McAfee Network Security Platform 10.1.x Integration Guide



Contents

Integration with McAfee ePO	
Endpoint details query from the McAfee ePO server	,
Additional details for managed endpoints	I
Start McAfee ePO console 10	I
Additional details for unmanaged endpoints	
Install Network Security Platform extension file in McAfee ePO	
Tags	1
Network Security Platform dashboard in McAfee ePO. 19	I
Configurations	1
Integration with McAfee Global Threat Intelligence	,
How Network Security Platform - GTI integration works. 37	
Configuring McAfee Global Threat Intelligence server for File Reputation in Manager	I
Configuring McAfee Global Threat Intelligence server for URL and IP Reputation in Manager	I
Network Security Platform integration with Private Global Threat Intelligence (GTI) Cloud	I
Configure Telemetry	,
Network Security Platform-GTI integration for IP Reputation. 52	
How Network Security Platform-GTI integration for IP Reputation works.	
Enhanced SmartBlocking	i
Configure Endpoint Reputation for an admin domain	,
Configure Endpoint Reputation for an interface	,
Configure Endpoint Reputation from sub-interface level	I
Viewing the Global Threat Intelligence alert category details	
Next generation reports	
How to view Telemetry report. 62	
Network Security Platform-GTI integration for connection limiting policies	i
Network Security Platform-GTI integration for File Reputation. 64	
Terminologies	,
Benefits of File Reputation	1
Network Security Platform-File Reputation integration in detail.	,
File Reputation integration configurations in the Manager	i
View File Reputation details in Attack Log	i
CLI commands for Network Security Platform - File Reputation integration	,
Limitations	,
Troubleshooting	,
Network Security Platform-GTI integration for URL Reputation	,

How Network Security Platform-GTI Integration for URL Reputation works.	. 86
Configuration of URL Reputation.	. 88
Configure URL Reputation for an interface.	. 90
Viewing URL Reputation details in the Manager	. 92
CLI commands for URL Reputation integration.	. 94
Troubleshooting scenarios.	. 94
Integration with McAfee MVISION Insights	. 96
How Network Security Platform - MVISION Insights integration works.	. 96
High-level steps to make the integration work.	. 98
Generate MVISION ePO registration token.	. 98
Enable Telemetry in the Manager	. 99
Register the Manager with MVISION ePO	100
Enable MVISION Insights integration.	102
Unregister MVISION ePO.	103
Integration with McAfee Advanced Threat Defense	105
Advantages.	105
Terminologies	106
How Network Security Platform - Advanced Threat Defense integration works	110
Details of how the integration works	111
Considerations.	113
High-level steps for integrating with McAfee Advanced Threat Defense	113
Integrating Network Security Platform and McAfee Advanced Threat Defense.	114
Enable McAfee Advanced Threat Defense integration for an admin domain	115
Enable McAfee Advanced Threat Defense integration for a Sensor	117
Add an Advanced Malware policy	119
Manage Advanced Malware policies	127
Sensor CLI commands	129
Analyze Malware Files	130
View the McAfee Advanced Threat Defense specific details for a detected malware	135
Manager reports for malware detections	137
Integration with McAfee Threat Intelligence Exchange	140
Why integrate Network Security Platform with Threat Intelligence Exchange?	140
How the integration works.	141
Computing the overall file reputation in the Sensor	144
High-level steps to make the integration work	144
Enable DXL integration for a domain.	145
Enable DXL integration for a device	146

Viewing Threat Intelligence Exchange detection in the Manager.	147
Sensor CLI commands specific to Threat Intelligence Exchange	150
Troubleshooting the integration between Network Security Platform and Threat Intelligence Exchange	150
Integrating with McAfee Endpoint Intelligence Agent.	151
Overview	151
Architecture	152
Benefits	153
How integration with McAfee EIA works	153
Setting up McAfee EIA integration	154
Verify system requirements	154
Setting up McAfee Agent with ePolicy Orchestrator server.	155
Setting up McAfee EIA with ePolicy Orchestrator server	160
Enabling McAfee EIA integration on the Manager.	167
Understanding executable classification	171
Working with allowed and blocked hashes	172
Import of allowed and blocked hashes	173
Export of allowed and blocked hashes	174
Move hashes from or to allow list or block list	176
Remove or replace hashes from allow and block lists.	176
Configuring NTBA policies for McAfee EIA alerts.	177
Viewing executables running on endpoint.	178
Sample scenario: Analyze an unclassified executable with high malware confidence	187
Viewing endpoint intelligence reports.	189
NTBA-EIA deployment scenarios.	189
Best practices.	190
NTBA-EIA sizing recommendations.	191
Troubleshooting.	192
Connectivity issues	192
Integration with McAfee Vulnerability Manager	196
McAfee Network Security Platform - Vulnerability Manager integration.	196
Vulnerability Manager installation	198
Menu options for Vulnerability Manager configuration	199
Configure Vulnerability Manager settings in Manager	199
Import non-vulnerability manager report	215
Vulnerability assessment	220
Relevance analysis of attacks	221
Menu options for relevance analysis	222
Relevance configuration details	223

	Use relevance configuration wizard	223
	Relevance analysis configuration in Manager	224
	Fault messages for Vulnerability Manager scheduler	233
	Support for Vulnerability Manager custom certificates.	234
	Generate Vulnerability Manager SSL custom certificate for Manager	234
	Import the custom certificates into the Manager keystore	235
	Troubleshooting options	236
	Reload Vulnerability Manager cache	236
	Reset relevancy cache	237
	Resubmission of database updates	237
	Vulnerability Manager - Certificate Sync and FC Agent issues.	238
	Error messages	239
Inte	egration with McAfee Logon Collector.	242
	Benefits	242
	Integration requirements.	242
	Download the software	242
	How Network Security Platform - Logon Collector integration works.	243
	Configuration details for Logon Collector integration.	244
	Configure integration at the admin domain level.	244
	Establishment of trust between Network Security Manager and Logon Collector server	245
	Display of Logon Collector details.	246
	Display user details (Logon Collector data) in Attack log	246
	Display of Logon Collector details in Network Security Manager reports.	247
	Next Generation custom reports	247
	Communication error	249
Inte	egration with HP Network Automation	251
	Configure HP Network Automation in the Manager	251
Inte	egration of the Manager with SIEM products	254
	Manager data available for SIEM products	254
	Methods of integration with SIEM products.	255
	Configure notification methods.	256
	Configure notifications based on attack severity.	256
	Configure notifications per attack	256
	Templates for syslog, email, and pager.	257
	Integration for fault information.	262
	- Integration using reports	265
	Data mining	265
	-	

IV_ALERT_DATA decoding)9
IPS alerts	19
NTBA alerts	13
File Reputation alert	2
Information on database queries	5
SQL query guidelines	5
Implications of database queries	5
Alert synchronization in an MDR deployment. 31	7
Create PCAP format packet logs	8
Create the PCAP file header and write them into a file	9
Creating the PCAP packet headers for all regular packets and write them into the file	9
Create the PCAP packet headers for all fragment packets and write them into the file	20
Enable communication between Syslog server and the Manager. 32	21
Create a database user in a MLOS system	!1
Sensor data available for MIB browsers	4
Integrate an SNMP MIB browser with a Sensor	<u>'</u> 4
Configure the SNMPv3 user details on the MIB browser	24
Load the Sensor MIBs onto to your MIB browser	25

Integration with McAfee ePO

McAfee ePO is a scalable platform for centralized policy management and enforcement of your system security products, such as anti-virus, desktop firewall, and anti-spyware applications. You can integrate McAfee Network Security Platform [formerly McAfee® IntruShield®] with McAfee ePO. The integration enables you to query McAfee ePO server from the Manager for viewing details of a network host.

The integration of Network Security Platform with McAfee ePO version is based on their compatibility. The current Network Security Platform version supports integrating with the current release of McAfee ePO and with some previous versions of McAfee ePO.

For more information about McAfee ePO, see the *McAfee ePolicy Orchestrator Product Guide*. You can download the guide from McAfee Download Server.

Integrating Network Security Platform and McAfee ePO enables you to send queries to McAfee ePO server to obtain details of the hosts on your network. The details that are fetched from McAfee ePO server include the host type, host name, user name, operating system details, top10 anti-virus events, and the details of system security products installed on the host. You can view these details in the Attack Log. If you have installed McAfee Host IPS [formerly McAfee® Entercept] as part of your McAfee ePO installation, you can also view the last 10 McAfee Host IPS events for a specific host. These details provide increased visibility and relevance for security administrators performing forensic investigation of security events seen on the network. When you are reviewing alert details for an endpoint in Attack Log, you can view the essential host data such host name, current user, and OS version in the alert details panel.

Consider the following scenario to understand how Network Security Platform -McAfee ePO integration works:

You notice in the Attack Log that a host in your network is port scanning the other hosts. You want to know more details about the source of these attacks. You can then double-click on an alert and see the details of the source IP address. The Manager sends queries to McAfee ePO server. You can view the host details by clicking on the exclamation icon next to the IP address. From these details, you may realize, for example, that VirusScan (McAfee's antivirus application) is outdated. Looking at the host name, you may also realize that it is the server that was taken off the network sometime back. Therefore, the VirusScan was not updated during this period.

In addition to these features, you may also assign tags through the Threat Explorer of the Manager. For more information on tags, see Tags.

McAfee ePO provides you the option to view Network Security Platform data on a dashboard.

This dashboard in McAfee ePO provides the following monitors:

- Attack Severity Summary
- Device Fault Summary
- Manager Fault Summary
- Top 10 Attack Destinations
- Top 10 Attacks

• Top 10 Attack Sources

Endpoint details query from the McAfee ePO server

After you enable Network Security Platform-McAfee ePO integration at an admin domain level, you can view the details of the corresponding network endpoints using the Attack Log. If you have installed McAfee Host Intrusion Prevention software and if the Host Intrusion Prevention is running on the endpoint, then you can view the top 10 McAfee Host Intrusion Prevention events for an endpoint as well.

Consider the following example. *My Company* is the root admin domain and *HR* and *Finance* are its child domains. *Sensor-HR* and *Sensor-Fin* are the respective Sensors of the two child domains. Assume that the Manager-McAfee ePO integration is enabled only for *Finance*. For an attack detected by *Sensor-Fin*, you can view the details of the source and destination endpoints from Attack Log because McAfee ePO integration is enabled for the *Finance* admin domain.

Note that for you to view the details, the information should be available on the McAfee ePO server. For example, if an attack is from outside your network, then your McAfee ePO server may not have any information about this source endpoint.

🗹 Note

The Network Security Platform extension running on McAfee ePO must be compatible with your current version of Network Security Platform. Consider that you integrated McAfee ePO with the earlier version of Network Security Platform, and then subsequently you upgraded Network Security Platform. Then the integration with McAfee ePO might not work as expected because the Network Security Platform extension on McAfee ePO is from an old installation. This extension might not be compatible with your current version of Network Security Platform. To verify this, you can use the **Test Connection** button in step 2 of the **ePO Configuration Wizard** in your current Manager. If the Network Security Platform extension is incompatible, then an error message is displayed along with the minimum required version for the extension.

An endpoint can belong to one of the following three types:

- Managed Endpoints These are endpoints currently managed by McAfee ePO agent.
- Unmanaged Endpoints These are endpoints recognized by McAfee ePO but are not currently managed by any McAfee ePO agent.
- Unrecognized Endpoints These are endpoints about which McAfee ePO has no information. In the Attack Log, an unrecognized endpoint is represented by a series of ellipses (- -).

You can view the details of the source and destination endpoints in an alert. Alternatively, you can also enter the IP address and get the details from the McAfee ePO server. These details may enable you to troubleshoot and fix any security-related issues in those endpoints. In the Attack Log, you can view the details of managed and unmanaged endpoints but not for unrecognized endpoints.

🗹 Note

If you modify the McAfee ePO server settings, re-launch the Attack Log to view the endpoint details.

Tags

Network Security Platform now provides you the ability to assign tags to source or destination endpoints managed by McAfee ePO. Tags assist a security analyst in identifying endpoints that do not meet security requirements on your network. To learn more about tags and their assignment through the Manager, see Tags.

Additional details for managed endpoints

For managed and unmanaged endpoints, you can click on the information icon next to the IP address to view additional details. These additional details are related to the point-products installed by ePO on the endpoint.

🗹 Note

In order for these additional details to appear, you must select the **Enable Endpoint Detail Queries?** check-box in the **Enable ePO Integration** page of the Manager.

If you have installed Host Intrusion Prevention and it is running on the endpoint, you can view the last 10 Host Intrusion Prevention events in the endpoint. Note that the last 10 events displayed are sorted based on their severity levels.

🗹 Note

A Host Intrusion Prevention event is an alert generated by Host Intrusion Prevention regarding an activity on the endpoint. For more information, see *McAfee Host Intrusion Prevention* documentation.

Based on the additional details and the events, you can tune the security applications on the endpoint for the best possible protection.

You can view the following details for the managed endpoint on the **Endpoint Information** tab:

Option	Definitions
Country	Country of the endpoint
DNS Name	DNS name of the endpoint to resolve the names to IP addresses
NetBIOS Name	NetBIOS name of the endpoint to access the host machines
Operating System	Operating system platform of the endpoint
Device Type	Type of the Sensor (for example, IPS Sensor)
MAC Address	MAC address of the endpoint

Option	Definitions
Domain/Workgroup	Domain or workgroup of the endpoint
User	Operating system user name of the endpoint
Data Source	Database tables from where information is retrieved
McAfee Agent Check-In Time	Check-in time of the McAfee Agent that communicates with the same ePO server integrated with the admin domain
Endpoint Type	 Type of endpoint: UNMANAGED (No Agent) — This indicates that there is no McAfee Agent installed on the endpoint. UNMANAGED (MANAGED) — This indicates that the endpoint has a McAfee Agent but there is no active communication channel between the Agent and ePO server integrated with the admin domain.
Installed Products	List of the installed products

Click the **ePO Threat Events** tab to view the latest **50 Threat Events** listed in the ePolicy Orchestrator for a selected endpoint. The information displayed under this sub-tab includes the date and time at which the threat event was generated, the ID associated with the event, the event description, event category, action taken on the event, and the type of the threat that triggered the event.

🗹 Note

Ensure that the ePO server has the latest NSP Extension file installed. For information on how to download and install the NSP Extension, see the section Install Network Security Platform extension file in McAfee ePO.

Start McAfee ePO console

You can view details for an endpoint by starting the McAfee ePO console from the Attack Log itself.

Task

- 1. Select Analysis \rightarrow <Admin Domain Name> \rightarrow Attack Log.
- 2. Double-click the alert for which you want to view the details. The alert details panel opens.
- 3. In the **Summary** tab under the **Attaker/Target** section, click the information icon next to the source or target IP address.

The Attacker IP address - <IP address> or the Target IP address - <IP address> pop-up opens.

Endpoint information

Threat Explorer				
0	Top: 5	 Attacks 	Any Direction	01/03/17 3:45 AM - 07/05/21 7:10 PM 💌 🔘
Filter: Attacker IP Address 10. X Add Filter View Attacks				
				Optional Tabs 👻
Endpoint Information	ePO Threat Events	Vulnerability Assessment		
				C
Country: DNS Name: NetBIOS Name:		Domain/Workgroup: User: Data Source:	WORKGROUP Administrator ePO (10.208.)	Installed Products DXL1000 (6.0.3.278) Endpoint Security Threat Prevention (10.7.0.2787)
Operating System: Device Type: MAC Address:	Windows Server 2016 000 2	McAfee Agent Check-In Time: Endpoint Type:	Fri Jan 15 22:43:31 IST 2021 MANAGED	Engine: N/A Virus Definitions: 0.5 Endpoint Security Firewall (10.7.0.1874) Endpoint Security Platform (10.7.0.2687) Endpoint Security Web Control (10.7.0.2303) Endpoint Security Adaptive Threat Protection (10.7.0.2913) Agent (5.7.2.127)
Network Forensics		ag (in ePO)		

4. Click ePO Threat Events and then click Open ePO console.

The actions that you can do on the McAfee ePO console will be based on the permissions assigned to the user credentials that you enter during McAfee ePO server configuration.

Additional details for unmanaged endpoints

Unmanaged endpoints do not have an McAfee ePO agent to manage their point-products. The following are the additional details that you can view for unmanaged endpoints:

Field	Description
DNS	DNS name of the endpoint.
NetBIOS name	NetBIOS name of the endpoint.
IP Address	IP address of the endpoint.
MAC Address	MAC address of endpoint.
Endpoint Type	One of the following is displayed as Endpoint Type:

Field	Description
	 UNMANAGED (No Agent)— This indicates that there is no McAfee Agent installed on the endpoint. UNMANAGED (MANAGED)— This indicates that the endpoint has a Host Intrusion Prevention but there is no active communication channel between the Agent and ePO server integrated with the admin domain.
Last detection time	The date and time when the endpoint was detected on the network.
Operating system	The operating system platform on the endpoint. For example: Windows 2003.
User(s)	Operating system user names of the endpoint.
Source ePO server	The IP address of the ePO server that sent the unmanaged endpoint details.

Install Network Security Platform extension file in McAfee ePO

To install the extension for Network Security Platform in McAfee ePO, do the following:

Task

- 1. Log onto the Manager.
- 2. Navigate to Manager \rightarrow <Admin Domain Name> \rightarrow Integration \rightarrow ePO \rightarrow ePO Integration. The Enable ePO Integration page is displayed.
- Enable the required options for McAfee ePO integration.
 (Optional) Select the checkbox for the Enable Endpoint Lookup? option.
 (Optional) Select the checkbox for the Enable Endpoint Tagging? option.

This option enables you to assign tags created in McAfee ePO to managed endpoints.

🗹 Note

At least one of the above options has to be selected for McAfee ePO integration.

Enable ePO Integration area

/My Company > Integration > eP	0 > ePO Integration	Ø
ePO Integration		
0		
Enable Endpoint Lookup?	⊴	
Enable Endpoint Tagging?		
ePo Configuration Wizard	step 1 of 2	Next >

4. Click Next to view ePO Server Settings page.

ePO Server Settings area

/My Company > Integration > ePO > ePO Integration				
Use this page to specify the ePO server and its listening port, and the credentials the Manager uses when communicating with ePO.				
ePO integration requires the N the NSP Extension for ePO:	ISP Extension for ePO to be installed on the eP	O server. To	install	
 Download the extension from here: <u>NSP Extension for ePO</u> From the ePO console, go to Menu > Software > Extensions and install it. From this page, enter the required information, confirm connectivity, and finish this wizard. 				
Tip: To optimize security, we recommended you use a local ePO user account with view-only permissions.				
Fields marked with an asterisk	(*) are required.			
ePO Server Settings				
Server Name or IP Address:				
Server Port:	8443			
User Name:	admin			
Password:	•••••			
		Test Conne	ection	
ePo Configuration Wizard	step 2 of 2	< Back	Finish	

5. Click NSP Extension for ePO link to download the NSPExtension.zip file.

🗹 Note

If this is an existing deployment using an obsolete version of the extension, you are prompted to update to the minimum require version.

File Download dialog

Opening NSPExtens	ion.zip	×				
You have chosen t	o open:					
NSPExtensio	on.zip					
which is: Co	mpressed (zipped) Folder (4.3 MB)					
from: https:/	//					
What should Firefox do with this file?						
Open with	Windows Explorer (default)	\sim				
○ <u>S</u> ave File						
Do this automatically for files like this from now on.						
	OK	Consol				
	OK	Cancel				

6. Save **NSPExtension.zip** in a convenient location.

You can also copy the product extension zip file from Manager installation folder in the following location: C:\Program Files \McAfee\Network Security Manager\App\EPOExtension

7. Log onto the McAfee ePO console.

The McAfee ePO console Home page is displayed.

- 8. Click \blacksquare , and navigate to **Software** \rightarrow **Extensions** page.
- 9. Click **Install Extension** at the top of the page.
- 10. Browse and select **NSPExtension.zip** from the location mentioned in step 5.

Once installed, the Manager is listed under the **Extensions** list. For more details on installation procedure for extension files, refer McAfee ePO documentation.

Extensions page

≡ 🔀 McAfee	Protection Workspace	e Dashboards	System Tree	Queries & Reports	Policy Catalog	Security Resources		▲ ▲ ~							
Software Extensions	tension														
Extensions															
McAfee Agent	Search							×							
McAfee Agent Smart Scheduler															
McAfee Client Proxy			0	Too do Hand	Mardada a Maharad	- Committee Direktorme	Duran in a	Pomovo							
McAfee DXL	Name:	Network Security Platform	Status: Requires:	Installed	Modules: Network	k Security Platform	Running	Kentove							
McAfee Security for Microsoft E	Version:	9.2.1.1	9.2.1.1 admin - March 4, 2019	9.2.1.1	9.2.1.1 admin - March 4, 2010	9.2.1.1	9.2.1.1 admin - March 4, 2010	9.2.1.1	9.2.1.1		• ePO Core 5.9.0				
McAfee Security for Microsoft Sł	instaned by.	10:32:56 PM PST	Details:	NSP Extension for ePO											
mobile															
MVISION Endpoint 1811															
MVISION Mobile															
Network Security Platform															
Rogue System Detection															
Server															
Shared Components															
SiteAdvisor Enterprise															
Solidcore															
VirusScan Enterprise															
✓ Third Party															

Tags

Tags in McAfee ePO assist you to identify and sort managed endpoints. If you are a McAfee ePO administrator, it is crucial for you to be able to identify individual endpoints or groups of endpoints when you create tasks and queries. Tags and tag groups make this task of identification simpler. For more details about tags and how they can be best used to benefit your network, refer to chapter *Using the System Tree* and *Tags* in the *McAfee ePOlicy Orchestrator 5.10.0 Product Guide*.

If McAfee ePO is integrated with Network Security Platform, which identifies endpoints by their IP addresses while McAfee ePO identifies endpoints by a unique ID, there are likely going to be events triggered in the Manager in Network Security Platform which are suspicious or confirmed malicious. In such instances, between the time that an endpoint IP address is identified as suspicious and the time that the McAfee ePO administrator tags the endpoint for further action, the IP address of the endpoint might have changed. To overcome this lag, the security analyst is provided a list of tags within the Manager in Network Security Platform. These tags are defined in McAfee ePO and are communicated to the Manager in real-time.

🗹 Note

Tags can be assigned only to managed endpoints, that are endpoints running a compatible version of the McAfee Agent.

Assign McAfee ePO tags to endpoints through Threat Explorer

Before you begin

To assign tags from the Manager, make sure you have enabled the **Enable Endpoint Tagging?** checkbox in the **ePO Integration** page in the Manager.

You are able to assign tags to endpoints managed by McAfee ePO through the Threat Explorer of the Manager. These assignments reflect in McAfee ePO in real-time.

Task

1. Go to Analysis \rightarrow <Admin Domain Name> \rightarrow Threat Explorer.

🗹 Note

You must select a domain in which integration with McAfee ePO is enabled. The integration must also have endpoint tagging enabled in the Manager.

2. Click an IP address from the **Top Attackers** or **Top Targets** panel.

Details about the IP address appear.

Endpoint Information tab

Threat Explorer									
0	Top: 5	 Attacks 	Any Direction	01/03/17 3:45 AM - 07/05/21 7:10 PM 💌 💭					
Filter: Attacker IP Address 10. X Add Filter View Attacks									
Endpoint Information	ePO Threat Events	Vulnerability Assessment		Optional Tabs *					
				C					
Country: DNS Name: NetBIOS Name: Operating System: Device Type: MAC Address:	 WIN- T Windows Server 2016 000 2	Domain/Workgroup: User: Data Source: McAfee Agent Check-In Time: Endpoint Type:	WORKGROUP Administrator ePO (10.208.) Fri Jan 15 22:43:31 IST 2021 MANAGED	Installed Products DXL1000 (6.0.3.278) Endpoint Security Threat Prevention (10.7.0.2787) Engine: N/A Virus Definitions: 0.5 Endpoint Security Firewall (10.7.0.1874) Endpoint Security Platform (10.7.0.2687) Endpoint Security Web Control (10.7.0.2303) Endpoint Security Adaptive Threat Protection (10.7.0.2913) Agent (5.7.2.127)					
Network Forensics		ag (in ePO)							

3. Within the **Endpoint Information** tab, look for the **Endpoint Type**.

You are able to assign tags only to endpoints that denote the **Endpoint Type** as **MANAGED**, which means that that endpoint is managed by McAfee ePO using the McAfee Agent.

4. If the endpoint is managed, click the Tag (in ePO) button.

The **Tag Endpoint** pop-up window appears with the IP address of the endpoint that you are about to tag, the ePO server that you have integrated with, and a drop-down list of tags you can assign. These tags are created in McAfee ePO.

Drop-down contains the list of tags created in McAfee ePO

Tag Endpoint		⊗
Assign a tag to the endpoint w	vithin ePolicy Orchestrator.	
Endpoint: ePO Server:	10. 10.	
Tag to Assign:	<select></select>	
		Tag
		-
	Server	
Target Country	Workstation	

5. Select the tag you want to assign and click **Tag**.

If the assignment is successful, you receive a message stating the same.

Tagging successful



If you have selected an unmanaged endpoint or the tagging is unsuccessful for another reason, you receive a message stating the failure.

Tagging fails when the endpoint is not managed by McAfee ePO



Results

The tag is assigned to the endpoint. You will be able to view it in McAfee ePO. To see the steps you need to follow to view the tags, see View tags in McAfee ePO.

Assign McAfee ePO tags to endpoints through Attack Log

Before you begin

To assign tags from the Manager, make sure you have enabled the **Enable Endpoint Tagging?** checkbox in the **ePO Integration** page in the Manager.

You are also able to assign tags to endpoints, managed by McAfee ePO, directly through Attack Log of the Manager. This facility makes it simple for any security analyst who notices an alert in the Attack Log to identify a suspicious or vulnerable endpoint and, beyond quarantining it, mark it for further action. These assignments also reflect in McAfee ePO in real-time.

Task

1. Go to Analysis \rightarrow <Admin Domain Name> \rightarrow Attack Log.

🗹 Note

You must select a domain in which integration with McAfee ePO is enabled. The integration must also have endpoint tagging enabled in the Manager.

- 2. Select the alert whose attacker or target IP address you want to tag in ePO. Click **Other Actions** at the bottom of the page.
- 3. Go to **Tag Endpoint** \rightarrow **in ePO** and select the attacker IP address or the target IP address you want to tag.

The **Tag Endpoint** pop-up appears with the IP address of the endpoint that you are about to tag, the ePO server that you have integrated with, and a drop-down list of tags you can assign. These tags must already have been created in McAfee ePO. If the tag does not show up in the list, click the refresh icon.

Tag an endpoint from Attack Log

Tag Endpoint		8					
Assign a tag to the endpoint within ePolicy Orchestrator.							
Endpoint:	190.						
ePO Server:	10.						
Tag to Assign:	Server 💌						
	Server	Tag					
03, 2013 12.1 Outbound	Workstation						

🗹 Note

Remember you allowed to assign tags only to managed endpoints, which are endpoints that are managed by McAfee ePO (using the McAfee Agent).

4. Select the tag you want to assign and click Tag.

If the assignment is successful, you receive a message stating the same. If you have selected an unmanaged endpoint or the tagging is unsuccessful for another reason, you receive a message stating the failure.

Results

The tag is assigned to the endpoint. You will be able to view it in McAfee ePO. To see the steps you need to follow to view the tags, see *McAfee ePolicy Orchestrator Product Guide*.

View tags in McAfee ePO

To view tags assigned to endpoints, refer to chapter *Using the System Tree* and *Tags* in the *McAfee ePolicy Orchestrator Product Guide*.

Network Security Platform dashboard in McAfee ePO

McAfee ePO provides you the option to view Network Security Platform data on a dashboard.

This dashboard in McAfee ePO[™] provides the following monitors:

- Attack Severity Summary
- Device Fault Summary

- Manager Fault Summary
- Top 10 Attack Destinations
- Top 10 Attacks
- Top 10 Attack Sources

To view product data in McAfee ePO, you need to install Network Security Platform extension file in McAfee ePO™.

When this Extension file is installed in McAfee ePO[™], a default dashboard with the above monitors is created on McAfee ePO[™] **Dashboards** page. This dashboard displays information from Network Security Platform. Optionally, you can create new dashboards for Network Security Platform in McAfee ePO[™].

A default server task is also created in McAfee ePO[™], as part of the installation of the product extension. This server task needs to be configured for pulling in the relevant data from Network Security Platform. For more details, refer to the section Configure a server task for Network Security Platform in McAfee ePO.

Data retrieval when the McAfee® Network Security Manager is in Manager Disaster Recovery (MDR) mode:

Consider the following scenarios when the Manager is in MDR mode:

If the Primary Manager is active, the data is retrieved from the Primary Manager to McAfee ePO[™]. In case the Primary Manager is in standby mode, and the Secondary Manager is active, data is retrieved from the Secondary Manager.

If both Primary and Secondary Managers are in standby mode, the data that was last available in the Primary Manager is retrieved to McAfee ePO[™] and displayed on the dashboard.

If both Primary and Secondary Managers are not available, the data is not retrieved to McAfee ePO[™] . In this case, all the dashboard data tables are cleared and empty dashboards are displayed in McAfee ePO[™] .

Configurations

The following configurations are required from McAfee ePO and the Manager, to view Network Security Platform data on the dashboard:

Create a user in the Manager for data retrieval in McAfee ePO

To pull the data from the Manager in McAfee ePO[™], you need to create a user and assign the role **ePO Dashboard Data Retriever** to the user.

To create a user and assign the Data Retriever role in the Manager, do the following:

Task

1. From the Manager, select Manager \rightarrow <Admin Domain Name> \rightarrow Users and Roles \rightarrow Users.

- 2. To add the new user, click +
- 3. Enter the details of the user in **Add a User** window.

Note that the **Login ID** and **Password** that you define in this window are to be entered in the **Actions** page, while configuring a Server Task in McAfee ePO^{M} .

Users sub-tab

/My Company > Users and Roles > Users								
Fields marked with an asterisk (*) are required.								
Add a User								
User Credentials								
Login ID:	ePO_DB_User							
Password:								
Verify Password:								
User Details								
First and Last Name:	John Doe							
Email:	john_d@mcafee.com							
Company:	McAfee LLC							
Phone:								
Address:								
State:								
Country:								
Role Assignment								
Admin Domain:	/My Company 🤝							
Role:	ePO Dashboard Data Retrie	ever 🔽						
			Save	Cancel				

- 4. Click Save, and a message pops up asking whether you need to assign a role to the user. To assign a role, click OK.
- 5. Select the role **ePO Dashboard Data Retriever**, and click **Save**.
- 6. The user with the assigned role is displayed in the Users tab, and Role Assignments tab. Note that the Login ID and Password that you define in this window are to be entered in the Actions page, while configuring a Server Task in McAfee ePO[™].

Configuration of ePO server settings in the Manager

Configuring McAfee ePO[™] server settings in the Manager involves configuring ePO server details.

Configure McAfee ePO server details

The integration between the Manager and McAfee ePO[™] server is performed with the help of an extension file, which needs to be installed on the McAfee ePO[™] server. You can download the extension file from the Manager. Before you configure McAfee ePO[™] server settings, follow the steps mentioned in Install Network Security Platform extension file in McAfee ePO[™] to install the extension file on the McAfee ePO[™] server. Following this, you need to configure McAfee ePO[™] server settings on the Manager.

To integrate the Manager with McAfee ePO[™], perform the following steps:

Task

- 1. Navigate to Manager \rightarrow <Admin Domain Name> \rightarrow Integration \rightarrow ePO \rightarrow ePO Integration. The ePO Integration page is displayed.
- 2. Enable the required options for McAfee ePO integration.

(Optional) Select the checkbox for the **Enable Endpoint Lookup?** option. (Optional) Select the checkbox for the **Enable Endpoint Tagging?** option.

This option enables you to assign tags created in McAfee ePO to managed endpoints.

🗹 Note

At least one of the above options has to be selected for McAfee ePO integration.

Enable ePO Integration area

/My Company > Integration > ef	PO > ePO Integration	ଟ
ePO Integration		
0		
Enable Endpoint Lookup?		
Enable Endpoint Tagging?	∽	
ePo Configuration Wizard	step 1 of 2	Next >

3. Click Next to view ePO Server Settings page.

ePO Server Settings

/My Company > Integration > ePO > ePO Ir	ntegration		8				
Use this page to specify the ePO server and its listening port, and the credentials the Manager uses when communicating with ePO.							
ePO integration requires the NSP Extension	on for ePO to be installed on the ePO server. To	install the NSP Extension for ePO:					
1. Download the extension from here: <u>NSP Extension for ePO</u> 2. From the ePO console, go to Menu > Software > Extensions and install it. 3. From this page, enter the required information, confirm connectivity, and finish this wizard.							
Tip: To optimize security, we recommend	ed you use a local ePO user account with view	-only permissions.					
Fields marked with an asterisk (*) are r	equired.						
ePO Server Settings							
Server Name or IP Address:							
Server Port:	8443						
User Name:	admin						
Password:	•••••						
		Test Connectio	on				
ePo Configuration Wizard	step 2 of 2	< Back Finis	sh				

4. Specify the ePO server details as described in the following table.

Field	Description
Server Name or IP Address	Enter the name or the IP address of the ePO server running the extension file. Note that this ePO server should have the details of the hosts covered by the admin domain. Contact your ePO administrator for the server name and IP address.
Server Port	Specify the HTTPS listening port on the ePO server that will be used for the Manager-ePO communication. Contact your ePO administrator for the port number.
User Name	Enter the username to be used while connecting to the ePO server. McAfee recommends you create an ePO user account with View-only permissions required for integration.
Password	Enter the password for connecting to the ePO server.

- 5. Click **Test Connection** to ensure that the extension file is installed and started on the McAfee ePO server.
- 6. If the connection is up, click **Finish** to save the configuration.

Configuring McAfee ePO server for separate admin domains

You can enable or disable the Manager - McAfee ePO integration for an admin domain. If you enable the Manager -McAfee ePO integration for an admin domain, you can view the details for the hosts of that admin domain from the Attack Log.

If you have more than one instance of McAfee ePO, the admin domains can be configured to different McAfee ePO servers. However, you should plan your deployment in such a way that an admin domain is configured with the appropriate McAfee ePO server. For example, if you have an exclusive McAfee ePO server for your Branch Office, the Branch Office Admin Domain should be configured to the Branch Office McAfee ePO server.

🗹 Note

For more information on ePO, refer to McAfee ePO documentation.

Viewing McAfee ePO configuration details

To view the McAfee ePO^M configuration details of an admin domain, select **Manager** \rightarrow **<Admin Domain Name>** \rightarrow **Integration** \rightarrow **ePO** \rightarrow **Summary**.

🗹 Note

To view the Network Security Platform- McAfee ePO[™] configuration details of multiple Admin Domains, you can use the **Admin Domains and Users** configuration report.

Configure a server task for Network Security Platform in McAfee ePO

As mentioned earlier, a default server task is created as part of the extension file installation. This server task can be scheduled for pulling in data to McAfee ePO from Network Security Platform.

The default server task needs to be configured to provide the user (with **ePO Dashboard Data Retriever** role) with the required credentials, so that data retrieval process takes place to McAfee ePO.

To configure the default server task in McAfee ePO, do the following:

Task

- 1. From McAfee ePO home page menu, click 💻
- 2. Select Automation \rightarrow Server Tasks.

The default server task is displayed in the main **Server Tasks** tab.

Server Tasks tab

	McAfee Dashboa	ards System	Tree Queries & Reports	Policy Catalog	Security Resources				- ~
Autom	ation								
Ser	ver Tasks New Task Impor	t Tasks							
erver T	asks							I	Hide Filte
Quick f	find: Apply Clear	Show select	ted rows						
Na	ame 🗸 🗸	Status	Туре	Schedule	Next Run	Last Run	Actions		
Ap	ply TIESERVER Tags to TIE Servers	Enabled	System	Daily	11/21/18 12:15 AM	11/20/18 3:46 AM	View Edit Run		
Di	saster Recovery Snapshot Server	Enabled	System	Daily	11/21/18 1:59 AM	11/20/18 3:48 AM	View Edit Run		
Do	wnload Software Product List	Enabled	User	Daily	11/21/18 1:56 AM	11/20/18 3:47 AM	View Edit Run		
Du	iplicate Agent GUID - clear error count	Disabled	User	Weekly	No next runtime	Task has never run	View Edit Run		
Du	plicate Agent GUID - remove systems with p	Disabled	User			Task has never run	View Edit Run		
En	dpoint Security Firewall Property Translator	Disabled	System	Daily	No next runtime	Task has never run	View Edit Run		
eP	0	Enabled	User	Daily	11/21/18 5:30 PM	11/20/18 5:30 PM	View Edit Run		
eP	O Database Index Maintenance	Enabled	System	Weekly	11/25/18 4:00 AM	11/18/18 8:42 PM	View Edit Run		
Ge	enerate Records for McAfee Agent Compliance	Enabled	User	Weekly	11/25/18 1:00 AM	11/18/18 8:42 PM	View Edit Run		
Но	st IPS 8.0 Catalog Maintenance Task	Disabled	System	Daily	No next runtime	Task has never run	View Edit Run		
На	st IPS 8.0 Property Translator	Disabled	User			Task has never run	View Edit Run		
In	active Agent Cleanup Task	Disabled	User	Weekly	No next runtime	Task has never run	View Edit Run		
Ld	apSync: Sync across users from LDAP	Enabled	System	Daily	11/21/18 12:00 AM	11/20/18 4:00 PM	View Edit Run		
Ma	anage DXL Brokers	Enabled	System	Daily	11/21/18 12:00 AM	11/20/18 3:46 AM	View Edit Run		
NS	iP: Dashboard Data Updating Task	Enabled	User	Advanced	11/20/18 8:00 PM	11/20/18 7:55 PM	View Edit Run		
Pu	rge Threat and Client Events Older than 90 E	Disabled	User	Daily	No next runtime	Task has never run	View Edit Run		
Ro	II up Data (Local McAfee ePO server)	Disabled	User			Task has never run	View Edit Run		
Se	nd DXL Certificate Revocations	Enabled	System	Daily	11/21/18 12:00 AM	11/20/18 3:45 AM	View Edit Run		
Se	nd DXL State Event	Disabled	System			Task has never run	View Edit Run	A stimute VAC: stands	
	mehranian Charad Delision	Disabled	Liner			Taek bas never run	Minue Edit Run	Activate windows	

3. In the **Server Tasks** page, select the task and click **Actions** and select any task to manage the server task.

≣ 🔰 Mc	Afee [®] Dat	shboards	System Tree	Queries & Repo	rts Policy	y Catalog Security Re	sources		2
Server Tas	KS New Task	Import Tasks							
rver Tasks									Hide
Quick find:	Apply C	lear s	how selected rows						
Name	~	Status	Type		Schedule	Next Run	Last Run	Actions	
Manage DXL Broke	rs	Enabled	System	1	Daily	11/24/18 12:00 AM	11/23/18 12:00 AM	View Edit Run	
NSP: Dashboard D	ata Updating Task	Enabled	User	1	Advanced	11/23/18 2:35 AM	11/23/18 2:30 AM	View Edit Run	
Purge Threat and O	lient Events Older than	Disabled	User		Daily	No next runtime	Task has never run	<u>View</u> <u>Edit</u> <u>Run</u>	
	1cAfee ePO server)	Disabled	User		Weekly	No next runtime	Task has never run	View Edit Run	
Choose Columns	Revocations	Enabled	System	1	Daily	11/24/18 12:00 AM	11/23/18 12:00 AM	View Edit Run	
Delete	nt	Disabled	System	1	Daily	No next runtime	Task has never run	View Edit Run	
Disable Tasks	Policies	Disabled	User		Daily	No next runtime	Task has never run	View Edit Run	
Duplicate	Tasks	Disabled	User	1	Daily	No next runtime	Task has never run	View Edit Run	
Edit	agement	Enabled	System	1	Daily	11/24/18 12:30 AM	11/23/18 12:30 AM	View Edit Run	
Enable Tasks	Maintenance	Enabled	System		Weekly	11/25/18 2:00 AM	11/18/18 8:42 PM	View Edit Run	
Export Table	g	Enabled	System	1	Daily	11/23/18 3:15 AM	11/23/18 2:15 AM	View Edit Run	
Export Tasks	ize CA	Enabled	System	1	Daily	11/24/18 12:15 AM	11/23/18 12:15 AM	View Edit Run	
Due .	ize Topology	Enabled	System	1	Daily	11/24/18 12:15 AM	11/23/18 12:15 AM	View Edit Run	
NUT									
View									

Server tasks management

4. To configure the Server task, click **Edit**. The **Server Task Builder** is displayed.

Server Task Builder page

≡ 🕽 McAfee	Dashboards S	ystem Tree	Queries & Reports	Policy Catalog	Security Resources			^ ~
Automation Server Tasks								
Server Task Builder	1 Description		2 Actions		3 Schedule	4 Summary		
Name:	NSP: Dashboard Da	ta Updating Task	k					
Notes:	Server task to pull o	erver task to pull data from Network Security Manager at the specified interval to populate NSP dashboard						
Schedule status:	 Enabled Disabled 							
						Back	lext Save	Cancel

- 5. Edit the name of the server, if required.
- 6. Select the **Schedule status** as **Enabled**.
- 7. Select Next. In the Actions configuration, select NSP: Dashboard Data pull task.

Actions option

Automation Server Tasks

Conver Task Pui	Idae	1 Description		2 Actions	2 Schodula	15		
Server Task Bui	lder	1 Description		2 Actions	3 Schedule	/ 4 SL	Immary	
What actions do y	ou want the task to take	e?						
 1. Actions: 	NSP: Dashboard Data	a pull task	~					- +
Manager	LdapSync: Sync acro	ss users from LDAP	1					
Primary M Secondary	Load Systems by File	2		*				
Port	Migrate Data to New	Tables						
Username Password	NSP: Dashboard Dat	a pull task		*				
Confirm P	Product License Usag	ge: Count by Product	-	*				
	Product License Usag	ge: Entitlement Information						
	Purge Audit Log							
	Purge Client Events		-					
						Back	Next Save	Cancel

- 8. The page refreshes and displays the following fields, related to the Manager.
 - Manager Type (Standalone or MDR)
 - Primary Manager IP
 - Secondary Manager IP
 - Port
 - Username
 - Password

Confirm Password

Note

When you select Manager Type as Standalone, you need to enter only the Primary Manager IP address, (an asterisk sign is displayed near Primary Manager IP address indicating that this is the required field).

🗹 Note

When you select Manager Type as MDR, you need to enter both Primary Manager IP address and Secondary Manager IP address. The Secondary Manager IP address corresponds to the IP address of the Secondary Manager in an MDR pair.

🗹 Note

The user name and password to be entered are the Login ID and Password of the user with **ePO Dashboard Data Retriever** role, which you have defined in the Manager.

9. Edit the required fields and select **Next**.

Server Task Builder tab

≡ 🔀 McAfee	Dashboards	System Tree	Queries & Reports	Policy Catalog	Security Resources		. .
Automation Server Tasks							
Server Task Builder	1 Description	\rightarrow	2 Actions	3 Schedule		4 Summary	
Schedule type:	Weekly 🗸						
Start date:	11 / 23 / 20)18					
End date:	 In 1 / 24 No end date 	/ 2018					
Schedule:	Weekdays ~	at 🗸	12 🗸 : 12 🗸 🛛 AM 🗸				- +
						Back Next	Save Cancel

- 10. Edit the task schedule details, if required.
- 11. Select **Next**. The **Server task summary** is displayed.

Server Task Builder tab

Automation Server Tasks Server Task Builder 10 Name: NSF Notes: Ser	1 Description NSP: Dashboard Data Updating Task Server task to pull data from Network S admin	2 Actions Security Manager at the spe	*	3 Schedule	4 Summary	A
Server Task Builder 1 D Name: NSF Notes: Ser	1 Description NSP: Dashboard Data Updating Task Server task to pull data from Network S admin	2 Actions Security Manager at the spec	·	3 Schedule	4 Summary	^
Name: NSF Notes: Ser	NSP: Dashboard Data Updating Task Server task to pull data from Network 9 admin	Security Manager at the spe	- 1			
Notes: Ser	Server task to pull data from Network s	Security Manager at the spe	-15 (1) (1) (1) (1)			
	admin		cified interval to popula	te NSP dashboard		
lask owner: adn						
Schedule status: Ena	Enabled					
Schedule: St En Sc Ne	Start date: 11/23/18 End date: No end date Scheduled time: Weekdays at 12:12 Next runtime: 11/26/18 12:12 AI 11/27/18 12:12 AI 11/28/18 12:12 AI	2 AM M M				
Actions: 1.	1. NSP: Dashboard Data pull task Manager Type :Standalone Primary Manager IP : Secondary Manager IP : Port :443 Username :admin					

12. Select Save.

Create new Network Security Platform dashboards in McAfee ePO (optional)

If you want to create new dashboards for Network Security Platformin McAfee ePO[™] , do the following:

Task

- 1. From McAfee ePO^M home page, click \blacksquare , and select **Menu** \rightarrow **Reporting** \rightarrow **Dashboard**.
- 2. Select Dashboard Actions and click New.
- 3. Type name for the dashboard in **Dashboard Name** field and **Dashboard Visiblity** form drop-down list. For more information on working with Dashboards in McAfee ePO[™], refer to the *McAfee ePolicy Orchestrator Product Guide*.
- 4. Click Add Monitor and choose the Category as Queries.

Select Monitor window

≡ 🗂 McAfee	Dashboards	System Tree	Queries & Reports	Policy Catalog	Security Resources	▲ ▲ ~
Category: All	U Hickfee	Custom URL Viewer	Getting	Started	Malware Detection Trends	Close
						•
4						

- 5. Drag the Queries monitor type to the dashboard and select a Monitor related to Network Security Platform. For example, you can choose Monitor as **NSP: Top 10 Attacks**.
- 6. Select **OK**.
- 7. Configure six different monitors available on the dashboard as per your requirements.
- 8. Click **Save**. The new dashboard tab is displayed in McAfee ePO^{M} .

A sample dashboard in McAfee ePO[™] with the data from Network Security Platform is displayed below.



Dashboards tab

9. To get an enlarged view of any of the monitor, click the arrow at the top left corner of the monitor and select **Full Screen**.

NSP Top 10 Attack Destinations window



10. Click Close to close the dashboard monitor and return to home page.

Manager alert data displayed in the ePO dashboards

The ePO dashboard displays the Manager alert data when integrated with Network Security Platform. When the alert data in the Manager is to be updated in the ePO dashboard, the ePO server sends a request to the Manager server. The Manager server sends a file consisting the alert details from the Attack Log. When subsequent requests are made by the ePO server, the Manager compiles a file again with the alert data and sends it to the ePO server. Upon receiving the file, the ePO server compares the new alert data with the existing alert data, and compiles a list of the difference in data. An updated list consisting of the old data and the difference in data is displayed on the dashboard. Each time the ePO server requests for the alert data from the Manager server, alert data from the last 48 hours is compiled and sent to the ePO server.

If you require alert data of more than 48 hours to be sent to the ePO server, perform the following steps:

Windows based Manager server

- 1. RDP to the Manager server.
- 2. Go to <Manager install directory>\McAfee\Network Security Manager\App\config\ems.properties
- 3. In the ems.properties file, locate the following:

epo.dashbaord.alert.data.in.days

4. Edit the above line as follows:

epo.dashbaord.alert.data.in.days=<Alert data duration>

Here, the <Alert data duration> is the time period for which the alert data is compiled and sent to the ePO server. By default, it is set to 2 days.

5. Save the changes.

Linux based Manager server

- 1. Log in to the Manager shell.
- 2. Execute the edit ems.properties command.

🗹 Note

The edit command will edit the file using **vi-editor**. McAfee recommends you to use **vi_editor** command to perform editing operations on the files.

3. In the ems.properties file, locate the following:

epo.dashbaord.alert.data.in.days

4. Edit the above line as follows:

epo.dashbaord.alert.data.in.days=<Alert data duration>

Here, the <Alert data duration> is the time period for which the alert data is compiled and sent to the ePO server. By default, it is set to 2 days.

5. Save the changes.

Define a permission set in McAfee ePO

To define a minimal permission set in McAfee ePO, you must do the following steps.

- · Creating a new Permission Set (minimal permissions)
- Viewing and editing a permission set

Creating a new permission set

To create a McAfee ePO user and assigning minimal permission, do the following:

Task

In the McAfee ePO Home page, click and select User Management → Permission Sets.
 Permission Sets page appears.

Permission Sets page

≡ 🖞 McAfee	Dashboards System Tree (Queries & Reports Policy Catalog Security Resources	. .
User Management Permission Sets	New Permission Set Import Export All		
Permission Sets			
Search ×	Name and users:	Executive Reviewer 0 users 0 data	Edit
Global Reviewer		o Active Directory group mappings	
Group Admin	Agent Handler:	No permissions	Edit
Group Reviewer	Audit Log:	No permissions	Edit
MCP Catalog Admin	Automatic Response:	No permissions	Edit
	Client Events:	View Client Events	Edit
	Client Task Management:	No permissions	Edit
	Common Catalog:	No permissions	Edit
	Contacts:	Use contacts	Edit
	Dashboards:	Use public dashboards	Edit
	DXL McAfee MePO Certificate Creation:	No permissions	Edit
	Actions V		

2. Click New Permission Set.

New Permission Set page opens.

New Permission Set window

≡	🕽 McAfee"	Dashboards System Tr	ee Queries & Reports	Policy Catalog	Security Resources		≜ ×
^{User N} Per	lanagement mission Sets						
New Pe	rmission Set						
Name:				*			
Users:		 ✓ admin ✓ defaultDxlUser □ mcp-admin ✓ system 					
Active I this per	Directory groups mapped to mission set:	No Active Directory servers conf	gured. Go to Registered Servers	to configure one.			
						Save	Cancel

- 3. Type the name of the permission set in **Name**.
- 4. Click **Save**. After the permission set is created, it appears on the page.

Permission Sets tab

= 🔰 McAfee	Dashboards System Tree (Queries & Reports Policy Catalog Security Resources	. ~
User Management Permission Sets	New Permission Set Import Export All		
Permission Sets			
Search ×	Name and users:	NSP Permissions 0 users 0 Active Directory aroup mappings	Edit
Global Reviewer		e recre en escar y graap mappinga	
Group Admin	Agent Handler:	No permissions	Edit
Group Reviewer	Audit Log:	No permissions	Edit
MCP Catalog Admin			
NSP Permissions	Automatic Response:	No permissions	Edit
	Client Events:	No permissions	Edit
	Client Task Management:	No permissions	Edit
	Common Catalog:	No permissions	Edit
	Contacts:	No permissions	Edit
	Dashboards:	No permissions	Edit
	DXL McAfee MePO Certificate Creation:	No permissions	Edit
	Actions ~		

View and edit a permission set

You can view and edit a permission set. To define a new permission set, perform the following steps.

Task

- 1. Click the permission set displayed in the **Permission Sets** page.
- Scroll down to view or edit the settings for defining permission for the following: Click on **Edit**, next to the relevant settings to make changes to the permission set.
 - Network Security Platform To view and change settings

 Systems — 							
	Dashboards	System Tree	Queries & Reports	Policy Catalog	Security Resources	_	^ ~
User Management Permission Sets							
Edit Permission Set for nsp-permissio	on-set: Systems						
System Tree:	View "System" Note: visibility of	Tree" tab groups and systems	within the tree is controlled	by the System Tree Acco	ess permission set section		
Actions:	Wake up agent Git System Tr Deploy age Note: Ability t Settings Access for	Wake up agents; view Agent Activity Log Edit System Tree groups and systems Deploy agents Note: Ability to deploy is also controlled by the Agent Handler permission set section. Deploy Agent also needs McAfee Agent:Tasks Change Settings Access for some deployment methods.					
Tag use:	Apply, exclude	, and clear tags					
Tag catalog:	 No permission Create and ed Create and ed 	ns lit tags and tag grou lit tags, tag groups a	ps nd tag criteria (also requires	"Create and edit privat	e queries" permission)		
						Save	Cancel

- System Tree: To view the **System Tree** tab
- Tag use: To apply, exclude, and clear tags

🗹 Note

A user can create and edit tags only if the user has a permission set with the option **Create and edit tags and tag groups** enabled.

• System Tree access — To search and access the nodes and portions of the System Tree

Permission Sets page

≡ 💆 McAfee	Dashboards System Tree	Queries & Reports Policy Catalog Security Resources	🔷 🔔 🔺
User Management			
Permission Sets	New Permission Set Import Export All		
Permission Sets			
Search ×	1040		
Executive Reviewer	LUAPI	No permissions	Edit
Global Reviewer	McAfee Agent:	No permissions	Edit
Group Admin	n Aberratza en enec		
Group Reviewer	Multi-server roll up data:	No permissions	Edit
NSP_DOC	Network Security Platform:	View and change settings	Edit
nsp-permission-set	· · · · · · · · · · · · · · · · · · ·		
test_hsp	Policy Assignment Rule:	No permissiona	Edit
	Policy Management:	No permissions	Ildit
	Product Improvement Program:	No permissions	Edit
	Queries and Reports:	No permissions	Edit
	Registered servers:	No permissions	Edit
	Report Anonymization:	No permissions	Edit
	Server tasks:	No permissions	Edit
	Software:	No permissions	Edit
	Software Catalog:	No permissiona	Edit
	Systems:	View' "System Tree" tab Apply, exclude, and clear tags	Edit
	System Tree accessi	Can search on the following nodes and parts of the System Tree:Ny Organization Can access the following nodes and parts of the System Tree:Ny Organization	Edit
	Threat Event Log:	No permissions	Edit

Create McAfee ePO users with minimal permission

You can create McAfee ePO[™] user and assign minimal permission. To do so, perform the following steps.

Task

1. In the McAfee ePO^M Home page, click and select **User Management** \rightarrow **Users**.

Users page

\equiv \Box McAfee	Dashboards System Tree	Queries & Reports Policy Catalog Security Resources	▲ ▲ ×
User Management USERS New User			
Users			
Search ×	User name:	admin	
admin	Logon status:	Enabled	
defaultDxlUser mcp-admin	Lock Status	Unlocked	
system	Authentication type:	ePO authentication	
	Full name:		
	Phone number:		
	Email address:		
	Notes:		
	Manually assigned permission sets:	User is an administrator.	
	Last logon time	11/23/18 4:15:38 AM	
	Actions V		

2. Click New User.

The **New User** page appears.

New User page

≡ 🔀 McAfee	Dashboards System Tree Queries & Reports Policy Catalog Security Resources
User Management Users	
New User	
User namei	1PS-Administrator The name can contain less than 100 characters. It can't contain leading or trailing spaces, leading backslashes (\), or any of these characters: " i j
Logon status:	Enabled Disabled
Authentication type:	Certificate for discussion bas not been configured yet.
Full name:	[] (optional)
Email address:	(optional)
Phone number:	(optional)
Notes:	(optional)
Manually assigned permission sets:	Advisional stater Status for diversare Cascalities fractionare Cascalities fractionare Cascalities fractionare Cascalities Advisionare Cascalities Advisionare Cascalities Advisionare TESP Permittations for User1

3. In the **User name**, type a name.

Logon status shows **Enabled** by default. **Authentication type** is selected as **ePO authentication** by default. Do not make any changes.

4. In **Password**, type the password.

- 5. In **Confirm Password**, re-type the password.
- 6. (Optional) Enter the Full name, Email address, Phone number, and Notes in their respective fields.
- 7. In **Manually assigned permission sets**, select either **Administrator** or **Selected permission sets**. Select a single or multiple permission sets for **Selected permission sets**.

Check the permission set with minimal permission to be assigned to the user.

🗹 Note

You must define the permission set before assigning it to a user in case of **Selected permission sets**.

8. Click Save.

🗹 Note

After a user is created, **ePO recommends** users to change their password on their first login. This process should be completed before users try to test NSM connection with ePO.
Integration with McAfee Global Threat Intelligence

McAfee® Global Threat Intelligence[™] is a global threat correlation engine and intelligence base of global messaging and communication behavior, which enables the protection of the customers against both known and emerging electronic threats across all threat areas. The communication behavior includes the reputation, volume, and network traffic patterns.

You get complete integration with Global Threat Intelligence (McAfee GTI) in exchange for sending detailed alert information to McAfee. You can report, filter, and sort hosts involved in attacks based on their network reputation and the country of the attack origin by this integration.

Global Threat Intelligence technologies



GTI cloud provides comprehensive, real-time, cloud-based threat intelligence services and the Network Security Platform fetches the following intelligence information from the GTI cloud. GTI has the following components:

- Formerly TrustedSource
 - Web reputation URL and web domain reputation service to protect against web-based threats
 - Web categorization URL and web domain categorization service to take policy-based action on user web activity as well as protect customers against both known and emerging web-based threats
 - **Network connection reputation [also referred to as IP reputation]** IP address, network port, and communications protocol reputation service to determine granular reputation intelligence for protection against network threats
- **File reputation [formerly Artemis]** Comprehensive, real-time, cloud-based file reputation service to protect against both known and emerging malware-based threats

Each of these technologies work together to provide information about the threats and vulnerabilities, which gives GTI the ability to predictively adjust reputations across all threat areas and thereby avoid attacks.

How Network Security Platform - GTI integration works

The integration between Network Security Platform and GTI can be described using the three-part framework shown below.

GTI integration



The top-most tier represents Network Security Platform sending the threat data to GTI. GTI queries the threat data from the Sensors that are deployed in real-world settings.

The middle tier represents the bidirectional communications that occurs between Network Security Platform and GTI. Network Security Platform queries the cloud, and the cloud renders the latest reputation or categorization intelligence to Network Security Platform so that it can take an action.

Finally, the bottom tier represents GTI (IP Reputation, URL Reputation, and File Reputation) that ensures threat intelligence services like file reputation, web reputation, URL reputation, web categorization, message reputation, and network connection reputation. GTI Queries the threat data from Sensors. With each query, the cloud system learns something new about the subject of the query. This information is then combined with data from other threat vectors to understand cyber threats from all angles and identify threat relationships, such as malware used in network intrusions, websites embedded in malware code, websites hosting malware, callback activity associations, and more.

The IP Reputation component of GTI helps in SmartBlocking and Connection Limiting.

SmartBlocking activates blocking when high confidence signatures are matched, thus minimizing the possibility of false positives.

Connection limiting policies consist of a set of rules that enable the Sensors to limit the number of connections a host can establish or a connection rate.

When GTI is enabled, the attacks can be detected both for inbound and outbound traffics.

Inbound traffic is that traffic received on the port designated as "Outside" (that is, originating from outside the network) in In-line or Tap mode. Typically, inbound traffic is destined to the protected network, such as an enterprise intranet.

Outbound traffic is that traffic sent by a system in your intranet, and is on the port designated as "Inside" (that is, originating from inside the network) in In-line or Tap mode.

The IP Reputation is applicable for every connection but it is used differently for inbound and outbound connections:

- For outbound connection– When GTI is enabled for IP reputation, any "High risk IP" based on IP/port will be smart blocked based on the combination of both IP reputation and BTP signature value.
- For inbound connection When GTI is enabled and Connection Limiting rules are configured, you can block the malicious traffic received on the inbound connections. For example, you can deploy a Sensor in front of a web server, and enable GTI along with Connection Limiting rules to limit access to the server and prevent DoS attacks.

Configuring McAfee Global Threat Intelligence server for File Reputation in Manager

Before you begin

To integrate the Public GTI Cloud for File Reputation with Network Security Platform you need to have the following:

- Communication between the Manager and the McAfee Update Server.
- Name resolution configuration that allows the Sensor to resolve the hostname of the server that hosts the URL database.

Complete the following steps to configure the McAfee Global Threat Intelligence server for File Reputation:

Task

1. Select Manager \rightarrow <Admin Domain Name> \rightarrow Integration \rightarrow GTI and select File Reputation.

/My Company > Integration > GTI			•
GTI			
0			
File Reputation	Endpoint/URL Reputation		
GTI Cloud for File R	eputation Queries:	Public 💌	
Public GTI File Reputation Server Name:		https://nsp.rest.gti.mcafee.com/1	
Public GTI File Reputation Server Port:		TCP 443	
			Save

- 2. In the GTI Cloud for File Reputation Queries, select Public.
- 3. Click Save.

The Manager pushes the McAfee Global Threat Intelligence server configurations to the Sensors connected to the Manager.

Note

The GTI configurations from the Manager are sent to the Sensors in the following scenarios:

- Trust establishment between the Manager and Sensor
- Configuration change from private GTI to public GTI
- When public GTI credentials are changed

Configuring McAfee Global Threat Intelligence server for URL and IP Reputation in Manager

Complete the following steps to configure the McAfee Global Threat Intelligence server for URL and IP Reputation:

Task

1. Select Manager \rightarrow <Admin Domain Name> \rightarrow Integration \rightarrow GTI and select Endpoint/URL Reputation.

/My Company > Integration > GTI		
GTI		
0		
File Reputation Endpoint/URL Reputation		
GTI Cloud for Endpoint/URL Reputation Queries:	Public	
Public GTI Endpoint/URL Reputation Queries: nsp.gti.mcafee.com		
Public GTI Endpoint/URL Server Port: TCP 443		
Test Connection		Save

- 2. In the GTI Cloud for Endpoint/URL Reputation Queries, select Public.
- 3. Click Save.

The Manager pushes the McAfee Global Threat Intelligence server for URL and IP Reputation configurations to the Sensors connected to the Manager.

Network Security Platform integration with Private Global **Threat Intelligence (GTI) Cloud**

McAfee Private Global Threat Intelligence (GTI) Cloud offers you the option to utilize the GTI information in a private cloud environment.

To integrate with Private GTI Cloud, you will need to configure Private Cloud Server IP to point to your Private Cloud instead of default name server IP. Private Cloud deployments are typically intended to operate in an air gapped environment.

The integration of Network Security Platform with Private GTI Cloud enables appliances and services to retrieve IP Reputation and File Reputation to more accurately filter communications and protect electronic communications and transactions between people, companies, and countries.

The Manager maps the country codes received from Private GTI Cloud IP Reputation to the country, and displays in the Attack Log page. IP Reputation can also be used to create Connection Limiting rules and SmartBlocking.

🗹 Note

This feature is only available in NS-series and Virtual IPS Sensors running Sensor software version 9.2 and above.

Configuring Private Cloud for File Reputation in Manager

Before you begin

To integrate the Private GTI Cloud for File Reputation with Network Security Platform you need to have the following:

- The Server name or IP address with credentials for the Private GTI Cloud server for File Reputation.
- Name resolution configuration that allows the Sensor to resolve the hostname of the server that hosts the URL database.

To integrate with Private GTI Cloud for File Reputation, you need to configure Private Cloud Server settings to communicate with the Private GTI Cloud. By default, Network Security Platform is configured to communicate with the McAfee Global Threat Intelligence server.

Complete the following steps to configure the GTI Private Server for File Reputation:

Task

1. Select Manager \rightarrow <Admin Domain Name> \rightarrow Integration \rightarrow GTI and select File Reputation.

/My Company > Integration > GTI			0
GTI			
0			
File Reputation	Endpoint/URL Reputation		
GTI Cloud for File Reputation Queries:		Private	
Private GTI File Reputation Server Name or IP:			
Privat GTI File Reputation Server Port:		TCP 443	
User Name:			
Password:			
		Si	ave

- 2. In the GTI Cloud for File Reputation Queries, select Private.
- 3. Enter the Private GTI File Reputation Server Name or IP.
- 4. Enter the **User Name** and **Password** for the Private GTI File Reputation Server.
- 5. Click Save.

The Manager pushes the Private GTI Cloud configurations to the Sensors connected to the Manager.

Configuring Private Cloud for URL and IP Reputation in Manager

Before you begin

To integrate the Private GTI Cloud for URL and IP Reputation with Network Security Platform you need to have the following:

- The IP address for the Private GTI Cloud server.
- ZIP file that contains the following files in the .pem format:
 - Network Security Platform certificate
 - Private key for Network Security Platform certificate
 - GTI Private Cloud CA certificate
- Name resolution configuration that allows the Sensor to resolve the hostname of the server that hosts the URL database.

To integrate with Private GTI Cloud for URL and IP Reputation, you need to configure Private Cloud Server settings to communicate with the Private GTI Cloud. By default, Network Security Platform is configured to communicate with the McAfee Global Threat Intelligence server.

Complete the following steps to configure the GTI Private Server for URL and IP Reputation:

Task

1. Select Manager \rightarrow <Admin Domain Name> \rightarrow Integration \rightarrow GTI and select Endpoint/URL Reputation.



- 2. In the GTI Cloud for Endpoint/URL Reputation Queries, select Private.
- 3. Enter the Private GTI Endpoint/URL Server Name or IP.
- 4. The Private GTI Cloud for URL and IP Reputation uses certificates to authenticate solutions that want to consume its services. Click **Import Certificates** to import the following certificate files:
 - Network Security Platform certificate
 - Private key for Network Security Platform certificate
 - Private GTI Cloud CA certificate

Import Certificates	8	
0		
ZIP File:	Browse	•
	Import	

The Import Server Certificate dialog box opens.

🗹 Note

The certificate files and the client private key should be in the .pem format.

The Private GTI Cloud for URL and IP Reputation uses the Network Security Platform certificate and private key to authenticate Network Security Platform.

The Network Security Platform uses the Private GTI Cloud CA certificate to authenticate Private GTI Cloud.

- 5. Click Browse.
- 6. Select the .zip file that contains the files.
- 7. Click Import.

Once the import is complete, the Manager validates the files. If the validation is successful, the Private GTI Cloud Server

Certificate Status will be displayed as

8. Click Save.

The Manager pushes the Private GTI Cloud for URL and IP Reputation configurations to the Sensors connected to the Manager.

Test the connection to the Private Cloud server

After configuring the GTI server, use the Test Connection feature to check if the communication to the Private GTI Server is established:

Task

- 1. Select Manager \rightarrow <Admin Domain Name> \rightarrow Integration \rightarrow GTI \rightarrow Endpoint/URL Reputation.
- 2. Click Test Connection.

The **Test Connection** dialog box opens.



- 3. Enter the IP address to determine the risk and country based on GTI data.
- 4. Click Test.

If the Private GTI Cloud is configured, the reputation of the endpoint from the Private GTI Cloud is displayed. If the Private GTI Cloud is not configured, the reputation of the endpoint from the Public GTI Cloud is displayed. If the connection to both Cloud was not successful, an error is displayed.

The table below shows the list of responses and what they interpret:

Response	What it means	Next steps
Reputation : Unverified Geo : -	GTI communication is successful. There is no information available for the IP address and hence no country flag.	None
Could not connect to the server	 HTTP Status Code 404 Error - AJAX file not found error HTTP Status Code 500 Error - AJAX internal system error AJAX Timeout Errors AJAX Abort Errors Browser/Connectivity Errors 	Check the ems.log file for more information about the issue.
Invalid IP address	The IP address you entered is not valid.	Try another IP address.
Test Connection Failed	The test connection to the GTI server failed.	Check your connection settings before you proceed.

Configure Telemetry

The purpose of Telemetry is to facilitate you in providing helpful information to McAfee about your usage of Network Security Platform solution so that McAfee in turn optimizes your protection.

🗹 Note

The **Telemetry** pop-up is displayed when you open the Manager for the first time.

🗹 Note

Telemetry data is stored in the Telemetry server indefinitely.

To configure Telemetry:

Task

1. Select Manager \rightarrow <Admin Domain Name> \rightarrow Setup \rightarrow Telemetry. The Telemetry page is displayed.

Telemetry page

/My Company > Setup > Telemetry		Ø
Telemetry		What am I Sending?
•		
🖶 Alert Data Details 🛛 Exclude I	P address information for e	ndpoints on this <u>list</u> .
		O Yes 🔍 No
🕀 Alert Data Summary		O Yes 🔍 No
🕀 General Setup		O Yes 🔍 No
🕀 Feature Usage		O Yes 🔍 No
🕀 System Faults		O Yes 🔍 No
🖶 vNSP Cluster Usage		🔍 Yes 🔍 No
Alert Data Details Filter		
Send Alert Details for the Following Severity Alerts:	🗹 High 🛛 Medium	Low Informational *
Send Contact Information?	• Yes • O No	
First Name:	John	
Last Name:	Doe	
Street Address:		
Phone Number:		
Email Address:	john_d@mcafee.com	-
Test Connection		Save

🗹 Note

The following options are enabled in the **Telemetry** page by default:

- Alert Data Details
- Alert Data Summary
- General Setup
- Feature Usage
- System Faults
- vNSP Cluster Usage

The **vNSP Cluster Usage** option can be configured only when there is a vNSP Cluster in the Manager.

🗹 Note

If at any point, you want to review what you are sending to the Telemetry server, run the **Default-Telemetry (NSP)** Next Generation report.

2. Select either **Alert Data Details** or **Alert Data Summary** to enable GTI IP Reputation integration. Using the **Telemetry** page, you can configure the following information categories:

• Select **Alert Data Details** for complete integration with GTI IP Reputation. This permits you to report, filter, and sort hosts involved in attacks based on their network reputation and/or country of their origin. When the **Alert Data Details** option is selected, the following attributes are sent in real time to McAfee Labs for each attack:

- Application Name
- Attack Name
- Attack Time
- Attacker DNS Name
- Attacker IP Address
- Attacker Country
- Attacker OS
- Attacker Port
- Attacker Risk
- Callback alert information
- Category
- Count
- Detection Mechanism
- Direction of Attack
- For correlated alerts: Triggered component attacks and their connection logs
- For heuristic attacks against Web application servers: Threshold, confidence, weight, and the matched blocked strings
- For ATD attacks: File name, size, type, MD5 hash, UUID, and malware confidence
- Malware Engine Results
- Malware URL
- NSP Attack ID
- Protocol
- Relevance (and method used to determine it)
- Result
- Signature ID
- Sub-Category
- Target DNS Name
- Target IP Address
- Target Country
- Target OS
- Target Port
- Target Risk
- Type
- URI

The following alert summary information is sent hourly to McAfee Labs:

- A count of each attack seen
- The list of NSP attack IDs seen

The following general setup information is sent daily to McAfee Labs (so the alert data can be correctly interpreted):

Manager software version and active signature set version

You also have the option to exclude data from specific endpoint IP addresses by using the **Exclude IP address** information for endpoints on this list. option in the header.

• Select **Alert Data Summary** to view partial alert details in the **Attack Log**. Using this option, you can query McAfee's http://www.trustedsource.org by right-clicking on an alert in the **Attack Log** and view details of the source or destination IP address, port, and country of origin.

The following alert summary information is sent hourly to McAfee Labs:

- A count of each attack seen
- The list of NSP attack IDs seen
- The number of alerts whose relevance was determined by each available method
- Top 10 (as per executable confidence) EIA attacks

The following general setup information is sent daily to McAfee Labs (so the alert data can be correctly interpreted):

- · Manager software version and active signature set version
- **General Setup** The following general setup information is sent daily to McAfee Labs:
 - Manager install type, software version, and active signature set version
 - Manager OS type, OS version, and VM type (if applicable)
 - Manager GUID, MDR GUID (as applicable), and Telemetry GUID
 - Is a Central Manager in use
 - Is Manager Disaster Recovery (MDR) in use
 - OS type, OS version, and VM type (if applicable) of each device
 - Serial number, model, software, and hardware version of each device
 - Is each device part of an HA pair and/or Stack
 - The number of monitor ports operating in inline, SPAN, and tap modes
 - The number of dedicated, CIDR, and VLAN interfaces defined
 - The number of administrative users, the custom roles in use, and the permissions in those roles
 - Callback Detector and GAM version for each active device
 - Interface name, protection category and assigned IPS, Malware and Inspection Options policy IDs
- Feature Usage The following feature usage information is sent daily to McAfee Labs:
 - Are inbound MSRPC/SMB fragments being reassembled
 - Are outbound MSRPC/SMB fragments being reassembled
 - Callback Detectors status and version
 - · Gateway Anti-Malware engine and DAT versions
 - Is ePO integration enabled
 - Is MVM integration enabled to run vulnerability scans
 - Is MVM integration enabled to calculate alert relevance
 - Is IPS alert notification enabled (SNMP, syslog, email, pager, script)
 - Is inbound GTI IP reputation lookup enabled
 - Is outbound GTI IP reputation lookup enabled
 - Is GTI IP reputation lookup used to enhance SmartBlocking decisions

- Is inbound heuristic Web application server protection enabled
- · Is outbound heuristic Web application server protection enabled
- Is inbound XFF header parsing enabled
- Is outbound XFF header parsing enabled
- · Is advanced callback detection enabled, and are events sent to NTBA for further analysis
- Is inbound chunked HTTP response traffic being decoded
- Is outbound chunked HTTP response traffic being decoded
- Is inbound HTML-encoded HTTP response traffic being decoded
- Is outbound HTML-encoded HTTP response traffic being decoded
- Is inbound base64-encoded SMTP traffic being decoded
- Is outbound base64-encoded SMTP traffic being decoded
- Is inbound GTI URL Reputation enabled
- Is outbound GTI URL Reputation enabled
- Is inbound Deep File Inspection enabled
- Is outbound Deep File Inspection enabled
- The L7 data collected (protocols and their fields)
- The advanced malware policy definitions
- The list of methods enabled for determining alert relevance
- The number of default IPS policies in use
- The number of custom IPS policies in use
- The number of custom McAfee-format attacks in use
- The number of Snort rules in use
- The number of ignore rules defined
- The number of M-series devices with IPS licenses assigned
- The number of sub-interfaces in use
- The number of device-pre firewall policies assigned
- The number of port firewall policies assigned
- The number of interface firewall policies assigned
- The number of device-post firewall policies assigned
- The number of IPS attack definitions whose default settings have been customized
- The number of custom NextGen reports and their SQL queries
- The number of interfaces with application identification enabled
- The number of IPS devices with ATD integration enabled and malware policies with ATD analysis enabled
- The number of NTBA devices with EIA integration enabled
- The number of Virtual IPS sensors and Virtual IPS sensor licenses
- The number of Interfaces using policy group
- The number of custom policy group assigned
- The number of default policy group assigned
- The number of devices enabled inbound SSL decryption
- · The number of devices enabled inbound SSL decryption with Diffie-Hellman
- · Total number of devices with outbound SSL decryption enabled

• Name, grant ID, license key, Sensor model, and allowance count associated with each proxy SSL decryption license

- Total number of devices assigned a system license
- The number of system licenses available and in use
- Name, grant ID, license key, expiration, model and device associated with each system license
- Block and alert only based CVE coverage for each of the IPS policies in use
- Engine status and file types enabled for each of the Malware policies in use
- Option status for each of the Inspection options policies in use
- System Faults The following System Fault information is sent daily to McAfee Labs:
 - Device Faults
 - Manager Faults

🗹 Note

Though these two events are represented separately, they are sent to GTI as a single event.

- **vNSP Cluster Usage** The following data specific to vNSP clusters is sent to McAfee daily:
 - Name and grant ID associated with each Virtual IPS Sensor license
 - Overall license compliance status
 - Total number of allowed virtual Sensors
 - Total number of Virtual Sensors currently in use with vNSP Clusters
 - Total number of Virtual Probes currently in use with vNSP Clusters
 - Maximum number of Virtual Probes used
 - Manager version
- 3. Select **Yes** on the relevant information categories for which you prefer to send details to McAfee Labs.
 - a. After configuring the Alert Data Details and Alert Data Summary, navigate to the Attack Log page.
 - b. Select the alert and click $\textbf{Other Actions} \rightarrow \textbf{Perform GTI Forensics}.$
 - c. Click on attacker or target IP address. A new browser window opens, displaying information on that URL.

🗹 Note

If Global Threat Intelligence is not enabled in the **GTI** page, the **Perform GTI Forensics** option is disabled.

4. In the **Alert Data Details Filter**, select the type of alert severity, based on which you want to send the information.

The available options are:

- High
- Medium
- Low
- Informational
- 🗹 Note

The Alert Data Details Filter is displayed only when you select Alert Data Details category.

- 5. In the **Technical Contact Information**, update the following fields to provide your contact information to McAfee Labs.
 - Send Contact Information?
 - First Name
 - Last Name
 - Street Address
 - Phone Number
 - Email Address
- 6. To check whether communication to the GTI server is established, click **Test Connection**.
- 7. Click Save.

Exclude IP address information for specific endpoints

You can define blocks of addresses to be grouped together. By defining these blocks, the information on any alert that contains any IP address matching these blocks will not be sent to McAfee Labs.

To exclude IP address information for hosts:

Task

1. Go to Manager \rightarrow <Admin Domain Name> \rightarrow Setup \rightarrow Telemetry.

The **Telemetry** page is displayed.

2. Click the **list** hyperlink within **Exclude IP address information for endpoints on this list.** displayed in the **Alert Data Details** section header.

The **Exclusions** dialog is displayed.



- 3. Enter the IP address for exclusion in the IP Address field.
- 4. Enter the CIDR value for the mask in the **Mask Length** field.

2 | Integration with McAfee Global Threat Intelligence

🗹 Note

The CIDR value should be between 0 to 32.

5. Click Add to List.

The IP address, mask length gets added and is displayed in the IP Address/Mask List field.

🗹 Note

You can remove an item in the IP Address/Mask List by clicking Remove Selection.

6. Click Save.

Network Security Platform-GTI integration for IP Reputation

The integration of Network Security Platform and GTI for IP Reputation [formerly TrustedSource] enables appliances and services to more accurately filter communications and protect electronic communications and transactions between people, companies, and countries.

The Manager maps the country codes received from GTI IP Reputation to the country, and displays in the Attack Log page.

IP Reputation can also be used to create Connection Limiting rules.

🗹 Note

Reputation is actually determined using a combination of IP address and port. The same IP address might, therefore, have a different reputation depending on the port currently in use.

How Network Security Platform-GTI integration for IP Reputation works

The Manager integrates with the GTI IP Reputation to obtain the reputation scores on hosts and geo-locations that are displayed in Attack Log.

The Sensor requests reputation for hosts from GTI. The reputation score acts as an important factor in determining whether to block the host. The scores are cached for one hour. After an hour, the information ages out and if the information is required again, the Sensor makes the GTI request again.

🗹 Note

Cache is not maintained on reboot.

Reputation scores:

• Minimal Risk (<=14)

- Unverified (15 to 29)
- Medium Risk (30 to 49)
- High Risk (> 49)

After a High Risk External IP host is found, the traffic from that host can be blocked or the host itself can be quarantined.

🗹 Note

The terms reputation scores and risk assessment scores are interchangeably used for Sensor and Manager in Network Security Platform.

🗹 Note

DNS must be configured for the Sensor to reach the GTI server.

🗹 Note

HTTPS is used to obtain the reputation of the hosts.

The Sensor does not request reputation scores for hosts that have internal IP addresses. The following private IP address blocks are considered as internal IP addresses by the Sensor:

- 0.0.0.0/8
- 10.0.0/8
- 100.64.0.0/10
- 127.0.0.0/8
- 169.254.0.0/16
- 172.16.0.0/12
- 192.0.2.0/24
- 192.88.99.0/24
- 192.168.0.0/16
- 198.18.0.0/15
- 198.51.100.0/24
- 203.0.113.0/24
- 224.0.0.0/3

Enhanced SmartBlocking

When IP Reputation is enabled, the Sensor uses the reputation of the source host as an additional factor for blocking which in turn enhances SmartBlocking.

Each attack has a signature set which is in turn associated with a confidence level. Confidence level and reputation score together play the role in Smartblocking an attack. An attack is Smartblocked only when the sum total of the confidence level and the reputation score becomes 6.

Risk levels of the hosts:

- Host is considered malicious— +2 increase in confidence level
- Host is considered of medium risk— +1 increase in confidence level

🗹 Note

Only attacks marked for Smartblocking are considered for IP reputation scores and thus only those attacks are SmartBlocked.

🗹 Note

The reputation score is used along with Benign Trigger Probability to increase the confidence level and make a blocking decision.

New IPS attack definitions are also added for High Risk hosts. This allows you to block/quarantine a host outright if it is a high risk.

This will only happen if :

- The attack definitions are included in the IPS Policy for the interface or sub-interface level.
- GTI is enabled for the interface and sub-interface level.

To optimize performance, you can place certain trusted IP addresses/networks under an exclusion list. The number of entries you can exclude per Sensor are:

Sensor model	Number of exclusion list entries permitted
NS9500 stack - 100 Gbps throughput	128
NS9500 stack - 60 Gbps throughput	128
NS9500 stack - 40 Gbps throughput	128
NS9500 standalone - 30 Gbps throughput	128
NS9500 standalone - 20 Gbps throughput	128
NS9500 standalone - 10 Gbps throughput	128
NS9300, NS9200, NS9100	128
NS7500 - 7.5 Gbps throughput	128
NS7500 - 5 Gbps throughput	128

Sensor model	Number of exclusion list entries permitted
NS7500 - 3 Gbps throughput	128
NS7300, NS7200, NS7100	128
NS5200, NS5100	64
NS3500	32
NS3200, NS3100	32

Refer to McAfee Network Security Platform Product Guide for more details.

Configure Endpoint Reputation for an admin domain

Before you begin

If the Manager is not integrated with McAfee GTI Lookup, you can see the following message: **Please enable sending of Alert Data Details on the Participation page to make integration with GTI Lookup available**. Select **Integration** \rightarrow **Global Threat Intelligence** to enable the integration.

If you configure Endpoint Reputation at an admin domain, you can inherit these settings for the interfaces of the Sensors in this domain. You can also customize these settings for specific interfaces.

Task

 In the Manager, go to Policy → <Admin_Domain_Name> → Intrusion Prevention → Policy Types → Inspection Options. The Inspection Options page is displayed.

/My Company > Intrusion Prevention > Policy Types > Inspection Options				0			
Inspection Options							
0							
Name							
Name I							
Default Client and Server Inspection	Inspect traffic both from internal end	/My Company	Owner and child domains	Mar 29, 2019 11:40:51	admin		No
Default Client Inspection	Inspect traffic from internal endpoint	/My Company	Owner and child domains	Mar 29, 2019 11:40:51	admin		No
Default Server Inspection	Inspect traffic to exposed Web and m	/My Company	Owner and child domains	Mar 29, 2019 11:40:51	admin		No
http-rsp-scan	http-rsp-scan	/My Company	Owner and child domains	Jun 19, 2019 11:28:45	admin	<u>14</u>	Yes
And 1999 199 199		/My Company	Owner and child domains	Jun 19, 2019 12:30:11	admin		Yes
+ 41 -							

2. Double-click a policy for which you want to configure Endpoint Reputation.

To add a new policy, click **+**. Using either action, a page with the policy details appears with the **Properties** tab selected. 3. Update the following fields as applicable:

Option	Definition
Name	Enter a unique name to easily identify the policy.
Description	Optionally describe the policy for other users to identify its purpose.
Owner Domain	Displays the admin domain to which the policy belongs
Visibility	When selected, makes the policy available to the corresponding child admin domains. However, the policy cannot be edited or deleted from the child admin domains. From the drop-down list, select the option for the visibility level of the rule object. Available options are Owner and child domains and Owner domain only .
Editable here	The status Yes indicates that the policy is owned by the current admin domain. This field is uneditable.
Statistics	
Lasted Updated	Displays the time stamp when the policy was last modified. This field is uneditable.
Last Updated By	Displays the user who last modified the policy. This field is uneditable.
Assignments	Indicates the number of inline ports to which the policy is assigned
Prompt for assignment after save	If you deselect this option you can save the policy now and assign it to the Sensor resources as explained in the following section. If you select this option, the Assignments window opens automatically when you save the policy and you can assign the policy to the required Sensor resources.
Cancel	Reverts to the last saved configuration

4. Click Next.

The screen shifts to the **Inspection Options** tab. By default, the **Traffic Inspection** tab is selected.

5. Click the **GTI Reputation Services** tab. Endpoint Reputation Analysis is used to influence SmartBlocking decisions, create connection limiting rules, or to take action when a connection to or from a high-risk endpoint is seen on your network.

/NSP_Doc_03 > Intrusion Prevent	/NSP_Doc_03 > Intrusion Prevention > Policy Types > Inspection Options				Ø		
Properties Inspection Optio	ons						
Traffic Inspection Advanced Call	lback Detection GTI R	eputation Services	Web Serve	er - Heuristic Analysis	Web Server - Der	nial-of-Servic	e Prevention
Endpoint URL							
•							
Endpoint Reputation Analysis:		Inbound and Outbo	und 👻				<u>^</u>
Use Endpoint Reputation to Inf	fluence SmartBlocking:	Enabled		•			
Exclude Internal Endpoints from	m GTI Lookups:	Disabled					
CIDRs Excluded from Endp	point Reputation Loo	kups					\odot
•							
New CIDR:							1
···· 10.1.1.0/24							
m. 10.1.2.0/24							
Protocols Excluded from Er	ndpoint Reputation I	Lookups					0
Available Protocols:							
1 CVS							
2 FTP DATA							
Test Inspection Option Policies				Prompt for assigned	nment after save	Save	Cancel

On the **Endpoint** tab, configure the following fields:

Option	Definition		
Endpoint Reputation Analysis	 Select any of the following options: Disabled Inbound only Outbound only Inbound and Outbound 		
Use Endpoint Reputation to Influence SmartBlocking	Select Enabled to enable endpoint reputation to Influence SmartBlocking. Select Disabled to disable the option.		
Exclude Internal Endpoints from GTI Lookups	Select Enabled to exclude internal endpoints from McAfee GTI Lookups. Select Disabled to disable the option.		
CIDRs Excluded from Endpoint Reputation Lookups			
New CIDR	Enter the new CIDR and click Add to add to the CIDR list to be excluded. Click to remove the CIDR from the list.		

Option	Definition
	Note: The CIDR exclusion list is shared by Advanced Callback Detection and Endpoint Reputation Analysis .
Protocols Excluded from Endpoint Reputation Lookups	In the drop-down list, select the protocol to be excluded from McAfee GTI Lookups and click Add . The selected protocol is displayed in the field below. Click to remove the protocol from the list.
Prompt for assignment after save	When selected, you are automatically prompted to select the Sensor resources to which you want to assign the policy.

6. Click **Save** to confirm your settings.

Clicking **Cancel** reverts to the last saved configuration.

Configure Endpoint Reputation for an interface

You must enable Endpoint Reputation at the interface level for the Sensor to perform IP address lookups. At the interface level, you can inherit the settings from the admin domain or customize it for the interface.

Task

- 1. In the Manager, select Policy \rightarrow <Admin Domain Name> \rightarrow Intrusion Prevention \rightarrow Policy Manager.
- Double-click the interface for which you want to configure Endpoint Reputation.
 A <Device Name/Interface> panel appears for the selected interface.
- 3. In the **Inspection Options** section of the **<Device Name/Interface>** panel, select the Endpoint Reputation policy you want from the **Policy** drop down list.

To create a new policy, click the 📩 icon or double click on the policy to edit an already assigned policy.

4. Click the + icon.

The **Properties** tab for a new policy appears.

- 5. Enter the **Name** and **Description**, select the **Visibility**, and click **Next**. The page shifts to open the **Inspection Options** tab.
- 6. Click the **GTI Reputation Services** tab and the **Endpoint** sub-tab opens.
- 7. Enable Endpoint Reputation Analysis in the required direction.

/My Company > Intrusion Prevention > Policy Types > Inspection Options						Ø
Properties Inspection	n Options					
Traffic Inspection Adva	nced Callback Detection	GTI Reputation Services	Web Server - Heuristic Analysis	Web Server - Denial-of-Service Prevention		
Endpoint URL						
0						
Endpoint Reputation Ana	alysis:	Disabled Disabled Inbound only Outbound only Inbound and Outbound				
HTTP_Policy				Prompt for assignment after save	Save	Cancel

If the outbound connection is enabled, the reputation of the destination IP address is identified. If the inbound direction is enabled, the reputation of the source IP address is identified.

8. Specify the Endpoint Reputation options in the corresponding fields.

/NSP_Doc_03 > Intrusion Preve	ention > Policy Types > I	inspection Options					Ø
Properties Inspection Opt	ions						
Traffic Inspection Advanced C	Callback Detection GTI	Reputation Services	Web Serv	er - He	euristic Analysis Web Serv	er - Denial-of-Servi	ice Prevention
Endpoint URL							
•							
Endpoint Reputation Analysis	s:	Inbound and Outbo	und 👻				Î
Use Endpoint Reputation to I	nfluence SmartBlocking	g: Enabled		•			
Exclude Internal Endpoints fr	rom GTI Lookups:	Disabled					
CIDRs Excluded from End	dpoint Reputation Lo	ookups					\circ
0							
New CIDR:							
···· 10.1.1.0/24							
I0.1.2.0/24							
Protocols Excluded from	Endpoint Reputation	1 Lookups					0
Available Protocols:							
1 CVS							
2 FTP DATA							
Test Inspection Option Policie	es				Prompt for assignment after s	save Save	Cancel

Option	Definition
Endpoint Reputation Analysis	 Select any of the following options: Disabled Inbound only Outbound only Inbound and Outbound

Option	Definition
Use Endpoint Reputation to Influence SmartBlocking	Enable to enhance the blocking of an attack by a high-risk host.
Exclude Internal Endpoints from GTI Lookups	Enable to exclude all the internal hosts from Reputation Lookups based on their IP addresses.
CIDRs Excluded from Endpoint Reputation Lookups	 List of IPv4 networks that are excluded from Reputation Lookup. New CIDR — Click to add an IPv4 network. After you enter the network address and the CIDR notation, click Add. Delete — Hover over the network you want to delete and click the "x" icon to delete the network. Iverse The IP addresses specified the exclusion list, the entire flow is marked as exclusion list irrespective of the direction of the flow.
Protocols Excluded from Endpoint Reputation Lookups	 Create the exclusion list for Reputation Lookup based on protocols. When a protocol is added, the Sensor does not perform Reputation Lookup with respect to the corresponding flow. Available Protocols — Select the protocol to be excluded from the drop down list and click Add. Delete — Hover over the protocol you want to delete and click the "x" icon to delete the protocol.
Save	Saves the Endpoint Reputation Lookup configuration.
Cancel	Cancels the configuration process and exits the page.

- 9. Click **Save** in the **<Device Name/Interface>** panel to save the configuration changes.
- 10. Do a configuration update for the corresponding Sensor.

Configure Endpoint Reputation from sub-interface level

You can configure Endpoint Reputation from the sub-interface level. Select **Policy** \rightarrow **<Admin Domain Name>** \rightarrow **Intrusion Prevention** \rightarrow **Policy Manager**. Endpoint Reputation for a sub-interface is configured in the same way as an interface.

Refer to the Configure Endpoint Reputation for an interface section for more information.

Viewing the Global Threat Intelligence alert category details

The following Global Threat Intelligence alert categories are included in the Attack Log page.

- Target IP Address
- Target Risk
- Target Country
- Target Port
- Target Hostname
- Target Proxy IP
- Attacker IP Address
- Attacker Risk
- Attacker Country
- Attacker Port
- Attacker Hostname
- Attacker Proxy IP

For more information on alerts and monitors, see the McAfee Network Security Platform Product Guide.

Next generation reports

The Next Generation report option allows you to generate customized reports. You can make selections, such as the type of data to base the report on, and the format in which you want the data to be presented like table, bar chart, pie chart, etc. From a list of fields that are applicable for a report, you can select the fields that you wish to display; you can also specify the conditions that must be met to include the information for those fields in the report.

You can then save the query that you have just built for later use. You can also generate the report immediately or schedule it to run automatically by setting options like the period to be considered for displaying data, report output format, etc.

Next Generation reports can be generated from **Analysis** \rightarrow **Event Reporting** in the Manager.

When you select the **Next Generation Reports** in the Manager, the **Next Generation Reports** page displays the **Saved Reports** on the left pane by default.

Next generation reports details

The following reports are included in the Next Generation Reports page under Event Reporting menu.

- Default Attack Source Reputation Summary
- Default Top Attack Destinations
- Default Top Attack Sources
- Default Top 10 Attack Source Countries
- Default Telemetry (NSP)
- Default Telemetry (McAfee)

You can customize and create user defined reports with a choice of data source, presentation and filter by selecting **New** in the **Next Generation Reports** page.

For more details, see the McAfee Network Security Platform Product Guide.

How to view Telemetry report

The GTI report is a report that shows all the details that will be sent to McAfee Labs. Viewing this report helps you in understanding the list of information sent by you. The report generates a complete information on **Alert Data Details**, **IP Exclusion List**, **Alert Data Summary**, **General Setup**, **Feature Usage**, **System Faults**, and **Technical Contact Information**.

To view the GTI Report, do the following:

1. In the Manager, go to Analysis \rightarrow <Admin Domain Name> \rightarrow Even Reporting \rightarrow Next Generation Reports.

The Next Generation Reports page is displayed.

2. Select Default - Telemetry (NSP) report and click Run.

The **Run Report** page is displayed.

3. Select the Date Options and Report Format and click Run.

🗹 Note

For **HTML** and **PDF** options, the report is displayed in the Manager. For **Save as CSV** and **Save as HTML**, use the **File Download** option to save the report.

The **Telemetry Report** is displayed.

/My Compa	My Company > Event Reporting > Next Generation Reports					0
						Â
			UM	CAfee Network Security Platform Report Default - Telemetry (NSP) Start Date: 2019-10-23 C End Date: 2019-10-23 C Report Generation Time: 2019-10-23 C	0:00:00 IST 3:59:59 IST 1:31:40 IST	
				1	efault - Telemetry (NSP)	
	#	Time		Data Type	Data Sent to McAfee Labs	
	1.	2019-10-23 09:12:19.0		System Faults	•	
	2.	2019-10-23 09:12:18.0		Version Information	Manager Telemetry ID: 806bf08-ca59-47be-9458-2f171ab934cc Manager Software Version: 10.1.7.1.73 Active Signature Set Version: 10.8.0.6	
					ABI: ABB MicroSCADA wserver.exe Remote Code Execution 10 ADORE: Adobe Flash Media Server Load Arbitrary DLL: File Vulnerability 1 ARKERA: Knox Arkeia Request Message Buffer Overflow 9 AllenYault: AlenYault OSSIM Framework Backup Command Execution 5 BACKDOOR: Back Onfice Trajan 76 BACKDOOR: MightDragon Communication Detected 17 BACKDOOR: MightDragon Communication Detected 17 BACKDOOR: Proxy-Agent.af.gen Detection 4 BACKDOOR: Shoft BackOnfice Detected 17 BACKDOOR: Shoft BackOnfice Detected 10 BACKDOOR: Shoft BackOnfice Detected 13 BACKDOOR: Shoft BackOnfice Detected 13 BACKDOOR: Shoft BackOnfice Detected 13 BACKDOOR: Shoft BackOnfice Detected 13 BACKDOOR: Win32 AckChard Trajan 13 BACKDOOR: Win32 AckChard Trajan 31 BACKDOOR: Win32 AckChard Trajan 31 BACKDOOR 32 BOTI: AnjaoL BTrajan Server DUPE Command Arbitrary File Upload 11 BOTI: AnjaoL/B Trajfic Detected 18 BOTI: AnjaoL/B Trajfic Detected 18 BOTI: AnjaoL/B Trajfic Detected 18 BOTI: AnjaoL/B Trajfic Detected 18 BOTI: AnjaoL/B Trajfic Detected 18	v

🗹 Note

The NS9500 Sensors in a stack will be listed individually in **Default - Telemetry (NSP)** report under **General Setup** section.

Network Security Platform-GTI integration for connection limiting policies

Connection Limiting policies consist of a set of rules that enable the Sensors to limit the number of connections a host can establish or a connection rate.

The Sensor provides the ability to define threshold values to limit number of connections (three-way handshakes for TCP) a host can establish. The number of connections or the connection rate that is less than or equal to the defined threshold value is allowed, whereas the same exceeding the value is dropped. This helps in minimizing the connection-based DoS attacks on server.

Connection Limiting rules are of two types:

- Protocol-based
- GTI-based

Only GTI-based rules are applicable for the integration of this technology with IP Reputation. These rules are defined for traffic to/from external hosts based on reputation and geo-location of the external hosts.

When GTI is enabled and Connection Limiting rules are configured, you can block the malicious inbound connections. In this scenario, if Sensor is deployed in front of the Web server, GTI along with Connection Limiting rules limit access to their servers (DOS prevention).

These defined Connection Limiting policies can also be assigned at the interface and sub-interface levels.

Refer McAfee® Network Security Platform Product Guide for more information.

Network Security Platform-GTI integration for File Reputation

Network Security Platform integrates with File Reputation (formerly Artemis technology), which is a cloud-based service that provides real-time protection from malicious file downloads.

Network Security Platform also provides users the option to upload custom fingerprints to the Manager which can be used for File Reputation instead of GTI lookups or to complement them.

Network Security Platform provides the following functionalities through this enhanced integration:

- Response actions for detected malware (for example, raise alerts, send a TCP reset or block the file)
- Enabling Network Security Platform administrators to upload custom fingerprints for File Reputation
- Reports on File Reputation detection, and other related statistical data

Following diagram gives an overview of Network Security Platform-File Reputation integration.

Integration between Network Security Platform and File Reputation



When a file download is detected over HTTP traffic, the file type is checked. If the file type matches the list of file types for which the malware is checked, the Sensor creates a fingerprint (MD5 hash value) of the file, embeds the fingerprint in a standard HTTPS request, and sends it to GTI cloud server. The list of file types to be checked for GTI fingerprints is defined in the signature set (read-only). You can enable or disable GTI fingerprints scanning for different supported file types in the malware policy. The cloud server compares the fingerprint against the threat database maintained by McAfee Labs. If the fingerprint is identified as a known malware, the cloud server notifies the Sensor and it enforces a response action for the malware. Note that the alerts for the malware can be viewed in Attack Log.

🗹 Note

The fingerprint is a short-bit string (MD5 hash value) that uniquely identifies the original file.

Terminologies

Sensitivity Level

Malware dirtiness level is the level of malicious content in the malware fingerprint. A very high dirtiness level indicates a known malware.

Sensitivity level indicates the level to which Network Security Platform needs to be sensitive to the malware dirtiness level contained in the responses from File Reputation.

Manager provides five different values for Sensitivity Level - Very Low, Low, Medium, High, and Very High. By default, the Sensitivity Level is Very Low.

When you set the Sensitivity Level as Very Low (the default), the Sensor only responds to the File Reputation fingerprints with a high dirtiness level (known malware). Response action from the Sensor can be alert, block, or both as described earlier.

Detection Type

Defines the type of detection that is required for the malware. You can detect malware using File Reputation alone, or the Custom fingerprints, or both. When you enable both File Reputation detection type and Custom detection type, the latter takes precedence over the former.

Public or Private GTI Server details

IP address or Server name information related to the Public or Private GTI Servers. To communicate with the Public GTI and Private GTI Cloud, you need to configure Public Cloud and Private Cloud Server settings. In both the cases, the Sensor embeds the MD5 hash value of the file in a HTTPS REST JSON Request. File Reputation server sends back HTTPS Responses (which contain information such as Malware dirtiness level) to the Sensor.

Benefits of File Reputation

The key benefits of File Reputation include the following:

- · Compresses the threat protection time period from days to milliseconds
- Increases malware detection rate.
- Reduces downtime and remediation costs associated with malware attacks

Network Security Platform-File Reputation integration in detail

Following diagram shows the communications between Sensor, Manager and File Reputation Server.

Communications between Sensor, Manager, and File Reputation server



File Reputation uses the Internet REST infrastructure to communicate and cache information related to the file downloads in the user systems.

As mentioned earlier, the Sensor detects file downloads, and classifies them as suspicious as defined in the protocol specification. For example, HTTP downloads of type .exe, .dll, .scr and a maximum file size of 1 MB (for signature set 7.5.13.7 and lower) and 4 MB (for signature set 7.5.14.25 and higher) are classified as "suspicious".

The Sensor creates a fingerprint (MD5 hash value) of the file, embeds the fingerprint in a standard HTTPS Request in REST JSON format, and sends it to File Reputation server. The Sensor exchanges HTTPS queries and responses directly with the File Reputation Server.

🗹 Note

Ensure that your firewall is configured so that the Sensor can send the request and receive the response from the File Reputation server.

The Sensor management port can handle multiple HTTPS requests and responses. File Reputation HTTPS Queries (which are TCP Requests) are sent out from the Management port of the Sensor to the File Reputation Server directly and it receives direct replies. File Reputation responses are encoded in the standard HTTPS responses.

Response actions for File Reputation alerts are now part of the policy and one can configure response actions, such as block/ reset in Policy Editor, or in the Attack Log for Malware attacks.

The Sensor takes a response action (alert/block or both) on the file as per the Response Action. If the Response Action is set to Alert, the alerts are raised in the Attack Log but the file download is not blocked. If the Response Action is set to Alert and Block, the alerts are raised in the Attack Log, and the file download is blocked.

Response actions are not persisted after Sensor reboot as this is part of the policy now. Only GTI Server, Sensitivity level and time out are persisted after reboot.

The alerts raised in Attack Log display the MD5 hash value of the malware, and the URL from where the malware was downloaded.

You can enable three types of detection in the Manager: File Reputation only, Custom, or both.

Custom fingerprint detection takes precedence over File Reputation detection type.

Also note that IPS attack detection takes precedence over User-defined fingerprint detection in the Sensor. When the traffic contains both IPS attack and malware content detected by Network Security Platform-File Reputation integration, the attack is detected as IPS attack, and not as a malware attack. The blocking of the attack takes place as per IPS attack definition.

🗹 Note

The DNS Server IP addresses, custom Response Action and Detection type settings are persisted even after a Sensor reboot. But the entries are cleared if you execute a resetconfig command on the Sensor.

Note that malicious files are detected and responded with the Network Security Platform-File Reputation integration for traffic types, such as fragmented, segmented, or tunneled traffic. Files are also detected with different HTTP versions (for example 1.0, 1.1, etc) of the browser.

File Reputation in different Sensor modes

In this integration, the Sensor provides malware detection in all the operating modes — inline, tap, and SPAN. In the inline mode, malware is detected in both Inline fail-open and Inline fail-closed modes.

Network Security Platform-File Reputation integration in a Manager Disaster Recovery (MDR) setup

Once the MDR is created, and all the Sensors have established trust with both Primary and Secondary Managers, same malware configuration is available in Secondary (Standby) Manager.

When there is a switchover and the Secondary Manager becomes active, it will continue the File Reputation scanning function as before. In case the Primary Manager switches back to the active mode, the changes made in the Secondary are retrieved and updated accordingly in the Primary Manager.

The Sensor File Reputation Alerts are sent to both Primary and Secondary Managers.

File Reputation integration configurations in the Manager

Following sections explain how you can set the Network Security Platform-File Reputation integration configurations in the Manager.

GTI fingerprints

The Sensor creates a fingerprint (MD5 hash value) of the file that is seen as potentially malicious, embeds the fingerprint in a standard HTTPS request, and sends it to GTI cloud server. The cloud server compares the fingerprint against the threat database maintained by McAfee Labs. If the fingerprint is identified as a known malware, the cloud server notifies the Sensor and it enforces a response action for the malware. Note that the details of the malware can be viewed from the Attack Log.

Manage allow and block lists

You can add the MD5 hash values of files to the block list or allow list, and import the resulting fingerprints into Network Security Platform. The Sensor scans the specified file types for potential malware and compares it with blocked and allowed hashes. If a blocked match is found, it enforces a response action.

Add hash values to the allow list

You can add a list of allowed fingerprints (MD5 hashes) for files you want to be exempted from malware analysis when found in HTTP or SMTP downloads.

Task

Select Policy → <Admin Domain Name> → Intrusion Prevention → Exceptions → File Hashes.
 You can view the current list of allowed hashes on the Allowed Hashes tab of the File Hashes page.

Allowed Hashes

/My Co	ompany > Intrusion Prevention > Exceptions > File H	ashes					Ø
File H	ashes						
0							
Block	ed Hashes Allowed Hashes						
	File Hach 🛧	File Name					
1	0386ff59d0f5c1cde453a3780353069f	telephon.cpl	Jul 24 12:01:39 2019	Administrator	desc		
2	0a614929df1ea09534403ab02a7e4b23	Python_Basics_and_M	Jul 24 12:01:39 2019	Administrator	desc		
з	152e5cedb1eb8c69ddd578b8548c611e	Helpdesk_Tax_Filing_F	Jul 24 12:01:39 2019	Administrator	desc		
4	1bd0b835db0f2535b10417df5048198c	ArtemisTest.zip	Jul 24 12:01:39 2019	Administrator	desc		
5	1bf588ba89e79829ad5d095e1b149839	sis.sys	Jul 24 12:01:39 2019	Administrator	desc		
6	2a480eff5df8c5a757add35aeadac4d8	NSAT_PPT_Template_v	Jul 24 12:01:39 2019	Administrator	desc		
7	300a2c5cbddb9131d1818dbc4a45381d	Artemis_and_CustomF	Jul 24 12:01:39 2019	Administrator	desc		
8	31e6002b21c489fbbdb0f88ddc02603e	hex-editor-setup.exe	Jul 24 12:01:39 2019	Administrator	desc		
9	35426e5fb884ca8a6b02135aa4c81280	ssText3d.scr	Jul 24 12:01:39 2019	Administrator	desc		
10	46bb30fbcf5628e45f1d3cd9d816344a	Malware_Files.rar	Jul 24 12:01:39 2019	Administrator	desc		
11	493ce956e5ed92003d0ce175ce2e4a23	bootstrap.jar	Jul 24 12:01:39 2019	Administrator	desc		
12	5ccb595383d3fc1864b604106893590b	sysmon.ocx	Jul 24 12:01:39 2019	Administrator	desc		
13	61e02cc3184b63fafe0b83eac8b3b8ef	winspool.drv	Jul 24 12:01:39 2019	Administrator	desc		
14	7fa5ca36b613a000f3a37e6b5170a195	d2d1.dll	Jul 24 12:01:39 2019	Administrator	desc		
15	c22c8e931f91a3f5a8eb86615d187d4d	AdvancedMalwareDete	Jul 24 12:01:39 2019	Administrator	desc		
16	ca780590a0070dd582dfffb679e3b2ed	NSAT_Infrastructure_v	Jul 24 12:01:39 2019	Administrator	desc		
17	f34302b45a616e934729f3b8189421b7	Artemis_and_CustomF	Jul 24 12:01:39 2019	Administrator	desc		
18	f551c4bc9c7f19af8934522dba37e812	tree.com	Jul 24 12:01:39 2019	Administrator	desc		
+ -	- Save as CSV Other Actions ▼					:	18 file hashes

The following table describes the details displayed on the **Allowed Hashes** tab.

Format	Description
File Hash	Specifies the file hash. The File Hash will be in the MD5 format.
File Name	Specifies the name of the file along with the file extension
Last Updated	 Displays the following: Time: Specifies the time stamp of the imported allow list By: Specifies the user who imported the allow list
Comment	Any comments about the list

- 2. Click **Other Actions** \rightarrow **Import** to import a file containing the hash values.
- 3. Click **Browse** to locate an XML or CSV file that contains the list of hashes you want to import.
- 4. Click Import.

The file to be imported should be in the following CSV format.

<Name of the file with extension (like .exe, .com)>,<File size>,<Hash type>,<File hash>,<Description>

🗹 Note

The file hash should be in the MD5 format.

Example file format: Application.exe, 1024000, MD5, 30a4edd18db6dd6aaa20e3da93c5f425, textual description. Also note that if you are importing multiple files, each file has to be in a new line.

The following is a sample for a CSV file with multiple file hashes.

```
1 ,2,MD5,54c652555dd2dab3c87e1b92c8302f1e
2 optional filename,1,MD5,7331df41dfb25c55271c1f111efc224e
3 ,1,MD5,96a65cad713f529c13d74802c89d7188,optional comment
```

The following table describes the details of the files to be imported in the CSV or XML format.

Format	Description
<name file="" of="" the="" with<br="">extension (like .exe, .com)></name>	Specifies the name of the file to be imported along with the file extension. This is an optional value.
<file size=""></file>	Specifies the size of the file to be imported. The file size should be a valid integer.
	Note: File size value is mandatory. It is used by the Sensor as a secondary matching criterion when the same hash has been added to both the block list and allow list.
	Note: If the file size is unknown, you can add a placeholder value like 1 to the CSV file as this value is mandatory.
<hash type=""></hash>	Specifies the format of the hash. The supported file hash type is the MD5 format.
<file hash=""></file>	Specifies the hash for the file to be imported
<description></description>	Specifies the description of the file to be imported. This is an optional value.

2 | Integration with McAfee Global Threat Intelligence

🗹 Note

If you are importing using CSV, you can import the same file hash to both allow list and block list.

5. To add a single file hash to the allowed hashes, click +.

Click Save after entering the values in File Hash, File Name, and Comment. The Comment field is optional.

🗹 Note

The **File Hash** should be a 32 digit hexadecimal value.

Add a single allow list file hash value

/My Co	ompany > Intrusion Preventi	on > Exceptions > File Hashes						Ø
File H								
•								
Blocked I	Hashes Allowed Hashes							
	File Hash 🕇	File Name				File Upeb.	of5e1ede45252780255	posof
						rile nasii.	0150100245533780555	50091
1	0386ff59d0f5c1cde4	telephon.cpl	Jul 24 12:01:39 2019	Administrator	desc	File Name:	Advanced.xml	
2	0a614929df1ea0953	Python_Basics_and_M	Jul 24 12:01:39 2019	Administrator	desc	Comment:	Advanced.xml	
з	152e5cedb1eb8c69d	Helpdesk_Tax_Filing_F	Jul 24 12:01:39 2019	Administrator	desc			
4	1bd0b835db0f2535b	ArtemisTest.zip	Jul 24 12:01:39 2019	Administrator	desc			
	1bf588ba89e79829a	sis.sys	Jul 24 12:01:39 2019	Administrator	desc	Last Updated:		
6	2a480eff5df8c5a757	NSAT_PPT_Template_v	Jul 24 12:01:39 2019	Administrator	desc			
7	300a2c5cbddb9131d	Artemis_and_CustomF	Jul 24 12:01:39 2019	Administrator	desc			
8	31e6002b21c489fbb	hex-editor-setup.exe	Jul 24 12:01:39 2019	Administrator	desc			
9	35426e5fb884ca8a6	ssText3d.scr	Jul 24 12:01:39 2019	Administrator	desc			
10	46bb30fbcf5628e45f	Malware_Files.rar	Jul 24 12:01:39 2019	Administrator	desc			
11	493ce956e5ed9200	bootstrap.jar	Jul 24 12:01:39 2019	Administrator	desc			
12	5ccb595383d3fc186	sysmon.ocx	Jul 24 12:01:39 2019	Administrator	desc			
13	61e02cc3184b63fafe	winspool.drv	Jul 24 12:01:39 2019	Administrator	desc			
	7fa5ca36b613a000f	d2d1.dll	Jul 24 12:01:39 2019	Administrator	desc			
	c22c8e931f91a3f5a8	AdvancedMalwareDete	Jul 24 12:01:39 2019	Administrator	desc			
16	ca780590a0070dd5	NSAT_Infrastructure_v	Jul 24 12:01:39 2019	Administrator	desc			
17	f34302b45a616e934	Artemis_and_CustomF	Jul 24 12:01:39 2019	Administrator	desc			
	f551c4bc9c7f19af89	tree.com	Jul 24 12:01:39 2019	Administrator	desc			
_								
		Other Actions 👻			18 file hashe			Save

- 6. To export the allowed hashes from the Manager to a local system, click **Other Actions** \rightarrow **Export All**.
- 7. To delete specific entries from the allow list, select them by holding the **Shift** or **Ctrl** key and clicking on the required rows.

Then click

The deleted hashes are now neither in the allow list nor in the block list.

- 8. To remove all the entries, select **Other Actions** \rightarrow **Delete All**.
- 9. To move specific entries to the block list, select the entries and then select **Other Actions** \rightarrow **Move to Block List**.
 - A manual signature set push is not required each time the allow list or the block list is updated. The Manager updates the Sensor dynamically with the modified entries in the allow list or block list, at an interval of 5 minutes. These updates occur in bulk (the complete list of entries) or increments (added/deleted entries). To view the status of these updates, use the show ab stats command. For more information, see the *CLI commands* section in the *McAfee Network Security Platform Product Guide*.
 - You can configure a maximum of 99,000 entries (allowed and blocked).

Add hash values to the block list

You can add MD5 hash values of files that you want to be treated as malicious when found in HTTP and SMTP downloads. If a file's hash matches a hash value in the block list, the Sensor treats the file as malicious of *very high* severity.

Task

Select Policy → <Admin Domain Name> → Intrusion Prevention → Exceptions → File Hashes.
 On the Blocked Hashes tab, you can add the hash values to be blocked, manage the file types to be checked for the blocked hashes, and view the maximum file size scanned.

/My Col	mpany > Intrusion Prevention > Exceptions > File Hashes						0
File Ha	ashes						
0							
Blocke	ed Hashes Allowed Hashes						
		File Ndfile					
1	0386ff59d0f5c1cde453a3780353069f	telephon.cpl	Oct 27 15:51:49 2020	Administrator	desc		
2	075c8160789eb0829488a4fc9b59ed6c	collectmail_notwo0a.pdf	Oct 27 15:51:49 2020	Administrator	description		
3	0a614929df1ea09534403ab02a7e4b23	Python_Basics_and_MySQL	Oct 27 15:51:49 2020	Administrator	desc		
4	0aac13cdef3602bab8544fe51df2641d	IEXPLORE.EXE	Oct 27 15:52:27 2020	Administrator	Added based o	n user request	
5	0b237b533bd87632c9ccac9b640147c4	notepad.ex	Oct 27 15:51:49 2020	Administrator	desc		
6	152e5cedb1eb8c69ddd578b8548c611e	Helpdesk_Tax_Filing_Form	Oct 27 15:51:49 2020	Administrator	desc		
+ -	─ Save as CSV Other Actions 🔻						43 file hashes

Blocked hashes

The following table describes the details displayed on the **Blocked Hashes** tab.

Format	Description
File Hash	Specifies the file hash. The File Hash will be in the MD5 format.
File Name	Specifies the name of the file along with the file extension
Last Updated	 Displays the following: Time: Specifies the time stamp of the imported block list file hash By: Specifies the user who imported the block list file hash
Format	Description
---------	-----------------------------
Comment	Any comments about the list

- 2. Select **Other Actions** \rightarrow **Import** to import a file containing the hash values.
- 3. Click Browse to locate the CSV file that contains the list of hashes you want to import.
- 4. Click Import.

The file to be imported should be in the following CSV format.

<Name of the file with extension (like .exe, .com)>,<File size>,<Hash type>,<File hash>,<Description>

Example file format: Application.exe, 1024000, MD5, 30a4edd18db6dd6aaa20e3da93c5f425, textual description. Also note that if you are importing multiple files, each file has to be in a new line.

The following is a sample for a CSV file with multiple file hashes.

1 ,2,MD5,54c652555dd2dab3c87e1b92c8302f1e
2 optional filename,1,MD5,7331df41dfb25c55271c1f111efc224e
3 ,1,MD5,96a65cad713f529c13d74802c89d7188,optional comment

The following table describes the details of the files to be imported in the CSV or XML format.

Format	Description
<name file="" of="" the="" with<br="">extension (like .exe, .com)></name>	Specifies the name of the file to be imported, along with the file extension. This is an optional value.
<file size=""></file>	Specifies the size of the file to be imported. The file size should be a valid integer.
	Note: File size value is mandatory. It is used by the Sensor as a secondary matching criterion when the same hash has been added to both the block list and allow list.

Format	Description			
	Note: If the file size is unknown, you can add a placeholder value like 1 to the CSV file as this value is mandatory.			
<hash type=""></hash>	Specifies the format of the hash. The supported file hash type is the MD5 format.			
<file hash=""></file>	Specifies the hash for the file to be imported			
<description></description>	Specifies the description of the file to be imported. This is an optional value.			

🗹 Note

If you are importing using CSV, you can import the same file hash to both allow list and block list.

5. To add a single file hash to the blocked hashes, click



Click Save after entering the values in File Hash, File Name, and Comment. The Comment field is optional.

Note

The **File Hash** should be a 32 digit hexadecimal value.

Add a single block list file hash value

/My Cor	npany > Intrusion Prevention >	Exceptions > File Hashes							0
File Ha	File Hashes								
•	0								
Blocke	d Hashes Allowed Hashes								
							Hash Details		
									_
	File Hash 🕇						File Hash:	0386ff59d0f5c1cde453a37803	
1	0386ff59d0f5c1cde453	telephon.cpl	Oct 27 15:51:49 2020	Administrator	desc	^	File Name:	telephon.cpl	
2	075c8160789eb08294	collectmail_notwo0a.pdf	Oct 27 15:51:49 2020	Administrator	description		Comment:	desc	
3	0a614929df1ea09534	Python_Basics_and_MySQL	Oct 27 15:51:49 2020	Administrator	desc				
4	0aac13cdef3602bab85	IEXPLORE.EXE	Oct 27 15:52:27 2020	Administrator	Added based on user request				
5	0b237b533bd87632c9	notepad.ex	Oct 27 15:51:49 2020	Administrator	desc		Last Updated:	Oct 27 15:51:49 2020	
6	152e5cedb1eb8c69dd	Helpdesk_Tax_Filing_Form	Oct 27 15:51:49 2020	Administrator	desc				
7	1bb69e3f010c80ad28	applwizard.jar	Oct 27 15:51:49 2020	Administrator	desc				
8	1bd0b835db0f2535b1	ArtemisTest.zip	Oct 27 15:51:49 2020	Administrator	desc				
9	1bf588ba89e79829ad	sis.sys	Oct 27 15:51:49 2020	Administrator	desc				
10	2a480eff5df8c5a757a	NSAT_PPT_Template_v1.pptx	Oct 27 15:51:49 2020	Administrator	desc				
11	2bfa250015e7c03fa5a	sihclient.exe	Oct 27 15:52:27 2020	Administrator	Added based on user request				
12	300a2c5cbddb9131d1	Artemis_and_CustomFP_Te	Oct 27 15:51:49 2020	Administrator	desc				
13	31e6002b21c489fbbd	hex-editor-setup.exe	Oct 27 15:51:49 2020	Administrator	desc	-			
+ -	- Save as CSV C	Other Actions 👻				shes		Sav	e

- 6. To export the blocked hashes from the Manager to a local system, click **Other Actions** \rightarrow **Export All**.
- 7. To delete specific entries from the block list, select them by holding the **Shift** or **Ctrl** key and clicking on the required rows.

Then click

The deleted hashes are now neither in the allow list nor in the block list.

- 8. To remove all the entries, select **Other Actions** \rightarrow **Delete All**.
- 9. To move specific entries to the allow list, select the entries and then select **Other Actions** \rightarrow **Move to Allow List**.

• A manual signature set push is not required each time the allow list or the block list is updated. The Manager updates the Sensor dynamically with the modified entries in the allow list or block list, at an interval of 5 minutes. These updates occur in bulk (the complete list of entries) or increments (added/deleted entries). To view the status of these updates, use the show ab stats command. For more information, see the *CLI commands* section in the *McAfee Network Security Platform Product Guide*.

• You can configure a maximum of 99,000 entries (allowed and blocked).

Configure File Reputation for Advanced Malware Detection

While creating an Advanced Malware policy for your network, you can set **Allow and Block Lists** and **GTI File Reputation** as the malware engines to scan the traffic across your network. For more information, see *McAfee Network Security Platform Product Guide*.

Add an Advanced Malware policy

You configure the anti-malware options in an Advanced Malware policy and then assign it to the required Sensor monitoring resources, such as ports, interfaces, and subinterfaces. You must do a configuration and signature set update for any changes in the policy to take effect.

Task

- 1. Select **Policy** and then select the required admin domain from the **Domain** drop-down list.
- 2. Select Intrusion Prevention \rightarrow Policy Types \rightarrow Advanced Malware.
- 3. Click

The Advanced Malware page for a new policy opens.

Update the properties of the Advanced Malware policy

Properties				
Name:	Default Malware Policy	Traffic to Inspect —		
Description:		HTTP:	🖌 Download 🛈	Upload 🕕
Owner:	/My Company	FTP SMTP		
Visible to Child Admin Domains?	Z			

4. Update the following properties.

Field name	Description
Name	Name of the policy
Description	Description of the policy
Owner	Name of the admin domain to which the policy belongs
Visible to Child Admin Domains?	Specifies whether the policy is applicable to all child admin domains
Traffic to Inspect	 Protocols over which advanced malware scanning is performed. The supported protocols are HTTP, FTP, and SMTP. Image: Note: The HTTP Download option allows you to scan HTTP download/response traffic for presence of malware. This option is enabled by default. The HTTP Upload option allows you to scan HTTP upload (POST and PUT) requests for presence of malware. This option is disabled by default. You need to select the Upload checkbox to enable it. For more information on scanning HTTP POST and PUT requests, refer to the Malware inspection on HTTP Upload requests section in McAfee Network Security Platform Product Guide. Image: Note: FTP malware detection overrides the accelerate-ftp feature even if it is enabled. For more information on the accelerate-ftp command, refer to the CLI commands section in McAfee Network Security Platform Product Guide.

5. Update the File Scanning Options.

ц.,												
File Scanning Options												
0												
					Gateway Anti-Malware					Send TCP Reset		
Executables	5120	V			V	7		High	High	High	Disabled	Disabled
I MS Office Files	1024	•		2		2		High	High	High	Disabled	Disabled
PDF Files	1024							High	High	High	Disabled	Disabled
Compressed Files	5120					7		High	High	High	Disabled	Disabled
i Android Applica	2048					7	V	High	High	High	Disabled	Disabled
i Java Archives	2048					1		High	High	High	Disabled	Disabled
• Flash Files	2048	V	V		7			High	High	High	Disabled	Disabled
										mpt for assignme	after save Sav	/e Cancel

🗹 Note

Name resolution must be enabled on devices which will be using the GTI File Reputation malware engine.

File scanning options

Field name	Description
File Type	The file types to be scanned. For information about the supported file types, refer to the table <i>Advanced malware file extension support</i> below.
Maximum File Size (KB) Scanned	The maximum size currently supported for the corresponding file type. Files that exceed the specified size are not analyzed for malware by any of the engines, including the block and allow lists. The default values are displayed in the Default Malware Policy as well as when you create a policy. The default values are the optimum sizes recommended by McAfee Labs based on their research on malware.
	You can set the maximum file size value up to (25*1024) KB/25 MB for all file types. However, the NSP Analysis engine and McAfee Cloud engine have a file-size limit. The limits for each Sensor model are as follows: • NS-series Sensors - (50*1024) KB/50 MB • Virtual IPS Sensors- (5*1024) KB/5 MB

Field name	Description
	Note: McAfee recommends that for any file type, you do not set a value more than (5*1024) KB/5 MB as the maximum file size as this might affect the Sensor's performance.
Malware Engines	 The Malware engines to scan the selected file type. If you select Gateway Anti-Malware for a File Type, you must either use an NS-series Sensor running on Sensor software version 9.1 or above, or NTBA. For Advanced Threat Defense to work, you must integrate the corresponding Sensors with McAfee Advanced Threat Defense. See the chapter Integration with McAfee Advanced Threat Defense for more
	information.
Action	Specifies the type of response to be made for the attack. The types of responses are:
Inresnoids	 Alert — Alerts are raised in Attack Log. Block — This action blocks packets for detected malware, thus preventing the malicious file from reaching the host.
	 The first step towards prevention is typically to block attacks that have a high severity level. When you know which attacks you want to block, you can configure your policy to perform the drop attack packets response for those attacks. If not configured in the policy, the Attack Log allows you to update the policy to block traffic. Send TCP Reset— Disconnects a TCP connection at the source, destination, or both ends of the transmission, thus preventing the malicious file from reaching the host.
	Note: This response may not work effectively with SPAN and tap deployments.
	• Add to Block List — If any of the engines report the submitted file to be malicious, the Manager adds the file's MD5 hash to the block list in its database. To be added to this list, the file's severity must be the same or more than what you specify in this field. For example, if you specify <i>high</i> as the criteria, then files of severity <i>high</i> and <i>very high</i> are added to the block list. Within the next 5 minutes, the Manager adds this file to the local block list of all the Sensors that it manages.
	Note: The TIE/GTI File Reputation engine does not support Add to Block List response action. You can manually add the desired malware file's MD5 hash to the block list from the Attack Log page.

Field name	Description
	• Save File — One of the response actions specified is the ability to archive the file in a file store based on the Advanced Malware policy. The files that are selected based on this configuration are forwarded to Manager.
	 For files greater than 5 MB, only the first 5 MB is available as the saved file. To prevent the Manager's disk from getting frequently filled up, use the Save File feature sparingly. The Sensor's simultaneous file scan capacity is reduced if the Save File option is enabled. See the table in this section for the details.

Advanced malware file extension support

File Type	HTTP Upload and Download	SMTP	FTP
Executables	acm	acm	acm
	.acm	.acm	.acm
	.ax	.ax	.ax
	.com	.com	.com
	.cpl	.cpl	.cpl
	.dll	.dll	.dll
	.drv	.drv	.drv
	.exe	.exe	.exe
	.fon	.fon	.fon
	.ocx	.ocx	.ocx
	.olb	.olb	.olb
	.pif	.pif	.pif
	.qts	.qts	.qts
	.qtx	.qtx	.qtx
	.scr	.scr	.scr
	.sys	.sys	.sys
	.vbx	.vbx	.vbx
	.vxd	.vxd	.vxd

File Type	HTTP Upload and Download	SMTP	FTP
MS Office Files	.doc	.doc	.doc
	.docx	.docx	.docx
	.ppt	.ppt	.ppt
	.pptx	.pptx	.pptx
	.rtf	.rtf	
	.xls	.xls	.xls
	.xlsx	.xlsx	.xlsx
PDF Files	.fdf	.fdf	.fdf
	.pdf	.pdf	.pdf
	.xdp	.xdp	
Compressed Files	.7z	.7z	
	.pkzip	.pkzip	.pkzip
	.rar	.rar	.rar
	.zip	.zip	.zip
Android Application Packages	.apk		.apk
Java Archive	.jar	.jar	.jar
Flash Files	.swf	.swf	

🗹 Note

McAfee might enhance the supported file types over time. The file types are subject to change with new signature sets. The Sensor cannot extract .zip, .jar, .apk and office open xml files if correct file extension is not present, as they share the same magic number 50 4B 03 04(PK).

Each file type is scanned by a Malware engine. Multiple malware engines can be selected to scan various file types. The Malware engines return a confidence level. Based on the confidence level, the following action thresholds can be set. The confidence levels supported are: Very low, low, medium, high, very high.

The Malware Engines supported per file type are:

File Type	TIE/GTI File Reputation	Allow and Block Lists	NSP Analysis	Gateway Anti- Malware	Advanced Threat Defense	McAfee Cloud
Executables	\checkmark	~		\checkmark	~	
MS Office Files	\checkmark	~	~	\checkmark	\checkmark	
PDF Files	\checkmark	~	~	\checkmark	~	
Compressed Files	✓	~		\checkmark	✓	
Android Application Package	~	~			~	~
Java Archive	~	~		\checkmark	~	
Flash Files	\checkmark	~	~	~	\checkmark	

The maximum simultaneous file scan capacity per Sensor model is as follows.

Sensor	Maximum simultaneous file scan capacity with file save	Maximum simultaneous file scan capacity without file save
NS9500 stack - 100 Gbps throughput	1,000	4,096
NS9500 stack - 60 Gbps throughput	1,000	2,048
NS9500 stack - 40 Gbps throughput	1,000	2,048
NS9500 standalone - 30 Gbps throughput	1,000	1,024
NS9500 standalone - 20 Gbps throughput	1,000	1,024

Sensor	Maximum simultaneous file scan capacity with file save	Maximum simultaneous file scan capacity without file save
NS9500 standalone - 10 Gbps throughput	1,000	1,024
NS9300, NS9200, NS9100	1,000	1,024
NS7500 - 7.5 Gbps throughput	1,000	1,024
NS7500 - 5 Gbps throughput	1,000	1,024
NS7500 - 3 Gbps throughput	1,000	1,024
NS7350, NS7250, NS7150	1,000	1,024
NS7300, NS7200, NS7100	1,000	1,024
NS5200, NS5100	32	1,024
NS3500	16	255
NS3200, NS3100	16	255
IPS-VM600	32	1,024

6. To assign the Advanced Malware Policy to the available interfaces and direction (Inbound, Outbound), select **Prompt for assignment after save**.

Assign Interfaces

Assignments				
Search available interfaces				
Available Interfaces † /My Company/PK_NS5100_17_209/G2/1-G2 /My Company/PK_NS5100_17_209/G2/1-G2 /My Company/PK_NS5100_17_209/G2/3-G2 /My Company/PK_NS5100_17_209/G2/5-G2 /My Company/PK_NS5100_17_209/G2/5-G2 /My Company/PK_NS5100_17_209/G2/7-G2 /My Company/PK_NS5100_17_209/G2/7-G2 /My Company/PK_NS5100_17_213/G0/1-G0 /My Company/PK_NS5100_17_213/G1/1-G1	Current Policy	Selected Interfaces (policy group) †		
Objects:72		Objects:0		
				Reset
			Save	Cancel

- 7. Select the required interface from the **Available Interfaces** column and add it to the **Selected Interfaces (Policy Group)** column.
- 8. Click Save.

You are directed to the new policy window.

View File Reputation details in Attack Log

You can view the details of the malware in the Attack Log. Double-click on the malware alert detected by Global Threat Intelligence File Reputation. The alert details are displayed with details, such as MD5 hash value of the malware, URL from where the malware was downloaded, and detection mechanism.

File Reputation details in Attack Log



How to view malware statistics per Sensor

You can view the malware statistics per Sensor by doing the following steps.

Task

- 1. Navigate to **Devices** \rightarrow **<Admin Domain Name>** \rightarrow **Devices** \rightarrow **<Device Name>** \rightarrow **Troubleshooting** \rightarrow **Traffic Statistics**.
- Click the Advanced Malware Analysis tab.
 You can view the traffic statistics for malware statistics either By Malware Engine or By File Type.

Malware traffic statistics

/Му	Company > NS7350_83 > Troubleshooting >	Traffic Stationes							Ø			
Traffic Statistics												
0												
Tra	Traffic Received / Sent Rows Dropped Packets Advanced Malware Analysis Advanced Callback Detection SSL Decryption											
0	By Malware Engine								C			
							Gateway Anti- Malware	Advanced Threat Defense	McAfee Cloud			
1	Files Submitted to Engine								📤			
2	Files Ignored by Engine											
3	Files Processed by Engine			ο (0			
∢ 4	ATD Files Drop Under Load								·			
5	ATD Static Analysis											
6	ATD Dynamic Analysis											
7	ATD Cache References											
8	Clean Files			0 (0			
9	Very High Malware Confidence Mat			0 (0			
10	High Malware Confidence Matches			0 (0			
11	Medium Malware Confidence Matc			0 (0			
12	Low Malware Confidence Matches			0 (0			
13	Very Low Malware Confidence Mat			0 (0			
14	Unknown Malware Confidence Mat		9	0 () 0	0	0	0	0 🖵			
									•			
S	ave as CSV								Reset Counters			

3. Click the refresh icon to view the updated malware statistics.

To view the number of malware alerts detected by Network Security Platform-File Reputation integration, use the status command. For more information on these commands, see the *CLI commands* section in the *McAfee Network Security Platform Product Guide*.

CLI commands for Network Security Platform - File Reputation integration

The Sensor CLI commands related to Network Security Platform-File Reputation integration are the following:

show gti config: Displays the GTI server configuration information

filerep gti md5: Displays the file reputation query response for the md5 hash from the GTI server configured in the device. This command is used to test connection to the GTI server and troubleshooting.

For more information on these command, see the CLI commands section in the McAfee Network Security Platform Product Guide.

Network Security Platform-File Reputation integration is supported on M-series, NS-series, and Virtual IPS Sensors.

Limitations

When the Sensor is in the Layer 2 mode (L2 mode), there is no detection of malware content as per the Network Security Platform-GTI File Reputation integration.

Troubleshooting

Clearing File Reputation counters

For clearing the File Reputation counters, use the clrstat command.

For more information on CLI commands, see the CLI commands section in the McAfee Network Security Platform Product Guide.

Disable HTTP Response Scanning to improve performance of File Reputation

In Network Security Platform 9.1 and above HTTP Response Scanning is not required for File Reputation to work. In fact, to improve the performance of File Reputation, disable HTTP Response Scanning on the corresponding port or port-pair.

Network Security Platform-GTI integration for URL Reputation

Network Security Platform integrates with GTI server to provide reputation scores for the URLs present in the header fields of the HTTP and HTTPS traffic inspected by the Sensor. The GTI server hosted in the cloud provides URL reputation information for millions of URLs and, by using this service, the Network Security Platform provides real-time protection when browsing websites.

🗹 Note

You can integrate Network Security Platform with McAfee GTI cloud server or a private GTI cloud server.

The URL reputation feature provides the following benefits:

- Real-time protection against visiting malicious URLs
- Increases end-user awareness of malicious URLs

How Network Security Platform-GTI Integration for URL Reputation works

The URL reputation, if enabled, checks the reputation of the URLs in the HTTP and HTTPS header fields present in the layer 7 of the TCP/IP stack.

The Sensor constructs the URLs from the headers of HTTP and HTTPS request and sends them to the cloud based GTI server for a reputation lookup. The GTI server processes the URL reputation request and returns a reputation score to the Sensor. The reputation score indicates the malicious score of the URL. An alert is generated in the Manager if the reputation score exceeds the configured threshold value.

The Sensor constructs the URLs from the following fields:

- Fields in the HTTP header:
 - HTTP_URI
 - HTTP_HOST

- HTTP_Referrer
- Fields in the SSL header:
 - CN field in the SSL certificate. Only first certificate in certificate chain will be scanned.
 - Host-Name field in the SNI extension of the "Client Hello" SSL handshake message

The following image shows the communication between the Sensor, the Manager, and the GTI server for looking up the URL reputation score.



A single HTTP(S) request can generate more than one URL reputation lookup in certain scenarios. For example, consider the case where the HTTP request message has the HTTP_REFERER header. In this case, the Network Security Platform performs 2 lookups, one for the HTTP_HOST / HTTP_URI values and another for the HTTP_REFERER value. This provides reputation scores for both the website being visited as well the referrer to the website.

🗹 Note

In case of a persistent HTTP traffic, there will be multiple HTTP requests going over the same HTTP connection. The Network Security Platform performs URL reputation lookup for each HTTP request.

The Sensor sends the constructed URLs to the GTI server for lookup but does not hold the packet flow. If the response is received from the GTI server while the flow is active, and the reputation score is equal to or above the configured threshold, an alert is generated. Based on the response action configured for the attack in the Manager, the URL is either blocked or an alert is sent to the Manager.

If blocking is configured for the attack, subsequent packets in the flow are dropped. If the response from the GTI server is received after the flow has terminated, no action is taken on the response. Flow is maintained to the Sensor till it reaches the **2MSL** timeout after the closure of the TCP connection through the TCP_FIN handshake.

2 | Integration with McAfee Global Threat Intelligence

🗹 Note

The **2MSL** timeout setting is used in various functions of the Manager. McAfee recommends you to not change the value of the setting as it might impact the behavior of other functions in the Manager.

High-level flow of the URL reputation check

The following flowchart describes the high-level flow of the URL reputation check:



🗹 Note

Network Security Platform can have a maximum number of outstanding URL requests to GTI which is equal to 20% of the flow capacity of the Sensor model.

Configuration of URL Reputation

Before you begin

Before configuring the URL reputation in the Manager, perform the following steps:

- If you are using GTI public cloud, enable Telemetry and Domain Name Resolution (DNS).
 - For information on enabling Telemetry, see the *Configure Telemetry* section in the *McAfee Network Security Platform Integration Guide*.
 - To enable DNS in the Manager, perform the following steps:
 - In the Manager, select the **Devices** tab.
 - * Go to, <Domain Name> \rightarrow Global \rightarrow Common Device Settings \rightarrow Name Resolution.
 - Select the Enable Name Resolution? checkbox.
 - Enter the details of the DNS servers.
 - Click **Test Connection** to verify the connection.

• Click **Save** to save the changes.

🗹 Note

If you are using GTI private cloud, configuring Telemetry and DNS is not mandatory.

You should have the name resolution configuration that allows the Sensor to resolve the hostname of the server that hosts the URL database.

Perform the following steps to enable URL reputation in the Manager:

Task

- 1. In the Manager, select the **Policy** tab.
- 2. Go to, **<Domain Name>** \rightarrow **Intrusion Prevention** \rightarrow **Policy Types** \rightarrow **Inspection Options**.
- 3. Select the required policy and clone it.
- 4. Double-click the cloned policy.
- 5. Select the GTI Reputation Services tab. The Endpoint and URL tabs are displayed.
- 6. Select the **URL** tab.

/My Company > Intrusion Prevention > Policy Types > Inspection Options											
Properties Inspection Options											
Traffic Inspection Advanced Callback Detection	GTI Reputation Services	Web Server - Heuristic Analysis	Web Server - Denial-of-Service Prevention								
Endpoint URL											
0											
URL Reputation Analysis:	Disabled										
Client Inspection		Prompt for ass	ignment after save Save Cancel								

- 7. Select a value in the **URL Reputation Analysis** field. The value can be any one of the following:
 - **Disabled** Disable the URL reputation feature
 - Inbound and Outbound Enable URL reputation for both inbound and outbound traffic
 - Inbound Only Enable URL reputation only for inbound traffic
 - Outbound Only Enable URL reputation only for outbound traffic

🗹 Note

By default, URL Reputation is disabled for a policy.

🗹 Note

Make sure to enable Layer 7 Data Collection in Traffic Inspection tab when URL Reputation Analysis is enabled.

- 8. Select the Minimum URL Risk. The value can be any one of the following:
 - Medium
 - High

/My Company > Intrusion Prevention > Policy Types > Inspection Options ?										
Properties Inspection Options										
Traffic Inspection Advanced Callback Detection	GTI Reputation Services	Web Server - Heuristic Analysis	Web Server - Denial-of-	Service Prevention						
Endpoint URL										
0										
URL Reputation Analysis:	Inbound and Outbo	und 💌								
Minimum URL Risk:	High	• 0								
			►							
Client Inspection		Prompt for as:	signment after save Sa	ave Cancel						

🗹 Note

• The default selection is **High**.

• If the selection is **Medium**, alerts are generated for both High-risk and Medium-risk URLs. If the selection is **High**, alerts are generated only High-risk URLs.

- 9. Click Save.
- 10. Publish the changes to the Sensor. Select **Devices** \rightarrow **<Domain Name>** \rightarrow **Devices** \rightarrow **<Device>** \rightarrow **Deploy Pending Changes** and click **Deploy**.
 - 🗹 Note

For configuring various Sensor response actions, see McAfee Network Security Platform Product Guide.

Configure URL Reputation for an interface

You can enable URL Reputation at the interface level of a Sensor. At the interface level, you can inherit the settings from the admin domain or customize it for the interface.

Task

- 1. In the Manager, select Policy \rightarrow <Admin Domain Name> \rightarrow Intrusion Prevention \rightarrow Policy Manager.
- Double-click the interface for which you want to configure URL Reputation.
 A <Device Name/Interface> panel appears for the selected interface.
- 3. In the Inspection Options section of the <Device Name/Interface> panel, select a policy from the Policy drop-down list.

To create a new policy, click the + icon or double click on the policy to edit an already assigned policy.

4. Click the + icon.

The **Properties** tab for a new policy appears.

- Enter the Name and Description, select the Visibility, and click Next. The page shifts to open the Inspection Options tab.
- 6. Click the GTI Reputation Services tab.
- 7. Click the **URL** tab.

/NSP_Doc_03 > Intrusion Prevention > Policy Manager										
Properties Inspection Options										
Traffic Inspection Advanced Caliback Detection GTI Reputation Services Web Server - Heuristic Analysis Web Server - Denial of Service Prevention										
Endpoint URL										
0										
URL Reputation Analysis:	Disabled Disabled Inbound only Outbound only Inbound and Outbo	aund								
test				Save Cancel						

8. Enable URL Reputation Anaysis in the required direction.

/NSP_Doc_03 > Intrusion Prevention > Policy Manager											
Properties Inspection Options											
Traffic Inspection Advanced Callback Detection GTI Ra	eputation Services	Web Server - Heuristic Analysis	Web Server - Denial-of-Service Prevention								
Endpoint URL											
0											
URL Reputation Analysis:	Outbound only										
Minimum URL Risk:	High	- 0									
test				Save	Cancel						

- 9. Select the required risk level for the URL Reputation.
- 10. Click **Save** in the **<Device Name/Interface>** panel to save the configuration changes.
- 11. Do a configuration update for the corresponding Sensor.

Viewing URL Reputation details in the Manager

You can view the details for a URL that is inspected by the Sensor in the Manager. The Manager dashboard provides **Top Risky URLs** and **Top Endpoints Using Risky URLs** monitors to view the details of URL reputation.

Viewing Top Risky URLs

You can view the top risky URLs that are accessed from your systems. To view the top risky URLs, perform the following steps:

- 1. Select the **Dashboard** tab in the Manager.
- 2. Click **w** to edit the dashboard settings. The **Dashboard Settings** window opens.
- 3. Select Top Risky URLs monitor.
- 4. Click OK. The Top Risky URLs monitor is visible on the Dashboard.

Top Risky URLs	00
0	Medium+ Risk 🔻 Any Result 🔻
http://wwwcom/contact/	152
http:// .es/	149
http://	142
http:// .com/wp-content/theme	137
http://ro/wp-content/th	121
http:// com/wp-content/plugi	115
http:// .ro/wp-content/themes/	108
http://kz/wp-content/plugins	105
http:// com/wp-content/	103
http://	99

- 5. Click on the graph bar that displays the number of connections. The Attack Log window opens.
- 6. Double click on an alert to view the details of the risky URL.

Viewing Top Endpoints Using Risky URLs

You can view the top endpoint systems that are sending requests to risky URLs. To view the top endpoints that sending requests to risky URLs, perform the following steps:

- 1. Select the **Dashboard** tab in the Manager.
- 2. Click **w** to edit the dashboard settings. The **Dashboard Settings** window opens.
- 3. Select Top Endpoints Using Risky URLs monitor.

4. Click OK. The Top Endpoints Using Risky URLs monitor is visible on the Dashboard.



- 5. Click on the graph bar that displays the number of connections. The **Attack Log** window opens.
- 6. Double click on an alert to view the details of the risky URL.

Viewing URL reputation alert details in Attack Log

You can view the alert details of a risky URL in the **Attack Log** page.

/My Com	/My Company > Attack Log														
Attack	Attack Log														
0							Unacknowledged	Last 14	days		 http: 	//1.1. //cmd.exe	× Cle	ar All Filte	rs 🔿 🏚
					<u>Result</u>	Attack Count									
1		HTTP: IIS cmd.exe Execution	Jul 27, 2021 00:16:39	Outbound	Attack Sm		CVE-2000-0886	Export		59470	0	-	80	۲	💴 China 🏠
2		HTTP: IIS cmd.exe Execution	Jul 27, 2021 00:16:35	Outbound	Attack Sm		CVE-2000-0886	Export		59470	0	-	80	۲	💴 China
3		HTTP: IIS cmd.exe Execution	Jul 27, 2021 00:16:32	Outbound	Attack Sm		CVE-2000-0886	Export		59473	9		80	۲	💴 China
4		GTI: Risky URL Detected	Jul 27, 2021 00:16:32	Inbound	Inconclusive			Export				—	59473		💴 Unite
5		HTTP: IIS cmd.exe Execution	Jul 27, 2021 00:16:30	Outbound	Attack Sm		CVE-2000-0886	<u>Export</u>	101100	53663	0	-	80	۲	💴 China
6		GTI: Risky URL Detected	Jul 27, 2021 00:16:30	Inbound	Inconclusive			Export		80	9	•••	53663	9	💴 Unite
7		HTTP: IIS cmd.exe Execution	Jul 27, 2021 00:16:27	Outbound	Attack Sm		CVE-2000-0886	Export		59473	0		80	۲	💴 China
8		GTI: Risky URL Detected	Jul 27, 2021 00:16:27	Inbound	Inconclusive			Export		80	9	<u></u>	59473	0	💴 Unite
9		HTTP: IIS cmd.exe Execution	Jul 27, 2021 00:16:26	Outbound	Attack Sm		CVE-2000-0886	<u>Export</u>		51815	0		80	۲	💴 China
10		HTTP: IIS cmd.exe Execution	Jul 27, 2021 00:16:25	Outbound	Attack Sm		CVE-2000-0886	Export		53663	0	-	80	۲	💴 China
11		GTI: Risky URL Detected	Jul 27, 2021 00:16:25	Inbound	Inconclusive			<u>Export</u>		80	0		53663	0	💴 Unite
12		GTI: Risky URL Detected	Jul 27, 2021 00:16:20	Inbound	Inconclusive			Export		80	0	200	51815	0	
13		HTTP: IIS cmd.exe Execution	Jul 27, 2021 00:16:20	Outbound	Attack Sm		CVE-2000-0886	Export		51815	0	-	80	۲	💴 China
14		HTTP: IIS cmd.exe Execution	Jul 26, 2021 21:42:01	Outbound	Attack Sm		CVE-2000-0886	Export		59470	0		80	۲	💴 China
Ack	Una	ack Delete Other Acti	ons 🔹									1-55 of 55 ale	rts 🕊	<	>

When you double-click on an alert, the alert details window opens. The **Layer 7** section of the alert details has the following information:

• Risky URL

- Risk category
- The header fields that are used to construct the URL

I GTI: Risky URL Detected					
			Export 🔹 💭		
Summary Details	s Description				
				ľ	
Time:	Oct 16, 2019	Domain:			
Direction:	Inbound	Device:	PK_NS5100	l	
Result:		Interface:		ł	
Relevance:		Matched Polic	y: NSM_QA_Default Brevention	ł	
Application:	🕏 нттр	Zone:		L	
Protocol:		VLAN:		L	
Detection:		Assigned To:		ł	
Acknowledged:		Alert ID:	856013869427782 3325		
Attacker / Target			۵		
	Attacker	1	Target		
IP Address (Port):	0	(6346)	🤌 🕕 (6348)	ł	
Country:		•	United States	L	
Hostname:				ł	
VM Name:				L	
VM IP:				L	
Proxy IP:				l	
OS:				l	
User:				l	
Network Object:				I.	

CLI commands for URL Reputation integration

The following Sensor CLI commands can be used to view the URL Reputation details:

- show urlrepstats
- show gti config
- show gti stats url

For more information, see the section CLI commands in McAfee Network Security Platform 10.1.x Product Guide.

Troubleshooting scenarios

This section describes the troubleshooting scenarios for the URL Reputation feature.

System faults

This section lists the system fault messages visible in the Manager Operational Status viewer.

Manager Warning Faults

Fault	Severity	Description/Cause	Action
GTI URL Reputation Services Disabled	Warning	The Manager generates this fault when you publish a policy to the Sensor and the name resolution is not configured in the Manager. GTI URL Reputation service requires name resolution configuration.	Configure name resolution in the Manager.

Cannot enable URL Reputation feature in the Manager

Possible Cause: Telemetry is not configured in the Manager.

You should configure Telemetry for the URL Reputation feature to work. You can configure Telemetry at **Manager** \rightarrow **<Admin domain name>** \rightarrow **Setup** \rightarrow **Telemetry**.

Integration with McAfee MVISION Insights

McAfee MVISION Insights is a cloud-based solution that provides the latest global intelligence on the top campaigns that threat actors are using to target business sectors and organizations around the world. You can view threat information for your business sector based on your geo-location, and prevalence data for both targeted campaigns and specific security threats that might impact your organization. With this information, you can take preventive action to protect your organization.

MVISION Insights analyzes the data based on the following features:

- **Proactive scanning and prioritization of threats**: MVISION Insights scans the attack data received from your network for globally known campaigns based on your geo-location and that are likely to impact your organization. It shows a comparison between your network and other sectors.
- **Predictive assessment of security posture**: The network topology is analyzed to provide insight regarding the security posture score and predict your network protection against cyber threats.
- **Prescriptive, preemptive security actions**: MVISION Insights studies your network protection devices and lists those that are likely to be impacted by the attacks or have insufficient information to detect attacks.

The MVISION Insights web console displays the analytic data as follows:

• **Security posture score** — MVISION Insights evaluates the network protection configuration, derives the network security posture score, and shares recommendations to improve the score and configuration. Network Security Platform integrates with MVISION Insights to send your network protection configurations.

🗹 Note

The security posture score will be available in the MVISION insights web console with the next MVISION Insights update release.

- Campaigns by severity The list of known campaigns detected by Insights that are categorized based on severity
- Campaign detections Number of findings in your network based on campaigns in last 10 days
- Devices Number of vulnerable devices in your network with insufficient coverage to detect possible threats
- Campaigns trending globally List of the top three campaigns having world wide impact
- Campaigns Displays detailed information regarding campaigns detected by Insights
- Threats Displays detailed information on threats and your network

Henceforth, MVISION Insights will be referred to as Insights, and Network Security Manager as the Manager.

How Network Security Platform - MVISION Insights integration works

This integration provides a registration workflow that enables Network Security Platform as an additional source of threat information for MVISION Insights. After successful integration, Network Security Platform sends the telemetry data to the GTI server and TITAN which is used by MVISION insights for predictive analysis. The integration works in three phases:

Network Security Platform registration with MVISION ePO

On registering the Manager with MVISION ePO, the following unique identifiers are sent as part of the telemetry data:

- Tenant ID: Unique identifier assigned to the MVISION account at the time of creation
- Manager GUID: Identifier for the Manager generated during the Manager installation

If you have two Managers registered with MVISION ePO using the same MVISION account, both the Managers will have the same Tenant ID but individual Manager GUID.

The telemetry data from Network Security Platform is identified by MVISION Insights through the Tenant ID and the Manager GUID.

Integration with MVISION Insights

Once the Manager is registered with the MVISION ePO, integration with Insights is disabled by default until the user enables it. Insights then collects the attack information from Network Security Platform telemetry data which includes alert data and feature configuration. Insights uses the Tenant ID to identify all the Managers in that network. The collected information is then processed by the engine residing in Insights to perform predictive analysis.

Analysis of the processed data

The processed data is available in MVISION Insights page hosted on the MVISION ePO console. This page includes analytics like security posture score, campaigns detected in your network, vulnerable devices, etc. The data is segregated and displayed based on features defined within the server for data analysis. This helps prioritize threats, predict methods to detect threats, and prescribe better ways to improvize attack detection in Network Security Platform.

Integration between Network Security Platform and MVISION Insights



High-level steps to make the integration work

Before you begin

You must have a McAfee MVISION ePO setup configured.

MVISION Insights integration requires a series of integration steps as outlined below.

- 1. Generate an MVISION ePO registration token.
- 2. Enable telemetry in the Manager.
- 3. Register the Manager server with the MVISION ePO.
- 4. Enable MVISION Insights integration.

Generate MVISION ePO registration token

Before you begin

You must have a McAfee MVISION ePO setup configured.

🗹 Note

For more information on configuring McAfee MVISION ePO, see McAfee MVISION ePO Product Guide and McAfee MVISION Insights Product Guide.

To generate MVISION ePO registration token, perform the following steps:

Task

1. Navigate to Appliance and Server Registration page.

For more information, see Register appliances and servers in McAfee MVISION ePO Product Guide.

2. Click **Add**.

The Add New Registration Token window opens.

- 3. Under Client Type, select McAfee Network Security Platform.
- 4. Under **Number of clients (1 10 max)** option, enter the number of clients you want to register with this MVISION ePO registration token.
- 5. Click Save.
- Go to Servers → McAfee Network Security Platform and make a note of the newly generated MVISION ePO registration token.

🗹 Note

The MVISION ePO registration token is valid only for 12 hours from the time of generation.

Enable Telemetry in the Manager

To enable Telemetry in the Manager, perform the following steps:

Task

 In the Manager, navigate to Manager → <Admin Domain Name> → Setup → Telemetry. The Telemetry page is displayed.

Telemetry page

/My Company > Setup > Telemetry	Ø
Telemetry	What am I Sending?
•	
🕀 Alert Data Details 🛛 Exclu	de IP address information for endpoints on this <u>list</u> .
	O Yes 🔍 No
Alert Data Summary	O Yes 🔍 No
🕣 General Setup	O Yes 🔍 No
🚭 Feature Usage	O Yes 🔍 No
🕣 System Faults	O Yes 🔍 No
🚭 vNSP Cluster Usage	● Yes ● No
Alert Data Details Filter	
Send Alert Details for the Following Severity Alerts:	🗳 High 🗳 Medium 🗳 Low 🔲 Informational 🍷
Technical Contact Information	
Send Contact Information?	OYes ONo
First Name:	John *
Last Name:	Doe *
Street Address:	
Phone Number:	
Email Address:	john_d@mcafee.com
Test Connection	Save

2. Select the Alert Data Details, General Setup, and Feature Usage to be sent to Telemetry.

🗹 Note

The **Alert Data Details**, **General Setup**, and **Feature Usage** details are mandatory data that should be sent to the MVISION Insights when integration is enabled.

3. In the Alert Data Details Filter, select the type of alert severity option to be sent.

The available options are:

- High
- Medium
- Low
- Informational

4. In the **Technical Contact Information**, update the following fields to provide your contact information to McAfee Labs.

- Send Contact Information?
- First Name

- Last Name
- Street Address
- Phone Number
- Email Address
- 5. [Optional] To check whether communication to the GTI server is established, click **Test Connection**.
- 6. Click Save.

Register the Manager with MVISION ePO

Before you begin

Make sure you have MVISION ePO registration token.

To register the Manager with MVISION ePO, perform the following steps:

Task

1. In the Manager, navigate to Manager \rightarrow <Admin Domain Name> \rightarrow Integration \rightarrow MVISION. The MVISION ePO page is displayed.

NSM				Administr	ator 🚢 /My Company 🛽 🖞	ज ?⊡
Trellix	⑦ Dashboard	🖳 Analysis	읂 Policy	E Devices	🖨 Manager	4
Domain: /My Company	✓ /M ₃	<pre>r Company > Integration > MVI</pre>	SION			0
Summary	M	/ISION ePO				
Users and Roles Setup Integration	M	IVISION ePO Registration:	1 Unregistered	0		
MVISION GTI MLC						
HIP HP Network Auto	omation					
▶ ePO ▶ Vulnerability Assert	essment					
 Reporting Maintenance 						
▶ Troubleshooting	F	Register MVISION ePO				

2. Click Register MVISION ePO.

The MVISION ePO Registration window opens.

MVISION ePO Registration	۲
0	
MVISION ePO Key:	
Regist	er

3. Enter the MVISION ePO registration token in the **MVISION ePO Key** field and click **Register**. On successful registration, the **MVISION** page opens with the following details:

Option	Description
MVISION ePO eRegistration	Displays the Manager and MVISION ePO registration status.
MVISION ePO Tenant GUID	Displays the unique identifier assigned to the McAfee MVISION account.
Enable MVISION Insights Integration	Enables integration with MVISION Insights.
Unregister MVISION	Removes trust established between the Manager and MVISION ePO.

/My Company > Integration > MVISION	I		0
MVISION ePO			
0			
MVISION ePO Registration: MVISION ePO Tenant GUID: Enable MVISION Insights Integration	✓ Registered	0	
Unregister MVISION ePO			Save

Enable MVISION Insights integration

Before you begin

- Network Security Manager registered with MVISION ePO
- Telemetry enabled in the Manager to add the following data to the MVISION insights:
 - Alert data Details

The **MVISION ePO** page is displayed.

- General setup
- Feature usage

To enable MVISION Insights integration, perform the following steps:

Task

1. In the Manager, navigate to Manager \rightarrow <Admin Domain Name> \rightarrow Integration \rightarrow MVISION.

10 13		
/My Company > Integration > MVISION		0
MVISION ePO		
0		
MVISION ePO Registration: MVISION ePO Tenant GUID: Enable MVISION Insights Integration	Registered	
Unregister MVISION ePO		Save

2. To enable the MVISION Insights integration, select the Enable MVISION Insights Integration checkbox and click Save.

🗹 Note

Network Security Platform integration with MVISION Insights takes 24 hours to reflect the feature usage telemetry data from the Manager in the MVISION Insights web console.

/My Company > Integration > MVISION	4	0
MVISION ePO		
0		
MVISION ePO Registration: MVISION ePO Tenant GUID: Enable MVISION Insights	Registered 1	
Integration	With MVISION Insights integration enabled, manager will send NSP feature usage telemetry to MVISION Insights for analyzing threats, identifying campaigns and evaluating Security Posture score. Enable the Feature Usage telemetry option from: Manager > Setup > Telemetry	
Unregister MVISION ePO	s	ave

3. In the Default - Telemetry (Insights Security Posture) report, the General Setup and Feature Usage sections list the Network Security Platform data shared with MVISION Insights. To view the data shared to MVISION Insights, go to Analysis → <Admin Domain Name> → Event Reporting → Next Generation Reports and run Default - Telemetry (Insights Security Posture) report.

🗹 Note

The **General Setup** and **Feature Usage** options in the telemetry page should be enabled when MVISION Insights integration is enabled in the Manager.

Unregister MVISION ePO

To unregister MVISION ePO in the Manager, perform the following steps:

Task

 In the Manager, navigate to Manager → <Admin Domain Name> → Integration → MVISION. The MVISION page is displayed.

/My Company > Integration > MVISION	I		0
MVISION ePO			
0			
MVISION ePO Registration: MVISION ePO Tenant GUID: Enable MVISION Insights Integration	✓ Registered	0	
Unregister MVISION ePO			Save

2. To remove Network Security Platform registration with MVISION ePO, click Unregister MVISION.

A Warning pop-up opens.



3. Click **OK** to unregister the Manager from MVISION ePO.



Integration with McAfee Advanced Threat Defense

Over the years, malware has evolved into a sophisticated tool for malicious activities, such as stealing valuable information, accessing your computer resources without your knowledge, and for disrupting business operations. At the same time, technological advancement provides limitless options to deliver malicious files to unsuspecting users. Hundreds of thousands of new malware variants every day make the job of malware detection even more complex. Traditional anti-malware techniques are no longer sufficient to protect your network.

McAfee's response to this challenge is the McAfee Advanced Threat Defense solution. This is an on-premise appliance that facilitates detection and prevention of malware. McAfee Advanced Threat Defense provides protection from known, near-zero day, and zero-day malware without compromising on the quality of service to your network users.

The McAfee Advanced Threat Defense solution primarily consists of the McAfee Advanced Threat Defense appliance and its preinstalled software. The McAfee Advanced Threat Defense appliance is available in two models. The low-end model is the ATD-3000. The high-end model is the ATD-6000. You can deploy McAfee Advanced Threat Defense as a stand-alone appliance or integrate it with some of the other McAfee products. For complete information on McAfee Advanced Threat Defense, see the *McAfee Advanced Threat Defense Product Guide*.

McAfee Advanced Threat Defense has the added advantage of being an integrated solution. In addition to its own multi-level threat detection capabilities, its ability to seamlessly integrate with other McAfee security products, protects your network against malware and other Advanced Persistent Threats (APTs).

You can integrate McAfee Advanced Threat Defense with Network Security Platform. After you integrate, both the Sensor and the Manager communicate with McAfee Advanced Threat Defense separately to augment your defense against malware.

Outline of how this integration works— Based on how you have configured the corresponding Advanced Malware policy, the IPS Sensor detects a file download and sends a copy of the file to McAfee Advanced Threat Defense for analysis. If McAfee Advanced Threat Defense immediately detects the file to be a malware, the Sensor can block the download. The Manager displays the results of the analysis from McAfee Advanced Threat Defense.

If McAfee Advanced Threat Defense requires more time for analysis, the Sensor allows the file to be downloaded. If McAfee Advanced Threat Defense detects a malware after the file has been downloaded, it informs Network Security Platform, and you can use the Sensor to quarantine the host until it is cleaned and remediated. You can configure the Manager to update all the Sensors about this malicious file. Therefore, if that file is downloaded again anywhere in your network, your Sensors might be able to block it.

🗹 Note

The Sensor that is integrated with McAfee Advanced Threat Defense can be deployed in inline, tap, or SPAN mode. However, similar to other malware engines, response actions such as *Block* and *Send TCP Reset* might not have the desired effect since the file might have reached the target host.

Advantages

The following are the advantages of integrating Network Security Platform with McAfee Advanced Threat Defense.

• When a supported file is being downloaded into your network, it can be analyzed in depth using McAfee Advanced Threat Defense. This fortifies your already strong anti-malware defense with Network Security Platform.

• McAfee Advanced Threat Defense is not an inline device. It can receive files from IPS Sensors for malware analysis. So, it is possible to deploy McAfee Advanced Threat Defense in such a way that you obtain the advantages of an inline antimalware solution but without the associated drawbacks.

• McAfee Advanced Threat Defense does not sniff or tap into your network traffic. It analyzes the files submitted to it for malware. This means that you can place the McAfee Advanced Threat Defense appliance anywhere in your network as long as it is reachable to all the integrated McAfee products. It is also possible for one McAfee Advanced Threat Defense appliance to cater to all such integrated products (assuming the number of files submitted is within the supported level). This design can make it a very cost-effective and scalable anti-malware solution.

• Android is currently one of the top targets for malware developers. With this integration, the Android-based handheld devices on your network are also protected. You can dynamically analyze the files downloaded by your Android devices such as smartphones and tablets.

• Files are concurrently analyzed by various engines. So, it is possible for known malware to be blocked in almost real time.

• When McAfee Advanced Threat Defense dynamically analyzes a file, it selects the analyzer virtual machine that uses the same operating system and other applications as that of the target host. This is achieved through its integration with McAfee ePO or through passive device profiling feature of Network Security Platform. This enables you to identify the exact impact on a targeted host, so that you can take the required remedial measures. This also means that McAfee Advanced Threat Defense executes the file only the required virtual machine, thereby preserving its resources for other files.

• Consider a host downloaded a zero-day malware, but a Sensor that detected this file downloaded submitted it to McAfee Advanced Threat Defense. After a dynamic analysis, McAfee Advanced Threat Defense determines the file to be malicious. Based on how you have configured the Advanced Malware policy, it is possible for the Manager to add this malware to the block list of all the Sensors in your organization's network. This file also might be on the blacklist of McAfee Advanced Threat Defense. Thus, the chances of the same file re-entering your network is reduced.

• Even the first time when a zero-day malware is downloaded, you can contain it by quarantining the affected hosts until they are cleaned and remediated.

• You can view the disassembly listing of PE files. The rich reporting feature of McAfee Advanced Threat Defense is also now available for the files detected by your Sensors.

Terminologies

Being familiar with the following terminologies facilitates malware analysis while using Advanced Threat Defense.

• **Static analysis** — When Advanced Threat Defense receives a supported file for analysis, it first performs static analysis of the file. The objective is to check if it is a known malware in the shortest possible time, and also to preserve the Advanced Threat Defense resources for dynamic analysis. For static analysis, Advanced Threat Defense uses the following resources.

4| Integration with McAfee Advanced Threat Defense

🗹 Note

Static analysis sequence is following.

1.Global Whitelist > 2.Local Blacklist > 3.McAfee GTI / McAfee Gateway Anti-Malware Engine / McAfee Anti-Malware Engine (These three resources are processed in tandem.)

• **Global Whitelist** — This is the list of MD5/SHA-256 hash values of trusted files and VBA scripts embedded inside a Microsoft Office application, which need not be analyzed.

The whitelist feature is disabled by default. To enable or disable it, use the setwhitelist command. Use the **Global Whitelist** page on the **Manage** tab to manage the entries in the whitelist. In a load-balancing scenario, after the
cluster creation, you need to run whitelistMerge cluster command on the Active node to manually copy the Global
Whitelist database of Active node onto Secondary/Backup nodes. This is only a one-time activity, after which the
Whitelist database of Secondary/Backup nodes is automatically overwritten by that of Active node at 0000 hours on a
daily basis.

🗹 Note

The default whitelist entries are not periodically updated. However, they might be updated when you upgrade the Advanced Threat Defense software. When you upgrade the Advanced Threat Defense software to build 3.4.8.190 and above, MD5 added into the whitelist will be merged into Global Whitelist.

The McAfee products that submit files to Advanced Threat Defense do have the capability to perform custom whitelisting as well. This includes the McAfee Web Gateway and the McAfee Network Security Platform.

• Local Blacklist — This is the list of MD5 hash values of known malware stored in the Advanced Threat Defense database. When Advanced Threat Defense detects a malware through its heuristic McAfee Gateway Anti-Malware engine or through dynamic analysis, it updates the local blacklist with the file's MD5 hash value. A file is added to this list automatically only when its malware severity as determined by Advanced Threat Defense is medium, high, or very high. There are commands to manage the entries in the blacklist.

• **McAfee GTI** — This is a global threat correlation engine and intelligence base of global messaging and communication behavior, which enables the protection of the customers against both known and emerging electronic threats across all threat areas. The communication behavior includes the reputation, volume, and network traffic patterns. Advanced Threat Defense uses both the IP Reputation and File Reputation features of GTI.

🗹 Note

DNS must be configured for GTI to run.

🗹 Note

For File Reputation queries to succeed, make sure Advanced Threat Defense is able to communicate with tunnel.message.trustedsource.org over HTTPS (TCP/443). Advanced Threat Defense retrieves the URL updates from List.smartfilter.com over HTTP (TCP/80).

• **Gateway Anti-Malware** — McAfee Gateway Anti-Malware Engine analyzes the behavior of web sites, web site code, and downloaded Web 2.0 content in real time to preemptively detect and block malicious web attacks. It

protects businesses from modern blended attacks, including viruses, worms, adware, spyware, riskware, and other crimeware threats, without relying on virus signatures.

McAfee Gateway Anti-Malware Engine is embedded within Advanced Threat Defense to provide real-time malware detection.

• Custom Yara Scanner — Custom Yara Scanner is a set of YARA rules.

• **Anti-Malware** — McAfee Anti-Malware Engine is embedded within Advanced Threat Defense. The DAT is updated automatically based on the network connectivity of Advanced Threat Defense.

Static analysis also involves analysis through reverse engineering of the malicious code. This includes analyzing all the instructions and properties to identify the intended behaviors, which might not surface immediately. This also provides detailed malware classification information, widens the security cover, and can identify associated malware that leverages code re-use.

🗹 Note

By default, Advanced Threat Defense downloads the updates for McAfee Gateway Anti-Malware Engine and McAfee Anti-Malware Engine every 90 minutes. To manually update these files, use CLI command, update_avdat.

• **Dynamic Analysis** — In this case, Advanced Threat Defense executes the file in a secure VM and monitors its behavior to check how malicious the file is. At the end of the analysis, it provides a detailed report as required by the user. Advanced Threat Defense does dynamic analysis after the static analysis is done. By default, if static analysis identifies the malware, Advanced Threat Defense does not perform dynamic analysis. However, you can configure Advanced Threat Defense to perform dynamic analysis regardless of the results from static analysis. You can also configure only dynamic analysis without static analysis. Dynamic analysis includes the disassembly listing feature of Advanced Threat Defense as well. This feature can generate the disassembly code of PE files for you to analyze the sample further.

🗹 Note

Dynamic analysis sequence is following.

1.Global Whitelist > 2.Local Blacklist > 3.McAfee GTI / McAfee Gateway Anti-Malware Engine / McAfee Anti-Malware Engine (These three resources are processed in tandem.) > 4.Yara Scanner > 5. Dynamic Analysis

• **Analyzer VM** — This is the virtual machine on the Advanced Threat Defense that is used for dynamic analysis. To create the analyzer VMs, you need to create the VMDK file with the required operating system and applications. Then, using SFTP, you import this file into the Advanced Threat Defense Appliance.

Only the following operating systems are supported to create the analyzer VMs:

- Microsoft Windows XP 32-bit Service Pack 2
- Microsoft Windows XP 32-bit Service Pack 3
- Microsoft Windows Server 2003 32-bit Service Pack 1
- Microsoft Windows Server 2003 32-bit Service Pack 2
- Microsoft Windows Server 2008 R2 Service Pack 1
- Microsoft Windows 7 32-bit Service Pack 1
- Microsoft Windows 7 64-bit Service Pack 1
- Microsoft Windows 8.0 Pro 32-bit
- Microsoft Windows 8.0 Pro 64-bit
- Android 2.3 or 4.3 by default. You can upgrade it to Android 5.0.

All of the above Windows operating systems can be in English, Chinese Simplified, Japanese, German, or Italian.

🗹 Note

The only pre-installed analyzer VM is the Android VM.

You must create analyzer VMs for Windows. You can create different VMs based on your requirements. The number of analyzer VMs that you can create is limited only by the disk space of the Advanced Threat Defense Appliance. However, there is a limit as to how many of them can be used concurrently for analysis. The number of concurrent licenses that you specify also affects the number of concurrent instances for an analyzer VM.

• VM profile — After you upload the VM image (.vmdk file) to Advanced Threat Defense, you associate each of them with a separate VM profile. A VM profile indicates what is installed in a VM image and the number of concurrent licenses associated with that VM image. Using the VM image and the information in the VM profile, Advanced Threat Defense creates the corresponding number of analyzer VMs. For example, if you specify that you have 10 licenses for Windows XP SP2 32-bit, then Advanced Threat Defense understands that it can create up to 10 concurrent VMs using the corresponding .vmdk file.

• **Analyzer profile** — This defines how to analyze a file and what to report. In an analyzer profile, you configure the following:

- VM profile
- Analysis options
- Reports you wish to see after the analysis
- Password for zipped sample files
- Maximum execution time for dynamic analysis

You can create multiple analyzer profiles based on your requirements. For each Advanced Threat Defense user, you must specify a default analyzer profile. This is the analyzer profile that is used for all files uploaded by the user. Users who use the Advanced Threat Defense web application to manually upload files for analysis can choose a different analyzer profile at the time of file upload. The analyzer profile selected for a file always takes precedence over the default analyzer profile of the corresponding user.

To dynamically analyze a file, the corresponding user must have the VM profile specified in the user's analyzer profile. This is how the user indicates the environment in which Advanced Threat Defense should execute the file. You can also specify a default Windows 32-bit and a 64-bit VM profile.

• **User** — An Advanced Threat Defense user is one who has the required permissions to submit files to Advanced Threat Defense for analysis and view the results. In case of manual submission, a user could use the Advanced Threat Defense web application or an FTP client. In case of automatic submission, you integrate McAfee products, such as McAfee Network Security Platform or McAfee Web Gateway with Advanced Threat Defense. Then when these products detect a file

download, they automatically submit the file to Advanced Threat Defense before allowing the download to complete. So, for these products default user profiles are available in Advanced Threat Defense.

For each user, you define the default analyzer profile, which, in turn, can contain the VM profile. If you use the Advanced Threat Defense for uploading files for analysis, you can override this default profile at the time of file submission. For other users, Advanced Threat Defense uses the default profiles.

How Network Security Platform - Advanced Threat Defense integration works

When you integrate Network Security Platform with McAfee Advanced Threat Defense, the Sensor initiates a communication channel with McAfee Advanced Threat Defense. This channel is open unless the Sensor is down, McAfee Advanced Threat Defense is down, or you disable the integration. By default, this communication channel is over SSL protocol. McAfee Advanced Threat Defense listens on port 8505 for such connections. You can also switch to TCP protocol for communication that McAfee Advanced Threat Defense listens on port 8506.

🗹 Note

If the communication channel between the Sensor and McAfee Advanced Threat Defense goes down, the system fault *Sensor* connectivity status with Advanced Threat Defense device is displayed.

The Manager accesses the RESTful APIs of McAfee Advanced Threat Defense for its communication. When a connection is required, the Manager establishes an HTTPS connection. McAfee Advanced Threat Defense listens on a fixed port number 443 for such connections.

The integration with McAfee Advanced Threat Defense enhances the Advance Malware feature of Network Security Platform. This enables you to detect even unknown malware. This integration takes advantage of the in-depth analyzing capabilities of McAfee Advanced Threat Defense including its ability to dynamically analyze and disassemble files.

🗹 Note

For McAfee Advanced Threat Defense, both the Manager and Sensor are like users. So, a user profile called *nsp* is pre-defined in McAfee Advanced Threat Defense. By default, the Manager uses the user name and password defined in this profile to establish its communication with McAfee Advanced Threat Defense. When the Sensor submits a file for analysis, McAfee Advanced Threat Defense uses the analyzer profile defined in the *nsp* to determine how to analyze the file and what to report back to the Manager. The Manager also allows different Sensors to have their own analyzer profile as per configured by the respective Sensor users.

When you integrate with McAfee Advanced Threat Defense, it is available as an additional malware engine for all the supported file types in the Advanced Malware Policies. You can select this engine along with any of the other malware engines except NTBA. Since McAfee Gateway Anti-Malware Engine is available in both McAfee Advanced Threat Defense and NTBA appliance, you can only select either of these engines for a file type.

Details of how the integration works

Following is the procedure and process flow when the integration with McAfee Advanced Threat Defense involves a standalone Sensor and Manager.

🗹 Note

McAfee GTI File Reputation is available both in the Advanced Malware policies of Network Security Platform as well as in McAfee Advanced Threat Defense. McAfee recommends that you enable McAfee GTI File Reputation in both Network Security Platform and McAfee Advanced Threat Defense. The Sensor can respond quicker if it is configured in the Advanced Malware policy because, in this case, it directly communicates with McAfee GTI.

- 1. You configure McAfee Advanced Threat Defense integration details for the required Sensor.
- 2. You enable the Advanced Threat Defense as one of the malware engines in the corresponding Advanced Malware policy. For the sake of explanation, assume that you have enabled all the engines except NTBA for all the file types.

🗹 Note

Based on which engine reports back first, the IPS Sensor takes the response action. Consider that you have configured high-severity malware to be blocked by the Sensor. McAfee GTI File Reputation configured in Network Security Platform reports a file as high-severity malware. Then, the Sensor blocks this file even before receiving the results from the Advanced Threat Defense engine.

3. You have applied this Advanced Malware policy to the required inline ports.

🗹 Note

The Advanced Threat Defense malware engine can be used with SPAN and tap ports. However, similar to other malware engines, response actions, such as *Block* and *Send TCP Reset*, might not have the desired effect since the file might have reached the target host.

- 4. If the Sensor detects a supported file type being downloaded over HTTP or SMTP (encoded using Base64 only), it extracts the file and checks it against its allow list and then its block list.
- 5. Assume that the file's hash value is not listed in the Sensor's allow or block list. The Sensor constantly streams the file, as the user downloads it, to all the other engines for a concurrent analysis. The Sensor holds the last packet from the user for a specific time period, while it awaits the results from any of the configured malware engines.
- 6. From the analyzer profile configured in the respective Network Security Platform user profile, McAfee Advanced Threat Defense determines the analysis methods and the reports to be generated.

• If McAfee Advanced Threat Defense responds with a malware score that meets the **Action Thresholds** for alerting in the Advanced Malware policy, the Sensor raises *Malware: Malicious file detected by ATD* alert and takes the other configured response actions.

• If McAfee Advanced Threat Defense responds with a malware score that does not meet the **Action Thresholds**, the Sensor raises an informational alert *Malware: Unknown file download detected and submitted to ATD for analysis*. As expected, no response actions are taken. If the file is determined to be clean, the Manager deletes this alert. If there is any change in the malware score, the Manager updates the same alert.

🗹 Note

As mentioned earlier, the Manager uses the user name and password defined in *nsp* profile to establish its communication with McAfee Advanced Threat Defense. The Manager also allows different Sensors to have their own analyzer profile as configured by the respective Sensor users.

Recall that McAfee Advanced Threat Defense must respond within the file scan timeout for the Sensor to function as explained above.

- 7. Network Security Platform performs malware analysis on files in the following sequence:
 - M-series and Virtual IPS: Allow and Block Lists → TIE/GTI File Reputation/McAfee Cloud (for apk files) → NSP Analysis → Advanced Threat Defense or NTBA (if Advanced Threat Defense is disabled)
 - NS-series: Allow and Block Lists → TIE/GTI File Reputation/McAfee Cloud (for apk files) → NSP Analysis → Gateway Anti-Malware → Advanced Threat Defense
- 8. The Manager continuously queries McAfee Advanced Threat Defense for the results of this analysis. When the reports are received, the Manager updates the record in the **Malware Files** page.
- 9. Since, dynamic analysis is a time taking process, there is a need to carefully employ this process for improved user experience. Network Security Platform submits files to McAfee Advanced Threat Defense for dynamic analysis only if the other engines enabled report back the malware confidence as medium or above.
- 10. Assume that the results of dynamic analysis indicate that the file is malicious with a *high* severity level. You can now use the **Quarantine** feature to quarantine the host from the rest of the network until you are sure that the host is safe again.
- 11. Because the malware severity is high, McAfee Advanced Threat Defense adds the MD5 hash of this file to its local blacklist. So, the next time this file is submitted by any source, it is able to respond in the shortest possible time.

🗹 Note

McAfee Advanced Threat Defense adds a file to its blacklist if the malware severity of the file is medium, high, or very high.

12. If you had configured the **Add to Block List** action threshold in the Advanced Malware policy, the Manager can include the MD5 hash of this file in the block list of all its Sensors. Therefore, when the same file is detected by any of the Sensors, it is blocked by that Sensor itself. This reduces the chances of such malware entering your network again.

🗹 Note

McAfee recommends that you verify how the Advanced Malware feature works for a period of time, fine-tune it until it functions as expected, and only then enable the **Add to Block List** action threshold in the Advanced Malware policies.

What happens in case of MDR?

• You configure the McAfee Advanced Threat Defense in the active Manager. It takes 15 minutes for this configuration to be copied to the standby. Alternatively, you can use the **Retrieve Configuration** feature in the standby to immediately copy the MDR configuration to the standby.

• When a Sensor submits a file to McAfee Advanced Threat Defense, it informs both the Managers. So, both the Managers query McAfee Advanced Threat Defense separately for the results of the file.

• Every 10 minutes, both the Managers cross-check their malware report data from McAfee Advanced Threat Defense and ensure that the data is synchronized.

What happens in case of Sensors in failover?

- When you configure the integration for the failover Sensors, both the Sensors establish separate communication channels with McAfee Advanced Threat Defense. So, McAfee Advanced Threat Defense considers them to be different users. It sends the update only to the Sensor that submitted the file.
- The file is extracted only by the Sensor that detected it. If a Sensor goes down within the packet hold time interval, based on the port configuration, the file might be forwarded without malware analysis or dropped.
- If the Sensor goes down after the packet hold time interval but before the file session time interval, the update from McAfee Advanced Threat Defense is lost since it is sent only to the Sensor that submitted the file.

Considerations

Review this section before your proceed to integrate Network Security Platform with McAfee Advanced Threat Defense.

- You need a Manager and Sensor running on versions 10.1 or later.
- You need McAfee Advanced Threat Defense 4.6.0 or later.
- You can integrate multiple Sensors with the same McAfee Advanced Threat Defense appliance. The Manager also allows different Sensors to have their own analyzer profile as configured by the respective Sensor users. This implies that the users can use a singleMcAfee Advanced Threat Defense device, but can use a different analyzer profile per IPS device or per interface.

High-level steps for integrating with McAfee Advanced Threat Defense

This section provides the high-level steps on how to integrate Network Security Platform with McAfee Advanced Threat Defense. This section assumes that McAfee Advanced Threat Defense is up and running. For information on how to install and configure McAfee Advanced Threat Defense, see its documentation.

Summarized steps for configuring malware analysis



1. Set up the McAfee Advanced Threat Defense appliance and ensure it is up and running.

• Make sure the McAfee Advanced Threat Defense appliance has the network connections it needs for your application. Make sure the Sensor, Manager, and the McAfee Advanced Threat Defense appliance are able to ping each other.

• Make sure the required static analysis modules, such as the McAfee GTI and McAfee Gateway Anti-Malware Engine have the latest DATs.

- 2. Create the required VMDK files for the analyzer VMs and import them into McAfee Advanced Threat Defense. The Android analyzer VM is available by default.
- 3. Convert the VMDK files to image files and then create the corresponding VM profiles.
- 4. Create the analyzer profiles you need under McAfee Advanced Threat Defense interface. You can select these analyzer profiles from the drop-down list under the Manager interface. The Manager also allows different Sensors to have their own analyzer profile as configured by the respective Sensor users. This implies that the users can use a single McAfee Advanced Threat Defense device, but can have different analyzer profile per Network Security Platform device or per interface.
- 5. If you want McAfee Advanced Threat Defense to upload the results to an FTP server, configure it and have the details with you before you create the profiles for the corresponding users.
- 6. Log on to McAfee Advanced Threat Defense web application using respective Network Security Platform user credential created for different Sensors integrated with McAfee Advanced Threat Defense and upload a sample file for analysis. This is to check if you have configured McAfee Advanced Threat Defense as required.
- 7. In the **Analysis Status** page, monitor the status of the analysis.
- 8. After the analysis is complete, view the report in the **Analysis Results** page.

For information on all the above tasks, see the *McAfee Advanced Threat Defense Product Guide*.

To integrate McAfee Advanced Threat Defense and Network Security Platform, these additional steps are required:

- 1. Configure the McAfee Advanced Threat Defense details for the required admin domains and enable communication.
- 2. Enable the integration for the required Sensors under those domains. You can inherit the McAfee Advanced Threat Defense details from the admin domain or override them at the Sensor level.
- 3. Configure an Advanced Malware policy with Advanced Threat Defense selected for the required file types. Ensure that you have assigned this Advanced Malware policy to the required inline monitoring ports. See the *McAfee Network Security Platform Product Guide* for information on how to configure and apply Advanced Malware policies.

Integrating Network Security Platform and McAfee Advanced Threat Defense

When you integrate Network Security Platform and McAfee Advanced Threat Defense, both the Manager and Sensor communicate with the McAfee Advanced Threat Defense separately. You have to configure the McAfee Advanced Threat Defense details for all the required Sensors and then enable the integration.

If you want to configure multiple Sensors with the same McAfee Advanced Threat Defense, you can specify the details at the admin domain and inherit the settings at the Sensor level. This saves you the trouble of having to configure the same details multiple times. If required, you can also customize the inherited settings for the required Sensors.

Enable McAfee Advanced Threat Defense integration for an admin domain

You can configure the details for the integration at an admin domain so that the corresponding Sensors and child domains can inherit these settings. However, you must enable the integration at the Sensor level for the Sensor and the Manager to be able to communicate with McAfee Advanced Threat Defense.

Task

- 1. In the Manager, select the **Devices** tab.
- 2. Select the required domain from the **Domain** drop-down list and then select **Global**.
- 3. Select IPS Device Settings \rightarrow ATD Integration.
- 4. Enter the configuration details in the corresponding fields.

Enabling the integration for an admin domain

/My Company > IPS Device Settin	gs > ATD Integration		Ø
ATD Integration			
0			
Enable ATD Integration?	2		
Sensor-to-ATD Communica	tion		
ATD IP Address:			
ATD Listening Port (TCP):	8505		
····· ································		'	
Manager-to-ATD Communic	ation		
Use a Different IP Address for Manager-to-ATD Communication?	-		
ATD IP Address:			
ATD Listening Port (TCP):	443		
Authentication and File Sub	mission		
ATD Username:			
Password for 'nsp':	•••••		
ATD User Profile for File Submission:	nsp 💌 💭		
Open ATD Console			Save

Option definitions

Option	Definition
Enable ATD Integration?	Select to configure the details for the integration at this domain level.
ATD IP Address	Enter the IPv4 address of McAfee Advanced Threat Defense for communicating with Sensor.

Option	Definition
ATD Listening Port (TCP)	This is the port that McAfee Advanced Threat Defense will listen for connections from Sensors. The default port is 8505. You can modify if required.
Use a Different IP Address for Manager-to- ATD Communication?	Check if you want Manager to communicate with the McAfee Advanced Threat Defense appliance using a different IP address than the IP address the Sensor is using to communicate with the same McAfee Advanced Threat Defense appliance.
ATD IP Address	Enter the IPv4 address of McAfee Advanced Threat Defense for communicating with Manager. Enter same IP address entered above incase you have not checked Use a Different IP Address for Manager-to-ATD Communication? box, else enter different IP address for communication between Manager and McAfee Advanced Threat Defense.
ATD Listening Port (TCP)	This is the port that McAfee Advanced Threat Defense will listen for connections from Sensors. The default port is 8505. You can modify if required.
Test connection	Click to verify if the Manager is able to communicate with McAfee Advanced Threat Defense using the details you configured. For the Sensor, you can ping the IP address of McAfee Advanced Threat Defense appliance from the Sensor CLI.
ATD Username	The pre-defined user name, which the Manager uses to log on to McAfee Advanced Threat Defense, is displayed. You cannot enter a different name or change this default name in McAfee Advanced Threat Defense.
Password for 'nsp'	 Enter the corresponding password. The default password is <i>admin</i>. As a precaution, change this password in the NSP User user record in McAfee Advanced Threat Defense. a. Click Open ATD Console to open McAfee Advanced Threat Defense web application. b. In McAfee Advanced Threat Defense web application, select Manage → User Management. c. Select NSP User and click Edit to change the password. d. Click Save.
ATD User Profile for File Submission	Select from the drop-down your user profile created under McAfee Advanced Threat Defense. With the 9.1 release, a Sensor can have its own analyzer profile as configured by the user.

Option	Definition
Save	Saves the McAfee Advanced Threat Defense details in the Manager database.
Open ATD Console	Click to access the logon page of McAfee Advanced Threat Defense with which the Sensor is currently integrated.

Enable McAfee Advanced Threat Defense integration for a Sensor

The integration between McAfee Advanced Threat Defense and Network Security Platform is established only when you enable this integration at the Sensor level. If you enable this integration globally for an admin domain, it is enabled for the corresponding Sensors by default. You can customize these settings at the Sensor level.

Task

- 1. In the Manager, select the **Devices** tab.
- 2. Select the domain from the **Domain** drop-down list.
- 3. On the left pane, click the **Devices** tab.
- 4. Select Setup \rightarrow ATD Integration.
- 5. Enter the configuration details in the corresponding fields.

Enabling the integration for a Sensor

/My Company > PK_NS5100_17_	209 > Setup > ATD Integration		8
ATD Integration			
•			
Inherit Settings? Enable ATD Integration?	■ ⊠		
Sensor-to-ATD Communica	tion		0
ATD IP Address: ATD Listening Port (TCP):	8505		
Manager-to-ATD Communic	ation		0
Use a Different IP Address for Manager-to-ATD Communication?	-		
ATD IF Address:	443		
		Test Connection	
Authentication and File Sub	mission		0
ATD Username:	nsp		
Password for 'nsp':			
ATD User Profile for File Submission:	nsp 🔹 💭	▶	
Open ATD Console		Save	a

Option definitions

Option	Definition
Inherit Settings?	Select to inherit the integration configuration from the corresponding admin domain. The remaining fields are available only if this is de-selected.
Enable ATD Integration?	Select to integrate the Sensor with McAfee Advanced Threat Defense. After you select, you are able to view and configure the details for the integration.
ATD IP Address	Enter the static IPv4 address of McAfee Advanced Threat Defense.
ATD Listening Port (TCP)	This is the port that McAfee Advanced Threat Defense will listen for connections from Sensors. The default port is 8505. You can modify if required.
Use a Different IP Address for Manager-to- ATD Communication?	Check if you want Manager to communicate with the McAfee Advanced Threat Defense appliance using a different IP address than the IP address the Sensor is using to communicate with the same McAfee Advanced Threat Defense appliance.
ATD IP Address	Enter the IPv4 address of McAfee Advanced Threat Defense.
ATD Listening Port (TCP)	This is the port that McAfee Advanced Threat Defense will listen for connections from Manager. The default port is 8505. You can modify if required.
Test Connection	Click to verify if the Manager is able to communicate with McAfee Advanced Threat Defense using the details you configured. For the Sensor, you can ping the IP address of McAfee Advanced Threat Defense appliance from the Sensor CLI.
ATD Username	The pre-defined user name, which the Manager uses to log on to McAfee Advanced Threat Defense, is displayed. You cannot enter a different name or change this default name in McAfee Advanced Threat Defense.
Password for 'nsp'	 Enter the corresponding password. The default password is <i>admin</i>. As a precaution, change this password in the NSP User user record in McAfee Advanced Threat Defense. a. Click Open ATD Console to open McAfee Advanced Threat Defense web application. b. In McAfee Advanced Threat Defense web application, select Manage → User Management.

Option	Definition
	c. Select NSP User and click Edit to change the password. d. Click Save.
ATD User Profile for File Submission	Select from the drop-down your user profile created under McAfee Advanced Threat Defense. With the releases 9.1 or later, a Sensor can have its own analyzer profile as configured by the user.
Save	Saves the McAfee Advanced Threat Defense details in the Manager database
Open ATD Console	Click to access the logon page of McAfee Advanced Threat Defense with which the Sensor is currently integrated.

Add an Advanced Malware policy

You configure the anti-malware options in an Advanced Malware policy and then assign it to the required Sensor monitoring resources, such as ports, interfaces, and subinterfaces. You must do a configuration and signature set update for any changes in the policy to take effect.

Task

- 1. Select **Policy** and then select the required admin domain from the **Domain** drop-down list.
- 2. Select Intrusion Prevention \rightarrow Policy Types \rightarrow Advanced Malware.
- 3. Click +

The **Advanced Malware** page for a new policy opens.

Update the properties of the Advanced Malware policy

Properties				
Name:	Default Malware Policy	Traffic to Inspect —		
Description:		HTTP:	🖌 Download 🛈	Upload 🕕
Owner:	/My Company	FTP SMTP		
visible to Child Admin Domains?				

4. Update the following properties.

Field name	Description
Name	Name of the policy
Description	Description of the policy
Owner	Name of the admin domain to which the policy belongs
Visible to Child Admin Domains?	Specifies whether the policy is applicable to all child admin domains
Traffic to Inspect	 Protocols over which advanced malware scanning is performed. The supported protocols are HTTP, FTP, and SMTP. Image: Note: The HTTP Download option allows you to scan HTTP download/response traffic for presence of malware. This option is enabled by default. The HTTP Upload option allows you to scan HTTP upload (POST and PUT) requests for presence of malware. This option is disabled by default. You need to select the Upload checkbox to enable it. For more information on scanning HTTP POST and PUT requests, refer to the Malware inspection on HTTP Upload requests section in McAfee Network Security Platform Product Guide. Image: Note: FTP malware detection overrides the accelerate-ftp feature even if it is enabled. For more information on the accelerate-ftp command, refer to the CLI commands section in McAfee Network Security Platform Product Guide.

5. Update the File Scanning Options.

2												
File Scanning Options												
0												
					Gateway Anti-Malware					Send TCP Reset		
Executables	5120	V				V		High	High	High	Disabled	Disabled
MS Office Files	1024				7	V		High	High	High	Disabled	Disabled
PDF Files	1024		V		V			High	High	High	Disabled	Disabled
Compressed Files	5120	V			V	7		High	High	High	Disabled	Disabled
i Android Applica	2048					V	V	High	High	High	Disabled	Disabled
i Java Archives	2048					V		High	High	High	Disabled	Disabled
I Flash Files	2048	V						High	High	High	Disabled	Disabled
										mpt for assignme	after save Sa	ve Cancel

🗹 Note

Name resolution must be enabled on devices which will be using the GTI File Reputation malware engine.

File scanning options

Field name	Description
File Type	The file types to be scanned. For information about the supported file types, refer to the table <i>Advanced malware file extension support</i> below.
Maximum File Size (KB) Scanned	The maximum size currently supported for the corresponding file type. Files that exceed the specified size are not analyzed for malware by any of the engines, including the block and allow lists. The default values are displayed in the Default Malware Policy as well as when you create a policy. The default values are the optimum sizes recommended by McAfee Labs based on their research on malware.
	You can set the maximum file size value up to (25*1024) KB/25 MB for all file types. However, the NSP Analysis engine and McAfee Cloud engine have a file-size limit. The limits for each Sensor model are as follows: • NS-series Sensors - (50*1024) KB/50 MB • Virtual IPS Sensors- (5*1024) KB/5 MB

Field name	Description
	Note: McAfee recommends that for any file type, you do not set a value more than (5*1024) KB/5 MB as the maximum file size as this might affect the Sensor's performance.
Malware Engines	 The Malware engines to scan the selected file type. If you select Gateway Anti-Malware for a File Type, you must either use an NS-series Sensor running on Sensor software version 9.1 or above, or NTBA. For Advanced Threat Defense to work, you must integrate the corresponding Sensors with McAfee Advanced Threat Defense. See the chapter <i>Integration with McAfee Advanced Threat Defense</i> for more information.
Action Thresholds	 Specifies the type of response to be made for the attack. The types of responses are: Alert — Alerts are raised in Attack Log. Block — This action blocks packets for detected malware, thus preventing the malicious file from reaching the host.
	 The first step towards prevention is typically to block attacks that have a high severity level. When you know which attacks you want to block, you can configure your policy to perform the drop attack packets response for those attacks. If not configured in the policy, the Attack Log allows you to update the policy to block traffic. Send TCP Reset— Disconnects a TCP connection at the source, destination, or both ends of the transmission, thus preventing the malicious file from reaching the host.
	Note: This response may not work effectively with SPAN and tap deployments.
	• Add to Block List— If any of the engines report the submitted file to be malicious, the Manager adds the file's MD5 hash to the block list in its database. To be added to this list, the file's severity must be the same or more than what you specify in this field. For example, if you specify <i>high</i> as the criteria, then files of severity <i>high</i> and <i>very high</i> are added to the block list. Within the next 5 minutes, the Manager adds this file to the local block list of all the Sensors that it manages.
	Note: The TIE/GTI File Reputation engine does not support Add to Block List response action. You can manually add the desired malware file's MD5 hash to the block list from the Attack Log page.

Field name	Description
	• Save File — One of the response actions specified is the ability to archive the file in a file store based on the Advanced Malware policy. The files that are selected based on this configuration are forwarded to Manager.
	 For files greater than 5 MB, only the first 5 MB is available as the saved file. To prevent the Manager's disk from getting frequently filled up, use the Save File feature sparingly. The Sensor's simultaneous file scan capacity is reduced if the Save File option is enabled. See the table in this section for the details.

Advanced malware file extension support

File Type	HTTP Upload and Download	SMTP	FTP
Executables	2500	acm	acm
	aciii	.acm	.acm
	.ax	.ax	.ax
	.com	.com	.com
	.cpl	.cpl	.cpl
	.dll	.dll	.dll
	.drv	.drv	.drv
	.exe	.exe	.exe
	.fon	.fon	.fon
	.ocx	.ocx	.ocx
	.olb	.olb	.olb
	.pif	.pif	.pif
	.qts	.qts	.qts
	.qtx	.qtx	.qtx
	.scr	.scr	.scr
	.sys	.sys	.sys
	.vbx	.vbx	.vbx
	.vxd	.vxd	.vxd

File Type	HTTP Upload and Download	SMTP	FTP
MS Office Files	.doc	.doc	.doc
	.docx	.docx	.docx
	.ppt	.ppt	.ppt
	.pptx	.pptx	.pptx
	.rtf	.rtf	
	.xls	.xls	.xls
	.xlsx	.xlsx	.xlsx
PDF Files	.fdf	.fdf	.fdf
	.pdf	.pdf	.pdf
	.xdp	.xdp	
Compressed Files	.7z	.7z	
	.pkzip	.pkzip	.pkzip
	.rar	.rar	.rar
	.zip	.zip	.zip
Android Application Packages	.apk		.apk
Java Archive	.jar	.jar	.jar
Flash Files	.swf	.swf	

🗹 Note

McAfee might enhance the supported file types over time. The file types are subject to change with new signature sets. The Sensor cannot extract .zip, .jar, .apk and office open xml files if correct file extension is not present, as they share the same magic number 50 4B 03 04(PK).

Each file type is scanned by a Malware engine. Multiple malware engines can be selected to scan various file types. The Malware engines return a confidence level. Based on the confidence level, the following action thresholds can be set. The confidence levels supported are: Very low, low, medium, high, very high.

The Malware Engines supported per file type are:

File Type	TIE/GTI File Reputation	Allow and Block Lists	NSP Analysis	Gateway Anti- Malware	Advanced Threat Defense	McAfee Cloud
Executables	\checkmark	~		\checkmark	~	
MS Office Files	\checkmark	~	~	\checkmark	~	
PDF Files	\checkmark	~	~	\checkmark	~	
Compressed Files	✓	~		\checkmark	✓	
Android Application Package	~	~			~	~
Java Archive	\checkmark	\checkmark		\checkmark	~	
Flash Files	~	~	~	~	\checkmark	

The maximum simultaneous file scan capacity per Sensor model is as follows.

Sensor	Maximum simultaneous file scan capacity with file save	Maximum simultaneous file scan capacity without file save
NS9500 stack - 100 Gbps throughput	1,000	4,096
NS9500 stack - 60 Gbps throughput	1,000	2,048
NS9500 stack - 40 Gbps throughput	1,000	2,048
NS9500 standalone - 30 Gbps throughput	1,000	1,024
NS9500 standalone - 20 Gbps throughput	1,000	1,024

Sensor	Maximum simultaneous file scan capacity with file save	Maximum simultaneous file scan capacity without file save	
NS9500 standalone - 10 Gbps throughput	1,000	1,024	
NS9300, NS9200, NS9100	1,000	1,024	
NS7500 - 7.5 Gbps throughput	1,000	1,024	
NS7500 - 5 Gbps throughput	1,000	1,024	
NS7500 - 3 Gbps throughput	1,000	1,024	
NS7350, NS7250, NS7150	1,000	1,024	
NS7300, NS7200, NS7100	1,000	1,024	
NS5200, NS5100	32	1,024	
NS3500	16	255	
NS3200, NS3100	16	255	
IPS-VM600	32	1,024	

6. To assign the Advanced Malware Policy to the available interfaces and direction (Inbound, Outbound), select **Prompt for assignment after save**.

Assign Interfaces

Assignments				
Search available interfaces				
Available Interfaces † /My Company/PK_NS5100_17_209/G2/1-G2 /My Company/PK_NS5100_17_209/G2/1-G2	Current Policy	Selected Interfaces (policy group) $f \uparrow$		
 /My Company/PK_NS5100_17_209/G2/3-G2 /My Company/PK_NS5100_17_209/G2/3-G2 /My Company/PK_NS5100_17_209/G2/5-G2 /My Company/PK_NS5100_17_209/G2/7-G2 /My Company/PK_NS5100_17_209/G2/7-G2 /My Company/PK_NS5100_17_213/G0/1-G0 /My Company/PK_NS5100_17_213/G0/1-G1 /My Company/PK_NS5100_17_213/G0/1-G1 	NSM QA ATD			
/My Company/PK_NS5100_17_213/G1/1-G1	NSM_QA_ATD			
Objects:72		Objects:0		
				Reset
			Save	Cancel

- 7. Select the required interface from the **Available Interfaces** column and add it to the **Selected Interfaces (Policy Group)** column.
- 8. Click Save.

You are directed to the new policy window.

Manage Advanced Malware policies

You can perform the following operations on an existing Advanced Malware policy.

Operation	Description
View Advanced Malware policies	The Advanced Malware policies page allows you to view the Malware policies that have been assigned to the various resources of your Network Security Platform. Policies are listed per the Sensor, interface, and subinterface. From the root admin domain, you can see policies assigned to all child domains. For non-root parent domains, you only see the assigned policies in your parent and child domains. For child domains, you only see the policies assigned to the resources in your domain. Select Policy \rightarrow Admin Domain Name \rightarrow Policy Types \rightarrow Advanced Malware to view the assigned Malware policies.
Edit an Advanced Malware policy	Editing an Advanced Malware policy allows you to make the changes necessary to match the policy with the traffic you are monitoring. Editing a policy permanently changes that policy. If you intend to make slight changes to a policy but want to save it under a different name, try cloning an Advanced Malware policy.

Operation	Description
	To edit an Advanced Malware policy:
	1. Select Policy \rightarrow <admin domain="" name=""> \rightarrow Policy Types \rightarrow Advanced Malware.</admin>
	The Advanced Malware policies are listed.
	2. Double click the policy to edit.
	4. Click Save .
Clone an Advanced Malware policy	Cloning duplicates an existing policy, and is similar to a "save as" function. You can edit a Network Security Platform-provided policy. However, if you want to edit a copy of a policy, you can clone any existing policy to further refine the policy for application in a new environment. You can clone a provided policy, save it under a new name, and customize it for your unique environment.
	1. Select Policy \rightarrow <admin domain="" name=""> \rightarrow Policy Types \rightarrow Advanced Malware.</admin>
	The policies are listed.
	2. Select the policy you want to clone.
	3. Click 🙆.
	4. Type a new name for the policy, if required and edit the policy parameters.
Delete an	To delete an Advanced Malware policy you have created:
Malware policy	1. Select Policy \rightarrow <admin domain="" name=""> \rightarrow Policy Types \rightarrow Advanced Malware.</admin>
	The Advanced Malware policies are listed.
	2. Select the policy to be deleted.
	3. Click —
	4. Click Yes to confirm the deletion.
	You cannot delete a currently applied policy.
Export an	You can export and save one or more Advanced Malware policies into a file.
Advanced Malware policy	1. Select Policy \rightarrow <admin domain="" name=""> \rightarrow Intrusion Prevention \rightarrow Advanced \rightarrow Policy Export \rightarrow Advanced Malware.</admin>
	The existing Advanced Malware policies are listed.
	2. Select one or more policies to be exported.
	3. Click Export . You are prompted to specify the location to save the file.

Operation	Description
	The policy is saved in an XML format in the specified location.
lmport an Advanced Malware policy	You can import an Advanced Malware policy from a saved file. 1. Select Policy → <admin domain="" name=""> → Intrusion Prevention → Advanced → Policy Import → Advanced Malware.</admin>
	To skip importing duplicate policy definition, select Skip duplicate policy definitions . 2. Browse to the file location. 3. Click Import . The import status is displayed.

Sensor CLI commands

The following are the Sensor CLI commands that show information related to McAfee Advanced Threat Defense integration.

- The status command additionally shows information related to the integration.
 - Status Shows whether the communication channel between the Sensor and McAfee Advanced Threat Defense is up or down
 - IP The IP address of the McAfee Advanced Threat Defense appliance with which the Sensor is integrated
 - Port The port number used for the communication

[Manager Communications]				
Trust Established		yes			
Alert Channel		up			
Log Channel		up			
Authentication Channel		up			
Last Error		None			
Alerts Sent		18			
Logs Sent		6			
[Alerts Detected]					
Signature		2	Alerts	Suppressed	: 0
Scan		0	Denial	of Service	: 0
Malware		16			
[McAfee NTBA Communicat	io	n]			
Status		down			
IP		0.0.0.0			
Port	:	8505			
McAfee MATD Communicat	io	n]			
Status		up			
TP		172.14.199.14	12		
Port		8505			

• From the debug mode, the switch matd channel command enables to select TCP or SSL channel for communication with McAfee Advanced Threat Defense.

• The show malwareenginestats command additionally shows the statistics for the ATD engine.

• A Sensor, for its connections through its management port with a McAfee Advanced Threat Defense appliance, uses AES128-GCM-SHA256 cipher by default. To know if the connection is currently encrypted, use show amchannelencryption status on the Sensor CLI.

🗹 Note

SSL encryption when enabled can have performance degradation, which may impact the analysis of large files and highvolume of files. To transfer large files, switch to TCP channel on the Sensor and Advance Threat Defense. Use command switch matd channel tcp on Sensor CLI and set nsp-tcp-channel enable on Advance Threat Defense CLI.

For more information on these commands, refer to McAfee Network Security Platform Product Guide.

Analyze Malware Files

You can leverage the analysis technique provided by Network Security Platform to perform an in-depth analysis of the malware detected in your network. The Manager provides you with a complete view of the malware and threats on your network for further analysis and actions, thus providing a comprehensive view of the threat landscape in your network. You can view the **Top Malware Files**. This dashboard is populated because a malicious file has been detected. In addition to viewing the threats to your network, the Manager also provides you the option to archive malware files.

To view malware detected by Network Security Platform, use the **Top Malware Files** monitor. The dashboard displays the **Malware File Hash** and the **Attack Count** of the detected malware. Security monitors are displayed as bar charts in the **Dashboard** page.

Top Malware Files

Top Malware Files		\$
0	Very Low+ Malware Confiden	Any Result
/Adobe-Geticon-PlainPDF-xpsp3.pdf/119		6,117
/~ssivakumaran/MS/CVE-2015-1642/poc.d 207		
/collectmail.pdf/7331df41dfb25c55271c 148		
/82Samples/27.pdf/095577e1456844a4963 120		
/82Samples/20.pdf/d292fd7316e915d964e — 90		
/82Samples/39.pdf/9af373dc300c8c6cd89 88		
/82Samples/c0dca57ca92d7196584817fd6b 86		
/82Samples/3.pdf/634715a8d86a8c7cd440 84		
/~ssivakumaran/W/poc.docx/81dff7a819a 84		
/82Samples/maliciousRC4-128.pdf/1113b 83		

If you want to drill down further on a specific malware, click on a bar, and you will be redirected to the **Analysis** \rightarrow **Malware Files** page, which displays additional details on that malware. This page provides you with the flexibility of filtering and sorting the information displayed based on your choice. In addition to these filtering/sorting options, you can also view the alerts that match

the filter criteria by opening the **Attack Log** page directly from the **Threat Explorer**. You can view the malware files specific to admin domains by selecting the required admin domain from the **Domain** drop-down list. Summarized data for malware files, which includes data from the child domains, also can be viewed. If you have integrated the Manager with McAfee ePolicy Orchestrator, McAfee® Logon Collector, or McAfee Vulnerability Manager, you can view the endpoint name, operating system, open ports, and known vulnerabilities.

The following chart gives you the comprehensive analysis options provided by the **Malware Files** page. These tabs are explained in the subsequent sections.

Malware analysis



The following filter options are provided.

View data specific to admin domain



Analyze detected malware within a specific time

Last 14 days	•
Last 5 minutes	
Last 1 hour	
Last 6 hours	
Last 12 hours	
Last 24 hours	
Last 48 hours	
Last 7 days	
Last 14 days	
Custom Time Period	

Analyze the type of malware, whether blocked, unblocked, or all

Any Result Any Result Blocked Unblocked

Analyze the malware based on malware confidence returned by engines

Any Malware Confidence Any Malware Confidence Very High Malware Confidence High+ Malware Confidence Medium+ Malware Confidence Low+ Malware Confidence Very Low+ Malware Confidence

Details of the detected malware

/My	Company > Malw	are Files														0
Malware Files																
0 Any Malware Confidence • Any Result • 07/13/21 1:57 PM - 08/23/21 1:57 PM • Search .										o						
Has																
					Overall Malware Confidence		TIE / GTI File Reputation		Gateway Anti- Malware	Advanced Threat Defense	Endpoint Intelligence Agent			Total Attacks		File Size (bytes)
1	Take action	54c652555			Low	Low							Aug 17 10:20 IST	88	/Artemis-High.e	1024
2	Take action	0276e42a1	f9a201f475c09	55c2a651d3bbr	Very High		Very High								/MS09-067_MSI	2560
3	Take action	83f6ac96fE	8727e88f450bc	8fca97e3e0aae	Very High		Very High						Aug 12 16:11 IST		/MS10-038_MSL	68608
4	Take action	7331df41d	76801e528023	fca955cc5004b!	Very High		Very High						Aug 17 10:19 IST	35	/collectmail.pdf	2931
																•
Manage allow and ck lists Sav																

Option	Definitions
Hash	 Displays the hash value of the file and the actions that you can take. Actions— Click Take action to take the following actions: Export— Click to download the malware file from the Manager server to a network location.
	The file is saved with an extension .mcafee. This prevents you from even accidentally opening the malicious file. The file is available for download only if you enable the Save File option for the corresponding file type in the Advanced Malware policy that detected this malware.
	Note: The antivirus program on your computer might prevent you from downloading the file.
	 Allow— Click to automatically add the file to the Manager's allow list. In the next 5 minutes, the Manager sends the MD5 hash value to the allow list of all the Sensors. Block— Click to automatically add the file to the Manager's block list. In the next 5 minutes, the
	Manager sends the MD5 hash value to the block list of all the Sensors.
	• MD5 — Displays the MD5 hash of the file
	 SHAT — Displays the SHAT hash of the file SHA256 — Displays the SHA256 hash of the file
Overall Malware Confidence	The overall malware confidence level returned by the configured malware scanning engines

Option	Definitions
Individual Engine Confidence	The confidence level returned by each configured malware scanning engine, individually. Click 🔟 to view the engine-specific details.
Last Attack	The date and time the last malware was detected.
Total Attacks	The number of times the malware was detected.
Last File Name	The name of the last saved malware file. In case of HTTP downloads it will be the URL.
File Size (bytes)	The size of the malware file saved
Comment	Additional comments on the detected malware

Attack Log

Upon double-clicking on the malware file hash, the **Attack Log** opens where you can view and analyze alerts related to the selected hash.

Attack log alerts for the hash selected

/My Comp	any > M	lalware Files																	0
Attack	Attack Log																		
0												Una	knowledge:	d 🔫 I	07/06/21 11:10 AM - 10/21/	21 11:10 / 👻		Clear All Filters	
								Packet Captu											
															MD5	SHA1			
1		MALWARE: Malicious File	Sep 22, 2	Inbound	Attack E			Export										HTTP Request Method: GET , HTTP U	RI:
2		MALWARE: Malicious File	Sep 22, 2	Inbound	Attack E			Export										HTTP Request Method: GET , HTTP U	RI:
3		MALWARE: Malicious File	Sep 22, 2	Inbound	Attack E			Export										HTTP Request Method: GET , HTTP U	RI:
4		MALWARE: Malicious File	Sep 22, 2	Inbound	Attack E			Export										HTTP Request Method: GET , HTTP U	RI:
5		MALWARE: Malicious File	Sep 22, 2	Inbound	Attack E			Export										HTTP Request Method: GET , HTTP U	RI:
6		MALWARE: Malicious File	Sep 22, 2	Inbound	Attack E			Export										HTTP Request Method: GET , HTTP U	RI:
7		MALWARE: Malicious File	Sep 22, 2	Inbound	Attack E			Export										HTTP Request Method: GET , HTTP U	RI:
8		MALWARE: Malicious File	Sep 22, 2	Inbound	Attack E			Export										HTTP Request Method: GET , HTTP U	IRI:
9		MALWARE: Malicious File	Sep 22, 2	Inbound	Attack E			Export										HTTP Request Method: GET , HTTP U	IRI:
10		MALWARE: Malicious File	Sep 22, 2	Inbound	Attack E			Export										HTTP Request Method: GET , HTTP U	RI:
11		MALWARE: Malicious File	Sep 22, 2	Inbound	Attack E			Export					-					HTTP Request Method: GET , HTTP U	IRI:
Ack		ack Delete Other /	Actions 🔻														1-22 a	« () » <ba< td=""><td>ck</td></ba<>	ck

To close the attack log, click **Back** or **See** icon.

Manage allow and block lists

The **Manage allow and block lists** is a link to the **File Hashes** page. For more information, see the *McAfee Network Security Platform Product Guide*.

View the McAfee Advanced Threat Defense specific details for a detected malware

Similar to viewing the specific details for other malware engines, you can also view the specific results returned by McAfee Advanced Threat Defense. In the **Malware Files** page, click next to the confidence level for **Advanced Threat Defense**.

Details returned by McAfee Advanced Threat Defense

Advanced Threat Defense Engine Results									
	Enviror	iment StaticAnalysis	-						
File Summary:	File Name - ftp://555 File Size (bytes) - 293 MD5 - 7331DF41DFB: SHA1 - 76801E52802	File Name - ftp://5555:0:0:0:0:0:0:9/collectmail.pdf File Size (bytes) - 2931 MD5 - 7331DF41DFB25C55271C1F111EFC224E SHA1 - 76801E52802334FE2955B1974BC93ADC5F4C267A							
Malware Confidence:	Very High								
Malware Indicators:	 Identified as JS/Exp Identified as TYPE_1 Identified as JS/Exp 	- Identified as JS/Exploit-BO.gen.a by Gateway Anti-Malware - Identified as TYPE_TROJAN by GTI File Reputation - Identified as JS/Exploit-BO.gen.a by Anti-Malwar <u>e</u>							
Individual Engine Results									
Engine	Malware Confidence	Malware Name							
Gateway Anti-Malware	Very High	JS/Exploit-BO.gen.a							
GTI File Reputation	Very High	TYPE_TROJAN							
Anti-Malware	Very High	JS/Exploit-BO.gen.a							
Sandbox	Inconclusive								
Sandbox Analysis Results									
Sandbox Analysis Results Sandbox analysis was not performed. (This is typically because malware was already found by another engine or sandboxing has been disabled from the ATD console.)									
Download Full Analysis Report	Open ATD Console								

Field descriptions

Field	Description
Environment	The VM profile that was used by McAfee Advanced Threat Defense to dynamically analyze the file. This indicates the operating system on which the file was executed.
File Summary	The name of the file, its size, and hash values are displayed.
Malware Confidence	The highest malware severity as returned by the components of McAfee Advanced Threat Defense

Field	Description
Malware Indicators	The summary of the reports from various analysis methods employed by McAfee Advanced Threat Defense
Individual Engine Results	This section lists the analysis methods available in McAfee Advanced Threat Defense. Here, they are referred to as Engine . The severity level returned by each method and the name for the malware are also displayed. If a particular method is not used, it indicates that it is not selected in the analyzer profile used for the Sensor.
Sandbox Analysis Results	This section displays the details if the file was dynamically analyzed by McAfee Advanced Threat Defense. This includes the details of the analyzer VM, the time and duration of the dynamic analysis, behavior during dynamic analysis, and so on.
Analysis Environment	This indicates the operating system on which the file was executed along with the build number of McAfee Advanced Threat Defense.
Download Full Analysis Report	Downloads a zip file that contains all the reports for the malware from McAfee Advanced Threat Defense. This is equivalent to downloading the reports zip file from the McAfee Advanced Threat Defense web application. This zip file contains the reports for each analysis. The contents of this zip file are explained beneath this table.
Open ATD Console	Click to open the logon page of the McAfee Advanced Threat Defense that analyzed the file.
Close	Closes the Advanced Threat Defense Engine Results window

Download the <file hash>.zip file to the desired location. The files in this zip are created and stored with a standard naming convention. Based on the reports selected in the analyzer profile used for the analysis, the zip contains the following results:

• <file hash>_summary.html (.json, .txt, .xml): This is the same as the Analysis Summary report in the McAfee Advanced Threat Defense web application. There are four file formats for the same summary report in the zip file. The html and txt files are mainly for end-users to review the analysis report. The .json and .xml files provide well-known malware behavior tags for high-level programming script to extract key information.

• <file hash>.log: This file captures the Windows user-level DLL API calling activities during dynamic analysis. You must thoroughly examine this file to understand the complete API calling sequence as well as the input and output parameters. This is the same as the User API Log report in the McAfee Advanced Threat Defense web application.

- <file hash>ntv.txt: This file captures the Windows native services API calling activities during dynamic analysis.
- <file hash>.txt: This file shows the PE header information of the submitted sample.

 <file hash>_detail.asm: This is the same as the Disassembly Results report in the McAfee Advanced Threat Defense web application. This file contains reverse-engineering disassembly listing of the sample after it has been unpacked or decrypted.

• <file hash>_logicpath.gml: This file is the graphical representation of cross-reference of function calls discovered during dynamic analysis. This is the same as the Logic Path Graph report in the McAfee Advanced Threat Defense web application. Use a graph editor, such as yWorks yEd Graph Editor, to view this file.

• log.zip: This file contains all the run-time log files for all processes affected by the sample during the dynamic analysis. If the sample generated any console output text, the output text messages are captured in the ConsoleOutput.log file zipped up in the log.zip file. Use any regular unzip utility to see the content of all files inside the log.zip file.

• dump.zip: This file contains the memory dump (dump.bin) of binary code of the sample during dynamic analysis. This file is password protected. The password is *virus*.

• dropfiles.zip: This is the same as the Dropped Files report in the **Analysis Results** page of McAfee Advanced Threat Defense web application. The dropfiles.zip file contains all files created or touched by the sample during the dynamic analysis. It is also password protected like dump.zip.

For a detailed explanation of all these files and McAfee Advanced Threat Defense reports, see the *McAfee Advanced Threat Defense Product Guide*.

Manager reports for malware detections

A default Next Generation Report called **Top 10 Malware Detections** provides details of the detected malware. For a given time period, this report shows the alerts raised for the top 10 most frequently downloaded malware in your network. Therefore, for a given file, you can view the results from various malware engines. However, these results are dependent on the Advanced Malware policy configuration for the period of the report.

Task

- 1. In the Manager, select **Analysis** \rightarrow **Event Reporting** \rightarrow **Next Generation Reports.**
- 2. From the list of Saved Reports, select Default Top 10 Malware Detections and then click Run.
- 3. Specify the time period for which you want to generate the report in the **Date Options** section.
- 4. Select the output format of the report from the Report Format list.
- 5. Click Run.

The default Top 10 Malware Detections report

/My Co	mpany > Even	t Reporting > No	ext Generation Re	ports							0
	UMcAfee Network Security Platform Report										
			Di Ac Si Er Ri								
								Default - Top 10 Malware Detections			
#	Time	Attack Name	Result	Src IP	Dest IP	Protocol	Device	File Hash	Detection Engine	File Malware Confidence	Layer7 Data
1.	2019-10- 17 06:52:02 IST	MALWARE: Malicious PDF file transfer detected VII	Attack Blocked	6.1.1.225	5.1.1.225	http	NS7150_32	d292fd7316e915d964ec4080ecc02676	NSP Analysis	Medium	HTTP Request Method : GET HTTP URI : VB2Samplex 20 pdf HTTP USer-Agent : Wget/1.11.4 (Red Hat modified) HTTP Return Code : 200 HTTP Server Type : Apache/2.2.13 (Fedora) Last-Modified Mon, 0.15 sep 2014 14:37:12 GMT HTTP Host : 1.1.1.12 HTTP Response Content Type : application/pdf
2.	2019-10- 17 06:52:02 IST	MALWARE: Malicious PDF file transfer detected	Attack Blocked	6.1.1.225	5.1.1.225	http	NS7150_32	d292fd7316e915d964ec4080ecc02676	NSP Analysis	Very High	HTTP Request Method : GFT HTTP URI : M2Samples/20.pdf HTTP User-Agent : Wgef/1.11.4 (Red Hat modified) HTTP Return Code : 200 HTTP Server Type : Apache/2.2.13 (Fedora) Last-Modified Mon, 0.1 Sep 2014 14:37:12 GMT HTTP Host : 1.1.1.12 HTTP Response Content Type : application/pdf
3.	2019-10- 17 06:52:02 IST	MALWARE: Malicious PDF file transfer detected II	Attack Blocked	6.1.1.225	5.1.1.225	http	NS7150_32	d292fd7316e915d964ec4080ecc02676	NSP Analysis	Medium	HTTP Request Method : GET HTTP URI: V82smplex20.pdf HTTP User-Agent : Wget/1.11.4 (Red Hat modified) HTTP Return Code : 200 HTTP Server Type : Agache(2.2.13 (Fedora) LamPholdified (Mon. 01 Gep 2014 14:37:12 GHT HTTP Response Content Type : application/pdf HTTP Response Content Type : application/pdf

The generated report is displayed.

Column definitions

Column	Definition
Time	The time stamp when a malware engine determined the file to be malicious
Attack Name	The alert raised by the Sensor for the file
Result	The response action taken by the Sensor for the file. For example, the Sensor could have blocked the file download.
Src IP	The source IP address as seen in the traffic for the malware traffic
Dest IP	The target host that is downloading the file
Protocol	The L7 protocol involved. This could be HTTP or SMTP.
Device	The Sensor that detected the file download
File Hash	The MD5 hash value of the file as calculated by the Sensor

Column	Definition
Detection Engine	The malware engine that reported the malware
File Malware Confidence	The malware score reported by the malware engine
Layer7 Data	The L7 data associated with the file

🗹 Note

The admin domain filter on the main **Analysis** tab (provided in the left pane) has no impact on the reports generated. The admin domain filter criteria selected for the reports show data specific to the admin domain selected.

• For information how to use the Next Generation Reports, see the section Next Generation reports in McAfee Network Security Platform Product Guide..

• You can also generate a User Defined report using all of the above columns. For example, you can generate a User Defined report that reports only very-high severity malware detected by Sensors of a particular domain. You must use **Alert Data** as the **Data Source** when you define the report. For more information on how to generate a User Defined report, see the section *Generate Next Generation user defined reports* in *McAfee Network Security Platform Product Guide.*

Integration with McAfee Threat Intelligence Exchange

Organizations face a plethora of security and operational challenges in an attempt to mount an effective defense strategy against today's emerging threats. To effectively combat emerging threats, organizations require security infrastructure that is a blend of behavioral, reputation, and signature-based assessment capabilities on both the network and endpoints. While each of these security layers might effectively identify threats when working alone, it's important that they work together to share insights, gain knowledge, and adapt in unison to address evolving threats. Time-consuming manual communications between network and endpoint solutions are simply not fast enough to address this requirement. McAfee Threat Intelligence Exchange enables you to use your security infrastructure collaboratively and share file reputation across the network.

🗹 Note

This integration is only available on NS-series and Virtual IPS Sensors.

Why integrate Network Security Platform with Threat Intelligence Exchange?

Currently, users face several challenges when securing a network. The more diverse your network, the larger the operational difficulties, and the harder it is to ensure that your security system is aware of the most recent detections or risks prevalent on the network. Majority of the security administrators today face these challenges.

- Cost of distributing DAT files across all endpoints in the network
- Inability to customize black, white, and gray policies for your network
- Impact of security products on network performance and system resources
- · Need for proactive protection from zero-day malware using reputations, prevalence, and flexible policies

These difficulties are a result of several devices in the network and the addition of new security systems to address different threats. Network Security Platform protects against threats orchestrated by several file types. To be able to achieve a security framework in which more security systems are able to share security awareness and provide adaptive security, you must have a medium that addresses such communication with ease. Data Exchange Layer is a bidirectional communications framework that enables security intelligence and adaptive security. Threat Intelligence Exchange uses Data Exchange Layer that serves as a local repository of file reputations. When enabled, it also acts a proxy to McAfee Global Threat Intelligence.

Benefits of integrating with Threat Intelligence Exchange and Data Exchange Layer

As a product, Threat Intelligence Exchange has been built to offer you the following benefits:

• **Comprehensive threat intelligence**: Security administrators are able to send file hashes of suspicious files to Threat Intelligence Exchange. Threat Intelligence Exchange uses threat intelligence from global data sources, such as Global Threat Intelligence, with local threat intelligence provided by real-time, and historical event data coming from endpoints, gateways, and other security components.

• **Immediate visibility into the presence of advanced targeted attacks**: When file reputation of a file is found as malicious after scanning through a security component like Advanced Threat Defense, you are able to communicate this information through Data Exchange Layer and dynamically contribute to Threat Intelligence Exchange. Shared insights

provide deeper awareness of threats targeting an organization. Attacks are discovered through the endpoints, gateways, and other security components that act in unison.

• **Proactive threat protection**: Threat information gathered through endpoints and gateways can be propagated quickly through Data Exchange Layer, ensuring all integrated security products proactively immunize against newly detected threats.

• **Lowered cost of ownership**: While improving security, the cost of ownership is lowered by extending existing security detection, prevention, and analytic technology investments to protect your organization as soon as a threat is revealed.

Important terminologies and components

The integration between Network Security Platform, Data Exchange Layer, and Threat Intelligence Exchange comprises several components. These components and their brief descriptions are listed.

• Sensor – Any NS-series or Virtual IPS Sensor running Sensor software version 9.1 or above.

• **Threat Intelligence Exchange server** – It is a repository of file reputation details which security products across the network access. By providing file reputation, it enables a security administrator to take corrective action.

• **McAfee ePO** – A management console for endpoints across the network. The Sensor is configured as an endpoint on the network.

• **McAfee Agent** – A management infrastructure extension which is loaded on an endpoint. An endpoint loaded with McAfee Agent is known as a managed endpoint. In the context of this integration, McAfee ePO considers the Sensor as a managed endpoint.

• **Data Exchange Layer (DXL)** – DXL is a real-time, bidirectional, communications infrastructure which provides the framework that enables context (situational awareness, commands, events, etc.) to be shared between different McAfee products. It is also an adaptive security system of interconnected services that communicate and share information to make real-time, accurate security decisions by individual security products, and as a collective solution. Network, endpoint, database, application, and other security solutions are meant to use DXL to operate as one synchronized, real-time, context aware, and adaptive security system.

• **DXL broker** – A network of DXL brokers (brokers) make up the DXL framework. Brokers act as liaisons between the Sensor and the Threat Intelligence Exchange server. In general, they are responsible for routing messages efficiently from senders to receivers. When the Threat Intelligence Exchange server and DXL brokers are set up, the administrator is prompted for McAfee ePO credentials. When the administrator provides these credentials, the broker registers itself with McAfee ePO. In this way, the McAfee ePO server is aware of every DXL broker in the network.

• **DXL client** – A client that is loaded on the Sensor by bundling with McAfee Agent. The Sensor communicates to the DXL framework through the DXL client which consists of broker IP addresses. McAfee ePO considers the Sensor an endpoint. The connection between the DXL client and DXL brokers is a persistent SSL connection, implying that communication between the Sensor and the DXL framework is always open and secure with no time wasted to establish or end a connection.

How the integration works

One server or a collection of servers acts as the Threat Intelligence Exchange server. McAfee ePO is provided with details of the Threat Intelligence Exchange server. The Threat Intelligence Exchange server connects to DXL, which facilitates real-time context sharing between products such as Network Security Platform. Within the Network Security Platform, the Sensor is integrated with DXL. McAfee Agent and the DXL client are bundled with the Sensor software. When the Sensor is integrated with DXL and

McAfee ePO, the client receives information about the location of DXL brokers through McAfee ePO. A network of DXL brokers constitutes the DXL framework which connects to the Threat Intelligence Exchange server.



Threat Intelligence Exchange deployment scenario

The integration between Network Security Platform and Threat Intelligence Exchange works in the following sequence:





• It begins when the Sensor detects a file in the network, computes its file hash, and recognizes that it is suspicious or one that warrants analysis. Whether or not a file is suspicious is determined by first looking up the Manager allow list, then the Manager block list.

• If the file hash is not present in either of these lists, the Sensor queries the Threat Intelligence Exchange server with the file hash through the DXL framework if DXL integration is enabled.

• If DXL integration is not enabled, the Sensor queries Global Threat Intelligence using a HTTPS query.

• Threat Intelligence Exchange receives file reputation for a specific file hash from three different sources. Each of these sources is called a **Provider**.

- It receives an **Enterprise** file reputation which is assigned in McAfee ePO by a network administrator.
- It receives an **Advanced Threat Defense** file reputation based on static and dynamic analyses.
- It receives a **Global Threat Intelligence** file reputation.
- The Threat Intelligence Exchange server forwards this file reputation to the Sensor through the DXL framework.

• Depending on the advanced malware policy configuration, the Sensor raises an alert or takes other configured action. The alert displays the file reputation with the following details that are also received from Threat Intelligence Exchange.

• Provider – Enterprise, Advanced Threat Defense, or Global Threat Intelligence. The table lists the details provided by each of these providers.

Provider	Detail – Description	
Enterprise	Total detections – The number of detections this file hash has triggered	
	Last detection – The last time a detection was triggered by this file hash	
	Distinct file names used by this file – The number of distinct filenames this hash has been detected to be using	
	Malware confidence observed for this file – As assigned by the network administrator in McAfee ePO	
Advanced Threat Defense	Overall malware confidence – As computed by Advanced Threat Defense	
	Individual engine malware confidenceGateway Anti-Malware EngineAnti-Malware EngineSandbox	Malware confidence for each of the individual engines

Provider	Detail – Description
Global Threat Intelligence	Malware confidence – As stored in Global Threat Intelligence

Computing the overall file reputation in the Sensor

Since the Sensor receives file reputation for a file from three different sources, it must choose the one that is most relevant to the security requirements of your network. To do this, the Sensor assigns varying importance to each of the three providers.

- First preference is given to the Enterprise malware confidence since it is specific to this environment.
- Second preference is given to the Advanced Threat Defense since it is configured in your policy and might carry out static and dynamic analysis if they are enabled in the appliance.
- Third preference is given to McAfee GTI.

After the Sensor has selected the appropriate score, it is displayed in the Manager. You can view this score in several pages in the Manager. One of the pages where you are able to see it mapped to the appropriate engine is the **Malware Files** page under the **TIE / GTI File Reputation** column. For more details on viewing detected threats in the Manager, refer to the *McAfee Network Security Platform Product Guide*.

High-level steps to make the integration work

Before you begin

You must make sure that you have

- Set up and configured a McAfee ePO server.
- Set up and configured the Threat Intelligence Exchange server and DXL brokers.

To implement the Threat Intelligence Exchange integration, you must follow a series of steps to make sure that the integration works as expected.

Task

- 1. Log on to the Manager.
- 2. Configure McAfee ePO by providing the appropriate McAfee ePO server IP address and credentials.
- 3. Configure DXL integration either for a domain or for a device.
- 4. Create an advanced malware policy in which TIE / GTI File Reputation is enabled for one or more file types.
- 5. Apply this policy to the Sensor ports you want to use and specify the direction of traffic that is to be monitored with this policy.
- 6. Perform a configuration update on the Sensor.
Results

The setup is ready to be used in a Threat Intelligence Exchange integration.

Enable DXL integration for a domain

Before you begin

Make sure that you have configured the integration with a McAfee ePO server.

DXL is disabled by default for a domain which you can configure. You can later choose whether to use this configuration for each device or override it and use different settings for a device.

To configure DXL integration for a domain, follow these steps.

Task

- 1. Go to Devices \rightarrow <Admin_Domain_Name> \rightarrow Global \rightarrow IPS Device Settings \rightarrow DXL Integration. The Data Exchange Layer (DXL) Integration page appears.
- 2. Select the Enable DXL Integration? checkbox.
- 3. To change McAfee ePO server settings for the Manager, in general, click the **ePO Integration Settings** hyperlink at the topright of the page.
- 4. Click **Save** to confirm your settings.

Data Exchange Layer integration page for a domain

/My Company > IPS Device Settin	ngs > DXL Integration	0
Data Exchange Layer (DXL) Integration	
0		<u>ePO Integration Settings</u>
Enable DXL Integration? ePO Server IP Address:		
ePO Server Port:	8443	
ePO Username:	admin	
Open ePO Console		Save

🗹 Note

To access the McAfee ePO console of the McAfee ePO server mentioned in this page, click the **Open ePO Console** button. Clicking this button takes you to the McAfee ePO logon screen where you need the appropriate credentials to log on.

Results

DXL integration is now enabled for this domain. To use these settings in each device, you need to go to a device and inherit these settings.

Enable DXL integration for a device

Before you begin

Make sure that you have enabled the integration with a McAfee ePO server.

DXL integration is disabled by default for a device. You can enable it to inherit settings from the domain or be independent for the device.

Task

- Go to Devices → <Admin_Domain_Name> → Device → <Device_Name> → Setup → DXL Integration. The Data Exchange Layer (DXL) Integration page appears.
- 2. You have the option to use DXL integration preferences including McAfee ePO server settings used in the domain. To use this option, select the **Inherit Settings?** checkbox.
- The remaining options are immediately disabled when you select this option.
- 3. If you have chosen to inherit settings from the domain, click **Save**. If not, proceed to step 4.
- Select the Enable DXL Integration? checkbox.
 The McAfee ePO server configuration fields are displayed.
- 5. Enter the McAfee ePO server IPv4 address.

Data Exchange Layer integration for a device shows settings specific to it

/My Company > PK_NS5100_17_2	213 > Setup > DXL Integratio	n	Ø
Data Exchange Layer (DXL)) Integration		
0			ePO Integration Settings
Inherit Settings?	•		
Enable DXL Integration?	\checkmark		
ePO Server IP Address:			
ePO Server Port:	8443		
ePO Username:	admin		
ePO Password:	•••••		
Open ePO Console			Save

- 6. Enter the port that the Sensor must use to communicate with McAfee ePO.
- 7. Enter the credentials the Sensor must use to access McAfee ePO.

🗹 Note

The credentials you configure here need not be the same credentials as those entered in the **ePO Integration** page. To review this configuration, click the **ePO Integration Settings** hyperlink at the top-right corner of this page.

8. Click **Save** to confirm your settings.

Results

DXL integration is now enabled with settings specific to this device.

Viewing Threat Intelligence Exchange detection in the Manager

After you have enabled Threat Intelligence Exchange for the Sensor, if you have configured this engine in your advanced malware policy, you will be able to view malware files by this engine in the Manager.

Consider a scenario in which a file is detected by the Sensor. The following sequence illustrates how the Sensor queries Threat Intelligence Exchange and provides the results to be displayed in the Manager. However, this is only one of the ways of viewing the results. For more options, see the *McAfee Network Security Platform Product Guide*.

• When a file appears on the network, the Sensor computes a file hash and checks the allow list and block list in the Manager. When this file hash is not found in these lists, it queries Threat Intelligence Exchange through DXL.

- Threat Intelligence Exchange receives the malware confidence for this file hash from **Enterprise**, Advanced Threat Defense, and Global Threat Intelligence and returns the various parameters to the Sensor.
- The Sensor finds that the malware confidence for the file hash is reported as **High** by **Enterprise** and, as a result, gives the file an overall malware confidence of **High** too.
- You see the malware confidence in the Malware Files page under the TIE / GTI File Reputation column.
- The Sensor also raises a MALWARE: Malicious File Detected by TIE Engine alert.

Malware Files page in the Manager

Ма	lware Files									
1-10										
0					Any Malware	Confidence	Any Result	 Last 5 minut 	es 🔻 Sear	
На				Individual Eng						
			Malware Confidence		TIE / GTI File Reputation ↓		Gateway Anti- Malware	Advanced Threat Defense	Endpoint Intelligence Agent	Last A
1	Take action	6ade202ddb9262	Very High		Very High					Oct
2	Take action	9bd190e40e05c7	Very High		Very High					Oct
3	Take action	743f71a7e78f86f	Very High		Very High					Oct
4	Take action	8d5c4118a0817b	Very High		Very High					Oct
5	Take action	9860b49773715	Very High		Very High					Oct
6	Take action	36f443c41a94f5a	Very High		Very High					Oct
7	Take action	311de1208665d	Very High		Very High					Oct
8	Take action	b1a5b60fb627a0	Very High		Very High					Oct
9	Take action	044cbfdd392380	Very High		Very High					Oct

• Click the icon to view file reputation from each of the three sources.

Threat Intelligence Exchange Engine results

Threat Intelligence Exchan	ge Engine Res	ults	8
Enterprise Advanced Threat	Defense Global	Threat Intelligence	
Total Attacks:			
Last Attack:			
Distinct File Names Used by this File:			
Malware Confidences Observed for this File:	High		

• Or, you can click the *MALWARE: Malicious File Detected by TIE Engine* hyperlink to be directed to the **Threat Explorer** with a filter on the alert.

Threat Explorer page with a filter on that alert

/My Company > Threat E	cplorer			Ø
Threat Explorer				
0			Top: 5 👻 Attacks 💌 Any Direction	- Last 12 hours - 🕤 💭
Filter: Attack Nam	MALWARE: Malicious File Detected by TIE X Add Filter View Attac	ks		
Attack Name - MAE	WARE: Malicious File Detected by TIE			₩.
Description:	This event indicates that a malware has been detected in a file analyzed advantage of McAfee Data Exchange Layer (DXL) to consolidate threat in include Global Threat Intelligence (GTI), Advanced Threat Defense (ATD	by the McAfee Threat Intelligence Exchange (TIE) advanced m nformation, including malware confidence, infection timelines a b) and ePolicy Orchestrator (ePO).	nalware engine, which takes Benign Trigger nd prevalence. TIE data sources Probability	Block Zone
Vulnerability Type:			Low . Medum	Block as Needed Zone
Attack Severity:			High Into Joy Midd H	Cautious Zone
Benign Trigger Probability:			Attack Sev	/erity
Category:				
Subcategory:				
Possible Effects:				
Affected Platforms:	Protocols • Hypertext Transfer Protocol • Simple Mail Transfer Protocol • File Transfer Protocol			
✓ Show More				
Top Attackers				۵
Attacker IP Address				
1 1.1.1.10		🕮 Australia	Unknown	
2 <u>1.1.1.98</u>		🕮 Australia	Unknown	
Top Targets				0
				Attack Count
1 1.1.1.9		🛱 Australia	Unknown	4

- Clicking the View Attacks button opens the Attack Log page that shows all alerts for this file hash.
- Double-clicking on one of these alerts opens the alert details panel.

• You can view the malware details on the **Details** tab where you see the details of the file hash from each of the providers. On this panel, you notice the correlation, if applicable to that file hash, between the provider and the overall malware confidence.

Malware Details panel, Alert Details window

I MALWARE: Malici	ous File Detected by TIE 🛛 🔕
	Export 👻 💭
Summary Details	Description
Malware File	0
File Name:	/root.exe
File Hash:	72bb11ccb133ffbf91aa979f8c4b8 Whitelist Blacklist 4d6
Malware Name:	
Malware Confidence:	High
Engine:	TIE File Reputation
Size (bytes):	1024
Description:	
CVE ID:	
Layer 7	0
HTTP Response Content Type:	application/octet-stream
HTTP Server Type:	Apache/2.4.16 (Fedora) OpenSSL/1.0.1k-fips Last-Modified: Fr i, 20 Feb 2015 17:02:37 GMT
HTTP Return Code:	200
HTTP Host:	1.1.1.10
HTTP URI:	/root.exe
HTTP User-Agent:	Wget/1.11.4
HTTP Request Method:	GET

Sensor CLI commands specific to Threat Intelligence Exchange

The NS-series Sensors are provided with CLI commands specific to the Threat Intelligence Exchange.

- Normal mode
 - show tiestats Displays the total requests and responses to file reputation requests and number of file reputation responses per source, the sources being Enterprise score, Advanced Threat Defense, and Global Threat Intelligence
 - show dxl status Displays whether Data Exchange Layer is enabled or disabled
- Debug mode
 - set ma wakeup port [<1-65536>] Enables you to change the port used to wake up McAfee Agent through the Sensor CLI

For more details on these commands, refer to the section CLI commands in McAfee Network Security Platform Product Guide.

Troubleshooting the integration between Network Security Platform and Threat Intelligence Exchange

The integration between these two products involves several components. Any issue with the integration can be a result of a malfunction in one of these components. The Manager faults mentioned below assist you in troubleshooting this integration.

Fault	Severity	Possible causes	Possible solutions
DXL Service is down	Critical	Failed to connect to the ePolicy Orchestrator Server.	 Check the connectivity between the Sensor and McAfee ePO, or check the logs. Check the logs
		Failed to connect to the Data Exchange Layer.	Check the logs.
		Failed to start the McAfee Agent service.	
		Failed to start the Data Exchange Layer service.	

Manager faults and possible causes

Integrating with McAfee Endpoint Intelligence Agent

This chapter explains how NTBA Appliance is integrated with McAfee® Endpoint Intelligence Agent (McAfee EIA).

Overview

Most enterprises today face a challenge in understanding executables running on the network. With malware increasing at a rampant pace, it has become imperative for security administrators to understand executables sending traffic on the network. Malware can exploit the network and endpoint's inability to coordinate information/policies. Some malware can name themselves as standard executables and make standard application connections on the network. Such malware cannot be detected by looking at just the endpoint processes or monitoring the network traffic flows in isolation.

Combining information obtained from the endpoints with information in the network can provide security administrators deeper visibility into your enterprise. McAfee Network Security Platform, along with Endpoint Intelligence Agent, provides security administrators insight into what executables are running at endpoints that are linked to the network traffic. You can also view malware status and details for non-executables like doc and pdf files. The administrator can then quickly investigate any unusual executable behavior, classify executables and files running on the network as malicious or safe, and take response actions.

McAfee® Endpoint Intelligence Agent (McAfee EIA) is an endpoint solution that provides executable and file information to the NTBA Appliance. It delivers real-time and dynamically analyzed detection results.

When McAfee EIA is installed on an endpoint, it monitors the system for execution of all executables irrespective of whether it is making outgoing connections. This helps you to even monitor data files like word and pdf documents. When a connection attempt is made by an executable, McAfee EIA sends the executable information to the NTBA over an encrypted channel. Using dynamic analysis, if EIA detects malicious data files, it sends the artifacts to NTBA over a separate channel. It also sends dynamic analysis information in metadata. This gives enough time for the NTBA Appliance to process the executable and artifact information and make it available at policy-decision points before the connection request packet is received.

With this solution, you can view all executables and files used on the endpoint. It also provides the number of endpoints using each executable. All executables and files are classified as known good (allowed), known bad (blocked), or unclassified. For the unclassified executables, the solution provides further malware confidence.

The executable information contains:

- 5-tuple information, such as source IP address, destination IP address, source port, destination port, and protocol
- Executable name, full path, and hash of the executable that generated the connection
- User and operating system information associated with the executable
- Details, such as MD5 hash value, product version, malware confidence, malware name, certificate signer, malware indicators, and classification details

The file information includes a detailed trace report or artifacts in JSON format. You can view details, such as file version and certificates. When network traffic is generated based on the reputation of the executable file, you can allow or block them.

Architecture

McAfee EIA resides on the endpoint where it collects details about the executables that initiate traffic. When integration with McAfee EIA is enabled, McAfee EIA sends the executable information to the NTBA Appliance, which uses it to enhance its analysis, such as determining which endpoints are infected or are at risk of infection.

The communication between the McAfee EIA and the NTBA Appliance is through the Datagram Transport Layer Security (DTLS) protocol with the McAfee EIA as the client and the NTBA Appliance as the server. The artifacts for a file are sent to NTBA using the Transport Layer Security (TLS) channel.

McAfee EIA and NTBA can integrate and communicate in either static or dynamic mode. If the DTLS channel doesn't exist when the packet is sent to McAfee EIA, then in:

- **Static mode** Based on the pre-configured NTBA and EIA details, a DTLS channel is created. EIA sends the metadata to mapped NTBA.
- **Dynamic mode** If an NTBA is not pre-configured for McAfee EIA, EIA automatically discovers the NTBA device and sends executable information. When endpoint traffic is going through a Sensor that sends flows to NTBA, and if NTBA does not have executable information for that endpoint, NTBA sends a discovery probe to that endpoint. McAfee EIA discovers the NTBA and starts to communicate with NTBA. This reduces the administrator's burden to figure out how Sensors, NTBA and endpoints are deployed in the network.

Both the client and the server must have the certificates signed by the common Certification Authority (CA). The common CA can be McAfee® ePolicy Orchestrator (McAfee ePO) server.



Architecture diagram

• **ePO Server**: The ePO server installs and configures the McAfee® Agent and McAfee EIA settings on the managed hosts. The server is used to exchange the certificates that will be used to authenticate and secure McAfee EIA communication with the NTBA Appliance.

• **McAfee EIA** : These are endpoints that have the McAfee EIA installed on them. They provide the executable information about all executables to the NTBA Appliance. Based on dynamic analysis, if data files like doc and pdf are malicious, EIA provides file information like malware name and artifacts to NTBA.

• **NTBA Appliance**: The McAfee EIA connects to the NTBA Appliance and sends the executable information to the NTBA Appliance. The IPS Sensor/router, if configured, sends NetFlows to the NTBA Appliance. The NTBA Appliance also responds to the Manager queries for monitors/dashboards data and also for endpoint intelligence information for existing NTBA and IPS alerts.

• **IPS Sensors/Routers**: The NetFlow data that come from the IPS Sensor is correlated with the executable information coming from the McAfee EIA. For the NTBA Appliance to receive NetFlows, you must configure the IPS Sensor/router as an exporter (optional).

• **McAfee Global Threat Intelligence**: McAfee EIA gets the GTI information via the NTBA Appliance and computes the malware confidence for an executable along with its own malware indicators.

• **Manager**: The Manager maintains the allowed and blocked hashes that can be leveraged by all devices configured on the Manager for reporting and blocking purposes. The Manager pushes all the imported hashes to all the available NTBA Appliances and the IPS Sensors.

Benefits

The benefits of McAfee EIA are as follows:

- Provides visibility into the executables used in the enterprise network
- · Provides file information for non-executables like doc and pdf files on an endpoint
- Provides characteristics of the executable such as the version, the endpoints where it was executed, the number of connections made, the applications invoked, and the events associated with it
- Provides reputation (malware confidence) for each executable and data file using its own malware indicators and dynamic analysis engine
- · Provides trust information for good and unknown executables
- Enables detection of unknown executables in the network that the administrator can classify as allowed or blocked, thereby creating an intelligent baseline for the network
- Provides the administrator the flexibility to enable auto-classification of known good executables as allowed and known bad executables as blocked
- Integrates with the IPS Sensor's **Allow and Block Lists** functionality to prevent further spread of malware in the network
- Provides correlation between the **Application Identification** feature provided by the IPS Sensor with the executable information for every flow
- Correlates McAfee EIA executable information with analysis from other network detections such as ATD and NTBA.

How integration with McAfee EIA works

This section provides the high-level steps to integrate NTBA Appliance with McAfee EIA.

Task

- 1. Set up McAfee Agent with ePolicy Orchestrator: Deploy McAfee Agent extension and McAfee Agent package to the ePolicy Orchestrator server. Skip this step if you have deployed McAfee Agent version 4.8 or higher.
- 2. Set up McAfee EIA with ePolicy Orchestrator: Deploy the Endpoint Intelligence Management extension and McAfee EIA package to the ePolicy Orchestrator server. Assign policy to managed systems for McAfee EIA to communicate with the NTBA Appliance.
- 3. Enable EIA integration on the Manager: Establish connections between the NTBA appliance and the managed host systems with the McAfee EIA by enabling EIA integration at the **Global** level or the **Device** level on the Manager. The **Auto-Classification Settings** are available only at the **Global** level.

🗹 Note

Maximum endpoint connections supported on the NTBA Appliance is 12000.

- 4. Work with allow and block lists: You can either enable the auto-classification settings or manually change the executable classification. The manually classified values of the executable hashes are added to the allowed/blocked hashes that the administrator maintains.
- 5. **Configure NTBA policies for McAfee EIA alerts**: There are seven attack definitions for the NTBA policies. Based on which of the alerts you want to see, you can configure policies to raise only those EIA alerts.
- View executables running on endpoints: You can view all the executables running on your internal endpoints that have made network calls on the Endpoint Executables page. The top endpoint executables are displayed in the Top Endpoint Executables monitor on the Home Dashboard page.
- 7. **Analyze executable behavior**: Even with auto-classification settings enabled, there might be instances where the executable classification is not justified with its behavior. In such cases, you might want to investigate these executables and accordingly change the executable classification as allowed or blocked so they appear with the modified value next time. The changes are updated to the allowed and blocked hashes maintained by the Manager. You can also generate reports to see more details on the top 10 endpoint executables and endpoint executable connections.

🗹 Note

Quarantine of endpoints is not supported.

Setting up McAfee EIA integration

McAfee EIA can be installed on ePO-managed endpoints. This section explains how you can deploy McAfee Agent and McAfee EIA and configure the agents to send the executable information to the NTBA Appliance in the ePolicy Orchestrator console. It also explains how to enable McAfee EIA integration on the Manager.

Verify system requirements

Make sure your NTBA, McAfee ePO, and managed systems meet the requirements.

- McAfee ePO server must be at version 5.10.0
- McAfee Agent must be at version 5.6 or later
- McAfee® Endpoint Intelligence Manager (McAfee EIM) extension must be at version 3.2.2
- McAfee EIA must be at version 3.2.x
- McAfee Network Security Manager (Manager) must be at version 10.1.7.35 or later or 9.1.7.83 or later
- McAfee Network Threat Behavior Analysis Appliance (NTBA Appliance) must be at version 9.1.3.12 or later

🗹 Note

McAfee recommends you upgrade McAfee EIA to version 3.2.2.

McAfee EIA 3.2.2 runs on these Microsoft operating systems:

- Windows 10 20H1 (64-bit)
- Windows 10 RS5 (64-bit)
- Windows 10 RS4 (64-bit)
- Windows 10 R2 (64-bit)
- Windows Server 2019 Standard
- Windows Server 2016 Standard
- Windows Server 2012 R2 (64-bit) Standard
- Windows Server 2012 (64-bit) Standard

Setting up McAfee Agent with ePolicy Orchestrator server

Install McAfee Agent extension, upload McAfee Agent package, and deploy McAfee Agent on managed systems.

Download McAfee Agent and the extension package

Before you begin

Locate your grant number.

Task

- 1. In a web browser, go to https://www.mcafee.com/enterprise/en-us/downloads/my-products.html.
- 2. Enter your grant number, then go to the appropriate product and version.
- Download the McAfee Agent extension, MA-WIN x.y.z Build <abcd> Package <#y> (ENU-LICENSED-RELEASE), and the agent packages to the system containing the McAfee ePO server.
 For more information, see the specific version of *McAfee Agent Product Guide*.

Install McAfee Agent extension

Task

- 1. From the ePolicy Orchestrator console, click 📃.
- 2. Select **Software** \rightarrow **Extensions**.

Navigating to software extensions on ePO console

	🗂 McAfee	Dashboards	System Tree 0	Queries & Repo	orts Policy Catalog	Security Resources	▲ ▲ ~	
Software Extei	nsions Install E	Extension						
Extensions								
Search	×	Search					×	
✓ McAfee								
Commo	on Catalog	Name:	dxl_help	Status:	Installed	Modules:	Remove	
Endpoir	nt Security	Version:	4.1.0.012 Requires:		Core Modules 3.0	Core Modules 3.0		
Endpoir	nt Upgrade Assistant	13, 2018 1	admin - November 13, 2018 10:37:57	Details:				
ePolicy	Orchestrator		PM PST					
Help C	ontent							
Host In	trusion Prevention	Name:	eti help	Status:	Installed	Modules:	Remove	
McAfee	Agent	Version:	10.2.0.030	30 Requires:	equires:			
McAfee	Client Proxy	Installed by:	admin - November 13, 2018 11:40:57		5.1.1			
McAfee	DXL		PM PST	Details:				
McAfee	Server Deployment							
McAfee	TIE Server							
Networ	k Security Platform	Name:	hip_800_help	Status:	Installed	Modules:	Remove	
Product	Improvement Program	Version: Installed by:	800.975 admin - October 30	Requires:	Core Modules 2.0			
Server			2018 7:14:27 AM	Details:				
Shared	Components		וטא					
✓ Third Par	rty	-						
1								

3. At the top of the **Extensions** pane on the left side of the **Extensions** page, click **Install Extension**.

Installing McAfee Agentextension





- Browse to the MA-WIN x.y.z Build <abcd> Package <#y> (ENU-LICENSED-RELEASE) file you downloaded from the McAfee downloads page.
- 5. Click **Open** to select the file, then click **OK** to proceed with the selection.
- 6. Click **OK** to install the extension.

Upload McAfee Agent package

Upload the McAfee Agent package to the ePolicy Orchestrator server. This package contains the files necessary to install McAfee Agent on managed systems.

Task

- 1. From the ePolicy Orchestrator console, click 🔳
- 2. Select **Software** \rightarrow **Master Repository**.

Master Repository in ePO console

≡ 🗂 McAfee	Dashboards	System Tree	Queries & Repor	ts Policy Catalog	Security Resources	✓ ▲ ▲ ✓
Software						
Master Repository	Check In Pack	age Pull Now				
Packages in Master Repository						Hide Filter
Preset: Quick find:		Apply <u>Clear</u>	Show selected	rows		
Name ~	Туре	Version	Minor Version	Check-In Date	Distribution Type	Branch
DAT	DAT	9071.0000		11/9/18 4:29:13 PM IST		Current
DXL Platform	Install	4.1.1	123	11/14/18 12:07:52 PM IST	Licensed	Current
Endpoint Intelligence Agent	Install	3.0.0	104	12/3/18 12:42:42 PM IST	Licensed	Previous
Endpoint Intelligence Agent	Install	3.0.0	104	11/4/18 3:29:51 PM IST	Licensed	Current
Endpoint Upgrade Assistant	Install	2.1.0	53	10/26/18 1:08:19 PM IST	Licensed	Evaluation
Endpoint Upgrade Assistant	Install	2.1.0	53	10/26/18 1:08:18 PM IST	Licensed	Previous
Endpoint Upgrade Assistant	Install	2.1.0	53	10/26/18 1:08:16 PM IST	Licensed	Current
Engine Engine	Engine	6000.8403	8403	10/26/18 3:27:34 PM IST	Licensed	Current
ePO Agent Key Updater	Plug-in	5.5.1	342	10/26/18 1:08:26 PM IST	Licensed	Current
Host Intrusion Prevention	Install	8.0.0	4789	11/2/18 2:53:36 PM IST	Licensed	Current
Host Intrusion Prevention Content	DAT	8.0.0	8701	10/31/18 3:27:31 PM IST		Current
Linux Engine	Engine	6000.8403	8403	10/26/18 3:27:43 PM IST	Licensed	Current
Mac Engine	Engine	6000.8403	8403	10/26/18 3:27:54 PM IST	Licensed	Current
4						-
Actions > 26 items	II Create Depl	oyment Task				

3. Click Check In Package.

The Check In Package page is displayed.

4. From the **Package type** list, select **Product or Update (.ZIP)**, then browse and select the McAfee Agent package file.

Uploading McAfee Agent package

≡	🗂 McAfee	Dashboards	System Tree	Queries & Reports	Policy Catalog	Security Resources	Server Settings		^ ~
Software Mas	^{re} ster Repository	,							
Check In	n Package	1 Package				2 Package Option	s		
What pac	kage are you checking in?								
Note: If a the replic	distributed repositories are set u ation task before checking in the	p to replicate only se e package.	elected packages, yo	ur newly check-in package w	ill be replicated by defa	ult. To avoid replicating a new	ly checked-in package, deselect it from each distril	outed repositor	y or disable
Package	type:	Product or Up Extra.DAT Super.DAT	date (.zip)						
File path	1:	Choose File	i	.zip					
								Back Nex	ct Cancel

- 5. Click Next.
- 6. Click Save.

The package is added to the Master Repository.

Deploy McAfee Agent

Deploy McAfee Agent to managed systems.

Task

- 1. From the ePolicy Orchestrator console, click
- 2. Select Menu \rightarrow Client Tasks \rightarrow Client Task Catalog.

Client Task Dialog in ePO console

≡ 🔰 McAfee	Dashboards Syste	em Tree Queries & Repo	orts Policy Catalog	Security Resources	▲ ▲~
Recent Pages	Search			^	
Client Task Catalog				-	
Master Repository	Reporting	Systems	Policy		
Product Deployment	Dashboards	System Tree	Policy Catalog		
Server Settings	Security Resources	Tag Catalog	Common Catalog		
System Tree	Queries & Reports	Systems	Policy Assignments	Assignments	
	Audit Log	TIE Reputations	Policy Assignment Rules		*
	Threat Event Log	Data Exchange Layer F	Policy History		
	Firewall Client Rules		Policy Comparison		
	Host IPS 8.0		Firewall Catalog		
	Exploit Prevention Eve		Host IPS Catalog		
	Threat Intelligence Eve				
	Client Tasks	Software	Automation		
	Client Task Catalog	Endpoint Upgrade Assi	Server Task Log		
	Client Task Assignments	Getting Started	Server Tasks		
	Client Task Comparison	Product Deployment	Automatic Responses		
		Software Catalog	Issues		
		Master Repository	Server Deployment		
		Distributed Repositories	Host IPS Policy Migrati		
		Extensions			
		Licensing			
	User Management	Configuration		_	
	Users	Server Settings			
	Contacts	Personal Settings			
	Permission Sets	Registered Servers			
		Agent Handlers			
		Certificate Manager			
		Registered Executables			
		MCP Help Desk			

- 3. Click New Task.
- 4. From the Task Types list, select Product Deployment.
- 5. Click **OK**.

The Client Task Catalog : New Task - McAfee Agent: Product Deployment page appears.

Selecting McAfee Agent to deploy

≡ 🔰 McAfee	Dashboards System Tree Queries & Reports	Policy Catalog Security Resources	Server Settings	▲ ▲ ~
Client Tasks Client Task Catalog	5			
Client Task Catalog : New Task - McA	e Agent: Product Deployment			
Task Name	New Task			
Description				
Target platforms:	AIX CHIAN AVES Security Appliances HP-UX HP-UX Houx Hac Solaris Solaris Wrind Yver Linux Wrindows Wind Solaris Wrind Yver Linux			
Products and components:	McAfee Agent for Windows 5.5.1.342	all 💙 Language: English 💙 Branch: Current 💙		
"Postpone Deployment" dialog box (Windows systems only):	Allow end users to postpone this deployment Maximum number of postpones allowed: 1 Option to postpone expires after (seconds): 20 Display this text:			
				Save Cancel

- 6. In the **Task Name** field, enter a name for the task.
- 7. From the **Products and components** menu, select **McAfee Agent <x.y>**.

- 8. Click Save.
- 9. Run the task.
 - a. Click the System Tree icon. The Systems tab appears.

= 🗶 McAfee	Dashboards System Tree Quer	ies & Reports Policy Catalog	Security Resources Serv	ver Settings		▲ ▲ ~
Systems System Tree	v Systems New Subgroups					
System Tree	Systems Assigned Policies Assigned Client	Tasks Group Details Agent Deploy	ment			
V My Organization V Lost and Found	Preset: Custom: This Group and All Subgroups V None	Quick find:	Apply <u>Clear</u>	Show selected rows		
HIPS	System Name V	Managed State	Tags	IP address	User Name	Last Communication
tie.com	CLDBGQALABS0046	Managed	HIPS_Rahul, Server	10.254.37.65	cloudadmin	12/4/18 4:40:38 PM IST
WORKGROUP	II NS5100	Managed	Workstation	10.213.2.101	admin	11/19/18 10:13:03 AM IST
	iiitie-22	Managed	DXLBROKER, Server, TIESERVER	10.213.169.113	root	12/4/18 4:21:45 PM IST
	WIN-68S2UEKS8FE	Managed	Server	10.213.169.104	Administrator	12/4/18 4:58:19 PM IST
	WIN-BPNFV0881V0	Managed	Server	10.213.172.183	Administrator	12/4/18 4:22:47 PM IST
		Deploy Agents				
		Deprovision Agent				
		Edit Policies on a Single System				
		Edit Tasks on a Single System				
	Changes Columns	Run Client Task Now				
	Create Time Record Recovered (Uset INC 8-0)	Set Description				
	Create Time-Based Password (Host IPS 8.0)	Set Policy & Inheritance				
	Export Table	Show Agent Log				
	System Health Indicator	Show Client Events				
	🖳 Тад	Show Threat Events				
	E DXL	Transfer Systems				
	😳 те	Update Now				
	C Agent	Wake Up Agents				· · · · · · · · · · · · · · · · · · ·
	Directory Management		-			•
System Tree Actions ~	Actions > 1 of 5 selected	lake Up Agents 🚦 Ping				

Selecting systems to deploy McAfee Agent

- b. Select the systems to deploy McAfee Agent.
- c. Select Actions \rightarrow Agent \rightarrow Run Client Task now.
- d. In the Task Type column, select Product Deployment, and in the Task Name column, select the task you created.
- e. Click Run Task Now.

For more information, see the specific version of *McAfee Agent Product Guide*.

Setting up McAfee EIA with ePolicy Orchestrator server

Install the Endpoint Intelligence Management extension, upload the Endpoint Intelligence Agent package, and deploy McAfee EIA on managed systems.

Download McAfee EIA and the extension package

Download McAfee EIA package and the Endpoint Intelligence Management extension to the ePolicy Orchestrator server.

Before you begin

Locate your grant number.

Task

- 1. In a web browser, go to https://www.mcafee.com/enterprise/en-us/downloads/my-products.html.
- 2. Enter your grant number, then go to the appropriate product and version.
- 3. Download the Endpoint Intelligence Management extension file, **eim_epo_extension_<version>.zip**.
- 4. Download the Endpoint Intelligence Agent file, **eia_epo_deploy_<version>.zip**.

Install the Endpoint Intelligence Management extension

Install the Endpoint Intelligence Management extension from your download location to your ePolicy Orchestrator server.

Task

1. From the ePolicy Orchestrator console, select $Menu \rightarrow Software \rightarrow Extensions$.

Navigating to software extensions on ePO console

≡	🕽 McAfee	Dashboards	System Tree	Queries & Report	s Policy Catalog	Security Resources	▲ ▲ ×
Software Exte	ensions	xtension					
Extensio	ns						
Search	×	Search					×
✓ McAfe	e						
Comr	non Catalog	Name:	dxl_help	Status:	Installed	Modules:	Remove
Endp	oint Security	Version: Installed by:	4.1.0.012 admin - November	Requires:	Core Modules 3.0		
Endp	oint Upgrade Assistant	inotaneu byi	13, 2018 10:37:57	Details:			
ePolic	cy Orchestrator		PM PS1				
Help	Content						
Host	Intrusion Prevention	Name:	eti help	Status	Installed	Modules:	Remove
McAfe	ee Agent	Version:	10.2.0.030	Requires:	- Caro Madulas		
McAfe	ee Client Proxy	Installed by:	admin - November 13. 2018 11:40:57		5.1.1		
McAfe	ee DXL		PM PST	Details:			
McAfe	ee Server Deployment						
McAfe	ee TIE Server						
Netw	ork Security Platform	Name:	hip_800_help	Status:	Installed	Modules:	Remove
Produ	uct Improvement Program	Version:	800.975 admin = October 20	Requires:	Core Modules 2.0		
Serve	51.	installed by.	2018 7:14:27 AM	Details:			
Share	ed Components		וטי				
✓ Third I	Party	·					

2. At the bottom of the Extensions pane on the left side of the Extensions page, click Install Extension.

Installing Endpoint Intelligence Management extension

Menu * O Durbbeurds	Svenam Tree	💰 Quenes à Regar	n 🛃 mai	n Catalog 🔄 Erfenn	ann 🔎 Sarow-Battings	I Harter Reporters	ing on C	U McAfee
Extensions								
fatermente: 1						_		
Internet. 9 Mollow atrylery Orchestrator High Carterot Mollow Agant Mollow Frendt Enterprine	Hamas Manutana Installed by:	aPD Garned Configuration B 4.4.0.000 points - Jakuary 6, 2014 12244 34 Art PCT	Aladası Roşerani	Installed - Commerciaerite 3.1 - Commite 5.1 - Commite 5.1 - Store 7.1 - Store 7.1 - Store 7.1	Haddan af O Gurani Caringin	Ren J.	Anne.	farmer.
Modifies Security The Historical Products Engineering Hinggram Real Tome Server Universe Companients Universe Companients		Choose File	ein_epa_ext	a initali rension_220.zp				
• Dead Parts • Designed	Nazzer Marstane Installed by:	14900 200 00.5 00 00 miletite 123-004 00					Runng	Barrans
					OK Cancel			
	tranne: Marstane Bestalled Dys	4PO Literine Management 3.1.0.508 edite - January 6. 3018 12-04 49 AM DET	Naturi Response	Installed • Controle 51 • Cont Modular 51 • ePC Cont 51	Modulaer (175) Liverine Manager		Anna '	fature
Contraction of the local division of the loc	Hanne Marstane Destalled by:	etti Userang Trifferent S.a. 6. 100 advis – January 6, 2014 19. 19. 19. 19. 19.	Station: Requires	Enstabled - Gree Missides 3.3 - alfo Gaie 5.1 - Scheduler 5.3	Modulest of O.Linearing Dottler	11 1	Anna .	Lanara

- 3. Browse to the **eim_epo_extension_<version>.zip** file you downloaded from the McAfee downloads page.
- 4. Click **Open** to select the file, then click **OK** to proceed with the selection.
- 5. Click **OK** to install the extension.

Upload McAfee EIA package

Upload McAfee EIA package to the ePolicy Orchestrator server. This package contains the files necessary to install McAfee EIA on managed systems.

Task

1. From the ePolicy Orchestrator console, select **Menu** \rightarrow **Software** \rightarrow **Master Repository**.

Master Repository in ePO console

Ξ	McAfee	Dashboards	System Tree	Queries & Report	s Policy Catalog	Security Resources	~	A A
so N	Master Repository	Check In Pack	cage Pull Now					
Pac	kages in Master Repository							Hide Fi
Pr A	eset: Quick find:		Apply <u>Clear</u>	Show selected r	ows			
	Name 🗸	Туре	Version	Minor Version	Check-In Date	Distribution Type		Branch
	DAT	DAT	9071.0000		11/9/18 4:29:13 PM IST			Current
	DXL Platform	Install	4.1.1	123	11/14/18 12:07:52 PM IST	Licensed		Current
	Endpoint Intelligence Agent	Install	3.0.0	104	12/3/18 12:42:42 PM IST	Licensed		Previous
	Endpoint Intelligence Agent	Install	3.0.0	104	11/4/18 3:29:51 PM IST	Licensed		Current
	Endpoint Upgrade Assistant	Install	2.1.0	53	10/26/18 1:08:19 PM IST	Licensed		Evaluation
	Endpoint Upgrade Assistant	Install	2.1.0	53	10/26/18 1:08:18 PM IST	Licensed		Previous
	Endpoint Upgrade Assistant	Install	2.1.0	53	10/26/18 1:08:16 PM IST	Licensed		Current
	Engine	Engine	6000.8403	8403	10/26/18 3:27:34 PM IST	Licensed		Current
	ePO Agent Key Updater	Plug-in	5.5.1	342	10/26/18 1:08:26 PM IST	Licensed		Current
	Host Intrusion Prevention	Install	8.0.0	4789	11/2/18 2:53:36 PM IST	Licensed		Current
	Host Intrusion Prevention Content	DAT	8.0.0	8701	10/31/18 3:27:31 PM IST			Current
	Linux Engine	Engine	6000.8403	8403	10/26/18 3:27:43 PM IST	Licensed		Current
	Mac Engine	Engine	6000.8403	8403	10/26/18 3:27:54 PM IST	Licensed		Current
A	ctions ✓ 26 items	II Create Dep	loyment Task				-	

2. Click Check In Package.

The **Check In Package** page is displayed.

3. From the **Package Type** list, select **Product or Update (.ZIP)**, then browse and select **ePO_Deploy.zip**.

Menn * O Castavarta	De Treten Tere	E Committees	Hatter Rep	untary 👷 Server Se	mage 🚺 Pulley Catalog	• Log 077 🕥	W McAfee
Extensions							
Terresona .			_				
VEABle Affaire Artailes Ordinaributur Incip Contarie Veable Agent Notice Agent	Martury Merenany Destablish by:	arto manet Carrigorenas 3.1.5.00 arres - Januari A. Jillio Luna Sa est res	Status: Reported	Installed - Gammar Sweets 3.3 - Conrols 3.1 - Conrols 1.1 - Self Modeler 3.1 - allO Exists.2 - allO Product	Madalan afte daniat Configuration	Journa	Ascess.
NATes Enerty for Hannet Fraduit Engranment Pragae East Time Sarrer States Components States Components		Select an exten	aion (2IP) Ale 6 ePO_Deploy.	o installi Zip			
v New Party 2 Newpool	Name Version Tradalist by:	are ho Names arrest				. Averag	Ration .
					CH Cancel		
	Name Termen Linstalied by:	490 Lisense Hanagament 5.1.0.001 atmis - Janosty 6. JB14 5200-49 AM RET	Atafaas Responses Owtailes	Installad - Converte 8.5 - Colo Modellin 5.5 - 4FO Colo 3.3	Mudulari e PO (zanije Marriponari Metid	Anne -	Carriers.
	Numer Termen Installed by:	utanung Leatenan 5.3-0-502 attas - January 6., 2014 (2015-07, 40-002	Status: Regiereur	tookalled - Core Modeles 7.1. - artO faxe 7.1 - Artistute 7.1	walalen altö Usersny/Ettilament	Annua -	Retries.

Uploading package

- 4. Click Next.
- 5. Click Save.

The package is added to the **Master Repository**.

Deploy McAfee EIA

Deploy McAfee EIA to managed systems.

Task

- 1. From the ePolicy Orchestrator console, click
- 2. Select Client Task \rightarrow Client Task Catalog.
- 3. Click New Task.
- 4. From the Task Types list, select Product Deployment.
- 5. Click **OK**.

The Client Task Catalog: New Task Endpoint Intelligence Agent: Product Deployment page appears.

Selecting Endpoint Intelligence Agent to deploy

≡ 🗂 McAfee	Dashboards System Tree Queries & Reports Policy Catalog Security Resources Server Settings		≗ ~
Client Tasks Client Task Catalog	7		
Client Task Catalog : New Task - McAf	ee Agent: Product Deployment		
Task Name	New Task		
Description			
Target platforms:	IX Email and Web Security Appliances HP-UX Lnux Mode Security Appliances Web Security Appliances		
Products and components:	Endpoint Intelligence Agent 3.0.0.104 V Action: Install V Language Reutral V Branch: Current V = +		
"Postpone Deployment" dialog box (Windows systems only):	Allow and users to postpone this deployment Maximum number of postpones allowed: Option to postpone expires after (seconds): 20 Display this text:		
		Sav	e Cancel

- 6. In the **Task Name** field, enter a name for the task.
- 7. From the Products and components menu, select Endpoint Intelligence Agent <version>.
- 8. Click Save.
- 9. Run the task.
 - a. Click the System Tree icon. The Systems tab appears.

Selecting systems to deploy McAfee Agent

≡ 🔀 McAfee	Dashboards System Tree Quer	ies & Reports Policy Catalog	Security Resources Serv	ver Settings		▲ ▲ ~
System Tree New	v Systems New Subgroups					
System Tree	Systems Assigned Policies Assigned Client	Tasks Group Details Agent Deploy	ment			
V My Organization	Preset: Custom:	Quick find:		Show selected rows		
	This Group and All Subgroups V	×	Apply Otean			
HIPS	System Name V	Managed State	Tags	IP address	User Name	Last Communication
tie.com	CLDBGQALABS0046	Managed	HIPS_Rahul, Server	10.254.37.65	cloudadmin	12/4/18 4:40:38 PM IST
WORKGROUP	NS5100	Managed	Workstation	10.213.2.101	admin	11/19/18 10:13:03 AM IST
	iiitie-22	Managed	DXLBROKER, Server, TIESERVER	10.213.169.113	root	12/4/18 4:21:45 PM IST
	WIN-68S2UEKS8FE	Managed	Server	10.213.169.104	Administrator	12/4/18 4:58:19 PM IST
	WIN-BPNFV0881V0	Managed	Server	10.213.172.183	Administrator	12/4/18 4:22:47 PM IST
		Deploy Agents				
		Deprovision Agent				
		Edit Policies on a Single System				
		Edit Tasks on a Single System				
	[🖳 Run Client Task Now				
	Choose Columns	Set Description				
	Create Time-Based Password (Host IP5 8.0)	Set Policy & Inheritance				
	Export Table					
	System Health Indicator	Show Agent Log				
	🖳 тад	Show Client Events				
	E DXL	Show Threat Events				
	Бо тте	Iransfer Systems				
	agent	See Up Agents				
	Directory Management		-			· · · · ·
System Tree Actions ~	Actions V 1 of 5 selected	ake Up Agents 👯 Ping				

- b. Select the systems to deploy McAfee EIA.
- c. Select $\textbf{Actions} \rightarrow \textbf{Agent} \rightarrow \textbf{Run Client Task now}.$
- d. In the Task Type column, select Product Deployment, and in the Task Name column, select the task you created.
- e. Click Run Task Now.

For more information, see the Endpoint Intelligence Agent Product Guide.

Create and assign policy to managed systems

For McAfee EIA to communicate with the NTBA Appliance, policy must be applied to managed systems.

Task

- 1. From the ePolicy Orchestrator console, select **Policy Catalog**:
 - a. Select **Product** as *Endpoint Intelligence Agent <version>.*
 - b. Select Category as EIA Settings.

Policy Catalog ePolicy Orchestrator page

	n Tree Queries & Reports Policy Catalo	g Security Resources Server Settings		▲ ▲ ~
Policy Catalog				
< Products	< Endpoint Intelligence Agent 2.6.3	3		New Policy 🗸
Search	Search			
Endpoint Intelligence Agent 2.6.3	✓ EIA Settings			
Endpoint Security Common	Name	Rule Assignments	Assigned To	Actions
Endpoint Security Firewall	McAfee Default	None	Global Root	View
Endpoint Security Threat Intelligence	My Default	None	My Organization	Edit
Endpoint Security Threat Prevention	ing benadic			
Endpoint Security Web Control				
Host Intrusion Prevention 8.0				
McAfee Agent				
McAfee Client Proxy 2.3.5				
McAfee DXL Broker Management 4.1.1				
McAfee DXL Client 4.1.1				
McAfee Threat Intelligence Exchange Server Management				
Product Improvement Program				

- 2. Click the **My Default** policy to edit it.
 - a. Select the **Device Type** as **NTBA** from the drop-down list.

General Settings tab

≡ 🗂 McAfee	Dashboards System Tree	Queries & Reports	Policy Catalog	Security Resources	Server Settings	* ~
Policy Policy Catalog 1	systems currently have policy "	My Default".				
Endpoint Intelligence Agent 2.6.3:Er	adpoint Intelligence > EIA Settings >	My Default				
Primary Gateway	NTBA V This gateway will be used for 2.3.x an	d 2.4.2 devices				
Routes	Add routes of different subnets Firewall NTBA I Add Dulate Clear AD	×				
Log Settings	Log level Error V Rotate log files 10 times Max log file size 10 MB					
Gateway Connection Settings	Retry Interval 1000 Recovery Interval 3000 Backoff Maximum Interval 10 Backoff Minimum Interval 5 Backoff Percentage 500 DTLS Keep Alive 20 s Session Expiry 60	milliseconds milliseconds milliseconds milliseconds econds minutes				
Real Protect Settings	Enable Real-Protect integration of Type the executable name to be analy cond-exe outlook.exe explore.exe chrome.exe chrome.exe fireflox.exe	Rh Endpoint Intelligence Agen zed by Real Protect	4 Add Executable semove Executable			
Other Settings	Ignore virtual traffic Dashboard Update Interval 6	hours				

- b. Enter the source IP address.
- c. Enter the subnet mask.
- d. Enter the device IP address. The device IP address you specify here must be the same as the NTBA Management IP address running on your Manager.

- e. Enter the port number. Select the NTBA listening port for McAfee EIA connections and make sure that this port is not blocked by Firewall rules. Default port used on NTBA is 9008.
- f. Click Add Route and click Save.
- On the System Tree tab, click Actions → Agent → Wake Up Agents for the new configurations to take effect. By default, the policy is applied to all groups/subgroups.

Wake Up Agents option on ePolicy Orchestrator console

≡ 🗂 McAfee	Dashboards System Tree Queri	es & Reports Policy Catalog	Security Resources Server Se	ettings		▲ ▲ ~
Systems						
System Tree	Systems New Subgroups					
System Tree	Systems Assigned Policies Assigned Client	Tasks Group Details Agent Deployr	nent			
	Preset: Custom:	Quick find:		Show selected rows		
> Lost and Found	This Group and All Subgroups V	Y [Apply <u>Clear</u>			
	System Name V	Managed State	Tags	IP address	User Name	Last Communication
	CLDBGQALABS0046	Managed	HIPS_Rahul, Server		cloudadmin	12/5/18 11:40:37 AM IST
	VS5100	Managed	Workstation		admin	11/19/18 10:13:03 AM IST
	tie-22	Managed	DXLBROKER, Server, TIESERVER		root	12/5/18 11:21:43 AM IST
	WIN-68S2UEKS8FE	Managed	Server		Administrator	12/5/18 10:58:18 AM IST
	WIN-BPNFV0881V0	Managed	Server		Administrator	12/5/18 11:22:46 AM IST
		Deploy Agents				
		Edit Policies on a Single System				
		Edit Tasks on a Single System				
	- during the second	😳 Run Client Task Now				
	Choose Columns	Set Description				
	 Create Time-Based Password (Host IPS 8.0) 	Set Policy & Inheritance				
	Export Table	Show Agent Log				
	System Health Indicator	Show Client Events				
	Tag 🕨 🕨	Show Threat Events				
	E DXL	Transfer Systems				
	Sig the Decision of the Decisi	Dig Update Now				
	C Agent	🐑 🔛 Wake Up Agents				
	Directory Management					•
System Tree Actions ~	Actions 🗸 2 of 5 selected	ke Up Agents 🔠 Ping				

For more information, see the Endpoint Intelligence Agent Product Guide.

Enabling McAfee EIA integration on the Manager

🗹 Note

You must have deployed McAfee Agent and McAfee EIA and configured the agents to send their results to NTBA in the ePolicy Orchestrator console as explained in the preceding sections.

You can enable McAfee EIA integration with the NTBA Appliance at the Global level and at the Device level.

When you enable McAfee EIA integration at the **Global** level, the settings are inherited by its child domain nodes as the **Inherit Settings** checkbox is enabled by default.

When you enable McAfee EIA integration at the **Device** level, you can apply the configuration settings only to that particular NTBA Appliance.

Enable McAfee EIA integration globally

By default, the **Inherit Settings** checkbox is enabled, so settings done at the global level are inherited by all NTBA Appliances in this domain (and child admin domains). The **Auto-Classification Settings** options are available only at the **Global** level and are inherited by all devices.

Task

1. Select Devices → <Admin Domain Name> → Global → NTBA Device Settings → Device Settings → Setup → EIA Integration.

The **EIA Integration** page is displayed.

🗹 Note

The settings done at the parent admin domain level are inherited by default by its child domains.

2. Select the **Enable EIA Integration** checkbox to enable the feature.

Enable EIA Integration page globally

/My Company > NTBA_doc_82 > Setup > EIA Int	tegration	
•		
Inherit Settings?		
Enable EIA Integration?		
Agent Connection Settings		
NTBA Listening Port (for agent connections):	9008	
View Agent Connectivity		
ePO Settings		
ePO Server Name or IP Address :	10.10.	l
ePO Server Port:	8443	
ePO Username:	admin	
ePO Password:		
Auto-Classification Settings		
Note: The below settings are configurable	at the root admin domain or	nly.
Automatically Allow Executables Signed by a Trusted Certificate Authority?		
Automatically Allow Executables Found on the GTI Allow List?		
Automatically Block Executables Found on the GTI Block List?		
Automatically Block Executables that Dynamic Analysis Indicates to be Malware?		
Update ePO Certificate		Save

Field descriptions

Field	Description
Agent Connection Settings	The NTBA Listening Port is the port on which the NTBA Appliance listens for incoming connections from endpoints running McAfee EIA. It is pre-populated with the value used by default by the agents. You can edit this field by specifying a port number between 0 and 65535.

Field	Description
	At a device level, click View Agent Connectivity to verify EIA connectivity with the configured NTBA device.
ePO Settings	 This section defines the parameters used to connect with the ePO server and exchange the certificates used to authenticate and secure agent communication with the NTBA Appliance. ePO Server IP Address: Displays the IP address of the ePO server ePO Server Port: This field is pre-populated with the value used by default by the ePO server. You can edit this field by specifying a port number between 0 and 65535. ePO User Name: Type the user name to log on to the ePO console.
	Note: ePO user must enable the Allow Download of Certificates present in the Endpoint Intelligence category of user permissions.
	 ePO Password: Type the password to log on to the ePO console. Open ePO Console: Click to configure the ePO settings from here.
Auto- Classification	This section provides options to automatically allow and block executables in which McAfee is confident of their posture. It provides the following options:
Settings	 Automatically Allow Executables Signed by a Trusted Certificate Authority: If the executable is found signed by a trusted CA or if there is a signer name, it is allowed. This is enabled by default. Automatically Allow Executables Found on the GTI Allow List: If GTI file reputation is clean, it is allowed. This is enabled by default. Automatically Block Executables Found on the GTI Block List: If GTI file reputation is malicious, it is blocked. This is disabled by default. Automatically Block Executables Found on the GTI Block List: If GTI file reputation is malicious, it is blocked. This is disabled by default. Automatically Block Executables that Dynamic Analysis Indicates to be Malware: If dynamic analysis reports a file as malicious, it is blocked. This is disabled by default.
Update ePO Certificate	Click this button if there have been changes in the certificate on the ePO side to automatically update all NTBA Appliances in the admin domain node (and devices in the child admin node that are inheriting them).

To check if McAfee EIA service is running on the NTBA Appliance, run the show endpointintelligence summary CLI command.

🗹 Note

ePO user must have the option 'Allow Download of Certificates' enabled in the Endpoint Intelligence category of user permissions.

Enable McAfee EIA integration per device

You can enable McAfee EIA integration for a particular device or domain at the Device level.

Task

1. Select Devices \rightarrow <Admin Domain Name> \rightarrow Devices \rightarrow <NTBA Appliance> \rightarrow Setup \rightarrow EIA Integration. The EIA Integration page is displayed.

Enabling McAfee EIA integration at Device level

•				
Inherit Settings?				
Enable EIA Integration?				
Agent Connection Settings				
NTBA Listening Port (for agent connections):	9008	I		
View Agent Connectivity				
ePO Settings				
ePO Server Name or IP Address :				
ePO Server Port:	8443			
ePO Username:	admin			
ePO Password:		l		
Auto-Classification Settings				
Note: The below settings are configurable	at the root admin domain or	aly.		
Automatically Allow Executables Signed by a Trusted Certificate Authority?				
Automatically Allow Executables Found on the GTI Allow List?				
Automatically Block Executables Found on the GTI Block List?				
Automatically Block Executables that Dynamic Analysis Indicates to be Malware?				
Update ePO Certificate		Save		

🗹 Note

If the **Inherit Settings** checkbox is selected (default), the settings from the Global level for the selected admin domain will be inherited by the device.

- 2. Deselect the **Inherit Settings** checkbox and select the **Enable EIA Integration** checkbox to configure settings for a particular device.
- 3. Follow the procedure as explained in Enable McAfee EIA integration globally to configure McAfee EIA at the device level.

Understanding executable classification

The Manager provides options to auto-classify or manually classify the executables. Executables that appear as unclassified can be allowed or blocked. The Manager pushes the updates in the allowed and blocked hashes to the NTBA Appliance every five minutes.

The executables are classified as the following:

- Allowed: Executables that are considered safe
- Blocked: Executables that are not considered safe or not allowed per corporate policy
- Unclassified: Executables that are yet to be classified

You can classify executables from any of the following:

• **Endpoint Baseline Generator**: When the Endpoint Baseline Generator tool is run on a computer, it scans the computer, calculates the heuristics for all the executable hashes on the system, and generates an XML file. This XML file contains information, such as file name, file size, hash type (MD5), and file hash.

McAfee recommends that you run the tool on a system that can be treated as a baseline computer profile for your organization. You can then use the import option in the Manager to append your list to the existing allow and block list in the Manager.

• Auto-Classification: You can configure Auto-Classification Settings at the Global level of the EIA Integration page to classify executables based on the following:

- If the executable is signed and trusted, it is allowed.
- If GTI file reputation is malicious, it is blocked.
- If GTI file reputation is clean, it is allowed.
- If dynamic analysis reports an executable or data file as malicious, it is blocked.

• Auto-classified blocked and allowed executables are added to the **Allowed and Blocked Hashes** tabs in **File Hashes** page.

🗹 Note

Make sure that GTI is reachable. This can be done by configuring the local DNS Server (or proxy) by selecting **Devices** \rightarrow **Admin Domain Name>** \rightarrow **Global** \rightarrow **Default Device Settings** \rightarrow **Common** \rightarrow **Name Resolution**. Enter the IP Address (IPv4 or IPv6) here.

• **Manual Classification**: You can also manually classify the executables from the Manager. Based on their overall malware confidence and their network behavior, you can classify them as allowed or blocked.

🗹 Note

Manual classification has the highest priority and takes precedence over auto-classification.

The following aspects are used to classify executables:

Executable classification

Manually allowed	Manually blocked	Digitally trusted	Dynamic analysis	Auto-GTI allowed	Auto-GTI blocked	Gets classified as
Yes	-	Yes or No	Any	Yes or No	Yes or No	Allowed
-	Yes	Yes or No	Any	Yes or No	Yes or No	Blocked
Not classified		Yes	Any	Yes or No	Yes or No	Allowed
Not classified		No	Malicious	Yes or No	Yes or No	Blocked
Not classified		No	Not malicious	Yes	No	Allowed
Not classified		No	Not malicious	No	Yes	Blocked
Scenario: A new executable is seen in your network						
-		Yes	Any	Unknown		Allowed
-		No	Malicious	Unknown		Blocked
-		No	Not malicious	Unknown		Unclassified

🗹 Note

A new executable is not known to McAfee GTI and an administrator cannot classify it until its behavior is analyzed. For the second occurrence, GTI discovers and computes reputation for an unclassified executable, and the NTBA classification may vary accordingly.

Working with allowed and blocked hashes

The Manager maintains a single list of allowed (good) and blocked (bad) hashes. Each list contains file hashes and executable names that can be leveraged by all devices configured on the Manager for reporting purpose.

Import of allowed and blocked hashes

You can use this page to import hashes into the allow and block list.

Supported file formats include XML and CSV. The XML format is used to import a list of hashes that have been exported from endpoints running McAfee EIA using the Endpoint Baseline Generator utility. The Manager exports the lists in CSV format, so CSV can be used to import previous exports. It also provides a straightforward way to create a list manually.

CSV file format

The file to be imported should be in the following CSV format:

<File name>,<File size>,<Hash type>,<File hash>,<Description>. For example:

Application.exe, 1024, MD5, 30a4edd18db6dd6aaa20e3da93c5f425, My description where:

- Application.exe is the file name. File name must be a string value and at least 1 character long.
- 1024 is the file size. File size must be an integer value and at least 1 character long. It is not currently used.
- *MD5* is the hash type. Hash type can only be MD5.
- 30a4edd18db6dd6aaa20e3da93c5f425 is the file hash. File hash must be a valid MD5 hash value.
- *My description* is the description. Description must be a string value and at least 1 character long.

If you are importing multiple files, each file has to be on a new line.

Once hashes are imported, the list of all available hashes is displayed. The Manager pushes all the imported hashes to all the available NTBA Appliances and the IPS Sensors. The auto-allowed and auto-blocked executable hashes are added to the Manager global list. The **Comment** column on the **Policy** \rightarrow **<Admin Domain Node>** \rightarrow **Intrusion Prevention** \rightarrow **Exceptions** \rightarrow **File Hashes** page provides details for the same.

🗹 Note

The Manager supports up to 99,000 hash entries (allowed and blocked combined).

Task

1. Select Policy \rightarrow <Admin Domain Node> \rightarrow Intrusion Prevention \rightarrow Exceptions \rightarrow File Hashes. The Allowed and Blocked Hashes tabs are displayed.

Note

You can also go to the **File Hashes** page by clicking the **Manage allow and block lists** link from the **Malware Files** page or the **Endpoint Executables** page.

2. Depending on the type of hashes you want to import, select the **Allowed Hashes** or the **Blocked Hashes** tab.

🔆 Tip

View **Comment** for auto-allowed and auto-blocked executables and decide to import the hashes.

3. Click Import.

The **Import** page is displayed.

Importing hashes into the allow list

Import from CSV			
0			
CSV File:		Browse	
		Import	

4. Browse to the location of the file and click **Import**. The list is populated.

🗹 Note

By default, the list is sorted in the ascending order of the file name. To sort it according to your choice, you can click any of the column name and select an option from the drop-down list.

5. You can append to the existing list by clicking the **Append** option, which is selected by default.

🗹 Note

For information about how to use the **Replace** option, see the section Remove or replace hashes from allow and block lists.

- 6. Use the **Search** option to locate an entry by the file hash, file name, or classifier.
- 7. You can consider adding a description in the **Comment** field as to why a file hash was allowed or blocked.

🗹 Note

The **Comment** field allows up to 250 characters.

Export of allowed and blocked hashes

If you want to export the hashes, you can go to the appropriate tab and click **Export Allowed** or **Export Block List**. The exported CSV file contains either allowed or blocked hashes based on the tab from where it is exported. You can use the exported file as source of import in another Manager.

🗹 Note

Currently, export of only CSV files is supported.

Task

1. Select Policy \rightarrow <Admin Domain Node> \rightarrow Intrusion Prevention \rightarrow Exceptions \rightarrow File Hashes. The Allowed and Blocked Hashes tabs are displayed.

•
Note

You can also go to the **File Hashes** page by clicking the **Manage allow and block lists** link from the **Malware Files** page or the **Endpoint Executables** page.

- 2. Depending on the type of hashes you want to export, select the **Allowed Hashes** or the **Blocked Hashes** tab.
- 3. Click **Export Allowed** or **Export Block List**. The **File Download** page is displayed.

Opening AllowedH	ashes.csv		×
You have chosen t	o open:		
🔯 AllowedHas	hes.csv		
which is: Mi from: What should Firef	crosoft Excel Comma	Separated Values File (1.3 I	 (B)
◯ <u>O</u> pen with	Excel (default)		\sim
		ОК	Cancel

4. Click Open or Save.

Exporting hashes

The exported CSV file will contain the file name, file size, hash function (MD5), file hash, and description.

🗹 Note

If you attempt exporting policies using Internet Explorer 10 in combination with Windows Server 2012, the Manager will generate the "Export of custom policy error". To avoid this, go to **Control Panel** \rightarrow **Add or Remove Programs** \rightarrow **Add/ Remove Windows Components**, the **Windows Components Wizard** window opens, select the **Internet Explorer Enhanced Security Configuration** and disable it. For more information on the fault, see the *Network Security Platform Product Guide*.

Move hashes from or to allow list or block list

After you have imported the list, you can move some or all of the hashes from one list to another.

🗹 Note

If a hash is part of both allow list and block list, the one in the allow list takes precedence.

Task

- 1. Select an entry that you want to move. To select multiple entries, hold the SHIFT key while selecting.
- 2. From the Other Actions drop-down list, select Move to Allow List.

Moving a selected hash to the allow list

Domain: /My Company	/My Co	/My Company > Intrusion Prevention > Exceptions > File Hashes					Ø	
Intrusion Prevention Relie: Manager	File H	File Hashes						
Policy Manager	0							
 Exceptions 	Block	red Hashes Allowed Hasher						
Ignore Rules	BIUCK	Allowed Hasiles	• 					
File Hashes								
Domain Names		File Hash ↑						
SSL Decryption Exclusions								
Auto-Acknowledgement	1	0386ff59d0f5c1cde453a37	'80353069f	telephon.cpl	Oct 27 15:51:49 2020	Administrator	desc	A
▹ Objects	2	075c8160789eb0829488a4	4fc9b59ed6c	collectmail_notwo0a.pdf	Oct 27 15:51:49 2020	Administrator	description	
▶ Advanced	3	0a614929df1ea09534403a	b02a7e4b23	Python_Basics_and_MySQL	Oct 27 15:51:49 2020	Administrator	desc	
 Network Threat Behavior Analysis 		0aac13cdef3602bab8544fe	251df2641d	IEXPLORE.EXE	Oct 27 15:52:27 2020	Administrator	Added based on user request	
NTBA Policies	5	0b237b533bd87632c9ccac	:9b640147c4	notepad.ex	Oct 27 15:51:49 2020	Administrator	desc	
Communication Rules	6	152e5cedb1eb8c69ddd578	3b8548c611e	Helpdesk_Tax_Filing_Form	Oct 27 15:51:49 2020	Administrator	desc	
NTBA Ignore Rules	7	1bb69e3f010c80ad282196	c31f2de5b5	applwizard.jar	Oct 27 15:51:49 2020	Administrator	desc	
Policy Import	8	1bd0b835db0f2535b10417	7df5048198c	ArtemisTest.zip	Oct 27 15:51:49 2020	Administrator	desc	
Policy Export	9	1bf588ba89e79829ad5d09	95e1b149839	sis.sys	Oct 27 15:51:49 2020	Administrator	desc	
	10	2a480eff5df8c5a757add35	aeadac4d8	NSAT_PPT_Template_v1.pptx	Oct 27 15:51:49 2020	Administrator	desc	
	11	2bfa250015e7c03fa5ad550	Da154a9555	sihclient.exe	Oct 27 15:52:27 2020	Administrator	Added based on user request	
	12	300a2c5cbddb9131d18184	dbc/12/15781d	Artemis_and_CustomFP_Te	Oct 27 15:51:49 2020	Administrator	desc	
	13	31e6002b21c489fbbdb	Import	hex-editor-setup.exe	Oct 27 15:51:49 2020	Administrator	desc	
	14	35426e5fb884ca8a6b0	Delete All	ssText3d.scr	Oct 27 15:51:49 2020	Administrator	desc	
	15	3f3f7c3b9722912ddedc	Move to Allow List	Firewall.cpl	Oct 27 15:51:49 2020	Administrator	desc	-
		— Save as CSV	Other Actions 🔹					43 file hashes

The selected entry is moved to the corresponding list that you have chosen. A message that the action is successful is displayed on top of the page.

Remove or replace hashes from allow and block lists

You can remove some or all of the hashes from the allow list or the block list and mark them as unclassified. The hashes are removed from the Manager database but are available in the NTBA database as unclassified.

Task

- 1. Select an entry that you want to remove. To select multiple entries, hold the SHIFT key while selecting.
- 2. From the Other Actions drop-down list, select Detele All.

The selected entry is no longer displayed on this page.

- 3. You can use the **Replace** option to put back the removed entry or to overwrite the old entries with new ones. A confirmation message will be displayed.
- 4. Click **OK** to continue.

The old list is replaced with the new list.

Configuring NTBA policies for McAfee EIA alerts

Seven attack definitions are added to the NTBA policies in **Policy** \rightarrow **Network Threat Behavior Analysis** \rightarrow **NTBA Policies**:

NTBA policy	Description	Enabled by default	Alert frequency
EXECUTABLE: Unclassified executable detected by Endpoint Intelligence Agent engine	This alert is raised when the executable is not classified by the administrator or is not auto-classified.	No	Raised once per executable from the NTBA Appliance
EXECUTABLE: Allowed executable detected by Endpoint Intelligence Agent engine	This alert is raised when the executable is marked as <i>allowed</i> by the administrator. This alert is also raised when the executable is found to be digitally allowed or GTI allowed.	No	
EXECUTABLE: Blocked executable detected by Endpoint Intelligence Agent engine	This alert is raised when the executable is marked as <i>blocked</i> by the administrator or when the executable is auto-classified based on GTI Block List.	Yes	Raised per executable per endpoint
MALWARE: Very High- confidence malware executable detected by Endpoint Intelligence Agent engine	This alert is raised when the malware confidence of the executable detected by McAfee EIA is very high and the executable is not <i>allowed</i> .	Yes	
MALWARE: High-confidence malware executable detected by Endpoint Intelligence Agent engine	This alert is raised when the malware confidence of the executable detected by McAfee EIA is high and the executable is not <i>allowed</i> .	Yes	

NTBA policy	Description	Enabled by default	Alert frequency
MALWARE: Medium- confidence malware executable detected by Endpoint Intelligence Agent engine	This alert is raised when the malware confidence of the executable detected by McAfee EIA is medium and the executable is not <i>allowed</i> .	No	
MALWARE: Very High- confidence malware file detected by Endpoint Intelligence Agent engine	This alert is raised when the malware confidence of the file detected by McAfee EIA is very high and the file is not <i>allowed</i> .	No	Raised per non- executable file such as doc or pdf file per endpoint

Depending on which of the attack definitions are enabled in the NTBA policies, alerts are generated for the matching traffic.

The malware attacks can be viewed in the **Top Malware Files** monitor on the Manager **Dashboard** page, and the **Top Attack Executables** table in the **Threat Explorer**.

Alert throttling

Run set endpointintelligence alertinterval CLI command to configure the time interval as to when the alert should be raised again. By default, it is 7 days. It can be configured between 0 and 30 days. Configure it as zero to disable alert throttling. Whenever a given executable property changes (malware confidence or classification), the alert generation interval is reset for that executable.

🗹 Note

Filter functionality is not supported for Endpoint Intelligence Agent alerts.

Viewing executables running on endpoint

The **Endpoint Executables** page on the **Analysis** tab provides a snapshot of all the executables running on your internal endpoints that have made network calls. It also provides network visibility on how many endpoints are running the executables, how many connections were made, and the events triggered by the executable during the selected timeframe.

🗹 Note

All NTBA Appliances that have McAfee EIA services running on them will be displayed in the **Devices** drop-down list. You can filter data based on the NTBA Appliance selection.

The executables listed here are processes and files. They can be allowed, blocked, and unclassified. You can use this page to investigate further on what factors led to the classification of the executable and manually change the classification.

By default, the order is sorted by the endpoints, so executables with most endpoint connections are displayed first.

🗹 Note

Maximum number of executables displayed on the **Endpoint Executables** page is 4096. Historical data and inactive executable data are kept for 30 days.

The page is divided into the **Executable** panel and the **Details** panel. Click a row in the **Executable** panel to view additional information about the executable hash in the **Details** panel.

Endpoint Executables page with default settings



ltem	Description
1	Filters and Search options
2	Executable panel
3	Details panel

Following are the filters and search option available:

Field	Description	Default Value
Malware Confidence	 Any Malware Confidence — Displays all executables irrespective of their malware confidence High+ Malware Confidence — Displays executables with high and very high malware confidence Medium+ Malware Confidence — Displays executables with medium, high, and very high malware confidence Very High Malware Confidence — Displays executables with very high malware confidence 	High+ Malware Confidence
Classification	 Any Classification — Displays all executables, whether blocked, allowed, and unclassified Blocked — Displays only blocked executables Unclassified — Displays executables that are neither blocked nor allowed Allowed — Displays only allowed executables 	Any Classification
Devices	Displays the list of NTBA Appliances that have McAfee EIA services running on them	Displays device names in the alphabetical order
Time interval	 Last 5 minutes Last 1 hour Last 6 hour Last 12 hours Last 24 hours Last 24 hours Last 48 hours Last 7 days Last 14 days Custom Time Period 	Last 12 hours
Search	Allows you to search executable by the file hash or the binary name of the executable	Blank

Attack Log
Upon double-clicking on any executable hash, you navigate to the **Attack Log** page. You can analyze and view alerts related to the selected hash.

Selected hash alerts in Attack Log

/My Com	Company > Endpoint Executables																	
Attack	Log																	
0									Unacknowledge	d 👻 01/0	PM - 08/11/21 8:28 PN	l 👻 Quid				Clear All	Filters	C 🗱
								Capture								<u>Hash</u>		
							No Ma	tching Attai	cks									
Ack	Un	ack Delete Other /	actions 🔻									0-0	of 0 alerts	«	۲	> 2)) < e	► Back

The date and time filter used in the **Endpoint Executables** page is persisted upon navigating to attack log. To close the attack log, click **Back** or sicon.

Manage Allow and Block lists

The Manage allow and block lists is a link to the File Hashes page.

For the selected NTBA Appliance, the **Executable** panel consists of the following:

Option	Definitions
Executable	 Actions — Click Take Actions to classify an executable as allowed, blocked, marked as, or unclassified Hash — Displays the file hash of the executable Name — Displays the binary name of the executable Version — Displays the product version
Malware Confidence	Displays the malware confidence level returned by the configured McAfee EIA. The malware confidence values are very high, high, medium, low, very low, and unknown.
Classification	Displays the executable classification whether blocked, allowed, or unclassified
First Seen	Displays when the executable was first reported by McAfee EIA to the NTBA Appliance for the selected timeframe

Option	Definitions
Last Seen	Displays when the executable was last reported by McAfee EIA to the NTBA Appliance
Counts	By default, the order is sorted by the endpoints, so executables with most endpoint connections are displayed first.
	 Endpoints — Displays the number of endpoints running the executable for the selected timeframe Attacks — Displays the number of attacks triggered by the executable for the selected timeframe Connections — Displays the number of connections made by the executable for the selected
	timeframe
Comment	Reason for changing the executable classification

Click any row to see additional information of the executable hash in the **Details** panel. The **Details** panel consists of the following:

EIA Details

This tab displays the executable or file information. This includes:

• **Properties** — Displays the malware confidence for the executable along with malware indicators that helped determine the reputation

Executa	ble or	file c	letails

Details for: Microsoft	t® Windows® Operating System	(svchost.exe) 10.0.14393.0 (rs1_release.160715-1616)
EIA Details Endpoint	s Applications	
Hash:	36f670d89040709013f6a4601767 67ec	File Execution Results
Binary Name:	svchost.exe	Dynamic analysis was not required for this file because of its certificate and/or GTI status
Product Name:	Microsoft® Windows® Operating System	
Version:	10.0.14393.0 (rs1_release.160715-1616)	
Malware Summary Malware Confidence:	Very Low	
Malware Name:		
File Certificate:	Signed and Trusted. (Microsoft Windows Publisher)	
GTI Reputation:	Very Low	
Local Classification:	Allowed	
Classified:	Auto Sep 23 17:53	

Field descriptions of EIA Details tab

Field	Description
Hash	Displays the file hash
Binary Name	Displays the binary name and the type, whether process or library
Product Name	Displays the product name for the executable or file
Version	Displays the product version number
Malware Summary	
Malware Confidence	Displays the malware confidence level returned by the configured McAfee EIA. The malware confidence values are very high, high, medium, low, very low, and unknown.
Malware Name	Displays the malware name, for example, gtalk.exe
File Certificate	Displays the certificate signer and status for the file certificate, for example, Microsoft Corporation

Field	Description
GTI Reputation	Displays the file reputation received from GTI. Valid values are Very Low, Low, Medium, High, Very High, and Unknown.
Local Classification	Displays the executable classification whether Blocked , Allowed , or Unclassified
Classified	Displays the method of classification (<i>Auto</i> if the executable has been auto-classified by the NTBA Appliance or <i>Manual</i> if it has been manually classified) and the timestamp, only for classified executables.
File Execution Summary	Displays a summary of the tasks performed when a program was executed. Examples: connects to the internet, changes proxy settings, adds host file entries.
File Execution Details	 Displays execution details as they happened Save as CSV — Exports the list of executables in CSV format Executable — Displays the executable name, example, gtalk.exe Action — Displays action performed by the program, example, create_dir Target Object — Specifies the path where this action was performed, example, \Device\Harddisk\Users\Ellie\Local Search — Displays details based on search criteria

• **File Execution Results** — Shows some of the methods and engines that were used to compute the executable reputation

Endpoints

This tab displays the list of endpoints running the executable during the selected timeframe.

Endpoints information

Details for: N	Details for: Microsoft® Windows® Operating System (svchost.exe) 10.0.14393.0 (rs1_release.160715-1616)								
EIA Details E	Endpoin	ts Applications							
						Search			
ID Addross		Hostnamo		05	llear	Counts			
IP Address		nosulaille		05	USEI	Attacks 🕹	Connecti		
10.213.		WIN-OO8U		Microsoft Windo	NT AUTHORITY\	0	4		

Field descriptions of Endpoints tab

Field	Description
IP Address	Displays the IP address of the endpoint
Hostname	Displays the name of the managed host
OS	Displays the version of the operating system running on the endpoint. For example: Windows 10.
User	Displays the user name who invoked the executable or the DLL. The user name can include system users and local users.
Counts	 Attacks — Displays the number of attacks triggered by the executable during the selected timeframe Connections — Displays the number of connections made by the executable during the selected timeframe

The **Search** field allows you to search by IP address, host name, operating system, or user columns.

Double-click the IP address to view alerts related to the IP address in the Attack Log. The alerts are filtered based on the IP address selected. To close Attack Log, click **Back** or sicon.

Alerts based on the IP address selected

/My Co	ompany >	Endpoint Executables															0
Atta	ck Log																8
0									Unacknowle	edged 👻	Last 7 days				Cl	ear All Filte	ers 🔿 🏟
														utable:			
						Attack Count	Capture								<u>Hash</u> 🕇		
1		MALWARE: Very High-confi	Sep 03, 2021 11:05:52	Unknown	Inconclusive		<u>Export</u>	· 10.		0		0	M08302.EXE		5f7504c02	2f50eb682	468b2b1ce545
																	•
Ac	k ι	Jnack Delete Other A	ctions 🔻									1-1	of 1 alerts	X	$\langle \rangle$	»	< Back

Applications

This tab displays the list of applications that have been invoked by the executable during the selected timeframe.

Applications invoked by the executable

Details for	Details for: Microsoft® Windows® Operating System (svchost.exe) 10.0.14393.0 (rs1_release.160715-1616)						
EIA Details	Endpoints	Applications					
						Search	
Application			Dick 🕈	Catagony		Counts	
Аррисаціон			NISK I	Calcyony		Attacks	Connections
				No Matches			

Field descriptions of Applications tab

Field	Description
Application	Displays the name of the application
Risk	Displays whether the application is high, medium, or low risk. McAfee Labs categorizes an application based on its vulnerability and the probability for it to deliver malware.
Category	Displays the category that the application falls under. For example, HTTP falls under the Infrastructure Services category.
Counts	 Attacks — Displays the number of attacks triggered by the executable during the selected timeframe Connections — Displays the number of connections made by the executable during the selected timeframe

The **Search** field allows you to search by application name, risk, or category.

Double-click the application to view alerts related to the application in the Attack Log. The alerts are filtered based on the application selected. To close Attack Log, click **Back** or sicon.

Alerts based on the application selected

/My C	/My Company > Endpoint Executables																		
Atta	Attack Log																		
0										Unacknowl	edged 👻	Last 7 days					Clear All	Filters	0 0
						Attack Count		Capture								Hash 1			
1		MALWARE: Very High-confi	Sep 03, 2021 11:05:52	Unknown	Inconclusive			Export	· 10.		9		9	M08302.EX	Æ	5f7504	c02f50et	682468b2	2b1ce545
•																			Þ
Ad	ack Unack Delete Other Actions * 1-1 of 1 alerts 伏 🕻 > >> < Back																		

Sample scenario: Analyze an unclassified executable with high malware confidence

Consider an executable, *DAP.exe*, is shown on the **Top Endpoint Executables** monitor with malware confidence as High and classification as Unclassified. This section provides you a workflow that you could follow in the Manager user interface to further investigate the executable properties, malware indicators used to compute the malware confidence, the type of alerts it triggered, the confidence assigned by other malware engines to this file, and subsequently allow or block it.

Task

- 1. Click **Dashboard** on the Home page to view the **Top Endpoint Executables** monitor.
 - a. Select Attacks to view executables that have generated most attacks.
 -OR-

Select **Endpoints** (default) to view executables that have made most connections. The **Device** drop-down list is shown when you select **Endpoints**. This list shows all NTBA Appliances configured that have McAfee EIA services running on them sorted in alphabetical order.

b. Click DAP.exe in the Top Endpoint Executables monitor to go the Endpoint Executables page.

🗹 Note

Hover the mouse on the bar graph to see the executable name, number of attacks/endpoints, executable hash name, classification type, and malware confidence level.

The executable, **DAP.exe**, shows high malware confidence but the classification type is shown as Unclassified.

2. The **Endpoint Executables** page provides network visibility on how many endpoints are running the executables, how many connections were made, and the events that it triggered. It also displays the malware indicators used to compute the malware confidence of the executable.

a. Click the Hash link, IP Address link, Application link, Attack link, Attacker IP Address link, or Target IP Address link in the **Details** panel to go to the **Threat Explorer** page.

🗹 Note

In some cases, alert count is shown even for allowed executables such as Mozilla Firefox. If bad or malicious sites were accessed and files downloaded using Mozilla Firefox, there could be executables generating alerts that result in increase of the attack count.

3. Click **View Attacks** in the **Threat Explorer** page to go to the **Malware Files** page to view the malware confidence alerts, how the malware confidence was computed by the individual malware engines, and overall malware confidence of the executable was computed. This page also allows an in-depth analysis of the malware detected in your network.

🗹 Note

You can also go to the Malware Files page from the Endpoint Executables page.

🗹 Note

For alerts triggered by McAfee EIA, the bottom panel displays the **Direction** and **Protocol** as unknown, **Attacker Country** and **Target Country** as blank, and **Result** as inconclusive.

4. Select **Analysis** \rightarrow **Network Forensics** to further analyze the endpoint behavior on your network.

a. Enter the IP address of the endpoint for the selected date and time and click **Analyze**.

The **Network Forensics** page is displayed with summary, conversation, and event information.

🗹 Note

All the executables invoked on the endpoint are displayed in the **Client connections** panel.

- b. Scroll to the **Top 10 Conversations** panel to see the connections made using this IP address.
- c. Scroll to the **Last 50 Events** to view more details about the attacks. The **Endpoint Executables** column displays hash, name, classification, and malware confidence. Click the hash link to go to the **Threat Explorer** page.
- 5. Click View attacks in the Attack Log to view and analyze alerts.
 - a. You can view and group by alerts based on the following:
 - Name: Displays binary name of the executable
 - **Hash**: Displays the file hash of the executable
 - **Malware Confidence**: Displays the malware confidence level returned by the configured McAfee EIA. The malware confidence values are very high, high, medium, low, very low, and unknown.

🗹 Note

All the executables invoked on the endpoint are displayed in the **Client connections** panel.

🗹 Note

The above-mentioned fields are not displayed for suppressed alerts.

The alert count and attack count are displayed for the attribute selected in the list.

b. Double-click an alert to open the Alert details panel.

For all alerts triggered by McAfee EIA, an additional panel called **Endpoint Intelligence** panel is displayed. This displays the hash, name, classification, and malware confidence of the executable.

c. Click **Real-time EIA Details** to view executable information for existing IPS and NTBA alerts that have 5-tuple information. Alerts, such as Exploits, Callback Activity, Behavioral, Malware, and Policy violation, have the 5-tuple information. It also gives information of the library invoked by the executable, the malware indicators used to compute the score, and classifier information.

As an administrator, you might want to investigate the alerts further.

🗹 Note

The malware confidence and classification values shown in the **Real-time EIA Details** window might be different from what is shown in the **Alert Details** window. This is because the **Alert Details** window shows the malware confidence and classification of the alert when it is first generated while the **Real-time EIA Details** shows the current details of the executable.

6. Based on the analysis, you can classify the executable as allowed or blocked by clicking the **Take Action** link on the **Malware Files** page.

These updates are made to the allowed and blocked hashes maintained in the Manager.

The Manager sends the changes in the allowed and blocked hashes to the NTBA Appliance every five minutes. Whenever the file's hash matches with the ones in the allowed and blocked hashes, the allowed hashes are exempted from malware analysis.

Viewing endpoint intelligence reports

From Analysis \rightarrow Event Reporting \rightarrow Next Generation Reports, run and view the Default-Top 10 Endpoint Executables and Default-Endpoint Executable Details for details based on EIA alerts.

NTBA-EIA deployment scenarios

Scenario	Solution
NTBA-EIA integration with IPS Sensor	The NTBA Appliance, the IPS Sensor, and McAfee EIA should be configured in such a way that traffic from endpoints passing through IPS, same endpoints must be configured to send executable information to the NTBA Appliance.
NTBA-EIA integration without netflows coming to NTBA	The solution will work. Applications associated with the executables will not be shown. Events will not have executable information. The Network Forensics page will be blank.

Scenario	Solution
NTBA-EIA integration in a setup with IPS Sensor and multiple NTBA Appliances	The Endpoint Executables page displays information per NTBA appliance. The block lists and allow lists maintained by the Manager are pushed to all NTBA Appliances with EIA integration enabled. McAfee recommends that you distribute EIA agents across various NTBAs depending on the maximum limit of endpoints supported by connected NTBA models.
	Note: When more than one NTBA is configured to get executable information from endpoints and if an NTBA is not connected to IPS Sensor, the Endpoint Executables \rightarrow Applications displays no applications. Sensor generated alerts do not display executable information.
NTBA-EIA integration in a setup with endpoints distributed across geo- locations	The NTBA Appliance must be deployed closer to the specific geo to be monitored in order to reduce data exchange across WAN links. The number of endpoints at a particular geo-location should be used as a factor to decide the location at which the NTBA Appliance is to be deployed. For more information, refer to the NTBA-EIA sizing recommendations.
NTBA-EIA integration in a setup with multiple ePO servers	If there are multiple ePOs managing different parts of the network and all endpoints need to communicate to a NTBA appliance on the network, this can be achieved by using third-party CA in ePO to provide the CA certificates. This way, all endpoints will receive certificates from the same CA.

Best practices

The auto-classification settings for allow list executables (based on GTI reputation or signed by a trusted authority) are enabled by default. Auto-classification for block list executables based on GTI reputation and dynamic analysis are disabled by default. McAfee recommends that you keep all auto-classification settings as enabled unless you want to investigate every executable manually.

For all executables, the malware confidence displayed on the Manager is a best effort based on malware indicators associated with each executable.

If time permits:

- Once the solution is deployed, learn the executables used in the network to create a baseline computer profile, investigate, and classify as allowed all the approved executables for your enterprise.
- Every time new patches are deployed, use the endpoint baseline generator to create an updated hash list and import into the Manager.

- Investigate each executable that displays malware confidence as low or very low. For example, use the malware indicators, alerts generated, and network forensics.
- Integrate with McAfee Advanced Threat Defense to leverage its sandboxing capabilities.
- Enable the Gateway Anti-Malware Engine running on NTBA as an additional engine for inspection of malware.
- Look at the number of endpoints using an executable, the type of applications, and events associated with the executable.
- If the number of endpoints is high, it is unlikely that it is a bot.

Analyze the results from all of these, and then make the final decision to allow list or block list an executable. If you have time constraints, investigate executables that have malware confidence displayed as medium and above.

NTBA-EIA sizing recommendations

SKU	Maximum endpoints
T-600	12,000
T-1200	12,000
T-VM	8,000
T-100VM	8,000
T-200VM	10,000

NTBA-EIA sizing recommendations

Below are the observations from tests conducted at McAfee:

- On a typical working day, the average number of executable information records sent by one endpoint in an enterprise is around 2500 per hour.
- The average size of each record is around 300 bytes.

Depending on the number of active endpoints, you can compute the bandwidth requirements for data sent by Endpoint Intelligence Agent on endpoints to NTBA.

Assume you have total 50,000 endpoints in your enterprise network:

- Number of NTBA Appliance recommended = 5 T-600 Appliances
- Assume 70% of endpoints are active => 7000 endpoints will be talking to each NTBA
- Network bandwidth requirement for each NTBA = [7000*2500*300/3600] *8 bits per second = 12 Mbps

Troubleshooting

This section addresses some of the issues that might be encountered while working with McAfee EIA.

Connectivity issues

This section covers the scenarios and solutions for connectivity issues.

To check if connection between ePO server and NTBA Appliance is established

Run the show endpointintelligence summary command:

Check the ePO connection status and the ePO certificate status as shown.

The output of the command is:

[Endpoint Configuration and Status]

Endpoint Intelligence Service : Not Running

ePO Server IP : 0.0.0.0

Last ePO connection attempt : 2013-10-01 09:12:20

Last ePO connection status : Failed (ePO server not reachable)

ePO certificate : Not available

Alert throttling : Disabled

GTI file reputation server : Reachable

[Endpoint connections]

Total active endpoint connections : 22

Total packets received : 16884

Total packets sent : 778

Last packet received time : 2013-10-01 07:49:05

Last packet sent time : 2013-10-01 08:06:23

Last endpoint connected : 172.16.232.109

If there is a failure in downloading the ePO certificate, the reason is displayed for troubleshooting purpose.

If there is any issue with SSL handshake

```
\mathsf{Run}\xspace{1.5} show endpointintelligence details \mathsf{CLI}\xspace{1.5}\xspace{1.5} command.
```

```
In Packet processing stats, check session failures as shown.
```

```
[Packet processing stats]
```

Total packets received : 17065

- Total packets sent : 790
- Total metadata flows : 16201

```
Total GTI file reputation requests : 6
```

```
Total GTI file reputation responses : 0
```

- Total Sysinfo packets received : 789
- Total keepalives received : 790
- Total keepalives sent : 790
- Total malformed packets : 0
- Total unsupported packets : 0
- Total packet send failures due to session not available : 0
- Total connections : 46
- Total active connections : 22
- Total connection timeouts : 1
- Total sessions : 23
- Total session failures : 1
- Total session failures due to certificate mismatch : 1
- Total session failures due to timeouts : 1

Total session failures due to certificate mismatch indicates that McAfee EIA is not able to talk to NTBA and that endpoints are using a different ePO certificate from what is available in NTBA. To resolve this, push the latest ePO certificate to NTBA using the Manager interface.

Critical faults

Critical faults are the highest severity faults and generally indicate a serious issue. See the Action column for potential troubleshooting tips.

Critical faults

Fault	Description/Cause	Action
Endpoint Intelligence Service is down	Endpoint Intelligence Service has not started as the ePO is not reachable.	Make sure that the ePO server is up and running and is reachable to NTBA.
	Endpoint Intelligence Service has not started as the ePO extension does not support auto-signing service.	Make sure that the ePO server supports ePO Auto Signing functionality (Change on Name confirmation).
	Endpoint Intelligence Service has not started because of authentication error connecting to the ePO server.	Provide valid ePO Server credentials.
	Endpoint Intelligence Service has not started because of internal error from the ePO server.	ePO server responded error; look at the ePO logs.
	Endpoint Intelligence Service has not started because of unexpected errors.	Look at the ePO server and NTBA logs for the error, and try again.
	Endpoint Intelligence Service has not started because of corrupt certificate.	Certificate invalid; retry saving again.
	Endpoint Intelligence Service has not started because the configured port for Endpoint Intelligence Service is already in use.	This port is already in use; configure an unused port.

If no data is seen in Executables panel of the Endpoint Executables page

- Make sure McAfee EIA service is running on the NTBA Appliance.
- Make sure that endpoint connections are made to the NTBA Appliance.
- Check the ntba.log file by running the TOP_PROCESS query:

```
2013-08-27 10:51:10,019 INFO iv.core.nba.control.command -
                                                                            NBA Command TD -> 0
2013-08-27 10:51:10,019 INFO iv.core.nba.control.command - NBA Command Name -> TOP PROCESS
2013-08-27 10:51:10,019 INFO iv.core.nba.control.command - Response returned from NBA Server
2013-08-27 10:51:10,019 INFO iv.core.nba.control.command - {message=0K, isXML=true, respcode=200,
msgcode=0.
data=<results> <proc p_id="172475594623937" p_hash="62880e4a7bd8d63aed832734836b4093" p_nm="HTMLayout" b_name="HTMLayout.dll" s_name="" p_ver="3, 3, 2, 4" p_conf="5" p_cls="0" f_size="0" f_sn="2013-08-26
23:00:00"
1 sn="2013-08-26 23:00:00" host cnt="1" con cnt="2" /></results>, Id=4697, isPartial=false, code=200}
2013-08-27 10:51:10,019 INFO iv.core.nba.control.command - Response -> {message=OK, isXML=true,
respcode=200,
msgcode=0, data=<results> <proc p id="172475594623937" p hash="62880e4a7bd8d63aed832734836b4093"
p_nm="HTMLayout"
  _name="HTMLayout.dll" s name="" p ver="3, 3, 2, 4" p conf="5" p cls="0" f size="0" f sn="2013-08-26
23:00:00"
1 sn="2013-08-26 23:00:00" host cnt="1" con cnt="2" /></results>, Id=4697, isPartial=false, code=200}
2013-08-27 10:51:10,019 INFO iv.core.nba.control.command - Response message text -> <results>
cprec p_id="172475594623937" p_hash="62880e4a7bd8d63aed832734836b4093" p_nm="HTMLayout"
b_name="HTMLayout.dll"
host cnt="1" con cnt="2"
                                /></results>
2013-08-27 10:51:10,019 INFO iv.core.nba.control.command -
```

This query returns the list of Top Executables from the NTBA Appliance.

Integration with McAfee Vulnerability Manager

Vulnerability assessment is the automated process of pro-actively identifying vulnerabilities of computing systems in a network in order to determine security threats to the network. Vulnerability scanner software automates the vulnerability discovery process, by remotely assessing your network, and finding the vulnerabilities in the systems.

McAfee® Network Security Platform provides integration with vulnerability scanners such as McAfee® Vulnerability Manager (formerly Foundstone), and Nessus Security Scanner. You can request remote scans, and use the vulnerability assessment reports from the scanners to determine the relevance of attacks on the hosts.

Vulnerability Manager scan configuration can be done from the root admin domain level or at child admin domain levels. There is an option to inherit configuration settings from the parent domain, or enable separate configuration at the child admin domain level.

Different Vulnerability Manager server settings and scan configurations can be done at the root and child admin domain levels.

McAfee Network Security Platform - Vulnerability Manager integration

Network Security Platform has been integrated with Vulnerability Manager Enterprise vulnerability scanner.

There are two main components to this enhanced integration. First, users can schedule the import of Vulnerability Manager scan data into Network Security Platform, to provide automated updating of IPS-event data relevancy. Second, users can initiate a Vulnerability Manager scan of a single IP address from the Vulnerability Scanning option. This provides a simple way for security administrators to access near real-time updates of host vulnerability details, and improved focus on critical events.

The figure below gives an overview of the Network Security Platform-Vulnerability Manager integration.



Network Security Platform-Vulnerability Manager integration

This integration provides the following major functionalities in McAfee® Network Security Manager:

On-demand scan

You can request a Vulnerability Manager scan from Threat Explorer, by selecting the Attacker/Target IP address of the host.

When you request a Vulnerability Manager on-demand scan, the selected host IP address is passed from the Threat Explorer to the Manager web-tier, which connects and establishes trust with the Vulnerability Manager engine. This initiates the scan for the requested endpoint IP address.

The Vulnerability Manager engine scans the host, and provides the vulnerability assessment data to the Manager. This data is processed and stored in the Manager database and have visibility to the recently invoked on-demand scans. For requesting an on-demand scan from Threat Explorer, you need to configure Vulnerability Manager settings in Manager.

If the scan traffic between the Vulnerability Manager server and the hosts being scanned passes through a Sensor monitoring port, the Sensor may consider it as attack traffic and take the corresponding response action such as quarantining the Vulnerability Manager server.

To prevent this:

- Create ACLs to exclude all traffic from the Vulnerability Manager server from attack inspection. For information on ACLs, see the section *Configuring ACL rules* in *McAfee Network Security Platform Product Guide*.
- If you have configured Quarantine, add the Vulnerability Manager server to the quarantine exceptions list. This prevents the Vulnerability Manager server being quarantined.

Automatic import of Vulnerability Manager reports via the scheduler in Manager

The vulnerability report from Vulnerability Manager database can be imported via the Vulnerability Manager Scheduler in Manager. Reports can be scheduled on a daily or weekly basis. Imported vulnerability data will be stored in the Manager database, and also updated in the *relevancy cache* used for relevancy analysis of attacks.

Manual import of Vulnerability Manager reports via Manager

You can manually import reports from Vulnerability Manager, and store them in your local machine. Manager client passes the imported vulnerability data into the *vulnerability assessment module* in the Manager server. This data is processed and stored in the Manager database in Network Security Platform format.

Relevance analysis of attacks

Once you have imported vulnerability reports into the Manager database, you can determine the vulnerability relevance for the alerts.

Vulnerability Manager installation

Vulnerability Manager and Manager should not be installed on the same system. Foundstone Configuration Management (FCM) Agent service is installed by default during the Manager installation; no other component need to be installed on the Manager system.

Vulnerability Manager Enterprise has the following major components:

- Vulnerability Manager Enterprise Manager Represents the browser-based user interface of the system
- Scan engine Used to scan hosts for vulnerability assessment
- Vulnerability Manager database server Is the data repository for Vulnerability Manager Enterprise containing information about organization settings, scan configurations, workgroups, user account information, and scan results
- Vulnerability Manager Certificate Manager (FCM) Server Hosts the Vulnerability Manager Certificate Management tool used for custom certificates

In an actual Vulnerability Manager deployment, you can deploy Vulnerability Manager Enterprise Manager, Vulnerability Manager console, one or more FoundScan engines and Vulnerability Manager database.

🗹 Note

For more information on system requirements for different Vulnerability Manager Enterprise deployment scenarios, and setup process for different Vulnerability Manager versions, see *McAfee Vulnerability Manager Product Guide*.

Configuring the Vulnerability Manager servers to use a DNS server

The server(s) used for Vulnerability Manager deployment should be configured to use Domain Name System (DNS) Server. Vulnerability Manager server must be defined as a record within the DNS zone.

Also make sure to configure the client machines used for on-demand scans, to use the DNS Server.

Without the above configurations, the Vulnerability Manager on-demand scans from Threat Explorer will result in error, due to incorrect name resolution.

🗹 Note

The product names "Foundstone", and "Vulnerability Manager" refer to the same product.

Menu options for Vulnerability Manager configuration

To configure Vulnerability Manager settings in the Manager, select **Manager** \rightarrow **<Admin Domain Name>** \rightarrow **Integration** \rightarrow **Vulnerability Assessment** or **Manager** \rightarrow **<Child Admin Domain Name>** \rightarrow **Integration** \rightarrow **Vulnerability Assessment** (for performing this action from root or child admin domains).

Configure Vulnerability Manager settings in Manager

Before you begin

Disabling CBC protection allows the integration. Cipher block chain (CBC) protection is an operating mode in cryptography. Java uses CBC protection in SSL connections to counter the Beast Exploit against SSL/TLS (BEAST) threat, and a security vulnerability in an SSL socketFactory method. This security fix was introduced in Java version 6u29, which also introduced a bug that prevents SSL connections to SQL Server 2008. As a result, CBC protection interferes in the integration between the Manager and MS SQL database of Vulnerability Manager. Therefore, before you proceed with your configuration of Vulnerability Manager in the Manager, disable this feature by performing the steps below:

- 1. Locate the tms.bat file in C:\Program Files (x86)\McAfee\Network Security Manager\App\bin.
- 2. Open the file in a notepad application.

Text to disable CBC protection in Java

- 3. Scroll to locate the text displayed in the image as 0
- 4. Once you have located the text, append it with the following entry:

set JAVA_OPTS=%JAVA_OPTS% -Djsse.enableCBCProtection=false

The text must be entered as displayed in the image as (2).

- 5. Save and the close the file.
- 6. Reboot the Manager.

Once the Manager is back up you may proceed with the configuration.

The Vulnerability Manager configuration settings allow Manager to connect directly to the Scan engine servers and database.

You can configure the settings in two ways:

Task

- 1. Manually navigating the configuration screens.
- 2. Using the Vulnerability Manager Configuration Wizard

Manually navigating the configuration screens

Following steps are essential for manually configuring Vulnerability Manager settings (in the given order):

- Enabling Vulnerability Manager scanning This is the first step required for successfully using the Vulnerability Manager on-demand scan functionality from Threat Explorer.
- Configuring Vulnerability Manager database settings This step is essential for Manager to connect to the Vulnerability Manager database server, and import the required information from the database.

- Configuring Vulnerability Manager Server settings Manager uses information from the Vulnerability Manager server to initiate Vulnerability Manager scans from Threat Explorer.
- Adding Vulnerability Manager scan configurations If the IP address of the scanned host falls within any of the scan configurations added to Manager, that scan configuration is used for on-demand scan of the host from Threat Explorer. This step completes the configuration settings for Vulnerability Manager in Manager.

Using the Vulnerability Manager Configuration Wizard

The Vulnerability Manager Configuration Wizard helps you to navigate the screens in the desired sequence.

Select Manager \rightarrow <Admin Domain Name> \rightarrow Integration \rightarrow Vulnerability Assessment \rightarrow MVM \rightarrow Vulnerability Scanning \rightarrow Summary.

Or,

$$\label{eq:scanning} \begin{split} \text{Manager} & \rightarrow \text{Child Admin Domain Name} \rightarrow \text{Integration} \rightarrow \text{Vulnerability Assessment} \rightarrow \text{MVM} \rightarrow \text{Vulnerability} \\ \text{Scanning} & \rightarrow \text{Summary and click Run Configuration Wizard to start the Vulnerability Manager Configuration Wizard}. \end{split}$$

Vulnerability Manager Summary sub-tab

Dor	main: /My Company 💌	/My Company > Integration > Vulnerability A	ssessment > MVM > Vulnerability Scanning	g > Summary	Ø
_	Summary	Summary			
-	Download Signature Sets	•			
	Download Callback Detectors	Status			
	Download Device Software	Allow Vulnerability Scans to be Initiated from the Manager?	Enabled	Run Configuration Wizard	
	Manual Import				
	Messages from McAfee	Database Settings			
	Automatic Updating	Server Name or IP Address			
	Users and Roles	Server Port:	1433		
	Setup	SSL Type:	Require		
*	Integration	Database Name:	Faultline		
	GTI	User Name:			
	MLC	Logon Domain:	n/a		
	HIP				
	HP Network Automation	API Server			
	▶ ePO	Vulnerability Manager Server	75		
	 Vulnerability Assessment 	Version:			
	Non-MVM Report Import	User Name:	administrator		
	✓ MVM	- 5 1 l-+			
	 Vulnerability Scanning 				
	Summary	NSM7 10_213_172_19 (detault)			
	Enable	/ Win_adv_scan			
	Database Settings	/ Win_adv_scan2			
	API Server	/ Full_vuln_scan2			
	Scans				
	Troubleshooting				
	Alert Relevance				

Configuring Vulnerability Manager Settings in the Secondary Manager

If you have an MDR setup, before you proceed with your configuration of Vulnerability Manager in the Secondary Manager, perform the steps below:

🗹 Note

Ensure that the Secondary Manager is in standby mode.

Task

- 1. Locate the tms.bat file in C:\Program Files (x86)\McAfee\Network Security Manager\App\bin.
- 2. Open the file in a notepad application.

Text to disable CBC protection in Java



- 3. Scroll to locate the text displayed in the image as 1
- 4. Once you have located the text, append it with the following entry:

set JAVA OPTS=%JAVA OPTS% -Djsse.enableCBCProtection=false

The text must be entered as displayed in the image as 2.

- 5. Save and close the file.
- 6. Reboot the Secondary Manager.
- 7. Make the Secondary Manager active by clicking **Force Switch** in the **Manager** → **<Admin Domain Name>** → **Setup** → **MDR**.
- 8. Start the FCM agent service. From the Windows **Start** button, click **Run** and open **Services**. You can find the **Found stone Configuration Management (FCM) Agent**.
- 9. Click the **Start** button (**P**) to start the FCM Agent service.
- 10. In the Manager, select Manager \rightarrow <Admin Domain Name> \rightarrow Integration \rightarrow Vulnerability Assessment \rightarrow MVM \rightarrow Vulnerability Scanning \rightarrow API Server.

The Retrive MVM Certificate option is enabled.

11. Click **Retrive MVM Certificate** to import the client certificates into the Manager keystore.

Use Vulnerability Manager configuration wizard

You can use the Vulnerability Manager Configuration Wizard for configuring Vulnerability Manager settings from Manager.

Task

- Select Manager → <Admin Domain Name> → Integration → Vulnerability Assessment → MVM → Vulnerability
 Scanning → Summary or Manager → <Child Admin Domain Name> → Integration → Vulnerability Assessment →
 MVM → Vulnerability Scanning → Summary to perform this action from root or child admin domains.
- 2. In the Summary page, click Run Configuration Wizard.
- 3. The wizard displays the following pages in order:
 - Enable
 - Database Settings
 - Vulnerability Manager Server Settings
 - Added Vulnerability Manager Scan Configurations
 - a. Use **Next >** or **< Back** buttons to navigate through the pages.
 - b. There are four configuration steps in total. Select **Finish** at the end of the fourth step.

Enable Vulnerability Manager integration at the admin domain level

Vulnerability Manager integration can be enabled both at the root and child admin domain levels.

Enabling Vulnerability Manager integration is the first step in configuring the Vulnerability Manager from Manager.

Task

 Select Manager → <Admin Domain Name> → Integration → Vulnerability Assessment → MVM → Vulnerability Scanning → Enable.

The **Enable** page is displayed.

2. Select **Yes** for the **Allow Vulnerability Scans to be Initiated from the Manager?** option to enable integration of Vulnerability Manager in the Manager.

Enable area



3. Click Save.

Enable Vulnerability Manager integration at the child admin domain level

You can enable Vulnerability Manager integration at the child admin domain level in the Manager. To do so perform the following steps.

Task

 Select Manager → <Child Admin Domain Name> → Integration → Vulnerability Assessment → MVM → Vulnerability Scanning → Enable.

The **Enable** page is displayed.

2. Select **Yes** or **Inherit Settings?** for the **Allow Vulnerability Scans to be Initiated from the Manager?** option to enable integration or inherit settings made in the parent admin domain.

Enable page in child admin domain level

Enable				
0				
Allow Vulnerability Scans to be Initiated from the Manager?	Yes	• No	• Inherit Settings	
				Save

3. Click Save.

Update successful message



By default all child admin domains inherit the Vulnerability Manager configuration settings from its parent domain.

The screen is refreshed, and a message that the changes have been successfully saved is displayed.

Configure Vulnerability Manager database settings

The second essential step in Vulnerability Manager configuration is configuring the Vulnerability Manager database settings.

Using these settings, Manager connects to the Vulnerability Manager database to get relevance information, scan configuration details, scan engine details, and vulnerability data for scanned hosts. The required data is fetched directly from the Vulnerability Manager database using stored procedures specific to the Manager.

🏹 Tip

Make sure that you have enabled Vulnerability Manager integration before configuring Vulnerability Manager Database Settings.

Task

1. Select Manager → <Admin Domain Name> → Integration → Vulnerability Assessment → MVM → Vulnerability Scanning → Database Settings.

Database sub-tab

Database Settings		
0		
Server Name or IP Address		
SQL Server Instance Type:	O Default Instance O Specific Instance	
Instance Name:		
Database Type:	Default 🔀	
Server Port:	1433	
SSL Type:	Require 🖌 *	
Database Name:	Faultline	
Authentication Type:	SQL 🖌	
User Name:	sa	
Password:	•••••	
		Test Connection Save

- 2. In Database Settings window, enter Server Name or IP Address of the Vulnerability Manager database.
- 3. Select the **Database Type**. You can choose **Default** database or a **Custom** database.
 - When you choose **Database Type** as **Default**, note that **Database Settings** window displays the following default values for three fields as given below:
 - Server Port as 1433

- SSL Type as Require
- Database Name as Faultline

• When the **Database Type** is selected as **Custom**, you can enter custom values in **Server Port**, **SSL Type** and **Database Name** fields.

If you select the **Default** option, go to step 7. If you select **Custom**, proceed with the next step.

- 4. Enter **Server Port** for the Vulnerability Manager database server.
- 5. Select **SSL Type**.

SSL type	Description
Off	SSL is not requested or used; this is the default.
Request	SSL is requested; if the server does not support it, a plain connection is used.
Require	SSL is requested; if the server does not support it, an exception is thrown.
Authenticate	Same as Require, except that the Vulnerability Manager server's certificate is signed by a trusted Certifying Authority (for example, VeriSign or DigiCert).

- 6. Enter the name of the Vulnerability Manager database server in **Database Name**.
- Next, you can select three different authentication type for logging into Vulnerability Manager database SQL, Windows Domain, or Windows Workgroup.

In all these authentication types, **User Name** and **Password** refer to those of the Vulnerability Manager database server that is used in the configuration.

- In the case of SQL Authentication,
 - Enter User Name.
 - Enter **Password**.
- In the case of Windows Domain Authentication,
 - Enter User Name.
 - Enter **Password**.
 - Enter Logon Domain.

🗹 Note

Logon Domain represents the network domain for the Windows NT system. This field is exclusively for Windows Domain Authentication.

- In the case of Windows Workgroup,
 - Enter User Name.

- Enter **Password**.
- Enter Server Name of the Windows Workgroup server.
- 8. Click **Test Connection** to check the availability of Vulnerability Manager database connection. The success or failure in connectivity is displayed as a message in the **Database Settings** page.

🗹 Note

The logon credentials (username and password) for both type of authentications should be given db_owner access rights in the Vulnerability Manager database. This is essential for Manager to establish connection with Vulnerability Manager database, and automatically install stored procedures in the Vulnerability Manager database.

🗹 Note

Note that when Vulnerability Manager database settings are configured for the first time, Manager automatically installs the Vulnerability Manager database with required tables and stored procedures that are used for retrieving information.

Configure Vulnerability Manager server settings

The third essential step in Vulnerability Manager configuration is configuring the Vulnerability Manager Server settings. The Manager needs to connect to the Vulnerability Manager Server to access the Scan engine. Scan engine is the component of Vulnerability Manager system that scans the hosts in your network for vulnerabilities.

Network Security Platform-Vulnerability Manager integration supports three versions of Vulnerability Manager engine: 6.8, 7.0, and 7.5. In the Network Security Platform Manager, configuration settings for the scan engine include the engine version and logon credentials to the scan engine server.

🏹 Tip

Before configuring **Vulnerability Manager Server Settings**, you should enable Vulnerability Manager integration and configure Vulnerability Manager database settings.

Below are the high level steps for successfully configuring the server settings:

- Before saving the server settings, make sure to provide full access rights to the user account used to run the Manager service. In case the required permissions are not provided, the **Failed to save settings** error appears.
- Start the FCM Agent Service before retrieving the MVM certificate.
- When changing the server settings, restart the FCM Agent Service even if the service is already running.

To configure the Vulnerability Manager server settings, do the following:

Task

1. Select Manager → <Admin Domain Name> → Integration → Vulnerability Assessment → MVM → Vulnerability Scanning → API Server.

The Vulnerability Manager Server Settings page appears.

- 2. Select Engine Version as 6.8, 7.0, or 7.5.
- 3. Enter the Server Name or IP Address.
- 4. Enter the Server Port, User Name and Password for the Vulnerability Manager server.

Vulnerability Manager Server Settings area

/My Company $>$ Integration $>$ Vulnerability Assessment $>$ MVM $>$	Vulnerability Scanning > API Server			Ø
API Server				
0				
Engine Version:				
Server Name or IP Address:				
Server Port:	3800			
User Name:	administrator			
Password:				
		Retrieve MVM Certificate	Save Test Co	onnection

🗹 Note

Username and password entered here should have full access rights in the Vulnerability Manager server. This is essential for successfully initiating Vulnerability Manager on-demand scans from Threat Explorer.

5. Click Save.

6. Start the FCM Agent service. Click Retrieve MVM Certificate to retrieve the MVM certificate.

🗹 Note

7.0 and 7.5 scan engines support only custom certificates.

7. Click Test Connection to check the availability of Vulnerability Manager server connection.

Update permissions for the integration

The Manager must update the Windows registry for a proper integration. However, the user account used to run Manager service does not have permissions to write to the Windows registry by default. For updating the permissions:

Task

- 1. On the server running the Manager, run regedit.exe.
- 2. Select My Computer → HKEY_LOCAL_MACHINE → SOFTWARE.
- 3. Right-click and select Permissions.
- 4. Add the user account used to run the Manager service. Allow full permission for this folder. Click Apply and OK.

Updating permissions

SAM	Name	Туре	Data		
SECURITY	(Default)	REC Devenio	cions for EDETWARE		
SOFTWARE		Permis	SIONS FOR SOFT WARE		
ATI Technologies		Security	1		
Classes					
Clients		Group c	or user names:		
Macromedia		🛛 🎎 CF	EATOR OWNER		
Martin Prikryl		SY 🎎 SY	'STEM		
Microsoft		😣 Ad	Iministrators (WIN-ULK55R	LE17U\Administr	ators)
MozillaPlugins		See Us	ers (WIN-ULK55RLE17U\	Users)	
Delision					
				L [
Wow6432Node				Add	Hemove
Adobe		Permiss Ov (NE)	ions for CREATOR	Alleru	Danu
Ariad		UWNER		Allow	Deny
		Full C	Control		
		Read	1	\checkmark	
E-Foundstone		Spec	ial permissions		
Components					
E FCM					
🗄 🔒 Foundscan					
🕀 🌗 JavaSoft	11	For spec	cial permissions or advance	ed settings,	Advanced
JreMetrics	11	CIICK AC	ivanceu.		
🕀 📕 Macromedia	11	Learn a	bout access control and pe	ermissions	
🕀 🦊 Martin Prikryl	11				
🕀 🛁 Microsoft	11		ок	Cancel	Apply

🗹 Note

Changes take effect immediately and a restart is not required.

5. Go back to the API Settings page in the Manager. Click Save.

Save Vulnerability Manager settings

Perform the following steps to save the Vulnerability Manager server settings.

Task

1. In the Manager, select Manager \rightarrow <Admin Domain Name> \rightarrow Integration \rightarrow Vulnerability Assessment \rightarrow MVM \rightarrow Vulnerability Scanning \rightarrow API Server.

The Vulnerability Manager Server Settings page appears.

- 2. Configure the following details:
 - Engine Version— The 7.5 version of Vulnerability Manager used
 - Server Name or IP Address— The IP address of the Vulnerability Manager server
 - Server Port— The server port number

🗹 Note

You can change the default port number.

- **User Name** The user name assigned to the user having the full rights to all the scans initiated from the Threat Explorer
- **Password** The password associated with the username above
- 3. Click Save.

API Server page

Before communication with the Vulnerability Manager server can be established: 1. Start the Foundstone Configuration Management Agent service on the Network S 2. Press the Retrieve MVM Certificate button on this page.	Security Manager server.
	ОК

When the API Server settings is saved, some of the settings like Server IP address and Port settings are updated in the Windows registry. These settings are required for the Foundstone Configuration Management (FCM) Agent Service to communicate with the Foundstone Configuration Management Server.

4. A pop-up opens with the message to start the Foundstone Configuration Management Agent Service. Click **OK**.

🗹 Note

Foundstone and Vulnerability Manager refer to the same product.

Start the FCM agent service

Start the FCM Agent service after updating the permissions for the Windows Registry.

Task

- 1. From the Windows Start button, click Run and open services.msc.
- 2. You can find Foundstone Configuration Management (FCM) Agent here.

Services page

😋 Services						
File Action View	Help					
Services (Local)	😋 Services (Local)					
			Description	1	Charles Trans	1
	Foundstone Configuration	Name -		Status	Startup Type	LOG UN AS
	Management Agent	Application Information	Pacilitates the running of interac		Manual	Local System
	Stop the service	Application Layer Gateway Service	Provides support for 3rd party p		Manual	Local Service
	Restart the service	Application Management Packaround Intelligent Transfer Service	Transfors files in the baskground	Started	Manual	Local System
		Base Eilbering Engine	The Page Silvering Series (PSS) :	Started	Automotic	Local System
	Description:	Cartificate Despendies	Contract services and services and services the services of th	Started	Manual	Local Service
	Provides configuration and updates for	CNG Key Isolation	The CNG key isolation service is	Starteu	Manual	Local System
	all locally installed Foundstone Enterprise	Cold Rey Isolation	Supports Suctor Event Notificati	Started	Automotic	Local System
	sortware components.	COM+ System Application	Manages the configuration and t	Started	Manual	Local System
		Computer Browcer	Mainages the coningulation and c		Dicabled	Local System
		Credential Manager	Provides secure storage and ret		Magual	Local System
		Cruptographic Services	Provides Secare Storage and rec	Started	Automatic	Network S
		DCOM Server Process Laupcher	The DCOMLALINCH service launc	Started	Automatic	Local System
		Desktop Window Manager Session Manager	Provides Desktop Window Mana	Started	Automatic	Local System
		DHCP Client	Registers and undates IP addres	Started	Automatic	Local Service
		Diagnostic Policy Service	The Diagnostic Policy Service en	Started	Automatic (D	Local Service
		Diagnostic Service Host	The Diagnostic Service Host is us	Dearcoa	Manual	Local Service
		Diagnostic System Host	The Diagnostic System Host is us		Manual	Local System
		Disk Defragmenter	Provides Disk Defragmentation C		Manual	Local System
		Distributed Link Tracking Client	Maintains links between NTES fil	Started	Automatic	Local System
		Distributed Transaction Coordinator	Coordinates transactions that sp	Started	Automatic (D	Network S
		ONS Client	The DNS Client service (doscach	Started	Automatic	Network S
		Encrypting File System (EES)	Provides the core file encryption		Manual	Local System
		Extensible Authentication Protocol	The Extensible Authentication Pr		Manual	Local System
		Foundstone Configuration Management Agent	Provides configuration and upda	Started	Automatic	Local System
		Eunction Discovery Provider Host	The FDPHOST service hosts the		Manual	Local Service
		Eunction Discovery Resource Publication	Publishes this computer and reso		Manual	Local Service
		Group Policy Client	The service is responsible for ap	Started	Automatic	Local System
		Arealth Key and Certificate Management	Provides X.509 certificate and k		Manual	Local System
		Human Interface Device Access	Enables generic input access to		Manual	Local System
	1	KE and AuthIP IPsec Keying Modules	The IKEEXT service hosts the Int	Started	Automatic	Local System
	1	A Interactive Services Detection	Enables user notification of user		Manual	Local System
	1	Internet Connection Sharing (ICS)	Provides network address transl		Disabled	Local System
		🔅 IP Helper	Provides tunnel connectivity usin	Started	Automatic	Local System
	1	Agent IPsec Policy Agent	Internet Protocol security (IPsec	Started	Manual	Network S

3. Click the **Start** button () to start the FCM Agent service.

After the FCM Agent Service is successfully started, the SSHStatuscache and Statuscache keys are pushed to Agent software from HKLM\Software\wow6432Node\Foundstone location, with a slight delay of 30 to 40 seconds. The two keys should appear in the registry before proceeding to retrieving the MVM certificate.

- Select Manager → <Admin Domain Name> → Integration → Vulnerability Assessment → MVM → Vulnerability Scanning → API Server.
 - The **Retrive MVM Certificate** option is enabled.
- 5. Click Retrive MVM Certificate to import the client certificates into the Manager keystore.

API Server				
0				
Engine Version:	7.5 🖌 *			
Server Name or IP Address:				
Server Port:	3800			
User Name:	administrator			
Password:				
		Retrieve MVM Certificate	e Save	Test Connection

Vulnerability Manager Server Settings area

Key considerations

Note the following:

- It is no longer required to run the Foundstone Certificate Management tool in the FCM Server. You can copy the client certificates and passphrase to a location in the Manager server.
 - When this version of the Manager is installed or upgraded, the FCM Agent software is installed as a service on the Manager server. This Agent software connects to the Foundstone Configuration Management server and automatically retrieves the client certificates into the Manager Server.
- It is no longer required to run the **FSCertImport.bat** file on the Manager server to import Vulnerability Manager Client certificates into the Manager keystore.
 - Click Retrieve MVM Certificate to import client certificates in the Vulnerability Manager Server Settings page.

Add Vulnerability Manager scan configurations

The fourth and final step in Vulnerability Manager configuration is adding Vulnerability Manager scan configurations.

You can define Scan Configurations (also known as scans) in the Vulnerability Manager system for different host IP address ranges, and then add them to Manager.

When you add a scan configuration to the Manager, a check on whether this scan configuration exists in the Vulnerability Manager database is done. If the scan configuration exists, it is saved in the Manager database. The scan configuration is also updated in the Manager cache.

Manager cache contains the scan configuration ID and the IP address ranges defined in the scan configuration. When the user requests for an on-demand scan of a host IP address from Threat Explorer, the appropriate scan configuration ID is selected. Then, the scan configuration associated with the scan configuration ID is used to scan the host IP address.

🗹 Note

Important pre-requisite: You need to run the scan configuration defined in the Vulnerability Manager engine once, before adding a scan configuration to Manager. Each scan configuration defined in the Vulnerability Manager is associated with a Vulnerability Manager engine. When you run the scan configuration for the first time at the Vulnerability Manager side, the Vulnerability Manager engine in which the scan configuration was last executed, gets associated with that scan configuration. This step is essential for successfully adding the scan configuration to Manager.

🔆 Tip

It is recommended that you define a common *user* in the *organizations* defined in the Vulnerability Manager side. Ensure that this user has full access permissions to Vulnerability Manager engine. Through this user, you can conveniently access various scan configurations defined in all the organizations in Vulnerability Manager. This will ease the access of scan configurations defined in Vulnerability Manager. For more information about organizations and scan configurations, see the section *Working with Scans* in *McAfee Vulnerability Manager Product Guide*. The product names "Foundstone", and "Vulnerability Manager " refer to the same product.

Task

1. Select Manager → <Admin Domain Name> → Integration → Vulnerability Assessment → MVM → Vulnerability Scanning → Scans.

Added Vulnerability Manager Scans dialog

Scans	5		
ı			
	Organization or Workgroup	Scan Name	Description
	NSM	(default)	
	NSM	<u>Win_adv_scan</u>	
	NSM	<u>Win_adv_scan2</u>	
	NSM	<u>Full_vuln_scan2</u>	Full vulnerability scan
			Add Delete

The Added Vulnerability Manager Scan Configurations page appears.

🗹 Note

You can delete individual scan configurations or multiple scan configurations from the **Added Vulnerability Manager Scan Configurations** page. Click **Delete** to delete a scan configuration. For deleting multiple scan configurations, select the required checkboxes, and then click **Delete**.

2. To add a scan configuration, click **New**.

Add a Scan dialog

		8	
Note: Before adding a scan configuration to Network Security Manager, it must first be activated from the McAfee Vulnerability Enterprise Manager user interface at least once.			
Fields marked with an asterisk (*) are required.			
NSP			
Vulnerability			
2			
Vulnerability Scan			
		Save Cancel	
	tion to Network Security Manager, it must first b are required. NSP Vulnerability ☑ Vulnerability Scan	tion to Network Security Manager, it must first be activated from the McAfee Vulnerat are required. NSP * Vulnerability Vulnerability Scan	

The **Add a Scan** window allows you to enter scan configurations, equivalent to already defined configurations in the Scan engine for the different host IP address ranges.

- 3. Enter the Organization or Workgroup name.
- 4. Provide a name for the scan.
- 5. Select Set As Default? if you want to set this scan configuration as the default configuration.
- 6. If necessary, enter a description of the scan configuration in **Description**.
- 7. Select **Save**. The **Added Vulnerability Manager Scan Configurations** page displays all the scan configurations that are added to Manager.

The configuration steps for Vulnerability Manager are complete at this point.

View Vulnerability Manager configuration details

You can view the Vulnerability Manager configuration details in Manager. To do so, perform the following steps.

Select Manager \rightarrow <Admin Domain Name> \rightarrow Integration \rightarrow Vulnerability Assessment \rightarrow MVM \rightarrow Vulnerability Scanning \rightarrow Summary to perform this action from root or child admin domains. The Summary page appears.

Summary page

Summary		
•		
Status		
Allow Vulnerability Scans to be Initiated from the Manager?	Enabled	Run Configuration Wizard
Database Settings		
Server Name or IP Address		
Server Port:	1433	
SSL Type:	Require	
Database Name:	Faultline	
User Name:	sa	
Logon Domain:	n/a	
API Server		
Vulnerability Manager Server Version:	7.5	
User Name:	administrator	
Scan List		
NSM / (default)		
/ Win_adv_scan		
/ Win_adv_scan2		
/ Full_vuln_scan2		

This page shows the details of Vulnerability Manager configuration, such as status of Vulnerability Manager scan enabled/ disabled, database settings, Vulnerability Manager Server settings, and list of scan configurations added to the Manager.

Note that the changes saved in all the pages related to Vulnerability Manager configuration are reflected in the **Summary** page. When you click on the individual links, you are re-directed to the respective pages.

You can also configure Vulnerability Manager settings using Run Configuration Wizard in Summary page.

Import non-vulnerability manager report

The vulnerability assessment scan results of an admin domain can be imported in an XML format from a location in the Manager's file system. You can reformat the scan results and save it to a specific location, so that the Manager automatically imports the result to be later used to determine alert relevance.

🗹 Note

The non-MVM report import feature is disabled if Alert Relevance feature is disabled in the Manager.

Task

 Select Manager → <Admin Domain Name> → Integration → Vulnerability Assessment → Non-MVM Report Import. The Non-MVM Report Import page is displayed.

Non-MVM Report Import	
•	
Enable Automatic Import?	
Import Settings	
Report File Location:	🗢 Default 🛛 🗢 Custom
Report File Name:	C:\Program Files\McAfee\Network Security Manager\App\temp\VA\Import.xml
	The Manager imports results from the above report file at the scheduled import frequency. Details:
	1. The above file must be located on the <u>Manager</u> file system.
	Relative file names are not permitted. (Only absolute file names are allowed.)
	3. The file must adhere to the McAfee XML format:
	Sample XML File
	• <u>McAfee DTD File</u>
	 Only results based on IP address are eligible for import. (Results based on hostname are ignored.)
Import Frequency:	Weekly - Sunday - at 11:30 PM -
Generate Informational Faults:	
Last Import	
Time:	
Result:	
IPs Added / Updated / Ignored:	
Domain Statistics	
Current IPs Tracked:	o 🕕
	Save

2. Select the **Enable Automatic Import?** checkbox.

🗹 Note

By default, this option is not selected.

The **Import Settings** panel is displayed with the following fields.

Option	Definition
Report File Location	Default : Specifies that the file to be imported is available in the default local location Custom : Specify a unique file to be imported for each admin domain.
Report File Name	This text field displays the default location path of the report file to be imported.
	Note: When the Default option is selected for the Report File Location , this text field is disabled and, therefore, cannot be modified. When the Custom option is selected, this text field is enabled and you can specify a unique file name for the specific active directory.
	In an enterprise environment, the default file can be used across all admin domains. In environments such as MSSP where a unique active directory is created for each customer, a unique file can be used for each active directory.
Option	Definition
-------------------------------------	---
Sample XML File	Click on the Sample XML File hyperlink to view the sample file located in the Manager file system, which is in the same directory as the default import file. This sample file can be used as a file template for the XML file.
McAfee DTD File	Click on the McAfee DTD File hyperlink to view the GenVulReportFlat.dtd located in the Manager file system. It provides the details of the XML rules for the XML format.
Import Frequency	 To configure the frequency of import, select the following options: Weekly: For weekly import, select the day (Example:Sunday) from the drop-down list, and select the weekly time for import from the at drop-down list. Daily: For a daily report, select the daily time for import from the at drop-down list.
	Note: The import frequency coincides with the server time.
Generate Informational Faults	Select the Generate Informational Faults to generate an informational fault when the import attempt is successful.

3. Click **Import Now** to import the results from the specified results file location.

Sample XML file

The sample XML file can be used an XML file template for importing the scan result. The sample XML file contains the following root elements.

- <Report Summary> Contains the summary of time and security vulnerability of the scanned vulnerability report
- **<Host Summary>** Contains the summary of the host in the scanned vulnerability report
- **<HostVulnerabilities>** Contains the host vulnerability details of each vulnerability

The following table explains the list of child elements under each root element.

XML child elements	Description
<time summary=""></time>	

XML child elements	Description
<report time=""></report>	The date when the scan was performed Example: 09.10.2015 (MM.DD.YYYY)
<scanstarttime></scanstarttime>	The starting time of the scan Example: 09.10.2015 (MM.DD.YYYY) 18:08:17 (HH:MM:SS)
	Note: The scan start time coincides with the server time.
<scanendtime></scanendtime>	The end time of the scan Example: 09.10.2015 (MM.DD.YYYY) 18:49:37 (HH:MM:SS)
<scanelapsedtime></scanelapsedtime>	The duration of the time elapsed since the scan was performed Example: 0 day(s) 00:41:19 (HH:MM:SS)
<securityvulnerability summary=""></securityvulnerability>	
<totalnumberofvulnerabilities></totalnumberofvulnerabilities>	The total number of vulnerabilities found in the scan
<highseverityvulnerabilities></highseverityvulnerabilities>	The total number of high severity vulnerabilities found during the scan
<mediumseverityvulnerabilities></mediumseverityvulnerabilities>	The total number of medium severity vulnerabilities found during the scan
<lowseverityvulnerabilities></lowseverityvulnerabilities>	The total number of low severity vulnerabilities found during the scan
<informationalvulnerabilities></informationalvulnerabilities>	The total number of informational vulnerabilities found during the scan
<host info=""></host>	
<hostip></hostip>	IP address of the host
<highseverityvulnerabilities></highseverityvulnerabilities>	High severity vulnerabilities found in the host
<mediumseverityvulnerabilities></mediumseverityvulnerabilities>	Medium severity vulnerabilities found in the host

XML child elements	Description					
<lowseverityvulnerabilities></lowseverityvulnerabilities>	Low severity vulnerabilities found in the host					
<informationalvulnerabilities></informationalvulnerabilities>	Informational vulnerabilities found in the host					
<singlevulnerability></singlevulnerability>						
<hostip></hostip>	IP address of the host					
<originaldescription></originaldescription>	The original description of the vulnerability					
<portnumber></portnumber>	The port number of the host					
<protocol></protocol>	The protocol used for communication					
<servicename></servicename>	The service name					
<severity></severity>	The severity of the vulnerability					
<vulnerabilitydescription></vulnerabilitydescription>	The description of the vulnerability					
<solution></solution>	The solution for the vulnerability					
<riskfactor></riskfactor>	The risk factor, if exists					
<cve></cve>	The CVE ID of the vulnerability					
<bid></bid>	BID ID for the vulnerability, if any					
<otherref></otherref>	Other references, if any Example: OSVDB:94 CWE:200					

View import result and domain statistics

After you import a non-MVM report, the details of the import are displayed in the **Last Import** panel. The following details of the import are displayed.

Field	Description
Time	The time stamp of when the import was done
Result	 Displays the status of the import. The following are the available status: Success The import is done successfully. Error The import is not done due to an error. The reason for the error is also displayed. Warning The import is done but not complete. The reason for the warning is also displayed.
IPs Added/ Updated/Ignored	Displays the number of IPs that are added, updated or ignored during the import

The **Domain Statistics** panel displays the number of endpoints for the admin domain for which the vulnerability assessment result is available.

By clicking the **Purge Current Results** in the **Domain Statistics** panel, you can delete all the vulnerability assessment results that are stored for the admin domain.

Purge vulnerability assessment results

In the **Domain Statistics** panel, you can delete the vulnerability assessment results that are stored in the admin domain. To do so, perform the following steps.

Task

- 1. Select Manager → Admin Domain Name → Integration → Vulnerability Assessment → Non-MVM Report Import.
- 2. Click Purge Current Results in the Domain Statistics panel.
- Click OK to purge all results.
 With Purge Current Results, all the details of the import are reset in the Last Import panel.

Vulnerability assessment

McAfee® Network Security Platform recommends the following while performing Vulnerability Assessment:

- Always use the latest signatures available for your vulnerability assessment (VA) software. This will help ensure the assessment is accurate.
- Where possible, scan all hosts you expect McAfee Network Security Platform to protect. This will help increase the probability that a relevancy status of "Unknown" really means that the attack is not relevant.

• If the scan traffic between the Vulnerability Manager server and the hosts being scanned passes through a Sensor monitoring port, the Sensor may consider it as attack traffic and take the corresponding response action such as quarantining the Vulnerability Manager server. To prevent this:

- Create ACLs to exclude all traffic from the Vulnerability Manager server from attack inspection. For information, see Configuring ACL rules, *McAfee Network Security Platform Product Guide*.
- If you have configured Quarantine, add the Vulnerability Manager server to the Quarantine Exceptions list. This prevents the Vulnerability Manager server being quarantined.
- Replace old reports with new reports on a routine basis (weekly or monthly). Given the frequency with which new attacks appear, reports can become obsolete quickly, and render VA integration ineffective.
- Replacing an old report with a new one might result in similar alerts having different relevance values. For example, if Network Security Platform uses an initial scanner report to analyze one alert and an updated scanner report to analyze the next, it may correctly draw different conclusions for each. To avoid confusion, consider acknowledging (or purging) all existing alerts each time you replace reports.

Relevance analysis of attacks

Relevance analysis involves the analysis of the vulnerability relevance of real-time alerts using the vulnerability data imported into the Manager database. The imported vulnerability data can be from Vulnerability Manager or other supported vulnerability scanners such as Nessus.

Vulnerability assessment reports from the scanners contain vulnerabilities detected in a specific host(s) in the network. For example, a vulnerability assessment report will display that the host 10.1.1.x is vulnerable to buffer overflow attack, along with the CVE ID /BugTraq ID of the attack. Manager uses the imported scan report to determine whether the host identified is vulnerable to that particular attack.

The attack cache in Manager stores the CVE ID of the attacks detected by the McAfee® Network Security Sensor. In the case of relevance analysis, the CVE ID of the vulnerability in the imported report is compared to the CVE ID in the attack cache in Manager. If a matching record is found, the corresponding alert is marked as Relevant. This record is used by the alert correlation module during alert processing to check for the relevancy type, and also used to update the **Relevance** field in the Attack Log.

The status of relevance analysis can be viewed in the **Attack Log** page. The Relevance column is displayed when it is selected from the **Columns** drop-down list.

You can also view the alerts sorted by **Relevance** category in the **Attack Log** page. For more information, see the section *Attack Log* in the *McAfee Network Security Platform Product Guide*.

Marking alerts from vulnerable hosts as relevant helps the network administrator to easily view and sort alerts by relative relevance.

The relevancy analysis lookup is done for real-time alerts by either importing the vulnerability data from Vulnerability Manager database, running an on demand scan, or manual import. You can opt to configure the lookup for relevancy from Vulnerability Manager database instead of the relevancy cache in the Manager.

Menu options for relevance analysis

The Manager gives you the option to use Vulnerability Manager data in relevance analysis. Select **Manager** \rightarrow **Admin Domain Name**> \rightarrow **Integration** \rightarrow **Vulnerability Assessment** \rightarrow **MVM** \rightarrow **Alert Relevance**.

The following menu options are displayed:

Relevance menu options



ltem	Menu option	Description
1	Alert Relevance	Contains the sub-menu options to configure relevance analysis settings
2	Summary	Summary details of relevance analysis configuration in the Manager
3	Enable	Enable relevance analysis.
4	Manual Import	Manually import vulnerability scanner reports to Manager database.
5	Automation	Schedule automatic import of vulnerability reports to Manager database.
6	Database	Configure the Vulnerability Manager database settings for relevance analysis.
7	Scans	Add scan configurations in Manager.

ltem	Menu option	Description
8	Troubleshooting	Troubleshooting options like reloading Vulnerability Manager cache, resetting relevancy cache, and re-submitting database updates

🗹 Note

The menu options explained above are mentioned as *Relevance menu options* throughout this document.

Relevance configuration details

To view the relevance configuration details in Manager, do the following:

Select Manager \rightarrow <Admin Domain Name> \rightarrow Integration \rightarrow Vulnerability Assessment \rightarrow MVM \rightarrow Alert Relevance \rightarrow Summary or Manager \rightarrow <Child Admin Domain Name> \rightarrow Integration \rightarrow Vulnerability Assessment \rightarrow MVM \rightarrow Alert Relevance \rightarrow Summary to perform this action from root or child admin domains. The Summary page is displayed.

This page shows the details of relevance configuration, such as status of relevance analysis enabled/disabled, Scanner Reports imported manually, Scan import schedule, database settings, and automated scan reports.

Note that the changes saved in all the pages related to relevance configuration are reflected in the **Summary** page. When you click on the individual links, you are redirected to the respective pages.

You can also configure relevance settings using Run Configuration Wizard in the Summary page.

Use relevance configuration wizard

You can use the Relevance Configuration Wizard for configuring relevance settings from Manager.

Task

1. Select Manager \rightarrow <Admin Domain Name> \rightarrow Integration \rightarrow Vulnerability Assessment \rightarrow MVM \rightarrow Alert Relevance \rightarrow Summary or Manager \rightarrow <Child Admin Domain> \rightarrow Integration \rightarrow Vulnerability Assessment \rightarrow MVM \rightarrow Alert Relevance \rightarrow Summary for performing this action from root or child admin domains.

2. In the **Summary** page, click **Run Configuration Wizard**.

- 3. The wizard displays the following pages in order:
 - Enable
 - Manual import
 - Automation
 - Database
 - Scans
 - Troubleshooting

- 4. Use **Next >** or **< Back** buttons to navigate through the pages.
- 5. There are five configuration steps in total. Select **Finish** at the end of the fifth step.

Relevance analysis configuration in Manager

You can configure the Relevance settings in Manager in two ways:

- 1. Manually navigating the configuration screens
- 2. Using the Relevance Configuration Wizard

Manually navigating the configuration screens

Following steps are essential for configuring Relevance settings in Manager (in the given order):

- Enabling attack relevance analysis
- Manual import of scan reports
- Automatic import of scan reports
- · Vulnerability manager database settings for relevance analysis
- Adding scan configurations for relevance analysis

Using the Relevance Configuration Wizard

You can also use the Relevance Configuration Wizard for the configuration tasks listed above.

Enable attack relevance analysis

This is the first essential step in configuring Manager for relevance analysis.

To enable relevance analysis, do the following:

- Select Enable from Relevance menu options (Manager → <Admin Domain Name> → Integration → Vulnerability Assessment → MVM → Alert Relevance → Enable or Manager → <Child Admin Domain Name> → Integration → Vulnerability Assessment → MVM → Alert Relevance → Enable to perform this action from root or child admin domains).
- 2. The **Enable** page is displayed.
- 3. Under **Enable**, select any of the following options from the drop-down list in the **Use Scan Results to Enhance Alert Relevance Accuracy?** field:
 - Passive Relevance
 - Active Relevance
 - Disabled

Passive relevance option

You can add a passive relevance option. To do so, perform the following steps.

Task

1. Under Enable, select Passive Relevance option from the drop-down list next to Use Scan Results to Enhance Alert Relevance Accuracy?.

Relevance tab

Enable		
0		
Enable Alert Relevance Analysis?	Active Relevance	anso analysis is analysis the Manager can determine
	Active Relevance Disabled	ally-imported vulnerability information and/or on that has been automatically imported from MVM on a poption requires MVM database and API server settings.)
		Save

- 2. The Manager uses the imported vulnerability scan report to determine the vulnerability relevance of real-time alerts. The CVE ID of the vulnerability in the imported report is compared to the CVE ID in the attack cache in the Manager. If a match is found, the corresponding attack is marked as Relevant.
- 3. Click Save.

The screen is refreshed and you get an update that the changes have been updated.

Active relevance option

You can add an active relevance option. To do so, perform the following steps.

- 1. Under Enable, select Active Relevance option from the drop-down list in Use Scan Results to Enhance Alert Relevance Accuracy? field.
- 2. The Manager queries the Vulnerability Manager database for the real-time lookup of the relevancy data. Unlike Passive Relevance, when **Active Relevance** option is configured, the Manager does not lookup for relevancy for every alert received into Manager alert queue from the Sensor. When the alert is received from IPS Sensor, Relevancy is set to "*Pending*" state initially. After a minute, relevancy for these alerts with pending state are updated by performing a relevancy lookup from Vulnerability Manager database.

🗹 Note

In addition to the current Relevancy cache, the Manager maintains a separate cache for the relevancy data returned by the stored procedure for the destination IPs.

3. Click Save to save your settings. The screen is refreshed and you get an update that the changes have been updated.

Disabled option

Under **Enable**, select the **Disabled** option from the drop-down list in **Use Scan Results to Enhance Alert Relevance Accuracy?** field to disable the relevance analysis.

Query and retrieve asset information from Vulnerability Manager database

For the host that has already been scanned using Vulnerability Manager Scan engine, the Asset Details are returned by the Vulnerability Manager. If the Vulnerability Manager fails to return the data, you can initiate a scan for that IP address from the Threat Explorer.

Follow this procedure to initiate a scan from the Threat Explorer

Task

1. In the Manager, navigate to **Analysis** \rightarrow **<Admin Domain Name>** \rightarrow **Threat Explorer**.

/My	Company > Threat Explorer								0
Thr	eat Explorer								
0					Top:	10 - Attacks	 Any Direction 	n 🔻 Last 7 days	- 0
Ad	ld Filter View Attacks								
То	p Attacks								•
								Attack Name	-
									ount
1	SNORT: test http uri for NOT	operation(sid:55555	Exploit	unassigned		High			368,396
2	MALWARE: Malicious PDF file	transfer detected	Malware	PDF-Emulation		High			347,469
3	MALWARE: Malicious PDF file	transfer detected VII	Malware	PDF-Emulation		Medium			347,469
4	MALWARE: Malicious PDF file	transfer detected II	Malware	PDF-Emulation		Medium			347,469
5	MALWARE: Malicious PDF file	transfer detected III	Malware	PDF-Emulation		Medium			347,469
6	P2P: BitTorrent Meta-Info Re	trieving	Policy Violation	restricted-application		Medium			259,064
7	SNORT: PROTOCOL DNP3 HE	ADER OPTION DNP3	Exploit	unassigned		High			77,112
8	IM: Gmail Chat Traffic Detect	ted	Policy Violation	restricted-application		Medium			64,675
9	P2P: BitTorrent File Transfer	HandShaking	Policy Violation	restricted-application		Medium			63,545
10	P2P: LimeWire Alive		Policy Violation	restricted-application		Medium			54,200
То	p Attackers								0
									; •
									ount
1					Unk	nown			1,392,904
2					Unk	nown			29,611
3					Unk	nown			19,734
- 4					Unk	nown			17,483
-5					- Onk	nowin			9,027

2. Click Add Filter.

The Add Filter Criterion dialog is displayed.

Add Filter Criterion				8
Filter On: Value:	Attacker IP Address	▼	•	
			Save	Cancel

3. Select **Attacker IP Address** in the **Filter On:** field, enter the attacker IP address in the **Value** field and click **Save** If the attacker IP has already been scanned, the scan results are displayed.

Threat Explorer													
0					Тор:			Attacks			Last 1 hour		
Filter: Attacker IP Address X Add Filter View Attacks													
Attacker IP Address -													
												al Tabs 🔻	
Endpoint Information	ePO Threat Events Vulner	ability Assessment											
Country:			Domain/Workgroup:										
DNS Name:			User:										
NetBIOS Name:			Data Source:										
Operating System:			McAfee Agent Check-In Time:										
Device Type:			Endpoint Type:										
MAC Address:													
Network Forensics													
Top Attacks													۵
Attack Name													
1 SNORT: SPYWARE-P	UT Trackware alexa runti	Exploit		unassigned				🔺 Medi	ium				258
2 IM: Web Based Insta	ant Messenger Services	Policy Violation		restricted-applicatio				🔺 Medi	ium				188
3 P2P: LimeWire Alive		Policy Violation		restricted-applicatio	n			🔺 Medi	ium				168

4. If the attacker IP has not been scanned, click **Scan for Vulnerabilities** to scan the attacker IP address and view the results.

Threat Explorer					
0	Top: 25	 Attacks 	 Any Direction 	01/01/17 6:07 PM - 08/24/21 6	5:07 PM 👻 💭
Filter: Attacker IP Address 10.20. X Add Fi	lter View Attacks				
Attacker IP Address - 10.20.					
					onal Tabs 🔻
Endpoint Information ePO Threat Events Vulnerabili	ty Assessment				
General Activity					
Overall Criticality: None					
Last Scan Time: 2021-08-2					
By Scan Engine: WIN-D6CC					
Open Ports					
ProtoPort Service Description					
Vulnerabilities					
Risk Name			CVE		
Scan for Vulnerabilities					

Import scan reports manually

This is the second (optional) step in configuring Manager for relevance analysis. This step is optional if you are using Vulnerability Manager scans, because you can import Vulnerability Manager scan reports either manually or automatically as per schedule. Other third party scans only be imported manually.

You can manually import scanner reports from supported scanners like Vulnerability Manager or NessusWX to the Manager. For importing other third-party vulnerability scanner reports (like Qualys or nCircle), you need to convert the report to the Network Security Platform format.

Refer the DTD included with Network Security Platform (GenVulReportFlat.dtd) when converting your XML-based format to the Network Security Platform format.

To manually import a vulnerability scanner report in Manager, do the following:

Task

 Select Manual Import from Alert Relevance menu options (Manager → <Admin Domain Name> → Integration → Vulnerability Assessment → MVM → Alert Relevance → Manual Import or Manager → <Child Admin Domain Name> → Integration → Vulnerability Assessment → MVM → Alert Relevance → Manual Import for performing this action from root or child admin domains).

Manually Imported Scan Reports area

Import a Scan Report dialog

Manually Imported Scan Reports					
0					
	File Name	Report Type	Description	Scan Time	State
No scan reports present					
	bbA				

Import a Scan Report		8
Use this page to import a vulner. Fields marked with an asterisk (Please Select Nessus	
Import a Scan Report		McAfee Vulnerability Manager
Report Type:	McAfee Vulnerability Manager 🔻 🚬 *	NSM
Description:	Malware Scan	
Report file:	Choose File NSP_10.1_Been-us.pdf *	
Enable on import?	2	
		Import Report Cancel

3. Select a **Report Type** from the drop-down list.

🗹 Note

The report can be from any of the supported scanners or formats.

- 4. Provide a **Description** corresponding to the selected scanner report type.
- 5. Click Choose File and choose a Report file. You can select a report file from the local machine.
- 6. To import the report to Manager database, select **Enable on import?** checkbox.
- 7. Click Import Report to import the scanner report.
- 8. The scanner report is imported to Manager database, and displayed in the Manually Imported Scan Reports page.

🗹 Note

The imported report is stored in Manager database in Network Security Platform format. In the **Manually Imported Scan Reports** window, if you select the link in **File Name** field, you can view the report in Network Security Platform format in a separate window.

Supported vulnerability scanners and formats

Network Security Platform supports the following vulnerability scanner versions and report formats:

Scanners supported	Scanner version	Report format
Vulnerability Manager Enterprise	7.0 and 7.5	XML
NessusWX	6.x	Plain text
Third party vulnerability scanners (for example, Qualys, nCircle)		Network Security Platform format

Vulnerability reports from the above scanners can be imported to Manager.

Vulnerability Manager format

McAfee Vulnerability Manager Enterprise is a vulnerability assessment (VA) platform for automated discovery and prioritization of system vulnerabilities and threats in an enterprise network.

Network Security Platform supports Vulnerability Manager reports in the XML format only. Vulnerability Manager XML reports include assessments sorted by hostname (Host_Data.xml) and risk (Risk_Data.xml). Network Security Platform supports both these formats.

You can manually or automatically import Vulnerability Manager scan reports to Manager.

NessusWX

Nessus is an open-source vulnerability assessment scanner that follows a client/server model. The Nessus server (nessusd) only runs on UNIX, but there are Nessus clients available for both UNIX and Windows.

Network Security Platform supports the popular Windows client, NessusWX. Note that NessusWX reports should be saved as plain text, since in this case, Network Security Platform supports only plain text format.

Network Security Platform format

Customers who use third-party vulnerability scanners (for example, Qualys and nCircle) can manually import the corresponding scanner reports to Manager.

To successfully import and view these scanner reports in the Manager, the third party reports should be converted to an intermediate XML format, as per the Document Type Definition (DTD) provided by Network Security Platform. This XML format is known as Network Security Platform format.

🗹 Note

Refer the DTD included with Network Security Platform (GenVulReportFlat.dtd) when converting your XML-based format to the Network Security Platform format.

Why Network Security Platform format is used?

Since, there is no industry standard for the format of vulnerability assessment reports, Network Security Platform converts all imported reports into the Network Security Platform format. In this way, support for new report formats can be added without having to change the way the Alert Correlation Engine works. The converted report and its metadata are stored in a new table called **iv_vul_record** in the Manager database, which is saved as part of the standard backup and MDR synchronization processes.

Import scans automatically

This is the third (optional) step in configuring Manager for relevance analysis. This step is optional if you are using Vulnerability Manager scans, because you can import Vulnerability Manager scan reports either manually or automatically as per schedule. Other third party scans only be imported manually.

For importing scanned vulnerability reports from Vulnerability Manager database to Manager database, you can use the Automation function in Manager.

During the automatic import process, the Automation scheduler invokes a stored procedure in the Vulnerability database, which returns all the vulnerability data to the Manager database. The vulnerability data retrieved corresponds to the scan configuration that was used for vulnerability assessment. Manager retrieves the relevance information based on the last import time of Automation.

Task

 Select Manager → <Admin Domain Name> → Integration → Vulnerability Assessment → MVM → Alert Relevance → Automation to perform this action from root or child admin domains. The Vulnerability Manager Scheduler window is displayed.

Automation sub-tab

Automation	
0	
Automate MVM Scan Report Import?	🛡 Yes 🔍 No
Frequency:	● Daily ● Weekly SUN ▼
	Start at: 00 • Hr and 05 • Min

- 2. Select **Yes** for **Automate MVM Scan Report Import?** option. This enables automatic import of reports by the scheduler.
- 3. To schedule the frequency of import on a weekly or daily basis, select **Daily** or **Weekly** import options for the **Frequency**.
- 4. Select the start time for scheduler operation from **Start At**.
- If you wish to import the vulnerability data from Vulnerability Manager immediately, select Import Now!.
 The page is refreshed, and a message is displayed that vulnerability data is successfully imported from Vulnerability Manager database.
- 6. Click **Apply**, to save your settings. The page is refreshed, and a message is displayed that the settings are successfully updated.

🗹 Note

The Import Now! feature available in the parent domain, at Manager \rightarrow <Admin Domain Name> \rightarrow Integration \rightarrow Vulnerability Assessment \rightarrow MVM \rightarrow Alert Relevance \rightarrow Automation, is not applicable for child domains that have Vulnerability Manager settings (Manager \rightarrow <Admin Domain Name> \rightarrow Integration \rightarrow Vulnerability Assessment \rightarrow MVM \rightarrow Alert Relevance \rightarrow Enable or Manager \rightarrow <Child Admin Domain Name> \rightarrow Integration \rightarrow Vulnerability Assessment \rightarrow MVM \rightarrow Alert Relevance \rightarrow Enable or Manager \rightarrow <Child Admin Domain Name> \rightarrow Integration \rightarrow Vulnerability Assessment \rightarrow MVM \rightarrow Alert Relevance \rightarrow Enable) set to Inherit Settings?. Consequently, Import Now! and Apply buttons are not seen in the Automation page (Manager \rightarrow <Admin Domain Name> \rightarrow Integration \rightarrow Vulnerability Assessment \rightarrow MVM \rightarrow Alert Relevance \rightarrow Automation or Manager \rightarrow <Child Admin Domain Name> \rightarrow Integration \rightarrow Vulnerability Assessment \rightarrow MVM \rightarrow Alert Relevance \rightarrow Automation or Manager \rightarrow <Child Admin Domain Name> \rightarrow Integration \rightarrow Vulnerability Assessment \rightarrow MVM \rightarrow Alert Relevance \rightarrow Automation or Manager \rightarrow <Child Admin Domain Name> \rightarrow Integration \rightarrow Vulnerability Assessment \rightarrow MVM \rightarrow Alert Relevance \rightarrow Automation or Manager \rightarrow <Child Admin Domain Name> \rightarrow Integration \rightarrow Vulnerability Assessment \rightarrow MVM \rightarrow Alert Relevance \rightarrow Automation or Manager \rightarrow <Child Admin Domain Name> \rightarrow Integration \rightarrow Vulnerability Assessment \rightarrow MVM \rightarrow Alert Relevance \rightarrow Automation of Such child domains.

Vulnerability Manager database settings for relevance analysis

This is the fourth step in configuring Manager for relevance analysis.

To retrieve the relevance information from Vulnerability Manager database, it is essential to configure the Vulnerability Manager database settings in the Manager.

Task

1. Select Manager \rightarrow <Admin Domain Name> \rightarrow Integration \rightarrow Vulnerability Assessment \rightarrow MVM \rightarrow Alert Relevance \rightarrow Database Settings to perform this action from root or child admin domains.

- 2. Database Settings window for relevance analysis configuration is displayed.
- 3. The fields in the **Database Settings** page under **Alert Relevance** are similar to the **Database Settings** page under the **Vulnerability Scanning**.

Add scan configurations for relevance analysis

This is the fifth and final step in configuring Manager for relevance analysis.

Scan configurations defined in Vulnerability Manager are to be added to the Manager. This is required for initiating Vulnerability Manager scans from the Threat Explorer. Depending on the host IP address, the appropriate scan configuration in Manager is used to scan the host.

When you enable relevance analysis, Manager automatically imports the latest results for each Vulnerability Manager scan, and uses them for relevance analysis.

Following steps are essential for adding scan configurations:

Task

- Select Manager → <Admin Domain Name> → Integration → Vulnerability Assessment → MVM → Alert Relevance → Scans to perform this action from root or child domains.
- 2. The Added Vulnerability Manager Scan Configurations page for relevance analysis is displayed.
- 3. The fields in the Added Vulnerability Manager Scan Configurations page under the Alert Relevance are similar to the Added Vulnerability Manager Scan Configurations page under the Vulnerability Scanning.

Fault messages for Vulnerability Manager scheduler

Following table lists the fault messages associated with Scheduler report import process:

Fault displayed	Severity	Description
Vulnerability data import from Vulnerability Manager database was successful	Informational	This message indicates that the vulnerability data import from Vulnerability Manager database by the Scheduler is successful.
Scheduled Vulnerability Manager vulnerability data import failed	Critical	This message indicates that the vulnerability data import by the Scheduler from Vulnerability Manager database has failed.

When you click on the fault links, you can view the details of the fault and the possible actions for correcting the fault.

Support for Vulnerability Manager custom certificates

In order to use Vulnerability Manager custom certificates, you should run the Vulnerability Manager *Certificate Management tool,* which generates the custom client certificates. Third-party SOAP clients can use the custom client certificates for SSL client authentication with FoundScan engine.

🗹 Note

For more information about FCM tool installation and importing custom certificates to java keystore, refer the *FSCustomCerts-Readme.txt* file in the following path in Manager server: //Network Security Platform/config/fscerts/

🗹 Note

For more information about creating custom client certificates using FCM tool, see Working with SSL certificates, *McAfee Vulnerability Manager Product Guide*.

🗹 Note

The product names, "Foundstone", and "Vulnerability Manager" refer to the same product.

Generate Vulnerability Manager SSL custom certificate for Manager

You can generate Vulnerability Manager SSL custom certificate for the Manager. To do so, perform the following steps.

Task

- 1. Download and unzip the Vulnerability Manager Certificate Manager Installer. Select the correct version for your installation of Vulnerability Manager.
- 2. Copy this file to the Vulnerability Manager server and run it. This installs the Vulnerability Manager Certificate Management Tool.

Note

The Certificate Management Tool must be run on the server hosting the 'FCM Server Component' depending on the version of the Vulnerability Manager (7.0 or 7.5).

- 3. Launch the Vulnerability Manager Certificate Management Tool.
 - a. Click the Create SSL Certificates tab.
 - b. Type the name of the Manager server in the Host Address field and click Resolve.
 - c. After the hostname is resolved, click Create Certificate using Common Name.

🗹 Note

After running the Vulnerability Manager Certificate Management Tool on the server hosting the Vulnerability Manager FCM Server application, a .zip file (ThirdPartyAPI-SSL.zip) gets generated. It contains certificates for the 3rd-party clients that can be used for SSL client authentication with the Vulnerability Manager engine. The .zip file contains the following certificate files:

- FoundstoneCAPublicCertificate.pem
- FoundstoneClientCertificate.p12
- FoundstoneClientCertificate.pem
- FoundstoneClientPublicCertificate.cer
- d. Save the resulting file (ThirdPartyAPI-SSL.zip) to the desktop.
- e. The tool also creates a new passphrase for the certificate.
- f. Copy and save the passphrase in a text file and name it passphrase.txt.
- g. Copy passphrase.txt into ThirdPartyAPI-SSL.zip.

Import the custom certificates into the Manager keystore

You can import the custom certificates into the Manager keystore. To do so, perform the following steps.

Task

- 1. On the Manager create a new folder named customcerts at <Manager install directory>\config\fscerts\customcerts
- 2. Copy the ThirdPartyAPI-SSL.zip from Vulnerability Manager server to a temporary folder on the Manager server and extract the contents to the customcerts folder you just created.
- 3. On the Manager server, select **Start** \rightarrow **Run**, type and then click **OK**. Navigate to <Manager install directory>\bin
- 4. At the command prompt, for the parent and each child domain created on the Manager, type the following commands using the following parameters:

FScertimport <MVM version #> <"MainDomainName\ChildDomainName">

For example, if your main domain in the Manager is "AmazingDeals", you have created child domains named "EastCoast", "MidWest", and "WestCoast" under that domain, and you are integrating with Vulnerability manager 7.0, your certificate install commands would be as follows:

- FScertimport 7.0 "AmazingDeals"
- FScertimport 7.0 "AmazingDeals\EastCoast"
- FScertimport 7.0 "AmazingDeals\MidWest"
- FScertimport 7.0 "AmazingDeals\WestCoast"
- 5. Each time you run the Vulnerability Manager Certificate importer, you will be asked for the Import password. Enter that passphrase at the **Import Password** prompt.

This is the passphrase that you captured when the Certificate Management Tool was run on Vulnerability Manager server.

- 6. Enter **Y** for the **Trust this Certificate? [no]** prompt.
- 7. The custom certificates are now imported to the Manager.

- 8. The FSCertImport.bat utility generates two keystore files (fs.keystore and fstrust.keystore) each time you run the utility. These files are placed in the customcerts folder in a hierarchy of \Version#\DomainName.
- 9. Run an OnDemand scan from Threat Explorer for any IP to check if the client authentication works for the newly imported keystore files generated for Vulnerability Manager custom certificates.

Troubleshooting options

Following troubleshooting options are available with respect to Network Security Platform-Vulnerability Manager integration and Relevance Analysis:

- Reloading Vulnerability Manager cache If the added scan configurations are suspected as missing from Manager
- Resetting the relevancy cache If you wish to reload the data in Manager Relevancy Cache, that is presently used by Manager for relevance analysis
- Updating the Vulnerability Manager database again If you suspect that the Vulnerability Manager database is not updated with the tables and stored procedures that are required for importing information from Vulnerability Manager database to Manager database.

To access the Troubleshooting options in Manager, Select Manager \rightarrow <Admin Domain Name> \rightarrow Integration \rightarrow Vulnerability Assessment \rightarrow MVM \rightarrow Alert Relevance \rightarrow Troubleshooting for performing this action from root or child admin domains.

Troubleshooting Options area

Troubleshooting Options	
0	
Cache	
	Reload Scan Cache
Database Updates	
	Resubmit Database Updates

🗹 Note

The Reload Scan Cache button is visible only when integration with Vulnerability Manager is enabled, and scans are added.

Reload Vulnerability Manager cache

The **Reload Scan Cache** option helps you to load the Vulnerability Manager web cache in Manager with the most recent scan configurations retrieved from Vulnerability Manager.

Task

- 1. Make sure that you have enabled Vulnerability Manager configuration and added the scan configurations to Manager.
- 2. You can access **Cache** page in two ways:
 - From Vulnerability Manager configuration settings— Select Manager \rightarrow <Admin Domain Name> \rightarrow Integration \rightarrow Vulnerability Assessment \rightarrow MVM \rightarrow Vulenrability Scanning \rightarrow Troubleshooting to perform this action from root or child admin domains.
 - From Relevance settings— Select Manager \rightarrow <Admin Domain Name> \rightarrow Integration \rightarrow Vulnerability Assessment \rightarrow MVM \rightarrow Alert Relevance \rightarrow Troubleshooting to perform this action from root or child admin domains.
- 3. Click **Reload Scan Cache** to update the Vulnerability web cache in Manager with the latest scan configurations from Vulnerability Manager.

A message is displayed that the reload is successful.

The **Reload Scan Cache** button will not be visible in the **Troubleshooting** link for the reasons provided in the following table.

#	Reason	Solution
1	Vulnerability Manager configuration is disabled.	Enable Vulnerability Manager configuration.
2	Vulnerability Manager scan configurations are not added to Manager.	Add scan configurations to Manager.

Reset relevancy cache

If you want to update the relevancy cache in Manager, reset the cache from the troubleshooting options.

Task

- 1. Select Manager \rightarrow <Admin Domain Name> \rightarrow Integration \rightarrow Vulnerability Assessment \rightarrow MVM \rightarrow Alert Relevance \rightarrow Troubleshooting.
- 2. Select **Resubmit Database Updates**. A message is displayed that the relevancy cache was successfully reloaded.

Resubmission of database updates

When the Vulnerability Manager database settings are configured, Manager automatically updates Vulnerability Manager database with tables and stored procedures that are required to retrieve relevance information from the database.

If you find that database is not properly updated with the required tables and stored procedures, you can resubmit the updates to the Vulnerability Manager database from Manager. Select **Manager** \rightarrow **<Admin Domain Name>** \rightarrow **Integration** \rightarrow **Vulnerability Assessment** \rightarrow **MVM** \rightarrow **Alert Relevance** \rightarrow **Troubleshooting** for this purpose.

Select **Resubmit Database Updates** to resubmit the updates to the Vulnerability Manager database.

Vulnerability Manager - Certificate Sync and FC Agent issues

Problem	Solution
FC Agent service doesn't get installed while installing the Manager	 To install FCAgent service: Download the software vcredist_x86.exe and run it in that host. Download link: https://www.microsoft.com/en-us/download/details.aspx?id=26999 At the command prompt, go to c:\Program Files (x86)\foundstone\FCM and run the command fcagent -i to install the service.
When you click on API tab in the Manager, internal server error is displayed	 This issue might be seen in some systems when the command sc query FCAgent is executed internally in the Manager. To run this command, the server in which manager is deployed might not have the right permission settings. The administrator has to provide permission to run sc.exe. To change permission settings for sc.exe: Go to //windows/system32/sc.exe. Right-click sc.exe and select Properties. Click the Security tab. Add a local service and provide full permission.
FCAgent service doesn't start in Manager server	 To integrate with Vulnerability Manager, the Manager must update the Windows registry. However, the user account used to run the Manager service will not have permissions to write to the Windows registry if the Manager is fully locked down. To give that user account the required permissions, follow these steps: 1. On the server running the Manager, run regedit.exe. 2. Change the permissions on registry and allow Full Control to 'Local Service' for the following keys: HKLM HKLMSoftware HKLM\Software\Foundstone

Problem	Solution
	 Right-click on these keys and choose Permissions. Add the user account used to run the Manager service (likely LOCAL SERVICE). Give that user account Full Control over the key. Click OK.
	Note: Changes take effect immediately. A reboot is not required.
	7. In the API Server page, click Save .
	Note: If the operating system is 64-bit, perform this procedure for the following keys:
	 HKLM HKLM\Software HKLM\Software\wow6432Node HKLM\Software\wow6432Node\Foundstone
You are able to start the FC Agent service, clicking	It might be because port 3801 is not enabled in the API server. Check if port 3801 has been enabled.
on 'Retrieve MVM Certificate' returns error message.	Vulnerability Manager could be deployed in distributed mode where FCM Server could be in one server, and the API Server, DB, Enterprise Manager, and Scan Engines could be in another server. In the API server page, try configuring the FCM Server IP address and port 3801. Try clicking the Retrieve MVM Certificate button. If the OnDemand scan fails, try changing the port back to 3800.
Retrieve MVM certificate is failing even though the SSHStauscache and Statuscache keys are present in the registry	 This might occur if C:\Program Files\Foundstone or C:\Program Files(x86)\Foundstone does not have write permission for Local Service. 1. Add local service and give full permission to local service. 2. Click Retrieve MVM Certificate again after giving the required permissions.

Error messages

The following error messages are associated with the integration:

Failed to save settings

This is displayed when the Manager fails to write the Foundstone specific keys into the Windows Registry.

Failed to retrieve the MVM certificate

This error message is displayed if:

- You click Retrive MVM Certificate before the start of the service
- The certificate synchronization is still in progress
- If the user account used to run the Manager service does not have permission to write to the Windows Registry or, if the Manager is fully locked down.

Solution

- 1. On the Network Security Manager server, click **Start** \rightarrow **run**, type regedit.exe.
- 2. Right-click the **HKEY_LOCAL_MACHINE HKEY_LOCAL_MACHINE\Software** key.
- 3. Select Permissions.
- 4. Add the user account used to run the McAfee Network Security Manager service.
- 5. Give that user account Full Control over the key.
- 6. Click **OK**.
- 7. Repeat steps 1 to 6 for the following keys:
 - HKEY_LOCAL_MACHINE\Software\wow6432Node
 - HKEY_LOCAL_MACHINE\Software\wow6432Node\Foundstone
- 8. Click **Start** \rightarrow **run**, type services.msc, and click **OK**.
- 9. Start the Foundstone Configuration Management Agent service.
 - 🗹 Note

The changes take effect immediately. You do not have to reboot.

- 10. If this service starts and stops again, add the following registry key:
 - a. Go to HKEY_LOCAL_MACHINE\Software\Wow6432Node\Foundstone\
 - b. Right-click the right panel.
 - c. Create a **String Value** and name it BasePath.
 - d. Double-click the newly created key and add the following value:

C:\Program Files (x86)\Foundstone (or path where the Foundstone files are located on the Manager server)

- e. Repeat steps 8 and 9 to start the Foundstone Configuration Management Agent service.
- f. To restart the Vulnerability Manager Configuration Wizard, go to Manager \rightarrow <Admin Domain Name> \rightarrow Integration \rightarrow Vulnerability Assessment \rightarrow MVM \rightarrow Vulnerability Scanning \rightarrow Summary, and click Run Configuration Wizard.

OR

Select Manager \rightarrow <Admin Domain Name> \rightarrow Integration \rightarrow Vulnerability Assessment \rightarrow MVM \rightarrow Vulnerability Scanning \rightarrow API server.

g. Click Retrieve MVM Certificate.

Failed to communicate with the API server

This error message is displayed for Vulnerability Scan Information.

Integration with McAfee Logon Collector

The Manager can display a variety of information about the hosts inside and outside a network.

In the Attack Log, the host user name is available along with the IP address.

The Manager integrates with McAfee Logon Collector (MLC) to display user names of the hosts in your IPS and NTBA deployments. The Logon Collector provides an out-of-band method to obtain user names from the Active Directories.

Benefits

This integration helps to provide information about source and destination users.

Integration requirements

The following are the minimum requirements for this integration:

- Manager version— 10.1 and later
- Logon Collector version 2.0 and later
- System requirements—
 - For running Logon Collector 2.0 and 2.1: Windows Server 2003 and 2008
 - For running Logon Collector 2.2: Windows Server 2008 R2 and 2012

🏹 Tip

The Logon Monitor is part of the Logon Collector bundle that you downloaded.

Download the software

Download the bundled Logon Collector and Logon Monitor software from the McAfee website.

- 1. In a web browser, go to https://secure.mcafee.com/apps/downloads/my-products/login.aspx?region=us.
- 2. Provide your grant number, and select the appropriate product category (for example, McAfee® Firewall Enterprise Appliance).
- 3. Select the McAfee Logon Collector version, for example McAfee Logon Collector 3.0.
- 4. Download the zip file for the Logon Collector installation. Extract the files to your local directory.
- 5. Find the Logon Collector installation program and download it to your local directory. The Logon Monitor is part of the Logon Collector bundle that you download.

8 | Integration with McAfee Logon Collector

🗹 Note

If you want to have a separate remote Logon Monitor installation, select the **McAfee Logon Monitor** folder and find the installation program.

How Network Security Platform - Logon Collector integration works

Logon Collector is a Microsoft Windows-based distributed collector. It is an independent service installed in a network, which obtains and preprocesses the network entities data from the Active Directories in the network. The data include users, IP to user bindings, computer groups, new IP addresses, and new computers. This information is published in the form of messages.

This solution does not require any modification to Active Directory or the Active Directory directory schema and requires no agents.

Logon Monitors can be used to poll nearby domain controllers and forward collected information on to the Logon Collector, shortening the distance domain controller communication must travel.

Identity Acquisition Agent (IAA), is deployed on the Network Security Platform side and is used as an interface to listen to the message service where the updates are published by the Logon Collector server. IAA listens to the Logon Collector Active Message Queue (MQ) service and regularly receives new updates from the Logon Collector server.

A listener for receiving the updates is registered with the IAA. The registered listener regularly receives new updates from the Logon Collector through IAA.

All IP to user bindings data are loaded into a newly created Manager cache for the first time. The cache is subsequently updated with the differences on subsequent updates. As all the other components of the Manager can query the Manager cache, it is not required to communicate with the Logon Collector server each time an update happens.

Manager-Logon Collector integration



Configuration details for Logon Collector integration

This section gives the configuration details for the integration between McAfee® Network Security Manager and Logon Collector server.

Configure integration at the admin domain level

You can enable the integration between the McAfee® Network Security Manager and the Logon Collector server at the admin domain level.

- 1. Navigate to Manager \rightarrow <Admin Domain Name> \rightarrow Integration \rightarrow MLC. The Enable page is displayed.
- 2. To enable the MLC integration, select the Enable MLC Integration? checkbox.
- 3. Enter the Server Name or IP Address and Server Port details.

Enable Logon Collector

MLC					
•					
Enable MLC Integ	gration?				
Server Name or I	IP Address:				
Server Port:					
Certificates					
Export Certifi	icate				
Export Manage	er Certificate:	Export to file	Open MLC Console		
Import Certif					
New MLC Certificate:	O Upload MLC	Certificate 🔍 🖣	Paste Certificate		
Upload MLC Certificate:	Browse No				
Current MLC Certificate:	BEGIN CERTI MIICIJCCAY+gAv BAYTADEJMACG DTI5MTAXM2A5 ADEJMACGA1UE NU5TNFUwg28 e7qK/KHklynko XoPKK9dh0Uu/y ASIJX387hIVXYD V28mi9PmRnm- qNuFH3/8sihg2/ T8F9WR32lyWk 	IFICATE VIBAGUAMbAEg29; A1UECBMAMQkw QDDBNNTENfV0IG M2E1NVowVTEJM CCMAMQkwBwYU CRFF25XmCY19J0C c/LyKHHeKBAgME +hsxrUPRgiLA11+k rTtgNP8pxUC2Lpy WwBtupOYliacdRzr (CATE	znGNMA0GCSqGSlb3DC JRWYDVQQHEwAxCTAH DLTZCRkFPODVOUzRVM AcGA1UEBhMAMQkwBh DVQQLEwAXHDAaBgNV QEBBQADgY0AMIGJAOG CEDXG+0AFpg2FwBq9SP DIByqnVYsFgZ2zbxtscUC 3AAEwDQYJKoZIhvcNAQ ca1djBm2J3M+rTJRSqDR c0E42btLRyIaQVD/6/PQ- xpO/TIXc=	2EBBQUAMFUxCTAHBgNV BgNVBAoTADEJMAcGA1UE IB4XDTE5MTAXNJA5MzE1N wYDVQQIEwAxCTAHBgNVB BAMME01MQ19XSU4INkJC BAJG0m1BzV1CNregkwC1 J0WD17f/hTMDNNIJ SUJmd9vGovh/4Cy+q IEFBQADgYEAg0pW9AIH mXqgWQkm0e8Rru1hUF 40wop0+cs31hDL98L	SCXMA IVOX BACT GQU84
				Re	emove
				Test Connection	Save

- 4. To complete the integration, you have to synchronize the certificates between the MLC console and the Manager. Click the **Export to file** link to export the Manager certificate to MLC.
- 5. To import the MLC certificate, select **Upload MLC Certificate**, import the certificate from the location by clicking **Choose File**.
- 6. Click Save.

To test the connection, click **Test Connection**.

Establishment of trust between Network Security Manager and Logon Collector server

Logon Collector communicates with the McAfee® Network Security Manager through a two-way SSL authentication. This requires the exchange of certificate between the McAfee® Network Security Manager and the Logon Collector server.

Import the Manager certificate into Logon Collector

Export the Manager certificate, save the file to your local directory, and import the file to Logon Collector. Refer to the *McAfee Network Security Platform Product Guide* for exporting the Manager certificate.

- 1. In the Logon Collector console, select **Menu** \rightarrow **Configuration** \rightarrow **Trusted CAs**.
- 2. Click New Authority to open the New Trusted Authority window.
- 3. Select Import From File, then click Browse to add the exported file saved in your local directory.

You can also use the Copy/Paste Certificate option.

4. Click Save.

Import the Logon Collector certificate

By default, Logon Collector is pre-installed with a self-signed certificate. If you have a different certificate signed by a CA, you can import this certificate and replace the existing Logon Collector certificate.

Task

- 1. In the Logon Collector console, select Menu \rightarrow Configuration \rightarrow Server Settings.
- 2. In the Settings Categories section, click Identity Replication Certificate.
- 3. Upload the Logon Collector certificate.
 - a. Copy the Logon Collector certificate from the Logon Collector console and paste it in a newly created file in your local directory.
 - b. Under Import Certificate section, click Upload MLC Certificate in the New MLC Certificate option.
 - c. Select Upload MLC Certificate, then click Browse to add the Logon Collector certificate from your local directory.

What to do next

🗹 Note

If the existing Logon Collector certificate is changed, the clients connecting to Logon Collector, such as Firewall Enterprise and Network Security Manager, need to import the new Logon Collector certificate.

Display of Logon Collector details

You can view user information received from the McAfee® Logon Collector server in **Attack Log**. Refer to the *McAfee Network Security Platform Product Guide* for details.

Display user details (Logon Collector data) in Attack log

If you have configured the Logon Collector you can view user details in the Attack Log page.

- 1. Navigate to Analysis \rightarrow <Admin Domain Name> \rightarrow Attack Log.
- Double-click the alert for which you want to view the alert details. The alert details panel opens.
- 3. You can view the user details in the Attacker / Target section.

User details in Attack Log

☆ MALWARE: File Submitted to ATD for Analysis				
			Export 👻 💭	
Summary Details	s Description			
Event			0	
Time:	Oct 23, 2019	Domain:	/My Company	
Direction:	Outbound	Device:	_169_225	
Result:	Inconclusive	Interface:		
Relevance:	Unknown	Matched Policy:	Default Prevention	
Application:	🕏 нттр	Zone:		
Protocol:	http	VLAN:		
Detection:	Signature	Assigned To:		
Acknowledged:	🗸 Yes	Alert ID:	319289602561443 6469	
Attacker / Target			8	
	Attacker	Target		
IP Address (Port):	🤣 🚺 1.1.	(80) 📀 📷 🌘	D 1.1. (48490)	
Hostname:				
VM Name:				
VM IP:				
Proxy IP:				
os:				
User:	\user2	\use	er2	

The user details (Logon Collector data) are displayed in the **Attack Log** page only if the option to display is enabled in the ems.properties file. If it is not enabled, perform the following steps to enable the option.

- a. In the Manager, using Windows Explorer go to C:\Program Files\McAfee\Network Security Manager\App\config.
- b. Locate the ems.properties file, and right-click and open it using Windows Notepad.
- c. Ensure that the following values are configured (If the entries are not available, add the entries manually): iv.mlc.alert.preprocessor.enabled=true iv.mlc.alert.preprocessor.daemon.enabled=true

Display of Logon Collector details in Network Security Manager reports

Manager reports display the user information received for Logon Collector. Refer to the *McAfee*® *Network Security Manager* documentation for details.

Next Generation custom reports

In the McAfee® Network Security Manager, select **Analysis** \rightarrow **Event Reporting** \rightarrow **Next Generation Reports** \rightarrow **New**.

Option 1

When you select the **Display Options** as **Table**, the **Available Fields** section includes **Src UserId** and **Dest UserId**. The generated custom reports contain the data about the source and destination users.

Table properties — Src UserId and Dest UserId fields

/My Company > Event Reporting > Next Generation Reports (?)			Ø			
Data Source		Presentation	Data Filter			
Choose the fields to be shown i	n this report.					
Available Fields	Selected Fields					
Dest Port >						
Dest Reputation						
Dest UserId >				_		
Dest VM >						
Detection Engine						
Src ESX Server	Select some columns to display.					
Src IMSI						
Src IP						
Src Name						
Src Object Name						
Src OS						
Src Phone >						
Src Port						
Src Reputation						
Src UserId						
Src VM						
Time >						
VLAN ID						
				Back	Next	Cancel

Option 2

When you select the **Display Options** as **Bar Chart**, the **Bar Labels** section includes the **Src UserID** and **Dest UserID** options. The generated custom reports contain the data about the source and destination users.

Src UserId and Dest UserId fields options in the bar chart



Option 3

When you select the **Display Options** as **Pie Chart**, the **Pie Slice Labels** section includes the **Src UserID** and **Dest UserID** options. The generated custom reports contain the data about the source and destination users.





Communication error

A connection error report is shown in the **Error** column of McAfee® Network Security Manager **System Faults** monitor on the McAfee® Network Security Manager **Dashboard** tab when there is an improper communication between the McAfee® Network Security Manager server and Logon Collector server. From the McAfee® Network Security Manager **Dashboard** tab, click any error listed in the **System Faults** monitor to display the error details on the **Faults** tab in **Manager** \rightarrow **Admin Domain Name**> \rightarrow **Troubleshooting** \rightarrow **Logs**.

Error link in the System Faults monitor



Error display in the Faults page

NSM						Adr	ninistrator 💄 <i>I</i> My Co	ompany IST ? 🗗
Trellix	⑦ Dashboard	🖳 Analysis	🗟 Policy	🖽 Devices	🏟 Manager			3₩
Domain: /My Company								Ø
▶ Updating	^	Logs						
 Setup 	1	Faults System Files	Background Tasks	User Activities MDR Eve	nts	k		
 Integration Reporting 		0		Unacknowledged	 Last 7 days 		Clear A	Il Filters
Maintenance			Fault <u>Severity</u>	Summary			Duration (minutes)	Device
 Troubleshooting Health Check Alert Relevance 		1 Oct 14, 2019 04:04	:15 📙 Error	GAM Engine U	Ipdate Status	Sensor NS7150_32 current status is: GAM update Failure while downloading update files . This fault will be cleared on successful update.		NS7150_32
Manager Policy Logs	Cache v	Ack Unack Del	ete Save as CS\	V Other Actions 🔻				1 Logs

Integration with HP Network Automation

McAfee® Network Security Platform supports integration with HP Network Automation (formerly Opsware). HP Network Automation is a network automation software that is used to automate network changes, configuration, and compliance management.

HP Network Automation Integration supports communication between the Manager and HP Network Automation server. The communication is about the changes in Sensor configuration due to the pushing of signature set to Sensors.

You can export the Sensor configuration XML file to a particular folder in the Manager. A syslog forwarder message with the path and name of the XML file (containing the changes in Sensor configuration) is sent to the HP Network Automation server. This is performed by configuring the IP address of the HP Network Automation server in the Manager. Each Sensor has its own Sensor configuration export XML file. So, the filename should contain the Sensor name (Example: Sensor name.xml). Whenever a signature set is pushed to the Sensor, the XML file pertaining to the Sensor is overwritten with the latest Sensor configuration changes and a syslog forwarder message is sent to the HP Network Automation server.

The syslog forwarder message contains the following information:

- Name of the Sensor configuration XML file
- Path on the Manager server where the Sensor configuration XML file is located
- User ID of the user or system that pushed the signature set
- Admin domain name of the Sensor

Configure HP Network Automation in the Manager

You can configure the HP Network Automation server details in the Manager. To do so, perform the following steps.

Task

1. Select Manager \rightarrow <Admin Domain Name> \rightarrow Integration \rightarrow HP Network Automation.

Enable page

/My Company > Integration > HP Network Automation			?
HP Network Automation			
0			
Enable HP Network Automation Integration ?	O Yes ● No		
Server Name or IP Address			
Server Port:	1099		
Facilities:	Security/authorization (code 4) <		
XML Directory:	folder/sample.xml		
Message Preference:	System default (Note: After you click Save and your HP Networ customized message instead of the System Def	rk Automation configuration is saved, you have the option to creat fault.)	e a
		Save	Reset

The **Enable** page is displayed.

2. Fill in the following fields.

Field	Description	
Enable HP Network Automation Integration?	Enables or disables HP Network Automation Integration. Yes to enable; No to disable.	
Server Name or IP Address	Server name or IP address of the HP Network Automation server.	
Server Port	HP Network Automation server port number.	
Facilities	Allows you to select the following from the drop down list: • Security/ authorization (code 4) • Security/ authorization (code 10) • Log audit (note 1) • Log alert (note 1) • Clock daemon (note 2) • Local user 0 (local0) • Local user 1 (local1) • Local user 2 (local2) • Local user 3 (local3) • Local user 4 (local4) • Local user 5 (local5) • Local user 7 (local7)	
Field	Description	
--------------------	--	
XML Directory	Path on the Manager server where the Sensor configuration XML file is located.	
Message Preference	Set the preferred type of message in syslog forwarder.	

3. Click Save.

Customizing Message Preference

Click Save.

System default is selected, by default.

- a. Select **Customized** to customize the message preference.
- b. Click **Edit** to edit a customized message preference.
- c. Click **Save** to save settings.

Integration of the Manager with SIEM products

You can extend Network Security Platform data to third-party management products. By integrating the Manager with Security Information and Event Management (SIEM) products, you can further process Network Security Platform data. A SIEM product might query the Manager database for information (pull model), or the Manager can send alert and system fault data to syslog servers (push model).

The following are some of the products that Network Security Platform customers are known to have used:

- McAfee
 NitroSecurity products such as NitroView DBM
- ArcSight
- Cisco MARS (Protego)
- eSecurity
- GuardedNet
- NetForensics
- NetlQ
- Network Intelligence
- QRADAR from Q1Labs
- Sequation
- Symantec Remote Importer
- Tenable Networks

Manager data available for SIEM products

There are various methods by which you can extend Manager data to SIEM products. You can choose one based on the data involved and the type of the SIEM product.

The following methods are available:

- Configure the Manager to push data to a SIEM product.
- Configure a SIEM product to pull data from the Manager.
- Query the Manager database for data.

The Manager itself provides multiple methods for backing up configuration and analysis data, including all policy, ignore rule, alert, and any associated packet information. These backup, archive, and export techniques, however, will only allow for the retrieval of the information through the Manager. A SIEM product must access the Manager through the standard system integration techniques.

The following data is available to SIEM products:

• Alert information — When an attack is detected, an alert is raised and the configured response is executed. The alert information contains, where applicable, the specific attack details such as type, attacker and target addresses and ports, packet logs, and outcome.

• Packet log information — A policy can include the requirement to log the packet information that is associated with an alert. This information is a record of the actual flow of traffic that triggered the attack and can be used for detailed packet analysis. This information must be pulled from the Manager database.

• System Faults — Fault information contains the following details:

- Admin domain where the fault is detected
- Sensor name
- Name of the fault
- Type of fault
- Fault owner
- Fault level
- Time of the fault
- Fault source
- Fault component
- Severity
- Description
- Acknowledged flag

To view the list of all fault informational items, select **Manager** \rightarrow **<Admin Domain Name>** \rightarrow **Setup** \rightarrow **Notification** \rightarrow **Faults** \rightarrow **Syslog**. Provide all the details and click **Save.** Then select **Customized** and click **Edit.** You can query faults from the iv_alarm table in the Manager database.

ACL Logs – Access Control Lists

Methods of integration with SIEM products

There are various methods to integrate SIEM products with Network Security Platform and access its information. For example, you can use SNMP traps, syslog, or scripts. The methods that you can use depend on the information that you want to access; not all information is available through all methods. The following is a matrix of the information that you can access from the Manager and the corresponding methods that you can use.

Method Data					
₽	SNMP	Syslog	Scripts	SQL query	Report
Alert data	Yes	Yes	Yes	Yes	Yes
Packet Log data	No	No	No	Yes	No

Method					
Data					
₽	SNMP	Syslog	Scripts	SQL query	Report
System fault	Yes	Yes	Yes	Yes	Yes
ACL	No	Yes	No	No	No
Audit	No	Yes	No	Yes	Yes

Configure notification methods

For some information, you can configure the Manager to trigger a notification to SIEM products. For example, you can configure the Manager to notify alerts and system faults. You can configure alert notification based on the severity of attacks or on a perattack basis. You can also configure notification per attack in the relevant policy.

Configure notifications based on attack severity

You can configure notifications based on attack severity. To do so, perform the following steps.

Task

- 1. Select Manager \rightarrow <Admin Domain Name> \rightarrow Setup \rightarrow Notification \rightarrow IPS Events.
- 2. Open the required notification method and select the respective severity level for each of the configured methods.

Configure notifications per attack

You can configure notifications per attack. To do so, perform the following steps.

Task

- 1. In the Manager, navigate to Policy \rightarrow <Admin Domain Name> \rightarrow Intrusion Prevention \rightarrow Policy Types \rightarrow IPS Policies.
- 2. Double-click the required policy.
 - The Attack Definitions page opens.
- 3. Double-click the attack for which you want to configure notifications.
 - The **<Attack Definitions Details>** panel opens on the right side.

- 4. Select the required notification methods in the **Manager Actions** section.
- 5. Click Update.
- Click Save in the Attack Definitions page to save the changes updated to the attack.
 In case of faults, you can use syslog to monitor for specific faults such as Link Failure or Bypass modes.

Templates for syslog, email, and pager

If you are parsing the notifications sent through email, script, or pager, McAfee recommends that you define your custom message template. Default template may change in newer releases and it may break your parsing algorithms.

The following tables describe the variables used in the various message templates.

🗹 Note

"%" "/" and "\$" are reserved characters. Do not use them as a delimiter in custom templates.

Variable name	Description
ALERT_ID	Unique ID assigned to an alert by the Manager
ALERT_TYPE	The type of the attack that triggered the alert. The value, for example, can be exploit, host sweep, or port scan.
ATTACK_TIME	Time when the attack was detected
ATTACK_NAME	Name of the attack that triggered the alert
ATTACK_ID	The Network Security Platform ID for the attack
ATTACK_SEVERITY	System impact severity posed by the attack: high, medium, low, or informational
ATTACK_SIGNATURE	Signature that matched the attack traffic (applicable only to signature-based attacks)
ATTACK_CONFIDENCE	Higher the confidence, the lower is the chance for the attack to be a false-positive.
ADMIN_DOMAIN	The admin domain to which the Sensor that detected the attack belongs
ATTACK_COUNT	The number of times the attack was detected within the throttle duration

Variable name	Description
SENSOR_NAME	The Sensor that detected the attack
INTERFACE	The Sensor's interface where the attack was detected
SENSOR_CLUSTER_MEMBER	The Sensor in a fail-over pair that detected the attack
SOURCE_IP	IP address of the host from where the attack originated
SOURCE_PORT	The source port number of the attack traffic
DESTINATION_IP	IP address of the targeted host
DESTINATION_PORT	The destination port number of the attack traffic
CATEGORY	General attack type
SUB_CATEGORY	Within the attack type, a specific classification such as virus and Trojan horse
DIRECTION	Whether the traffic was inbound or outbound
RESULT_STATUS	Whether the attack was successful, blocked, or a failed attempt
DETECTION_MECHANISM	The method used to detect the attack. Each method relates to a specific attack category. Some of these methods are signature, threshold, statistical anomaly, and flow correlation.
APPLICATION_PROTOCOL	The application protocol found in the attack traffic
NETWORK_PROTOCOL	The transport protocol used for the attack traffic
RELEVANCE	Information whether the attack is relevant for the targeted host based on information from McAfee Vulnerability Manager
QUARANTINE_END_TIME	Time when an attacking host will be out of quarantine
SENSOR_ALERT_UUID	Unique ID assigned to an alert by the Sensor

Variable name	Description
SOURCE_VM_ESX_NAME	The VMware ESX server that hosts the VMware from which the attack traffic originated
SOURCE_VM_NAME	The VMware host from which the attack traffic originated
TARGET_VM_NAME	The targeted VMware host for the attack
TARGET_VM_ESX_NAME	The VMware ESX server that hosts the targeted VMware
URI_INFO	The URI found in the attack traffic
VLAN_ID	The VLAN tagged with the attack traffic
DEST_APN	Applicable only to attacks targeted at data-enabled mobile equipments such as a mobile phone or a tablet PC.
	The Access Point Name (APN) of the targeted mobile equipment
DEST_IMSI	Applicable only to attacks targeted at data-enabled mobile equipments such as a mobile phone or a tablet PC.
	The International Mobile Subscriber Identity (IMSI) of the targeted mobile equipment
DEST_PHONE_NUMBER	Applicable only to attacks targeted at data-enabled mobile equipments such as a mobile phone or a tablet PC.
	The phone number of the targeted mobile equipment
SRC_APN	Applicable only to attacks from data-enabled mobile equipments such as a mobile phone or a tablet PC.
	The Access Point Name (APN) of the mobile equipment that is the source of the attack traffic
SRC_IMSI	Applicable only to attacks from data-enabled mobile equipments such as a mobile phone or a tablet PC.
	The International Mobile Subscriber Identity (IMSI) ID of the source mobile equipment
SRC_PHONE_NUMBER	Applicable only to attacks from data-enabled mobile equipments such as a mobile phone or a tablet PC.

Variable name	Description
	The phone number of the source mobile equipment
LAYER_7_DATA	The application-layer data found in the attack traffic
ZONE_NAME	Zone from which the alert was raised; applicable only for NTBA alerts
SOURCE_OS	Source OS name
DEST_OS	Destination OS name
MALWARE_FILE_TYPE	Malware file type
MALWARE_FILE_LENGTH	Malware file length
MALWARE_FILE_NAME	Malware file name
MALWARE_FILE_MD5_HASH	Malware file MD5 hash
MALWARE_VIRUS_NAME	Malware virus name
MALWARE_CONFIDENCE	Malware confidence
MALWARE_DETECTION_ENGINE	Malware detection engine

The following table describes the fault template variables.

Name	Description
ADMIN_DOMAIN	The admin domain associated with the fault message
FAULT_NAME	Name of the fault
FAULT_TYPE	The state of the fault, whether it is created, acknowledged, or cleared
OWNER_ID	The Sensor ID where the fault occurred. This field is not applicable to Manager faults.

Name	Description
OWNER_NAME	The user-defined name of the Sensor where the fault occurred. For Manager fault, the value is 'Manager.'
FAULT_LEVEL	The level of the fault. Whether it occurred at the Manager system level, Sensor level, or Sensor interface level.
FAULT_TIME	Timestamp of when the fault occurred
FAULT_SOURCE	Whether the fault was sent by the Sensor to the Manager or it was generated by the Manager
FAULT_COMPONENT	The component where the fault occurred
SEVERITY	Whether the fault is critical, an error, warning, informational, or unknown
DESCRIPTION	The description as found in the faultNameAndText.properties file
ACK_INFORMATION	If true, the fault has been acknowledged by someone.
SENSOR_NAME	The user-defined name of the Sensor where the fault occurred

The following table describes Firewall access rule template variables.

Name	Description
SENSOR_NAME	The Sensor that parsed the traffic matching the Firewall access rule
ADMIN_DOMAIN	The admin domain to which the Sensor belongs
INTERFACE	The interface where the matching traffic was detected
ACL_ACTION	Whether the traffic was inspected, dropped, denied, or ignored
SOURCE_IP	The IP address of the host from which the traffic originated

Name	Description
SOURCE_PORT	The source port number of the traffic that matched the Firewall access rule
DESTINATION_IP	The IP address of the destination host for the traffic
DESTINATION_PORT	The destination port number of the traffic that matched the Firewall access rule
APPLICATION_PROTOCOL	The layer 7 protocol associated with the traffic that matched the Firewall access rule
NETWORK_PROTOCOL	The IP protocol that matched
ALERT_DURATION	The number of Firewall syslog messages that were suppressed
ALERT_COUNT	The number of Firewall syslog messages that were forwarded
ALERT_DIRECTION	Whether the traffic that matched was inbound or outbound
APPLICATION	The layer 7 application associated with the matched traffic
ACL_DESCRIPTION	The user-entered description of the Firewall policy
SOURCE_HOSTNAME	The host DNS name from which the traffic originated
DESTINATION_HOSTNAME	The host DNS name to which the traffic is destined
SOURCE_COUNTRY	The country from which the traffic originated
DESTINATION_COUNTRY	The country to which the traffic is destined to
ACL_POLICY	The name of the Firewall policy
ACL_RULE_NUMBER	The order of the rule in the effective list of Firewall access rules

Integration for fault information

Fault provides information about the current status of your Network Security Platform installation. Fault notification can be configured based on the severity of a fault.

A complete list of faults is available in the <Manager install directory>/config/FaultNameAndText.properties file.

You can use the following methods to forward fault information:

- SNMP traps
- Syslog
- Scripts
- Email
- Pager

If you are parsing fault notifications, it is recommended that you customize the notification that suits your needs.

🗹 Note

Default fault notification format may change in newer releases of the Manager.

The following table details the methods to forward fault information.

Method	Information
SNMP traps	 You need the following to configure the Manager to send SNMP traps: SNMP trap daemon to receive traps SNMP trap server IP address SNMP trap server Community string SNMP trap server port
	 Note: If you are using SNMPv3, you might also need the following: Authentication type authentication password Encryption type Privacy password
Syslog	You can configure the Manager to notify syslog servers for alerts, system faults, Firewall access rule matches, and user-activity audit for the Manager. If you enable syslog notification for Firewall access rules, and if you have enabled Firewall access rules logging per Sensor, the Manager sends a syslog message to the configured syslog server for each connection attempt matching an rule. This enables you to track your users' connection attempts and the results. You need the following to configure the Manager to forward syslog messages: • Syslog server IP

10| Integration of the Manager with SIEM products

Method	Information
	 Communication port number Syslog facility Note: Syslog is based on UDP. Therefore, the Manager doesn't retransmit data in case of network
	connectivity issues or if the syslog server is unreachable.
	Configuring syslog notification involves the following steps:
	1. To forward alerts to a syslog server, configure the syslog details in the Manager. See <i>McAfee Network Security Platform Product Guide</i> .
	 To forward fault notifications to a syslog server, configure the syslog details at Manager → <admin domain="" name=""> → Setup → Notification → Faults → Syslog. See the Manager's Help for the steps.</admin> To forward ACL rule matches to a syslog server, configure the syslog details in the Manager. See <i>McAfee Network Security Platform Product Guide</i> To forward user-activity details of the Manager server to a syslog, configure the details at Manager
	\rightarrow Common Domain Name \rightarrow Setup \rightarrow Notification \rightarrow Oser Activity \rightarrow Sysing. See the Managers Help for the steps.
Email and	You can configure the Manager to do the following:
pager	Notify alerts and faults through email or pager.Send scheduled reports through email.
	Note the following:
	 Make sure the antivirus application is not blocking outgoing emails. Make sure you have enabled mail relay on the SMTP server.
	Configuring email notification involves the following steps:
	1. Configure the email server settings in the Manager. The following features use this email server settings:
	 Reports Fault notification Alert notification Pager
	 See the <i>McAfee Network Security Platform Product Guide</i> for the details. 2. To enable e-mail notification only for specific attacks, edit those attacks in the relevant policies. See <i>McAfee Network Security Platform Product Guide</i>

10 | Integration of the Manager with SIEM products

Method	Information
	 For alert notification through email or pager, configure the email notification and the email recipients in the Manager. See <i>McAfee Network Security Platform Product Guide</i>. To enable fault notification through email or pager, configure the email notification and the email recipients in the Manager. Go to Manager → <admin domain="" name=""> → Setup → Notification → Faults → E-mail. See the Manager's Help for the steps.</admin> To enable the Manager to email auto-generated reports, configure the recipients in the General Settings of the Reports module. See <i>McAfee Network Security Platform Product Guide</i>
Scripts	Scripts are useful for complex integrations. Scripts are a sequence of commands that can use template variables. The Manager replaces these variables with the relevant values before executing the command. For example, you can use scripts to extract information from the alerts and send customized emails for specific conditions. Scripts can invoke another batch file and provide variables as command line parameters for the invoked program. For more information, refer to <i>McAfee Network Security Platform Product Guide</i> . Also see the Readme.doc at <manager directory="" installed="">\McAfee\Network Security Manager\App\diag\AlertNotificationScript</manager>
Suppression	 While configuring some of the notification methods, you can specify the suppression time value. Suppression time is the time (minutes and seconds) the Manager should wait after an alert notification has been sent before sending another alert notification. The default and minimum value is 10 minutes. Suppression time is useful to avoid sending excessive notifications when there is heavy attack traffic. The specify suppression time value for the following notification methods: Email Pager Scripts Suppression time value does not apply to syslog and SNMP. All events are forwarded.

Integration using reports

In the Reports module of the Manager, you can schedule reports on a daily or weekly basis. You can configure the Manager to email the reports. You need to create relevant reports and parse CSV files. See the *McAfee Network Security Platform Product Guide* for details.

Data mining

Applications that require the real-time synchronization of Manager data, including packet logs, are best served by performing regular SQL queries to the Manager database. An example would be Security Information and Event Management (SIEM) applications. SIEM applications can use direct database-based integration through which they can poll the Manager database and monitor specific tables for new records. Applications that do not require the packet log data that is associated with an alert can use the push techniques of SNMP or Syslog.

For applications like reports that are more ad-hoc in nature, an efficient approach would be to copy the database and manipulate it off-line. The less work the database has to do within the Manager, the better will be the performance of the Manager. Therefore, by cloning or copying the database, operations, such as large queries, or creating additional indices, can be performed on the off-line database. In addition to just copying the files from the Manager, you can use the Manager's data back-up feature (i.e. back-up, alert & packet log archival). See *McAfee Network Security Platform Product Guide* for details about these features.

🗹 Note

Alert information is stored in the iv_alert and iv_alert_data tables. Packet captures for alerts are stored in the iv_packetlog table.

You can query Manager database tables for several types of IV_<variable> information.

The following table describes IV_Alert information.

Field	Туре	Null	Key	Default value	Description/Comments
uuid	bigint(20)	NO	MUL	Unique	Unique ID number of message
state	smallint(6)	YES	MUL		state of alert (NULL = closed, 1 = new, others) 1: unacknowledged 10: acknowledged
markForDelete	char(1)	YES			First in line for deletion during old-alert purging
lastModTime	timestamp	NO		Current time stamp.	the last time this alert was modified in the database
lastModUserRef	char(32)	YES			User who last modified the alert in the database

Field	Туре	Null	Key	Default value	Description/Comments
assignedUserRef	char(32)	YES			To whom the alert is assigned to for action
sensorId	int(11)	NO	PRI		The ID of the Sensor raising the alert. This ID is assigned to a Sensor by the Manager.
vsaId	int(11)	NO		-1	The VSA ID of the VIDS to which the alert applies
vidsId	int(11)	YES			The VSA ID of the VIDS to which the alert applies
liId	int(11)	NO		-1	The LI ID to which the alert applies.
subscriberIdl	int(11)	YES			Subscriber1, subscriber2, and so on are
subscriberId2	int(11)	YES			the last non-null id being the admin domain to whom this VIDS belongs, and
subscriberId3	int(11)	YES			the earlier ones being its parents going back to the root admin domain ID. Alerts
subscriberId4	int(11)	YES			for the root subscriber will have all these columns as NULL.
alertType	smallint(6)	NO			 The type of alert, where: 1 = signature 2 = statistical anomaly 3 = threshold anomaly 4 = port scan 5 = host sweep 6 = throttle summary
categoryId	int(11)	YES			The attack category id of the alert
subCategoryId	int(11)	YES			The attack sub-category id of the alert

Field	Туре	Null	Key	Default value	Description/Comments
detectionMechanism	int(11)	YES			The method used to detect the attack
attackId	int(11)	NO			The 24-bit part of the attack ID
creationTime	timestamp	NO	MUL		The timestamp on the Sensor when this alert raised
emsReceivedTime	timestamp	YES			The timestamp on the Manager when this alert is received. This may be greater than creation time if alert was in Sensor buffer due to connectivity issues with Manager.
severity	tinyint(4)	NO			High, Medium, Low, Informational
alertDuration	int(11)	YES			If alerts are suppressed, then these many alerts were suppressed for this duration before this one. These are only filled for a throttle summary alert.
slotId	smallint(6)	NO			The slot number of the port from which the alert was raised
portId	smallint(6)	NO			The port number of the port from which the alert was raised
alertCount	int(11)	YES			Greater than 1 in case of throttled alerts
packetLogId	bigint(20)	YES			The packet log ID corresponding to this alert
packetLogGrpId	bigint(20)	NO			The packet log group ID corresponding to this alert
packetLogSeq	int(11)	YES			A sequence number within the packet log stream

[11] [11]	YES			For alerts that have previous-256-byte fragments, the offset of the last byte in that packet in the request streams.
(11)	YES			
				For alerts that have previous-256-byte fragments, the offset of the last byte in that packet in the response streams.
ar(1)	YES			Whether a previous-256-byte fragment was sent
allint(6)	YES			The signature ID within the attack ID
(11)	YES			The protocol ID from protocols.xml file
allint(6)	YES			The protocol ID from the IP-header of the packet
ar(32)	YES			The IP address of the source of the attack
(11)	YES			The source port for the attack traffic
ar(32)	YES			The IP address of the target for the attack
(11)	YES			The destination port of the attack traffic
vint(4)	YES			The confidence level of the signature that was matched. Inverse of BTP value. High confidence
				means low BTP.
				Confidence value ranges from 1-7.
				 S. night confidence 3-5: Medium
	ar(1) allint(6) (11) allint(6) (11) (11) (11) (11) (11) (11) (11) ((11)YESar(1)YESallint(6)YES(11)YESallint(6)YESar(32)YES(11)YESar(32)YES(11)YES(11)YESyint(4)YES	YESar(1)YESallint(6)YES(11)YESallint(6)YESar(32)YES(11)YESar(32)YES(11)YES(11)YES(11)YES(11)YES(11)YES	YESYESar(1)YESallint(6)YES(11)YESallint(6)YESar(32)YES(11)YESar(32)YES(11)<

Field	Туре	Null	Кеу	Default value	Description/Comments
					>=6: Low
					Note: When the BTP value is 0, there is no corresponding confidence value for the attack.
protoQuall	int(11)	YES			
protoQual2	int(11)	YES			
protoParsingState	int(11)	YES			The inner state of the protocol parsing machine
direction	tinyint(4)	YES			Whether the attack was inbound or outbound
suppressedSigIds	int(11)	YES			Corresponding signature IDs of the alerts that were suppressed
nidId	int(11)	YES			Global VIDS network ID from where the alert is raised
firstAlarmTime	timestamp	YES			
accumulateTime	int(11)	YES			
thresholdId	int(11)	YES			
observedValue	bigint(20)	YES			The threshold measurement which triggered the alarm
thresholdValue	int(11)	YES			The actual threshold value that was crossed

Field	Туре	Null	Key	Default value	Description/Comments
thresholdDuration	int(11)	YES			The duration over which the value was measured
attackIdRef	char(20)	YES			The Network Security Platform attack ID reference
resultSetValue	int(11)	YES			 Whether the attack succeeded, blocked, failed, suspicious and so on. 100 ATTACK_SUCCESSFUL 200 INCONCLUSIVE 300 ATTACK_FAILED 400 NOT_APPLICABLES 999 ATTACK_BLOCKED 888 DOS_BLOCKING_ACTIVATED 10100 BLOCKING_SIMULATED_ATTACK SUCCESSFUL 10200 BLOCKING_SIMULATED_INCONCLUSIVE 10300 BLOCKING_SIMULATED_ATTACK_FAILED 10400 BLOCKING_SIMULATED_N
inlineDropAction	int(11)	YES			Information used by the Sensor to tell the Manager whether the attack was blocked or not. INLINE_ACTION_PACKET_DROPPED = 0x01; INLINE_ACTION_BROWSER_MATCHED = 0x04; INLINE_ACTION_BROWSER_FAILED = 0x08; INLINE_ACTION_SMART_BLOCK = 0x80;

Field	Туре	Null	Кеу	Default value	Description/Comments
					INLINE_ACTION_IPS_SIMULATION = 0x40;
relevance	char(1)	YES			Y/N/U. It is related to vulnerability scanner reports.
					Y – relevant. As per vulnerability report, this host is vulnerable to attack in the context.
					N – not relevant. As per vulnerability report, this host is not vulnerable to attack in the context.
					U – unknown. U is very common.
					Y and N shows up in TA only if the Manager has integration with MVM or they have imported vulnerability report.
VLANId	int(11)	YES			The VLAN found in the attack traffic
policyid	char(20)	YES			The Network Security Platform policy that was applied on the Sensor interface
hostIsolationState	tinyint(4)	NO			Whether the attacking host is quarantined or not. This action is based on the attack quarantine settings.
sensorAlertUUID	bigint(20)	NO	PRI		Unique ID sent by Sensor
sourceUserId	int(11)	YES			User name of the attacking host
destinationUserId	int(11)	YES			User name of the targeted host
sourceOSId	int(11)	YES			The ID of the operating system on the source host of the attack
destinationOSId	int(11)	YES			The ID of the operating system on the target of the attack

Field	Туре	Null	Key	Default value	Description/Comments
sourceOSId1	tinyint(4)	YES			
sourceOSId2	tinyint(4)	YES			
sourceOSId3	tinyint(4)	YES			
sourceOSId4	tinyint(4)	YES			
destinationOSId1	tinyint(4)	YES			
destinationOSId2	tinyint(4)	YES			
destinationOSId3	tinyint(4)	YES			
destinationOSId4	tinyint(4)	YES			
zoneId	int(11)	YES			Zone in which the alert was raised; applicable only to NTBA alerts.
deviceType	tinyint(3)	NO			IPS Sensor – 0 NTBA Appliance – 1 HIPS Sensor – 2
sourceReputation	smallint(6)	YES			Reputation of the source host of the attack. This reputation is fetched from McAfee Global Threat Intelligence. Low: good <14: minimal risk. 15-29: unverified, 30-49:medium risk >49: high risk high: bad

Field	Туре	Null	Key	Default value	Description/Comments
destinationReputation	smallint(6)	YES			Reputation of the targeted host.
sourceGeoLocation	char(32)	YES			Geographical location of the source host from McAfee Global Threat Intelligence. two-digit country code: CN:China, US:USA, IN:India.
destinationGeoLocation	char(32)	YES			Geographical location of the targeted host. Same as above
exporterId	int(11)	NO		-1	This is relevant only for NTBA alerts. This is the ID of the exporter.
interfaceId	int(11)	NO		-1	
sourceVmId	bigint(20)	NO			
targetVmId	bigint(20)	NO			
appId	int(11)	NO		-1	The ID of the layer 7 application that matched a Firewall access rule
appCategoryId	int(11)	NO			The ID of the application category that matched a Firewall access rule
proxyIpFlag	smallint(6)	NO			
appRisk	int(11)	NO			
xffTarget	smallint(6)	NO			

Field	Туре	Null	Кеу	Default value	Description/Comments
tag	int(11)	NO		-1	The userld for which the alert has been assigned, (-1 in case it is unassigned).
srcPhone	char(16)	YES			Applicable only to attacks from data- enabled mobile equipments such as a mobile phone or a tablet PC. The phone number of the source mobile equipment
srcIMSI	char(16)	YES			Applicable only to attacks from data- enabled mobile equipments such as a mobile phone or a tablet PC. The International Mobile Subscriber Identity (IMSI) ID of the source mobile equipment
SICAPN	varchar(120)	YES			Applicable only to attacks from data- enabled mobile equipments such as a mobile phone or a tablet PC. The Access Point Name (APN) of the mobile equipment that is the source of the attack traffic
destPhone	char(16)	YES			Applicable only to attacks targeted at data-enabled mobile equipments such as a mobile phone or a tablet PC. The phone number of the targeted mobile equipment
destIMSI	char(16)	YES			Applicable only to attacks targeted at data-enabled mobile equipments such as a mobile phone or a tablet PC. The International Mobile Subscriber Identity (IMSI) of the targeted mobile equipment

Field	Туре	Null	Key	Default value	Description/Comments
destAPN	varchar(120)	YES			Applicable only to attacks targeted at data-enabled mobile equipments such as a mobile phone or a tablet PC. The Access Point Name (APN) of the targeted mobile equipment
fileType	int(11)	YES			Malware File type
fileLength	int(11)	YES			Malware File length
fileMD5Hash	Char(32)	YES			Malware File MD5 Hash
virusName	Varchar(256)	YES			Malware Virus Name
fileUUID	Varchar(16)	YES			Malware file id
malwareScore	Int(11)	YES			Malware confidence
detectionEngine	Int(11)	YES			Malware detection engine
srcDNSName	Varchar(255)	YES			Source DNS name
destDNSName	Varchar(255)	YES			Destination DNS Name

The following table describes IV_PacketLog information.

Field	Туре	Null	Кеу	Default	Description/Comments
sensorId	int(11)	NO	Primary		The ID of the Sensor raising the alert. This ID is assigned to a Sensor by the Manager.
packetLogId	bigint(20)	NO	Primary		The packet log ID corresponding to this alert

Field	Туре	Null	Кеу	Default	Description/Comments
packetLogGrpId	bigint(20)	NO	MUL		The packet log group ID corresponding to this alert
packetLogType	char(1)	NO	Primary		F in case of a fragment; P in case of a packet.
packetLogSeq	int(11)	NO	Primary		A sequence number within the packet log stream. In case of fragments, this is 1 for request logs, and 2 for response logs.
lastReqByteStreamOffset	int(11)	NO	Primary		The offset in the TCP stream of the last byte of a request fragment. It is 0 for packet logs.
lastRespByteStreamOffset	int(11)	NO	Primary		The offset in the TCP stream of the last byte of a response fragment. It is 0 for packet logs.
markForDelete	char(1)	YES			First in line for deletion during old-alert purging
vsaId	int(11)	YES			The VSA ID of the VIDS to which the alert applies
vidsId	int(11)	NO			The VSA ID of the VIDS to which the alert applies
slotId	smallint(6)	NO			The slot number of the port from which the log packet originated
portId	smallint(6)	NO			The port number of the port from which the log packet originated
creationTime	timestamp	NO	MUL	Current time stamp	The time stamp on the log

Field	Туре	Null	Кеу	Default	Description/Comments
creationSeqNumber	int(11)	YES			The sequence number used to differentiate records with the same creation time
sensorPacketlogUUID	bigint(20)	NO	Primary		Unique ID generated by the Sensor for each packet log
packetData	longblob	YES			The actual packet or fragment data

The following table describes IV_Sensor information.

Field	Туре	Null	Key	Default value	Description/Comments
sensor_id	int(11)	NO	Primary		The ID is assigned to a Sensor by the Manager
subscriber_id	int(11)	NO	MUL		The ID of the admin domain to which the Sensor belongs
last_modified	timestamp	NO		Current time stamp	When this record was last modified
name	varchar(255)	NO	MUL		User-defined name of the Sensor
description	varchar(255)	YES			User-provided description for the Sensor
location	varchar(255)	YES			An arbitrary string filled in by the user
contact	varchar(255)	YES			An arbitrary string filled in by user

Field	Туре	Null	Кеу	Default value	Description/Comments
nepk	varchar(36)	YES	MUL		A pointer to the Lumos network element record for this Sensor
shared_secret	varchar(255)	YES			The shared secret to be used to initialize keys for the Sensor
device_class	tinyint(4)	YES			Not used
model	varchar(50)	YES			The main model name for this Sensor; populated after Sensor discovery
sub_model	tinyint(4)	YES			The sub model name for this Sensor; populated after Sensor discovery
serial_number	varchar(50)	YES			Sensor's serial number; populated after Sensor discovery
slot_count	tinyint(4)	YES			The number of slots in the chassis
tempSensorCount	tinyint(4)	YES			The number of the temperature Sensors on the device
shellMgrCount	tinyint(4)	YES			The number of the shell managers
fanCount	tinyint(4)	YES			The number of the fans
powerSupplyCount	tinyint(4)	YES			The number of power supplies
ip_address	varchar(32)	YES			The user-assigned IP address for the Sensor's management port
command_port	int(11)	YES			The port on which the Sensor contacts the Manager for its command channel

Field	Туре	Null	Кеу	Default value	Description/Comments
transport_type	varchar(10)	YES			Whether TCP or UDP
snmp_version	varchar(5)	YES			Whether v1, v2c or v3
foPeerAddress	varchar(32)	YES			The IP address of the peer Sensor
failover_enable	enum('Y','N')	NO		Ν	Whether failover is enabled
failopen_enable	enum('Y','N')	NO		N	Whether failopen is enabled when the Sensor is in failover mode
peer_sensorid	int(11)	YES			The Sensor ID of the peer Sensor
real_time_update_allowed	enum('Y','N')	NO		N	Whether real-time updates to the Sensor are allowed
sch_update_allowed	enum('Y','N')	NO		N	Whether schedule updates to the Sensor are allowed
sensorReservedVLANId	int(11)	YES			The VLAN ID reserved for the Sensor. If this value is -1, then there is no VLAN ID reserved.
isFOEnforced	enum('Y','N')	NO		N	Is the Sensor, a failover-only Sensor.
createDefaultLogicConfig	enum('Y','N')	NO		Y	
tacacsConfig	tinyint(4)	YES			Whether the tacacs configuration is inherited from the admin domain. 0 means yes.
inheritMPE	tinyint(4)	NO		0	Status of MPE configuration inherited from the admin domain. 0 means yes. inheritHQ Status of HQ config inherited from AD. 0-No

Field	Туре	Null	Кеу	Default value	Description/Comments
					0
inheritHQ	tinyint(4)	NO		0	Status of HQ configuration inherited from the admin domain. 0 means no.
config_flags	int(11)	YES			A flag set maintained by the Sensor config service indicating an internal maintenance state
lastRebootTime	timestamp	NO			Time when the Sensor rebooted last as per the information in the Manager
lastSignatureUpdateTime	timestamp	NO			The latest time that a sigset update went through successfully
isRateLimitEnabled	enum('Y','N')	NO		N	Whether the rate limit feature is enabled
lastRLmodifiedTS	timestamp	NO			Time when the rate limit feature was last modified
sw_version	varchar(25)	YES			The Sensor software version
fips_mode	int(11)	NO		0	Whether the Sensor is FIPS compliant
strong_crypto_version	varchar(5)	YES			
download_mode	tinyint(4)	NO		0	Whether the Sensor uses offline download(1) or online download mode (0)
inheritArtemis	tinyint(4)	NO		0	Status of File Reputation feature configuration inherited from the admin domain. 0 means no.

Field	Туре	Null	Кеу	Default value	Description/Comments
foStpForwardStatus	tinyint(4)	NO		2	This column is now deprecated
lastSoftwareUpdateTime	timestamp	NO			Time when the Sensor was last successfully updated

The following table describes IV_Categories information.

Field	Туре	Null	Key	Default value	Description/comments
categoryId	int(11)	Yes			Represents a category ID. The possible values are 111, 112, 113, and 114.
displayableName	varchar(64)	Yes			 The displayableName for each categoryld is provided below: 111 - Exploit 112 - Volume DOS 113 - Reconnaissance 114 - Policy violation
description	varchar(64)	Yes			 The description for each categoryld is provided below: 111 - Exploit category 112 - Volume DOS category 113 - Reconnaissance category 114 - Policy violation category

The following table describes IV_NTBA information.

Field	Туре	Null	Key	Default value	Description/comments
nba_id	int (11)	NO	PRI		The unique ID that the Manager assigns to an NTBA device.
subscriber_id	int (11)	NO	MUL		ID of the admin domain that owns the NTBA device.
last_modified	timestamp	NO		Current time stamp	Time when this record was last modified.
Name	varchar (255)	NO	MUL		User-specified name of the NTBA device.
description	varchar (255)	YES			Description of the NTBA device that a user optionally provides.
location	varchar (255)	YES			An arbitrary string entered by the user.
contact	varchar (255)	YES			An arbitrary string entered by the user.
shared_secret	varchar (255)	YES			The shared secret to be used to initialize keys for this Sensor.
device_class	tinyint (4)	YES			NTBA device class.
model	varchar (50)	YES			NTBA device model.
sub_model	tinyint (4)	YES			The submodel that is populated after device discovery.
serial_number	varchar (50)	YES			The serial number of the device populated after device discovery.

Field	Туре	Null	Key	Default value	Description/comments
ip_address	varchar (32)	YES			User-assigned IP address to the NTBA device management port.
command_protocol	varchar (32)	YES			١N
command_port	int (11)	YES			The port on which the NTBA device contacts the Manager for its command channel.
ne_pk	varchar (36)	YES	MUL		A pointer to the Lumos network element record for this NTBA device.
real_time_update_allowed	enum('Y','N')	NO		n	Whether real-time updates to the NTBA device are allowed.
sch_update_allowed	enum('Y','N')	NO		n	Whether schedule updates to the NTBA device are allowed.
config_flags	int (11)	YES			A flag set maintained by the NTBA device config service indicating an internal maintenance state.
last_reboot_time	timestamp	NO			Time when the NTBA device rebooted last as per the information in the Manager.
last_signature_update_time	timestamp	NO			The latest time that a sigset update went through successfully.
sw_version	varchar (25)	YES			The NTBA device software version.
fips_mode	int (11)	NO	0		Whether the NTBA device is FIPS compliant

The following table describes IV_Alarm information.

Field	Туре	Null	Key	Default	Description/comments
Id	char (36)	NO	PRI		The alarm PK from Lumos.
Name	varchar (128)	YES			The name of the alarm.
Source	varchar (255)	NO			A human-readable string version of the alarm source entity (not used to reconstruct the alarm).
sourceBlob	blob	YES			Serialized copy of the actual source entity object.
conditionType	varchar (128)	YES			Name of the alarm condition, for example, down and lowmem
Туре	varchar (128)	YES			Type of alarm, for example, management, equipment.
Severity	varchar (128)	YES			Severity of the alarm, for example, critical, major, minor, and so on.
lastUpdated	timestamp	NO		Time stamp	When this alarm was last modified.
creationTime	timestamp	NO		Time stamp	When this alarm was created.
serviceAffecting	char (1)	NO			Indication to the user whether this will interrupt service. For example, a condition type of "down" will but "lowmem" may not.
autoCleared	char (1)	NO			Indication whether the Manager will auto-clear this alarm eventually.
acknowledged	char (1)	NO			Whether this alarm has been acknowledged by a user.
additionalText	text	YES			Additional text provided by alarm-creating component.

Field	Туре	Null	Key	Default	Description/comments
additionalData	blob	YES			Additional data provided by alarm-creating component.
customData	blob	YES			Used by user agents to piggyback client data on the alarm.
occurrenceCount	int (11)	YES			The number of times the alarm occurred.
lastUpdateTime	bigint (20)	YES			The last time this record was updated.
sensorId	int (11)	YES			Unique ID assigned to the Sensor by the Manager.

The following table describes iv_subcategories information.

Field	Туре	Null	Кеу	Default value	Description/comments
idnum	int(11)	No	Primary		The unique ID number of the subcategory.
category_name	varchar(50)	No	Primary		The name of the subcategory.
parent_category	varchar(50)				The corresponding parent category name.
display_name	varchar(50)				The displayable name of the subcategory.
description	text				Description of the subcategory.
release_version	varchar(20)	No	Primary		Version of the signature set.
ts	date				Time stamp when a row was last updated.

The following table describes iv_vids information.

Field	Туре	Null	Кеу	Default value	Description/comments
vids_id	int(11)	No	Primary		The primary key. This is assigned by the Manager.
subscriber_id	int(11)	No	MUL		ID of the corresponding admin domain. This is a foreign key.
entity_subscriber_id	int(11)	No			
parent_id	int(11)	Yes	MUL		ID of the parent VIDS.
last_modified	Timestamp	No			When this record was last modified.
last_resourcechildchanged	Timestamp				
last_resourcetreechanged	Timestamp				
name	varchar(255)	No			User-specified name of the VIDS.
description	varchar(255)	Yes			User-specified description of the VIDS.
intftype	enum ('C','D','V','F','B')	No			Whether the interface is of type CIDR, dedicated, or VLAN.
vids_level	tinyint(4)	No			0 for Sensor; 1 for interface; 2 for subinterface.
sensor_id	int(11)	Yes			ID of the Sensor on which this VIDS is created.
wasp_inherit_status	tinyint(4)	No		0	
vsa_id	int(11)	Yes			This column is deprecated.

Field	Туре	Null	Кеу	Default value	Description/comments
network_link_id	int(11)	Yes			The network link on which this VIDS is created.
has_anomaly	enum('Y', 'N')	No		Ν	Whether anomaly detection is enabled for this VIDS.
ids_profile_id	varchar(20)	Yes			The IDS profile ID. References iv_policy(policy_id)
recon_policy_id	int(11)	Yes			Foreign key (recon_policy_id) References iv_recon_policy(recon_policy_id)
anomaly_profile_id	varchar(20)	Yes			The Anomaly profile ID.
ref_vids_id	int(11)	Yes	MUL		In an interface group, ref_vids_id is set to the primary VIDS of the group; otherwise set to nil.
intf_group_id	int(11)	Yes			The interface group this refers to (if any).
subintf_id	int(11)	Yes			The sub-interface this refers to (if any)
lwg_profile_id	varchar(20)	Yes			Local IPS Policy ID.
ipsSimulationVal	int(11)	No		0	Whether the Simulation Blocking feature is enabled for the VIDS.

The following table describes IV_Policy information.

Field	Туре	Null	Кеу	Default	Description / Comments
policy_id	varchar(20)	NO	Primary		Unique ID of the policy.
Field	Туре	Null	Кеу	Default	Description / Comments
--	---------------	------	--------	---------	---
policy_name	varchar(255)	YES	Unique		Name of the policy.
outbound_id	varchar(20)	YES			Outbound policy ID for the policy.
isOutboundPolicy	varchar(10)	YES			Whether it is an outbound policy or not.
owner_id	varchar(20)	NO			Corresponding admin domain ID.
env_ref_fks	text	YES			iv_env_pref foreign key.
ui_filter_fks	text	YES			iv_ui_filter foreign key.
isVisibleToChild	varchar(10)	YES			Whether this policy can be inherited by a child admin domain.
Digest	varchar(100)	YES			Digest value.
isEditable	varchar(10)	YES			Whether this policy is editable.
last_Modified	timestamp	NO			Time stamp when this policy was last modified.
is_mom_defined	enum('Y','N')	NO		Ν	Whether this policy is inherited from the Central Manager.
lwg_flag ENUM('Y','N') NOT NULL default 'N',	enum('Y','N')			N	Whether this policy is local.
policy_desc	varchar(150)				User-defined description for the policy.
version_num	int(11)	YES		0	Manager-assigned policy version number.

The following table describes iv_attack information.

Field	Туре	Null	Кеу	Default	
id	varchar(20)	NO	Primary		Unique ID assigned by McAfee.
version	varchar(20)	NO	Primary		Attack version. CONSTRAINT ivattack_pk PRIMARY KEY (id, version)
name	varchar(255)	YES			Name fo the attack.
launchpoint	varchar(50)	YES			
visible	varchar(50)	YES			
specversion	varchar(20)	YES			
description	longtext	YES			Description of the attack.
xml	longblob	YES			Attack definition in the XML format.
isUserDefined	varchar(10)	YES			Whether this is a Custom Attack.
TS	timestamp	NO			Timestamp of when the record was last modified.
isActive	varchar(10)	YES			Whether the attack is active.
release_version	varchar(15)	NO			Attack release version.
digest	varchar(100)	YES			Digest value.
isUDSDeleted	varchar(10)	NO		False	

The following table describes IV_Filtered_Attack_List information.

Field	Туре	Null	Key	Default	Description / Comments
owner_id	varchar(20)	YES	MUL		Corresponding policy ID. CONSTRAINT ifal_ownerid_fk FOREIGN KEY (owner_id) REFERENCES iv_policy (policy_id)
attack_id	varchar(20)	YES	MUL		Attack ID.
filter_id	varchar(20)	YES	MUL		CONSTRAINT iv_filteredattklist_fk FOREIGN KEY (owner_id, filter_id) REFERENCES iv_ui_filter (owner_id, filter_id)
isActive	varchar(10)	YES			Status of the attack in a policy.
last_modified	timestamp	NO			When the record was last modified.
attack_membership	varchar(20)	YES			
digest	varchar(100)	YES			Digest value.

The following table describes IV_impact information.

Field	Туре	Null	Key	Default	Description / Comments
severity	int(11)	YES			Attack severity.
category	varchar(20)	YES			Attack category.
xml	longtext	YES			Impact definition in XML format.
attack_id_ref	varchar(20)	NO	MUL		CONSTRAINT ivimpact_fk FOREIGN KEY(attack_id_ref,attack_version) REFERENCES iv_attack(id, version)
attack_version	varchar(20)	YES	MUL		Attack version.
TS	timestamp	NO			Timestamp when this record was last modified.

Field	Туре	Null	Key	Default	Description / Comments
isActive	varchar(10)	NO			Whether the record is active.
release_version	varchar(15)	NO			Signature set version.
digest	varchar(100)	YES			Digest value.

The following table describes iv_intf_group information.

Field	Туре	Null	Кеу	Default	Description / Comments
intf_group_id	int(11)	NO	Primary		Unique ID assigned by the Manager to a port cluster.
last_modified	timestamp	NO			The time when this record was last modified.
sensor_id	int(11)	NO	MUL		Unique ID of the Sensor. CONSTRAINT iig_sensorid_fk FOREIGN KEY(sensor_id)
name	varchar(255)	NO			User-defined name for the port cluster.
primary_intf_id	int(11)	NO	MUL		ID of the primary interface in the port cluster.

The following table describes IV_Subscriber information.

Field	Туре	Null	Key	Default	Description / Comments
SUBSCRIBER_ID	int (11)	NO	PRI	١N	The primary key of the admin domain.
LAST_MODIFIED	timestamp	NO		CURRENT _TIMESTAMP	When this record was last modified.
LAST_RESOURCECHILDCHANGED	timestamp	NO		0000-00-00 00:00:00	

Field	Туре	Null	Key	Default	Description / Comments
LAST_RESOURCETREECHANGED	timestamp	NO		0000-00-00 00:00:00	
LAST_SUBCHILDCHANGED	timestamp	NO		0000-00-00 00:00:00	
LAST_SUBTREECHANGED	timestamp	NO		0000-00-00 00:00:00	
NAME	varchar(255)	NO		١N	User-defined name of the admin domain.
DESCRIPTION	varchar(255)	NO		١N	User-specified description for the admin domain.
COMPANY	varchar(255)	YES		\N	The name of the company or owner of this admin domain.
PRIMARY_CONTACT_ID	int(11)	YES	MUL	١N	Reference to the primary contact for this subscriber. CONSTRAINT is_primarycontactid_fk FOREIGN KEY(primary_contact_id) REFERENCES iv_contact(contact_id),
SECONDARY_CONTACT_ID	int(11)	YES	MUL	١N	Secondary contact (unused for now) CONSTRAINT is_secondarycontactid_fk FOREIGN KEY(secondary_contact_id) REFERENCES iv_contact(contact_id)

Field	Туре	Null	Key	Default	Description / Comments
RESP_EMAIL_ADDR	varchar(255)	YES		١N	Default email address for Manager responses
RESP_PAGER_EMAIL_ADDR	varchar(255)	YES		١N	Default text-pager email address for Manager responses
RESP_SCRIPT_PATH	varchar(255)	YES		١N	Default script to be executed for script responses
SUBSCRIBER_LEVEL	tinyint(4)	NO		١N	The level in the admin-domain tree that this admin domain is defined at.
PARENT_ID	int(11)	YES	MUL	١N	ID of the parent admin domain. It is 0 if the parent admin domain is My Company.
GROUP_TYPE	tinyint(4)	NO		0	0 if this is a leaf subscriber, 1 if it is not.
MAXUSERS	int(11)	NO		0	The maximum number of users that can be defined under this admin domain.
MAXSUBSCRIBERS	int(11)	NO		0	The maximum number of child admin domains that can be defined under this admin domain.
MAXALERTS	int(11)	NO		10000	
HAS_ANOMALY	enum('Y','N')	NO		N	Whether this admin domain has anomaly detection turned on by default for all its VIDS.

Field	Туре	Null	Key	Default	Description / Comments
ALLOW_CHILD_SUBSCRIBERS	enum('Y','N')	NO		Ν	Whether this admin domain can create additional child admin domains under itself.
ALLOW_DELEGATION	enum('Y','N')	NO		N	Whether child admin domains of this admin domain can set their own policies.
ALLOW_VIDS	enum('Y','N')	NO		N	Whether this admin domain can create additional VIDS as subsets of its overall VIDS.
ALLOW_NONSTD_PORTS	enum('Y','N')	NO		N	Whether this admin domain can specify nonstandard ports to be considered equivalent to standard protocol ports, for example, alternate HTTPserver ports.
ALLOW_PHYSICAL_RESOURCES	enum('Y','N')	NO		N	Whether this admin domain can have Sensors and the network links owned by them.
IS_OVERRIDERULESET_ENABLE	enum('Y','N')	NO		N	
ALLOW_SENSORLVL_HST_ISOLATION	enum('Y','N')	NO		Y	Whether this admin domain is allowed to config Sensor level host quarantine.
IDS_PROFILE_ID	varchar(20)	YES	MUL	١N	The default signature profile ID for this admin domain. CONSTRAINT is_idsprofileid_fk FOREIGN KEY(ids_profile_id) REFERENCES iv_policy(policy_id)
RECON_POLICY_ID	int(11)	YES		0	ID of the Sensor recon policy.

Field	Туре	Null	Key	Default	Description / Comments
EMAIL_ENABLED	enum('Y','N')	NO		N	A flag to enable email responses.
EMAIL_THRESHOLD	tinyint(4)	YES		١N	An alert severity threshold beyond which the Manager must send email notification of alerts. If null, the Manager must never send email notifications of alerts.
EMAIL_SUPP_INTERVAL	int(11)	YES		600	Once the Manager has emailed a notification, it should not send any more email notification for this interval (seconds).
PAGER_ENABLED	enum('Y','N')	NO		N	A flag to enable pager responses.
PAGER_THRESHOLD	tinyint(4)	YES		١N	An alert severity threshold beyond which the Manager must send pager notification of alerts. If null, the Manager must never send pager notifications of alerts.
PAGER_SUPP_INTERVAL	int(11)	YES		600	Once the Manager has paged a notification, it should not send any more pages for this interval (seconds).
SCRIPT_ENABLED	enum('Y','N')	NO		N	A flag to enable Script responses.
SCRIPT_THRESHOLD	tinyint(4)	YES		١N	An alert severity threshold beyond which the Manager must execute the corresponding scripts. If null,

Field	Туре	Null	Key	Default	Description / Comments
					the Manager must never execute scripts.
SCRIPT_SUPP_INTERVAL	int(11)	YES		600	Once the Manager has executed the scripts, it should not execute any more scripts for this interval (seconds).
BYATTACK_EMAIL	tinyint(4)	YES		١N	Per attack forwarder based on global policy settings.
BYATTACK_PAGER	tinyint(4)	YES		١N	Per attack forwarder based on global policy settings.
BYATTACK_SCRIPT	tinyint(4)	YES		١N	Per attack forwarder based on global policy settings.
BYAV_EMAIL	tinyint(4)	YES		١N	
BYAV_PAGER	tinyint(4)	YES		١N	
BYAV_SCRIPT	tinyint(4)	YES		١N	
IS_MPE_POLICY_ENABLE	enum('Y','N')	NO		Υ	
EMAIL_FILTERID	int(11)	YES			Email alert filter ID associated with this admin domain.
PAGER_FILTERID	int(11)	YES			Pager alert filter ID associated with this admin domain.
SCRIPT_FILTERID	int(11)	YES			Script alert filter ID associated with this admin domain.
ANAMOLY_POLICY_ID	int(11)	YES			ID of the NTBA anamoly policy.
WORM_POLICY_ID	int(11)	YES			ID of the NTBA worm policy.

The following table describes IV_Audit information.

Field	Туре	Null	Key	Default	Description / Comments
TS	timestamp	NO	MUL		The time when the audit message was audited.
USERID	varchar(64)	YES			The user ID of the user whose action is audited.
ACTION	varchar(255)	YES			The action being audited.
TARGET	text	YES			The resource on which the action is performed.
SUBSCRIBERID1	int(11)	YES			Subscriber1, subscriber2, and so on are the list of nested admin domains, with the last non-null id being the admin domain to whom this audit message, and the earlier ones being its parents going back to the root admin domain ID. Audit messages of the root subscriber will have all these columns as NULL.
SUBSCRIBERID2	int(11)	YES			
SUBSCRIBERID3	int(11)	YES			
SUBSCRIBERID4	int(11)	YES			
RESULT	int(11)	YES			The result of the operation (0 == success).
MESSAGE	text	YES			Additional explanatory text (especially for failures).
ACTIONTYPE	smallint(6)	YES			The action type column "ld" in table.
STARTTS	timestamp	YES			
AUDIT_DETAIL_ID	int(11)	YES	Unique		CONSTRAINT iv_auditdetailid_uq UNIQUE (audit_detail_id)

IV_ALERT_DATA decoding

The alert specific data is stored as a blob in the field called typeSpecificData in the iv_alert_data table. Following sections describe the format of the data stored in the blob.

IPS alerts

Port scan alert

All alerts that has iv_alert.alertType = 4 are port scan alerts. Its iv_alert_data.typeSpecific data has the following format:

First byte contains number of port information to follow. If there are five ports involved in port scan then first byte of typeSpecificData will contain value 5. Each subsequent 2 bytes will contain the actual port number values.

Total length of typeSpecificData will be 1 + (5*2) = 11 bytes.

The source and destination VLAN ID follow with each being 4 bytes. These fields are applicable only for NTBA alerts.

Number of bytes	Value
1	Version information
4 (IPv4) or 16 (Ipv6)	IP address
1	Total number of ports
2	Port information
Variable length	Packet logs

Port scan



Host sweep alert

All alerts that have iv_alert.alertType = 5 are hostsweep alerts. Its iv_alert_data.typeSpecific data has following format:

First byte contains number of IP information to follow. If there are ten IPs involved in the hostsweep, then first byte of typeSpecificData will contain value 10. Each subsequent four bytes will contain the actual IP values.

Total length of typeSpecificData in above example will be 1 + (10*4) = 41 bytes.

The source and destination VLAN ID follow with each being 4 bytes. These fields are applicable only for NTBA alerts.

Number of bytes	Value
4	Connection rule ID
4	Connection drop count
1	External geographical location
1	External reputation
1	Connection rule type
4	Protocol ID
2	IP address count
4 (IPv4) or 16 (IPv6)	Version of the target IP address

Number of bytes	Value
1	Version information
4 (IPv4) or 16 (IPv6)	Proxy IP address
Variable length	Packet logs

Host sweep alert



Statistical anomaly alert

All alerts that have iv_alert.alertType = 2 are statistical anomaly alerts. The Statistical Anomaly Alert blob data contains two data blocks as shown in the following figure.

Statistical anomaly type specific data

Anomaly Measure Data

DoS Packet Type Data Block

Anomaly measure data block

The anomaly measure data block contains a set of measures. The first byte in the block represents a count which tells how many measures are in the data block. The measures are followed by the count byte as shown in the following figure.

Anomaly measure data block



Each measure contains two sets of floating point (4 bytes) values. The first set represents the bins and the second set represents the bin-count data values.

The first byte in the measure contains the measure id, the second byte contains a count that tells how many four byte values are in each set, and rest of the bytes contain floating point values as shown in the following figure.

Measure



DoS packet type data block

The DoS packet type data block contains a set of Packet Type data. The first byte in the block contains a count that tells how many packet type data are in the block.

Packet type data block



Packet type data

Each packet type data contains a set of IP Range data. The first four bytes in the packet type data represent the packet count, the next one byte represents the packet type, the next one byte represents a count that tells how many IP range data are in the packet type data and the rest of the bytes represent the IP range data as shown in the figure below.

Packet type data



IP range data

IP range

The IP Range Data contains 20 bytes information as shown in the following figure.

4 bytes 4 bytes 4 bytes 4 bytes 4 bytes Minimum Source IP Maximum Source IP Minimum Destination IP Maximum Destination IP Packet count

- First four bytes Minimum source IP address
- Second four bytes Maximum source IP address
- Third four bytes Minimum destination IP address
- · Fourth four bytes Maximum destination IP address
- Fifth four bytes Packet count

Threshold anomaly alert

iv_alert.alertType = 3 are threshold anomaly alerts. It only contains DoS Packet Type Data Block.

NTBA alerts

Port scan alert

All alerts that have iv_alert.alertType = 20 are NTBA port scan alerts. Its iv_alert_data.typeSpecific data has following the format:

First byte contains the number of port information to follow. If there are five ports involved in the port scan, then the first byte of typeSpecific data will have a value of 5. Each subsequent pair of bytes will contain the actual port number values. Total length of typeSpecificData will be 1 + (5*2) + 8 = 19 bytes.

The details of the alert are as follows:

Number of bytes	Value
1	Version information
4 (IPv4) or 16 (Ipv6)	Proxy IP address
1	Total number of ports
2	Port details
Variable length	Packet logs

NTBA port scan



Host sweep alert

All alerts that have iv_alert.alertType = 21 are NTBA host sweep alerts. Its iv_alert_data.typeSpecific data has the following format:

First byte contains number of the IP information to follow. If there are ten IPs involved in the hostsweep, then the first byte of typeSpecificData will have a value of 10. Every subsequent four bytes will contain the actual IP values.

Total length of typeSpecificData in the above example will be 1 + (10*4) + 8 = 49 bytes.

The details of the alert are as follows:

Number of bytes	Value
4	Connection rule ID
4	Connection drop count
1	External geographical location
1	External reputation
1	Connection rule type
4	Protocol ID
2	IP address count
4 (IPv4) or 16 (IPv6)	Version of the target IP address
1	Version information
4 (IPv4) or 16 (IPv6)	Proxy IP address
Variable length	Packet log

NTBA host sweep alert



Statistical anomaly alert

All alerts that have iv_alert.alertType = 14, are NTBA statistical anomaly alerts.

NTBA statistical anomaly type specific data

Anomaly Measure Data	Misc Data Block

Anomaly measure data block

The anomaly measure data block contains a set of measures. The first byte in the block represents a count which shows how many measures are present in the data block. The measures are followed by the count byte.

Anomaly measure data block



Measure

Each measure contains two sets of floating point (4 bytes) values. The first set represents the bins and the second set represents the bin-count data values.

The first byte in the measure contains the measure ID, the second byte contains a count that shows how many four-byte values are present in each set, and the rest of the bytes contain floating point values.



Miscellaneous data block

Service Block	VLAN Block
---------------	------------

Service block



VLAN block



Simple threshold alert

All alerts that have iv_alert.alertType = 15, are NTBA simple threshold alerts.

🗹 Note

Either the serviceld or applicationId will be -1 in an alert depending upon the type of the attack.

Number of bytes	Value
4	Service ID
4	Source VLAN ID

Number of bytes	Value
4	Destination VLAN ID

NTBA simple threshold type specific data



Generic behavioral alert

All alerts that have iv_alert.alertType = 201 are NTBA Generic Behavioral Alerts.

Number of bytes	Value
4	Destination VLAN ID
4	Source VLAN ID
4	Service ID
4	Protocol ID
4	Port ID

NTBA generic behavioral type specific data



Policy violation alert

All alerts that have iv_alert.alertType = 200 are NTBA policy violation alerts.

Number of bytes	Value
4	Rule ID
4 (Empty/String Length)	Uniform Resource Locator (URL)
4 (Empty/String Length)	File name
2	Type of access for the file
4	Operating System ID
4	Service ID
4	Protocol ID
4	Port ID
4	Application type ID
1	IP address version
4 (IPv4) or 16 (IPv6)	Host ID

Number of bytes	Value
4	Source VLAN ID
4	Destination VLAN ID
4 (Empty/String Length)	Email address
4	Email duration
4	Source zone ID
4	Destination zone ID
4	Match bitmap object
2	Behavioral index of the host

NTBA policy violation type specific data



String

URL and file name are strings which are represented as shown below.



IP address

Host IP address is represented as shown below.

Host IP address



Worm alert

All alerts that have iv_alert.alertType = 13 are NTBA worm alerts.

The worm alert has anomaly measure data block, hosts block, and 3 sets of data blocks with base and observed values showing the deviation. The hosts block contains a list of host IDs which were involved in the worm attack. The observed and base data blocks are for bi-directional out connection and sent received ratios.

Worm alert type specific data



Anomaly measure data block

The anomaly measure data block contains a set of measures. The first byte in the block represents a count which shows how many measures are present in the data block. The measures are followed by the count byte.

Anomaly measure data block



Measure

Each measure contains two sets of floating point (4 bytes) values. The first set represents the bins and the second set represents the bin-count data values.

The first byte in the measure contains the measure ID, the second byte contains a count that shows how many four-byte values are present in each set, and the rest of the bytes contain floating point values.

Measure



Generic block

Generic block



File Reputation alert

All alerts that have iv_alert.alertType = 7 are File Reputation alerts. The iv_alert_data.typeSpecific data has the following format.

File reputation alert



🗹 Note

The port-type mapping bit is not currently used but allocated for future use.

The details of the alert are as follows:

Number of bytes	Value
Variable	Port type
Variable	Malware classification
Variable	The level of malicious content in the file
Variable	File type
Variable	MD5 hash value of the file

The following table describes file type mapping.

Value	File type
1	exe
2	dll
3	cpl
4	осх
5	sys
6	scr
7	drv
8	com

Value	File type
9	doc
10	docx
11	ppt
12	pptx
13	xls
14	xlsx
15	pdf

The following table describes dirtiness level mapping.

Value	Dirtiness level	
0	Not applicable	
2	Hash denotes a heuristic score less than 10	
4	Hash denotes a heuristic score between 10 and 39	
8	Hash denotes a heuristic score between 40 and 74	
16	Hash denotes a heuristic score between 75 and 100	
32	Hash denotes a heuristic score above 100	
64	Hash is assumed clean	

The following table describes classification mapping.

Value	Classification
0	No classification
2	Application
4	Virus
8	Trojan
16	Application

Information on database queries

If you plan to use database queries, note that iv_alert table receives a lot of new records if incoming rate of alert is high. Any query using a join with this table can bring down the performance of database significantly.

SQL query guidelines

For applications that use SQL queries to access data, the database query guidelines discussed in this section must be followed to minimize the impact on the Manager's performance. Frequent, large queries can negatively impact the performance of the Manager.

🗹 Note

Copy the Manager database on a different system before you run your queries.

The following are the guidelines that you must follow:

- Avoid joins joined queries lock the entire table for longer periods of time.
- Include the index-key as the first condition, wherever possible. Some examples of index keys are uuid and creation time.
- Allow time between queries to accommodate database updates. Some users leave at least a few minutes between queries.
- Query the small increments of data possible. The maximum number should be 3000 (use a limit class).

Implications of database queries

Scenario 1 — Query error

If an application queries the database at some point during the tuning exercise there is a remote chance that during the transition to (or from) the temporary tables, the SQL query will result in an error. If an SQL query error occurs, simply retry the query.

Scenario 2 — Query occurs while tuning is underway

If an SQL query is run during the tuning exercise the response and behavior would look the exact same as it would today. However, given the query has been made to the valid iv_alert and iv_packetlog tables that have just been created, there is now the likelihood that some records will be missed as in the case below:

- 1. The SIEM product has forwarded alerts up to uuid x.
- 2. Additional n alerts, x+1 to x+n are received prior to database tuning and before the application had a chance to forward them.
- 3. The SIEM product starts accepting alerts from the newer temporary alert table and forwards x+n+1 and so on.
- 4. When the merge occurs, the SIEM product is not aware of x+1 through x+n and they would never be forwarded.

To determine if the iv_alert and iv_packetlog tables are freshly created tables needed to enable online database tuning, you should include an additional query for table size with the standard query. If the table size is less than 100 records it can be concluded that a tuning exercise is underway and you must apply further logic to future queries to ensure no records are missed. Note that records forwarded during these queries are perfectly valid.

It is recommended that, upon determining that a query has just been made during tuning, the first query after determining a full-sized database (that is, tables have merged again) include records unid x-200 to x+(whatever increment is typically used). This query will include records that have already been forwarded, however it will also include any records that may have been missed during the tuning process. Duplicate records should be discarded.

Example queries

Following query can provide Sensor, interface, policy name, attack name for selected set of alerts.

```
select
        alrt.uuid,
        atk.name.
        sen.name,
        vids.name.
        pol.policy_name
from
        alert sample alrt,
        iv_sensor sen,
        iv vids vids,
        iv_policy pol,
        iv attack atk
where
        alrt.sensorid = sen.sensor id and
        alrt.policyid = pol.policy_id and
        concat("0x", hex(alrt.attackid), "00") = atk.id and
        alrt.vidsid = vids.vids id;
```

Attacks included in policy

```
select
    pol.policy_name,
    list.attack_id,
    atk.name
from
    iv_policy pol,
    iv_filtered_attack_list_list,
    iv_attack_atk
where
    pol.policy_id = list.owner_id_and
    atk.id = list.attack_id;
```

Finding list of policies that is including given attack id

```
select
    pol.policy_name,
    list.attack_id,
    atk.name
from
    iv_policy_pol,
    iv_filtered_attack_list_list,
    iv_attack_atk
where
    pol.policy_id = list.owner_id_and
    atk.id = list.attack_id_and
    list.attack_id = "0x4la0le00";
```

Fetching only NTBA alerts

Just add the following clause to any query involving iv_alert table: AND deviceType = 1

Alert synchronization in an MDR deployment

Sensors generate events with an ID unique to them. Sensors forward the events to both Managers in an MDR deployment to provide high availability and no loss of events. These events can come in any order from multiple Sensors connected to the individual Managers and hence, the association of UUID assigned at the Manager level to the individual events are potentially different between Managers. So, you cannot rely on UUID as a unique identifier to associate with events across Managers in an MDR configuration.

Since the Sensors send the events to both the Managers, events are duplicated across the Managers. When a Manager is temporarily down, and comes back up, the events that were not received during the downtime are not re-sent by the Sensors. There is an MDR mechanism to synchronize the missing events with the peer Manager. This synchronizes the missing events from the last 24 hours to a maximum of 10,000 events between the Managers. So, the only ID that is unique across both managers is the one generated by the Sensor itself. The Sensor-generated IDs are in monotonically increasing order. This imposes effort on the part of the SIEM products to de-duplicate events between Managers.

There is a new column added in iv_alert table for Sensor-generated ids. It is called SensorAlertUUID.

The current suggestions are:

- Access the database using the UUID to look for newer events.
- Look for events on a per Sensor basis with the SensorAlertUUID.
- For the most part, it is sufficient to consume events from one of the Manager's database tables.

- If there is a jump in sensorAlertUUID for a Sensor, do one of the following:
 - Peer Manager can provide the missing events based on sensorAlertUUID.
 - Wait for the automatic event synchronization that occurs between the peer Managers for the missing data.
 - In case the peer Manager cannot come up with the misssing SensorAlertUUID, it is likely the case that due to a restart of the Sensor, the Sensor will skip on the current sequence of SensorAlertUUID and start from a new base which is monotonically higher than the previous event received.

• If there are no new events in the current Manager's database table, the Manager may be down. Check the peer Manager for new events. If any, switch to the peer Manager's table and continue reading the table.

- The UUID is still valid for accessing the variable data part stored in iv_alerts_data table for events from iv_alert table.
- NTBA alerts are not synched to the peer Manager; they only exist in the Manager that has been configured in the NTBA device.

There are new columns added for operating system and user information. These columns will have values only for certain events.

- · sourceUserId user ID in the host that belongs to the sourceIpaddr
- destinationUserId user ID in the host that belongs to the targetIpAddr
- sourceOSId Operating system ID in the host that belongs to the sourceIpaddr
- destinationOSId Operating system ID in the host that belongs to the targetIpAddr

Create PCAP format packet logs

Packet logs are stored in a raw format in the Manager database. This section provides information on how to convert the packet log data into PCAP format.

There are two types of packet logs stored in the table. One is regular packets and other one is fragment packets. Packet logs are applicable only to signature alerts (that is, alert of alertType = 1). For a given UUID, we may have both regular and fragment packet logs. So, the PCAP will have a file header and one or more packet headers for both regular and fragment packet logs.

🗹 Note

The Manager does provide packet logs in the order of creationTime. So, creationTime is not unique, and the microseconds in appended based on the packet log sequence numbers in the PCAP.

The high-level steps involved in creating PCAP for packet logs based on a UUID are provided below.

Task

- 1. Retrieve an alert data for the given UUID, from the iv_alert.
 - a. Use an SQL query to retrieve the alert data. For example, if UUID is 12890, Select * from iv_alert where UUID = 12890
- 2. Retrieve both regular and fragment packet logs data using the SensorId and the packetLog id in the alert data, from the iv_packetlog.

- a. Use an SQL query to retrieve all regular packets with the Sensorld and the packetLogId. Example: For Sensorid = 101 and packetlog id = 2002, the following is the query to get the regular packets from the iv_packetlog: select * from iv_packetlog WHERE SensorId = 101 AND packetLogId = 2002 AND packetLogType = `P' ORDER BY SensorId, packetLogId, packetLogType, packetLogSeq, lastReqByteStreamOffset, lastRespByteStreamOffset";
- b. Use an SQL query to retrieve all fragment packets: Select * from iv_packetlog WHERE SensorId = 101 AND packetLogId = 2002 AND packetLogType = 'F' ORDER BY SensorId, packetLogId, packetLogType, packetLogSeq, lastRegByteStreamOffset, lastRespByteStreamOffset";
- 3. Create the pcap file header and write them into a file. The PCAP file header format is described below.
- 4. Create the pcap packet headers for all regular packets and write them into the file.
- 5. Create the pcap packet headers for all fragment packets and write them into the file.
- 6. Use the file with Wireshark.

More information regarding steps 3, 4, and 5 are provided in the subsequent sections.

Create the PCAP file header and write them into a file

The following table describes PCAP file header format.

Bytes	Value	Comment
4	0xA1B2C3D4	Magic number
2	2	Major number
2	4	Minor number
4	gmtOff/1000	Time zone correction
4	0	sigfigs
4	65536	samplen
4	1	linktype

Creating the PCAP packet headers for all regular packets and write them into the file

A packet header must be created for every packet.

Also capture the source and target ip addresses defined in the first 12 bytes of the regular packet log data. You can use the first one because all packet logs data will have the same information. You may have to use these addresses in fragment PCAP packet headers. First 6 bytes are source and next 6 bytes are target.

Packet header for regular packets

The following table describes packet header for regular packets.

Bytes	Value	Comment
4	creationTime	It is the 'creationTime' from the table
4	TimeStamp	Microseconds
4	len	Packet log data length (blob length)
4	len	Packet log data length (blob length)
n	packets	Actual packet log data

Create the PCAP packet headers for all fragment packets and write them into the file.

You must create a packet header for every fragment packet. The following table describes the packet header for fragmented packets.

Bytes	Value	Comment
4	creationTime	It is the "creationTime" from the table.
4	TimeStamp	Microseconds.
4	len + 14	Packet log data length (blob length) + 14
4	len + 14	Packet log data length (blob length) + 14

Bytes	Value	Comment
6	sourceAddr	0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
6	targetAddr	0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
2	0xFFFF	IP type
n	Packets	Actual packet log data.

Enable communication between Syslog server and the Manager

To enable communication between the Syslog server and the Manager, perform the following tasks:

- Create a user account in the Manager
- Configure Syslog events in the Manager

Create a user account in the Manager

The Syslog server communicates with the Manager using a user account available in the Manager. You should create a user account in the Manager. To create a user in the Manager, login to the Manager MariaDB and create a user. This user can connect remotely to the Manager from the specified Syslog server. You should grant **SELECT** permissions to the user on the database.

Run the following commands on the MariaDB command prompt:

• GRANT SELECT ON lf.* TO 'user_name'@'receiver_ip_address' IDENTIFIED BY 'user_name_password' WITH GRANT OPTION;

This command creates the user and sets the required privileges. In the command, <u>user_name</u> is the desired username, <u>user_name_password</u> is the password for the newly created user, and <u>receiver_ip_address</u> is the IP address of the Syslog server that will connect to the Manager.

• FLUSH PRIVILEGES;

This command applies the privilege changes without restarting MariaDB.

Configure Syslog events in the Manager

For information on configuring Syslog events in the Manager, see the McAfee Network Security Platform Product Guide.

Create a database user in a MLOS system

To create a database user for accessing the Manager database on a MLOS system, perform the following steps:

Task

- 1. Login to the Manager instance.
- 2. Switch to the restricted shell.

To switch to the restricted shell, use the <u>5n3ak1n</u> command. After running the command, it will prompt for the root password followed by the admin password.

- 3. Enable listening on port 3306.
 - If you are using Manager version 9.1.x or 9.2.x, run the following command:

#iptables -A INPUT -p tcp --dport 3306 -j ACCEPT

• If you are using Manager version 10.1.x, run the following commands:

#firewall-cmd --zone=public --permanent --add-port=3306/tcp

#firewall-cmd --reload

4. Comment the bind-address and the skip-networking properties in the /etc/my.cnf file.

```
For example:
```

```
#bind-address=127.0.0.1
#skip-networking
```

5. Restart the mysql service.

#systemctl restart mysqld

6. Login to MariaDB as a root user.

#<Manager installation path>/MariaDB/bin/mysql -uroot -p

Running this command will prompt you to enter the root password of the database. On successful login, you will get the MariaDB prompt and in the prompt, run the use mysql; command.

7. Create the required database user.

>create user <new user name of the database>@<IP address of the system from which the user will connect to the database> identified by '<password>';

For example:

>create user nsmtst@192.168.1.20 identified by 'nsmtp';

8. Provide read only access to the newly created database user.
>grant select on lf.* to nsmtst@192.168.1.20;

What to do next

To verify if the database user creation was successful, from a Windows client, run the following command:

C:\MariaDB\bin\mysql -u nsmtst -h <IP address of the Manager instance> -P 3306 -p

For example:

```
C:\MariaDB\bin\mysql -u nsmtst -h 192.168.1.30 -P 3306 -p
```

You will be prompted for password. On successful authentication, you can access the database server running on the Manager instance.

Sensor data available for MIB browsers

You can view the values of the Sensor's MIB (Management Information Base) objects. For this purpose, you can integrate SNMP tools such as MIB browsers with the Sensor. The Sensor supports this integration only through SNMPv3.

Integrate an SNMP MIB browser with a Sensor

You can integrate third-party SNMP MIB browsers to a Sensor. Then using the MIB browser, you can directly read data from a Sensor for analysis or just monitoring Sensor performance.

The following are the high-level steps involved in integrating an SNMP MIB browser with a Sensor:

Task

- Because the Sensor uses only SNMPv3 to communicate with a third-party SNMP MIB browser, you need to set up the SNMPv3 user accounts in the Manager. The Manager automatically pushes these details to the Sensor so that the Sensor can authenticate the requests from a MIB browser. You can set up these details per Sensor or configure it at an admin domain level, and inherit it at the Sensor level. See the *McAfee Network Security Platform Product Guide* for the steps.
- 2. For security reasons, you must configure the IP address of the MIB browser that will query the Sensor. You can configure this per Sensor or configure it at the admin domain level, and inherit it at the Sensor level. See the *McAfee Network Security Platform Product Guide* for the steps.
- 3. Configure the SNMPv3 details on your MIB browser. Information is provided in the next section.
- 4. Load the Sensor MIBs on your MIB browser.

The Sensor uses proprietary MIB objects. These objects are contained in various files that are available in the Manager server. You can load these files on a MIB browser to view the MIB objects and to understand the hierarchy of the MIB structure in the Sensor. The steps are provided in the subsequent section.

Configure the SNMPv3 user details on the MIB browser

For your MIB browser to be able to query the Sensor successfully, it should use the SNMPv3 account details that you have configured on the Sensor. So, you must configure the corresponding SNMPv3 details in your MIB browser.

The details that you would generally need while configuring the SNMPv3 details in your MIB browser are as follows:

- The Management port IP address of the Sensor.
- Communication port for SNMPv3. You can specify only the standard port, which is 161. Make sure port 161 is open in the relevant firewalls of your network.
- The user name that you configured in the SNMPv3 Users page of the Manager.
- The security level, which is authPriv.
- The authentication algorithm, which is MD5.
• The authentication password. This is the **Authentication Password** that you configured in the SNMPv3 Users page of the Manager.

- The privacy algorithm, which is DES.
- The privacy password. This is the **Private Password** that you configured in the SNMPv3 Users page of the Manager.

Load the Sensor MIBs onto to your MIB browser

Before you begin

Make sure you have the Sensor MIB files available. In your Manager installed directory, go to McAfee\Network Security Manager \App\config\mibs and copy all of the contents.

Task

- 1. Open your MIB browser.
- 2. Configure the third-party SNMPv3 users and other SNMP-related configurations, such as timeouts (preferred value is 30 seconds) and retries (preferred value is 3), in the MIB browser.
- 3. Load the following files in the same order:
 - a. MCAFEE-SMI
 - b. MCAFEE-TC
 - c. MCAFEE-SENSOR-SMI
 - d. MCAFEE-SENSOR-CONF-MIB
 - e. MCAFEE-SENSOR-PERF-MIB
 - f. MCAFEE-INTRUVERT-EMS-TRAP-MIB

After you load the MIB files, you can view the MIB tree structure in your MIB browser. Based on the features available in your MIB browser, you can use the data from the Sensor for analysis or just for monitoring. All the following snapshots are taken using MG-SOFT MIB Browser Professional SNMPv3 Edition.

The following snapshot provides the view of the configuration and performance MIB supported for McAfee Network Security Platform.

MIB configuration



The following snapshot provides the SNMP walk output of the system group under the McAfee Network Security Platform configuration MIB.

Edit View SNMP Act inio x a a 🔹 🖬 🔒 🙀 🖉 🖉 🕾 🕾 🕾 🖉 🖉 ety Mil Ping • 🔝 🔚 🛛 Vetical 7216210.2 663.6647.6282 02. [10.10.10.12.lbm] 2 Prompt For OID. W Multiple Yariable Binding H Multiple D Collaps 🕻 Get Nei GetBuik Info Ph Find Copy OID Taggle i 🖲 Prope

For restricted write access to a section of the MIB, refer to the section *Management of permitted NMS IP address* in *McAfee Network Security Platform Product Guide*.

SNMP walk output

The following snapshot provides information about the MIB subgroup, which has write access from third-party SNMP applications.

SNMP walk output

A MG-SOFT MIB Browser Professional SNMPv3 Edition	
Eile Edit View SNMP Agtion Iook Window Help	
=] 71] (0) 🛠 명의 💁 👔 📖 🔛 📚 🚟 🚷 감 (영 🕸 🗇 💷	
Dave and Dave	
Renote SMP arent . Out	
172.16.233.25 Vertical	
HE IN	Guerrandia
jg i ka j j j ka j j j ka j j j j j j j j j j j j j j j j j j j	Davinski
en onlieition	< compared by the second secon

The following snapshot provides the SNMP set output for quarantining the host with IP 192.168.218.5 under the host quarantine group of McAfee Network Security Platform MIB.

SNMP set output

l 11 0 🛠 54 🜒 🗴 🖩 🗿 😜 🔤 🖓 🖓 🐨 🖓 🗂 📲	
uny MB Ping	
Genote SNMP egent Split	
172, 16, 233, 25 - 🔀 🔝 🐨 Vertical	
d B bee	Quep esuits
Construction C	In tradition of interface with 19 (18, 29, 50, 0) in tradi- mean of the interface
hostQBukFilesEndTiseV6 hostQBukFilesQRStatusV6	Set - hostQUserDefFilterA add(1)
hostQBuBFibeMPETtepiyMogVG	- C - C
Image: Sector	
 Image: https://www.com/articles/art	Resole SNMP agent
[1] hour(MakevedDevy) abd/44 [1] hour(MakevedDevy) abd/42 [2] hour(MakevedDevy) abd/42 [2] hour(MakevedDevy) abd/42 [2] hour(MakevedDevy) abd/42 [2] hour(MakevedDevy) abd/42	Resola SNMP agent 172 16 233 25 • 20 16
 in hord/NeveClery/LdW/K in hord/NeveClery/LdW/K in hord/UveDrsFitef.tdW/K in hord/UveDrsFitef.tdW/K in hord/UveDrsFitef.tdW/K 	Renole SHMP agent 172.16.233.25 • 20 (2) 010 to Set
▷ · · · · · · · · · · · · · · · · · · ·	Hendal SHMP agent 172:16:23:25 • (2) (2) 000 to Set 36.14.19862.21.21.226.15.192.168.218.50.0 • •
(a) (b) (Renda SMMP agerd 17216 233 25 • 20 (2) 00 to 5el 36.1.4.1966 21.9.1.26.1.5.192168 218.5.00 • •
() () 아이킹에 가지 한 사망 가지 않는 것 수 있는 것 수 있 같 같 수 있 같 수 있 같 ? 안 가 같 같 수 있 같 수 있 같 ? 안 가 같 같 수 있 같 ? 안 있 같 ? 안 가 있 같 수 있 같 ? 안 있 같 같 ? 안 있 같 같 ? 안 있 같 ? 안 있 같 ? 안 있 같 ? 안 있 같 ? 안 있 같 ? 안 있 같 ? 안 있 같 ? 안 있	Microsoft SMMP agend 172 16 233 25 0 Dis Set 361.4 18662 21 21 22 61 51 182 168 296 500 Value to Set
(a) (b) (Hendra SHM Pagnet 172 14 223 25 • (2) (2) 0D to Set 36.1 4.1 6962 21 21 22.6 1.5 152 168 2168 50 • • (2) Value to Set 1 • (2) (2)
() 이 아이킹에 가지 한 아이킹에 가지 한 아이킹에 가지 않는 것을 수 있는 것을 하는 아이킹에 가지 않는 아이킹에 가지 않는 아이킹에 가지 않는 것을 수 있는 것을 하는 아이킹에 가지 않는 것을 가지 않는 것을 하는 아이킹에 가지 않는 것을 하는 것을 수 있다. 것을 하는 것을 하는 것을 수 있다. 것을 하는 것을 하는 것을 하는 것을 수 있는 것을 수 있는 것을 하는 것을 하는 것을 수 있는 것을 수 있다. 것을 수 있는 것을 수 있다. 것을 수 있는 것을 수 있다. 것을 수 있는 것을 수 있다. 것을 것 같이 않아? 것	Henola SHMP agend 172 16 233 25 • 20 File 0 10 16 54 36.1.4.18662 21.2.122.6.1.5.192.168.2165.00 • • Value to Set 1 • % @ @ @ @ @ 5yntex • • % @ @ @ . • % @ . • % @ . • % @ . • % @ . . . % .
(a) (b) (Hendra SHMP agent 172 14 223 5 • (2) (2) 0D Is Set • (2)
(a) (b) (Rende SIMP agerd 172 15 223 25 • (a) (b) 90 16 Sef 36 14 10662 21 21 22 61 5182 168 216 500 • (c) Value to Sef 1 • (c) 9 Mages2 Translot 9 Mages2 (c) 9 Mages2 (c) <td< td=""></td<>
box(DirectCey) date/4 box(DirectCey) date/4 box(DirectEey) date/4 box(DirectEe) addres box(DirectEe) date/4 box(DirectEe) date/6 box(DirectEe)	Newode SIMM* agend 172 14 223 5 • (2) (2) 0D Is Set • (2)
bog Devo Ceng Table / 4	Hennold SIMM* agard 172 15 222.5 • (a) (b) 900 to Self 361.41 60962 21 21 22 61 5192 169 206 500 • (a) Value to Self 1 • (b) (c) 1 • (b) (c) (c) (c) 10 to Self 1 • (c) (c) (c) (c) 10 to Self 10 to Self 0 (c) (c) <t< td=""></t<>
boyldiverderyi Jakki 4 boyldiverderyi Jakki 4 boyldiverderyi Jakki 4 boyldiverderiyi Jakki 4 boyldiverderiyi Jakki 4 boyldiverderiyi 4 boyldiverder	Hende SHMP agent 172 14 223 5 Image: Control of the set 0D to Set Image: Control of the set Via to Set Image: Control of the set Via to Set Image: Control of the set Synta Image: Control of the set Utriespond The dots Control of the set Dispate One set One set Synta Image: Control of the set One set One set One set One set Dispate Dispate

COPYRIGHT

Copyright © 2022 Musarubra US LLC.

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others.

