

#### Malwarebytes Breach Remediation for Forescout CounterACT<sup>®</sup> 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<sup>®</sup> 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.

Open				×
Look in:	Forescout	Rohin	~ 🦸 🏱 🖽 •	
Recent Items	FS_MBBR			
	CounterA	CT-Plugin-malwarebytes-1.0.0-42.fpi		
	ForeScou	t-plugin_sdk-1.1.1-11010025.fpi		
Desktop	File name:	CounterACT-Plugin-malwarebytes-1.0.0-42.fpi		Install
Decumente	Files of type:	Forescout Package Installation files (.fpi)	~	Cancel

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.

	() Malwarebytes	Not running	1.0.0
--	-----------------	-------------	-------

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

## Configuration

1. Select <u>Malwarebytes</u> and click **Configure**.



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

CounterACT Devices          Defauit       +         Choose where MBBR package is located       Local Path >         MBBR License       xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	Maiwarebytes		
Default       +         Choose where MBBR package is located       Local Path >         MBR.License       xxxxx+xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	CounterACT Devices ~		
Choose where MBBR package is to call Path >         MBR.License       xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	Default +		
MBR License       xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	Choose where MBBR package is located	Local Path 🗸	
Enable Systog         Systog Server IP/Hostname         Systog Port	MBBR License	00000-00000-00000	
Syslog Port	Enable Syslog		
Syslog Port	Syslog Server IP/Hostname		
	Syslog Port		
Tot Annu Undo Holo			
Tot Apply Linds Hole			
Tet Apply Upda Hain			
Tet Apply Upda Hain			
Test Apply Upda Hain			
Test Jonly Undo Holo			
Test deply linds Hole			
Test Apply Updo Holo			
Tast Apply Updo Holo			
Test Apply Undo Holo			
Test Apply Under Hole			
Test Apply Ondo <u>H</u> elp			Test Apply Undo Help

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

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

The assigned license key <u>must</u> be entered In the **MBBR License** field

<u>Note</u>: If the correct license key is not entered, the user cannot initiate the scan. CounterACT will display "Action Failed – Please Enter Correct License Key".

Host Details 10.153	.0.208	-	×
lost Details			
Profile Compliance	All Policies Policy Actions		
Malwarebytes Breac	h Remediation Scan		
Action triggered by:	CounterACT operator		
Action Status:	Failed		
Request for Action Time	e: December 09 11:51:24 AM		
Remediation ZIP:	FS_MBBR.zip		
Scan Type:	Threat		
Scan Action:	Scan		
Update Interval (second	ds): 0		
Action Schedule:	Action runs immediately.		
3 Time ▼	CounterACT Appliance	Problems	
😣 12/09 11:52:28 AM	10.153.0.223	Action Failed - Please Enter Correct License Key	
Kill Process on Wind	dows		
Action triggered by:	CounterACT operator		
Action Status:	Success		
Request for Action Time	e: November 12 03:06:39 PM		
The name of the proces	ss to kill: Notepad		
Action Schedule:	Action starts immediately.		
🔊 Timo 🗸	Counter&CT Appliance	Droklome	

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. <u>If you are</u> using a web path, set Update Interval to a minimum of 500 seconds.

**<u>Note</u>**: If the SecureConector<sup>™</sup> 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.

Remediation ZIP	FS_MBBR.zip	~	
Scan Type	Full 🗸		
Scan Action	Scan 🗸		
Jpdate Interval (seconds)	0 0		
Fags :	Add Tags		

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 <u>Remediation ZIP</u> file name). The Remediation Repository window opens.
- 2. Click **Add**. Download the Malwarebytes Breach Remediation package file from <u>https://downloads.malwarebytes.com/file/FS\_MBBR</u>.

Remediation Re	pository	×
File Name 🔺	Title	Add
FS_MBBR.zip		Edit
		Remove
		Download
1 items (0 selected)		
		OK Cancel

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

ile Name 🔺	File editor     X	Add
S_MBBR.zip	File name:	Edit
		Remove
	Title:	Download
	Description:	
		E .
items (0 selec	<u>H</u> elp OK Cancel	

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**.

Look in:	Jownload		~	🏚 😂 🖽 •
-	7z1900-x	54.exe		
	2019-08-	23 release - draft 001.docx		
ecent Items	Archive.z	p		
	ChromeS	etup.exe		
	CounterA	CT-Plugin-malwarebytes-1.0.0-1	000008.fpi	
Desktop	ereds.zip			
_	DOC-334	).pdf		
	DOC-336	2.pdf		
ocuments	ForeScou	-plugin_sdk-1.1.1-11010025.fpi		
	FS_MBBR	zip		
	Malwarel	ytes _CEM-5_vm-init-demo_requ	uestID-92faf541-f2ac-4	13ab-9941-68e636ce9
This PC				
	<u> </u>			
1	File name:	FS_MBBR.zip		Open

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

File Name 🔺	File ed	ditor X	Add
FS_MBBR.zip	File name:	FS_MBBR.zip	Edit
			Remove
	Title:	mbbr	Download
	Description		
	mbbr pack	age	
1 itams /0 salar		Help OK Cancel	

6. Click **OK** to close the <u>File editor</u> window. Click **OK** again to close the <u>Remediation Repository</u> 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.

- <) FORESCOUT B Policy 🚖 Home All Hosts 10 Online Views MAC Address IPv4 Address Segment Display Name Switch IP/FQDN and <) All Hosts FSLABW 10.153.0.208 FS 0r 💾 Export Table > 
  Policies
  > 
  History 🕑 Manage Classify 🐥 Notity **O**Restrict AWS EC2 Filters Search 8 AWS IAM AWS VPC Seg A Azure Organizationa arebytes Breach Remediation Get Re **€** Ma 🔠 Default Gr Malwarebytes Breach Remediation Scan Where NSX IPv4 Address: 10.163. MAC Address: 000c29 Vendor and Model: V Groups del: Vi × Cancel Actions + Add To List. General G Recheck 10.11 To Delete DHC No Clear Dete Winc Clear Dete Applicatio IPv4 Addres 22+ Comment. 1 Information corp. WIN-63,6 1,3,6 Excent
- 2. Choose Malwarebytes Breach Remediation Scan.

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

Remediation ZIP	FS_MBBR.zip	~	
Scan Type	Full 🗸		
Scan Action	Scan 🗸		
Update Interval (seconds)	0 0		
Tags :	Add Tags		

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

Host Details 10.153.0.	208			>
lost Details				
Profile Compliance	All Policies Policy Actions			
Malwarebytes Breach I	Remediation Scan			
Action triagered 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		
Malwarabytas Braach I	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.			
				Clos

# **Getting the Results**

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

<) FORESCO	UT.			6	а н	lome	a ·	Asset Inventory	Policy	
Views	«	All Hosts	10.153.0.20	8		Online/Offline V	Show	only unassigned		
Search	Q	Host 🕶	IPv4 Address	Segment	M	AC Address	Comm	ent Display N	ame Switch IP/FQ	ON and Swit
<) All Hosts (202)		FSLARWIN-RV7LH21N008	10 153 0 208	FS	00					
> 🚯 Policies						💾 Export Table				
> 🏦 History						🛃 Manage	>			
						Classify	>			
						A Notity	>			
						W Aunda				
						A AGAI	<i></i>			
						2 Authenticate	>			
						+ Remediate	>			
						Ø Restrict	>			
Filters						AWS EC2	>			
Search	Q					8 AWS IAM	>			
<1 All						AWS VPC				
> Seaments (202)							ĺ.			
						Azure	,			
Organizational Onlia		Profile Compliance All Policies				Malwarebytes	>	Malwarebytes Breach	Remediation Get Results	
> 🔠 Detault Groups		IPv4 Address	10.153.0.208 Hostname:	WIN-BV7LH21NQ08 Fu	unctie	Whiware NSX	>	Malwarebytes Breach	Remediation Scan	
> 🔢 Groups		MAC Address	: 000c29a886c8 Domain: F	SLAB Operating Sys	tem:	🛃 VMware vSphere	>			
		Vendor and M	Iodel: VMware			× Cancel Actions	>			
		Search Q A Y Host	classification: Windows			+ Add To List				
		General Ge	neral			C Bashark				
		Applications IPv	Address		10.1:	Greener				
		Adr	nission:	2	DHC	Delete				
		Der	ice is NAT:	2	No	ntertion 🖉 Clear Detection				
		DH	CP device class:	+	Wind	Comment				
		DH	CP device OS:			1 Information	>			
		DH	CP Domain Name:		corp.	×				
		DH	CP Hostname:	I	62.6	X Threat Protection	>			
		DH	CP request financoint	I	1.26	Exceptions	>	262		
		04	°P Saruar Arkirass		10.15	944				

${f 0}$ Specify Malwarebytes Breach Remediation Get $ imes$
Malwarebytes - Remediation Scan Results
Parameters Schedule
Update Interval (seconds)
OK Cancel

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

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.         Image: Time *       CounterACT Appliance       Problems	Host Details 10.153.0.208 -							
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.	Host Detai	ls						
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.         Immediate Time *       CounterACT Appliance	Profile Cor	npliance	All Policies	Policy Actions				
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.	Malwarebyt	es Breach R	emediation	Get Results				
Action Status:     Success       Request for Action Time:     November 26 11:10:08 AM       Update Interval (seconds):     0       Action Schedule:     Action runs immediately.       Immediate:     CounterACT Appliance   Problems	Action trigger	ed by:	CounterACT of	operator				
Request for Action Time: November 26 11:10:08 AM Update Interval (seconds): 0 Action Schedule: Action runs immediately. Immer CounterACT Appliance Problems	Action Status:		Success					
Update Interval (seconds): 0 Action Schedule: Action runs immediately.	Request for A	ction Time:	November 26	11:10:08 AM				
Action Schedule: Action runs immediately.  CounterACT Appliance Problems	Update Interv	al (seconds):	0					
CounterACT Appliance Problems	Action Sched	ule:	Action runs im	nmediately.				
	🕑 Time 🕶		Coun	terACT Appliance	Problems			
O 11/26 11:10:43 AM 10.153.0.223 Action Success - Please check the scan results in Inventory	✓ 11/26 11:1	0:43 AM	10.15	3.0.223	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	Γ.				4	Home Home	Asset Inventor		Policy					
Views		Malwarebytes - Scan	Results Search		Q									
-G- External Devices	Q	Logged on User +	Threat Name	Threat Path		Threat Type	MD5 Hash	Action Ta	ken Threat Count	Scan End Time	No. of Hosts	Last Update		Last Host
Geolocation		FSLA8IA.dministrator	None	None		None	None	acan	0	2019-11-21712:05		11/26/19 11:10	43 AM	10.153.0.208
AWS IMM User		WINDOWS1(MALWAR)User	Backdoor/Farfi	C:IUSERSIUSERIO	DESKTOPIDHLEXE	file	1170AAABFC50BA1D8AFD2BDD3	DE5E33 quarantin	27	2019-10-22708:40	1	11/26/19 11:28	24 AM	10.153.0.208
Advanced Threat Detection		WINDOWS10MALWARiUser	Trojan Dropper	CIUSERSIUSERIO	DESKTOPI711_2.RAR	file	D3696E10DAB576DF1ABFD483ED	I9C66E0 quarantin	27	2019-10-22T08:40	.1	11/26/19 11:28	24 AM	10.153.0.208
Malwarebytes - Scan Results		WINDOWS1(MALWAR)User	Generic Matware/Suzp	C:IUSERSIUSERID	DESKTOP/711_2.RAR	file	D3696E10DAB576DF1ABFD483ED	9C55E0 quarantin	27	2019-10-22T08:40	1	11/26/19 11:28	24 AM	10.153.0.208
Wicrosoft Vulnerabilities		WINDOWS10MALWAR/User	Generic Malware/Susp.	CIUSERSIUSERIO	DESKTOPI2211.RAR	file	C12A00304641ED09ADF280B7280	205EF quarantin	27	2019-10-22708.40	1	11/26/19 11:28	24 AM	10.153.0.208
😳 VMware NSX		WINDOWS10MALWARiUser	Backdoor.Agent.ZG	C:IUSERSIUSERIO	DESKTOPMH3.EXE	tia	E48E897D5308DE6E88B0EDBCF0	C05664 guarantin	27	2019-10-22708:40	Ŧ	11/26/19 11:28	24 AM	10.153.0.208
fft Switch		WINDOWS10MALWARUJaer	Generic Mahware/Susp	CIUSERSIUSERIO	DESKTOPIWINEXE	tie	2C8193D55CCA8A776C77DC3F37	1C6C11 guarantin	27	2019-10-22708:40	1	11/26/19 11:28	24 AM	10.163.0.208
Filtors		WINDOWS10MALWAR/User	RiskWare Agent Keyger	CIUSERSIUSERID	DESKTOPICN.EXE	tie	2033A6D7D02690C31FA53D87178	C7FFB guarantin	27	2019-10-22T08:40		11/26/19 11:28	24 AM	10.153.0.208
earch	Q	WINDOWS1(MALWAR)User	Backdoor.Bot	C:IUSERSIUSERIO	DESKTOPIXIAOQLEXE	Tie .	6EFCA10C8E17AFE05D27D95FC0	B716F7 guarantin	27	2019-10-22708-40	1	11/26/19 11:28	24 AM	10.153.0.208
All		WINDOWS10MALWARNIser	Trojan Dropper	CHISERSUISER	DESKTOPIYK EXE	file.	748482735839C8838D18D763D7	626595 ausrantin	27	2019-10-22708:40	1	11/26/19 11:28	24.654	10 153 0 208
Segments (202)		WINDOWS1(MALWARV.Iser	Generic Matware/Sute	CHISERSUSERI	DESKTOPHEMH 2 EXE	Tie	6ED2034ED13690653DECC90REE	AC16DF quarantin	27	2019-10-22708:40	1	11/26/19 11:28	24 AM	10 153 0 208
Organizational Units		WINDOWS1(MALWARV.law	Trojan Dropper	CHISERSUSERI	DESKTOPIRJEXE	tie	A0DD7583FAFF234783DCF527F4	937C1D quarantin	27	2019-10-22708-40		11/26/19 11:28	24 AM	10 163 0 208
E Default Groups		WINDOWS1 (MALI WARU Iser	Conorie Mahwara/Surre	CHICEPSHICEPH	DESKTORIBINISTS RAP	Nie	7DE90C37ECA904EB0BC650ED17	A0220E Augestin	27	2010.10.22709.40		11/26/10 11:20	24.84	10 163 0 209
🔠 Groups		WINDOWST (MALWARVING	Ganatic Matazara/Suzn	CHISERSUSER	DESKTOP/SERVER EVE	Nie .	176593076928549782082205004	C2DB1 avarantin	27	2010-10-22108-40	-	11/26/10 11:20	24 844	10 153 0 208
				0.036H3/036H6	DESKTOPGENVEREXE			(200) qualation		2010-10-22100.40				10.103.0.200
		Hosts												
		Malwarebytes - Scan Resu	Logged on User. 1 Threat Name. Get Threat Path. C.3U Is MD5 Hash: D3691 Action Taken. qu Threat Count. 27 Scan End Time: 2	WINDOWS10MAL seric Matware/Su SERSIUSERIDES SE10DA8576DF1. irantine 019-10-22108.40	WARIUSer Ispicious KTOPU711_2.RAR ABFD483ED9C55E0 9:47Z	Search	Q							1 OF 202 HOST
		Host *		IPv4 Address	Segment	MAC Addre	ss Comment	Display Name	Switch IP/FQDN	and Switch PortAl	as Swit	th Port Name	Function	Actions
		FSLABIWIN-BV7LH21NG	108	10.153.0.208	FS	000c29a886	c8						Computer	(M in 10)

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.		Get Results operator 11:32:37 AM omediately.						
🕑 Time 🕶	Cour	iterACT Appliance	Problems					
🙁 11/26 11:33:11 AM	10.15	3.0.223	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**.

		Â		Asset Inv		Policy		
n 🗌	-	Q. 🗹 Show su	bfolder policies					
Sta	O Policy - Wizard	i - Step 2 of 5					×	
		Name						
	Policy Type Iller Name Scope	Enter a na	me and description for the	policy.				
	Main Rule Sub-Bulat							
		Name	Incident Response MB					
		Description						
			Help	Previous	Next	Einish Cance	-1	

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

		🖌 Home	Asset Inv		Policy	
U.S.	Q 🖬 s	how subfolder policies				
Stal 🥥 Policy - Wiz	ard - Step	3 of 5			×	
Połcy Type     Połcy Type     Name     se Scope     Main Rule     Sub-Rules	Sc De Hos	ope Ine the range of Hosts to be to inspected by the policy	inspected for this policy.			
	Seg	IP Address Range     All IPs     Segment FS     Unknown IP addres	e	×	Add Remove Segments	
			ок	Cancel		
			Help Previous	Next	Elnish Cancel	

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.

		🏫 Hom	e 📄 Asset Inventory	Policy ···
rch	Policy - Wizard - Step 1			×
Stat	Policy Type Create a policy using a template	or create a c	ustom policy.	
	Search  ■ Temptates  > 2  Search  Temptates  > 2  Search/anagement  > 2  Compliance       Compliance  > 2  Compliance  > 2  Compliance  > 2  Matwarebytes  Matware Remediation  > 2  Mause Act  > 3  AUS  > 2  Ause	Q	Malwarebytes Template Use the template in this tolocite Malware Remediation e incident Response	s that helps you:
			Help Previous Next	Einish Cancel

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	- Home	a		6	Policy	
h.:	Q	Show s	ubfolder policies					
Sta	Policy - Wizard -	Step 3 of 5					×	
	Policy Type Name We Scoe Main Rule Sub-Rules	Scope Define the Hosts insp- Segr	range of Hosts to be inz whet by the policy IP Address Range All IPs Segment PS Unknown IP addresses	spected for	this policy. × OK Cancel		Add Remove Segments	
			He	ip f	Previous Next	Einish	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.

