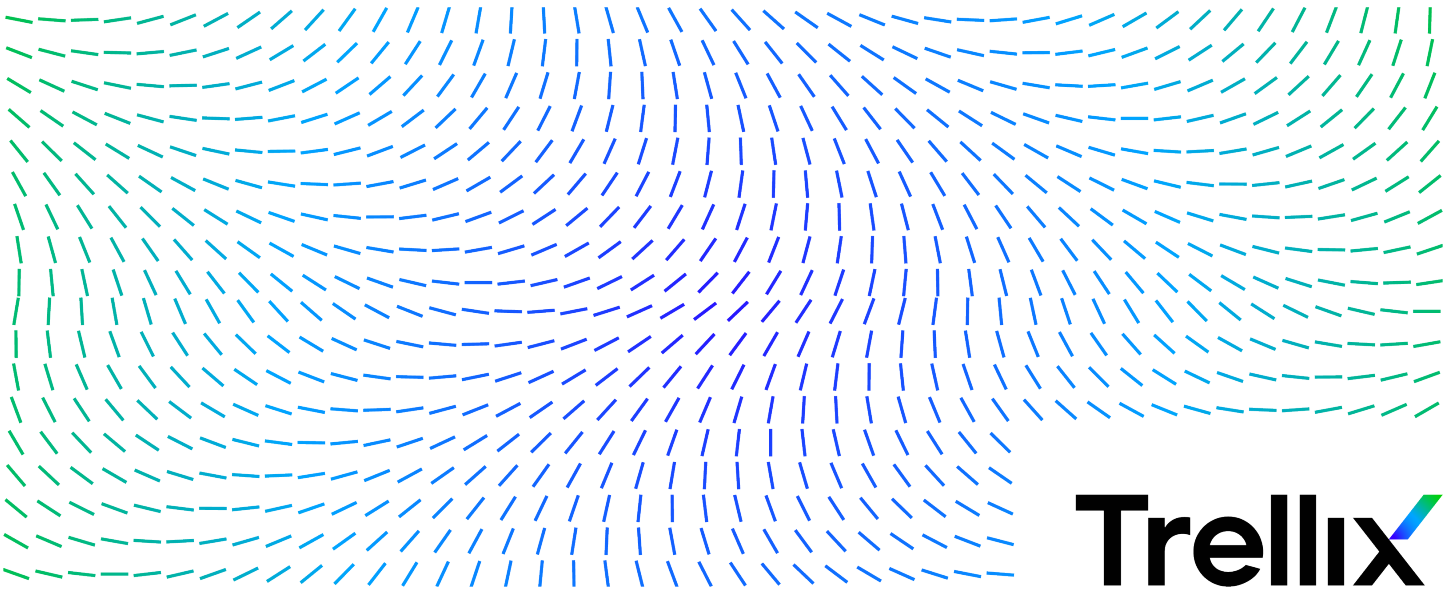
McAfee Threat Intelligence Exchange 3.0.x Installation Guide



Trellix

Contents

Installation overview

Benefit from installing the components for McAfee® Threat Intelligence Exchange (TIE) manually after McAfee® Endpoint Security installation is complete to manage Threat Intelligence Exchange features from McAfee® VirusScan® Enterprise.

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 McAfee® ePolicy Orchestrator® (McAfee® ePO™) 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 McAfee Endpoint Security, a server for file and certificate reputation storage, and McAfee® Data Exchange Layer (DXL) brokers for bidirectional communication between managed systems on a network.

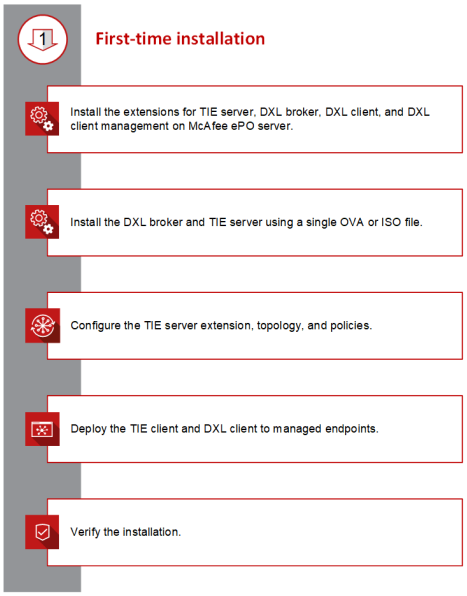
Which type of installation do you need?

Note

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

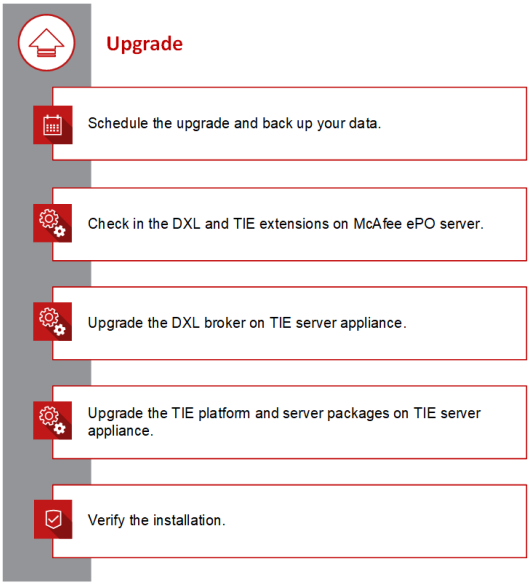
First-time installation workflow

As a McAfee ePO administrator, you can install the TIE Server appliance using an OVA or an ISO file on a Virtual Machine (VM) after you deploy the McAfee 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 McAfee ePO 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.

See TIE sizing and deployment guide for details.

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. McAfee 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 McAfee 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 McAfee ePO 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 McAfee products at their recommended configuration were tested.

- McAfee Agent 5.0.3
- McAfee ePolicy Orchestrator 5.3.2
- McAfee 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 McAfee 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.

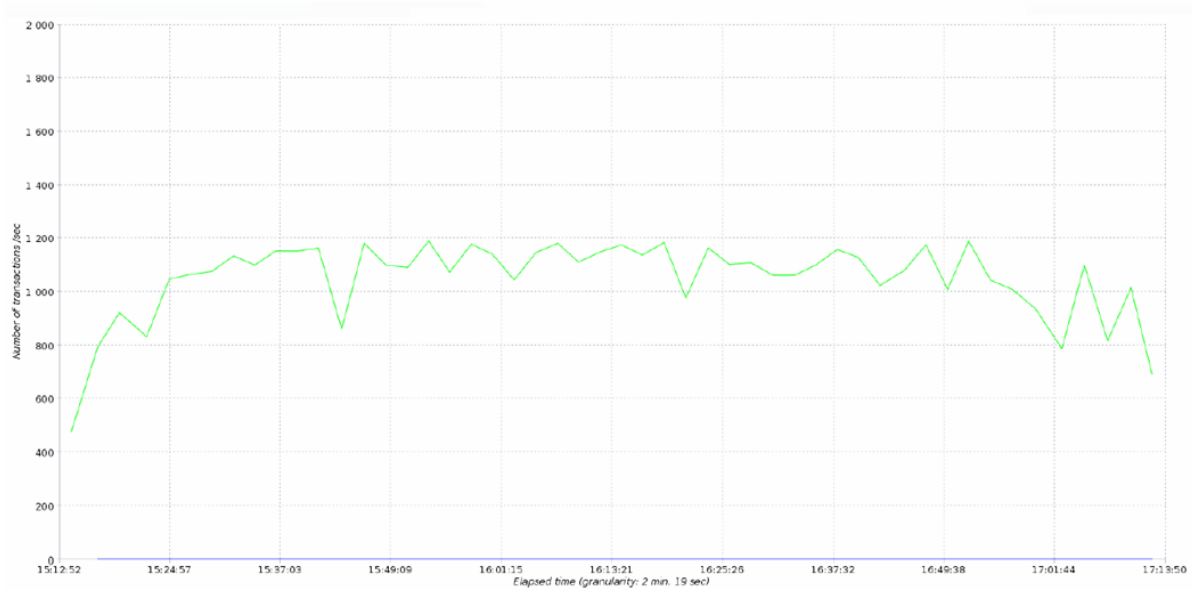
Test description

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 McAfee 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.

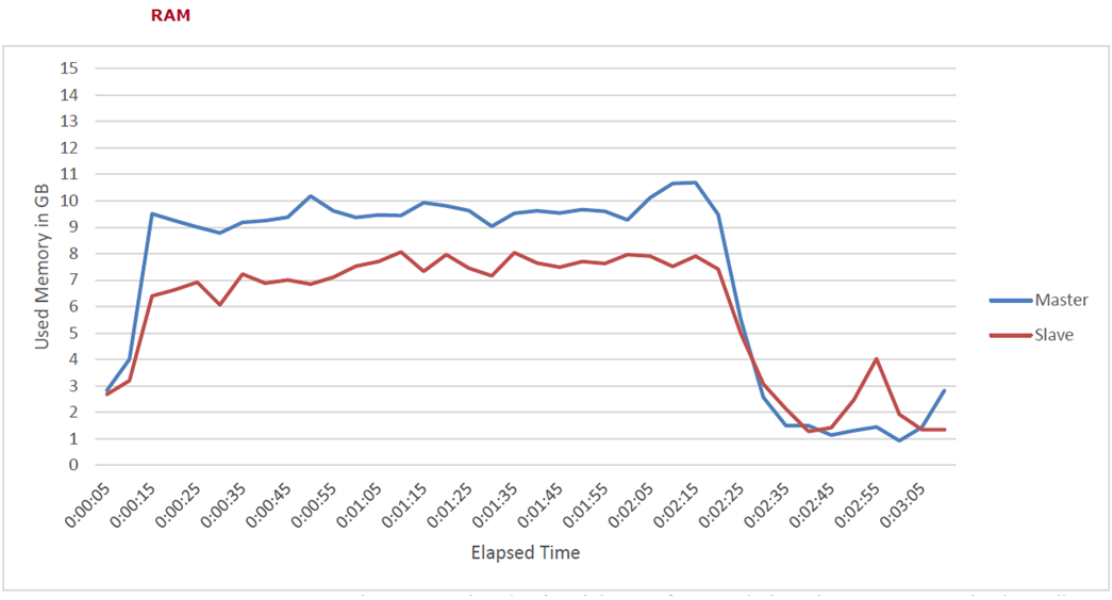


Use the following charts of resource usage for reference on CPU, RAM, Disk, and Network.

CPU

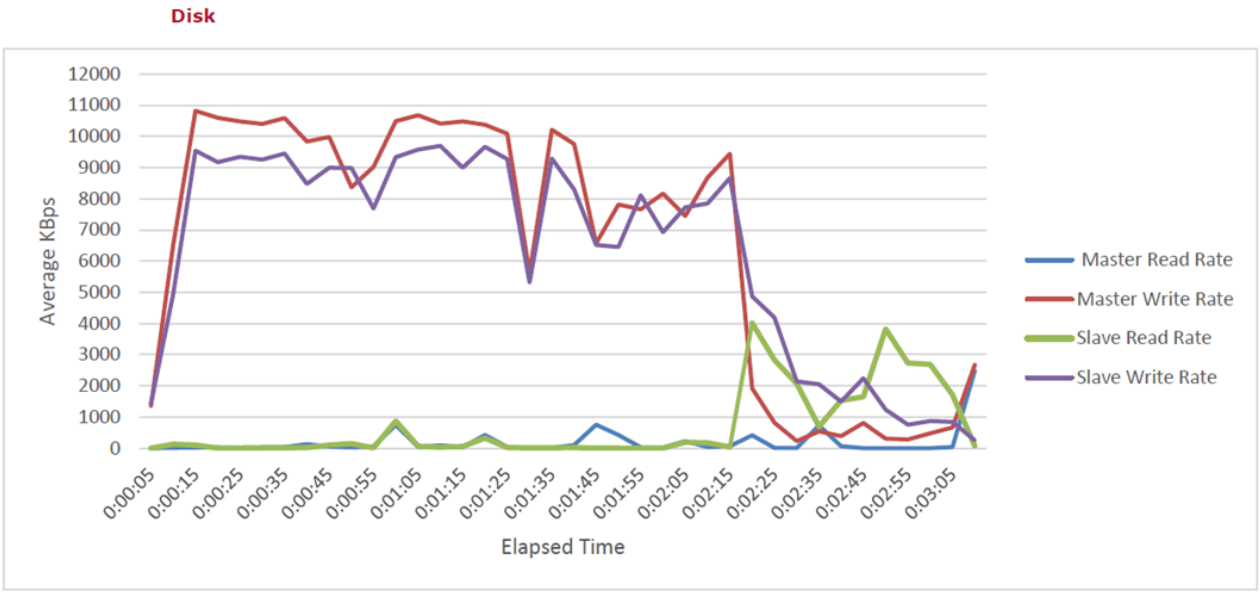
Average CPU usage is sustained at 80% when load stabilizes; after concluding the test, usage is back to idle. We monitored the CPU usage as a percentage of the interval metric provided by VMWare vCenter.

RAM



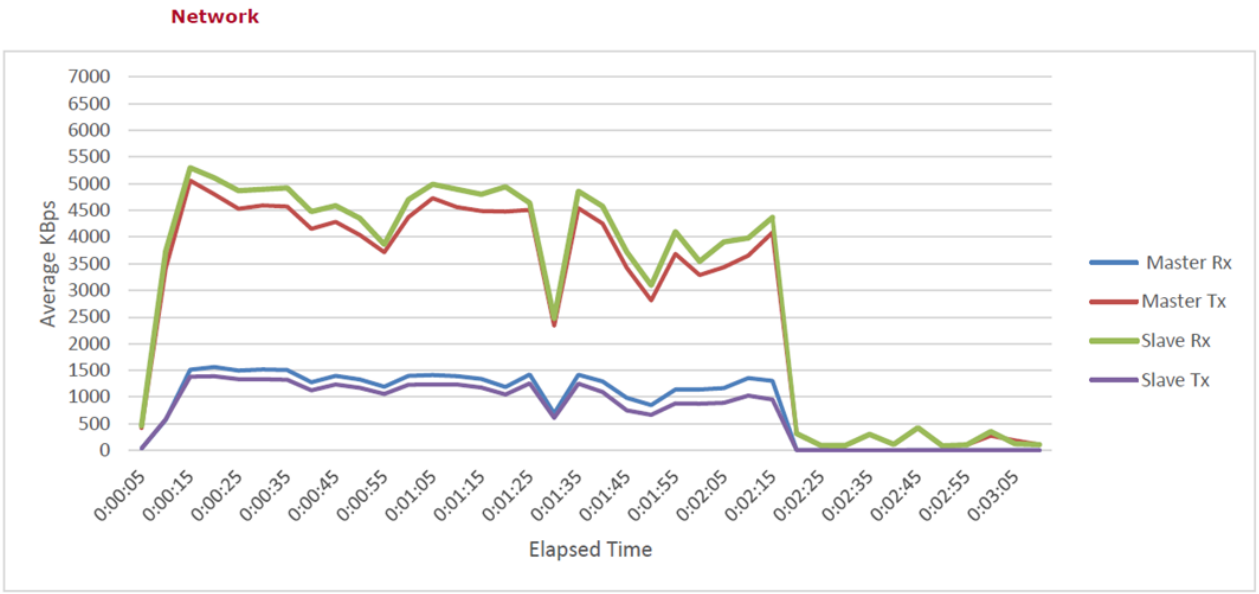
Memory usage is sustained at 10 GB when load stabilizes; after concluding the test usage is back to idle. We monitored the amount of memory that is actively used metric provided by VMWare vCenter.

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 McAfee 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.

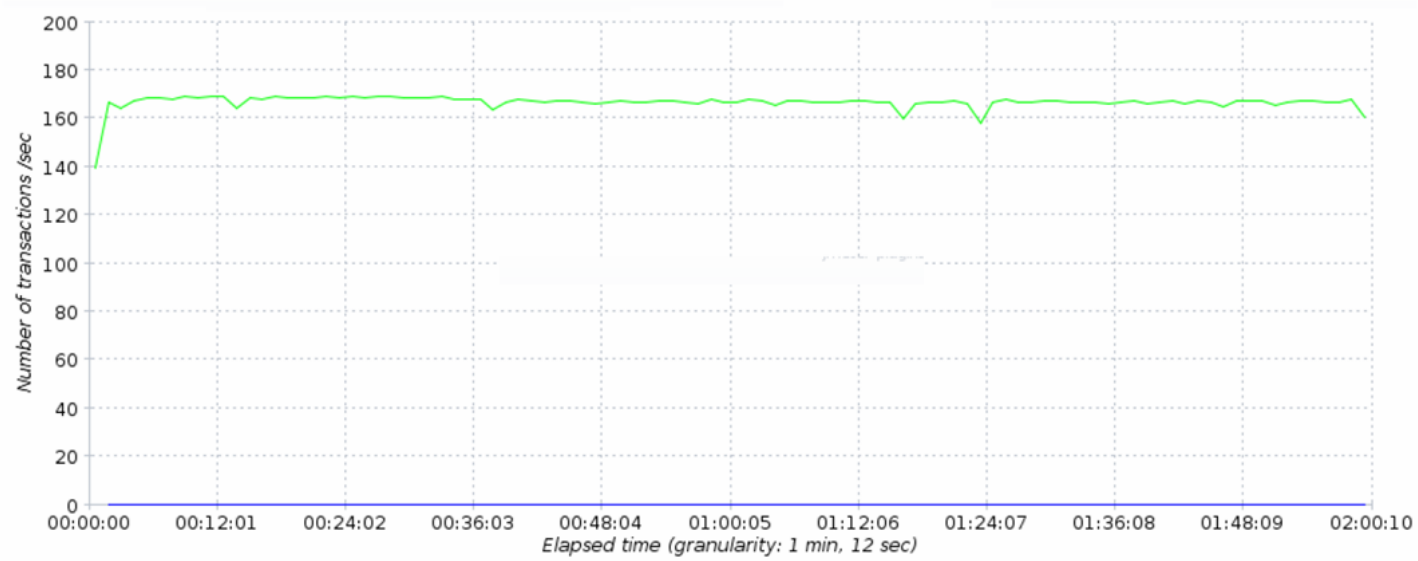
While processing requests, secondary issues update to the primary database that queues up internally until served. Non-trivial latency between primary and secondary might cause the internal queue to fill up which ends up in service disruption in case of sudden spikes of load.

Scenario 1: No latency

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

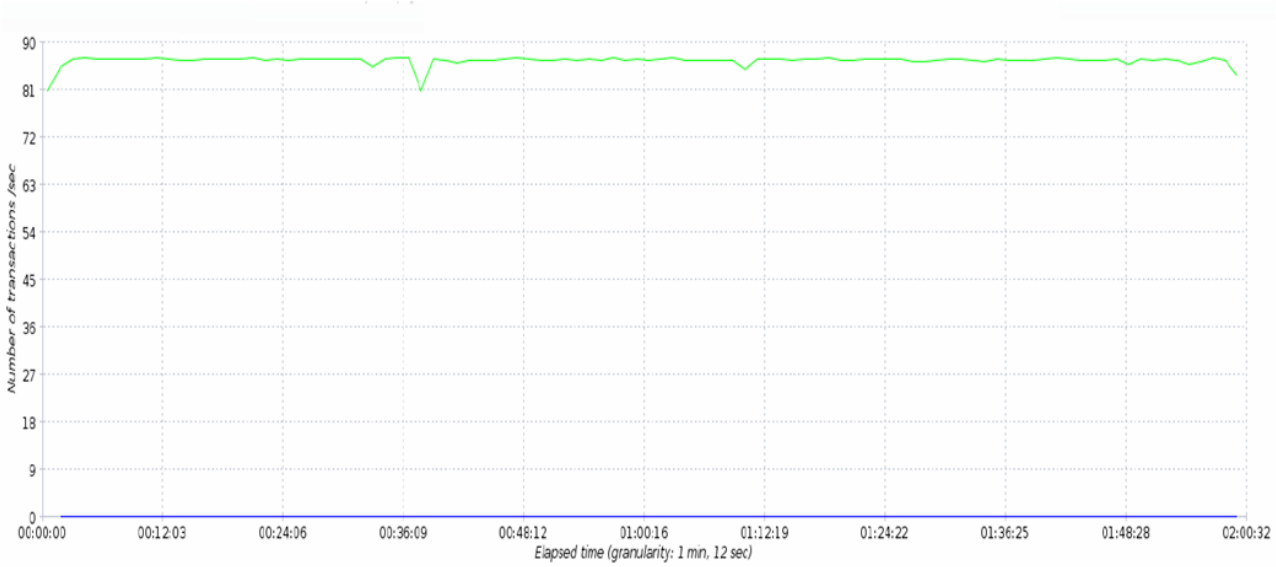
Scenario 2: Remote site

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.

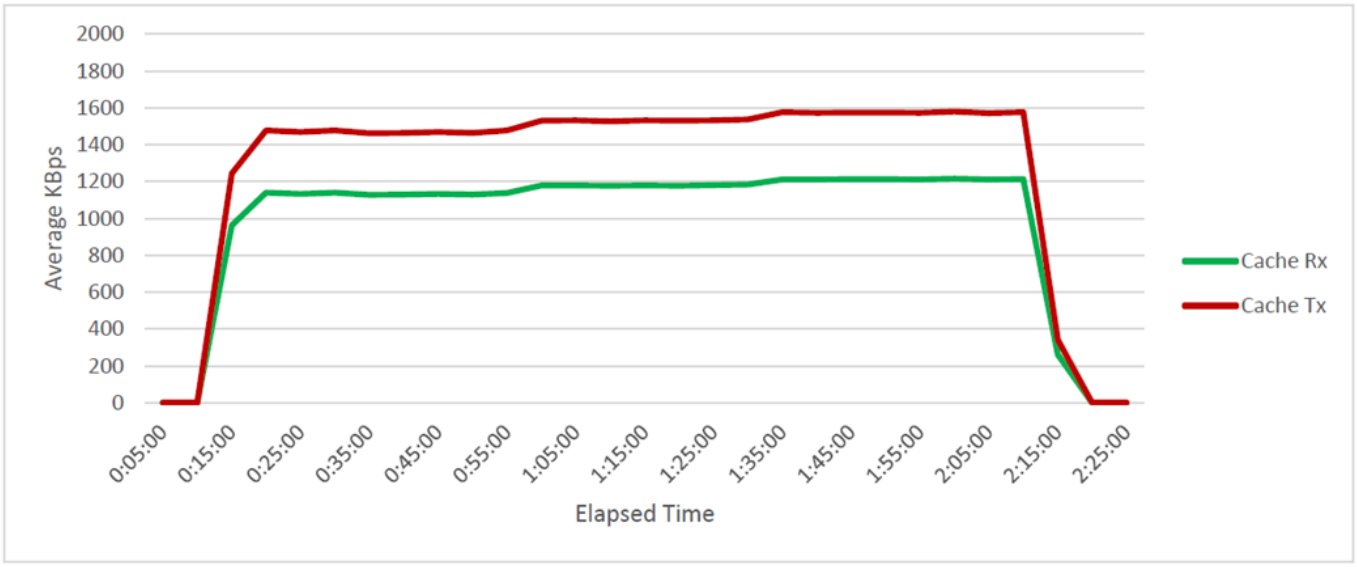
Test description

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.

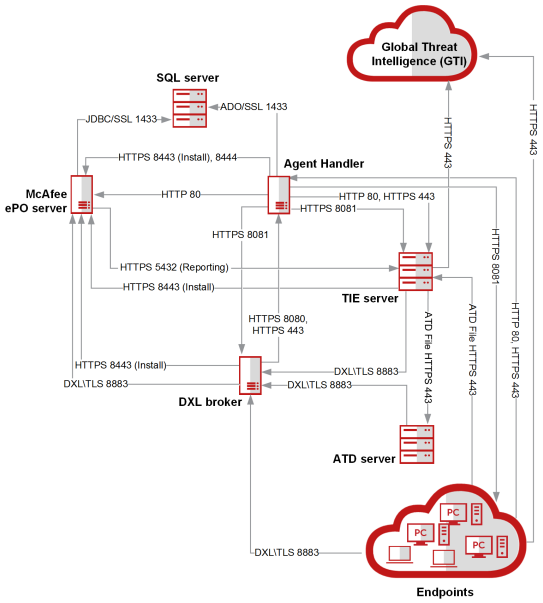
System requirements

Network overview

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

McAfee® Web Gateway server and McAfee® Advanced Threat Defense 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 McAfee GTI lookups. If DNS server isn't available, or the current DNS doesn't resolve public URLs, it should resolve to tie.gti.mcafee.com and tieserver.rest.gti.mcafee.com

Default port	Protocol	Description
80	TCP	See McAfee® Agent KB66797.
80	TCP	File upload from the TIE client to the TIE server for Advanced Threat Defense analysis.
123	UDP	Network time synchronization.
443	TCP	Secure file upload from the TIE client to the TIE server for Advanced Threat Defense analysis. Required for TIE server 1.3.0 and later.
5432	TCP	McAfee ePO connectivity applicable to the TIE server used for the McAfee ePO reporting function only. Monitoring and replication traffic sent from secondary TIE servers to primary TIE servers.
8081	TCP	See McAfee Agent KB66797.
8443	TCP	Required only during the TIE server installation to configure the McAfee 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 McAfee ePO 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		6.0 or later
Threat Intelligence Exchange	Threat Intelligence Exchange server	2.x or later for upgrades **Important:** TIE server 1.2.1 reached its EOL on December 31, 2017, and 1.3.0 did on August 15, 2018. See KB89670 for details.
	DXL client	4.x or later **Important:** 1.x reached its EOL on February 15, 2018, and 2.x and 3.0 did on October 16, 2018.
	McAfee® Endpoint Security Adaptive Threat Protection (ATP) 10.5, or TIE client module for VirusScan Enterprise	• For VirusScan Enterprise — 8.8 Patch 5 or later • For Endpoint Security — 10.5 or later

Products	Components	Version
McAfee ePO server (on-premises only)		5.3.x, 5.9.x, and 5.10 **Note:** See KB88491 for compatibility considerations with McAfee ePO 5.9. **Important:** McAfee ePO 5.1 reached its EOL on December 31, 2017, and McAfee ePO 5.3 did on September 30, 2018. See KB88252 for details.
McAfee ePO product extensions (installed in **Extensions**)	VirusScan Enterprise or Endpoint Security	8.8 Patch 5 10.5 or later
	McAfee Agent extension	5.5 or later (for TIE versions earlier than 3.0.0) **Note:** If you upgrade to TIE server 3.0, the appliance runs a task to upgrade the McAfee Agent for MLOS. You don't need to manually upgrade the McAfee Agent for MLOS.
	DXL Client Management DXL Client for McAfee ePO DXL Broker Management	4.x or later 4.x or later 4.x or later
	TIE server Extension	2.x or later for upgrades
McAfee ePO product packages (checked in to the **Master Repository**)	VirusScan Enterprise or	8.8 Patch 5 10.5 or later

Products	Components	Version
	Endpoint Security	This package can be deployed as part of the Endpoint Security deployment.
	McAfee Agent	5.5 or later (for TIE versions earlier than 3.0.0) **Note:** If you upgrade to TIE server 3.0, the appliance runs a task to upgrade the McAfee Agent for MLOS. You don't need to manually upgrade the McAfee 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 McAfee Endpoint Security.

See KB87945 for Windows Servers 2016 compatibility with McAfee products.

First-time installation

Installation 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, either VirusScan Enterprise (legacy) or Endpoint Security 10.5 or later.

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

Download the software

Download the software from McAfee product download site or use **Software Manager** (**Software Catalog** in McAfee ePO 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.

Download the TIE software from McAfee ePO

When using McAfee ePO 5.10 to install Threat Intelligence Exchange, you need to install product extensions and installation extensions on the McAfee ePO server.

Task

1. Log on McAfee ePO as an administrator.
2. In McAfee ePO, **Menu** → **Software** → **Software Catalog**.
3. From the **Category** list, expand **McAfee Threat Intelligence Exchange 3.0**, then click **Extensions**.
4. Select **McAfee Threat Intelligence Exchange 3.0**.
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 **Master repository**.

Download the TIE software from McAfee product download site

Download the Installation packages from McAfee product download site to install Threat Intelligence Exchange on your endpoints using a valid grant number.

Task

1. Log on to the McAfee 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 McAfee ePO.
4. Log on to the McAfee ePO server as an administrator.
5. Select, **Menu** → **Software** → **Master 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 Installation packages are ready to deploy to your endpoints.

Deploy the TIE server automatically through McAfee ePO

Deploy the TIE server automatically using a single appliance.

Important

This unattended deployment is for VMW 6.0 (or later) infrastructure only.

Task

1. Log on to McAfee ePO as an administrator.
2. Select **Menu** → **Automation** → **Server Deployment**.
3. On the **Server Deployment** page, configure these settings.
4. In **VMware vCenter Access**:
   a. Type the **URL**, **User Name**, and **Password**.
   b. Click **Validate Certificate** and follow the instructions to verify whether the fingerprint matches the one on the vSphere web client. This checkbox is displayed if the access URL starts with HTTPS.
   If the access URL uses HTTP, the **Allow insecure connection (http)** checkbox is displayed. We don't recommend using an http connection because it is not secure.
5. In **VMware vCenter infrastructure**:
   a. Type the **VMware vCenter infrastructure** details such as the name of the **Data center**, **Host/Cluster**, **Datastore**, **Network**, **Folder**, and **Virtual Machine Name**.

Keep any default values or change them as needed.

Note

Make sure that the names are unique and that the folder exists.

6. In McAfee ePO:
   a. Type the **User Name** and **Password**.
      The **Hostname**, **Port**, and **Wake up port** fields are automatically populated.
   b. Click **Validate Certificate** and follow the instructions to verify whether the fingerprint matches the one on McAfee ePO
7. In **New Server Credentials** :
   a. Create a **Root Password**, **User Name**, and **Password** for the new server where you want to deploy the services.
8. In **New Server Network**:
   a. Enter a new **Hostname** and the **Domain** of the server network through which the services are deployed.
      The mode is set as DHCP by default. The **NTP** and **DXL port** fields are also populated. The **DXL port** field appears when the DXL service option is selected.
   b. Select the checkbox next to the respective services that you want to deploy to the server.
      TIE and DXL checkboxes are selected by default. To deploy the McAfee® Active Response services, select the **MAR** checkbox. Both McAfee Active Response and TIE services are deployed to the server. As a result, the **TIE** option is disabled.
   c. Accept the license agreement and click **Deploy**.
9. For TIE health status checkups, select **Menu → Configuration → Server Settings → TIE Server Topology Management**.
10. Verify that the TIESERVER name is provisioned. In McAfee ePO, select **Menu → System Tree → My organization → Preset → This group and All subgroups**.
11. Verify that the registered server is provisioned correctly in McAfee ePO as a managed system. Select **Menu → Configuration → Registered Servers Configuration**.

Results

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

Install the TIE server manually

Install and configure the TIE server, DXL brokers, and the Active Response server 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.

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 McAfee ePO 5.10) or from the McAfee 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. Press **C** to view each page or **E** (End) to view the last page.
4. Press **Y** to accept the terms to continue.
5. Create a root password for the new server appliance.
6. Enter the operational account name, real name, and password, using the **Tab** key to move to the next field. When finished, press **Y** to continue.
   The account name is typically something like `jsmith` and is used to log on to the server and to the managed services. The real name is your full name, for example, `John Smith`.
7. On the **Network Selection** page, press **N** to continue.
8. Select a configuration type, then press **Y** to continue.
9. Enter the host name and domain name of the computer where you are installing the new server appliance. Press **Y** to continue.
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.

    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 McAfee ePO.

    Press **Y** to continue.

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

    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.

    The Active Response server is optional.

    Deploy the Active Response server through McAfee ePO if you upgrade from TIE 2.2.0 or earlier versions.

    See the documentation for McAfee® Active Response for more information about deploying the Active Response server.

    Press **Y** to continue.

13. Configure the DXL Broker port, then press **Y** 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 McAfee ePO, 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 McAfee ePO as a managed system. Select **Menu → Configuration → Registered Servers**.
18. Verify that the operation modes are configured correctly. In McAfee ePO, 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 MARSERVER, DXLBROKER, and TIESERVER tag, depending on the products installed.

Install the 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.

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 in its own McAfee® Linux Operating System (MLOS) distribution based on CentOS 6 (x86_64). To support different virtualization methods, initial scripts load different kernel modules depending on the virtualization platform detected. Visit www.mcafeelinux.org for more information.

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.

Considerations before upgrading to TIE server 3.0.0

Upgrading to TIE server 3.0.0 includes full database replication and high network utilization.

Important

The upgrade process to TIE server 3.0.0 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. McAfee 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.

TIE server upgrade

Considerations for the TIE server upgrade are:

- Make sure that the build numbers of the TIE server management extension, TIE platform, and TIE server packages match.
- You must upgrade the primary server first, then continue with all secondary servers. A secondary server fails if the primary server is still running an older version.

  Important

  The Primary and Secondaries servers upgrade process must be performed as a single effort, ideally under the same upgrade task. The Primary and Secondaries upgrade process should be completed within a six hours window to avoid replication reset in the Secondary servers which might lead to unstable situations.

- You can't upgrade the DXL client using a McAfee ePO deployment task on a TIE server system. You can only get an upgraded DXL client when installing a new TIE server.
- The TIE server help extension build version is expected to be different from the other components because it is built separately.

DXL

Considerations for the DXL are:

- If you plan to upgrade the DXL Brokers in your fabric, or if you plan to deploy new appliances with bundled TIE server and DXL Broker from an ISO file or OVF images, first upgrade all DXL extensions in McAfee ePO.
- For troubleshooting DXL Broker upgrades or installation, see the product documentation for DXL. The DXL platform package is not intended for the TIE appliance and isn't compatible with the TIE appliance.

McAfee Agent for MLOS

Considerations for McAfee Agent for MLOS are:

- If you upgrade TIE to 3.0.0 version, the McAfee Agent for MLOS is upgraded after you upgrade the server appliance.
- Do not install the McAfee Agent for Linux because it is not compatible.

Note

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

Upgrade paths

TIE server components (extension, platform, and service) are expected to run across the same build version in different appliances.

You don't need to perform an interim upgrade of TIE supported releases which didn't reach their EOL support. For example, if you have a 1.3.x TIE server version installed in your environment, it's a version that reached its EOL so you need an interim upgrade before you can upgrade to the latest available version. The upgrade path is:

- Upgrade from 1.3.x to 2.3.x
- Upgrade from 2.3.x to 3.0.0

Note

TIE server 1.2.1 reached its EOL support on December 31, 2017, and 1.3.0 did on August 15, 2018. See KB89670 for details. McAfee CTD reached its EOL support on December 31, 2018. For more information, see KB90296.

We recommend that you run the latest and greatest versions of McAfee ePO, McAfee Agent, and DXL. See KB90383 for details about McAfee ePO minimum supported extension versions. See KB90642 for details about McAfee Agent minimum supported versions for upgrades. 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 extension, the TIE platform, and the TIE package on the appliance.
- Always start with the Primary server, then continue with the other server instances you have.

Review the requirements before you upgrade to TIE 3.0.0

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 McAfee GTI (if enabled):
   - tieserver.rest.gti.mcafee.com
   - tie.gti.mcafee.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 3.0.0 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 McAfee ePO, 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 McAfee ePO, by selecting **Menu** → **Configuration** → **Server Settings** → **TIE Server Topology Management**, then click on each server to verify its status.

Download the TIE upgrade packages from Software Catalog

Download the software manually from the McAfee product download site or using the **Software Catalog** in McAfee ePO.

Task

1. Log on to the McAfee ePO server as an administrator.
2. Select **Menu** → **Software** → **Software Catalog**.
   The **Updates Available** tab lists the latest versions available for updates.
3. Search for **McAfee Threat Intelligence Exchange 3.0** to see the available packages.
4. Check in or download these packages:
   - TIE Platform
   - TIE Server
   - Server Management extension

   If **Software Catalog** doesn't show the TIE server packages, you can download and check in the packages manually.

Download the TIE upgrade packages manually

Download the TIE upgrade package from the McAfee product download site using your Grant number and registered Email address.

Task

1. Log on to the McAfee 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 McAfee ePO.
4. Log on to the McAfee ePO server as an administrator.
5. Select **Menu** → **Software** → **Master 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.

Deploy the Threat Intelligence Exchange products

To deploy the TIE products to the server appliance, create a client task for deployment on the McAfee ePO server.

Task

1. Install TIE server extension.
   a. Log on to the McAfee ePO server as an administrator.
   b. In McAfee ePO, select **Menu** → **Software** → **Extension**.
   c. Click **Install Extension**, select the extension file, then click **OK**.
   d. Check the details of the extension, make sure it matches the version of the server before you deploy upgrade packages, then click **OK** to complete the installation.
2. In McAfee ePO, select **Menu** → **Client Tasks** → **Client Task Catalog**.

3. Select **McAfee Agent**, then click **New Task**.
    a. Select **Product Deployment**, then click **OK**.
    b. Complete the new deployment information. For the **Target platforms** option, make sure that only **McAfee Linux OS** is selected.
4. Upgrade the packages in this order:
    a. TIE platform
    b. TIE server
5. Save and run the task on the TIE server.
   If any package doesn't deploy successfully, try to deploy them again. If they still are unsuccessful, collect logs and contact support. See KB82850.
6. If you already configured a registered server, verify connectivity.
    a. In McAfee ePO, select **Menu** → **Configuration** → **Registered Servers**.
    b. Select the server from **Database Servers**, then select **TIE Server**.
    c. From the **Actions** drop-down list, select **Edit**.
    d. After the edit is complete, click **Next** and **Save**.
7. Reboot the appliance so that the operating system picks up the new kernel provided by the new TIE platform package.
8. Upgrade the Intel microcode package on TIE servers that are running on bare metal. See KB90843 for details.

Verify the upgrade

Make sure the TIE components are configured correctly.

Note

If you enabled Active Response server during the TIE server deployment on the appliance, see the documentation for McAfee Active Response for information about verifying the upgrade of Active Response.

In McAfee ePO, 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 McAfee ePO, 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 McAfee ePO.

Note

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

Task

1. On the **Server Settings** page in McAfee ePO, 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 McAfee ePO 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 McAfee ePO servers, only TIE servers managed by a local McAfee ePO server are editable. For an environment with a single McAfee ePO server, managed TIE servers are displayed in a tree structure where the root is the instance operating in primary mode.
2. In McAfee ePO, 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 McAfee ePO 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 McAfee Agent service. Otherwise, it takes time for the policy to reach the appliance.
   See KB52707 for details about restarting the McAfee Agent service.

Edit the TIE server topology

Change the operation mode of your TIE server instances managed by the local McAfee ePO server.

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

Important

The server instances managed by another McAfee ePO appear disabled for editing.

Task

1. In the **TIE Server Topology Management** page, select the TIE server instance and click **Edit**.
   In a multiple McAfee ePO environment, only TIE servers managed by a local McAfee ePO 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 McAfee GTI and McAfee Advanced Threat Defense settings for the server.

Task

1. In McAfee ePO, select **Menu → Policy → Policy Catalog**.
2. Select **McAfee 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 McAfee to collect anonymous data about certificates, file paths, and hashes. This data helps McAfee learn about threats and prioritize what is allowed or blocked.
4. On the **McAfee Global Threat Intelligence** tab, enable McAfee GTI to get file reputation.
   McAfee GTI is used if the TIE server does not have reputation information for a file, or if the server is unavailable.

5. On the **Sandboxing** tab, enable Advanced Threat Defense to send file information for further evaluation.
   In the Advanced Threat Defense 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 Advanced Threat Defense. See KB87692 for details before enabling **Enforce Certificate Validation**.

   Important

   McAfee Cloud Threat Detection reached its EOL on December 31, 2018. See KB90296 for details. McAfee recommends that you migrate to Virtual Advanced Threat Defense.

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 ATP 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 Advanced Threat Defense. 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 McAfee ePO reports and dashboards.

Before you begin

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

Task

1. In McAfee ePO, 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 Threat Intelligence Exchange database, select this option only for the database that you want as the default.
   b. In the **Database Vendor** field, select **TieServerPostgres**.
   c. In the **Host name or IP address** field, enter the IP address of the system where you installed the server.
   d. 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

McAfee ePO 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 Threat Intelligence Exchange 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:
   - **McAfee DXL Broker** (if configured when deploying the appliance)
   - **McAfee DXL Client**
   - **McAfee Threat Intelligence Exchange Server**

- **McAfee Active Response Server** (if configured when deploying the appliance)

Note

If you configured the Active Response server, see the McAfee Active Response documentation for details and instructions about verifying its installation.

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 McAfee ePO 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 McAfee ePO 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 McAfee ePO through DXL. • Warn — The connection between the server instance and McAfee ePO is degraded. • Error — The server instance and McAfee ePO 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 McAfee 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 Advanced Threat Defense keystore can be opened if the Advanced Threat Defense certificate validation is enforced.
Extension Compatibility	This checkup verifies that the version of the McAfee ePO extension matches the version of each TIE server instance.

Checkup	Definition and status
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.
ATD Connection	This checkup verifies if the connection to Advanced Threat Defense 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 McAfee ePO 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 McAfee ePO, select **Menu** → **System Tree**, then select the checkbox for the TIE server. • Click **Wake Up Agents**. • On the **Wake Up McAfee Agent** page, select **Force complete policy and task update**, then click **OK**. This option sends the server properties from the TIE server appliance to McAfee ePO.

Problem	Troubleshooting
	• 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: **McAfee DXL Broker**, **McAfee DXL Client**, and **McAfee 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
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:
	`service cma status`
	`service dxlbroker status`
	`service tieserver-policy-listener status`
	`service tieserver status`

Access the log files

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

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

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

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

TIE server

- /var/McAfee/tieserver/logs/tieserver.log
- /var/McAfee/tieserver/logs/tieserver-start.log
- /var/McAfee/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

Active Response — /opt/McAfee/marserver/apache-tomcat/logs/catalina.out

McAfee 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 McAfee products.

Reconfigure the installation using scripts

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

Accessing the scripts

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

Script name	Description	Reboot?
change-hostname	Changes the host name of the current appliance. It restarts the McAfee Agent and the broker.	Recommended
change-services	Enables or disables the DXL broker and the TIE server services.	No

Script name	Description	Reboot?
	If the broker was initially disabled during first boot, the script prompts for broker configuration information.	
reconfig-dxl	Reconfigures the DXL port.	No
reconfig-ma	Reconfigures the McAfee 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 McAfee ePO and stores it in the TIE server.	No
reconfig-cert	Generates a new certificate and sends a signing request to McAfee ePO through the TIE server extension.	No

Troubleshoot the consolidated appliance deployment

For troubleshooting Active Response service, see the product documentation for McAfee Active Response at www.docs.mcafee.com.

Task

1. If the Active Response service is deployed on a Secondary or Reporting Secondary TIE server instance and doesn't work, verify that the TIE Primary server is up and running.
2. If the Active Response service is deployed on a Reputation Cache mode, it will not work until you transition the TIE server to a Secondary or Reporting Secondary operation mode.
3. You can access Active Response log files at /opt/McAfee/marserver/apache-tomcat/logs/catalina.out.

Manually upgrade McAfee Agent

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

Before you begin

Make sure that the McAfee Agent automatic upgrade failed after you deployed the TIE platform package.

Task

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

Remove the TIE software

Uninstall the TIE server software from your system.

If you have an appliance that contains TIE, DXL, Active Response components, but you only want to remove TIE, deploy an OVA with DXL before you remove the TIE component.

Task

1. Navigate to **Menu** → **Policy** → **Policy Catalog** → **McAfee Threat Intelligence Exchange Server Management x.x.x**, then click **Export** to download a file with the policies.
2. Navigate to **Menu** → **Software** → **Extensions**, then select a TIE server extension. Click **Remove**.
   Make sure you remove all the extensions you have deployed, either the **TIE Server Management** or the **Server Deployment** one.
3. Decommission all the TIE appliance instances you have deployed.
4. Remove the TIE appliances from the **System Tree**.
5. Remove the TIE server packages (platform and server) from the **Master Repository**.
   Make sure you remove all the packages from all the branches you have in the **Master Repository**.

COPYRIGHT

Trellix