# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirements</td>
<td>2</td>
</tr>
<tr>
<td>Installation Scenarios</td>
<td>2</td>
</tr>
<tr>
<td>Existing Malwarebytes Installations</td>
<td>2</td>
</tr>
<tr>
<td>Install / Update Malwarebytes Plugin</td>
<td>3</td>
</tr>
<tr>
<td>Configuring Malwarebytes Plugin</td>
<td>5</td>
</tr>
<tr>
<td>About the Screens</td>
<td>7</td>
</tr>
<tr>
<td>System Dashboard</td>
<td>7</td>
</tr>
<tr>
<td>Settings</td>
<td>7</td>
</tr>
<tr>
<td>Client Licenses</td>
<td>8</td>
</tr>
<tr>
<td>Deployment History</td>
<td>8</td>
</tr>
<tr>
<td>Global Ignore List</td>
<td>9</td>
</tr>
<tr>
<td>Policy Templates</td>
<td>10</td>
</tr>
<tr>
<td>Global Dashboard, Client and Location Screens</td>
<td>11</td>
</tr>
<tr>
<td>Overview</td>
<td>11</td>
</tr>
<tr>
<td>Deployment</td>
<td>12</td>
</tr>
<tr>
<td>Deployment Settings</td>
<td>12</td>
</tr>
<tr>
<td>Anti-Malware Details</td>
<td>13</td>
</tr>
<tr>
<td>Quarantined Items</td>
<td>14</td>
</tr>
<tr>
<td>Ignored Items Tab</td>
<td>15</td>
</tr>
<tr>
<td>Anti-Exploit Details</td>
<td>16</td>
</tr>
<tr>
<td>Computer Screen</td>
<td>17</td>
</tr>
<tr>
<td>Overview</td>
<td>17</td>
</tr>
<tr>
<td>Scan History</td>
<td>18</td>
</tr>
<tr>
<td>Threat History Tab</td>
<td>18</td>
</tr>
<tr>
<td>Quarantined Items</td>
<td>18</td>
</tr>
<tr>
<td>Ignore List</td>
<td>18</td>
</tr>
<tr>
<td>Policy Management</td>
<td>19</td>
</tr>
<tr>
<td>Policy Editor</td>
<td>19</td>
</tr>
<tr>
<td>How to Create a Policy Template</td>
<td>19</td>
</tr>
<tr>
<td>How to Modify an existing Policy Template</td>
<td>20</td>
</tr>
<tr>
<td>Apply Policy Template</td>
<td>21</td>
</tr>
<tr>
<td>Change Log</td>
<td>22</td>
</tr>
<tr>
<td>Known Issues</td>
<td>22</td>
</tr>
</tbody>
</table>
Requirements
The Malwarebytes Plugin has been designed with the Following Assumptions and Minimum or Maximum requirements.

- The Plugin requires **LabTech 10.5** or **LabTech 11.0**
- Malwarebytes Anti-Malware version 1.8 (LabTech) is required for full compatibility any existing installations of Malwarebytes Anti-Malware will need to be manually removed and re-installed.
- Malwarebytes Anti-Malware installation is to be handled by the plugin as certain settings are required for the Log and Scan history to be collected correctly.
- If you are using any third-party application update tools please ensure Malwarebytes is excluded from updates.

Installation Scenarios
Here are a couple of Scenarios for existing Malwarebytes Anti-Malware users that have current deployments of the software.

Existing Malwarebytes Installations
Existing installations of Malwarebytes Anti-Malware using versions 1.75 and 1.8 (Non-LabTech) will still collect some information however these versions are not supported by the plugin as result you will need to re-install the supported version Malwarebytes Anti-Malware from the plugin.

You can trigger the uninstall process from the Malwarebytes Tab on the Computer Screen
Install / Update Malwarebytes Plugin

**WARNING:** Installing or Updating the Malwarebytes Plugin will cause the LabTech Database Agent to immediately restart which will terminate any scripts that are currently running. Before Installing the Plugin ensure that all scripts have completed.

For additional information, refer to [View Running Scripts](#).

1. Launch the Solution Centre and Navigate to Security Solutions and add the “Malwarebytes” solution to the queue.

2. Install / Update the Plugin.

3. Navigate to the Plugin Manager (Help > Plugin Manager) and Locate the following two plugins and right click and select “enable”.

<table>
<thead>
<tr>
<th>Plugin</th>
<th>Version</th>
<th>Status</th>
<th>Copyright Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malwarebytes</td>
<td>1.5.0.12</td>
<td></td>
<td>2014</td>
</tr>
<tr>
<td>Malwarebytes – Remote A</td>
<td>1.5.0.12</td>
<td></td>
<td>2016</td>
</tr>
</tbody>
</table>
4. Reload the Database Agent and trigger a remote agent plugin update by going to Advanced > Reload Plugins > Update Remote Agent Plugins.

5. Restart the LabTech Control Center and continue to Configuring Malwarebytes Plugin.
Configuring Malwarebytes Plugin

Ensure that you have restarted the LabTech Control Center after installing or updating the Malwarebytes Plugin.

1. Navigate to the Malwarebytes Global Settings which is located under **System Dashboard > Config > Integration > Malwarebytes**.

2. **Enter License Details** for Malwarebytes Anti-Malware and Malwarebytes Anti-Exploit, into the appropriate section on the **Settings** tab.

   **NOTE:** Please take note of the following.
   
   I. License Keys entered on this screen will be used globally unless a Client License key is defined (on the **Client Licenses** tab)
   
   II. Once a License Key has been saved, it cannot be modified without being removed.
   
   III. Removing a License Key will trigger an **Uninstall** command to all Malwarebytes installations that are registered with the License Key that is being removed.

3. **Enable Password Protection**, if enabled specify a Password to be used. Enabling Password Protection is used to limit access to certain features of Malwarebytes Anti-Malware. This password will be required to access those features.

   **NOTE:** Please take note of the following.
   
   - Passwords are for **Malwarebytes Anti-Malware** only.
   - Passwords cannot contain Double Quotes ("")
   - Passwords are only configured during the installation of Malwarebytes Anti-Malware and will not be applied to pre-existing installations

4. **Configure Installation Options**, Malwarebytes has a few limited options that can help control the installation of Malwarebytes Anti-Malware, you are able to select the following
to be applied for new installations of Malwarebytes Anti-Malware.

- Disable Desktop Icon
- Disable Start Menu Icons
- Enable Password Protection

5. **Configure Auto Deployment**, in the Malwarebytes Plugin to automatically deploy both Malwarebytes Anti-Malware and Malwarebytes Anti-Exploit. To do this you will need to enable the Auto Deployment option and then configure which clients will have auto deployment enabled.

Once enabled, click on the **Configure** button to continue with the deployment setup; it’s just a matter of checking the boxes to enable Auto Deployment.

**NOTE:** Please take note of the following.

- Auto Deployment is handled automatically by the LabTech Server every 6 minutes.
- In the event of the installation process failing, the Auto Deployment will not re-attempt the installation for 24 hours.
- Malwarebytes will not be Deployed to Any Device or Location that is Excluded from Auto Deployment (configurable on the **Computer Screen** or **Location Screen**).
- The Installation process will use the Product ID and License Key from the Client License section first, in the event that no specific Client License record exists, it will fall back to using the Global Values. In the event that these values have not been defined, Malwarebytes will **NOT** be installed.
- Malwarebytes Auto Deployment is for Windows devices only.
About the Screens
The Malwarebytes Plugin will add tabs labelled “Malwarebytes” to your LabTech System allowing you to configure settings, review collected information and interact directly with Malwarebytes, a brief overview of each tab / section.

System Dashboard
The System Dashboard Tab for Malwarebytes is primarily used for Configuring Settings such as Licensing, Deployment and Policy Management

Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-Malware Product ID and License Key</td>
<td>DEFAULT: Not Entered Registration details for Anti-Malware Deployment, can be overwritten by a Client Specific Key.</td>
</tr>
<tr>
<td>Anti-Exploit Product ID and License Key</td>
<td>DEFAULT: Not Entered Registration details for Anti-Exploit Deployment, can be overwritten by a Client Specific Key.</td>
</tr>
<tr>
<td>Disable Desktop Icon</td>
<td>DEFAULT: Disabled Prevents Malwarebytes Anti-Malware from creating a desktop icon on Installation.</td>
</tr>
<tr>
<td>Disable Start Menu Icons</td>
<td>DEFAULT: Disabled Prevents Malwarebytes Anti-Malware from creating start menu icons on Installation.</td>
</tr>
<tr>
<td>Enable Password Protection</td>
<td>DEFAULT: Disabled Specifies a password that is required to access certain functionality of the Malwarebytes Anti-Malware product.</td>
</tr>
<tr>
<td>Enable Auto Deployment</td>
<td>DEFAULT: Disabled Enabling this Feature will enable the Malwarebytes Plugin to Automatically Deploy both Anti-Malware and Anti-Exploit products as configured by using the Configure button</td>
</tr>
</tbody>
</table>
Client Licenses
This section allows you to specify product registration information for Anti-Malware and Anti-Exploit specific to a customer, values defined here will be used in place of the globally defined registration information.

You can remove a record by Right clicking on the record in the summary window and selecting Remove License.

Deployment History
This section is used to review installations of Malwarebytes Anti-Malware and Anti-Exploit, this uses information from the LabTech Command history and will show you commands in one of three stats: Success, Failed and Executing.
Global Ignore List

The global ignore list is used to define items for Malwarebytes Anti-Malware to ignore / exclude from scans, the ignore list is applied to agents when Malwarebytes Anti-Malware is installed as well as when issuing the “Apply Ignore List” task from the **Global Dashboard, Client** or **Location** screens.

Additional details about Item Classes and required input formats

<table>
<thead>
<tr>
<th>Item Class</th>
<th>Description</th>
</tr>
</thead>
</table>
| File       | Format: <Drive><Directory><File>  
Example: C:\Windows\file.exe |
| Folder     | Format: <Drive><Directory>  
Example: C:\Windows\LTSvc |
| IP         | Format: xxx.xxx.xxx.xxx  
Example: 111.222.33.444 |
| Key        | Format: <hive><key>  
Example: “HKLM\Software\Key” |
| Value      | Format: <hive><key><value>  
Example: “HKLM\Software\Key\Value” |
Policy Templates

Policy Templates allow you to create, modify or remove policies that are to be used for Malwarebytes Anti-Malware, for more information, refer to the Policy Management section.
Global Dashboard, Client and Location Screens
The following screens are available throughout the Malwarebytes Integration and are accessible from the Global Dashboard, Client and Location screens.

Overview
Provides a graphical overview of threat and exploit history

Available on
- Global Dashboard > Overview
- Client Screen > Malwarebytes Tab > Overview
- Location Screen > Malwarebytes Tab > Overview

<table>
<thead>
<tr>
<th>Gadget Name</th>
<th>Gadget Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Threats</td>
<td>Number of threats detected by Malwarebytes Anti-Malware in the most recent scan results.</td>
</tr>
<tr>
<td>Recent Exploits</td>
<td>Number of Exploits detected by Malwarebytes Anti-Exploit in the previous 24-hours</td>
</tr>
<tr>
<td>Quarantined Items</td>
<td>Number of items that are currently in Malwarebytes Anti-Malware quarantine.</td>
</tr>
<tr>
<td>Anti-Malware Threat Detection</td>
<td>Graph depicting the number of threats detected by Malwarebytes Anti-Malware over the previous 7.</td>
</tr>
<tr>
<td>Anti-Exploit Threat Detection</td>
<td>Graph depicting the number of exploits detected by Malwarebytes Anti-Exploit over the previous 7 days.</td>
</tr>
</tbody>
</table>
Deployment
view all Windows devices allowing for manual actions Install or Uninstall action as well as control the Auto-Deployment state of Malwarebytes Products.

Available on

- Global Dashboard > Deployment
- Client Screen > Malwarebytes Tab > Deployment
- Location Screen > Malwarebytes Tab > Deployment

Deployment Settings
This button will present you with options related to the auto deployment of Malwarebytes Anti-Malware and Malwarebytes Anti-Exploit allowing you to:

- Enable auto deployment of Anti-Malware
- Enable auto deployment of Anti-Exploit
- Specify which deployment policy to use

Notes
1. When viewing on the Client Screen the Deployment Settings will be specific to the client
2. When viewing on the Location Screen the Deployment Settings button is replaced with Location exclusion options.
Anti-Malware Details

View all computers that have Malwarebytes Anti-Malware installed selecting the computer in top part of the window will populate the Threat history for that specific computer below.

Available on

- Global Dashboard > Anti-Malware > Details (Note 1)
- Client Screen > Malwarebytes Tab > Anti-Malware > Details
- Location Screen > Malwarebytes Tab > Anti-Malware > Details

Functions

- Right click on computers in the List to open the computer Screen
- Right click on a threat in the threat history to add it to that individual computers ignore list.
- Run On-Demand tasks against all selected agents using the with Selected dropdown
  - Perform a Scan (Quick, Full, Flash)
  - Apply the Ignore List
  - Apply Policy Template
  - Update Database Definitions

Notes

1. When viewing on the Global Dashboard the Computer Specific Details and Threat history information is not available.
Quarantined Items
Directly interact with the Malwarebytes Quarantine.

Available on

- Client Screen > Malwarebytes Tab > Anti-Malware > Quarantined Items
- Location Screen > Malwarebytes Tab > Anti-Malware > Quarantined Items

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete Selected</td>
<td>Deletes the Selected items from the Quarantine</td>
</tr>
<tr>
<td>Delete All</td>
<td>Deletes all items from the Quarantine</td>
</tr>
<tr>
<td>Restore Selected</td>
<td>Restores the selected items from Quarantine</td>
</tr>
<tr>
<td>Restore All</td>
<td>Restores all items from Quarantine</td>
</tr>
</tbody>
</table>

Malwarebytes Plugin Version 3.10.10
Ignored Items Tab
Directly interact with the Malwarebytes Anti-Malware Ignore list.

Available on

- Client Screen > Malwarebytes Tab > Anti-Malware > Ignored Items
- Location Screen > Malwarebytes Tab > Anti-Malware > Ignored Items

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove Selected</td>
<td>Removes the selected item from the Ignore List</td>
</tr>
</tbody>
</table>
Anti-Exploit Details

View all computers that have Malwarebytes Anti-Exploit installed selecting the computer in top part of the window will populate the Threat history for that specific computer below.

Available on

- Global Dashboard > Anti-Exploit > Details (Note 1)
- Client Screen > Malwarebytes Tab > Anti-Exploit > Details
- Location Screen > Malwarebytes Tab > Anti-Exploit > Details

Functions

- Right click on computers in the List to open the computer Screen
- Run On-Demand tasks against all selected agents using the with Selected dropdown
  - Enable Protection
  - Disable Protection

Notes

1. When viewing on the Global Dashboard the Computer Specific Details and Threat history information is not available.
Computer Screen
The following screens are available on the Computer screen.

Overview
Provides a quick and general overview of the state of Malwarebytes on this device.

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install</td>
<td>Install Malwarebytes Anti-Malware</td>
</tr>
<tr>
<td>Uninstall</td>
<td>Uninstall Malwarebytes Anti-Malware</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install</td>
<td>Install Malwarebytes Anti-Exploit</td>
</tr>
<tr>
<td>Uninstall</td>
<td>Uninstall Malwarebytes Anti-Exploit</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exclude Anti-Malware Deployment</td>
<td>Excludes from Anti-Malware Auto Deployment</td>
</tr>
<tr>
<td>Exclude Anti-Exploit Deployment</td>
<td>Excludes from Anti-Exploit Auto Deployment</td>
</tr>
<tr>
<td>Policy</td>
<td>Define a Policy Template override to be used on Deployment or when Applying the Policy Template</td>
</tr>
</tbody>
</table>
Scan History
From this tab you will be able to see all scan history collected by LabTech.

Threat History Tab
From this tab you will be able to see all of the threat history collected by LabTech.

- You are able to right on a threat in the threat history to add it to that individual computers ignore list.

Quarantined Items
Refer [Here](#)

Ignore List
Refer [Here](#)
Policy Management

There are three pre-configured policy templates that are available as part of the Malwarebytes Integration. In addition to using these three pre-configured policies you are able to create your own or modify the existing using the Policy Editor.

Pre-Configured Policy Templates

- Default Policy
- Aggressive Policy
- Silent Policy

Policy Editor

Using the Policy editor, you are able to configure settings related to the following modules or components which can then be applied to existing and new deployments of Malwarebytes Anti-Malware.

- Protection Module
- General Settings
- Scanner Settings
- Database & Definition Settings
- Schedules

How to Create a Policy Template

1. Navigate to the Policy Templates within the System Dashboard  
(System Dashboard > Config > Integration > Malwarebytes > Policy Templates)

2. Click the “Add” Button located towards the bottom left section of the screen you will be presented with a new Policy Template, for additional information on the Policy settings available please refer to the Malwarebytes Administration Guide provided by Malwarebytes.
How to Modify an existing Policy Template

1. Navigate to the Policy Templates within the System Dashboard (System Dashboard > Config > Integration > Malwarebytes > Policy Templates)

2. Select the Policy you wish to modify and click the “Edit” button located towards the bottom left section of Screen, you can also Double click the policy in the list to open the editor.
Apply Policy Template

After creating or modifying a policy template you may find that you are required to updated the Policy Template to machines that already have Malwarebytes Anti-Malware, this can be achieved a number of ways.

Use Case - Globally Re-Apply a Specific Policy

You’ve just updated the default policy and want to re-apply the policy to all computers that are using the Default Policy.

1. Navigate to the Policy Templates within the System Dashboard
   (System Dashboard > Config > Integration > Malwarebytes > Policy Templates)
2. Right click on the “Default Policy” from within the Policy List and select “Push Policy” this will re-apply the Policy to all agents that are configured to use the Default Policy

Notes

1. Policy Templates association can be configured per Client within the Deployment settings available on the Global Dashboard or Client Screen

Use Case – Selectively Re-Apply Policy Template

You’ve recently made changes to one or more policies and have associated them to Clients or Computers, but because these policies are only applied on installation you need to force the policy to update.

1. Open the System Dashboard / Client Screen or Location Screen (depending on requirements) and navigate to Malwarebytes > Anti-Malware > Details
2. Select the Machines you want to have the Policy Template Re-Apply to
3. Select “Apply Policy Template” from the “with Selected” task dropdown this will apply the Policy template specific to machine selected.

Notes

1. You can see which policy template will be applied / re-applied within the Data grid column “Policy Template”
Change Log

Version: 1.5.0.12 | October 1st 2016
- Re-designed User Interface
- Anti-Malware Policy Editor
- Anti-Malware updated to 1.80.2.1012
- Numerous Enhancements and Bug fixes.

Version: 1.0.0.18 | February 14th 2016
- Ability to add Registry Values to the Global Ignore List
- Ability to Right click and add Data / Registry Values to the Ignore List on the Threat history on the Client, Location and Computer Screens
- Resolved a Date/Time issue for some time zones on the Threat history of the Computer Screen

Version: 1.0.0.17 | December 9th 2015
- Resolved an issue where Inventories were not being correctly written to the Database on LabTech 10.5 systems that had been Upgraded from 10.0

Version: 1.0.0.16 | November 27th 2015
- Resolved an issue that was causing Scan History to show an incorrect Time/Date in some Time zones
- Resolved a Typo on the – Uninstall Action Prompt
- Added the ability to add Registry Key’s to the Global Ignore list.

Version: 1.0.0.14 | November 6th 2015
- Resolved issue with some processing on the LabTech server which was preventing Scan History and Installation status from correctly being displayed.
- Added the ability to trigger DB Definition updates from the Clients, Location & Computer screen Tabs.

Version: 1.0.0.13 | November 1st 2015
- Added the ability to disable Desktop Icon for new installations of Malwarebytes Anti-Malware
- Added the ability to disable Stat Menu Icons for new installations of Malwarebytes Anti-Malware
- New Policy of “Silent” has been added to the plugin, which controls whether protection module operates in Full Silent mode. This mode gives no visual indications when threats are blocked and/or quarantined, and there is no visible tray icon. Default value is off.
- System Dashboard > Config > Integration > Malwarebytes > Settings tab has had its layout adjusted to accommodate the new options available.
- Refined Malwarebytes Anti-Malware installation process to reduce change of failures.

Known Issues

System Dashboard
- Specifying or Changing Password on the System Dashboard will only apply to new Installations of Malwarebytes. All previously deployed versions will continue to use the password that was specified at the time of installation.