Revision J

McAfee Network Security Platform 8.3

(Integration Guide)

COPYRIGHT

Copyright © 2018 McAfee, LLC

TRADEMARK ATTRIBUTIONS

McAfee and the McAfee logo, McAfee Active Protection, ePolicy Orchestrator, McAfee ePO, McAfee EMM, Foundstone, McAfee LiveSafe, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, McAfee Stinger, True Key, TrustedSource, VirusScan 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.

LICENSE INFORMATION

License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Contents

Preface **7**
About this guide . . . 7
Audience . . . 7
Conventions . . . 7
Find product documentation . . . 8

1 Integration with McAfee ePO **9**
Endpoint details query from the McAfee ePO server . . . 10
View details of source and destination endpoints . . . 11
View endpoint details using IP address . . . 14
Tags . . . 19
Network Security Platform dashboard in McAfee ePO . . . 23
Configurations . . . 24

2 Integration with McAfee Global Threat Intelligence **41**
How Network Security Platform - GTI integration works . . . 42
Configure GTI . . . 43
Network Security Platform-GTI integration for IP Reputation . . . 49
How Network Security Platform-GTI integration for IP Reputation works . . . 50
Enhanced SmartBlocking . . . 50
Configure IP Reputation for an admin domain . . . 51
Configure IP Reputation for an interface . . . 54
Configure IP Reputation from sub-interface level . . . 57
Exclude IP Address Information for Specific Hosts . . . 57
Viewing the Global Threat Intelligence alert category details . . . 58
Next generation reports . . . 58
How to view GTI report . . . 59
Network Security Platform-GTI integration for connection limiting policies . . . 62
Network Security Platform-GTI integration for File Reputation . . . 62
Terminologies . . . 63
Benefits of File Reputation . . . 64
Network Security Platform-File Reputation integration in detail . . . 64
File Reputation integration configurations in the Manager . . . 66
View File Reputation details in Attack Log . . . 74
CLI commands for Network Security Platform - File Reputation integration . . . 75
Limitations . . . 75
Troubleshooting . . . 75

3 Integration with McAfee Cloud **77**
About McAfee Mobile Cloud Engine for Mobile APK Files . . . 77
About McAfee Cloud Threat Detection . . . 77
Configure McAfee Cloud Threat Detection . . . 78
Configure advanced malware policies to send files to McAfee CTD . . . 80
How to view malware statistics . . . 81
Analysis of Malware Files . . . 82

View System Faults for Licensing . . . 85

4 Integration with McAfee® Advanced Threat Defense 89

Advantages . . . 90
Terminologies . . . 91
How Network Security Platform - integration works . . . 94
Details of how the integration works . . . 94
Considerations . . . 96
High-level steps for integrating with McAfee Advanced Threat Defense . . . 97
Integrating Network Security Platform and McAfee Advanced Threat Defense . . . 98
Enable McAfee Advanced Threat Defense integration for an admin domain . . . 98
Enable McAfee Advanced Threat Defense integration for a Sensor . . . 100
Add an Advanced Malware policy . . . 102
Manage Advanced Malware policies . . . 107
Sensor CLI commands . . . 108
Analyze Malware Files . . . 109
View the McAfee Advanced Threat Defense specific details for a detected malware . . . 113
Manager reports for malware detections . . . 115

5 Integration with McAfee Threat Intelligence Exchange 117

Why integrate Network Security Platform with Threat Intelligence Exchange? . . . 117
How the integration works . . . 119
Computing the overall file reputation in the Sensor . . . 121
High-level steps to make the integration work . . . 122
Enable DXL integration for a domain . . . 122
Enable DXL integration for a device . . . 123
Viewing Threat Intelligence Exchange detection in the Manager . . . 124
Sensor CLI commands specific to Threat Intelligence Exchange . . . 126
Troubleshooting the integration between Network Security Platform and Threat Intelligence Exchange . . . 127

6 Protecting the private cloud 129

High-level description of the integration . . . 129
Components of the integration . . . 130
How do these components come together . . . 132
Real world scenarios to illustrate deployment . . . 134

7 Integration with McAfee Vulnerability Manager 137

McAfee Network Security Platform - Vulnerability Manager integration . . . 137
Vulnerability Manager installation . . . 139
Menu options for Vulnerability Manager configuration . . . 139
Configure Vulnerability Manager settings in Manager . . . 140
Import non-vulnerability manager report . . . 155
Vulnerability assessment . . . 159
Relevance analysis of attacks . . . 159
Menu options for relevance analysis . . . 160
Relevance configuration details . . . 161
Use relevance configuration wizard . . . 161
Relevance analysis configuration in Manager . . . 162
Fault messages for Vulnerability Manager scheduler . . . 170
Support for Vulnerability Manager custom certificates . . . 171
Generate Vulnerability Manager SSL custom certificate for Manager . . . 171
Import the custom certificates into the Manager keystore . . . 172
On-demand scan of endpoints from Threat Explorer . . . 172
On-demand scan of endpoints listed in alerts in the Threat Analyzer . . . 173
Network scenarios for Vulnerability Manager scan . . . 180
On-demand scan of endpoints . . . 181

Concurrent scan of endpoints . . . 181
Troubleshooting options . . . 182
Reload Vulnerability Manager cache . . . 183
Reset relevancy cache . . . 183
Resubmission of database updates . . . 184
Vulnerability Manager - Certificate Sync and FC Agent issues . . . 184
Error messages . . . 185

8 Integration with McAfee Host Intrusion Prevention 187
Configure Host Intrusion Prevention details . . . 188
Add a Host Intrusion Prevention Sensor . . . 188
Configure the Host Intrusion Prevention Sensor in McAfee ePO™ . . . 189

9 Integration with McAfee Logon Collector 191
Benefits . . . 191
Integration requirements . . . 191
Download the software . . . 192
How Network Security Platform - Logon Collector integration works . . . 192
Configuration details for Logon Collector integration . . . 194
Configure integration at the admin domain level . . . 194
Establishment of trust between Network Security Manager and Logon Collector server . . . 195
Display of Logon Collector details . . . 195
Display of Logon Collector details in the Threat Analyzer — Dashboards page . . . 196
Display of user information in NTBA monitors . . . 196
Display user details (Logon Collector data) in Attack log . . . 196
Display of Logon Collector details in Network Security Manager reports . . . 197
Next Generation custom reports . . . 198
Communication error . . . 200

10 Integration with OSC 203
Security challenges in an SDDC . . . 204
Deploying next-generation IPS service to virtual networks . . . 205

11 Integration with HP Network Automation 207
Configure HP Network Automation in the Manager . . . 207

12 Integration of the Manager with SIEM products 211
Manager data available for SIEM products . . . 212
Methods of integration with SIEM products . . . 212
Configure notification methods . . . 213
Configure notifications based on attack severity . . . 213
Configure notifications per attack . . . 213
Templates for syslog, email, and pager . . . 214
Integration for fault information . . . 217
Integration using reports . . . 220
Data mining . . . 220
IV_ALERT_DATA decoding . . . 238
IPS alerts . . . 238
NTBA alerts . . . 241
File Reputation alert . . . 246
Information on database queries . . . 247
SQL query guidelines . . . 247
Implications of database queries . . . 248
Alert synchronization in an MDR deployment . . . 249
Create PCAP format packet logs . . . 250
Create the PCAP file header and write them into a file . . . 251

Creating the PCAP packet headers for all regular packets and write them into the file 251
Create the PCAP packet headers for all fragment packets and write them into the file. 252

13 Sensor data available for MIB browsers 253

Integrate an SNMP MIB browser with a Sensor 253
Configure the SNMPv3 user details on the MIB browser 253
Load the Sensor MIBs onto to your MIB browser 254

Index 259

Preface

This guide provides the information you need to configure, use, and maintain your McAfee product.

Contents

- *About this guide*
- *Find product documentation*

About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

Audience

McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.
- **Users** — People who use the computer where the software is running and can access some or all of its features.

Conventions

This guide uses these typographical conventions and icons.

Book title, *term*, *emphasis*	Title of a book, chapter, or topic; a new term; emphasis.
Bold	Text that is strongly emphasized.
`User input, code, message`	Commands and other text that the user types; a code sample; a displayed message.
Interface text	Words from the product interface like options, menus, buttons, and dialog boxes.
Hypertext blue	A link to a topic or to an external website.
	Note: Additional information, like an alternate method of accessing an option.
	Tip: Suggestions and recommendations.
	Important/Caution: Valuable advice to protect your computer system, software installation, network, business, or data.
	Warning: Critical advice to prevent bodily harm when using a hardware product.

Find product documentation

On the **ServicePortal**, you can find information about a released product, including product documentation, technical articles, and more.

Task

1. Go to the **ServicePortal** at https://support.mcafee.com and click the **Knowledge Center** tab.
2. In the **Knowledge Base** pane under **Content Source**, click **Product Documentation**.
3. Select a product and version, then click **Search** to display a list of documents.

1 Integration with McAfee ePO

McAfee ePolicy Orchestrator (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.

Typically, the current McAfee Network Security Platform version supports integrating with the current release of McAfee ePO as well as with some previous versions. For example, at the time of McAfee Network Security Platform 8.3, the current release of McAfee ePO is 5.9.1. So, you can integrate McAfee Network Security Platform 8.3 with McAfee ePO 5.9.1 as well as with McAfee ePO 5.3.2 and 5.9.0. 5.9.0 was the previous release and 5.3.2 was the release prior to 5.9.1.

For more information on McAfee ePO, see the *McAfee ePolicy Orchestrator Product Guide*. You can download the guide from http://www.mcafee.com/us/enterprise/downloads/index.html.

Integrating McAfee 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 Intrusion Prevention [formerly McAfee® Entercept] as part of your McAfee ePO installation, then you can also view the last 10 Host Intrusion Prevention 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.

For more information on McAfee Host Intrusion Prevention events, see *McAfee Host Intrusion Prevention Product Guide.* You can download the guide from http://www.mcafee.com/us/enterprise/downloads/index.html.

Consider the following scenario to understand how McAfee 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 on page 19.

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

Contents

- *Endpoint details query from the McAfee ePO server*
- *Network Security Platform dashboard in McAfee ePO*

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 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.

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.

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 on page 19.

View details of source and destination endpoints

You can view the details of the source and destination ports in an alert. To do so, perform the following steps.

Task

1 In the Manager, select **Analysis** | **Threat Analyzer** | **Real-time** | **Start the Real-Time Analyzer** or **Analysis** | **Threat Analyzer** | **Historical** | **Start the Historical Threat Analyzer**.

2 Click **Alerts**. Right-click an alert, select **ePO Endpoint Information** and then select **Source IP** or **Destination IP**. You can also right-click on many alerts and query the server.

An informational message is displayed stating that the McAfee ePO™ query is successful.

You should have enabled Network Security Platform-McAfee ePO™ integration at the domain level to see the McAfee ePO™ option in the right-click menu.

You can query many IP address at a single time. For example, RFC-Overflow alert has 11 destination addresses. You can query all of them using a single query.

> You can query the McAfee ePO™ server for endpoint information from the Alerts page as well as Endpoints page. Right-click an IP address on the **Endpoints** page and select **View McAfee ePO™ Information**. The Manager notifies you if your McAfee ePO™ query is successful and then allows you to navigate to the Forensics page to display the query results.

3 Click **Yes**.

The **Forensics** page with the summary of the endpoint details is displayed. The name or the IP address of the McAfee ePO™ server is also displayed in parentheses next to **McAfee ePO™ Endpoint Information**.

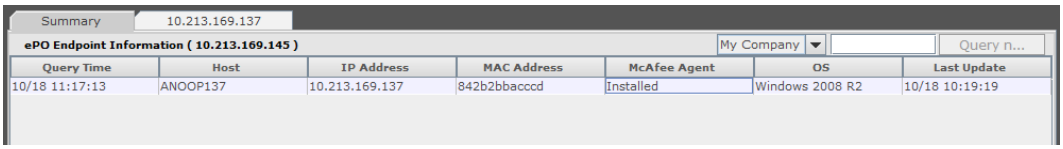


Figure 1-1 Summary window

4 For a managed or an unmanaged endpoint, double-click a row of information in **McAfee ePO™ Endpoint Information** to view the additional details.

The details are displayed in a tabbed region named after the endpoint's IP address. If a double-click does not display the additional details then it could be that the endpoint is an unrecognized endpoint or you had

earlier queried for the same managed/unmanaged endpoint and the tabbed region for the endpoint is still available.

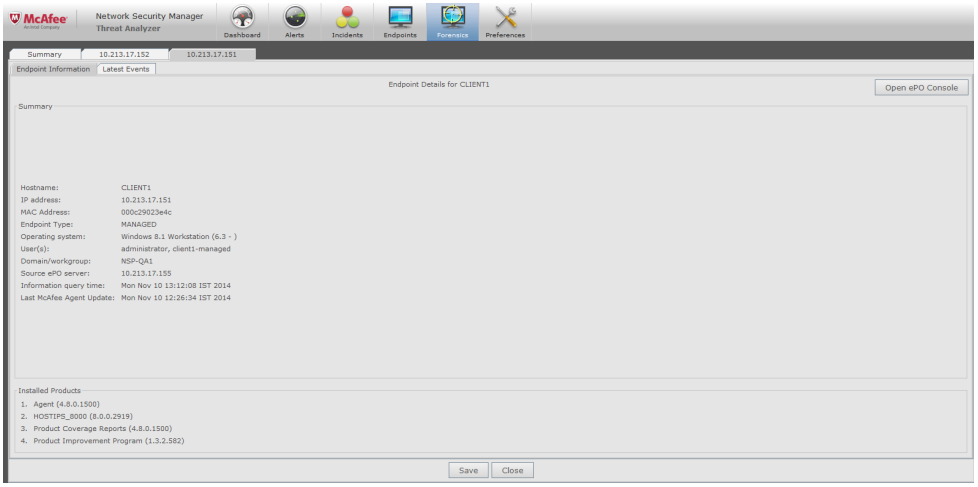


Figure 1-2 Additional details — Managed endpoint

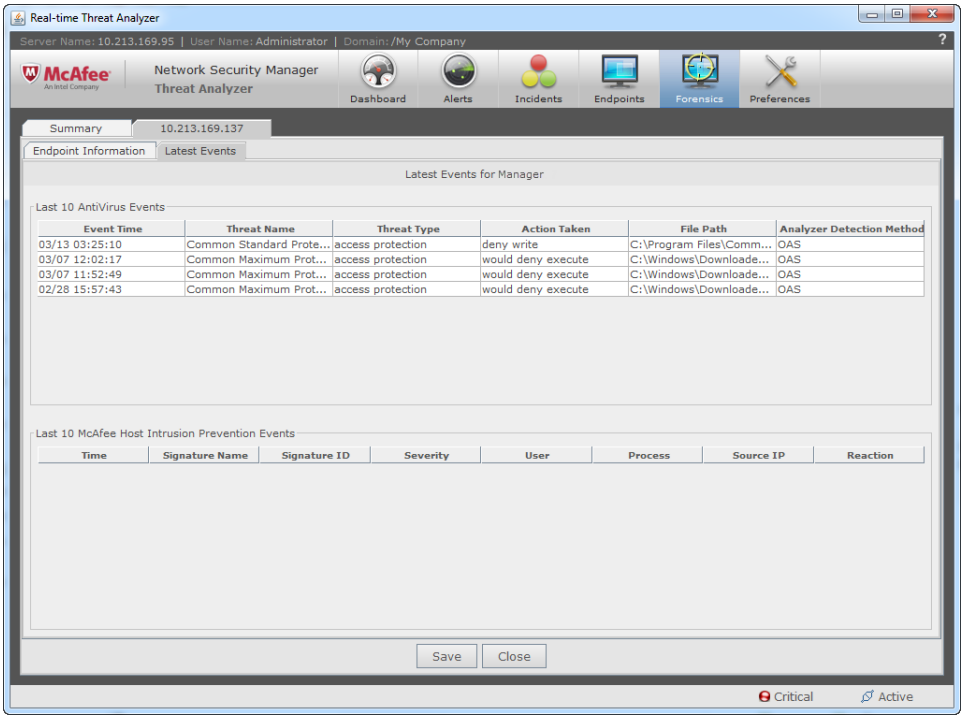


Figure 1-3 Latest Events tab

You can also view the details of source and destination endpoints from the **Endpoints** page.

Right-click options on the Forensics page

You can select an McAfee ePO™ query and right-click to view the following:

- **View Details**— Viewing additional details of managed/unmanaged endpoints
- **Query again**— Querying the endpoint once again

- **Delete**— Deleting the queried endpoint information
- **Delete All**— Deleting all rows in the endpoint information section

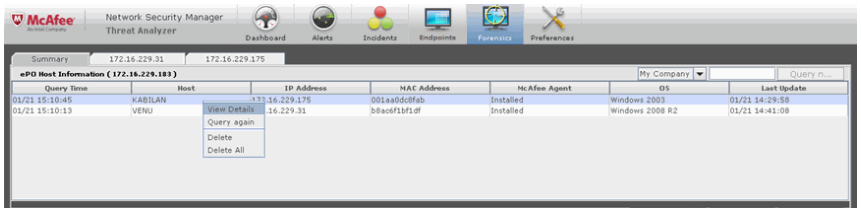


Figure 1-4 Right-click option on ePO Endpoint Information window

See also

Additional details for unmanaged endpoints on page 17

Mouse-over summary display

You can mouse over an IP address in the **Alerts** page to display a summary of essential endpoint data, such host name, user, and OS version.

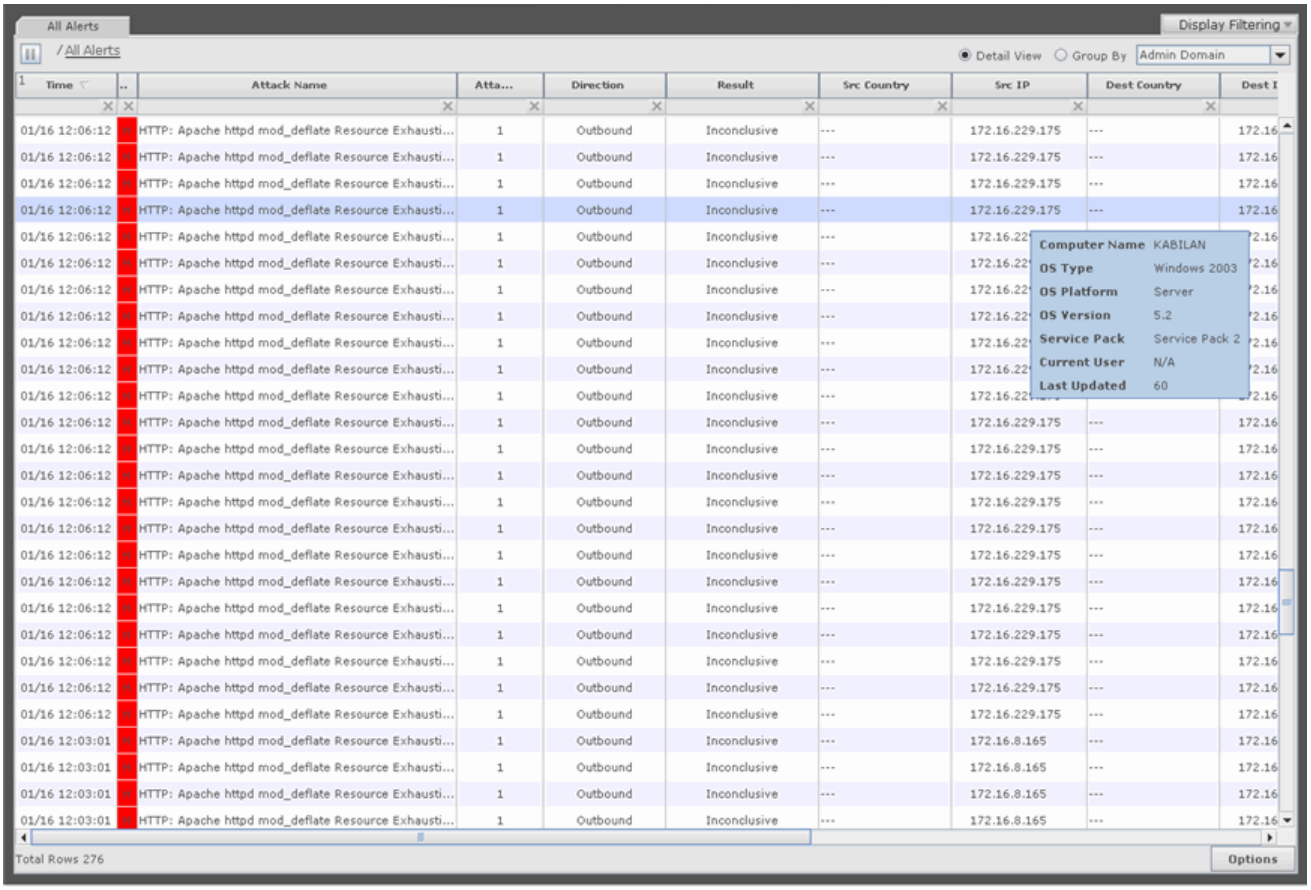


Figure 1-5 Mouse-over option

Enable this option from the **Enable ePO Integration** page. The summary is visible in the **Alerts** page only when ePO integration is also enabled in the Manager.

View endpoint details using IP address

You can query using a endpoint's IP address in the Forensics page to view the details of the endpoint. You can view the details of up to 100 endpoints at a time. If the number of queries exceeds 100, then the earliest row of detail is deleted.

Task

1. Select **Analysis** | **Threat Analyzer** | **Real-time** | **Start the Real-Time Analyzer** or **Analysis** | **Threat Analyzer** | **Historical** | **Start the Historical Threat Analyzer**.
2. Click the **Forensics** tab.
3. Enter the IP address.
4. Select the admin domain name that is configured to the ePO database.

5 Click **Query now**.

The source or destination IP address is listed in **ePO Endpoint Information** of the **Forensics** page. The name or the IP address of the ePO server is also displayed in parentheses next to **ePO Endpoint Information**.

> If you are querying an unknown endpoint and then click on that row for information (the row has only dashes displayed), a pop-up message is shown stating that the data is not available.

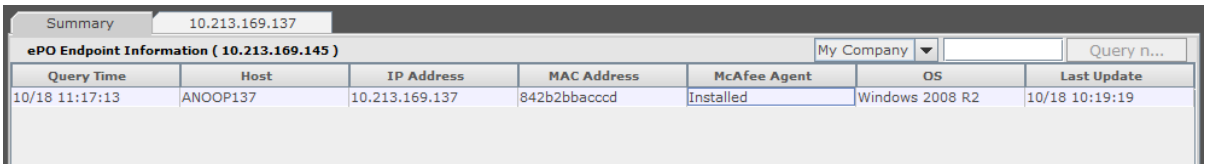


Figure 1-6 Summary window

6 For a managed or unmanaged endpoint, double-click a row of information in **ePO Endpoint Information** to view the additional details.

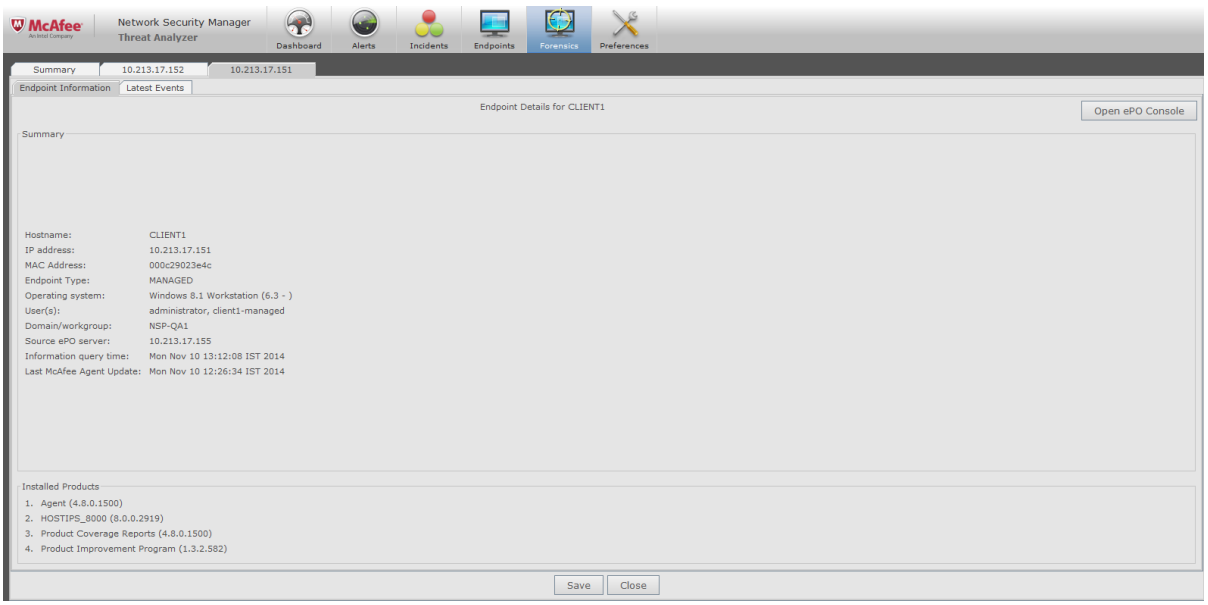


Figure 1-7 Endpoint Information tab

> When you double-click on a row of information, then the details are displayed in a tabbed region named after the endpoint's IP address. If double-click does not display the additional details then it could be that the endpoint is unrecognized or you had earlier queried for the same managed/unmanaged endpoint and the tabbed region for the endpoint is still available.

Tasks

- *Start McAfee ePO console* on page 17
- *Install Network Security Platform extension file in McAfee ePO* on page 18

See also

Additional details for managed endpoints on page 16
Additional details for unmanaged endpoints on page 17

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.

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

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

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 are the 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.
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 **Endpoint Security Events** tab to view the following information on the latest 10 Host Intrusion Prevention and anti-virus events.

Field	Description
Latest Anti Virus Events	The latest events including the date and time when the event was received by the anti virus agent, the name of the threat that caused the event to appear, the type of the threat that triggered the event, and the action taken by the anti virus agent on the reported event.
Latest Host Intrusion Prevention Events	The latest host intrusion prevention events including the date and time when the event was received by the Host Intrusion Prevention agent, the name of the signature that caused the event to appear, the ID of the Host Intrusion Prevention signature that caused the event to appear.

See also

View endpoint details using IP address on page 14

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** | **<Admin Domain Name>** | **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.

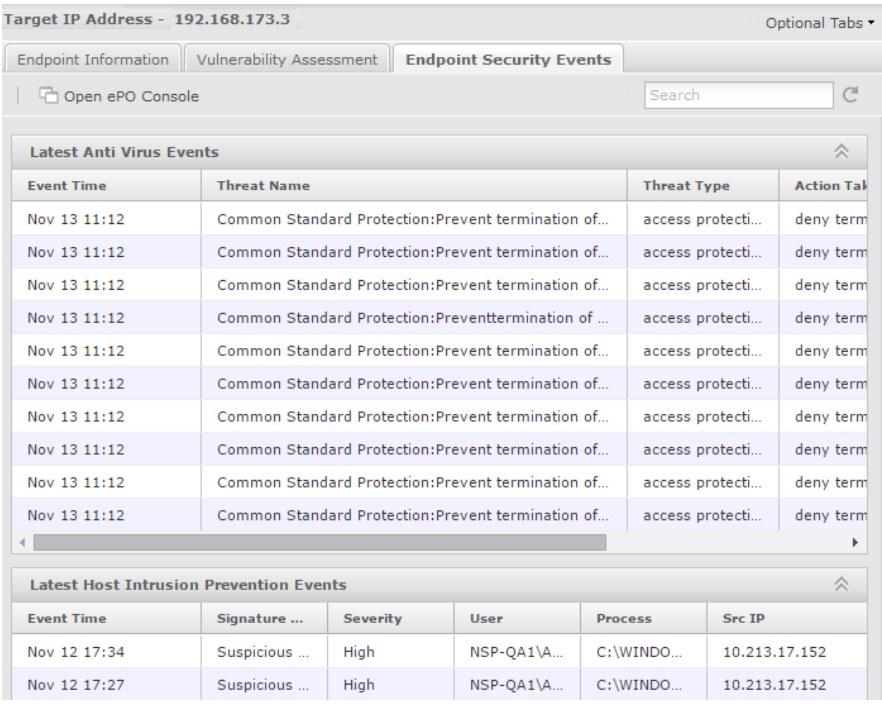


Figure 1-8 Endpoint information

4 Click **Endpoint Security 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.

Field	Description
MAC Address	MAC address of endpoint.
Endpoint Type	One of the following is displayed as Endpoint Type: • **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.
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.

See also

View details of source and destination endpoints on page 11
View endpoint details using IP address on page 14

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 Download the product extension zip file (**NSPExtension.zip**) from **Manager** | **<Admin Domain Name>** | **Integration** | **ePO** | **ePO Integration** in the Manager.

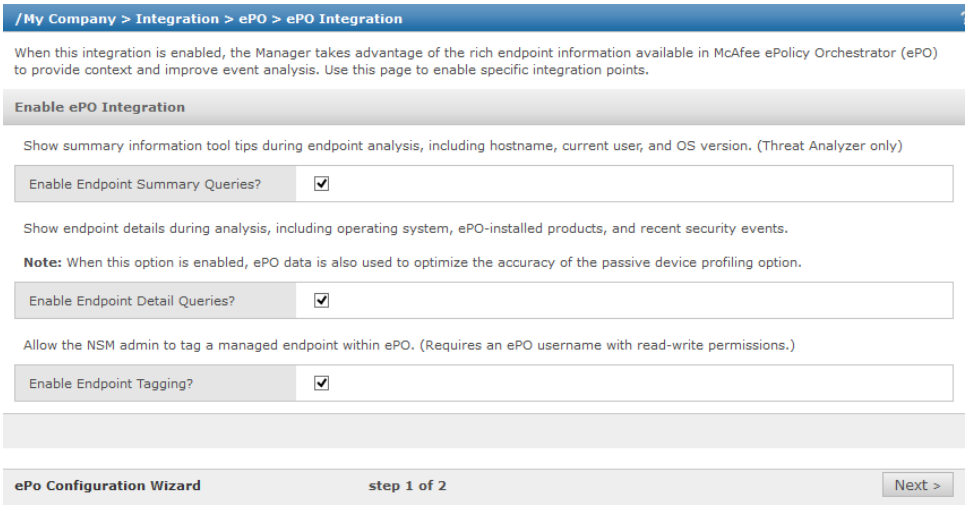


Figure 1-9 Enable ePO Integration area

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

2 From the McAfee ePO home page, select **Menu** | **Software** | **Extensions**.

3 Click **Install Extension** at the top left corner of the page.

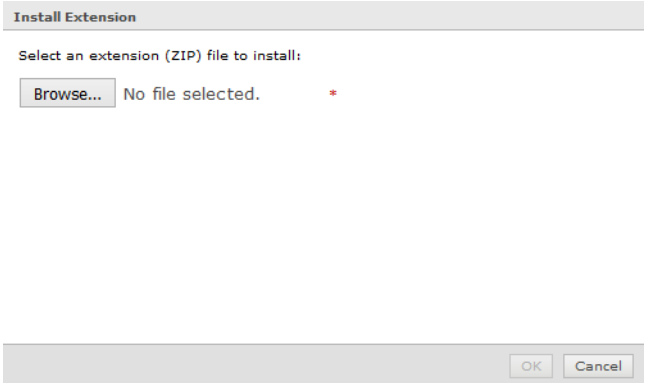


Figure 1-10 Install Extension dialog

A window is displayed asking to browse the extension file as a .zip file.

4 Click **OK**. The extension file is installed and displayed in the list of extensions.

> If you have the Network Security Platform 5.1.x extension installed, then note that a direct upgrade of this extension (to 6.0.x, for example) is not supported. You need to uninstall the 5.1.x extension and then install the new extension.

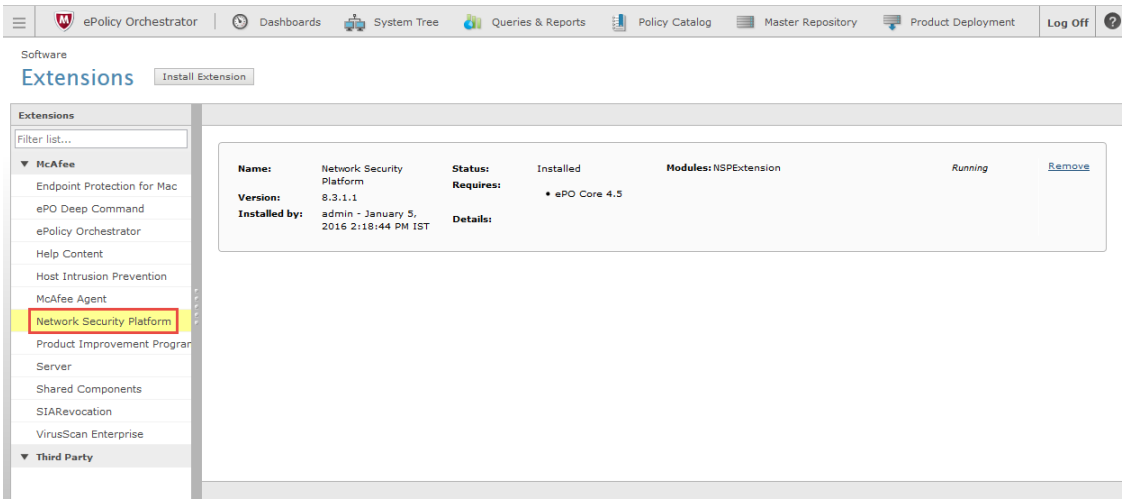


Figure 1-11 Extensions tab

See also

Configurations on page 24

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 chapters *The System Tree* and *Tags* in the *McAfee ePolicy Orchestrator 5.9.1 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.

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

Assign McAfee ePO tags to endpoints through the Threat Explorer

Before you begin

To assign tags from the Manager, make sure you have enabled the **Enable Endpoint Tagging?** checkbox in the **Enable 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** | **<Admin Domain Name>** | **Threat Explorer**.

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

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

Details about the IP address appear.

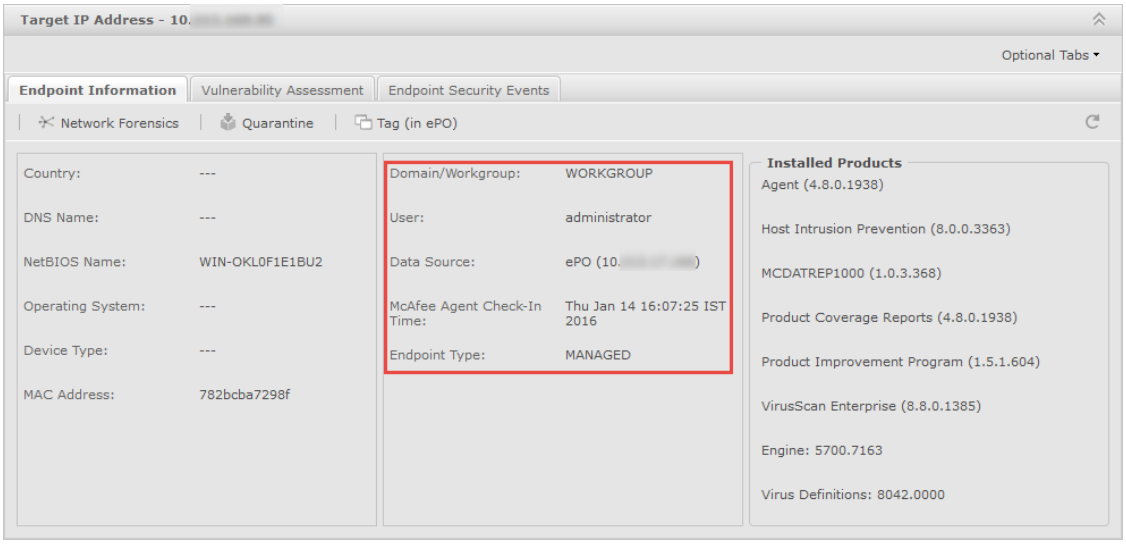


Figure 1-12 Endpoint Information tab

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.

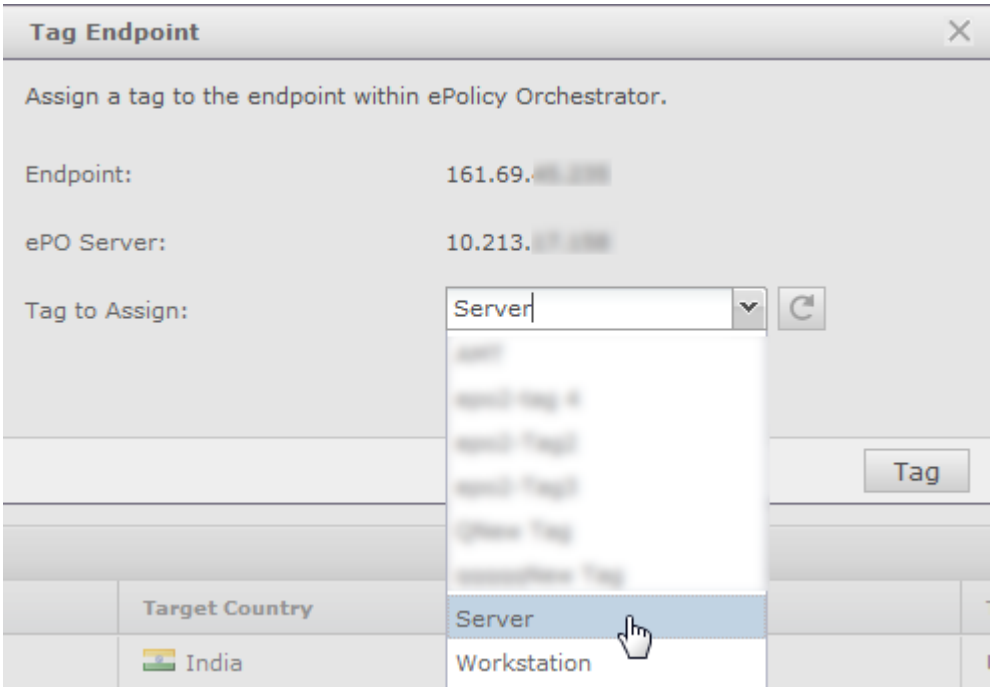


Figure 1-13 Drop-down contains the list of tags created in McAfee ePO

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

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

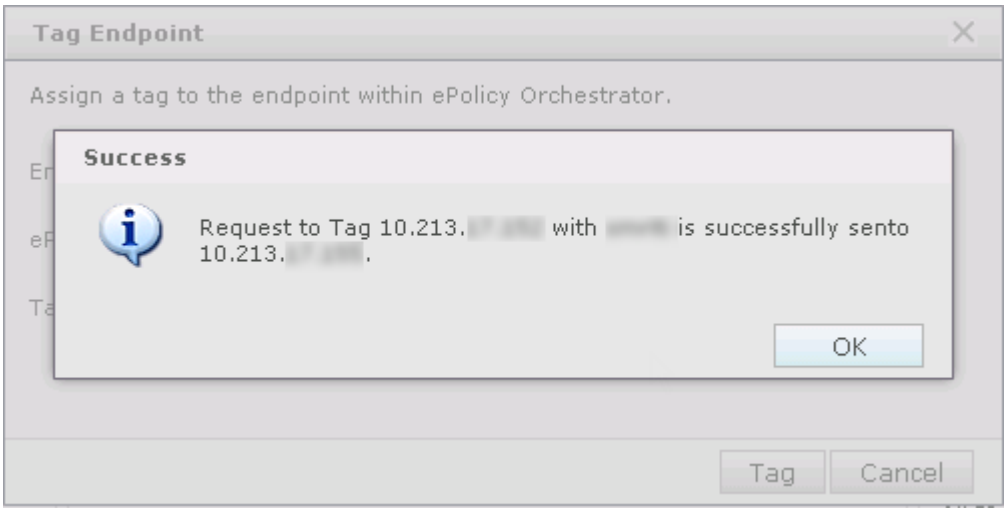


Figure 1-14 Tagging successful

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

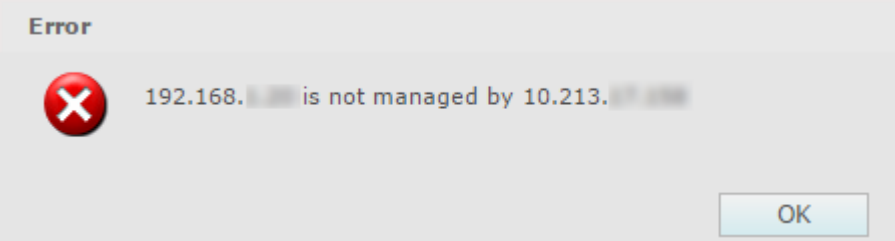


Figure 1-15 Tagging fails when the endpoint is not managed by McAfee ePO

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 on page 23

Assign McAfee ePO tags to endpoints through the Attack Log

Before you begin

To assign tags from the Manager, make sure you have enabled the **Enable Endpoint Tagging?** checkbox in the **Enable 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** | **<Admin Domain Name>** | **Attack Log**.

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

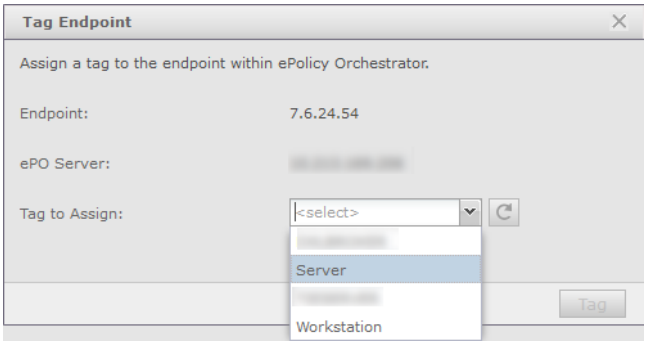


Figure 1-16 Tag an endpoint from Attack Log

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

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*.

View tags in McAfee ePO

To view tags assigned to endpoints, refer to chapters *The System Tree* and *Tags* in the *McAfee ePolicy Orchestrator 5.9.1 Product Guide*.

Network Security Platform dashboard in McAfee ePO

McAfee ePO provides you the option to view Network Security Platformdata 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 Platformextension 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 the section Configuring 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, then 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, then 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 Manager s are not available, then 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:

See also

Install Network Security Platform extension file in McAfee ePO on page 18
Create a user in the Manager for data retrieval in McAfee ePO™ on page 24
Configure a server task for Network Security Platform in McAfee ePO on page 29
Create new Network Security Platform dashboards in McAfee ePO (optional) on page 33
Configuration of ePO server settings in the Manager on page 25

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** | **<Admin Domain Name>** | **Users and Roles** | **Users**.
2. To add the new user, select **New**.

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, is to be entered in the **Actions** page, while configuring a Server Task in McAfee ePO™.

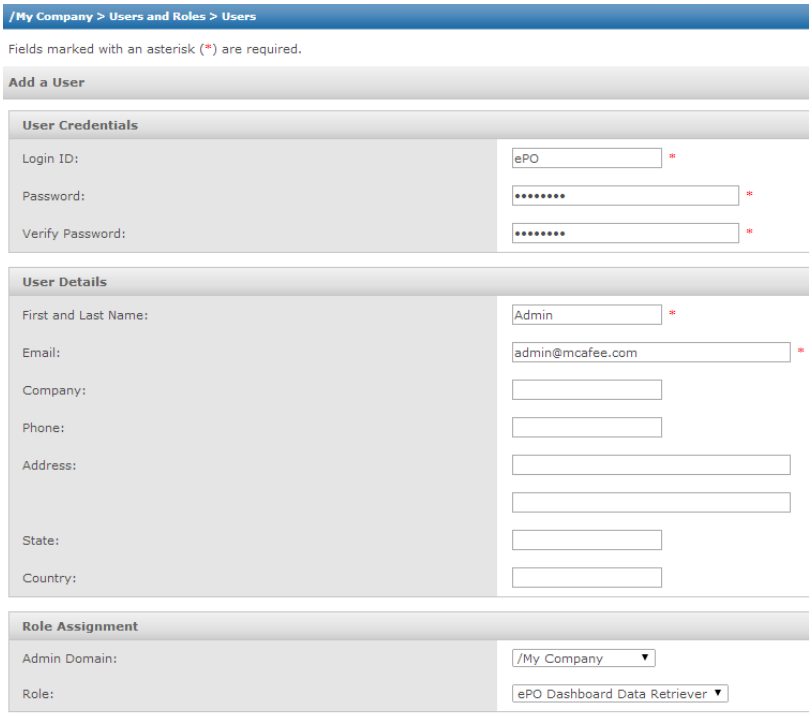


Figure 1-17 Users sub-tab

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, is to be entered in the **Actions** page, while configuring a Server Task in McAfee ePO™.

See also

Configurations on page 24

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 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, you need 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 Log onto the Manager.

2 Navigate to **Manager** | **<Admin Domain Name>** | **Integration** | **ePO** | **ePO Integration**.

The **Enable ePO Integration** page is displayed.

3 Enable the required options for McAfee ePO integration.

(Optional) Select the checkbox for the **Enable Endpoint Summary Queries?** option.

Enabling this option allows you to view the essential host data such as, host name, current user, and OS version in the Attack Log. The summary is visible in the alerts details panel only when the McAfee ePO™ integration is also enabled in the Manager.

(Optional) Select the checkbox for the **Enable Endpoint Detail Queries?** 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.

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

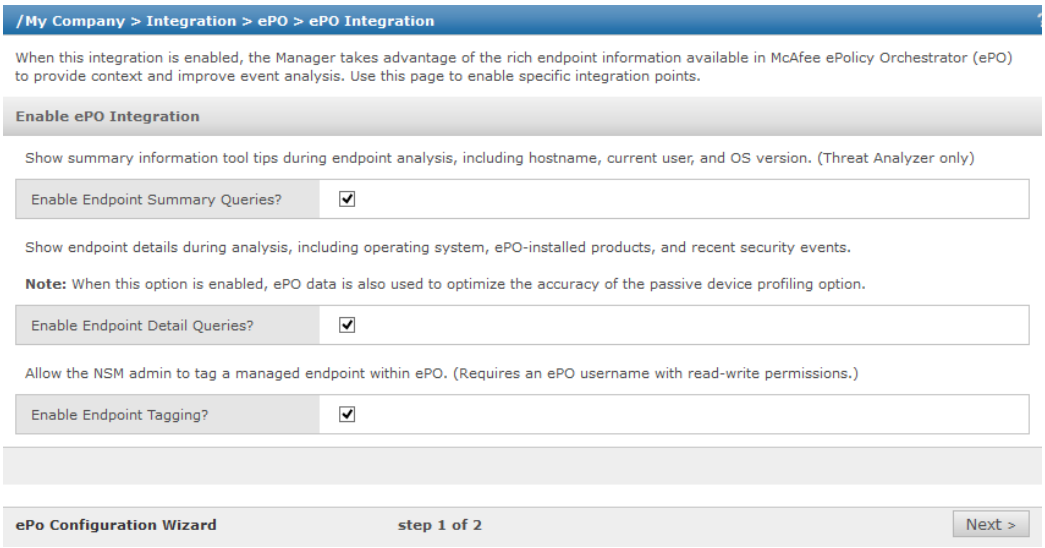


Figure 1-18 Enable ePO Integration area

4 Click **Next** to view **ePO Server Settings** page.

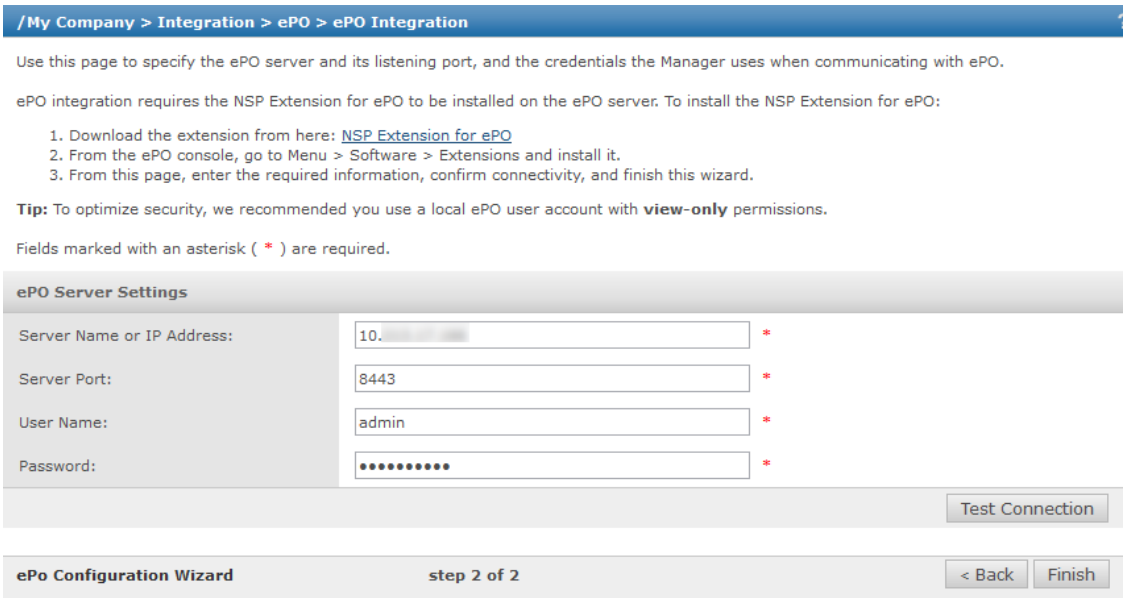


Figure 1-19 ePO Server Settings area

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

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

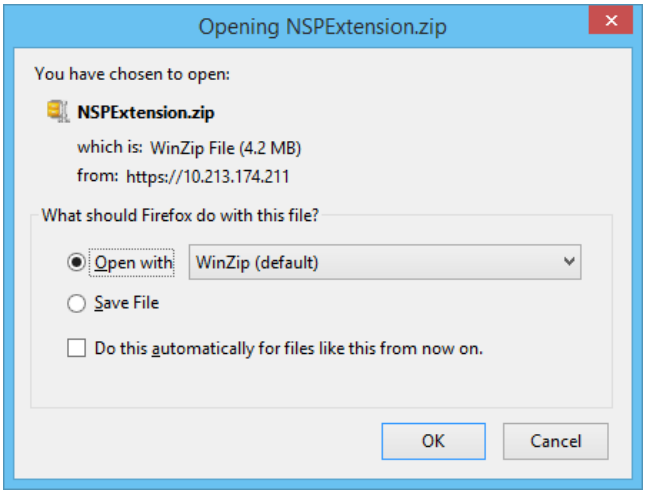


Figure 1-20 File Download dialog

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

7 Log onto the McAfee ePO console.

The McAfee ePO console Home page is displayed.

8 In the **Menu**, navigate to **Software** | **Extensions** page.

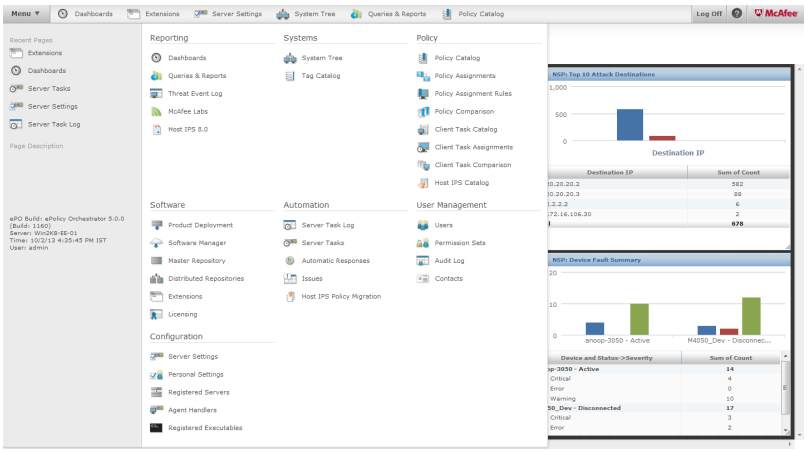


Figure 1-21 Extensions page

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.

11 Close the McAfee ePO console and return to the Manager.

12 Navigate to **Manager** | **<Admin Domain Name>** | **Integration** | **ePO** | **ePO Integration** | **Enable ePO Integration** | **ePO Server Settings**.

13 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.

14 Click **Test Connection** to ensure that the Extension file is installed and started on the McAfee ePO server.

15 If the connection is up, then 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, then 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, then 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, then the Branch Office Admin Domain should be configured to the Branch Office McAfee ePO server.

For more information on ePO refer to McAfee ePO documentation.

Viewing McAfee ePO configuration details

To view the McAfee ePO™ configuration details of an admin domain:

- From the Manager, select **Manager** | **<Admin Domain Name>** | **Integration** | **ePO** | **Summary**.

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 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, select **Menu** | **Automation** | **Server Tasks**.

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

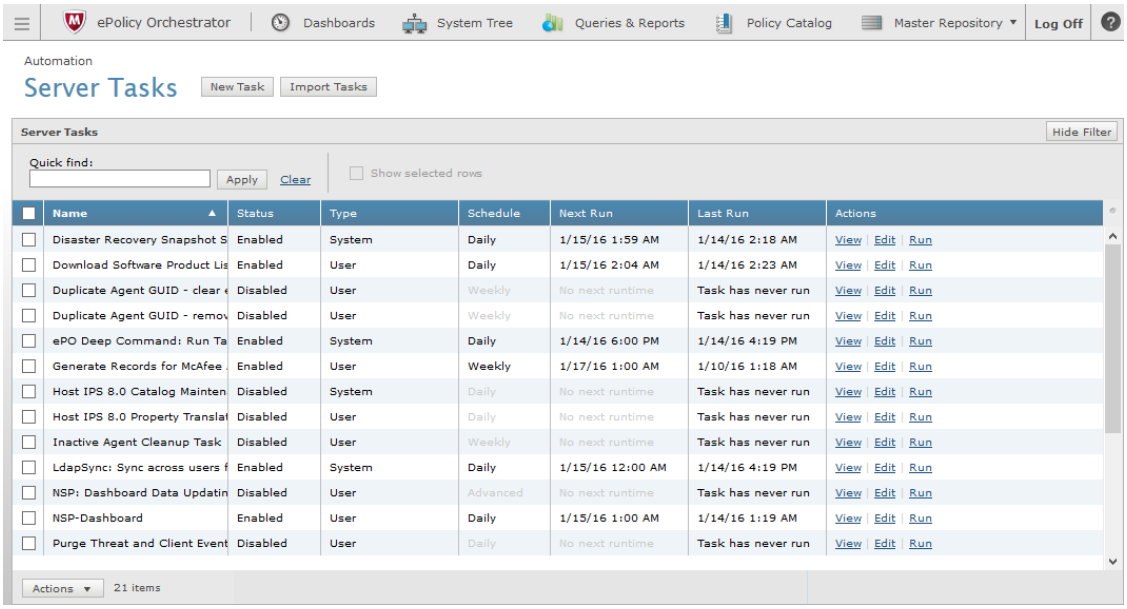


Figure 1-22 Server Tasks tab

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

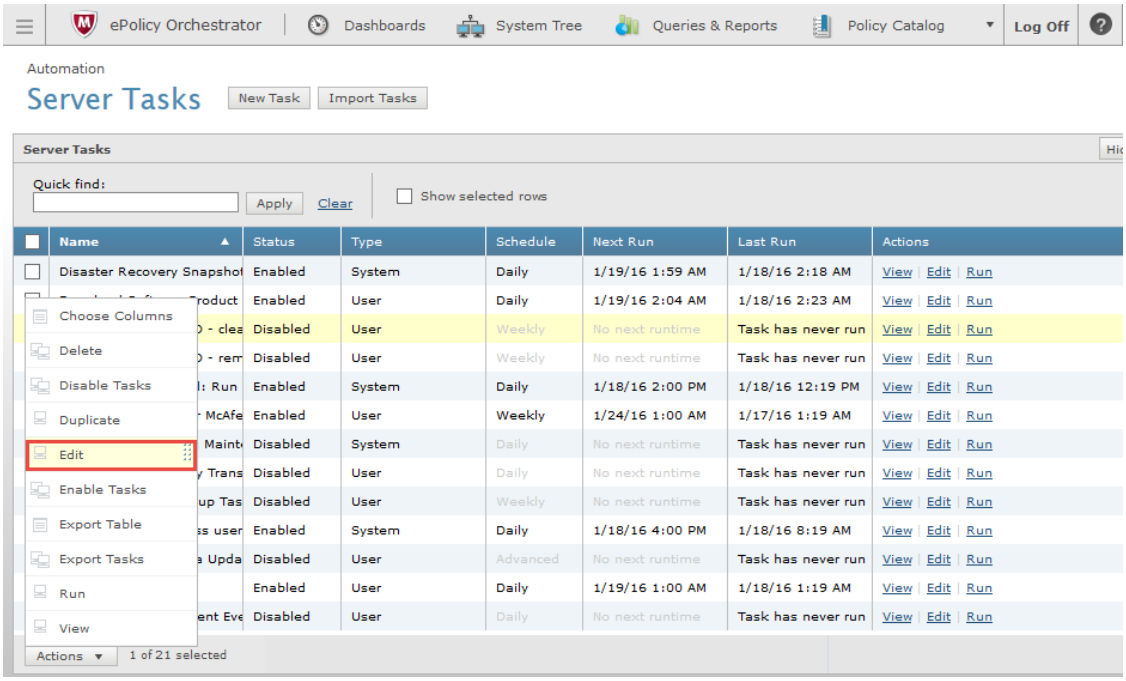


Figure 1-23 Server tasks management

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

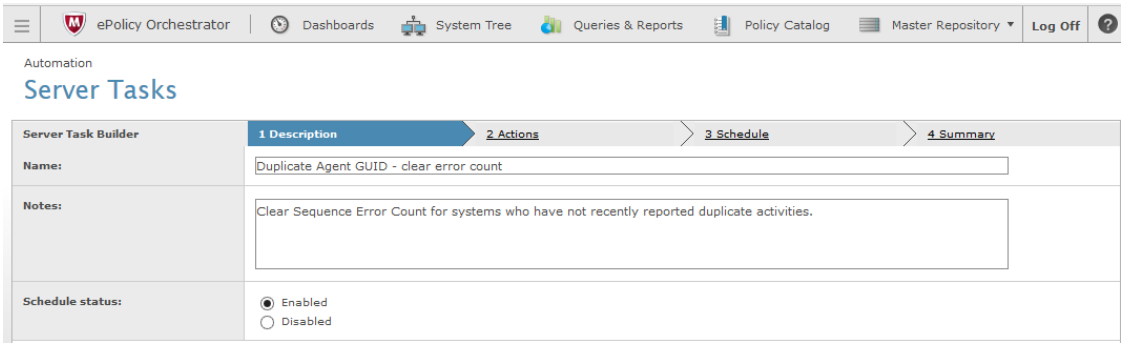


Figure 1-24 Server Task Builder page

3 Edit the name of the server, if required.

4 Select the **Schedule status** as **Enabled**.

5 Select **Next**. In the **Actions** configuration, select **NSP: Dashboard Pull Task**.

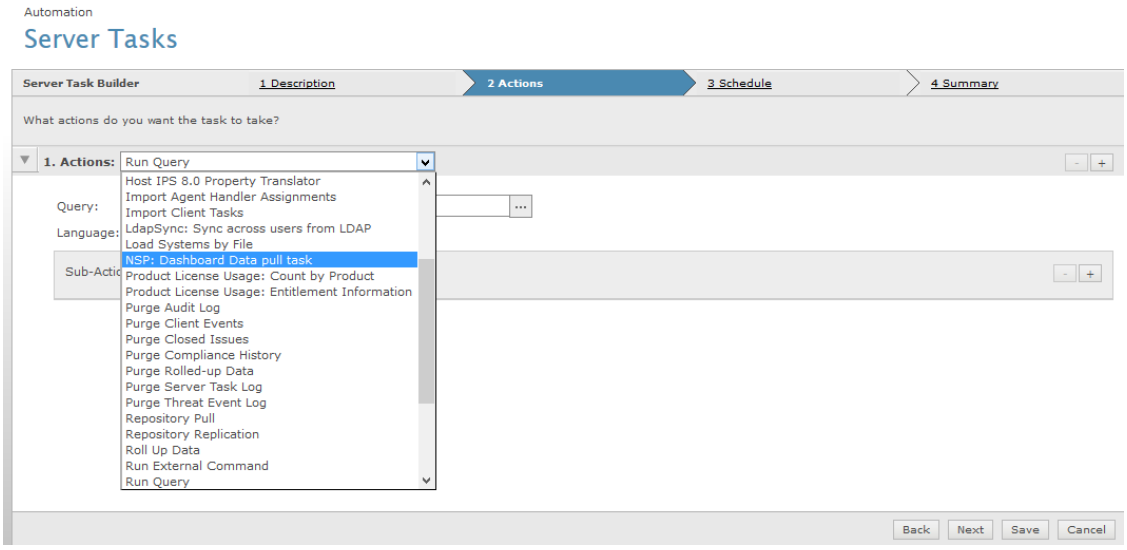


Figure 1-25 Actions option

6 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**

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).

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.

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

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

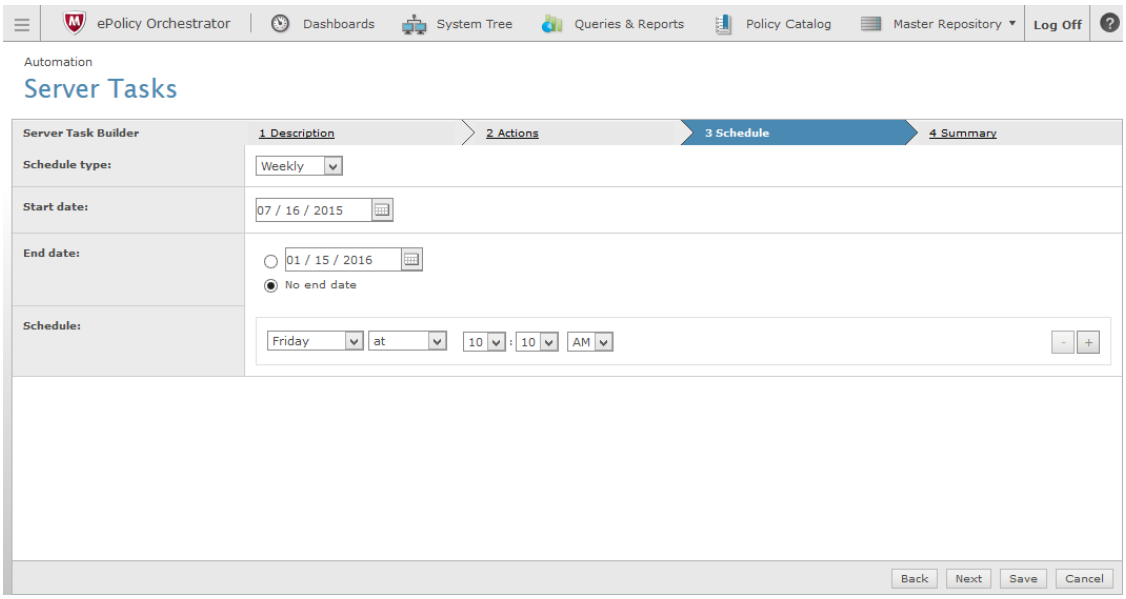


Figure 1-26 Server Task Builder tab

8 Edit the task schedule details, if required.

9 Select **Next**. The **Server task summary** is displayed.

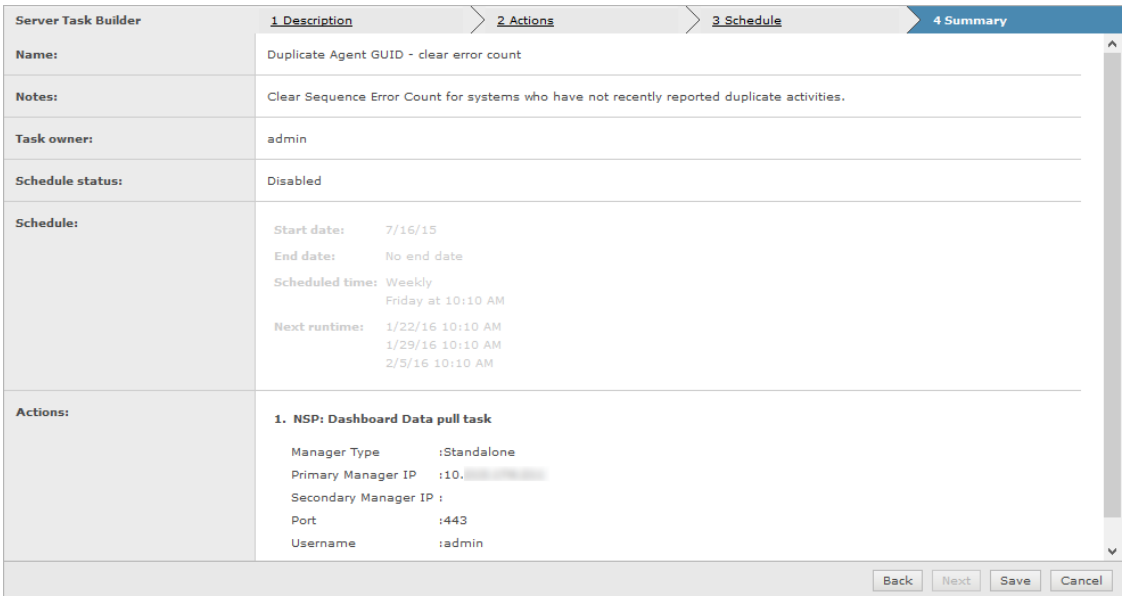


Figure 1-27 Server Task Builder tab

10 Select **Save**.

See also

Configurations on page 24

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™ home page, select **Menu** | **Dashboard** | **Dashboard Actions** | **New**.

2 Choose a layout for the dashboard.

3 You need to configure the monitors in the dashboard. While configuring a monitor, click on **New Monitor**

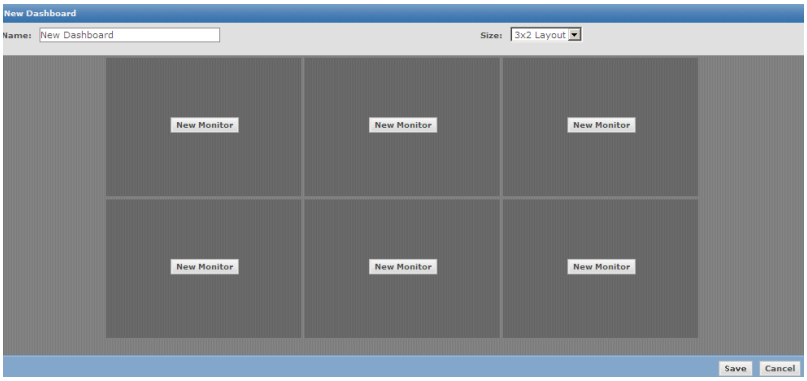


Figure 1-28 New Dashboard window

4 Choose the Category as **Queries** and select a Monitor related to Network Security Platform. For example, you can choose Monitor as **NSP: Top 10 Attacks**.

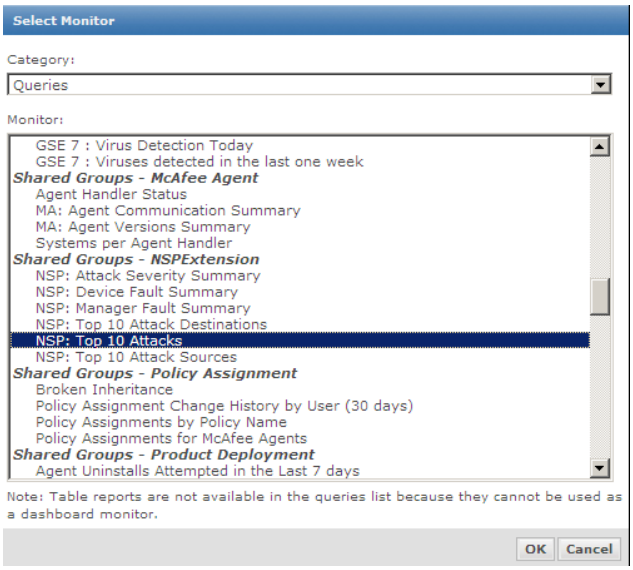


Figure 1-29 Select Monitor window

5 Select **OK**.

6 Configure six different monitors available on the dashboard as per your requirements.

7 Click **Save**. The new dashboard tab is displayed in McAfee ePO™.

A sample dashboard in McAfee ePO™ with the data from Network Security Platformis displayed below.

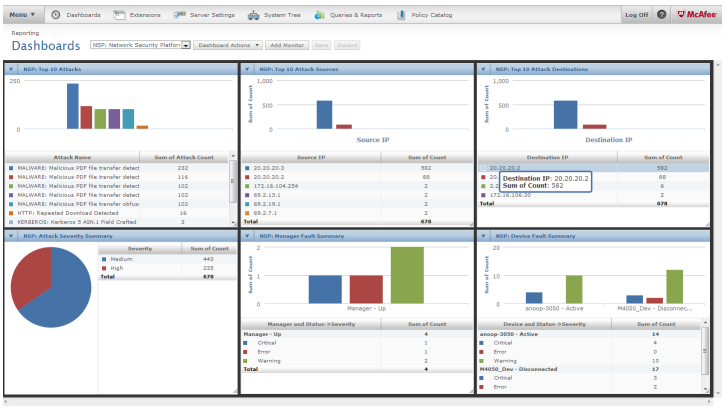


Figure 1-30 Dashboards tab

8 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**.

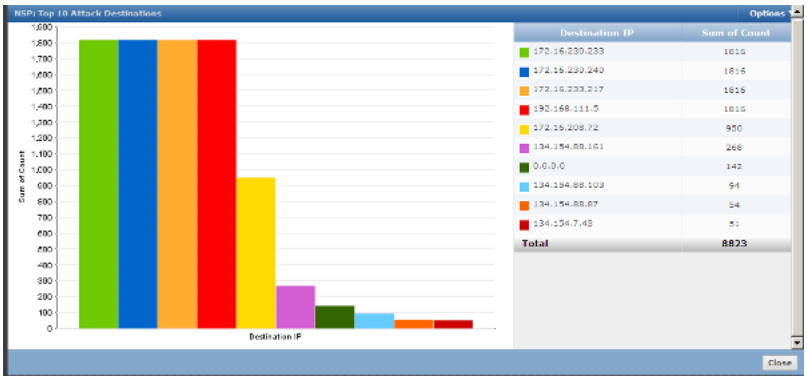


Figure 1-31 NSP Top 10 Attack Destinations window

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

See also

Configurations on page 24

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

1 From the McAfee ePO Home page, select **Menu** | **User Management** | **Permission Sets**.

Permission Sets page appears.

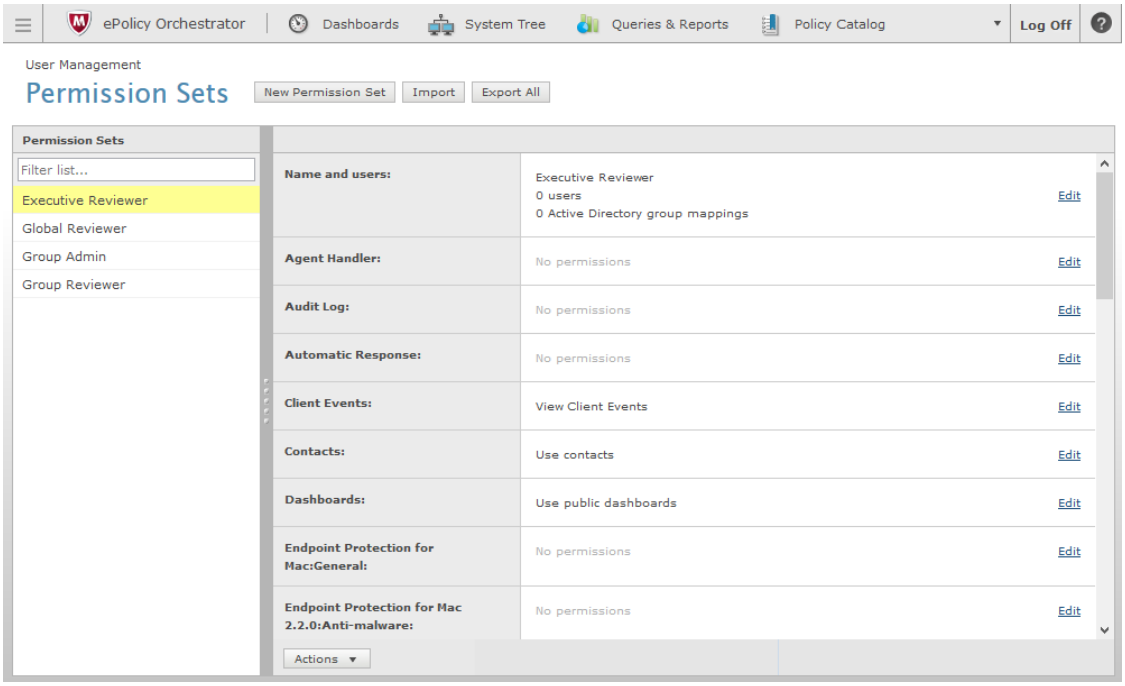


Figure 1-32 Permission Sets page

2 Click **New Permission Set**.

New Permission Set page opens.

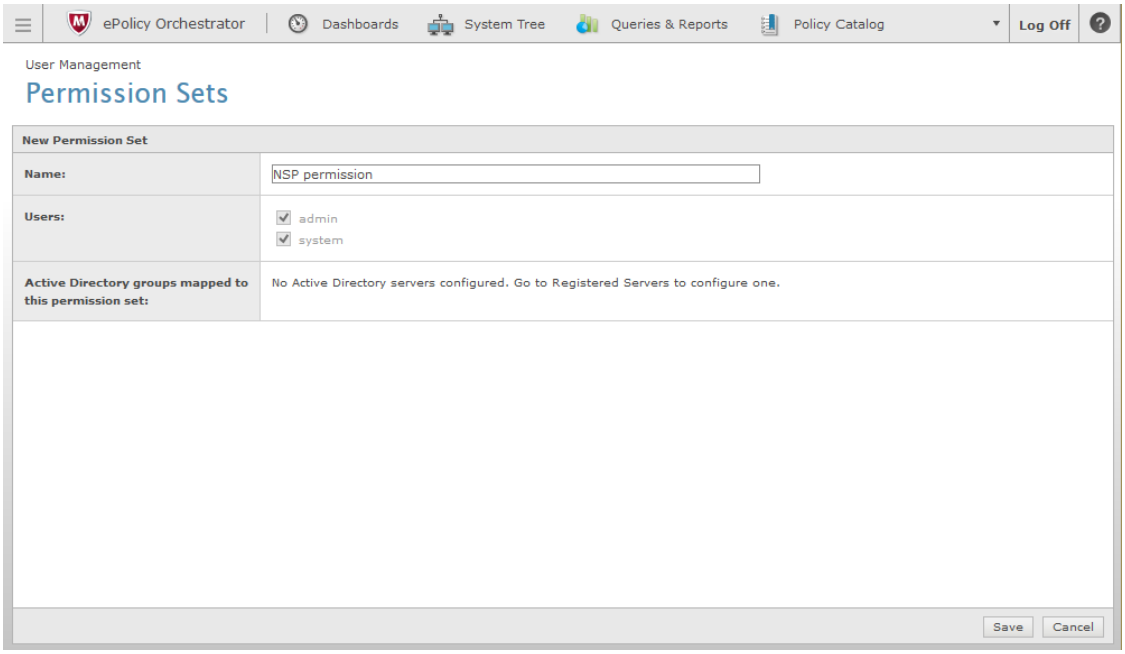


Figure 1-33 New Permission Set window

3 Type the name of the permission set in **Name**.

4 Click **Save**. After the permission set is created, it appears on the page.

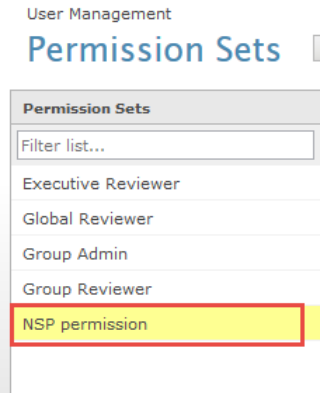


Figure 1-34 Permission Sets tab

View and edit a permission set

To 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.

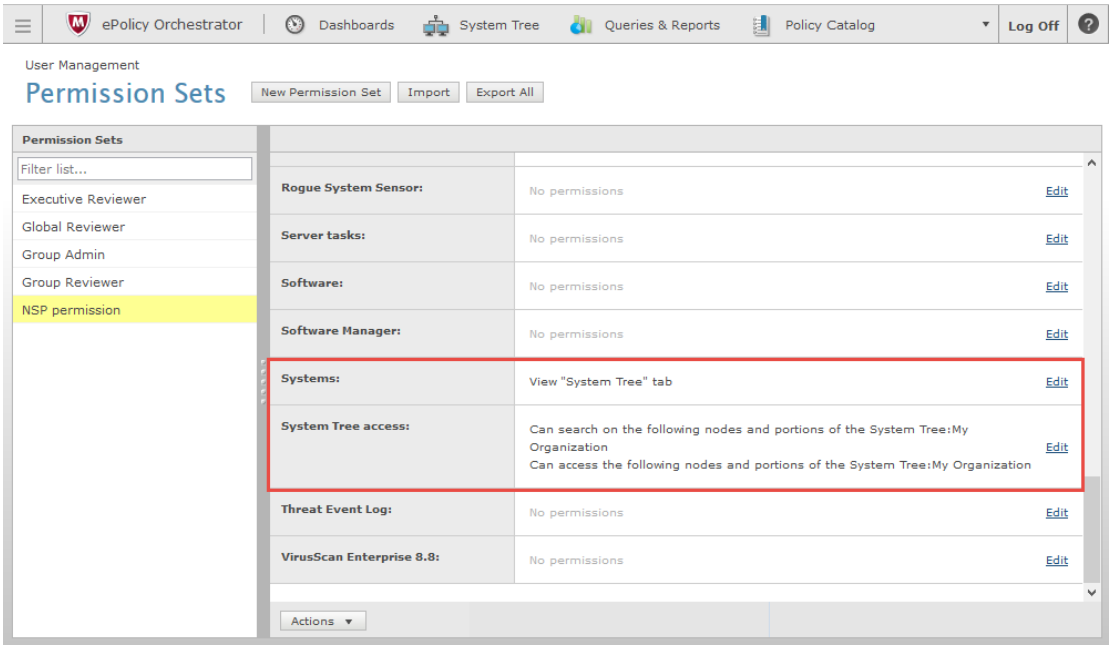


Figure 1-35 Permission Sets page

2 Scroll down to view or edit the settings for defining permission for the following:

- **Network Security Platform** — to view and change settings
- **Systems** — to view the **System Tree** Tab
- **System Tree access** — for accessing the nodes and portions of the System Tree.

Click on **Edit**, next to the relevant settings to make changes to the permission set.

Create McAfee ePO™ users with minimal permission

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

Task

1 From the McAfee ePO™ Home page, select **Menu** | **User Management** | **Users**.

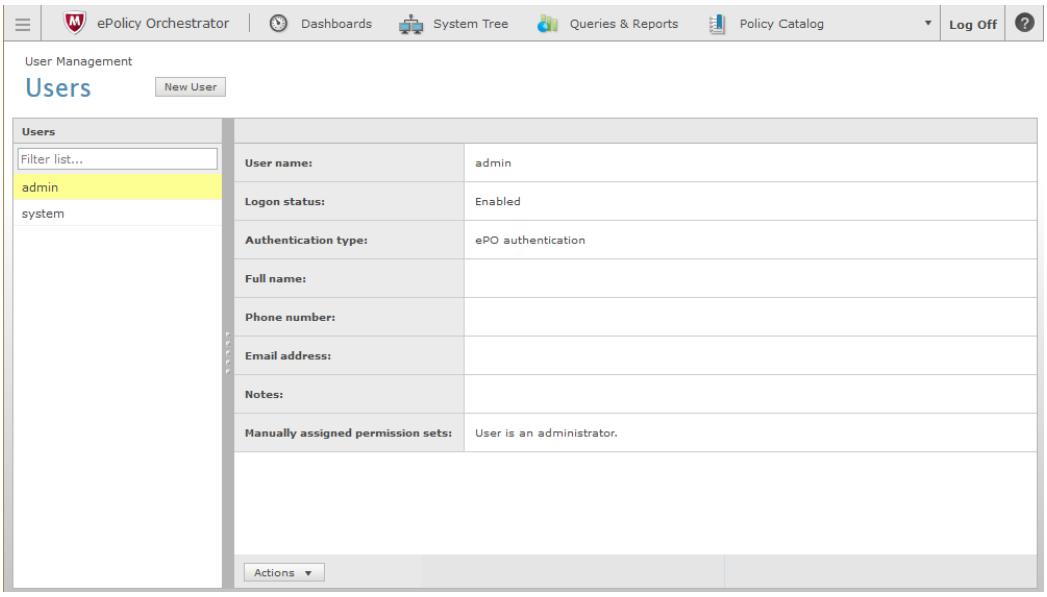


Figure 1-36 Users page

2 Click **New User**.

The **New User** page appears.

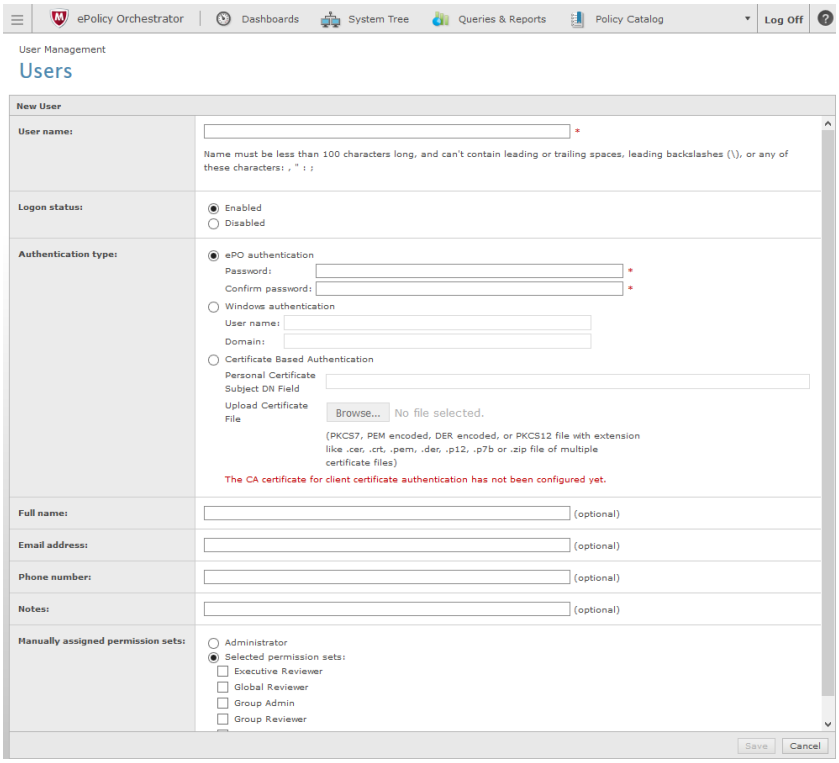


Figure 1-37 New User page

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.

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

8 Click **Save**.

2 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.

Figure 2-1 Global Threat Intelligence technologies

GTI has two components:

- **IP Reputation [formerly TrustedSource]** — Comprehensive, real-time, cloud-based IP Reputation service to provide
  - **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.
  - **Message reputation** — Message and sender reputation service to protect against message-based threats such as spam
  - **Network connection reputation** — IP address, network port, and communications protocol reputation service to determine granular reputation intelligence protect 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.

See also

Network Security Platform-GTI integration for IP Reputation on page 49

Contents

- *How Network Security Platform - GTI integration works*
- *Network Security Platform-GTI integration for IP Reputation*
- *Network Security Platform-GTI integration for connection limiting policies*
- *Network Security Platform-GTI integration for File Reputation*

How Network Security Platform - GTI integration works

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

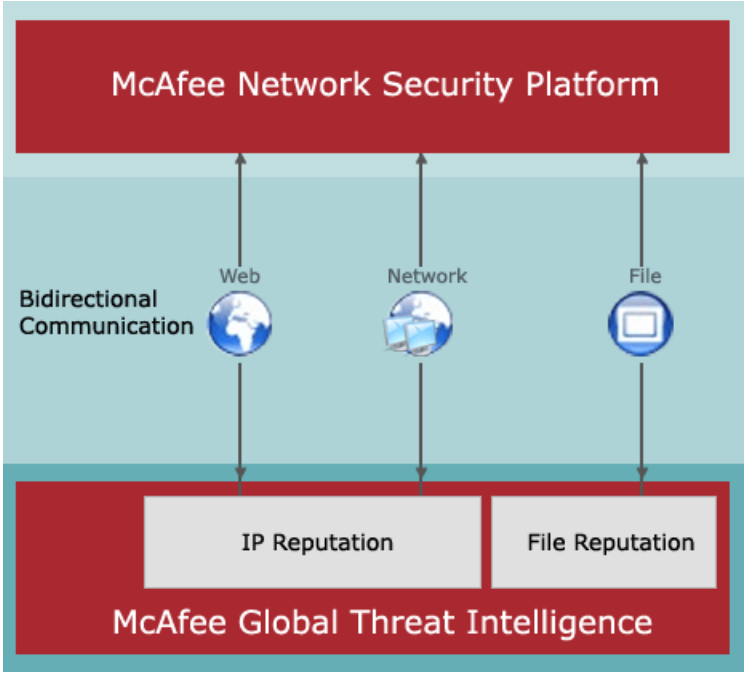


Figure 2-2 GTI integration

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 and File Reputation) that ensures threat intelligence services like file reputation, web 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 cyberthreats 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.

Configure GTI

The purpose of GTI 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.

To configure the Global Threat Intelligence:

Task

1 Select **Manager** | **<Admin Domain Name>** | **Integration** | **GTI** .

The **Global Threat Intelligence** page is displayed.

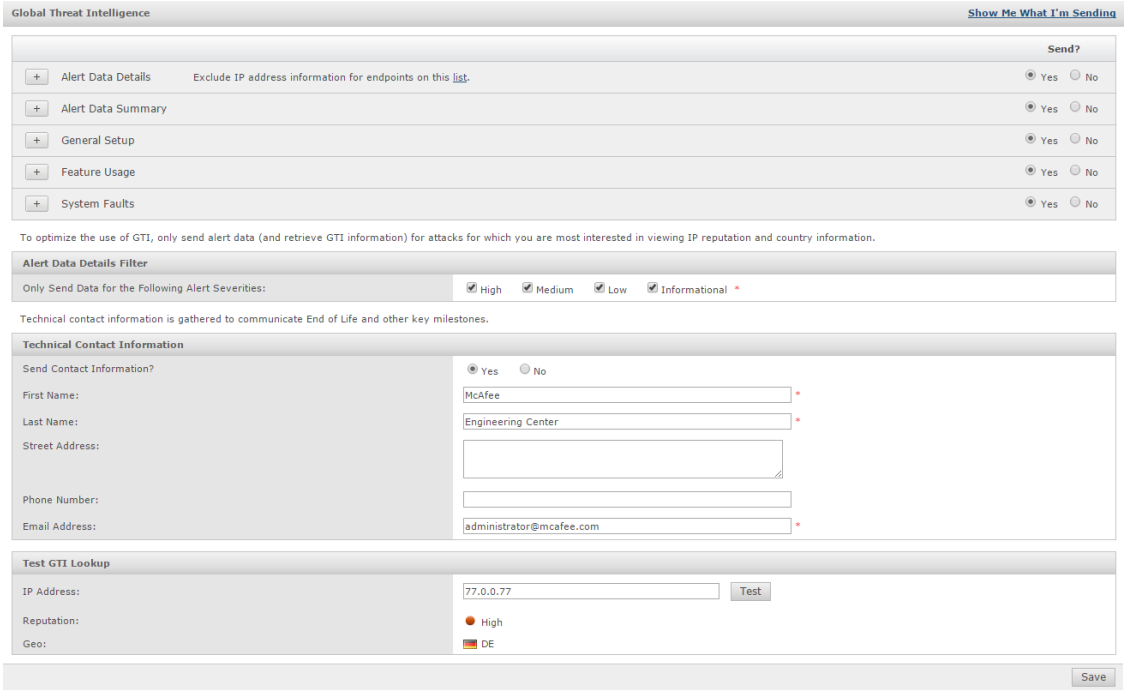


Figure 2-3 Global Threat Intelligence page

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

If at any point, you want to review what you are sending to GTI, click **Show Me What I'm Sending**. Clicking this option opens up a pop-up window which displays all the options selected on this page.

Telemetry data is stored in the telemetry server indefinitely.

2 Select either **Alert Data Details** or **Alert Data Summary** to enable GTI IP Reputation integration.

Using the **Global Threat Intelligence** 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.
- By selecting this option you can view data in the following columns in **Attack Log** page.
  - **Target IP Address**
  - **Target Risk**
  - **Attacker IP Address**
  - **Attacker Risk**
- 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 OS
- Attacker Port
- 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 blacklisted 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 OS
- Target Port
- 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

The following alert results are sent to McAfee Labs:

- Successful
- May be successful
- Failed
- Suspicious
- Blocked
- Smartblocked

- Select **Alert Data Summary** to view alert details in Attack Log. Using this option you can query McAfee's http://www.trustedsource.org for details of the source or destination host based on the IP address.

  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:
  - A count of devices configured as Failover Pairs, per device model
  - Automatically deployment of new signature sets and Callback Detectors to devices
  - Automatic downloading of signature sets and Callback Detectors from McAfee
  - Is a Central Manager in use?
  - Is Manager Disaster Recovery (MDR) in use?
  - Model and software version of each managed device
  - Manager software version and active signature set version
  - The number of monitoring 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

- **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?
- 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 custom dashboards and the monitors they contain
- 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

- **System Faults** — The following System Fault information is sent daily to McAfee Labs:
  - Device Faults
  - Manager Faults

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

3 Select **Yes** on the relevant information categories for which you prefer to send details to McAfee Labs.

1 After configuring the **Alert Data Details** and **Alert Data Summary**, navigate to the **Attack Log** page.

2 Select the alert and click **Other Actions** | **Perform GTI Forensics**.

3 Click on attacker or target IP address. A new browser window opens, displaying information about that URL.

If GTI is not enabled in the **Global Threat Intelligence** 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**

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, use the **Test GTI Lookup** section. Enter an IP address and determine its risk based on GTI data.

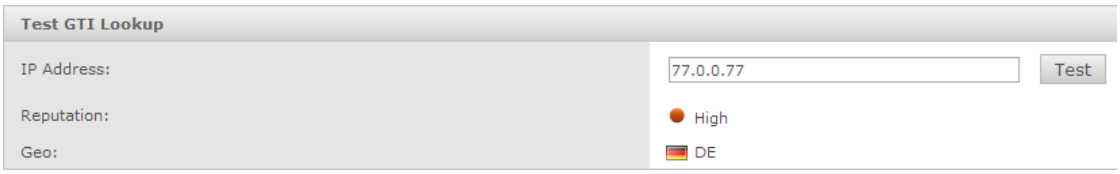


Figure 2-4 Test GTI Lookup

If you enter a known high risk IP address when GTI is functioning, you will notice a color code for the **Reputation** and a flag for the **Geo**. The reputation indicates the perceived risk of the server and geography the location of that server. The table below shows you a list of responses and what they interpret:

Table 2-1 List of responses when you test GTI look-up

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 if your Manager server functioning properly.
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.

7 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.

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.

See also

Integration with McAfee Global Threat Intelligence on page 3

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.

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.

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

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

HTTPS is used to obtain the reputation of the hosts.

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

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

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 a whitelist. The number of entries you can whitelist per Sensor are:

Sensor model	Number of whitelist entries permitted
NS9300, NS9200, NS9100	128
NS7300, NS7200, NS7100	128
NS5200, NS5100	64
NS3200, NS3100	32
M-8000, M-6050, M-4050, M-3050	128
M-2950, M-2850	64
M-1450, M-1250	32

Refer to *McAfee Network Security Platform IPS Administration Guide* for more details.

Configure IP 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** | **Global Threat Intelligence** to enable the integration.

If you configure IP 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

1 In the Manager, click **Policy** and select the required **Domain.**

2 Select **Intrusion Prevention** | **Policy Types** | **Inspection Options Policies.**

The **Inspection Options Policies** page is displayed.

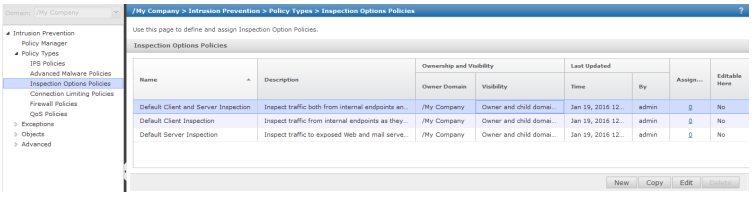


Figure 2-5 Inspection Options Policies page

3 Double-click on the policy for which you wish to configure file reputation.

The **New Policy** window opens with the **Properties** tab selected. The **Inspection Options** page is displayed.

4 Update the following fields:

Table 2-2 Properties option definitions

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	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.

5 Click **Next**.

The **Inspection Options** tab is displayed. By default, the **Traffic Inspection** tab within the **Inspection Options** tab is displayed.

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

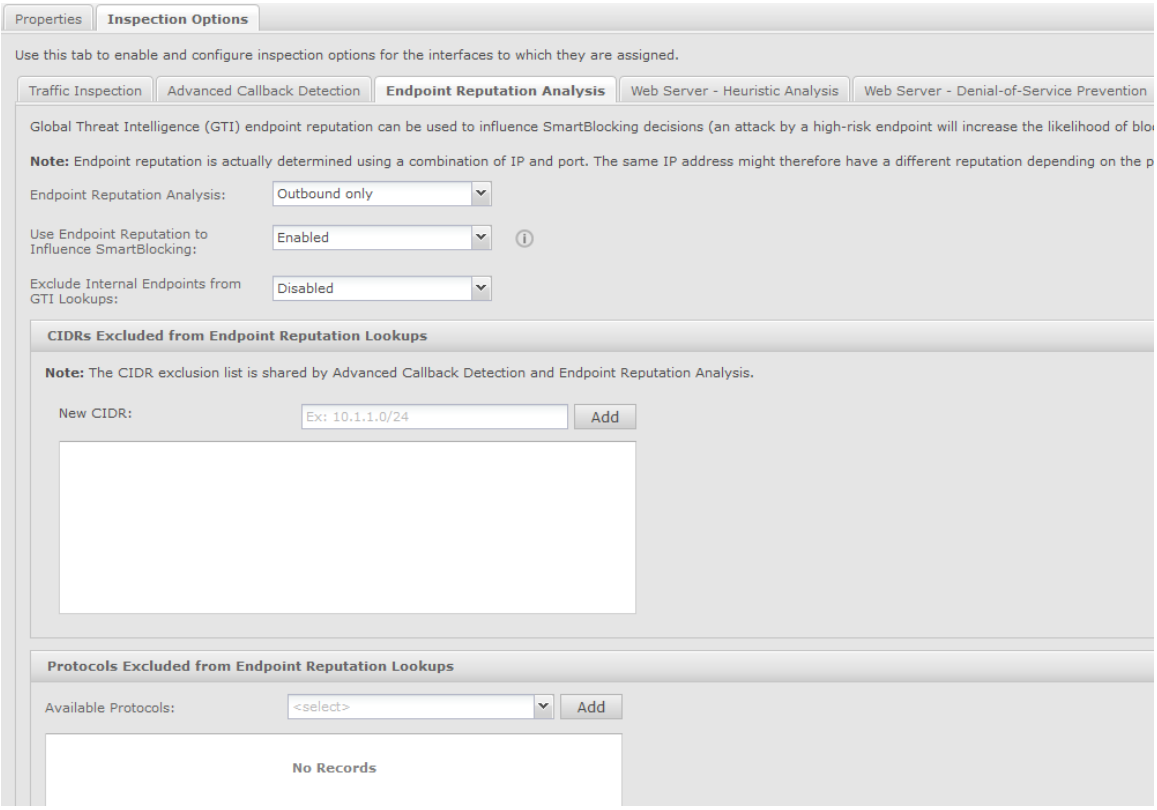


Figure 2-6 Endpoint Reputation Analysis

The **Endpoint Reputation Analysis** tab configure the following fields:

Table 2-3 Endpoint Reputation Analysis

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. The CIDR exclusion list is shared by **Advanced Callback Detection** and **Endpoint Reputation Analysis**

Table 2-3 Endpoint Reputation Analysis *(continued)*

Option	Definition
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.
Save	Click **Save** to save the changes.
Cancel	Reverts to the last saved configuration.

Configure IP Reputation for an interface

You must enable IP 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** | **<Admin Domain Name>** | **Intrusion Prevention** | **Policy Manager**.
2. In the **Interfaces** tab, double-click the interface to enable the advanced traffic inspection.

   The **<Device name/Interface>** panel opens.
3. In the **Inspection Options** section, select the policy from the **Policy** drop down list.

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

   If you are creating a new policy proceed to step 5. If you are editing an existing policy proceed to step 6.

4 The **Properties** page opens. Enter the **Name** and **Description**. Select the **Visibility** and click **Next**.

The **Inspection Options** page opens.

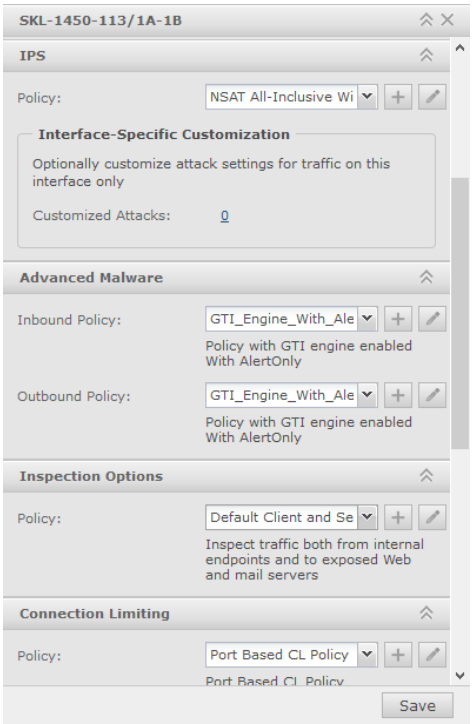


Figure 2-7 Configure IP Reputation from interface level

5 In the **Endpoint Reputation Analysis** tab, enable **Endpoint Reputation Analysis** in the required direction.

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

6 Specify the IP Reputation options in the corresponding fields.

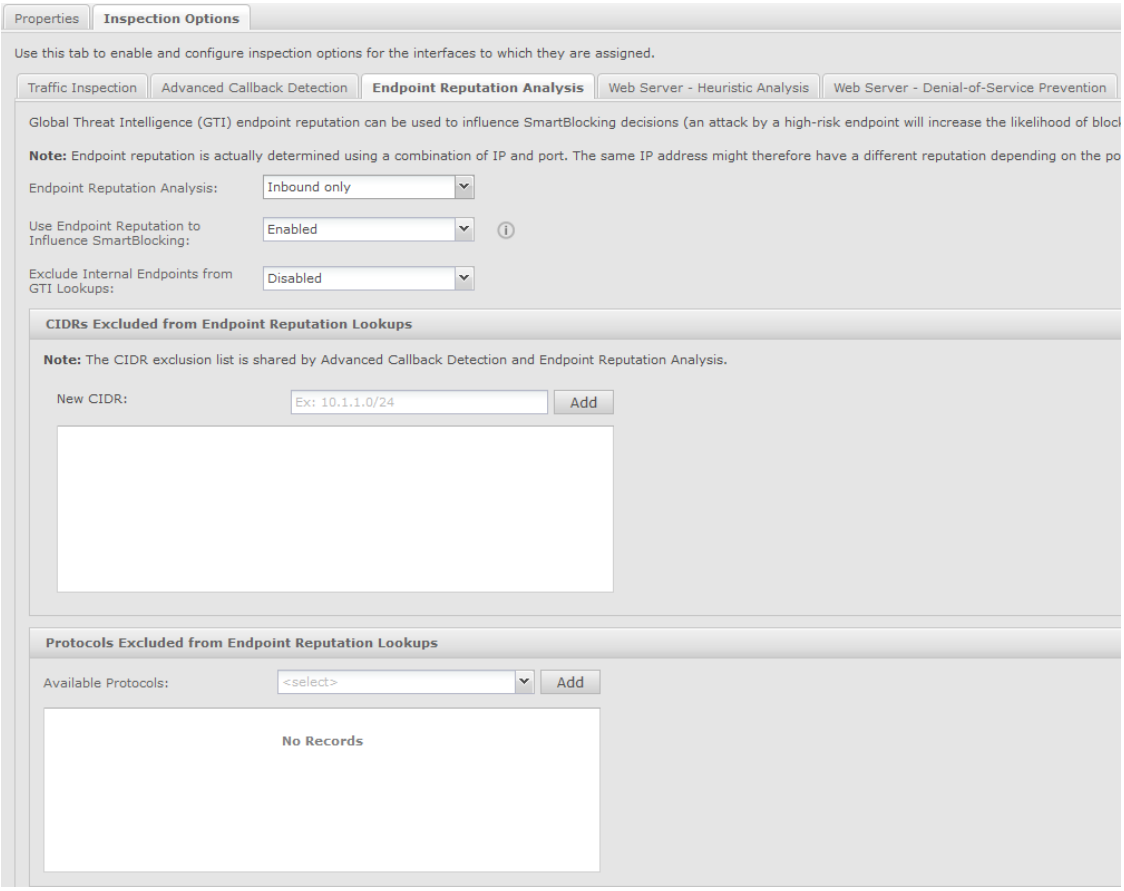


Figure 2-8 IP Reputation dialog for an interface

Table 2-4 Option definitions

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. Select **Inherit CIDR Exclusion list** from **Global Threat Intelligence** page to add the exclusion list directly from **Manager** | **<Admin Domain Name>** | **Integration** | **GTI**.

Table 2-4 Option definitions *(continued)*

Option	Definition
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 Reputation Lookup configuration.
Cancel	Cancels the configuration process and exits the page.

7 Click **Save** in the **<Device Name/Interface>** panel to save the configuration changes.

8 Do a configuration update for the corresponding Sensor.

Configure IP Reputation from sub-interface level

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

Refer to *McAfee Network Security Platform IPS Administration Guide* for more information.

Exclude IP Address Information for Specific Hosts

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

To exclude IP address information for hosts:

Task

1 On the **Global Threat Intelligence** page, click **list** under **Alert Data Details**.

The **Exclusions** page is displayed.

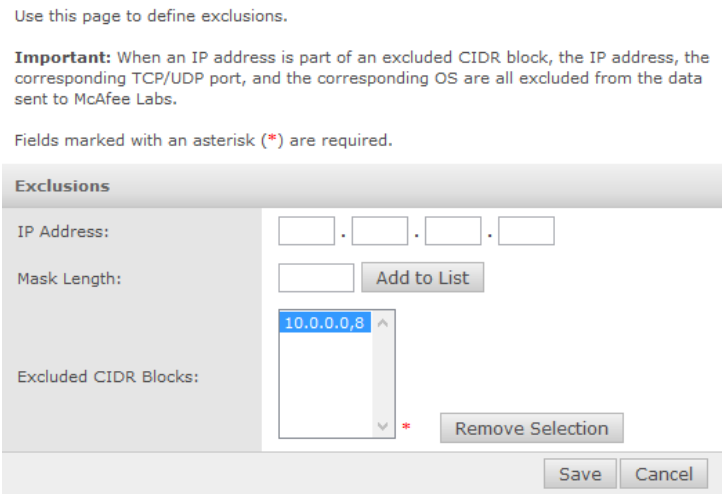


Figure 2-9 IP Address Exclusions dialog

2 Type the IP address for exclusion in the **IP Address** field.

3 Type the CIDR value for the mask in the **Mask Length** field.

The CIDR value should be between 0 to 32.

4 Click **Add to List**.

The CIDR block for the IP address gets added and is displayed in the **Excluded CIDR Blocks** field.

You can remove a CIDR block by clicking **Remove Selection**.

5 Click **Save**.

Viewing the Global Threat Intelligence alert category details

The following Global Threat Intelligence alert categories are included in the **Alerts** page.

- **Dest Country**
- **Dest Reputation**
- **Src Country**
- **Src Reputation**

For more information on alerts and monitors, see the *McAfee Network Security Platform Manager Administration 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, the format in which you want the data to be presented such as 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** | **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 - GTI Participation Summary
- Default - Attack Source Reputation Summary
- Default - Top Attack Destinations
- Default - Top Attack Sources
- Default - Top 10 Attack Source Countries

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 Manager Administration Guide*.

How to view GTI 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**, and **General Setup**.

To view the GTI Report, on the **Global Threat Intelligence** page, click **Show Me What I'm Sending**.

The **Global Threat Intelligence Report** is displayed.

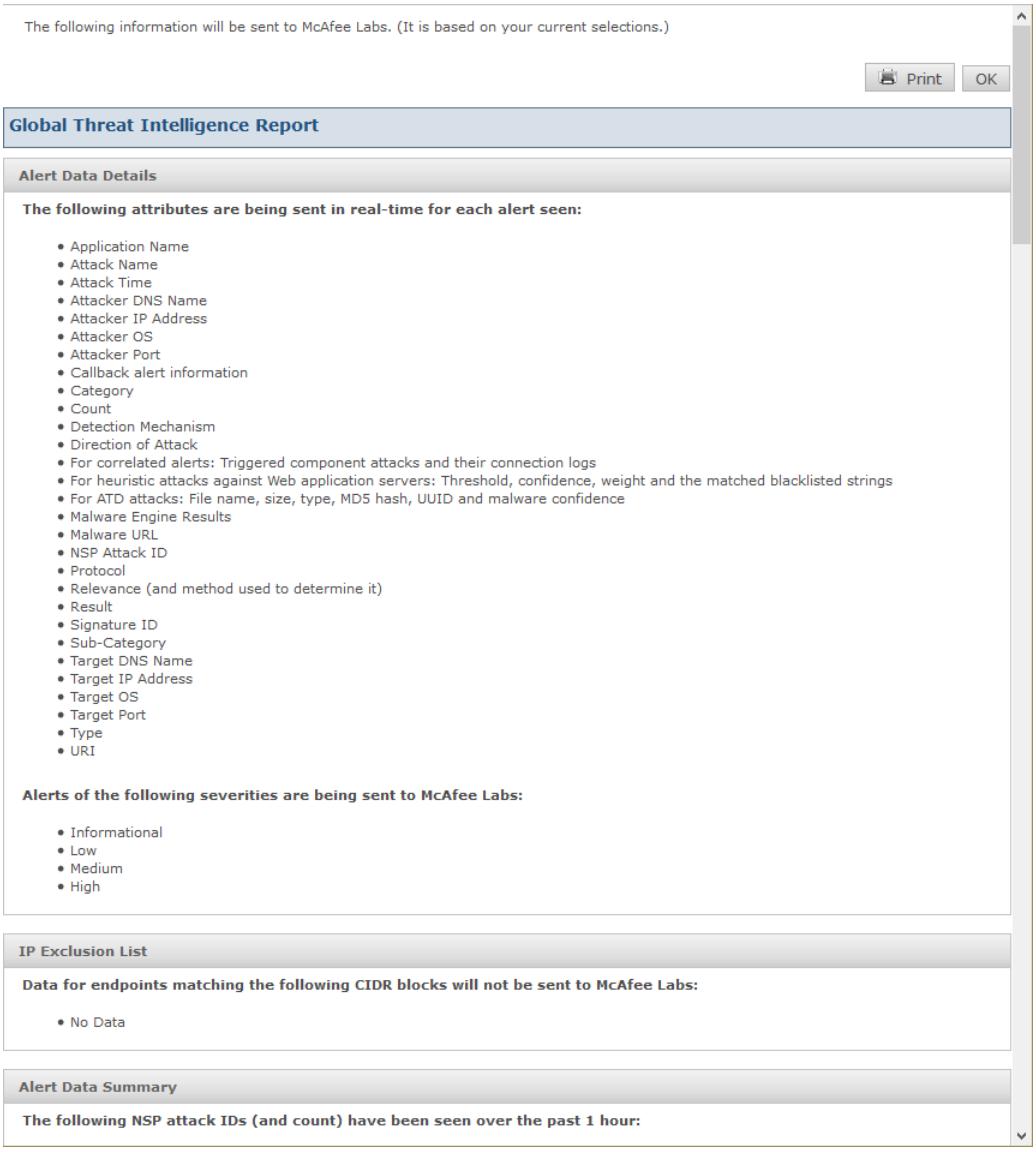


Figure 2-10 Global Threat Intelligence report

Alert data details

The **Alert Data Details** section of the GTI report, displays the attributes being sent in real-time for each alert seen.

It also displays the severities of the alerts being sent to McAfee Labs.

Alert Data Details

The following attributes are being sent in real-time for each alert seen:

- Application Name
- Attack Name
- Attack Time
- Attacker DNS Name
- Attacker IP Address
- Attacker OS
- Attacker Port
- 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 blacklisted 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 OS
- Target Port
- Type
- URI

Alerts of the following severities are being sent to McAfee Labs:

- Informational
- Low
- Medium
- High

Figure 2-11 Alert Data Details area

General Setup display

The following data is displayed under the **General Setup** section in the GTI report:

General Setup

Manager Software Version:	8.
Active Signature Set Version:	8.7.64.37
Inline Port Count:	44
SPAN Port Count:	4
Tap Port Count:	0
Dedicated Interface Count:	23
CIDR Interface Count:	0
VLAN Interface Count:	6
Is Manager Disaster Recovery (MDR) in use:	false
Is a Central Manager in use:	false
Automatic downloading of signature sets and Callback Detectors from McAfee:	false
Automatic deployment of new signature sets and Callback Detectors to devices:	false
Administrative User Count:	1
Custom Role Count:	0
Custom User Role Names and Their Permissions:	

Device Model (software version)

M-8000 (8.2.3.96)
IPS-NS7200 (8.3.5.2)
IPS-NS7300 (8.3.4.11)

Failover Pairs in Use (by device model)

No Data

Figure 2-12 General Setup area

Feature usage display

The **Feature Usage** section displays the feature usage information sent daily to McAfee Labs.

Feature Usage

The following feature usage information is sent daily to McAfee Labs:

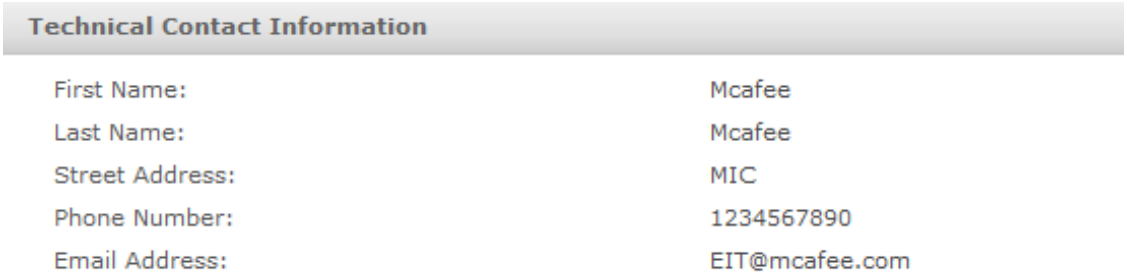
The number of default IPS policies in use:	4
The number of custom IPS policies in use:	3
The number of custom McAfee-format attacks in use:	4384
The number of Snort rules in use:	274
The number of ignore rules defined:	0
The number of M-series devices with IPS licenses assigned:	1
The number of sub-interfaces in use:	60
The number of device-pre firewall policies assigned:	1
The number of port firewall policies assigned:	2
The number of interface firewall policies assigned:	5
The number of device-post firewall policies assigned:	2
Is ePO integration enabled:	false
Is MVM integration enabled:	false
Is alert relevance analysis enabled:	false
Is IPS alert notification via SNMP enabled:	true
Is IPS alert notification via syslog enabled:	false
Is IPS alert notification via email enabled:	false
Is IPS alert notification via pager enabled:	false
Is IPS alert notification via script enabled:	false
The number of custom dashboards:	0
The number of IPS attack definitions whose default settings have been customized:	13980
The number of custom NextGen reports:	0
Is inbound GTI IP reputation lookup enabled:	true
Is outbound GTI IP reputation lookup enabled:	true
Is GTI IP reputation lookup used to enhance SmartBlocking decisions:	false
Is inbound heuristic Web application server protection enabled:	true
Is outbound heuristic Web application server protection enabled:	true
Is inbound XFF header parsing enabled:	true
Is outbound XFF header parsing enabled:	true
Is inbound advanced callback detection enabled:	true
Is outbound advanced callback detection enabled:	true
Are potential callback events sent to NTBA:	true
Callback Detectors Version:	1221
Is automatic download of Callback Detectors from the McAfee update server enabled:	false
Is automatic deploy of Callback Detectors to devices enabled:	false
Are inbound MSRPC/SMB fragments being reassembled:	true
Are outbound MSRPC/SMB fragments being	

Figure 2-13 Feature Usage area

Technical Contact Information display

The following data is displayed under the **Technical Contact Information** section in the GTI report:

- **First Name**
- **Last Name**
- **Street Address**
- **Phone Number**
- **Email Address**



Technical Contact Information

First Name:	Mcafee
Last Name:	Mcafee
Street Address:	MIC
Phone Number:	1234567890
Email Address:	EIT@mcafee.com

Figure 2-14 Technical Contact Information area

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 IPS Administration 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.

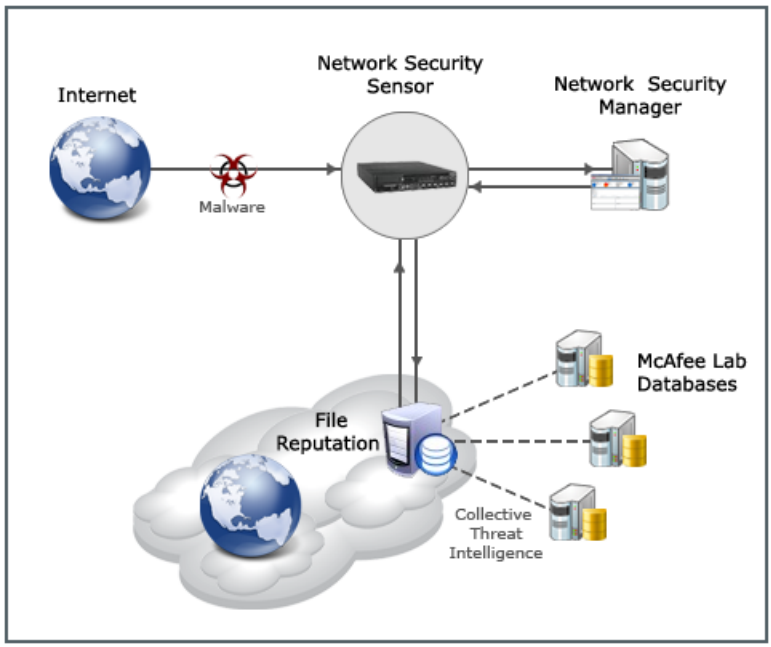


Figure 2-15 Integration between Network Security Platform and File Reputation

When a file download is detected over HTTP traffic, the file type is checked. If the file type matches the list of the file types for which the malware is checked, then, the Sensor creates a fingerprint (MD5 hash value) of the file, embeds the fingerprint in a standard DNS 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.

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, 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 detection, or both. When you enable both File Reputation detection type and Custom detection type, the latter takes precedence over the former.

Primary and Secondary DNS Server IP Address

IP address information related to the local Primary and Secondary DNS Servers. The Sensor embeds the MD5 hash value of the file in a DNS Request. The local DNS Servers forward the DNS Requests from the Sensor to File Reputation server. File Reputation server sends back DNS Responses (which contain information such as Malware dirtiness level) to the Sensor through the local DNS Server.

Benefits of File Reputation

The key benefits of File Reputation include:

- Compresses the threat protection time period from days to milliseconds.
- Increases malware detection rates.
- 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 DNS Server.

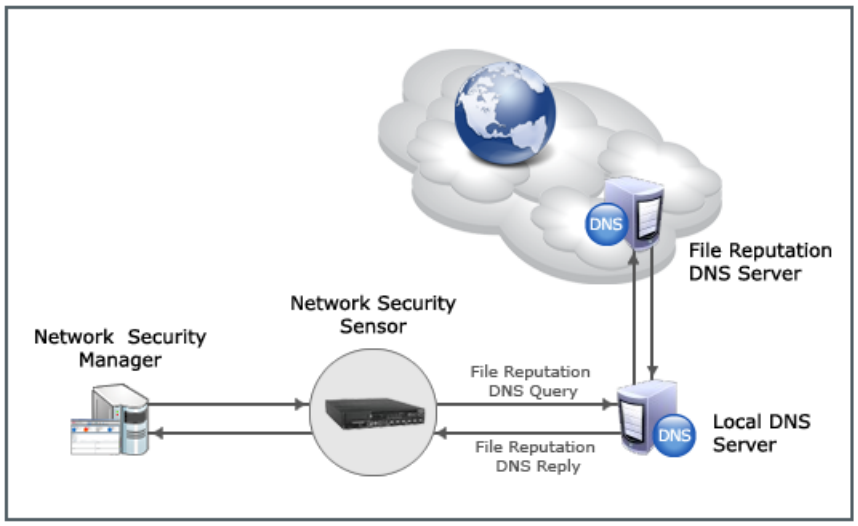


Figure 2-16 Communications between Sensor, Manager, and File Reputation DNS server

File Reputation uses the Internet DNS mechanism 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 DNS Request and sends it to File Reputation DNS server. The Sensor exchanges DNS queries and responses with File Reputation DNS Server through configured local DNS Servers (Primary and Secondary).

> The Primary and Secondary local DNS servers can be configured in the Manager from the **Devices** tab in **Name Resolution** settings. Depending on the Sensor management port configurations, you can set IPv4 or IPv6 local DNS servers. The DNS Server configurations in the Manager are pushed to the Sensor during the configuration update.

The Sensor management port can handle multiple DNS requests and responses. File Reputation DNS Queries (which are UDP DNS Requests) are sent out from the Management port of the Sensor to the local DNS server. File Reputation replies back via the local DNS Server. File Reputation DNS Replies from the local DNS server are encoded in the standard DNS 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 Attack Log for the attack for Malware attacks.

The Sensor takes a response action (alert/block or both) to 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.

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

If the Response Action is set to Alert and Block, the alerts are raised in the Attack Log, and the file download is blocked.

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. That is, 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.

> 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, that is, inline, tap, and SPAN. In the inline mode, malware is detected in both Inline fail-open and Inline fail-closed modes.

In versions earlier than Network Security Platform 7.1, for File Reputation to work, you must enable HTTP Response Scanning in the corresponding port or port-pair. In Network Security Platform 7.1 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-File Reputation integration in a Manager Disaster Recovery (MDR) setup

Once the MDR is created, and all the Sensor s 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. Also, if the Primary Manager switches back to the active mode as before, the changes made in the Secondary are retrieved and updated correctly 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 DNS 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 from 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.

In versions earlier than Network Security Platform 7.1, for File Reputation to work, you must enable HTTP Response Scanning in the corresponding port or port-pair. In Network Security Platform 7.1 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.

Configure File Reputation

Before you begin

You must determine if a DNS Server (referred to as Name Resolution) has been configured on the specific Sensor. If you have not, go to **Devices** | **<Admin Domain Name>** | **Global** | **Common Device Settings** | **Name Resolution** to enable it.

Follow these steps to configure file reputation.

Task

1 Select **Devices** | **<Admin Domain>** | **Global** | **IPS Device Settings** | **File Reputation**.

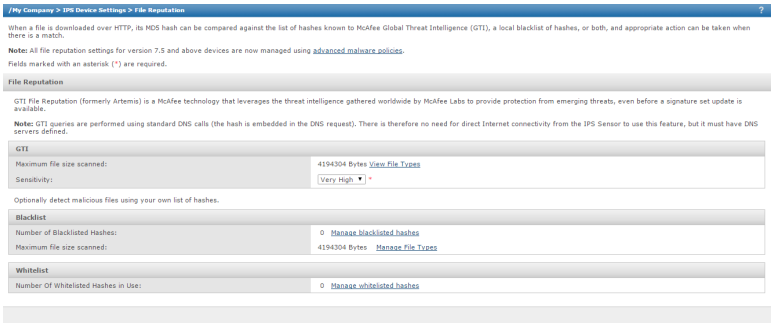


Figure 2-17 File Reputation area

2 Under **GTI** section, you can view the maximum file size scanned.

You can also view the file types that are scanned by GTI File Reputation from **View File Types**.

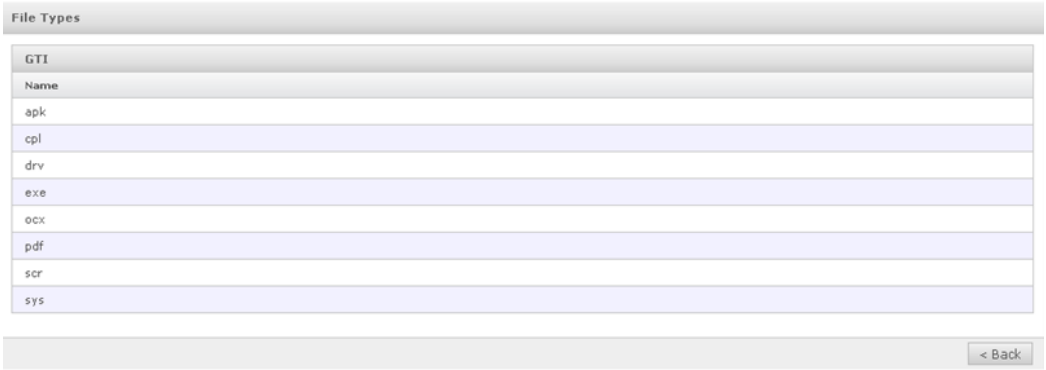


Figure 2-18 File Types area

3 Select the **Sensitivity Level**.

- **Very Low**
- **Low**
- **Medium**
- **High**
- **Very High**

The default value is **Very Low**.

4 To manage blacklisted and whitelisted hashes, see the subsequent sections.

5 Click **Save** to save the configuration.

Manage whitelist and blacklist

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

In versions earlier than Network Security Platform 7.1, for File Reputation to work, you must enable HTTP Response Scanning in the corresponding port or port-pair. In Network Security Platform 7.1 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.

See also

Add hash values to the whitelist on page 67
Add hash values to the blacklist on page 68

Add hash values to the whitelist

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

Task

1 Select **Devices** | **<Admin Domain>** | **Global** | **IPS Device Settings** | **File Reputation**.

In the **Whitelist** section, you can add the hash values to be whitelisted.

2 Click **Manage whitelisted hashes**.

You can view the current list of whitelisted hashes in the **Whitelisted Hashes** tab of the **File Hash Exceptions** page.

3 Click **Import** to import a file containing the hash values.

4 Click **Browse** to locate an XML or CSV file that contains the list of hashes that you want to import.

5 Select **Append** or **Replace** depending on whether you want to append to the current whitelist or replace it, and then click **Import**.

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

Format	Description
File Hash	Specifies the file hash.
File Name	Specifies the name of the file to be imported, along with the file extension.
Classifier	Specifies the location from where the whiltelist is imported.
Classified	Specifies the time stamp of the imported whitelist.
Comment	Any comments about the list.

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.

To export the whitelisted hashes from the Manager to a local system, click **Export Whitelist**.

6 To delete specific entries from the whitelist, select them by holding the *Shift* or *Ctrl* key and click on the required rows. Then select **Remove selected hashes (reset as Unclassified)** from the **Take action** drop-down list.

The deleted hashes are now neither in the whitelist nor in the blacklist.

7 To remove all the entries, select **Remove all hashes (reset as Unclassified)** from the **Take action** drop-down list.

8 To move specific entries to the blacklist, select the entries and then select **Move selected hashes to blacklist** from the **Take action** drop-down list.

9 To move all entries to the blacklist, select **Move all hashes to blacklist** from the **Take action** drop-down list.

Add hash values to the blacklist

You can add MD5 hash values of files to treat as malicious when found in HTTP and SMTP downloads. If a file's hash matches a hash value in the blacklist, the Sensor treats the file as malicious of *very high* severity.

Task

1 Select **Devices** | **<Admin Domain>** | **Global** | **IPS Device Settings** | **File Reputation**.

In the **Blacklist** section, you can add the hash values to be blacklisted, manage the file types to be checked for the blacklisted hashes, and view the maximum file size scanned.

2 Click **Manage blacklisted hashes.**

3 Click **Import** to import a file containing the hash values.

4 Click **Browse** to locate an XML or CSV file that contains the list of hashes that you want to import.

5 Select **Append** or **Replace** depending on whether you want to append to the current blacklist or replace it, then click **Import**.

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

Format	Description
File Hash	Specifies the file hash.
File Name	Specifies the name of the file to be imported, along with the file extension.
Classifier	Specifies the location from where the blacklist is imported.
Classified	Specifies the time stamp of the imported blacklist.
Comment	Any comments about the list.

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.

6 To export the blacklisted hashes from the Manager to a local system, click **Export Blacklist**.

7 To delete specific entries from the blacklist, select them by holding the *Shift* or *Ctrl* key and clicking on the required rows. Then select **Remove selected hashes (reset as Unclassified)** from the **Take action** drop-down list.

The deleted hashes are now neither in the whitelist nor in the blacklist.

8 To remove all the entries, select **Remove all hashes (reset as Unclassified)** from the **Take action** drop-down list.

9 To move specific entries to the whitelist, select the entries and then select **Move selected hashes to whitelist** from the **Take action** drop-down list.

10 To move all entries to the whitelist, select **Move all hashes to whitelist** from the **Take action** drop-down list.

- A manual signature set push is not required each time the whitelist or the blacklist is updated. The Manager updates the Sensor dynamically with the modified entries in the whitelist or blacklist, 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 wb stats` command. For more information, see the *McAfee Network Security Platform CLI Guide*.
- You can configure a maximum of 99,000 entries (whitelist and blacklist). The manager retrieves a maximum of 1000 hashes. The callback detectors file can have 0 to 1000 McAfee blacklisted file hashes. For more information, see *Advanced callback detection*

Configure File Reputation for Advanced Malware Detection

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

Tasks

- *Add an Advanced Malware policy* on page 69

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** | **Policy Types** | **Advanced Malware Policies.**

3 Click **New**.

The **New Policy** page opens.

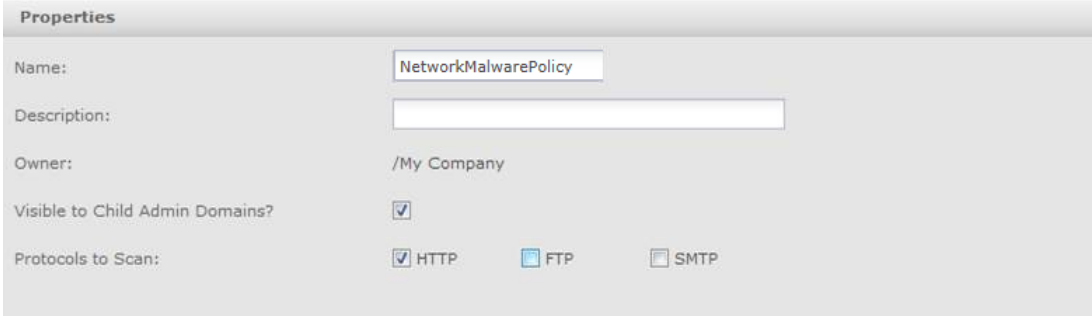
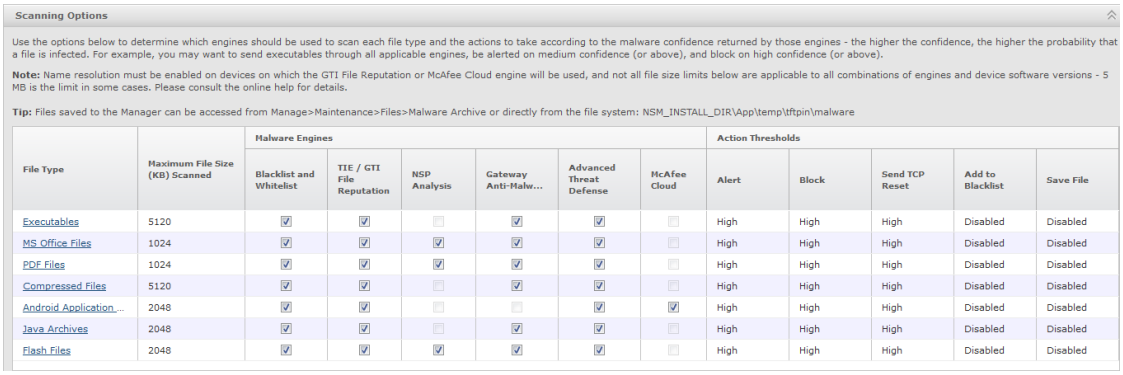


Figure 2-19 Update the properties of the Advanced Malware policy

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.
Protocols to Scan	Protocols over which advanced malware scanning is performed. The supported protocols are HTTP, FTP, and SMTP. Enable **HTTP Response scanning** to scan files in the HTTP data stream. FTP malware detection overrides the accelerate-ftp feature even if it is enabled. For more information on the `accelerate-ftp` CLI command, see *McAfee Network Security Platform CLI Guide.*

5 Update the **Scanning Options**.



Scanning Options

Use the options below to determine which engines should be used to scan each file type and the actions to take according to the malware confidence returned by those engines - the higher the confidence, the higher the probability that a file is infected. For example, you may want to send executables through all applicable engines, be alerted on medium confidence (or above), and block on high confidence (or above).

Note: Name resolution must be enabled on devices on which the GTI File Reputation or McAfee Cloud engine will be used, and not all file size limits below are applicable to all combinations of engines and device software versions - 5 MB is the limit in some cases. Please consult the online help for details.

Tip: Files saved to the Manager can be accessed from Manage>Maintenance>Files>Malware Archive or directly from the file system: NSM_INSTALL_DIR\App\temp\tftpin\malware

File Type	Maximum File Size (KB) Scanned	Malware Engines						Action Thresholds				
		Blacklist and Whitelist	TIE / GTI File Reputation	NSP Analysis	Gateway Anti-Malw...	Advanced Threat Defense	McAfee Cloud	Alert	Block	Send TCP Reset	Add to Blacklist	Save File
Executables	5120	☑	☑	☐	☑	☑	☐	High	High	High	Disabled	Disabled
MS Office Files	1024	☑	☑	☑	☑	☑	☐	High	High	High	Disabled	Disabled
PDF Files	1024	☑	☑	☑	☑	☑	☐	High	High	High	Disabled	Disabled
Compressed Files	5120	☑	☑	☐	☑	☑	☐	High	High	High	Disabled	Disabled
Android Application ...	2048	☑	☑	☐	☐	☑	☑	High	High	High	Disabled	Disabled
Java Archives	2048	☑	☑	☐	☑	☑	☐	High	High	High	Disabled	Disabled
Flash Files	2048	☑	☑	☑	☑	☑	☐	High	High	High	Disabled	Disabled

Figure 2-20 Update the scanning options of the Advanced Malware policy

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

Field name	Description
File Type	The file types to be scanned. The supported file types are: • Executables (.exe, .dll, .scr, .ocx, .sys, .com, .drv, .cpl) • MS Office Files (.doc, .docx, .xls, .xlsx. .ppt, .pptx) • PDF Files (.pdf, .xdp) • Compressed files (.zip, .rar) • Android application package (.apk) .apk files are not supported for SMTP traffic. • Java Archive (.jar) • Flash files (.flv) Flash files (.flv) are not supported for FTP traffic. 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) .
Maximum File Size (KB) Scanned	This 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 black and white 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 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 MB • M-series Sensors - 5 MB • Virtual IPS Sensors- 5 MB McAfee recommends that for any file type, you do not set a value more than 5 MB as the maximum file size as this might affect the Sensor's performance.

Field name	Description
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 Sensor software version 8.2 or above or NTBA. For **Advanced Threat Defense** to work, you must integrate the corresponding Sensors with McAfee Advanced Threat Defense. See the *Network Security Platform Integration Guide* for 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.
	This response may not work effectively with SPAN and tap deployments.
	• **Add to Blacklist**— If any of the engines report the submitted file to be malicious, then the Manager adds the file's MD5 hash to the blacklist 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 *high* as the criteria, then files of severity *high* and *very high* are added to the blacklist. Within the next 5 minutes, the Manager adds this file to the local blacklist of all the Sensors that it manages.
	• **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.
	  • If McAfee Advanced Threat Defense is integrated, then note that McAfee Advanced Threat Defense does not provide you access to the original sample files that it analyzed. Therefore, you must use the **Save File** option, if you need to archive the samples that a Sensor submits to McAfee Advanced Threat Defense. However, note that 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.

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	Blacklist and Whitelist	NSP Analysis	Gateway Anti-Malware	Advanced Threat Defense	McAfee Cloud
Executables	x	x		x	x	
MS Office Files	x	x		x	x	
PDF Files	x	x	x	x	x	

File Type	TIE/GTI File Reputation	Blacklist and Whitelist	NSP Analysis	Gateway Anti-Malware	Advanced Threat Defense	McAfee Cloud
Compressed Files	x	x		x	x	
Android Application Package	x	x		x	x	x
Java Archive	x	x		x	x	
Flash Files	x	x	x	x	x	

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
NS9300, NS9200, NS9100	50	4,094
NS7300, NS7200, NS7100	50	4,094
NS5200, NS5100	32	1,024
NS3200, NS3100	16	255
IPS-VM600	32	1,024
IPS-VM100	16	255
M-8000, M-6050, M-4050, M-3050, M-8030, M-6030, M-4030	50	1,024
M-2950, M-2850, M-3030	32	1,024
M-1450, M-1250	16	255

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

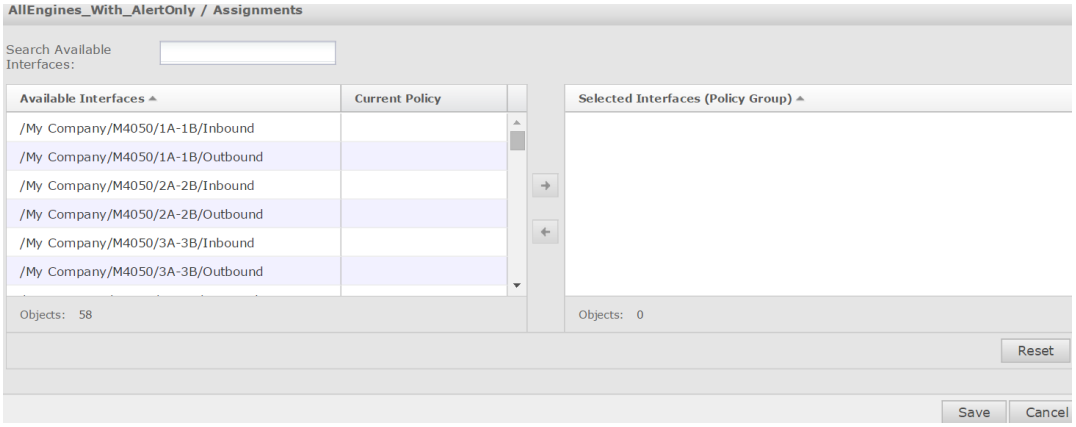


Figure 2-21 Assign Interfaces

7 Select the required interface from the **Available Interfaces** column and add it to the **Selected Interfaces** 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 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, detection mechanism.

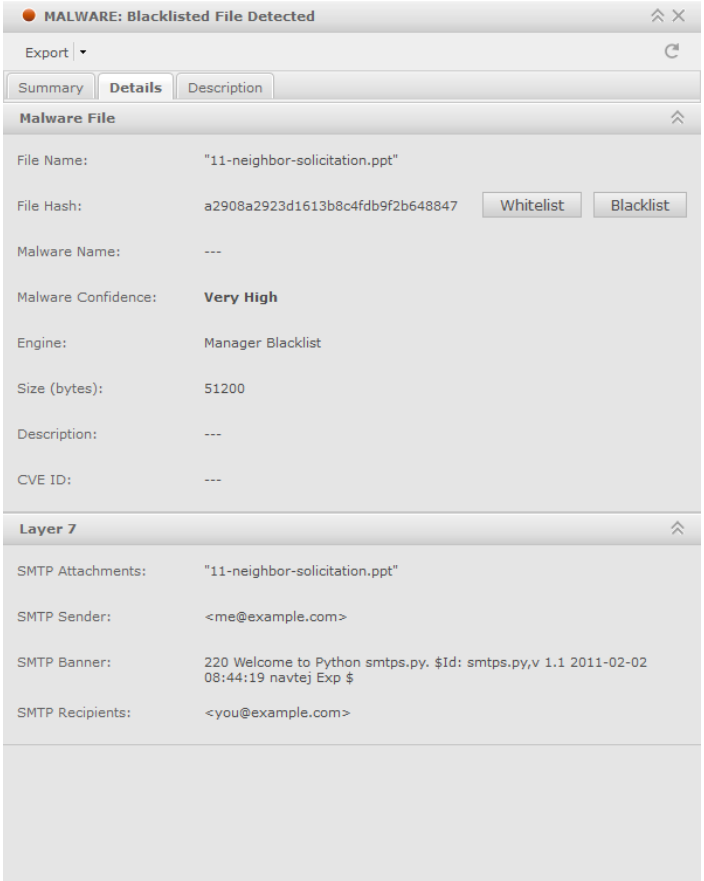


Figure 2-22 File Reputation details in Attack Log

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** | **<Admin Domain Name>** | **Devices** | **<Device Name>** | **Troubleshooting** | **Traffic Statistics**.

2 Click the **Advanced Malware Analysis** tab.

You can view the traffic statistics for malware statistics either **By Malware Engine** or **By File Type**.

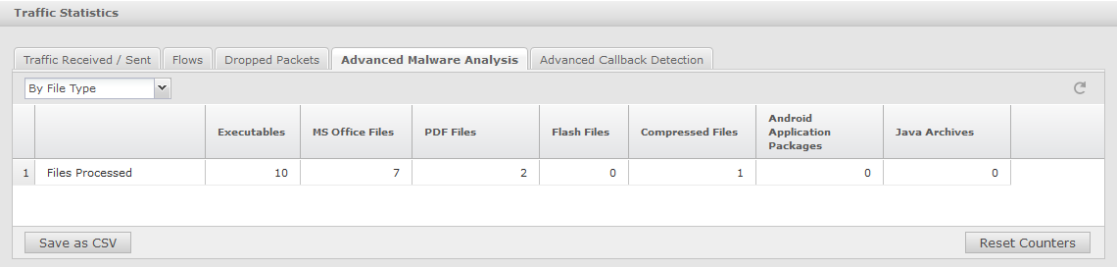


Figure 2-23 Malware traffic statistics

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

You can view the File Reputation detection and Custom fingerprints detection statistics also using the `show gti stats` CLI command. 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 *McAfee Network Security Platform CLI Guide*.

CLI commands for Network Security Platform - File Reputation integration

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

- `show gti config`: Displays the GTI server configuration information.
- `show gti stats ip`: Displays the statistics of the IP sent to the GTI server.

For more information on these commands see, *McAfee Network Security Platform CLI Guide*.

Network Security Platform-File Reputation integration is supported on M-series, NS-series, and VM 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

Nameserver connectivity errors

The DNS server might sometimes give continued delayed response to the Sensor. A delay for 10 minutes triggers a system event for Nameserver Connectivity errors.

In such scenarios, view the Nameserver statistics by using the `show gti config` command. If the parameter **Nameserver Connectivity issues** displays more error counts, you will have to set the time of File Reputation timeout by using the `set gtifilelookup timeout` command. This would mean that if the query is not resolved in the time configured, it is assumed to be clean.

Clearing File Reputation counters

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

For more information on CLI commands, see *McAfee Network Security Platform CLI Guide*.

System event for DNS error

If there is an incorrect File Reputation DNS configuration, the File Reputation DNS Error is displayed.

Disable HTTP Response Scanning to improve performance of File Reputation

In versions earlier than Network Security Platform 7.1, for File Reputation to work, you must enable HTTP Response Scanning in the corresponding port or port-pair. In Network Security Platform 7.1 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.

3 Integration with McAfee Cloud

Zero day threats that appear in the network which may ultimately morph into APTs and ransomware are an ever growing threat to enterprises today. With the growth in the number of mobile devices and an extension of the enterprise beyond the network perimeter, files that reside on individual devices pose a serious threat to your critical business infrastructure.

To counter such threats Network Security Platform is able to forward certain types of files to advanced malware scanning engines in the cloud. This engine, known in the Manager as McAfee Cloud engine, is a consolidation of two separate malware scanning engines:

- Mobile Cloud engine - A cloud-based engine that performs dynamic analysis on APK files only.
- McAfee Cloud Threat Detection (henceforth, referred to as McAfee CTD) engine - A cloud-based engine that performs static and dynamic analysis on executables and PDF files.

Contents

- *About McAfee Mobile Cloud Engine for Mobile APK Files*
- *About McAfee Cloud Threat Detection*

About McAfee Mobile Cloud Engine for Mobile APK Files

McAfee Mobile Cloud engine performs dynamic analysis on Android Application Package (APK) files. If any malicious content is found, the Sensor sends an alert to the Manager. The Sensor computes the APK file's SHA-256 hash and makes the initial request to McAfee Cloud. If the file is known and clean, the Sensor allows the file to enter the network. For known malicious APKs, the Sensor raises a malware detected alert. After the alert is raised, the Manager issues a separate query to McAfee Cloud to look up detailed information about the APK, such as reputation or privacy score, advertisement libraries on the APK, and information exposed by the APK.

If the file is unknown, the Sensor sends the APK file to the Manager and raises a file-submitted alert. The Manager uploads the file to McAfee Cloud. After the McAfee Cloud scans the file and returns a result to the Manager, the Manager updates the file-submitted alert with a malware reputation.

About McAfee Cloud Threat Detection

McAfee CTD is a service that plugs into existing McAfee security solutions to detect advanced malware that appears through several attack vectors. McAfee CTD provides you the ability to send files for static and dynamic analysis. Static analysis extracts file characteristics through heuristics based engines while dynamic analysis executes the file in a controlled environment and analyses behavior.

Configure McAfee Cloud Threat Detection

To be able to send suspicious executable and PDF files to a cloud sandboxing engine, you are required to integrate Network Security Platform with McAfee CTD.

> The scanning of executable and PDF files is also possible when connecting to McAfee CTD through a proxy server. For more information on how to specify a proxy server, see the *Specify a proxy server for Internet connectivity* section in the *McAfee Network Security Platform Manager Administration Guide*.

To integrate Network Security Platform with McAfee CTD follow these steps:

Task

1 Select **Manager** | **<Admin Domain Name>** | **Integration** | **CTD**.

The **CTD** page is displayed.

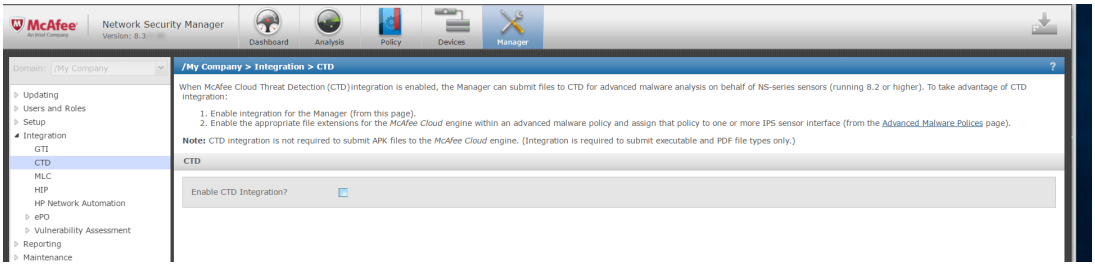


Figure 3-1 Cloud Threat Detection

2 Select the **Enable CTD Integration?** checkbox.

The **Activation Key** section along with the following is displayed:

- **Provisioning Key**
- **Activation Key Status**

A **Provisioning Key** is a unique identifier for the Network Security Platform which is used by McAfee ePO Cloud to generate an encrypted activation key. Keep the **Provisioning Key** handy by making a note of it since this will be required to generate an **Activation Key**.

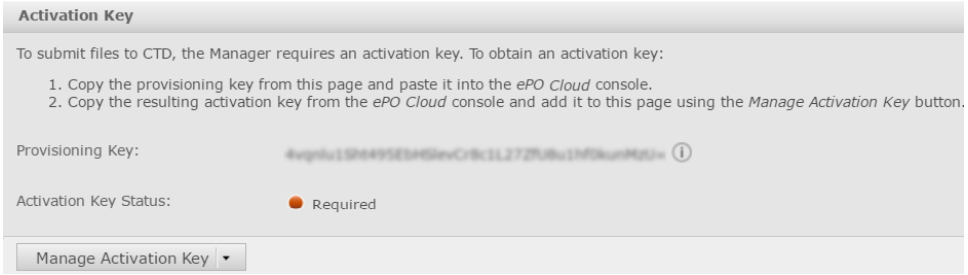


Figure 3-2 Activation Key required

3 From the **Manage Activation Key** drop-down list, select **Open ePO Cloud Console**.

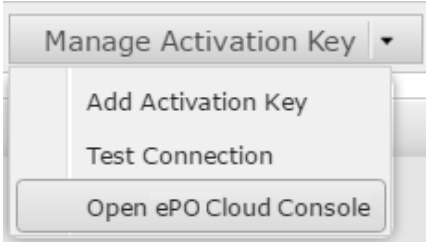


Figure 3-3 Open ePO Cloud Console

The McAfee ePO Cloud login page appears in a new browser. McAfee ePO Cloud 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.

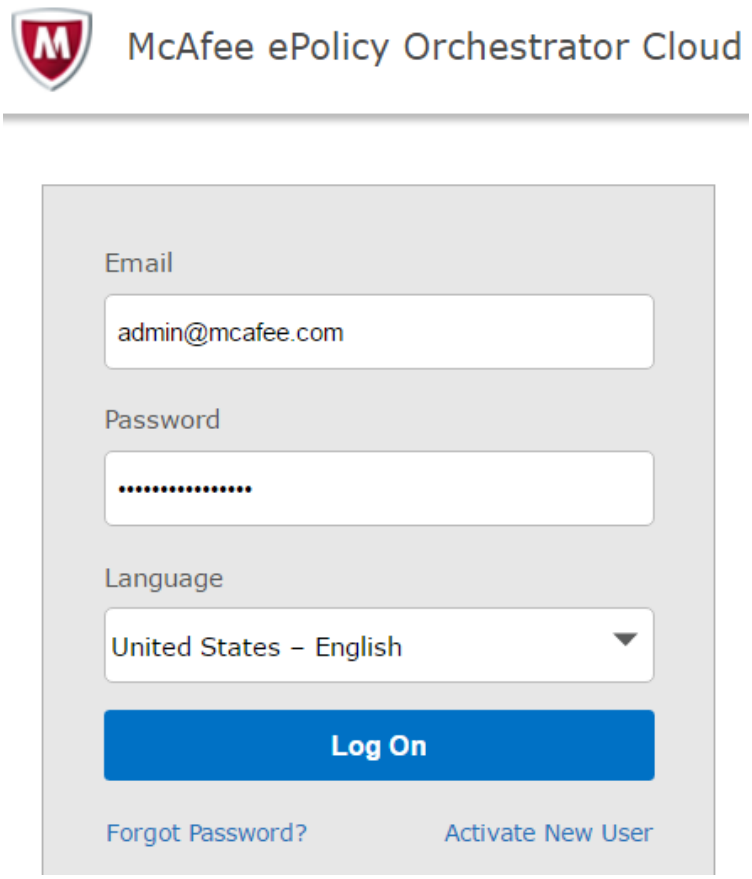


Figure 3-4 McAfee ePO Cloud Log On page

4 Enter the **Email** to be used while connecting to the McAfee ePO Cloud server.

5 Enter the **Password** for connecting to the McAfee ePO Cloud server and select **Log on**.

6 On the McAfee ePO Cloud console page, select **Server Settings** | **Cloud Threat Detection Setup**.

7 Copy and paste the **Provisioning Key** that you made note of from the Network Security Platform and select **Generate Activation Key**.

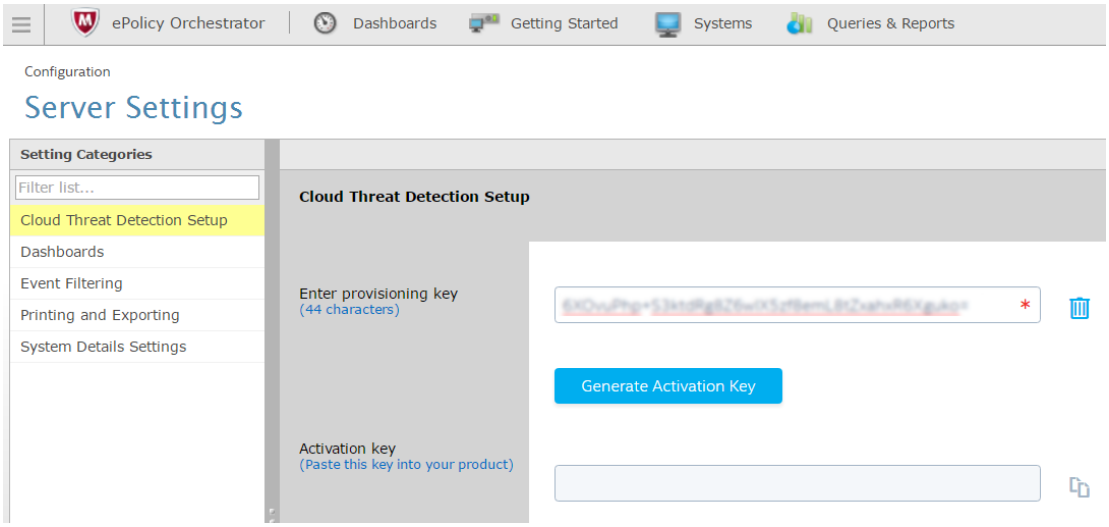


Figure 3-5 Cloud Threat Detection Setup page

An **Activation Key** is generated. An **Activation Key** is a unique identifier used by the Network Security Platform to submit files to McAfee Cloud.

8 Copy the **Activation Key** from the McAfee ePO Cloud server.

9 Return to Network Security Platform and on the **CTD** page, click **Add Activation Key** from the **Manage Activation Key** drop-down list.

10 Enter the **Activation Key** in the **New Activation Key** box and select **Add**.

11 Once the activation key is added, the **Activation Key Status** changes to **Present** indicating that the integration between the Network Security Platform and McAfee CTD is complete.

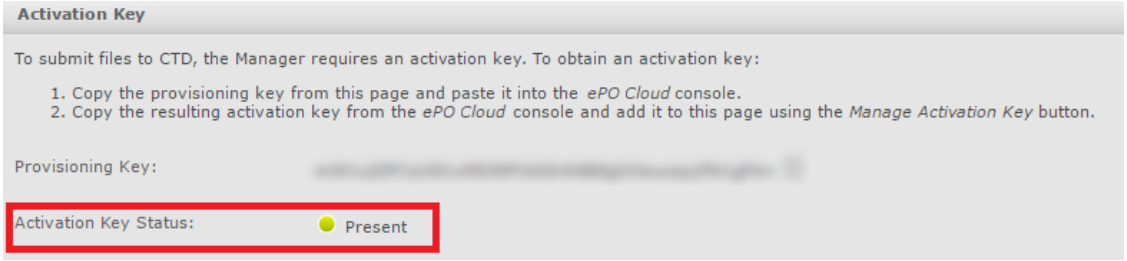


Figure 3-6 CTD Integration is complete

12 Once the **Activation Key Status** changes to **Present**, select **Save**.

Once the integration is complete, you can choose to send executable and PDF files to McAfee CTD.

Configure advanced malware policies to send files to McAfee CTD

To configure advanced malware policies to send files to McAfee CTD, perform the following steps:

Task

1 Go to **Policy** | **<Admin Domain Name>** | **Intrusion Prevention** | **Policy Types** | **Advanced Malware Policies** page.

2 Verify and enable the **TIE / GTI File Reputation** for executables and PDF files in the **Advanced Malware Policy** page before enabling McAfee Cloud option for both these file types.

You will get a confirmation message asking if you want to enable **TIE / GTI File Reputation** for executables and PDF files.

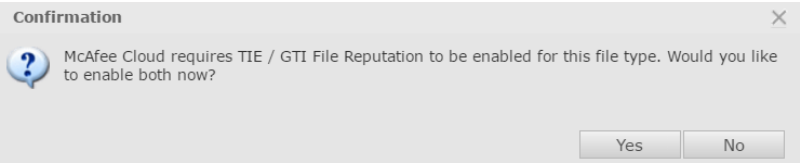


Figure 3-7 Enable TIE / GTI File Reputation

3 Click **Yes** to continue.

4 From the **McAfee Cloud** malware engine, select the **Executables** and **PDF Files** check-box.

When you enable submission of both these file types to McAfee Cloud, the **Scanning Options** area will appear to be as shown in the below figure:

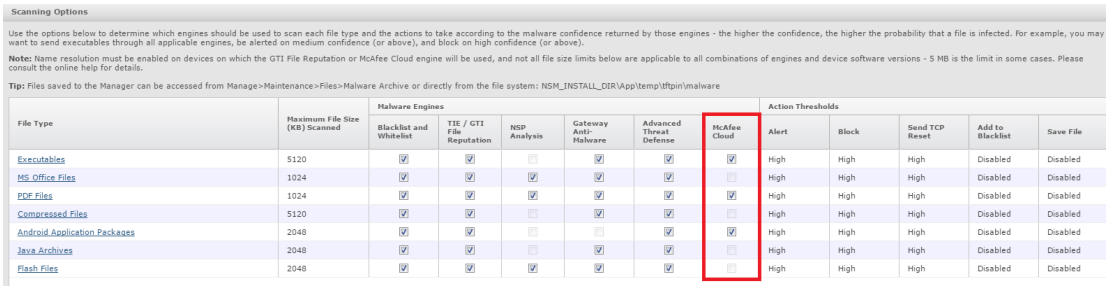


Figure 3-8 Scanning Options

How to view malware statistics

The **Statistics** page provides a count of malware identified in the suspicious files that were submitted to McAfee Cloud for scanning.

- To view malware statistics, go to **Manager** | **<Admin domain>** | **Integration** | **CTD** | **Statistics.**

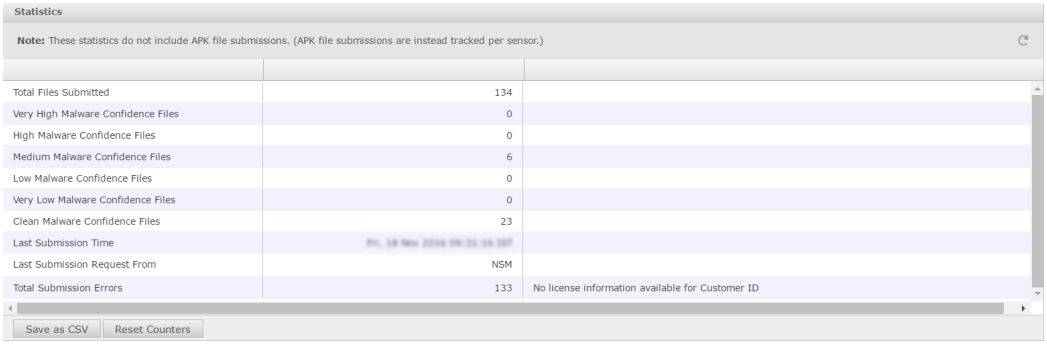


Figure 3-9 Statistics page

Option	Definition
Total Files Submitted	Total number of files submitted to McAfee Cloud since you last reset the counters.
Very High Malware Confidence Files	Files that contained any one of these file reputation values which were stored on McAfee Cloud and were not submitted afresh for analysis.
High Malware Confidence Files	
Medium Malware Confidence Files	
Low Malware Confidence Files	
Very Low Malware Confidence Files	
Clean Malware Confidence Files	
Last Submission Time	The last time when a file was submitted to the McAfee Cloud.
Last Submission Request From	The point product from which the last file was submitted.
Total Submission Errors	The total number of files submitted to McAfee Cloud that contained some error. • The last submission error is displayed in the third grid column as and when there is an error.
Save as CSV	Exports information as a .csv file which you can use for further analysis.
Reset Counters	Resets all the data counters to zero.
Save	Make sure to save your changes after you have reset the counters.
	You can refresh the data displayed by clicking this icon.

Analysis of Malware Files

Consider a scenario in which a suspicious file attempts to enter the network and intercepted by the Sensor. The following sequence illustrates how Network Security Platform works in conjunction with McAfee Cloud to scan the suspicious file.

This illustration is only one way of viewing the results of malware analysis. To learn about alternate ways, see the *McAfee Network Security Platform Manager Administration Guide*.

- When a suspicious file attempts to enter the network, the Sensor computes a file hash, if advanced malware scanning is enabled, consults various malware engines for scanning.
- If the results from the malware engines are *unknown*, *low*, or *very low*, the Sensor flags this file and forwards it to the Manager.
- The Manager sends the file to McAfee Cloud for further scanning and polls for results every 5 minutes.

  The Manager raises a *MALWARE: Unknown File Download Detected and Submitted to McAfee Cloud Service for Analysis* alert in the **Attack Log** which indicates that a suspicious file has been submitted.

  If file reputation returned by McAfee Cloud is clean, the alert is cleared from the **Attack Log**. If the file reputation is shown as **Pending** in the **Attack Log** for over 3 hours, the alert is cleared.

  If you have enabled the **Save File** option in the **Advanced Malware Policies** page, the file for which the alert is cleared from the **Attack Log** is saved in the **Manage** | **Maintenance** | **Files** | **Malware Archive** folder. You can resend this file for scanning.

- If McAfee Cloud returns a file reputation of *medium*, *high*, or *very high*, the Manager raises a *MALWARE: Malicious File Detected by McAfee Cloud Service* alert in the **Attack Log**. In this case, the submission alert is replaced with the malicious file detection attack ID. If the file is returned as unknown or clean, the submission alert is deleted.
- If the file submission to McAfee CTD exceeds its daily limit or when the rate of file submission is too high, system faults are generated. The daily file submission limit and the rate of submission is based on the type of licenses that you purchased at the time of your contract with McAfee. The system faults can be viewed in the Network Security Manager user interface. To view licensing related system faults, go to **Manager** | **<Admin Domain>** | **Troubleshooting** | **System Faults**. For more information, see View System Faults for Licensing on page 85.
- Double-click the alert for which you want to view the alert details.

  The **Alert Details** panel opens.
- You can view the user details in the **Attacker** / **Target** section.

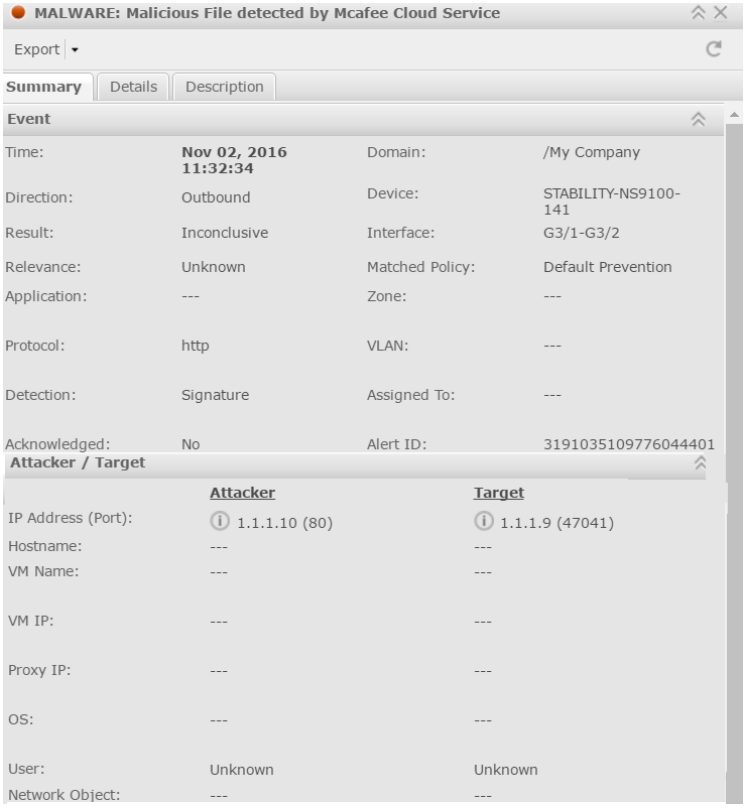


Figure 3-10 User details in Attack Log

- You can view the malware confidence in the **Malware Files** page.

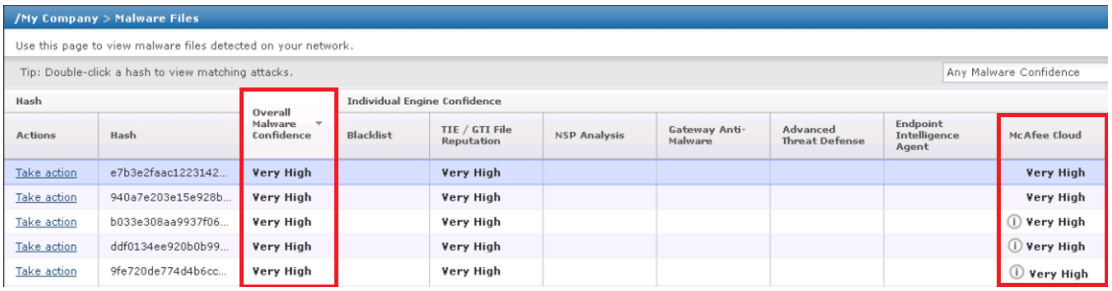


Figure 3-11 Malware Files page in the Manager

- View the McAfee CTD specific details for a detected malware.

  In the **Malware Files** page, click ⓘ next to the confidence level for **McAfee Cloud**. A report generated by McAfee Cloud opens in a window.

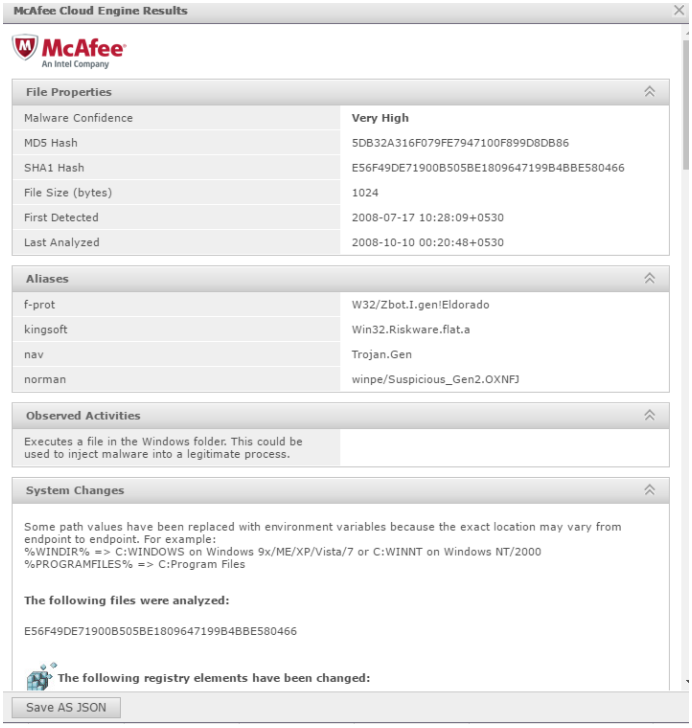


Figure 3-12 Details returned by McAfee Cloud

Table 3-1 Field descriptions

Field	Description
File Properties	Displays the highest malware severity returned by the components of McAfee Cloud, MD5 hash value of the file, file size, files that were detected first and last.
Aliases	
Observed Activities	Activities performed by the malware.
System Changes	

- View malware statistics.

  To view malware statistics, go to **Manager** | **<Admin domain>** | **Integration** | **CTD** | **Statistics**.

The **Statistics** page provides an insight on the PDF and executable files submitted by the Manager to McAfee Cloud.

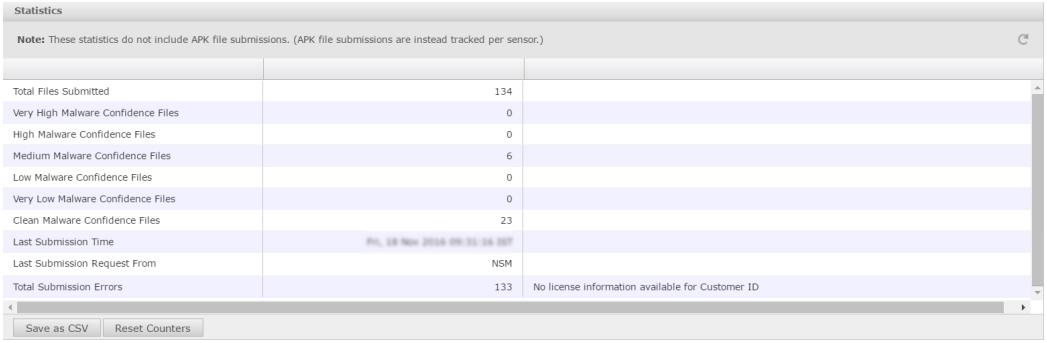


Figure 3-13 Statistics page

View System Faults for Licensing

You are provided with licenses depending on your contract with McAfee. The type of licenses you purchase decides the number of files you can submit on a daily basis. When the number of files submitted exceeds the daily limit or when the rate of file submission is too high, system faults are generated. These system faults can be viewed in the Network Security Manager user interface.

To view these system faults, go to **Manager** | **<Admin Domain>** | **Troubleshooting** | **System Faults**. When you click on the fault link, you can view the details of the fault and the possible actions to be taken to correct the fault. For more information on the system faults, refer to the *McAfee Network Security Platform Troubleshooting Guide*.

- **Invalid CTD subscription** — This type of fault is generated when the attempts to submit files to McAfee CTD are rejected because the activation key used for McAfee CTD integration is not associated with a valid customer subscription.

  Workaround — Correct the subscription in the ePO Cloud console and import a new activation key into the Manager.

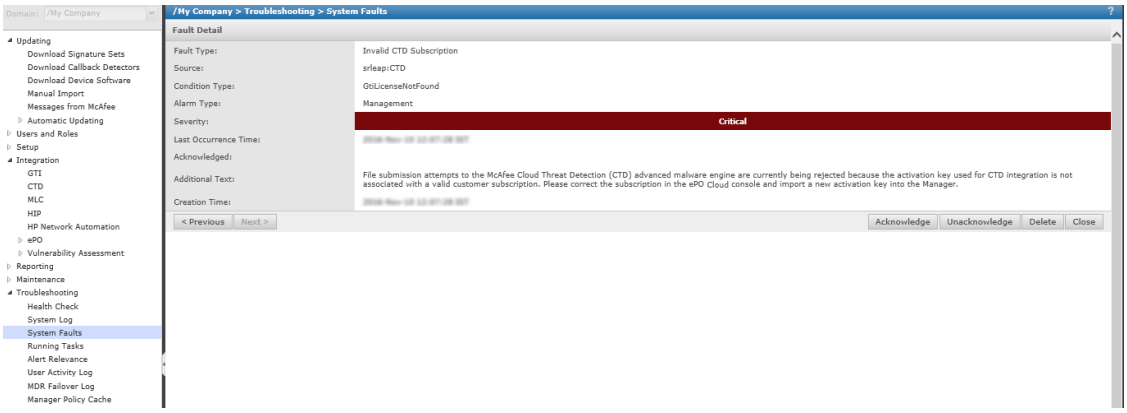


Figure 3-14 Error due to an invalid activation key

- **Expired CTD subscription** — This type of fault is generated when the attempts to submit files to McAfee CTD are rejected because the activation key used for McAfee CTD integration is associated with an expired subscription.

  Workaround — Correct the subscription in the ePO Cloud console and import a new activation key into the Manager.

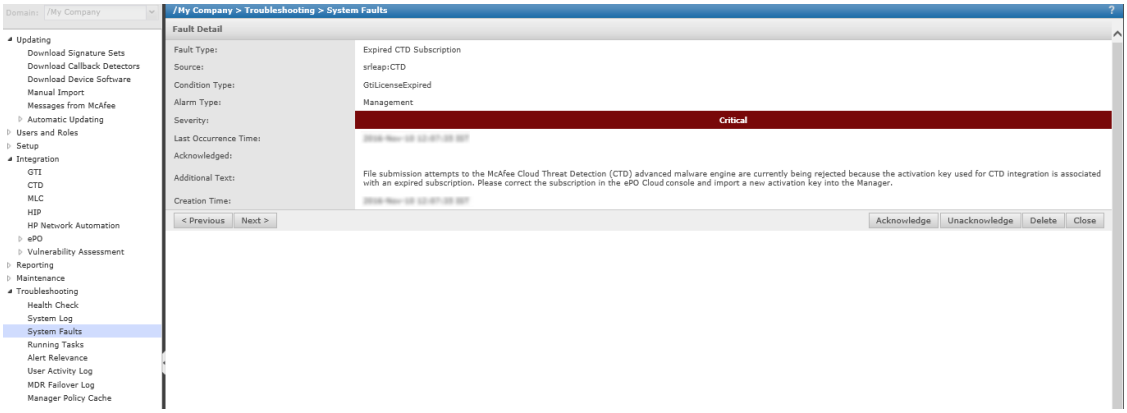


Figure 3-15 Error due to an expired activation key

- **CTD file submission limit reached** — This type of fault is generated when the daily limit for file submissions to McAfee CTD is reached.

  Workaround — You may need to purchase an additional license.

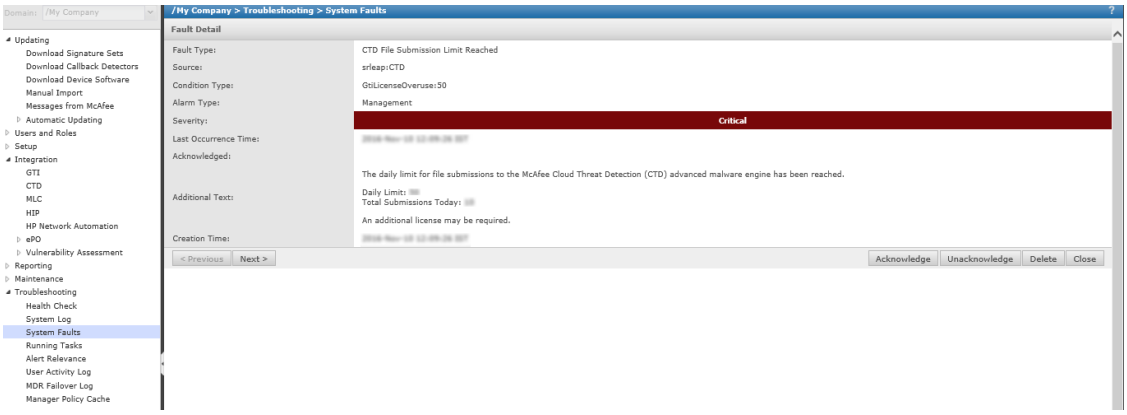


Figure 3-16 Error due to file submission reaching its daily limit

- **CTD file submission rate too high** — This type of fault is generated when the attempts to submit files to McAfee CTD are rejected because the file submission rate is too high.

  Workaround — You may need to purchase an additional license.

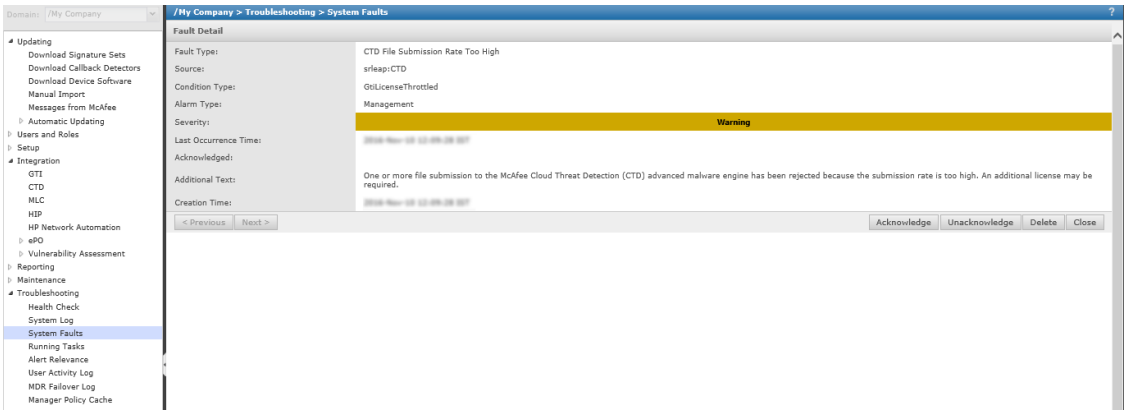


Figure 3-17 Error due to high rate of file submission

4 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 pre-installed 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 detects the file to be a malware immediately, 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.

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.

Contents

- *Advantages*
- *Terminologies*
- *How Network Security Platform - integration works*
- *Considerations*
- *High-level steps for integrating with McAfee Advanced Threat Defense*
- *Integrating Network Security Platform and McAfee Advanced Threat Defense*
- *Add an Advanced Malware policy*
- *Manage Advanced Malware policies*
- *Sensor CLI commands*
- *Analyze Malware Files*

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 anti-malware 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 blacklist 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 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.

  Static analysis sequence is following.

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

  - **Local Whitelist —** This is the list of MD5 hash values of trusted files, which need not be analyzed. This whitelist is based on the McAfee® Application Control database that is used by other solutions in the McAfee suite. This has over 230,000,000 entries.

    The whitelist feature is disabled by default. To enable or disable it, use the `setwhitelist` command. There are commands to manage the entries in the whitelist. The static McAfee® Application Control database cannot be modified. However, you can add or delete entries based on file hash. You can also query the whitelist for a certain file hash to see if it has been added to the database.

    The default whitelist entries are not periodically updated. However, they might be updated when you upgrade the Advanced Threat Defense software.

    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.

    DNS must be configured for GTI to run.

    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.

- **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.

  By default, Advanced Threat Defense downloads the updates for McAfee Gateway Anti-Malware Engine and McAfee Anti-Malware Engine every 90 minutes. Manual update of DAT is not allowed.

- **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.

- **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 by default. You can upgrade it to Android 4.3. See Upgrade the Android analyzer VM.

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

  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
  - Minimum and 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. Always, the analyzer profile selected for a file 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 —** A 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 - 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.

The TCP channel feature will work with McAfee Advanced Threat Defense 3.4.8 and higher.

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.

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, Advanced Threat Defense 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. Because 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.

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.

   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.

> The Advanced Threat Defense malware engine can be used with SPAN and tap ports as well. 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), then it extracts the file and checks it against its whitelist and then its blacklist.

> The Sensor's black and white lists are different from the black and white lists of McAfee Advanced Threat Defense.

5 Assume that the file's hash value is not listed in the Sensor's white or black 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 called, *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.

> 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 per 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**: **Blacklist and Whitelist** | **TIE/GTI File Reputation/McAfee Cloud (for apk files)** | **NSP Analysis** | **Advanced Threat Defense or NTBA (if Advanced Threat Defense is disabled)**
- **NS-series**: **Blacklist and Whitelist** | **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 severity level of *high.* You can now use the **Quarantine** feature to quarantine the host from the rest of the network until you are sure 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.

> Recall that 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 Blacklist** action threshold in the Advanced Malware policy, the Manager can include the MD5 hash of this file in the blacklist 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.

> 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 Blacklist** action threshold in the Advanced Malware policies.

What happens in case of MDR?

1 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.

2 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.

3 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?

1 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.

2 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.

3 If the Sensor goes down after the packet hold time interval but before the file session time interval, the updates 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 8.0 or later.
- You need McAfee Advanced Threat Defense 3.0 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 per 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.

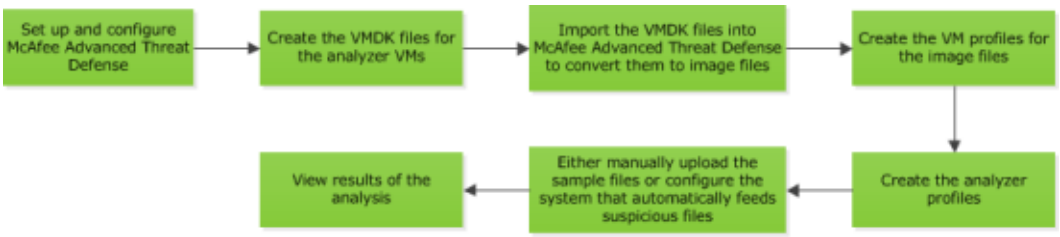


Figure 4-1 Summarized steps for configuring malware analysis

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 . Select this analyzer profile from the drop-down list under under the Maganer interface.The Manager also allows different Sensors to have their own analyzer profile as per 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, then 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 IPS Administration 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 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** | **ATD Integration**.

4 Enter the configuration details in the corresponding fields.

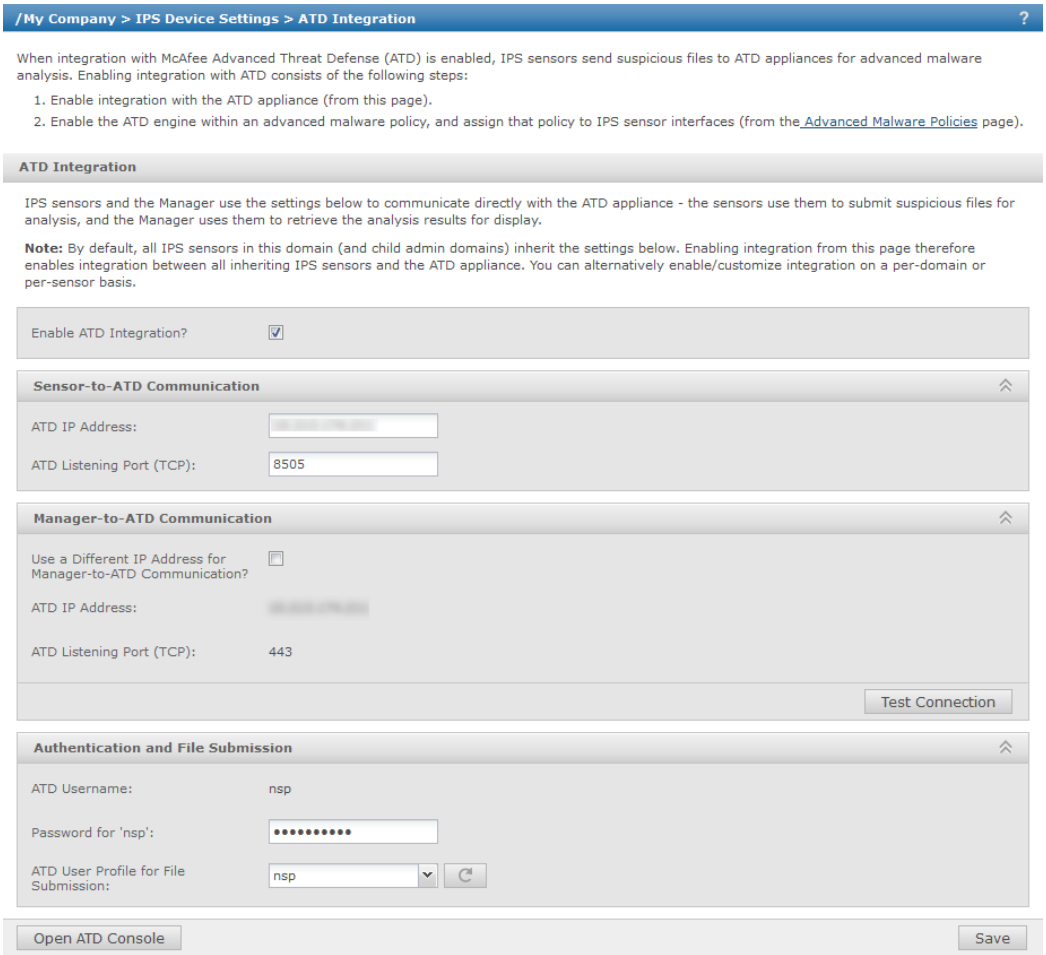


Figure 4-2 Enabling the integration for an admin domain

Table 4-1 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.
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.

Table 4-1 Option definitions *(continued)*

Option	Definition
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 *admin*. As a precaution, change this password in the **NSP User** user record in McAfee Advanced Threat Defense. 1 Click **Open ATD Console** to open McAfee Advanced Threat Defense web application. 2 In McAfee Advanced Threat Defense web application select **Manage** | **User Management.** 3 Select **NSP User** and click **Edit** to change the password. 4 Click **Save.**
ATD User Profile for File Submission	Select from the drop-down your user profile, created under McAfee Advanced Threat Defense. With the 8.2 release a Sensor can have its own analyzer profile as per 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.

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, then by default this integration is enabled for the corresponding Sensors. 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** | **ATD Integration.**

5 Enter the configuration details in the corresponding fields.

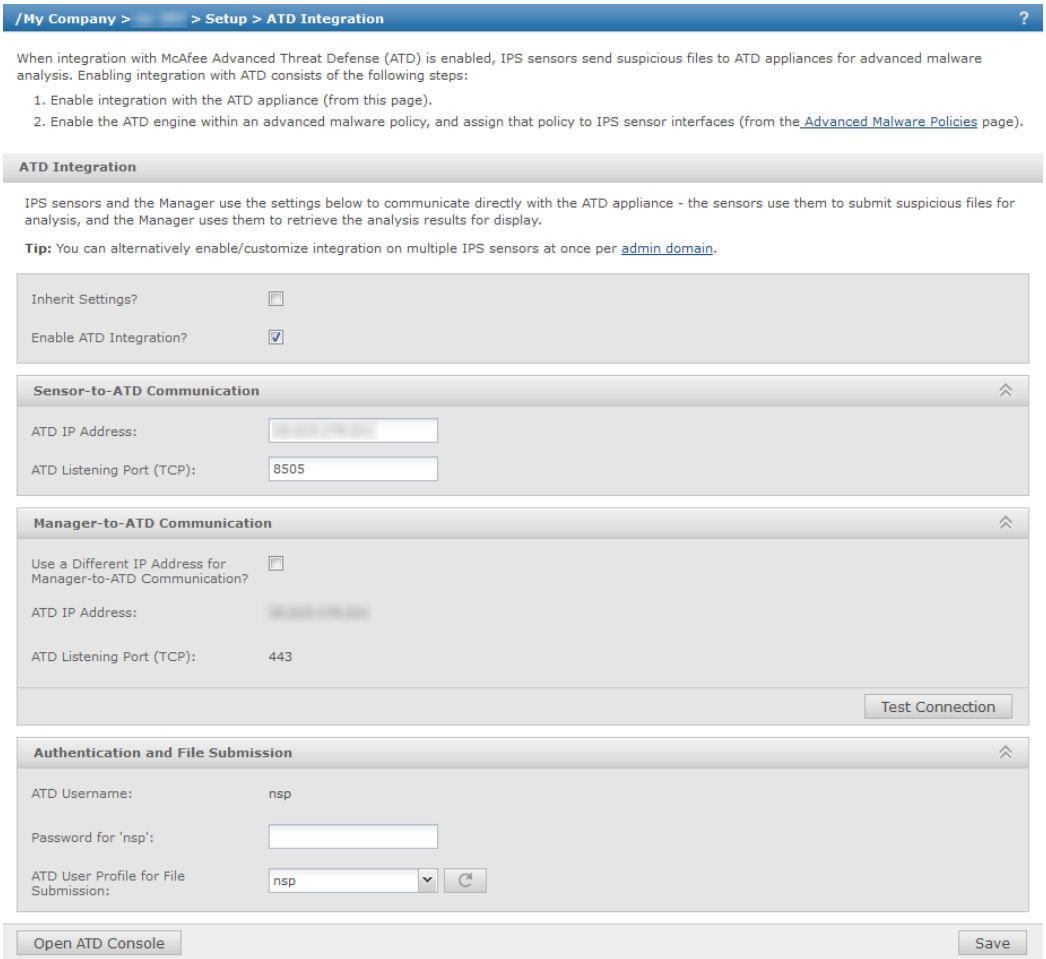


Figure 4-3 Enabling the integration for a Sensor

Table 4-2 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.

Table 4-2 Option definitions *(continued)*

Option	Definition
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 *admin*. As a precaution, change this password in the **NSP User** user record in McAfee Advanced Threat Defense. 1 Click **Open ATD Console** to open McAfee Advanced Threat Defense web application. 2 In McAfee Advanced Threat Defense web application select **Manage** | **User Management.** 3 Select **NSP User** and click **Edit** to change the password. 4 Click **Save.**
ATD User Profile for File Submission	Select from the drop-down your user profile, created under McAfee Advanced Threat Defense. With the 8.2 release a Sensor can have its own analyzer profile as per 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** | **Policy Types** | **Advanced Malware Policies.**

3 Click **New**.

The **New Policy** page opens.

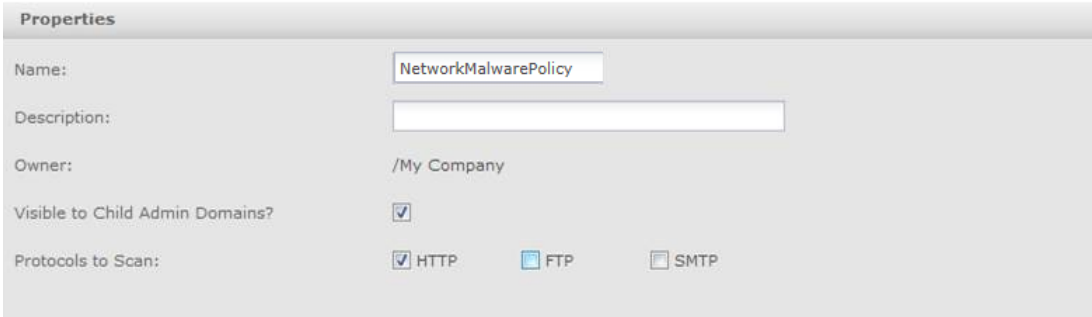
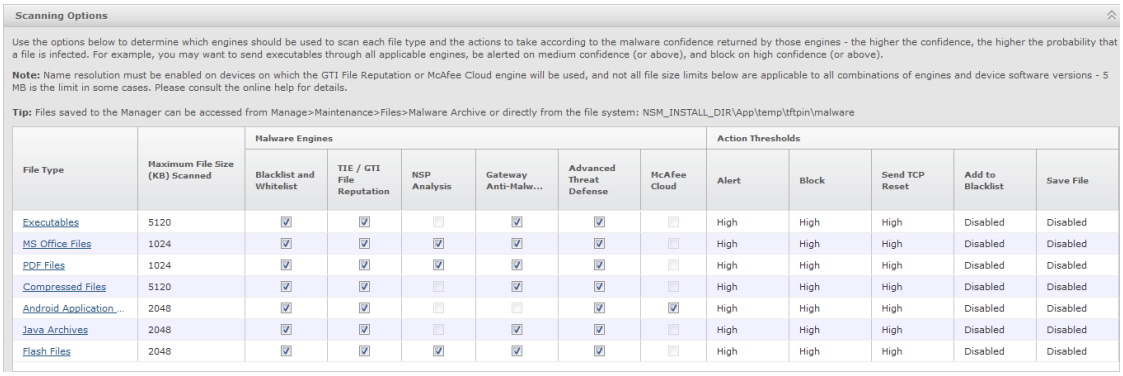


Figure 4-4 Update the properties of the Advanced Malware policy

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.
Protocols to Scan	Protocols over which advanced malware scanning is performed. The supported protocols are HTTP, FTP, and SMTP. Enable **HTTP Response scanning** to scan files in the HTTP data stream. FTP malware detection overrides the accelerate-ftp feature even if it is enabled. For more information on the `accelerate-ftp` CLI command, see *McAfee Network Security Platform CLI Guide.*

5 Update the **Scanning Options**.



Scanning Options

Use the options below to determine which engines should be used to scan each file type and the actions to take according to the malware confidence returned by those engines - the higher the confidence, the higher the probability that a file is infected. For example, you may want to send executables through all applicable engines, be alerted on medium confidence (or above), and block on high confidence (or above).

Note: Name resolution must be enabled on devices on which the GTI File Reputation or McAfee Cloud engine will be used, and not all file size limits below are applicable to all combinations of engines and device software versions - 5 MB is the limit in some cases. Please consult the online help for details.

Tip: Files saved to the Manager can be accessed from Manage>Maintenance>Files>Malware Archive or directly from the file system: NSM_INSTALL_DIR\App\temp\tftpin\malware

File Type	Maximum File Size (KB) Scanned	Malware Engines						Action Thresholds				
		Blacklist and Whitelist	TIE / GTI File Reputation	NSP Analysis	Gateway Anti-Malw...	Advanced Threat Defense	McAfee Cloud	Alert	Block	Send TCP Reset	Add to Blacklist	Save File
Executables	5120	☑	☑	☐	☑	☑	☐	High	High	High	Disabled	Disabled
MS Office Files	1024	☑	☑	☑	☑	☑	☐	High	High	High	Disabled	Disabled
PDF Files	1024	☑	☑	☑	☑	☑	☐	High	High	High	Disabled	Disabled
Compressed Files	5120	☑	☑	☐	☑	☑	☐	High	High	High	Disabled	Disabled
Android Application ...	2048	☑	☑	☐	☐	☑	☑	High	High	High	Disabled	Disabled
Java Archives	2048	☑	☑	☐	☑	☑	☐	High	High	High	Disabled	Disabled
Flash Files	2048	☑	☑	☑	☑	☑	☐	High	High	High	Disabled	Disabled

Figure 4-5 Update the scanning options of the Advanced Malware policy

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

Field name	Description
File Type	The file types to be scanned. The supported file types are: • Executables (.exe, .dll, .scr, .ocx, .sys, .com, .drv, .cpl) • MS Office Files (.doc, .docx, .xls, .xlsx. .ppt, .pptx) • PDF Files (.pdf, .xdp) • Compressed files (.zip, .rar) • Android application package (.apk) .apk files are not supported for SMTP traffic. • Java Archive (.jar) • Flash files (.flv) Flash files (.flv) are not supported for FTP traffic. 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) .
Maximum File Size (KB) Scanned	This 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 black and white 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 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 MB • M-series Sensors - 5 MB • Virtual IPS Sensors- 5 MB McAfee recommends that for any file type, you do not set a value more than 5 MB as the maximum file size as this might affect the Sensor's performance.

Field name	Description
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 Sensor software version 8.2 or above or NTBA. For **Advanced Threat Defense** to work, you must integrate the corresponding Sensors with McAfee Advanced Threat Defense. See the *Network Security Platform Integration Guide* for 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.
	This response may not work effectively with SPAN and tap deployments.
	• **Add to Blacklist**— If any of the engines report the submitted file to be malicious, then the Manager adds the file's MD5 hash to the blacklist 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 *high* as the criteria, then files of severity *high* and *very high* are added to the blacklist. Within the next 5 minutes, the Manager adds this file to the local blacklist of all the Sensors that it manages.
	• **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.
	  • If McAfee Advanced Threat Defense is integrated, then note that McAfee Advanced Threat Defense does not provide you access to the original sample files that it analyzed. Therefore, you must use the **Save File** option, if you need to archive the samples that a Sensor submits to McAfee Advanced Threat Defense. However, note that 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.

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	Blacklist and Whitelist	NSP Analysis	Gateway Anti-Malware	Advanced Threat Defense	McAfee Cloud
Executables	x	x		x	x	
MS Office Files	x	x		x	x	
PDF Files	x	x	x	x	x	

File Type	TIE/GTI File Reputation	Blacklist and Whitelist	NSP Analysis	Gateway Anti-Malware	Advanced Threat Defense	McAfee Cloud
Compressed Files	x	x		x	x	
Android Application Package	x	x		x	x	x
Java Archive	x	x		x	x	
Flash Files	x	x	x	x	x	

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
NS9300, NS9200, NS9100	50	4,094
NS7300, NS7200, NS7100	50	4,094
NS5200, NS5100	32	1,024
NS3200, NS3100	16	255
IPS-VM600	32	1,024
IPS-VM100	16	255
M-8000, M-6050, M-4050, M-3050, M-8030, M-6030, M-4030	50	1,024
M-2950, M-2850, M-3030	32	1,024
M-1450, M-1250	16	255

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

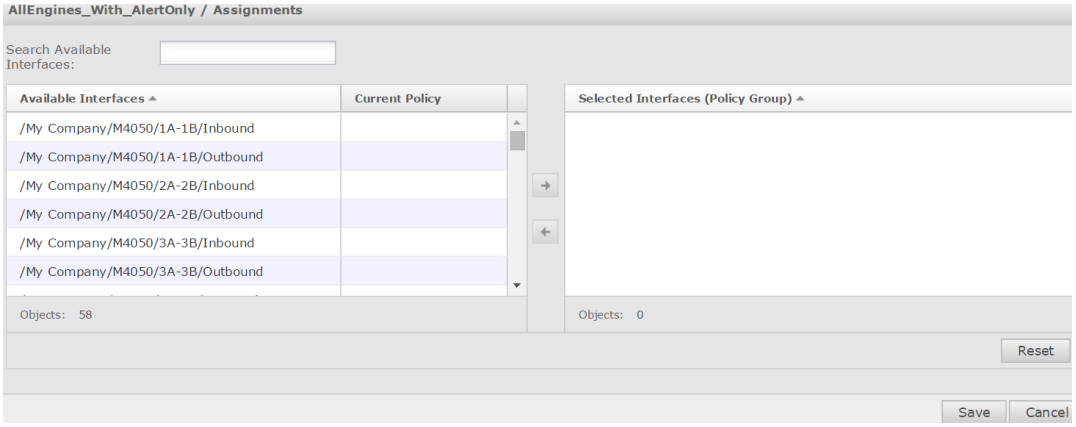


Figure 4-6 Assign Interfaces

7 Select the required interface from the **Available Interfaces** column and add it to the **Selected Interfaces** 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** | **<Admin Domain Name>** | **Policy Types** | **Advanced Malware Policies** 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. **1** Select **Policy** | **<Admin Domain Name>** | **Policy Types** | **Advanced Malware Policies**. The Advanced Malware policies are listed. **2** Select the policy to edit. **3** Click **Edit**. **4** Edit the policy parameters. **5** 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** | **<Admin Domain Name>** | **Policy Types** | **Advanced Malware Policies**. The policies are listed. **2** Select the policy you want to clone. **3** Click **Clone**. **4** Type a new name for the policy, if required and edit the policy parameters.
Delete an Advanced Malware policy	To delete an Advanced Malware policy you have created. **1** Select **Policy** | **<Admin Domain Name>** | **Policy Types** | **Advanced Malware Policies**. The Advanced Malware policies are listed. **2** Select the policy to be deleted. **3** Click **Delete**. **4** Click **Yes** to confirm the deletion. You cannot delete a currently applied policy.

Operation	Description
Export an Advanced Malware policy	You can export and save one or more Advanced Malware policy into a file. **1** Select **Policy** | **<Admin Domain Name>** | **Intrusion Prevention** | **Advanced** | **Policy Export** | **Advanced Malware Policies**. 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. The policy is saved in an XML format in the specified location.
Import 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 Policies**. 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 Communication]
Status                   : down
IP                       : 0.0.0.0
Port                     : 8505

[McAfee MATD Communication]
Status                   : up
IP                       : [redacted]
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 TCP channel feature works with McAfee Advanced Threat Defense 3.4.8 or later.

- 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 NULL cipher (no encryption) by default. Using NULL cipher is required to support the analysis of much larger files. If you want this connection to be encrypted, use the following CLI command on the Sensor: `set amchannelencryption <on><off>`. To know if the connection is currently encrypted, use `show amchannelencryption status` on the Sensor CLI.

  Enabling encryption can have a performance degradation, which may impact the analysis of large files and high-volume of files.

For the details on these commands refer to *McAfee Network Security Platform CLI 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 dashboards displays the **Malware File Hash** and the **Attack Count** of the detected malware. The **Dashboard** page security monitors are displayed as bar charts.

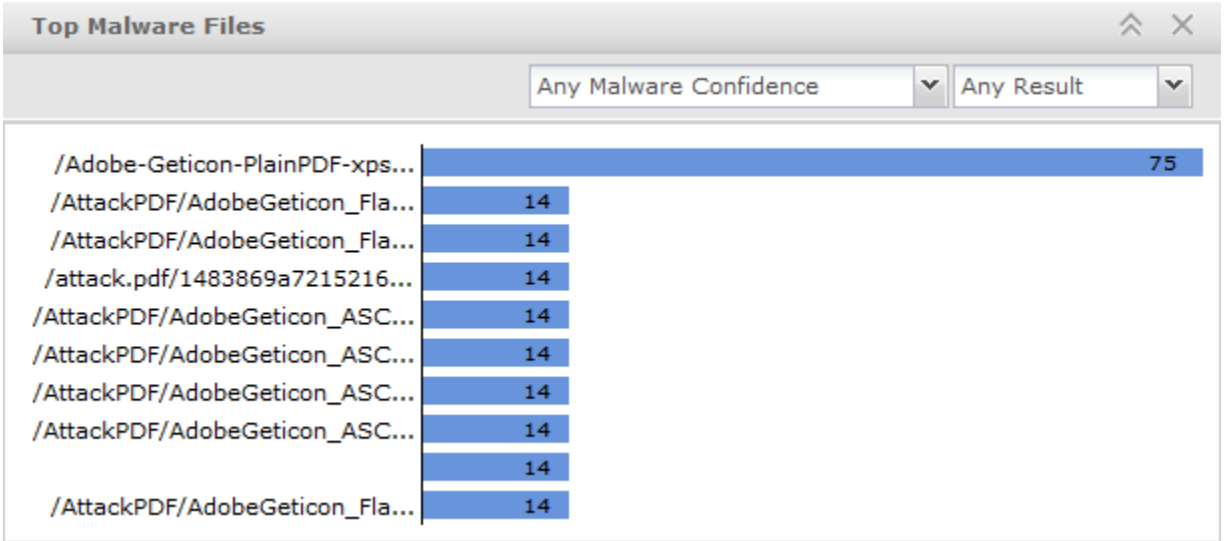


Figure 4-7 Top Malware Files

If you want to drill down further on a specific malware, click on a bar, and you will be redirected to the **Analysis** | **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.

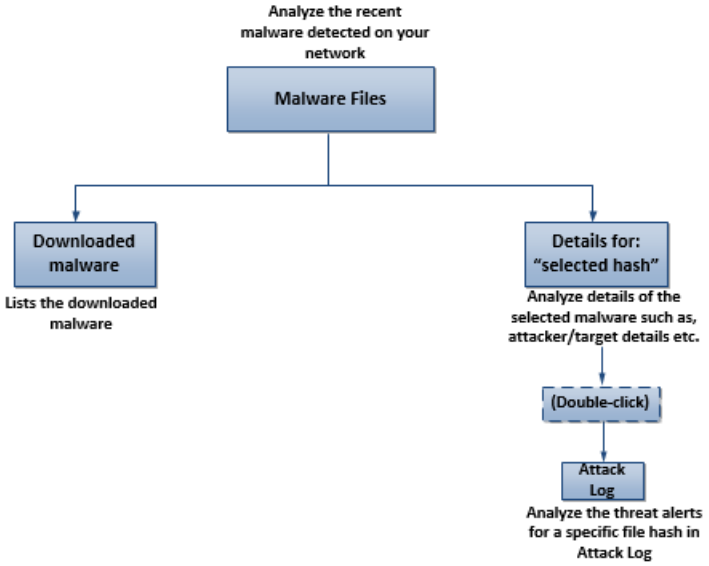


Figure 4-8 Malware analysis

The following filter options are provided.

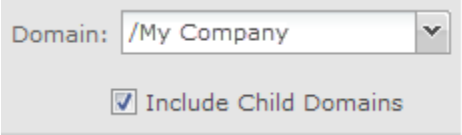


Figure 4-9 View data specific to admin domain

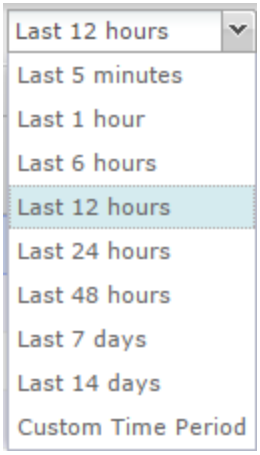


Figure 4-10 Analyze detected malware within a specific time

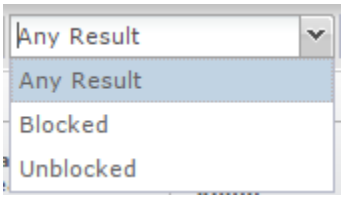


Figure 4-11 Analyze the type of malware, whether blocked, unblocked, or all

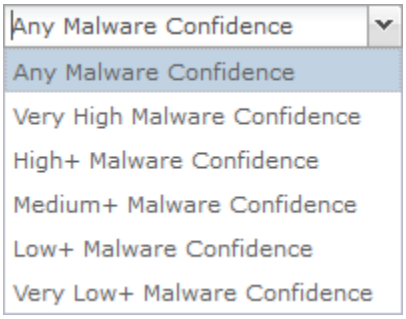


Figure 4-12 Analyze the malware based on malware confidence returned by engines

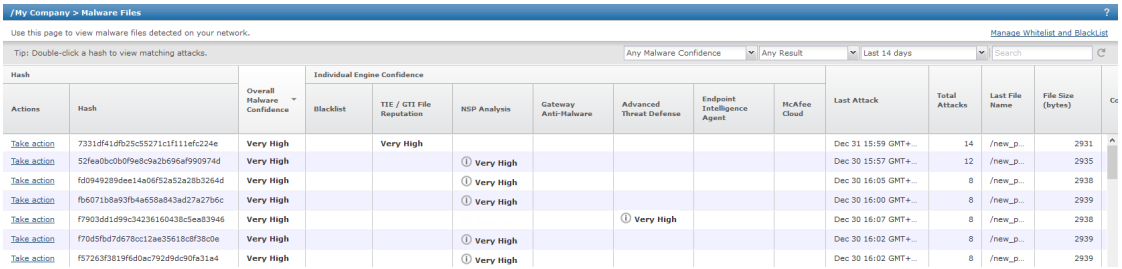


Figure 4-13 Details of the detected malware

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.
	  The antivirus program on your computer might prevent you from downloading the file.
	  • **Submit**— Click to submit the malware detection to the GTI Cloud.
	  • **White List**— Click to automatically add the file to the Manager's whitelist. In the next 5 minutes, the Manager sends the MD5 hash value to the whitelist of all the Sensors.
	  • **Black List**— Click to automatically add the file to the Manager's blacklist. In the next 5 minutes, the Manager sends the MD5 hash value to the blacklist of all the Sensors.
	• **Hash**— Displays the MD5 hash of the file.

Overall Malware Confidence	The overall malware confidence level returned by the configured malware scanning engines.
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-click on the malware file hash, the **Attack Log** opens where you can view and analyze alerts related to the selected hash.

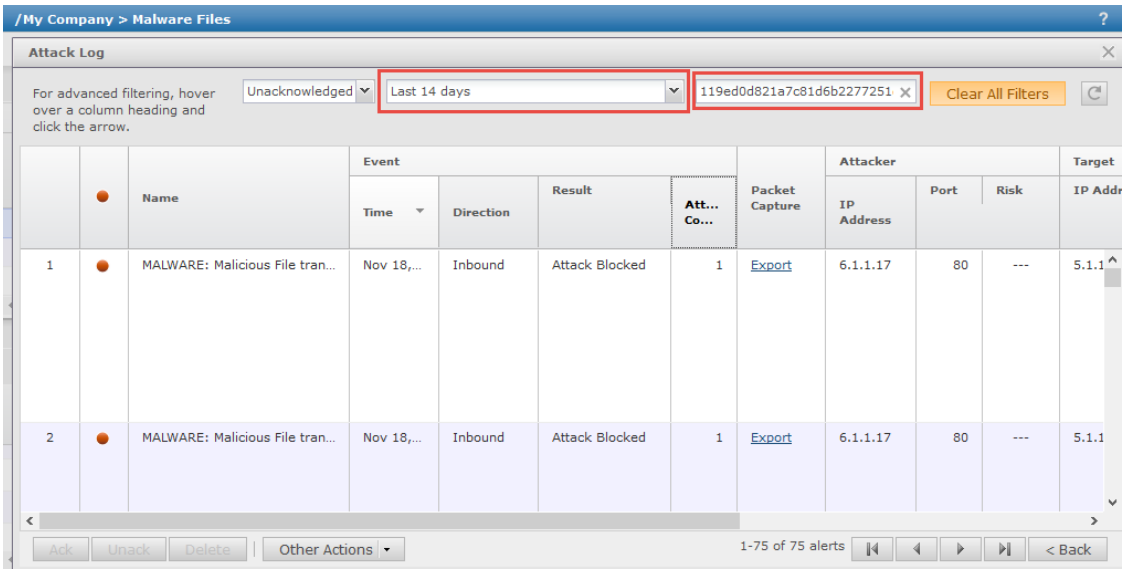


Figure 4-14 Attack log alerts for the hash selected

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

Manage Whitelist and Blacklist

The **Manage Whitelist and Blacklist** is a link to the **File Hash Exceptions** page. You can manage the whitelisted and blacklisted hash from this page. For more information on whitelisting/blacklisting file hash, see the *McAfee Network Security Platform IPS Administration 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**.

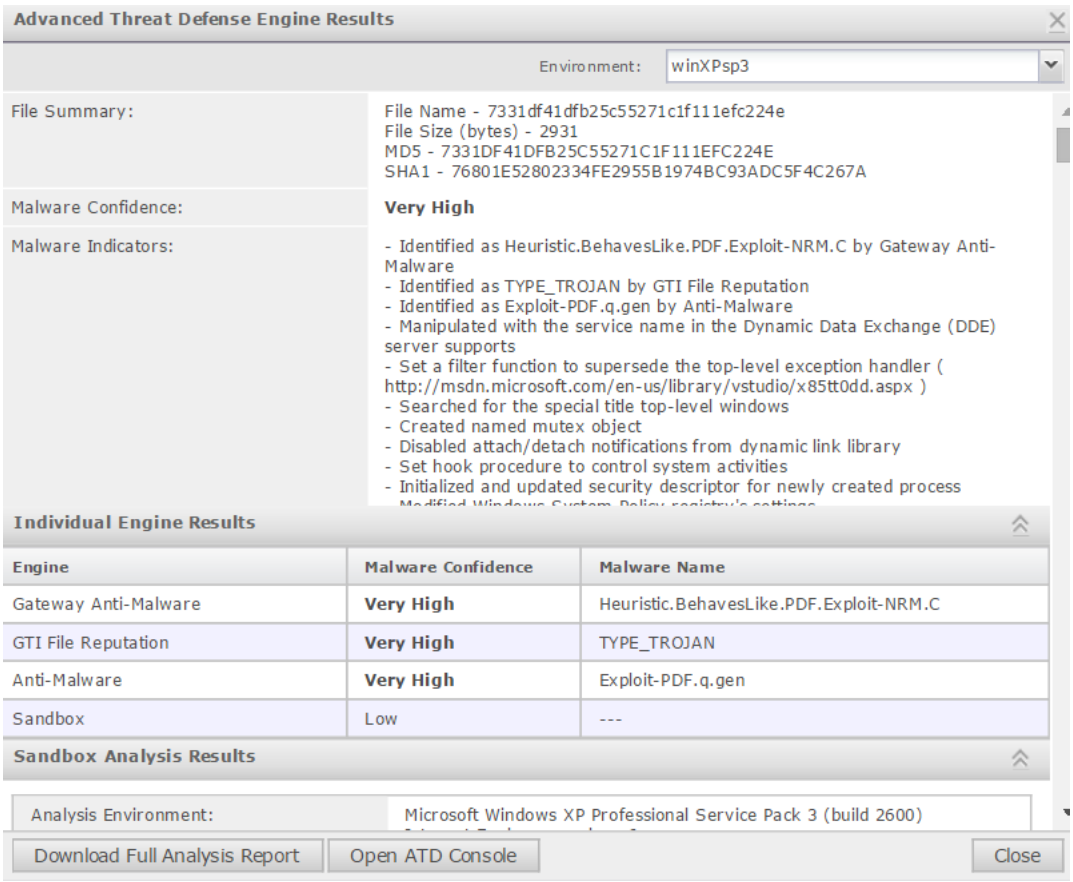


Figure 4-22 Details returned by McAfee Advanced Threat Defense

Table 4-3 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 returned by the components of McAfee Advanced Threat Defense.
Malware Indicators	The summary of the reports from the various analysis methods employed by McAfee Advanced Threat Defense.

Table 4-3 Field descriptions *(continued)*

Field	Description
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 is 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 this 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 dependant on the Advanced Malware policy configuration for the period of the report.

Task

1 In the Manager select **Analysis** | **Event Reporting** | **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.**

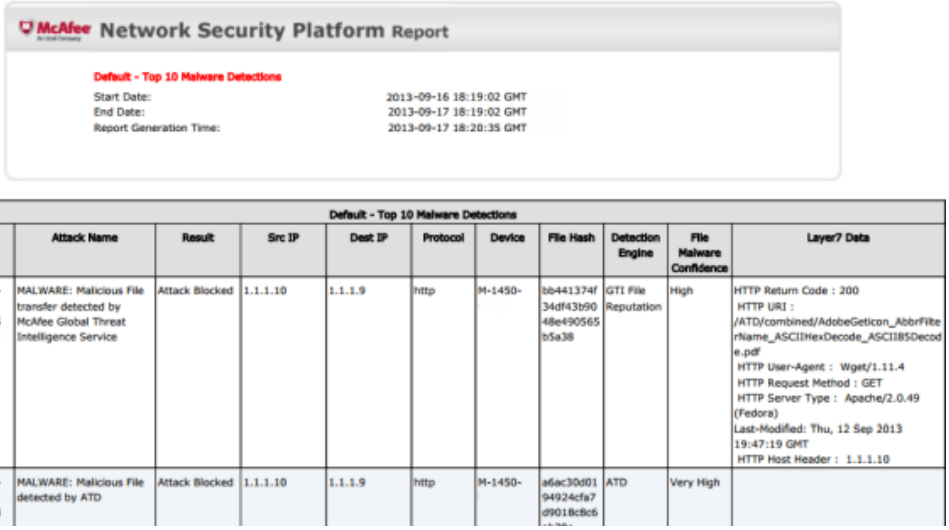


Figure 4-23 The default Top 10 Malware Detections report

The generated report is displayed.

Table 4-4 Column definitions

Column	Definition
Time	The time stamp when a malware engine determined the file to be malicious. In other words, this is the time when the
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.

Table 4-4 Column definitions *(continued)*

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.

The admin domain filter in the main **Analysis** page (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 *Network Security Platform Manager Administration 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 *Network Security Platform Manager Administration Guide.*

5 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 on 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.

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

Contents

- *Why integrate Network Security Platform with Threat Intelligence Exchange?*
- *How the integration works*
- *High-level steps to make the integration work*
- *Enable DXL integration for a domain*
- *Enable DXL integration for a device*
- *Viewing Threat Intelligence Exchange detection in the Manager*
- *Sensor CLI commands specific to Threat Intelligence Exchange*
- *Troubleshooting the integration between Network Security Platform and Threat Intelligence Exchange*

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 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 such as 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 8.2 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.

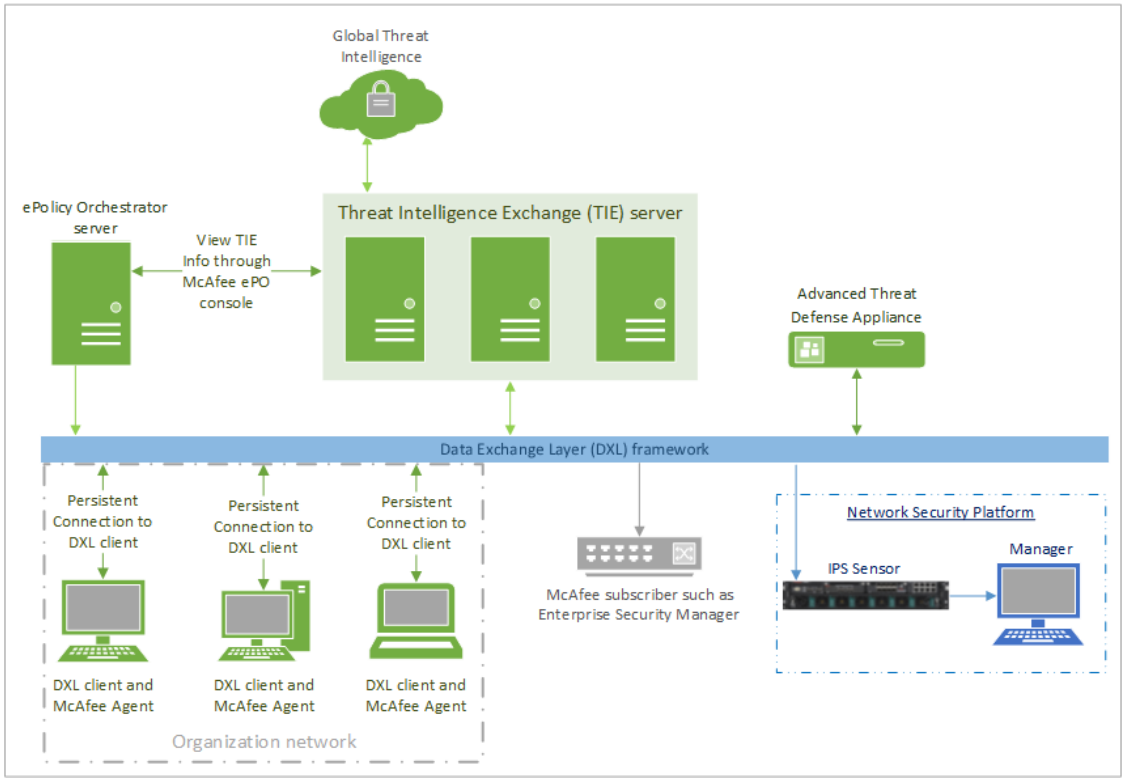


Figure 5-1 Threat Intelligence Exchange deployment scenario

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

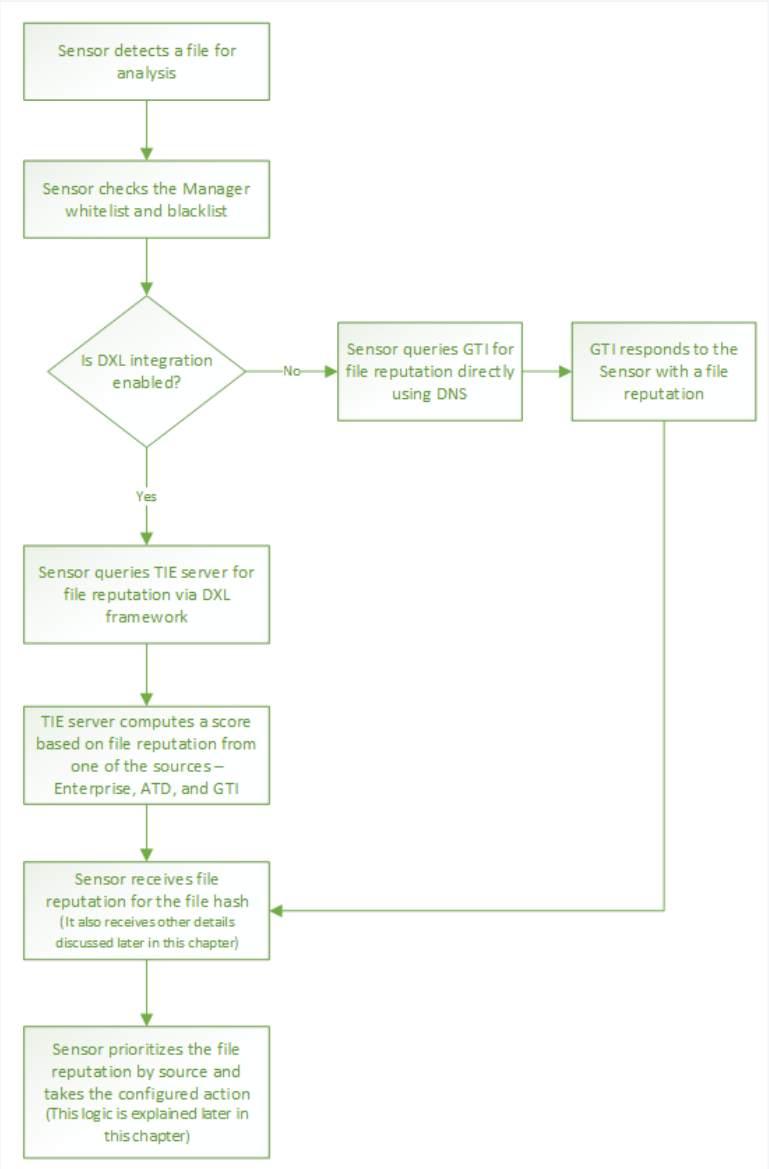


Figure 5-2 Threat Intelligence Exchange flow

- 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 whitelist, then the Manager blacklist.
- 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 DNS 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 confidence • Gateway Anti-Malware Engine • Anti-Malware Engine • Sandbox	Malware confidence for each of the individual engines.
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 the *McAfee Network Security Platform Manager Administration 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.

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** | **<Admin_Domain_Name>** | **Global** | **IPS Device Settings** | **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 top-right of the page.

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

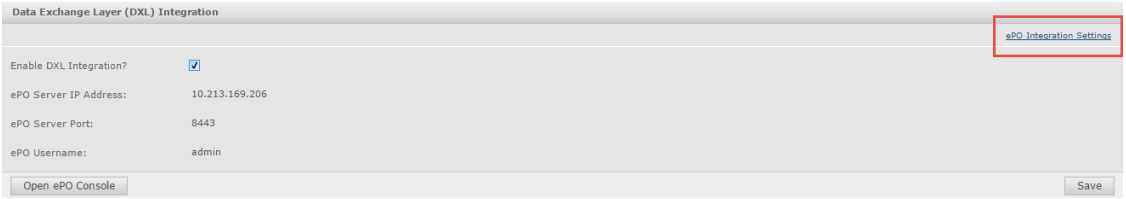


Figure 5-3 Data Exchange Layer integration page for a domain

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.

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

1 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.

4 Select the **Enable DXL Integration?** checkbox.

The McAfee ePO server configuration fields are displayed.

5 Enter the McAfee ePO server IPv4 address.

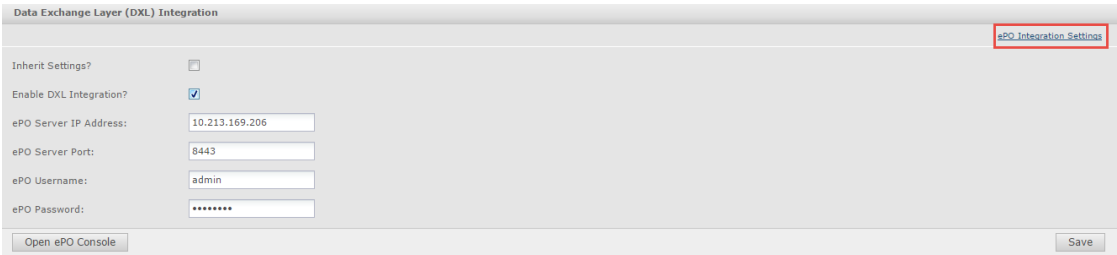


Figure 5-4 Data Exchange Layer integration for a device shows settings specific to it

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.

> 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.

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 Manager Administration Guide*.

- When a file appears on the network, the Sensor computes a file hash and checks the whitelist and blacklist 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.

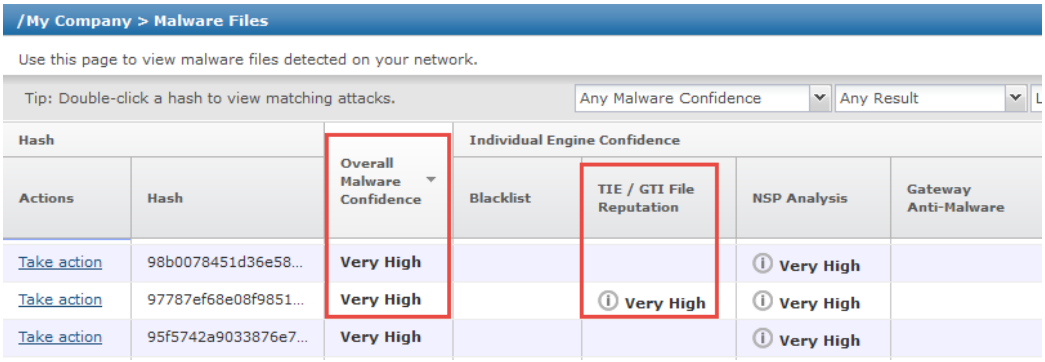


Figure 5-5 Malware Files page in the Manager

- Clicking the icon to view file reputation from each of the three sources.

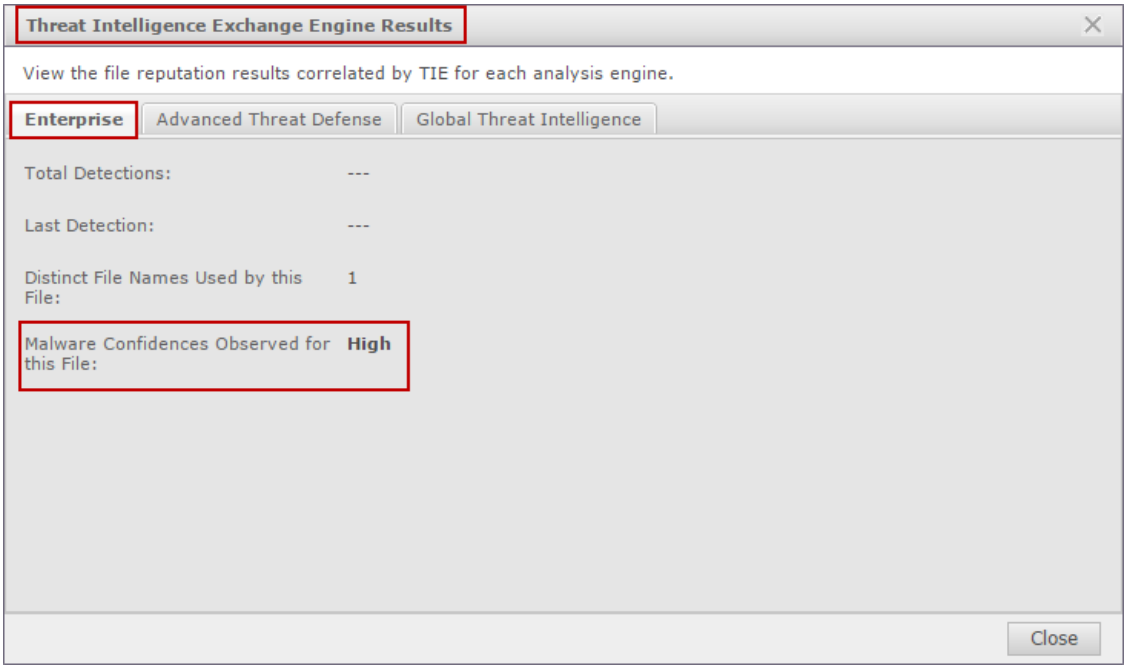


Figure 5-6 Threat Intelligence Exchange Engine results

- 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.

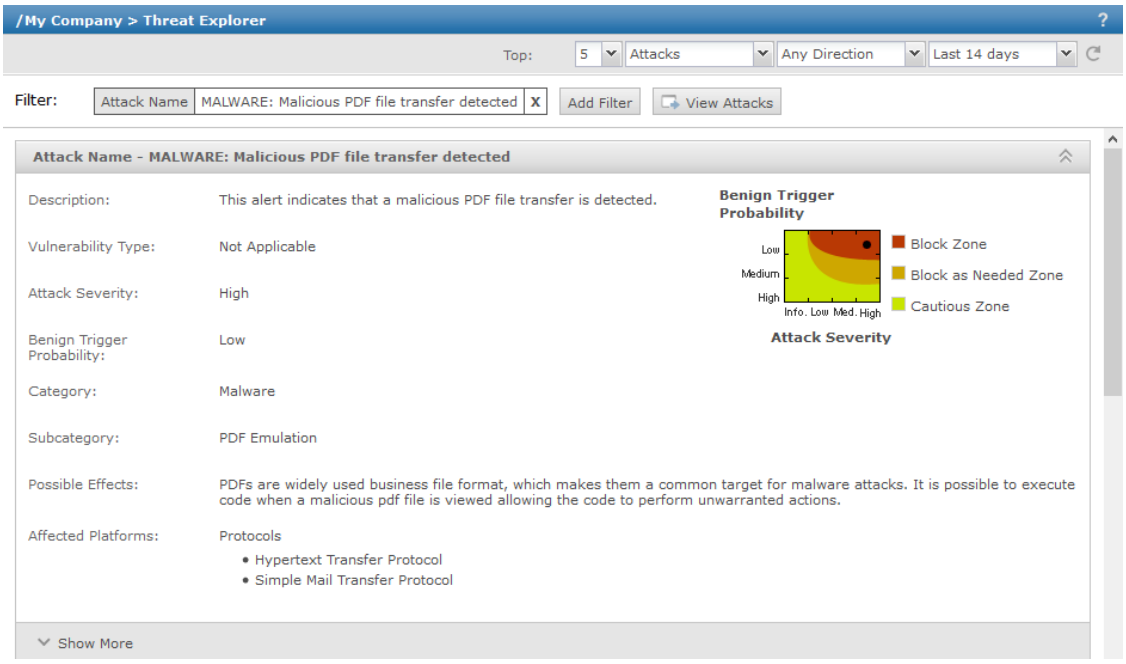


Figure 5-7 Threat Explorer page with a filter on that alert

- Clicking the **View Attacks** button opens the **Attack Log** page that shows all alerts for this file hash.

- Double-clicking one of these alerts opens the alert details panel.
- You can view the malware details in 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.

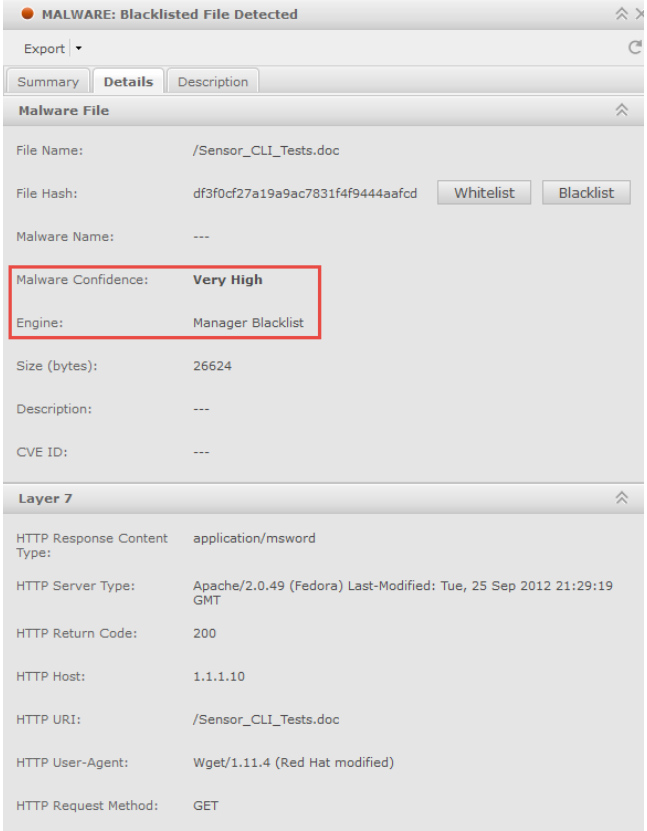


Figure 5-8 Malware Details panel, Alert Details window

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 about these commands, refer to the *McAfee Network Security Platform CLI 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.

Table 5-1 Manager faults and possible causes

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.	
		Failed to start the McAfee Agent service.	
		Failed to start the Data Exchange Layer service.	

6 Protecting the private cloud

With organizational networks expanding rapidly, data centers are expanding alongside to meet growing needs. Breaches in data centers are difficult to detect and can go unnoticed far too long. Advanced analysis capabilities are needed to effectively improve detection capabilities of sophisticated advanced attacks within the data center. Organizations need to detect breaches faster and adopt a continuous state of incident response as the frequency and sophistication of attacks have risen. So they require a connected security strategy that is multi-layered and thereby ensures that a threat that might evade one security measure is picked up by another.

As data centers transition to a software defined architecture and organizations begin moving critical assets to the cloud, these challenges become more pronounced since visibility of traffic within the virtual environment is reduced owing to the complexity in monitoring both north-south and east-west traffic. The cloud can broadly be either a public cloud or a private cloud.

A public cloud is a model under which cloud services are provided in a virtual environment, constructed using shared physical resources, and accessible over a public network. To some extent they work in contrast to private clouds which ring-fence a pool of underlying computing resources, creating a distinct cloud platform to which only a single organization has access. Public clouds, although have strict logical boundaries separating applications and data, provide services to several clients within the same shared infrastructure.

A private cloud involves a distinct and secure cloud based environment in a data center for a specific client to operate. It provides computing power as a service within a virtualized environment. The 'cloud' is the pool of physical computing resources and it is called 'private' since it is accessible only by a single organization thereby ensuring greater control and privacy. However, virtual presents threats and vulnerabilities that necessitate security.

McAfee offers a solution for protecting a private cloud environment which is an integration of several products that share threat information with one another. This enables your security infrastructure to allow or block a file in real time without the need for manual intervention each time suspicious activity is noticed in the network.

Contents

- *High-level description of the integration*
- *Components of the integration*
- *How do these components come together*
- *Real world scenarios to illustrate deployment*

High-level description of the integration

All necessary products, a number of enterprise class security products, are listed below along with the minimum versions required to make such an integration work:

- Network Security Platform — 8.3.7.28 or later
- McAfee® MOVE AntiVirus (MOVE)
  - MOVE AntiVirus Agentless — 4.0.0.317 or later
  - MOVE AntiVirus Multi-Platform — 4.0.0 or later
- Advanced Threat Defense — 3.4.8.96, 3.6.0.25, or later
- McAfee ePO — 5.1, 5.3.1, or later
- Threat Intelligence Exchange — 1.1.1, 1.2, or later
- Data Exchange Layer — 1.0.0 or later

This solution protects data centers with hybrid environments in which legacy systems and other on-premise infrastructure integrate and interconnect with cloud based applications. The integration of these products provides visibility into data and applications running in these hybrid environments. It offers both virtual network security and virtual machine-based security through Network Security Platform and MOVE.

You have a centralized management system in the Manager where you can define security policies, monitor security status, and respond to threats. The security policies are automatically applied as the compute resources scale up and down as per requirements. You also have a management console for endpoint security solutions through McAfee ePO and to deploy security within the SDDC through the Intel Security Controller.

Components of the integration

Several individual point products come together to offer a cohesive security solution as illustrated below. Each product is defined in this section along with its role in protecting a private cloud datacenter.

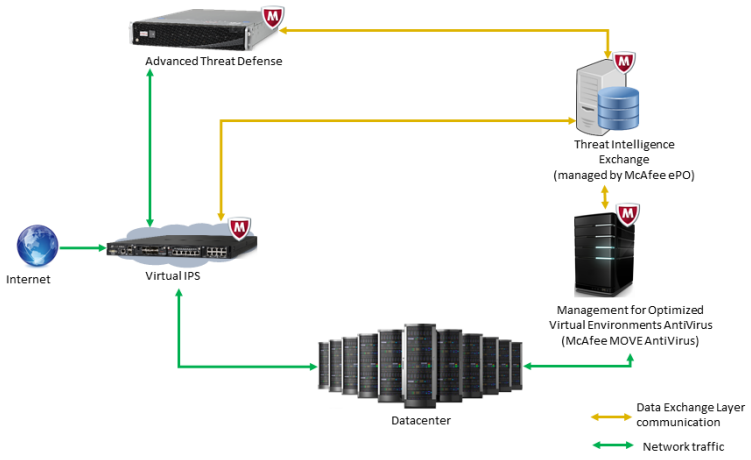


Figure 6-1 Solution architecture

McAfee Network Security Platform

The McAfee Network Security Platform IPS Sensor is the component that detects any threats present in the traffic. It can either be a physical IPS Sensor, a Virtual IPS Sensor, or a Virtual Security System which holds multiple instances of a Virtual IPS Sensor. This depends entirely on the expected throughput and intended functionality.

Regardless of the type of Sensor you decide to use in your deployment, you use the Network Security Manager for configuration and administration. The Manager can be installed on a physical server or on a virtual machine. Also, you can use the same Manager to manage both virtual and physical Sensors including those that are part of heterogeneous Sensor environments.

To know more about installation of the Manager, refer the *McAfee Network Security Platform Installation Guide*.

Whenever the IPS Sensor detects a suspicious file which cannot be determined malicious by other malware scanning engines, the Sensor sends the file to Advanced Threat Defense for static and dynamic analysis. Advanced Threat Defense returns a score for the file. Based on this score, the IPS Sensor initiates the configured response actions such as blocking the file.

To know more about configuring policies in Sensors to detect various types of threats, refer the *McAfee Network Security Platform IPS Administration Guide*.

MOVE AntiVirus

MOVE is an anti-virus solution for virtual environments. It removes the need to install an anti-virus application on every virtual machine (VM), and yet provides the protection and performance needed for your organization's requirements. The multi-platform and agentless deployment options offload all scanning to a dedicated VM - an offload scan server - that runs McAfee VirusScan Enterprise software. Guest VMs are no longer required to run anti-virus software locally, which improves performance for anti-virus scanning, and increases VM density per hypervisor.

MOVE does not directly communicate with Network Security Platform or Advanced Threat Defense. All such communication is facilitated through the Data Exchange Layer and Threat Intelligence Exchange. MOVE AntiVirus communicates with Advanced Threat Defense for file reputation scores through the Data Exchange Layer, which in turn contacts Threat Intelligence Exchange. When MOVE AntiVirus detects a threat either during an on-demand scan or an on-access scan, it queries Threat Intelligence Exchange for the reputation score through the Data Exchange Layer. If Threat Intelligence Exchange does not have a score for the file, then the file is sent to Advanced Threat Defense to obtain a file reputation score.

To know more about the configuration of MOVE in a network and its administration, refer the following guides:

- *McAfee MOVE AntiVirus (Multi-Platform) 4.0.0 Product Guide*
- *McAfee MOVE AntiVirus (Agentless) 4.0.0 Product Guide*

McAfee Threat Intelligence Exchange

Threat Intelligence Exchange 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. As Threat Intelligence Exchange is installed within McAfee ePO, you can use the McAfee ePO dashboard to deploy policies to the server.

Data Exchange Layer is the main communications infrastructure that Threat Intelligence Exchange uses to communicate with the IPS Sensor, MOVE AntiVirus, and Advanced Threat Defense. In general, communications to and from the Threat Intelligence Exchange servers are always through the Data Exchange Layer.

To know more about integrating Network Security Platform with Threat Intelligence Exchange, refer the chapter, *Integration with Threat Intelligence Exchange*, within this guide.

McAfee Data Exchange Layer

Data Exchange Layer 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. Network, endpoint, database, application, and other security solutions are meant to use the Data Exchange Layer to operate as one synchronized, real-time, context aware, and adaptive security system.

Threat Intelligence Exchange uses the Data Exchange Layer to query for information about file reputation that is requested by either Advanced Threat Defense or McAfee MOVE AntiVirus.

Integration between Network Security Platform and the Data Exchange Layer is part of the sequence of steps to integrate with Threat Intelligence Exchange.

To know more, refer the chapter, *Integration with McAfee Threat Intelligence Exchange*.

McAfee Advanced Threat Defense

Advanced Threat Defense is a multi-layer security product that includes pattern matching, global reputation, program emulation, static analysis, and dynamic analysis. All these layers are seamlessly integrated to provide you with a single point of control for easy configuration and management. It uses the sandboxing technology to provide scores for the malware files sent for analysis.

Advanced Threat Defense integrates with the IPS Sensor to provide malware scores to files. When the IPS Sensor detects a malware, it sends the file to Advanced Threat Defense for sandboxing and static analysis. Advanced Threat Defense then analyses the file and returns a malware score to the Sensor. The IPS Sensor then takes the configured corrective action depending on the score.

Advanced Threat Defense communicates with Threat Intelligence Exchange through the Data Exchange Layer to provide file reputation for malware files that have already been scanned.

To know more about integration of Network Security Platform with Advanced Threat Defense, refer the chapter, *Integration with McAfee Advanced Threat Defense*.

McAfee ePolicy Orchestrator

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. McAfee ePO can be integrated with multiple products to deploy polices to the endpoints. In this solution, Threat Intelligence Exchange is managed by McAfee ePO. Any policy update that has to be made to the endpoints is deployed through McAfee ePO.

To know more about integration of Network Security Platform with McAfee ePO, refer the chapter, *Integration with McAfee ePO*.

How do these components come together

In the current threat landscape, it is a priority to protect the virtualized environment. With more and more new threats being detected, any traffic flowing in the network needs to be monitored. All environments are exposed to threats from outside and inside. The Intel Private Cloud Security Solution helps detect the malware files in the network.

The IPS Sensor acts as the first line of defense for inspecting any traffic entering the network. It inspects traffic packets before allowing it to endpoints. When the IPS Sensor is not able to detect malware due to unsupported file formats, that file is sent to the endpoint without inspection. In this case, McAfee MOVE AntiVirus helps detect malware during an on-demand scan or an on-access scan. Together, the solution acts as layered protection where malware is either detected before it enters the network or is detected and blocked after it enters the network. This provides complete protection to the virtualized environment regardless of the mode in which it enters the network.

The general working of this solution is explained depending on where the threat originates.

Threat originates outside the network

- When any known malware attempts to enter the network, the IPS Sensor immediately blocks the file as it already contains information about the malware through attack signatures and on-board heuristics
- When up against an unknown file which might end up being a 0-day attack, the IPS Sensor sends the file to Advanced Threat Defense for dynamic analyses.
- Advanced Threat Defense returns a malware reputation for the file based on which the file is either blocked or allowed to the endpoint.
- If Advanced Threat Defense is not able to send back a reputation within a stipulated time, the IPS Sensor holds the file for 6 seconds and then passes it through to the endpoint.
- When the file reaches the endpoint, and an on demand or on-access scan is triggered, MOVE AntiVirus queries Threat Intelligence Exchange for the reputation.
- Although Advanced Threat Defense does not respond to Network Security Platform within 6 seconds it does respond and also sends the results of the scanning to Threat Intelligence Exchange.
- The file is then deleted by MOVE AntiVirus if its reputation determined malicious.
- When such a file attempts to enter the network the next time, the IPS Sensor queries Threat Intelligence Exchange and blocks the file.

Threat originates within the network

- When a suspicious file is already in the network, MOVE AntiVirus helps in detecting such files during an on-demand scan or an on-access scan.
- When MOVE AntiVirus detects a suspicious file, it queries Threat Intelligence Exchange for a reputation score through the Data Exchange Layer.
- If Threat Intelligence Exchange contains a reputation score for the suspicious file, it responds to MOVE AntiVirus with the score.
- If Threat Intelligence Exchange does not contain the score, it sends the file for scanning to Advanced Threat Defense through the Data Exchange Layer.
- When a reputation score is available from Advanced Threat Defense, Threat Intelligence Exchange passes it on to MOVE AntiVirus.

- Depending on the score, MOVE AntiVirus blocks or allows the file.
- Customized policies for your environments can be configured from McAfee ePO and updated in the McAfee MOVE AntiVirus server.

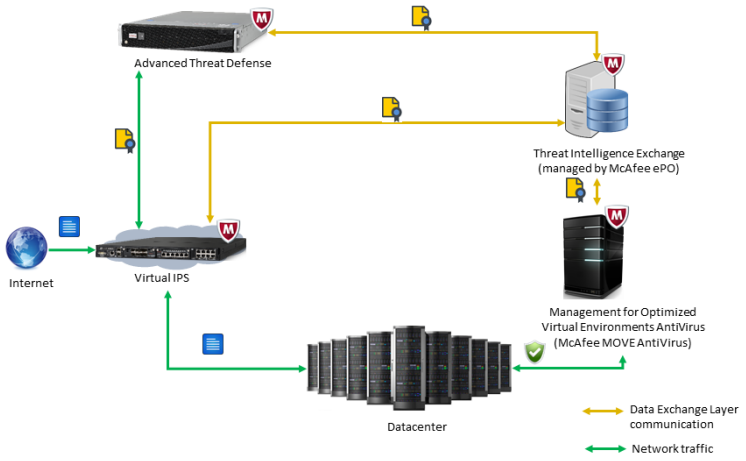


Figure 6-2 Solution architecture for protecting the private cloud

Real world scenarios to illustrate deployment

The working mentioned in the section above has been explained through two real world scenarios.

Scenario 1

An endpoint user accesses a web portal and attempts to download a file. The file arrives at the IPS Sensor and is scanned using policies configured in the IPS Sensor. The Sensor establishes that the file is unknown and suspicious, and after completing scanning using the various malware scanning engines on board, routes the file to Advanced Threat Defense.

The IPS Sensor sends a file to Advanced Threat Defense for scanning. The Sensor has a 6 second hold time when the file goes to Advanced Threat Defense. This hold time means that the last packet of the file is withheld by the Sensor. If after 6 seconds Advanced Threat Defense does not return a result, the file is permitted into the network. Advanced Threat Defense shares the results of the scan with Threat Intelligence Exchange and IPS Sensor. But since the file has entered the network, IPS Sensor cannot act to block the file and can only raise an alert, after which a security administrator must take corrective action. If such an event occurs during a weekend or after work hours for instance, there is the likely risk of the malicious file proliferating across the network and infecting other endpoints.

However, McAfee MOVE AntiVirus discovers the suspicious file on the endpoint during a scan, and queries Threat Intelligence Exchange, which earlier received malware reputation for the file from Advanced Threat Defense. McAfee MOVE AntiVirus is provided intelligence about the file and is able to block it based on the file reputation shared by Advanced Threat Defense.

As for the network perimeter, IPS Sensor is aware of the malicious file and is able to keep it out of the network by blocking it if it makes another attempt to enter the network.

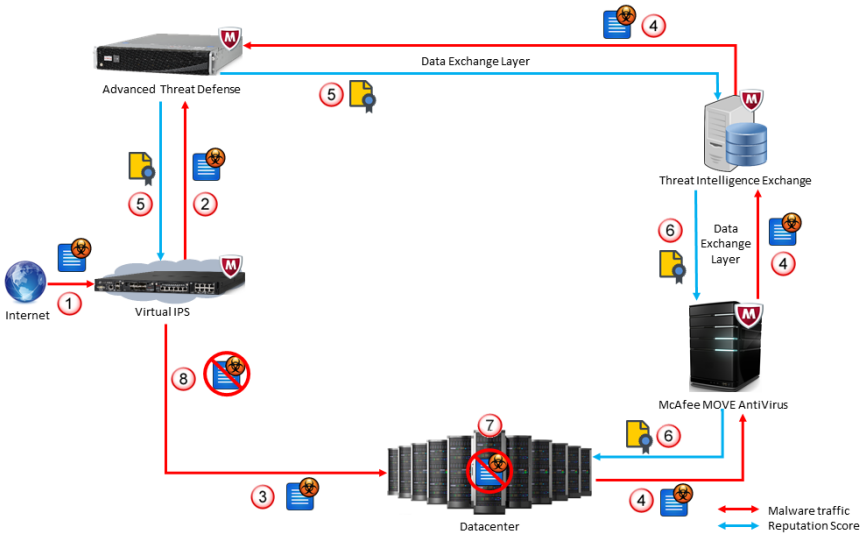


Figure 6-3 Scenario where a malicious file is allowed to enter network due to non-availability of reputation

1. The malware file enters the network from the Internet when an endpoint user requests it.
2. The IPS Sensor does not have the reputation score for the file. Hence, it sends the file to Advanced Threat Defense for sandboxing.
3. When Advanced Threat Defense does not send the reputation score within the stipulated time, the IPS Sensor sends the file to the endpoint after the 6 second hold time.
4. During an on-demand scan, McAfee MOVE AntiVirus discovers the suspicious file in an endpoint and queries Threat Intelligence Exchange for the reputation score through Data Exchange Layer.
5. Advanced Threat Defense has by now shared the malware reputation of the file as "Known Malicious" with IPS Sensor and Threat Intelligence Exchange.
6. Threat Intelligence Exchange returns this reputation to McAfee MOVE AntiVirus.
7. McAfee MOVE AntiVirus blocks deletes the file from the endpoint.
8. Since the IPS Sensor is aware of the malicious file, it is automatically blocked if it tries to enter the network again.

Scenario 2

When a file enters the network through a source within the network such as a USB device or from a DMZ network, or another vector, an inline IPS Sensor does not even see the file. The file which has slipped in to the network, for instance, on a Linux-based system begins proliferating laterally to Windows-based endpoints. At this point, McAfee MOVE AntiVirus detects the suspicious file during a scan and queries Advanced Threat Defense through Threat Intelligence Exchange. If Threat Intelligence Exchange does not have a malware reputation for the file, McAfee MOVE AntiVirus sends the file to Advanced Threat Defense for analysis.

Advanced Threat Defense then returns a reputation to McAfee MOVE AntiVirus through Threat Intelligence Exchange. McAfee MOVE AntiVirus now deletes the file. Next time the file tries to enter the network, the IPS Sensor queries Threat Intelligence Exchange, which responds with a "Known Malicious" file reputation and which enables the IPS Sensor to block the file.

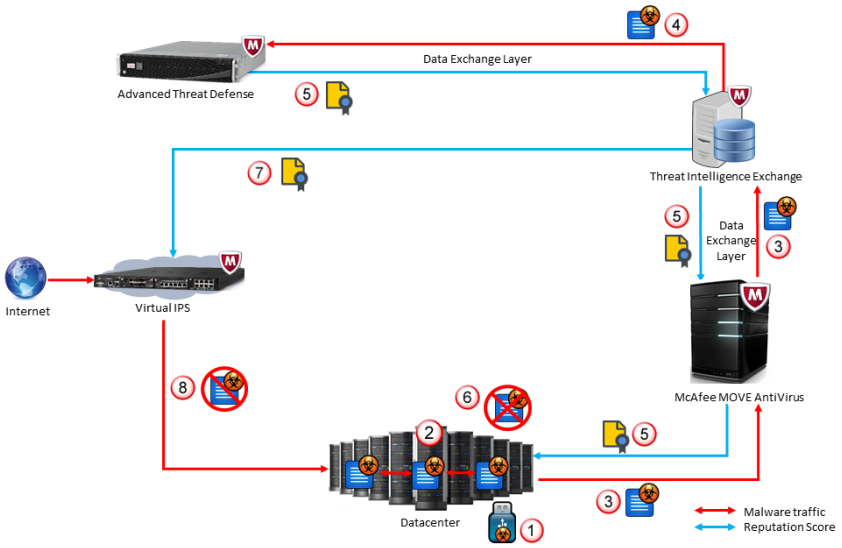


Figure 6-4 Scenario where a malicious file enters the network through an external device

1. The malicious file enters the network through an external device like the USB device.
2. The file proliferates in the network laterally.
3. McAfee MOVE AntiVirus detects the file during an on-demand scan and queries Threat Intelligence Exchange for the malware reputation of the file through Data Exchange Layer.
4. Since Threat Intelligence Exchange does not have the score for the file, Threat Intelligence Exchange queries with Advanced Threat Defense through Data Exchange Layer.
5. Advanced Threat Defense returns the reputation to McAfee MOVE AntiVirus as "Known Malicious" through the Threat Intelligence Exchange server.
6. McAfee MOVE AntiVirus deletes the file from the endpoint.
7. Next time the file tries to enter the network, the IPS Sensor queries Threat Intelligence Exchange for the score.
8. The file is blocked.

Integrating both endpoint and network security products provides you a means of determining malicious traffic in your network regardless of whether the threat emerges from the endpoint or from outside the network. As more organizations transition to deploying their business critical assets in the cloud the emphasis on security that is flexible enough to adapt to different threat vectors only increases.

7 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.

Contents

- *McAfee Network Security Platform - Vulnerability Manager integration*
- *Vulnerability assessment*
- *Relevance analysis of attacks*
- *Support for Vulnerability Manager custom certificates*
- *On-demand scan of endpoints from Threat Explorer*
- *Network scenarios for Vulnerability Manager scan*
- *Troubleshooting options*

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.

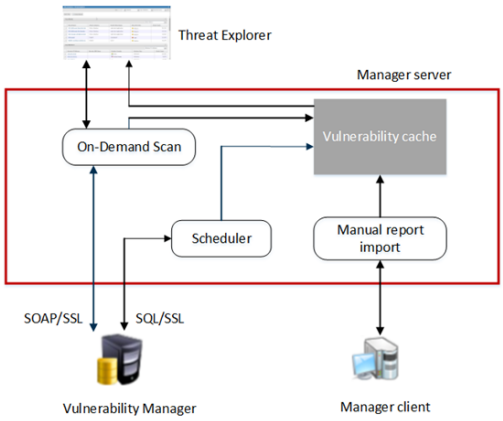


Figure 7-1 Network Security Platform-Vulnerability Manager integration

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 Configuring ACL rules, *McAfee Network Security Platform IPS Administration 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 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 — Which 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.

For more information on system requirements for different Vulnerability Manager Enterprise deployment scenarios, and setup process for different Vulnerability Manager versions, see *McAfee Network Security Platform Vulnerability Manager Administrator 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.

The product names, "Foundstone", and "Vulnerability Manager" refer to the same product.

See also

Configure Vulnerability Manager server settings on page 147
Support for Vulnerability Manager custom certificates on page 171
Configure Vulnerability Manager database settings on page 145

Menu options for Vulnerability Manager configuration

To configure Vulnerability Manager settings in the Manager , select **Manager** | **<Admin Domain Name>** | **Integration** | **Vulnerability Assessment** or **Manager** | **<Child Admin Domain Name>** | **Integration** | **Vulnerability Assessment** (for performing this action from root or child admin domains).

See also

Configure Vulnerability Manager database settings on page 145
Enable Vulnerability Manager integration at the admin domain level on page 143
Configure Vulnerability Manager server settings on page 147
Add Vulnerability Manager scan configurations on page 152

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.

```
rem ==========================================================================
rem required for loading NaiSignUtil DLL
rem ==========================================================================
set path=%path%;%APPROOT%\bin;%APPROOT%\bin\Microsoft.VC80.CRT;C:\Program Files\Foundstone\FCM;

set JAVA_OPTS=
REM This Section Specifically for NTService Mode
REM turns off default SIGHUP Handler
REM TOP ---- DO NOT REMOVE CODE BETWEEN THESE LINES
if ("%1") equ ("-Xrs")  (
    set JAVA_OPTS=-Xrs -DEnableCTRLCHandler=false
    REM NO application arguments
    set APP_ARGS=
)
REM BOTTOM - DO NOT REMOVE CODE BETWEEN THESE LINES

set JAVA_OPTS=%JAVA_OPTS% -server -Xms2007m -Xmx4014m -Xss128K
set JAVA_OPTS=%JAVA_OPTS% -XX:NewRatio=4 -XX:PermSize=128m -XX:MaxPermSize=320m -XX:+UseParallelOldGC
set JAVA_OPTS=%JAVA_OPTS% -Dapp.home.dir="%APPROOT%"
set JAVA_OPTS=%JAVA_OPTS% -Dapp.install.root="%APPROOT%"
set JAVA_OPTS=%JAVA_OPTS% -Dapp.home.dir.url="%APPROOT%"
set JAVA_OPTS=%JAVA_OPTS% -Dwin.dir="%WINDIR%"
set JAVA_OPTS=%JAVA_OPTS% -Dlumos.fixedManagerSNMPUDPPort="4167"
set JAVA_OPTS=%JAVA_OPTS% -Dlumos.fixedManagerSNMPIPaddress=""
set JAVA_OPTS=%JAVA_OPTS% -Dlumos.fixedManagerSNMPIPv6address="2001:0:0:0:0:0:233:103"
set JAVA_OPTS=%JAVA_OPTS% -Dpython.path="%JYTHONLIB%"
set JAVA_OPTS=%JAVA_OPTS% -Div.policymgmt.RuleEngine.compiler.netl7antlr.strictCheckEnabled="FALSE"
set JAVA_OPTS=%JAVA_OPTS% -Div.compiler.snort.dumpPCRE="TRUE"
rem set JAVA_OPTS=%JAVA_OPTS% -Div.policymgmt.RuleEngine.compiler.enableAPforSPM="FALSE"
set JAVA_OPTS=%JAVA_OPTS% -Div.compiler.snort.dumpSSIDandStates="TRUE"
set JAVA_OPTS=%JAVA_OPTS% -Div.controlchannel.snmpv3.useLocalizedKeys="FALSE"
set JAVA_OPTS=%JAVA_OPTS% -Dsun.lang.ClassLoader.allowArraySyntax=true
set JAVA_OPTS=%JAVA_OPTS% -Djava.rmi.server.hostname="localhost"
set JAVA_OPTS=%JAVA_OPTS% -Dcatalina.home="%CATALINA_HOME%"
set JAVA_OPTS=%JAVA_OPTS% -Djsse.enableCBCProtection=false
```

Figure 7-2 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 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 — 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** | **<Admin Domain Name>** | **Integration** | **Vulnerability Assessment** | **MVM** | **Vulnerability Scanning** | **Summary**.

OR

Manager | **<Child Admin Domain Name>** | **Integration** | **Vulnerability Assessment** | **MVM** | **Vulnerability Scanning** | **Summary** and click **Run Configuration Wizard** to start the Vulnerability Manager Configuration Wizard.

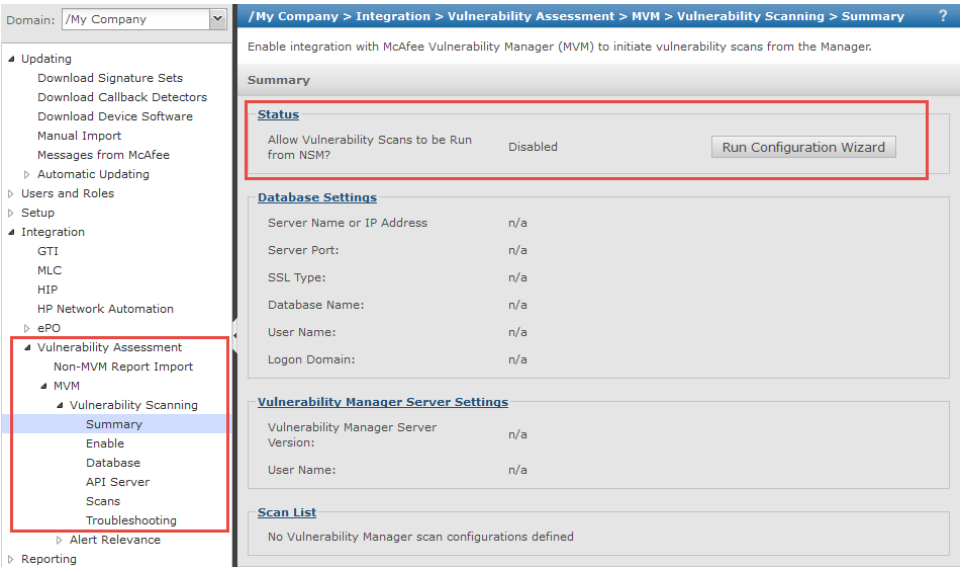


Figure 7-3 Vulnerability Manager Summary sub-tab

Tasks

- *Use Vulnerability Manager configuration wizard* on page 143
- *Enable Vulnerability Manager integration at the admin domain level* on page 143
- *Enable Vulnerability Manager integration at the child admin domain level* on page 144
- *Configure Vulnerability Manager database settings* on page 145
- *Configure Vulnerability Manager server settings* on page 147
- *Add Vulnerability Manager scan configurations* on page 152

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:

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.

```
rem ==========================================================================
rem required for loading NaiSignUtil DLL
rem ==========================================================================
set path=%path%;%APPROOT%\bin;%APPROOT%\bin\Microsoft.VC80.CRT;C:\Program Files\Foundstone\FCM;

set JAVA_OPTS=
REM This Section Specifically for NTService Mode
REM turns off default SIGHUP Handler
REM TOP ---- DO NOT REMOVE CODE BETWEEN THESE LINES
if ("%1") equ ("-Xrs")  (
    set JAVA_OPTS=-Xrs -DEnableCTRLCHandler=false
    REM NO application arguments
    set APP_ARGS=
)
REM BOTTOM - DO NOT REMOVE CODE BETWEEN THESE LINES

set JAVA_OPTS=%JAVA_OPTS% -server -Xms2007m -Xmx4014m -Xss128K
set JAVA_OPTS=%JAVA_OPTS% -XX:NewRatio=4 -XX:PermSize=128m -XX:MaxPermSize=320m -XX:+UseParalleloldGC
set JAVA_OPTS=%JAVA_OPTS% -Dapp.home.dir="%APPROOT%"
set JAVA_OPTS=%JAVA_OPTS% -Dapp.install.root="%APPROOT%"
set JAVA_OPTS=%JAVA_OPTS% -Dapp.home.dir.url="%APPROOT%"
set JAVA_OPTS=%JAVA_OPTS% -Dwin.dir="%WINDIR%"
set JAVA_OPTS=%JAVA_OPTS% -Dlumos.fixedManagerSNMPUDPPort="4167"
set JAVA_OPTS=%JAVA_OPTS% -Dlumos.fixedManagerSNMPIPaddress=""
set JAVA_OPTS=%JAVA_OPTS% -Dlumos.fixedManagerSNMPIPv6address="2001:0:0:0:0:0:233:103"
set JAVA_OPTS=%JAVA_OPTS% -Dpython.path="%JYTHONLIB%"
set JAVA_OPTS=%JAVA_OPTS% -Div.policymgmt.RuleEngine.compiler.netl7antlr.strictCheckEnabled="FALSE"
set JAVA_OPTS=%JAVA_OPTS% -Div.compiler.snort.dumpPCRE="TRUE"
rem set JAVA_OPTS=%JAVA_OPTS% -Div.policymgmt.RuleEngine.compiler.enableAPforSPM="FALSE"
set JAVA_OPTS=%JAVA_OPTS% -Div.compiler.snort.dumpSSIDandStates="TRUE"
set JAVA_OPTS=%JAVA_OPTS% -Div.controlchannel.snmpv3.useLocalizedKeys="FALSE"
set JAVA_OPTS=%JAVA_OPTS% -Dsun.lang.ClassLoader.allowArraySyntax=true
set JAVA_OPTS=%JAVA_OPTS% -Djava.rmi.server.hostname="localhost"
set JAVA_OPTS=%JAVA_OPTS% -Dcatalina.home="%CATALINA_HOME%"
set JAVA_OPTS=%JAVA_OPTS% -Djsse.enableCBCProtection=false
```

Figure 7-4 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** page.

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 ( ) to start the FCM Agent service.

10 In the Manager, select **Manager** | **<Admin Domain Name>** | **Integration** | **Vulnerability Assessment** | **MVM** | **Vulnerability Scanning** | **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

1 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.

See also

View Vulnerability Manager configuration details on page 154

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

1 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.

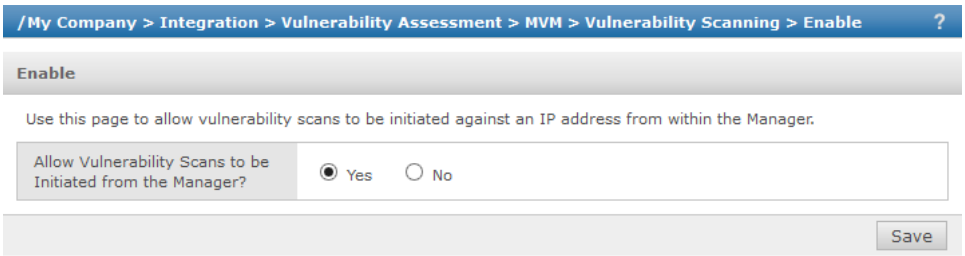


Figure 7-5 Enable area

3 Click **Save**.

See also

Menu options for Vulnerability Manager configuration on page 139

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

1 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.

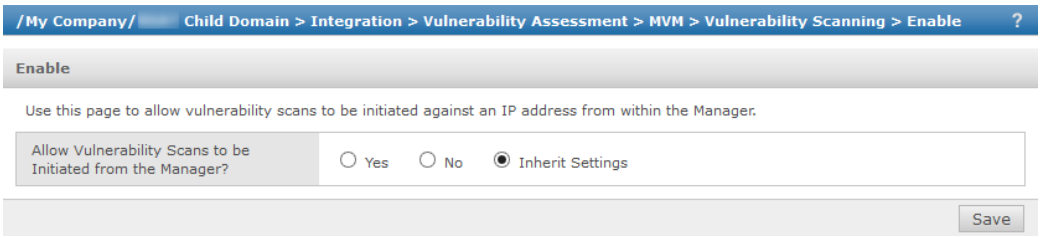


Figure 7-6 Enable page in child admin domain level

3 Click **Save**.

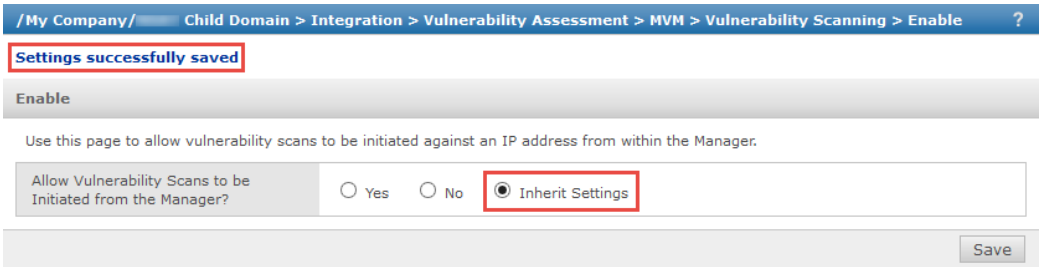


Figure 7-7 Update successful message

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.

> 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**.

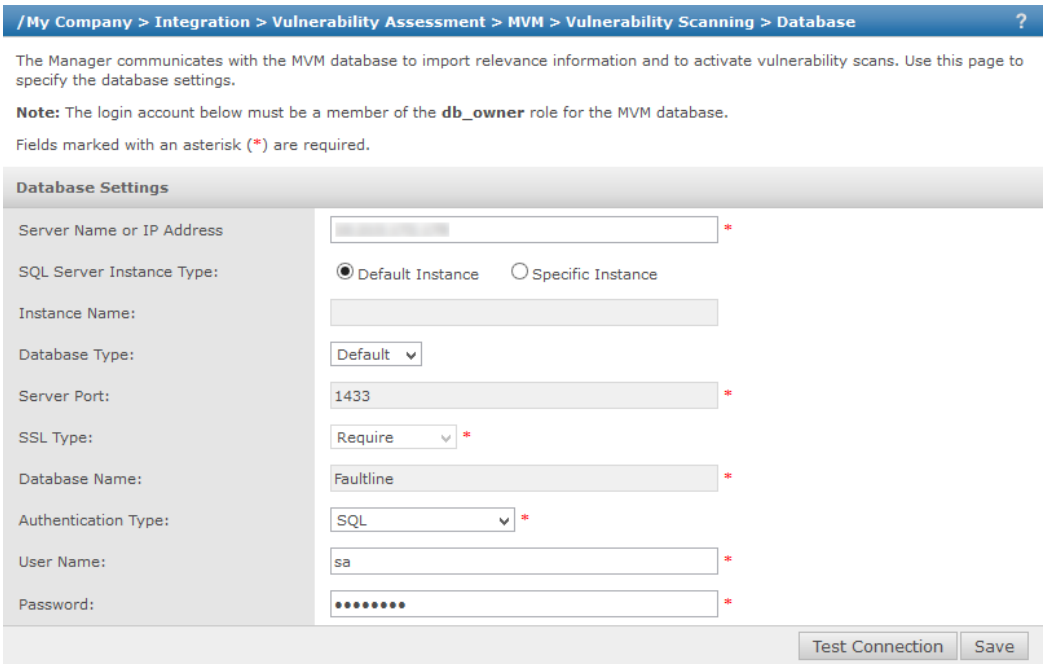


Figure 7-8 Database sub-tab

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, and
  - **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, then a plain connection is used.
Require	SSL is requested; if the server does not support it, then 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**.

7 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**.

    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.

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 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.

See also

Vulnerability Manager installation on page 139
Menu options for Vulnerability Manager configuration on page 139
Resubmission of database updates on page 184

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.

> 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.

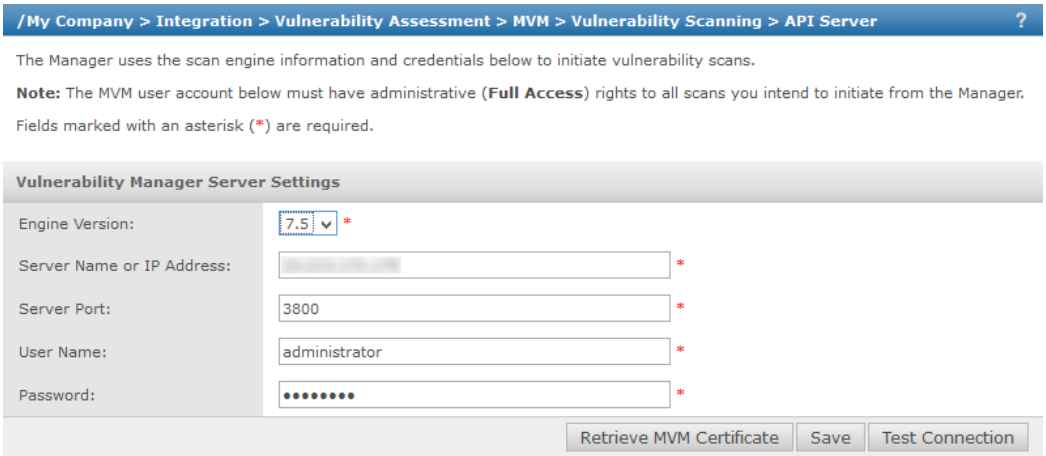


Figure 7-9 Vulnerability Manager Server Settings area

> Username and password entered here should have Update permissions for the integration on page 148 in the Vulnerability Manager server. This is essential for successfully initiating Vulnerability Manager on-demand scans from Threat Explorer.

5 Click Save Vulnerability Manager settings on page 149.

6 Start the Start the FCM agent service on page 150. Click **Retrieve MVM Certificate** to retrieve the MVM certificate.

> 7.0 and 7.5 scan engines support only custom certificates.

7 Click **Test Connection** to check the availability of Vulnerability Manager server connection.

Tasks

- *Update permissions for the integration* on page 148
- *Save Vulnerability Manager settings* on page 149
- *Start the FCM agent service* on page 150

See also

Vulnerability Manager installation on page 139
Menu options for Vulnerability Manager configuration on page 139
On-demand scan of endpoints listed in alerts in the Threat Analyzer on page 173

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**.

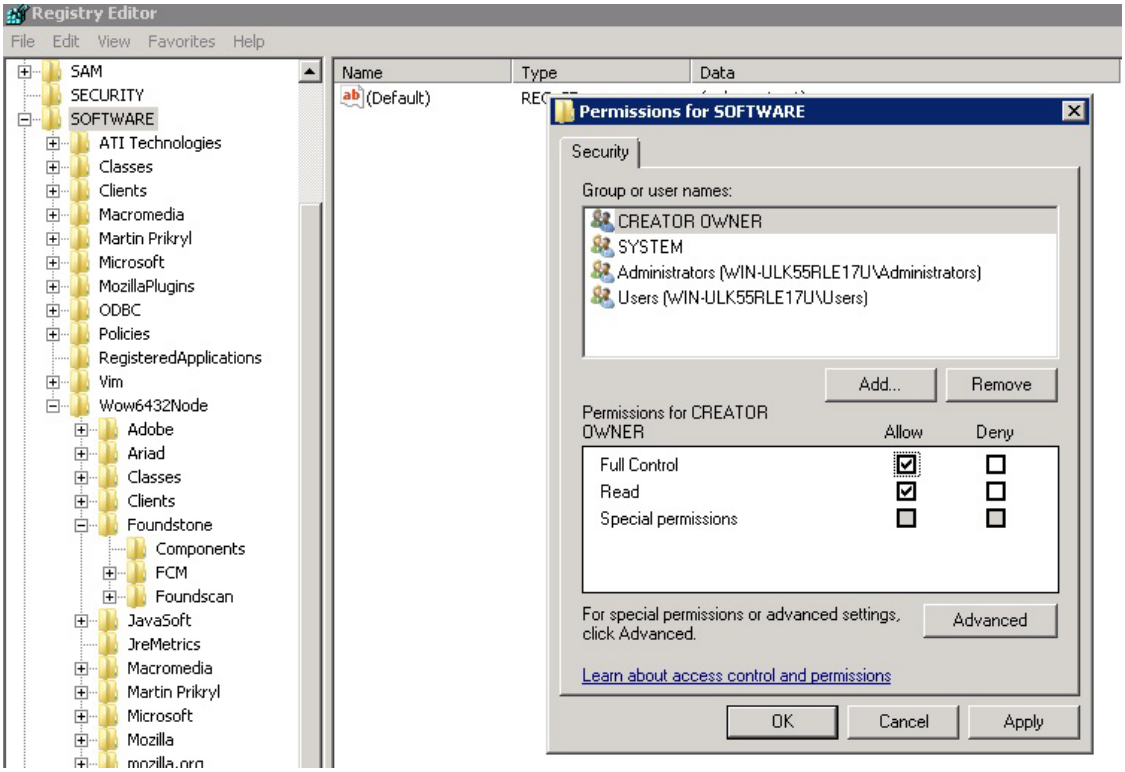


Figure 7-10 Updating permissions

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

To save the Vulnerability Manager server settings:

Task

1 In the Manager, select **Manager** | **<Admin Domain Name>** | **Integration** | **Vulnerability Assessment** | **MVM** | **Vulnerability Scanning** | **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.

  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**.

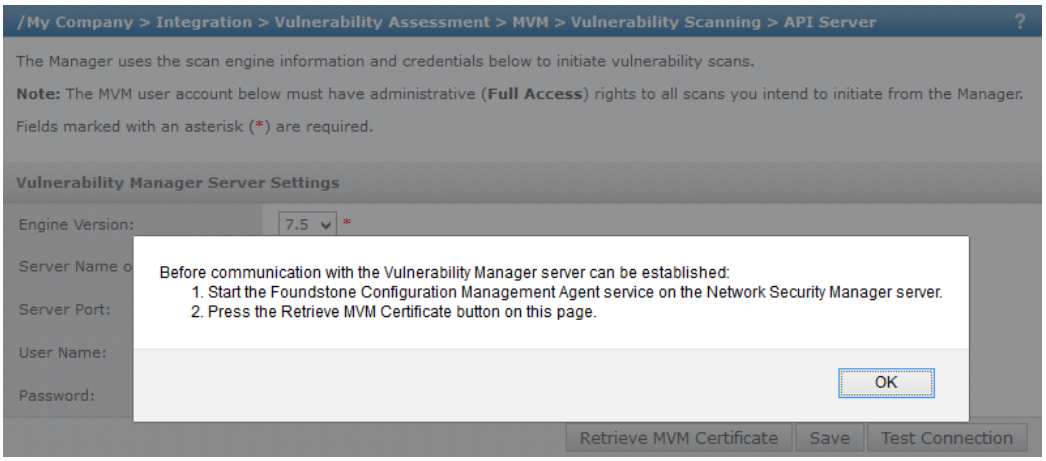


Figure 7-11 API Server page

When the API Server settings is saved, some of the settings like Server IP address and Port settings are updated into 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**.

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.

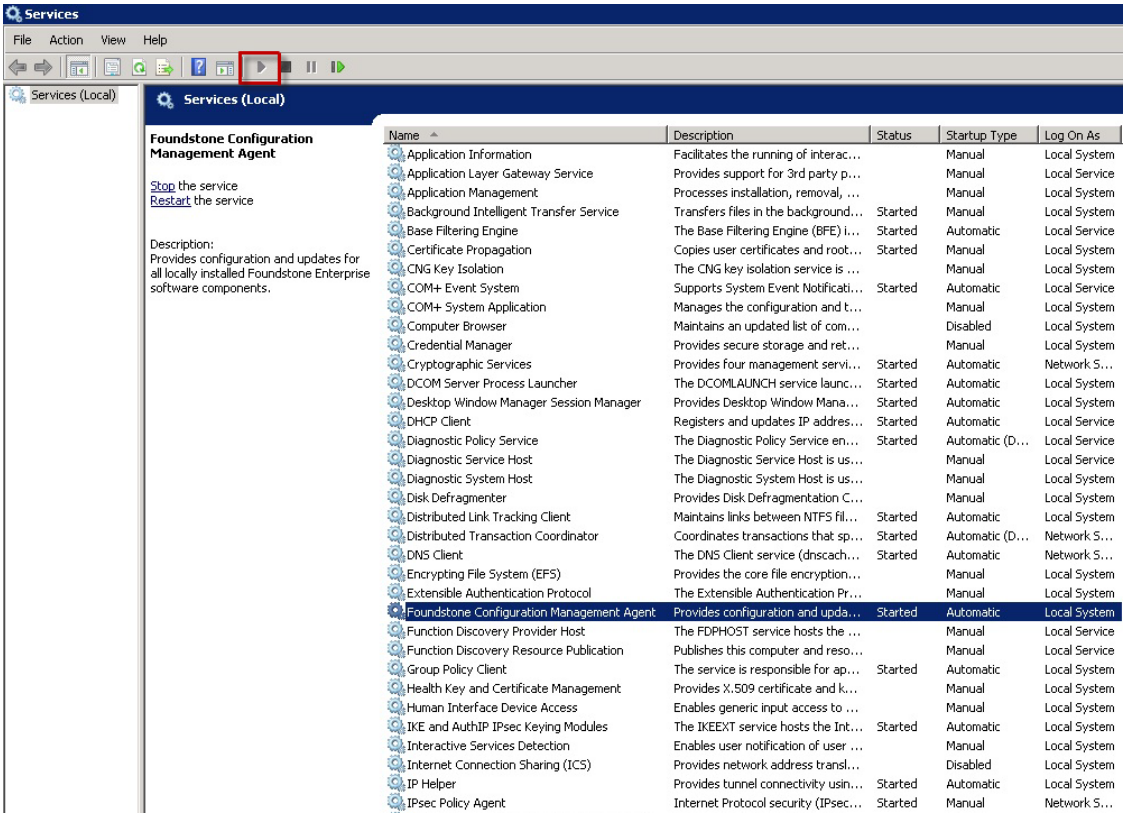


Figure 7-12 Services page

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.

4 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.

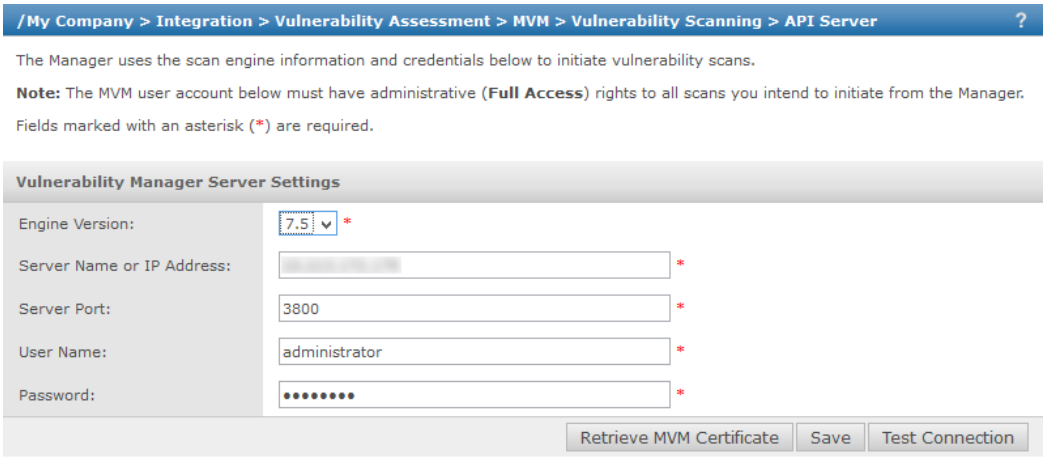


Figure 7-13 Vulnerability Manager Server Settings area

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, then 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.

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.

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 Working with Scans, *McAfee Network Security Platform Foundstone Administrator Guide*. The product name "Foundstone", and "Vulnerability Manager " refer to the same product.

Task

1 Select **Manager** | **<Admin Domain Name>** | **Integration** | **Vulnerability Assessment** | **MVM** | **Vulnerability Scanning** | **Scans**.

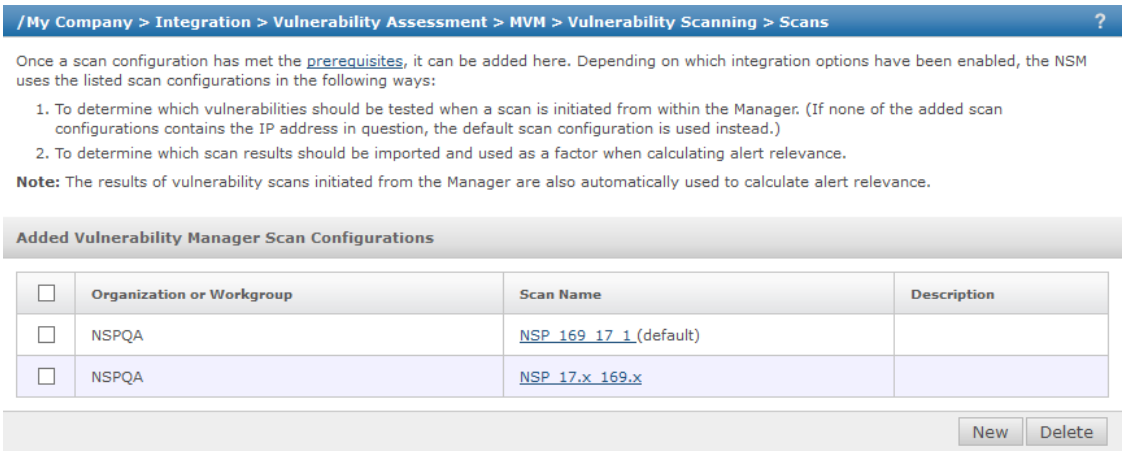


Figure 7-14 Added Vulnerability Manager Scans dialog

The **Added Vulnerability Manager Scan Configurations** page appears.

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**.

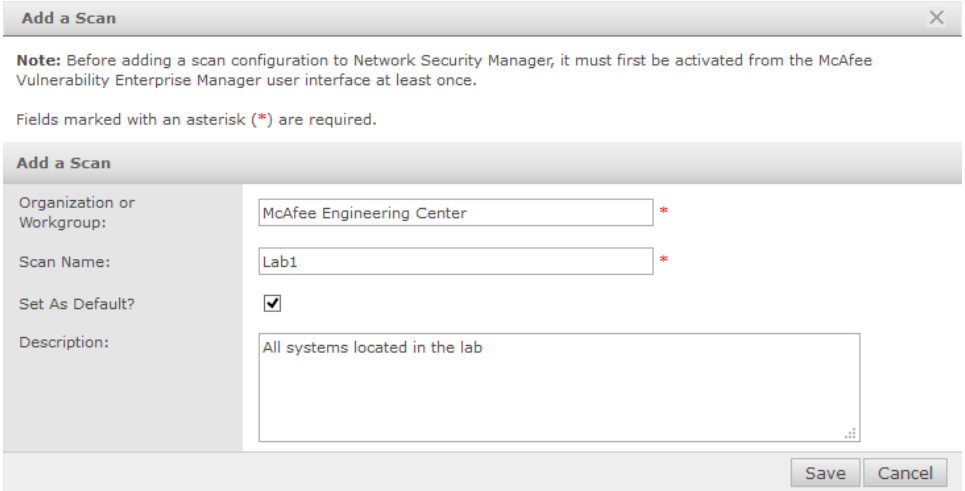


Figure 7-15 Add a Scan dialog

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.

See also

Concurrent scan of endpoints on page 181
Menu options for Vulnerability Manager configuration on page 139

View Vulnerability Manager configuration details

You can view the Vulnerability Manager configuration details in Manager. To do so perform the following steps.

Select **Manager** | **<Admin Domain Name>** | **Integration** | **Vulnerability Assessment** | **MVM** | **Vulnerability Scanning** | **Summary** to perform this action from root or child admin domains. The **Summary** page appears.

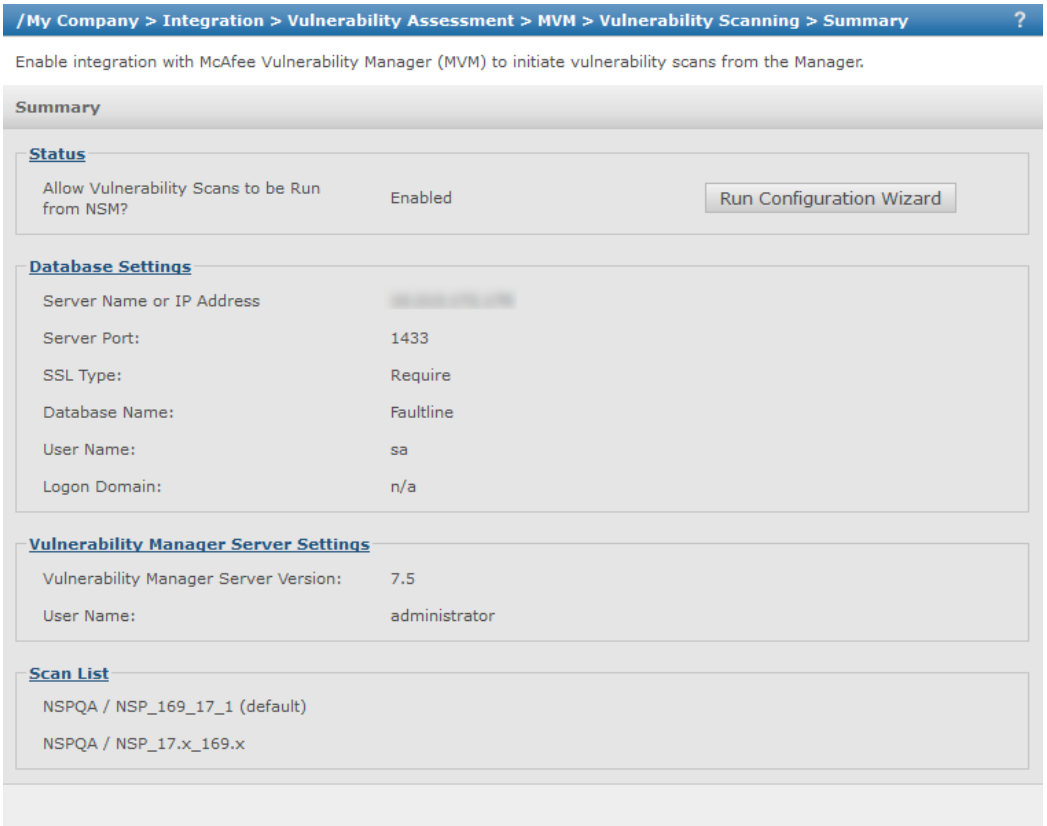


Figure 7-16 Summary page

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 **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.

See also

Use Vulnerability Manager configuration wizard on page 143

Import non-vulnerability manager report

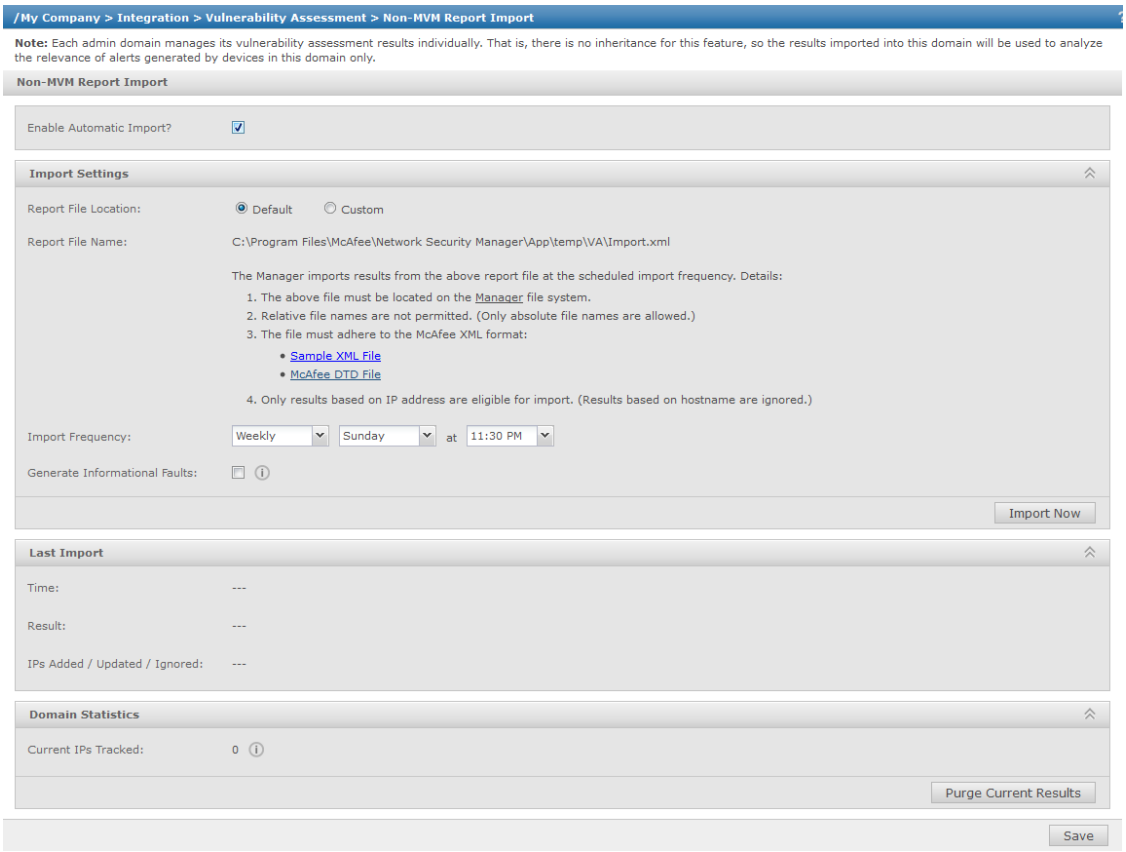
The vulnerability assessment scan results of an admin domain can be imported in an XML format from a location in the Manager's file system. You can reformat the scan results and save it to a specific location, so that the Manager automatically imports the result to be later used to determine alert relevance.

The non-MVM report import feature is disabled if **Alert Relevance** feature is disabled in the Manager.

Task

1 Select **Manager** | **<Admin Domain Name>** | **Integration** | **Vulnerability Assessment** | **Non-MVM Report Import**.

The **Non-MVM Report Import** page is displayed.



2 Select the **Enable Automatic Import?** checkbox.

> By default, this option is not selected.

The **Import Settings** panel is displayed with the following fields.

Table 7-1 Import Settings

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. When the **Default** option is selected for the **Report File Location** this text field is disabled and so 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.
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.

Table 7-1 Import Settings *(continued)*

Option	Definition
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. 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>	
<Report Time>	The date when the scan was performed. Example: 09.10.2015 (MM.DD.YYYY)
<ScanStartTime>	The starting time of the scan. Example: 09.10.2015 (MM.DD.YYYY) 18:08:17 (HH:MM:SS) The scan start time coincides with the server time.
<ScanEndTime>	The end time of the scan. Example: 09.10.2015 (MM.DD.YYYY) 18:49:37 (HH:MM:SS)
<ScanElapsedTime>	The duration of the time elapsed since the scan was performed. Example: 0 day(s) 00:41:19 (HH:MM:SS)
<SecurityVulnerability Summary>	
<TotalNumberOfVulnerabilities>	The total number of vulnerabilities found in the scan.
<HighSeverityVulnerabilities>	The total number of high severity vulnerabilities found during the scan.
<MediumSeverityVulnerabilities>	The total number of medium severity vulnerabilities found during the scan.
<LowSeverityVulnerabilities>	The total number of low severity vulnerabilities found during the scan.
<InformationalVulnerabilities>	The total number of linformational vulnerabilities found during the scan.
<Host Info>	

XML child elements	Description
<HostIP>	IP address of the host.
<HighSeverityVulnerabilities>	High severity vulnerabilities found in the host
<MediumSeverityVulnerabilities>	Medium severity vulnerabilities found in the host
<LowSeverityVulnerabilities>	Low severity vulnerabilities found in the host
<InformationalVulnerabilities>	Informational vulnerabilities found in the host
<SingleVulnerability>	
<HostIP>	IP address of the host.
<OriginalDescription>	The original description of the vulnerability.
<PortNumber>	The port number of the host
<Protocol>	The protocol used for communication
<ServiceName>	The service name
<Severity>	The severity of the vulnerability
<VulnerabilityDescription>	The description of the vulnerability
<Solution>	The solution for the vulnerability.
<RiskFactor>	The risk factor, if exists.
<CVE>	The CVE ID of the vulnerability.
<BID>	BID ID for the vulnerability, if any.
<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, all the vulnerability assessment results that are stored for the admin domain gets deleted.

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.

3 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 IPS Administration 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.

For more information see *McAfee Network Security Platform Integration Guide.*

Relevance analysis of attacks

Relevance analysis involves the analysis of the vulnerability relevance of real-time alerts, using the vulnerability data imported into 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 Attack Log in the *McAfee Network Security Platform Manager Administration 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, by running an on demand scan, or by 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 give you the option to use Vulnerability Manager data in relevance analysis. Select **Manager** | **<Admin Domain Name>** | **Integration** | **Vulnerability Assessment** | **MVM** | **Alert Relevance**.

The following menu options are displayed:

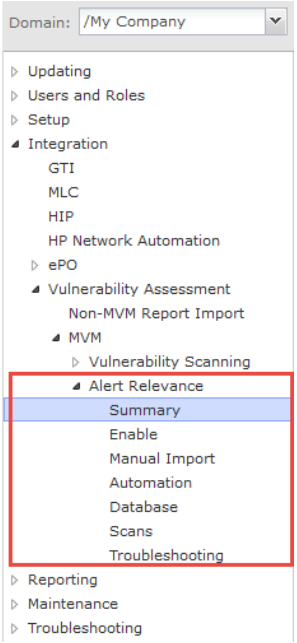


Figure 7-17 Relevance menu options

Item	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.

Item	Menu option	Description
7	**Scans**	Add scan configurations in Manager.
8	**Troubleshooting**	Troubleshooting options like reloading Vulnerability Manager cache, resetting relevancy cache, and re-submitting database updates.

The menu options explained above are mentioned as *Relevance menu options* throughout this document.

See also

Vulnerability Manager database settings for relevance analysis on page 169
Add scan configurations for relevance analysis on page 170
Enable attack relevance analysis on page 162
Import scans automatically using Scheduler on page 168

Relevance configuration details

To view the relevance configuration details in Manager, do the following:

Select **Manager** | **<Admin Domain Name>** | **Integration** | **Vulnerability Assessment** | **MVM** | **Alert Relevance** | **Summary** or **Manager** | **<Child Admin Domain Name>** | **Integration** | **Vulnerability Assessment** | **MVM** | **Alert Relevance** | **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 **Summary** page. When you click on the individual links, you are re-directed to the respective pages.

You can also configure relevance settings using **Run Configuration Wizard** in **Summary** page.

Use relevance configuration wizard

You can use the *Relevance Configuration Wizard* for configuring relevance settings from Manager.

Task

1. Select **Manager** | **<Admin Domain Name>** | **Integration** | **Vulnerability Assessment** | **MVM** | **Alert Relevance** | **Summary** or **Manager** | **<Child Admin Domain>** | **Integration** | **Vulnerability Assessment** | **MVM** | **Alert Relevance** | **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.

See also

Enable attack relevance analysis on page 162
Import scans automatically using Scheduler on page 168
Add scan configurations for relevance analysis on page 170
Import scan reports manually on page 166
Vulnerability Manager database settings for relevance analysis on page 169

Enable attack relevance analysis

This is the first essential step in configuring Manager for relevance analysis.

To enable relevance analysis, do the following:

Task

1 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**

See also

Menu options for relevance analysis on page 160
Relevance analysis configuration in Manager on page 162

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?**.

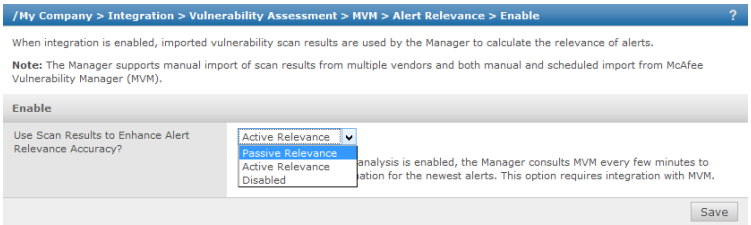


Figure 7-18 Relevance tab

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.

Task

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.

> 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 Analyzer and later can query for the Asset Details.

1 In the Manager, navigate to **Analysis** | **Threat Analyzer** | **Real-Time** | **Start the Real-Time Threat Analyzer**.

2 In the Threat Analyzer, navigate to the **Alerts** page. Right-click the alert.

3 Select **Start Vulnerability Scan** | **Scan Source IP** or **Start Vulnerability Scan** | **Scan Destination IP** option.

You can also query and retrieve the asset information from the Vulnerability Manager database:

Task

1 Right-click the alert, and select **Source Host Details** or **Destination Host Details**.

2 The Manager retrieves Asset Information like OS, Service pack, open ports, protocols, services, and list of known vulnerabilities for the given host IP address.

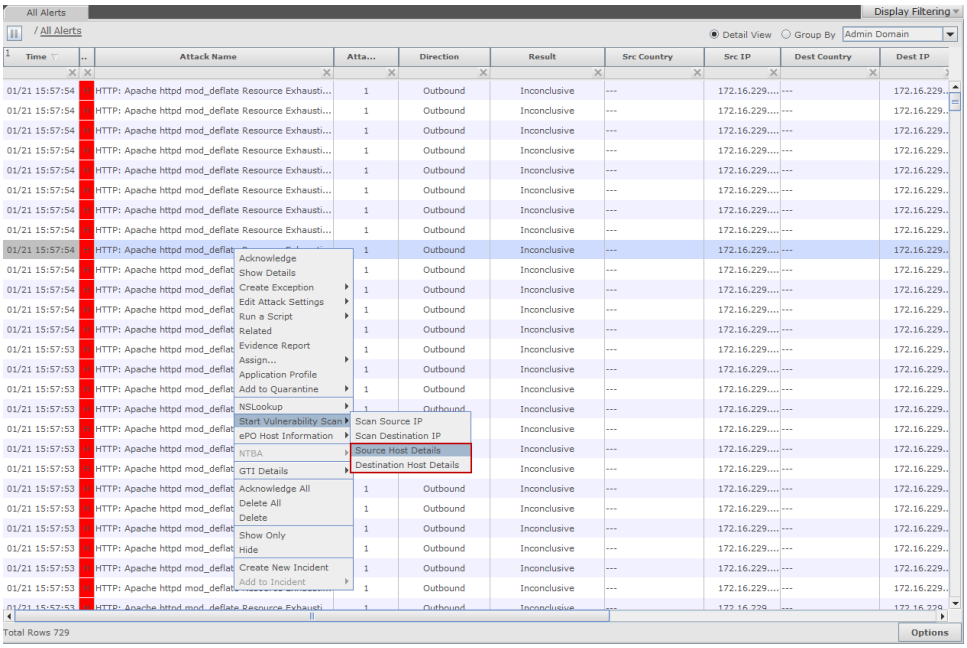


Figure 7-19 Host Details option

3 If the host has already been scanned by the Vulnerability Manager Engine, the following **Asset Details** pages are displayed. Use to view the Asset details in table or pie chart formats.

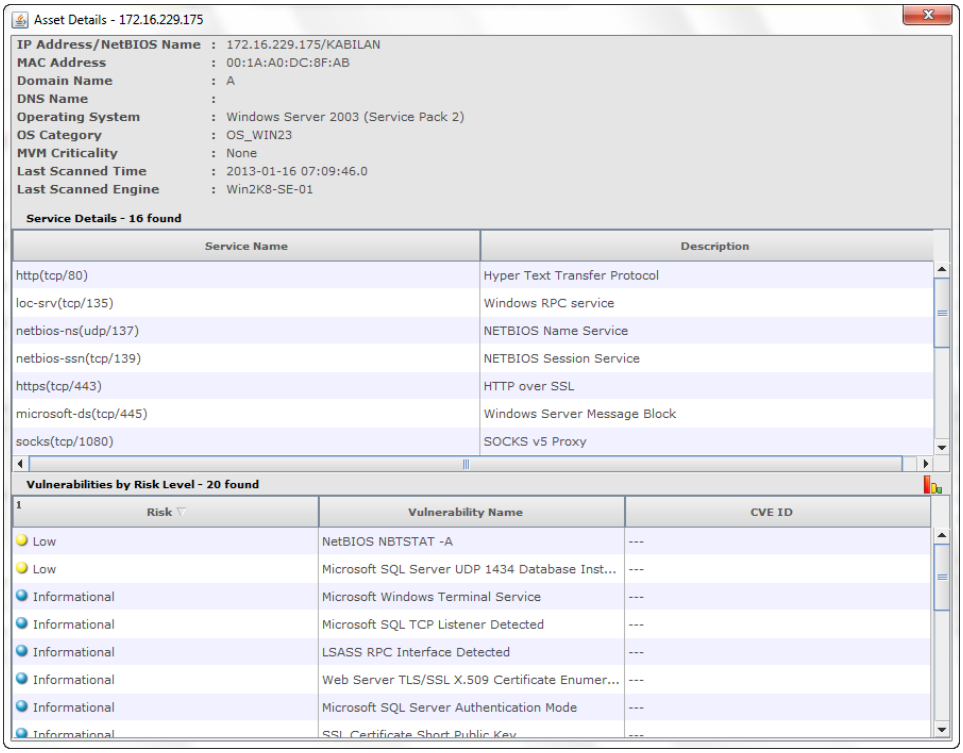


Figure 7-20 Asset Details Window (table format)

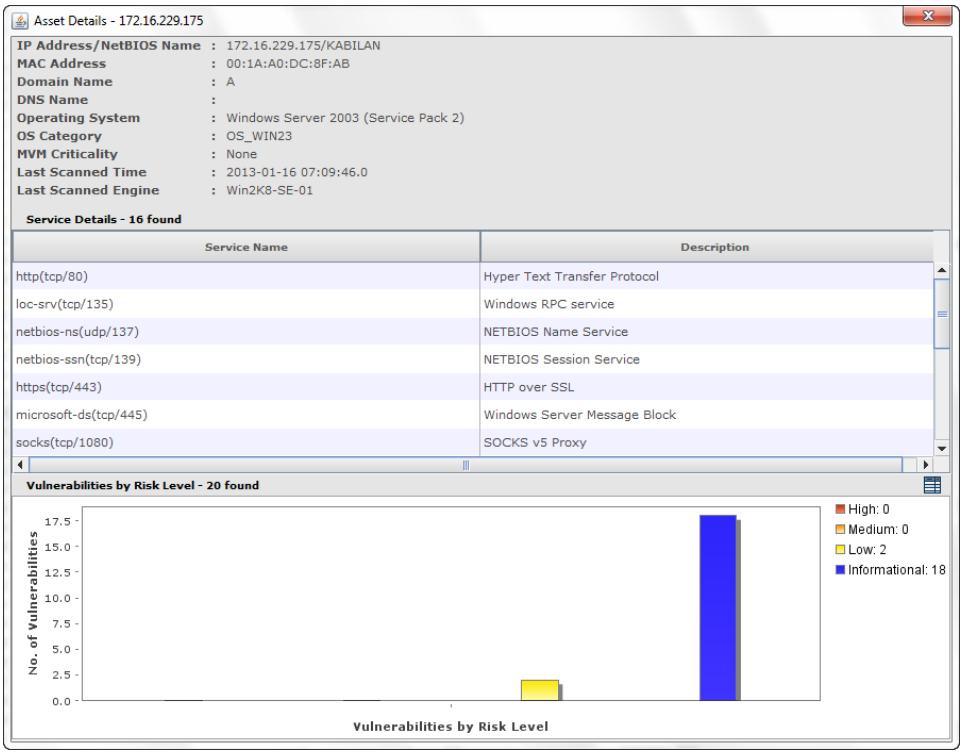


Figure 7-21 Asset Details Window (bar chart format)

4 The Asset details are described in the following table:

Field	Description
IP Address/NetBIOS Name	IP address of the scanned host / LDAP attribute containing the NetBIOS name
MAC address	MAC address of the scanned host
Domain name	The domain name is displayed as • **WORKGROUP** in Windows operating system • **Not Available** for other operating systems
DNS Name	LDAP attribute containing the host (Domain) name
Operating System	The operating system used
OS Category	The category of the operating system (Windows or Linux)
MVM Criticality	The criticality levels of the scanned result (None, Low, Limited, Moderate, Significant, Extensive) By default all assets are counted as Moderate.
Last Scanned Time	The last time when the scan was performed
Last Scanned Engine	The machine where the last scan was performed

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

1 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).

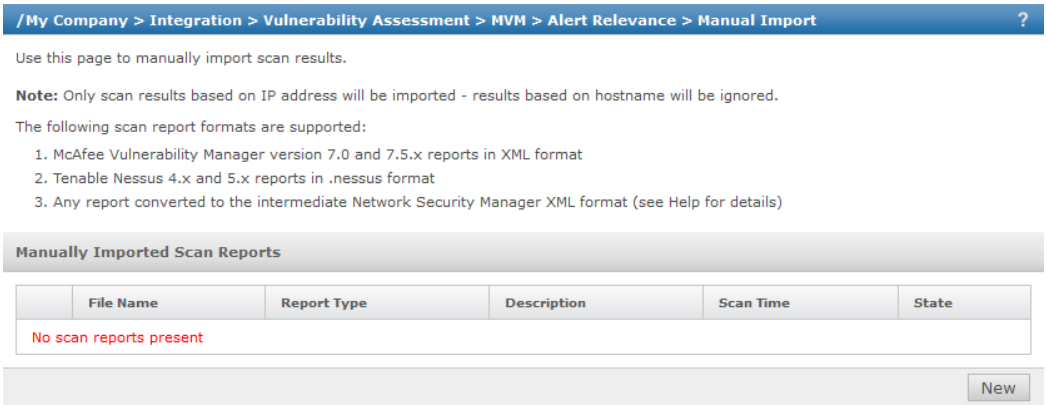


Figure 7-22 Manually Imported Scan Reports area

2 In **Manually Imported Scan Reports**, click **New**.The **Import a Scan Report** window appears.

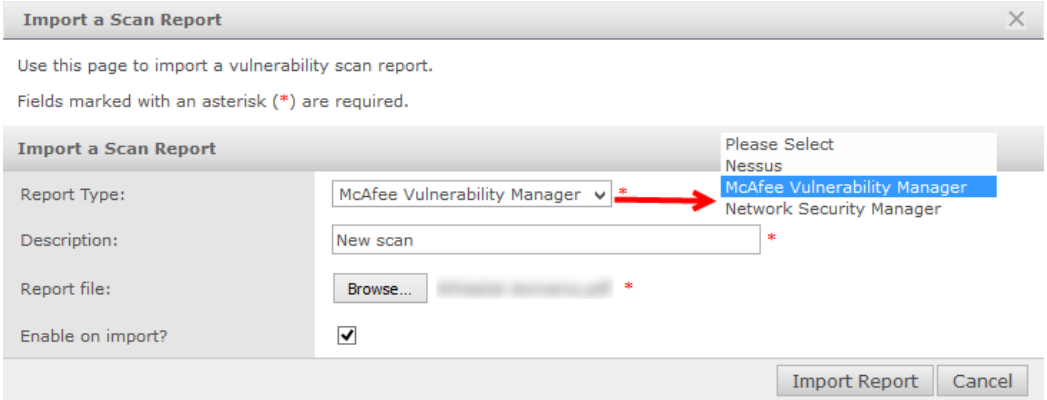


Figure 7-23 Import a Scan Report dialog

3 Select a **Report Type** from the drop-down list.

> 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 **Browse** 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.

> 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.

See also

NessusWX on page 168
Network Security Platform format on page 168
Supported vulnerability scanners and formats on page 167
Vulnerability Manager format on page 168
Relevance analysis configuration in Manager on page 162

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.

See also

Import scan reports manually on page 166

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.

See also

Import scan reports manually on page 166
Import scans automatically using Scheduler on page 168

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.

See also

Import scan reports manually on page 166

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.

But for successfully importing and viewing these scanner reports in 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.

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.

See also

Import scan reports manually on page 166

Import scans automatically using Scheduler

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 Scheduler in Manager.

During the automatic import process, the 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 the Scheduler.

Task

1 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.

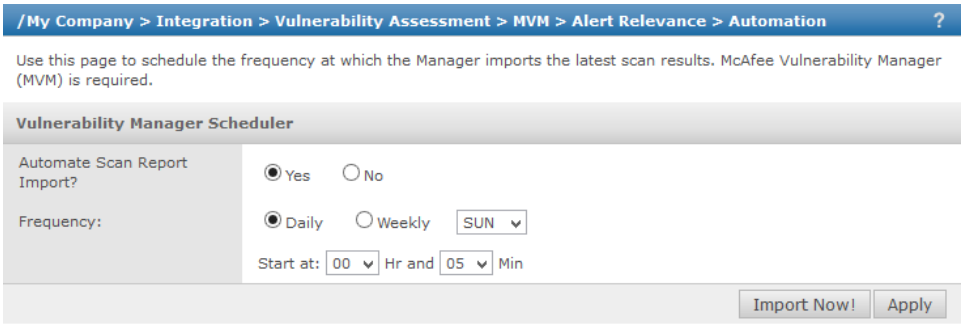


Figure 7-24 Automation sub-tab

2 Select **Yes** for **Automate Scan Report Import?**. 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**.

5 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.

> The **Import Now!** feature available in the parent domain, at **Manager** | **<Admin Domain Name>** | **Integration** | **Vulnerability Assessment** | **MVM** | **Alert Relevance** | **Automation**, is not applicable for child domains that have Vulnerability Manager settings (**Manager** | **<Admin Domain Name>** | **Integration** | **Vulnerability Assessment** | **MVM** | **Alert Relevance** | **Enable** or **Manager** | **<Child Admin Domain Name>** | **Integration** | **Vulnerability Assessment** | **MVM** | **Alert Relevance** | **Enable**) set to **Inherit Settings?**. Consequently, **Import Now!** and **Apply** buttons are not seen in the **Automation** page (**Manager** | **<Admin Domain Name>** | **Integration** | **Vulnerability Assessment** | **MVM** | **Alert Relevance** | **Automation** or **Manager** | **<Child Admin Domain Name>** | **Integration** | **Vulnerability Assessment** | **MVM** | **Alert Relevance** | **Automation**) of such child domains.

See also

Fault messages for Vulnerability Manager scheduler on page 170
Vulnerability Manager format on page 168
Menu options for relevance analysis on page 160
Relevance analysis configuration in Manager on page 162

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** | **<Admin Domain Name>** | **Integration** | **Vulnerability Assessment** | **MVM** | **Alert Relevance** | **Database** 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 the **Alert Relevance** tab are similar to the **Database Settings** page under the **Vulnerability Scanning** tab.

See also

Menu options for relevance analysis on page 160
Relevance analysis configuration in Manager on page 162

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

1 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** tab are similar to the **Added Vulnerability Manager Scan Configurations** page under the **Vulnerability Scanning** tab.

See also

Menu options for relevance analysis on page 160
Relevance analysis configuration in Manager on page 162

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 also the possible actions for correcting the fault.

See also

Import scans automatically using Scheduler on page 168

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.

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/`

For more information about creating custom client certificates using FCM tool, see Working with SSL certificates, *McAfee Network Security Platform Foundstone Configuration Manager Guide*.

The product names, "Foundstone", and "Vulnerability Manager" refer to the same product.

See also

Vulnerability Manager installation on page 139

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.

   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**.

   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** | **Run**, type **cmd**, 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” and you have created child domains under that named “EastCoast”, “MidWest”, and “WestCoast” and you are integrating with Vulnerability manager 7.0, then 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.

On-demand scan of endpoints from Threat Explorer

You can now perform an on-demand scan of endpoints from the **Threat Explorer** page based on the attacker or target IP address. You can view the vulnerabilities for that IP address under the **Vulnearbility Assessment** tab.

Task

1 Navigate to **Analysis** | **<Admin Domain Name>** | **Threat Explorer**.

2 Click the IP address for which you want to perform the scan.

The details panel for the selected IP address opens.

3 Select the **Vulnerability Assessment** tab.

4 Click **Scan for Vulnerabilities**.

If the IP address is not listed in the MVM scan Manager, a warning message appears. Click **OK**.

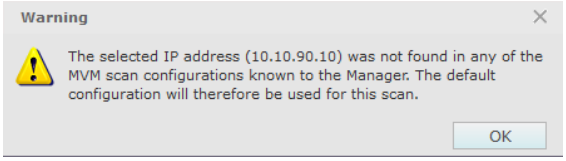


Figure 7-25 Scan configuration pop-up

An informational message appears which displays that a scan request is placed for the IP address. Click the refresh icon to view the scan results.

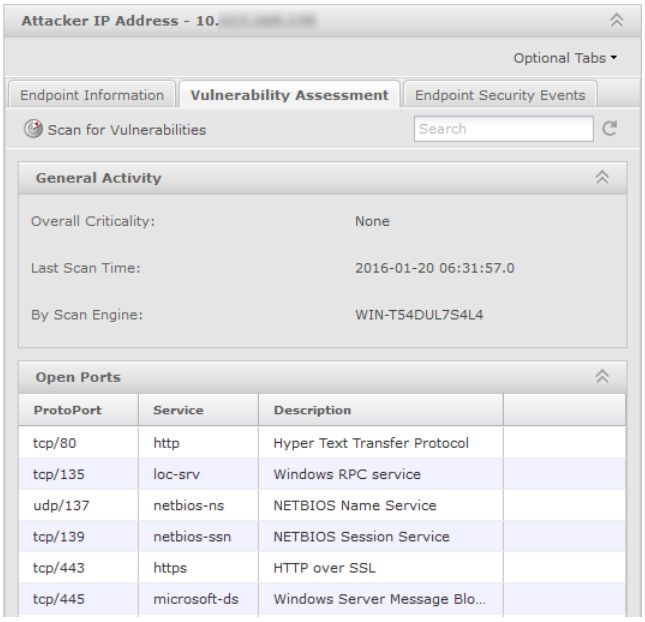


Figure 7-26 Scan information

On-demand scan of endpoints listed in alerts in the Threat Analyzer

The on-demand scan functionality helps you to scan endpoints using Vulnerability Manager, based on the *source* or *destination IP addresses*, in the Real-time, and Historical Threat Analyzer.

When you request an on-demand scan for an IP address listed under **Vulnerability Scan Information** in **Forensics** page, or for an alert listed in the **Alerts** page, the selected IP address is sent from the Threat Analyzer to the API Server of Vulnerability Manager.

The API Server acts as a gateway interface between the Manager and Vulnerability Manager.

The API Server delegates the scan request from Manager to the Scan Engine. Once the scan is successfully completed, Manager queries the API Server for Vulnerability Assessment data. The Vulnerability data returned by the API server is processed and stored in Manager database. This data is also updated in the memory cache maintained in the Manager.

The Manager uses SOAP/SSL channel to communicate with the API Server of Vulnerability Manager.

> On an average, the Scan engine takes 4 minutes to scan the endpoint for vulnerabilities.

The Scan engine scans the endpoint, and provides the vulnerability assessment data to Manager over a SOAP/SSL response. The vulnerability data is processed and stored in the Manager database. This data is also updated in the cache maintained in Threat Analyzer client.

For requesting an on-demand scan from Threat Analyzer, you need to configure Vulnerability Manager settings in the Manager client interface.

On-demand scan from Threat Analyzer

On Demand scan of Source or Destination IP address for alerts in the **Alerts** page, or for the IP address listed in the **Forensics** page, uses the Scan Configuration configured, or inherited from the parent admin domain level.

You can request a Vulnerability Manager on-demand scan on individual alerts from the right-click menu for an entry listed in the **All Alerts** page of the Threat Analyzer. Right-click the alert, and select **Start Vulnerability Scan** | **Scan Source IP** or **Start Vulnerability Scan** | **Scan Destination IP** option.

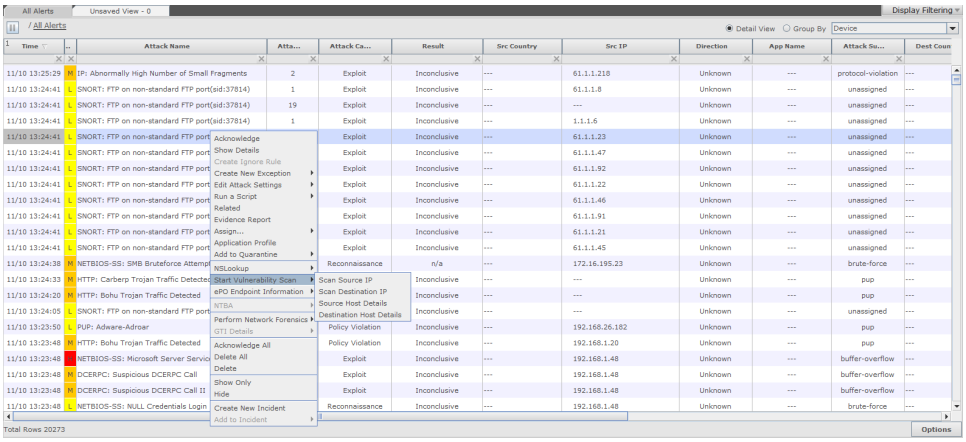


Figure 7-27 Start Vulnerability Scan option

When you select either option (**Scan Source IP** or **Scan Destination IP**), and the scan matches a scan added in the relevant admin domain in the Manager, a message pop-up indicating that the scan falls within the IP address range of a named scan added in the Manager and that this particular scan will be used.

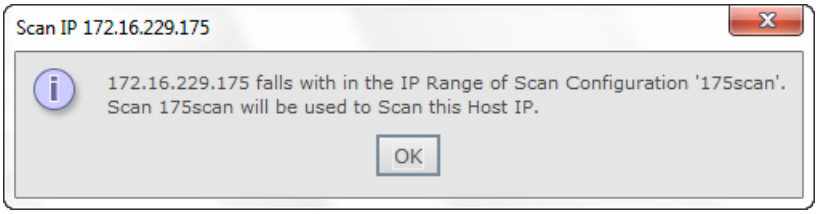


Figure 7-28 Scan fall message

When the IP address of the endpoint on which the scan is initiated does not fall within the range of any of the scans added to the Manager, a message pop-up indicates that a default scan will be used.

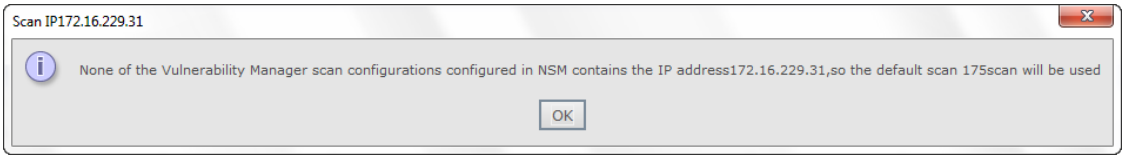


Figure 7-29 Default scan message

If you want to view the scan results, select **Yes** in the pop-up that follows. You are re-directed to the **Forensics** page.

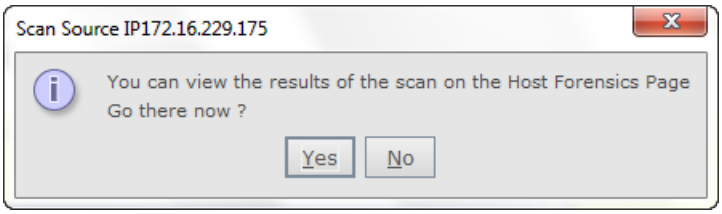


Figure 7-30 Message for viewing the scan results

See also

On-demand scan of endpoints on page 181
Configure Vulnerability Manager server settings on page 147

Vulnerability Manager scans

The **Forensics** page in Threat Analyzer indicates the progress of the Vulnerability Manager scans of alerts from the Threat Analyzer.

To view the list of all Vulnerability Manager scan processes in a domain, select **Forensics** from the Threat Analyzer, and select a domain from the drop-down. The **Vulnerability Scan Information** for the selected domain is displayed under **Summary** | **Vulnerability Scan Information**, as shown below.

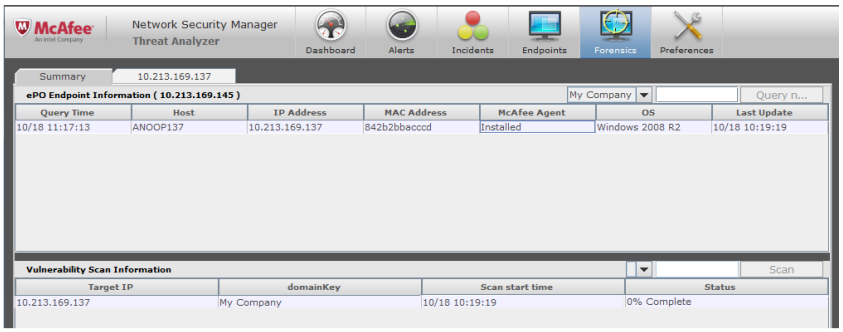


Figure 7-31 Vulnerability Scan Information area

Following information is displayed in the **Vulnerability Scan Information** section.

Field Name	Description
Target IP	The IP address of the endpoint which is scanned
domain key	The domain key name
Scan start time	Starting time of the Vulnerability Manager scan
Status	This field shows the status of completion of the Vulnerability Manager scans

Depending on the progress of the scan, **Status** field displays the following:

Status	Description
Queued	The Queued status indicates that requested Vulnerability Manager scans are queued.
%n Complete	The percentage of completion of the scan, where n ranges from 0 to 100.
Retrieved	This status indicates that the Vulnerability Manager scan is complete, and the endpoint vulnerability information is available to the user (to be viewed).
Failed	Vulnerability Manager scan has failed.
Scan TimedOut	If a scan takes more then 30 minutes, Manager cancels the scan by setting the status to Scan TimedOut.

Vulnerability Manager scan results displayed in the **Status** field are stored in the cache. Note that when Manager is restarted, the scan results are not seen in the **Status** field. In case, you want to view the scan results for the same endpoint, you need to scan the endpoint once again from the **Forensics** page.

When you select a domain in **Forensics** | **Summary** | **Vulnerability Scan Information**, you see the scans for that domain and for the domains that are set to Inherit from it. For example; if **FORD-Child1** domain has **HR1** and **HR2** as child domains, and these domains are set to **Inherit from parent domain** in the Manager, the **Forensics** page of **FORD-Child1** will show the scans of **FORD-Child1**, **HR1**, and **HR2**.

Vulnerability Manager scan information

- You can also scan an endpoint by entering the endpoint IP address in the **Scan** field in **Vulnerability Scan Information** section, and then clicking the **Scan** button.

The **Scan** button is enabled only when you completely fill in the IP address.

- All the domains in which Vulnerability Manager is configured are displayed in the drop down list. You can select the domain, enter the IP address and click **Scan** to start an on demand scan.

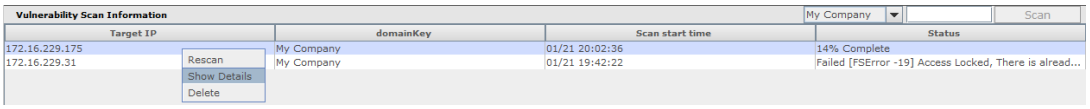


Figure 7-32 Show Details option

While initiating an on-demand scan, you need to select the admin domain in which you have already configured the intended scan. You also need to ensure that the IP address entered is part of the intended scan configuration. If this is not ensured, the default scan as per configuration in the Vulnerability Manager is used.

- If there are overlapping configurations for two scans from a single admin domain, you can choose the scan you want to apply. In this case a **Cancel** option is also given.
- If you want to see the detailed scan result for an endpoint that was scanned, select the required Scan entry from **Forensics** page, and right click on it to view the **Rescan**, **Show Details**, and **Delete** options.

Select **Show Details** option. Here the message pops up depending on two conditions:

- If the scan is in progress, a pop-up is displayed in the same screen, with the percentage level of completion (a value between 0 and 100).

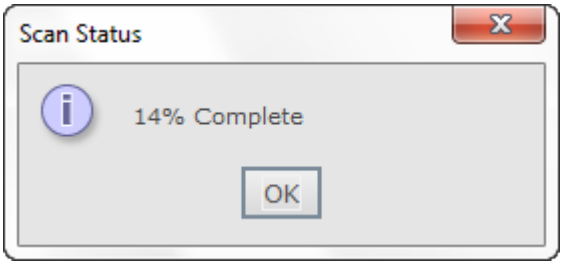


Figure 7-33 Popup message

- If the scan is complete and status is seen as **Retrieved**, if you right-click on the scan, and select **Show Details**, a new page under the sub tab **Vulnerability Information** (the main tab displays the IP address of the scanned endpoint) displays vulnerability information.

  The **Vulnerability Information** page displays details such as the *total number of vulnerabilities* found, *scan configuration* for the on-demand scan, and details of the *vulnerabilities* identified in the endpoint.

  By default, the vulnerabilities are sorted in the order of severity and are displayed in a tabular format. Each row in the table contains additional vulnerability details such as *severity*, *vulnerability name*, *vulnerability description*, *recommendation details* that lists the steps or patches that needs to be applied to the identified vulnerability, *CVE ID* and *IAVA (Information Assurance Vulnerability Alert) Reference Number*.

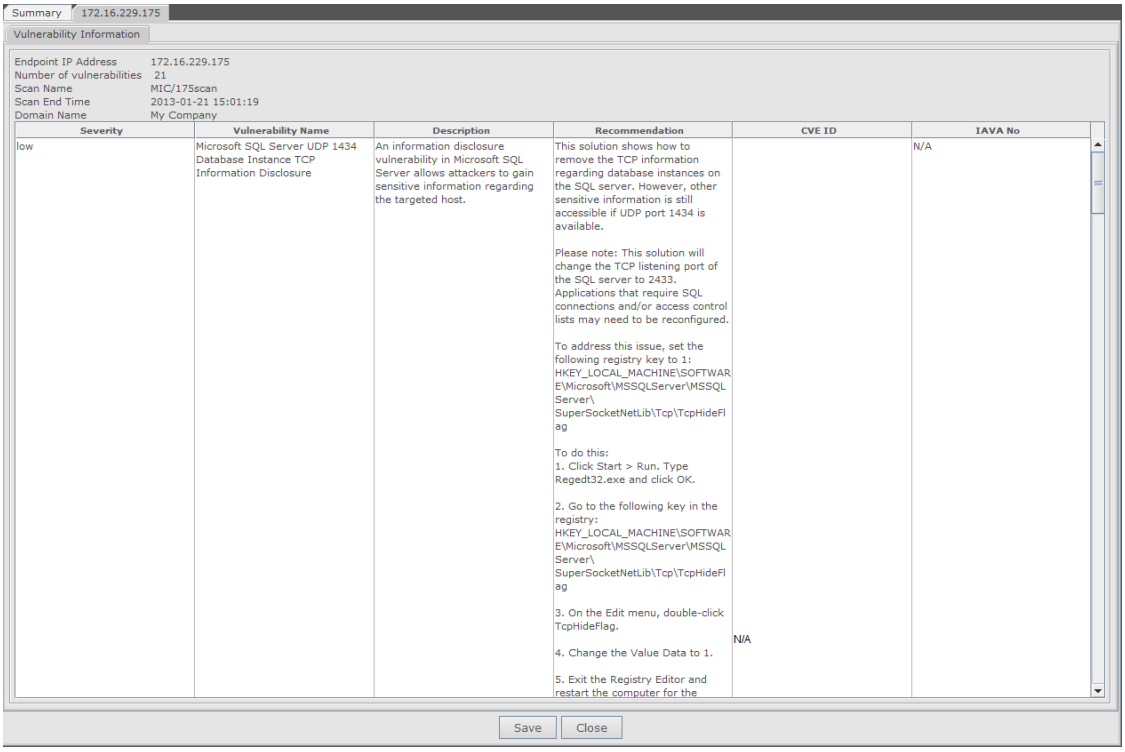


Figure 7-34 Vulnerability Information in Threat Analyzer

For a scanned endpoint, data on vulnerabilities (such as target IP address, CVE or BugTraq ID) is stored in the Manager database. Note that the information is not stored in the format for display in the **Vulnerability Information** page. So, when you restart Manager, this information is not seen in the **Vulnerability Information** page. You need to perform the scan again to view the information.

In the **Vulnerability Information** window, when you click on the CVE ID link for a vulnerability, you are re-directed to the CVE page (http://cve.mitre.org), as shown below.

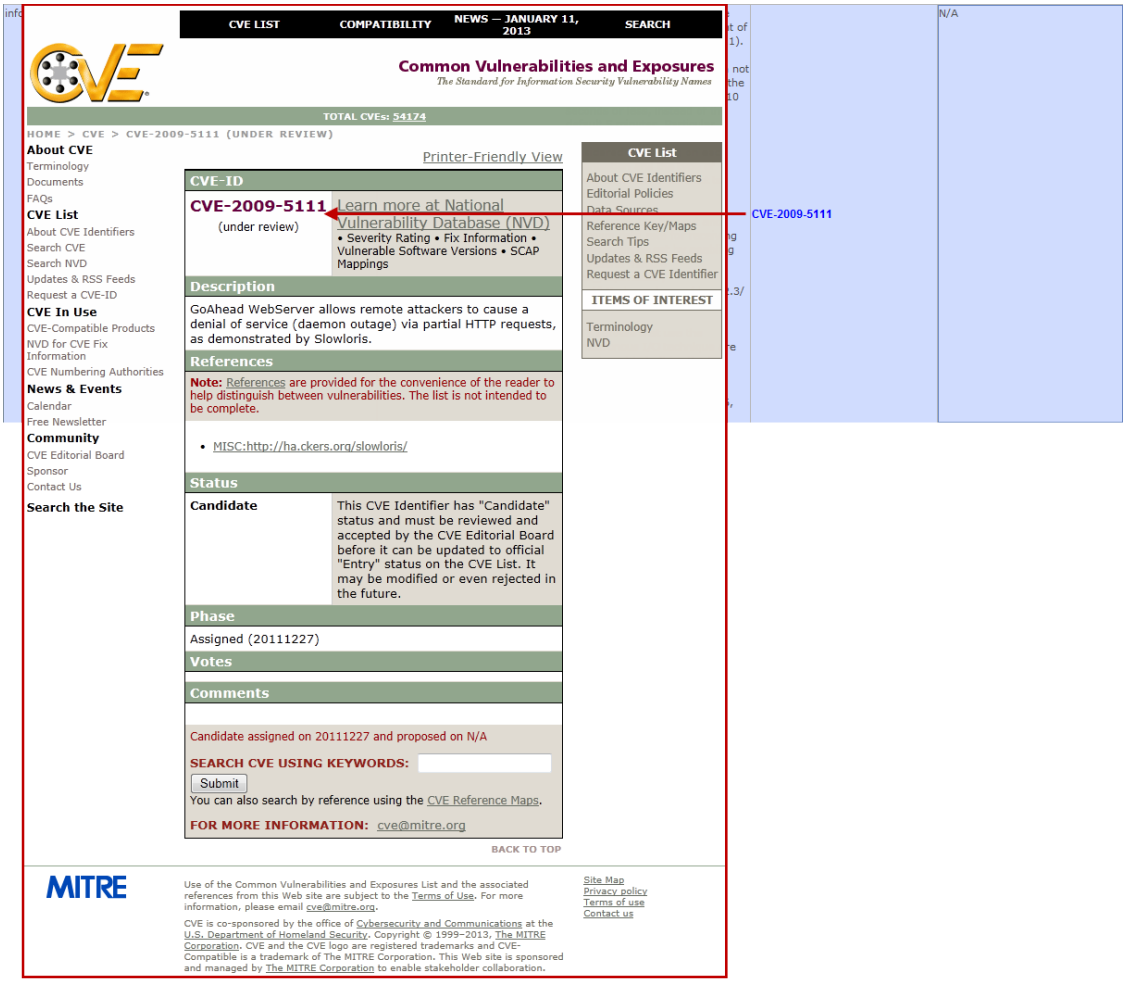


Figure 7-35 CVE page

You can also just double-click on any IP address scan listed in the **Vulnerability Scan Information** to view the Vulnerability Information for that IP address.

Endpoint rescan

You can *rescan* the endpoint which was once scanned by Vulnerability Manager. Right-click the scan in the **Vulnerability Scan Information** page, and select **Rescan**.

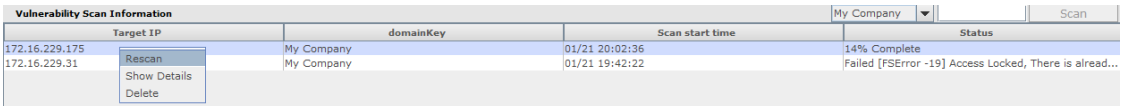


Figure 7-36 Rescan option

The endpoint will be scanned once again by Vulnerability Manager, and the vulnerability information is retrieved and displayed as before.

Concurrent scans

Threat Analyzer supports concurrent Vulnerability Manager scans.

The maximum poolsize (maxpoolsize) for concurrent scans is three.

Maxpoolsize represents total number of threads available in the ThreadPool. (ThreadPool is a component for working with pools of threads and asynchronously executing tasks.)

If scan requests exceed the maxpoolsize, they are queued, and processed depending on the free pool size.

> It is recommended to run a maximum of three concurrent Vulnerability Manager scans from the Manager, for optimal results.

See also

Concurrent scan of endpoints on page 181

Fault messages for Vulnerability Manager on-demand scan

The following table shows the fault messages associated with Vulnerability Manager on-demand scan:

Fault displayed	Severity	Description
On-demand scan failed because connection was refused to FoundScan engine	Critical	This fault can be due to two reasons- the user has not specified the Fully Qualified Domain Name OR the FoundScan engine is shutdown. For more information on using Fully Qualified Domain Name, see *Vulnerability Manager Installation*.

You can view the faults from the **System Health** menu in Manager.

When you click on the fault link, you can view the details of the fault and the possible actions to be taken to correct the fault. The fault detail for "on-demand scan failed" is shown below.

Perform Vulnerability Manager scans from the Endpoints page

You can request a Vulnerability Manager scan from **Endpoints** page.

Task

1. From the Threat Analyzer, select **Endpoints**. Right-click on an entry.
2. To initiate an on-demand scan of the selected IP address, select **Start Vulnerability Scan**.

   If the IP address does not fall under any of the defined scans in Manager, a message pop-up shows that the default scan configuration (defined in Manager) will be used to scan the IP address.
3. In the pop-up message, select **Yes** if you want to view the scan results. You are re-directed to the **Forensics** page.

Network scenarios for Vulnerability Manager scan

In this section, you can find network scenarios related to:

- On-demand scan of endpoints
- Concurrent scan of endpoints

On-demand scan of endpoints

While reviewing the alerts in **Real-time** or **Historical Threat Analyzer**, assume that you want to:

- View the current status of a particular endpoint listed in the list of alerts.
- Scan the particular endpoint using Vulnerability Manager, from the Threat Analyzer.
- Know the relevancy of the scanned alert/event.

This is possible by the on-demand scan functionality in the Threat Analyzer for individual alerts.

You can request for a Vulnerability Manager scan from the Threat Analyzer, by selecting either the Source IP address or the Destination IP address of the endpoint to be scanned. The status of the scan - whether the scan is relevant, is displayed in the Threat Analyzer.

You can maintain up to N number of scan information (N default is 100) in the Threat Analyzer.

See also

On-demand scan of endpoints listed in alerts in the Threat Analyzer on page 173

Concurrent scan of endpoints

When concurrent on-demand scan of many endpoints is initiated from the Threat Analyzer, you need to first define scan configuration in the Manager in order to get error free results.

Scenario

Consider the scenario, where you initiated the on-demand scan of three *endpoint IP addresses* concurrently from the **Vulnerability Scan Information** pane in the **Forensics** page of the Threat Analyzer. Assume that the endpoint IP addresses do not fall in the IP address ranges specified by any of the scan configurations defined in Manager. Further, you have **not** defined any scan configuration in Manager.

Scan process when scan configuration is not defined

In Vulnerability Manager, when you request for multiple on-demand scans, all the scans are executed with the default scan configuration and with the same name, that is, *QuickScan_<User Name>*. This is because, the same user name that you used to login to Vulnerability Manager gets associated with the three scan names. Since all the three scans have the same name, only one of the three concurrent scans is successfully completed. That is, Scan engine does not permit concurrent scans to be run with the same scan name.

Similar behavior can be seen if multiple on-demand scans are executed from the Threat Analyzer. All the scans executed from Threat Analyzer will have the same name *QuickScan_<User Name>*, For example, if you have logged into Vulnerability Manager as *admin*, then the scan configuration names for all the three endpoints will be *QuickScan_admin*.

In the scenario described above, when you initiate three concurrent on-demand scans without any scan configuration defined in Manager, Scan engine uses its default scan configuration for scanning the endpoints, with the default scan name "*QuickScan_<User Name>*". The three scans will have the same name, for the reason mentioned earlier. The first scan will be executed successfully, and the remaining two scans result in concurrent task exception. Therefore, using the Scan default scan configuration settings, you cannot run concurrent on-demand scans from Threat Analyzer.

Recommended solution

It is recommended that for concurrent scans, you should define at least one scan configuration in Scan engine and add the same to Manager. This scan configuration will be used as the default one. If more than one scan configuration is defined in Manager, you can change the default scan settings.

For more information on setting the default scan, see *Adding Vulnerability Manager scan configurations*.

When you have defined the default scan configuration in Manager as well as in Vulnerability Manager, and when the concurrent on-demand scans are requested, Manager will make use of the scan configuration ID and set a unique name for each endpoint that is scanned.

Manager creates scan name in the format Network Security Platform_<Actual Scan Name>_Thread-N where N=1,2,3,.. etc. Each scan configuration name will be different, for example, the scan names will be *Network Security Platform_<Actual Scan Name>_Thread-1*, *Network Security Platform_<Actual Scan Name>_Thread-2*, and *Network Security Platform_<Actual Scan Name>_Thread-3*. So, all the concurrent scans are successfully completed.

When any one scan in the execution pool completes its task, the next scan request waiting in queue for execution is pushed into the execution pool for execution. The scan requests are executed in order or First In First Out (FIFO).

Threads are created in the Manager depending upon the *threadpool size*. If the threadpool size is set to 3, three worker threads (Thread-1,Thread-2 and Thread-3) are created in the pool to service the scan requests. If the threadpool size is set to 3, and if more then 3 concurrent scans requests are sent to Scan engine, only 3 scans will be executed in the engine, and the rest of the scan requests are queued.

Before adding a scan to the Manager, you need to run the newly defined scan configuration at least once in the Scan engine. Each scan configuration defined in the Vulnerability Manager is associated with a Scan engine. When you run the scan configuration for the first time at the Vulnerability Manager side, the Scan engine in which the scan configuration is executed, gets associated with that scan configuration. This step is essential for successfully adding the scan configuration to Manager.

See also

Add Vulnerability Manager scan configurations on page 152
Concurrent scans on page 179

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 required 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** | **<Admin Domain Name>** | **Integration** | **Vulnerability Assessment** | **MVM** | **Alert Relevance** | **Troubleshooting** for performing this action from root or child admin domains.

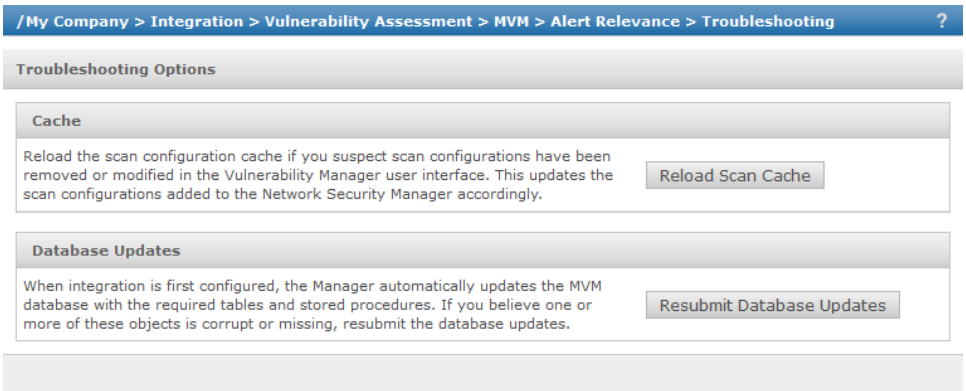


Figure 7-37 Troubleshooting Options area

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** | **<Admin Domain Name>** | **Integration** | **Vulnerability Assessment** | **MVM** | **Vulenrability Scanning** | **Troubleshooting** to perform this action from root or child admin domains.
- From Relevance settings— Select **Manager** | **<Admin Domain Name>** | **Integration** | **Vulnerability Assessment** | **MVM** | **Alert Relevance** | **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** | **<Admin Domain Name>** | **Integration** | **Vulnerability Assessment** | **MVM** | **Alert Relevance** | **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** | **<Admin Domain Name>** | **Integration** | **Vulnerability Assessment** | **MVM** | **Alert Relevance** | **Troubleshooting** for this purpose.

Select **Resubmit Database Updates** to resubmit the updates to the Vulnerability Manager database.

See also

Configure Vulnerability Manager database settings on page 145

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: 1 Download the software vcredist_x86.exe and run it in that host. 2 Download link http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=5638. 3 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. 1 Go to //windows/system32/sc.exe. 2 Right-click sc.exe and select **Properties**. 3 Click the **Security** tab. 4 Add a local service and provide full permission.

Problem	Solution
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 keys: • HKLM • HKLM\Software • HKLM\Software\Foundstone **3** Right-click on these keys and choose **Permissions**. **4** Add the user account used to run the Manager service (likely LOCAL SERVICE). **5** Give that user account Full Control over the key. **6** Click **OK**. Changes take effect immediately. A reboot is not required. **7** In the API Server page, click **Save**. If the operating system is 64-bit, perform this procedure for these keys: • HKLM • HKLM\Software • HKLM\Software\wow6432Node • HKLM\Software\wow6432Node\Foundstone.
You are able to start the FC Agent service, clicking on 'Retrieve MVM Certificate' returns error message.	It might be because port 3801 is not enabled in the API server. Check if port 3801 has been enabled. Vulnerability Manager could be deployed in distributed mode where FCM Server could be in one server. The API Server, DB , Enterprise Manager and Scan Engines could be 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\found stone or C:program Files(x86) \Foundstone" does not have write permission for Local Service. **1** Add local service and giving 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 or
- The certificate synchronization is still in progress or
- 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** | **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** | **run**, type `services.msc`, and click **OK**.
9. Start the **Foundstone Configuration Management Agent** service.

   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** | **<Admin Domain Name>** | **Integration** | **Vulnerability Assessment** | **MVM** | **Vulnerability Scanning** | **Summary**, and click **Run Configuration Wizard**.

       OR

       Select **Manager** | **<Admin Domain Name>** | **Integration** | **Vulnerability Assessment** | **MVM** | **Vulnerability Scanning** | **API server**.
    g. Click **Retrieve MVM Certificate**.

Failed to communicate with the API server

This error message is displayed for Vulnerability Scan Information.

8 Integration with McAfee Host Intrusion Prevention

McAfee® Network Security Platform integrates with McAfee® Host Intrusion Prevention version 8.0.

Host Intrusion Prevention is a Host-based intrusion prevention system, which prevents external and internal attacks on the hosts in the network, thus protecting services and applications running on them.

Host Intrusion Prevention is now completely integrated with McAfee ePO™ 5.9.1. The Manager uses an McAfee ePO™ extension file to obtain real-time Host Intrusion Prevention events from the McAfee ePO™ server. The extension file (NSPExtension.zip) needs to be downloaded from the Manager , and installed on the McAfee ePO™ server using McAfee ePO™ console. Once the extension file is installed on the McAfee ePO™ console, ensure that the Host Intrusion Prevention extension is also installed on the McAfee ePO™ server. You can use the **Download the ePO extension for the Network Security Manager here** link in the **Enable** page (**Manager** | **<Admin Domain Name>** | **Integration** | **HIP** | **Enable**) to download the (NSPExtension.zip) extension.

Within the Manager's context, the Host Intrusion Prevention integration functions like a Sensor. In other words, Manager treats the McAfee ePO™ server running the server portion of the Host Intrusion Prevention software as a special type of Sensor. That is, the Manager receives the events information from Host Intrusion Prevention, incorporates these events into its database and provides these events for further viewing/actions in the Attack Log and reports, like any other Network Security Platform alert.

Configure the Host Intrusion Prevention Sensor in the Manager by providing a name and a shared secret key. You need to then configure that Manager's IP address and the shared secret on the McAfee ePO™ server console as well. Once trust is established, the Host Intrusion Prevention Sensor is displayed in the **Device** drop-down list of the Manager . You can use the **Add a virtual Host Intrusion Prevention sensor here** link in the **Enable** page (**Manager** | **<Admin Domain Name>** | **Integration** | **HIP** | **Enable**) to begin the process of configuring the Host Intrusion Prevention Sensor in the Manager .

The Host Intrusion Prevention events are displayed in the Attack Log. You can view the alerts by filtering the Host Intrusion Prevention device in the **Device** column of the Attack Log page.

Only Host Intrusion Prevention IPS events are sent to the Manager.

Quarantine is not applicable to Host Intrusion Prevention events in the Attack Log.

In case of MDR pair, alerts are sent to both the active and the standby Manager .

Contents

- *Configure Host Intrusion Prevention details*
- *Add a Host Intrusion Prevention Sensor*
- *Configure the Host Intrusion Prevention Sensor in McAfee ePO™*

Configure Host Intrusion Prevention details

You can integrate the Manager with Host Intrusion Prevention. To do so, perform the following steps.

Task

1. In the Manager navigate to **Manager** | **<Admin Domain Name>** | **Integration** | **HIP**.

   The **Enable** page appears.

2. Click **Download the ePO extension for the Network Security Manager here** link.

   A dialog box appears prompting you to confirm whether you want to Open or Save **NSPExtension.zip**

3. Save the **NSPExtension.zip** to a location for future use.

4. Logon to McAfee ePO™ console.

5. Navigate to **Menu** | **Software** | **Extensions**.

   The **ePolicy Orchestrator** page appears.

6. Click **Install Extension**.

   The **Install Extension** dialog-box appears.

7. Browse and select the McAfee ePO™ extension file from the location mentioned in step 4.

   Once installed, the Manager is listed under the **Settings Categories** list.

8. Verify on the McAfee ePO™ console that the Host Intrusion Prevention extension is installed.

Add a Host Intrusion Prevention Sensor

Installation of a Host Intrusion Prevention Sensor is similar to adding a Sensor.

Task

1 Select **Devices** | **<Admin Domain Name>** | **Global** | **Add and Remove Devices**.

2 Click **New**.

The **Add New Device** area is displayed.

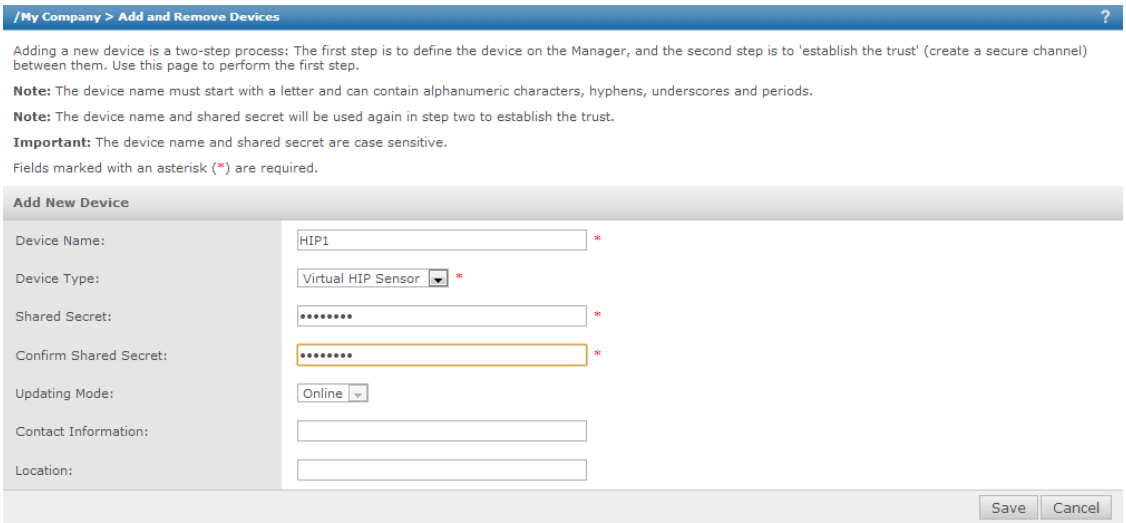


Figure 8-1 Add New Device area

3 Type a unique name at **Device Name** to identify the Host Intrusion Prevention Management Server in the Manager. The name can contain up to 25 alphanumeric (upper or lower case letters and numbers) characters, including hyphens, underscores, and periods. The name must begin with a letter.

4 Select the **Device Type** as **Virtual HIP Sensor** .

5 Type a password at **Shared Secret** for verifying the Manager -Host Intrusion Prevention communication. The shared secret must be a minimum of 8 characters in length and can contain up to 25 alphanumeric (upper or lower case letters and numbers) characters, including hyphens, underscores, and periods. The secret cannot start with an exclamation mark nor have any spaces.

> The exact, case-sensitive **Device Name** and **Shared Secret** must also be entered on the ePO console for Host Intrusion Prevention integration.

6 (Optional) Type the **Contact Information** and **Location**.

7 Click **Save** to begin the Manager -ePO server handshake process.

> You need to configure the Host Intrusion Prevention Sensor details on the ePO console as well to establish trust.

Once trust is established, the Host Intrusion Prevention Sensor is displayed in the **Device** drop-down list and the **Add and Remove Devices** page.

Configure the Host Intrusion Prevention Sensor in McAfee ePO™

To configure a Host Intrusion Prevention Sensor on the McAfee ePO™ server and establish trust between the Manager and McAfee ePO™, perform the following steps:

Task

1 Logon to McAfee ePO™ console.

McAfee ePO™ console Home page is displayed.

2 Select **Menu** | **Configuration** | **Server Settings**.

3 Browse and select **NSP & HIP Integration**.

4 Click **Edit**.

> You need to stop the Scheduler before editing existing settings.

The **Edit NSP & HIP Integration** page is displayed.

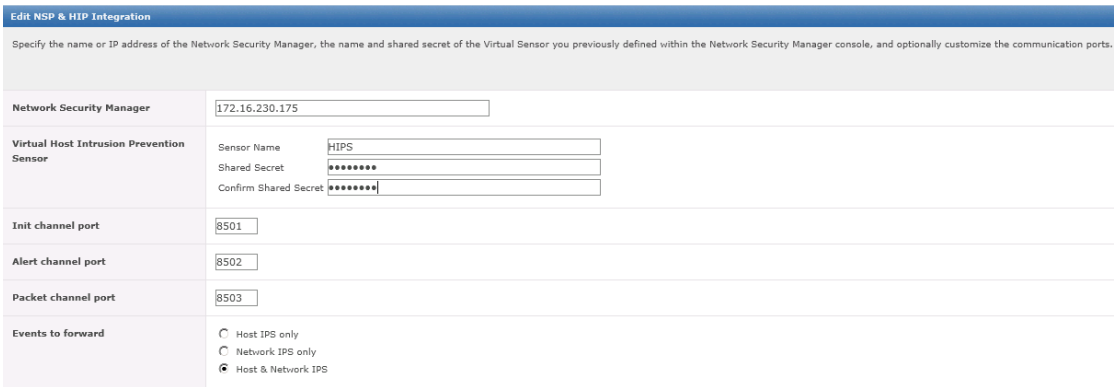


Figure 8-2 Edit NSP & HIP Integration page

5 Enter the following to configure:

Field	Description
Manager IP	The IP address of the Manager server on which the Host Intrusion Prevention Sensor is to be configured.
Sensor Name	Name of the Sensor
Shared Secret	The shared secret key that must match with the shared secret entered in the Manager
Confirm Shared Secret	Confirmation of the shared secret key.
Init channel port	The port the Manager uses to exchange configuration information with the Sensor.
Alert channel port	The port on which the Manager listens for Sensor alerts.
Packet channel port	The port the Manager uses for sending the signature ID mapping information.

6 Click **Save** to save changes and return to the previous page.

9 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.

Contents

- *Benefits*
- *Integration requirements*
- *Download the software*
- *How Network Security Platform - Logon Collector integration works*
- *Configuration details for Logon Collector integration*
- *Display of Logon Collector details*
- *Display of Logon Collector details in Network Security Manager reports*
- *Communication error*

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**— 7.1.5.14 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

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.

Task

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.

   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.

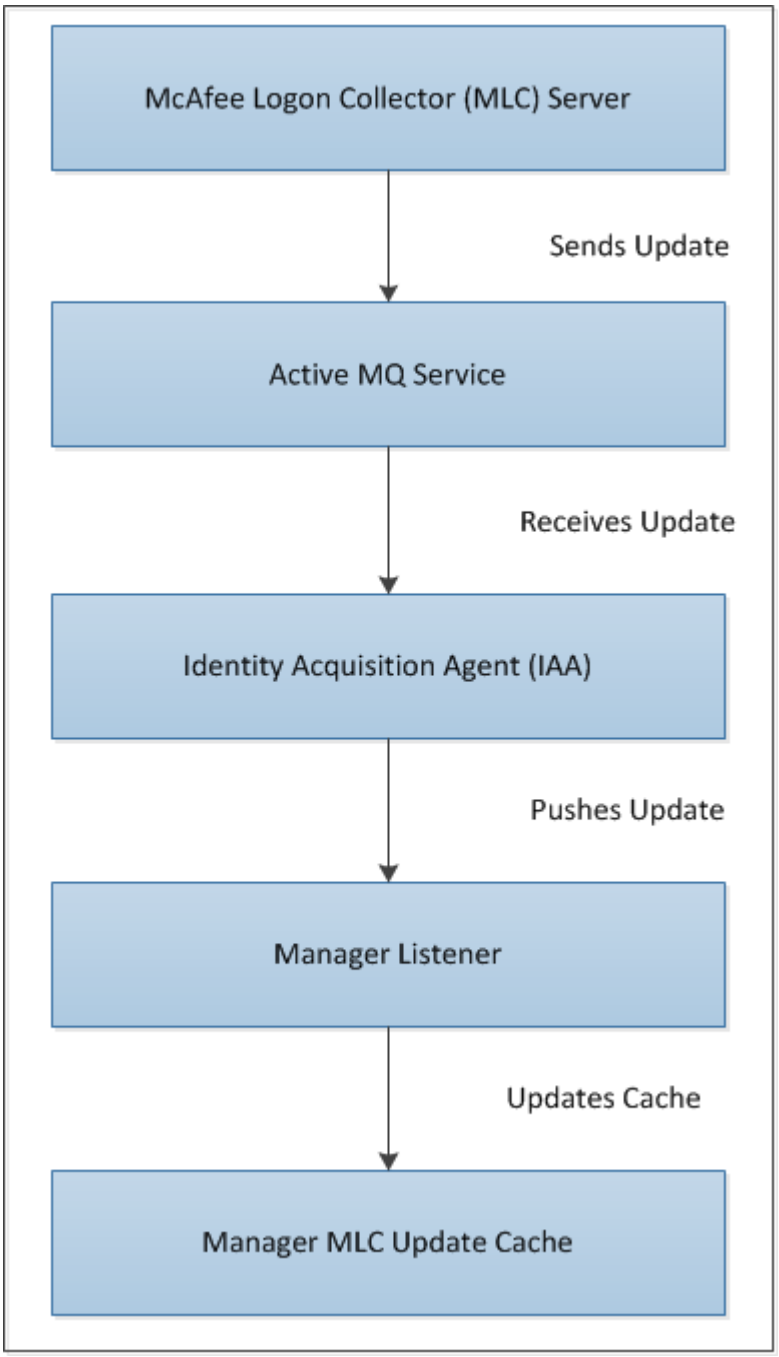


Figure 9-1 Manager-Logon Collector integration

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.

Task

1 Navigate to **Manager** | **<Admin Domain Name>** | **Integration** | **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.

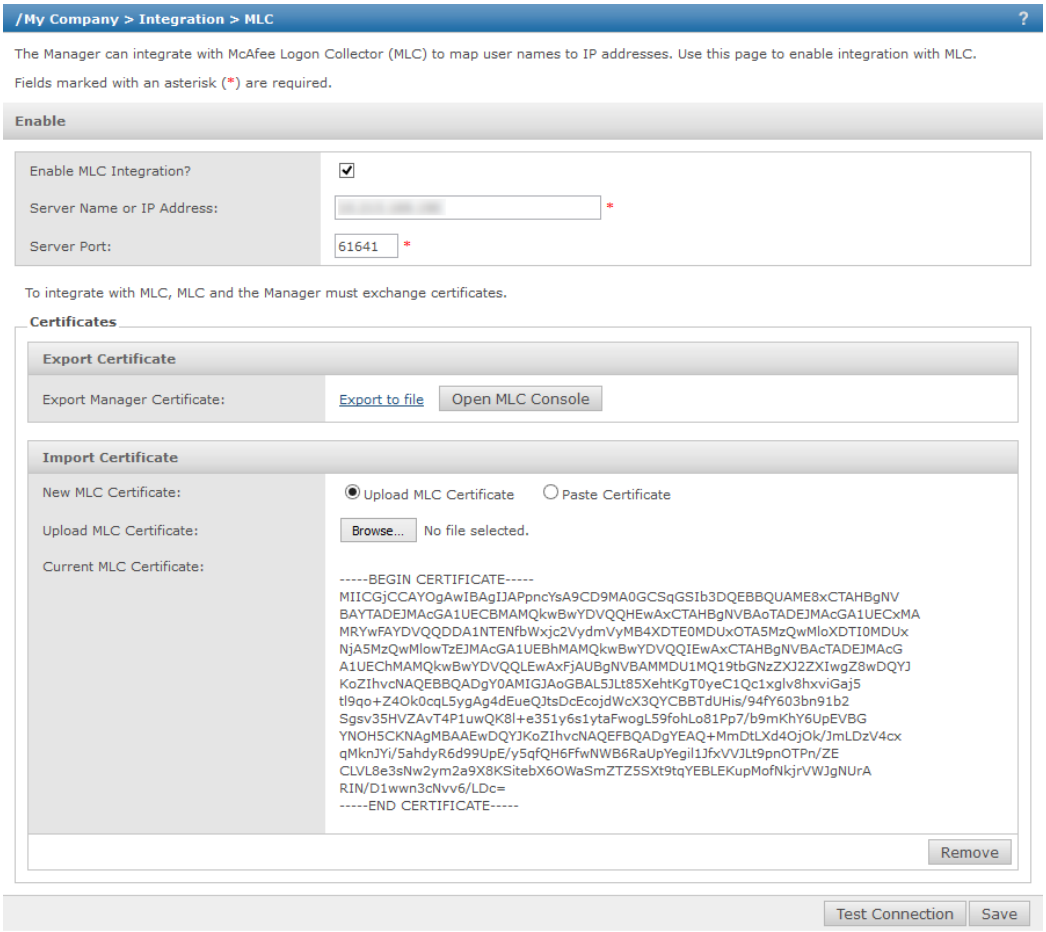


Figure 9-2 Enable Logon Collector

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 Manager* documentation for exporting the Manager certificate.

Task

1 In the Logon Collector console, select **Menu** | **Configuration** | **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** | **Configuration** | **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.

If the existing Logon Collector certificate is changed, the clients connecting to Logon Collector like Firewall Enterprise, 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 Manager documentation for details.

Display of Logon Collector details in the Threat Analyzer — Dashboards page

You can assign monitors based on the source and destination users while creating a new dashboard. The following monitors are added:

- Top 10 Attack Destination Users
- Top 10 Attack Source Users

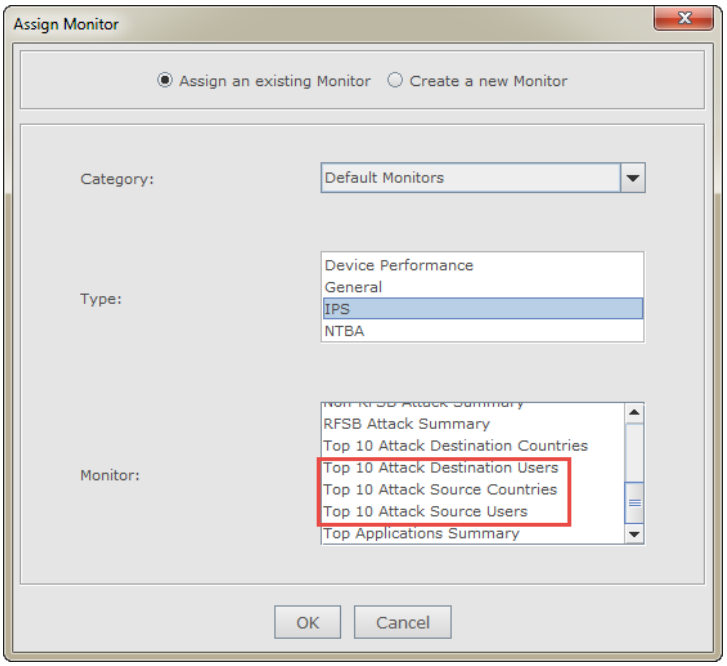


Figure 9-3 Assign Monitor window

Display of user information in NTBA monitors

The **Dashboards** page of the Threat Analyzer now displays the user names along with the Endpoint IP addresses in NTBA monitors.

The following NTBA monitors display the user names in the **User Name** column.

- Endpoints - Threat Factor
- Traffic Volume (Bytes) - Top Source Endpoints
- Top External Endpoints By Reputation
- Endpoints - New

The **User name** section is displayed as "---" when no user name is received from the Logon Collector server for that particular endpoint IP address.

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.

Task

1 Navigate to **Analysis** | **<Admin Domain Name>** | **Attack Log**.

2 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.

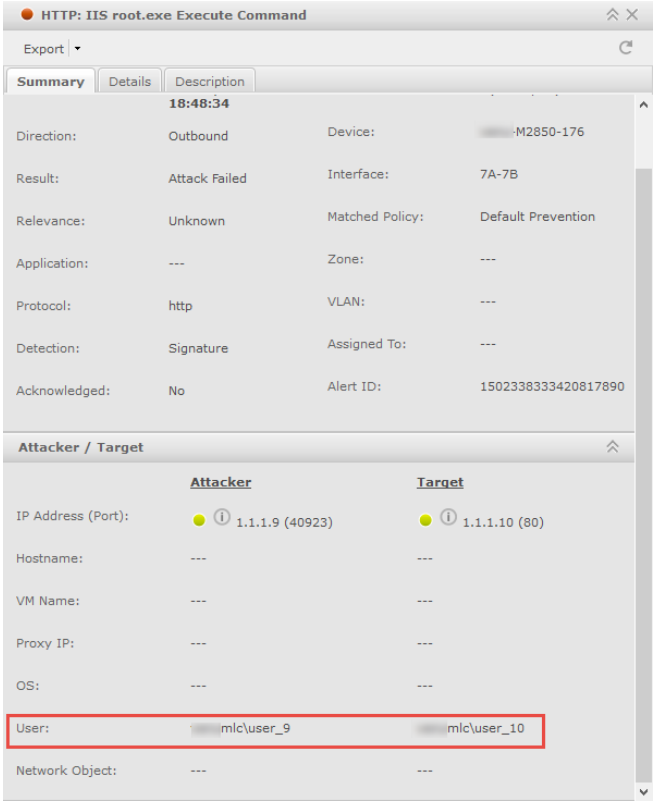


Figure 9-4 User details in Attack Log

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** | **Event Reporting** | **Next Generation Reports** | **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.

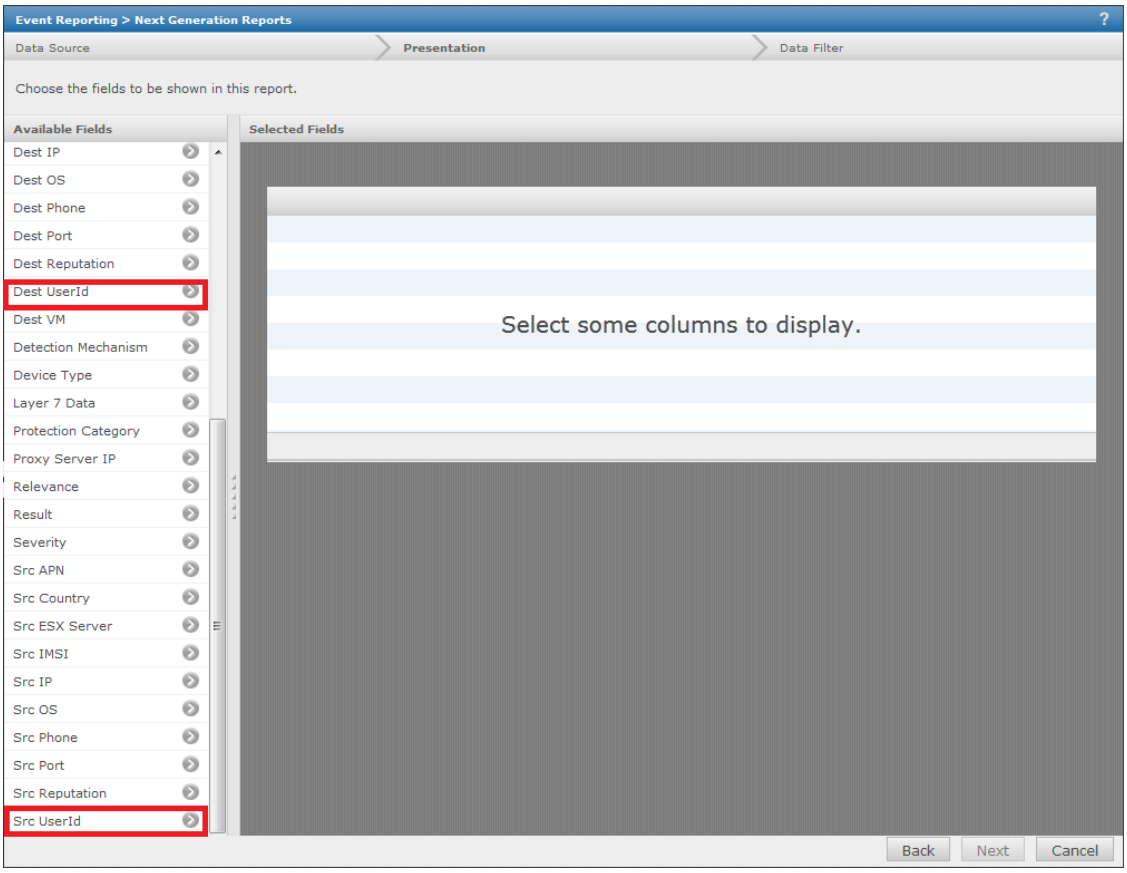


Figure 9-5 Table properties — Src UserId and Dest UserId fields

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.

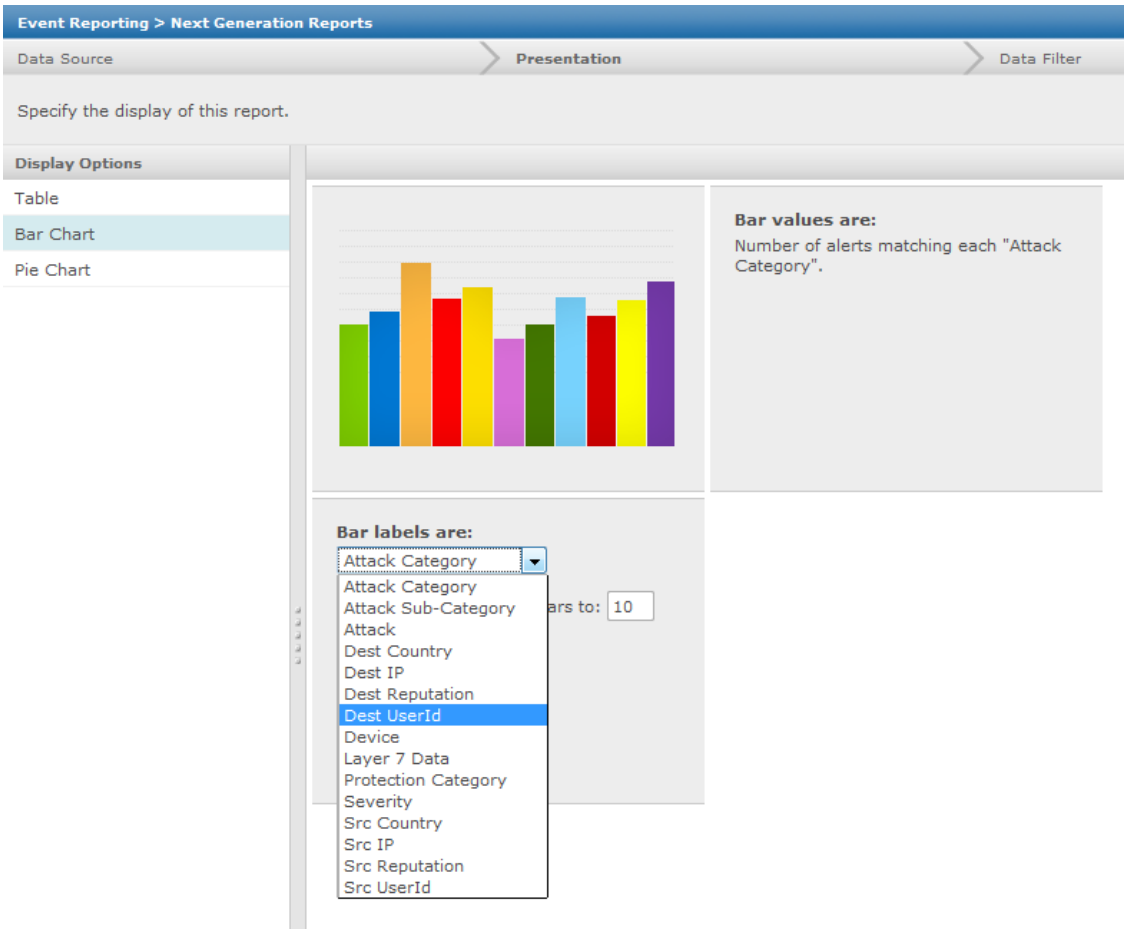


Figure 9-6 Src UserId and Dest UserId fields options in the bar chart

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.

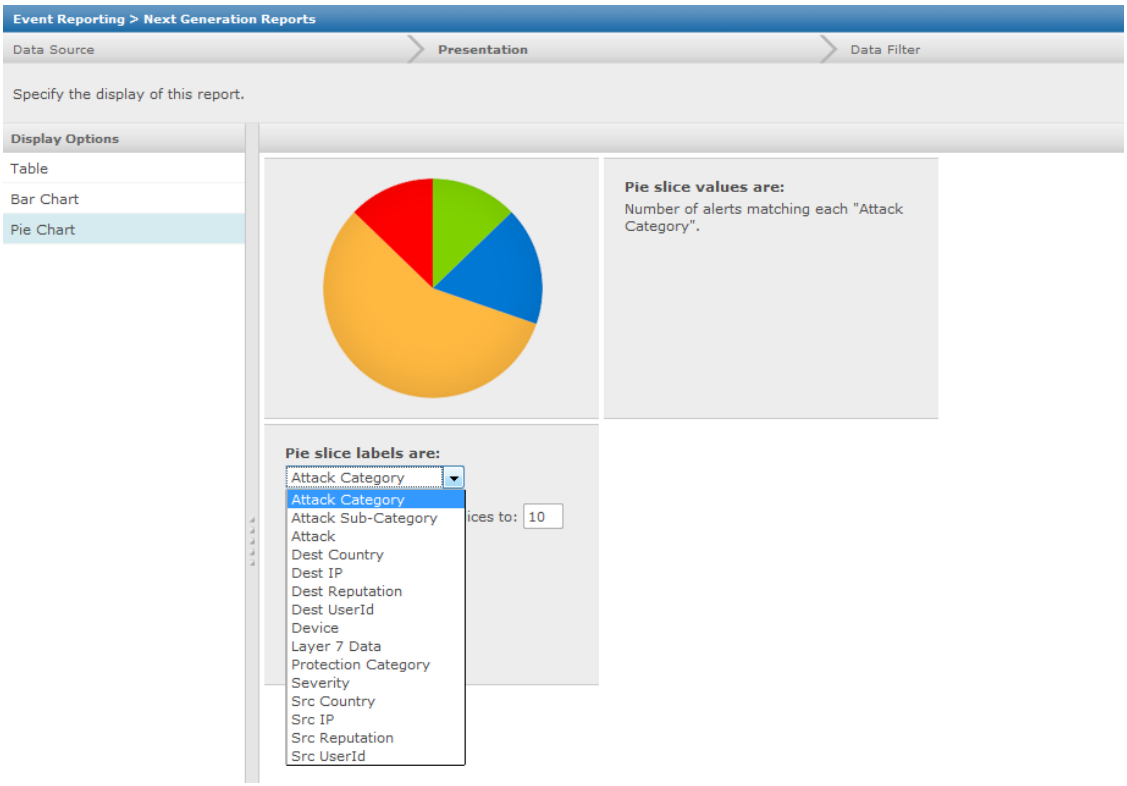


Figure 9-7 Src UserId and Dest UserId fields options in the pie chart

Communication error

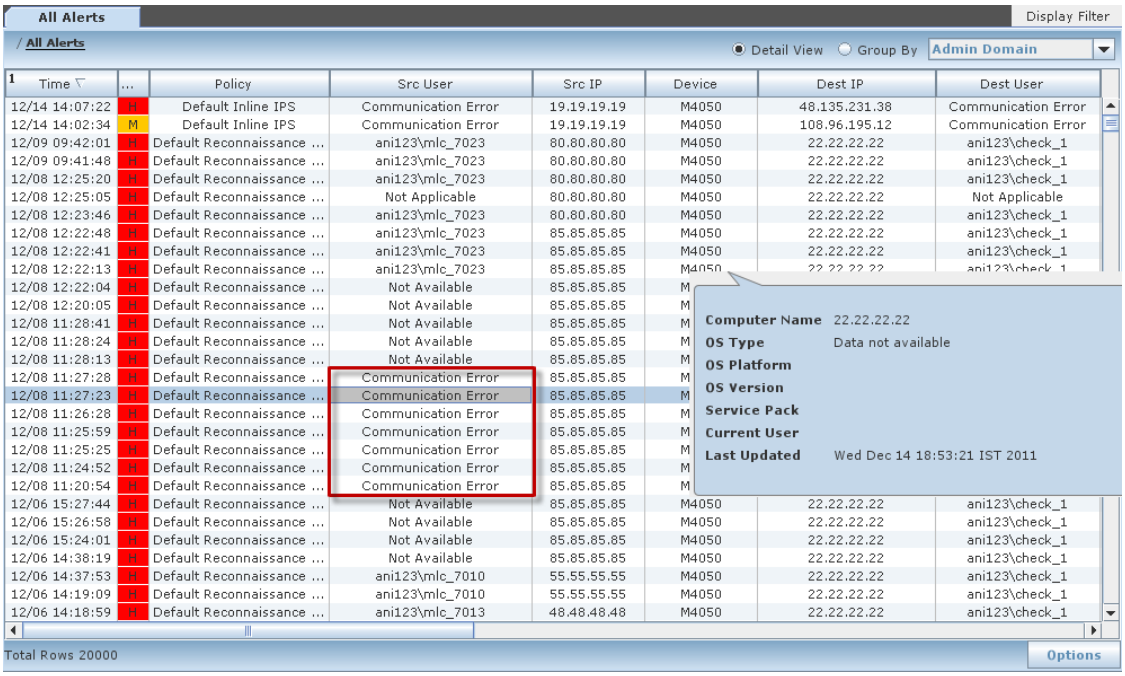
A connection error report is shown in the **Status** window of McAfee® Network Security Manager when there is an improper communication between the McAfee® Network Security Manager server and Logon Collector server. From the McAfee® Network Security Manager **Home** page, go to **System Health**. Click **Error** to display the error message.

Figure 9-8 Error on Dashboard page

You can also view the communication error message alerts in the Attack Log page for an improper connection.

The following details are displayed under the **Src User** column:

- **Communication Error** — Error in communication with the Logon Collector server
- **Not Applicable** — Improper mapping



Time	...	Policy	Src User	Src IP	Device	Dest IP	Dest User
12/14 14:07:22	H	Default Inline IPS	Communication Error	19.19.19.19	M4050	48.135.231.38	Communication Error
12/14 14:02:34	M	Default Inline IPS	Communication Error	19.19.19.19	M4050	108.96.195.12	Communication Error
12/09 09:42:01	H	Default Reconnaissance ...	ani123\mlc_7023	80.80.80.80	M4050	22.22.22.22	ani123\check_1
12/09 09:41:48	H	Default Reconnaissance ...	ani123\mlc_7023	80.80.80.80	M4050	22.22.22.22	ani123\check_1
12/08 12:25:20	H	Default Reconnaissance ...	ani123\mlc_7023	80.80.80.80	M4050	22.22.22.22	ani123\check_1
12/08 12:25:05	H	Default Reconnaissance ...	Not Applicable	80.80.80.80	M4050	22.22.22.22	Not Applicable
12/08 12:23:46	H	Default Reconnaissance ...	ani123\mlc_7023	80.80.80.80	M4050	22.22.22.22	ani123\check_1
12/08 12:22:48	H	Default Reconnaissance ...	ani123\mlc_7023	85.85.85.85	M4050	22.22.22.22	ani123\check_1
12/08 12:22:41	H	Default Reconnaissance ...	ani123\mlc_7023	85.85.85.85	M4050	22.22.22.22	ani123\check_1
12/08 12:22:13	H	Default Reconnaissance ...	ani123\mlc_7023	85.85.85.85	M4050	22.22.22.22	ani123\check_1
12/08 12:22:04	H	Default Reconnaissance ...	Not Available	85.85.85.85	M		
12/08 12:20:05	H	Default Reconnaissance ...	Not Available	85.85.85.85	M		
12/08 11:28:41	H	Default Reconnaissance ...	Not Available	85.85.85.85	M		
12/08 11:28:24	H	Default Reconnaissance ...	Not Available	85.85.85.85	M		
12/08 11:28:13	H	Default Reconnaissance ...	Not Available	85.85.85.85	M		
12/08 11:27:28	H	Default Reconnaissance ...	Communication Error	85.85.85.85	M		
12/08 11:27:23	H	Default Reconnaissance ...	Communication Error	85.85.85.85	M		
12/08 11:26:28	H	Default Reconnaissance ...	Communication Error	85.85.85.85	M		
12/08 11:25:59	H	Default Reconnaissance ...	Communication Error	85.85.85.85	M		
12/08 11:25:25	H	Default Reconnaissance ...	Communication Error	85.85.85.85	M		
12/08 11:24:52	H	Default Reconnaissance ...	Communication Error	85.85.85.85	M		
12/08 11:20:54	H	Default Reconnaissance ...	Communication Error	85.85.85.85	M		
12/06 15:27:44	H	Default Reconnaissance ...	Not Available	85.85.85.85	M4050	22.22.22.22	ani123\check_1
12/06 15:26:58	H	Default Reconnaissance ...	Not Available	85.85.85.85	M4050	22.22.22.22	ani123\check_1
12/06 15:24:01	H	Default Reconnaissance ...	Not Available	85.85.85.85	M4050	22.22.22.22	ani123\check_1
12/06 14:38:19	H	Default Reconnaissance ...	Not Available	85.85.85.85	M4050	22.22.22.22	ani123\check_1
12/06 14:37:53	H	Default Reconnaissance ...	ani123\mlc_7010	55.55.55.55	M4050	22.22.22.22	ani123\check_1
12/06 14:19:09	H	Default Reconnaissance ...	ani123\mlc_7010	55.55.55.55	M4050	22.22.22.22	ani123\check_1
12/06 14:18:59	H	Default Reconnaissance ...	ani123\mlc_7013	48.48.48.48	M4050	22.22.22.22	ani123\check_1

Figure 9-9 Communication error in the Threat Analyzer

10 Integration with OSC

OSC is a centralized platform to enable software-defined security for software-defined datacenters (SDDC). OSC provides a common set of management services, acting as a broker between the security solutions and the virtual infrastructure. You can use OSC to provide services such as next-generation IPS and firewall to virtual infrastructures.

OSC integrates with a hypervisor and an networking provider to provide security solutions as a service to your virtual networks. Using Intel Security Controller as a liaison between the security service and its associated components, and the virtualization providers, you are able to provide security services for virtual networks. Currently, you are able to integrate with:

- McAfee® Network Security Platform (Network Security Platform)
- McAfee® Next Generation Firewall (McAfee NGFW)

To illustrate this, consider a virtual environment that uses VMware vCenter as its hypervisor and VMware NSX as its SDN controller to deploy security services on virtual infrastructure.

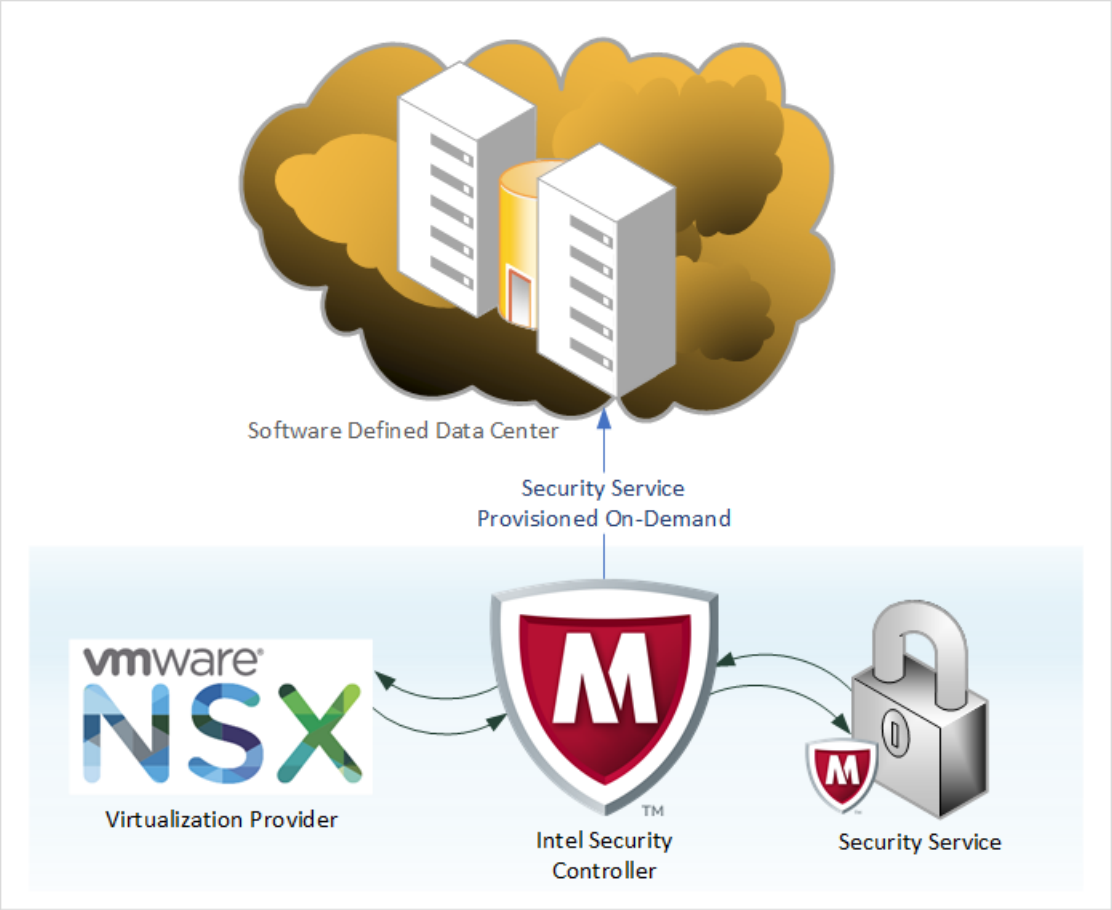


Figure 10-1 OSC solution overview

OSC is a virtual appliance that you install on an ESXi host. It provides a Java-based web application for configuration and management. You can deploy OSC on existing virtual infrastructure without any configuration changes to those virtual networks.

Contents

- *Security challenges in an SDDC*
- *Deploying next-generation IPS service to virtual networks*

Security challenges in an SDDC

Consider a large-scale SDDC consisting of hundreds of hosts aggregated under multiple clusters. Virtualization provides flexibility and agility to its users, wherein they can spin up virtual machines (VMs). Users can spin up isolated logical networks as easily as one can spin up VMs. All these possibilities require no changes in the physical networking configuration. When multiple users spin up new networks and move working VMs across physical boxes in such a large-scale data center, security is threatened.

To match with the capabilities of virtualization solutions, OSC can seamlessly, non-intrusively, and non-disruptively integrate security services with existing virtualized environments. This enables network security services to keep pace with the speed, agility, and scalability of virtualization features and solutions.

Deploying next-generation IPS service to virtual networks

If your Manager version is later than 8.2.7.5, you can integrate Network Security Platform with OSC to provide next-generation IPS service to virtual networks. When you deploy IPS service, OSC collaborates with Network Security Platform and VMware NSX such that a special type of virtual IPS Sensor is installed in each protected hypervisor. These virtual Sensors in each hypervisor provide IPS service to the corresponding VMs. In the Manager and OSC, the container object of these virtual Sensors are referred to as virtual security system or virtual system. In the hypervisors, these virtual Sensors are installed as ESX agents.

You can use Network Security Manager to manage the instances of virtual security systems. The virtual security system instances are configured similarly but function independently. That is, the virtual security system instances provide IPS to their respective hypervisors but implement the same IPS policy, advanced firewall policy, and other IPS configuration.

To deploy a virtual security system, OSC integrates with NSX. This integration also ensures that the relevant traffic is routed through the virtual security system instance for inspection.

The IPS service makes available the relevant next-generation IPS features for your dynamic virtual networks. Deploying the IPS service is non-intrusive and non-disruptive even though the virtual Sensors are deployed in inline mode only. Scaling up or modifying your virtual networks do not warrant any kind user-intervention to your IPS service deployment. Also, any changes to the IPS configuration is automatically applied to all the virtual Sensors. OSC does not take any action directly but orchestrates the actions by its integration with NSX, vCenter, Manager, and the virtual security system instances.

- Refer to the latest *Network Security Platform IPS Administration Guide* or *OSC Product Guide* for the following information:
  - An overview of OSC and how it collaborates with McAfee Network Security Platform and NSX to provide IPS service to SDDCs.
  - Detailed procedures to deploy next-generation IPS for virtual networks using OSC.

    To deploy IPS service to SDDCs, you configure OSC, Manager, and NSX. To configure NSX, you need vCenter web client.
- For information on how to install and set up OSC virtual appliance, see the latest *OSC Product Guide*.
- For information on installing and configuring VMware NSX, refer to VMware documentation.
- For information on installing and configuring the virtual infrastructure, refer to the corresponding documentation. For example, for VMware virtual infrastructure, refer to VMware documentation.

11 Integration with HP Network Automation

McAfee® Network Security Platform 6.0 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 containing 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 who 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** | **<Admin Domain Name>** | **Integration** | **HP Network Automation.**

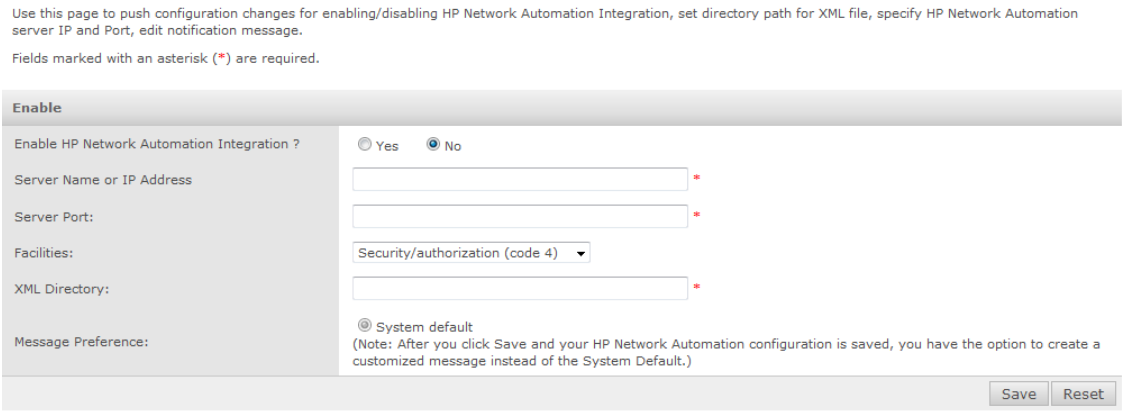


Figure 11-1 Enable page

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 6 (local6)** • **Local user 7 (local7)**
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.

12 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
- NetIQ
- Network Intelligence
- QRADAR from Q1Labs
- Sequation
- Symantec Remote Importer
- Tenable Networks

Contents

- *Manager data available for SIEM products*
- *Methods of integration with SIEM products*
- *Configure notification methods*
- *Templates for syslog, email, and pager*
- *Integration for fault information*
- *Integration using reports*
- *Data mining*
- *IV_ALERT_DATA decoding*
- *Information on database queries*
- *Alert synchronization in an MDR deployment*
- *Create PCAP format packet logs*

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** | **<Admin Domain Name>** | **Setup** | **Notification** | **Faults** | **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	Running scripts from the Threat Analyzer	Report
Alert data	Yes	Yes	Yes	Yes	Yes	Yes
Packet Log data	No	No	No	Yes	No	No
System fault	Yes	Yes	Yes	Yes	No	Yes
ACL	No	Yes	No	No	No	No
Audit	No	Yes	No	Yes	No	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 per-attack 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** | **<Admin Domain Name>** | **Setup** | **Notification** | **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** | **<Admin Domain Name>** | **Intrusion Prevention** | **Policy Types** | **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**.

6 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, then 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.

“%” "/” 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 confidence means the lower 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.
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 targetted 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 signagure, threshold, statistical anomaly, and flow corelation.
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 targetted 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 targetted VMware host for the attack.
TARGET_VM_ESX_NAME	The VMware ESX server that hosts the targetted VMware.
URI_INFO	Not applicable to Sensors running on 7.1 software. The URI found in the attack traffic.
VLAN_ID	The VLAN tagged with the attack traffic.
DEST_APN	Applicable only to attacks targetted at data-enabled mobile equipments such as a mobile phone or a tablet PC. The Access Point Name (APN) of the targetted mobile equipment.
DEST_IMSI	Applicable only to attacks targetted at data-enabled mobile equipments such as a mobile phone or a tablet PC. The International Mobile Subscriber Identity (IMSI) of the targetted mobile equipment.
DEST_PHONE_NUMBER	Applicable only to attacks targetted at data-enabled mobile equipments such as a mobile phone or a tablet PC. The phone number of the targetted 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. 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.
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.
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 then it is recommended that you customize the notification that suits your needs.

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 If you are using SNMPv3 then 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 • Communication port number • Syslog facility 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 *McAfee Network Security Platform IPS Administration Guide*. 2 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. 3 To forward ACL rule matches to a syslog server, configure the syslog details in the Manager. See *McAfee Network Security Platform IPS Administration Guide.* 4 To forward user-activity details of the Manager server to a syslog, configure the details at **Manager** | **<Admin Domain Name>** | **Setup** | **Notification** | **User Activity** | **Syslog**. See the Manager's Help for the steps.

Method	Information
Email and pager	You can configure the Manager to do the following: • 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 *McAfee Network Security Platform Manager Administration Guide* for the details. **2** To enable e-mail notification only for specific attacks, edit those attacks in the relevant policies. See *McAfee Network Security Platform IPS Administration Guide.* **3** For alert notification through email or pager, configure the email notification and the email recipients in the Manager. See *McAfee Network Security Platform IPS Administration Guide.* . **4** 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. **5** To enable the Manager to email auto-generated reports, configure the recipients in the General Settings of the Reports module. See *McAfee Network Security Platform Manager Administration Guide.*
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, see Specifying script parameters, *McAfee Network Security Platform IPS Administration Guide.* . Also see the Readme.doc at `<Manager installed directory>\McAfee\Network Security Manager\App\diag\AlertNotificationScript`.
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.

Running scripts from the Threat Analyzer

You can store custom scripts in the Manager server or locally in a Manager client. The Manager does not trigger these scripts, but you can trigger them per alert from the Threat Analyzer. This feature is useful when you want to respond to an attack using a custom script from the Threat Analyzer. For example you can write a script to modify router ACL using IP address found in the alert information. Similarly, you can also invoke a script that disables switch port of the source host of an attack.

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 Manager Administration 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. That is, 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 that are more ad-hoc in nature such as reports, 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 Manager Administration Guide* for details about these features.

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	Type	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	Type	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.
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 VIDS belongs, and the earlier ones being its parents going back to the root admin domain ID. Alerts for the root subscriber will have all these columns as NULL.
subscriberId2	int(11)	YES			
subscriberId3	int(11)	YES			
subscriberId4	int(11)	YES			
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.
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 this 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.

Field	Type	Null	Key	Default value	Description/Comments
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.
lastByteReqStreamOffset	int(11)	YES			For alerts that have previous-256-byte fragments, the offset of the last byte in that packet in the request streams.
lastByteRespStreamOffset	int(11)	YES			For alerts that have previous-256-byte fragments, the offset of the last byte in that packet in the response streams.
hasPreviousBuffer	char(1)	YES			Whether a previous-256-byte fragment was sent.
signatureId	smallint(6)	YES			The signature ID within the attack ID.
ivProtocolId	int(11)	YES			The protocol ID from protocols.xml file.
networkProtocolId	smallint(6)	YES			The protocol ID from the IP-header of the packet.
sourceIPAddr	char(32)	YES			The IP address of the source of the attack.
sourcePort	int(11)	YES			The source port for the attack traffic.
targetIPAddr	char(32)	YES			The IP address of the target fo the attack.
targetPort	int(11)	YES			The destination port of the attack traffic.
confidence	tinyint(4)	YES			The confidence level of the signature that was matched. Inverse of BTP value. High confidence means low BTP. Range is from 0-7. <3: high confidence 3-5: Medium >=6: Low
protoQual1	int(11)	YES			
protoQual2	int(11)	YES			
protoParsingState	int(11)	YES			The inner state of the protocol parsing machine.
direction	tinyint(4)	YES			Wether 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	Type	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; 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.

Field	Type	Null	Key	Default value	Description/Comments
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 targetted 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.
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
destinationReputation	smallint(6)	YES			Reputation of the targeted host. Same as sourceReputation
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

Field	Type	Null	Key	Default value	Description/Comments
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			
tag	int(11)	NO		-1	The userId 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.
srcAPN	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 targetted at data-enabled mobile equipments such as a mobile phone or a tablet PC. The phone number of the targetted mobile equipment.
destIMSI	char(16)	YES			Applicable only to attacks targetted at data-enabled mobile equipments such as a mobile phone or a tablet PC. The International Mobile Subscriber Identity (IMSI) of the targetted mobile equipment.
destAPN	varchar(120)	YES			Applicable only to attacks targetted at data-enabled mobile equipments such as a mobile phone or a tablet PC. The Access Point Name (APN) of the targetted mobile equipment.
fileType	int(11)	YES			Malware File type

Field	Type	Null	Key	Default value	Description/Comments
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	Type	Null	Key	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.
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.
creationSeqNumber	int(11)	YES			The sequecne number used to differentiate records with the same creation time.

Field	Type	Null	Key	Default	Description/Comments
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	Type	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.
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.
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.

Field	Type	Null	Key	Default value	Description/Comments
failover_enable	enum('Y','N')	NO		N	Whether failover is enabled or not.
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 reservered 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 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 or not.
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	Type	Null	Key	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	Type	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 categoryId is provided below: • 111 - Exploit • 112 - Volume DOS • 113 - Reconnaissance • 114 - Policy violation
description	varchar(64)	Yes			The description for each categoryId 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	Type	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.

Field	Type	Null	Key	Default value	Description/comments
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.
ip_address	varchar (32)	YES			User-assigned IP address to the NTBA device management port.
command_protocol	varchar (32)	YES			\N
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 or not.

The following table describes IV_Alarm information.

Field	Type	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
Type	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.

Field	Type	Null	Key	Default	Description/comments
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.
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	Type	Null	Key	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	Type	Null	Key	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.

Field	Type	Null	Key	Default value	Description/comments
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.
network_link_id	int(11)	Yes			The network link on which this VIDS is created.
has_anomaly	enum('Y', 'N')	No		N	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	Type	Null	Key	Default	Description / Comments
policy_id	varchar(20)	NO	Primary		Unique ID of the policy.
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.

Field	Type	Null	Key	Default	Description / Comments
`is_mom_defined`	enum('Y','N')	NO		N	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	Type	Null	Key	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	Type	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	Type	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.
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	Type	Null	Key	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	Type	Null	Key	Default	Description / Comments
SUBSCRIBER_ID	int (11)	NO	PRI	\N	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	
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		\N	User-defined name of the admin domain.
DESCRIPTION	varchar(255)	NO		\N	User-specified description for the admin domain.
COMPANY	varchar(255)	YES		\N	The name of the company or owner of this admin domain.

Field	Type	Null	Key	Default	Description / Comments
PRIMARY_CONTACT_ID	int(11)	YES	MUL	\N	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	\N	Secondary contact (unused for now) CONSTRAINT is_secondarycontactid_fk FOREIGN KEY(secondary_contact_id) REFERENCES iv_contact(contact_id)
RESP_EMAIL_ADDR	varchar(255)	YES		\N	Default email address for Manager responses
RESP_PAGER_EMAIL_ADDR	varchar(255)	YES		\N	Default text-pager email address for Manager responses
RESP_SCRIPT_PATH	varchar(255)	YES		\N	Default script to be executed for script responses
SUBSCRIBER_LEVEL	tinyint(4)	NO		\N	The level in the admin-domain tree that this admin domain is defined at.
PARENT_ID	int(11)	YES	MUL	\N	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.
ALLOW_CHILD_SUBSCRIBERS	enum('Y','N')	NO		N	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.

Field	Type	Null	Key	Default	Description / Comments
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, like 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	\N	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.
EMAIL_ENABLED	enum('Y','N')	NO		N	A flag to enable email responses.
EMAIL_THRESHOLD	tinyint(4)	YES		\N	An alert severity threshold beyond which the Manager must send email notification of alerts. If null, then 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		\N	An alert severity threshold beyond which the Manager must send pager notification of alerts. If null, then 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		\N	An alert severity threshold beyond which the Manager must execute the corresponding scripts. If null, then the Manager must never execute scripts.

Field	Type	Null	Key	Default	Description / Comments
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		\N	Per attack forwarder based on global policy settings.
BYATTACK_PAGER	tinyint(4)	YES		\N	Per attack forwarder based on global policy settings.
BYATTACK_SCRIPT	tinyint(4)	YES		\N	Per attack forwarder based on global policy settings.
BYAV_EMAIL	tinyint(4)	YES		\N	
BYAV_PAGER	tinyint(4)	YES		\N	
BYAV_SCRIPT	tinyint(4)	YES		\N	
IS_MPE_POLICY_ENABLE	enum('Y','N')	NO		Y	
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	Type	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 "Id" 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.

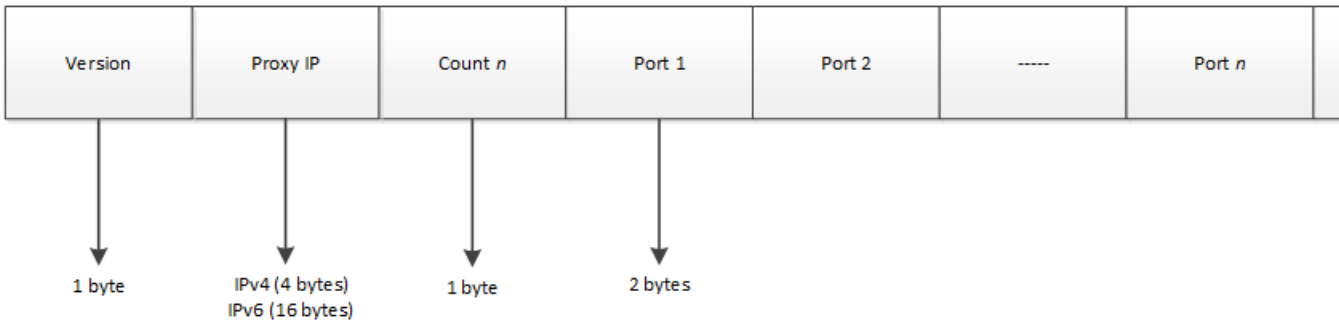


Figure 12-1 Port scan

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.

Figure 12-2 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.

Figure 12-3 Statistical anomaly 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 tells how many measures are in the data block. The measures are followed by the count byte as shown in the following figure.

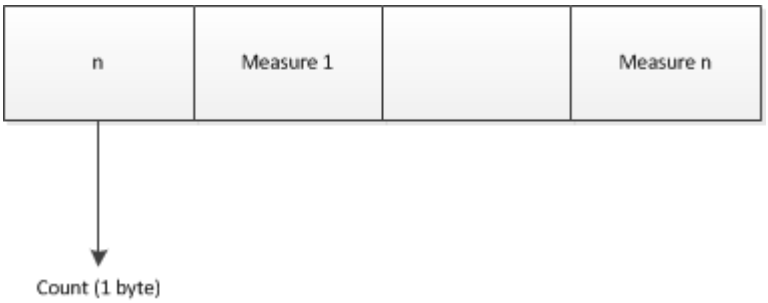


Figure 12-4 Anomaly measure data block

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.

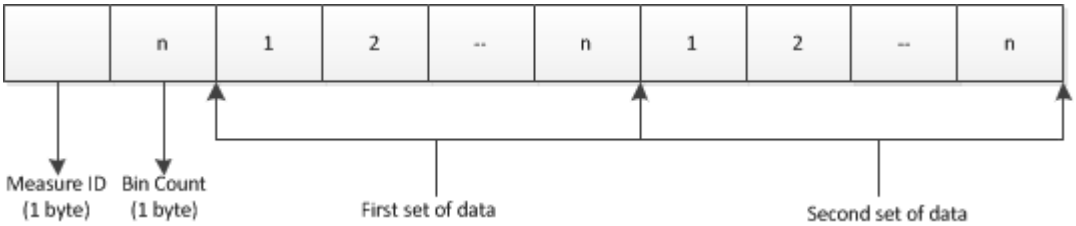


Figure 12-5 Measure

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.

Figure 12-6 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.

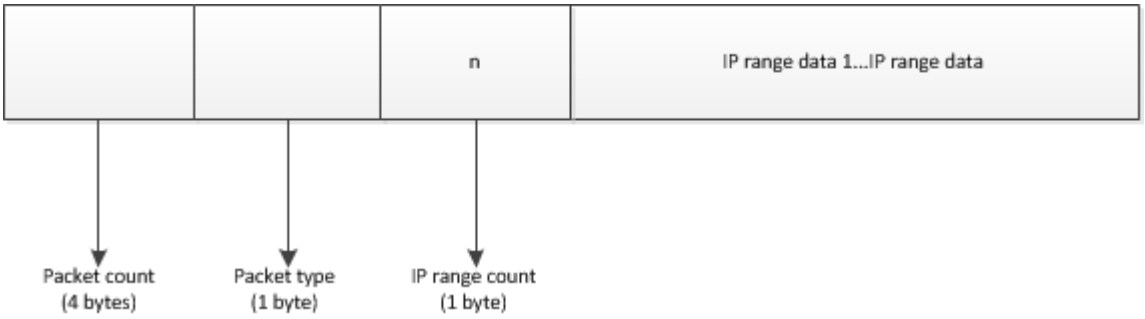


Figure 12-7 Packet type data

IP range data

The IP Range Data contains 20 bytes information as shown in the following figure.

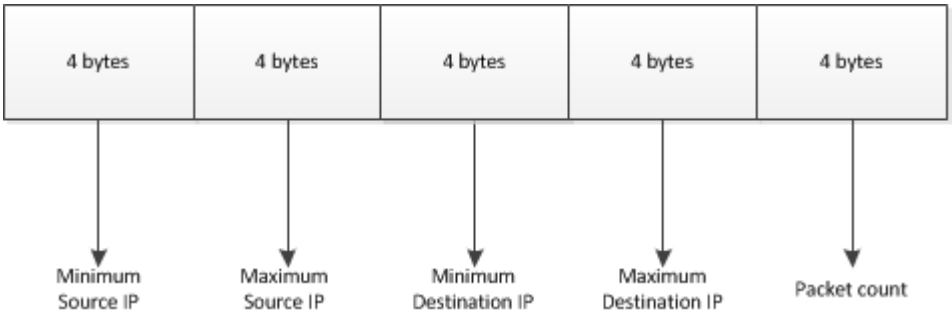


Figure 12-8 IP range

- 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.

Figure 12-9 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.

Figure 12-10 NTBA host sweep alert

Statistical anomaly alert

All alerts that have iv_alert.alertType = 14, are NTBA statistical anomaly alerts.

Figure 12-11 NTBA statistical anomaly 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.

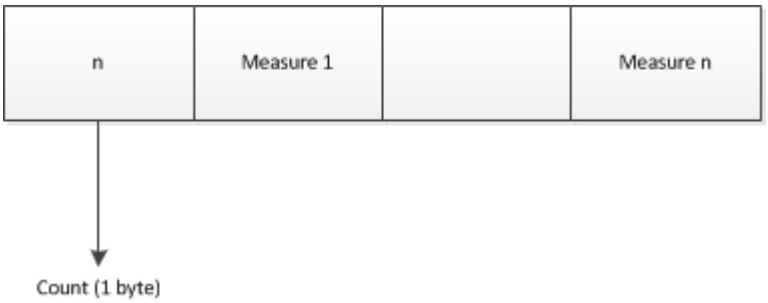


Figure 12-12 Anomaly measure data block

Measure

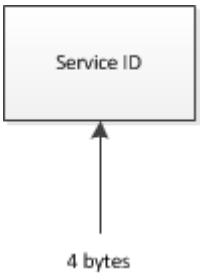
Each measure contains two sets of floating point (4 bytes) values. The first set represents the bins and the second set represents the bin-count data values.

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.

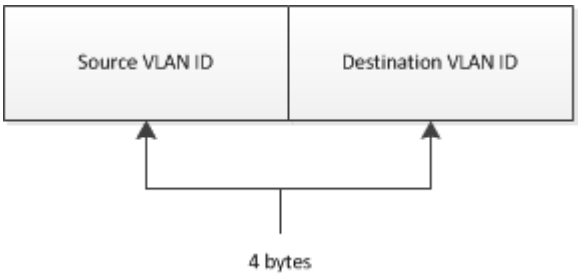
Figure 12-13 Measure

Miscellaneous data block

Service block



VLAN block



Simple threshold alert

All alerts that have iv_alert.alertType = 15, are NTBA simple threshold alerts.

Either the serviceId or applicationId will be -1 in an alert depending upon the type of the attack.

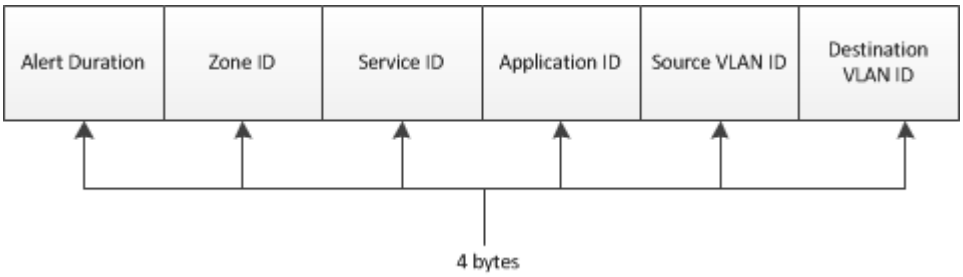


Figure 12-14 NTBA simple threshold type specific data

Generic behavioral alert

All alerts that have iv_alert.alertType = 201 are NTBA Generic Behavioral Alerts.

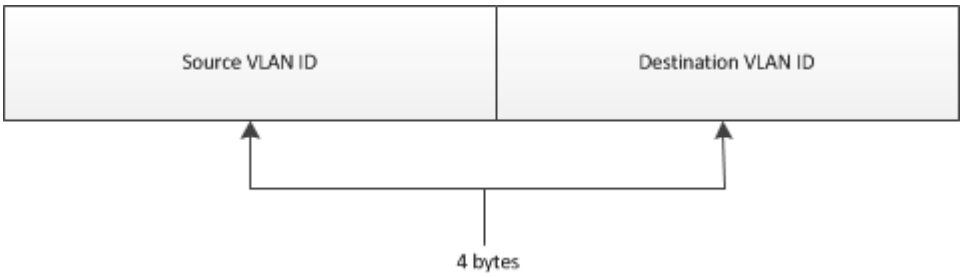


Figure 12-15 NTBA generic behavioral type specific data

Policy violation alert

All alerts that have iv_alert.alertType = 200 are NTBA policy violation alerts.

The details of the alert are as follows:

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
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

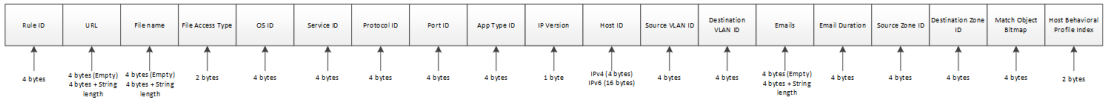
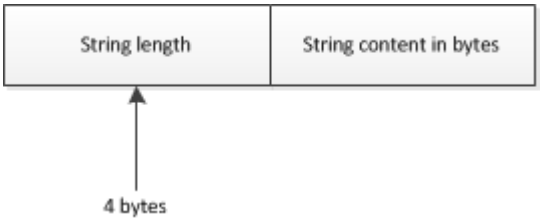


Figure 12-16 NTBA policy violation type specific data

String

URL and file name are strings which are represented as shown below.



IP address

Host IP address is represented as shown below.

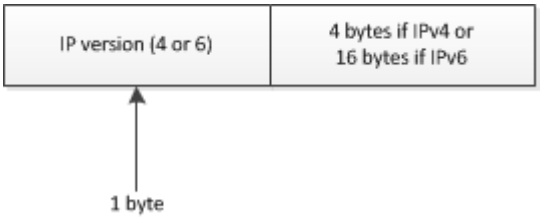


Figure 12-17 Host IP address

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.

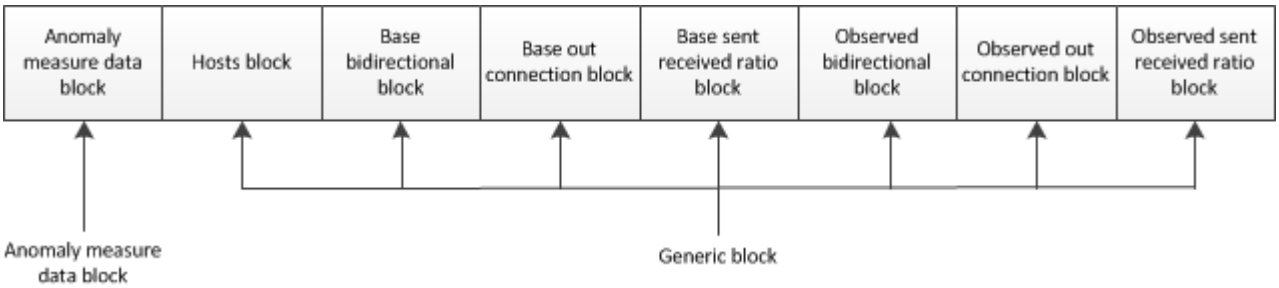


Figure 12-18 Worm alert type specific data

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.

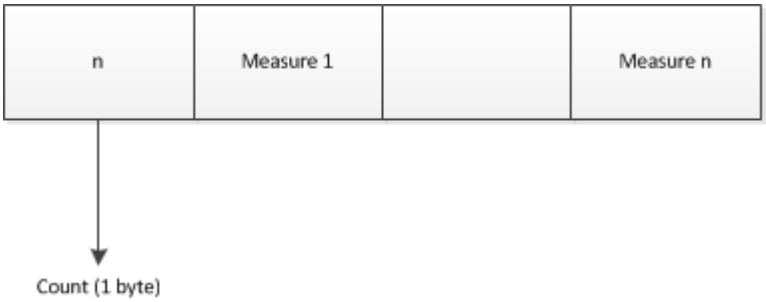


Figure 12-19 Anomaly measure data block

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.

Figure 12-20 Measure

Generic block

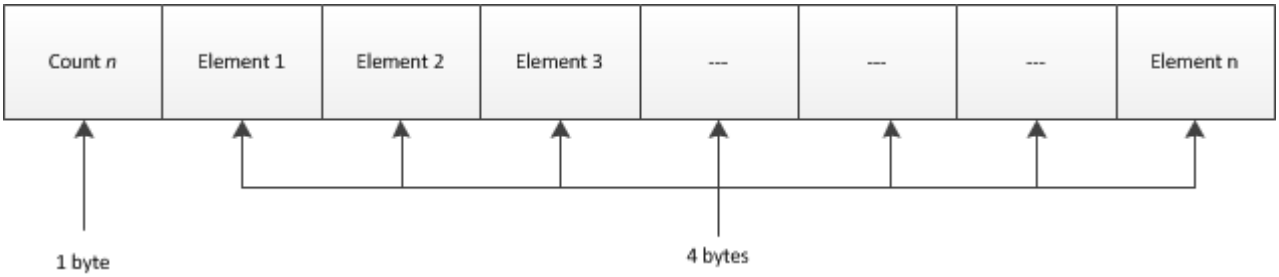


Figure 12-21 Generic block

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.

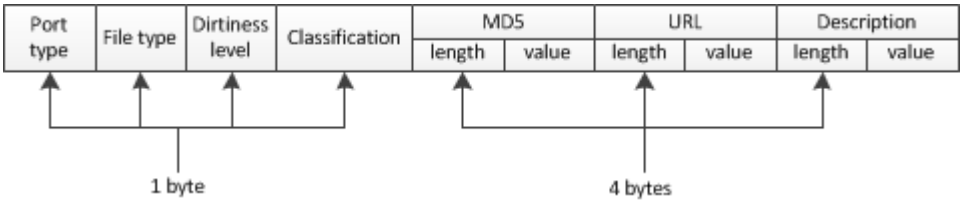


Figure 12-22 File reputation alert

The port-type mapping bit is not currently used but allocated for future use.

The following table describes file type mapping.

Value	File type
1	exe
2	dll
3	cpl
4	ocx
5	sys
6	scr
7	drv
8	com
9	doc

Value	File type
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.

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 uuid 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 = “0x41a01e00”;
```

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, then 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, then 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.

> 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 SensorId 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, lastReqByteStreamOffset, lastRespByteStreamOffset";`
3. Create the pcap file header and write them into a file. The PCAP file header format is as follows:
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 Ethereal.

   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)

Bytes	Value	Comment
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
6	sourceAddr	0xFFFFFFFFFFFF if it is 0: Got it from step 4
6	targetAddr	0xFFFFFFFFFFFF if it is 0: Got it from step 4
2	0xFFFF	IP type
n	Packets	Actual packet log data.

13 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

1. 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. Then 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 IPS Administration 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 and inherit it at the Sensor level. See the *McAfee Network Security Platform IPS Administration 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.

Tasks

- *Load the Sensor MIBs onto to your MIB browser* on page 254

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:
   1. MCAFEE-SMI
   2. MCAFEE-TC
   3. MCAFEE-SENSOR-SMI
   4. MCAFEE-SENSOR-CONF-MIB
   5. MCAFEE-SENSOR-PERF-MIB
   6. 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.

Figure 13-1 MIB configuration

The following snapshot provides the SNMP walk output of the system group under the McAfee Network Security Platform configuration MIB.

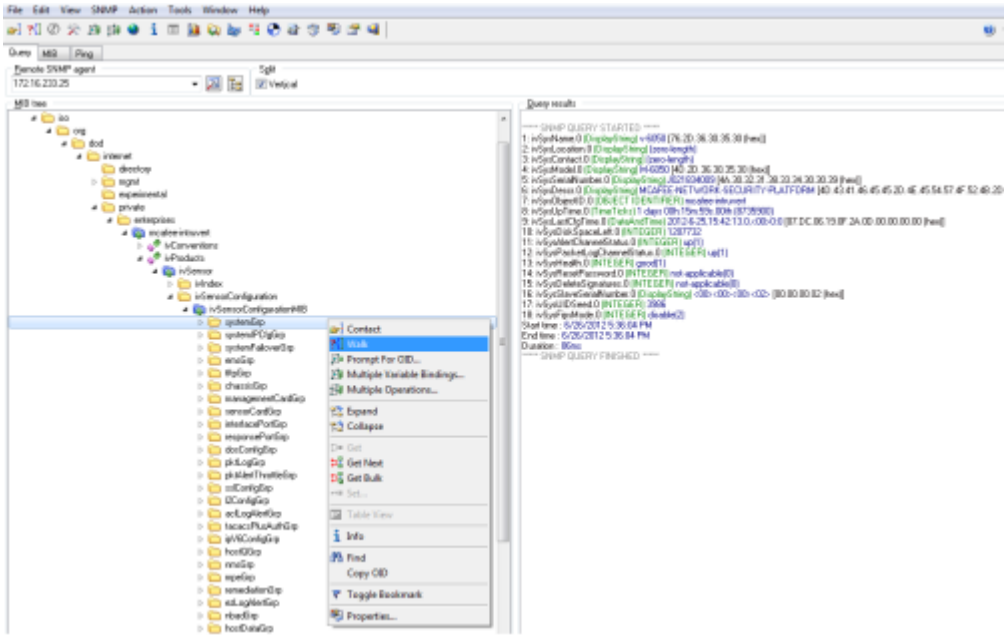


Figure 13-2 SNMP walk output

From release 6.1.5, restricted write access to a section of the MIB is available. Refer to Management of permitted NMS IP address , *IPS Administration Guide*.

The following snapshot provides information about the MIB subgroup, which has write access from third-party SNMP applications.

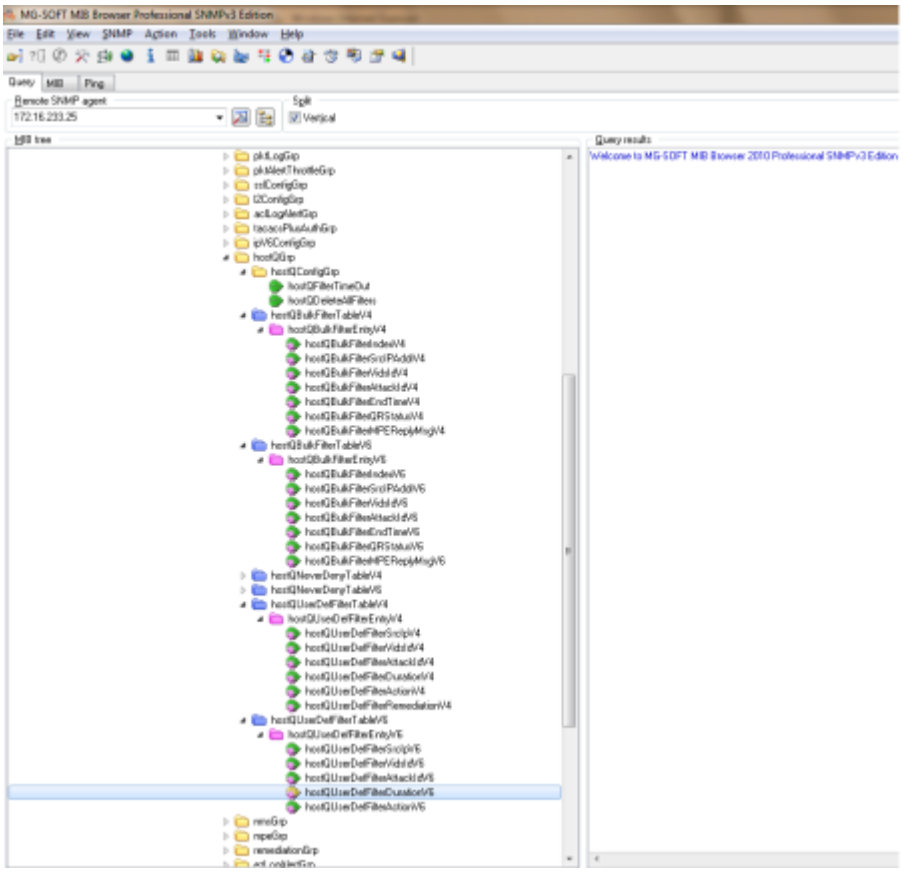


Figure 13-3 SNMP walk output

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.

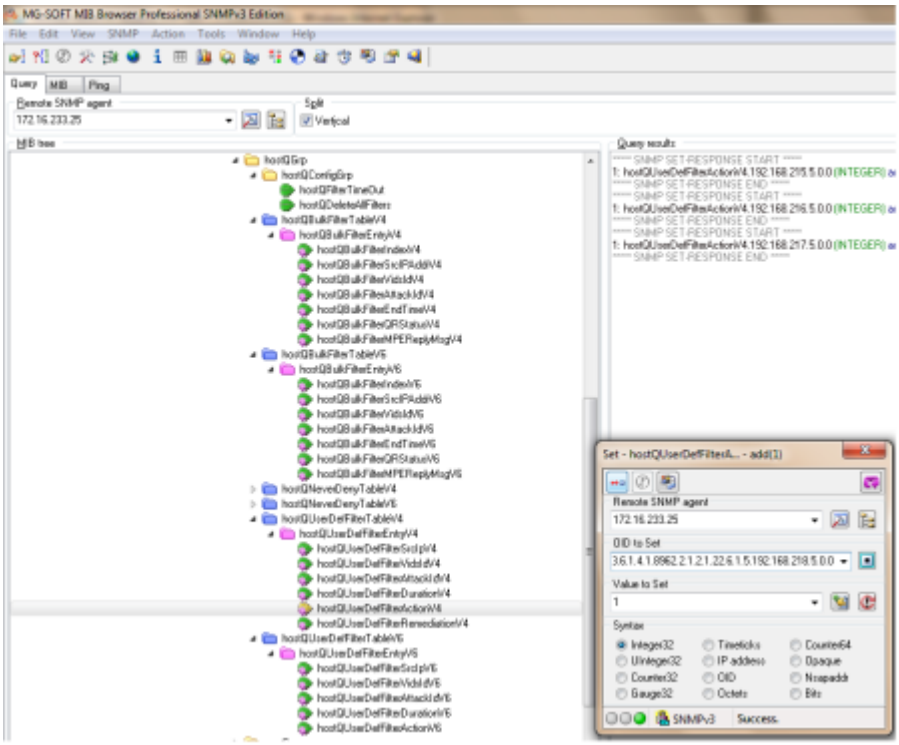


Figure 13-4 SNMP set output

Index

A

about this guide 7
active relevance option 163
alert synchronization
    MDR 249
analyzer profile 91
analyzer VM 91
Anti-Malware Engine 91
attack relevance analysis
    enable 162

C

concurrent scan; endpoints 181
concurrent scans 179
conventions 187
conventions and icons used in this guide 7
custom certificates; Manager keystore 172
custom client certificates 171
custom fingerprints 67
    Sensor response 69

D

data mining
    SIEM applications 220
database queries 247
    implications 248
    SQL query guidelines 247
database updates
    resubmit 184
documentation
    audience for this guide 7
    product-specific, finding 8
    typographical conventions and icons 7
dynamic analysis 91

E

endpoint rescan 179
enhanced smartblocking 50
ePO
    endpoint details query 10
ePO configuration 29
ePO console 17
ePO integration 9
    configurations 24
    dashboard 23
    dashboards 33
    endpoint details 14
    install 18
    mouse-over 13
    permission set; define 35
    server task 29
    source and destination endpoints 11
ePO server
    configure 25
ePO server settings 25
ePO user 38

F

FCM agent service 150
FCM; considerations 152
file reputation 64
    benefits 64
    CLI commands 75
    configurations 66
File Reputation alert 246
file reputation; attack log 74
file reputation; custom fingerprints 68
file reputation; GTI fingerprints 66

G

Gateway Anti-Malware Engine 91
GTI 43, 78, 80, 82
GTI fingerprints 66
GTI integration 41, 42, 77, 81, 85
    connection limiting policies 62
    file reputation 62
    IP reputation 49, 50
    terminologies 63
GTI report
    alert data details 59
    feature display 61
    general setup 60
    technical contact information 62
    view 59

H

host intrusion prevention 188
host intrusion prevention Sensor
    add 188
    ePO 189
HP network automation 207
    configure 207

I

integration
    fault notification 217
    reports 220
IP address information
    exclude 57
IP reputation
    configure 51
    interface 54
    sub-interface 57
IPS alerts 238
    anomaly measure data block 239
    DoS packet type data block 240
    IP range data 240
    packet type data 240
    port scan alert 238
    statistical anomaly alert 239
    threshold anomaly alert 241
IV_ALERT_DATA decoding 238

L

limitations 75
local blacklist 91
local whitelist 91

M

malware statistics
    Sensor 74
managed endpoints 16
McAfee Logon Collector 191, 192
    communication error 200
    reports 198
    threat analyzer; dashboards 196
    threat analyzer; dashboards; NTBA 196
McAfee ServicePortal, accessing 8
MIB browser
    Sensor MIBs; load 254
    SNMPv3 user details 253
MIB browsers
    Sensor 253

N

NessusWX 168
Network Security Platform format 168
new alert category 58
next generation reports 58
NTBA alerts 241
    anomaly measure data block 242, 245
    generic behavioral alert 243
    generic block 246
    host sweep alert 241
    IP address 245
    measure 242, 245
    miscellaneous data block 242
    policy violation alert 243
    port scan alert 241
    service block 243
    simple threshold alert 243
    statistical anomaly alert 242
    string 244
    VLAN block 243
    worm alert 245

O

on-demand scan of endpoints; threat analyzer 173
on-demand scan; endpoints 181
on-demand scan; fault messages 180

P

packet header 251
passive relevance option 162
PCAP file header 251
PCAP format packet logs
    create 250
PCAP packet headers 251, 252
permission set
    view; edit 37

Q

query and retrieve asset information 163

R

relevance analysis 160, 162
    disabled option 163
relevance analysis of attacks 159
relevance analysis; scan configurations
    add 170
relevance analysis; vulnerability manager database settings 169
relevance configuration details
    view 161
relevance configuration wizard 161
relevancy cache
    reset 183

S

scan reports
    import 166
scheduler; automatic report import 168

security information and event management products 211
sensoruser groups 191
ServicePortal, finding product documentation 8
SIEM products 212
    integration 212
    notification 213
SNMP MIB browser
    integrate 253
SSL custom certificate 171
static analysis 91
supported vulnerability scanners 167

T

technical support, finding product information 8
templates
    syslog; email; pager 214
terminologies 91
troubleshooting 75
troubleshooting options 182

U

umanaged endpoints 17
user 91
    create 24

V

VM profile 91
vulnerability assessment best practices 159
vulnerability manager cache
    reload 183
vulnerability manager configuration 143
    options 139
Vulnerability Manager configuration details
    view 154
vulnerability manager database settings
    configure 145
vulnerability manager format 168
Vulnerability Manager installation 139
vulnerability manager integration 137
    admin domain level 143
    child admin domain 144
    update permissions 148
vulnerability manager scan configurations
    add 152
vulnerability manager scan information 176
vulnerability manager scan; network scenarios 180
vulnerability manager scans 175
vulnerability manager scans; endpoints 180
vulnerability manager scheduler
    fault messages 170
vulnerability manager server settings 147
vulnerability manager settings 140
Vulnerability Manager settings
    save 149

0J00

McAfee™
Together is power.