Product Guide

McAfee Threat Intelligence Exchange 2.0.0
For use with McAfee ePolicy Orchestrator
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**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Preface</strong></td>
<td>5</td>
</tr>
<tr>
<td>About this guide</td>
<td>5</td>
</tr>
<tr>
<td>Audience</td>
<td>5</td>
</tr>
<tr>
<td>Conventions</td>
<td>5</td>
</tr>
<tr>
<td>Find product documentation</td>
<td>6</td>
</tr>
<tr>
<td><strong>1 Introduction</strong></td>
<td>7</td>
</tr>
<tr>
<td>Benefits of Threat Intelligence Exchange</td>
<td>7</td>
</tr>
<tr>
<td>Threat Intelligence Exchange components</td>
<td>8</td>
</tr>
<tr>
<td>Threat Intelligence Exchange client</td>
<td>9</td>
</tr>
<tr>
<td>Threat Intelligence Exchange server</td>
<td>9</td>
</tr>
<tr>
<td>Data Exchange Layer</td>
<td>10</td>
</tr>
<tr>
<td>How Threat Intelligence Exchange works</td>
<td>10</td>
</tr>
<tr>
<td>How a reputation is determined</td>
<td>11</td>
</tr>
<tr>
<td><strong>2 Installation</strong></td>
<td>13</td>
</tr>
<tr>
<td>System requirements</td>
<td>13</td>
</tr>
<tr>
<td>Threat Intelligence Exchange network overview</td>
<td>15</td>
</tr>
<tr>
<td>Plan your deployment</td>
<td>16</td>
</tr>
<tr>
<td>Combine TIE server deployments</td>
<td>16</td>
</tr>
<tr>
<td>Installing Threat Intelligence Exchange</td>
<td>16</td>
</tr>
<tr>
<td>Install the TIE server appliance</td>
<td>17</td>
</tr>
<tr>
<td>Install the server using an ISO file</td>
<td>23</td>
</tr>
<tr>
<td>Deploy the TIE client module</td>
<td>24</td>
</tr>
<tr>
<td>Deploy the Data Exchange Layer client</td>
<td>24</td>
</tr>
<tr>
<td>Configure the TIE server extension</td>
<td>24</td>
</tr>
<tr>
<td>Configure the TIE server topology</td>
<td>25</td>
</tr>
<tr>
<td>Configure the TIE server policy</td>
<td>25</td>
</tr>
<tr>
<td>Verify the installation</td>
<td>26</td>
</tr>
<tr>
<td>Verify registered servers</td>
<td>27</td>
</tr>
<tr>
<td>Troubleshooting the installation</td>
<td>28</td>
</tr>
<tr>
<td>Verify installed components</td>
<td>28</td>
</tr>
<tr>
<td>Accessing the log files</td>
<td>29</td>
</tr>
<tr>
<td>Reconfiguring the installation using scripts</td>
<td>30</td>
</tr>
<tr>
<td><strong>3 Using Threat Intelligence Exchange</strong></td>
<td>31</td>
</tr>
<tr>
<td>Getting started</td>
<td>31</td>
</tr>
<tr>
<td>Building file prevalence and observing</td>
<td>31</td>
</tr>
<tr>
<td>Monitoring and making adjustments</td>
<td>32</td>
</tr>
<tr>
<td>Data storage management</td>
<td>33</td>
</tr>
<tr>
<td>Blocking or allowing files and certificates</td>
<td>33</td>
</tr>
<tr>
<td>Create a TIE module policy</td>
<td>33</td>
</tr>
<tr>
<td>Submitting files for further analysis</td>
<td>34</td>
</tr>
<tr>
<td>Changing default threat reputations</td>
<td>35</td>
</tr>
<tr>
<td>Change the reputation of a file or certificate</td>
<td>35</td>
</tr>
</tbody>
</table>
Preface

This guide provides the information you need to work with 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.

Conventions

This guide uses these typographical conventions and icons.

- *Italic* Title of a book, chapter, or topic; a new term; emphasis
- **Bold** Text that is emphasized
- Monospace Commands and other text that the user types; a code sample; a displayed message
- Narrow Bold 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] Note: Extra information to emphasize a point, remind the reader of something, or provide an alternative method
- ![Tip] Tip: Best practice information
- ![Caution] Caution: Important advice to protect your computer system, software installation, network, business, or data
- ![Warning] 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.
Introduction

McAfee® Threat Intelligence Exchange (TIE) server 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 server 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
- Threat Intelligence Exchange components
- How Threat Intelligence Exchange works
- How a reputation is determined

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.
- Integration with McAfee® Endpoint Security Web Control and McAfee® Network Security Platform, among other McAfee products, for exchanging threat reputation information that increases protection and detection capabilities end-to-end.
Threat Intelligence Exchange components

Threat Intelligence Exchange includes these components.

- A module for McAfee® VirusScan® Enterprise or for Endpoint Security that allows you to create policies for blocking and allowing a file 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 client for Endpoint Security (or, optionally, for VirusScan Enterprise) 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.

The client uses rules for determining actions based on multiple datapoints such as reputations, local intelligence, and contextual information. You can update the rules independently.

You can perform these tasks using Threat Intelligence Exchange.

- 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, see McAfee 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 McAfee Data Exchange Layer Product Guide for details about installing and using Data Exchange Layer.

How Threat Intelligence Exchange works

Threat Intelligence Exchange server 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 server 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 server 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 server database. Those reputations are used immediately with no further action.

• See additional information about a file — Threat Intelligence Exchange server 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 online scanning service for viruses, malware, and URLs.
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 client module for McAfee Endpoint Security or for VirusScan Enterprise 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.
   - 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.
   - 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" or "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.

5. 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 server returns the reputation of the file.

6. The module evaluates this metadata to determine the file's reputation:
   - File and system properties
   - Enterprise age and prevalence data
   - Reputation

7. The module acts based on the policy assigned to the system that is running the file.

8. 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.

9. 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 server-enabled systems to immediately protect your environment. TIE server or any other McAfee product can initiate this process. In either case, TIE server processes the reputation and saves it in the database.

For information about how Advanced Threat Defense is integrated with Threat Intelligence Exchange, see *McAfee Advanced Threat Defense Product Guide*.

If McAfee Web Gateway is present

If McAfee Web Gateway is present, the following 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 *McAfee Web Gateway Product Guide*.

If Endpoint Security Web Control is present

When you download a file, SiteAdvisor sends a message to the TIE server with the URL from where the file was downloaded, the URL reputation from McAfee GTI, and the hash value of the file. The information is available on the Associated URL tab on the hash information page. When the TIE server receives a file reputation request, it returns this information as part of its response.
Installation

Threat Intelligence Exchange has these major components: a TIE server and a client for either McAfee Endpoint Security or for VirusScan Enterprise.

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

- TIE server extension
- Threat Intelligence Exchange client module

 Installing the TIE server in FIPS mode

Installing TIE server in *Federal Information Processing Standard* (FIPS) mode follows the same basic procedure described in this guide. But FIPS mode installation requires a McAfee ePO server operating in FIPS mode. See the *McAfee ePolicy Orchestrator FIPS Mode User Guide* at https://support.mcafee.com/.

⚠️ The FIPS mode in the TIE server can't be changed after the installation. Upgrading the TIE server doesn't change the operation mode of FIPS.

Contents

- System requirements
- Threat Intelligence Exchange network overview
- Plan your deployment
- Combine TIE server deployments
- Installing Threat Intelligence Exchange
- Deploy the Data Exchange Layer client
- Configure the TIE server extension
- Verify the installation
- Troubleshooting the installation

System requirements

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

⚠️ The TIE server is distributed as an OVA appliance optimized for VMware or as an ISO image used with compatible hardware or other virtualization technologies.

<table>
<thead>
<tr>
<th>Products</th>
<th>Components</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware vSphere</td>
<td></td>
<td>5.1.0 with ESXi 5.1 or later</td>
</tr>
<tr>
<td>Threat Intelligence</td>
<td>Threat Intelligence</td>
<td>1.2.1 or later for upgrades</td>
</tr>
<tr>
<td>Exchange</td>
<td>Exchange server</td>
<td></td>
</tr>
<tr>
<td>Products</td>
<td>Components</td>
<td>Version</td>
</tr>
<tr>
<td>----------</td>
<td>------------</td>
<td>---------</td>
</tr>
<tr>
<td>Data Exchange Layer client</td>
<td>1.1 or later</td>
<td></td>
</tr>
</tbody>
</table>
| Threat Intelligence Exchange client either for VirusScan Enterprise or for Endpoint Security | • For VirusScan Enterprise — 8.8 Patch 5  
• For Endpoint Security — 10.1 or later |
| McAfee ePO | 5.1.1, 5.1.2, 5.1.3, 5.3.0, 5.3.1, 5.3.2 |
| Product extensions installed on McAfee ePO | VirusScan Enterprise or Endpoint Security 8.8 Patch 5 10.1 or later |
| McAfee Agent | 5.0.1 and 5.0.3 |
| McAfee Agent extension | 5.0 |
| Products installed on managed systems | VirusScan Enterprise or Endpoint Security 8.8 Patch 5 10.1 or later  
This package can be deployed as part of the Endpoint Security deployment. |
| McAfee Agent | 5.0.1 and 5.0.3 |

For detailed information about managed products like VirusScan Enterprise or Endpoint Security, see the product documentation for those products.

For installing the appliance with an ISO image, your Virtual Machine (VM) must meet the following requirements:

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

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

### Operating system on client 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 server 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.

Best practice: Use the default port configuration settings.

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 used with Threat Intelligence Exchange

<table>
<thead>
<tr>
<th>Network components</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Threat Intelligence (McAfee GTI)</td>
<td>HTTPS 443</td>
</tr>
<tr>
<td>SQL Server</td>
<td>JDBC/SSL and ADO/SSL 1433</td>
</tr>
<tr>
<td>ePolicy Orchestrator server</td>
<td>HTTPS 8443, 8444; HTTP 80; DXL/TLS 8883</td>
</tr>
<tr>
<td>Agent Handler</td>
<td>HTTP 80 and HTTPS 443</td>
</tr>
<tr>
<td>DXL Broker</td>
<td>DXL/TLS 8883</td>
</tr>
<tr>
<td>TIE server</td>
<td>HTTP 8081; HTTPS 443; DXL/TLS 8883; ATD File HTTPS 443; HTTP 5432; TCP 5432; HTTPS 8443</td>
</tr>
<tr>
<td>Advanced Threat Defense server</td>
<td>ATD File REST 443; DXL/TLS 8883</td>
</tr>
</tbody>
</table>
Plan your deployment

Determine your infrastructure requirements before you deploy TIE server.

Sizing and performance

Determine your hardware requirements before your TIE server deployment by gathering reference metrics. McAfee performed these tests on different server-class systems. The metrics include:

- **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 pass through multiple appliances before reaching a TIE server.

For detailed information about each item, see McAfee Threat Intelligence Exchange Sizing and Performance Guide.

Designing your infrastructure

Determine your DXL broker topology and TIE server database replication needs based on managed endpoints and their geographical distribution. See the McAfee Data Exchange Layer Architecture Guide.

Combine TIE server deployments

Combine your TIE server deployment in an environment with multiple McAfee ePO servers.

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 all McAfee ePO servers.

For details about the bridging capabilities of DXL Broker and using service zones, see McAfee Data Exchange Layer Product Guide.

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

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

See KB83896 for details about migrating TIE servers and recommendations.

Installing Threat Intelligence Exchange

Download the software, install the TIE server appliance, and install the TIE client module on your managed endpoints.

TIE server supports McAfee VirusScan Enterprise and Endpoint Security Threat Intelligence for endpoints.
Task
For details about product features, usage, and best practices, click ? or Help.

- Download 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 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.

After completing the installation, configure your TIE server instances managed by your local McAfee ePO with an operation mode.

Tasks

- **Install the TIE server appliance on page 17**
  Install and configure the TIE server and the Data Exchange Layer brokers.

- **Install the server using an ISO file on page 23**
  Deploy the TIE server using an auto-installable ISO file to run on these virtualization platforms: XEN, Hyper-V or bare metal.

- **Deploy the TIE client module on page 24**
  Install the client module for the managed product, for example Endpoint Security or VirusScan Enterprise (optional).

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

**Before you begin**
Make sure the server extension is installed correctly and is the same version of the appliance before you deploy the OVA appliance.
Store your root password in a secure location since it is not possible to recover it.

The TIE server appliance is available on the **Software Manager** and the McAfee download site. There are two options, an OVA and an ISO. Both are packaged as a .zip file and must be extracted before installing.
Task

1. If you downloaded the OVA component, open the VMware vSphere client, then click File | Deploy OVF Template. Browse to and select the TIE server .ova file on your computer. Click Next and complete the steps in the wizard, then turn on the virtual machine and open a Console window.

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

3. Create a root password for the TIE server appliance. The password must be at least nine characters. Make sure to store your password on a secure location since you can’t recover it. Press Y to continue.
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 and to the managed services. The real name is your full name, for example, John Smith.

On the Network Selection page, press N to continue.
Select a configuration type, then press Y to continue.

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

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

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.

Before proceeding, verify the authenticity of the certificate fingerprint of your McAfee ePO. In a
browser navigate to McAfee ePO and verify that the fingerprint matches the one shown on the
installation screen. If it does, press Y to continue.

💡 Use Firefox for checking the fingerprint.
Select the services to run on the TIE server, then press **Y** to continue.

**Service Selection**

Select the services that need to run on this appliance.
(At least one service must be selected.)

DXL Broker (Y/N) : [ 2 ]
TIE Server (Y/N) : [  ]
Proceed? (Yes/No) : [  ]

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

**DXL Service Configuration**

Please select a port for the DXL Broker

DXL Broker Port : 8883 [1024-65535]
Proceed? (Yes/No) : [  ]

Select the services to run on the TIE server, then press **Y** to continue.
When the logon screen appears, close it.

13 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.

See section Monitor the health status of the TIE server for setting monitoring with the automatic responses from McAfee ePO.

**Install the server using an ISO file**

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

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

> Use Hyper-V and XEN as virtualization platforms. See KB86324 for details.

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

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.
   - The ISO file detects the type of virtualization and loads the corresponding kernel modules.
   - The complete disk is partitioned.
   - Basic RPMs are installed.
   - The TIE server Platform and several custom RPMs are installed.
   - The ISO installs the correct kernel.
   - A dialog box informs that ISO is turning off the VM.
2 Remove the ISO file and turn on the VM.
You can continue installing and configuring the TIE server.

**Deploy the TIE client module**
Install the client module for the managed product, for example Endpoint Security or VirusScan Enterprise (optional).

> The TIE client module is installed by default for VirusScan Enterprise.

**Task**
1 Log on to the McAfee ePO server as an administrator.

2 Install the client module for your environment by using one of these methods:
   - For VirusScan Enterprise, in McAfee ePO select Software Manager | McAfee Threat Intelligence Exchange, then download or check in the components, or manually download the TIE files from the McAfee product download website.
   - For Endpoint Security, in McAfee ePO select Menu | Dashboards, then select Guided Configuration from the drop-down list and follow the wizard.

For detailed information, see the documentation for those products.

**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 In McAfee ePO, 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.

**Configure the TIE server extension**
Configure the TIE server extension for use with VirusTotal.

**Before you begin**
Request your VirusTotal credentials to configure your TIE server.

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 server when viewing file reputation information.
**Task**
For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, 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 topology on page 25**
  Configure the operation mode of the existing TIE server instances from the McAfee ePO server settings page.
- **Configure the TIE server policy on page 25**
  Specify McAfee GTI and McAfee Advanced Threat Defense settings for the server.

**Configure the TIE server topology**
Configure the operation mode of the existing TIE server instances from the McAfee ePO server settings page.

In an environment with multiple McAfee ePO servers, only TIE servers managed by a local McAfee ePO are editable. For an environment with a single McAfee ePO server, managed TIE servers are displayed in a tree structure where the root is the instance operating in master mode.

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

1. In McAfee ePO, select Menu | Configuration | Server Settings | TIE Server Topology Management, then click Edit.

2. For each server you want to edit:
   a. Select the TIE server instance to edit, then select the Operation Mode from the drop-down list.
   b. Click Save.

   If you promote your master to a different instance, for example, master to slave and an unassigned to master, you might lose data because the new master instance does not replicate the database.

   In a single master instance scenario, you can have only one master instance managed by your local McAfee ePO after the update.

3. Promote the slave to a master instance and reconfigure the old master instance as a slave.
   You can drag and drop the instances from the tree structure.

After you saved your changes, the background processing takes place to apply the changes on each TIE server instance. This process can take several minutes to be completed. Wait a few minutes and press F5 or click the refresh button in the browser to see your new TIE server topology.

If your appliance wake-up port is filtered, manually restart the CMA service. Otherwise, it takes time for the policy to reach the appliance.

**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.
   - **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** — Allow McAfee to collect anonymous data about certificates and file hashes. This data helps McAfee learn about threats and prioritize what's allowed or blocked.

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.
   
   You can enable certificate validation in the communication between the TIE server and Advanced Threat Defense. See KB87692 for details before enabling Enforce Certificate Validation.

5. On the McAfee Web Gateway tab, accept or ignore incoming reports sent to the TIE server about potential web threats.

6. On the Server Configuration tab, configure the logging level of the server, enable or disable collecting metrics, and modify the sampling period for collecting performance metrics.

7. Select Menu | Configuration | Server Settings | Threat Intelligence Exchange Server. The VirusTotal service certificates are validated. If you experience network filtering restrictions, click Edit to disable the Skip VirusTotal certificate validations, then click Save.
   
   You can configure the type of files that the TIE server recognizes and processes. You can add or remove file types from the list.

---

**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.

7  Verify that the operation mode of your TIE server instances have changed based on your edit.
   Select Menu | Server Settings | TIE Server Topology and verify that your changes were applied.

Tasks
• Verify registered servers on page 27
   Verify that the servers are registered correctly to view TIE server information in McAfee ePO reports and dashboards.

Verify registered servers
Verify that the servers are registered correctly to view TIE server information in McAfee ePO reports and dashboards.

Before you begin
You might have a registered server created automatically during the installation process. Make sure that the dashboards are working properly. If they aren't, follow the instructions below.

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 if you don't have a registered server. Click Edit to manually modify an existing registered 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).
For the **Database name**, enter **tie**.

| In the **User name** field, enter the read-only PostgreSQL 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 TIE client module 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 server 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**, then run **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**, then run **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  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 the 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 — \ProgramData\McAfee\EndpointSecurity\Logs\ThreatIntelligence_Activity.log

TIE client module for VirusScan Enterprise — \ProgramData\McAfee\TIEM\TIEMVe.log

Threat Intelligence Exchange server — /var/McAfee/tieserver/logs/tieserver.log and /var/McAfee/tieserver/logs/tieserver-start.log

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 the server appliance.

See KB59385 for details about using the MER tool with other 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/mynname/change-hostname.

<table>
<thead>
<tr>
<th>Script name</th>
<th>Description</th>
<th>Reboot?</th>
</tr>
</thead>
<tbody>
<tr>
<td>change-hostname</td>
<td>Changes the host name of the current appliance. It restarts the McAfee Agent and the broker.</td>
<td>Recommended</td>
</tr>
<tr>
<td>change-services</td>
<td>Enables or disables the DXL broker and the TIE server services. If the broker was initially disabled during first boot, the script prompts for broker configuration information.</td>
<td>No</td>
</tr>
<tr>
<td>reconfig-dxl</td>
<td>Reconfigures the DXL port.</td>
<td>No</td>
</tr>
<tr>
<td>reconfig-ma</td>
<td>Reconfigures the McAfee Agent. The agent, the DXL broker, and the TIE server services are restarted. New keystores are generated when the service starts.</td>
<td>Recommended</td>
</tr>
<tr>
<td>reconfig-network</td>
<td>Reconfigures the current network interface (from DHCP to manual, or from manual to DHCP).</td>
<td>Recommended</td>
</tr>
<tr>
<td>reconfig-ntp</td>
<td>Reconfigures the Network Time Protocol servers.</td>
<td>No</td>
</tr>
<tr>
<td>reconfig-ca</td>
<td>Obtains an updated Certificate Authorities chain from McAfee ePO and stores it in the TIE server.</td>
<td>No</td>
</tr>
<tr>
<td>reconfig-cert</td>
<td>Generates a new certificate and sends a signing request to McAfee ePO through the TIE server extension.</td>
<td>No</td>
</tr>
</tbody>
</table>
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
- Blocking or allowing files and certificates
- Changing default threat reputations
- Searching for files and certificates
- Determine where a file or certificate ran in your environment
- Determine what files or certificates ran on your system
- Detection events
- Server tasks
- Recommended workflow

Getting started

After you install Threat Intelligence Exchange server, what do you do next?
To get started with TIE server, do the following:

1. Create TIE server policies to determine what is allowed and blocked. Then run TIE server in observation mode to build file prevalence and observe what TIE server detects in your environment. File prevalence is how often a file is seen in your environment.

2. 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 server 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 Threat Intelligence Exchange 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 the Threat Intelligence Exchange server 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 endpoint, 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. The application is then allowed to run in your environment without being blocked or prompting the user for action. You might change the reputation 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.

- 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.

- The Composite Reputation column on TIE Reputations page shows the most prevalent reputation and its provider.

- The Latest Applied Rule column on the TIE Reputations page shows and tracks reputation information based on the latest detection rule applied for each file at the endpoint.

You can customize this page by selecting Actions | Choose Columns. See Customize queries in this guide.
Data storage management
Manage your database size with data retention policies for avoiding service degradation for database growth.

This server task is now in McAfee ePO and checks the database size and compares it with a size threshold. If the database exceeds the threshold, the cleanup is executed.

You can run the task as needed and configure the frequency from McAfee ePO on the Server Tasks page.

The task cleans the database of the required number of files and, by default, is executed every day at midnight for keeping the size of the database within 20 GB.

The file selection criteria determines that files without an Enterprise reputation (or a reputation override) 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 Endpoint Security Threat Intelligence.

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. In McAfee ePO, select Menu | Policy | Policy Catalog.
2. From the Product list, select Endpoint Security Threat Intelligence.
3 Select My Default, then 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 server 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 server 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.

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

McAfee does not collect personally identifiable information, and does not share information outside of McAfee.
Changing default threat reputations

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

Based on settings in the TIE server 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 server database

File and certificate reputations are added to the TIE server 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 server 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 In McAfee ePO, 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 ?.

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 server database.

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

1. In McAfee ePO, 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.

<table>
<thead>
<tr>
<th>Reputation setting</th>
<th>Numeric value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Known trusted</td>
<td>99</td>
</tr>
<tr>
<td>Most likely trusted</td>
<td>85</td>
</tr>
<tr>
<td>Might be trusted</td>
<td>70</td>
</tr>
<tr>
<td>Unknown</td>
<td>50</td>
</tr>
<tr>
<td>Might be malicious</td>
<td>30</td>
</tr>
<tr>
<td>Most likely malicious</td>
<td>15</td>
</tr>
<tr>
<td>Known malicious</td>
<td>1</td>
</tr>
<tr>
<td>Not Set</td>
<td>0</td>
</tr>
</tbody>
</table>

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.

Table 3-1 Option definitions

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Known trusted</td>
<td>It is a trusted file or certificate.</td>
</tr>
<tr>
<td>Most likely trusted</td>
<td>It is almost certain that the file or certificate is trusted.</td>
</tr>
<tr>
<td>Might be trusted</td>
<td>It seems a benign file or certificate.</td>
</tr>
<tr>
<td>Unknown</td>
<td>The reputation provider has encountered the file or certificate before but the provider can’t determine its reputation at the moment.</td>
</tr>
<tr>
<td>Might be malicious</td>
<td>It seems a suspicious file or certificate.</td>
</tr>
<tr>
<td>Most likely malicious</td>
<td>It is almost certain that the file or certificate is malicious.</td>
</tr>
</tbody>
</table>
### Table 3-1  Option definitions (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Known malicious</td>
<td>It is a malicious file or certificate.</td>
</tr>
<tr>
<td>Not set</td>
<td>The file or certificate's reputation hasn't been determined yet.</td>
</tr>
<tr>
<td>Not Available</td>
<td>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 show Not Available reputation because the specific file reputation hasn't been queried yet. The client has only queried about its associated certificate reputation.</td>
</tr>
</tbody>
</table>

#### 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
<?xml version="1.0" encoding="UTF-8"?>
<TIEReputations>
    <FileReputation>
      <FileName>HackIt.exe</FileName>
      <SHA1Hash>0x98AF3632E17677A8A23739F720B1a2F215CB8836</SHA1Hash>
      <MD5Hash>0xDEF30CBEA881149C2AFFDF9A059FB751</MD5Hash>
      <SHA256Hash>0xEF127619BAC96790FBC925C33911806DA71FAA0CF0A1E630BEF328B1DF91</SHA256Hash>
      <ReputationLevel>15</ReputationLevel>
    </FileReputation>
    <FileReputation>
      <FileName>trayMan.dll</FileName>
      <SHA1Hash>0x7F618396A910908019B580B4DA9031AF4A433C</SHA1Hash>
      <MD5Hash>0xB2B3DAE040F6B5AE1DF52B0CD7631A18</MD5Hash>
      <SHA256Hash>0xAF37EBACF8697B55A82E5FA0D742E65ABE0953BA6B9EABA6B35B5BA95F583EC</SHA256Hash>
      <ReputationLevel>15</ReputationLevel>
      <Comment>Comment for ALTFAB</Comment>
    </FileReputation>
</TIEReputations>
```

**Example import certificate**

```xml
<?xml version="1.0" encoding="UTF-8"?>
<TIEReputations>
    <CertReputation>
      <SHA1Hash>13D90CAC5FC2C5086E882B13B4BA8115C6F65D09</SHA1Hash>
      <PublicKeySha1>108F9887A4481B94F4C53A9097884F58E29123B8</PublicKeySha1>
      <ReputationLevel>15</ReputationLevel>
      <Comment>Comment for ALTFAB</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. In McAfee ePO, 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 with McAfee ePO Web API**
Use the remote command provided by the TIE server to automate reputation overrides of files and certificates using McAfee ePO Web API.

![Best practice]
Periodically reconcile the overrides against other reputations and remove those reputations that are already covered for maintaining the adaptive capabilities.

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

JSON strings represent files and certificates with the Base64 hashes encoded and the following reputation scores:

<table>
<thead>
<tr>
<th>Reputation</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Known Malicious</td>
<td>1</td>
</tr>
<tr>
<td>Most Likely Malicious</td>
<td>15</td>
</tr>
<tr>
<td>Might Be Malicious</td>
<td>30</td>
</tr>
<tr>
<td>Unknown</td>
<td>50</td>
</tr>
<tr>
<td>Might Be Trusted</td>
<td>70</td>
</tr>
<tr>
<td>Most Likely Trusted</td>
<td>86</td>
</tr>
<tr>
<td>Known Trusted</td>
<td>99</td>
</tr>
</tbody>
</table>

The command syntax is **tie.setReputations [fileReps] [certReps]**. You must specify at least one **fileReps** or one **certReps**. Both can be provided in the same payload call.

The following example of a payload sets one file as Known Trusted:

```javascript
fileReps = [{"name":"test.exe",
"sha1":"udrarumiyyjtffybxaflkxzjhpao=",
"md5":gixbyabniwaangznufuxe==",
"sha256":"icidutgqksorzzvqsepfmkyiambtbufcckwarjmqth==",
"reputation":"99"}]
```
The attributes MD5, SHA-1, and reputation are mandatory. The name and SHA-256 are optional.

**Best practice:** Use as many hash types as possible for a given file because integrating products might not honor all.

The following payload sets one certificate as Known Trusted:

```json
constReps = [{"sha1":"frATnSF1c5s8yw0REA24ILSqvSk=",
"publicKeySha1":"udrarummyjtffybxaflkkzjhpao=",
"reputation":"99"}]
```

The attributes SHA-1 and reputation are mandatory. publicKeySha1 is optional.

For details about using this API, see *McAfee ePolicy Orchestrator Web Scripting Guide* or the online Help for McAfee ePO.

---

**Searching for files and certificates**

You can search for files and certificates in the TIE server 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 SHA-1, SHA-256, and MD5 hashes
- Company information
- File name, version, type, and company information
- Systems that ran a specific file
- Systems that ran files signed by a specific certificate

On the **TIE Reputations** page on the **File Search** tab, you see files with metadata and that are searchable. The page can show the file type by default. The page shows these columns, for example:

- **Composite Reputation** — Potential effective reputation score based on local reputation (if available) or an estimate based on other reputation scores (if the hash value isn't available at the endpoints).

- **Latest Local Reputation** — Last effective reputation score informed by the endpoints of a hash.

- **Latest Applied Rule** — Last content rule applied at the endpoints for determining the effective score of the hash.

On the **TIE Reputations** page, select **Actions | Choose column** to customize and add more columns.

**Search for a file or certificate**

There are several ways to search for a file or certificate in the TIE server database.
**Task**
For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, 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.
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. In McAfee ePO, 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. In McAfee ePO, 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. In McAfee ePO, 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 server policy.

- **Observation Events** — Events, such as Would Block, that indicate what the action would be 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 SHA-1 hash value, and the number of certificates that were cleaned, blocked, or prompted.

- **File Hash** — The file name and SHA-1 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 For VirusScan Enterprise, in McAfee ePO, select Menu | Reporting | TIE module for VSE Events or for Endpoint Security, select Menu | Reporting | Threat Intelligence Events.

The TIE module for VSE Events and the Threat Intelligence Events pages show 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, such as Would Block, 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 details about this configuration.

On the Advanced Threat Defense tab, you can configure which file types are enabled for submitting them to analysis. From the Available File Types list, you select the file types to be sent to Advanced Threat Defense, including Portable Executable (PE) and other non-PE files. PE files are enabled by default. See the online Help for more information.

You can add reputation information from Advanced Threat Defense to the TIE server database if the file or the reputation information does not exist. It enables threat information seen by Advanced Threat Defense, but not by the TIE server, to be added to the database.

Make sure that the TIE servers and the Advanced Threat Defense instances are connected to secured internal networks. The file sample submission from the TIE server to Advanced Threat Defense uses a TLS connection. To enforce the authentication of the connection, first upload certificates signed by public certificate authorities (CA) to Advanced Threat Defense, then enable the Enforce Certificate Validation policy in the TIE server.

You can locally install trusted CAs certificates or use the certificates provided by Advanced Threat Defense by default.

See KB87692 before enabling the Enforce Certificate Validation policy.

For a list of trusted CA, see OpenJDK 1.8 documentation. For instructions on how to upload the certificates to Advanced Threat Defense, see the McAfee Advanced Threat Defense Product guide.

Configure file types for analysis

Configure which file types are uploaded to Advanced Threat Defense for exploiting and analysis.

Before you begin

Verify that Advanced Threat Defense is enabled and configured correctly in McAfee ePO on the Policy Catalog page.

If you select multiple file types, the portable executable (PE) files are prioritized and sent first to Advanced Threat Defense.

1. In McAfee ePO, select Policy Catalog | Advanced Threat Defense.
2. Select the file types that are available from the list, then click Add.
3. Click Save.

TIE server submits the file types selected to Advanced Threat Defense for further analysis.
**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. In McAfee ePO, select **Menu** | **Systems Section** | **System Tree**.
2. Select one or multiple systems.
3. From the **Actions** menu, select **System Health Indicator**, 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.

See KB87743 for regenerating CA certificates used by the TIE server.

When bridging DXL fabrics, if the TIE Server Topology Management page isn't showing the server instances correctly, perform this task.
Task
For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, select Menu | Automation | Server Tasks, then run TIE Server synchronize CA.
2. Verify that the task is completed in the server 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 that they are connected to DXL and are running.

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

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

1. In McAfee ePO, select Menu | Automation | Automatic Responses.
2. Create notifications and actions using Automatic Responses.
   See McAfee ePolicy Orchestrator Product Guide for 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.

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Severity</th>
<th>Level</th>
<th>Event name</th>
</tr>
</thead>
<tbody>
<tr>
<td>37175</td>
<td>4</td>
<td>Critical</td>
<td>TIE Server Master Unreachable</td>
</tr>
<tr>
<td>37176</td>
<td>4</td>
<td>Critical</td>
<td>TIE Server Master Write-Only Unreachable</td>
</tr>
<tr>
<td>37177</td>
<td>3</td>
<td>Major</td>
<td>TIE Server Slave Unreachable</td>
</tr>
<tr>
<td>37178</td>
<td>3</td>
<td>Major</td>
<td>TIE Server Reporting Unreachable</td>
</tr>
<tr>
<td>37179</td>
<td>3</td>
<td>Major</td>
<td>TIE Server Unreachable</td>
</tr>
</tbody>
</table>

Following this approach you use McAfee ePO Automatic Responses for sending email notifications, creating McAfee ePO tracking issues, and customizing actions to provide monitoring capabilities.

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

Monitoring the TIE server connections
Monitor the health status of your TIE server instances on the TIE Server Topology Management page in McAfee ePO.

The TIE Server Topology Management page shows an overview of your environment health status. If there is an error on a specific master or slave server instance, it is highlighted in red.

Consider that the health status is set based on the worst case scenario described in the checkups. The checkups are DXL Connection, Database Replication, and GTI Connection.
DXL Connection checkup
This check tests the connection between the TIE server instance that you selected and McAfee ePO through DXL. This checkup is valid for all operation modes of the TIE servers.

Database Replication checkup
This checkup verifies if the replication of the database is running. This checkup is applicable only to slave and slave-reporting server instances.

GTI Connection checkup
This checkup verifies if the connection to McAfee GTI is enabled and properly configured. This checkup is applicable to all server instances, except slave-reporting server instances.

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 server 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.


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
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.

Contents
- Viewing queries
- Customize queries

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 server reports using McAfee ePO to view TIE server events and file and certificate information.

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

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

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

Create custom queries using McAfee ePO query system and reuse them in dashboard monitors and report sections.

We provide an overview on using McAfee ePO query capabilities for gathering TIE server information. For more details, see McAfee ePO online Help.

- The **TieServerSchema** retrieves information about Enterprise reputation, files, and certificates from the TIE server.
- The **ePO** schema queries about client and threat events enriched by TIE server information.

**Task**

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

1. In McAfee ePO, select Queries & Reports | New Query.
2. In the drop-down list for Database Type, select a schema:
   - **TieServerSchema** — On the Result Type tab, select which results are displayed, then click Next.

**Table 4-1 Option definitions**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificates</td>
<td></td>
</tr>
<tr>
<td>Certificate Enterprise Reputation</td>
<td>Shows the Enterprise reputation of the certificates.</td>
</tr>
<tr>
<td>Certificate Reputation</td>
<td>Retrieves summarized non-Enterprise reputation for certificates from the TIE server.</td>
</tr>
<tr>
<td>Certificates</td>
<td>Retrieves certificate information from the TIE server.</td>
</tr>
<tr>
<td>New Certificates on Systems</td>
<td>Retrieves information about systems with new certificates.</td>
</tr>
<tr>
<td>TIE Data Storage Management Cleanup Trending Summary</td>
<td>Retrieves TIE server cleanup trending summary.</td>
</tr>
<tr>
<td>Files</td>
<td></td>
</tr>
<tr>
<td>File Enterprise Reputation</td>
<td>Retrieves summarized Enterprise Reputation from files.</td>
</tr>
<tr>
<td>File Reputation</td>
<td>Retrieves summarized non-Enterprise reputation for files from the TIE server.</td>
</tr>
<tr>
<td>Files</td>
<td>Retrieves file information from the TIE server.</td>
</tr>
<tr>
<td>New Files on Systems</td>
<td>Retrieves information about systems with new files.</td>
</tr>
</tbody>
</table>

- **ePO** — Select Events and follow the prompts.

3. On the Chart tab, customize how the results are displayed, then click Next.
4. On the Columns tab, customize the columns for displaying the results, then click Next.
5. On the Filter tab, narrow the results of your query using the drop-down list, then click Run.

You obtain a customized chart with the threat intelligence information from your TIE server.
Index

A
about this guide 5
Advanced Threat Defense 34
    configuring for TIE 33
    sending files to 33
    used in determining reputations 11
Advanced Threat Defense settings 25

B
bridging servers 9

C
certificate authorities, synchronize 44
certificates
    blocking or allowing 33
    changing a reputation 35
    details about 39
    determine where a certificate has run 40
    how reputations are determined 11
    importing a reputation 36
    searching for 39
combining TIE server deployment 16
compromised systems 44
configuration
    bridging servers 9
    scripts, reconfiguring the server 30
    server policy settings 25
    VirusTotal, file reputation information 24
conventions and icons used in this guide 5
custom queries 48
custom search filters 40

D
Data Exchange Layer
    about 10
    deploying 24
    reconfiguring using scripts 30
    troubleshooting the installation 28
    verifying the installation 26
deployment
    Data Exchange Layer client 24
    OVF template 17
details about files and certificates 39
documentation
    audience for this guide 5
    product-specific, finding 6
    typographical conventions and icons 5

E
events
    enforced 41
    observed 41
    responding to 42
    setting system health status 44

F
files
    blocking or allowing 33
    changing a reputation 35
    details about 39
    determine where a file has run 40
    how reputations are determined 11
    importing a reputation 36
    searching for 39
files and certificates, blocking 33
files and certificates, sending 33

G
going started with Threat Intelligence Exchange 31
Global Threat Intelligence 33
    server settings 25

H
hardware requirements 16

I
import file reputations 39
importing file and certificate reputations
    import file reputations using STIX 36
    import file requirements 36
    STIX 36
installation
    components 13
    log files for troubleshooting 29
    overview 13
installation (continued)
requirements 13
server appliance 17
Threat Intelligence Exchange server 16
troubleshooting 28
verifying the installation 26

L
log files, troubleshooting the installation 29

M
marking a system as compromised 44
McAfee Agent
installation requirements 13
reconfiguring using scripts 30
McAfee ePO registered server, creating 27
McAfee ePO Web API 38
McAfee ServicePortal, accessing 6
migration tool 16
module for VirusScan Enterprise
creating policies 33
installation requirements 13
installing 16
supported operating systems 13
troubleshooting the installation 28
verifying the installation 26
multiple McAfee ePO environment 16

N
network overview 15

O
observed events 41
offline behavior 33
operating systems, supported 13
operation mode 25

P
performance 16
policies
creating 33
policy settings 25
ports used 15
Product Improvement Program 34
settings 25
prompting
setting up 33
protocols used 15

R
reconfiguring using scripts 30
registered server, creating 27
reports, creating a registered server 27
reputations
changing for a file or certificate 35
changing using McAfee ePO API 38
how they are added to the database 35
how they are determined 11
import file requirements 36
importing into the database 36
requirements for installation 13

S
scripts for reconfiguring 30
search for files and certificates 39
security levels
examples 33
server
about 9
bridging servers managed by McAfee ePO 9
policy settings 25
server appliance, installing 17
server tasks 44, 45
ServicePortal, finding product documentation 6
settings, configuring the server policy 25
sizing 16
STIX
import file reputations using 39
STIX, about 36
submit files for further analysis
Advanced Threat Defense 34
Product Improvement Program 34
supported operating systems 13
system health 44
system requirements 13

T
technical support, finding product information 6
Threat Intelligence
Endpoint Security 9
Threat Intelligence Exchange
about 7
benefits of 7
creating policies 33
events 41
installing 13
module for VirusScan Enterprise 9
scenarios 10
server 9
troubleshooting the installation 28
viewing details 42
workflow examples 31
Threat Intelligence Exchange server
Advanced Threat Defense settings 25
bridging servers managed by McAfee ePO 9
configuring 24
Global Threat Intelligence settings 25
Threat Intelligence Exchange server (continued)
   installing 16
   policy settings 25
   Product Improvement Program settings 25
   reconfiguring using scripts 30
   server appliance 17
   troubleshooting the installation 28
threats
   viewing details with Threat Intelligence Exchange 42
TIE capabilities 46
TIE server topology 25
TIE server, monitor the 45
troubleshooting
   installation issues 28
   viewing log files for installation issues 29

V
verification, installation success 26

VirusScan clean action 33
VirusTotal, accessing file reputation information 24
VMware vSphere
   deploying the OVF template 17
   installation requirements 13

W
where has a certificate run 40
where has a file run 40
workflow examples 31
   build file prevalence and observe 31
   monitoring and adjusting 32
   submit files for further analysis 34
workflow of TIE activities 46