

## Anti-Virus

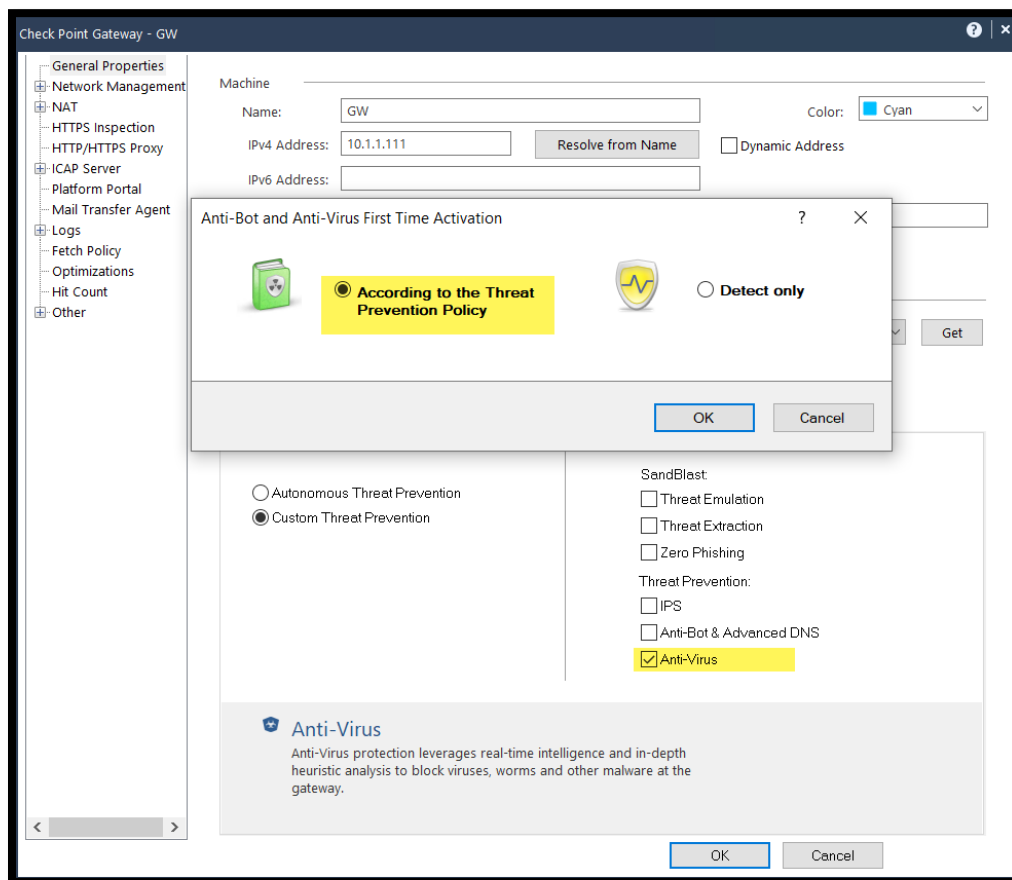
### Introduction

Anti-virus solutions protect computers and remove malicious software or code designed to damage computers or data. Advanced anti-virus solution adopts methodologies that combine global scanning, human expert threat analysis, industry collaboration, cloud integration, and alerting services.

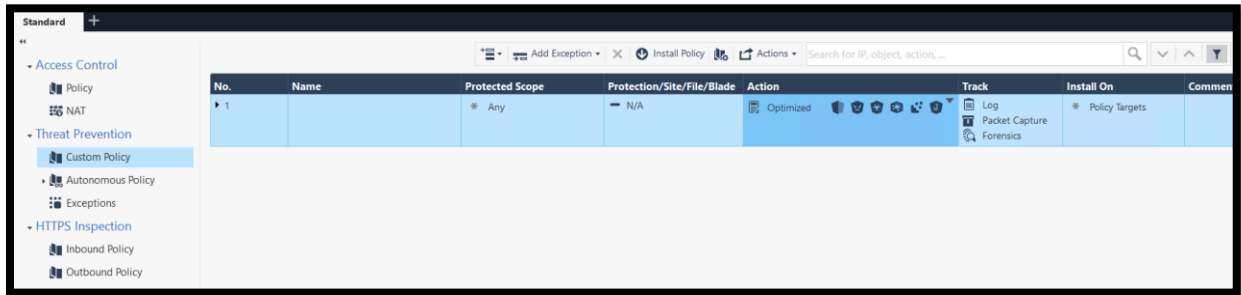
### Exercise 1: Onboarding

In this exercise, we will enable and test the protections provided by the Anti-Virus blade.

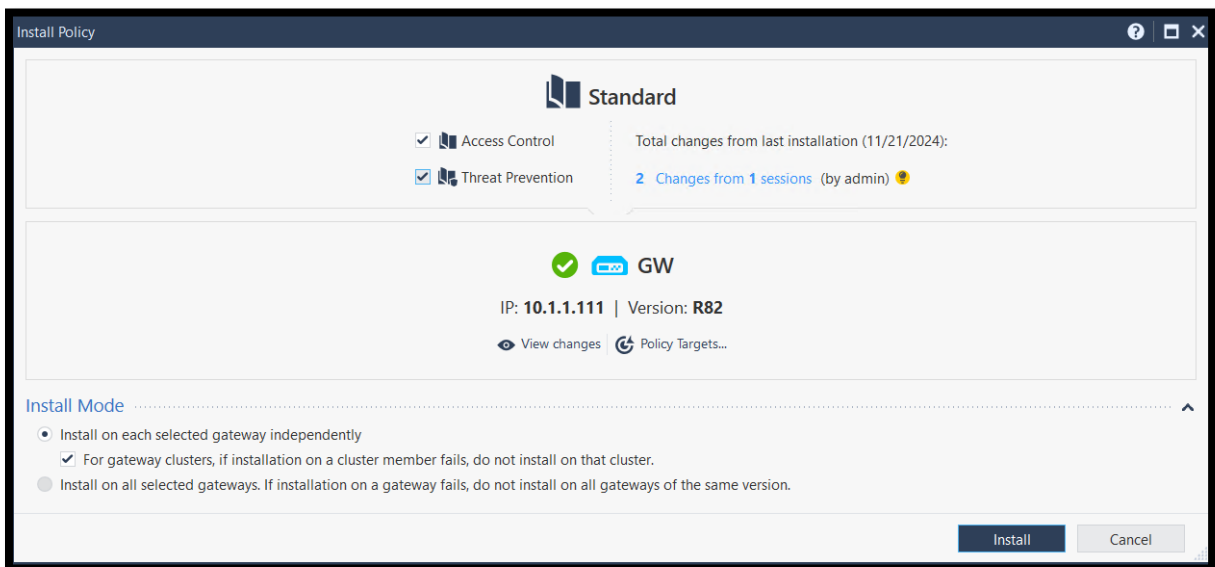
1. Edit the GW object and enable the **Anti-virus** blade. Make sure IPS is disabled. And save the changes.



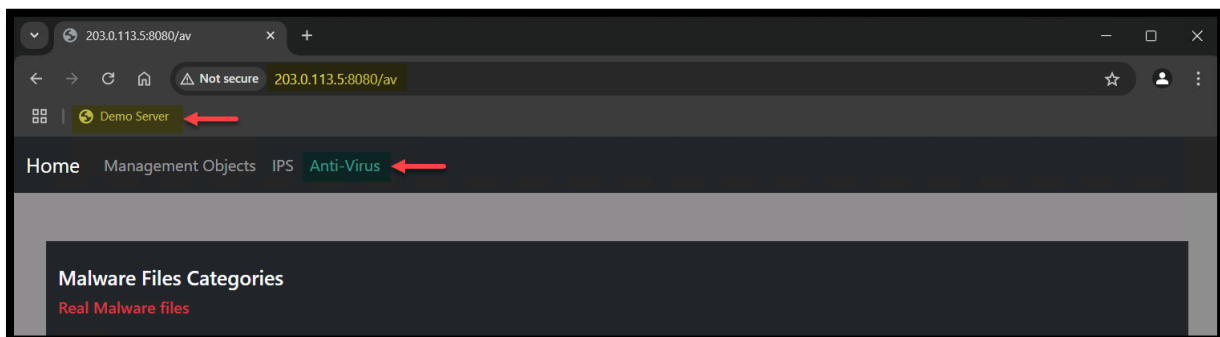
2. Review the default Threat Prevention and the assigned profile.



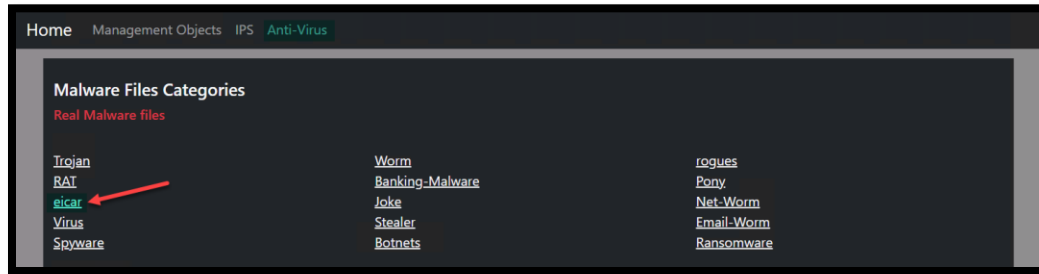
3. Install the Access Control and Threat Prevention Policies.



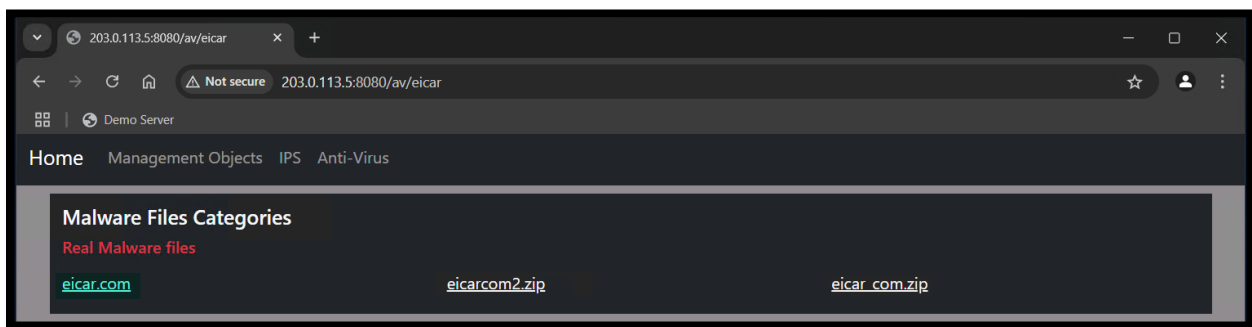
4. Open the RDP session to the Windows Client (10.1.1.222) and use the bookmarked link to access the Demo server (<http://203.0.113.5:8080>)



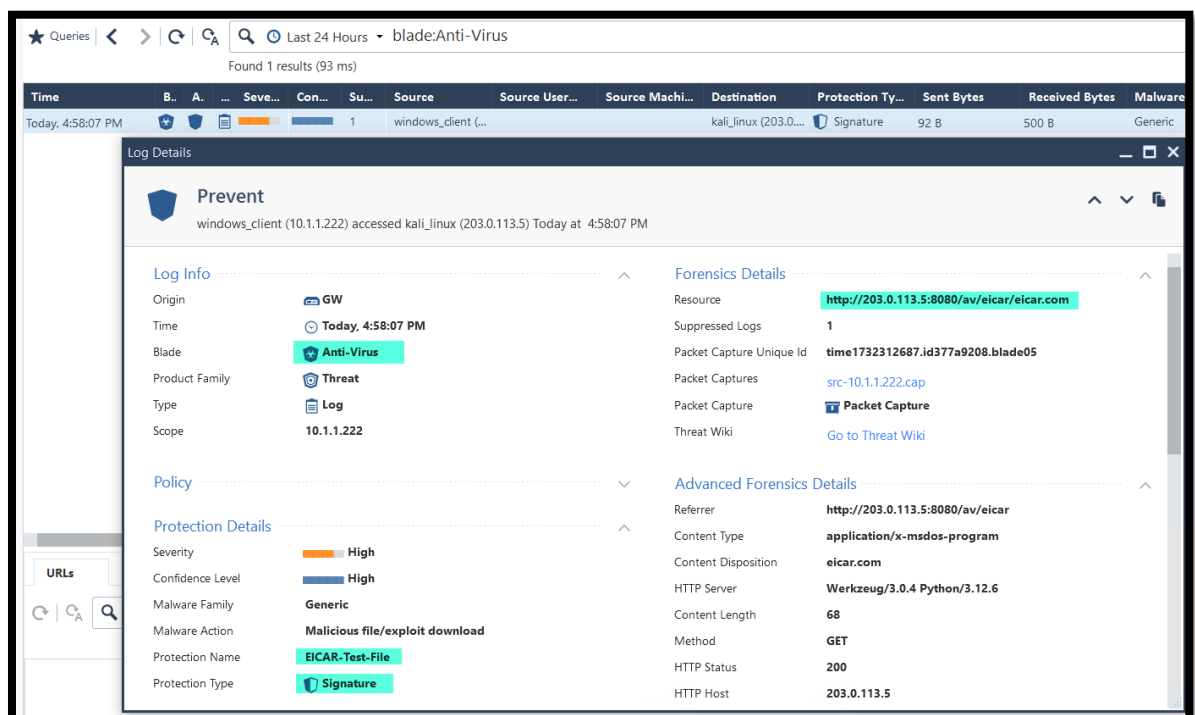
- While in the Anti-Virus test page, open the **eicar** directory.



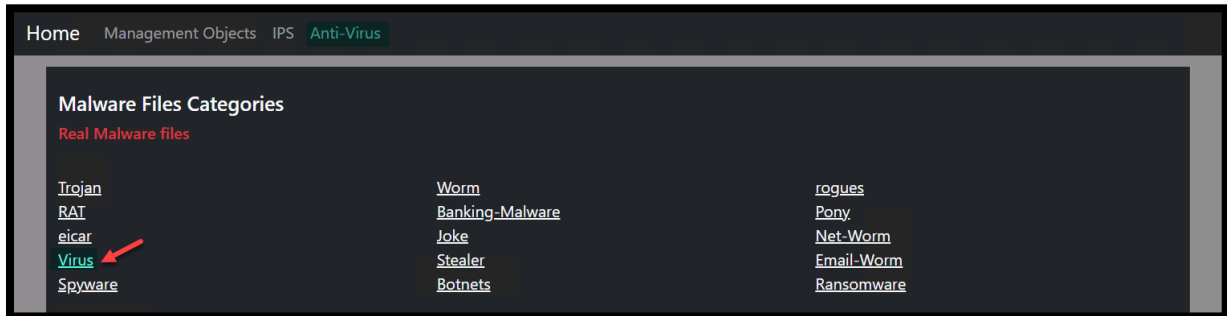
- Try to download the file eicar.com by clicking on it. Notice that the connection was blocked.



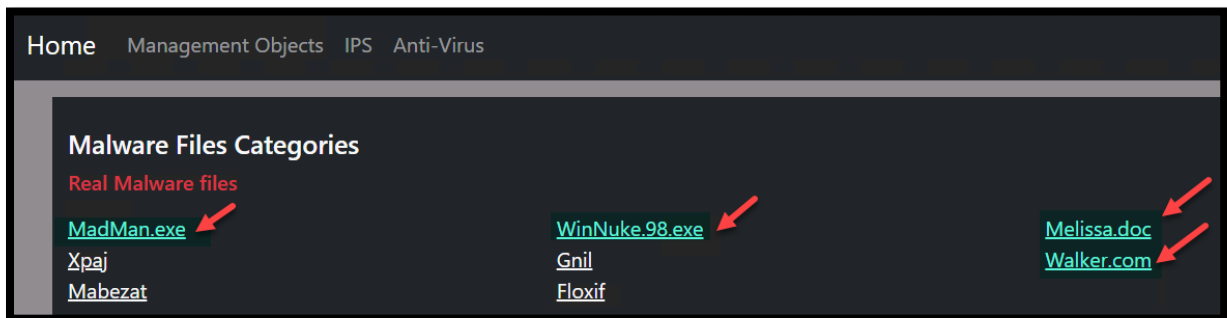
- From SmartConsole, filter the logs to show only anti-virus logs.



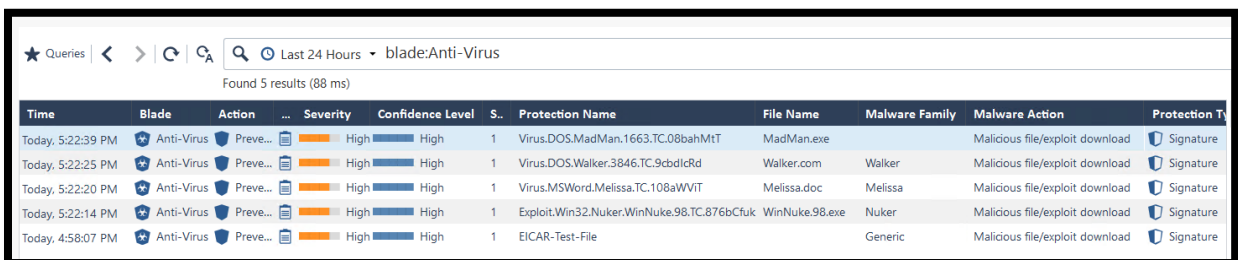
8. From the Windows Client, browse to the **Virus** directory on the demo server.



9. Try to download multiple known malicious files.



10. Reorder the default columns (drag & drop) to show the **Protection Name**, **File Name** and the **Malware family** fields by default.

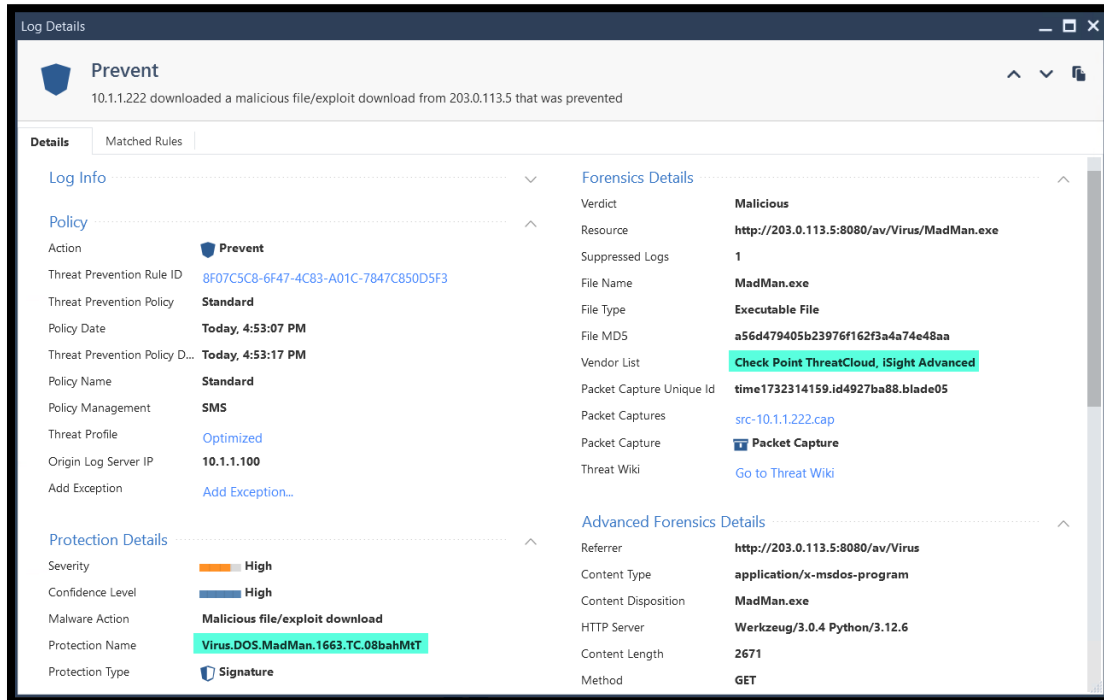


The screenshot shows the 'Queries' section of the Check Point management console. A search filter 'Last 24 Hours blade:Anti-Virus' is applied. The results table is displayed with the following columns: Time, Blade, Action, Severity, Confidence Level, S., Protection Name, File Name, Malware Family, Malware Action, and Protection Type.

Time	Blade	Action	Severity	Confidence Level	S.	Protection Name	File Name	Malware Family	Malware Action	Protection Type
Today, 5:22:39 PM	Anti-Virus	Prevent	High	High	1	Virus.DOS.MadMan.1663.TC.08bahMtT	MadMan.exe		Malicious file/exploit download	Signature
Today, 5:22:25 PM	Anti-Virus	Prevent	High	High	1	Virus.DOS.Walker.3846.TC.9cbdlcRd	Walker.com	Walker	Malicious file/exploit download	Signature
Today, 5:22:20 PM	Anti-Virus	Prevent	High	High	1	Virus.MSWord.Melissa.TC.108aWvT	Melissa.doc	Melissa	Malicious file/exploit download	Signature
Today, 5:22:14 PM	Anti-Virus	Prevent	High	High	1	Exploit.Win32.Nuker.WinNuke.98.TC.876bCfuk	WinNuke.98.exe	Nuker	Malicious file/exploit download	Signature
Today, 4:58:07 PM	Anti-Virus	Prevent	High	High	1	EICAR-Test-File		Generic	Malicious file/exploit download	Signature

11. Review the log generated for one of the files we tried to download in the previous step.

- Note:
  - In many cases, more than one protection or blade can block the same attack. For example, IPS blade can block the **eicar.com** malware.
  - A packet capture is generated like the IPS blade.



**Log Details**  
Prevent  
10.1.1.222 downloaded a malicious file/exploit download from 203.0.113.5 that was prevented

**Details** | Matched Rules

**Log Info**

**Policy**

- Action: Prevent
- Threat Prevention Rule ID: 8F07C5C8-6F47-4C83-A01C-7847C850D5F3
- Threat Prevention Policy: Standard
- Policy Date: Today, 4:53:07 PM
- Threat Prevention Policy D...: Today, 4:53:17 PM
- Policy Name: Standard
- Policy Management: SMS
- Threat Profile: Optimized
- Origin Log Server IP: 10.1.1.100
- Add Exception: [Add Exception...](#)

**Protection Details**

- Severity: High
- Confidence Level: High
- Malware Action: Malicious file/exploit download
- Protection Name: Virus.DOS.MadMan.1663.TC.08bahMT
- Protection Type: Signature

**Forensics Details**

- Verdict: Malicious
- Resource: http://203.0.113.5:8080/av/Virus/MadMan.exe
- Suppressed Logs: 1
- File Name: MadMan.exe
- File Type: Executable File
- File MD5: a56d479405b23976f162f3a4a74e48aa
- Vendor List: Check Point ThreatCloud, iSight Advanced
- Packet Capture Unique Id: time1732314159.id4927ba88.blade05
- Packet Captures: src-10.1.1.222.cap
- Packet Capture: [Packet Capture](#)
- Threat Wiki: [Go to Threat Wiki](#)

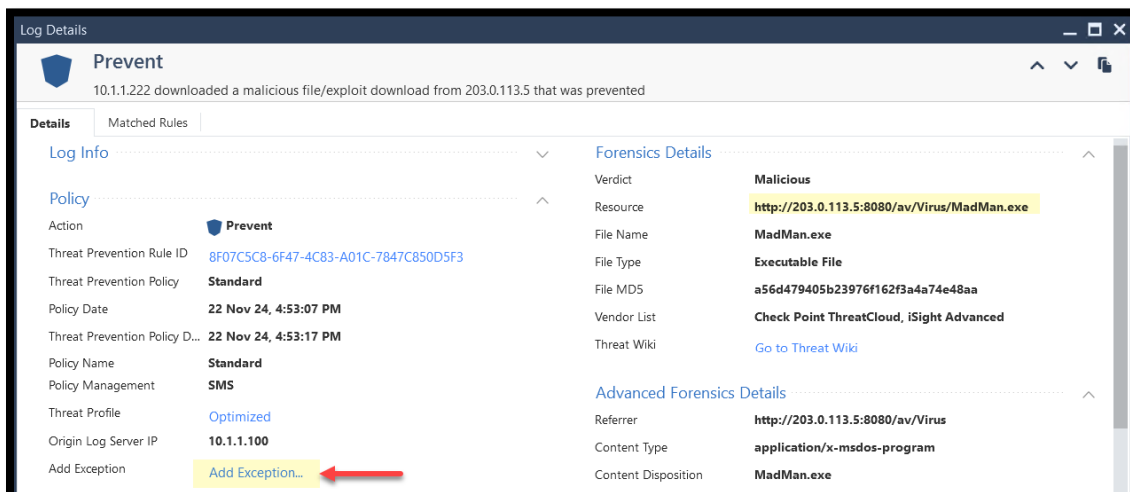
**Advanced Forensics Details**

- Referrer: http://203.0.113.5:8080/av/Virus
- Content Type: application/x-msdos-program
- Content Disposition: MadMan.exe
- HTTP Server: Werkzeug/3.0.4 Python/3.12.6
- Content Length: 2671
- Method: GET

## Exercise 2: Exceptions – Overriding the Default Actions

In some scenarios, it is required to override the default action of the Anti-Virus blade. For example, a file is believed to be dropped due to a false-positive verdict, or a file should be delivered for testing purposes. In this exercise, we will test creating such exceptions.

1. In the prevent log file for the last file we downloaded (MadMan.exe), click Add Exception.



**Log Details**  
Prevent  
10.1.1.222 downloaded a malicious file/exploit download from 203.0.113.5 that was prevented

**Details** | Matched Rules

**Log Info**

**Policy**

- Action: Prevent
- Threat Prevention Rule ID: 8F07C5C8-6F47-4C83-A01C-7847C850D5F3
- Threat Prevention Policy: Standard
- Policy Date: 22 Nov 24, 4:53:07 PM
- Threat Prevention Policy D...: 22 Nov 24, 4:53:17 PM
- Policy Name: Standard
- Policy Management: SMS
- Threat Profile: Optimized
- Origin Log Server IP: 10.1.1.100
- Add Exception: [Add Exception...](#)

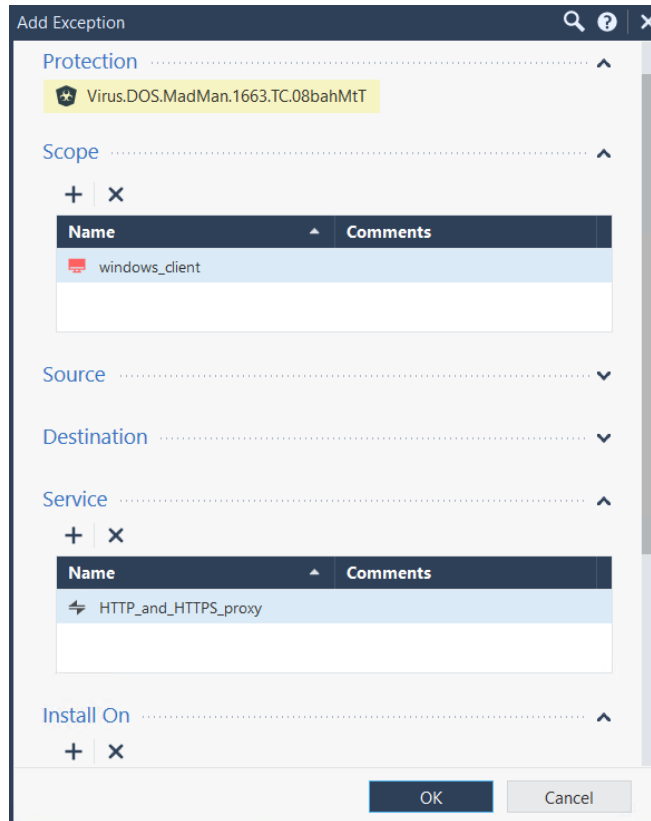
**Forensics Details**

- Verdict: Malicious
- Resource: http://203.0.113.5:8080/av/Virus/MadMan.exe
- File Name: MadMan.exe
- File Type: Executable File
- File MD5: a56d479405b23976f162f3a4a74e48aa
- Vendor List: Check Point ThreatCloud, iSight Advanced
- Threat Wiki: [Go to Threat Wiki](#)

**Advanced Forensics Details**

- Referrer: http://203.0.113.5:8080/av/Virus
- Content Type: application/x-msdos-program
- Content Disposition: MadMan.exe

2. Review the fields and save the changes.



**Add Exception**

**Protection**

Virus.DOS.MadMan.1663.TC.08bahMtT

**Scope**

+ x

Name	Comments
windows_client	

**Source**

**Destination**

**Service**

+ x

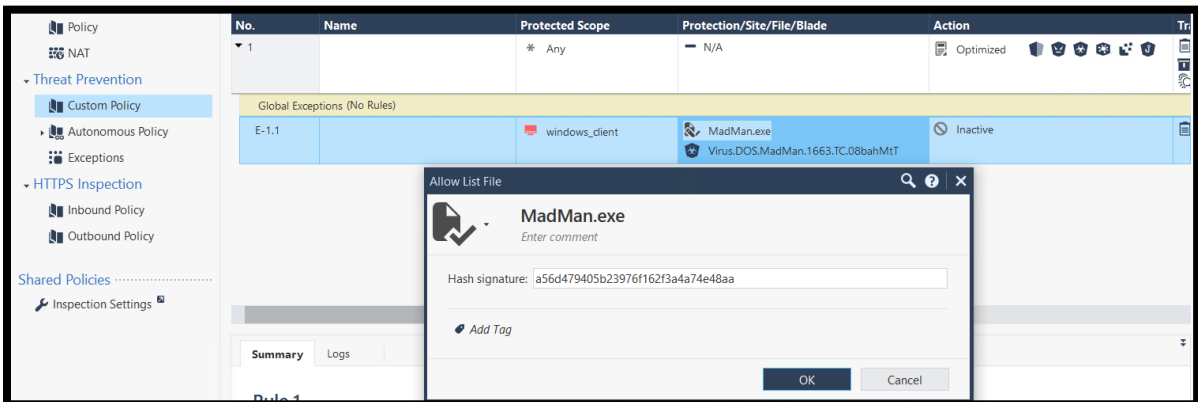
Name	Comments
HTTP_and_HTTPS_proxy	

**Install On**

+ x

OK Cancel

3. Review the changes in the Threat Prevention rule base (Expand the rule to see the exception list).



**Policy**

NAT

Threat Prevention

Custom Policy

Autonomous Policy

Exceptions

HTTPS Inspection

Inbound Policy

Outbound Policy

Shared Policies

Inspection Settings

No.	Name	Protected Scope	Protection/Site/File/Blade	Action
1		* Any	N/A	Optimized

Global Exceptions (No Rules)

No.	Name	Protected Scope	Protection/Site/File/Blade	Action
E-1.1		windows_client	MadMan.exe	Inactive

**Allow List File**

MadMan.exe

Enter comment

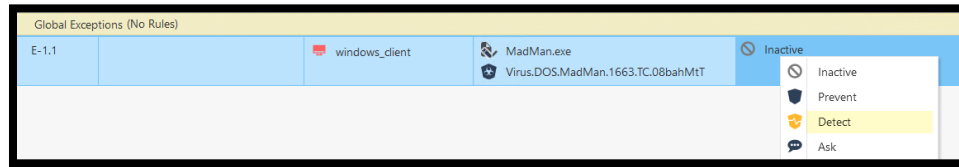
Hash signature: a56d479405b23976f162f3a4a74e48aa

Add Tag

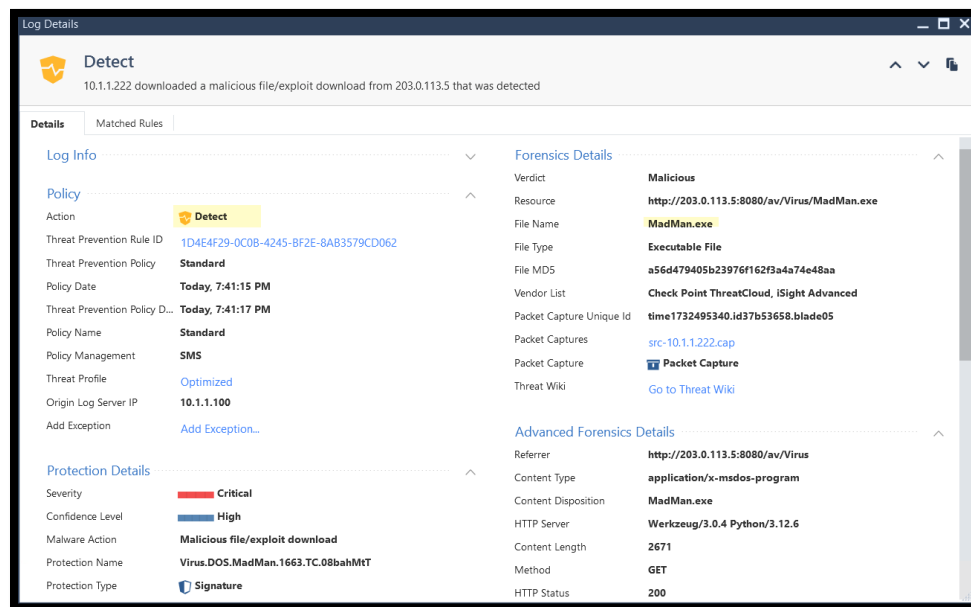
OK Cancel

- Note that the exception was added using the protections name and the file hash (MD5).
- Either one can enforce the rule.

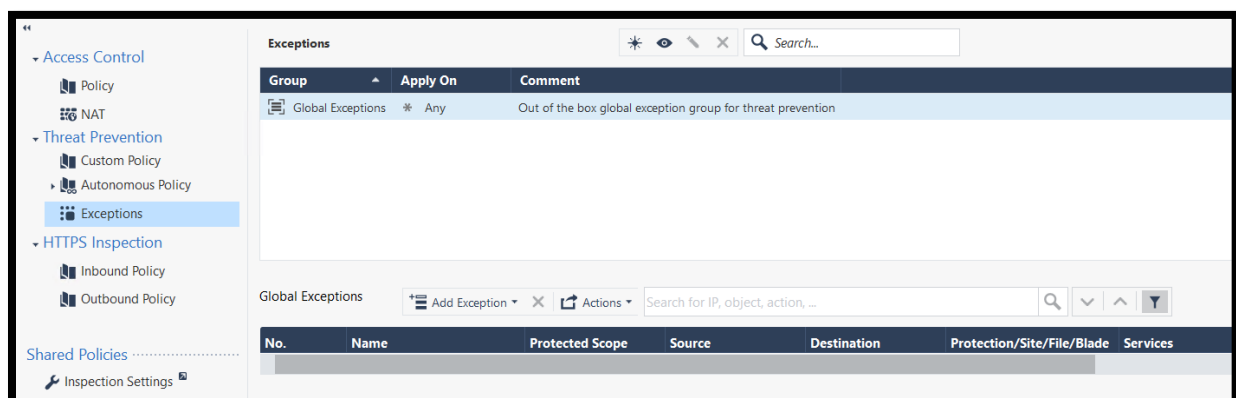
4. Change the action of the exception to Detect so we can get a detect log and install the Threat Prevention policy.



5. Try to download the same file again and notice it is now possible download the file through the gateway and is blocked by the browser. Review the log and make sure that the file was detected.



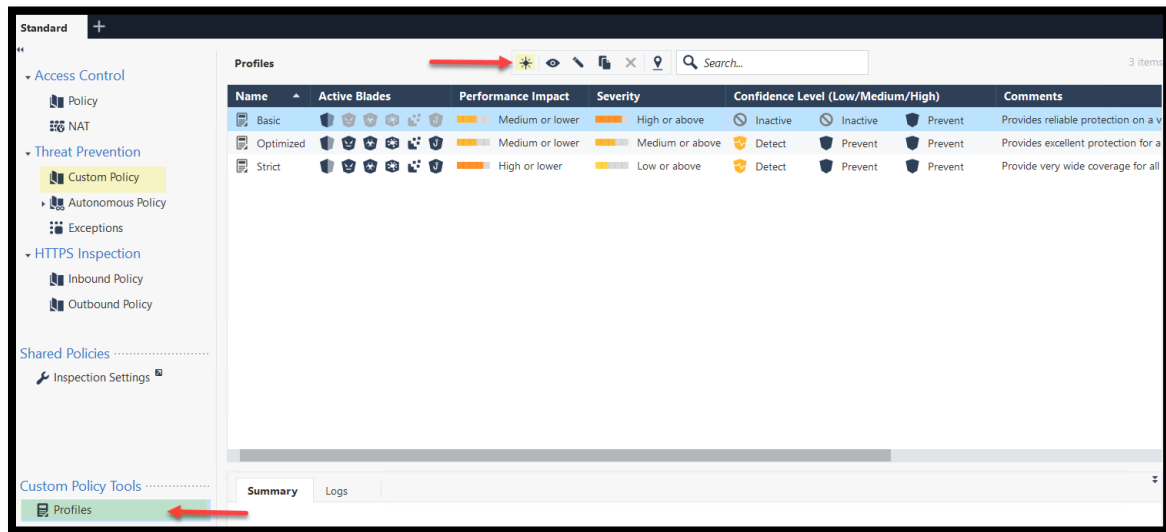
- The exception we made is known as a local exception. It is applied to one rule. Global exceptions can be added via the global exceptions list.



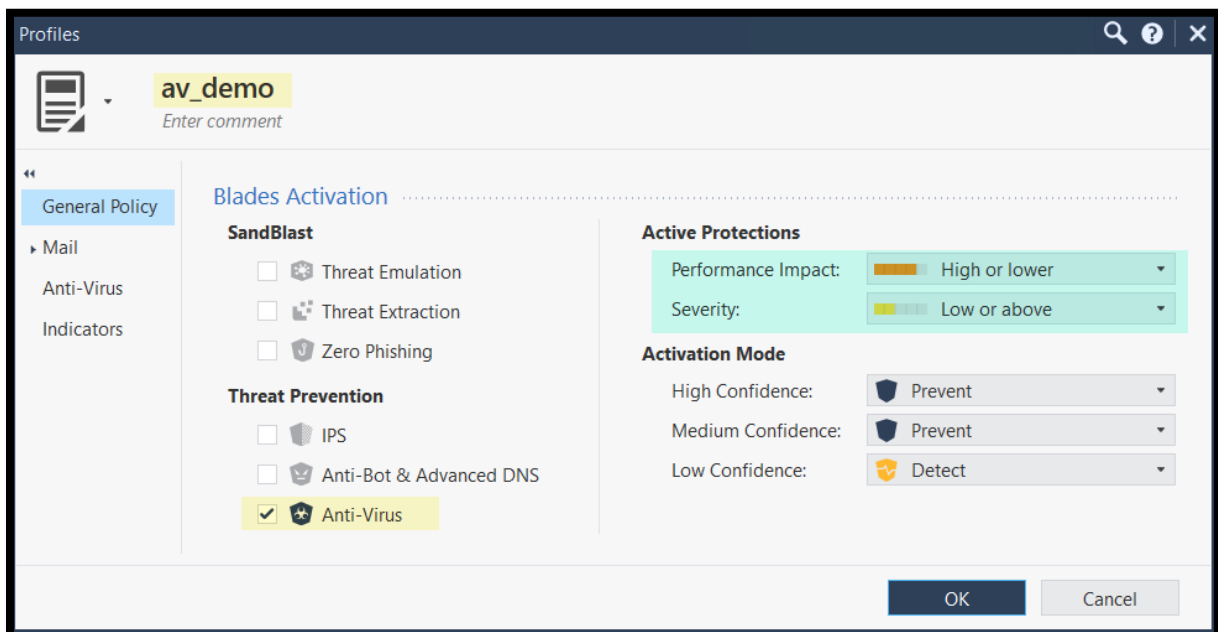
## Exercise 3: Profile Customizations

It is possible to configure the Anti-Virus settings to drop/Allow/Deep inspect certain file type. In this exercise, we will create a new threat profile and customize the settings.

1. Under the Custom Threat Prevention Policy, select Profiles and create a new profile.

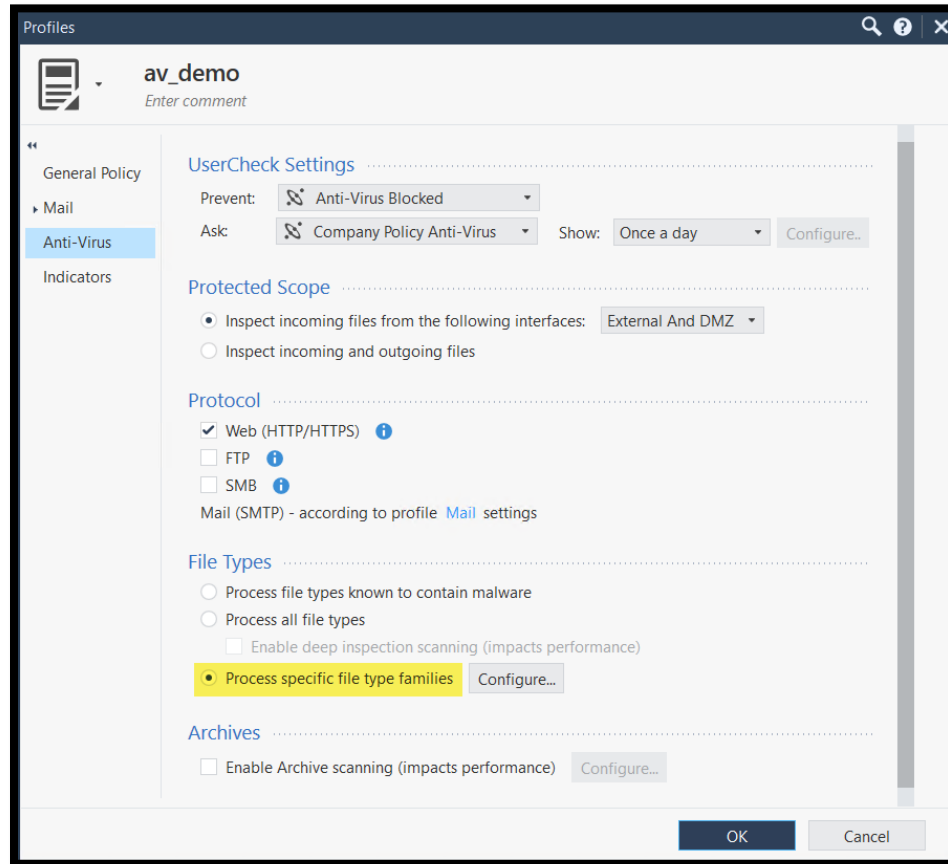


2. Give it a proper name, with only Anti-Virus enabled and customize the Active Protections to match the settings below.

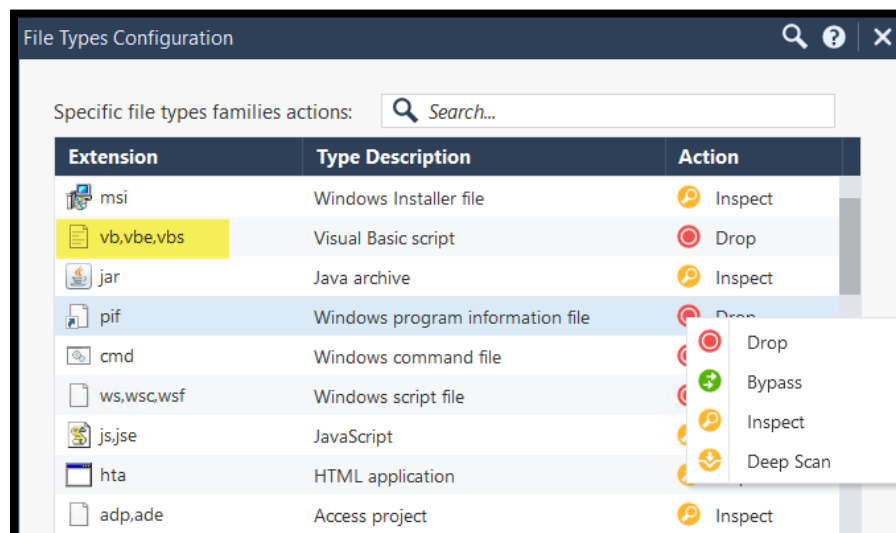




- Under the Anti-virus tab in the profile settings, change the File Types settings to “Process specific file type families”.



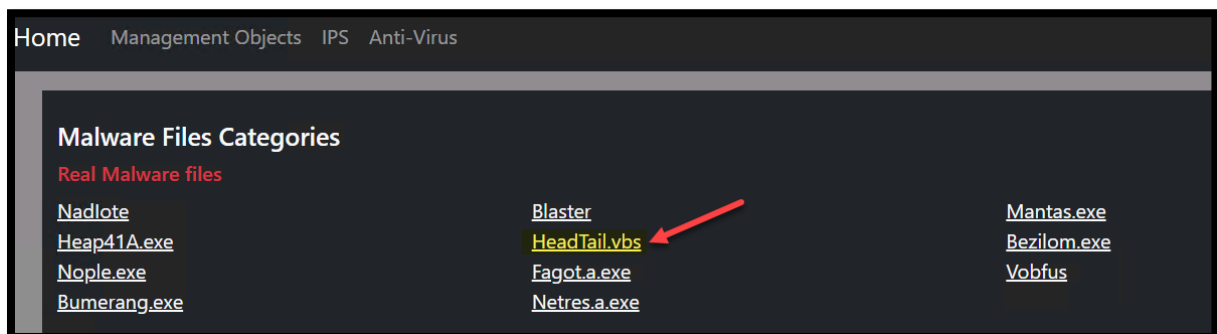
- Click Configure and review the actions per file type family.



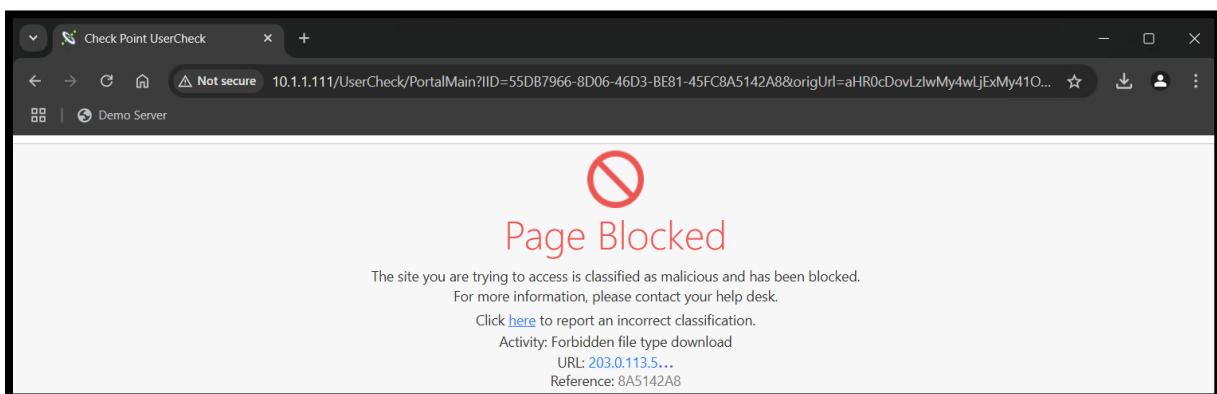
- This feature allows you to take different actions based on the file type.
  - The default action for the file type with action set to Drop will always be dropped by the Anti-Virus blade.
5. Assign the newly created profile to the default rule in the Threat Prevention policy and Install the policy.

No.	Name	Protected Scope	Protection/Site/File/Blade	Action
1		* Any	N/A	av_demo
Global Exceptions (No Rules)				
E-1.1		windows_client	MadMan.exe Virus.DOS.MadMan.1663.TC.08bahMtT	Detect

6. Try to download the under Worm - > **HeadTail.vbs**

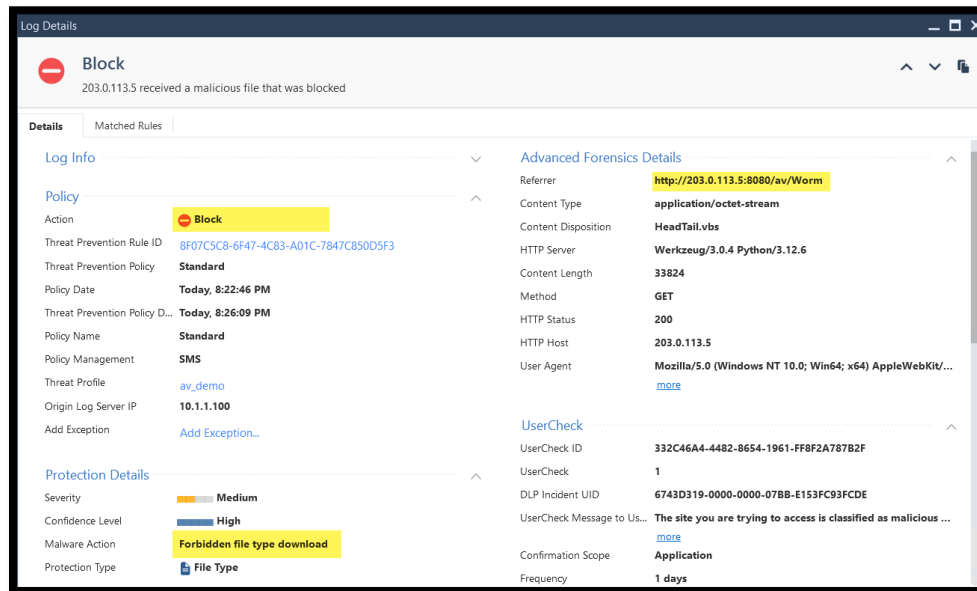


7. Notice that the user is redirected to a block message. In such configurations, the GW can block the attempt without the need to analyze the file.



- Note that in the case above, it is unnecessary to consult the cloud to retrieve the verdict before enforcing the policy. The file is blocked based on its type.

8. Review the log in SmartConsole and notice that the action is Block.

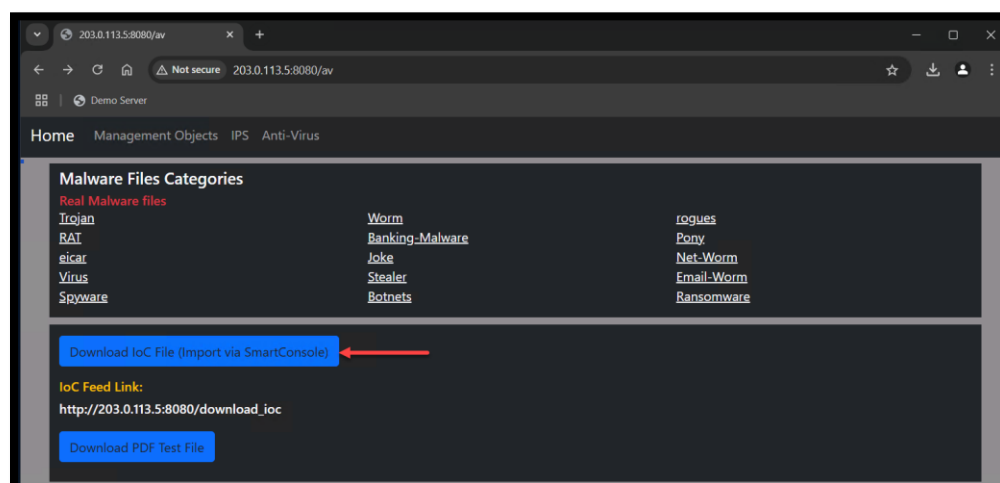


## Exercise 4: Threat Indicators - IoC

Threat Indicators lets you upload Indicator files that contain sets of observables. These observables are added to the Threat Prevention policy.

- Indicator – Set of observables which represent a malicious activity in an operational cyber domain, with relevant information on how to interpret it and how to handle it.
- Observable – An event or a stateful property that can be observed in an operational cyber domain. For example: IP address, MD5 file signature, URL, Mail sender address.

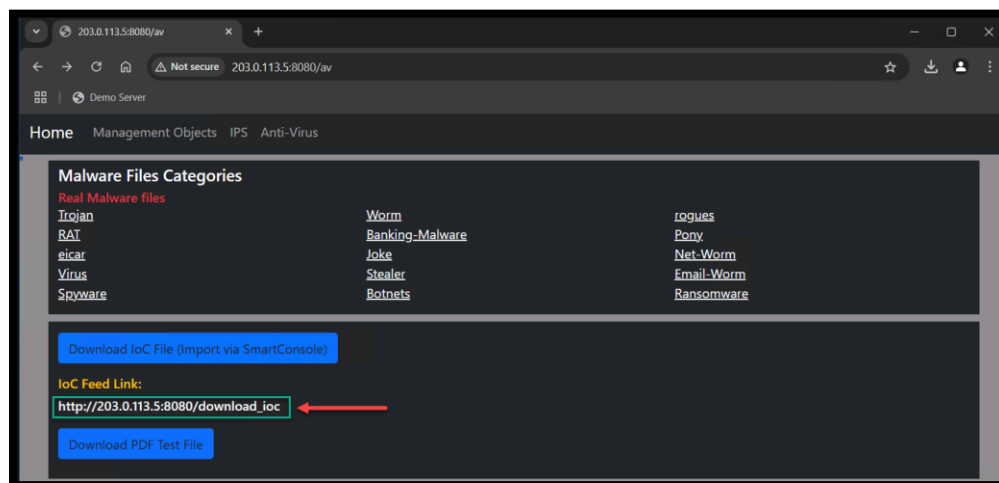
1. Download the IoC demo file from the Demo Server



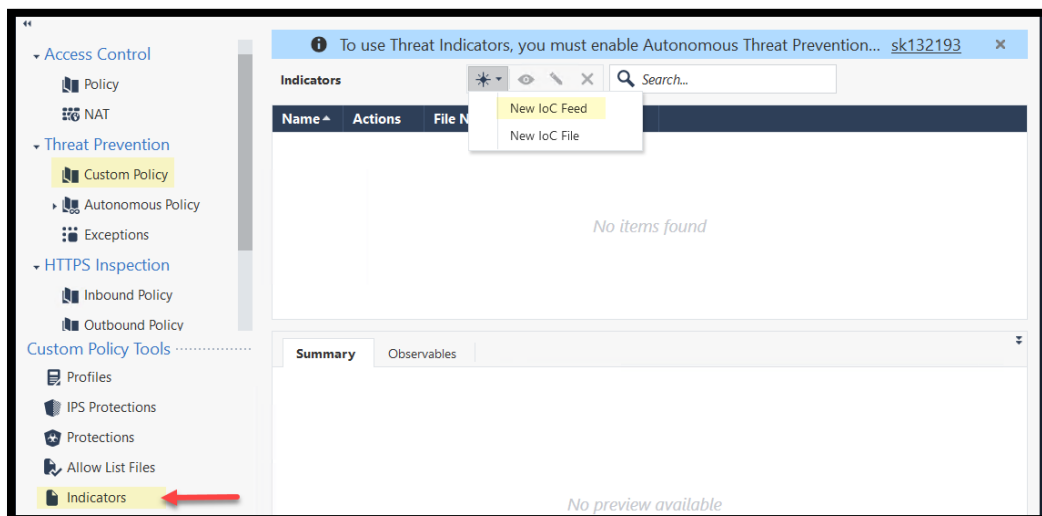
- Open the file and review the contents and the format. The file adds a feed of observables to block a URL and a File using its MD5 with the Anti-Virus blade.

	A	B	C	D	E	F	G
1	#! DESCRIPTION = IoC Demo						
2	#! REFERENCE = SBT						
3	# All lines beginning "#" are comments						
4	# All lines beginning "#!" are metadata read by the SW						
5	# UNIQ-NAME,VALUE,TYPE,CONFIDENCE,SEVERITY,PRODUCT,COMMENT						
6	block_md5	20b2ca0d0694fdc37e3fb3f55754bdd4	MD5	high	high	AV	ioc_test_md5
7	block_url	http://example.com	URL	high	high	AV	ioc_test_url
8	block_domain	stamdomain.com	domain	high	high	AB	ioc_test_domain
9	block_ip	4.2.2.1	IP	high	medium	AB	ioc_block_ip
10							

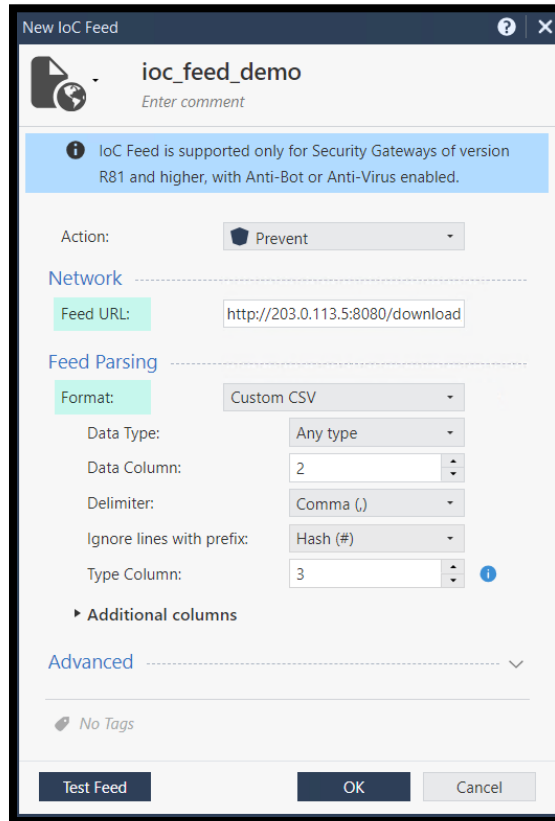
- We can either upload the file via SmartConsole or use the feed URL and the GW will pull the feed automatically. Copy the link of the CSV feed file.



- Under Custom Policy -> Indicators, add a new IoC feed.

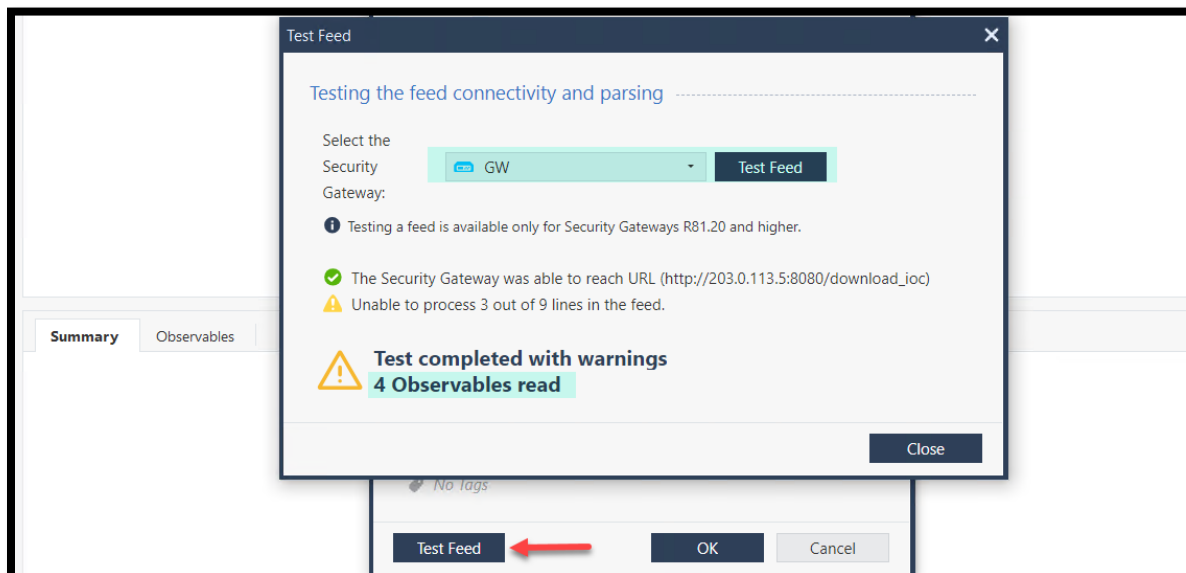


5. Give it a proper name, paste the feed URL, and change the format to Custom CSV.



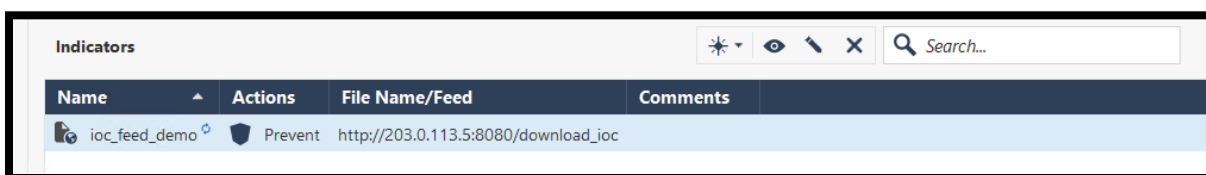
The 'New IoC Feed' dialog box is shown. It has a title bar with a question mark and a close button. The main area has a header with a document icon, the name 'ioc\_feed\_demo', and a comment field. Below this is a blue information banner stating: 'IoC Feed is supported only for Security Gateways of version R81 and higher, with Anti-Bot or Anti-Virus enabled.' The 'Action' dropdown is set to 'Prevent'. The 'Network' section has a 'Feed URL' field containing 'http://203.0.113.5:8080/download'. The 'Feed Parsing' section has a 'Format' dropdown set to 'Custom CSV'. Below this are several fields: 'Data Type' (Any type), 'Data Column' (2), 'Delimiter' (Comma (,)), 'Ignore lines with prefix' (Hash (#)), and 'Type Column' (3). There is an 'Additional columns' section with a plus icon. At the bottom, there is an 'Advanced' section with a dropdown arrow, a 'No Tags' label, and three buttons: 'Test Feed', 'OK', and 'Cancel'.

6. Test the feed from the GW and make sure it can load the observables. We will accept using HTTP site Instead of the recommended HTTPS since this is a lab environment.

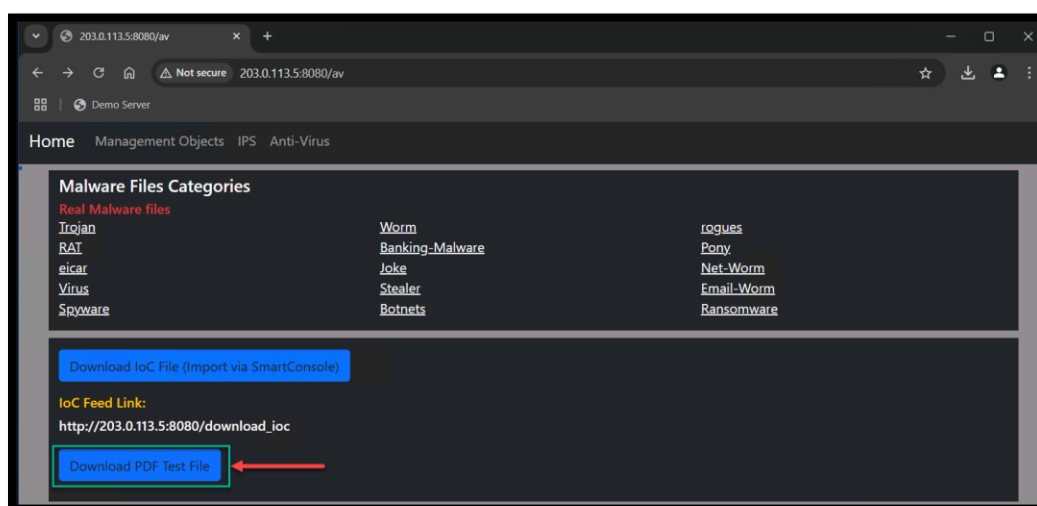


The 'Test Feed' dialog box is shown. It has a title bar with a close button. The main area has a header with the text 'Testing the feed connectivity and parsing'. Below this is a 'Select the Security Gateway' dropdown set to 'GW' and a 'Test Feed' button. A blue information banner states: 'Testing a feed is available only for Security Gateways R81.20 and higher.' Below this are two status messages: a green checkmark indicating 'The Security Gateway was able to reach URL (http://203.0.113.5:8080/download\_ioc)' and a yellow warning triangle indicating 'Unable to process 3 out of 9 lines in the feed.' A large yellow warning triangle icon is followed by the text 'Test completed with warnings' and '4 Observables read'. At the bottom right is a 'Close' button. In the background, the 'New IoC Feed' dialog box is visible, with a red arrow pointing to its 'Test Feed' button.

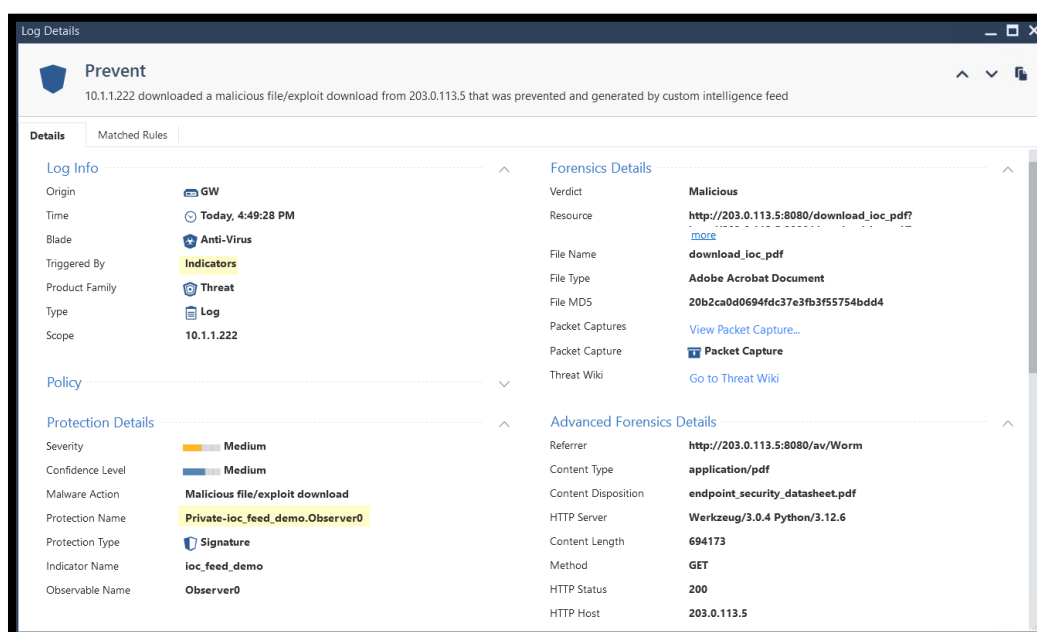
- Confirm the feed was added successfully and Install the Threat Prevention Policy.



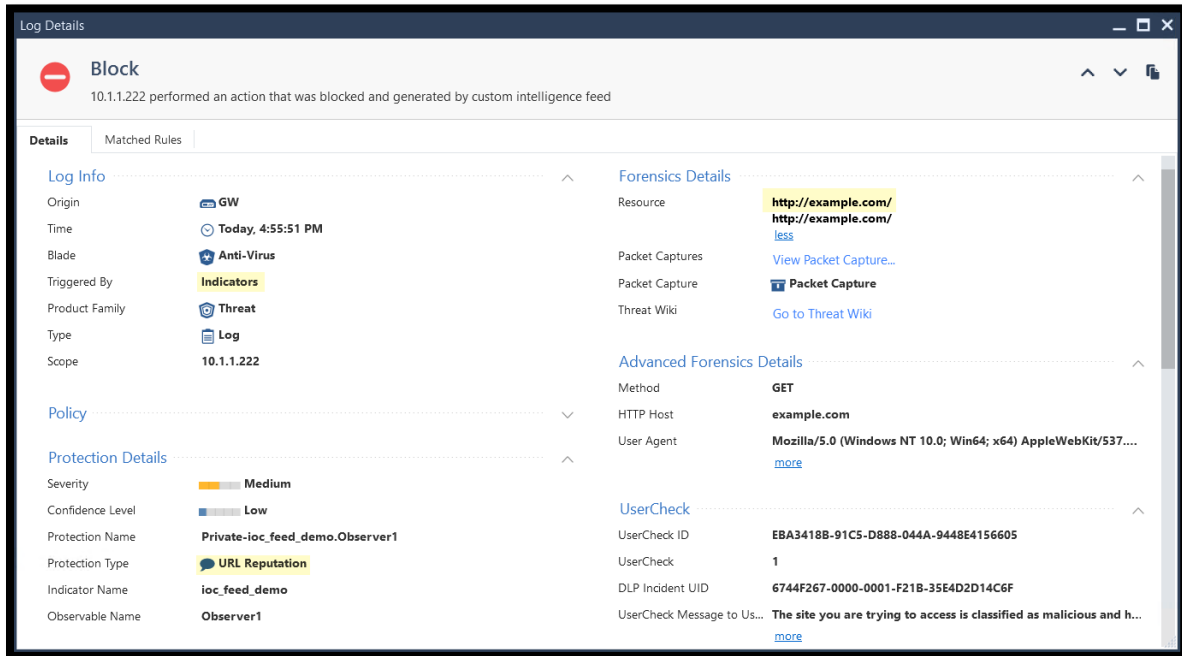
- From the windows client, and try download the PDF test file.



- Review the log. Notice the Protection name and triggered by fields.



10. Test accessing the URL configured in the CSV feed <http://example.com> (we only configured HTTP not HTTPS).
11. Review the log and pay attention to the Protection Type.



The screenshot shows the 'Log Details' window for a blocked action. The title bar indicates 'Block' and the subtitle states '10.1.1.222 performed an action that was blocked and generated by custom intelligence feed'. The window is divided into several sections:

- Log Info:** Origin (GW), Time (Today, 4:55:51 PM), Blade (Anti-Virus), Triggered By (Indicators), Product Family (Threat), Type (Log), Scope (10.1.1.222).
- Policy:** Matched Rules.
- Protection Details:** Severity (Medium), Confidence Level (Low), Protection Name (Private-ioc\_feed\_demo.Observer1), Protection Type (URL Reputation), Indicator Name (ioc\_feed\_demo), Observable Name (Observer1).
- Forensics Details:** Resource (<http://example.com/>), Packet Captures (View Packet Capture...), Packet Capture (Packet Capture), Threat Wiki (Go to Threat Wiki).
- Advanced Forensics Details:** Method (GET), HTTP Host (example.com), User Agent (Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537....), UserCheck ID (EBA3418B-91C5-D888-044A-9448E4156605), UserCheck (1), DLP Incident UID (6744F267-0000-0001-F21B-35E4D2D14C6F), UserCheck Message to Us... (The site you are trying to access is classified as malicious and h...).

End of Lab 6