

DXL Configuration

Integration Step 1

- **Before we 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.
- DXL integration can either be configured globally or on a per device basis.

DXL/TIE Configuration

Integration Step 1

Check in the NSP extension into the ePO Server.

It is recommended to create a dedicated ePO user account for NSP integration.

The screenshot shows the McAfee Network Security Manager interface in Internet Explorer. The browser title is "McAfee Network Security Manager - 192.168.222.132 - Internet Explorer". The page URL is "/My Company > Integration > ePO > ePO Integration". The left sidebar shows a navigation tree with "ePO Integration" selected. The main content area contains instructions for ePO integration, a list of steps, a tip, and a form for "ePo Server Settings". The form fields are: "Server Name or IP Address" (192.168.222.1), "Server Port" (8443), "User Name" (admin), and "Password" (masked with dots). A "Test Connection" button is at the bottom right of the form. The footer of the page indicates "ePo Configuration Wizard" and "step 2 of 2".

McAfee Network Security Manager - 192.168.222.132 - Internet Explorer

GMT+01:00 | /My Company | Administrator | Login History

McAfee Network Security Manager Version: 8.3.7.7

Dashboard Analysis Policy Devices Manager

Domain: /My Company

/My Company > Integration > ePO > ePO Integration

Use this page to specify the ePO server and its listening port, and the credentials the Manager uses when communicating with ePO.

ePO integration requires the NSP Extension for ePO to be installed on the ePO server. To install the NSP Extension for ePO:

1. Download the extension from here: [NSP Extension for ePO](#)
2. From the ePO console, go to Menu > Software > Extensions and install it.
3. From this page, enter the required information, confirm connectivity, and finish this wizard.

Tip: To optimize security, we recommended you use a local ePO user account with **view-only** permissions.

Fields marked with an asterisk (*) are required.

ePo Server Settings

Server Name or IP Address: *

Server Port: *

User Name: *

Password: *

Test Connection

ePo Configuration Wizard step 2 of 2

< Back Finish

DXL/TIE Configuration

Integration Step 2

Configuration is done under the Devices tab

/My Company > Global > IPS Device Settings > DXL Integration

Enter Credentials for ePO Login. The default port for communication is 8443, but might be different.

The screenshot displays the McAfee Network Security Manager web interface. The browser title is "McAfee Network Security Manager - 192.168.222.132 - Internet Explorer". The interface includes a navigation bar with tabs for Dashboard, Analysis, Policy, Devices, and Manager. The left sidebar shows a tree view with "Global" and "Devices" sections. Under "Devices", "Common Device Settings" is expanded, and "DXL Integration" is selected. The main content area shows the "Data Exchange Layer (DXL) Integration" configuration page. It includes instructions on enabling DXL and TIE integration, a list of steps, and a note about default settings. The configuration fields are as follows:

Field	Value
Enable DXL Integration?	<input checked="" type="checkbox"/>
ePO Server IP Address:	192.168.222.1
ePO Server Port:	8443
ePO Username:	admin

Buttons for "Open ePO Console" and "Save" are visible at the bottom of the configuration area.

DXL/TIE Configuration

Integration Step 2

- Credentials used for DXL integration 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.

The screenshot displays the McAfee Network Security Manager interface. The browser title is "McAfee Network Security Manager - 192.168.222.132 - Internet Explorer". The page shows the "Data Exchange Layer (DXL) Integration" configuration page. The breadcrumb navigation is "/My Company > IPS Device Settings > DXL Integration".

When integration with McAfee Data Exchange Layer (DXL) is enabled, IPS sensors can send suspicious files to Threat Intelligence Exchange (TIE) servers for advanced malware analysis. Enabling integration with DXL/TIE consists of the following steps:

1. Enable DXL so that IPS sensors can locate TIE servers on the network (from this page).
2. Enable the TIE engine within the advanced malware policy and assign the policy to a sensor interface (from the [Advanced Malware Policies](#) page).

Note: By default, all IPS sensors in this domain (and child admin domains) inherit the settings below. Enabling integration from this page therefore enables DXL integration on all inheriting IPS sensors. You can alternatively enable/customize integration on a per-domain or per-sensor basis.

Data Exchange Layer (DXL) Integration

Enable DXL Integration?	<input checked="" type="checkbox"/>
ePO Server IP Address:	192.168.222.1
ePO Server Port:	8443
ePO Username:	admin

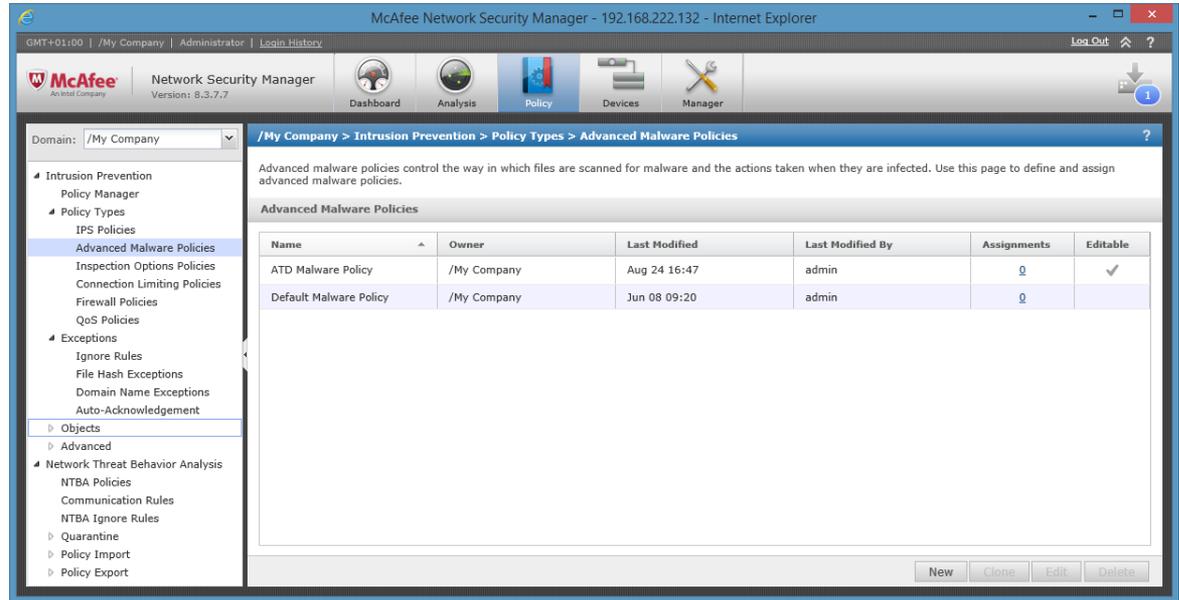
Buttons: Open ePO Console, Save

A red circle highlights the [ePO Integration Settings](#) link in the top right corner of the configuration area.

DXL/TIE Configuration

Integration Step 3 – Enable TIE in the Advanced Malware Policy

- /My Company > Policy Types > Advanced Malware Policies
- The Default Malware Policy can't be edited. So create a new one or clone the default.



The screenshot displays the McAfee Network Security Manager web interface. The breadcrumb navigation path is: /My Company > Intrusion Prevention > Policy Types > Advanced Malware Policies. The interface includes a left-hand navigation tree with categories like Intrusion Prevention, Policy Manager, Policy Types, and Network Threat Behavior Analysis. The main content area shows a table of Advanced Malware Policies.

Name	Owner	Last Modified	Last Modified By	Assignments	Editable
ATD Malware Policy	/My Company	Aug 24 16:47	admin	0	✓
Default Malware Policy	/My Company	Jun 08 09:20	admin	0	

At the bottom of the table, there are buttons for 'New', 'Clone', 'Edit', and 'Delete'.

Enable TIE/ File Reputation

In the advanced Malware Policy

McAfee Network Security Manager - 192.168.222.132 - Internet Explorer

GMT+01:00 | /My Company | Administrator | Login History

McAfee Network Security Manager Version: 8.3.7.7

Dashboard Analysis Policy Devices Manager

Domain: /My Company

/My Company > Intrusion Prevention > Policy Types > Advanced Malware Policies

Use this page to specify the basic properties of the policy, including the protocols over which advanced malware scanning is performed, and the scanning options per file type.

Advanced Malware Policy

Properties

Scanning Options

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\ftpin\malware

File Type	Maximum File Size (KB) Scanned	Malware Engines							Action Threshold
		Blacklist and Whitelist	TIE / GTI File Reputation	NSP Analysis	Gateway Anti-Malware	Advanced Threat Defense	McAfee Cloud	Alert	
Executables	5120	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	High	
MS Office Files	1024	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	High	
PDF Files	1024	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	High	
Compressed Files	5120	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	High	
Android Application..	2048	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	High	
Java Archives	2048	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	High	
Flash Files	2048	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	High	

Prompt for assignment after save Save Cancel

File Reputation by contacting the local TIE server can be configured for

- Executables
- MS Office Files
- PDF Files
- Compressed Files
- Android
- Java Archives
- Flash Files

TIE/GTI File Reputation

Viewing Threat Intelligence Exchange detection in the Manager

- Information is displayed in the Attack Log
- The Sensor also raises a *MALWARE: Malicious File Detected by TIE Engine* alert.

/My Company > Malware Files

Use this page to view malware files detected on your network.

Tip: Double-click a hash to view matching attacks. Any Malware Confidence

Actions	Hash	Overall Malware Confidence	Individual Engine Confidence	
			TIE / GTI File Reputation	NSP Au
Take action	e7584031896cb948...	Very High		
Take action	2f014cd07be3517427...	High		High
Take action	e90fa0072e6188199...	High		High
Take action	16b04c664a405b9f2...	High		High
Take action	a81a62622b3111f13...	Very High		
Take action	56383df0469f70e4e...	Very High		
Take action	112d699c1eb75a27...	Very High		
Take action	493d146a59a155ed...	Very Low	Very Low	
Take action	0a2ea148641b3b22...	Very High		Ver
Take action	e2cfe1c8970335204...	High	High	
Take action	a4bf70bdfa21192c1...	Very High		Ver
Take action	7331df41dfb25c552...	Very High	Very High	Ver
Take action	1b1592edb46211eb...	Very High	Very High	
Take action	5f039a57e481c5a5...	Very High	Very High	

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

Threat Intelligence Exchange Engine Results

View the file reputation results correlated by TIE for each analysis engine.

Enterprise | Advanced Threat Defense | Global Threat Intelligence

Total Detections: ---

Last Detection: ---

Distinct File Names Used by this File: 1

Malware Confidences Observed for this File: **High**

Close

Sensor CLI commands for TIE and DXL

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, ATD and GTI.
 - 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.