



Malwarebytes Breach Remediation for Forescout CounterACT® Guide

**Version 1.1
12 March 2020**

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. All other trademarks or registered trademarks listed belong to their respective owners.

Copyright © 2019 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://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!



Table of Contents

| | |
|--|----|
| About the Plugin | 2 |
| Requirements | 2 |
| Installation | 2 |
| Configuration | 3 |
| Scan Setup | 5 |
| Adding a Remediation ZIP file | 6 |
| Running a scan | 8 |
| Getting the Results | 10 |
| Policy Templates | 12 |
| Create a custom Incident Response policy | 13 |
| Create a custom Malware Remediation policy | 16 |

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:

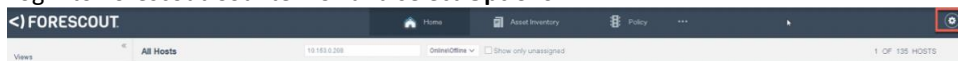
- Forescout CounterACT Appliance running 8.1.2
- Malwarebytes Breach Remediation for Windows v4.1.1

Installation

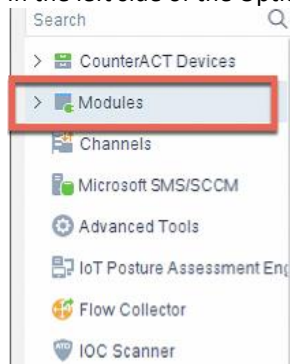
Use the provided file and follow the steps below to install the Malwarebytes plugin.

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

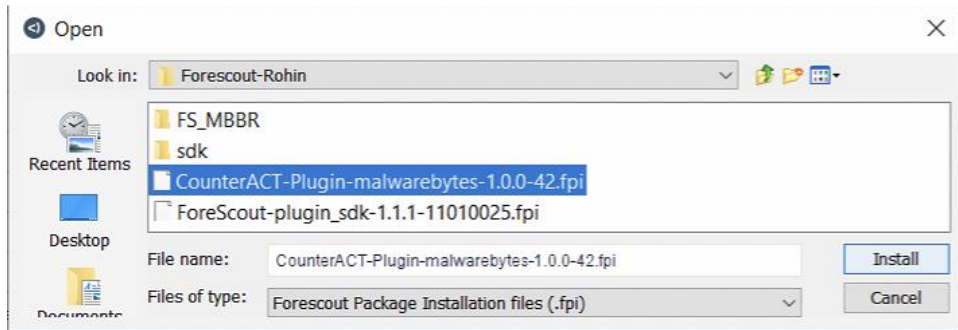
2. Login to Forescout CounterACT and select **Options**.



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.

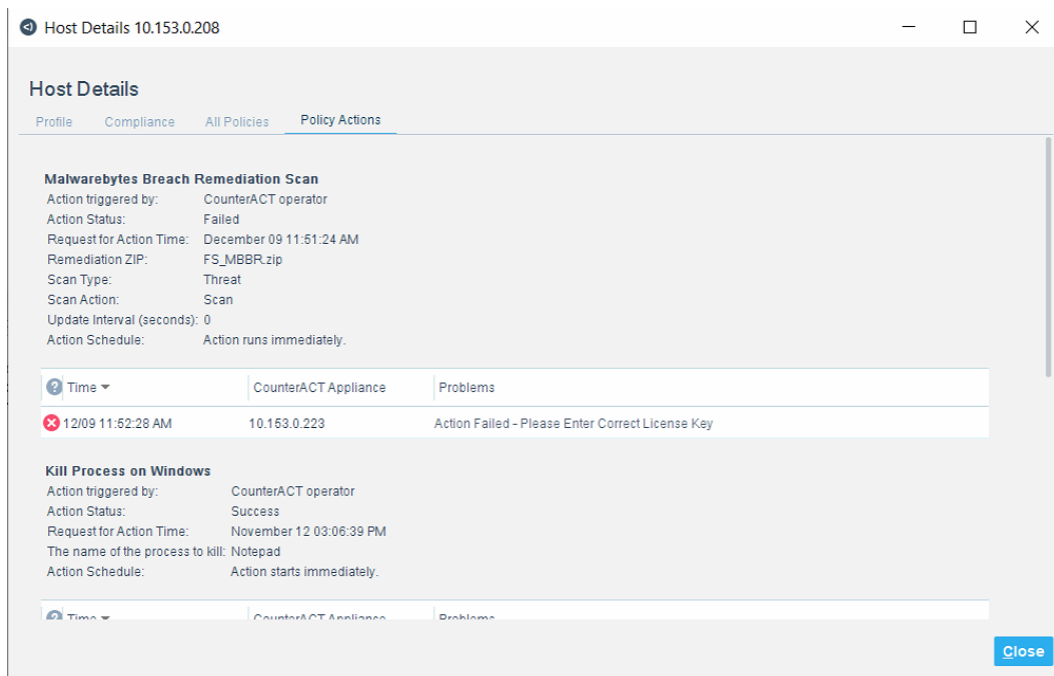
The screenshot shows the Malwarebytes configuration page. At the top, there's a 'CounterACT Devices' dropdown menu. Below it, a 'Default' tab is selected, indicated by a green plus sign. The main configuration area is titled 'Choose where MBBR package is located' with a 'Local Path' dropdown. Below this, there's a text field for 'MBBR License' containing a placeholder 'xxxxx-xxxxx-xxxxx-xxxxx'. There's an unchecked checkbox for 'Enable Syslog'. Below that are two text fields: 'Syslog Server IP/Hostname' and 'Syslog Port'. At the bottom right, there are four buttons: 'Test', 'Apply', 'Undo', and 'Help'.

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 SecureConnector™ 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.

Specify Malwarebytes Breach Remediation Scan parameters

Parameters | Schedule

Remediation ZIP: FS_MBBR.zip

Scan Type: Full

Scan Action: Scan

Update Interval (seconds): 0

Tags: Add Tags

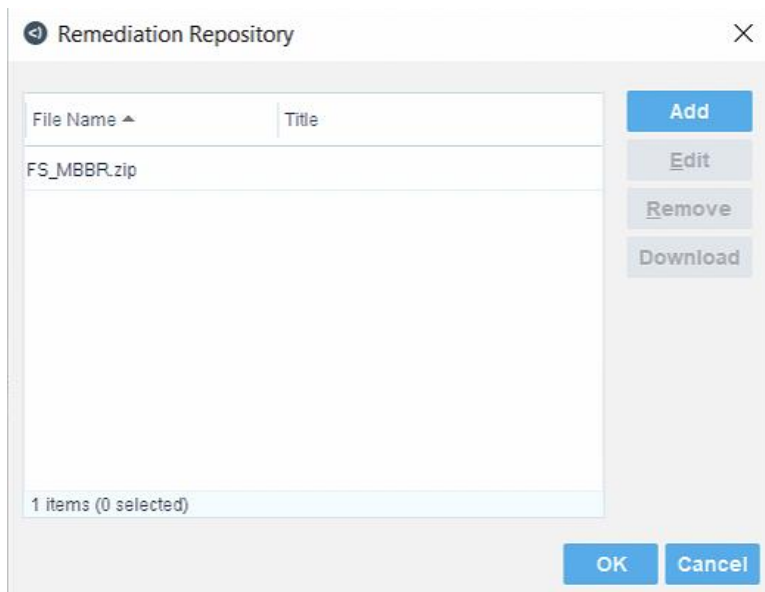
OK Cancel

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

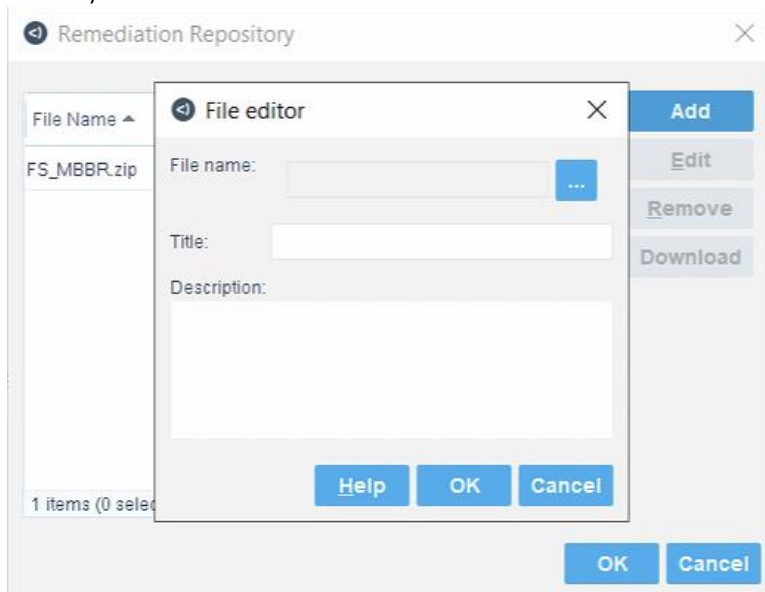
Adding a Remediation ZIP file

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

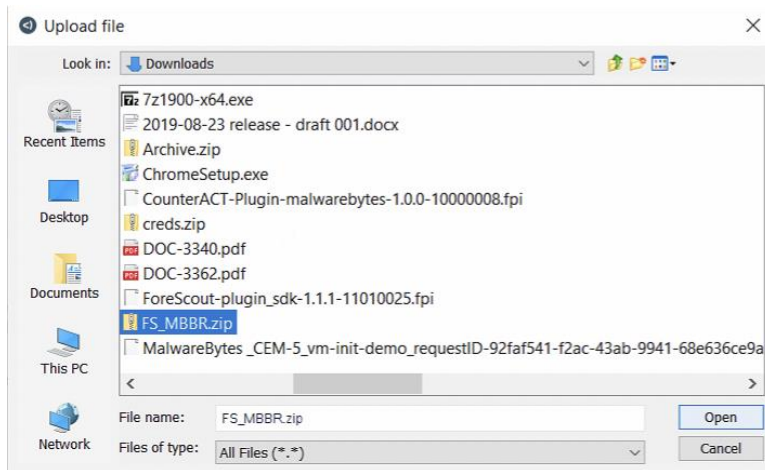
1. Click the “...” button (to the right of the Remediation ZIP file name). The Remediation Repository window opens.
2. Click **Add**. Download the Malwarebytes Breach Remediation package file from https://downloads.malwarebytes.com/file/FS_MBBR.



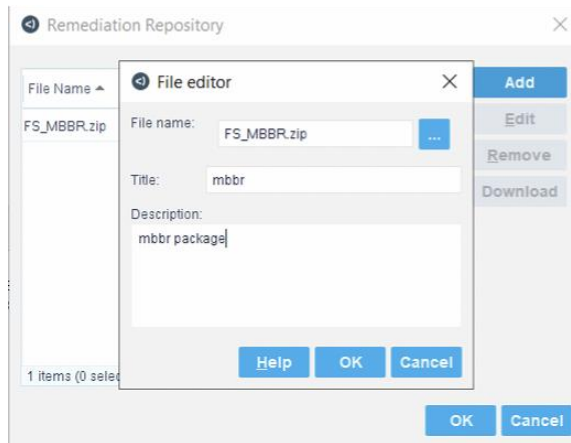
3. The File Editor window opens over the Remediation Repository window. Click "..." (next to the File name textbox).



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.



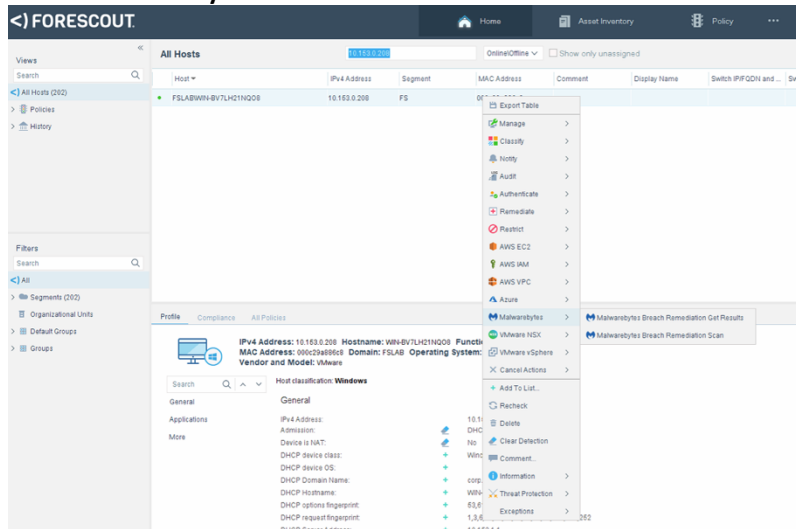
6. Click **OK** to close the File editor window. Click **OK** again to close the Remediation Repository window.

Running a scan

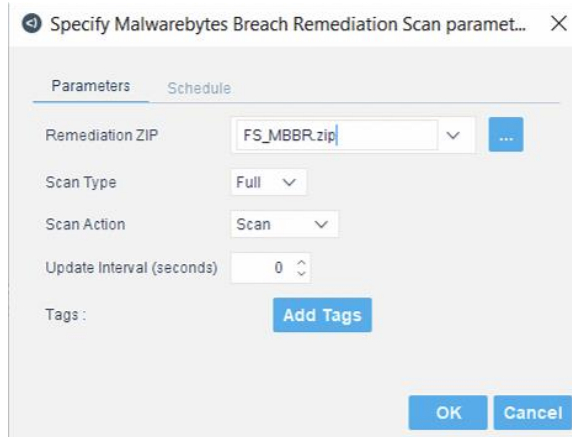
To run a Malwarebytes scan from within the Forescout CounterACT application, refer to the following screenshot and steps.

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**.



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

Host Details 10.153.0.208

Host Details

Profile Compliance All Policies Policy Actions

Malwarebytes Breach Remediation Scan

Action triggered by: CounterACT operator
Action Status: Success
Request for Action Time: October 23 12:04:15 PM
Remediation ZIP: FS_MBBR.zip
Scan Type: Hyper
Scan Action: Scan
Update Interval (seconds): 500
Action Schedule: Action runs immediately.

Time CounterACT Appliance Problems

| | | |
|-------------------|--------------|----------------|
| 10/23 12:06:53 PM | 10.153.0.223 | Action Success |
|-------------------|--------------|----------------|

Malwarebytes Breach Remediation Scan

Action triggered by: CounterACT operator
Action Status: Success
Request for Action Time: October 23 11:58:28 AM
Scan Type: Hyper
Scan Action: Scan
Update Interval (seconds): 1000
Action Schedule: Action runs immediately.

Close

Getting the Results

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

< FORESCOUT

Home Asset Inventory Policy

Views All Hosts 10.153.0.208 Online/Offline Show only unassigned

| Host | IPv4 Address | Segment | MAC Address | Comment | Display Name | Switch IP/FQDN and ... |
|----------------------|--------------|---------|-------------------|---------|--------------|------------------------|
| FSLABWIN-BV7LHC1N208 | 10.153.0.208 | FS | 08:00:27:18:8C:18 | | | |

Export Table

- Manage
- Classify
- Hosts
- Audit
- Authenticate
- Remediate
- Restrict
- AWS EC2
- AWS IAM
- AWS VPC
- Azure
- Malwarebytes
- Malwarebytes Breach Remediation Get Results
- Malwarebytes Breach Remediation Scan
- Malwarebytes vSphere
- Cancel Actions
- Add To List...
- Refresh
- Delete
- Clear Detection
- Comment
- Information
- Threat Protection
- Exceptions

Profile Compliance All Policies

IPv4 Address: 10.153.0.208 Hostname: WV-BV7LHC1N208 Function: Vendor and Model: VMware Operating System: Windows

Host classification: Windows

General

IPv4 Address: 10.153.0.208
Admission: DHCP
Device is NAT: No
DHCP device class: Win7
DHCP device OS: corp
DHCP hostname: WV-BV7LHC1N208
DHCP options fingerprint: 1,3,6
DHCP request fingerprint: 10.153.0.208

Specify Malwarebytes Breach Remediation Get ...

Malwarebytes - Remediation Scan Results

Parameters Schedule

Update Interval (seconds) 0

OK Cancel

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

Host Details 10.153.0.208

Host Details

Profile Compliance All Policies Policy Actions

Malwarebytes Breach Remediation Get Results

Action triggered by: CounterACT operator
 Action Status: Success
 Request for Action Time: November 26 11:10:08 AM
 Update Interval (seconds): 0
 Action Schedule: Action runs immediately.

| Time | CounterACT Appliance | Problems |
|-------------------|----------------------|---|
| 11/26 11:10:43 AM | 10.153.0.223 | Action Success - Please check the scan results in Inventory |

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

<) FORESCOUT Home Asset Inventory Policy

Views Malwarebytes - Scan Results

Search External Devices

Geolocation

AWS IAM User

Advanced Threat Detection

Malwarebytes - Scan Results

Microsoft Vulnerabilities

Vulnerability

Switch

Filters

All

Segments (252)

Organizational Units

Default Groups

Groups

| Logged on User | Threat Name | Threat Path | Threat Type | MD5 Hash | Action Taken | Threat Count | Scan End Time | No. of Hosts | Last Update | Last Host |
|-----------------------|-----------------------|---------------------------------|-------------|---------------------------------|--------------|--------------|---------------------|--------------|----------------------|--------------|
| FSLABAdmin@7LUC11HQ08 | None | None | None | None | scan | 0 | 2019-11-27T12:06... | 1 | 11/26/19 11:10:43 AM | 10.163.0.208 |
| WINDOWS10MALWUser | Backdoor.Farfi | C:\USER\USER\DESKTOP\DL.EXE | file | 1175A48FC6B410B47D2BDD9FDEF33 | quarantine | 27 | 2019-10-22T08:40... | 1 | 11/26/19 11:20:24 AM | 10.163.0.208 |
| WINDOWS10MALWUser | Trojan.Dropper | C:\USER\USER\DESKTOP\U11_2.PAR | file | D3698E15DAB76CF1ABFD43ED9C6E0 | quarantine | 27 | 2019-10-22T08:40... | 1 | 11/26/19 11:20:24 AM | 10.163.0.208 |
| WINDOWS10MALWUser | Generic.Malware.Susp. | C:\USER\USER\DESKTOP\U11_2.PAR | file | D3698E15DAB76CF1ABFD43ED9C6E0 | quarantine | 27 | 2019-10-22T08:40... | 1 | 11/26/19 11:20:24 AM | 10.163.0.208 |
| WINDOWS10MALWUser | Generic.Malware.Susp. | C:\USER\USER\DESKTOP\U211.PAR | file | C12A00304E41ED0ACDF20B72920E6F | quarantine | 27 | 2019-10-22T08:40... | 1 | 11/26/19 11:20:24 AM | 10.163.0.208 |
| WINDOWS10MALWUser | Backdoor.Agent.ZG | C:\USER\USER\DESKTOP\PAH3.EXE | file | E4B8B7D630DEE8B8B8EDCF0C6564 | quarantine | 27 | 2019-10-22T08:40... | 1 | 11/26/19 11:20:24 AM | 10.163.0.208 |
| WINDOWS10MALWUser | Generic.Malware.Susp. | C:\USER\USER\DESKTOP\WIN.EXE | file | 2C8193D8DCAB76C77DC3F371C6C11 | quarantine | 27 | 2019-10-22T08:40... | 1 | 11/26/19 11:20:24 AM | 10.163.0.208 |
| WINDOWS10MALWUser | RiskWare.Agent.Kaygen | C:\USER\USER\DESKTOP\WIN.EXE | file | 2033A07D02690C31FA33D817FC7FB | quarantine | 27 | 2019-10-22T08:40... | 1 | 11/26/19 11:20:24 AM | 10.163.0.208 |
| WINDOWS10MALWUser | Backdoor.Bot | C:\USER\USER\DESKTOP\KVAQI.EXE | file | 6EFC410CE17AFED027D04FC8B71F7 | quarantine | 27 | 2019-10-22T08:40... | 1 | 11/26/19 11:20:24 AM | 10.163.0.208 |
| WINDOWS10MALWUser | Trojan.Dropper | C:\USER\USER\DESKTOP\RYV.EXE | file | 74A4B2736939C83B01BD76307626595 | quarantine | 27 | 2019-10-22T08:40... | 1 | 11/26/19 11:20:24 AM | 10.163.0.208 |
| WINDOWS10MALWUser | Generic.Malware.Susp. | C:\USER\USER\DESKTOP\PHM42.EXE | file | 6ED2034FD13690653DCC00BFAE16DF | quarantine | 27 | 2019-10-22T08:40... | 1 | 11/26/19 11:20:24 AM | 10.163.0.208 |
| WINDOWS10MALWUser | Trojan.Dropper | C:\USER\USER\DESKTOP\BJL.EXE | file | A10D7893FAF234783DC6F2E4337C1D | quarantine | 27 | 2019-10-22T08:40... | 1 | 11/26/19 11:20:24 AM | 10.163.0.208 |
| WINDOWS10MALWUser | Generic.Malware.Susp. | C:\USER\USER\DESKTOP\BIN333.PAR | file | 7DF6C37FCA04F8B0C66F9D1A0728E | quarantine | 27 | 2019-10-22T08:40... | 1 | 11/26/19 11:20:24 AM | 10.163.0.208 |
| WINDOWS10MALWUser | Generic.Malware.Susp. | C:\USER\USER\DESKTOP\SERVER.EXE | file | 17F83D76928E497870827C60AC3D81 | quarantine | 27 | 2019-10-22T08:40... | 1 | 11/26/19 11:20:24 AM | 10.163.0.208 |

Hosts

Logged on User: WINDOWS10MALWUser
Threat Name: Generic.Malware.Suspicious
Threat Path: C:\USER\USER\DESKTOP\U11_2.PAR
Threat Type: file
MD5 Hash: D3698E15DAB76CF1ABFD43ED9C6E0
Action Taken: quarantine
Threat Count: 27
Scan End Time: 2019-10-22T08:40:47Z

1 OF 202 HOSTS

| Host | IP Address | Segment | MAC Address | Comment | Display Name | Switch IP/Port and... | Switch Port Alias | Switch Port Name | Function | Actions |
|-----------------------|--------------|---------|--------------|---------|--------------|-----------------------|-------------------|------------------|----------|---------|
| FSLABAdmin@7LUC11HQ08 | 10.163.0.208 | FS | 000c29a886c8 | | | | | | Computer | |

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

Host Details 10.153.0.208

Host Details

Profile Compliance All Policies Policy Actions

Malwarebytes Breach Remediation Get Results

Action triggered by: CounterACT operator

Action Status: Failed

Request for Action Time: November 26 11:32:37 AM

Update Interval (seconds): 0

Action Schedule: Action runs immediately.

| Time | CounterACT Appliance | Problems |
|-------------------|----------------------|---------------------------------------|
| 11/26 11:33:11 AM | 10.163.0.223 | Action Failed - MBBR Scan In Progress |

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

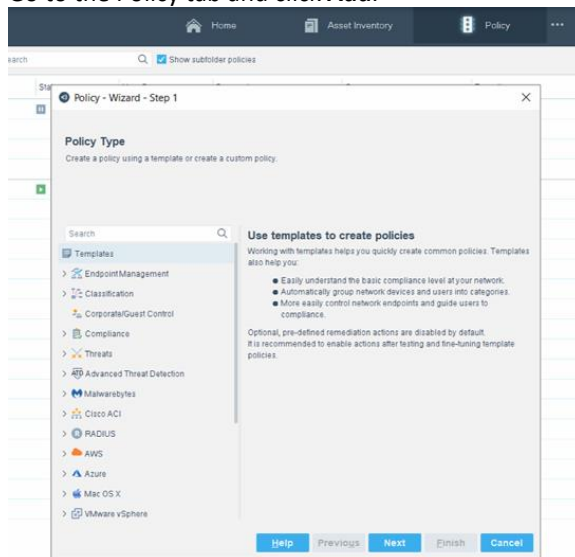
Policy Templates

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**.

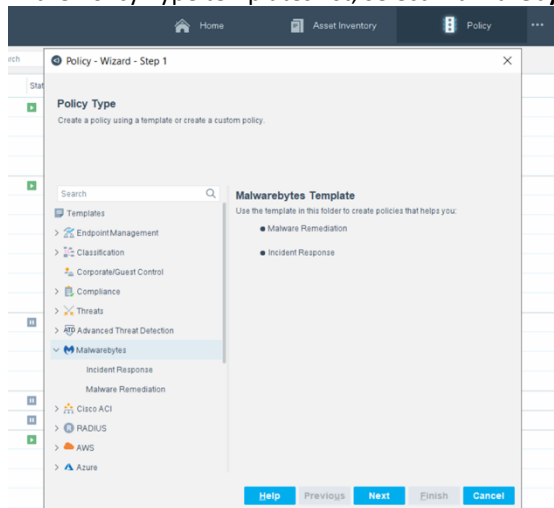
Follow the steps below to create a custom policy based on each of the default Malwarebytes policy templates.

Create a custom Incident Response policy

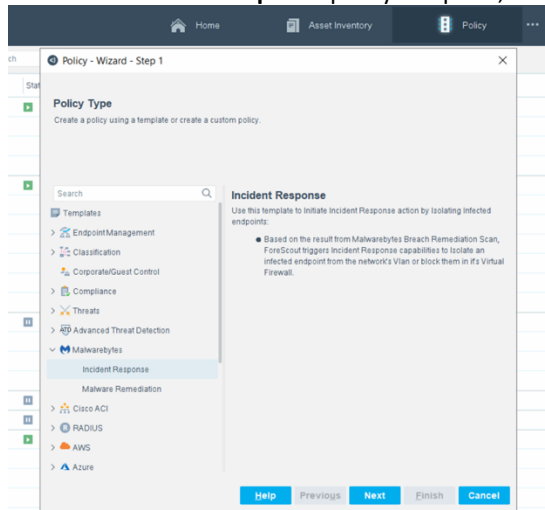
1. Go to the Policy tab and click **Add**.



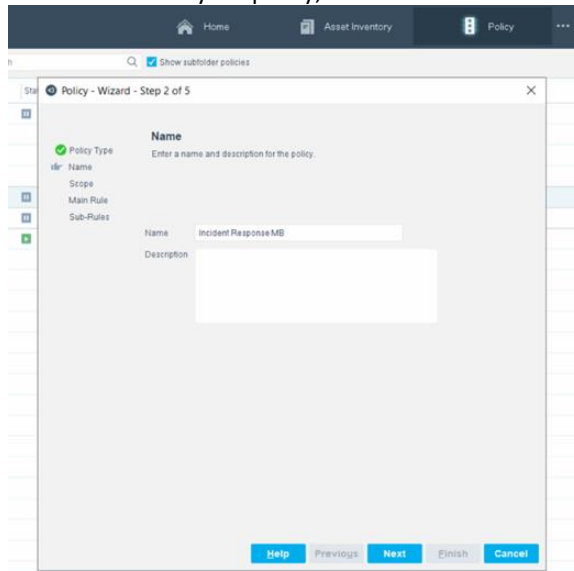
2. In the Policy Type templates list, select **Malwarebytes**.



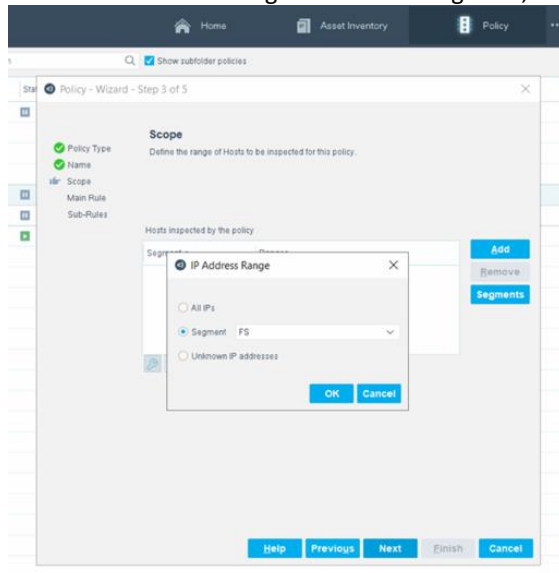
3. Select the **Incident Response** policy template, then click **Next**.



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

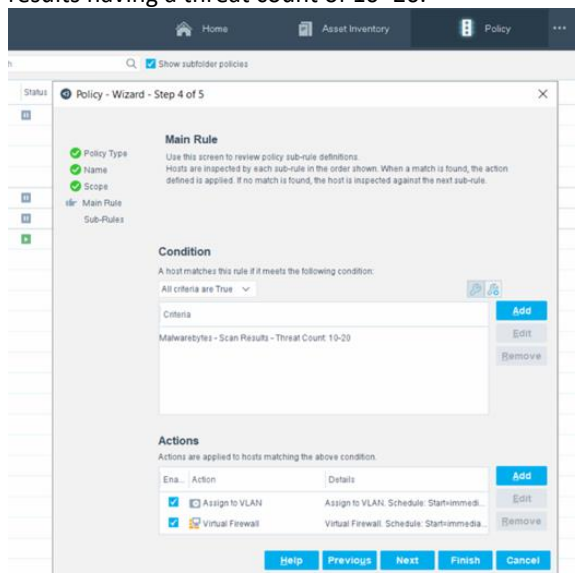


5. Select an IP address range or Network Segment, then click **Next**.



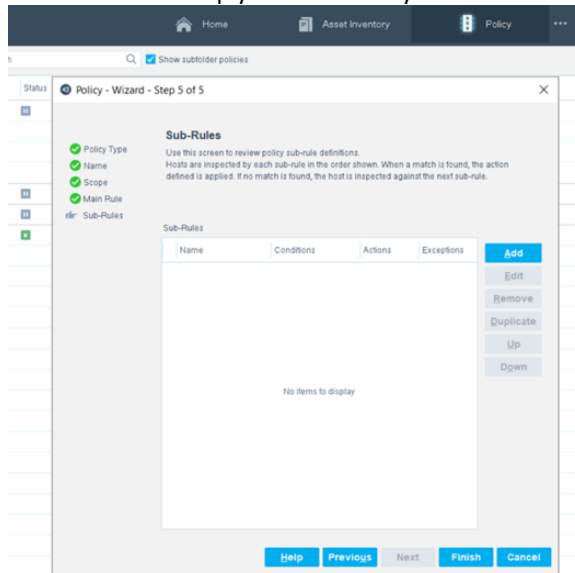
6. Edit the conditions and actions which trigger the policy automation.

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



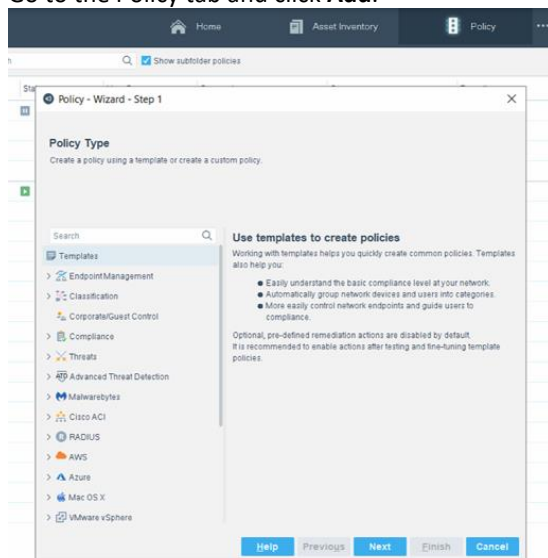
7. After setting conditions and actions, click **Next**.

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

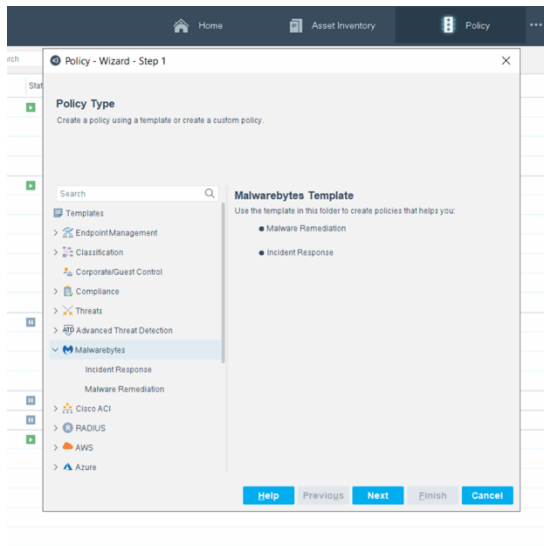


Create a custom Malware Remediation policy

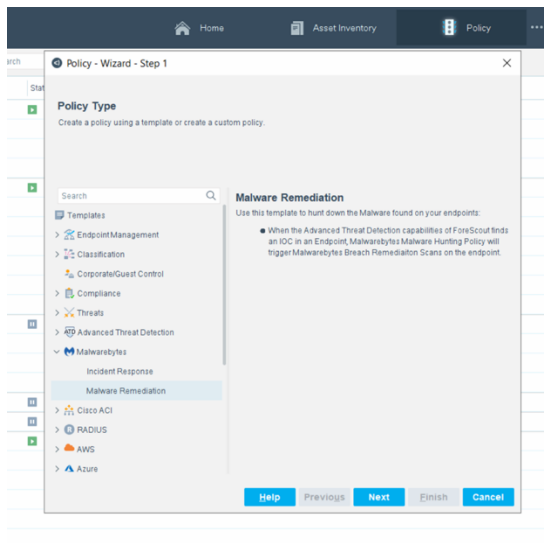
- Go to the Policy tab and click **Add**.



- 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**.

Policy - Wizard - Step 2 of 5

Name
Enter a name and description for the policy.

Name: Malware Remediation M...

Description:

Help Previous Next Finish Cancel

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

Policy - Wizard - Step 3 of 5

Scope
Define the range of Hosts to be inspected for this policy.

Hosts inspected by the policy

Segment: FS

IP Address Range

☐ All IPs

☒ Segment: FS

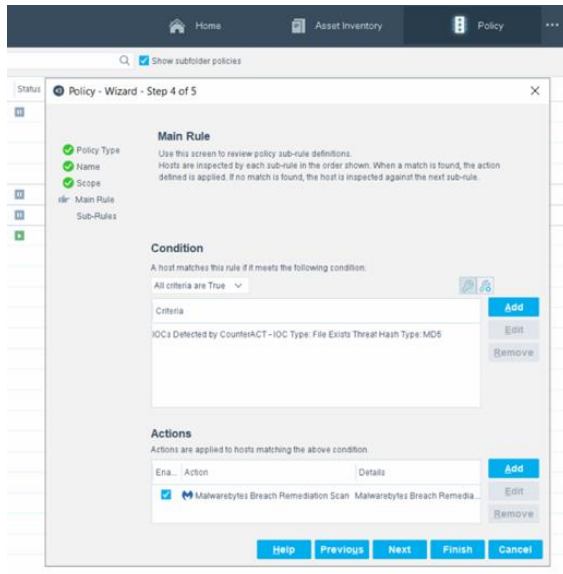
☐ Unknown IP addresses

OK Cancel

Help Previous Next Finish Cancel

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.

