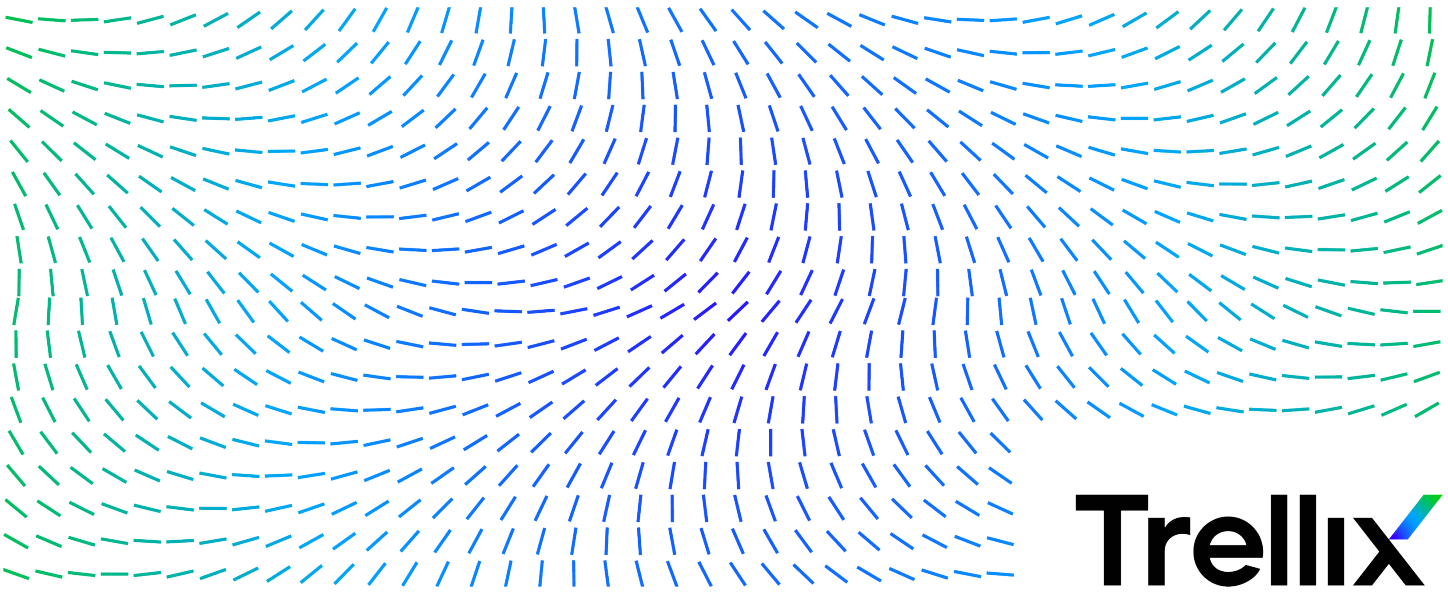
Trellix Threat Intelligence Exchange 4.0.x Product Guide



Contents

Product Overview

Trellix Threat Intelligence Exchange (TIE) optimizes threat prevention by narrowing the gap from malware encounter to containment from days, weeks, and months down to milliseconds.

Threat Intelligence Exchange 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 the criteria set by you.

TIE manages multiple devices and systems intelligently, so that security information is shared. These devices and systems include the cloud, BYOD, managed nodes, servers, and network appliances.

Key features

TIE server integrates with other **Trellix** products for fast and effective response to security threats. Also, products share threat information throughout your environment.

Allow or block files and certificates based on the threat information consumed. You can store the threat information in your database to apply detection capabilities and to increase end-to-end protection.

Collaborative and relevant security intelligence is built in with global and local threat intelligence gathering. Integration is simplified with **Trellix Data Exchange Layer** .

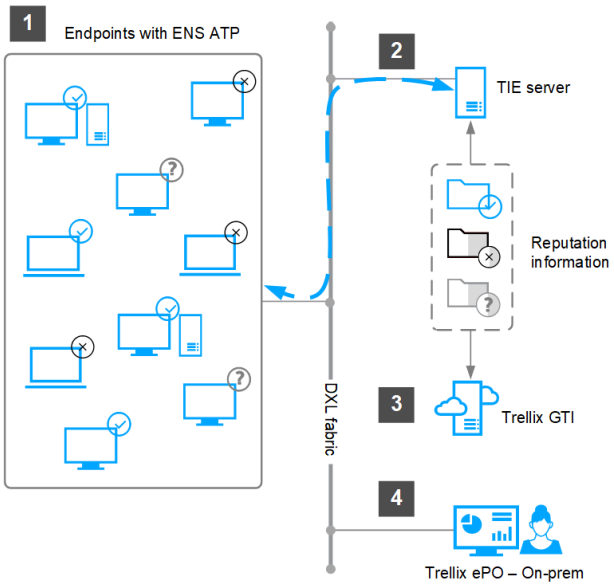
Threat Intelligence Exchange provides these benefits.

- 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 reputations and your risk criteria.
- Real-time integration with **Trellix Intelligent Sandbox** and **Trellix 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 **Trellix Endpoint Security (ENS) Web Control** and **McAfee® Network Security Platform**, among other **Trellix** products, for exchanging threat reputation that increases protection and detection capabilities end-to-end.
- Integration with **McAfee® Enterprise Security Manager (McAfee ESM)** for creating reports of files and certificates while monitoring file and certificate events, like file first instance and file reputation change, prevalence events, and reputations changes.
- Integration with **Trellix GTI** Private Cloud for consuming reputations that come from a single-tenant and dedicated private setup instead of **Trellix GTI** .
- You can now configure **McAfee Application Control** to work with **TIE** server and **Trellix GTI** server. For more information, see **McAfee Application Control** product guide.

How it works

TIE comprises a module for Endpoint Security that allows you to create policies for blocking and allowing a file based on its reputation. It has a server that stores information about file and certificate reputations, then passes that information to other systems. Finally, it has **Data Exchange Layer** brokers that allow bidirectional communication between managed systems on a network.

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



1. Endpoints running Trellix Endpoint Security Adaptive Threat Protection (ATP) query the **TIE** server on every executed file in the environment, including unknown files. Files are automatically blocked or allowed based on information stored on **TIE** and **Trellix GTI** .
2. **TIE** server analyzes the files and shares threat information throughout the environment based on its security reputation and criteria set by you. In addition to identifying the file's reputation, the TIE server also adds local intelligence capabilities to the ecosystem such as age and prevalence of files.
3. Integration with **Trellix GTI** provides a base reputation to the **TIE** server.
4. The security administrator can spend time monitoring unusual activity.

Components of Threat Intelligence Exchange

Threat Intelligence Exchange client

The client **Trellix Endpoint Security (ENS) Adaptive Threat Protection** 10.7.x or later 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 data points such as reputations, local intelligence, and contextual information. You can enable some optional rules. For more information, visit www.docs.trellix.com for product documentation about **Endpoint Security**.

The client applies policies and scans files to determine whether to send the files to the sandbox.

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.
- 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.
- 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.
- Generate dashboards and reports on the managed local threat intelligence.

Bridging DXL fabrics

If you have **TIE** servers and endpoints managed by different **Trellix ePO - On-prem** systems, you can combine them to share reputation information. For details, see the product guide for **Trellix Data Exchange Layer** , and KB88621.

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 the product guide for **Trellix Data Exchange Layer** for details about installing and using **Data Exchange Layer**.

Trellix OpenDXL

OpenDXL is a framework that enables real-time security context sharing between products, integrating and connecting all your products across a single communications fabric.

Any product can be integrated — whether it's a **Trellix** product or not. Product owners only need to integrate once for access to many, and integration can be done in days — not weeks or months.

The **DXL** fabric is made up of brokers designed for sharing, receiving, and acting on communal threat information. **DXL** allows scalable communication between anything on the fabric through an easy-to-use, easy-to-manage product.

These are the four key capabilities that **OpenDXL** allows:

- Publish an event
- Receive an event
- Ask a question
- Take action

For more information about how to create and deploy integrations with **OpenDXL**, see the OpenDXL website.

Using Threat Intelligence Exchange

Scenarios for using Threat Intelligence Exchange

Consider these basic use case scenarios for using the **TIE** server to block and allow files to run in your environment and to import reputations.

- **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 **Trellix** 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 **Trellix** 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** — For any file or certificate with unknown reputation, the **Threat Intelligence Exchange** server allows the network administrator to inspect its details. 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.

Dashboards

Threat Intelligence dashboard

TIE Server reviews trending, recent, and prevalent files according to threat reputation. **TIE** Server Files reviews last week, new, and changed **Trellix GTI** reputations, trend on suspicious file count, top systems with new files, and overrides split by score. **TIE** Server Certificates similarly review certificates.

Overrides dashboard

TIE Server Overrides reviews new and used administrator reputation overrides, also showing redundant and conflicting overrides. **TIE** Server Signed Unknown Files and **TIE** Server Unsigned Unknown Files reviews unclassified files on the environment.

Monitoring dashboard

TIE Server Infrastructure reviews **DXL** connectivity status and component version split at the **TIE** Server appliances, also shows trending on **Trellix GTI** refresh counts. **TIE** Server Data Cleanup reviews data management by showing cleanup executions, the incoming new files, and size of the database.

Sandboxing dashboard

TIE Server **Intelligent Sandbox** Submissions reviews on-premise sandboxing information including daily trending count of analyzed samples, overall split of reputation of analysis reports, new and recent trends, top prevalent submissions.

Reports

TIE Server extension includes a sample **TIE** Server Summary report including most dashboard monitors which can be scheduled through a **Trellix ePO - On-prem** Server Task into an email notification with a **Trellix ePO - On-prem** Automatic Response.

Retrieving files and certificates

You can view detailed information about the files and certificates in the **TIE** server database and make a note of the change in reputation settings for any investigation and remediation.

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.

The default filters show the following options.

- For files, you can see files with at least one file name and with a valid composite reputation to prioritize files already seen at the endpoints.
- With the **Certificate Search** you can see only certificates that actually sign files to avoid unnecessary overriding.

You can view a host of information about the file and certificates, which includes:

- The associated certificate for a specific file
- Details about a certificate's parent certificate
- Details about a file's parent process
- Current enterprise, **Trellix GTI** , **McAfee Web Gateway**, **Intelligent Sandbox** reputations
- 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
- List of files and certificates signed by a given certificate

Note

The **TIE Reputations** page is view-only and requires permission to access it. To set permissions to access the fabric, use the **Trellix TIE Reputations** page permission set in **Trellix ePO - On-prem**.

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).

  Important

  The **Composite Reputation** is an estimation until the endpoint reports back what did really happen in the endpoint. After getting the updated information such as updated reputation from **Trellix GTI** , the updated information becomes the latest estimation until the next report, and this cycle continues.

  The hierarchy used to display the estimation is as follows.

  - Reputation hierarchy: **File Enterprise Reputation**, **Certificate Enterprise Reputation**, **Latest Local Reputation**. If there is a reputation (whether it's definitive or nor) for any of these sources, the value is show in the Composite Reputation column with the hierarchy mentioned before.
  - Reputation hierarchy: **Certificate GTI Reputation**, **File GTI Reputation**, **ATD Reputation**, **MWG reputation**, and **External reputation**. If there isn't a reputation available for the previous ones (File Enterprise, Certificate Enterprise, and Latest Local), the hierarchy rule changes as described before. If **all or some** of those sources have a definitive reputation, the composite estimation shows the reputation from the top provider on the hierarchy. If none of those sources have a definitive reputation, the composite estimate shows the reputations available based on the hierarchy defined above.
- **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.

Accessing files and certificates present in your system

You can see the systems in your environment that used a particular file. You can also see used files signed by a specific certificate and sort files or certificates that were used on your system.

Determine where files and certificates were used

Systems that used a specific file or files signed by a certificate are listed, including the system name, IP address, and the first date when the file was identified on the **System Tree** of **Trellix ePO - On-prem**. The **Where Was File Used** and **Where was Certificate Used** actions search into the system where the selected file and certificate was used.

Determine what files and certificates were used in 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.

What files or certificates were used on your system

Show Files used on your system and **Show Certificates used on your system** sort and display the files and certificates used on your system.

The Option definitions table describes the shared information for files and certificates. After you execute **Show Files used on your system** or **Show Certificates used on your system**, you can select from the **Actions** menu how to continue.

Option definitions

Option	Definition
Preset	Filter your search by date.
First Reference	It shows what files or certificates the agent saw for the first time.

Searching for files and certificates

You can use custom filters, wildcard characters, predetermined filters, and sorting the filtered data when searching for files and certificates.

Task

1. **To determine where the files or the certificates were used in your system, select Menu → Systems → TIE Reputations.**
   a. Click the **File Search** or **Certificate Search** tab, depending on what you want to search for.
   b. **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 ?, and the hash value when searching.**
   c. **Select the file or certificate that you want to see.**
   d. **From the Actions menu, select Where Was File Used or Where Was Certificate Used.**
2. **To determine what the files and certificates were used, select Menu → System Tree.**
   a. **Select a system, then click Actions → TIE → Show files used on system or Show certificates used on system.**
   The list of files or certificates that were used on your system are sorted by reference date and in descending order.

File search

Search for files in the **TIE** database. The longer the module runs in your environment, the more populated the database becomes. A file is added to the database when the module requests information about it.

Option definitions

Option	Definition
Custom	Search for files using a custom filter. You can use one of the default filters, or create your own: • **Malicious files** — Lists files with a malicious reputation. This includes files whose reputation is Known Malicious, Might be Malicious, and Most Likely Malicious. • **Missing names** — Lists files that don't have name. • **Unknown files** — Lists files whose reputation is unknown. • **Add...** — Create your own custom search filter to view specific rows of data. Click **Add...** to specify the search criteria to use. The custom filter is named "Unsaved". Click the right arrow next to the Unsaved label, then click **Edit** to name the custom search filter.
Quick find	Search for a specific file name or type of file. You can use search characters * or ?.
Show selected rows	List only files that are selected.
Selecting a column heading	Select a column heading to sort the information. When sorting by any type of reputation, for example by Enterprise or **Global Threat Intelligence** reputation, the files are listed in this order: • Known Trusted • Most Likely Trusted • Unknown • Most Likely Malicious • Known Malicious • Not Set **Remember:** Sorting results appear by reputation value rather than alphabetically. For more information about the values, see *Specifying the reputation as a number*.

Option	Definition
	Attention: When **TIE** doesn't have information available for a file or its reputation, in the Reputation column appears "Not Available".
Selecting a file	Select a file to see its details.
Actions	See *File actions*.

TIE Reputations column headings

For each file, you have its name, company and product names, and its version. The information of its reputation and the reputation providers are displayed in different columns.

Option	Definition
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).
Enterprise Reputation	File reputation assigned by the administrator.
Certificate Enterprise Reputation	Reputation assigned by the administrator to a certificate associated to a specific file.
Latest Local Reputation	Latest effective reputation used by the endpoint. If it's not available or informed, the server informs the next reputation based on its value and which provider informed it first.
Certificate GTI Reputation	Certificate reputation information provided by **Global Threat Intelligence**.
GTI Reputation	File reputation information provided by **Global Threat Intelligence**.

Option	Definition
ATD Reputation	File reputation information provided by **Intelligent Sandbox**.
MWG Reputation	File reputation information provided by **Web Gateway**.
Latest Applied Rule	Latest detection rule applied at the endpoint based on file type.
External Reputation	File reputation information provided by an external provider.

Certificate search

Search for certificates in the **TIE** database.

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

Option definitions

Option	Definition
Custom	Search for certificates using a custom filter. You can use one of the default filters, or create your own: • **Malicious Certificates** — Lists certificates with a malicious reputation. This includes certificates whose reputation is Known Malicious, Might be Malicious, and Most Likely Malicious. • **Unknown in GTI** — Lists certificates whose reputation is unknown in **Global Threat Intelligence**. • **Add...** — Create a custom search filter. Click **Add...** to specify the search criteria. The custom filter is named "Unsaved". Click the right arrow next to the Unsaved label, then click **Edit** to name the filter.

Option	Definition
Quick find	Search for a specific certificate. You can use the search characters * or ?.
Show selected rows	Lists only certificates that are selected.
Selecting a column heading	Select a column heading to sort the information. When sorting by any type of reputation, for example by Enterprise or **Global Threat Intelligence** reputation, the certificates are listed in this order: • Known Trusted • Most Likely Trusted • Unknown • Most Likely Malicious • Known Malicious • Not Set **Remember:** Sorting results appear by reputation value rather than alphabetically. For more information about the values, see *Specifying the reputation as a number*. **Remember:** When **TIE** doesn't have information available for a file or its reputation, in the Reputation column appears "Not Available".
Selecting a certificate	Select a certificate to see details about it.
Actions	See *Certificate actions*.

Create a custom search filter

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

Task

1. **In Trellix ePO - On-prem, 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.**

File and certificate details

View more reputation information about a specific file or a certificate.

File Details Option definitions

Option	Definition
File Details	View details about the metadata and reputations of the selected file.
Additional Information	View more file information from the first system that executed the file. The information might not reflect the state of the file on all systems.
Associated URL	The URL reputation for the selected file from. This information comes from **McAfee® SiteAdvisor® Enterprise**.
VirusTotal	Queries a file's Hash in VirusTotal. • **View File Information on VirusTotal website** — Select to open the VirusTotal website and view information about the file. • If you have a VirusTotal API key, you can get additional information. Enter the key in the **Threat Intelligence Exchange Server Settings** page, then return to this page to view detailed information about the file.
Actions	See *File actions*.

Certificate Details Option definitions

Option	Definition
Certificate Details	View details about the selected certificate.
Actions	See *Certificate actions*.

File and certificate actions

The following actions are available for selected files and certificates.

File Actions options

Option	Definition
Actions	**File Known Trusted Installer** — Change the file's reputation to **File Known Trusted Installer**. **Warning:** If you change a file reputation to **File Known Trusted Installer**, all actions and files that the file executes and creates are, by default, treated as known trusted. **File Known Trusted** — Change the file's reputation to **Known Trusted**. **File Most Likely Trusted** — Change the file's reputation to **Most Likely Trusted**. **File Unknown** — Change the file's reputation to **Unknown**. **File Most Likely Malicious** — Change the file's reputation to **Most Likely Malicious**. **File Known Malicious** — Change the file's reputation to **Known Malicious**. **Associated Certificate Details** — View details about the certificate that with which the file is signed, including its issuer. A file can be signed by more than one certificate. **Children Files** — Shows the children file (.exe) or installer for the selected file. **File Parents** — Shows the file parent file (.exe) or installer for the selected file.

Option	Definition
	Where Was File Used — View the systems where the selected file was used. **Choose Columns** — Specify which columns display in the table. **Export Table** — Save the file information to an external file format. **Refresh GTI Reputation** — On the **Actions** menu, select **Refresh GTI Reputation** to update the reputation value of the selected file. **Remove** — Offers the option to **Remove Override** to delete the Enterprise Reputation, **ATD Provider Reputation** to delete the reputation reported by **Intelligent Sandbox**, and **Reputation from External Provider** to delete the reputations reported by an external provider.

Certificate Actions options

Option	Definition
Actions	The following actions are available for the selected certificate. **Cert Known Trusted** — Change the certificate's reputation to **Known Trusted**. **Cert Most Likely Trusted** — Change the certificate's reputation to **Most Likely Trusted**. **Cert Unknown** — Change the certificate's reputation to **Unknown**. **Cert Most Likely Malicious** — Change the certificate's reputation to **Most Likely Malicious**. **Cert Known Malicious** — Change the certificate's reputation to **Known Malicious**. **Associated Files Details** — View files that are signed with the selected certificate. **Parent Certificate Details** — View information about the parent certificate for the selected certificate. Multiple certificates can share a single parent certificate.

Option	Definition
	Signed Certificates — View the certificates that are signed with the selected certificate. **Where Was Certificate Used** — View the systems that have used files signed by the certificate. **Choose Columns** — Specify which columns are displayed in the table. **Export Table** — Save the certificate information to an external file format. **Refresh GTI Reputation** — On the **Actions** menu, select **Refresh GTI Reputation** to update the reputation value of the selected certificate. **Remove** — Remove the override and use the certificate's default reputation setting.

Threat reputations

Managing threat reputations on the TIE server database

Based on the settings in the **TIE** server policies, allow, block, or require user action for the file and certificate reputations used in your environment. You can fine-tune what is allowed or blocked by overriding default reputation settings for specific files and certificates.

File and certificate reputations are added to the **TIE** server database in four ways.

- Running the **TIE** client module **VirusScan Enterprise** or **Endpoint Security Adaptive Threat Protection** 10.5.
- **Intelligent Sandbox** and **McAfee Web Gateway** send reputation information over the **Data Exchange Layer** framework and is added to the database.
- External Reputation provider through **OpenDXL**.
- Manually import files or certificates to the database.

Scenarios where you might override reputations

You can allow or block a file or certificate in your environment if there is false positive mitigation or for managing unknown reputations.

In certain scenarios, you might adjust the reputation for a file or certificate in your environment as an override, for example, to mitigate false positives when **Endpoint Security** has incorrectly blocked a file that you know might be trusted. For other scenarios, see KB90344 for details about reputation management.

Automation should rely on external reputations and not on the overrides since the override of reputations aren't safe in case of false positives.

Task

1. **In Trellix ePO - On-prem, 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. #369845: false positive (jsmith, 0604221584)`
5. **To make sure the change is implemented, click the File Overrides or Certificate Overrides tab to see that the file or certificate is listed with its updated reputation.**

Changing reputations with Trellix ePO - On-prem Web API

Use the remote command provided by the **Threat Intelligence Exchange** server to automate reputation overrides of files and certificates using **Trellix ePO - On-prem** Web API.

We recommend that you enable an external reputation provider configuring **OpenDXL** and visualizing the reputation score on **TIE Reputations** page.

Tip

Best practice: Periodically reconcile the overrides against other reputations and remove those reputations that are already covered for maintaining the adaptive capabilities. You can see the **TIE Server Override** dashboard that shows redundant and conflicting overrides.

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 reputation scores.

Note

You need minimum one hash value present and Base64 values have to be URL escaped.

Reputation	Score
Known Malicious	1

Reputation	Score
Most Likely Malicious	15
Might Be Malicious	30
Unknown	50
Might Be Trusted	70
Most Likely Trusted	86
Known Trusted	99
Known Trusted Installer	100

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.

See example of JSON string of file reputations. You need minimum one hash value present. The optional parameters are **name** and **comment**.

```
fileReps =[{"sha1"."frATnSF1c5s8yw0REAZ4IL5qvSk=","md5":"
8se7isyX+S6Yei1Ah9AhsQ==","sha256":"39Gv4ExOzWr5SMNMrObQJ3A3SSSzEoz2MFi4X8YNAVQ=","reputation":"99"}
{"sha1":"d3HtjhR0Eb3qN6c+vVxeqVVe0t4=","md5":"V+0uApv5yjk4PSpnHvT7UA==","reputation":"85"}]
```

You need one attribute, minimum. The others are optional. For example, you can have a SHA-1 hash value only.

Tip

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

See example of JSON string of certificate reputations:

```
certReps = [{"sha1":"frATnSF1c5s8yw0REAZ4IL5qvSk=","publicKeySha1":"
frATnSF1c5s8yw0REAZ4IL5qvSk=","reputation":"99"}]
```

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

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

Enhancing TIE with External Reputation provider with OpenDXL

Enhance your threat intelligence and detection platform by enabling an external reputation provider in your environment through **OpenDXL**.

If the endpoint doesn't detect a match from other reputation providers, it can allow or block files based on the trust level assigned to the External Reputation Provider as a fallback rule. This new External Reputation provider allows you to differentiate between automated integrations and actual manual Enterprise Overrides. This is useful to avoid false-positives, as this new provider acts as a fallback and it will be considered only if there is no other definitive reputation for the file. Presently, an Enterprise Reputation has precedence over any other provider, potentially causing issues when **Trellix GTI** or **Intelligent Sandbox** have conflicting reputations.

If you already have an **OpenDXL** integration which sets Enterprise Reputations, it's advisable to migrate to External Reputation.

Enable external reputation providers with OpenDXL

Enhance your threat intelligence and detection platform by enabling an external reputation provider in your environment through **OpenDXL**.

Before you begin

Make sure you have a **DXL** client provisioned in your local environment.

For details and troubleshooting about **OpenDXL**, visit the OpenDXL website.

If the endpoint doesn’t detect a match from other reputation providers, it can allow or block files based on the trust level assigned to the provider as a fallback rule.

Note

This feature supports only the file reputation and doesn't support the certificate reputation.

Task

1. **Select Menu → Server Settings → DXL Topic Authorization, then click Edit.**
2. **From the Topic Group list, select TIE Server External Reputation Provider Event → Actions → Restrict Send Certificates.**
   You are redirected to a window with all **Trellix ePO - On-prem** managed client certificates.
3. **On the window, you have a list of the Trellix ePO - On-prem managed client certificates. Choose External Reputation Provider certificate.**
4. **Select the certificate, then click OK to allow the TIE server to receive events from the external provider.**
5. **Navigate to Policy Catalog → Trellix Threat Intelligence Exchange Management x.x.x, select a policy and click Edit.**
6. **Enable the External Reputation Provider. Click Save.**
   The OpenDXL integration can now publish external reputation events into the TIE Server. The recommended workflow is:
   a. Check if **TIE** server can provide a definitive reputation for the file from any other provider.
   b. If there is no reputation available for the file at the moment, publish an External Reputation event.
   For more information and guidance, see python documents.

Overriding rules for file and certificate reputations

You can analyze the impact an override action has in the **TIE** ecosystem before executing the action.

Be aware of the impact an override action has in the **TIE** ecosystem as for inconsistency in the **TIE** server or how it affects future decisions the ecosystem makes.

The impact analysis consists of a list of insights about the action to be performed. Each one has an associated severity that warns about potential undesirable effects in the Ecosystem.

File and certificate overrides tabs

View or change the current reputation information for files and certificates to better control what is allowed or blocked in your environment.

File Overrides tab

Option	Definition
Custom	Search for files using a custom filter. You can use one of the default filters, or create your own: • **None** — Leave the default values to filter your search. • **Malicious files** — Lists files with a malicious reputation. It includes files whose reputation is Known Malicious, Might be Malicious, and Most Likely Malicious. • **Missing names** — Lists files that don't have a name assigned to them. • **Unknown files** — Lists files that don't have a reputation assigned to it yet. • **Add...** — Create your own custom search filter to view specific rows of data. Click **Add...** to specify the search criteria to use. The custom filter is named "Unsaved". Click the right arrow next to the Unsaved label, then click **Edit** to name the custom search filter.
Quick find	Search for a specific file name or type of file. You can use search characters * or ?.
Show selected rows	Lists only those files that are selected.

Option	Definition
All File Names	Lists the files and their details. Selecting a column heading sorts the list by that information.
Selecting a column heading	Select a column heading to sort the information by that type of information. When sorting by any type of reputation, for example by Enterprise or **Global Threat Intelligence** reputation, the files are listed in this order: • Trusted Installer score • Known Trusted • Most Likely Trusted • Unknown • Most Likely Malicious • Known Malicious • Not Set It lists only file reputation and not certificate reputation. **Remember:** Sorting results appear by reputation value rather than alphabetically. For more information about the values, see *Specifying the reputation as a number*.
Selecting a file	Select a file to see details about it.
Actions	See *File actions*.

Certificate Overrides tab

Option	Definition
Custom	Search for certificates using a custom filter. You can use one of the default filters, or create your own: • **None** • **Malicious Certificates** — Lists certificates with a malicious reputation. This includes certificates

Option	Definition
	whose reputation is Known Malicious, Might be Malicious, and Most Likely Malicious. • **Unknown in GTI** — Lists certificates whose reputation is unknown in **Global Threat Intelligence**. • **Add...** — Create a custom search filter. Click **Add...** to specify the search criteria to use. The custom filter is named "Unsaved". Click the right arrow next to the Unsaved label, then click **Edit** to name the filter.
Quick find	Search for a specific certificate. You can use search characters * or ?.
Show selected rows	List only those certificates that are selected.
Selecting a column heading	Select a column heading to sort the information by that type of information. When sorting by any type of reputation, for example by Enterprise or **Global Threat Intelligence** reputation, the certificates are listed in this order: • Known Trusted • Most Likely Trusted • Unknown • Most Likely Malicious • Known Malicious • Not Set **Remember:** Sorting results appear by reputation value rather than alphabetically. For more information about the values, see *Specifying the reputation as a number*.
Selecting a certificate	Select a certificate to see details about it.
Actions	See *Certificate actions*.

Option	Definition
Subject	Shows information for the selected certificate.
Enterprise Reputation	It shows the enterprise reputation as it appears in **TIE**. This reputation that might be present or not. If it is not present, it means that it is not present in **TIE** environment.
GTI Reputation	**Global Threat Intelligence** is the main reputation source that **TIE** uses.
GTI certificate revocation	To be added.

Impact analysis when you override file and certificate reputations

You can analyze the impact analysis before you override a file or a certificate reputation.

When you override a file that is prevalent, it generates many reputation change events that might impact the overall performance. When overriding a certificate, it impacts the signed files associated to that certificate.

Important

The impact analysis is only applicable on the files or certificates selected.

When you override a file or a certificate, the confirmation dialog box includes an impact analysis of how the action affects your files and certificates. It includes a warning message with an assigned severity level if the action has a negative impact. This analysis allows you to safely override a file or a certificate reputation, keeping your **TIE** servers' ecosystem consistent and protected.

Tip

Running an override generates a significant number of reputation change events.

Severity levels during reputation override

Consider these three severity definitions when overriding reputations: Informational rules, warning rules, and blocking rules.

Informational override rules inform the administrator of the impact of the override. For example, it informs the administrator that the reputation override impacts on prevalent items when at least a prevalent file or certificate is selected.

Warning rules alert the administrator of a possible inconsistency or a major impact on the ecosystem. For example, it warns the administrator that an override reputation conflicts with **Trellix GTI** reputation when you try to override a Known Trusted with a Known malicious reputation in **Trellix GTI** . If you receive a warning message and still want to do the override, click the checkbox to continue.

Blocking rules prevent the administrator from running an override that might harm the ecosystem. If the administrator receives a blocking rule message, the override can't continue. For example, the override is blocked when the **Trellix GTI** reputation is Known Trusted.

Override rules for file reputations

Evaluates when	Severity	Message displayed	Applicable (when)	Impact description
Override to Known Trusted Installer	Block	Reputation override and composite reputation are in conflict.	Override to Known Trusted Installer and existing composite is Unknown or Malicious.	Number of selected files affected, usually 1.
Always	Warn	This reputation override will have significant impact.	Sum of all file's enterprise count is greater than 5000 (prevalence default value).	Sum of enterprise count of all selected files.
File that has local reputation	Warn	This reputation override is in conflict with local reputation.	Override to Trusted and local reputation is Malicious or the other way around.	Number of selected files affected.
File that has GTI reputation	Warn	The reputation override is in conflict with GTI reputation.	Override to Trusted and GTI reputation is Malicious or the other way around.	Number of selected files affected.

Evaluates when	Severity	Message displayed	Applicable (when)	Impact description
Only for signed files	Warn	The reputation override is in conflict with the signed certificate reputation.	Override to Trusted and Certificate Enterprise reputation is Malicious or the other way around.	Number of selected files affected.
Only for files that have children	Warn	The reputation override is in conflict with children files with malicious reputation previously generated.	Children files have Not Trusted composite reputation.	Number of children files in conflict.
Always	Informational	The reputation override will have the same value as the existing one.	Override reputation is the same as existing enterprise reputation.	Number of selected files affected.
Always	Informational	The reputation override will be done on prevalent items.	Files/s selected are prevalent.	Number of selected prevalent items.
Override to Known Trusted Installer and has children	Informational	This override will only apply to new child files created in the future.	Override to Known Trusted Installer and has children files.	Number of children files.

Override rules for certificate reputations

Evaluates when	Severity	Message displayed	Applicable when	Impact description
Override to Known Trusted	Block	The reputation override will not be done because the GTI reputation is Known Trusted.	Override reputation is different from existing GTI Reputation.	Number of selected certificates affected: 1
Always	Block	The reputation override will not be done because the certificate is not end entity.	The selected certificate is not an End Entity.	Number of selected certificates affected: 1
Always	Warn	The reputation override will have significant impact.	The sum of enterprise count of every file signed by the selected certificate.	Sum of enterprise count
Certificate has GTI Reputation	Warn	The reputation override is in conflict with GTI reputation.	Override to Trusted and GTI reputation is Malicious or the other way around.	Number of selected certificates affected: 1
Always	Warn	The reputation override will be done on revoked items.	Certificate was GTI revoked	Number of selected certificates affected: 1
Always	Warn	Conflict between reputation override and	Composite reputation of signed files is in conflict with	Number of selected certificates affected: 1

Evaluates when	Severity	Message displayed	Applicable when	Impact description
		some associated files.	new override reputation.	
Override to Malicious reputation	Warn	The reputation override might imply that the endpoint will ask for the file reputation anyways.	Override to Known Malicious, Most Likely Trusted, or Unknown.	Number of selected certificates affected: 1
Always	Informational	The reputation override will be done on prevalent items.	Certificate selected is prevalent.	Number of selected certificates affected: 1
Always	Informational	The reputation Override will have the same value as the existing one.	Override reputation is the same as existing enterprise reputation.	Number of selected certificates affected: 1

Access file details from a threat event log

In **Trellix ePO - On-prem** server, the action **Show File Details** appears enabled only for detection threat events (of **TI ENS** or **VirusScan Enterprise**) and can only be done if the associated file has SHA-1 or MD5 hash. The action shows the file details of the file that caused the threat event.

You can access file details of associated files only for files with MD5 or SHA-1 hashes from detection threat events.

First, in **Trellix ePO - On-prem**, select **Menu** → **Reporting** → **Threat Event Log**, then select a threat event. Then, click **Actions** → **Show File Details** to see the details of the file that caused the threat event.

Note

For a description of events and security threats and the actions taken, see the documentation for **TIE** or for the TIE client module for **VirusScan Enterprise**.

Submitting file samples

All **TIE** server instances (except Write-Only Primary and Reporting Secondary) can forward file samples to **Trellix Intelligent Sandbox** for analysis.

On the **Sandboxing** tab on the **Intelligent Sandbox** section, 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 **Intelligent Sandbox**, including Portable Executable (PE) and extended file type support. PE files are enabled by default. For more information, visit https://docs.trellix.com/.

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

You can locally install trusted CAs certificates or use the certificates provided by **Intelligent Sandbox** 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 **Intelligent Sandbox**, see the ***Trellix Intelligent Sandbox*** *Product guide*.

It is configured via **Trellix ePO - On-prem** policies for different endpoint groups. The **Intelligent Sandbox** instances can be grouped based on their geographical distribution. You might assign **TIE** server policies for each group of **Intelligent Sandbox** instances based on their geographical location. Use this configuration especially in large-scale deployments.

Under Polling Settings, you can choose which **Intelligent Sandbox** servers should be polled for detonation results. By default all servers are polled. You can change this policy to poll only local **Intelligent Sandbox** servers for results, or none, which requires **DXL** integration enabled in **Intelligent Sandbox** to guarantee that **Intelligent Sandbox** reports are received by **TIE** server.

This configuration is used together with **DXL** broker service zone to determine which broker a reputation request is sent to. See **DXL** product documentation for more details.

See KB86707 for details about this configuration.

Submitting files for further analysis

If a file's reputation is unknown, you can submit it to Intelligent Sandbox for further analysis. Use the TIE server settings to specify which files you submit.

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

Trellix GTI telemetry information

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

Attention

Consider that this is detection telemetry, not product telemetry.

Category	Description
File and certificate	• **TIE** server and client versions • Reputation override settings made with the **TIE** server • External reputation information, for example from **Intelligent Sandbox**
File-only	• File name, type, path, size, product, publisher, and prevalence • SHA-1, SHA-256, and MD5 information • Operating system version of the reporting computer • Maximum, minimum, and average reputation set for the file • Whether the reporting client is in Observation mode • Whether the file was allowed to run, was blocked, or was cleaned • The product that detected the file, for example **Intelligent Sandbox** or **VirusScan Enterprise** **Note:** The username is obfuscated at the endpoint if the path contains it.
Certificate-only	• SHA-1 information • The name of the certificate's issuer and its subject • The date the certificate was valid and its expiration date

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

Configure file types for analysis

Configure the file types that need to be uploaded to **Intelligent Sandbox** for execution and analysis.

Before you begin

Verify that **Intelligent Sandbox** is enabled and configured correctly in **Trellix ePO - On-prem** on the **Policy Catalog** page through health checks.

If you select multiple file types, the portable executable (PE) files are prioritized and sent first to **Intelligent Sandbox**.

1. In **Trellix ePO - On-prem**, select **Policy Catalog** → **Sandboxing**.
2. In **Intelligent Sandbox**, enable the service and configure the server list, the connection settings and the file types available on the list.
3. Click **Save** when you are finished.

Results

TIE server submits the file types selected to **Intelligent Sandbox** 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 **Trellix ePO - On-prem** 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 **Trellix ePO - On-prem**, 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 ***Trellix ePolicy Orchestrator - On-prem*** *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.

Important

After 3.0.x release, we are deprecating this feature. You can use **Trellix ePO - On-prem** to tag the compromised system and run reports.

Task

1. **In Trellix ePO - On-prem, 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.**

Results

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 **System Health Indicator**.

Tie server notifications

When using **TIE** server on **Trellix ePO - On-prem** 5.10 or later, you can get an alert is shown in the notifications section.

TIE server notifies you when a given File or Certificate is considered relevant:

- For files, when it's a parent file with not definitive Composite Reputation and it's prevalent.
- For certificates, when its reputation is not definite and the impact is high considering the impact as the number of files signed by the certificate and the number of endpoints running those files.

so the administrator retrieves the File or Certificate and act on them. These notifications are generated by running a weekly Server Task.

Recommended workflow

Assess, prioritize, analyze, and react against threats using the **TIE** services activities in **Trellix ePO - On-prem**.

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

For an effective use of **TIE** services 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 **Trellix ePO - On-prem** determine which files or certificates are a priority for analysis. Navigate: **TIE Reputations → File Search → Custom**, or **TIE Reputations → Certificate Search → Custom**.

3. Analyzing — It presents the list of associated files or certificates, their parent files or certificates, where they were run, and their details including behavioral attributes. 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 **Trellix ePO - On-prem** can list queries for the systems that were tagged as compromised. Navigate: **TIE Reputations** → **File Search** → **Actions** → **System Health Indicator** → **Set Possibly Compromised**

Queries and reports

You can see reports and customize queries to access threat information for files, certificates, and events of your **TIE** server instances.

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

Viewing queries and reports

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

The queries are available in the **Trellix ePO - On-prem 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

View TIE server reports

You create and view **Threat Intelligence Exchange** server reports using **Trellix ePO - On-prem** to view **TIE** server events and file and certificate information.

Task

1. **In Trellix ePO - On-prem, select Menu → Reporting → Queries & Reports.**
2. **Use Quick find to access TIE server reports.**
    - For server reports, enter `TIE`.
3. **Click Run to see the report data.**

Results

See the **Trellix ePO - On-prem** documentation for details about creating and using queries and reports.

Customize queries

Create custom queries using **Trellix ePO - On-prem** query system and reuse them in dashboard monitors and report sections.

We provide an overview on using **Trellix ePO - On-prem** query capabilities for gathering **TIE** server information. For more details, see **Trellix ePO - On-prem** 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

1. **In Trellix ePO - On-prem, 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**.

      Option definitions

Option	Definition
Certificates	▫ **Certificate Enterprise Reputation** — Shows the Enterprise reputation of the certificates. ▫ **Certificate Reputation** — Retrieves summarized non-Enterprise reputation for certificates from the TIE server. ▫ **Certificates** — Retrieves certificate information from the **TIE** server. ▫ **New Certificates on Systems** — Retrieves information about systems with new certificates.
TIE Data Storage Management	**Cleanup Trending Summary** — Retrieves **TIE** server cleanup trending summary.
Files	▫ **File Enterprise Reputation** — Retrieves summarized Enterprise Reputation from files. ▫ **File Reputation** — Retrieves summarized non-Enterprise reputation for files from the **TIE** server. ▫ **Files** — Retrieves file information from the **TIE** server.

Option	Definition
	▫ **New Files on Systems** — Retrieves information about systems with new files.

- **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.**

Results

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

Maintaining the TIE server

Maintain TIE server database

Schedule a server database maintenance task to claim the empty space available after executing the task.

Before you begin

- Keep the task enabled. If you disable the task, the database can't use the free space available after running the cleanup task and claim the free space constantly thus impacting performance.
- Run and schedule the task during low traffic hours to avoid impacts on performance.

For details about **TIE** server data management server task runs daily, see Managing database size and task details.

Task

1. **In Trellix ePO - On-prem server, select Menu → Automation → Server Tasks → TIE Server Database Maintenance, then click Edit.**
2. **On the Server Task Builder page, click the Schedule tab.**
   Verify the schedule information of the task. By default, the task is executed on Sundays at 2 a.m..
   Click **Save** to finish.

Results

The **TIE Server Data Cleanup** page from the drop-down list of **Dashboards** shows an overview of cleanup executions, server new files, and database size.

Synchronize certificate authorities

After bridging **DXL** fabrics in an environment with multiple **Trellix ePO - On-prem** servers, synchronize certificate authorities (CA) of the **TIE** servers.

Task

1. **In Trellix ePO - On-prem, select Menu → Automation → Server Tasks, then run TIE Server Synchronize CA.**
2. **Verify that the task is completed in the Server Task Log.**
   If you don't see the **TIE** server instances, verify that the topology is synchronized.

Using Update Metadata Aggregation for Local intelligence

The **Update Metadata Aggregation for Local Intelligence** option improves the Update Metadata messages processing and reduces the bandwidth utilization.

The **Update Metadata Aggregation for Local Intelligence** filters interesting updates from metadata messages and summarizes in-memory relevant information, publishing it to **TIE** Server for processing with a predictive frequency or when any urgent information arrives.

The Update Metadata Aggregation for Local Intelligence is implemented as a **DXL** Broker extension and you can enable it from **DXL** Topology section in **Server Settings** in **Trellix ePO - On-prem**.

When to enable Update Metadata Aggregation for Local Intelligence

Each environment could be unique in configuration and complexity, where you can find complex topologies, multiple **Endpoint Security** versions installed in different groups of endpoint, and the same for multiple content and rules. This scenario produces that multiple endpoints can publish the same or similar information multiple times or can publish the hash information in multiple messages.

Tip

This situation can arise when some beta rules are enabled.

In consequence, multiple and duplicated messages travel in the **DXL** fabric that **TIE** server needs to process, and it consumes resources and performs unnecessary database searches and writes. This feature improves the Metadata message processing.

Enable Update Metadata Aggregation for Local Intelligence

Enable Update Metadata Aggregation for Local Intelligence in the **DXL** topology.

Task

1. **Log on to the Trellix ePO - On-prem server as an administrator.**
2. **Select Menu → Configuration → Server Settings → DXL Topology, then click Edit.**

   Note

   The option on the page varies based on whether you selected a broker or a hub. Unassigned brokers are listed below to the hubs.

3. **Select a broker item from the list.**
4. **In the Broker Extensions section, find the Update Metadata Aggregation for Local Intelligence extension and check it.**
5. **Repeat the step 4 in every broker where you want to enable the extension, then click Save.**
   For more information about enabling or disabling DXL Broker Extension, see *McAfee Data Exchange Layer 5.0.x product guide*.

Synchronize TIE server topology

Manage the synchronization of the **TIE** server topology in a multiple-**Trellix ePO - On-prem** environment.

Task

1. **In Trellix ePO - On-prem, select Automation → Server Tasks → TIE Server Synchronize Topology.**
2. **Click Edit to configure the task, or Run to perform the task.**
3. **If you click Edit, you can configure the task settings.**

Option	Description
Description	Details of the task like name, frequency and notes.
Actions	Command to execute the task. No configuration required.
Schedule	Configure how often and when the task is executed. By default, the task is run daily at 12:15 A.M.
Summary	Summarize the details of the configuration.

Monitor the health status of the TIE server

Configure server tasks and 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 **Trellix ePO - On-prem**, 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 creates a server event in **Trellix ePO - On-prem**.

Note

Consider that the task is enabled but the **Automatic Response** handler must be configured since it isn't available by default.

Task

1. **In Trellix ePO - On-prem, select Menu → Automation → Automatic Responses.**
2. **Create notifications and actions using Automatic Responses**
   See ***Trellix ePolicy Orchestrator - On-prem*** *Product Guide* for details about Events and Responses.

Results

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

Event ID	Severity	Level	Event name
37191	3	Error	TIE Server didn't register reputation search service
37175	1	Alert	Primary TIE Server Unreachable
37176	1	Alert	Write-only Primary TIE Server Unreachable
37177	3	Error	Secondary TIE Server Unreachable
37178	3	Error	Reporting Secondary TIE Server Unreachable
37179	3	Error	TIE Server Unreachable
37180	3	Error	Cache TIE Server Unreachable
37181	2	Critical	TIE Server Database Replication Fail
37182	2	Critical	Primary TIE Server can't connect with GTI
37183	3	Error	Secondary TIE can't connect with GTI
37184	3	Error	TIE Server can't connect with ATD
37186	4	Warning	TIE Server certificates Error

Event ID	Severity	Level	Event name
37187	4	Warning	TIE Server Writer queues are reaching its maximum size
37188	2	Critical	TIE Server Writer queues are full
37189	3	Error	TIE Server in cache mode isn't working
37190	3	Error	TIE Server in cache mode isn't properly configured
37274	7	Debug	TIE Server status is OK
37192	2	Critical	TIE Server ran out of available database connections
37193	3	Error	TIE Server running out of available database connections
37194	2	Critical	TIE Server ran out of space for data
37195	3	Error	TIE Server running out of space for storage
37196	2	Critical	TIE Server deep maintenance tasks not running
37197	3	Error	Primary or Write-only Primary didn't run

Event ID	Severity	Level	Event name
			maintenance tasks in more than a day
37198	2	Critical	TIE Server database engine is not running
37199	3	Error	TIE Server time is not synchronized

Following this approach, you use **Trellix ePO - On-prem** Automatic Responses for sending email notifications, creating **Trellix ePO - On-prem** 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 and making adjustments

As the Threat Intelligence Exchange runs in your environment, reputation data is added to the database.

Use the **Trellix ePO - On-prem** 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 reputation is 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 **Trellix GTI** information. For files, you can also access VirusTotal data directly from the **TIE Reputations** details page to see additional information (see About VirusTotal).
- 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 reputations 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 the product documentation for **Trellix Threat Intelligence Exchange**.

Monitoring the TIE server

Monitor the health status of your **TIE** server instances on the **TIE Server Topology Management** page in **Trellix ePO - On-prem**.

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

Important

Consider that the health status is set based on the worst case scenario described in the checkups.

Status of health events

Status	Definition
OK	The **TIE** server topology is healthy and works correctly.
WARN	The **TIE** server topology might be degraded.
ERROR	The **TIE** server topology isn't working as expected.

TIE server connection checkups

Checkup	Definition
DXL Connection	This check tests the connection between the **TIE** server instance that you selected and **Trellix ePO - On-prem** through **DXL**. This checkup is valid for all operation modes of the **TIE** servers. Click **[+]** to

Checkup	Definition
	see details about the **IP Address**, **System Name**, and **Broker UID** of the **DXL** Broker.
Database Replication	This checkup verifies if the replication of the database is running. This checkup is applicable only to secondary and secondary-reporting server instances.
GTI Connection	This checkup verifies if the connection to **Trellix GTI** is enabled and properly configured. This checkup is applicable to all server instances, except secondary-reporting server instances.
Certificates Compliance	This checkup verifies that: • The stored certificate is valid for the current IP address. • The certificate is valid against the CA. • The keystore used for sample submission from the endpoints can be opened using the stored password. • The **Intelligent Sandbox** keystore can be opened if the **Intelligent Sandbox** certificate validation is enforced.
Extension Compatibility	This checkup verifies that the version of the **Trellix ePO - On-prem** extension matches the version of each **TIE** server instance.
Performance Status	Click **[+]** to see details about **CPU Usage**, **Throughput**, and **General Write Buffer Usage**. **Reputation Cache** displays hits and misses ratios.
Cache topology configuration	This checkup verifies that the topology configuration of the cache mode is correct.
Internal Cache status	This checkup verifies the status of the cache mode regarding initialization, the percentage of use, and the number of objects saved, among others.

Checkup	Definition
ATD Connection	This checkup verifies if the connection to **Intelligent Sandbox** is enabled and properly configured.
Database and Storage	This checkup verifies database available storage, local connections, and maintenance executions.
Reputation Search Service	This checkup verifies that the search service works correctly.
NTP Status	This checkup verifies that the **TIE** servers and **Trellix ePO - On-prem** are synchronized.

Using TIE server telemetry information

Collect the health and performance information of all **TIE** server instances managed locally by the **Trellix ePO - On-prem** server to send operational telemetry data.

Important

This feature is deprecated after 3.0.x release in favor of **Trellix Agent**-based telemetry information. This is not detection telemetry sent by **TIE** server to GTI and does not affect any **TIE** server workflow.

By enabling this task in **Trellix ePO - On-prem** server, **Trellix** can collect anonymous information about performance metrics through the Product Improvement Program extension of **Trellix ePO - On-prem**. This task improves supportability by sending consolidated information collected from each **TIE** server that **Trellix ePO - On-prem** server manages. The information is stored temporally in **Trellix ePO - On-prem** database until the PIP extension collects the information and sends it to the **Trellix ePO - On-prem** Telemetry Platform in the cloud.

Configure the TIE server telemetry task

You can change the default configuration of the **TIE Server Telemetry** task in **Trellix ePO - On-prem** server.

Before you begin

Verify that the task is added on the **Server Tasks** page in **Trellix ePO - On-prem**.

Task

1. **Select Menu → Server Tasks → TIE Server Telemetry, then click Edit to modify the task configuration or Run to run the task.**
2. **To edit the task, on the Schedule tab, configure how often and when you want to run the task. Click Next to continue.**

3. **On the Summary tab, verify the configuration is correct.**
4. **Click Save to finish.**
5. **To run the task manually, select TIE Server Telemetry, then click Run.**
   You are redirected to the **Server Task Log** page.

   Trellix ePO - On-prem collects the telemetry information and the server receives it when the PIP task is run.

Managing TIE server database

Manage your database size with data retention policies for avoiding service degradation during database growth.

This server task in **Trellix ePO - On-prem** checks the database size and compares it with a size threshold. If the database exceeds the threshold, the cleanup is executed.

Note

You can run the task as needed and configure the frequency from **Trellix ePO - On-prem** on the **Server Tasks** page.

The task cleans the database of files that are old enough to keep the database under the configured file count. By default, the task is executed every day at 12.30 a.m. midnight for keeping the size of the database within 15 GB.

The file selection criteria determines that files without an Enterprise reputation (or a reputation override) are candidates for a purge, to avoid removing locally generated Threat Intelligence.

For details about **TIE** server database maintenance server task runs weekly, see Maintain TIE server database.

Manage TIE server database

Perform a daily cleanup of the **TIE** server database to optimize performance.

Task

1. **In Trellix ePO - On-prem server, select Menu → Automation → Server Tasks → TIE Server Data Management, then click Edit.**
2. **On the Actions tab, configure the task.**

Setting	Description
Data Management General Configuration	In the **Database Size Threshold** field, enter the maximum size of the **TIE** database. Actions on this page take effect only when the database size is exceeded.
Data Management General Rules	• **File Retention Period** — Set the retention period of a file in the database, between a minimum of 1 day and a maximum of 120 days. **Important:** Files that are older than 90 days and without a request are deleted.

Setting	Description
	• **Idle Agent Retention Period** — How many days of inactivity before an endpoint ID is removed from the database. This can occur when an endpoint's ID has changed. The maximum retention period is 120 days. By default, files are deleted after 60 days. • **Remove File References For Prevalent Files** — Delete redundant file references for Known Trusted files that become prevalent (have run on more than 5000 endpoints). • **Remove Certificate References For Prevalent Certificates** — Delete redundant certificate references for Known Trusted certificates that become prevalent (have run on more than 5000 endpoints).
File Type Configuration	Select the types of files to be removed from the database. • **File Type** — Select the file type to be removed. • **Retention period** — Specify the number of days to retain the file information before it is deleted from the database. By default, it is set in 90 days or the maximum defined on the **File Retention Period**. Click **Add** to select more than one file type.

3. **On the Schedule tab, configure when the task is run.**
   Best practice: Schedule the task daily at low traffic hours.
4. **On the Summary tab, verify the configuration details of the task. Click Save to finish.**

Results

The **TIE Server Data Cleanup** page from the drop-down list of **Dashboards** shows an overview of cleanup executions, server new files, and database size.

Managing file reputations

How is a reputation determined?

When a file tries to run on a managed system, the **TIE** server stores and share threat information based on file and certificate reputations that it receives from different reputation providers, on premise and in the cloud, and determines its reputation.

A file or certificate's reputation is determined as follows.

1. A user or system tries to run a file.
2. **VirusScan Enterprise** or **Endpoint Security** inspects the file and is unable to determine its validity and reputation.
3. The client for **Trellix Endpoint Security (ENS)** or **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 file's prevalence and reputation data from the cache.
    - If the file hash is not found, the module queries the **TIE** server. If the hash is found, the module gets the prevalence data (and any available reputations) for that file hash.
    - If the file hash is not found in the **TIE** server database, the server queries **Trellix GTI** for the file hash reputation. **Trellix GTI** sends the available information, for example "unknown" or "malicious," and the server stores that information.
    - If **Intelligent Sandbox** (sandboxing) is enabled as a reputation provider, the file is identified as a candidate for submission.
5. The **TIE** server returns the file hash's enterprise age, prevalence data, and other data points to the client based on the data found. If the file is new to the environment, the server sets the flag to submit metadata on the response. Reputation response can include information from different providers other than **Trellix GTI** or **Enterprise Overrides**, for example, **McAfee Web Gateway** or **Intelligent Sandbox**.
6. The module evaluates the following metadata to determine the file's reputation, plus all metadata sent, and uses the **TIE** Content rules to determine local reputation.
    - File and system properties
    - Enterprise age and prevalence data
    - Reputation
7. The client responds according to the settings on the system that is running the file and blocks or allows executing the file.
8. The client updates the server with the reputation information defined by a set of **TIE** content rules, and whether the file is allowed or blocked. It also sends threat events to **Trellix ePO - On-prem** via the **Trellix Agent**.

Managing reputations if sandboxing is enabled

If **Intelligent Sandbox** is enabled on the **TIE** server, the response to a reputation request includes a flag requesting the submission of the binary, if all conditions are met

1. If **TIE** server reputation response includes a flag with a sandboxing candidate tag, the endpoint sends the file to **Threat Intelligence Exchange** server. Then the **TIE** server sends the file to **Intelligent Sandbox** for scanning. Then, the **TIE** server polls for analysis reports until they are available. You can enable **Intelligent Sandbox** sandbox reputation provider or both from the **Policy Catalog** page in **Trellix ePO - On-prem**.
2. **Intelligent Sandbox** scans the file and can send file reputation results to the **TIE** server through **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. The **TIE** server or any other **Trellix** product can initiate this process. In either case, the **TIE** server processes the reputation and saves it in the database.

Managing reputations if Trellix GTI Private Cloud is present

If **Trellix GTI** Private Cloud is present, the reputation requests are routed to the private cloud, instead of routing them to **Trellix GTI**

Managing unknown reputations

The **TIE** reports a composite reputation for a file as unknown when it doesn't have enough evidence to classify the file reputation as trusted or malicious.

Depending on the endpoint products available, the endpoint monitors files with unknown reputation. A sandbox engine might be used as well.

Age and prevalence of the file also affect its reputation since the file eventually increases its reputation to trusted if it is prevalent in the organization and if it is frequently used.

For more information, see KB90344.

Importing file reputations

Identifying file and certificate reputations

You can identify the reputation of the file or the certificate to be imported by its hash values.

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.

Note

File name and comment are optional but we recommend to have them.

Example of importing a file

When you import a file, you can add a comment field to the XML file to describe the file or certificate to import. The **<Comment>** includes an appropriate comment to identify it on the reports.

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

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.

Note

Files can have SHA-1, SHA-256, and MD5 hash values (minimum, one required) while the certificates can have SHA-1 hash and Public Key SHA-1 (both required).

Example of importing a certificate

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

Requirements for creating an XML import file

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

- 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 both hash values and one reputation.

Reputation values and definitions

Reputation setting	Numeric value	
Known trusted installer	100	All files created by that file are trusted.
Known trusted	99	It is a trusted file or certificate.
Most likely trusted	85	It is almost certain that the file or certificate is trusted.
Might be trusted	70	It seems a benign file or certificate.
Unknown	50	The reputation provider has encountered the file or certificate before but the provider can't determine its reputation at the moment.
Might be malicious	30	It seems a suspicious file or certificate.
Most likely malicious	15	It is almost certain that the file or certificate is malicious.
Known malicious	1	It is a malicious file or certificate.
Not Set	0	The file or certificate's reputation hasn't been determined yet.
Not Available	—	The reputation provider hasn't been queried about the specific item. This reputation label also appears for disabled reputation providers or providers with pending reputation reports.

Reputation setting	Numeric value	
		Important: 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.

Import reputations from an XML file

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

Before you begin

The XML file must have one hash value, minimum.

Make sure that you are overriding file and certificate reputations not seen on the environment yet, files home brewed by the customer, or reputations from third-party sources. Check the **TIE Server Overrides** dashboard before importing reputations.

Import XML file format is different from the export XML file format.

Note

Don't import files or certificates with a matching **Trellix GTI** reputation.

Task

1. **On the TIE Reputations page, click File Overrides, then select Actions → Import Reputations.**
2. **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. Click **OK** to complete the import.
    - **Import Single Reputation** — Enter the information for the file.

Launch import wizard

Launch import wizard

Launch the import wizard and select a STIX (Structured Threat Information eXpression) standard XML file or a CSV file to import file hashes in a wizard and to add a file reputation overrides to the **TIE** services database.

Before you begin

The STIX or the CSV file must have one hash value, minimum.

You can generate CSV files by exporting **TIE** reputation tables. Add the columns for hash values, then use the **Export Table** task.

Important

Overriding file and certificate reputations not seen on the environment yet, files home brewed by the customer, or reputations from third party sources. We don't recommend that you import files or certificates with a matching **Trellix GTI** reputation.

Task

1. **In Trellix ePO - On-prem, select Menu → Systems → TIE Reputations.**
2. **On the File Overrides tab, click the Actions menu and then select Launch import wizard.**
3. **On the Select file tab, browse to the file location, whether for importing a STIX or a CSV file, then click Next.**
   For information about STIX, go to www.stix.mitre.org.

   Note

   TIE services doesn't support conditions.

4. **On the Review details tab, select checkbox, then click Submit selected items.**
5. **On the Confirm action tab, select Reputation to import information, and add comment, then click Confirm.**

Results

File and certificate overrides are imported.

Review details of STIX import

In STIX import wizard, there are 10 columns that show the details of the file imported. See the table ***Option definitions*** to learn about each of them.

Option definitions

Option	Definition
SHA1	It is a hash value that identifies a file.
MD5	It is a hash value necessary to perform a file import because TIE interacts with **Global Threat Intelligence**. For more information about **Global Threat Intelligence** interaction with TIE, see **Trellix Global Threat Intelligence** web page.

Option	Definition
SHA265	It is a hash value that identifies a file.
Important: When there are no hash values present, the hash column is not displayed.	
Filename in STIX	It is the name of the file to be imported. The name might be present or not.
Enterprise reputation	It shows the enterprise reputation as it appears in **TIE**. This reputation that might be present or not. If it is not present, it means that it is not present in **TIE** environment.
GTI reputation	**Global Threat Intelligence** is the main reputation source that TIE uses.
ATD reputation	**Intelligent Sandbox** (ATD) reputation might be present or not. If no results are shown, it means one of the following options: • **Intelligent Sandbox** is not installed in your environment. • **Intelligent Sandbox** has no records of the file. • **TIE** and **Intelligent Sandbox** haven't viewed the file, or • The environment has not viewed the file.
Local reputation	It shows the reputation given by the TIE module. See also *TIE Module*.
Enterprise count	It shows how many times the TIE environment has viewed the file. If there isn't an enterprise count, the reputation value has not been set.
VirusTotal detection ratio	It shows how many times different tools detected a file and the reputation given by those tools. For

Option	Definition
	more information about VirusTotal detections, go to www.virustotal.com.
Validations	See *Validations in STIX import*.

Validations in STIX or CSV import

After you submit the files to be imported, step 2 shows a Validations column.

Validation definitions

Validation	Definition
Ready for import	The file has all necessary information to be imported.
Valid. Reputation already set	The file is valid for import and has a reputation already set.
Warning: Enterprise count > 0	The file has at least one reputation already set.

Attention: If the file has at least one valid hash value, it is imported. However, if there is a hash value but it is invalid or malformed, the import is not completed.

Building file prevalence and observing

You can see what is running in your environment and add file and certificate reputation information to the **TIE** services database. This information also populates the graphs and dashboards in **Trellix ePO - On-prem** where you view detailed information about files and certificates.

To get started, create one or more **TI ENS** 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 **Intelligent Sandbox** 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 **TIE** services block or allow if the policy is enforced.

COPYRIGHT

Trellix