Release Notes

McAfee Threat Intelligence Exchange 2.0.0

For use with McAfee ePolicy Orchestrator

Contents

About this release

This document contains important information about the current release. We strongly recommend that you read the entire document.

McAfee® Threat Intelligence Exchange (TIE) server 2.0.0 release includes these features and enhancements.

> McAfee® Threat Intelligence Exchange (TIE) server 1.0.x and 1.1.x ended availability on August 15, 2016, and are scheduled for end of support on August 15, 2017. To ensure protection, upgrade to TIE server 1.3.x or later. See End-of-life Policy for more details.

New features

This release of the product includes these new features.

- Manage the topology settings of the appliances — You can configure the operation mode of the appliances after the installation from the **Server Settings** page in McAfee ePO.
- Local threat intelligence reporting — The **Queries and Reports** page searches into threat details that include effective endpoint reputation for generating reports.
- New **Latest Local Reputation** column — It includes the most recent effective reputation computed by the endpoint by using local threat intelligence.
- Simplified **TIE Reputations** page — We show one column with consolidated reputation information and track the last detection rule applied at the endpoint.
- Data Management Cleanup task — You can now schedule a cleanup on the **Server Tasks** page in McAfee ePO.

Enhancements

This release of the product includes these enhancements.

Security

- Updated PostgreSQL configuration to allow only TLS 1.2 ciphers.
- Updated multiple packages, including PostgreSQL 9.3.14, OpenSSH 6.6.1p1, glibc 2.12-15, and dhclient 4.1.1-36.
- Cleanup of legacy MD5-hashed passwords from the TIE server database.
- Updated MLOS kernel to version 3.18.39-2.
- Updated OpenSSL libraries to version 1.0.2i with FIPS Crypto-module.
- Optional authentication of the McAfee ePO host fingerprint when setting up the TIE server.
- Updated HttpClient library to 4.5 version to provide better certificate identification validation when retrieving information for VirusTotal.
- Hardened hash validation in internal APIs to filter malformed DXL messages.
- Added more mechanisms to authenticate Advanced Threat Defense servers.
- SSH version string no longer returned by the SSH server to harden vulnerability scanner.

Updated product design and encryption internals to comply with Federal Information Processing Standard 140-2 (FIPS) and Common Criteria (CC) certification requirements.

Installation and configuration

- Automatic configuration of the McAfee ePO registered server database for dashboard functionality.
- Improved workflow and coordination via appliance configuration managed by McAfee ePO, and split installation and configuration steps.
- Easy reconfiguration and management of operation modes.

Data management

- Automatic database size management and cleanup of prioritized relevant data to keep data under the configurable threshold.
- Automatic and manual purge via McAfee ePO.

File type support and certificate attributes

- Richer reputation attributes for files on the **File Search** tab, and greater visibility into file reputation displayed on the **Composite Reputation** column.
- Filtering of file types based on incoming reputations reported by McAfee® Advanced Threat Defense and McAfee GTI.
- Extended file type support for file reputations by enabling different file types for keeping reputations in the TIE server, and by configuring which file types are sent to Advanced Threat Defense for further analysis.
- Description of the latest rule applied for each file, filtered by column or informed in reports.
- Display **GTI certificate revocation** status on the **Certificate Search** tab.

Sample submission to Advanced Threat Defense

- Improved logs to troubleshoot covering file sample submission.
- Additional processes to authenticate Advanced Threat Defense servers. See KB87692.

Health and replication topology management

- Setting the logging level and enable performance metrics logging from McAfee ePO policy for the TIE server appliance.
- Hiding files and certificates on default search pages that don't have metadata available when you open the **TIE Reputations** page.
- Display of information about the last time the reputation from each provider was updated on the file and certificate details pages .
- Checking the master-slave connectivity and health status, **DXL connectivity**, **GTI connectivity**, and database replication checks on the **TIE Server Topology Management** page.

Resolved issues

These issues are resolved in this release of the product.

Server extension

- The download for exported reputations now doesn't timeout when the results exceed the maximum size configured in DXL (1140414).
- The query "TIE server malicious or unidentified files by McAfee GTI reputation in last month" now includes the trust level criteria. For detailed information, see KB87244 (1138909).
- You can now use the host name to create a registered database in McAfee ePO (1133262).

Server

- File names that contain Unicode characters are now preserved when TIE submits them to Advanced Threat Defense for a dynamic analysis (1135905).
- When receiving process reputation from Advanced Threat Defense, the file reputation now includes an IP address aggregate as Enterprise reputation (1151622).

Appliance

- When McAfee GTI isn't available, you now receive a warning message that it wasn't possible to refresh McAfee GTI reputation (1145745).

Upgrade to 2.0

Follow these instructions to upgrade your software to version 2.0.0.

Before you begin

Run a vacuum analyze task for database maintenance before the upgrade. See KB86092.

For troubleshooting issues during the upgrade, see KB84856.

The DXL Java Client in the TIE appliance is embedded and is automatically upgraded when the TIE server is upgraded.

Upgrading the TIE server doesn't make your version of the product FIPS-compliant. See the related documentation for installing TIE server in FIPS mode.

When upgrading, consider the following:

- To minimize network disruption, schedule maintenance downtime for the upgrade.
- First upgrade the extension in McAfee ePO, then the TIE platform package and the service on the TIE appliance.
- Upgrade the McAfee® Agent to 5.0.3 version or later before upgrading the TIE server appliance.
- If you upgrade from 1.2.0 or earlier, you must upgrade first to 1.2.1, then to 2.0.0.
- If you upgrade TIE from a version earlier than 1.2.1, see the release notes for TIE server 1.2.1 and KB86128.
- If you are prompted to upgrade the TIE client and the DXL Broker and Client, see the release notes of those products.
- The builds between the extension and the package must match.

Task

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

1 Upgrade the product extension for TIE server 2.0.0 on the McAfee ePO server.

   a In McAfee ePO, select **Menu** | **Software** | **Extensions**.

   b Click **Install Extension**, select **TIE Server Management**, then click **OK**.

   If your DXL extension is not compatible with TIE server 2.0.0, you are prompted to upgrade, which you must do before continuing. For instructions, see the *McAfee Data Exchange Layer Release Notes*.

2 Create a snapshot of your virtual machine (master instance, if applicable) on the VMware vSphere client. For instructions, see the VMware vSphere documentation.

Use one of these methods to download the product files:

- **Software Manager** — Contains the Threat Intelligence Exchange 2.0.0 components. Select each product for viewing and installing the component files.
- **Manual** — Download the Threat Intelligence Exchange 2.0.0 files from the McAfee product download website, then check in the files to the Master Repository in McAfee ePO.

3 Check in the Threat Intelligence Exchange platform and server 2.0.0 packages to the Master Repository in McAfee ePO.

   a In McAfee ePO, select **Menu** | **Software** | **Master Repository**.

   b Click **Check in Package**, select **Package type**, then click **Next**.

   c On the **Package Options** tab, check the details of your package. Click **Save** to complete the check-in.

Perform these steps for each package that you want to check in. First check in the platform package, then the server package.

Tasks

- *Deploy the Threat Intelligence Exchange products* on page 5
  To deploy the TIE products on the server appliance, create a client task for deployment on the McAfee ePO server.
- *Verify the installation* on page 6
  After upgrading the TIE components, verify the installation.

Deploy the Threat Intelligence Exchange products

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

> **Before you begin**
> Make sure that you have full connectivity in the DXL fabrics. In McAfee ePO, select **Menu** | **Data Exchange Layer Fabric**, then click the **Refresh** button. All your brokers must be listed in green.

For troubleshooting DXL Broker upgrades or installation, see the product guide and release notes for DXL.

Task

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

1 In McAfee ePO, select **Menu** | **Policy** | **Client Task Catalog**.

2 Select **McAfee Agent**, then click **New Task**.

3 Select **Product Deployment**, then click **OK**.

4 Complete the new deployment information. For the **Target platforms** option, make sure that only **Linux OS** is selected.

5 Create a task for each package. When deploying the TIE server package, make sure to complete the master instance first. Packages must be upgraded in this order:

   a TIE platform

   b TIE server

6. Save and run the task on the TIE server.

   If the TIE Platform package doesn't deploy successfully, you can't continue. See KB82850.

7. If you have already configured a registered server, follow these steps to verify connectivity.

   > If you are upgrading from 1.2.1, you must perform this step to reload the database driver.

   a. In McAfee ePO, select **Menu | Registered Servers**.

   b. Select the server from **Database Servers**, then select **TIE Server**.

   c. In the **Actions** drop-down list, select **Edit**.

   d. After the edit is complete, click **Next** and **Save**.

8. Reboot the appliance so that the operating system picks up the new kernel provided by the new TIE platform package.

Verify the installation

After upgrading the TIE components, verify the installation.

Task

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

1. In McAfee ePO, select **System Tree**, select the TIE server name, then click the **Products** tab.

   Repeat this step for each server instance you have under **System Tree**.

2. Verify that the TIE server component is listed with the latest version number.

3. In the **System Tree**, make sure that the TIESERVER tag is applied to the system.

4. Verify the connectivity to the DXL fabrics. In McAfee ePO, select **Menu | Data Exchange Layer Fabric**, then click **Refresh**.

   The brokers in your environment must be listed in green.

5. In McAfee ePO, select **Menu | Server Settings | TIE Server Topology Management** and verify that your server instances are configured correctly.

For troubleshooting, use the Minimum Escalation Requirements (MER) tool to collect product data from the server and contact technical support. See KB82850.

Known issues

See KB85172 for a list of known issues.

Find product documentation

On the **ServicePortal**, you can find information about a released product, including product documentation, technical articles, and more.

Task

1. Go to the **ServicePortal** at https://support.mcafee.com and click the **Knowledge Center** tab.
2. In the **Knowledge Base** pane under **Content Source**, click **Product Documentation**.
3. Select a product and version, then click **Search** to display a list of documents.

0-00