# Malwarebytes Breach Remediation for Forescout CounterACT® Guide

**Version 1.1**

**12 March 2020**

# 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 web page.

https://service.malwarebytes.com/hc/en-us/articles/4414986433683

# 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!

Malwarebytes

Table of Contents

# About the Plugin

Malwarebytes supplies a plugin that integrates Malwarebytes Breach Remediation into the Forescout CounterACT® security platform. This enables deployment of Malwarebytes Breach Remediation and allows for Malwarebytes scans on Forescout CounterACT endpoints.

# Requirements

The following requirements must be satisfied for successful integration:

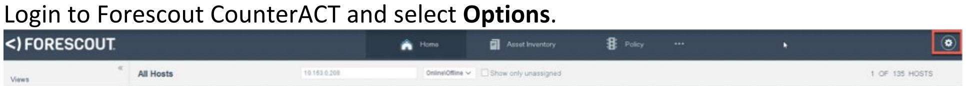
- Forescout CounterACT Appliance running 8.1.2
- Malwarebytes Breach Remediation for Windows v4.1.1

# Installation

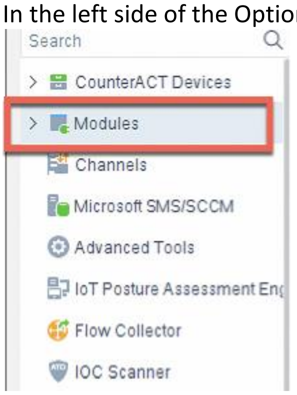
Use the provided file and follow the steps below to install the Malwarebytes plugin.

1. Download the integration plugin at the following link:
   https://downloads.malwarebytes.com/file/forescout-mb-int

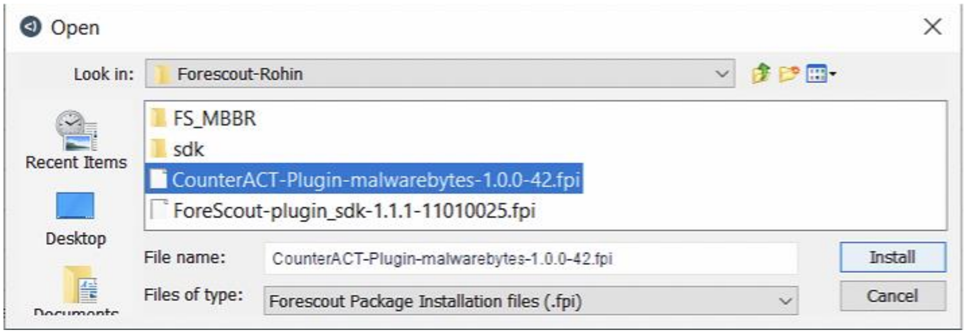
2. Login to Forescout CounterACT and select **Options**.




3. In the left side of the Options window, click **Modules**.




4. Installed plugins are displayed in the right panel. Click **Install**.




5. A new file selection opens. Browse to the location where you saved the <.fpi> file, select the file, and click **Install**.

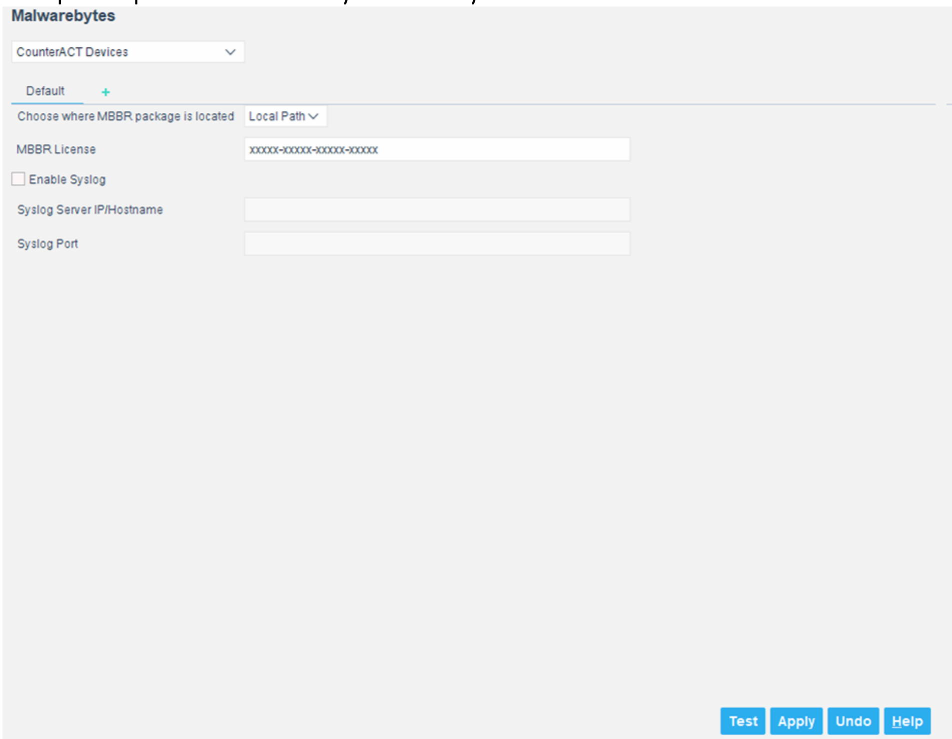
The exact filename varies depending on the version and build. The way it is displayed in Forescout CounterACT is shown below.


The installation is performed. Click **Close** when installation is complete.

# Configuration

1. Select Malwarebytes and click **Configure**.

2. Set up the options to be used by Malwarebytes Breach Remediation.

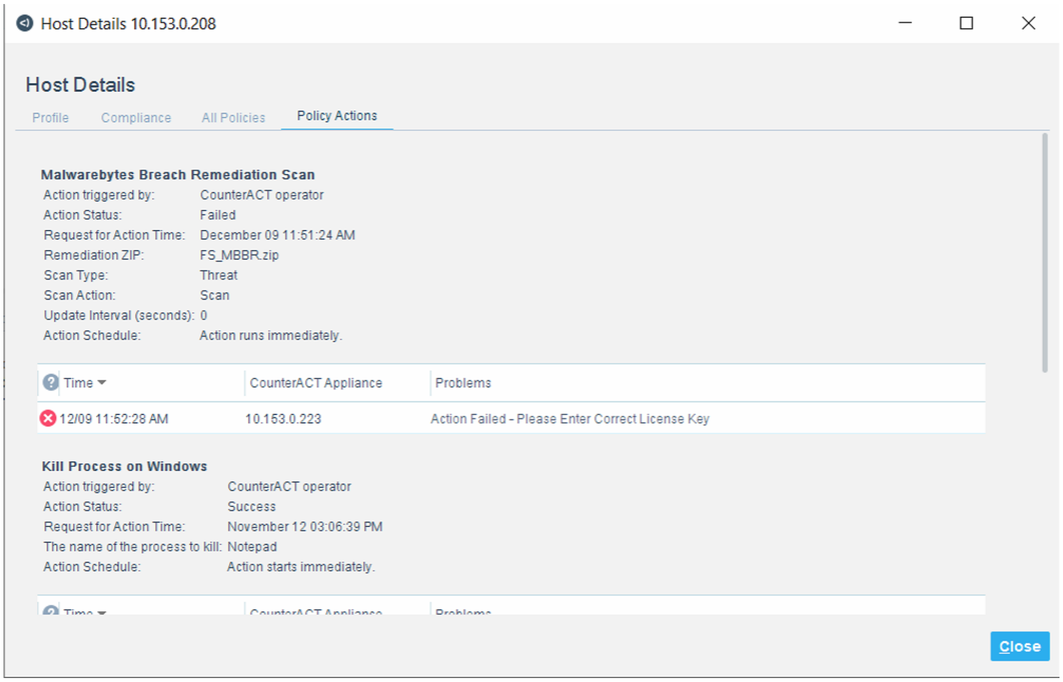



Malwarebytes Breach Remediation must be put in a Local Path or a Web Path.

- If a Local Path is selected, you must specify the Windows path to be used when executing a Malwarebytes Breach Remediation scan.
- If a Web Path is selected, Forescout CounterACT will download the Malwarebytes Breach Remediation package automatically from the Malwarebytes website.

The assigned license key *must* be entered In the **MBBR License** field

**Note**: If the correct license key is not entered, the user cannot initiate the scan. CounterACT will display “Action Failed – Please Enter Correct License Key”.




You may also choose to enable Syslog logging of activities related to the scan. If so, enter the **Syslog Server IP/Hostname** and **Syslog port** number to be used for communication with the Syslog server.

Click **Apply** to save your configuration. Click **Start** in the Modules for the Malwarebytes Plugin.

# Scan Setup

When performing a scan, Malwarebytes Breach Remediation operates according to settings specified by the user. These are:

- **Remediation ZIP** is the Malwarebytes Breach Remediation “package” file that Forescout CounterACT deploys to endpoints when a Malwarebytes scan executes. This file includes MALWAREBYTES BREACH REMEDIATION program settings.

  Once deployed to the endpoint, contents of the file are extracted into the user’s temp folder for immediate use and deleted when the scan completes.

  **Notes**:
  - If the Malwarebytes Breach Remediation package is obtained from a web path, this setting can be ignored.
  - If the Malwarebytes Breach Remediation package is obtained from a local path, instructions for integrating the package file into the Forescout CounterACT file repository immediately follows this section of the guide.

- **Scan Type** selects the type of scan that Malwarebytes Breach Remediation will perform.
  - **Full** – Scans all areas of disk and memory
  - **Threat** – Scans areas which are likely targets of malware

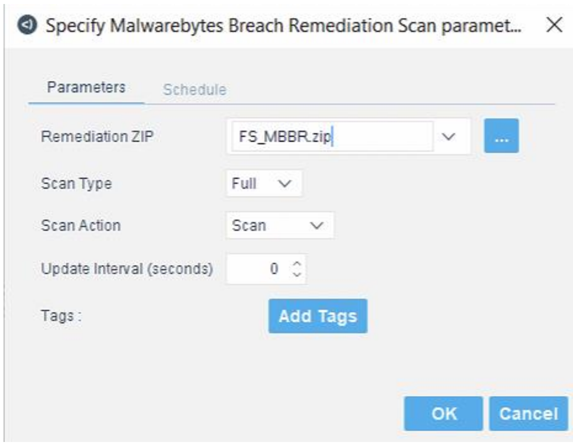
- **Hyper** – Scans only memory objects and heuristics in search of actively running malware.

- **Scan Action** determines whether the purpose of the scan is inspection or remediation.
  - **Scan** inspects the endpoint according to the selected Scan Type and reports its findings
  - **Quarantine** inspects the endpoint, performs remediation, and reports its findings.

- **Update Interval (seconds)** is the time interval between status updates when Malwarebytes Breach Remediation is executing a scan. If set to 0 seconds, the default value of 300 seconds is used. **If you are using a web path, set Update Interval to a minimum of 500 seconds.**

**Note:** If the SecureConector™ module is installed on the endpoint, you must use a Web Path to deploy the Malwarebytes agent and initiate a scan. A Local Path is not supported when using SecureConnector.

The Scan Parameters screen is shown here. It is also used in the next section.



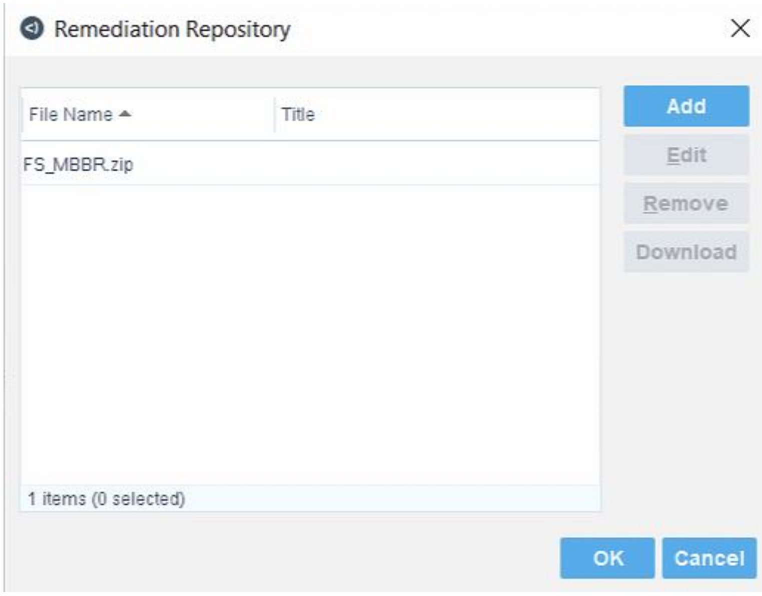

This setup is required each time a scan is to be executed on an endpoint.

# Adding a Remediation ZIP file

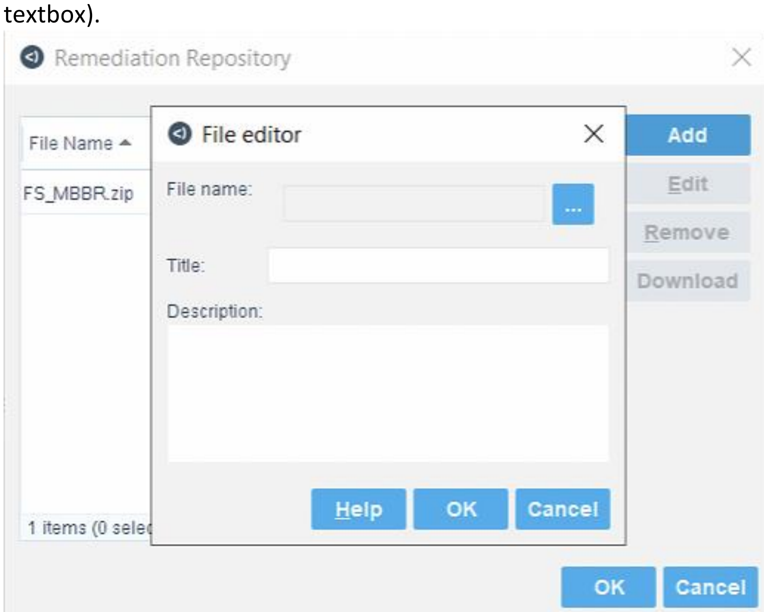
To add a Malwarebytes Breach Remediation package file to the Forescout CounterACT file repository, perform the following steps:

1. Click the "…" button (to the right of the Remediation ZIP file name). The Remediation Repository window opens.

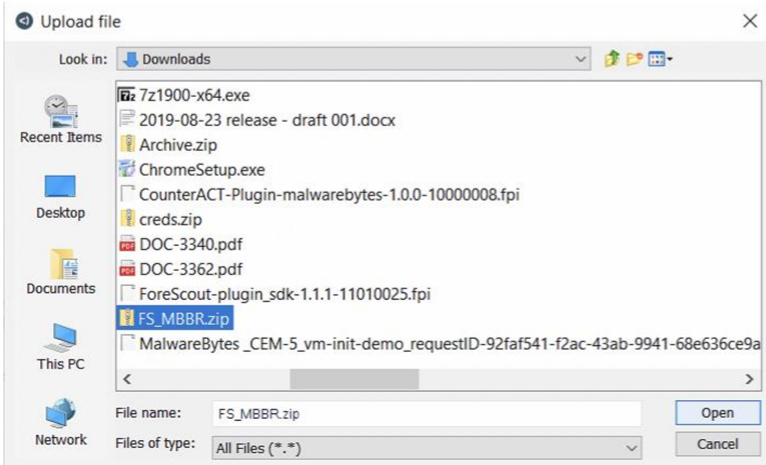
2. Click **Add**. Download the Malwarebytes Breach Remediation package file from https://downloads.malwarebytes.com/file/FS_MBBR.



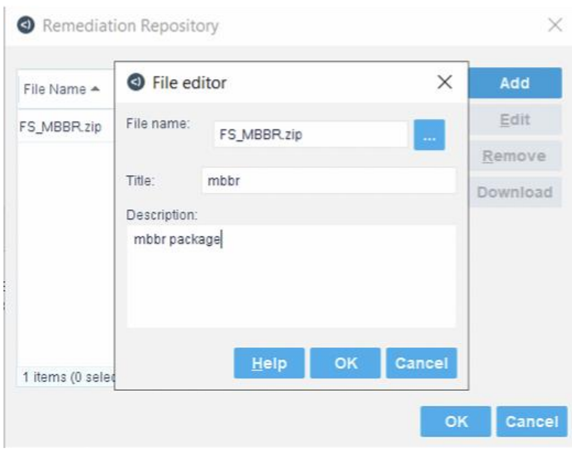

3. The File Editor window opens over the Remediation Repository window. Click "…" (next to the File name textbox).




4. A Windows Explorer dialog opens to allow you to select a file from the local file system. Navigate to the proper directory, select the file, and click **Open**.




5. In the File editor window, enter an optional **Title** and **Description**. These are for your own information and are not used elsewhere.



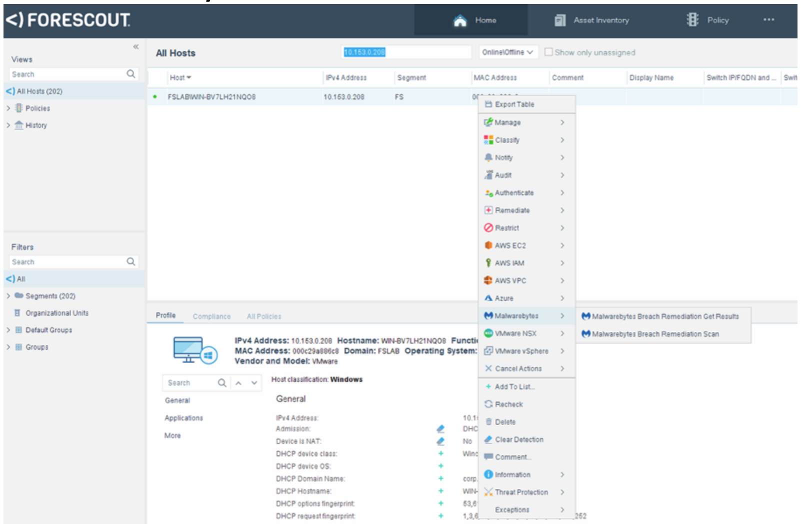

6. Click **OK** to close the File editor window. Click **OK** again to close the Remediation Repository window.

# Running a scan

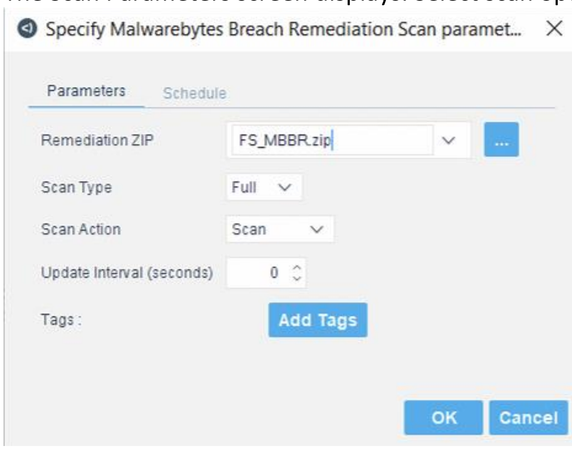
To run a Malwarebytes scan from within the Forescout CounterACT application, refer to the following screenshot and steps.

1. Right-click on the endpoint you want to scan.

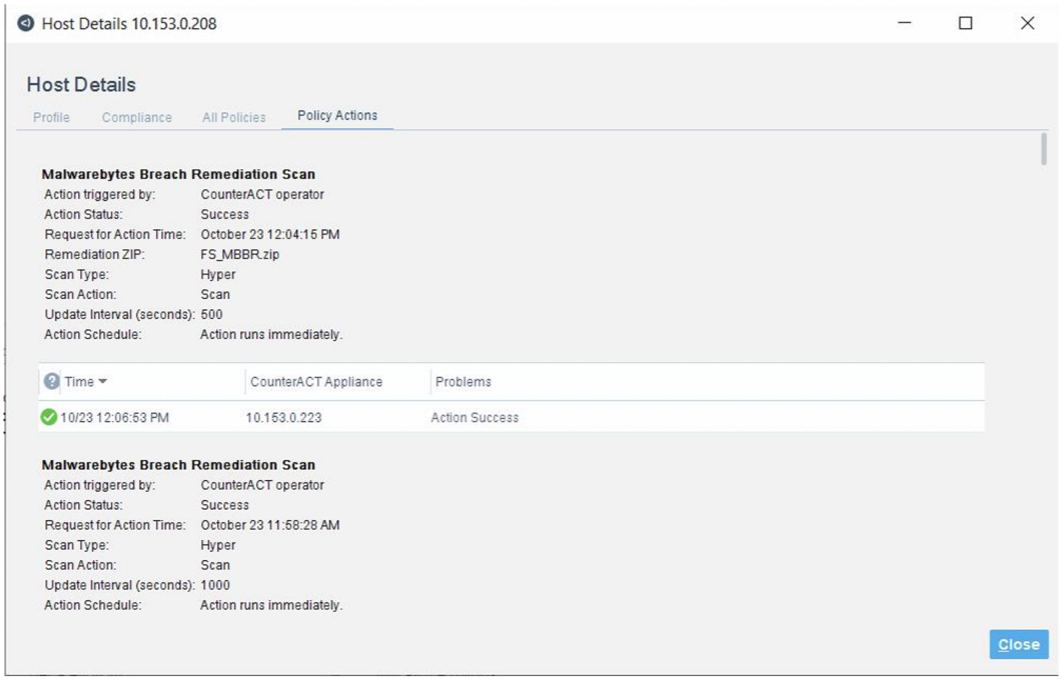
2. Choose **Malwarebytes Breach Remediation Scan**.




3. The Scan Parameters screen displays. Select scan options (as previously outlined) and click **OK**.

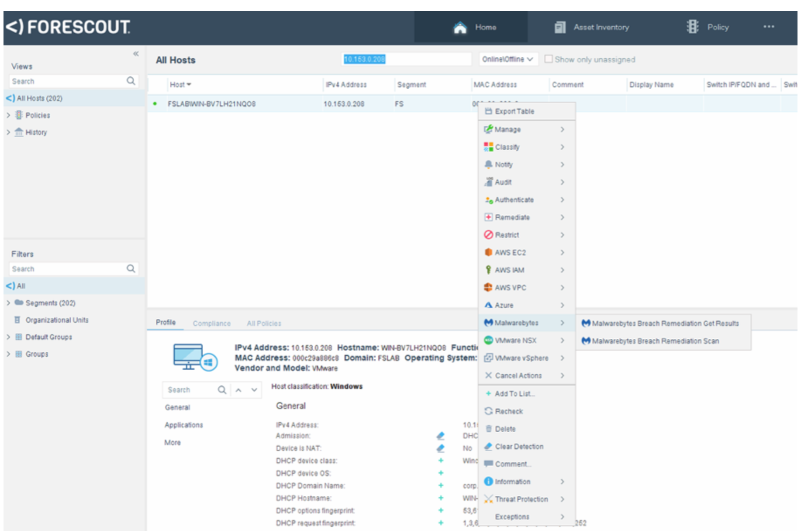


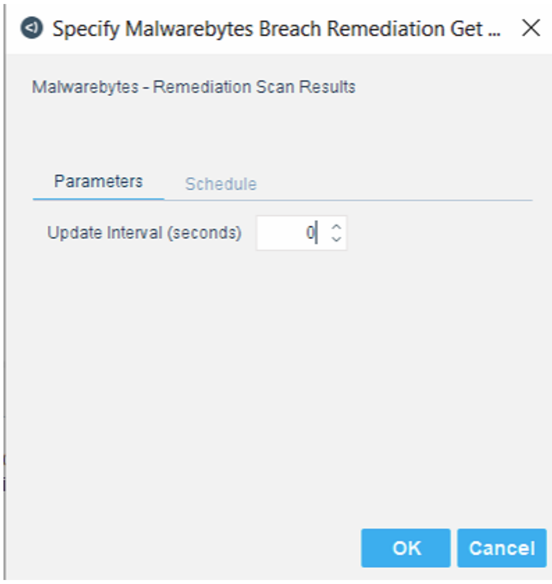
4. After the Malwarebytes scan has completed, double-click the endpoint to view the **Host Details** screen. This shows final status of the scan.



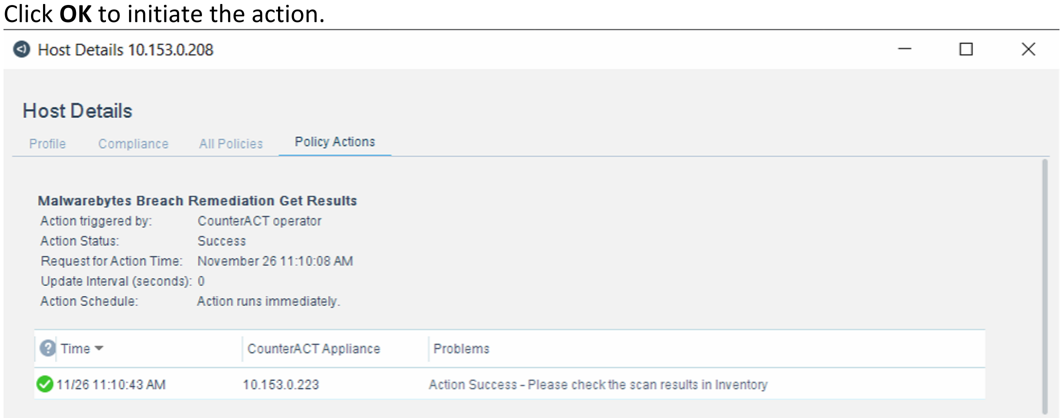

# Getting the Results

1. Right-click on the host name and select the action **Malwarebytes Breach Remediation Get Results**.

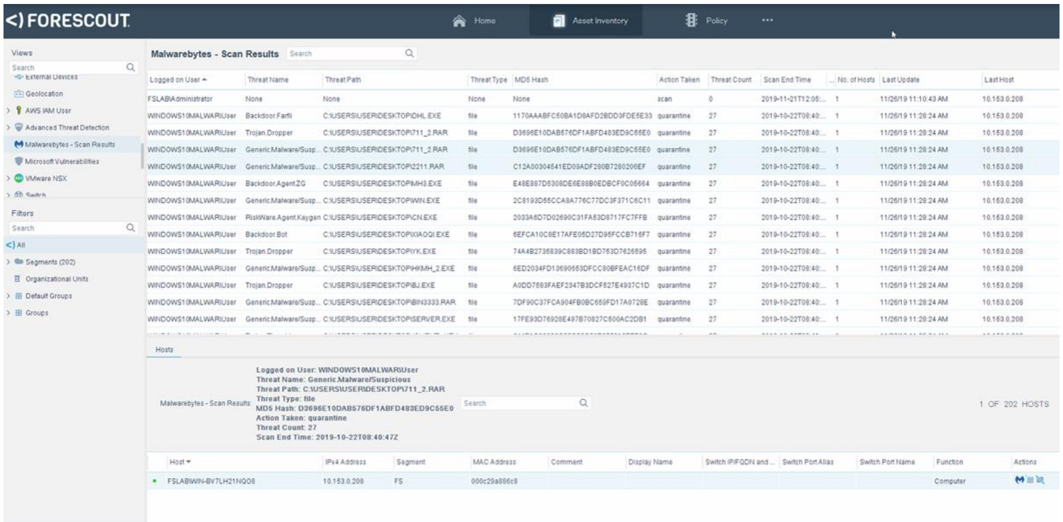




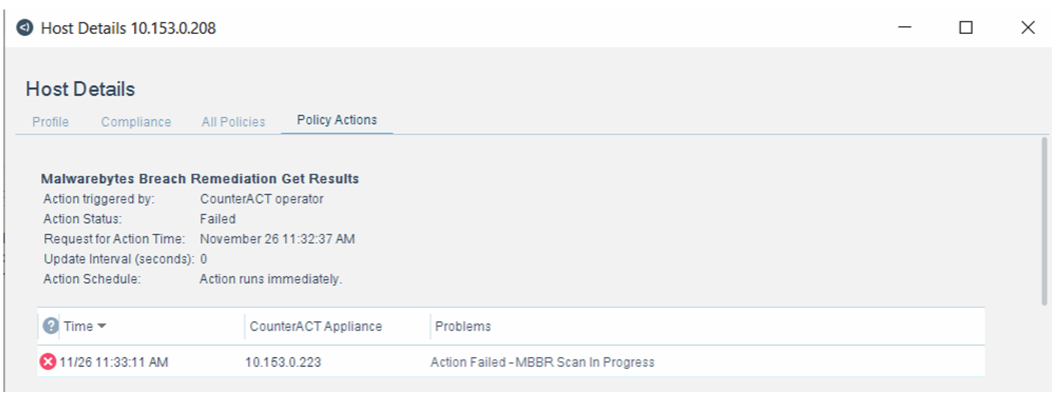

2. Click **OK** to initiate the action.



If the scan has completed, you can see the results on the **Asset Inventory** screen under **Views** > **Malwarebytes - Scan Results**.




If the scan has not completed, CounterACT displays “Action Failed – MBBR Scan in Progress”.




<u>**Note**</u>: If the Malwarebytes Breach Remediation syslog option is enabled, scan results are sent to the specified syslog server.

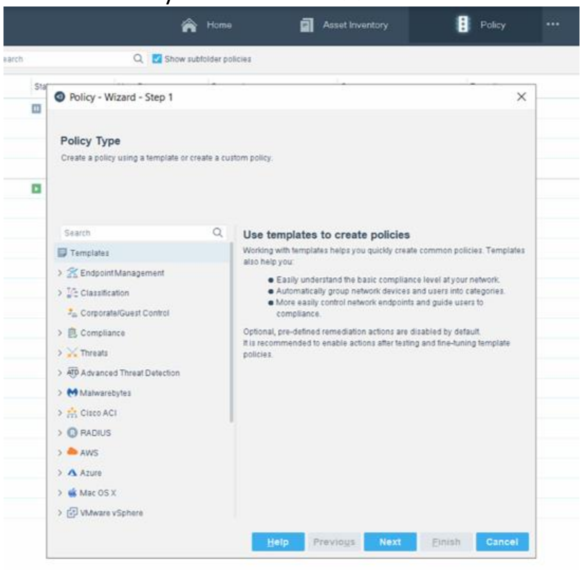
# Policy Templates

Users can quickly create common policies by using templates. Forescout CounterACT allows for automation of Malwarebytes scan actions based on policies. There are two Malwarebytes policies available: **Incident Response** and **Malware Remediation**.

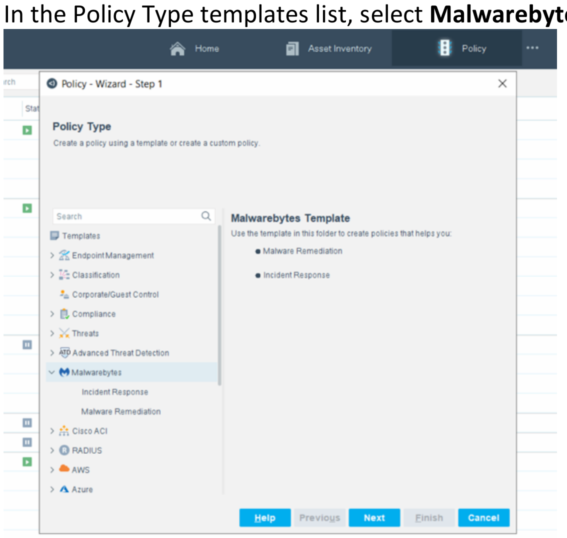
Follow the steps below to create a custom policy based on each of the default Malwarebytes policy templates.

# Create a custom Incident Response policy

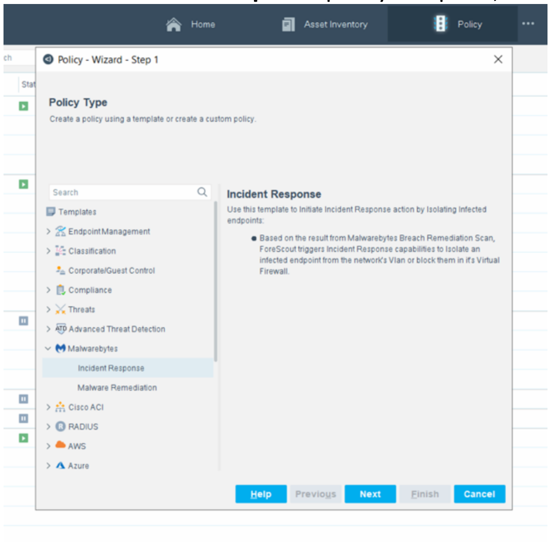
1. Go to the Policy tab and click **Add**.



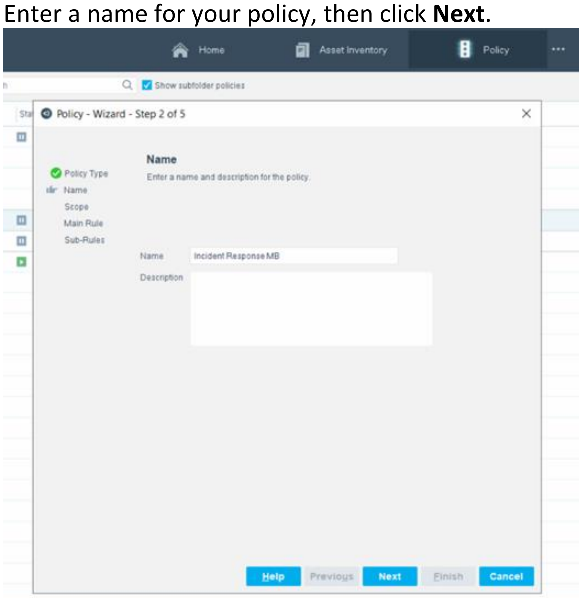

2. In the Policy Type templates list, select **Malwarebytes**.



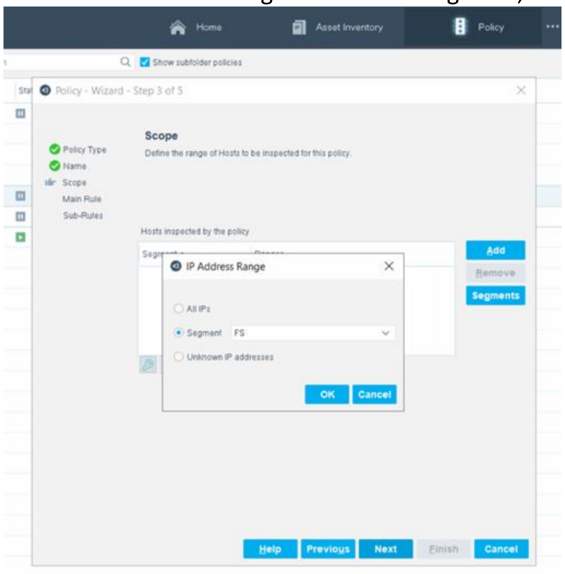
3. Select the **Incident Response** policy template, then click **Next**.




4. Enter a name for your policy, then click **Next**.

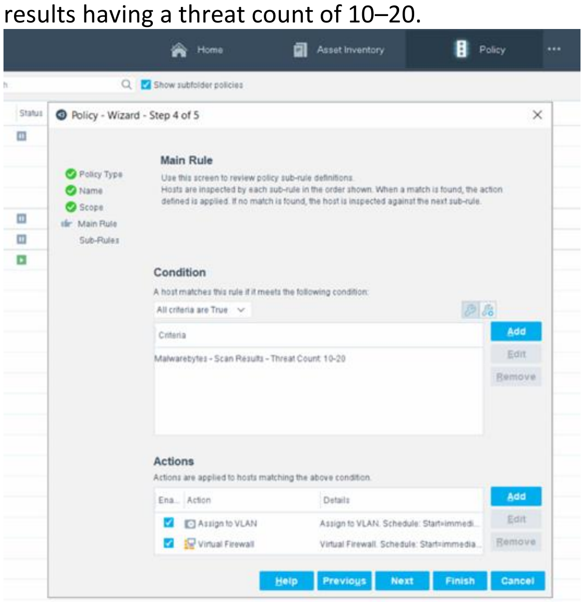


5. Select an IP address range or Network Segment, then click **Next**.



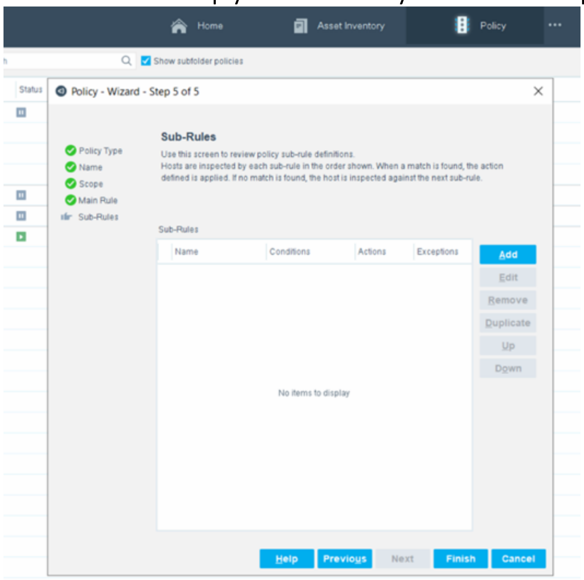

6. Edit the conditions and actions which trigger the policy automation.

   In the example below, Forescout CounterACT triggers isolation capabilities based on Malwarebytes scan results having a threat count of 10–20.



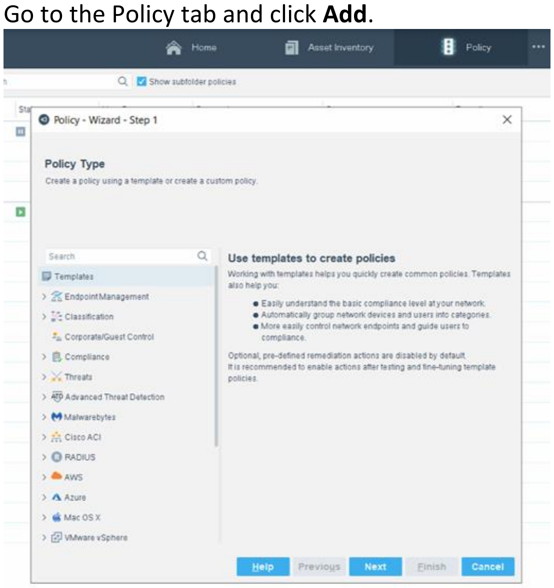

7. After setting conditions and actions, click **Next**.

8. Click **Finish** to set up your Malwarebytes Incident Response policy.

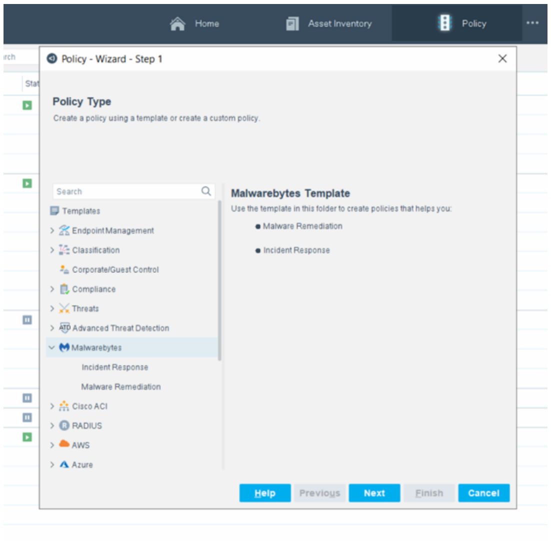



## Create a custom Malware Remediation policy

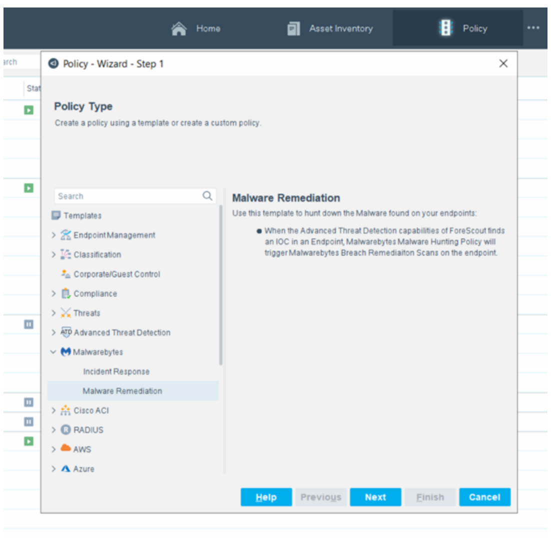
1. Go to the Policy tab and click **Add**.



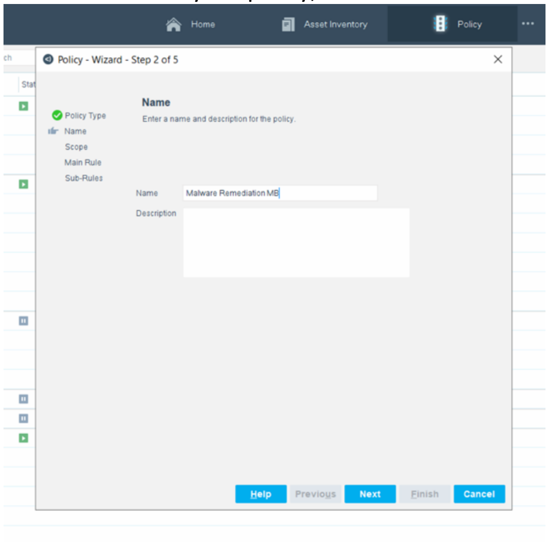

2. In the Policy Type templates list, select **Malwarebytes**.



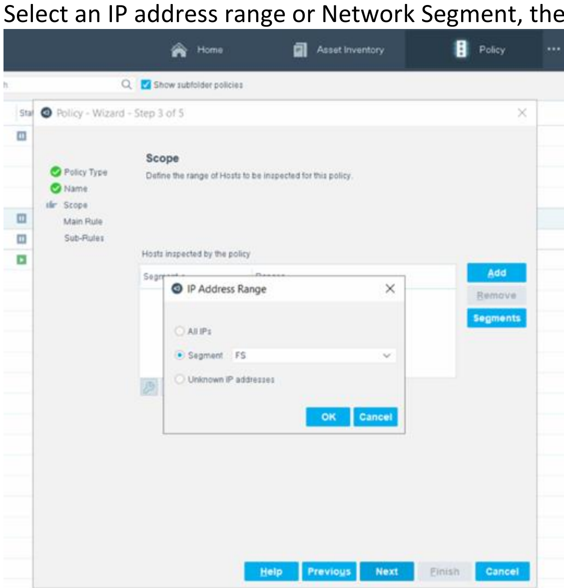

3. Select the **Malware Remediation** policy template, then click **Next**.



4. Enter a name for your policy, then click **Next**.

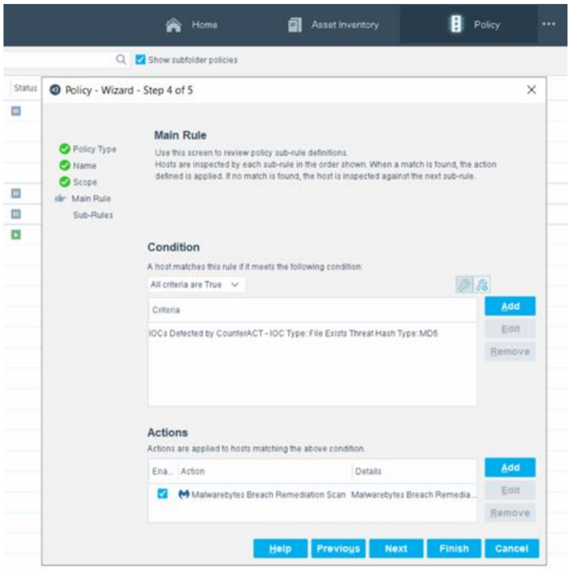



5. Select an IP address range or Network Segment, then click **Next**.




6. Edit the conditions and actions which trigger the policy automation.

   In the example below, Forescout CounterACT uses its IOC scanner on endpoints to find a specific IOC file using its MD5 hash. If the condition matches, Malwarebytes triggers a Malwarebytes Breach Remediation scan on affected endpoints to remove the threat.




7. After setting conditions and actions, click **Next**.

8. Click **Finish** to set up your Malwarebytes Malware Remediation policy.