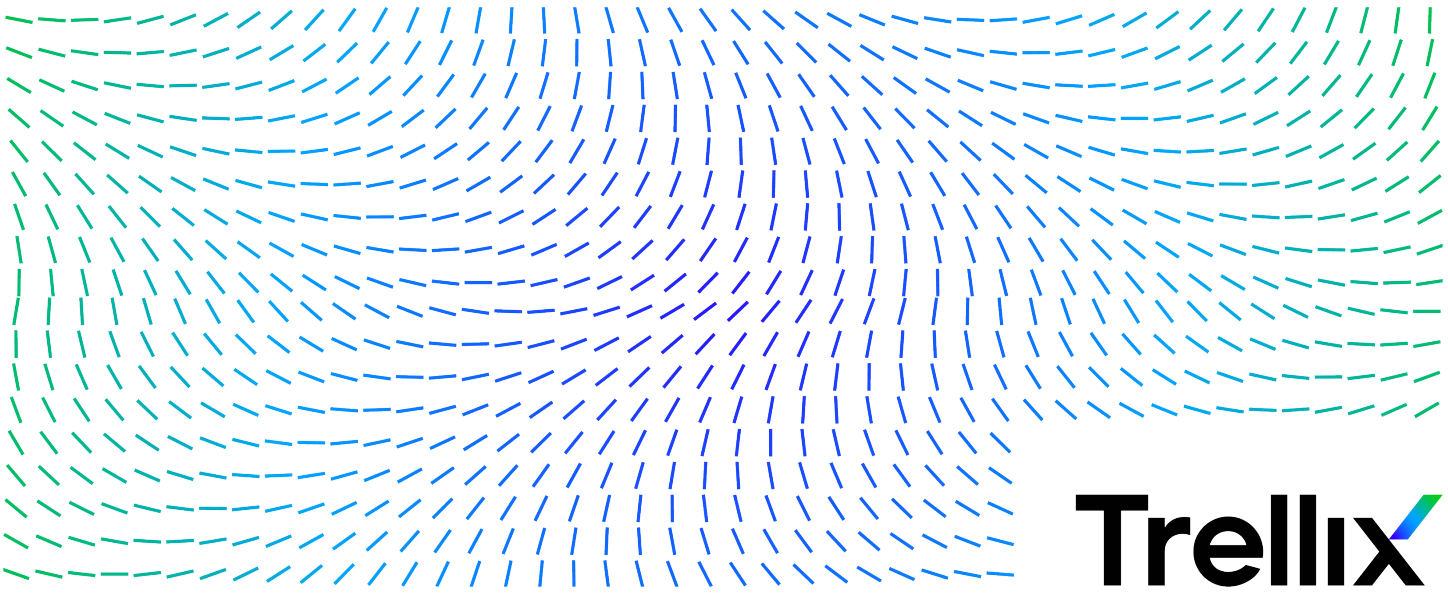
Trellix Threat Intelligence Exchange 4.0.x Installation Guide



Contents

Installation overview

Benefit from installing the components for **Trellix Threat Intelligence Exchange (TIE)** manually after **Trellix Endpoint Security (ENS)** installation is complete to manage **Threat Intelligence Exchange** features from **Trellix Endpoint Security (ENS)**.

The **TIE** server is a real-time adaptive prevention provider that gives customers the power of knowledge by telling them what is malicious, trusted, and unknown in their environment, where it was used and when. Installing the Threat Intelligence components as **Trellix ePolicy Orchestrator - On-prem** extensions, you can manage **TIE** features for enterprise-wide protection against new emerging and discovered threats within milliseconds.

The components are a client module for **Trellix Endpoint Security (ENS)**, a server for file and certificate reputation storage, and **Trellix Data Exchange Layer** (DXL) brokers for bidirectional communication between managed systems on a network.

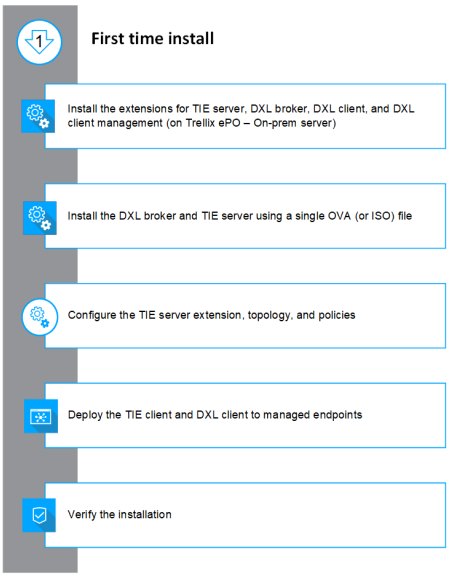
Which type of installation do you need?

Note

When downloading your software, either for the first-time installation or for upgrade installation, in **Trellix ePolicy Orchestrator - On-prem**, you find the necessary files in **Software Manager** (**Software Catalog** in **ePolicy Orchestrator - On-prem** 5.10).

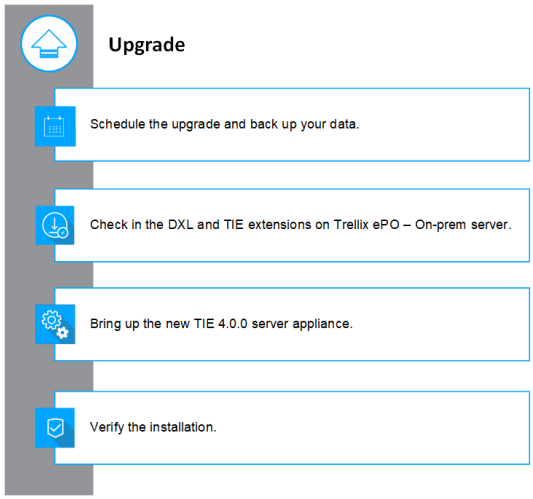
First-time installation workflow

As a **Trellix ePO - On-prem** administrator, you can install the **TIE** Server appliance using an OVA or an ISO file on a Virtual Machine (VM) after you deploy the **Trellix Data Exchange Layer** brokers. For your endpoints, you install the **TIE** client module and the **Data Exchange Layer** client you need. To complete the installation, you need to configure the operation mode of the **TIE** server and assign its policies.



Upgrade installation workflow

If you have your TIE server installed, upgrade to the latest version to benefit from the latest improvements.



Planning your deployment

Designing your infrastructure

For deploying **DXL** brokers, enable service zones so the closest **TIE** server handles the requests. Enable **DXL** Client affinity so **TIE** Reputation Cache servers work efficiently. See KB89775 for details.

For deploying **TIE** servers, follow these guidelines to determine the number of servers you need.

- Always deploy at least two **TIE** servers instances, one Primary, and one Secondary, for fault tolerance. This minimum server topology supports up to 1000 requests per second in a dedicated infrastructure.
- Deploy collocated **TIE** Secondary servers to increase capacity as required. Deploying additional Secondary servers (7 secondary instances, maximum) ensures that the network infrastructure meets multiplied replication bandwidth requirements.

  Note

  You can experience throughput reduction when adding remote Secondary servers to your topology.

- Change the operation mode of a Primary server to a Write-Only Primary to maximize replication potential for deploying multiple Secondaries.
- Add a Reporting Secondary server to concentrate load from **Trellix ePO - On-prem** reporting and only enable search services on it.
- Rely on Reputation Cache servers when remote bandwidth isn't enough to replicate the full reputations database, or to increase reputation throughput of reused files and certificates.

For more details, see Sizing and performance topic from **Trellix Threat Intelligence Exchange (TIE)** Installation Guide.

Sizing and performance

Determine your hardware requirements before your **TIE** server deployment by gathering reference metrics such as resource usage and capacity, latency impact and scalability, and caching benefits. **Trellix** performed these tests on different server-class systems.

The following information helps you determine the number of instances, location and level of server hardware, system core, memory, storage, and network bandwidth that **TIE** recommends for the components of your **TIE** software deployment. This information can help you make hardware purchasing and provisioning decisions.

This document assumes base knowledge of **DXL** infrastructure internals as described in the **DXL** Architecture Guide. Service Zones and Affinity should be used to optimize reputation requests.

Important

Results have been estimated or simulated using internal **Trellix** analysis or modeling and provided to you for informational purposes. Any differences in your system hardware, software, or network configuration might affect your actual performance. These are guidelines only; proof of concepts and incremental deployments are always recommended to understand the practical impact.

Estimating the number and location of TIE servers

The recommended deployment procedure involves running the solution in a small subset of the total managed endpoints to extrapolate the number of requests per second that will be required to handle.

Considering all the reference metrics in the following sections, use these guidelines when determining the number of **TIE** servers to deploy:

1. Always deploy at least two **TIE** servers instances, one primary and one secondary for fault tolerance. This supports up to 1000 requests per second in a dedicated infrastructure.
2. Place additional collocated **TIE** secondary servers to increase capacity as required, making sure multiplied replication bandwidth requirements are met by the network infrastructure. Consider latency impact on throughput when adding remote **TIE** secondary servers.
3. Switch to Write-Only primary Server to maximize replication potential for deploying multiple Secondaries. Add a Report-Only secondary server to concentrate load from **Trellix ePO - On-prem** reporting.
4. Rely on Reputation Cache servers when remote bandwidth is not enough to replicate the full reputations database or to increase the reputation throughput of reused files and certificates.

Reputation traffic is reduced significantly when endpoints have already cached reputations; however, spikes might be seen after endpoint upgrades (including content) as they clear their local cache.

Each customer vertical imposes different traffic characterization impacting the load against the **TIE** server capacity (file and certificate reuse and the number of new files are the key factors). For instance, companies in the financial vertical are expected to have more reuse and less unique files than those in the software research and development segment. To estimate requests coming from integrated gateways at the perimeter, product-specific dashboards can be used to dimension the number of requests.

As a basic rule 1000 requests per second can cope with traffic from 25000–50000 endpoints; and 500 requests per second can cope with traffic from 25000–50000 gateway users, assuming down-selection is properly configured to ask for the reputation of relevant files.

Make sure network requirements between the primary and every secondary are met by the networking infrastructure, available bandwidth should properly cover database replication needs.

Major deployments must avoid workload consolidation of virtual appliances on shared physical hosts and even consider running directly in bare-metal to avoid resource conflicts.

What is measured and determined

To determine the recommended sizing and performance guidelines, measure:

- Resource usage and capacity
- Latency impact and scalability
- Caching benefits

Products tested

The following **Trellix** products at their recommended configuration were tested.

- **Trellix Agent** 5.0.3
- **Trellix ePolicy Orchestrator - On-prem** 5.3.2
- **Trellix Data Exchange Layer** 3.0.1
- **Threat Intelligence Exchange** 2.1.0

The products were running over the following infrastructure.

- VMware ESXi 6.0.0
- ProLiant BL 460c G8

Note

The sizing and performance details mentioned are simulated only considering TIE 2.1.0, other **Trellix** product versions, and infrastructure versions listed above. The details will be updated with latest versions in near future.

Resource usage and capacity

This section describes resource usage when running the **TIE** solution over a few hours.

The objective is to show CPU, RAM, Disk, and Network usage metrics at peak load of the minimum recommended setup.

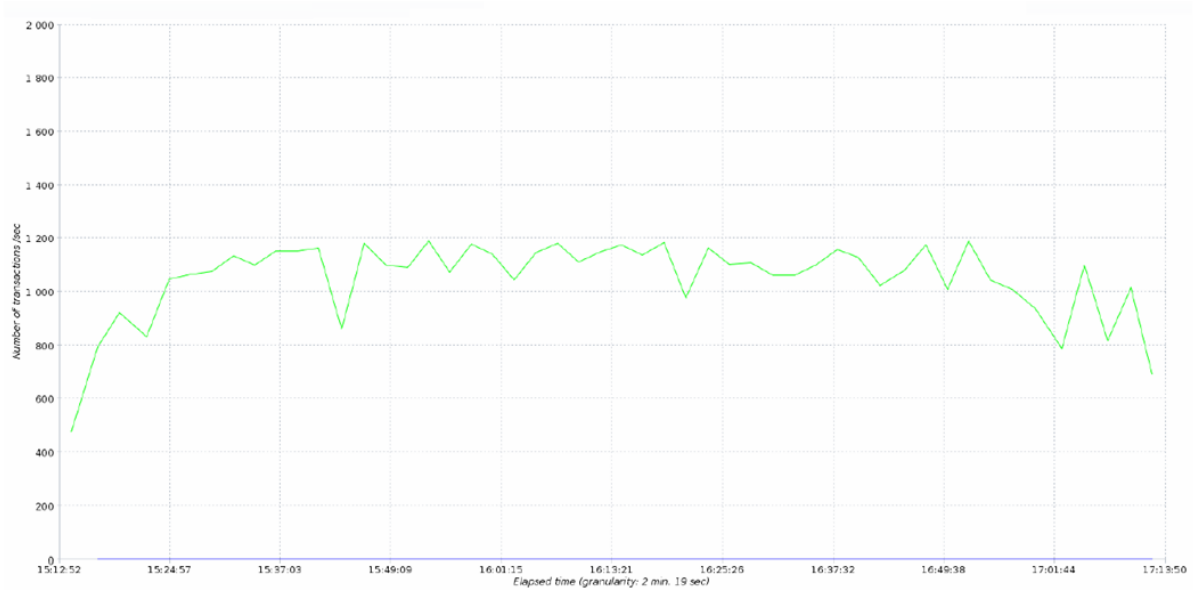
Test description

Run simulated worst-case scenario on mixed workload as seen on production environments against collocated primary/secondary setup for several hours. The **DXL** brokers are in a hub and service zones are enabled.

The workload requests were 30% of file reputation, 30% of certificate reputation, 15% of file metadata, 15% of certificate metadata, 2% of reputation synchronization and the remaining were reporting queries.

The environment has an average delay of 150ms on its **Trellix GTI** queries for new files. Endpoints are also simulated to be collocated with respect to **TIE** secondary servers having low latency access to them. The average latency between endpoints is 1ms with no dropped or corrupted packets.

The test sent sustained 1000 requests per second for 2 hours, with an overall of more than 7.3 million requests in 7,200 seconds, with an average response time of 76 ms and an error rate under 0.1%. 90% of file related requests ask for reputation and metadata of known files. 95% of certificate-related requests ask for the reputation and metadata of known certificates.

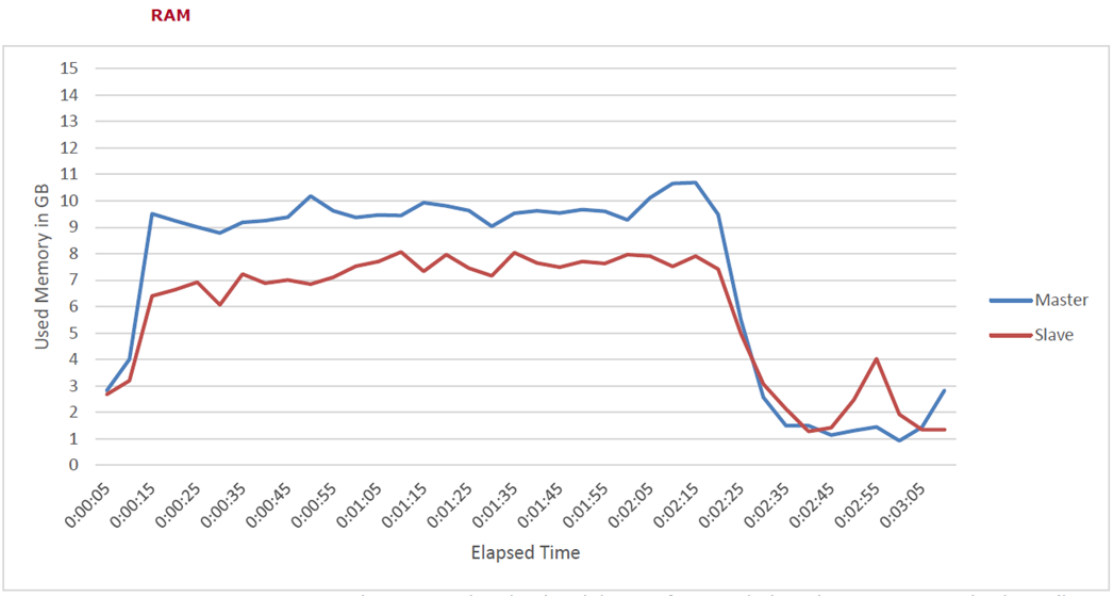


Use the following charts of resource usage for reference on CPU, RAM, Disk, and Network.

CPU

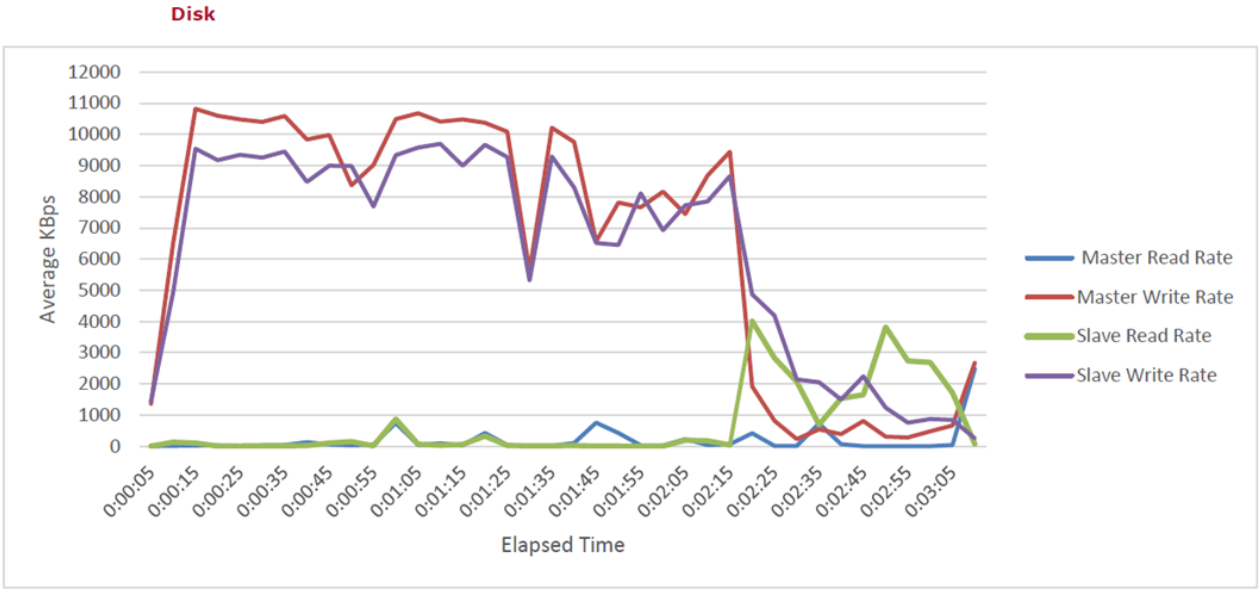
Average CPU usage is sustained at 80% when load stabilizes; after concluding the test, usage is back to idle. We monitored the CPU usage as a percentage of the interval metric provided by VMWare vCenter.

RAM



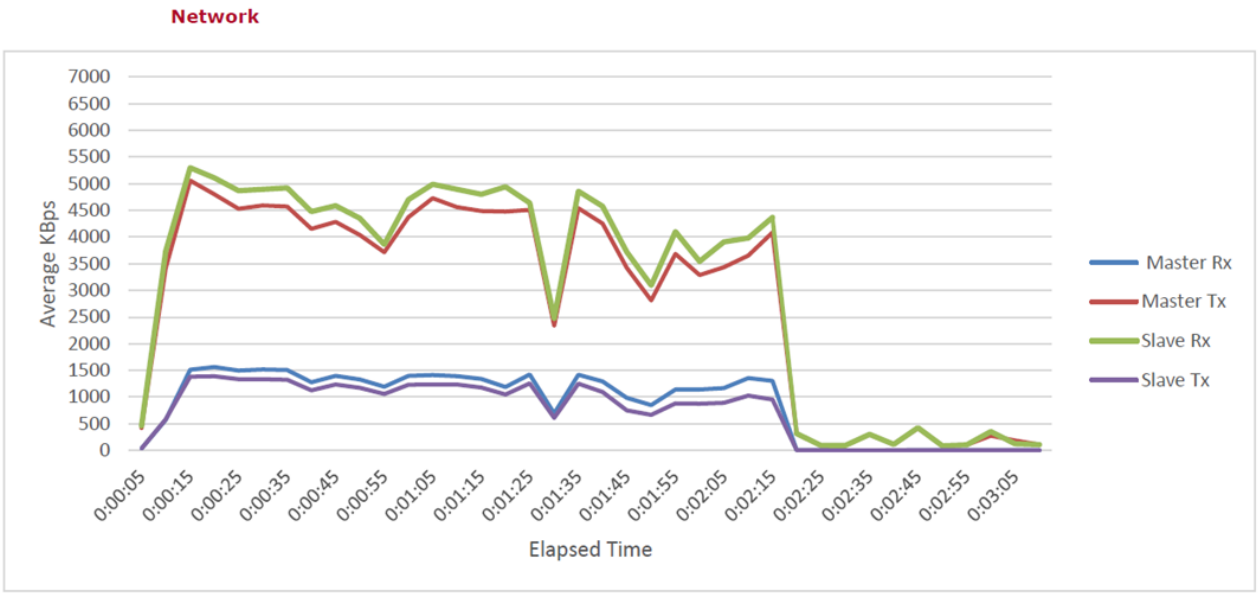
Memory usage is sustained at 10 GB when load stabilizes; after concluding the test usage is back to idle. We monitored the amount of memory that is actively used metric provided by VMWare vCenter.

Disk



Average disk read and write usage is sustained at 10,000 KBps when load stabilizes; after concluding the test disk usage is back to idle. We monitored the Average number of kilobytes written and read to disk each second provided by VMWare vCenter

Network



Primary data received is sustained at 1000 KBps and transmitted at 4500 KBps when load stabilizes. Secondary data received is sustained at 4500 KBps and transmitted at 1000 KBps when load stabilizes. We monitored the average rate at which data was received or transmitted during the interval provided by VMWare vCenter.

Note that database streaming replication is optimized for minimal replication delay so it uses as much bandwidth as available. Each new replicating secondary will increase bandwidth requirements approximately linearly as shown above as replication happens point-to-point between primary and every secondary using direct links.

This test includes combined **DXL** requests and database replication in LAN, plus access to **Trellix GTI** in WAN. Real replication bandwidth depends on latency and dropped packet ratio. If replication happens through a noisy link, synchronization might not find enough usable bandwidth to be updated.

Latency impact and scalability

This section describes the latency impact on throughput when adding new secondary servers to the minimum recommended setup. The objective is to measure the throughput capacity difference as latency is added.

Test description

Run simulated worst-case scenario on mixed workload as seen on production environments against a primary plus a remote secondary setup for several hours.

The test sent sustained requests per second against a remote secondary placed under different latency delays. The resulting throughput on each case shows the impact caused by latency.

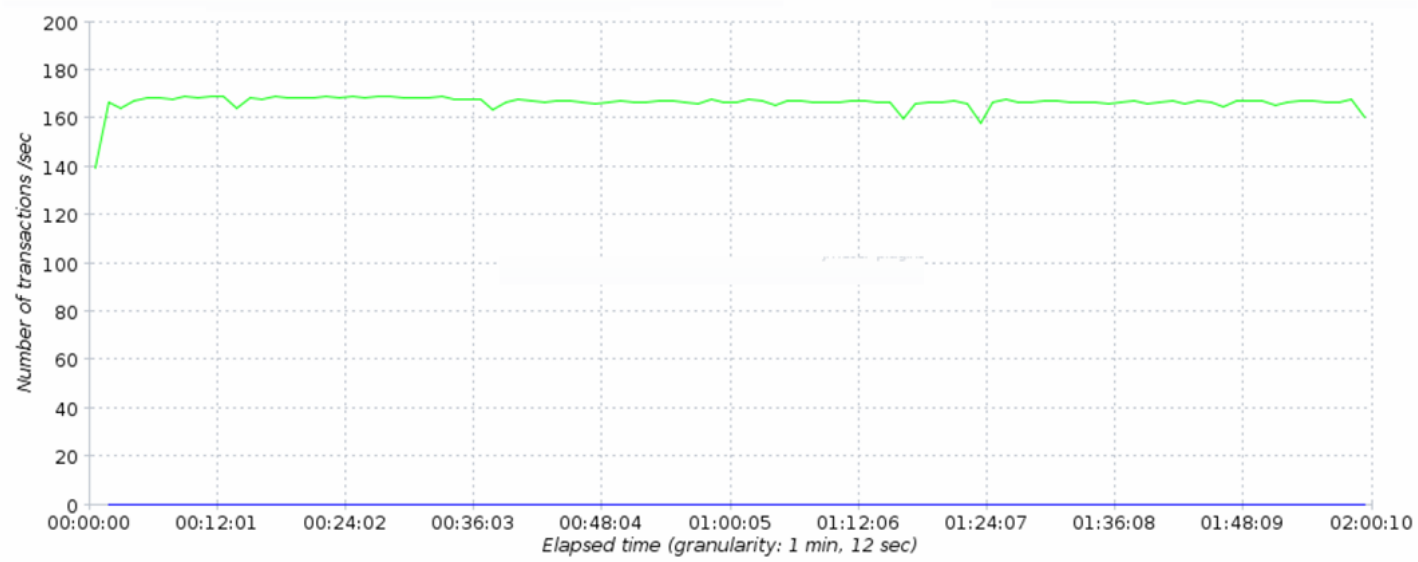
While processing requests, secondary issues update to the primary database that queues up internally until served. Non-trivial latency between primary and secondary might cause the internal queue to fill up which ends up in service disruption in case of sudden spikes of load.

Scenario 1: No latency

A collocated secondary handle sustained a workload of up to 500 requests per second.

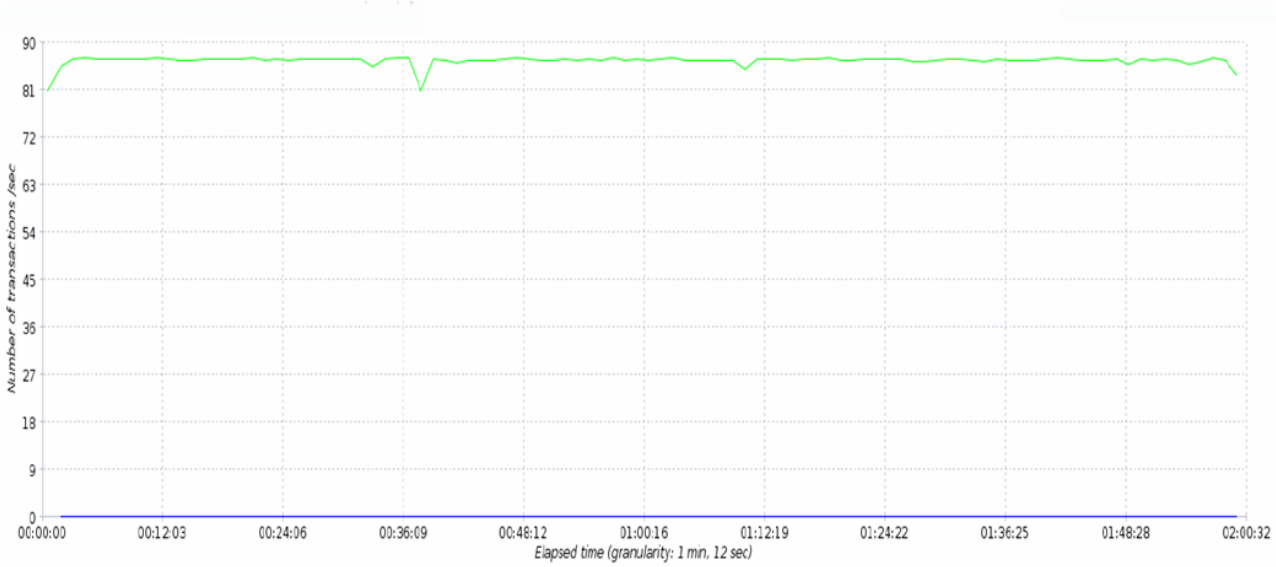
Scenario 2: Remote site

A secondary placed off-site, but still in the same region has a latency of 100 ms ± 10 ms, can handle the sustained workload of about 170 requests per second.



Scenario 3: Remote region

A secondary placed in a remote region having latency of around 200 ms ± 20 ms can handle the sustained workload of about 85 requests per second.



Caching benefits

This section describes caching impact on required bandwidth and throughput when adding **TIE** Reputation Cache servers. The objective is to measure reduced network requirements and increased service throughput when implementing cached reputation stores.

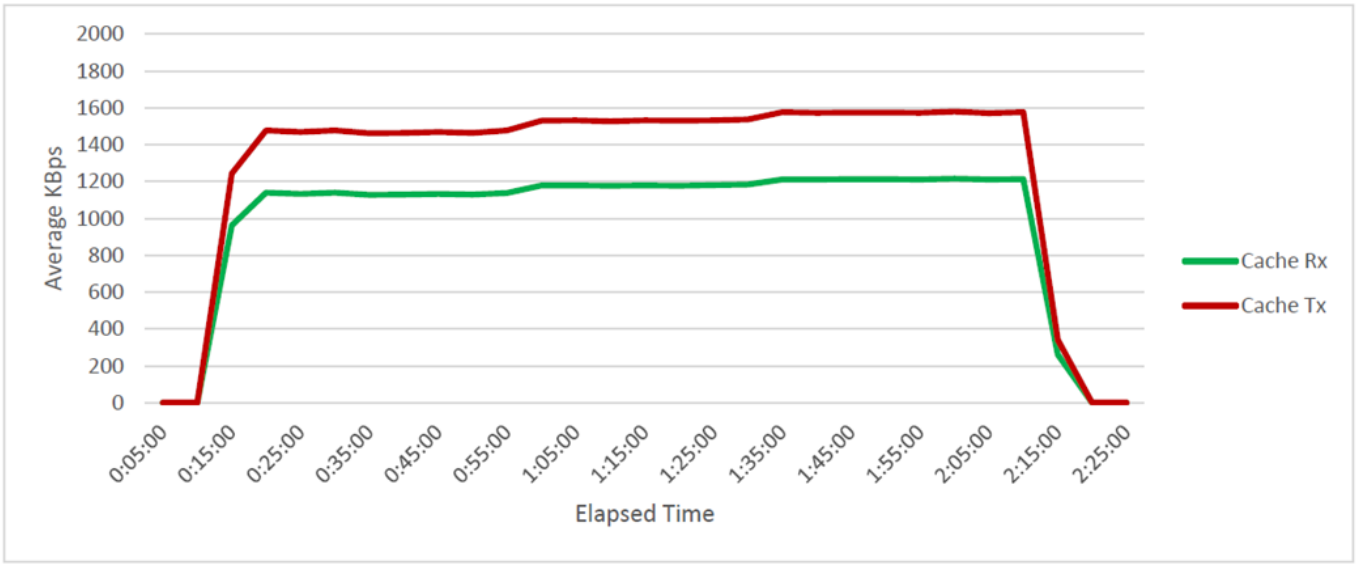
Test description

Run simulated worst-case scenario on mixed workload as seen on production environments against a primary and secondary setup plus a remote **TIE** reputation cache to understand the impact. First, measure the network consumption of forwarding and caching reputation requests instead of replicating the full reputation database. Second, dimension how throughput is increased when pairing a reputation cache with a secondary.

Scenario 1: Remote reputation cache

The same workload used to dimension resource usage and capacity above was executed against a remote reputation cache having a latency of 100 ms ± 10 ms against a collocated pair of primary and secondary.

A **TIE** reputation cache server shows sustained network consumption of close to 1200 KBps in comparison with the close to 4000 KBps required in the first test scenario to cope with full database replication



The cache increases effectiveness when file reuse is significant and there are few unique files.

While processing requests, the **TIE** reputation cache server forwards requests of new files and certificates, and it will cache them for future use.

The in-memory cache is kept updated based on a combination of reputation change broadcasts and an internal time-to-live of each stored item. File prevalence is periodically updated to the primary or secondaries as required.

Scenario 2: Local reputation cache

The same workload used to dimension resource usage and capacity above was executed against a remote secondary and reputation cache having a latency of 100 ms ± 10 ms against a primary instance.

The **TIE** reputation cache server only helps to increase the throughput of reused file and certificate reputation requests. Primary and secondary servers should be deployed to cover spikes on new files.

Multiple **TIE** reputation cache instances can be placed inside different **DXL** Service Zones with a single secondary without significant impact in bandwidth for the reputation of reused files and certificates.

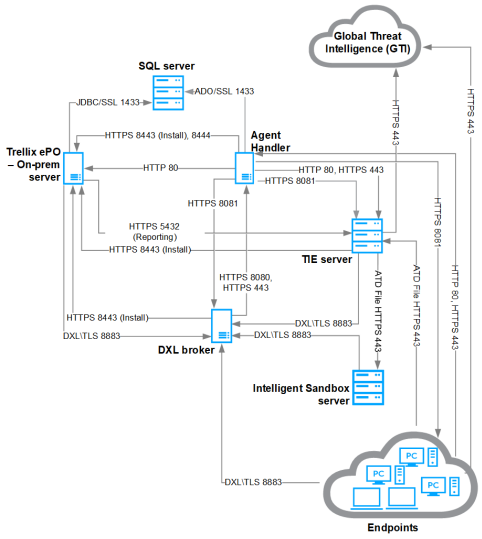
System requirements

Network overview

Threat Intelligence Exchange uses network protocols and ports to allow communication with its environment.

McAfee® Web Gateway server and **Trellix Intelligent Sandbox** communicate with the **TIE** server through **DXL**.

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



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

Default ports used with Threat Intelligence Exchange

Default port	Protocol	Description
22	TCP (SSH)	SSH console to **DXL/TIE** appliances.
53	UDP/TCP	Required for **Trellix GTI** lookups. If DNS server isn't available, or the current DNS doesn't resolve public URLs, it should

Default port	Protocol	Description
		resolve to tie.repl.gti.trellix.com and tieserver.rest.gti.trellix.com
80	TCP	See **Trellix Agent** KB66797.
80	TCP	File upload from the **TIE** client to the **TIE** server for **Intelligent Sandbox** analysis.
123	UDP	Network time synchronization.
443	TCP	Secure file upload from the **TIE** client to the **TIE** server for **Intelligent Sandbox** analysis. Required for **TIE** server 2.3.0 or later.
5432	TCP	**Trellix ePO - On-prem** connectivity applicable to the **TIE** server used for the **Trellix ePO - On-prem** reporting function only. Monitoring and replication traffic sent from secondary **TIE** servers to primary **TIE** servers.
8081	TCP	See **Trellix Agent** KB66797.
8443	TCP	Required only during the **TIE** server installation to configure the **Trellix Agent** (outbound).
8883	TCP	**DXL** messaging.

Important

These are the default ports used with **TIE** server. The list varies if you customize the ports.

For details about the default ports required for each component, see KB66797.

Network requirements

Make sure that:

- The network environment is healthy and can reach Internet directly or through a web proxy.
- DNS is available for both, servers and endpoints.
- There isn't encrypted traffic inspection.
- NTP services are already available with known servers or local ones (if available).
- There isn't Network Address Translation (NAT) among the **TIE** servers or between **Trellix ePO - On-prem** and the registered **TIE** server database.

Environment requirements

The **TIE** server is distributed as an OVA appliance optimized for VMware or as an ISO image used with compatible hardware or other virtualization technologies.
For installing the appliance with an OVA or an ISO image, your Virtual Machine (VM) must meet the following requirements:

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

Important

For upgrades from previous versions of **TIE** server, see the release notes of previous releases.

Products	Components	Version
VMware vSphere		7.0 or later
Threat Intelligence Exchange	**Threat Intelligence Exchange** server	4.0.0 or later
	DXL client	6.0.3 or later
	Endpoint Security Adaptive Threat Protection (ATP)	10.7.x or later
Trellix ePO - On-prem server (on-premises only)		5.10.0 CU 14 or later

Products	Components	Version
Trellix ePO - On-prem product extensions (installed in **Extensions**)	**Endpoint Security**	10.7.x or later
	Trellix Agent extension	5.7.8 or later **Note:** If you upgrade to **TIE** server 4.x.x, the appliance runs a task to upgrade the **Trellix Agent** for MLOS. You don't need to manually upgrade the **Trellix Agent** for MLOS.
	DXL Client Management **DXL** Client for **Trellix ePO - On-prem** **DXL** Broker Management	6.0.3 or later
	TIE server Extension	4.0.0 or later
Trellix ePO - On-prem product packages (checked in to the **Main Repository**)	**Endpoint Security**	10.7.x or later This package can be deployed as part of the **Endpoint Security** deployment.
	Trellix Agent	5.7.8 or later **Note:** If you upgrade to **TIE** server 4.x.x, the appliance runs a task to upgrade the **Trellix Agent** for MLOS. You don't need to manually upgrade the **Trellix Agent** for MLOS.

Client operating systems

Threat Intelligence Exchange server supports all operating systems that **Endpoint Security** supports.

See KB82761 for details about the operating systems supported by **Trellix Endpoint Security (ENS)**.

See KB87945 for Windows Servers 2016 compatibility with **Trellix** products.

First-time installation

You can use the following steps to install the **TIE** software.

- Install the prerequisites
- Install the **TIE** Server Management extension
- Install the **TIE** Server manually
- Install the **TIE** Server using an ISO file

Install the prerequisites

Install Data Exchange Layer

For details about installing the **DXL**, see the product documentation for **DXL**.

Install TIE client module

Install the client module for the managed product **Endpoint Security** 10.7.x or later.

For details about installing the client module, see the product documentation for **Endpoint Security**.

Install the TIE software

Install the **TIE** software using the packages from **Trellix** product download site or use **Software Manager** (**Software Catalog** in **Trellix ePO - On-prem** 5.10) .

Note

You can run the software using an ISO file in XEN, Hyper-V, or bare metal. See KB86324 for details about these virtualization platforms.

You can install the software using the following ways:

- Install the **TIE** software using Software Catalog
- Install the **TIE** software manually

Install the TIE software using Software Catalog

When using **Trellix ePO - On-prem** 5.10 to install **Threat Intelligence Exchange**, you need to install product extensions and installation extensions on the **Trellix ePO - On-prem** server.

Task

1. **Log on Trellix ePO - On-prem as an administrator.**
2. **In Trellix ePO - On-prem, Menu → Software → Software Catalog.**
3. **From the Category list, expand Trellix Threat Intelligence Exchange 4.x.x, then click Extensions.**
4. **SelectTrellix Threat Intelligence Exchange 4.x.x.**

5. **From the Actions column, click check In all.**
6. **Select the checkbox to accept End-User License Agreement.**
7. **Select the branch, then click check In.**

Results

When the check-in is complete, the product **Extensions** are listed on the Extensions page and the installation packages are listed in the **Main repository**.

Install the TIE software manually

You can download the Installation packages from **Trellix** product download site to install **Threat Intelligence Exchange** on your endpoints using a valid grant number.

Task

1. **Log on to the Trellix Product download site using your Grant number and the registered Email address.**
2. **Search for Threat Intelligence Exchange.**
3. **Download the software to your system where you have installed Trellix ePO - On-prem.**
4. **Log on to the Trellix ePO - On-prem server as an administrator.**
5. **Select, Menu → Software → Main Repository.**
6. **Click Check in Package, select Package type, then click Next.**
7. **On the Package Options tab, check the details of your package, then click Save to complete the check-in.**

Results

The **TIE** Server extension is installed on **Trellix ePO - On-prem**.

Install the TIE server manually

Install and configure the **TIE** server, **DXL** brokers on a single appliance.

Before you begin

- Make sure that the server extension is installed correctly and that it matches the version of the server before you deploy the OVA appliance.
- Store your root password in a secure location.
- Make sure that you have the following versions installed or upgraded to:
    - **Trellix ePO - On-prem** to version 5.10.0 CU 14.
    - **Trellix Agent** to version 5.7.8 or later
    - **DXL** to version 6.0.3 or later

See KB83368 for details about supported platforms, environments, and operating systems.

Task

1. **Download the OVA component for the server appliance from Software Manager (or Software Catalog on Trellix ePO - On-prem 5.10) or from the Trellix product download site, then extract.**
2. **Open the VMware vSphere client, then click File → Deploy OVF Template.**

a. **Browse to and select the *.ova file on your computer.**
b. **Click Next and complete the steps in the wizard.**
c. **Turn on the virtual machine and open a Console window.**

3. **Read and accept the license agreement. You can use scroll up and down arrows to see the details.**
4. **Select I Agree and press enter to accept the terms to continue.**
5. **Create a root password for the new server appliance.**
   For the root user, the username is `root` and password is whatever you have set it.

   Note

   Root user has complete access to the server appliance. Choose the secure password accordingly.

6. **Enter the operational account name, real name, and password for the admin user. Select Submit and click enter to continue**
   The account name is typically something like `jsmith` and is used to log on to the server and to the managed services. The real name is your full name, for example, `John Smith`.

   Note

   Admin user has access to the server appliance but not the complete access as root user.

7. **On the Network Selection page, select a network device and continue.**
8. **On the Network Setup page, select the configuration type and continue.**
9. **Enter the host name and domain name of the computer where you are installing the new server appliance. Select OK and click enter to continue.**
   The host name entered here is shown on System tree in **Trellix ePO - On-prem**.
10. **Enter up to three Network Time Protocol servers to synchronize the time of the new server. Use the default servers listed, or enter the address for up to three servers.**
    Verify with your networking team that you can access the URLs from your network, or you can provide internal or external NTP servers. Select **Submit** and click enter to continue.

    Caution

    If the NTP servers are not synchronized, **DXL** and **TIE** handshake isn't completed immediately. The handshake process might take longer and might also fail if time isn't correctly synchronized among **DXL** Brokers, **TIE** servers, and **Trellix ePO - On-prem**.

11. **Enter the IP address or fully qualified domain name, port, and account information for your Trellix ePO - On-prem server and continue. The user account must have administrator rights.**
    Before proceeding, verify the authenticity of the certificate fingerprint of your **Trellix ePO - On-prem**. In a browser, navigate to **Trellix ePO - On-prem** and verify that the fingerprint matches the one shown on the installation screen. If it does, select **Yes** and click enter to continue.

Note

In Windows, Internet Explorer and Chrome show the certificate information about using a built-in SHA-1 thumbprint. Firefox implements its own cross-platform and shows the certificate SHA-256 fingerprint.

12. **You can select the services that you want to run on the new server.**
13. **(Applicable only if the DXL Broker is installed) Configure the DXL Broker port, select Submit and click enter to continue.**
14. **Verify that the installation finishes successfully.**
    All components must be in green to continue. If not, follow the suggestions to troubleshoot the issue.
15. **When the logon screen appears, close it.**
16. **Verify that the new server is provisioned. In Trellix ePO - On-prem, select Menu → System Tree → My organization → Preset → This group and All subgroups to look in the domain where you installed the server appliance.**
17. **Verify that the registered server is provisioned correctly in Trellix ePO - On-prem as a managed system. Select Menu → Configuration → Registered Servers.**
18. **Verify that the operation modes are configured correctly. In Trellix ePO - On-prem, select Menu → Configuration → Server Settings → TIE Server Topology Management.**

Important

The first two installed servers are assigned with an operation mode automatically. If you have more than two servers, the third instance is left unassigned (the operation mode of the third instance depends on your environment settings).

Results

The appliance shows the DXLBROKER and TIESERVER tag, depending on the products installed.

Install the TIE Server using an ISO file

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

Before you begin

- Make sure the server extension is installed correctly and matches the version of the appliance before you use the ISO.
- Store your root password in a secure location.
- Make sure that you have the following versions installed or upgraded to:
    - **Trellix ePO - On-prem** to version 5.10.0 CU 14.
    - **Trellix Agent** to version 5.7.8 or later
    - **DXL** to version 6.0.3 or later

Tip

You can also use an ISO file to create a VM in VMWare. We recommend using the OVA appliance as it preconfigures virtual resources.

See KB83368 for details about supported platforms, environments, operating systems, and Network Interface Card (NIC) vendors.

Note

The **TIE** server does not support multiple Network Interface Cards (NICs).

See KB95084 for details about an issue with Network Interface Card (NIC) detection on a Bare Metal server during the **TIE** server installation.

The **TIE** server runs on its own **McAfee® Linux Operating System (MLOS)** distribution based on CentOS 7 (x86_64). To support different virtualization methods, initial scripts load different kernel modules depending on the virtualization platform detected.

See KB86324 for details about supported virtualization methods for **TIE** server.

The prerequisites and the installation steps apply for XEN, Hyper-V, and bare metal. The installation is automatic and doesn't need interaction with the user.

Task

1. **Create your VM and boot the ISO provided.**
   Wait to complete the process.
2. **Remove the ISO file and turn on the VM.**

Caution

The Intel microcode package must be installed on **TIE** servers that are running on bare metal. See KB90843 for details.

Results

You can continue installing and configuring the **TIE** server.

Upgrade to a new software version

You must meet requirements and follow procedures to benefit from the new features and enhancements of a new software version.

You can use the following steps to upgrade to a new version:

- Consideration before upgrading to the **TIE** Server 4.x.x
- Upgrade paths
- Review the requirements before you upgrade to the **TIE** Server 4.x.x
- Upgrade the **TIE** Server to version 4.x.x
- Verify the upgrade

Considerations before upgrading to TIE server 4.x.x

Upgrading to **TIE** server 4.x.x includes full database replication and high network utilization.

Important

The upgrade process to **TIE** server 4.x.x forces a full database replication from the primary server to every Secondary and Reporting Secondary server of the topology. You can expect high network usage during the Secondary servers upgrade. The database upgrade can take several minutes depending on the database size and bandwidth conditions.

TIE Ecosystem

Considerations for the **TIE** Ecosystem are:

- The endpoint reputation cache is rebuilt when upgrading the components. **Trellix** recommends you to perform incremental upgrades to minimize the impact on the **TIE** server capacity.
- Upgrade the **TIE** client and the **DXL** Client in the endpoints first, then upgrade the **DXL** broker appliance. For more information about upgrading these products, see the release notes for those products.

Trellix Agent for MLOS

Considerations for **Trellix Agent** for MLOS are:

- If you upgrade **TIE** to 4.x.x version, the **Trellix Agent** for MLOS is upgraded after you upgrade the server appliance.
- Do not install the **Trellix Agent** for Linux because it is not compatible.

Note

The task for upgrading the **Trellix Agent** for MLOS runs at 12 a.m. on the same day you upgrade the appliance. If you can't complete the **Trellix Agent** upgrade after that period, you can upgrade it manually. For more information, see the Troubleshooting section.

Upgrade paths

The supported upgrade path is:

- Upgrade from 3.x.x to 4.x.x

We recommend that you run the latest and greatest versions of **Trellix ePO - On-prem**, **Trellix Agent**, and **DXL**. See KB90383 for details about **Trellix ePO - On-prem** minimum supported extension versions. See the product documentation for **DXL** for details about upgrades.

Upgrade paths in a multi-TIE server environment

Given that you have different TIE server instances deployed in your environment, for example, a Primary, a Secondary, and a Reporting Secondary instance, perform a progressive upgrade.

- Make sure the Secondary server database replication is up-to-date.
- Upgrade the **TIE** extension
- Always start with the Primary server, then continue with the other server instances you have.

Review the requirements before you upgrade to TIE 4.x.x

Make sure that your systems meet all requirements.

Follow these procedures to benefit from the new features and enhancements of this version.

Task

1. **Not all manual customization of the appliance configuration is preserved when upgrading. If the TIE server properties or database configuration were modified, create a backup and apply changes after the upgrade.**
2. **Make sure the following URLs are whitelisted in your enterprise firewall for the TIE server to access Trellix GTI (if enabled):**
    - tieserver.rest.gti.trellix.com
    - tie.repl.gti.trellix.com
3. **To minimize network disruption, schedule maintenance downtime for the upgrade and run a vacuum analyze task for database maintenance. For more information see KB86092.**

    Important

    The upgrade process to TIE server 4.x.x forces a full database replication from the Primary Server to every Secondary and Reporting Secondary Server of the topology. Expect high network usage during the Secondary servers upgrade. Database upgrade can take several minutes depending on database size and bandwidth conditions.

4. **Create a snapshot of your virtual machine (Primary instance, if applicable) on the VMware vSphere client. For instructions, see the VMware vSphere documentation. If you are using a non-virtual environment, see KB86092 for instructions to create bare-metal backups.**
5. **Make sure that you have full connectivity in the DXL fabrics. All your brokers must be listed in green.**

Tip

You can verify this in **Trellix ePO - On-prem**, by selecting **Menu** → **Data Exchange Layer Fabric**, then click the **Refresh** button.

6. **Make sure the health check status is OK on the TIE Server Topology Management page.**

Tip

You can verify this in **Trellix ePO - On-prem**, by selecting **Menu** → **Configuration** → **Server Settings** → **TIE Server Topology Management**, then click on each server to verify its status.

Upgrade the TIE Server to version 4.x.x

You can upgrade the **TIE** server from an earlier version to the latest version 4.x.x.

Before you begin

Make sure that you have the following versions installed or upgraded:

- **Trellix ePO - On-prem** to version 5.10.0 CU 14.
- **Trellix Agent** to version 5.7.8 or later.
- **DXL** to version 6.0.3 or later.

Note

TIE doesn't support the **TIE** Server upgrade using Trellix ePO - On-prem. The **TIE** Server in-place upgrade from version 3.0.3 or earlier to 4.0.0 is not supported on the same appliance. In this case, you can only upgrade the **TIE** Server by setting up a new server using an ISO file or OVA component. However, **TIE** 4.0.0 or later supports in-place upgrade to upgrade the **TIE** server on the same appliance.

Task

1. **Upgrade the existing TIE Server Management extension to version 4.x.x.**
2. **Setup a new TIE Server with 4.x.x version.**
    - If your environment is managed using **TIE** 3.0.x as a Primary Server, upgrade it to **TIE** 4.0.x by deploying the new **TIE** 4.0.x Server. Initially, the new **TIE** 4.0.x server will be configured as a Secondary Server.
    - The transition to Secondary mode initiates the database migration to the new **TIE** Server, which might take hours to complete depending on the database size.
    - The data migration completion can be verified by the log statement "**The database sync was successful**" in the **/tmp/reconfig-tie.log** file.
    - The command below will search for the log statement in reconfig-tie.log. Run this command as root on the **TIE** 4.0.x server to check if the database replication was completed.

```
grep -i -B 3 -A 3 "The database sync was successful" /tmp/reconfig-tie.log
```

3. **Make the new TIE Server as a Primary Server.**
    - Once the database migration is completed for **TIE** 4.0.x Server as a Secondary Server, you need to manually promote the **TIE** 4.0.x server as a Primary Server and demote the **TIE** 3.0.x server as a Secondary Server, or it can be decommissioned.
    - The existing **TIE** 3.0.x Server must be maintained as a Secondary **TIE** Server if Active Response Server runs on it.

    Caution

    Never promote a new **TIE** Server to Primary mode, and do not demote the existing Primary **TIE** Server at the same time. Doing so will lead to irreversible data loss.

4. **Manually update the TIE server certificate paths in TIE 3.0.x server after demoting to Secondary Server. See, KB96204.**

    Note

    If you also have MAR version 2.4.4 installed on your TIE 3.x server:
    - Bring up a new **TIE** server on the MLOS3 instance.
    - Switch the **TIE** 4.0 instance to primary.
    - The older version 3.x instance of TIE with MAR should remain as the secondary instance.

Verify the upgrade

Make sure the **TIE** components are configured correctly.

In **Trellix ePO - On-prem**, select **Menu** → **Configuration** → **Server Settings** → **TIE Server Topology Management** and verify that your server instances are configured correctly. You can also view connectivity status on this page.

Post-installation tasks

Configure the VirusTotal key for using the TIE server extension

Configure the TIE server extension for use with VirusTotal, a free virus, malware, and URL online scanning service.

Before you begin

Request your VirusTotal credentials to configure your **TIE** server. Visit www.virustotal.com for more information.

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

Task

1. **In Trellix ePO - On-prem, select Menu → Configuration → Server Settings → Threat Intelligence Exchange Server.**
2. **Click Edit and enter your VirusTotal key.**

Results

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

What to do next

Once the server extension is configured, create, monitor, and adjust **TIE** server policies to determine what is allowed and blocked.

Use the **TIE** server policies to run the **TIE** server in observation mode to build file prevalence (how often a file is seen in your environment) and observe what the **TIE** server detects in your environment. You can monitor and adjust the policies, or individual file or certificate reputations to control what is allowed in your environment.

Configure the TIE server topology

TIE server appliances can run in different operation modes for scaling and fail-over capabilities.

After completing the installation, configure the operation mode of your **TIE** server instances that are managed by your local **Trellix ePO - On-prem**.

Note

In fresh installations, the operation modes of the first two appliances are configured automatically.

Task

1. **On the Server Settings page in Trellix ePO - On-prem, configure the operation modes of the server appliances.**
    - **Primary** — Holds and writes the **TIE** server database and replicates the updates to all Secondary instances.

Caution

We support only one Primary server per **DXL** fabric.

- **Write-Only Primary** — Writes, maintains, and replicates the database. It includes metadata and reputation update requests since it doesn't process endpoint requests.
- **Secondary** — Processes **DXL** requests exactly like a Primary instance using a database that is replicated from the Primary server.
- **Reporting Secondary** — Improves the **Trellix ePO - On-prem** reporting services. It doesn't process reputation requests.
- **Reputation Cache** — An in-memory cache synchronized through **DXL** that minimizes network requirements and provides endpoint operational reputation services. The Reputation cache rebuilds after rebooting because it resides in memory.

In an environment with multiple **Trellix ePO - On-prem** servers, only **TIE** servers managed by a local **Trellix ePO - On-prem** server are editable.
For an environment with a single **Trellix ePO - On-prem** server, managed **TIE** servers are displayed in a tree structure where the root is the instance operating in primary mode.

2. **In Trellix ePO - On-prem, select Menu → Configuration → Server Settings → TIE Server Topology Management, then click Edit.**
3. **For each server instance you want to edit:**
   a. **Select the TIE server instance to edit, then select the Operation Mode from the drop-down list.**
   b. **Click Save.**

Caution

Changing a primary to a secondary operation mode during a disaster recovery might delete its database content. Always promote a secondary to primary operation mode before trying a synchronization from another primary server.

In a single primary instance scenario, you can have only one primary instance in your fabric after the update, regardless of which **Trellix ePO - On-prem** manages the primary instance.

4. **After you save your changes, the background processing applies the changes on each TIE server instance. This process can take several minutes. Wait a few minutes and press F5 or click Refresh in the browser to see your new TIE server topology.**
5. **If your appliance wake-up port is filtered, manually restart the Trellix Agent service. Otherwise, it takes time for the policy to reach the appliance.**
   See KB52707 for details about restarting the **Trellix Agent** service.

Edit the TIE server topology

Change the operation mode of your **TIE** server instances managed by the local **Trellix ePO - On-prem** server.

You can configure the operation mode of the server instances listed and enabled for editing in your local **Trellix ePO - On-prem**. Repeat this process for each server managed by your local **Trellix ePO - On-prem**.

Important

The server instances managed by another **Trellix ePO - On-prem** appear disabled for editing.

Tip

To view the latest reconfiguration status — **tmp/reconfig-tie.log**.

Task

1. **In the TIE Server Topology Management page, select the TIE server instance and click Edit.**
   In a multiple **Trellix ePO - On-prem** environment, only **TIE** servers managed by a local **Trellix ePO - On-prem** are editable.
2. **From the drop-down list, select an operation mode, then click Save to finish.**
   The changes in topology can take several minutes to be applied.
   If you leave a server instance as **Unassigned**, it remains non-operative.

   Important

   Changing a primary to a secondary operation mode during a disaster recovery might delete its database content. Always promote a secondary to primary operation mode before attempting a synchronization from another primary server.

   The new topology of your **TIE** server instances is displayed when the changes are applied.
3. **Click Refresh to verify the changes.**

Configure the TIE server policy

Specify **Trellix GTI** and **Trellix Intelligent Sandbox** settings for the server.

Task

1. **In Trellix ePO - On-prem, select Menu → Policy → Policy Catalog.**
2. **Select Trellix Threat Intelligence Exchange Server Management x.x.x → TIE Server Settings , then select a policy name or an action.**
   You can create a policy using **My Default** as a template, or copy an existing policy and change it as needed.
3. **On the General page, complete these options:**
   - **Proxy Settings for Internet** — If you use a web proxy for Internet access and it requires authentication, enter the proxy information.
   - **Product Improvement Program** — Allow **Trellix** to collect anonymous data about certificates, file paths, and hashes. This data helps **Trellix** learn about threats and prioritize what is allowed or blocked.
4. **On the Trellix Global Threat Intelligence tab, enable Trellix GTI to get file reputation.**
   Trellix GTI is used if the **TIE** server does not have reputation information for a file, or if the server is unavailable.
5. **On the Sandboxing tab, enable Intelligent Sandbox to send file information for further evaluation.**
   In the **Intelligent Sandbox** section, enter the server name and access credentials, available servers, timeout settings, polling settings, and the file types.

You can enable certificate validation in the communication between the **TIE** server and **Intelligent Sandbox**. See KB87692 for details before enabling **Enforce Certificate Validation**.

6. **On the McAfee Web Gateway tab, accept or ignore incoming reports sent to the TIE server about potential web threats.**
7. **On the External Reputation Provider tab, enable an external provider for Adaptive Threat Protection to determine whether to accept the reputations.**
8. **On the Server Configuration tab, configure the logging level of the server, enable collecting information of DXL traffic, enable or disable collecting metrics and modify the sampling period for collecting performance metrics.**
9. **Select Menu → Configuration → Server Settings → Threat Intelligence Exchange Server. The VirusTotal service certificates are validated. If you experience network filtering restrictions, click Edit to disable Skip VirusTotal certificate validations, then click Save.**
   You can configure the type of files that the **TIE** server recognizes and processes when accessing the **TIE** server through **McAfee Web Gateway** and **Intelligent Sandbox**. You can add or remove file types from the list.

Configure Metadata aggregator

Reduce the bandwidth and the number of messages that the **TIE** server needs to process by discarding duplicated data and summarizing information.

Enable Metadata aggregator feature if you have one of these scenarios which implies sending multiple updates to the **TIE** server.

- Frequent changes in your organization
- Add new endpoints to your environment
- Frequently have new files
- New rules
- Constantly restarting your endpoints

Verify registered servers

Verify that the servers are registered correctly to view **TIE** server information in **Trellix ePO - On-prem** reports and dashboards.

Before you begin

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

Task

1. **In Trellix ePO - On-prem, select Menu → Configuration → Registered Servers, then click New Server if you don't have a registered server, or click Edit to manually modify an existing registered server.**
2. **In the Server type drop-down list, select Database Server.**
3. **Enter a name, for example,** TIE Server**, then click Next.**
4. **On the Details page:**
   a. **Select Make this (TIE server) the default database for the selected database type.**
      This option is automatically selected when you create the first registered server. If you have more than one **TIE** database, select this option only for the database that you want as the default.
   b. **In the Database Vendor field, select TieServerPostgres.**

c. **In the Host name or IP address field, enter the IP address of the system where you installed the server.**
d. **In the SSL host name validation field, select Enforce Certificate Validation from the drop-down list.**
e. **Leave the Database server instance and Database server port fields blank (if they appear).**
f. **For the Database name, enter tie.**
Both database and user names are case sensitive. Make sure you type the names using lower case for both, database and user name.
g. **In the User name field, verify that the PostgreSQL user name is readonly.**

5. **Click Test Connection.**

Results

Trellix ePO - On-prem communicates with the server and retrieves data for the reports and dashboards.

What to do next

Register the servers again if you change the hostname or IP address of the appliance.

Verify the installation

Make sure that **TIE** and **Data Exchange Layer** components were installed successfully.

For troubleshooting any of these steps, see the section **Troubleshooting**.

Task

1. **In the System Tree, click the TIE server name, then click the Products tab. Verify that the following components are listed with the corresponding version for the installation process:**
    - **Trellix DXL Broker** (if configured when deploying the appliance)
    - **Trellix DXL Client**
    - **Trellix Threat Intelligence Exchange Server**
2. **In the System Tree, on the Tags column, verify that the tags are applied correctly to the deployed systems.**
3. **Verify that the DXL Topology settings and the DXL Fabric are configured correctly.**
    a. **In the System Tree, select the TIE server, then from the Actions menu, select DXL → Lookup in DXL.**
    Verify that the connection state is **Connected**.
    b. **Verify that the DXL broker is running. Select Menu → Systems → TIE Reputations to verify that you can search for files and certificates. It might take some time for reputation information to populate the database.**
4. **Select Menu → Configuration → Server Settings, then click DXL Client for ePO.**
Verify that the **Connection State** is **Connected**.
5. **Select Menu → Configuration → Server Settings → TIE Server Topology Management and verify that the operation mode of your TIE server instances have changed based on your edit.**
6. **Select Menu → Configuration → Server Settings, then click on each server and verify that is running.**
Make sure the health check status is **OK** on the **TIE Server Topology Management** page.

Troubleshooting the installation

Troubleshooting installed components

Verify the health status of the installed components to troubleshoot installation issues.

Verify health checkups

For verifying the health check status of the server instances managed locally by **Trellix ePO - On-prem** server on the **TIE Server Topology Management** page, select each server instance you deployed. The health status event is set as **OK**, **Warn**, and **Error**.

TIE server connection checkups

Checkup	Definition and status
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. The health check status are: • OK — The server instance you selected is connected to **Trellix ePO - On-prem** through DXL. • Warn — The connection between the server instance and **Trellix ePO - On-prem** is degraded. • Error — The server instance and **Trellix ePO - On-prem** are not connected.
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.

Checkup	Definition and status
	• 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.
Intelligent Sandbox 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.

Troubleshooting topology and configuration of the components

If you experience problems accessing the installed components, verify their topology and configuration.

Troubleshooting options

Problem	Troubleshooting
The components don't appear on the **Products** tab.	Wake up the agent on the **TIE** server. • In **Trellix ePO - On-prem**, select **Menu** → **System Tree**, then select the checkbox for the **TIE** server. • Click **Wake Up Agents**. • On the **Wake Up Trellix Agent** page, select **Force complete policy and task update**, then click **OK**. This option sends the server properties from the **TIE** server appliance to **Trellix ePO - On-prem**. • Select **Menu** → **Automation** → **Server Task Log** to verify that the task completed. • In the **System Tree**, click the server name, click the **Products** tab, then verify that these components are listed: **Trellix DXL Broker**, **Trellix DXL Client**, and **Trellix Threat Intelligence Exchange Server** .
The tags aren't applied correctly on the deployed components.	Run the server task to check what tag is missing and apply the tag again. • Select **Menu** → **Automation** → **Server Tasks**, then run **Apply TIESERVER tags to TIE Server**. • Select **Menu** → **Automation** → **Server Task Log** to verify that the task is complete. • In the **System Tree**, verify that the **TIESERVER** tag was applied to the system.
The **DXL** topology settings and the **DXL** fabric configuration aren´t correct. The **DXL** broker isn't running because it is disconnected.	Check the connection status of the **DXL** broker. • In the **System Tree**, select the **TIE** server, then from the **Actions** menu, select **DXL** → **Lookup in DXL**. Verify that the connection state is **Connected**. • Verify that the **DXL** broker is running. Select **Menu** → **Systems** → **TIE Reputations** to verify that you can search for files and certificates. It might take some time for reputation information to populate the database

Problem	Troubleshooting
The topology of your **TIE** server instances isn't correct or doesn't show the configuration you set.	Select **Menu** → **Configuration** → **Server Settings** → **TIE Server Topology Management**. Click **Edit**. Modify the operation mode, then click **Save**. Verify that the operation mode of your **TIE** server instances have changed based on your edit.

DXL and **TIE** services aren't running.	Open a console window, log on, and type these commands in order:
	`systemctl status cma`
	`systemctl status dxlbroker`
	`systemctl status tieserver-policy-listener`
	`systemctl status tieserver`

Access the log files

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

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

Endpoint Security Threat Intelligence module — \ProgramData\McAfee\EndpointSecurity\Logs\ThreatIntelligence_Activity.log

TIE server

- **/var/Trellix/tieserver/logs/tieserver.log**
- **/var/Trellix/tieserver/logs/tieserver-start.log**
- **/var/Trellix/tieserver/logs/tieserver-lib.log**
- **/tmp/reconfig-tie.log** (for operation mode transitions)

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

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

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

Trellix Agent — /var/log/MFEcma-[MA_VERSION]-[MA_BUILD].log

See KB82850 for details about using the Minimum Escalation Requirements (MER) tool to collect product data from the server and contact Technical Support. This tool runs in the server appliance.

See KB59385 for details about using the MER tool with other **Trellix** products.

Reconfigure the installation using scripts

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

Accessing the scripts

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

Script name	Description	Reboot?
change-hostname	Changes the host name of the current appliance. It restarts the **Trellix Agent** and the broker.	Recommended
change-services	Enables or disables the **DXL** broker and the **TIE** server services. If the broker was initially disabled during first boot, the script prompts for broker configuration information.	No
reconfig-dxl	Reconfigures the **DXL** port.	No
reconfig-ma	Reconfigures the **Trellix Agent**. The agent, the **DXL** broker, and the **TIE** server services are restarted. New keystores are generated when the service starts.	Recommended
reconfig-network	Reconfigures the current network interface (from DHCP to manual, or from manual to DHCP).	Recommended
reconfig-ntp	Reconfigures the Network Time Protocol servers.	No
reconfig-ca	Obtains an updated Certificate Authorities chain from **Trellix**	No

Script name	Description	Reboot?
	ePO - On-prem and stores it in the **TIE** server.	
reconfig-cert	Generates a new certificate and sends a signing request to **Trellix ePO - On-prem** through the **TIE** server extension.	No

Manually upgrade Trellix Agent

Use the rpm package distributed with the **TIE** package to upgrade manually the **Trellix Agent**, only if the automatic upgrade failed.

Task

1. **Log on as root.**
2. **Run the command rpm -qa MFEcma**
   Verify that the version of the installed **Trellix Agent** matches the version of the Agent distributed with the **TIE** package.
3. **If the versions don't match, run the command less /var/log/MFEcma- [MA_VERSION]-[MA_BUILD].log to check the Trellix Agent upgrade log for errors.**
4. **Run the command rpm -Uvh /apps/MFEma- [MA_VERSION]-[MA_BUILD].mlos2.x86_64.rpm to upgrade the Trellix Agent manually.**

COPYRIGHT

Trellix