Product Guide

McAfee Threat Intelligence Exchange 1.3.0

COPYRIGHT

TRADEMARK ATTRIBUTIONS

LICENSE INFORMATION

License Agreement

Contents

1 Introduction

McAfee® Threat Intelligence Exchange (TIE) provides context-aware adaptive security for your enterprise environment.

The challenge in today's enterprise environment is the growing number of devices and systems and their inability to communicate security information with each other. These devices and systems include the cloud, BYOD, managed nodes, servers, and network appliances. Until now, they have acted independently and were not intelligently managed as a whole.

Threat Intelligence Exchange is changing that. It quickly analyzes files and content from several sources in your environment and makes informed security decisions. These decisions are based on a file's security reputation and your own criteria.

Contents

Benefits of Threat Intelligence Exchange

Imagine the systems and devices on your network communicating security information in real time, then acting immediately to prevent the threat from spreading, even to remote networks and systems.

Threat Intelligence Exchange provides these benefits:

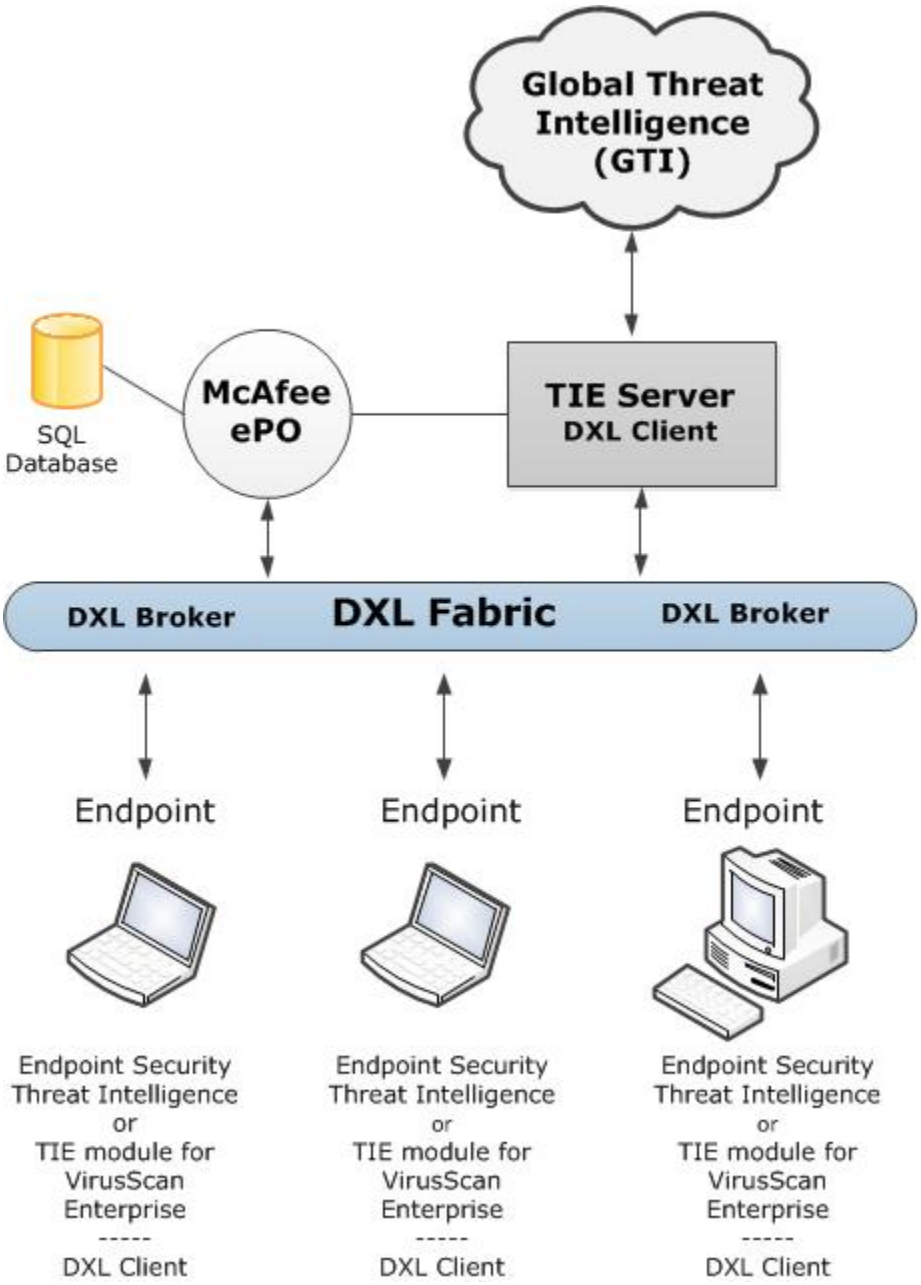
- Fast detection and protection against security threats and malware.
- The ability to know which systems or devices are compromised, and how the threat spread through your environment.
- The ability to immediately block or allow specific files and certificates based on their threat reputations and your risk criteria.
- Real-time integration with McAfee® Advanced Threat Defense and McAfee® Global Threat Intelligence™ (McAfee GTI) to provide detailed assessment and data on malware classification. This integration allows you to respond to threats and share the information throughout your environment.

Threat Intelligence Exchange components

Threat Intelligence Exchange includes these components.

- A module for McAfee® VirusScan® Enterprise that allows you to create policies for blocking and allowing a file or certificate based on its reputation, or a module for Endpoint Security that allows you to create policies for blocking and allowing a file or certificate based on its reputation.
- A server that stores information about file and certificate reputations, then passes that information to other systems.
- Data Exchange Layer brokers that allow bidirectional communication between managed systems on a network.

These components are installed as McAfee® ePolicy Orchestrator® (McAfee ePO™) extensions and add several new features and reports.



The module and server communicate file reputation information. The Data Exchange Layer framework immediately passes that information to managed endpoints. It also shares information with other McAfee products that access the Data Exchange Layer, such as McAfee® Enterprise Security Manager (McAfee ESM) and McAfee® Network Security Platform.

Threat Intelligence Exchange client

The module for VirusScan Enterprise and for an endpoint allows you to determine what happens when a file with a malicious or unknown reputation is detected in your environment. You can also view threat history information and the actions taken.

You can perform these tasks using the Threat Intelligence Exchange client.

The TIE module for Endpoint Security is now called McAfee® Threat Intelligence Exchange (TIE). For details, see the installation guide and release notes for Endpoint Security Threat Intelligence.

- Create policies to:
  - Allow or block files and certificates depending on their reputation.
  - Receive a prompt each time a file or certificate with a certain reputation attempts to run.
  - Send files automatically to Advanced Threat Defense for further evaluation.
- View events on the Threat Intelligence Exchange dashboards. You can view cleaned, blocked, and allowed events for the past 30 days or by event type.

Threat Intelligence Exchange server

The server stores information about file and certificate reputations, then passes that information to other systems in your environment.

The server enables you to:

- Control what is allowed to run in your environment. For example, if your organization routinely uses a file that has an unknown security reputation but you know it's safe, you can set its reputation to allow the file to run.
- Identify and track new files that try to run in your environment. If the new file is allowed to run, the server identifies the first system to run the file, and all other systems that ran the file.
- Instantly stop threats from spreading throughout your environment. As soon as the reputation of a file or certificate is detected as malicious (or suspicious, depending on your settings) the file is immediately blocked from running anywhere in your environment.
- Identify which files were blocked and where they tried to run. You can see where threats originate and see patterns as they occur. For example, specific systems might be more prone to detecting and blocking malicious files, so you can increase the security settings on those systems.
- Specify the rules used in policies, based on the system type. Rules are available for:
  - Systems that change frequently (programs and files are often installed and uninstalled)
  - Typical business systems that change infrequently
  - IT-managed systems that access critical or sensitive information and rarely change

Combining TIE servers and databases

If you have TIE servers and databases managed by different McAfee ePO systems, you can combine them to share reputation information. For details about combining TIE servers and databases, see *Data Exchange Layer Product Guide*, and the KnowledgeBase article KB83896.

Data Exchange Layer

The Data Exchange Layer includes client software and brokers that allow bidirectional communication between endpoints on a network.

The Data Exchange Layer works in the background, communicating with services, databases, endpoints, and applications. The Data Exchange Layer client is installed on each managed endpoint, so that threat information from security products that use DXL can be shared immediately with all other services and devices. Sharing reputation information as soon as it is available reduces the security assumptions that applications and services make about each other when they exchange information. This shared information reduces the spread of threats.

DXL clients maintain a persistent connection to their brokers regardless of their location. Even if a managed endpoint running the client is behind a NAT (network address translation) boundary, it can receive updated threat information from its broker located outside the NAT.

See *Data Exchange Layer Product Guide* for details about installing and using Data Exchange Layer.

How Threat Intelligence Exchange works

Threat Intelligence Exchange uses the Data Exchange Layer framework to share file and threat information instantly across the entire network.

In the past, you sent an unknown file or certificate to McAfee for analysis, then updated the file information throughout the network days later. Threat Intelligence Exchange enables file reputation to be controlled at a local level, your environment. You decide which files can run and which are blocked, and the Data Exchange Layer shares the information immediately throughout your environment.

Scenarios for using Threat Intelligence Exchange

- **Immediately block a file** — Threat Intelligence Exchange alerts the network administrator of an unknown file in the environment. Instead of sending the file information to McAfee for analysis, the administrator blocks the file immediately. The administrator can then use Threat Intelligence Exchange to learn whether the file is a threat and how many systems ran the file.
- **Allow a custom file to run** — A company routinely uses a file whose default reputation is suspicious or malicious, for example a custom file created for the company. Because this file is allowed, instead of sending the file information to McAfee and receiving an updated DAT file, the administrator can change the file's reputation to trusted and allow it to run without warnings or prompting.
- **Import known reputations** — A company has several files that are trusted and used regularly, and other files that are not allowed. Because the reputations are already known and set, the administrator can import a list of files and their reputations directly into the Threat Intelligence Exchange database. Those reputations are used immediately with no further action.
- **See additional information about a file** — Threat Intelligence Exchange notifies the network administrator of an unknown file. The administrator can see several details about the file, such as the file's parent process, company and version information, Hash information, and the systems that ran the file. The administrator can also see more detailed information about the file with VirusTotal, a free virus, malware, and URL online scanning service.

How a reputation is determined

File and certificate reputation is determined when a file attempts to run on a managed system.

These steps occur in determining a file or certificate's reputation.

1. A user or system attempts to run a file.
2. VirusScan Enterprise or Endpoint Security inspects the file and can't determine its validity and reputation.
3. The module for VirusScan Enterprise or the Threat Intelligence Exchange module inspects the file and gathers file and local system properties of interest.
4. The module checks the local reputation cache for the file Hash. If the file Hash is found, the module gets the enterprise prevalence and reputation data for the file from the cache.
5. If the file Hash is not found in the local reputation cache, the module queries the TIE server. If the Hash is found, the module gets the enterprise prevalence data (and any available reputations) for that file Hash.
6. If the file Hash is not found in the TIE server or database, the server queries McAfee GTI for the file Hash reputation. McAfee GTI sends the information it has available, for example "unknown malicious", and the server stores that information.

   The server sends the file for scanning if one of the following is true:

   - Advanced Threat Defense is available or activated as reputation provider, the server looks locally if the Advanced Threat Defense reputation is present; if not, it marks the file as candidate for submission.
   - The policy on the endpoint is configured to send the file to Advanced Threat Defense.

   See the additional steps under *If Advanced Threat Defense is present*.
7. The server returns the file Hash's enterprise age, prevalence data, and reputation to the module based on the data that was found. If the file is new to the environment, the server also sends a first instance flag to the Threat Intelligence Exchange module. If McAfee Web Gateway is present and eventually sends a reputation score, TIE returns the reputation of the file.
8. The module evaluates this metadata to determine the file's reputation:
   - File and system properties
   - Enterprise age and prevalence data
   - Reputation
9. The module acts based on the policy assigned to the system that is running the file.
10. The module updates the server with the reputation information and whether the file is allowed or blocked. It also sends threat events to McAfee ePO via the McAfee Agent.
11. The server publishes the reputation change event for the file Hash.

If Advanced Threat Defense is present

If Advanced Threat Defense is present, the following process occurs.

1. If the system running the file has access to Advanced Threat Defense and this is the first time the file is seen in the environment, the Threat Intelligence Exchange server sends the file to Advanced Threat Defense for scanning.
2. Advanced Threat Defense scans the file and sends file reputation results to the TIE server using the Data Exchange Layer. The server also updates the database and sends the updated reputation information to all TIE-enabled systems to immediately protect your environment. TIE or any other McAfee product can initiate this process. In either case, TIE processes the reputation and saves it in the database.

For information about how Advanced Threat Defense is integrated with Threat Intelligence Exchange, see the chapter *Malware detection and Advanced Threat Defense* in the *McAfee Advanced Threat Defense Product Guide*.

If McAfee Web Gateway is present

If McAfee Web Gateway is present, the following process occurs.

- When downloading files, McAfee Web Gateway sends a report to the TIE server that saves the reputation score in the database. When the server receives a file reputation request from the module, it returns the reputation received from McAfee Web Gateway and other reputation providers, too.

For information about how McAfee Web Gateway exchanges information using a TIE server, see the chapter *Proxies* (p 162) in the product guide of McAfee Web Gateway.

2 Installation

Threat Intelligence Exchange has two major components: a TIE server and a client module for VirusScan Enterprise or for Endpoint Security Threat Intelligence.

Install each component in the order presented here. When you are finished, these items are added to your network:

- Two McAfee ePO managed extensions
  - TIE server management extension, and
  - Threat Intelligence Exchange module for VirusScan Enterprise extension or the Endpoint Security Threat Intelligence

    For more details, see the installation guide for TI ENS.
- The TIE server appliance needs:
  - A Threat Intelligence Exchange module for VirusScan Enterprise or for Endpoint Security on each managed system in your network
  - Data Exchange Layer (DXL) Client on each managed system in your network

Contents

System requirements

Make sure that your system environment meets these requirements and that you have administrator rights.

Products	Components	Version
VMware vSphere		5.1.0 with ESXi 5.1 or later
Threat Intelligence Exchange software	Threat Intelligence Exchange server	1.1.1 (for upgrades)
	Data Exchange Layer client	1.1

Products	Components	Version
	Threat Intelligence Exchange module for VirusScan Enterprise or for Endpoint Security	1.1.1 (for upgrades)
McAfee ePO		5.1.1, 5.1.2, 5.1.3, 5.3.0, 5.3.1
McAfee ePO product extensions and packages (checked in)	VirusScan Enterprise or Endpoint Security	8.8 Patch 5 Patch 4 and Hotfix 929019
	McAfee® Agent	5.0.1
	McAfee Agent extension	5.0
Products installed on each of your managed systems	VirusScan Enterprise or Endpoint Security	8.8 Patch 5 Patch 4 and Hotfix 929019 10.1 This package can be deployed as part of the Endpoint Security deployment.
	McAfee Agent	5.0.1

The McAfee Agent is included in the TIE Server appliance for first-time installation. See the release notes for TIE server for more details about upgrade instructions.

If you need more details about Threat Intelligence Exchange for Endpoint Security, see the installation guide and release notes for Endpoint Security.

For upgrades from previous versions of TIE, see the release note of previous releases. See also *Find product documentation*.

Operating system

You can install the Threat Intelligence Exchange module for VirusScan Enterprise or Endpoint Security Threat Intelligence on the following operating systems.

Microsoft Windows	Windows 7 (32-bit and 64-bit)
	Windows 8.0 (32-bit and 64-bit)
	Windows 8.1 (32-bit and 64-bit)
	Windows 8.1U1/U2 (32-bit and 64-bit)
	Windows 10
	Windows Server 2008 R2
	Windows Server 2012
	Windows Server 2012 R2

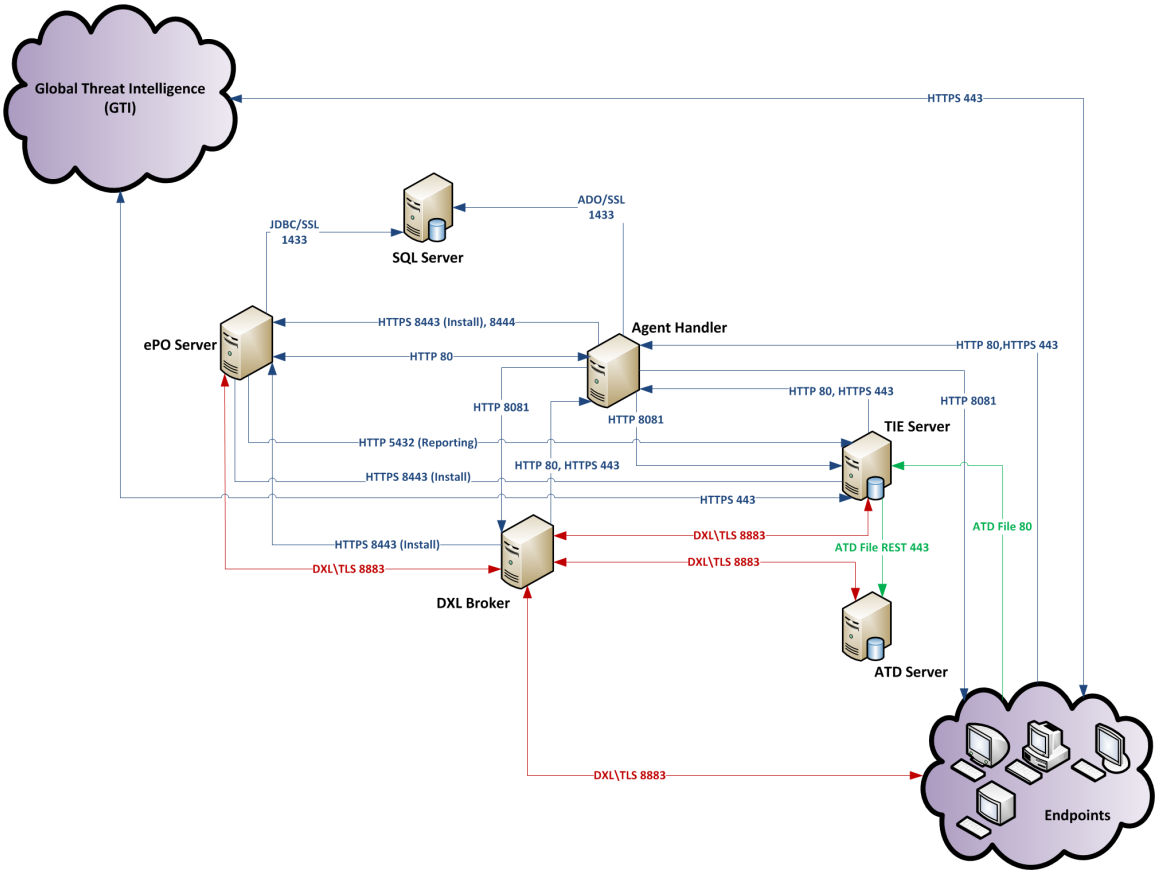
Threat Intelligence Exchange supports all operating systems that McAfee Endpoint Security supports except Windows Vista.

Threat Intelligence Exchange network overview

Threat Intelligence Exchange uses these network protocols and ports.

Make sure that these ports are open and available for use with Threat Intelligence Exchange.

We recommend using the default configuration of the ports.



This table describes the endpoints, network protocols, and ports of the diagram, from top to bottom, left to right.

McAfee Web Gateway Server and Advanced Threat Defense communicate with the TIE Server through DXL.

Table 2-1 Default ports for use with Threat Intelligence Exchange

Network components	Port
Global Threat Intelligence (McAfee GTI)	HTTPS 443
SQL Server	JDBC/SSL and ADO/SSL 1433
ePolicy Orchestrator Server	HTTPS 8443 (Install), 8444; HTTP 80; DXL/TLS 8883
Agent Handler	HTTP 80 and HTTPS 443
DXL Broker	DXL/TLS 8883

Table 2-1 Default ports for use with Threat Intelligence Exchange *(continued)*

Network components	Port
TIE Server	HTTP 8081; HTTP 80; HTTPS 443; DXL/TLS 8883; ATD File HTTPS 443, HTTP 80; HTTP 5432; TCP 5432; HTTPS 8443 (Install)
Advanced Threat Defense Server	ATD File REST 443; DXL/TLS 8883

Installing Threat Intelligence Exchange server and module

Install the server and the module using one of the following methods.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- Install the software using one of these methods:
  - **Software Manager** — Click **McAfee Threat Intelligence Exchange**, then download or check in the components.
  - **Auto-installable ISO file** — Run the ISO file in XEN, Hyper-V, or bare metal. See KB86324 for more details about these virtualization platforms.
  - **Manually** — Download the Threat Intelligence Exchange files from the McAfee product download website at www.support.mcafee.com. Download the server appliance file and save it locally before continuing. The following tasks include detailed instructions for installing the server.

Tasks

- *Install the TIE client module* on page 14
  Install the client module for VirusScan Enterprise or for Endpoint Security.
- *Install the TIE server appliance* on page 14
  Install and configure the TIE server and the Data Exchange Layer brokers.

Install the TIE client module

Install the client module for VirusScan Enterprise or for Endpoint Security.

- For installing the TIE module for VirusScan Enterprise, navigate to **Software Manager** | **McAfee Threat Intelligence Exchange**, then download or check in the components, or manually download the TIE files from McAfee product download website.
- For installing Threat Intelligence for Endpoint Security, on the security management console, navigate to **Menu** | **Dashboards**, then select **Guided Configuration** from the drop-down list and follow the wizard steps.

Install the TIE server appliance

Install and configure the TIE server and the Data Exchange Layer brokers.

Make sure the server extension is installed correctly before you deploy the OVA appliance.

Task

1 Deploy the OVF template:

   a Extract the TIE Server Appliance .zip file that you downloaded from McAfee ePO Software Manager.

   b Open the VMware vSphere client, then click **File** | **Deploy OVF Template**.

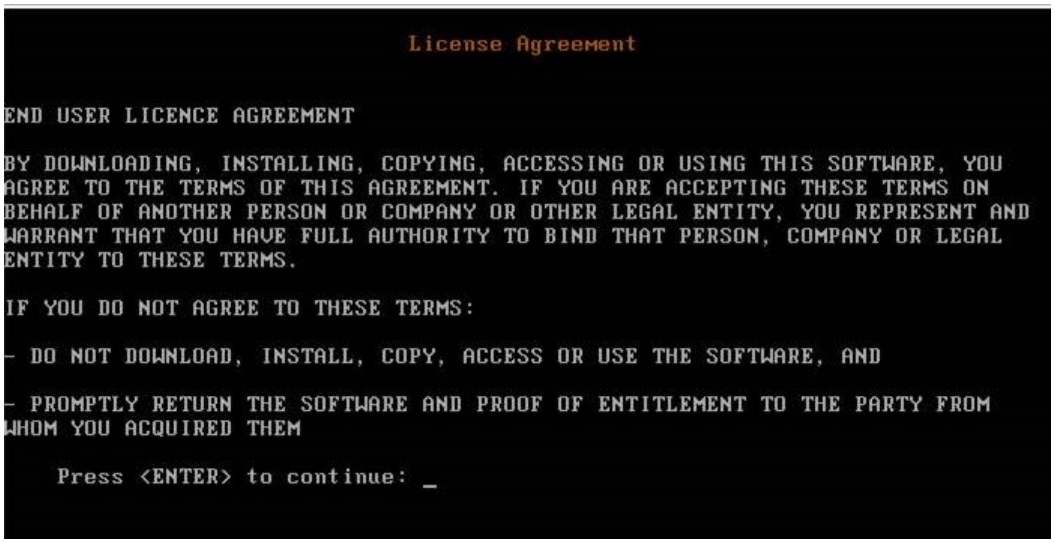
   c Browse to and select the TIE .ova file on your computer, then click **Next** to start the installation wizard.

   d Complete the steps in the wizard, accepting the default values or entering different values as needed.

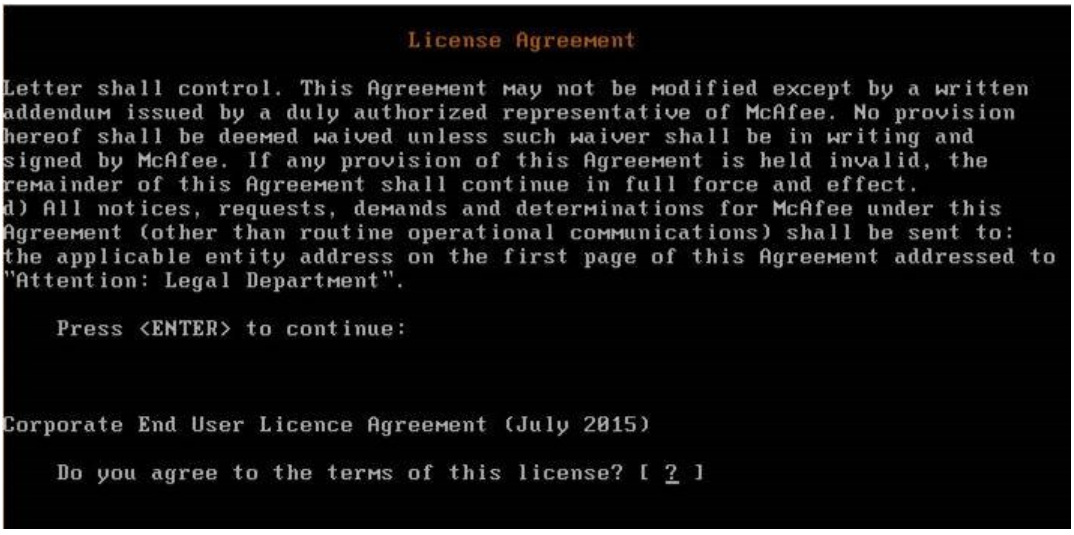
2 When finished, select **Power On** to turn on the virtual machine and open a **Console** window.

3 Install the server appliance.

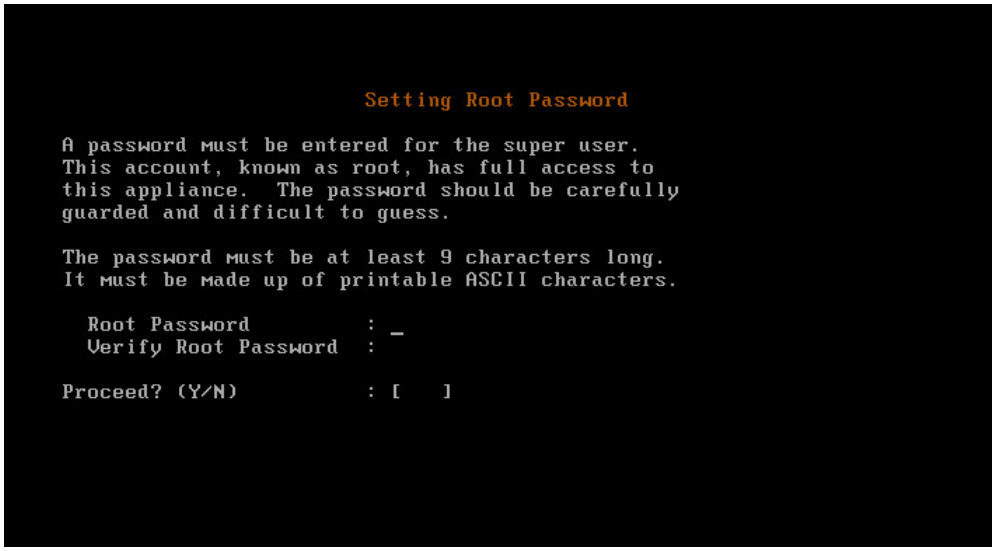
   a Read and accept the license agreement. Press **Enter** to view each page.



When finished reading the license agreement, enter **Y** to accept the terms and continue.

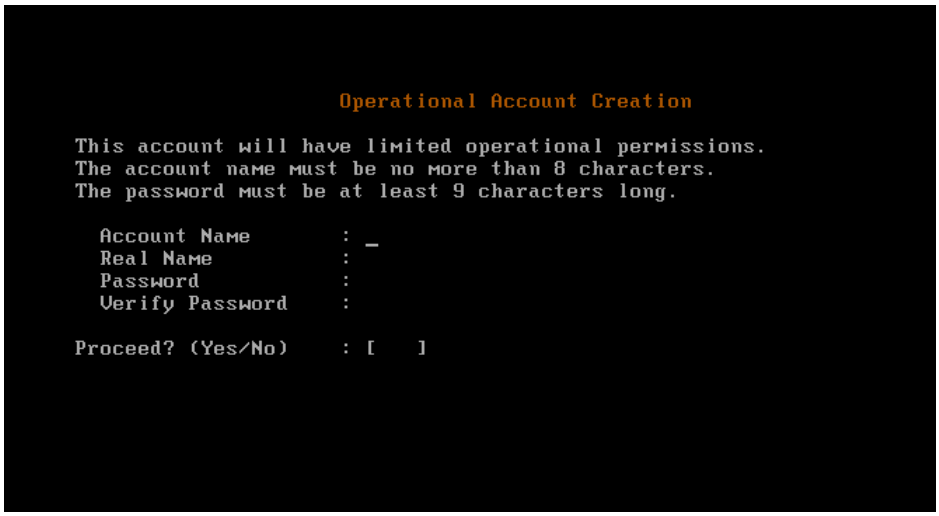


b Create a root password for the TIE appliance. The password must be at least nine characters. Then press **Y** to continue.

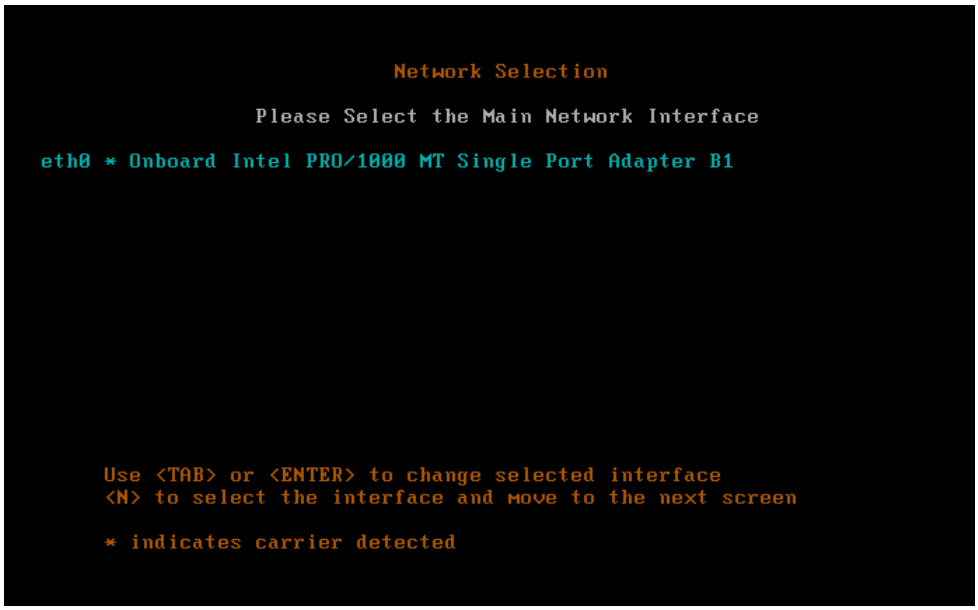


c Enter the operational account name, real name, and password, using the **Tab** key to move to the next field. When finished, press **Y** to continue.

The account name is typically something like `jsmith` and is used to log on to the server. The real name is your full name, for example, `John Smith`.

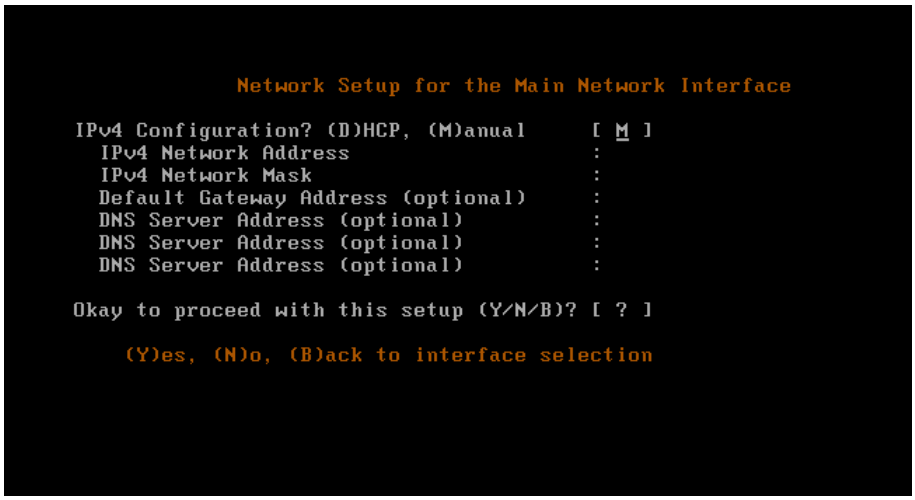


d On the **Network Selection** page, enter **N** to continue.

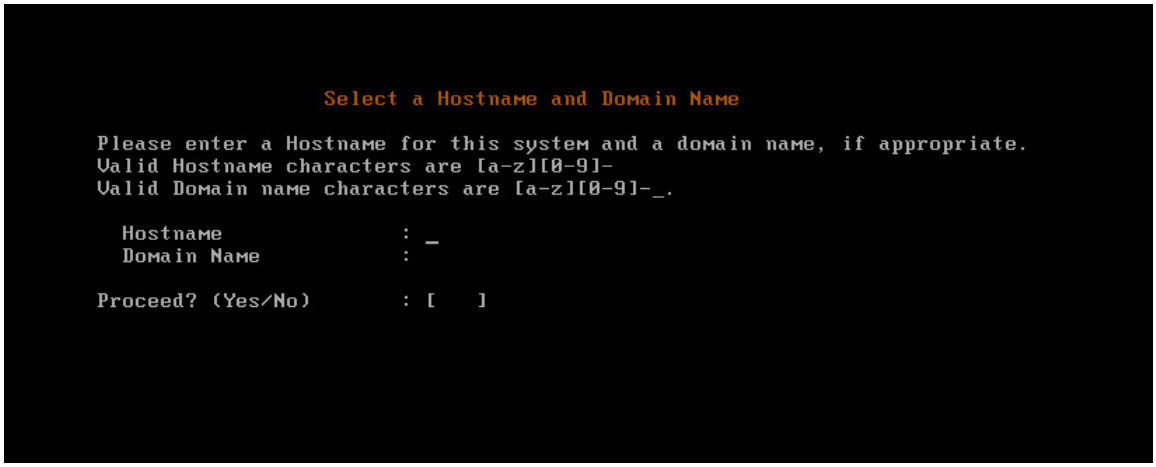


e Select a configuration type, then enter **Y** to continue.

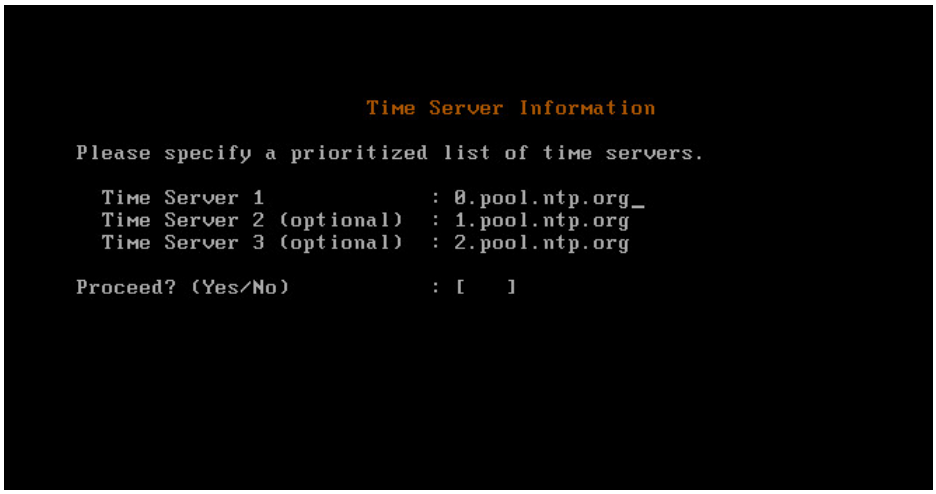
- Manual IP address — Enter **M**, then enter the remaining information.
- DHCP — Enter **D**.



f Enter the host name and domain name of the computer where you are installing the TIE server appliance. Enter **Y** to continue.

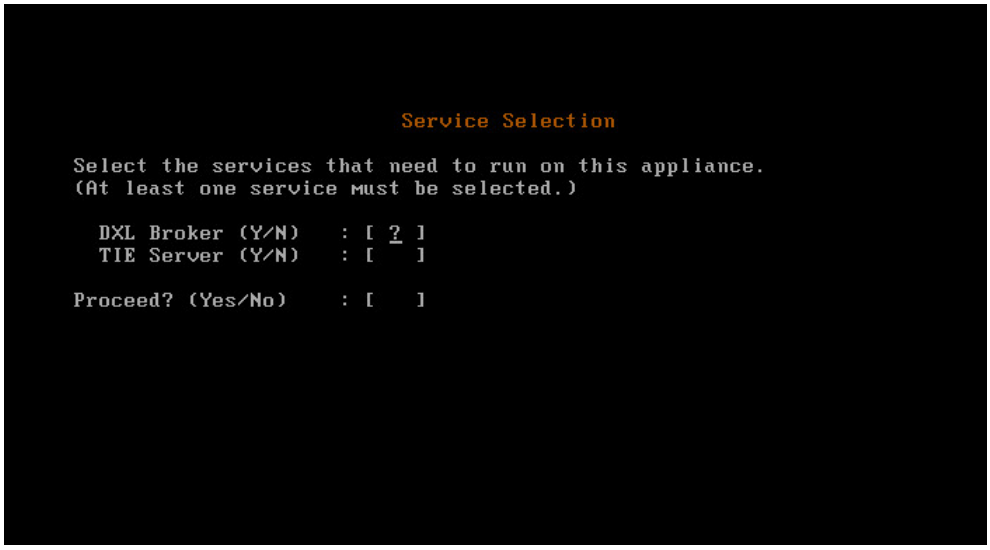


g Enter up to three Network Time Protocol servers to synchronize the time of the TIE server. Use the default servers listed, or enter the address for up to three servers. Enter **Y** to continue.



h Enter the IP address or fully qualified domain name, port, and account information for your McAfee ePO server. The user account must have administrator rights. Enter **Y** to continue.

i Select the services to run on the TIE server, then enter **Y** to continue.



The next page appears only if you selected the **TIE Server** option on the previous page.

j Specify how to configure the primary and secondary servers.

You can have only one primary server in your environment, but you can have several optional secondary servers. Install the primary server first.

- **Master** server replicates the TIE database to all slave servers, if you have them. There can be only one Master server at a time.
- **Write-only Master** server doesn't process reputation requests or any non-essential functionality beyond writing and maintaining the database. Because a write-only master server doesn't process requests over the Data Exchange Layer, it increases system performance by replicating the database, leaving the Data Exchange Layer requests to the slave servers.

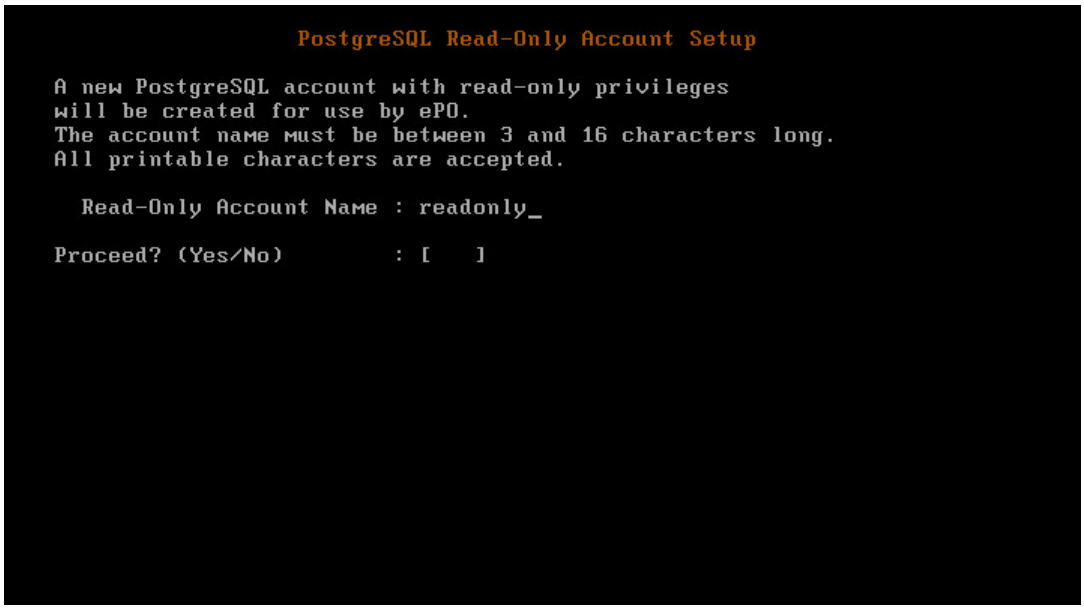
- **Slave** server processes Data Exchange Layer requests exactly like a master server, using a database that's replicated from the master database. Slave servers provide faster response time, and increased availability and scalability. The slave server must have access to the master server.
- **Reporter** is a slave server that provides data to McAfee ePO and does not process reputation requests. The Reporter does not serve queries or aggregate updates, however it has a complete copy of the database and reduces the load on the Master server.

For more details, see the architecture guide for DXL.

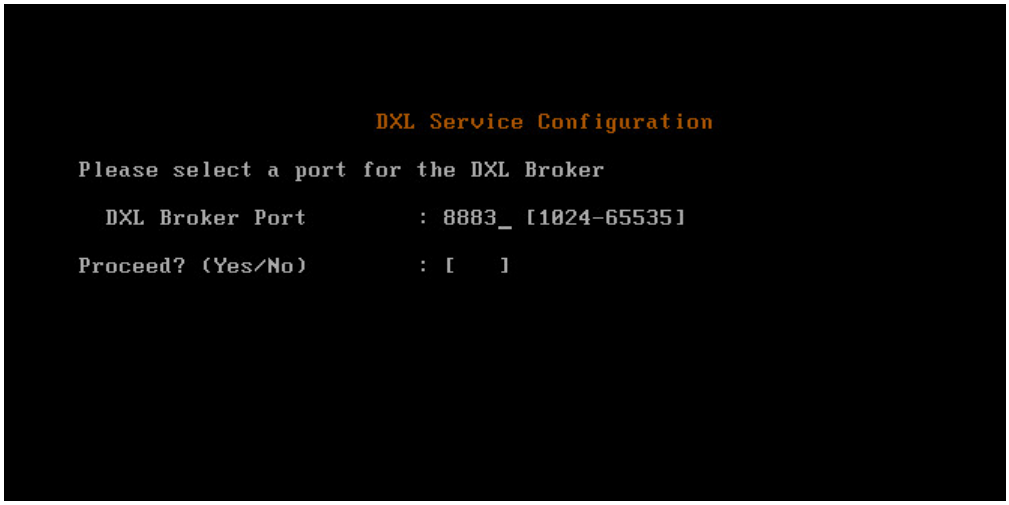
k Enter the Postgres database account information.

The PostgreSQL account allows the McAfee ePO server to connect to and receive data from the TIE server. The information entered here is used in the McAfee ePO **Registered Servers** page.

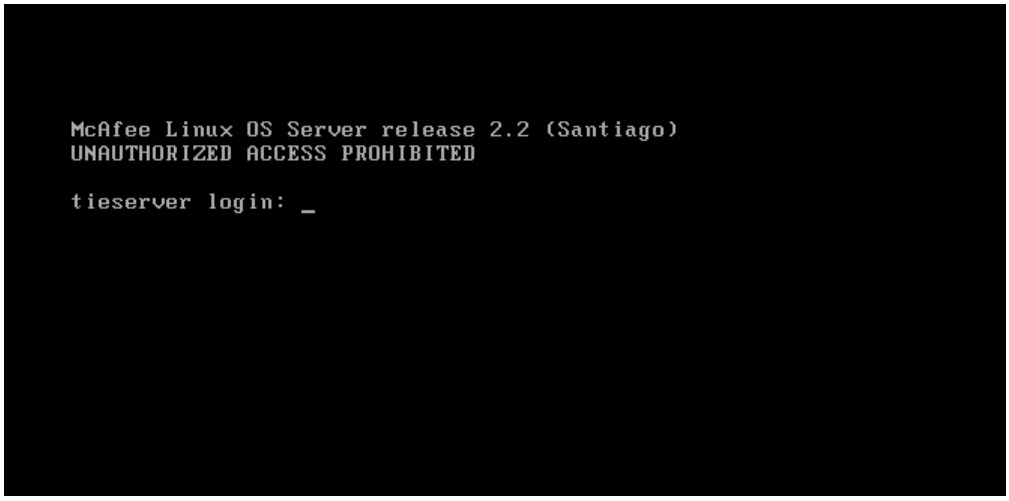
The account name can be anything you like within the stated parameters.



l Specify the port that the Data Exchange Layer uses. Use the default port, or enter a port number within the range shown, then enter **Y** to continue.



m When the logon screen appears, close it.



4 Verify that the TIE server is provisioned: open the System Tree in McAfee ePO and look in the domain where you installed the server appliance.

If provisioned correctly, the server is listed as a managed system. The appliance also shows the DXLBROKER or TIESERVER tag, depending on the products installed.

Tasks

- *Install the server using an ISO file* on page 22
  Deploy the TIE Server using an auto-installable ISO file to run in these virtualization platforms: XEN, Hyper-V or bare metal.

Install the server using an ISO file

Deploy the TIE Server using an auto-installable ISO file to run in these virtualization platforms: XEN, Hyper-V or bare metal.

Before you begin

Your Virtual Machine (VM) must meet the following requirements.

- One CPU with 8 cores.
- 16 GB of RAM (minimum 4 GB).
- 120-GB disk (thick provisioning).

The TIE Server runs in its own custom Linux distribution based on CentOS 6 (x86_64) with Linux kernel v3.18.26. To support different virtualization methods, initial scripts load different kernel modules depending on the virtualization platform detected.

TIE was tested in the Hyper-V virtualization software that is packaged in Windows Server 2012 and Windows Server 2012 R2, and in Citrix XEN 6.5.0 build 90233c. We recommend using Hyper-V and XEN as virtualization platforms. See KB86324 for details.

The pre-requisites and the installation steps described apply for XEN, Hyper-V, and bare metal.

We describe the steps that appear during the installation. The installation is automatic and doesn't need interaction with the user. Wait for the process to be completed.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1. Create your VM and boot the ISO provided.

   Remember to create your VM meeting the requirements mentioned.

   The ISO file detects the type of virtualization and loads the corresponding kernel modules.
2. The complete disk is partitioned.
3. Basic RPMs are installed.
4. The TIE Platform and several custom RPMs are installed.
5. The ISO installs the correct kernel.
6. A dialog box informs that ISO is turning off the VM.
7. Remove the ISO file and turn on the VM.

You can continue installing and configuring the TIE Server.

Supporting multiple ePO servers

Combine TIE server deployments and determine your hardware requirements before you deploy TIE.

Combining TIE server deployments

When bridging multiple McAfee ePO servers (for example, ePO-A and ePO-B) to shared DXL brokers, TIE servers are also shared by users of both McAfee ePO servers.

For details about the bridging capabilities of DXL Broker, see the product guide and the *Data eXchange Layer Architecture Guide*for DXL.

The DXL Client is embedded and can't be deployed or upgraded.

Managed endpoint systems, as the appliance, are still managed by McAfee ePO.

See KB83896 for details about how to migrate TIE servers and recommendations.

Sizing and performance

Determine your hardware requirements before your TIE deployment by gathering reference metrics. McAfee performed these tests on different server-class systems. The metrics were caching impact, scalability, replication bandwidth, and broker latency.

Here is an overview of each item. See *McAfee Threat Intelligence Exchange Sizing and Performance Guide* for more details.

- Caching — Measures the effect of the TIE Client and TIE Server caching over network usage and the response time for receiving TIE reputation requests for existing and new files.
- Scalability — Measures the response time for receiving TIE reputation requests for existing and new files as the number of clients increases and the bandwidth usage when many clients make TIE requests at once.

- Replication bandwidth usage— Identifies and describes the network traffic generated when deploying one TIE Server and different TIE server master/slave instances.
- Broker latency — Analyzes response time when a connected client requests TIE reputation information, and the request must undergo different number of appliances before reaching a TIE Server.

Deploy the Data Exchange Layer client

Deploy the DXL client to each of your managed systems.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1. Select **Menu** | **Software** | **Product Deployment**, then click **New Deployment**.
2. Complete the new deployment information, then start the deployment.

For details about deploying software in McAfee ePO, see the *McAfee ePolicy Orchestrator Product Guide*.

Verify the installation

After installing the Threat Intelligence Exchange and Data Exchange Layer components, perform this task to verify the installation.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1. In the **System Tree**, click the TIE server name, then click the **Products** tab. Verify that the following components are listed with the corresponding version for the installation process:
   - McAfee DXL Broker
   - McAfee DXL Client
   - McAfee Threat Intelligence Exchange Server
2. In the **System Tree**, verify that the TIESERVER tag was applied to the system.
3. Select **Menu** | **Configuration** | **Server Settings**, then click **DXL Client for ePO**.
4. Verify that the **Connection State** is **Connected**.
5. In the **System Tree**, select the TIE server, then from the **Actions** menu, select **DXL** | **Lookup in DXL**.
6. Verify that the **Connection State** is **Connected**.

The DXL broker is now up and running. You can select **Menu** | **Systems Section** | **TIE Reputations** to verify that you can search for files and certificates. It might take some time for reputation information to populate the database. If you can't search for files and certificates, see *Troubleshooting the installation*.

Configure the TIE server extension

Configure the TIE server extension for use with VirusTotal.

If you use VirusTotal, enter your public or private key to access additional file reputation information. VirusTotal is a service that analyzes files and helps to detect viruses, trojans, and other malware. You can access VirusTotal data directly from Threat Intelligence Exchange when viewing file reputation information.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1. Select **Menu** | **Configuration** | **Server Settings** | **Threat Intelligence Exchange Server**.
2. Click **Edit** and enter your VirusTotal key.

When viewing file reputations on the **TIE Reputations** page, click the **VirusTotal** tab to see additional file information.

Tasks

- *Configure the TIE server policy* on page 25
  Specify McAfee GTI and McAfee Advanced Threat Defense settings for the server.

Configure the TIE server policy

Specify McAfee GTI and McAfee Advanced Threat Defense settings for the server.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1. In McAfee ePO, select **Menu** | **Policy** | **Policy Catalog**.
2. From the **Product** drop-down list, select **McAfee Threat Intelligence Exchange Server Management**, then select a policy name or an action.

   You can create a policy using **Default** as a template, or copy an existing policy and change it as needed.
3. On the **General** tab, complete these options:
   - **GTI Reputations** — Specify whether to use McAfee GTI to get file reputation. McAfee GTI is used if the TIE server does not have reputation information for a file, or if the server is unavailable (offline).
   - **Proxy Settings for GTI Requests** — If you use a web proxy for Internet access and it requires authentication, enter the proxy information.
   - **Product Improvement Program** — Specify whether to send file and certificate information to McAfee. For details about what is sent to McAfee, see *Submitting files for further analysis*.
4. On the **Advanced Threat Defense** tab, specify whether to send file information to Advanced Threat Defense for further evaluation. Enter the Advanced Threat Defense server name and access credentials, available servers, and timeout settings.
5. On the **McAfee Web Gateway** tab, view the report sent to the TIE server about potential web threats. On the same tab, there is a checkbox for the user to accept or ignore incoming McAfee Web Gateway reports.

Create a new registered server

To view TIE information in McAfee ePO reports and dashboards, create a new registered server in McAfee ePO.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1. In McAfee ePO, select **Menu** | **Configuration** | **Registered Servers**, then click **New Server**.
2. In the **Server type** drop-down list, select **Database Server**.
3. Enter a **Name**, for example, `TIE Server`, then click **Next**.
4. On the **Details** page:
   a. Select **Make this the default database for the selected database type**.

      This option is automatically selected when you create the first registered server. If you have more than one Threat Intelligence Exchange database, select this option only for the database that you want as the default.

   b. In the **Database Vendor** field, select **TieServerPostgres**.

   c. In the **Host name or IP address** field, enter the IP address of the system where you installed the server.

   d. Leave the **Database server instance** and **Database server port** fields blank (if they appear).

   e. For the **Database name**, enter `tie`.

   f. In the **User name** field, enter the read-only Postgres user name that you specified on the PostgreSQL page during the server installation.
5. Click **Test Connection**.

McAfee ePO communicates with the server and retrieves data for the reports and dashboards.

Troubleshooting the installation

Find solutions for common issues that might occur during installation.

You can also access scripts for reconfiguring the TIE server, DXL brokers, and the McAfee Agent.

Verify installed components

If you experience problems installing and accessing the Threat Intelligence Exchange module for VirusScan Enterprise server, or the Data Exchange Layer client, follow these steps.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1. Wake up the agent on the TIE server.
   a. In McAfee ePO, select **Menu** | **System Tree**, then select the checkbox for the TIE server.

   b. Click **Wake Up Agents**.

   c. On the **Wake Up McAfee Agent** page, select **Force complete policy and task update**, then click **OK**.

      This option sends the server properties from the TIE appliance to McAfee ePO.

d Select **Menu** | **Automation** | **Server Task Log** to verify that the task completed.

e In the **System Tree**, click the server name, click the **Products** tab, then verify that these components are listed:

- McAfee DXL Broker
- McAfee DXL Client
- McAfee Threat Intelligence Exchange Server

2 Apply the TIESERVER tag to the TIE server.

a Select **Menu** | **Automation** | **Server Tasks** and run the task **Apply TIESERVER tags to TIE Server**.

b Select **Menu** | **Automation** | **Server Task Log** to verify that the task completed.

c In the **System Tree**, verify that the TIESERVER tag was applied to the system.

3 Run the **Manage DXL Brokers** task.

a Select **Menu** | **Automation** | **Server Tasks** and run the task **Manage DXL Brokers**.

b Select **Menu** | **Automation** | **Server Task Log** to verify that the task completed.

c In the **System Tree**, click the server name and verify that the DXLBROKER tag was applied to the system.

4 After the tags are successfully applied, wake up the agent on the TIE server.

a In McAfee ePO, select **Menu** | **System Tree**, then select the checkbox for the TIE server.

b Click **Wake Up Agents**.

c On the **Wake Up McAfee Agent** page, select **Force complete policy and task update**, then click **OK**.

d Select **Menu** | **Automation** | **Server Task Log** to verify that the task completed.

5 Verify DXL configuration.

a Select **Menu** | **Configuration** | **Server Settings**, then click **DXL ePO Client**.

b Verify that the **Connection State** is **Connected**.

If it isn't, repeat steps 2–4.

6 In the **System Tree**, select the TIE server, and from the **Actions** menu, click **DXL** | **Lookup in DXL**.

Verify that the **Connection State** is **Connected**.

7 Verify that the DXL and TIE services are running:

a On the virtual machine, open a Console window and log on.

b Enter `service dxlbroker status`.

c Enter `service tieserver status`.

8 With the DXL broker up and running successfully, verify that you can search for files and certificates.

a Select **Menu** | **Systems Section** | **TIE Reputations**.

b Enter `*` in the **Quick find** box, then click **Apply**.

c Select any file from the result and verify that the **TIE File Reputations Information** is displayed.

d If it isn't, repeat steps 2–4.

Accessing the log files

To troubleshoot installation problems, see the following directories and access the log files.

Endpoint Security Threat Intelligence server — `/var/McAfee/tieserver/logs/tieserver.log`

Endpoint Security Threat Intelligence module for VirusScan Enterprise — `%programdata%\McAfee\TIEM`

Endpoint Security Threat Intelligence — `%programdata%\McAfee\Endpoint Security\Logs\ThreatIntelligence_Activity` and `ThreatIntelligence_Debug`

Data Exchange Layer Client — `%programdata%\McAfee\Data_eXchange_Layer`

Data Exchange Layer Broker — `/var/McAfee/dxlbroker/logs/dxlbroker.log`

See KB82850 for details about using the Minimum Escalation Requirements (MER) tool to collect product data from the server and contact technical support. This tool runs in McAfee ePO and endpoints. See KB59385 for details about using the MER tool with McAfee products.

Reconfiguring the installation using scripts

Scripts are available to reconfigure the TIE server, the DXL brokers, and the McAfee Agent.

Accessing the scripts

The scripts are located in the `/home/<username>` directory. They must be executed with sudo permissions, for example, `sudo /home/myname/change-hostname`.

Script name	Description	Reboot?
change-hostname	Changes the host name of the current DXL broker appliance. It restarts the McAfee Agent and the broker.	Recommended
change-services	Enables or disables the DXL broker. If the broker was initially disabled during first boot, the script prompts for broker configuration information.	No
reconfig-dxl	Reconfigures the DXL port.	No
reconfig-ma	Reconfigures the McAfee Agent. The agent and DXL broker services are restarted. New keystores are generated when the service starts.	Recommended
reconfig-network	Reconfigures the current network interface (from DHCP to manual, or from manual to DHCP).	Recommended
reconfig-ntp	Reconfigures the Network Time Protocol servers.	No
reconfig-tie	Changes the role of the TIE server. For example, changes the server from a slave to a master, or from a master to a reporter.	No
reconfig-ca	Obtains an updated Certificate Authorities chain from McAfee ePO and stores it in the TIE server.	No
reconfig-cert	Generates a new certificate and sends a signing request to McAfee ePO through the TIE server extension.	No

3 Using Threat Intelligence Exchange

Block or allow files and certificates in your environment based on their reputation settings, and view and respond to threat events.

Contents

Getting started

After you install Threat Intelligence Exchange, what do you do next?

To get started with TIE, do the following:

- Create TIE policies to determine what is allowed and blocked. Then run TIE in observation mode to build file prevalence and observe what TIE detects in your environment. File prevalence is how often a file is seen in your environment.
- Monitor and adjust the policies, or individual file or certificate reputations to control what is allowed in your environment.

Building file prevalence and observing

After installation and deployment, start building file prevalence and current threat information.

You can see what is running in your environment and add file and certificate reputation information to the TIE database. This information also populates the graphs and dashboards available in the module where you view detailed reputation information about files and certificates.

To get started, create one or more TIE policies to run on a few systems in your environment. The policies determine:

- When a file or certificate with a specific reputation is allowed to run on a system
- When a file or certificate is blocked
- When the user is prompted for what to do
- When a file is submitted to Advanced Threat Defense for further analysis

While building file prevalence, you can run the policies in Observation mode. File and certificate reputations are added to the database but no action is taken. You can see what Threat Intelligence Exchange blocks or allows if the policy is enforced.

For details, see *Create a new policy*.

Monitoring and making adjustments

As the policies run in your environment, reputation data is added to the database.

Use the McAfee ePO dashboards and event views to see the files and certificates that are allowed or blocked based on the policies.

You can view detailed information by system (computer), file, rule, or certificate, and quickly see the number of items identified and the actions taken. You can drill-down by clicking an item, and adjust the reputation settings for specific files or certificates so that the appropriate action is taken.

For example, if a file's default reputation is suspicious or unknown but you know it's a trusted file, you can change its reputation to trusted so that it runs in your environment without being blocked or prompting the user for action. This is especially useful for internal or custom files used in your environment.

- Use the TIE Reputations feature to search for a specific file or certificate name. You can view details about the file or certificate, including the company name, SHA-1 and SHA-256 Hash values, MD5, description, and McAfee GTI information. For files, you can also access VirusTotal data directly from the TIE Reputations details page to see additional information.
- Use the Reporting Dashboard page to see several types of reputation information at once. You can view the number of new files seen in your environment in the last week, files by reputation, files whose reputations recently changed, systems that recently ran new files, and more. Clicking an item in the dashboard displays detailed information.
- If you identified a harmful or suspicious file, you can quickly see which systems ran the file and might be compromised.
- Change the reputation of a file or certificate as needed for your environment. The information is immediately updated in the database and sent to all devices in your environment. Files and certificates are blocked or allowed based on their reputation.

  If you're not sure what to do about a specific file or certificate, you can block it from running while you learn more about it. Unlike a VirusScan Enterprise Clean action, which might delete the file, blocking keeps the file in place but doesn't allow it to run. The file stays intact while you research it and decide what to do.
- Import file or certificate reputations into the database to allow or block specific files or certificates based on other reputation sources. This allows you to use the imported settings for specific files and certificates without having to set them individually on the server.

Data storage management

Manage your database size with data retention policies to avoid service degradation for database growth.

A scheduled task is executed to check database size and to compare it with a size threshold. If the database exceeds the configured threshold, the cleanup is executed.

The task cleans the database of files older than 90 days and, by default, is executed every day at midnight when the size of the database grows beyond 20GB.

The file selection criteria determines that files without an Enterprise reputation or a reputation override, which are older than 90 days are candidates for a purge.

Blocking or allowing files and certificates

Files and certificates have threat reputations based on their content and properties. The Threat Intelligence Exchange policies determine whether files and certificates are blocked or allowed on systems in your environment based on reputation levels.

There are three security levels depending on how you want to balance the rules for particular types of systems. Each level is associated with specific rules that identify malicious and suspicious files and certificates.

- **High change systems** — Systems that change frequently, often installing and uninstalling programs and receiving frequent updates. Examples of these systems are computers used in development environments. Fewer rules are used with policies for this setting. Users see minimum blocking and prompting when new files are detected.
- **Typical systems** — Typical business systems where new programs and changes are installed infrequently. More rules are used with policies for this setting. Users experience more blocking and prompting.
- **Low change systems** — IT-managed systems with tight control and little change. Examples are systems that access critical or sensitive information in a financial or government environment. This setting is also used for servers. The maximum number of rules are used with policies for this setting. Users experience even more blocking and prompting.

To view the specific rules associated with each security level, select **Menu** | **Server Settings**. From the Setting Categories list, select **Threat Intelligence Exchange module for VSE**.

When determining which security level to assign a policy, consider the type of system where the policy is used, and how much blocking and prompting you want the user to encounter. After you create a policy, assign it to computers or devices to determine how much blocking and prompting occurs.

Create a TIE module policy

Policy settings determine when a file or certificate is allowed to run, is blocked, or if users are prompted what to do.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1. Select **Menu** | **Policy** | **Policy Catalog**.
2. From the **Product** list, select **Threat Intelligence Exchange module for VSE**.
3. On the **My Default** line, click **Duplicate** to create a policy.
4. Enter a name for the new policy and a brief description, then click **OK**.
5. Complete the fields on the Policy Catalog page. See the online Help for details about each field.

After you create a policy, assign it to computers or devices to determine how much blocking and prompting occurs. After the policy runs in your environment for a time, you might need to fine-tune what is allowed, blocked, and prompted.

Submitting files for further analysis

If a file's reputation is unknown, you can submit it to Advanced Threat Defense for further analysis. Specify in the TIE policy which files you submit.

Advanced Threat Defense detects zero-day malware and combines anti-virus signatures, reputation, and real-time emulation defenses. You can send files automatically from TIE to Advanced Threat Defense based on their reputation level and file size. File reputation information sent from Advanced Threat Defense is added to the TIE server database.

McAfee GTI Telemetry Information

The file and certificate information sent to McAfee GTI is used to understand and enhance reputation information. See the table for details on the information provided by McAfee GTI for files and certificates, file-only, or certificate-only.

Category	Description
File and certificate	• TIE server and module versions • Reputation override settings made with the TIE server • External reputation information, for example from Advanced Threat Defense
File-only	• File name, path, size, product, publisher, and prevalence • SHA-1, SHA-256, and MD5 information • Operating system version of the reporting computer • Maximum, minimum, and average reputation set for the file • Whether the reporting module is in Observation mode • Whether the file was allowed to run, was blocked, or was cleaned • The product that detected the file, for example Advanced Threat Defense or VirusScan Enterprise
Certificate-only	• SHA-1 information • The name of the certificate's issuer and its subject • The date the certificate was valid and its expiration date

McAfee does not collect personally identifiable information, and does not share information outside of McAfee.

Changing default threat reputations

With Threat Intelligence Exchange, you can set file and certificate reputations for use in your specific environment.

Based on settings in the TIE policies, files and certificates are allowed or blocked, or require user action depending to their reputation. To fine-tune what is allowed or blocked in your environment, you can override default reputation settings for specific files and certificates.

How reputations are added to the TIE database

File and certificate reputations are added to the TIE database in three ways:

- Run the Threat Intelligence Exchange module for VirusScan Enterprise.
- Advanced Threat Defense sends reputation information over the Data Exchange Layer framework and is added to the database.
- Manually add files or certificates to the database.

Scenarios

- Your environment commonly uses a file whose default reputation is unknown or might be classified malicious because it is a custom file. Because you know that the file is safe, you can change its reputation to trusted so that it runs without interference.
- You want to block a common, trusted file from running in your environment, such as a file that allows remote desktop access. You can change its reputation to malicious, blocking it from running on systems in your environment.
- Users prompted when a specific file tries to run. You look up the file's reputation and see that is in unknown. You then look at the file details and determine that it is a trusted file. You can then change its reputation to trusted so that it no longer prompts users.
- You have set file or certificate reputations and you want to import them into the TIE database. You can add those reputations one at a time, or in a batch using an XML file.

Change the reputation of a file or certificate

Change the reputation of a file or a certificate to allow or block it in your environment.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1. Select **Menu** | **Systems** | **TIE Reputations**.
2. Click the **File Search** or **Certificate Search** tab.
3. Search for files or certificates by name or by file type, such as .dll or .exe. You can also use wildcard search characters * or ?. See *Searching for a file or certificate* for more details about searching for files and certificates.

   To view details about a specific file or certificate, including its Hash number, click its name. Examine the details and VirusTotal information for the file to determine how to classify it.
4. Select items in the list and use the **Actions** menu to change the reputation settings. The files or certificates are then added to the overrides list.

   You can add a note about the change, for example, `Researched the file's reputation. Blocking this file.`
5. To verify the change, click the **File Overrides** or **Certificate Overrides** tab to see that the file or certificate is listed with its updated reputation.

Import reputations

Import a file containing file or certificate reputation information to the TIE database.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1. Select **Menu** | **Systems** | **TIE Reputations**.
2. Click the **File Overrides** or **Certificate Overrides** tab.
3. From the **Actions** menu, select **Import Reputations**.

4 In the **Import Reputations** dialog box, specify whether to import an XML file with one or more reputations, or a single reputation.

- **Select the reputation XML file to import** — Browse to the file location. See *Requirements for creating an XML import file* for details.
- **Import single reputation** — Enter the information for the file.

Requirements for creating an XML import file

When importing reputation information in an XML file, the file must meet these requirements.

Specifying the reputation as a number

You must specify the file or certificate reputation as a numeric value in the XML file.

It is mandatory that the file or certificate has, minimum, one hash value and one reputation.

Reputation setting	Numeric value
Known trusted	99
Most likely trusted	85
Might be trusted	70
Unknown	50
Might be malicious	30
Most likely malicious	15
Known malicious	1
Not Set	0

When you change the order of the reputation setting, descending or ascending, the setting list changes its order. For example, when setting the reputation in ascending order, "Not Set" appears first, while in descending order, "Known trusted" appears first.

See the definitions for TIE reputation labels in the following table.

Table 3-1 Option definitions

Option	Definition
Known trusted	It is a trusted file or certificate.
Most likely trusted	It is almost certain that the file or certificate is trusted.
Might be trusted	It seems a benign file or certificate.
Unknown	The reputation provider has encountered the file or certificate before but the provider can't determine its reputation at the moment.
Might be malicious	It seems a suspicious file or certificate.
Most likely malicious	It is almost certain that the file or certificate is malicious.
Known malicious	It is a malicious file or certificate.

Table 3-1 Option definitions *(continued)*

Option	Definition
Not set	The file or certificate's reputation hasn't been determined yet.
Not Available	The reputation provider hasn't been queried about the specific item. This reputation label also appears for disabled reputation providers or providers with pending reputation reports. Most of signed files shows Not Available reputation because the specific file reputation hasn't been queried yet. The client has only queried about its associated certificate reputation.

File reputations

For each file, include its known hash values (SHA-1, SHA-256, and MD5) in hexadecimal encoding. At least one hash value is required for each file. Include the file name to identify it in reports.

Certificate reputations

For each certificate, include its SHA-1 Hash and Public Key SHA-1 values in hexadecimal encoding. Include the certificate name to identify it in reports.

Example import file

```
<?xml version="1.0" encoding="UTF-8"?>
<TIEReputations>
    <FileReputation>
        <FileName>HackIt.exe</FileName>
        <SHA1Hash>0x98AF3632E17677A8A23739F720B1A2F215CB8836</SHA1Hash>
        <MD5Hash>0xDEF30CBEA881149C2AFFDF9A059FB751</MD5Hash>
        <SHA256Hash>0xEF127619BAC9E6790FBC925C339111806DA71FAA0CFA0A1E630BEF32B8B1DF91</
SHA256Hash>
        <ReputationLevel>15</ReputationLevel>
    </FileReputation>
    <FileReputation>
        <FileName>trayMan.dll</FileName>
        <SHA1Hash>0x7F618396A910908019B5580B4DA9031AF4A433CA</SHA1Hash>
        <MD5Hash>0xB2B3DAE040F6B5AE1DF52B0CD7631A18</MD5Hash>
        <SHA256Hash>0xAF37EBACF8697B55A82E5FA0D742E65ABE0953BA6B09EABA6B35B5B1958F37EC</
SHA256Hash>
        <ReputationLevel>15</ReputationLevel>
        <Comment>Comment for ALTTAB</Comment>
    </FileReputation>
</TIEReputations>
```

Example import certificate

```
<?xml version="1.0" encoding="UTF-8"?>
<TIEReputations>
    <CertReputation>
        <SHA1Hash>13D90CAC5FC2C5086E882B13B4BA8115C6F65D09</SHA1Hash>
        <PublicKeySha1>108F9887A4481B94F4C535A9097884F5E29123B8</PublicKeySha1>
        <ReputationLevel>15</ReputationLevel>
        <Comment>Fake ACME certificate</Comment>
    </CertReputation>
</TIEReputations>
```

STIX import

Structured Threat Information eXpression (STIX) import allows the user to import file reputations.

The user selects a STIX standard XML file to import file reputations in a wizard.

Parsing capabilities are built on top of version 1.1.1 of STIX XML schemes.

For more information about STIX, go to www.stix.mitre.org.

Import file reputations using STIX

Add a file reputation to the TIE server.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1. Select **Menu** | **Systems** | **TIE Reputations**.
2. Click the **File Overrides** tab, then from the **Actions** menu, select **STIX import**.
3. Browse to and select the file to import, then click **Next**.
4. Select the items you want to import, then click **Submit selected items**.

   For more information about the Review details and Validations in STIX import, see the online Help.
5. Select the reputation of the file to be imported, add a comment as needed, then click **Confirm** to complete the action.

Changing reputations using McAfee ePO Web API

Use McAfee ePO Web API to change the default reputation for files and certificates with a script.

Threat Intelligence Exchange includes the `tie.setReputations` command. Use the `core.help` command to see details about syntax and options for the `tie.setReputations` command. Data passed to the Web API calls must be URL-encoded. Additional syntax includes:

```
tie.setReputations [fileReps] [certReps]
Json string for file and/or certificate reputation(s) with Base64 encoded hash
values. At least one of fileReps or certReps needs to be specified. Both can be
specified too.
Parameters:
fileReps (param 1) - Json string of file reputation(s). Ex
[{"sha1":"frATnSF1c5s8yw0REAZ4IL5qvSk=","md5":"8se7isyX+S6Yei1Ah9AhsQ==","reputation":"99"},
{"sha1":"d3HtjhR0Eb3qN6c+vVxeqVVe0t4=","md5":"V+0uApv5yjk4PSpnHvT7UA==","reputation":"99"}]
certReps (param 2) - Json string of certificate reputation(s). Ex
[{"sha1":"frATnSF1c5s8yw0REAZ4IL5qvSk=","publicKeySha1":"frATnSF1c5s8yw0REAZ4IL5qvSk=","reput
ation":"99"}]]
```

For details about using this API, see *McAfee ePO Web Scripting Guide*.

Searching for files and certificates

You can search for files and certificates in the TIE database to see detailed information and change reputation settings.

The longer a client or module runs in your environment, the more populated the database. A file or certificate is added to the database when a client requests information about it.

Searching for files and certificates allows you to see specific details. For example, you can see:

- The associated certificate for a specific file
- Details about a certificate's parent certificate
- Details about a file's parent process
- Current enterprise, McAfee GTI, McAfee Web Gateway, and Advanced Threat Defense reputation settings
- Information of SHA1, SHA256, and MD5 hashes
- Company information
- File name, version, and company information
- Systems that ran a specific file
- Systems that ran files signed by a specific certificate

Search for a file or certificate

There are several ways to search for a file or certificate in the TIE database.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1. Select **Menu** | **Systems** | **TIE Reputations**.
2. Click the **File Search** or **Certificate Search** tab, depending on what you want to search for.
3. Search for a file or certificate using one of these methods:
   - **Custom filter** — Search using specific criteria. Use a default filter or create one of your own. The default filters available are **Malicious files**, **Named files**, **Unknown in GTI**, and **Unnamed files**. See *Create a custom search filter*.
   - **Quick Find** — Search for a specific file or certificate name. You can also use wildcard characters * and ? to find multiple items with similar characteristics.
   - **Sorting results** — Select a column heading to sort the information.

     Sorting results in the Reputations column appear by reputation value rather than alphabetically. For more information about the values, see *Specifying the reputation as a number*.
4. When you find the file or certificate you want, select it to see its details.
5. Use the **Actions** menu to access more information.

Create a custom search filter

You can create a custom filter when searching for files and certificates using the **TIE Reputations** page.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1. Select **Menu** | **Systems** | **TIE Reputations**.
2. In the **Custom** drop-down list, select **Add**.
3. In the Edit Filter Criteria page, select **Reputation Provider**, then select **Reputation**. You must select both of these properties.

4 Enter the search filter criteria for the properties.

5 Click **Update Filter**.

6 From the **Custom** drop-down list, select **(unsaved)**, then click **Save** to name the custom search filter.

Determine where a file or certificate ran in your environment

See the systems in your environment that ran a particular file, or ran files signed by a specific certificate.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1 Select **Menu** | **Systems** | **TIE Reputations**.

2 Click either the **File Search** or **Certificate Search** tab.

3 Enter a specific file or certificate name, or search by type, such as .dll or .exe, then click **Apply**. You can also use wildcard search characters * or ? when searching.

4 Select the file or certificate that you want to see.

5 From the **Actions** menu, select **Where Has File Run** or **Where Has Certificate Run**.

Systems that ran a specific file or files signed by a certificate are listed, including the system name, IP address, and the first date when the file ran on that system.

Determine what files or certificates ran on your system

Sort files or certificates that ran on your system.

The TIE server tracks the files and certificates seen by an agent. This tracking optimizes targeted events, for example, sending an event for a change of reputation. After a threshold of an event of 5,000 agents, the events are only broadcasted.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1 Select **Menu** | **System Tree**.

2 Select a system, then click **Actions** | **TIE** | **Files ran on system** or **Certificates ran on system**.

The list of files or certificates that ran on your system are sorted by reference date and in descending order.

Detection events

The TIE module for VSE and Endpoint Security events page shows recent Threat Intelligence Exchange events and security threats, and the actions taken.

Viewing recent events

Viewing recent events allows you to see threat information about your systems.

You can view enforced or observed events:

- **Enforcement Events** — Events that occur as a result of an enforced Threat Intelligence Exchange policy.
- **Observation Events** — Events that would occur if the policy were enforced. It allows you to view, evaluate, and adjust policy and configuration settings before enforcing them. You can see which files or certificates are causing events, and change their reputation settings so they no longer generate an event.

You can view threat events in several ways and drill down for more information:

Past 30 days — Event summary information for the past 30 days.

Top 10 — The top 10 events by system, file, or certificate.

Certificate — The certificate name, its SHA1 Hash value, and the number of certificates that were cleaned, blocked, or prompted.

File Hash — The file name and SHA1 Hash value, and the number of files that were cleaned, blocked, or prompted.

Rule — The rule name, events where the rule was applied, and the number of rules that were cleaned, blocked, or prompted.

System — The system name, total events for that system, and the number of events that were cleaned, blocked, or prompted on a particular system.

Examples

- If a specific system regularly prompts users, select the system from the list on the **TIE module for VSE Events** page. You can then see details about the specific files or certificates that are causing the prompts. Select individual files or certificates from the Events page and change their reputation levels to allow or block them so that they no longer generate a prompt.
- If a specific file generates events, select it from the list on the Events page and see which systems tried to run it and what action was taken. You can then change the file's reputation so that it no longer generates events. For example, if the file generates a prompt and you want it blocked, change its reputation so that it is blocked and does not generate an event.

View details about recent threats

View information about recent files and certificates seen in your environment and the actions taken.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1 Select **Menu** | **Reporting** | **TIE module for VSE Events**.

The **TIE module for VSE Events** page shows several views of recent events.

2 In the **Select Event View** drop-down list, select the type of events to show.
   - **Enforcement Events** show enforced policy events and the actions taken.
   - **Observation Events** show the observed policy events where no action was taken.

3 Select a chart to see detailed information.

4 In the **Select Pivot Point** drop-down list, select how to view events: by certificate, file hash, rule, or system. Then, select a specific item in the list to see more details.

Respond to events

Use the information on the **TIE module for VSE Events** page to adjust file and certificate reputations to prevent threats and other events.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1 On the **Events** page, you can see the items that are generating events. Click an event to see its details.

2 If you selected a file or certificate that's causing a block or prompt based on its reputation, change its reputation setting to stop the event.

   Use the options on the Actions menu to change its reputation.

Submitting file samples

Every TIE master and slave server instance (except Reporters and Write-only) can submit file samples to McAfee® Advanced Threat Defense for analysis.

It is configured via McAfee ePO policies for different endpoint groups. The Advanced Threat Defense instances should be grouped based on their geographical distribution. You assign TIE server policies for each group of Advanced Threat Defense instances based on their geographical location. Use this configuration especially in large scale deployments.

This configuration is used together with the broker affinity and the service zone features of Data Exchange Layer. See the product documentation for DXL for more details.

See KB86707 for more details about this configuration.

Setting a system's health status

Based on the threat events reported and files executed on a system, you can set its health status to see compromised systems and healthy systems.

As events are reported and files are blocked or allowed, you can set the health status of specific systems. You can then monitor compromised systems for threat events, or change policy settings for systems that have run, or often block, malicious or suspicious files.

There are three settings for system health status: **Compromised**, **Healthy**, and **Possibly Compromised**. You can manually set the health status for particular systems using Threat Intelligence Exchange, or create an automatic response query or server task in McAfee ePO to apply a status automatically. You can then create a query that looks for compromised systems and run a server task to take a specific action on those systems.

When creating the automatic response in McAfee ePO, the system health status options are on the Actions page of the wizard. Choose the **Run System Command** action, and from the **System command** drop-down, choose **Set System Health Indicator** and specify the health status.

For details about creating automatic responses, queries, and server tasks, see McAfee ePolicy Orchestrator Best Practices Guide.

Set system health status

Manually set the Threat Intelligence Exchange health status for a system to indicate if it is healthy, compromised, or potentially compromised.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1. Select **Menu** | **Systems Section** | **System Tree**.
2. Select one or multiple systems.
3. From the **Actions** menu, select **System Health**, then choose the health status to apply to the selected systems.

The health status is displayed in the TIE System Health column on the System Tree.

To display the TIE System Health column on the System Tree, from the **Actions** menu, select **Choose Columns**, then from the **Available Columns** list, select **TIE System Health**.

Server tasks

Use synchronizing and monitoring tasks to monitor your TIE servers.

Synchronize certificate authorities in TIE servers

Join different fabrics or synchronize certificate authorities (CA) of the TIE servers in an environment with multiple McAfee ePO servers.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1. Go to **Menu** | **Automation** | **Server Tasks** and run **TIE Server synchronize CA**.
2. Verify that the task is completed in the server task log.

Monitor the health status of the TIE server

Follow the steps to configure server tasks and to generate a server event for each TIE server instance.

This task is created when you install the TIE extension. The task generates a server event for each unreachable TIE server managed by McAfee ePO, and is enabled and scheduled to run by default every hour. The task checks if the TIE server instances respond to the health check message. If the instances respond, it means they are connected to DXL and are running.

If the TIE server instance is unreachable, it doesn't respond to the health check message, then a server event is created by the TIE server extension in McAfee ePO.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1 Navigate to **Menu** | **Automation** | **Automatic Responses**.

2 Create notifications and actions using **Automatic responses**

See the product guide for McAfee ePO for more details about Events and Responses.

You receive a report with information about the severity, the level, the event name, the IP address, the agent ID of the unreachable TIE server instance, and the host name.

Event ID	Severity	Level	Event name
37175	4	Critical	TIE Server Master Unreachable
37176	4	Critical	TIE Server Master Write-Only Unreachable
37177	3	Major	TIE Server Slave Unreachable
37178	3	Major	TIE Server Reporting Unreachable
37179	3	Major	TIE Server Unreachable

The server task is enabled by default during the installation of the TIE extension. If no action is required, disable the task.

Recommended workflow

Assess, prioritize, analyze, and react against threats using the TIE server activities in McAfee ePO.

We provide a brief introduction and overview of each activity. See KB86307 for details about each activity.

For an effective use of TIE capabilities, follow a repeatable and scalable workflow to prioritize and analyze high impact or prevalent threats in the managed environment.

1 Assessing — The dashboards for **TIE Server Files** or **TIE Server Certificates** quickly assess the health status of the environment. From the **Custom** menu you add a new dashboard and specify a name and its visibility.

Navigate: To create a custom dashboard, **Dashboards** | **Dashboards Actions** | **Custom** | **Add**.

2 Prioritizing — The default filters and the **Query and Reports** system in McAfee ePO determine which files or certificates are a priority for analysis.

Navigate: **TIE Reputations** | **File Search** | **Custom**, or **TIE Reputations** | **Certificate Search** | **Custom**.

3 Analyzing — It presents the list of associated files or certificates, their parent files or certificates, where they were run, and their details.

Navigate: **TIE Reputations** | **TIE Files Reputations**, then select an option. Navigate to **TIE Certificate Reputations**, then select an option.

4 Reacting — The manual overrides handle existing malware and protect the environment against future executions. The McAfee ePO can list queries for the systems that were tagged as compromised.

Navigate: **TIE Reputations** | **File Search** | **Actions** | **System Health Indicator** | **Set Possibly Compromised**

4 Queries

You can access Threat Intelligence Exchange reports from the McAfee ePO Queries & Reports feature. There are reports for the TIE server and the TIE module for VirusScan Enterprise or the Threat Intelligence Exchange for Endpoint Security.

Viewing queries

Threat Intelligence Exchange includes several reports that show threat information for files, certificates, and events.

The queries are available in the McAfee ePO **Queries & Reports** page. They show the following information:

- New files and certificates seen in the enterprise
- Files and certificates organized by reputation
- Files and certificates with changed reputations
- Files and certificates with an Enterprise reputation
- Top 10 systems with new files or certificates
- Blocked, allowed, and cleaned events
- Observed events
- Data storage management with a cleanup trending summary

Access reports

You create and view Threat Intelligence Exchange reports using McAfee ePO to view TIE events and file and certificate information.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1. Select **Menu** | **Reporting** | **Queries & Reports**.
2. Use **Quick find** to access TIE reports.
   - For server reports, enter `TIE`.
   - For server and client reports.
3. Click **Run** to see the report data.

See the McAfee ePO documentation for details about creating and using queries and reports.

Index

L

M

N

O

P

R

S

T

V

W