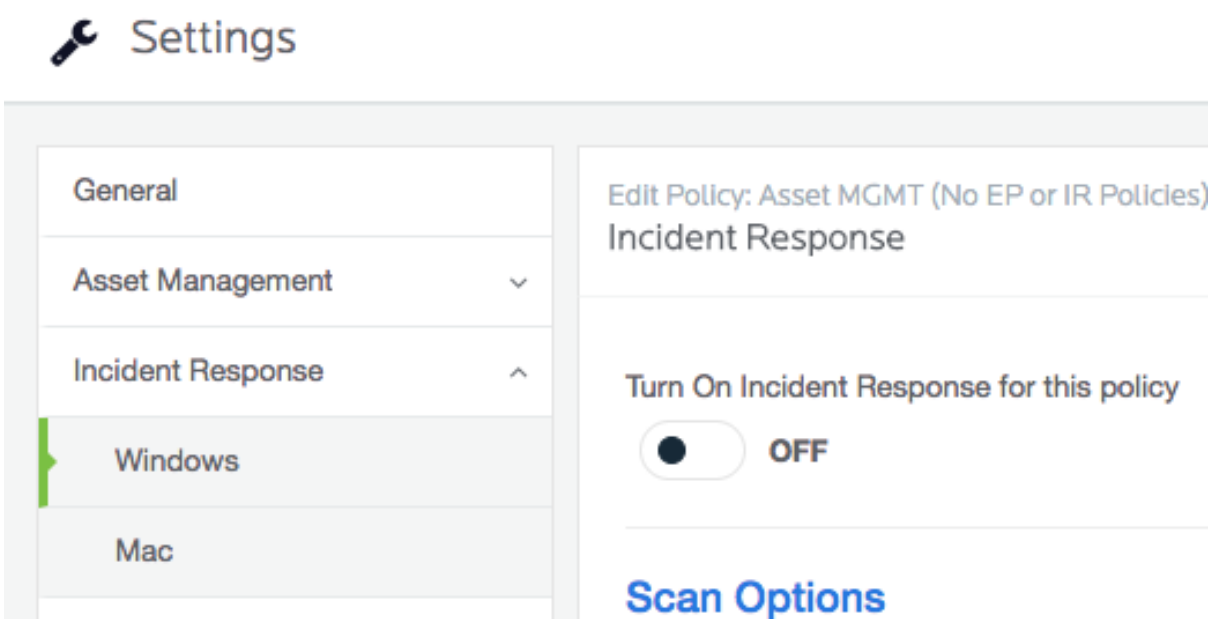
Complete your details and you will be logged into the Malwarebytes Cloud Console and presented with the console dashboard. **A detailed explanation of each tab and setting can be found in the Malwarebytes Administration Guide.**

Clicking on the "Endpoints" tab you will see there is already a Default Group. **Any agents that you install will automatically be placed into this group and will inherit whatever policy is applied to this default group.**

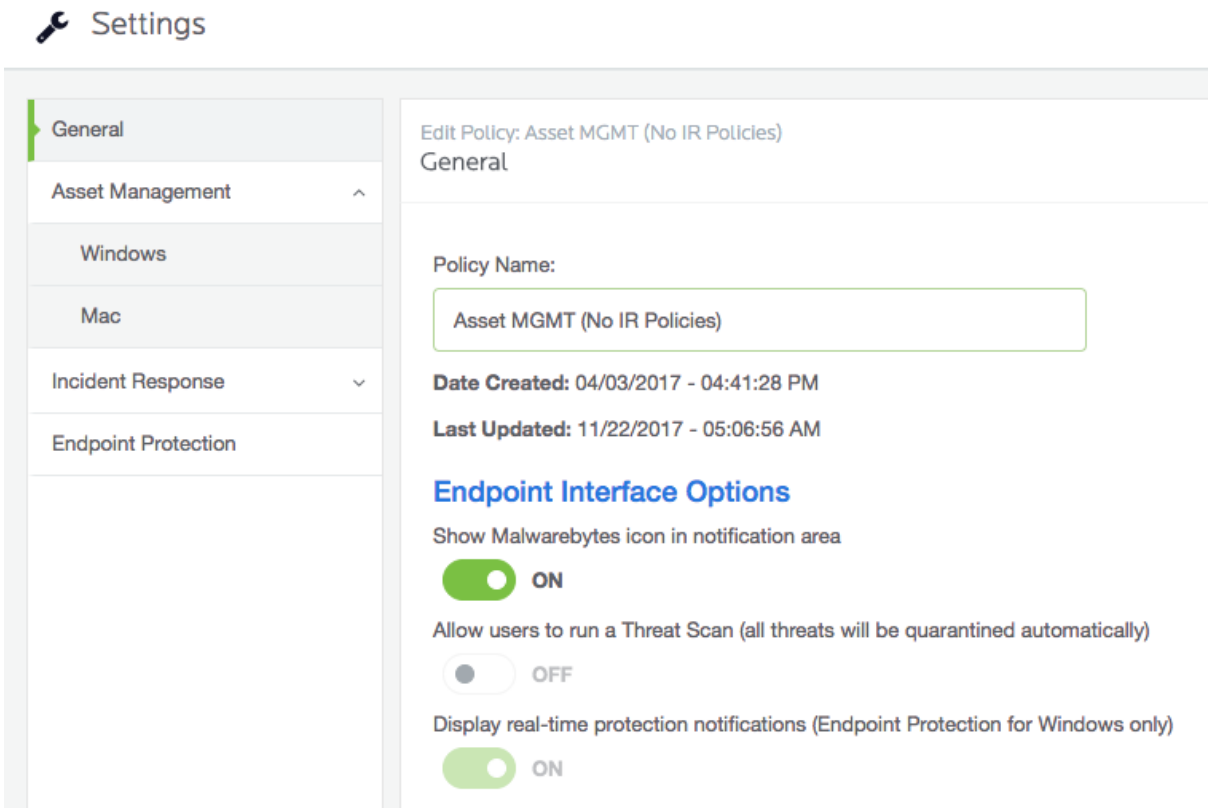
Policies

If planning to deploy multiple agents simultaneously, it is a good idea to adjust the policy applied to the default group.

To do this navigate to Settings -> Polices under the sidebar panel and click the "Default Policy". Expand "Incident Response" Windows and Mac and ensure the Incident Response policy is set to "OFF" as shown below



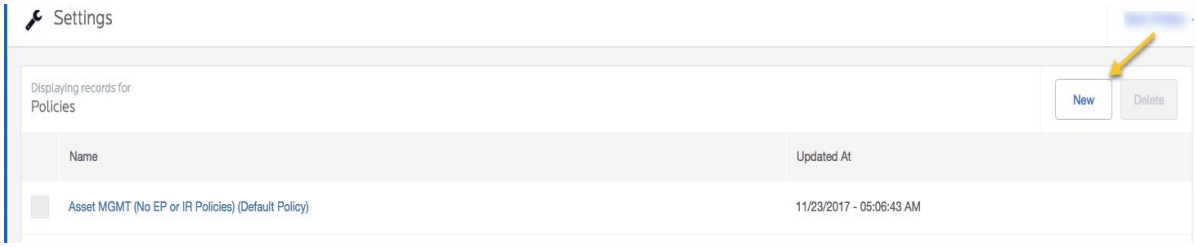
Next, click on “General” and rename the Policy Name appropriately. Below is an example; since we have disabled Incident Response in the policy, but left Asset Management enabled, we have decided to name our policy “Asset MGMT (No IR Policies)”. However, the naming convention is up to you.



As you will notice, there are other settings you can adjust to do with whether you want to show the Malwarebytes icon in the system tray, or whether you will allow users to be able

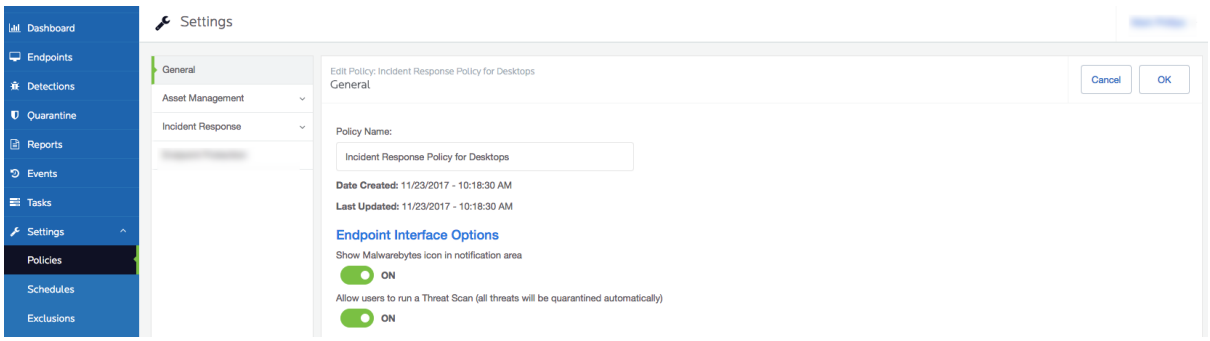
to initiate scans, but this will be down to individual customer preference. Remember to save your changes.

Now, let's create a new policy. Navigate again to "Settings" in the sidebar panel and click on "Policies" and click "New" as shown in the screenshot below.



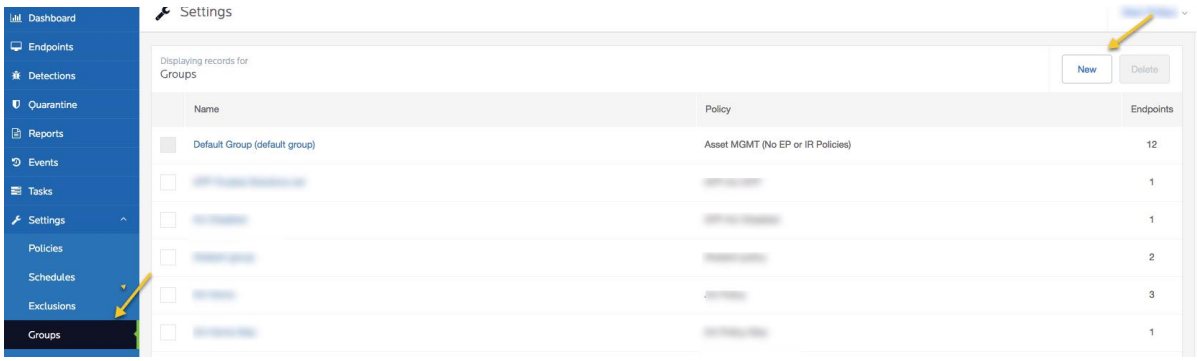
Choose an appropriate name for your policy. This could refer to a group of machines, department or geographical location. Leave the defaults under Asset Management (unless you would rather not have a software inventory) and go to the Windows and Mac tabs configuring the settings as necessary. When finished, remember to click "OK" to save your changes.

For a full explanation of each setting please see the Malwarebytes Administration Guide.

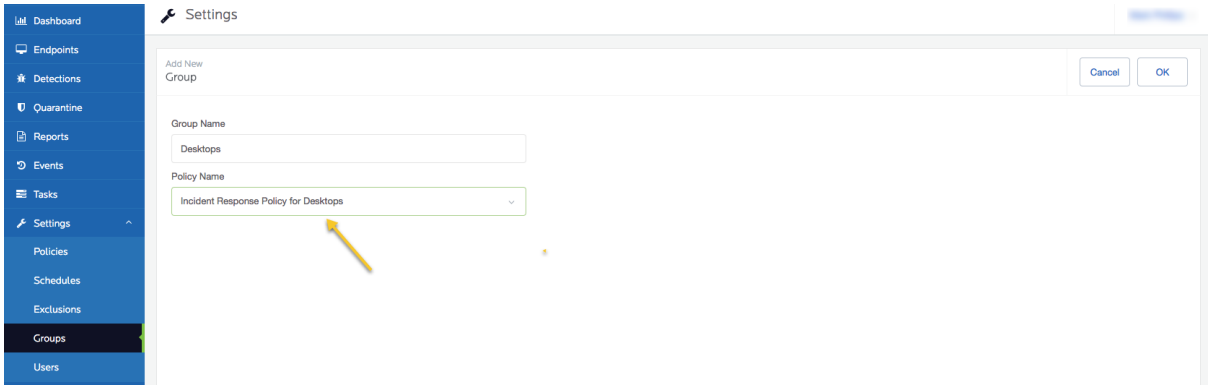


Groups

Now let's create a new group which we will apply our newly created policy to. In the sidebar panel navigate to Settings -> Groups and click "New"



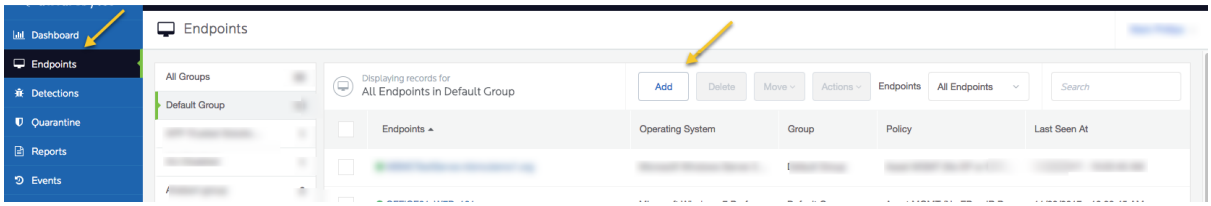
Under the “Group Name” field, type in a group name that reflects the machines that will be in the group. This could refer to a group of machines, department or geographical location. Next, from the dropdown “Policy Name” box, choose the policy you created in the previous step as show below.



Click “OK” to save your changes. You have now created a new group with your new policy applied to this group. Any machines that you move to this group, will inherit this policy and will be applied to the machines.

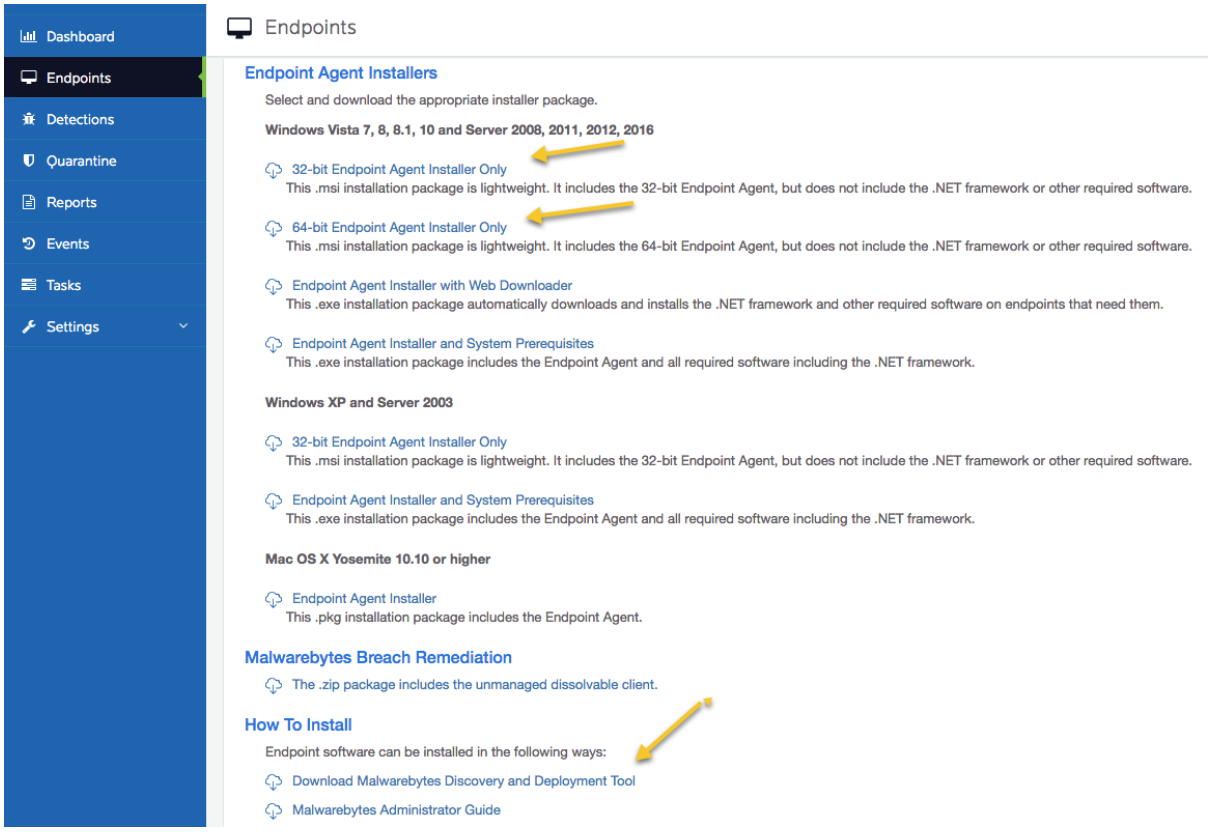
Incident Response Agent Deployment

Now let’s deploy a Malwarebytes Incident Response agent. In the sidebar panel navigate to “Endpoints” and click “Add”



In the pane displayed you find a variety of installers. If you have your own software delivery layer you can choose one of the MSI 32-bit or 64-bit installers and deploy using that as the recommended approach. A prerequisite of the agent is to have .NET 4.5.2 or later installed but if your Windows machines are up-to-date they should already have this.

You can also deploy using the Malwarebytes Discovery and Deployment Tool. For instructions on how to use this see the Malwarebytes Administration Guide page 5.



Once you have installed an endpoint, this will automatically appear in the Default Group under Endpoints in the sidebar panel. Let's move our newly installed endpoint(s) to the correct group, so that it will apply the correct policy.

In the sidebar panel navigate to Endpoints -> Default Group and check the box next to the endpoint you wish to move. Next, click on the "Move" tab to see the dropdown selection as shown in the screenshot below. Choose the group we created earlier. The machine will be moved into the chosen group and have the policy assigned.

If you navigate back to "Endpoints" in the sidebar panel you will now see the machine you just moved appear in the new group you created earlier.

You are now ready to run malware scans and remediate using Malwarebytes Incident Response.

To do this navigate to your endpoint, check the box and select the "Actions" tab. Choose "Scan + Report" to initiate an anti-malware scan and report back any malware discovered. You can then select "Scan + Quarantine" to remove any discovered malware. This allows

you to be selective about which PUPs or PUMs to remove should you wish to keep them. Malwarebytes recommends removing all discovered PUPs and PUMs.
In some cases, certain policies enforced such as resetting the browser homepage, or setting the desktop wallpaper by a GPO are discovered as a PUM. In this case, you will find the following support article helpful in setting exclusions up for these PUMs https://support.malwarebytes.com/docs/DOC-1417

Additional Reporting

The Malwarebytes Cloud server collects a rich set of information from the endpoints and a common request we get is to turn this data into useful information. Malwarebytes provides a complete set of RESTful APIs for this purpose. The Management Console uses these same APIs to extract the data. However, it does require some scripting and technical work to make the data useful.

To make this easier for our customers, we have introduced the Malwarebytes Excel Addin, which provides easy access to import data directly into Microsoft Excel.

You can access this tool at https://support.malwarebytes.com/docs/DOC-2672 it will also explain how to use and the purposes of it.

Technical Support

The majority of technical support solutions can be found via our support forum accessible here - https://support.malwarebytes.com/

Should you wish to raise a technical support case the recommended way to access Malwarebytes technical support is through our support portal. Please create a support ticket here - https://www.malwarebytes.com/support/business/#techhelp. Once you complete the form you will receive an automated response from our support system providing you with a reference number which you can quote on all correspondence.

Please give as much detail as possible when creating support cases. If you would like to attach screenshots or need to provide logs, you can attach these in your response to the automated email you received upon support case creation.

You can also access business technical support over the phone by calling +44 808 164 9330

Prerequisites

The URL's below are accessed by the Malwarebytes Incident Response agent for communication, updates and licensing etc. so you will need to whitelist or have these bypassed if you think it will be an issue. They are all over https (port 443 – outbound) so unless you're doing some kind of SSL inspection, blocking at the firewall or proxy it shouldn't be a problem. If you are doing SSL inspection you will need to bypass it for the URL's below or add exclusions to your proxy so that agents can communicate without issue.

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