DXL Configuration

Integration Step 1

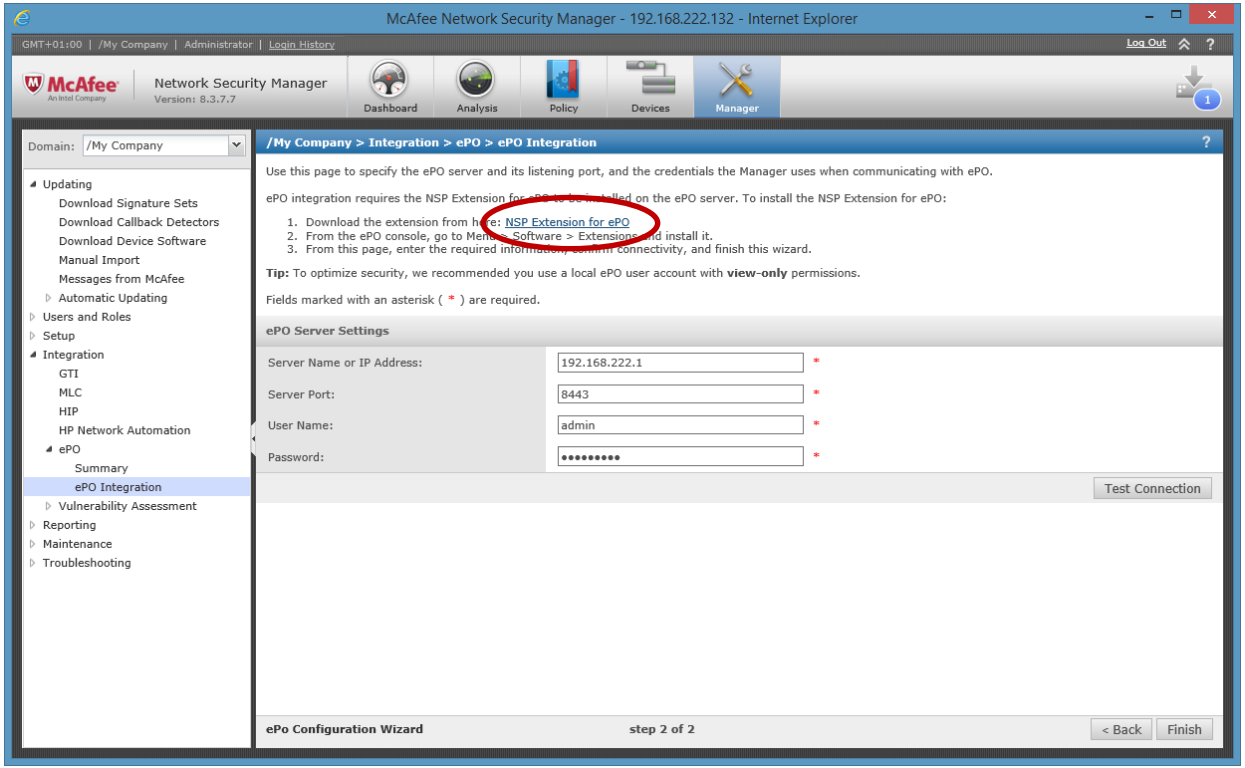
- **Before we begin**
- You must make sure that you have
  - Set up and configured a McAfee ePO server.
  - Set up and configured the Threat Intelligence Exchange server and DXL brokers.
- DXL integration can either be configured globally or on a per device basis.

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.



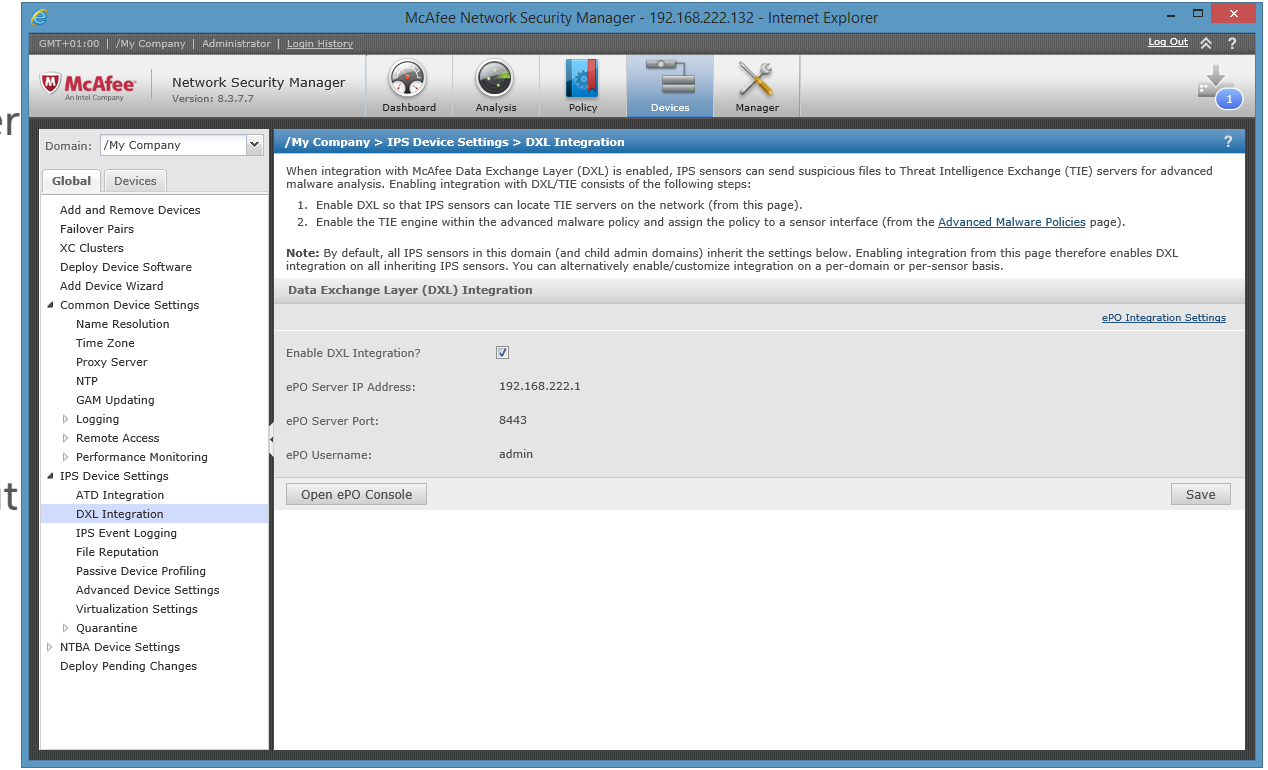
DXL/TIE Configuration

Integration Step 2

Configuration is done under the Devices tab

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

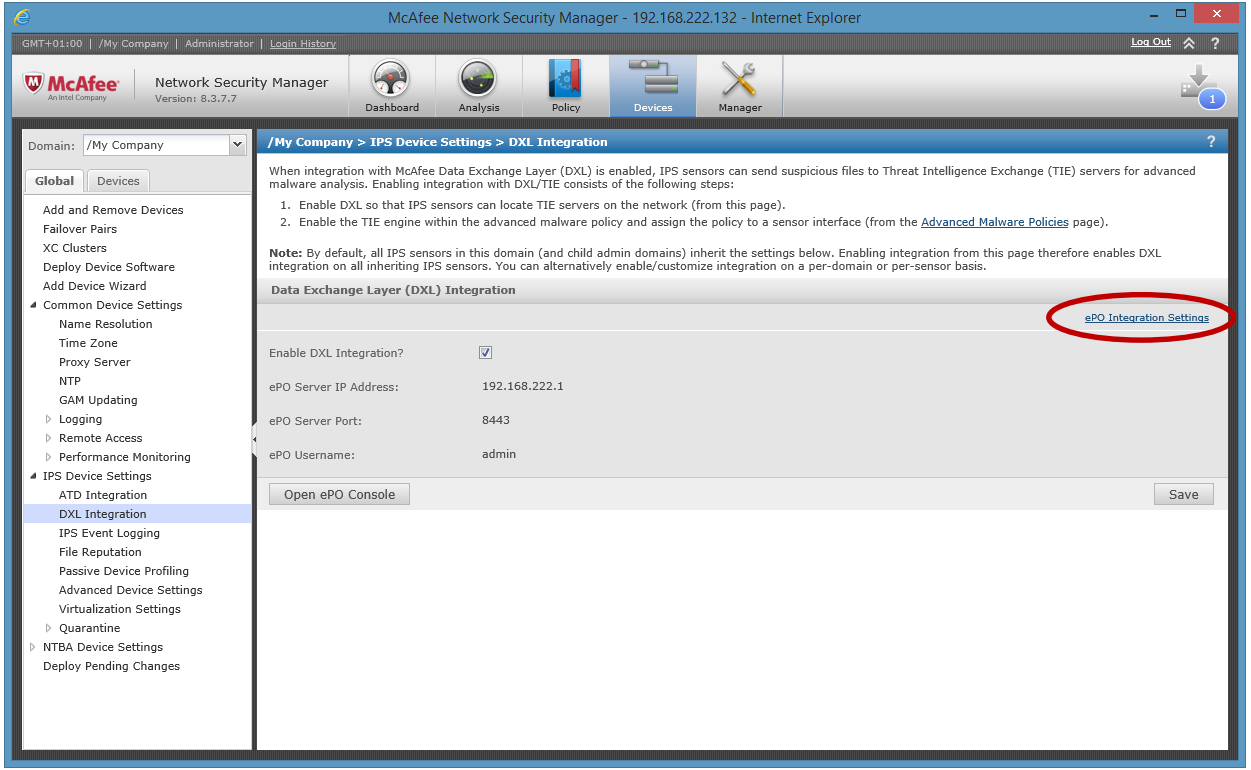
Enter Credentials for ePO Login. The default port for communication is 8443, but might be different.



DXL/TIE Configuration

Integration Step 2

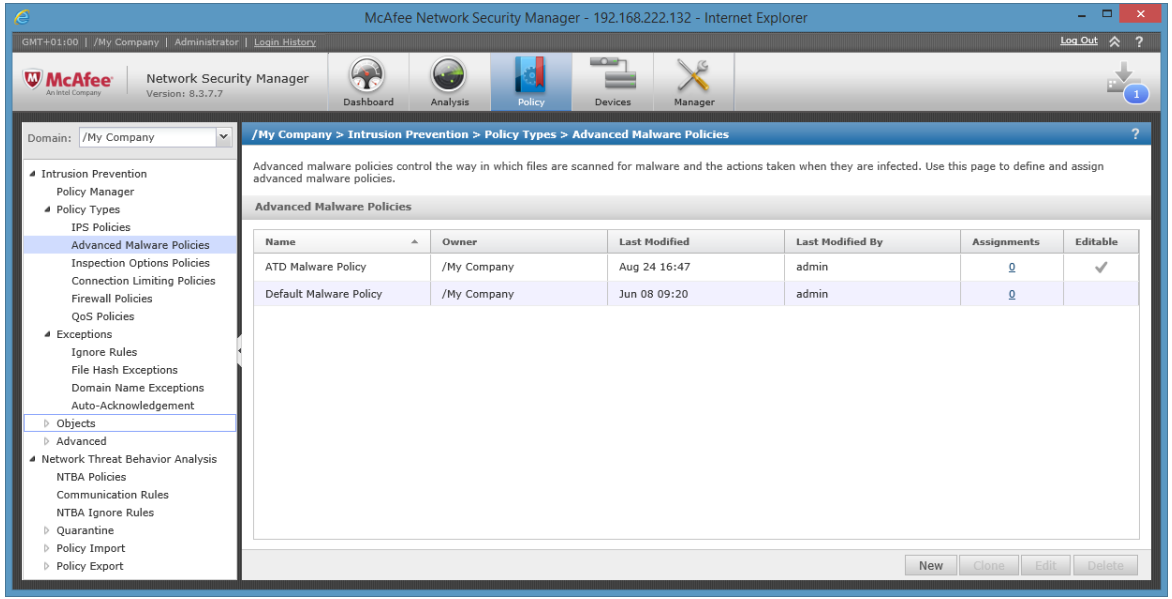
- Credentials used for DXL integration need not be the same credentials as those entered in the **ePO Integration** page. To review this configuration, click the **ePO Integration Settings** hyperlink at the top-right corner of this page.



DXL/TIE Configuration

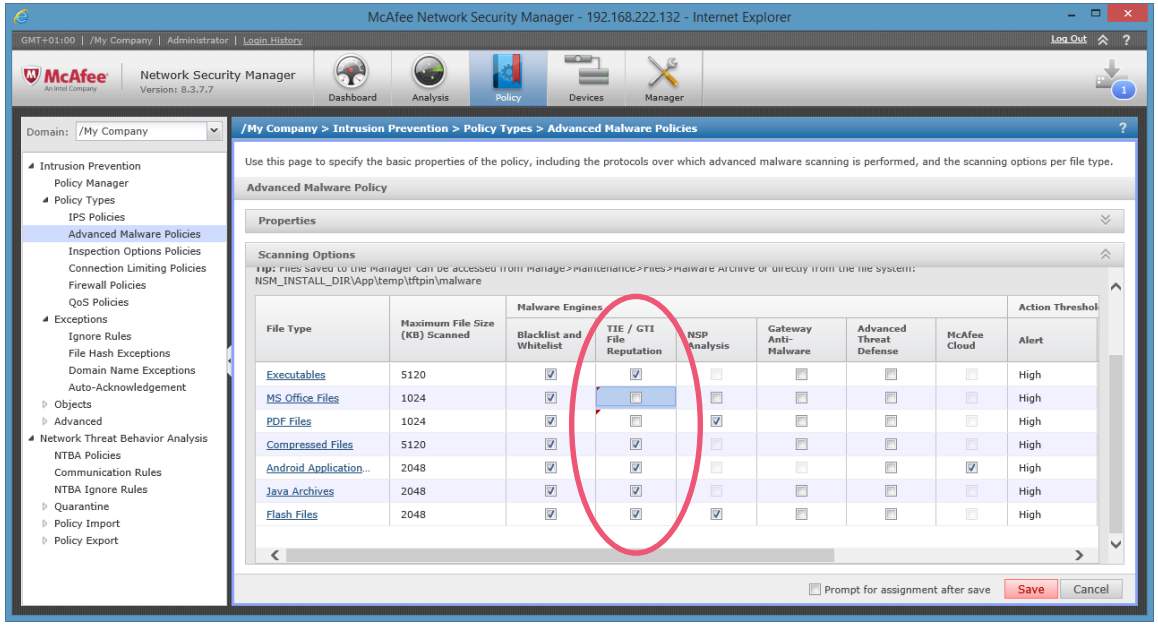
Integration Step 3 – Enable TIE in the Advanced Malware Policy

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



Enable TIE/ File Reputation

In the advanced Malware Policy



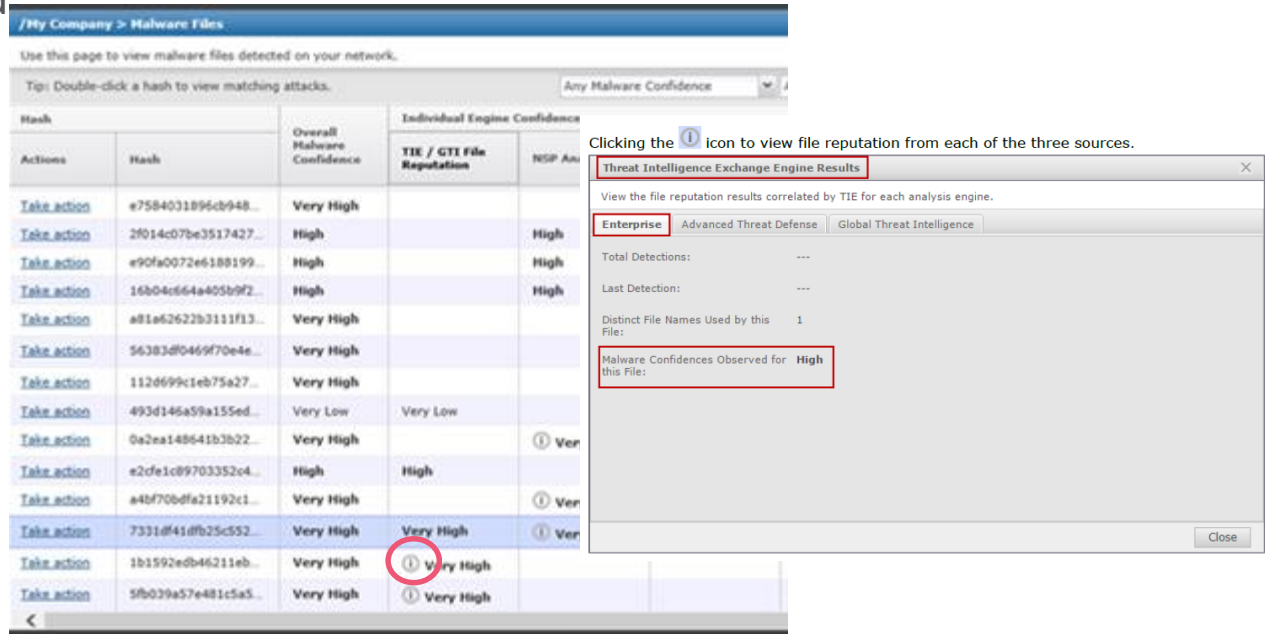
File Reputation by contacting the local TIE server can be configured for

- 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.



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.